Web Service Configuration

To use the features of dynamic revocation, number of accesses and number of prints (additional access rights control), you should configure the web service and SQL first. Please follow the steps as below:

1. Configure the Web Service on your on-premise AIP server.

- a) Log on AIP server as Administrator.
- b) Download the Web Service zip from: <u>The Web Service zip (for X86)</u> <u>The Web Service zip (for X64)</u>
- c) Unzip the Web Service zip and get the fxrmsext from it.
- d) Copy the fxrmsext to C:\inetpub\wwwroot_wmcs.



- e) Run "Internet Information Services" (IIS).
- f) Right-click "_wmcs", and then choose "Add Application...".



- g) Input the following information into the **Add Application** dialog box.
 - Alias: fxrmsext
 - Application Pool: DRMSAppPool1

Physical path: C:\inetpub\wwwroot_wmcs\fxrmsext

	Add Application	? X
Site name: Default Web Site Path: /_wmcs		
<u>A</u> lias:	App <u>l</u> ication pool:	
fxrmsext	_DRMSAppPool1	S <u>e</u> lect
Example: sales		
<u>P</u> hysical path:		
C:\inetpub\wwwroot_wmcs\fxrm	nsext	
Pass-through authentication		
<u>C</u> onnect as Test Settings		
Enable Preload		
	ОК	Cancel

h) To avoid repeated authentication, we should disable the Windows Authentication and enable the Anonymous Authentication. Click "fxmsext" in Connections Pane, and then double-click "Authentication".

NOTE: For data communication security, PDFs will be encrypted with AES algorithm by default.



i) Enable the "Anonymous Authentication" and disable the "Windows Authentication".

9			Inte
C DRS > Sites	Default Web Site _wmcs fx	rmsext 🕨	
File View Help			
Connections	Authentication		
 ▲ ● DRS (FRMS\administrator) ▲ ♀ DRS administrator) ▲ ♀ Default Web Site ▲ ♀ Default Web Site ▲ ♀ Default Web Site 	Name Anonymous Authentication ASP.NET Impersonation Forms Authentication Windows Authentication	Status Enabled Disabled Disabled Disabled	Response Type HTTP 302 Login/Redirect HTTP 401 Challenge
▷ artification			

2. Configure the SQL.

- a) Navigate to C:\inetpub\wwwroot_wmcs\fxrmsext.
- b) Right-click "Web.config" file -> "Open with" -> "Notepad".



c) If you want to log on to the SQL Server through Windows Authentication, you just need to alter the SQL Server information by inputting the IP address or computer name and then saving the change.

```
<appSettings>
    <add key="MyDB"
    value="Server=SQL2005; DataBase=RMSExtService;
Integrated Security=SSPI; Persist Security Info=False" >
        </add>
```

NOTE: If the computer name include '-', please ensure you are using SQL 2012 version or higher.

d) If you want to log on to the SQL Server through SQL Server Authentication, please follow the steps:

- i. Copy "Server=SQL2005; DataBase=RMSExtService; User ID=myUsername; Password=myPassword".
- ii. Paste and replace "Server=SQL2005; DataBase=RMSExtService; Integrated Security=SSPI; Persist Security Info=False".



- iii. Alter the SQL Server information. You can input the IP address or the computer name.
- iv. Alter the "User ID" and "Password".
- v. Save changes.
- e) Create the data base and tables.
 - i. Log on to the SQL Server as Administrator.
 - ii. Get the .sql file from the <u>Web Service zip</u> you downloaded before.
 - iii. Double-click this file to create the database and tables, and then click "Execute".



- f) Grant AIP administrator the database operations rights.
 - i. Open "Internet Information Services" (IIS).
 - ii. Click "Application Pools" in Connections Pane. Then you can get the account information from Identity column.

8]					Internet Informatio	on Services (IIS) Manager
	tion Pools					
File View Help						
Connections	Application This page lets you view and applications.	1 POOls d manage th	e list of applica	tion pools on the se	erver. Application pools are ass	ociated with worker processes, cor
⊿ Sites	Filter:	- 🛒 Go	- 🕁 Show All	Group by: No G	rouping •	
⊿ 🌍 Default Web Site	Name	Status	.NET Fram	Managed Pipel	Identity	Applications
⊿ - 🔐 _wmcs	@.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
⊳-@ admin	.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
ertification	DRMSAppPool1	Started	v4.0	Classic	FRMS\rms_service	7
 p-gr decommission p-gr disconsing p-gr licensing p-gr fixmsext aspnet_client 	DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	2

- iii. Open SQL Server management.
- iv. Navigate to "Security" -> "Logins".
- v. Check if the AIP administrator account is listed.



If yes, skip to Step vi. If not, right-click "Logins", then click "New Login".

🧏 CreateDataba	seRMSExtService.sq	I - DRS.RMSExtService
File Edit View Project	Debug Tools Wind	dow Help
i 🛅 • 🛅 • 📂 🔒 🥔	일 New Query 🏻 👔 🕎	5 📸 🌇 X 🖬 🛍 4
: ഈ 맨 RMSExtService	- 🕴 Exe	cute 🕨 Debug 🔲 🧹
Object Explorer		- ₽ ×
Connect - 📑 🛃 🔳 🦷	7 🛃 🎿	
🕀 📔 WSS_Loggi	ng	^
🖃 🧰 Security		
Logins	New Login	in##
2, ##	Filter	##
👗 FR	-	-
🐣 FR	Start PowerShell	-
A FR	Reports •	
A NT	Refresh	
Å NT Serv	ice\MSSQLSERVER	·
A NT SER	VICE\ReportServer	
A NT SER	VICE\SQLSERVERAGENT	_
A NT SER	/ICE\Winmgmt	=
🐣 sa	-	
🕀 🧰 Server Role	s	
Gredentials Contouran	hic Providers	
		×
		· · · · · · · · · · · · · · · · · · ·

Input the Login name, click **OK**.

8	Login -	New	_ 🗆 X
Select a page	🔄 Script 🔻 📑 Help		
Server Roles		FRMS\ms service	Search
Securables	Windows authentication		
🚰 Status	SOL Server authentication		
	Password:		
	<u>C</u> onfirm password:		
	Specify old password		
	Old password:		
	Enforce password policy		
	Enforce password expiration	tion	
	User must change passv	vord at next login	
	 Mapped to certificate 		V
	O Mapped to asymmetric key		×
Connection	Map to Credential		✓ <u>A</u> dd
Server: DRS	Mapped Credentials	Credential Provider	
Connection: sa			
View connection properties			
Progress			Remove
Ready	Default <u>d</u> atabase:	master	~
	Default language:	<default></default>	~
		01	Cancel

vi. Grant AIP administrator as the database owner.

B	Lo	gin Properties - FR	MS\rms_service		_	x
Select a page General Server Boles	Script	🕶 🎼 Help				
Car Mapping Securables Status	Users maj	pped to this login: Database Report Server Record Server TemoDR RMSEd Service TemoDR RMSEd Service Appli Search_Service_Appli Search_Service_Appli Search_Service_Appli Secure_Store_Service Share Point_AdminCon	User FRMS\ms_service	dbo	ema	× =
Connection	Database	role membership for: RMSE	xtService			
Server: RMS Connection: FRMS\administrator Wew connection properties	db_ac db_ba db_da db_da db_da db_da db_da db_ov	cessadmin lockupoperator tareader tawriter Iladmin mydatareader roydratawriter wrer				
Progress Ready	db_se ✔ public	cuntyadimin				
				ОК	Ca	ncel Activ

- g) Set up the firewall.
 - i. In SQL Server Configuration Manager, expand SQL Native Client Configuration, and click "Client Protocols" and right-click "TCP/IP Properties" to get the default port.

	Sql	Server Configuration	Manager			x
File Action View Help						
🗢 🄿 🖄 🖾 🗟						
SQL Server Configuration Manager (Local)	Name Shared Memory	Order 1	Enabled Enabled	7		
J. SQL Server Network Configuration (32) P SQL Native Client 11.0 Configuration (32) SQL Native Client 11.0 Configuration Image: SQL Native Client 11.0 Configuration	उँ TCP/IP उँ Named Pipes	2 3	Enabled Enabled TCP/IP Properties 1433 Yes 30000 1000	s ? ×		
< <u> </u>		Default Port Default port on which	n connection will be mad	le Apply Help		

ii. Run "Windows Firewall" and click "Advanced settings".

		Windows Firewall			
۲	-) -> - 🕆 🔗 • Control Par	nel 🔸 System and Security 🔸 Windows Firewall	Search Control Panel		
	Control Panel Home	Help protect your PC with Windows I	Firewall		
	Allow an app or feature through Windows Firewall	Windows Firewall can help prevent hackers or m Internet or a network.	alicious software from gaining access to your PC through the		
8	Change notification settings	🕑 Domain networks	Connected 📀		
0	Turn Windows Firewall on or off	Networks at a workplace that are attached to a	domain		
0	Restore defaults	Windows Firewall state:	On		
	Advanced settings Troubleshoot my network	Incoming connections:	Block all connections to apps that are not on the list of allowed apps		
		Active domain networks:	frms.com		
		Notification state: Do not notify me when Windows Firewall blocks a new app			
		Private networks	Not connected \overline{igodot}		
		Guest or public networks	Not connected \overline{igodot}		
	See also				
	Action Center				
	Network and Sharing Center				

iii. Click "Inbound Rules".

<i>\</i>	Windows Firewall with Advan	ced Security	
File Action View Help			
🗢 🌳 🖄 🖬 🗟 🖬			
Windows Firewall with Advance	Inbound Rules		Actions
Intoound Rules Ornection Security Rules Monitoring	Name SQL1433 Teamviewer Remote Control Application Teamviewer Remote Control Application Teamviewer Remote Control Service Cont- Ache Content Retrieval (HTTP-In) TeamchCache Dest Discovery (WSD-In) COM+ Network Access (DCOM-In) COM+ Network access (DCOM-In) COM+ Remote Administration (DCOM-In) COM+ Remote Administration (DCOM-In) COM+ Networking - Destination Unreacha Core Networking - Dynamic Host Config Core Networking - Dynamic Host Config Core Networking - IPHTTPS (TCP-In) Core Networking - IPHTTPS (TCP-In) Core Networking - Multicast Listener Po Core Networking - Multicast Listener Rep Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A C	Group ∧ Group Group Group	Inbound Rules ▲ Image: Second Seco

iv. Click "New Rule...".

@	Windows Firewall with Advan	ced Security	
File Action View Help			
🗢 🤿 🙇 🖬 🗟 🖬			
Windows Firewall with Advance Inbound Rules Connection Security Rules Monitoring	Inbound Rules Name SQL1433 Teamviewer Remote Control Application Teamviewer Remote Control Service Teamviewer Remote Control Service BranchCache Content Retrieval (HTTP-In) BranchCache Hosted Cache Server (HTT BranchCache Hosted Cache Server (HTT BranchCache Access (DCOM-In) COM+ Remote Access (DCOM-In) Core Network access (DCOM-In) Core Networking - Destination Unreacha	Group ∧ BranchCa BranchCa BranchCa BranchCa COM+ Ne COM+ Ne COM+ Re	Actions Inbound Rules Inbound Rules
< <u> </u>	Core Networking - Destination Unreacha Core Networking - Dynamic Host Config Core Networking - Internet Group Mana Core Networking - Internet Group Mana Core Networking - IPHTTPS (TCP-In) Core Networking - IPHTTPS (TCP-In) Core Networking - Multicast Listener Do Core Networking - Multicast Listener Rep Core Networking - Nulticast Listener Rep Core Ne	Core Netv Core Netv	

v. Select "Port" and then click "Next".

@	New Inbound Rule Wizard
Rule Type Select the type of firewall rule to cre	eate.
Steps: Rule Type Protocol and Pots Action Profile Name	What type of rule would you like to create?

vi. Select "TCP", then select "Specific local ports", type the SQL port number, and click "Next".

2	New Inbound Rule Wizard	x						
Protocol and Ports	Protocol and Ports							
Specify the protocols and ports to v	which this rule applies.							
Steps:	Does this rule apply to TCP or UDP?							
 Rule Type Protocol and Ports Action Profile Name 	Does this rule apply to TCP or UDP? UDP Does this rule apply to all local ports or specific local ports? All local ports Specific local ports: 1433 Example: 80, 443, 5000-5010]						
	< Back Next > Car	ıcel						

vii. Select "Allow the connection", and then click "Next".

<i> </i>	New Inbound Rule Wizard	x
Action		
Specify the action to be taken w	hen a connection matches the conditions specified in the rule.	
Steps:		
Rule Type	What action should be taken when a connection matches the specified conditions?	
Protocol and Ports	Allow the connection	
Action	This includes connections that are protected with IPsec as well as those are not.	
Profile	Allow the connection if it is secure	
Name	This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize Block the connection	1

viii. Choose when to apply the rule.



ix. Specify the name and description of the rule and then click "Finish".