

## **ReportPlus Web 5 Kerberos Sign-on Configuration**

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY EXPRESS REPRESENTATIONS OF WARRANTIES. IN ADDITION, INFRAGISTCS, INC. DISCLAIMS ALL IMPLIED REPRESENTATIONS AND WARRANTIES, INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTURAL PROPERTY RIGHTS.

ReportPlus<sup>™</sup> Web 5.0 –Kerberos Sign-on Configuration 1.0.

All text and figures included in this publication are the exclusive property of Infragistics, Inc., and may not be copied, reproduced, or used in any way without the express permission in writing of Infragistics, Inc. Information in this document is subject to change without notice and does not represent a commitment on the part of Infragistics, Inc. may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents except as expressly provided in any written license agreement from Infragistics, Inc.

Infragistics, Inc. and SharePlus are trademarks of Infragistics in the United States and/or other countries.

This document also contains registered trademarks, trademarks and service marks that are owned by their respective owners. Infragistics, Inc. disclaims any responsibility for specifying marks that are owned by their respective companies or organizations.

©2015 Infragistics, Inc. All rights reserved.



# **Table of Contents**

Table of Contents	3
Requirements	4
Configuration Steps	5



### Requirements

To successfully configure a Kerberos based single sign-on, you need **Windows Identity Foundation** installed on the Web server.

#### Validation

If you want to validate that WIF is installed on the server, you can search for this key in the registry:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsIdentityFoundation\setup\v3.5\

#### Installation

In case you don't have it installed then you can download an installer from here:

http://www.microsoft.com/en-us/download/details.aspx?id=17331



## **Configuration Steps**

#### 1. Server delegation

The first step is to grant delegation rights from the Web server to the SQL Server Analysis Services (SSAS). In order to do this you should use the Server Principal Name (SPN) of the SSAS machine and set it up in the Active Directory (AD) server.

- i) Go to Active Directory Server.
- ii) Open the Active Directory Users and Computers console, find *WEBSERVER* computer, rightclick on it and select *Properties*.

📃 Active Directory Users and Computers					
File Action View Help					
🗢 🔿 🖄 📅 🖌 📋  🕻	i Q 🗟	🛿 🖬 🙁 🐮	7 🗾 🍇		
Active Directory Users and Comput	Name 🔺			Туре	
🗄 🚞 Saved Queries	N 5010650	QL2T		Computer	
🖃 🏭 rplus1.local	👰 SQL			Computer	
🕀 🧮 Builtin	💽 WEBSEP	VEN		Computer	
Computers	🜉 WIN81	Add to a group		Computer	
🛨 🧾 Domain Controllers		Disable Account			
ForeignSecurityPrincipals		Reset Account			
🛨 🔛 Users		Move			
		Manage			
		All Tasks 🔹 🕨			•
Jopens the properties dialog box for the c	urrent select	Cut			
		Delete			
		Delete			
		Properties			
		Help			

iii) Navigate to the *Delegation* tab and select the *Trust this computer for delegation to specified services only* option.

WEBSERVER Properti	25				? ×	
General	Operating System			Member Of		
Delegation	Location	Manageo	іВу	Dial-	in [	
Delegation is a secu behalf of another use	Delegation is a security-sensitive operation, which allows services to act on behalf of another user.					
C Trust this comput	ter for delegation to :	ion anu service (k	arbaros r	ulu)		
<ul> <li>Trust this compute</li> </ul>	Inst this computer for delegation to any service (Nerberos only)					
	I rust this computer for delegation to specified services only					
Use <u>K</u> erbero	O Use Kerberos only					
Use any auth	nentication protocol					
<u>S</u> ervices to whic	h this account can p	present delega	ated cred	entials:		
Service Type	User or Computer	Port	Service	Name	-	
browser	SQL.rplus1.local					
HOST	SQL.rplus1.local					
http	SQL.rplus1.local					
MSSQLSvc	SQL.rplus1.local					
MSSQLSvc	SQL.rplus1.local	14		_		



iv) Use the Add button to specify which back-end servers can be accessed by the accounts.

WEBSERVER Prop	erties				?	×	
Add Services					? >	3	
To allow services users or compute	to be delegat rs, and then cl	ed for a user or ick the service	computer s.	r, select the	e appropriate		
To select one or Users or Compute	more user or c ers.	omputer names	;, click	Users or C	Computers		
Available service Service Type	s: User or Com	outer Po	ort Serv	vice Name	Domain		
	Select Use	s or Comput	ers				? ×
	Select this	object type:					
	Users, Cor	nputers, Built-in	i security p	orincipals, c	or Other objec	ts	Object Types
	, From this lo	cation:					
	rplus1.loca	ıl					Locations
	Enter the o	hiect names to	select (ex	amples);			
	SSAS SP	I HERE		,			Check Names
	Advanc	ed			[	OK	Cancel
			1	1			
	OK	Cancel	<u> </u>	pply	Help		

v) (Only SSAS Server) Enable a specific service.

In case you want to configure a SSAS Server, you should ensure that the **MSOLAPSvc.3** service is selected.

If you can't find that service listed, that's because a Service Principal Name (SPN) must be created in the Active Directory (AD) for the Analysis service. You can make that with the following command:

setspn -s MSOLAPSvc.3/<serverFQDN> <server>

A real use case should be similar to the following example:

setspn -s MSOLAPSvc.3/SQL.rplus1.local SQL

If you prefer to do it manually, you can do it by launching *ADSIEdit* on the DC, locating the SQL computer object, going to its properties and editing the *ServicePrincipalName* attribute. **MSOLAPSvc.3/SQL.rplus1.local** was the value we added in the example above.

After that you should be able to grant trust for delegation to the service, in a screen similar to the following one:

WEBSERVER Pr	operties ? 🗙
Add Services	? 🗙
To allow servic users or compu To select one Users or Comp	ces to be delegated for a user or computer, select the appropriate uters, and then click the services. or more user or computer names, click Users or Computers uters.
Available servi	ces:
Service Type	e User or Computer 🛛 Port Service Name Domain 🔺
mesve	SQL
messenger	SQL
msdtc	SQL
msiserver	SQL
MSOLAPSvo	2.3 SQL
MSSQLSvc	SQL.rplus1.local
MSSQLSvc	SQL.rplus1.local 14
netdde	SQL
	Select All
	OK Cancel
	OK Cancel Apply Help

#### 2. Claims to Windows Token Service

- i) Open a cmd prompt on the server as System Administrator.
- ii) Execute the following command:

sc config "c2wts" depend= CryptSvc

- iii) Navigate to *C*:\*Program Files*\*Windows Identity Foundation*\*v3.5*\ and open the **c2wtshost.exe.config** file with a text editor.
- iv) Add NT AUTHORITY\Network Service, NT AUTHORITY\Local Service
- v) Find the Claims to Windows Token Service in the Services console (run services.msc to open the console).
- vi) Double-click on it. Then, on the *General tab*, change the *startup type* to **Automatic**, then navigate to the *Log On* tab and select *LocalSystem*.
- vii) Right-click on the service and select Start.

#### 3. Application configuration.

After configuring server's delegation you need to modify ReportPlus Web application configuration in order to support Single Sign-on.

- i) Go to ReportPlus Web application physical path and open the **Web.config** file. Normally, the path is: *C:\inetpub\wwwroot\RPlusServer*
- ii) Find the tag *security* and add the following two properties in that line:

```
useRoleBasedModel="false"
useClaims2WindowsTokenService="true"
```

iii) Add the mappings for SSAS SPN under the ServerNameMapping tag, inside security.

The complete security section configuration in the **Web.config** file should be similar to this:

<security requiresSSL="false" useRoleBasedModel="false" useClaims2WindowsTokenService="true" secureStorageConnectionString="..connectionstring..">

<serverNameMapping>

<map originalName="10.20.37.248" targetName="SQL.rplus1.local"/>

</serverNameMapping>

</security>

