



RPA User Guide

Copyright © 2014 Radical Blue Gaming, Inc. All rights reserved.

All trademarks used within this document are the property of their respective owners. No part of this work may be reproduced in whole or in part, in any manner, without the prior written permission of Radical Blue Gaming, Inc.

Radical Blue Gaming, Inc.

85 Keystone Avenue Suite F
Reno, Nevada 89503

call us: +1.775.329.0990

visit us: www.radblue.com

drop us an email: sales@radblue.com

Need help?

At the RadBlue forum you can find the latest release information, report issues, get your questions answered, and submit suggestions for improving our products. Simply log on to:

<http://radblue.mywowbb.com>

Find out more about the GSA protocols

If you want to find out more about the Gaming Standards Association and the work being done in the area of protocol standardization for the gaming industry, we encourage you to visit their website at www.gamingstandards.com.

Contents

RPA User Guide	1
About RadBlue	3
Contents	5
Chapter 1: Installing RPA	13
About the RPA Installation	13
Pre-installation Requirements	13
Computer Requirements	13
Install RPA on Windows	14
Install RPA on Linux	15
Uninstall RPA	16
Chapter 2: Getting Started	17
About RPA	17
Using SSL	18
Additional Resources	18
Supported GSA Versions	18
Review the RPA User Interface	19
Menu Bar (1)	20
Tools	22
Help	22
Layout Tabs (2)	22
Control Panel (3)	22
Object Windows (4)	23
Floor Tabs (5)	23
About the Garbage Collector	24

RPA Configuration Overview	24
Configure RPA for G2S	25
Configure the EGM	27
Configure the G2S Host	27
Configure RPA for S2S	28
Configure S2S Edge Server	30
Configure the S2S Central Server	30
Configure RPA Options	31
Configure RPA to Run as RGS	31
Install a Custom Schema File (Optional)	32
Add a New Schema to RPA with Disruptive Filters (Optional)	32
Force Stronger Encryption (Optional)	33
Configure RPA with Multiple EGMs and Hosts	34
Configure RPA for Multiple Hosts	35
Configure EGMs to Communicate with RPA	38
Add Additional Hosts in the EGM through the setCommChange Command	39
View Message Activity for Multiple EGMs and Hosts	41
Chapter 3: Using RPA	43
RPA Layout	43
Configuring the RPA	44
View Summary Statistics	45
View Summary Received Commands	45
View Errors	46
Chapter 4: Using Disruptive Filters	49
About Disruptive Filters	49
View Disruptive Filters	50

Edit a Filter Set	50
Change the Filter Set Name and Description	50
Change the Schema Used for Disruptive Filters	51
Enable/Disable Individual Filters	51
Configure Automatic Filters	52
Using Automatic Filter Control	54
Configure Commands and Events for Interactive Filters	55
Using the Interactive Filter Control	56
Chapter 5: Available Filters	59
About Available Disruptive Filters	59
Add Valid Attribute Filter (G2S)	60
Add Valid Attribute Filter Code Examples	61
Class	61
Command	61
g2sBody	62
g2sMessage	62
Sub-Element	63
Add Valid Element Filter (G2S)	63
Add Valid Element Filter Code Examples	64
Class	64
Command	65
g2sBody	66
g2sMessage	66
Sub-Element	67
Application-Level Error Filter (G2S)	68
Attribute Replacement (G2S)	68

Change Host ID/EGM ID Filter (G2S)	70
Comm Host List Filter (G2S)	71
CommsOnline Filter (G2S and S2S)	71
Duplicate Message Filter (G2S)	72
Edit Message Filter (G2S)	73
Event Data Filter (G2S)	74
Message Delay Filter (G2S)	75
Message-Level Error Filter (G2S)	77
Resend Filter (G2S and S2S)	78
Retry Filter (G2S and S2S)	79
Set Comm Change Filter (G2S)	80
S2S Header Filter (S2S)	81
S2S Reply to System Filter (S2S)	81
Toggle Session Type Filter (G2S)	82
Chapter 6: Using the Message Transcript	83
Working with the Message Transcript	83
Transcript Column Headers	85
Filter Transcript Messages Using the Quick Filter	86
What Are You Looking for in the Transcript?	86
Load Messages into the Transcript	87
Compare Messages in the Transcript	88
Filter Messages in the Transcript	89
Search the Content of Transcript Messages	90
View Command Objects through the Transcript	91
View the Event Report	92
Add a Comment to a Transcript Message	93

Export Message Content to Excel	94
Export Transcript Entries	95
Clear the Transcript Display	96
Clear the Transcript Database	96
Chapter 7: Using the Transcript Analysis Report	97
About the EGM Transcript Analysis Report	97
Generate the Transcript Analysis Report	98
Navigating the Transcript Analysis Report File	98
Sample Transcript Report	99
Device Commands	99
Device States	99
Events	99
G2S ACKs That Have Errors	99
Messages	100
Meters	100
Sessions	101
Transcript	101
Transcript Summary	102
Chapter 8: Using the Advanced Transcript Analyzer	103
About the Advanced Transcript Analyzer	103
Review the Advanced Transcript Analyzer Layout	104
Get Started Analyzing Command Data	105
Filter Advanced Transcript Analysis Report	107
Generate a PDF of the Advanced Transcript Analysis Report	108
Chapter 9: Using the Multicast Transcript	111
Working with the Multicast Transcript	111

Multicast Transcript Column Headers	111
Filter Multicast Transcript Records Quickly	112
Load Messages into the Multicast Transcript	112
Receive Real-Time Data in the Multicast Transcript	113
View the Content of a Multicast Message	113
Search the Content of a Multicast Message	114
Clear the Multicast Transcript Display	114
Clear the Multicast Transcript Database	114
Clear the Multicast Listeners	115
Chapter 10: Using Watchables	117
About Watchables	117
About XPath Expressions	118
XPath Expression Format	118
Sample XPath Expressions	118
XPath References	118
Boolean Expression Usage	119
Clear All Watchable Data	119
Copy a Watchable	120
Create a New Watchable	121
Delete a Watchable	121
Edit a Watchable	122
Select Attribute(s) to Track in Watchables	123
View a Watchable	124
Appendix A: Troubleshooting	127
About the Debug Console	127
Clear the Debug Log Display	128

Filter Debug Messages	128
What to Do If You Can't Resolve an Error	129
Appendix B: Customizing RPA	131
Configuring Desktop Options	131
Configuring RPA Engine Options	132
General	132
Transport	133
Transcript Filters	135
Database	135
G2S Endpoints	136
Edit EGM Endpoints	137
Delete a G2S Endpoint	137
Set EGM Endpoint Timeout	137
Add a G2S Host Endpoint	138
Edit a G2S Host Endpoint	139
S2S Endpoints	139
Edit the S2S Client Endpoint	141
Edit the S2S Host Endpoint	142
Configure Security Options	143
Configure General Security Options	144
Enable and Configure OCSP	145
Create or Import a Signed Certificate	146
Load a Self-Signing Certificate	147
Use SCEP to Request a Certificate	149
Load a Third-Party Certificate	151
Obtain a Signed Certificate Using Microsoft Active Directory Certificate Services	153

Manage Key Store Options	156
Import a PKCS #12 File	157
Configure Filter Options	158
Add a Filter Set	161
Edit a Filter Set	164
Set or Clear the Default Filter	164
Delete a Filter Set	164
Configure License Manager Options	165
Load a New License File	166
Index	167

About the RPA Installation

RPA is available for both [Windows](#) and [Linux](#) operating systems.

Pre-installation Requirements

1. If you are using a student license, note that the computer you install RPA on must have a network connection. If it does not, you will not be able to send multicast commands successfully.
2. If you have a previous version of the tool installed, remove it before installing the new version.
3. You must have the RPA license file on your computer prior to installing RPA. If you are using a special version of RPA , you must have a license for that version. If you have not received an RPA license file, contact [RadBlue Support](#).

Computer Requirements

The minimum requirements for computers running the protocol analyzer are:

- Operating System (32- or 64-bit): Windows (Vista or 7) or Linux
- Memory: 4 GB (minimum)
- Disk Space: 250 MB

Install RPA on Windows

Follow these steps to install RPA.

1. Double-click **RPA_x_x_x.exe**.
2. Click **Next**.
3. Review the RadBlue click-through agreement, and select **I accept the agreement** to accept the agreement.
4. Click **Next**.
5. Type the location where you want the RPA application installed, or click **Browse** to navigate to the location.
6. Click **Next**.

If you have a previous version of the tool installed, you are prompted to remove it before installing the new version. Click **Next** to uninstall the previous version before continuing with the new installation, or click **Back** to install the new version in a different directory.

7. Click **Browse**, and navigate to the location of the RPA license file.

Note: For version 34 and higher, if you install a version of RPA over an existing version, you can choose to use the existing license. If you do not want to use the existing license, you can browse to a new license. Note that this option is only available when you install RPA over a previous installation. All components of the previous installation are removed by the installer except the license file and any backup files.

7. Click **Next**.
9. Select the **Start Menu folder** for RGS.

If you only want to create a shortcut for the current user, clear the **Create shortcuts for all users** checkbox.

If you do not require a Start Menu folder for RPA, select **Don't create a Start Menu** folder.

10. Click **Finish**.
11. Double-click the RPA desktop icon to launch the application.

Install RPA on Linux

Follow these steps to install RPA on a Linux operating system.

1. Download the tool's self-extracting install script from the RadBlue website onto your Linux computer.
2. Make the downloaded install script executable by typing the following command:
chmod +x script_name.sh
3. Run the install script using the format:
/script_path/script_name.sh
4. If you do not have Java installed on the computer, type **y** to install a JRE.
5. Click **Next**.
6. If you accept the RGS licensing terms, select **I accept the agreement**, and click **Next**.
7. Type the location of the directory where you want to install RGS, or click **Browse** to navigate to a location.
8. Click **Next**.

Note: If you have a previous version of the tool installed, you are prompted to remove it before installing the new version. Click **Next** to uninstall the previous version before continuing with the new installation, or click **Back** to install the new version in a different directory.

9. Navigate to the location of the RGS license file, and click **Next**.

Note: For version 34 and higher, if you install a version of RPA over an existing version, you can choose to use the existing license. If you do not want to use the existing license, you can browse to a new license. Note that this option is only available when you install RPA over a previous installation. All components of the previous installation are removed by the installer except the license file and any backup files.

10. Click **Finish**.

Uninstall RPA

You can uninstall RPA through the **Uninstall** option (**Start > All Programs > RadBlue Protocol Analyzer**) or by running the **uninstall.exe** file in the RPA installation directory.

When RPA is uninstalled, a backup folder is created in the RPA directory that saves the installation's security and configuration parameters. When a subsequent RPA version is installed, the installer uses the backed up data to populate security and configuration settings, so you do not need to re-key the information into the new installation.

Note: Backup files are **not** available for versions using student licenses, which always use default values for upgrades.

The backup folder is located in the RPA installation directory. The following files are saved in the backup folder:

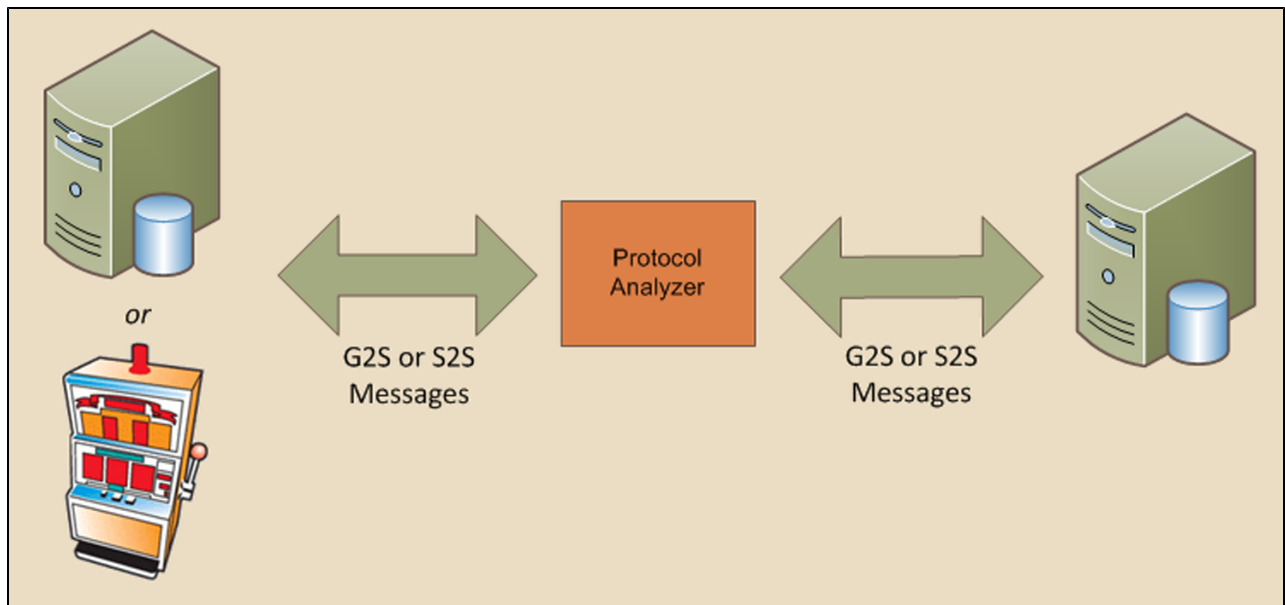
- All Java Keystore Files (.jks)
- scep_config.xml
- security_manager.xml
- webserver.xml
- Derby Port
- SOAP Address
- SOAP Inbound Port
- SOAP Outbound Port
- SSL Inbound Port
- SSL Outbound Port
- Schema Name
- Schema Version
- Side 1 Display Name (Side 1: EGM/Edge)
- Side 1 Location URI
- Side 1 Schema Version
- Side 1 GZIP Enabled
- Side 1 SSL Enabled
- Side 2 Display Name (Side 2: Host/Central)
- Side 2 Location URI
- Side 2 Schema Version
- Side 2 GZIP Enabled
- Side 2 SSL Enabled

About RPA

The RadBlue Protocol Analyzer (RPA) verifies that G2S or S2S messages sent between two endpoints have been implemented according to GSA messaging standards.

These two endpoints consist of a system on one end, and either an EGM or a system on the other end. The Protocol Analyzer sits between the two endpoints, receives messages from each side, verifies the messages, and forwards them on to their destination.

RPA can connect with up to five hosts at once; the RPA must be configured to support each host.

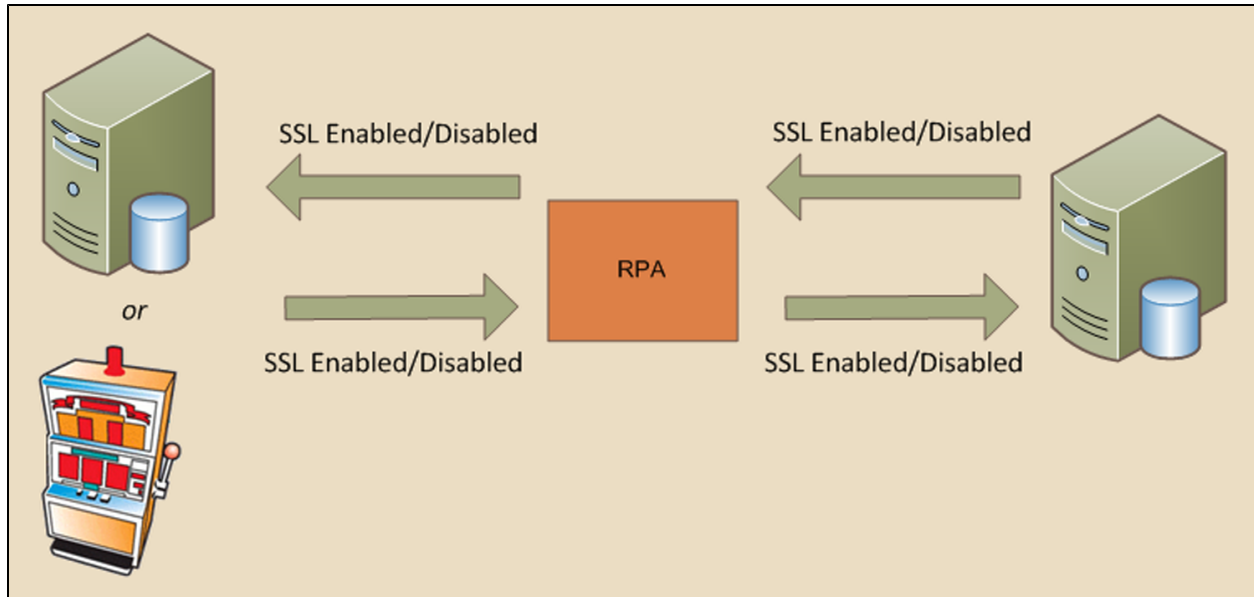


RPA overview.

In addition, the optional disruptive filter set feature lets you manipulate messages that pass through RPA. See [About Disruptive Filters](#) for more information.

Using SSL

The Protocol Analyzer supports SSL authentication and encryption. You have the option to enable SSL for each endpoint.



Enable/disable SSL for each portion of the trip between endpoints.

Additional Resources

- [RPA Release Notes](#)
- [Quick Start](#)

Supported GSA Versions

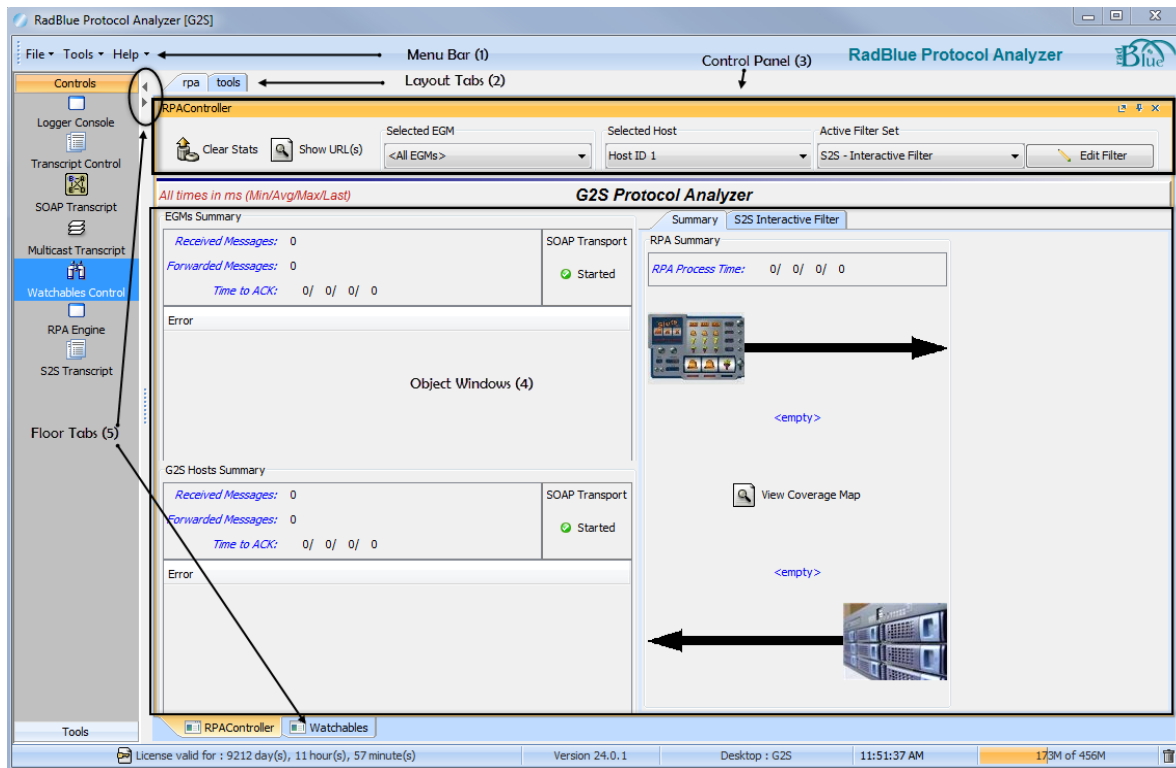
The following Gaming Standards Association (GSA) protocol versions are supported by RPA:

Protocol	Versions		
G2S	1.1.0	2.1.0	
S2S	1.2.6	1.3.1	1.4.2

Review the RPA User Interface

The RPA layout changes slightly depending on whether or not you are using [disruptive filters](#).

Let's take a look at the RPA user interface with disruptive filters.

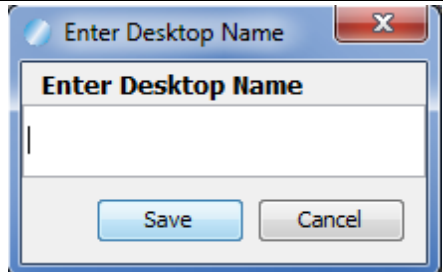
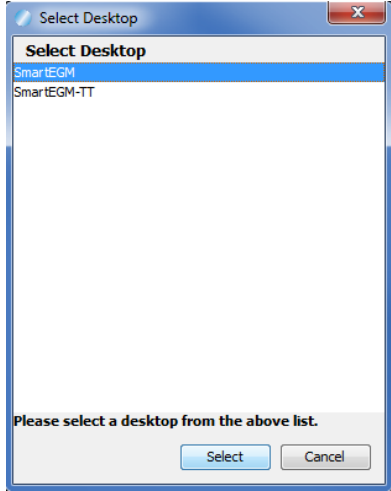
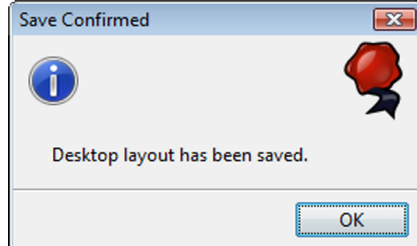


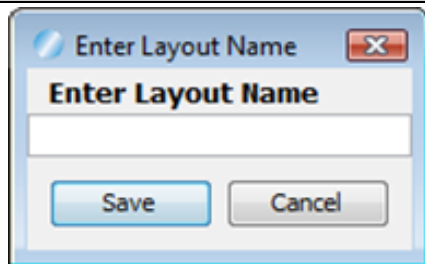
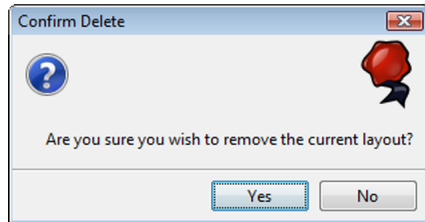
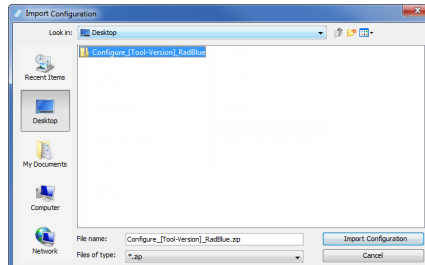
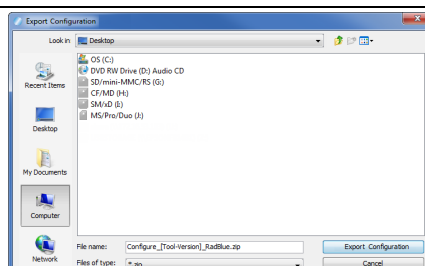
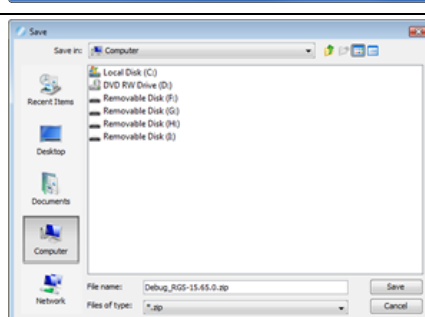
With Disruptive Filters

Menu Bar (1)

From the menu bar you can access product options.

File

Menu Option	Description	Screen
New Desktop	<p>Select to create a new desktop. The <i>desktop</i> is a collection of objects and tabs that constitute the work area of the tool.</p> <p>Type the name of the new desktop, and click Save.</p>	
Open Desktop	<p>Select to change the current desktop. When you save a desktop, it becomes available in the Select Desktop list.</p> <p>Highlight the desktop you want to use, and click Select.</p>	
Save Desktop	<p>Select to save the current desktop. Once you save a desktop, you can open it at any time by selecting Open Desktop.</p> <p>Click OK.</p>	

Menu Option	Description	Screen
Add Layout	Select to add a new layout. The <i>layout</i> is a series of tabs on the desktop, used to organize objects by function. Within each layout, objects can be placed next to each other, or on top of each other (in which case they are accessed by object tabs). Type the name of the new layout, and click Save .	
Remove Layout	Select to delete the currently displayed layout. Click Yes to delete the layout.	
Import Configure...	Select to import all configuration settings for the tool, exported from another version of the same tool, including security certificates. This option is used when you want to quickly set up a specific configuration for the tool that is already set up in another version of the tool.	
Export Configure...	Select to export all configuration settings for the tool, including security certificates. The resulting ZIP file can then be imported into another version of the same tool.	
Export Debug	Select to create a ZIP file of troubleshooting information that can be sent to RadBlue support or used with the RadBlue Analysis Suite (RAS) . Browse to the location where you want to save the ZIP file, and click Save .	
Exit	Select to close the product.	

Tools

Option	Short cut	Description
Configure	F2	Select to see configuration options.
Toggle Floor Tab	F3	See <i>Floor Tabs</i> below.
GSA Message Validator	F4	Allows you to paste in a sample XML document and see if the message is valid against the selected schema.

Help

RPA Help	Select to launch RPA Help system.
Contact Us	Select to open the contact page of the RadBlue web site.
About RPA	Select to see the copyright, licensing, and version information.

Layout Tabs (2)

Layout Tabs	Description
RPA	Lets you see messages as they are passed between the two endpoints. You can: view all messages set up specific message types on a “watch” list easily identify non-compliant message view the XML document behind a message use custom protocol schema
Tools	Lets you configure tests so you can monitor remotely.

Control Panel (3)

The control panel lets you

- **Clear** the Summary tab (right-side of screen) data with one press of the button.
- **Show URL(s)** for RPA EGMs, SSL EGMs, and Hosts
- **Select EGM** to test up to five EGMs at once. See [Configure RPA with Multiple GEMS and Hosts](#)
- **Select Host** to test up to five hosts at once. RPA must be configured to support each host.
- Add and Edit a G2S or S2S disruptive filter set of features to manipulate messages that pass through the RPA. See [About Disruptive Filters](#) for more information.

Object Windows (4)

There are three major sections of the object window:

- Client Side Information - showing all EGM error messages for each connection.
- Host Side Information - showing all error G2S messages for each connection.
- Summary tab - showing all statistics about the messages received from each endpoint as well as the Protocol Analyzer.

See [RPA Layout](#) for more information about using these windows.

Floor Tabs (5)

Open/Close - The floor tab displays objects that you can drag and drop onto an *Object Window* when you want to create a custom desktop or layout.

Open this window using the arrows on the interface screen, or by going to **Tools > Toggle Floor Tabs**.

This panel contains views that you can see when you click the bars: General and Tools.


- When you drag and drop an object from one of these views, the object opens as a tab.
- Click and hold the tab to open it into a floating window.
- When you find a custom layout, save that desktop, go to **File > Save Desktop**

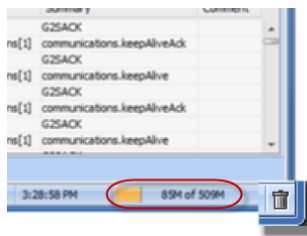
About Objects - Objects contain a single function (or group of functions) that you work with in the tool. They are populated from the tool's data model. The data model reflects all of the data that has been captured by the tool and any updates that are received while the tool is running.

When you first start the tool, all of the objects are empty. As messages are received by the tool, the appropriate objects are updated automatically. New objects are updated based on what's in the tool's data model.

As a result, objects are immediately populated when dragged onto a layout, as long as the tool has been running for a while and has received the applicable command. The same behavior holds true when switching between desktops. If the command is in the data model, the object is automatically populated.

About the Garbage Collector

The Garbage Collector lets you reclaim memory that is no longer in needed in order to improve tool performance. To use the Garbage Collector, click the garbage can () icon in the lower right corner of the user interface.



RPA Configuration Overview

To get up and running on RPA, follow these steps:

1. [Configure RPA for G2S](#) or [Configure RPA for S2S](#)
2. Configure Protocol Analyzer Startup Options
3. [Configure RPA to Run As RGS](#) (Optional)
4. Install a Custom Schema File (Optional)
5. Add a New Schema to RPA with Disruptive Filters (Optional)
6. Force Stronger Encryption (Optional)

Configure RPA for G2S

Use the following instructions to configure RPA on a Game-to-System (G2S) network, in which a host communicates to one or more EGMs.

If possible, we recommend that you configure RPA without SSL first, get communications working, and then enable SSL. If you configure SSL on first use, be sure that you enter all URLs correctly and check the SSL Enabled checkbox under the Host Side Information option.

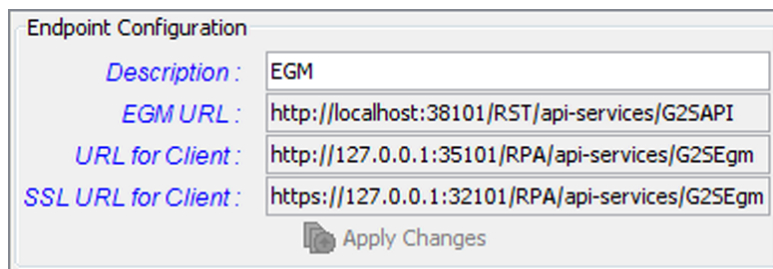


Game-to-System endpoints.

1. Record the Host URL (http://[host2]), to be entered in step 4c.
2. Create the From URL for the Protocol Analyzer.
 - a. Select **Configure** from the menu bar.
 - b. Select **Engine Options**.


The screenshot shows the "Engine Options" dialog box. It has several sections: "IP Address and SOAP Port" with fields for "Bind To" (127.0.0.1), "SOAP Port" (35101), "Emulate RGS" (checkbox), and "SSL SOAP Port" (32101); "From URLs" with fields for "From URL" (http://127.0.0.1:35101/RPA/api-services/S2SCentral) and "SSL From URL" (https://127.0.0.1:32101/RPA/api-services/S2SCentral); and "Protocol Options" with fields for "Protocol Name" (S2S), "Version" (1.2.6), and "Schema Location" (../schemas/s2s/1.2.6). There are also three blue instructional links: "Select IP Address and SOAP Port.", "From Locations are set automatically from the Protocol Options, IP Address and", and "Select the G2S/S2S protocol to use."

- c. Set the **IP Address** and **SOAP Port** number.
 - **Bind To** - Click the drop-down arrow, and select the IP Address that you want RPA to use for communications. If the RPA, EGM and host are all running on the same computer, select **127.0.0.1** (localhost).
 - **SOAP Port** - Enter the port that you want RPA to use for communications. We recommend that you do not change the SOAP port unless you have a port conflict.
 - **SSL SOAP Port** - Enter the port that you want RPA to use for SSL-enabled communications. This port number is used when you select **SSL Enabled** on the Host Side Information screen and when the EGM uses SSL.
 - **Emulate RGS** - Select Emulate RGS if you want the Protocol Analyzer to appear as RGS to your EGM. In most configurations this option should be cleared.
 - d. Set the **Protocol Options**.
 - **Protocol Name** - Click the drop-down arrow, and select G2S. This setting is used to create the Schema Location.
 - **Version** - Click the drop-down, and select the G2S version you want to use. This setting is used to create the Schema Location.
 - e. Click **OK**.
3. Configure the client side.
- a. On the RPA layout, click **Client Side Information**.



Endpoint Configuration

Description :	EGM
EGM URL :	http://localhost:38101/RST/api-services/G2SAPI
URL for Client :	http://127.0.0.1:35101/RPA/api-services/G2SEgm
SSL URL for Client :	https://127.0.0.1:32101/RPA/api-services/G2SEgm

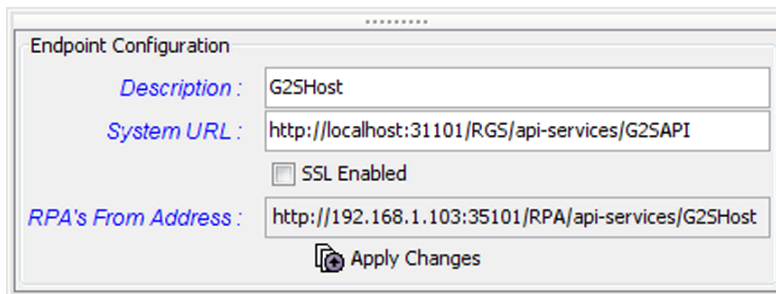
 Apply Changes

- b. Enter a description for the client (for example, EGM).

Note: The EGM URL, URL for Client and SSL URL for Client are automatically calculated based on the information you enter in step 2. Be sure that the EGM uses the URL for Client or SSL URL for Client for the Protocol Analyzer network address. *If the EGM does **not** use this address, it will not be able to communicate with the Protocol Analyzer.*

- c. Click **Apply Changes**.

4. Configure the **host side**.
 - a. On the RPA layout, click **Configure Host Side**.



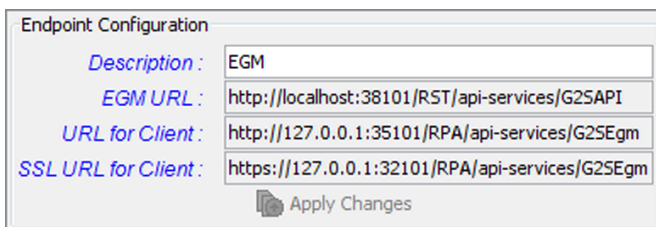
The screenshot shows a dialog box titled "Endpoint Configuration". It contains the following fields and controls:

- Description :** G2SHost
- System URL :** http://localhost:31101/RGS/api-services/G2SAPI
- ☐ SSL Enabled
- RPA's From Address :** http://192.168.1.103:35101/RPA/api-services/G2SHost
- Apply Changes** button

- b. Enter a description for the host (for example, G2SHost).
 - c. Enter the URL for the G2S host from step 1.
 - d. Select **SSL Enabled** if you are using SSL messaging between the Protocol Analyzer and the host system.
 - e. Click **Apply Changes**.
5. **Close** and **re-launch** the Protocol Analyzer to make sure the web service is properly configured.
6. Click **Start RPA** on the RPA layout to start the Protocol Analyzer engine.

Configure the EGM

To configure the EGM to communicate with RPA, use the **URL for Client** (for non-SSL communications) or **SSL URL for Client** (for SSL-enabled communications) address from the **Client Side Information** screen.



The screenshot shows a dialog box titled "Endpoint Configuration". It contains the following fields and controls:

- Description :** EGM
- EGM URL :** http://localhost:38101/RST/api-services/G2SAPI
- URL for Client :** http://127.0.0.1:35101/RPA/api-services/G2SEgm
- SSL URL for Client :** https://127.0.0.1:32101/RPA/api-services/G2SEgm
- Apply Changes** button

Client Side Information screen.

Configure the G2S Host

No configuration is required on the G2S host for communication with RPA.

Configure RPA for S2S

To configure RPA for System-to-System (S2S) messaging, you must have two S2S hosts. The first host is the S2S Edge server, and the second is the S2S Central server. The S2S Edge server is a peripheral server, such as a voucher or player kiosk. The S2S Central server is a host server, such as a voucher system or player tracking system.



System-to-System endpoints.

1. Record the following information:
 - a. **S2S Edge Server URL:** `http://[host1]`
 - b. **S2S Central Server URL:** `http://[host2]`
2. Set RPA configuration options.
 - a. Select **Configure** from the menu bar.
 - b. Select **Engine Options**.

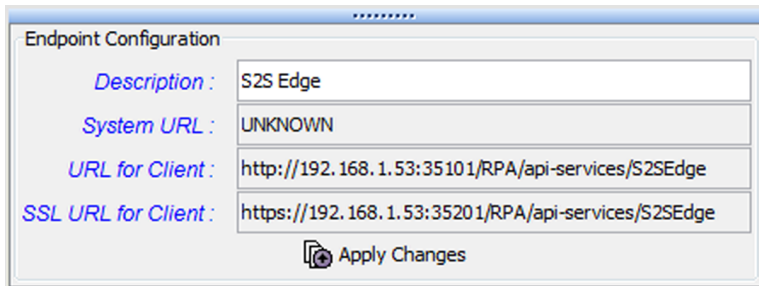
The screenshot shows the "Engine Options" dialog box. It has several sections:

- IP Address and SOAP Port:** Includes a "Bind To" dropdown set to "127.0.0.1", a "SOAP Port" field set to "35101", and an "SSL SOAP Port" field set to "32101". There is an "Emulate RGS" checkbox which is unchecked.
- From URLs:** Includes a "From URL" field set to `http://127.0.0.1:35101/RPA/api-services/S2SCentral` and an "SSL From URL" field set to `https://127.0.0.1:32101/RPA/api-services/S2SCentral`.
- Protocol Options:** Includes a "Protocol Name" dropdown set to "S2S", a "Version" field set to "1.2.6", and a "Schema Location" field set to `../schemas/s2s/1.2.6`.

 There are blue italicized instructions: "Select IP Address and SOAP Port." and "Select the G2S/S2S protocol to use."

- c. Set the IP Address and SOAP Port number.

- **Bind To** - Click the drop-down arrow, and select the IP Address that you want RPA to use for communications. If the RPA, EGM and host are all running on the same computer, select **127.0.0.1** (localhost).
 - **SOAP Port** - Enter the port that you want RPA to use for communications. We recommend that you do not change the SOAP port unless you have a port conflict.
- d. Set the **Protocol Options**.
- **Protocol Name** - Click the drop-down arrow, and select **S2S**. This setting is used to create the Schema Location.
 - **Version** - Click the drop-down, and select the S2S version you want to use. This setting is used to create the Schema Location.
- e. Click **OK**.
3. Configure the **client side**.
- a. On the RPA screen, click **Client Side Information**.



Endpoint Configuration

Description : S2S Edge

System URL : UNKNOWN

URL for Client : http://192.168.1.53:35101/RPA/api-services/S2SEdge

SSL URL for Client : https://192.168.1.53:35201/RPA/api-services/S2SEdge

Apply Changes

- b. Enter a description for the client for example (for example, S2S Edge).

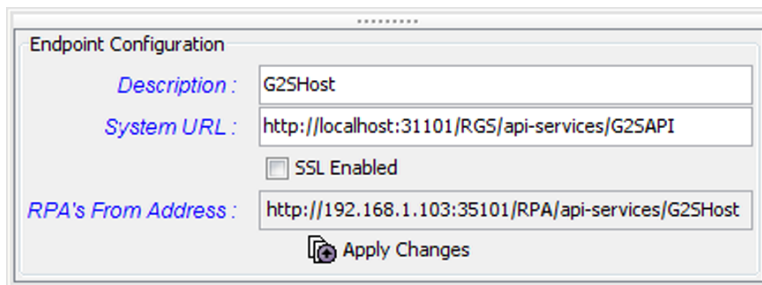
Note: The **System URL** is automatically completed by RPA. This field is *read-only*.

The **URL for Client** and **SSL URL for Client** are automatically calculated based on the information you enter in step 2.

Be sure that the client host uses the **URL for Client** or **SSL URL for Client** for the Protocol Analyzer network address. If the client host does not use this address, it will not be able to communicate with the Protocol Analyzer.

- c. Click **Apply Changes**.

4. Configure the **host side**.
 - a. On the RPA screen, click **Configure Host Side**.



The screenshot shows a dialog box titled "Endpoint Configuration". It contains three text input fields and a checkbox. The first field is labeled "Description :" and contains the text "G2SHost". The second field is labeled "System URL :" and contains the text "http://localhost:31101/RGS/api-services/G2SAPI". The third field is labeled "RPA's From Address :" and contains the text "http://192.168.1.103:35101/RPA/api-services/G2SHost". There is a checkbox labeled "SSL Enabled" which is currently unchecked. At the bottom right of the dialog box is a button labeled "Apply Changes" with a circular arrow icon.

- b. Enter a description for the host (for example, S2S Central).
 - c. Enter the S2S Central **System URL** from step 1b.
 - d. Select **SSL Enabled** if you are using SSL messaging between the Protocol Analyzer and the central host system.
 - e. Click **Apply Changes**.
5. Start the Protocol Analyzer by clicking **Start RPA**.

Configure S2S Edge Server

To configure the S2S Edge server to communicate with RPA, use the URL for Client (for non-SSL communications) or SSL URL for Client (for SSL-enabled communications) address from the Client Side Information screen.

Client Side Information screen.

Configure the S2S Central Server

To configure the S2S Central server to communicate with RPA, use the URL for Host address from the Host Side Information screen. This address changes depending on whether or not you have SSL Enabled selected.

Host Side Information screen.

Configure RPA Options

Startup configuration options need to be configured one time, but they can be modified as needed. To access the startup configuration options, click **Configure** on the menu bar.

You can configure the following options for RPA:

- [Desktop Options](#)
- [Engine Options](#)
- [License Manager](#)
- [Filter Options](#)
- Security Options

Configure RPA to Run as RGS

The Emulate RGS option allows the Protocol Analyzer to appear as the RadBlue G2S Scope to your EGM.

1. From the RPA layout, select **Configure**.
2. Click **Engine Options**.
3. Select **Emulate RGS**.
4. Click **Apply**, and then click **OK**.

Install a Custom Schema File (Optional)

To install and use custom protocol schemas that may be required for testing.

1. Unpack the custom schema into:
 - **for G2S:** ..\schemas\g2s\[**version number**]
 - **for S2S:** ..\schemas\s2s\[**version number**]
2. Verify that the following files exist:
 - for G2S: schemas\g2s\[**version number**]\g2sMessages.xsd
 - for S2S: schemas\s2s\[**version number**]\s2sMessages.xsd

The file should take on the following formats:

```
<commands>
  <command name="bonus.bonusActivity" />
  <command name="bonus.bonusAwardAck" />
  <command name="bonus.bonusLogList" />
  <command name="bonus.bonusLogStatus" />
</commands>
```

3. Open the Protocol Analyzer, and click **Configure**.
4. Click **Engine Options**.
5. Go to **Protocol Options > Protocol Name**.
6. Click the drop-down arrow, and select the protocol (**G2S** or **S2S**) you want to use.
7. Click the **Version** drop-down arrow, and select your custom schema version number.
The **Schema Location** field should now match the location of your custom schema.
8. Click **Apply**, and then click **OK**.

Add a New Schema to RPA with Disruptive Filters (Optional)

1. Close the RPA application.
2. Create a new directory (named to represent your version) and add your schema files to it as described in [Install a Custom Schema File \(Optional\)](#).
3. Copy the following files from the ../schemas/g2s/1.0.3 directory into the new directory:
 - g2s-command-set.xml
 - g2s-event-set.xml
4. Add any new commands and events to the files in step 3, using the same format as is used for GSA standard commands and events.
5. Start RPA.

The new schema is available on the RPA Configuration screen (**Configure > Engine Options > Protocol Options**).

Force Stronger Encryption (Optional)

RST can force stronger encryption ciphers first in its cipher list. However, host systems must also support this methodology for that feature to work.

To use stronger encryption ciphers, you must take the following steps:

1. Go to: <http://java.sun.com/javase/downloads/index.jsp>
2. Scroll down to the **Additional Resources > Other Downloads**.
3. Download **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6**.

Follow the installation instructions in the README document, located in the download's ZIP file.

Configure RPA with Multiple EGMs and Hosts

You can configure a single instance of RPA to monitor up to five hosts and five EGMs at one time. Hosts that are monitored by RPA can be configured through the EGM before testing begins, or through the [commConfig.setCommChange](#) command once communications with the first host are established. In either case, the identifier and URL of each host must be [configured in RPA](#) before testing begins.

Note: If you are using RGS or RST to simulate multiple hosts or EGMs, you can create as many instances of the tool as necessary with your existing license.

Once configured, all messages, for all connected EGMs and hosts, are displayed in the [Summary](#) sections on the RPA Controller. The view for each Summary (EGM and host) can be filtered to display the summary of a specific host or EGM, or all hosts and/or EGMs. In addition, the [Message Transcript](#) can be filtered to view individual hosts and EGMs, or all hosts and/or EGMs.

Note that there are three filters that may impact a multiple endpoint configuration:

[CommsOnLine Filter](#) - This filter changes the *egmLocation* attribute in the G2S `commsOnLine` command from the EGM's location to the RPA's location, so response commands are sent to RPA rather than to the EGM. This filter is **enabled** by default.

[Comm Host List Filter](#) - The Comm Host List filter sets the *canModRemote* attribute to **false** for the `commHostItem` element that has RPA's URL. When this filter is selected, the host cannot modify the `commHostItem` in the `commHostList`, which effectively disables `commConfig` changes for that host. This allows you to continue to use RPA because the host cannot re-write the *hostLocation* to something other than the RPA URL. This filter is **disabled** by default.

[Set Comm Change Filter](#) - The Set Comm Change replaces the host's URL in the `setCommChange` command with RPA's URL. Additionally, this filter lets you use RPA even if the host has re-written the *hostLocation* to something other than the RPA location by re-writing RPA's URL in the `commHostList` command and replacing it with the host's URL. This means that the host sees itself in the `commHostList` command and should not resend the `setCommChange` command unless it is absolutely necessary. This filter is **enabled** by default.

Configure RPA for Multiple Hosts

RPA can connect with up to five hosts at once. To use multiple hosts, RPA must be configured to support each host. However, it does not have to connect to each host right away. If you are testing the `commConfig.setCommChange` command, you can change device ownership to any of the configured hosts. Once device ownership is updated through `commConfig.setCommChange`, RPA will begin sending messages to the new host (device owners) as required. See [Add Hosts through commConfig.setCommChange](#) for more information.

Note: If you are using RGS to simulate a host, you must install a separate instances of RGS for each host you want to use for the simulation.

To configure multiple hosts:

1. Go to **Tools > Configure > Engine Options > G2S Endpoints**.

Engine Options

General Transport Transcript Filters Database **G2S Endpoints**

EGM Endpoints

Edit Remove Remove All Inactive Timeout : 05:00 [mm:ss]

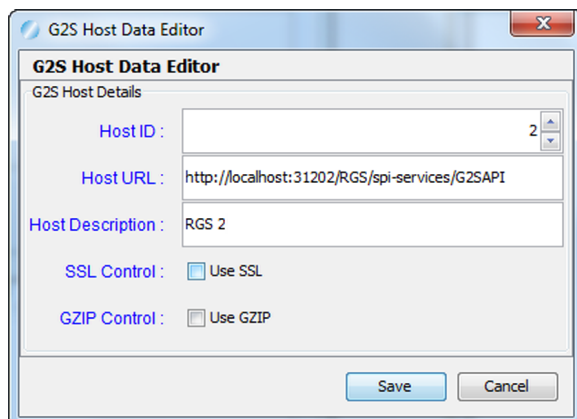
EGM ID	EGM URL	Description
--------	---------	-------------

G2S Host Endpoints

Add Remove Edit

ID	URL	Description	SSL
1	https://localhost:31201/RGS/api-services/G2SAPI	RGS	Enabled

- To add an additional host, click **Add**.

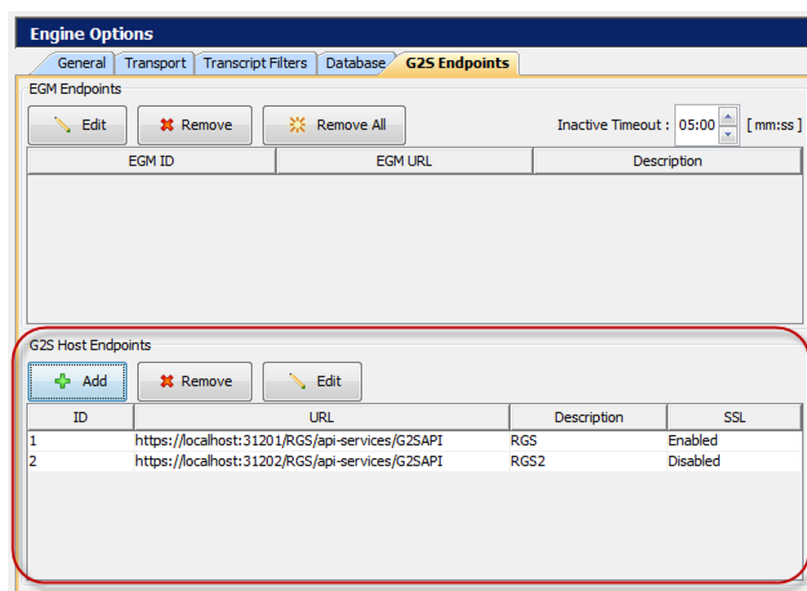


The G2S Host Data Editor dialog box contains the following fields and controls:

- Host ID :** A text field with a spinner box set to 2.
- Host URL :** A text field containing `http://localhost:31202/RGS/spi-services/G2SAPI`.
- Host Description :** A text field containing `RGS 2`.
- SSL Control :** A checkbox labeled ☒ Use SSL.
- GZIP Control :** A checkbox labeled ☐ Use GZIP.
- Buttons:** Save and Cancel.

- Enter the G2S host information as needed.
 - Host ID** - Type or select the host identifier.
 - Host URL** - Type the G2S host system URL. This is the location to which RPA forwards messages from the EGM.
 - Host Description** - Type a description of the defined host.
 - SSL Control** - Select to enable SSL for messages forwarded from the host to RPA.
 - GZIP Control** - Select to enable GZIP for messages forwarded from the host to RPA. Note that, when this option is selected, RPA allows GZIP, but **does not require** a GZIP message.
- Click **Save**.

The new endpoint is added to the G2S Host Endpoints list.

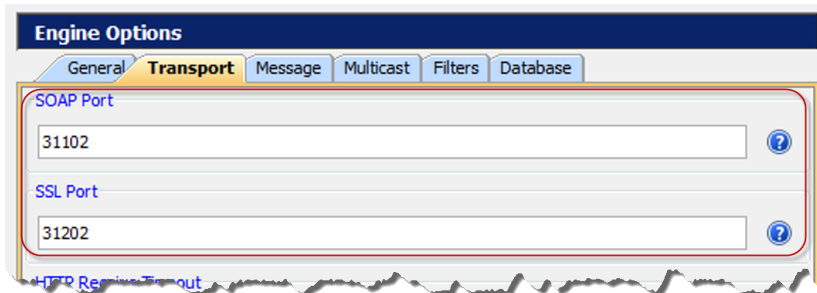


The Engine Options dialog box, G2S Endpoints tab, shows the following:

- EGM Endpoints:** A table with columns EGM ID, EGM URL, and Description. It includes buttons for Edit, Remove, and Remove All, and an Inactive Timeout of 05:00 [mm:ss].
- G2S Host Endpoints:** A section highlighted with a red border, containing an Add button, a Remove button, and an Edit button. Below these is a table with columns ID, URL, Description, and SSL.

ID	URL	Description	SSL
1	https://localhost:31201/RGS/api-services/G2SAPI	RGS	Enabled
2	https://localhost:31202/RGS/api-services/G2SAPI	RGS2	Disabled

5. Click **Apply**, and then click **OK** to exit the configuration screen.
6. If you are using RGS to simulate a host, install a separate instances of RGS for each host you want to use for the simulation.
7. Configure each RGS instance.
 - a. Launch **RGS**.
 - b. Go to **Tools > Configure > Engine Options > General**.
 - c. Change the **Host ID** number to a unique identifier (for example, 2).
 - d. Click the **Transport** tab.

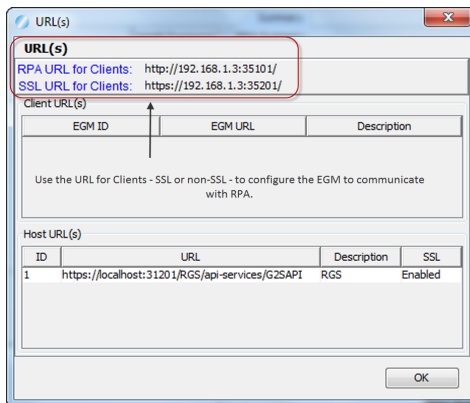


- e. Change the last digit of the **SOAP Port** and **SSL Port** numbers. Note that the final digit must be unique.
8. Click **Apply**, and then click **OK** to exit the configuration screen.
9. Start the EGM, RGS or RST.
10. View communications between all hosts and all EGMs through the [Message Transcript](#).

Configure EGMs to Communicate with RPA

RPA can connect with up to five EGMs at once. To configure multiple EGMs:

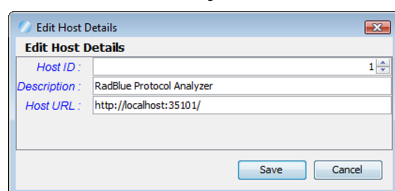
1. Go to the **rpa** layout, and click the **RPA Controller** sub-tab.
2. Click **Show URL(s)**.



3. Use either the **RPA URL for Clients** (for non-SSL connections) or **SSL URL for Clients** (for secure connections) to configure each EGM for communications with RPA.

If you are using RST to simulate an EGM:

- a. Launch **RST**.
- b. Go to the **SmartEGM** layout.
- c. If RST is running, click **Stop SmartEGM**.
- d. Click **Change SmartEGM Configuration**.
- e. Select the **smartegm-config-gsa-rap.xml** file, and click **Open**.
- f. Edit the host list as needed by clicking the **Hosts** tab on the **SmartEGM** layout.
- g. Select the host you want to edit, click **Edit Host**.



- h. Enter the **RPA URL for Clients** or **SSL URL for Clients** information from RPA.
- i. Click **Save**.
- j. Click **Start SmartEGM** to begin communications.

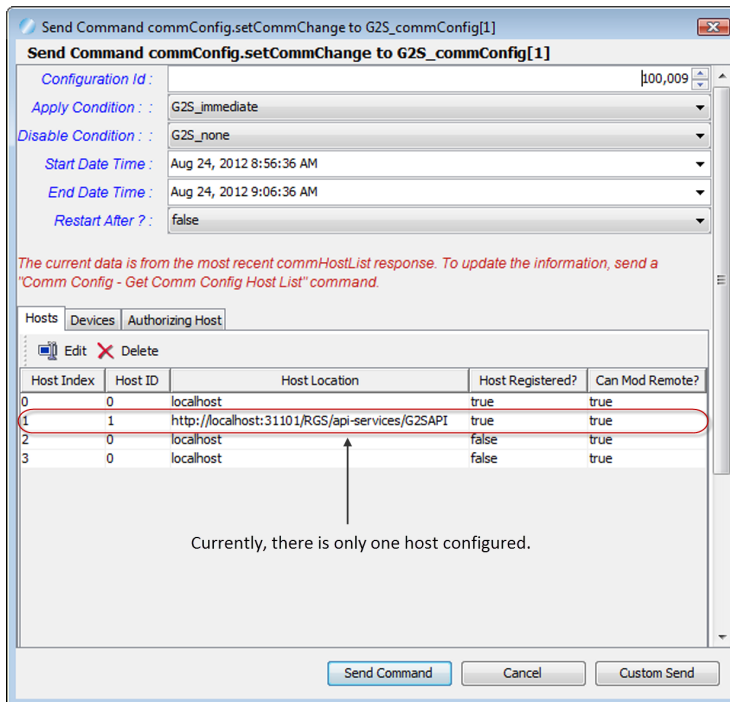
Add Additional Hosts in the EGM through the setCommChange Command

Once you have a host-RPA-EGM configuration running, you can add additional hosts through the `commConfig.setCommChange` command. Before you do this, however, you must configure the URL of the additional host in RPA.

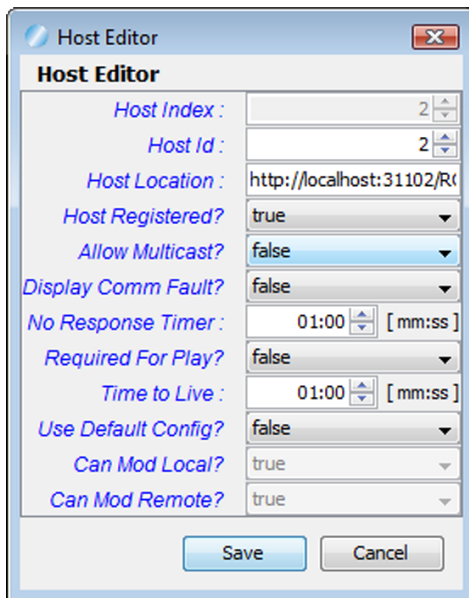
1. [Configure RPA for multiple hosts.](#)

Note: You must configure all hosts that you want to monitor through RPA. Each host URL must be entered in the G2S Endpoints screen **exactly** as it appears in the `commConfig.setCommChange` command. If you are using RGS as the host, click **RGS URLs** on the Engine layout of the RGS host you are adding, click **CTRL+C** to copy the URL, and paste the URL into G2S Endpoint [G2S Host Data Editor](#) in RPA.

2. Start the EGM, RST or RLT.
3. Confirm through the [Message Transcript](#) that the host, RPA and the EGM are communicating.
4. Send the `commConfig.setCommChange` command to RPA from the host.
5. If you are using RGS as the host:
 - a. Go to the **Send Command** layout.
 - b. Click to highlight **G2S_commConfig** in the Current Devices tab.
 - c. Double-click **setCommChange** under **Available Commands**.



- d. Click to select any Host Index entry that is **not** the currently connected host.



The Host Editor dialog box contains the following fields and controls:

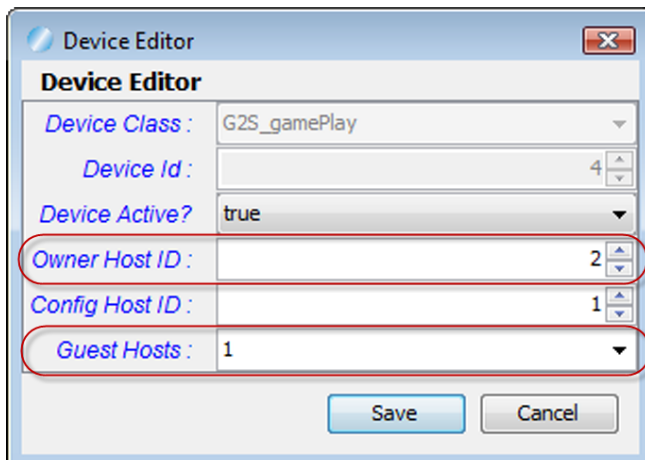
- Host Index :** 2
- Host Id :** 2
- Host Location :** http://localhost:31102/Rt
- Host Registered?** true
- Allow Multicast?** false
- Display Comm Fault?** false
- No Response Timer :** 01:00 [mm:ss]
- Required For Play?** false
- Time to Live :** 01:00 [mm:ss]
- Use Default Config?** false
- Can Mod Local?** true
- Can Mod Remote?** true

Buttons: Save, Cancel

- e. Change the **Host ID** to the identifier of the host you are setting device permissions for.
- f. Type the **Host Location** URL **exactly** as it appears on the [G2S Endpoints](#) screen in RPA.
- g. Click the **Host Registered?** drop-down arrow, and select **true**.
- h. Set the **No Response Timer** and **Time To Live** fields as required for testing.

Note: All other fields can be set as required for testing, but are not required for this operation.

- i. Click **Save**. The host list is updated with your changes immediately.
- j. Click the **Devices** tab.
- k. Click to highlight the device you want to assign to the new host, and click **Edit**.



The Device Editor dialog box contains the following fields and controls:

- Device Class :** G2S_gamePlay
- Device Id :** 4
- Device Active?** true
- Owner Host ID :** 2
- Config Host ID :** 1
- Guest Hosts :** 1

Buttons: Save, Cancel

- l. Change either the **Owner Host ID** or the **Guest Hosts** identifier to the new host, and click **Save**. The device list is updated with your changes immediately.
- m. Perform steps d through l to add additional hosts.
- n. Click **Send Command**.
- o. Go to the RPA [Message Transcript](#) to view messages between all hosts and EGMs.

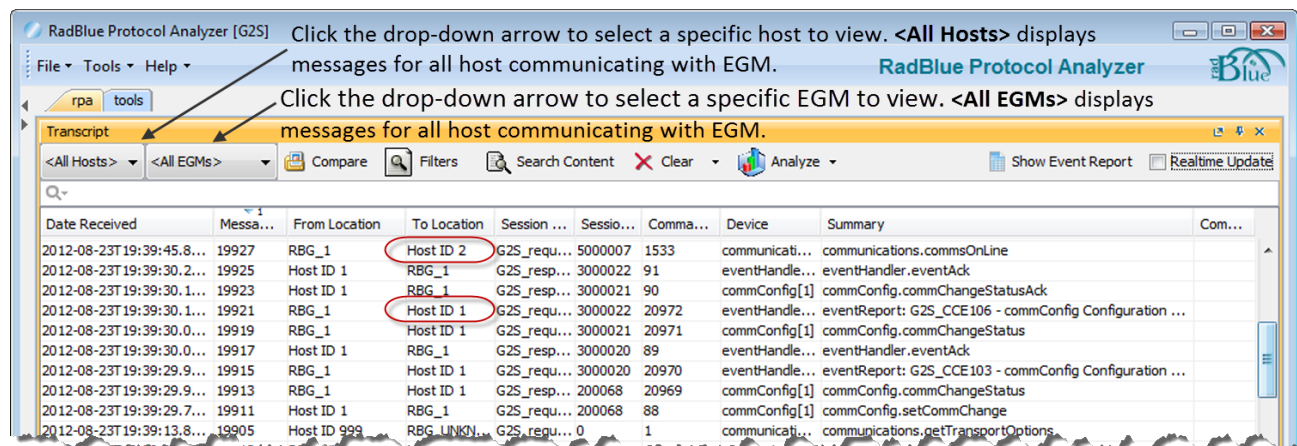
View Message Activity for Multiple EGMs and Hosts

When RPA is monitoring multiple EGMs and hosts, EGM and host selectors allow you to monitor message activity of all EGMs and/or hosts, or a specific EGM and/or host. In all cases, changes to a selector take effect immediately.

To change the EGM activity displayed in the **EGMs Summary** on the RPA Controller, click the **Selected EGM** drop-down arrow, and select a specific EGM to view or **<All EGMs>**.

To change the host activity displayed in the **G2S Hosts Summary** on the RPA Controller, click the **Selected Host** drop-down arrow, and select a specific EGM to view or **<All Hosts>**.

From the Message Transcript, you can view all messages sent and received by RPA, regardless of the number of hosts and EGMs being monitored by RPA. All standard Message Transcript functionality is available with multiple EGMs and hosts. However, you can use the **Host Selector** and **EGM Selector** to filter the display to show a single EGM and/or host, or **<All EGMs>** and/or **<All Hosts>**.



RPA Layout

With the RPA layout screen, you can view messages as they pass between two endpoints.

The screenshot shows the RadBlue Protocol Analyzer (RPA) interface. The layout includes a menu bar (File, Tools, Help), layout tabs (rpa, tools), and a controls panel on the left with options like Logger Console, Transcript Control, SOAP Transcript, Multicast Transcript, Watchables Control, and RPA Engine. The main display area is divided into several sections:

- EGM Summary:** Displays statistics for the selected EGM (RBG_1234), including Received Messages (388), Forwarded Messages (388), and Time to ACK (12/ 22/ 336/ 87). It also shows a SOAP Transport status (Started).
- Host Side Information:** Displays statistics for the host side, including Received Messages (388), Forwarded Messages (388), and Time to ACK (14/ 26/ 159/ 23). It also shows a SOAP Transport status (Started).
- Interactive Filter Control:** Allows users to select a filter set (G2S - Interactive Filter) and apply it to the message list.
- Message List:** A table showing a list of messages with columns for Time, EGM, Command / Event, Applied Filter, and Message. The messages are filtered by the selected filter set.

Annotations on the screenshot provide additional context:

- Menu Bar (2):** Points to the File, Tools, and Help menu.
- Layout Tabs (3):** Points to the rpa and tools tabs.
- Indicates currently displayed EGM:** Points to the Selected EGM dropdown menu.
- Select to user G2S, S2S or no filters:** Points to the Active Filter Set dropdown menu.
- Click to edit current filter set options:** Points to the Edit Filter button.
- Active filters for the selected filter set:** Points to the Command / Event field in the Interactive Filter Control.
- Click to disconnect and connect the connection with the client side:** Points to the SOAP Transport status in the EGM Summary.
- Indicates currently held command. Click Apply to apply the selected filter or Forward to send the command without making changes:** Points to the Apply Filter and Forward buttons.
- Endpoint 1 message summary and list of errors:** Points to the EGM Summary section.
- Endpoint 2 message summary and list of errors:** Points to the Host Side Information section.
- Double-click any message to view its XML content:** Points to a message in the Message List.

Configuring the RPA

Using the RPA layout, you can configure both endpoints, start and stop RPA, view RPA processing statistics and messaging errors.

- **Clear Stats** - Click to clear the statistics that appear in the Summary section.
- **Client Side Information** - Configuration information for the client side. See [Configure RPA for G2S](#).
- **Host Side Information** - Configure the host side. See [Configure RPA for G2S](#).

RadBlue Protocol Analyzer [rpa]

File Tools Help

Clear Stats

Selected EGM: <All EGMs>

Active Filter Set: G2S - Interactive Filter

G2S Protocol Analyzer

Summary Interactive Filter

Interactive Filter Control

Command / Event: keepAliveAck [RBG_1234]

Action: Auto-send in 8 sec(s)

Select Filter: Add Valid Attribute

Apply Filter Forward

Load Clear Display Clear DB

Client Side Information

EGM Summary

Received Messages: 476

Forwarded Messages: 476

Time to ACK: 11/ 23/ 315/ 17

SOAP Transport: Started

Host Side Information

G2S Host Summary

Received Messages: 476

Forwarded Messages: 476

Time to ACK: 13/ 25/ 115/ 19

SOAP Transport: Started

Error

element2.element2

2011-07-20T14:18:32.662-07:00

Cannot find the declaration of element 'document'.

communications.keepAlive

Message Log

Time	EGM	Command / Event	Applied Filter	Message
14:46:29	RBG_1234	keepAlive	Message Delay	Timeout: 15 sec(s). Queu...
14:46:18	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:46:08	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:45:58	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:45:44	RBG_1234	keepAlive	Message Delay	Timeout: 15 sec(s). Queu...
14:45:30	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:45:29	RBG_1234	meterInfo	Message Delay	Timeout: 15 sec(s). Queu...
14:45:20	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:45:10	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:44:55	RBG_1234	keepAlive	Message Delay	Timeout: 15 sec(s). Queu...
14:44:45	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:44:35	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:44:25	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...
14:44:11	RBG_1234	keepAlive	Message Delay	Timeout: 15 sec(s). Queu...
14:44:00	RBG_1234	keepAliveAck	Message Delay	Timeout: 15 sec(s). Queu...

Transcript

<All EGMs> Load Compare Filters Search Content Set Comment Clear Analyze Realtime Update

Date Received	From Location	To Location	Command ID	Session ID	Session Type	Summary	Comment
2011-07-20T14:46:30.109-0700	Host ID 1	RBG_1234	0	0	N/A	G2SACK	
2011-07-20T14:46:30.092-0700	RBG_1234	Host ID 1	49877	3000348	G2S_request	communications.keepAlive	
2011-07-20T14:46:19.007-0700	RBG_1234	Host ID 1	0	0	N/A	G2SACK	
2011-07-20T14:46:18.988-0700	Host ID 1	RBG_1234	1813	3000347	G2S_response	communications.keepAliveAck	
2011-07-20T14:46:08.905-0700	RBG_1234	Host ID 1	0	0	N/A	G2SACK	
2011-07-20T14:46:08.884-0700	Host ID 1	RBG_1234	1813	3000347	G2S_response	communications.keepAliveAck	
2011-07-20T14:45:58.799-0700	RBG_1234	Host ID 1	0	0	N/A	G2SACK	

License valid for : 10761 day(s), 10 hour(s), 51 minute(s)

Desktop : rpa 2:46:36 PM 97M of 252M

View Summary Statistics

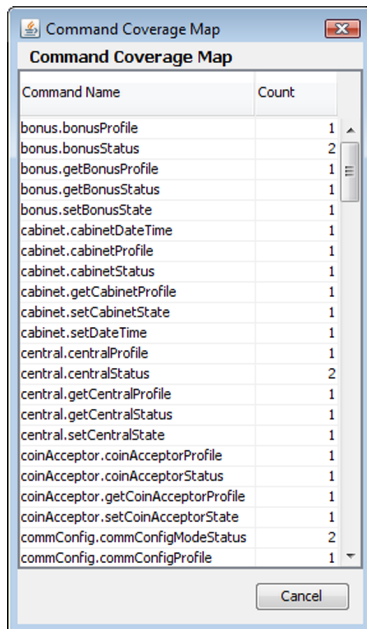
The Summary section provides statistics about the messages received from each endpoint as well as the Protocol Analyzer.

- **Error** - This section displays any messaging errors between the two endpoints. Double-click on an error to view additional details.
- **Forwarded Messages** - Number of messages RPA forwarded to the other side.
- **Time to ACK** - Minimum, Average, Maximum and Last time (in milliseconds) for the other side to send an acknowledgment message (G2SACK or S2SACK) for a command.
- **Received Messages** - Number of messages received from the endpoint.
- **SOAP Transport** - Click to connect (**Started**) or disconnect (**Stopped**) from client or host side.

View Summary Received Commands

The Coverage Map is a quick lookup for commands that have been processed by the Protocol Analyzer. It displays the command and the number of times the command has been sent.

To launch the Coverage Map, click **View Coverage Map**.



The Coverage Map does not update dynamically. To view the latest information, you must exit the screen by clicking **Cancel**, and re-launch the Coverage Map.

View Errors

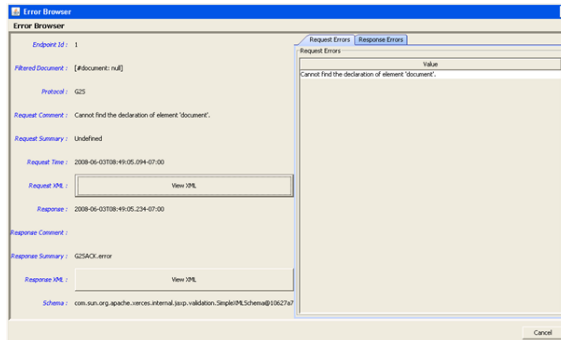
When the Protocol Analyzer receives a message with an error, it is displayed in the Error section of either the host or client endpoint.

The screenshot displays the RadBlue Protocol Analyzer interface. The top section shows the 'RPAController' and 'G2S Protocol Analyzer' tabs. The 'Error' section on the left highlights a message: 'Cannot find the declaration of element 'document''. Below this, the 'Host Side Information' section shows 'G2SHost Summary' with statistics for received and forwarded messages. A callout box explains: 'An empty Error section means that no errors were found in the messages received by RPA for the specified connection (for example, G2S Host or EGM).' The main area shows a list of messages with columns for Time, EGM, Command / Event, Applied Filter, and Message. A callout box states: 'Errors are reported for each connection.' The bottom section shows a 'Transcript' table with columns for Date Received, From Location, To Location, Command ID, Session ID, Session Type, Summary, and Comment.

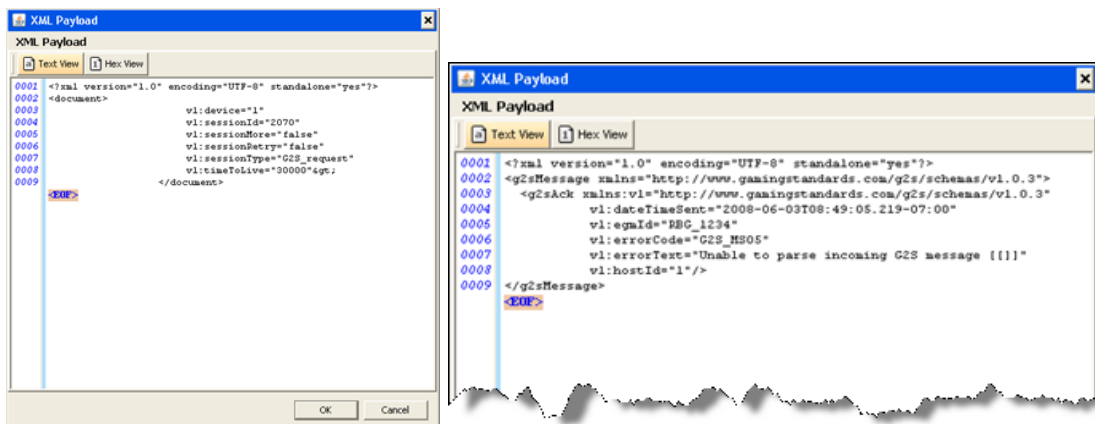
Date Received	From Location	To Location	Command ID	Session ID	Session Type	Summary	Comment
2011-07-20T14:46:30.109-0700	Host ID 1	RBG_1234	0	0	N/A	G2SACK	
2011-07-20T14:46:30.092-0700	RBG_1234	Host ID 1	49877	3000348	G2S_request	communications.keepAlive	
2011-07-20T14:46:19.007-0700	RBG_1234	Host ID 1	0	0	N/A	G2SACK	
2011-07-20T14:46:18.988-0700	Host ID 1	RBG_1234	1813	3000347	G2S_response	communications.keepAliveAck	
2011-07-20T14:46:08.905-0700	RBG_1234	Host ID 1	0	0	N/A	G2SACK	
2011-07-20T14:46:08.884-0700	Host ID 1	RBG_1234	1813	3000347	G2S_response	communications.keepAliveAck	
2011-07-20T14:45:58.799-0700	RBG_1234	Host ID 1	0	0	N/A	G2SACK	

To view errors, do the following:

1. Double-click the error you want to view.



3. The **Request Errors** and **Response Errors** tabs display the descriptive text associated with the error.
4. Click **View XML** to see the XML message associated with either the request or response.



The default view shows the XML message in text. Click **Hex View** to display the message in hexadecimal.

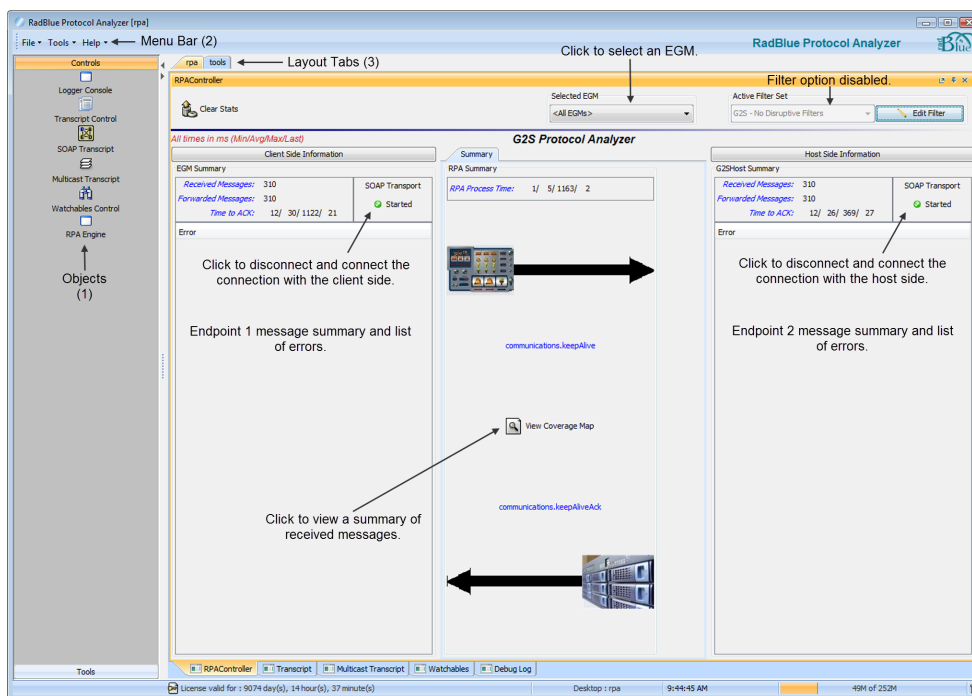
About Disruptive Filters

The optional Disruptive Filters feature provides additional RPA functionality that lets you manipulate selected G2S and S2S commands received by RPA to test system and EGM error handling functionality. All supported commands are available for filtering.

Disruptive filters are organized into filter sets. A filter set is a group of individual filters. By default, there is a filter set containing no disruptive filters and a filter set containing interactive filters. You can edit the filters in an existing set or create new filter sets to suit your testing needs.

There are two types of filters: interactive and automatic. Interactive filters, once configured, require manual handling of the selected command(s). Automatic filters, once configured, automatically filter the specified commands and events as messages are received by RPA. In addition, the commsOnline filter causes response commands to be routed through RPA. For information on each filter, see [Available Disruptive Filters](#).

To use disruptive filters, you must have a special RPA license that enables this feature. Otherwise, the disruptive filter functionality will be disabled as shown below.



Without Disruptive Filters

If you have any license issues with disruptive filters, please contact [Radical Blue Gaming](#).

View Disruptive Filters

You can see which disruptive filters are enabled through the [Debug Log](#).

When the RPA engine is started, an informational (INFO) message is logged with the active filter set and all enabled filters within the set. For example:

```
2010-01-29T15:18:26.275-08:00 [INFO] {general} G2S Interactive Filter
  Enabled filter : CommsOnline Filter
  Enabled filter : Interactive Filter
```

When you change the filter set or make changes to the active filters, your changes are reported in the Debug Log as well. For example:

```
2010-01-29T15:20:01.636-08:00 [INFO] {general} Setting active filter set to G2S Automatic
Filter
  Enabled filter : CommsOnline Filter
  Enabled filter : Automatic Filter
```

Edit a Filter Set

Filter sets are groupings of individual filters. When you modify an individual filter, you are modifying the individual filter associated with the specified filter set only.

You can configure the commands that are filtered for a filter set through the [RPA layout](#).

From the Edit Filter Set screen, you can:

- [Change the Filter Set Name and Description](#)
- [Change the Schema Used for Disruptive Filters](#)
- [Enable/Disable Individual Filters](#)
- [Configure Automatic Filters](#)
- [Configure Commands and Events for the Interactive Filter](#)

Once you have configured the filters, you can get started. See [Using the Automatic Filter Control](#) and [Using the Interactive Filter Control](#).

Change the Filter Set Name and Description

You can change the name and description for a filter set through the Edit Filter dialog box.

1. From the **RPA** layout, select the filter set you want to modify by clicking the **Active Filter Set** drop-down arrow.
2. Click **Edit Filter**.

3. The **Edit Filter Set** screen displays all available filters for the selected filter set.
4. Click in the **Filter Set Name** text box, and type a new name.
5. Click in the **Filter Set Description** text box, and type a new name.
6. Click **Save**.

Change the Schema Used for Disruptive Filters

You can change the schema used by a filter set through the Edit Filter dialog box.

1. From the **RPA** layout, select the filter set you want to modify by clicking the **Active Filter Set** drop-down arrow.
2. Click **Edit Filter**.
The **Edit Filter Set** screen displays all available filters for the selected filter set.
3. Click the **Schema Supported** drop-down arrow, and select the schema you want the filter set to validate against.
4. Click **Save**.

Enable/Disable Individual Filters

From the Edit Filter dialog box, you can enable or disable individual filters as needed.

1. From the **RPA** layout, select the filter set you want to modify by clicking the **Active Filter Set** drop-down arrow.
2. Click **Edit Filter**.
3. The **Edit Filter Set** screen displays all available filters for the selected filter set.
4. Select the checkbox in front of a filter to enable it, or clear the checkbox in front of a filter to disable it.
5. Click **Save**.

Configure Automatic Filters

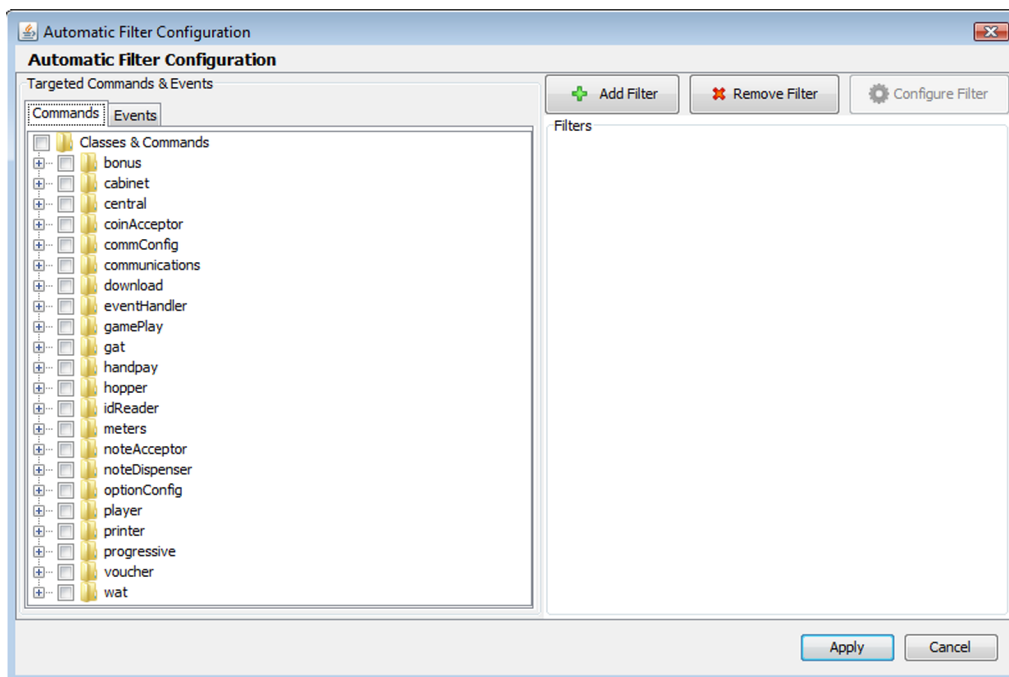
From the Automatic Filter Configuration screen, you can configure all automatic filters.

New or modified filters are applied immediately. Note that the RPA engine must be running to use disruptive filters.

For information on configuring each individual filter, see [Available Disruptive Filters](#).

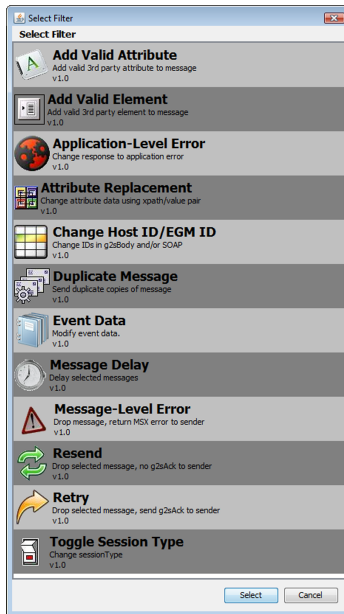
For information on using the Automatic Filter Control, see [Using the Automatic Filter Control](#).

1. From the RPA layout, click the **Active Filter Set** drop-down arrow and select **[G2S or S2S] - Automatic Filters**.
2. Click **Edit Filter**.
3. Click **Automatic Filter** to highlight it.
4. Click **Configure Filter**.

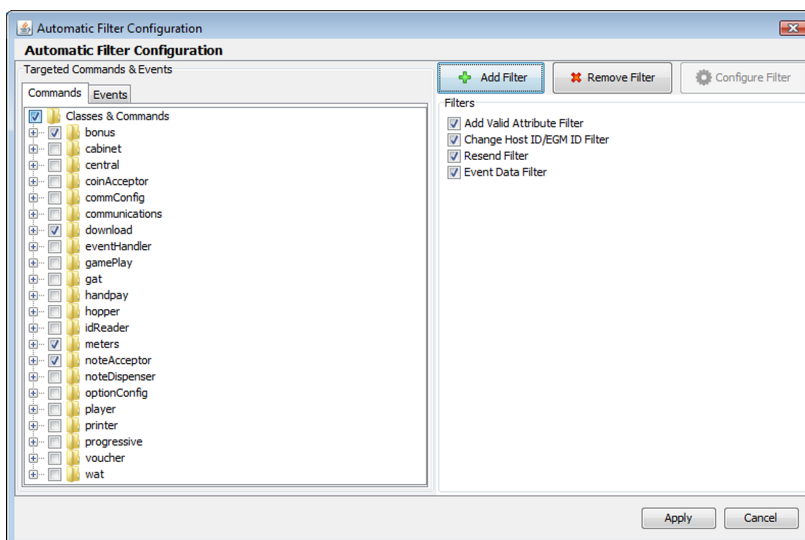


5. Select the classes and events you want to filter. Available classes and events reflect the protocol (G2S or S2S) and schema version in use.

- To add automatic filters, click **Add Filter**.



- Click the filter you want to add, and click **Select**.
Note: The filters available depend on the protocol, G2S or S2S, in use.
- Configure the selected filter as needed. For information on configuring each filter, see [Available Disruptive Filters](#).
- Once you configure the filter, click **Apply**. The filter is added to the Filters section of the Automatic Filter Configuration screen.



- Follow steps 1 to 9 for each automatic filter you want to add.

Using Automatic Filter Control

The Automatic Filter Control lets you specify filters that are automatically applied to messages as they pass through RPA. Note that the RPA engine must be running to use disruptive filters.

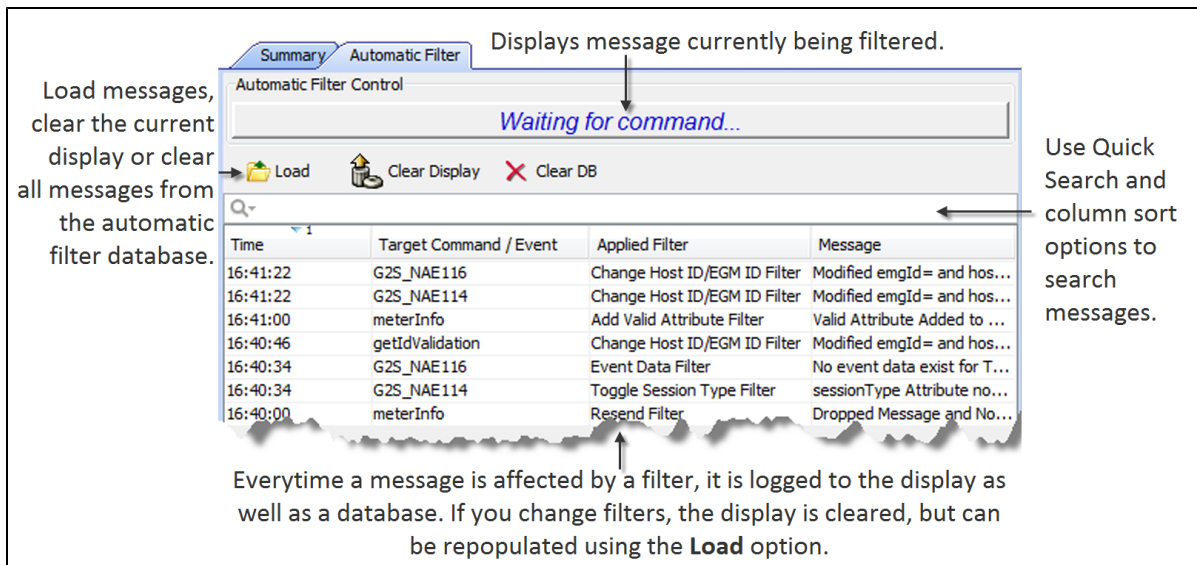
Each affected message is displayed in the Automatic Filter Control as well as in a database. The display is cleared each time you change filters, but you can use the Load option to import messages from the database into the display.

If the Clear Database on Startup configuration option is selected, the automatic filter database is cleared each time you start RPA. This is the same option that controls whether the transcript is cleared on startup. If you want to retain the automatic filter database information, clear the checkbox.

To access the Clear Database on Startup option, from the menu bar, select **Configure > Engine Options > Clear Database on Startup**.

1. From the RPA layout, click the **Active Filter Set** drop-down arrow, and select **[G2S or S2S] - Automatic Filters**.
2. Configure the commands and events you want to filter through the **Edit Filter Set** dialog box, which you can access by clicking **Edit Filter**. See [Configure Automatic Filters](#).
3. Configure the filters you want to apply to the selected commands and events. See [Available Disruptive Filters](#). Changes to automatic filters take effect immediately.

- Click the **Automatic Filter** tab to display the Automatic Filter Control.



- **Time** - Time message was sent to target entity.
 - **Target Command** - The G2S or S2S command that was affected by the filter.
 - **Applied Filter** - Filter applied to message. For information on individual filters, see [Available Disruptive Filters](#).
 - **Message** - Summary of how the message was acted upon by the applied filter.
- Double-click any row to display the message content in either text or hexadecimal. This information represents the message content as it was sent by RPA after the filter was applied.

Configure Commands and Events for Interactive Filters

From the Interactive Filter Configuration screen, you can select the commands and events you want to filter. Changes to this screen take effect immediately. Note that the RPA engine must be running to use disruptive filters.

When you apply a filter to a message, you may be prompted to select a filter option. For information on using each individual filter, see [Available Disruptive Filters](#).

For information on using the Interactive Filter Control, see [Using the Interactive Filter Control](#).

- From the RPA layout, click the **Active Filter Set** drop-down arrow and select **G2S - Interactive Filter**.
- Click **Edit Filter**.

The **Edit Filter Set** screen displays all available filters for the selected filter set.

3. Highlight the filter you want to modify by clicking the text.
4. Click **Configure Filter**.
5. In the **Timeout in sec** box, type select the number of seconds before messages not acted upon by the user are forwarded to the target entity. We recommend a number less than 30 seconds as messages typically time out after 30 seconds.

Note: When RPA receives multiple messages for filtering, it queues the messages and then handles each one in turn. The message delay begins once the message leaves the queue. If a message is queued more than zero (0) seconds, the Message column displays:

Delayed for x seconds. Queued for x sec(s).

“Delayed for x seconds” represents the queued time plus the delayed time.

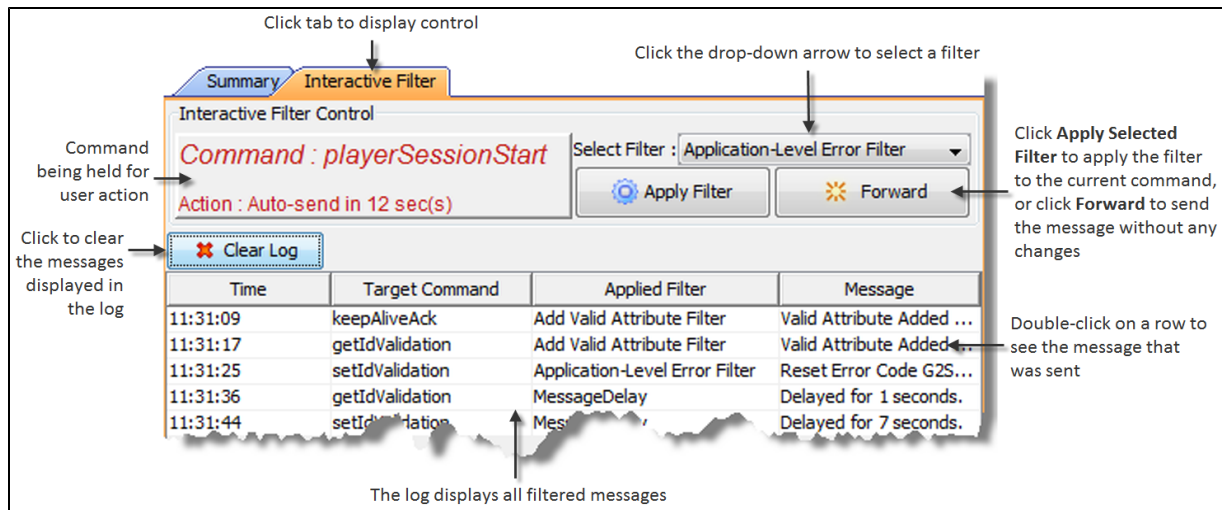
6. Select the check box for all commands you want to filter. You can select entire command classes, or click the plus (+) sign in front of a particular class to drill down to specific commands.
7. Click **Save**. Your changes take effect immediately.

Using the Interactive Filter Control

The Interactive Filter Control lets you apply filters to selected commands. Note that the RPA engine must be running to use disruptive filters.

1. From the **RPA** layout, click the **Active Filter Set** drop-down arrow, and select **[G2S or S2S] - Interactive Filters**.
2. Configure the commands you want to filter through the **Edit Filter Set** dialog box, which you can access by clicking the **Edit Filter** button on the RPA layout. See [Configure Commands and Events for the Interactive Filter](#).

3. Click the **Interactive Filter** tab to display the **Interactive Filter Control**.



4. For each command that RPA holds (displayed in red text on the lefthand side of the control), do one of the following:

- Click the **Select Filter** drop-down arrow, select the filter you want to apply, and click **Apply Filter**.
- Click **Forward** to send the command to the target entity without changes to the message.
- Let the command time out, and it will be sent without changes to the target. For information on setting the time-out value, see [Configure Commands and Events for the Interactive Filter](#).

5. Each filtered message appears in the log.
 - **Time** - Time message was sent to target entity.
 - **Target Command** - The G2S or S2S command that was affected by the filter.
 - **Applied Filter** - Filter applied to message. For information on individual filters, see [Available Disruptive Filters](#).
 - **Message** - Summary of how the message was acted upon by the applied filter.
6. Double-click any row to display the message content in either text or hexadecimal. This information represents the message content as it was sent by RPA after the filter was applied.

About Available Disruptive Filters

The following S2S and G2S disruptive filters are currently available in RPA:

- [Add Valid Attribute Filter \(G2S\)](#)
- [Add Valid Element Filter \(G2S\)](#)
- [Application-Level Error Filter \(G2S\)](#)
- [Attribute Replacement \(G2S\)](#)
- [Change Host ID/EGM ID Filter \(G2S\)](#)
- [Comm Host List Filter \(G2S\)](#)
- [CommsOnline Filter \(G2S and S2S\)](#)
- [Duplicate Message Filter \(G2S\)](#)
- [Edit Message Filter \(G2S\)](#)
- [Event Data Filter \(G2S\)](#)
- [Message Delay Filter \(G2S\)](#)
- [Message-Level Error Filter \(G2S\)](#)
- [Resend Filter \(G2S and S2S\)](#)
- [Retry Filter \(G2S and S2S\)](#)
- [Set Comm Change Filter \(G2S\)](#)
- [S2S Header Filter \(S2S\)](#)
- [S2S Reply to System Filter \(S2S\)](#)
- [Toggle Session Type Filter \(G2S\)](#)

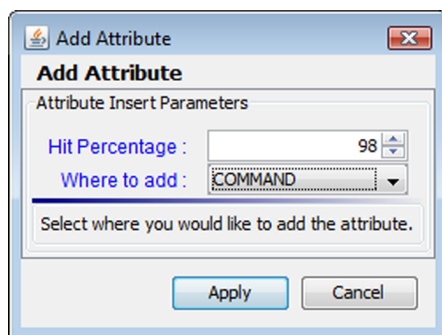
Note that disruptive filters are an optional feature and are subject to additional licensing requirements.

Add Valid Attribute Filter (G2S)

You specify the location within the message (`g2sBody`, `g2sMessage`, `class`, `command` and `sub-element`), and RPA supplies the added data.

1. If you are using interactive filters, access this filter by clicking the **Select Filter** drop-down on the Interactive Filter Control. See [Configure Commands and Events for the Interactive Filter](#).
or

If you are using automatic filters, access this filter by selecting **G2S - Automatic Filter** and clicking **Edit Filter** > **Configure Filter** option. See [Configure Automatic Filters](#).



2. For the automatic filter only, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click the **Where to add** drop-down arrow, and select where you want to insert an attribute into the message. See [Add Valid Attribute Filter Code Examples](#).
Note: The “random” option is available in the automatic filter only.
4. Click **Apply**.

Add Valid Attribute Filter Code Examples

When you apply the Add Valid Attribute filter to a message, you must choose where in the message you want the attribute placed. The following examples show where in a message a valid attribute would appear for each insertion option. Added attribute information is highlighted in blue.

Class

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody g2s:dateTimeSent="2009-07-21T13:58:20.279-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications xmlns:radblue="http://www.radblue.com/" g2s:commandId="19166"
      g2s:dateTime="2009-07-21T13:58:20.277-07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="3000290"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000"
      radblue:newAttribute="Valid Attribute Added">
      <g2s:keepAlive/>
    </g2s:communications>
  </g2s:g2sBody>
</g2s:g2sMessage>
```

Command

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody g2s:dateTimeSent="2009-07-21T14:00:27.557-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications g2s:commandId="19169" g2s:dateTime="2009-07-21T14:00:27.555-
      07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="3000293"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:keepAlive xmlns:radblue="http://www.radblue.com/"
        radblue:newAttribute="Valid Attribute Added"/>
    </g2s:communications>
  </g2s:g2sBody>
</g2s:g2sMessage>
```

g2sBody

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody xmlns:radblue="http://www.radblue.com/"
    g2s:dateTimeSent="2009-07-21T14:01:48.808-07:00"
    g2s:egmId="RBG_1234"
    g2s:hostId="1"
    radblue:newAttribute="Valid Attribute Added">
    <g2s:communications g2s:commandId="19171" g2s:dateTime="2009-07-21T14:01:48.806-07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="3000295"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:keepAlive/>
    </g2s:communications>
  </g2s:g2sBody>
</g2s:g2sMessage>
```

g2sMessage

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3"
  xmlns:radblue="http://www.radblue.com/"
  radblue:newAttribute="Valid Attribute Added">
  <g2s:g2sBody g2s:dateTimeSent="2009-07-21T14:02:25.810-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications g2s:commandId="19172" g2s:dateTime="2009-07-21T14:02:25.807-07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="3000296"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:keepAlive/>
    </g2s:communications>
  </g2s:g2sBody>
</g2s:g2sMessage>
```

Sub-Element

If there are multiple sub-elements in a message, the attribute is added to the first sub-element.

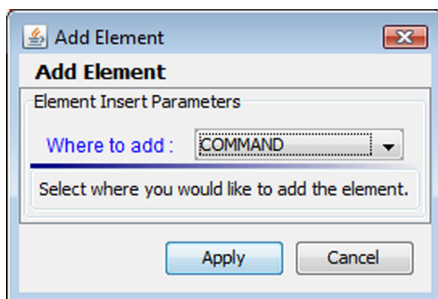
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<v1:g2sMessage xmlns:v1="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <v1:g2sBody v1:dateTimeSent="2009-07-21T14:07:32.340-07:00" v1:egmId="RBG_1234"
    v1:hostId="1">
    <v1:meters v1:commandId="14463" v1:dateTime="2009-07-21T14:07:32.341-07:00"
      v1:deviceId="1"
      v1:sessionId="4658"
      v1:sessionMore="false"
      v1:sessionRetry="false"
      v1:sessionType="G2S_request"
      v1:timeToLive="30000">
      <v1:getMeterInfo>
        <v1:getDeviceMeters xmlns:radblue="http://www.radblue.com/"
          radblue:newAttribute="Valid Attribute Added"
          v1:deviceClass="G2S_all"
          v1:deviceId="-1"
          v1:meterDefinitions="false"/>
        <v1:getGameDenomMeters v1:deviceClass="G2S_all" v1:deviceId="-1"
          v1:meterDefinitions="false"/>
        </v1:getMeterInfo>
      </v1:meters>
    </v1:g2sBody>
  </v1:g2sMessage>
```

Add Valid Element Filter (G2S)

You specify the location within the message (g2sBody, g2sMessage, class, command and sub-element), and RPA supplies the added data.

1. If you are using interactive filters, access this filter by clicking the **Select Filter** drop-down on the **Interactive Filter Control**. See [Configure Commands and Events for the Interactive Filter](#).
or

If you are using automatic filters, access this filter by selecting **G2S - Automatic Filter** and clicking **Edit Filter > Configure Filter** option. See [Configure Automatic Filters](#).



2. For the automatic filter only, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click the **Where to add** drop-down arrow, and select where you want to insert an element into the message. See [Add Valid Element Filter Code Examples](#).
Note: The “random” option is available in the automatic filter only.
4. Click **Apply**.

Add Valid Element Filter Code Examples

When you apply the Add Valid Element filter to a message, you must choose where in the message you want the element placed. The following examples show where in a message a valid element would appear for each insertion option. Added element information is highlighted in blue.

Class

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody g2s:dateTimeSent="2009-07-21T15:29:10.393-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications g2s:commandId="19303" g2s:dateTime="2009-07-21T15:29:10.391-
      07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="3000417"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:keepAlive/>
      <radblue:newElement xmlns:radblue="http://www.radblue.com/" />
    </g2s:communications>
  </g2s:g2sBody>
</g2s:g2sMessage>
```

Command

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody g2s:dateTimeSent="2009-07-21T15:30:36.394-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications g2s:commandId="19305" g2s:dateTime="2009-07-21T15:30:36.391-
      07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="3000419"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:keepAlive>
        <radblue:newElement xmlns:radblue="http://www.radblue.com/" />
      </g2s:keepAlive>
    </g2s:communications>
  </g2s:g2sBody>
</g2s:g2sMessage>
```

g2sBody

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<v1:g2sMessage xmlns:v1="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <v1:g2sBody v1:dateTimeSent="2009-07-21T15:31:30.790-07:00" v1:egmId="RBG_1234"
    v1:hostId="1">
    <v1:communications v1:commandId="14577" v1:dateTime="2009-07-21T15:31:30.791-07:00"
      v1:deviceId="1"
      v1:sessionId="3000420"
      v1:sessionMore="false"
      v1:sessionRetry="false"
      v1:sessionType="G2S_response"
      v1:timeToLive="0">
      <v1:keepAliveAck/>
    </v1:communications>
    <radblue:newElement xmlns:radblue="http://www.radblue.com/" />
  </v1:g2sBody>
</v1:g2sMessage>
```

g2sMessage

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody g2s:dateTimeSent="2009-07-21T15:34:18.935-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications g2s:commandId="19310" g2s:dateTime="2009-07-21T15:34:18.933-
      07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorText=""
      g2s:sessionId="3000424"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:keepAlive/>
    </g2s:communications>
  </g2s:g2sBody>
  <radblue:newElement xmlns:radblue="http://www.radblue.com/" />
</g2s:g2sMessage>
```

Sub-Element

If there are multiple sub-elements in a message, the element is added to the first sub-element.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<v1:g2sMessage xmlns:v1="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <v1:g2sBody v1:dateTimeSent="2009-07-21T15:36:05.957-07:00" v1:egmId="RBG_1234"
    v1:hostId="1">
    <v1:meters v1:commandId="14583" v1:dateTime="2009-07-21T15:36:05.957-07:00"
      v1:deviceId="1"
      v1:sessionId="4659"
      v1:sessionMore="false"
      v1:sessionRetry="false"
      v1:sessionType="G2S_request"
      v1:timeToLive="30000">
      <v1:getMeterInfo>
        <v1:getDeviceMeters v1:deviceClass="G2S_all" v1:deviceId="-1"
          v1:meterDefinitions="false">
          <radblue:newElement xmlns:radblue="http://www.radblue.com/" />
        </v1:getDeviceMeters>
        <v1:getGameDenomMeters v1:deviceClass="G2S_all" v1:deviceId="-1"
          v1:meterDefinitions="false"/>
        <v1:getWagerMeters v1:deviceClass="G2S_all" v1:deviceId="-1"
          v1:meterDefinitions="false"/>
      </v1:getMeterInfo>
    </v1:meters>
  </v1:g2sBody>
</v1:g2sMessage>
```

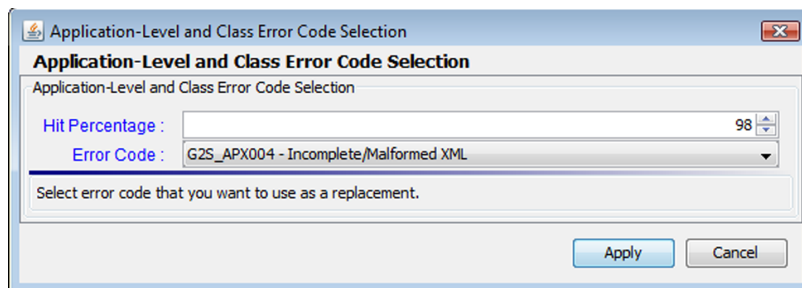
Application-Level Error Filter (G2S)

This filter acts on responses only. If the specified command is a request, it is not affected.

You select an application-level or command class error from a list. The available errors depend on the current schema. The error replaces the response and RPA forwards it to the intended recipient. The response may originate from an EGM or a host.

1. If you are using interactive filters, access this filter by clicking the **Select Filter** drop-down on the **Interactive Filter Control**. See [Configure Commands and Events for the Interactive Filter](#).
or

If you are using automatic filters, access this filter by selecting **G2S - Automatic Filter** and clicking **Edit Filter > Configure Filter** option. See [Configure Automatic Filters](#).



2. For the automatic filter only, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click the **Error Code** drop-down arrow, and select an application-level error to add to the response command.

For information on each error, see the Gaming Standard Association (GSA) message protocol document for the protocol you are using.

4. Click **Apply**.

Attribute Replacement (G2S)

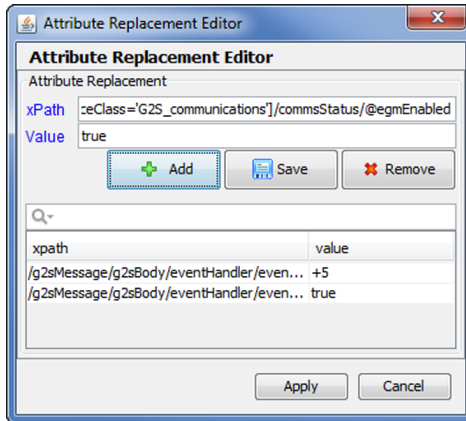
This filter allows you to use an XPath expression to replace a value in a command attribute. When the Attribute Replace filter is enabled, RPA looks for the attribute you specify and replaces the existing value with the new value. You can configure multiple attribute replacements through this filter.

Note that you can increment or decrement a numeric value using the notation “+n” or “-n” as the value. For example “+5” would increment the existing attribute value by five. Otherwise, the attribute value is replaced by the exact value you specify.

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Interactive Filter**. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



2. Type an XPath expression in the **xPath** field.

Sample XPath Expression Format

/g2sMessage/g2sBody/communications/commsOnLine/@metersReset

g2s:g2sMessage	g2s:g2sBody	g2s:cabinet	g2s:cabinetStatus	@g2s:denomId
message	body	class	message type	attribute name

3. Type the replacement value in the **Value** field.
You can increment or decrement a numeric value using the notation “+n” or “-n” as the value. For example “+5” would increment the existing attribute value by five. Otherwise, the attribute value is replaced by the exact value you specify.
4. Click **Add**.
5. Repeat steps 2 through 4 to add additional XPath expressions.
6. Click **Apply**.

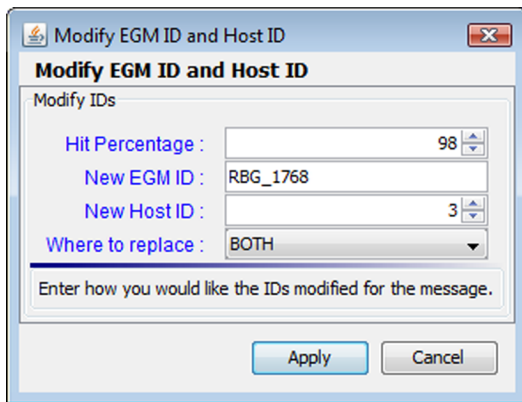
Change Host ID/EGM ID Filter (G2S)

This filter lets you modify the host ID and/or EGM ID within a message, which tests whether the target entity validates these attributes for each received message.

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Interactive Filter**. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



Note: For convenience, the default values are the values in the selected message.

2. For the automatic filter only, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click inside the **New EGM ID** text box, and type a new EGM identifier. Note that the EGM ID must conform to the GSA message protocol standard for EGM identifiers.
4. In the **New Host ID** box, type or select a new host identifier.
5. Click the **Where to replace** drop-down arrow, and select whether to change the IDs in the `g2sBody`, in the SOAP header, or in both locations.
6. Click **Apply**.

Comm Host List Filter (G2S)

The Comm Host List filter sets the *canModRemote* attribute to **false** for the `commHostItem` element that has RPA's URL. When this filter is selected, the host cannot modify the `commHostItem` in the `commHostList`, which effectively disables `commConfig` changes for that host. This allows you to continue to use RPA even if the host re-writes the *hostLocation* to something other than the RPA URL. By default, this filter is disabled.

CommsOnline Filter (G2S and S2S)

For G2S, the `commsOnline` filter changes the *egmLocation* attribute in the G2S `commsOnline` command from the EGM's location to the RPA's location, so response commands are sent to RPA rather than to the EGM.

For S2S, the `commsOnline` filter changes the *s2sLocation* attribute in the S2S `commsOnline` command from the target host's location to the RPA's location.

If the `commsOnline` filter is not enabled, response commands are sent directly to the EGM or host, with responses going around rather than through RPA. There is no user interface tab associated with the `commsOnline` filter.

Duplicate Message Filter (G2S)

This filter duplicates a message from one to 10 times.

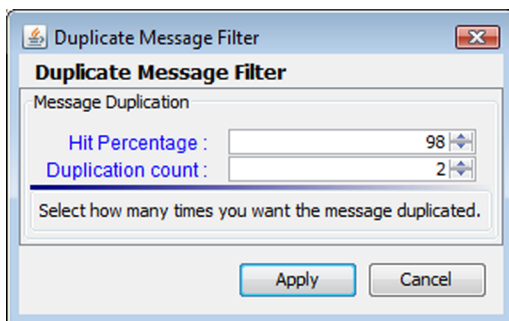
For the automatic filter, you define the minimum and maximum number of times the filter should be duplicated.

Duplicate copies of the message are resent as soon as the `g2sAck` response is received. A `g2sAck` command response is sent to the originator after all duplicate messages have been sent.

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Interactive Filter**. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).

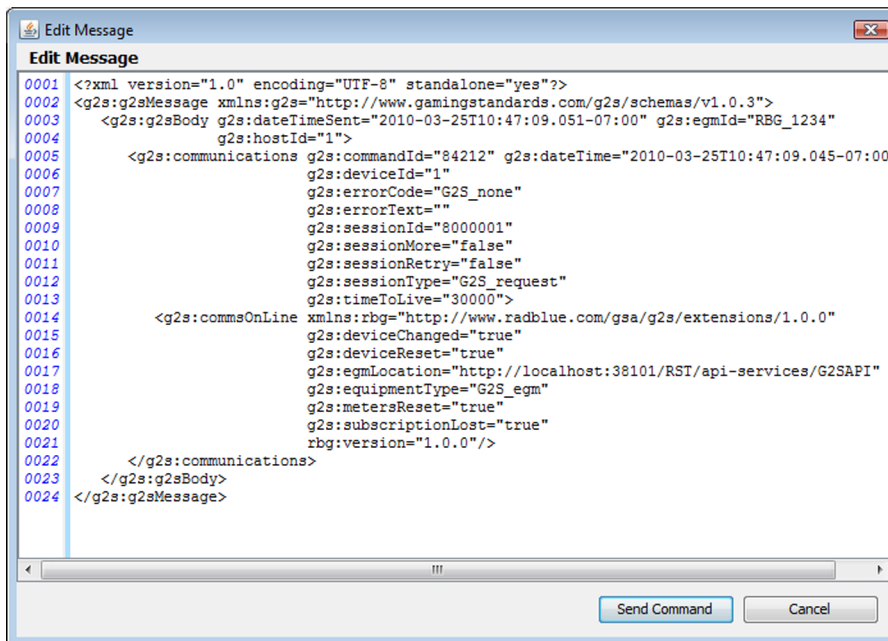


2. *For the automatic filter only*, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. In the **Duplication count** box, type or select the number of additional times you want RPA to send the message. For example, if you select three (3), the duplicate message would be sent four times - once for the original message, plus three additional times.
4. Click **Apply**.

Edit Message Filter (G2S)

This filter lets you change the selected message's XML content. This filter is available as an interactive filter only.

1. Click the **Select Filter** drop-down on the Interactive Filter Control, and select **Edit Message**. See [Configure Commands and Events for the Interactive Filter](#).
2. When a selected command or event is received by RPA (appearing in upper left corner of the Interactive Filter Control), click **Apply Filter**.



3. Click inside the **Edit Message** screen, and make changes as required.
4. Click **Send Command**.

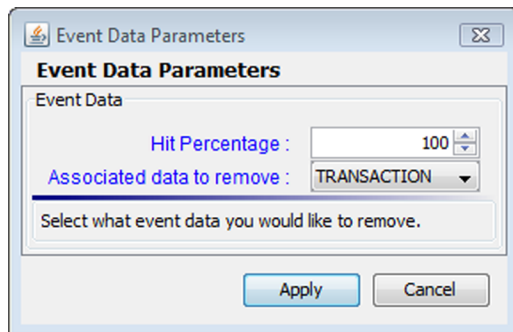
Event Data Filter (G2S)

This filter removes associated data for specific data types, randomly selected data types or all data types. You can remove class meters, device meters, all meters, transaction data or status information.

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting G2S - Interactive Filter. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



2. *For the automatic filter only*, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click the **Associated data to remove** drop-down arrow, and select the associated data you want to remove from the message.
4. Click **Apply**.

Message Delay Filter (G2S)

Interactive filter messages are delayed while waiting for user input. Messages that are not acted upon within a user-specified amount of time are automatically forwarded to the target entity.

Note: When RPA receives multiple messages for filtering, it queues the messages and then handles each one in turn. The message delay begins once the message leaves the queue. If a message is queued more than zero (0) seconds, the Message column displays:

Delayed for x seconds. Queued for x sec(s).

“Delayed for x seconds” represents the queued time plus the delayed time.

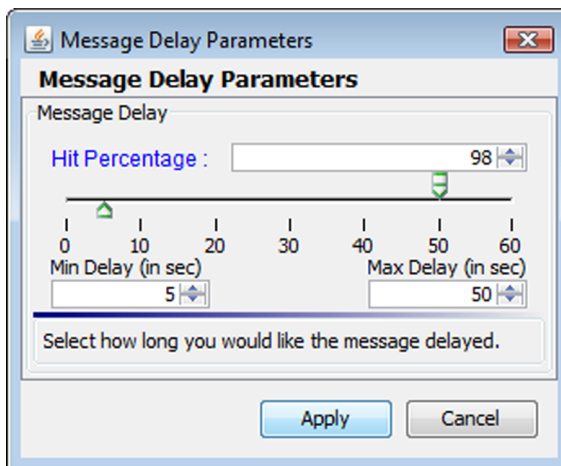
For automatic filter messages, the filter configuration includes a delay range (X to Y seconds), after which the message is forwarded to the recipient.

For information on setting the time-out value, see [Change the Filter Set Name and Description](#).

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Interactive Filter**. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



2. For the automatic filter only, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click the **Associated data to remove** drop-down arrow, and select the associated data you want to remove from the message.
4. Click **Apply**.

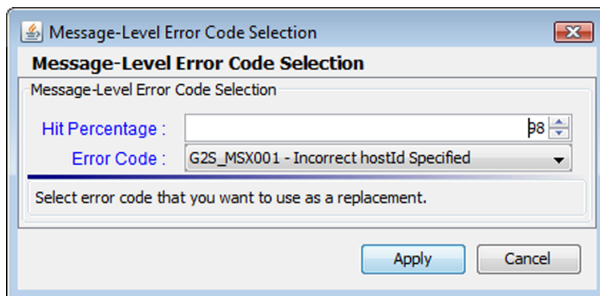
Message-Level Error Filter (G2S)

Select a message-level error from list. The error replaces the `g2sAck` to the originator, and the original message is not forwarded to the recipient.

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Interactive Filter**. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



2. For the automatic filter only, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
3. Click the **Error Code** drop-down arrow, and select an message-level error to add to the response command.

For information on each error, see the Gaming Standard Association (GSA) message protocol document for the protocol you are using.

4. Click **Apply**.

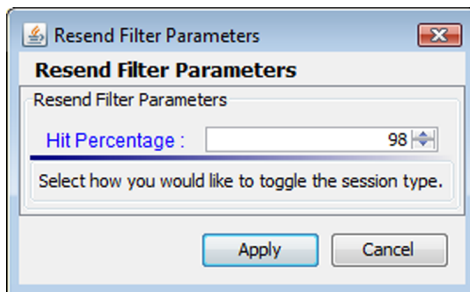
Resend Filter (G2S and S2S)

The resend filter drops the specified message without sending a `g2sAck` or `s2sAck` to the originator (so the originator realizes the message was lost).

1. If you are using interactive filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Interactive Filter**. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



2. *For the automatic filter only*, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
If you are using the interactive filter, no prompt is displayed. The filter is applied to the message when you click **Apply Filter**.
3. Click **Apply**.

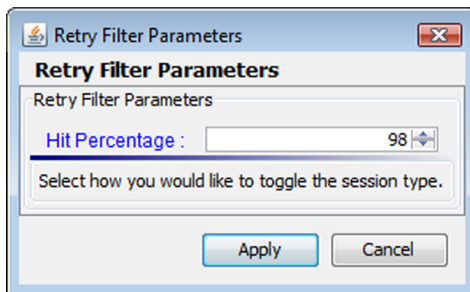
Retry Filter (G2S and S2S)

The retry filter drops the specified message, but sends a `g2sAck` or `s2sAck` to the originator (so the originator thinks the message was sent successfully, but then times out when the response message is not received).

1. If you are using interactive filters, access this filter by clicking the Select Filter drop-down on the Interactive Filter Control. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by selecting **[G2S or S2S] - Automatic Filter** and clicking **Edit Filter > Configure Filter** option. See [Configure Automatic Filters](#).



2. *For the automatic filter only*, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect.
If you are using the interactive filter, no prompt is displayed. The filter is applied to the message when you click **Apply Filter**.
3. Click **Apply**.

Set Comm Change Filter (G2S)

The Set Comm Change filter lets you use RPA even if the host has re-written the *hostLocation* to something other than the RPA location by re-writing RPA's URL in the `commHostList` command and replacing it with the host's URL. Additionally, this filter replaces the host's URL in the `setCommChange` command with RPA's URL.

This means that the host sees itself in the `commHostList` command and should not resend the `setCommChange` command unless it is absolutely necessary.

S2S Header Filter (S2S)

This filter changes the *fromSystem* attribute in the `s2sHeader` element from the sending system URL to the RPA URL. For example:

s2sHeader Element into RPA	RPA	S2sHeader Element Out of RPA
<pre><s2sHeader fromSystem = "hostA" toSystem = "hostB" messageId = "12345678" dateTimeSent = "2004-2-27T10:54:27.123-05:00" /></pre>	<p>s2sHeader Filter Applied</p>	<pre><s2sHeader fromSystem = "rpa" toSystem = "hostB" messageId = "12345678" dateTimeSent = "2004-2-27T10:54:27.123-05:00" /></pre>

The `s2sHeader` element appears in all S2S commands. This filter cannot be disabled.

S2S Reply to System Filter (S2S)

This filter changes the *replyToSystem* attribute in the `s2sHeader` element from original value to the RPA URL. For example:

replyToSystem Attribute into RPA	RPA	replyToSystem Attribute Out of RPA
<pre><s2s:communications s2s:commandId="27" s2s:dateTime="2010-02-12T16:57:59.979-08:00" s2s:propertyId="12" s2s:replyToSystem="hostA" s2s:sessionId="23" s2s:sessionRetry="0" s2s:sessionType="request" s2s:timeToLive="30000"></pre>	<p>replyToSystem Filter Applied</p>	<pre><s2s:communications s2s:commandId="27" s2s:dateTime="2010-02-12T16:57:59.979-08:00" s2s:propertyId="12" s2s:replyToSystem="rpa" s2s:sessionId="23" s2s:sessionRetry="0" s2s:sessionType="request" s2s:timeToLive="30000"></pre>

The *replyToSystem* attribute appears in all complex command requests. This filter cannot be disabled.

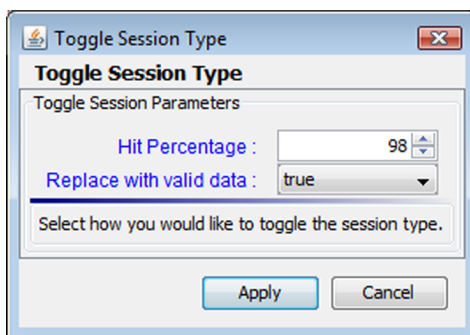
Toggle Session Type Filter (G2S)

This filter changes the *sessionType* attribute for the specified message. You can replace the session type with valid data (for example, change “request” to “notification”) or replace the session type with invalid data.

1. If you are using interactive filters, access this filter by clicking the Active Filter Set drop-down and selecting G2S - Interactive Filter. See [Configure Commands and Events for the Interactive Filter](#).

or

If you are using automatic filters, access this filter by clicking the **Active Filter Set** drop-down and selecting **G2S - Automatic Filter**. See [Configure Automatic Filters](#).



3. *For the automatic filter only*, click the **Hit Percentage** drop-down arrow, and select the percentage of applicable messages received that you want this filter to affect. Click the **Replace with valid data** drop-down arrow, and select either **true** or **false**.
4. Select true to replace the *sessionType* attribute with different, valid data:
 - G2S_request is changed to G2S_notification
 - G2S_response is changed to G2S_request
 - G2S_notification is changed to G2S_requestSelect false to replace the *sessionType* attribute value with invalid data (`g2s:sessionType="RBG_junk"`).
4. Click **Apply**.

Working with the Message Transcript

The Message Transcript lets you examine individual commands sent from, or received by, the tool. The data displayed is extracted directly from received G2S or S2S messages (depending on the protocol you are using).

Filtering options offer you a variety of ways to view information. Each instance of the transcript within the tool can be filtered differently.

At the top of the Transcript screen are several options:

- **EGM Selector** - Click the drop-down arrow, and select to view the transcript information for a specific EGM, all EGMs or multiple EGMs (CTRL+click).
- **Host Selector** - Click the drop-down arrow, and select to view the transcript information for a specific host system or all host systems.
- **[Load](#)** - Load transcript messages from the database so you can work with them through the user interface.
- **[Compare](#)** - View the details of any two messages side-by-side.
- **[Filters](#)** - This control allows you to select which commands are to be included on the display. Make any changes, and then press **OK** to have the tool update the display. This control currently resets when a new data set is loaded.
- **[Search Content](#)** - Search through the contents of all displayed messages in this transcript instance for the entered text pattern (case sensitive). Clicking on a row in the returned list gives you access to the HTTP header and message contents of the selected message.
- **[Set Comment](#)** - Adds a comment to the Comment column of the selected message.
- **[Clear Display](#)** - Clears the displayed messages in this instance of the transcript control.
- **[Clear Database](#)** - Clears all records of this type in the database for this instance of the tool.
- **[Analyze](#)** - *Available for G2S messaging only.* Provides a user-friendly summary of transcript messages.

The size limit of the Message Transcript file is 1 GB. Once the limit is reached, older records are purged.

A Note on Converting Time in the Message Transcript

If the tool receives a date/time with the seconds parsed greater than milliseconds, the time/date is truncated to milliseconds in the transcripts. For example:

The date/time `2013-04-30T08:03:46.1234567890-07:00`

displays as `2013-04-30T08:03:46.123-07:00` in the transcript.

You can view the longer date/time format on the **XML** tab of the [command object](#). To access the command object, double-click any message in the transcript.

Transcript Column Headers

The following columns are available in the transcript:

- **Command ID** - Command ID associated with message.
- **Comment** - Information entered by the user about a specific message. This field is *not* part of the actual message. Comments exist *only* in the tool in which they are entered.
- **Date Received** - Date and time message was received by the tool.
- **Device** - Class and identifier of device where the message is being sent to or from.
- **Event Code** - Code for associated event.
- **Event Date/Time** - Date and time that event was sent.
- **Event ID** - Identifier for associated event.
- **Event Text** - Description of associated event.
- **From Location** - Identifier of entity (for example, EGM or host) that sent the message.
- **Message ID** - Unique identifier associated with the message.
- **Session ID** - Session ID associated with message.
- **Session Type** - Indicates how the message should be processed: as a request, response or notification.
- **Summary** - Actual G2S or S2S command within the message. If more than one command is sent in a message, only the first command appears in the transcript. However, all commands with the message are displayed in the detail view, which you can access by double-clicking the message.
For G2S_GPE112 (Game Ended) events, the outcome of game play (the *playResult* attribute) is shown in the Summary column in brackets (for example, **eventReport:G2S_GPE112 - Game Ended [Lost]**).
- **To Location** - Identifier of the intended target of the message.

You can slide the columns around to rearrange their order. To move a column header, left-click and hold while you move the column to its new location. You can also click any column to re-sort it, or use CTRL + left-click to sort on multiple columns.

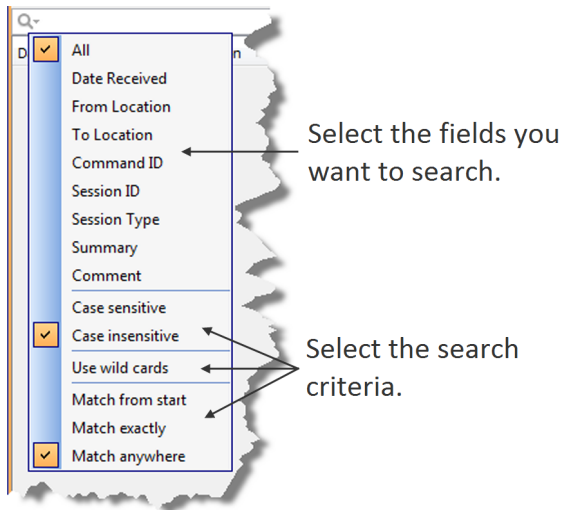
If you right-click on a column header, a menu displays that allows you to automatically resize one or all columns (based on the displayed data in the columns), as well as to indicate which columns you would like to display.

Clicking on any column header causes the data to be sorted using that header. Click once to sort the column in ascending order. Click a again to sort the column in descending order. The third click clears the sort.

If you want to sort on multiple columns, use the CTRL key when clicking the column headers.

Filter Transcript Messages Using the Quick Filter

Just below the Transcript options is a magnifying glass and entry field that allows you to filter messages based on entered data. To filter the displayed data, click inside the entry field and start typing. The displayed data is automatically filtered as you type.



Clicking on the magnifying glass gives you a menu that you can use to provide additional selection criteria.

This powerful tool allows you to immediately view any set of messages that you can imagine, limited only by the data displayed in the columns.

What Are You Looking for in the Transcript?

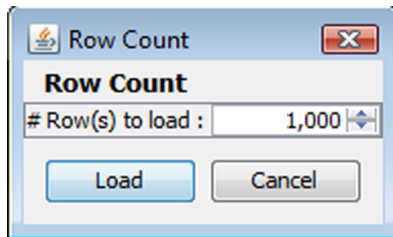
- *Are the correct commands being sent?*
For example, is the `commsOnLine` command being sent during startup?
- *Are messages being acknowledged* (for example, with a `g2sAck` as well as a message acknowledgments?)
- *Are there correct request-response pairs?*
For example, if a `communications.getDescriptor` command is sent (outbound), a corresponding `communications.descriptorList` command should be received (inbound). Note that the Session ID is the same for the request and response.

Load Messages into the Transcript

The Load option lets you display a pre-defined number of messages in the transcript.

If you are using RGS, be sure the EGM for which you want to view information is selected.

1. Click the **Transcript** tab on the **Transcripts** layout.
2. From the Transcript object, click **Load**.



3. Type the number of messages you want to display, and click **Load**.
The Transcript display populates with the requested number of messages.

Compare Messages in the Transcript

The Compare option lets you view the details of two messages, side-by-side. You can choose to view the message content in three different formats: in a user-friendly format, XML format, and XML format with the differences between the two messages highlighted in **red**.

The Compare option is available when you view the [Event Report](#) as well as in the main Message Transcript.

1. While holding down the CTRL key, click the two messages you want to compare.
2. Click **Compare**.

The selected messages display side-by-side, allowing you to scroll through the details of each message to compare them.

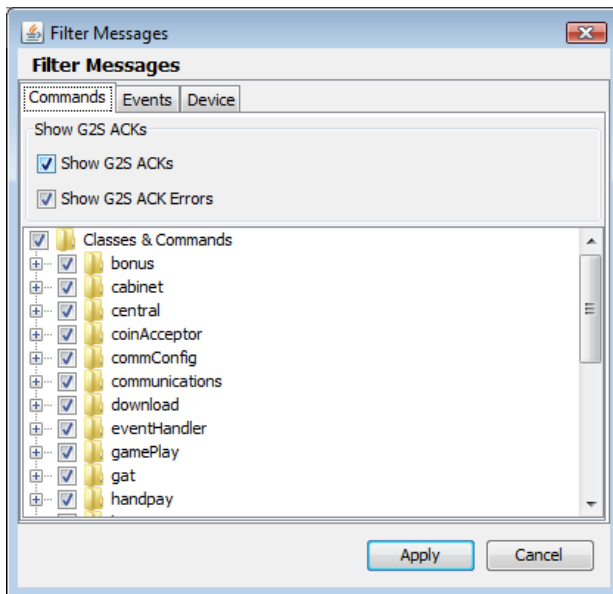
The **Command** tab displays command information in an easy-to-read format along with any meters.

4. Click **View XML** to view the XML for the messages.
5. Click **Diff** to view the XML with the changes highlighted in red.
6. Click **OK** to close the compare view.

Filter Messages in the Transcript

The Filters option in the Transcript lets you select the commands, events or devices you want to display in the transcript window. Use this option to narrow the transcript view to just the messages that interest you. The excluded data is not deleted from the transcript database; it is just not displayed and can always be included again.

1. Click the **Transcript** tab on the **Transcripts** layout.
2. Click **Filters**. The Filter Messages screen displays with three tabs: Commands, Events and Device.



3. On each tab, select the check box of the commands, events and devices you want to display in the Transcript, and clear the check box of the commands, events and devices you want to hide.
By default, the `g2sAck` command is cleared (does not display).

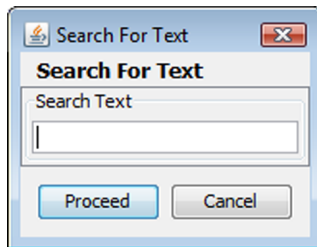
4. Click **OK**.

Your changes take effect immediately.

Search the Content of Transcript Messages

The Search Content option lets you search transcript message content for keywords.

1. Click the **Transcript** tab on the **Transcripts** layout.
2. Click **Search Content**.



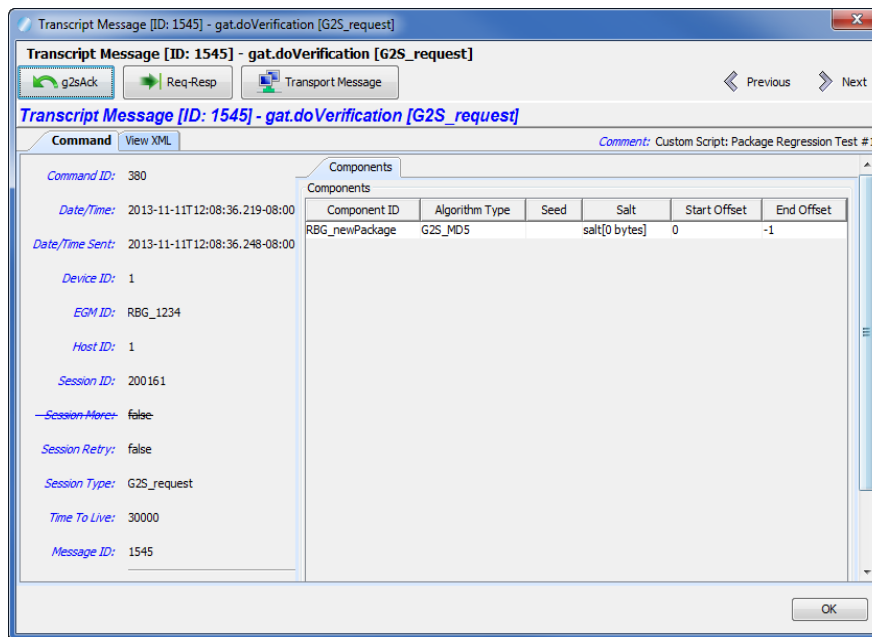
3. Type the keywords for your search, and click **Proceed**.
The **Transcript Search Results** screen displays all conforming messages.
4. To view the details of a message, double-click the message.
5. Click **Back** to close the Transcript Search Results window.

View Command Objects through the Transcript

A command object is a graphical representation of a command (as opposed to viewing the command in XML format). You can view command objects on the message details screen. List information for complex commands displays in tabs to the right of the command attributes. From the message details screen you can link to the `g2sAck` message, corresponding request-response pair command or to the associated SOAP message for any command. Attributes that are deprecated in G2S 2.1 display in a strike-through font (for example, ~~Enable Money Out~~). Comments associated with the message are displayed next to the Command and View XML tabs.

To display a message's command object:

1. Double-click the command you want to view.
2. Click the **Command** tab.

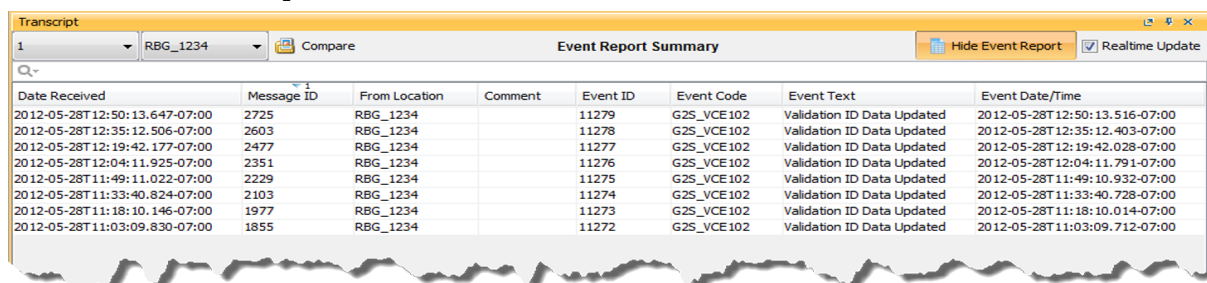


3. Click **Previous** and **Next** to navigate through the transcript list while in the message detail view.
4. Click **g2sAck** to view the corresponding acknowledgment to the selected command.
5. Click **Req-Resp** to view the corresponding command in the request-response pair.
6. Click **Transport Message** to view the command's associated SOAP message.
7. Click **OK** to return to the transcript.

View the Event Report

The Event Report displays all events sent and received by the tool. You can toggle between the Transcript view and the event view by clicking **Show/Hide Event Report**. The [Compare](#) option lets you compare two event messages.

1. Click the **Transcript** tab on the **Transcripts** layout.
2. Click **Show Event Report**.



The screenshot shows a window titled "Transcript" with a tab labeled "1" and a dropdown menu showing "RBG_1234". There is a "Compare" button and a "Hide Event Report" button. The main area is titled "Event Report Summary" and contains a table with the following data:

Date Received	Message ID	From Location	Comment	Event ID	Event Code	Event Text	Event Date/Time
2012-05-28T12:50:13.647-07:00	2725	RBG_1234		11279	G2S_VCE102	Validation ID Data Updated	2012-05-28T12:50:13.516-07:00
2012-05-28T12:35:12.506-07:00	2603	RBG_1234		11278	G2S_VCE102	Validation ID Data Updated	2012-05-28T12:35:12.403-07:00
2012-05-28T12:19:42.177-07:00	2477	RBG_1234		11277	G2S_VCE102	Validation ID Data Updated	2012-05-28T12:19:42.028-07:00
2012-05-28T12:04:11.925-07:00	2351	RBG_1234		11276	G2S_VCE102	Validation ID Data Updated	2012-05-28T12:04:11.791-07:00
2012-05-28T11:49:11.022-07:00	2229	RBG_1234		11275	G2S_VCE102	Validation ID Data Updated	2012-05-28T11:49:10.932-07:00
2012-05-28T11:33:40.824-07:00	2103	RBG_1234		11274	G2S_VCE102	Validation ID Data Updated	2012-05-28T11:33:40.728-07:00
2012-05-28T11:18:10.146-07:00	1977	RBG_1234		11273	G2S_VCE102	Validation ID Data Updated	2012-05-28T11:18:10.014-07:00
2012-05-28T11:03:09.830-07:00	1855	RBG_1234		11272	G2S_VCE102	Validation ID Data Updated	2012-05-28T11:03:09.712-07:00

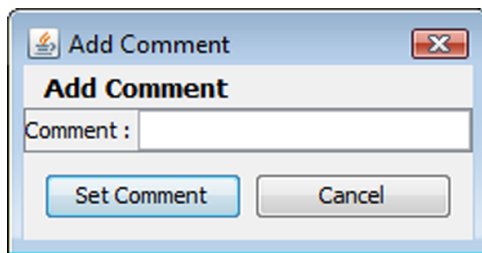
- **Date Received** - Date and time message was received by the tool.
 - **Event Code** - Code associated with event (for example, G2S_VCE102).
 - **Event Date/Time** - Date and time message was received by the tool.
 - **Event ID** - Event identifier.
 - **Event Text** - Text of associated event code (for example, Validation ID Data Updated).
 - **From Location** - Identifier of entity (for example, EGM or host) that sent the event.
 - **Message ID** - Message identifier.
3. Double-click any record to view the details of the message in which the event was sent.
 4. Click **OK** to close the message detail screen.
 5. Click **Hide Event Report** to return to the Transcript view.

Add a Comment to a Transcript Message

The Set Comment option lets you add a comment to any message in the transcript. Comments are part of the transcript only. Messages are not modified by comments.

Note: Comments associated with a message are displayed next to the Command and View XML tabs when you view the message details.

1. Single-click the message to highlight it.
2. Click **Set Comment**.



3. Type your comment, and click **Set Comment**.

The message is highlighted in blue, and the comment appears in the Comment field.

Export Message Content to Excel

The Export to Excel File right-click option lets you quickly export the content of a G2S command to a Microsoft Excel spreadsheet. The following G2S commands can be exported to Excel:

- **`communications.descriptorList`**

Exports all attributes for each supported device, sorted by device class and device ID.

- **`eventHandler.eventSubList`**

- **`eventHandler.setEventSub`**

- **`eventHandler.supportedEvents`**

If an event in the `eventHandler.supportedEvents` command does not contain the event text, the event text is added automatically if it is not included in the original message.

- **`meters.meterInfo`**

- **`optionConfig.optionList`**

To export message content to an Excel spreadsheet:

1. Click the **Transcript** tab on the **Transcripts** layout.
2. Click to highlight the command you want to export.
3. Right-click inside the selected record, and select **Export to Excel File**.
4. Type a name for the file.
5. Click **Save**.

A confirmation message displays with the number of records saved in the file.

6. Click **OK**.

Export Transcript Entries

The Export to Transcript File option lets you quickly export all or select Transcript entries for review. This file can then be imported into the RadBlue Analysis Suite (RAS) for further analysis.

This option is useful when an issue has been narrowed down to a limited set of commands. Rather than exporting a large set of troubleshooting data using the Export Debug option on the Debug tab, you can send only the specific command(s) involved in the issue.

You can import the Transcript file directly into RAS by using the Import option.

1. Click the **Transcript** tab on the **Transcripts** layout.
2. Select the Transcript records you want to export.
There are several ways to select records:
 - a. Click to select a single record.
 - b. CTRL+click to select multiple records.
 - c. SHIFT+click to select a block of records. Click once on the first record and once on the last record to highlight the entire block.
 - d. For another way to select a block of records, right-click and hold on the first row. Then, drag the cursor down the screen, highlighting each row as you go, until you come to the last row you want to export.
 - e. CTRL+a to select all Transcript records.
3. Right-click inside the Transcript, and select **Export to Transcript File**.
4. Type a name for the file.
5. Click the Files of Type drop-down arrow, and select either a **S2S Transcript (*.s2t)** or a **G2S Transcript (*.g2)** file extension. Your selection corresponds to the protocol you are using with the tool (either G2S or S2S).
6. Click **Save**.
A confirmation message displays with the number of records saved in the file.
7. Click **OK**.

Clear the Transcript Display

The Clear Display option lets you clear all transcript messages from the table. This option *does not* remove messages from the transcript database.

Click **Clear > Display** to remove all messages from the current view.

Clear the Transcript Database

The Clear Database option lets you remove all transcript records from the transcript database, clears transcript messages from the table and clears the EGM selector list. Note that this action cannot be undone.

1. Click **Clear > Database**.
2. Click **Yes** to remove all data from the transcript database, or click **No** to return to the transcript without clearing the database.

About the EGM Transcript Analysis Report

The EGM Transcript Analysis report provides information about messages that were sent from and received by the application for the period requested. The purpose of this report is to provide the user with a user-friendly summary of G2S messages.

The report is divided into several sections to assist your analysis of the information:

- [Transcript Summary](#) - Information related to the computer running the installed application.
- [Transcript](#) - Transaction log of sent and received G2S and S2S messages. G2S acknowledgements and, optionally, keepAlive messages are filtered out.
- [Sessions](#) - Transcript messages grouped by session ID.
- [Device Commands](#) - Transcript messages grouped by affected G2S device.
- [Device States](#) - Status of each device and any device status changes for the requested time period.
- [Events](#) - Events generated by the EGM.
- [G2S ACK Errors](#) - G2S acknowledgement messages containing errors.
- [Meters](#) - Meter values.
- [Messages](#) - G2S XML messages from the transcript.

The EGM Transcript Analysis report can be output to an HTML page or to an XML file.

Generate the Transcript Analysis Report

1. Click **Analyze**. If you are using the Advanced Transcript Analyzer feature, click the **Analyze** drop-down arrow and select **General**.
 - **EGM ID** (required) - *RGS only*. Type the identifier of the EGM on which you want to report. If you are using a RadBlue product other than RGS, this field does not display.
 - **Start Date** - Click the drop-down arrow to select the beginning date and time of the reporting period.
 - **End Date** - Click the drop-down arrow to select the ending date and time of the reporting period.
 - **Ignore keepAlives** - Select if you do not want to see `keepAlive` and `keepAliveAck` commands on your report.
 - **OutPut Options** - Select **Produce Transcript Report** to export the Transcript Analysis report directly to HTML, or select **Produce Transcript File** to export the Transcript Analysis report to an XML file. If you export the report to an XML file, you can accept the default output location or browse to the location of your choice.
2. Click **Start Analysis Process**.

Navigating the Transcript Analysis Report File

The top of the report contains links to each section.

- Click a link to move through the file.
- Click the browser's **Back** button to return to the previous location in the file.

Sample Transcript Report

Device Commands

The Device Commands section contains sent and received transcript messages grouped by individual G2S devices.

If Session ID numbers are reused, each row will contain all of the messages with the same Session ID. Currently, the report does not display legal pairs.

[bonus\[1\]](#)

Serial Number	Date/Time	Date/Time Sent	Direction	Command ID	Session ID	Session Type	Retry?	Device ID	Summary
42	2008-04-24T09:18:58:357-07:00	2008-04-24T09:18:58:543-07:00	INBOUND	831	721	G2S_request		bonus[1]	bonus.ar.bonus[Data]
43	2008-04-24T09:18:58:635-07:00	2008-04-24T09:18:58:635-07:00	OUTBOUND	2247	721	G2S_response		bonus[1]	bonus.bonus[Data]
46	2008-04-24T09:18:58:733-07:00	2008-04-24T09:18:58:733-07:00	INBOUND	832	722	G2S_request		bonus[1]	bonus.ar.bonus[Data]
47	2008-04-24T09:18:58:760-07:00	2008-04-24T09:18:58:760-07:00	OUTBOUND	2248	722	G2S_response		bonus[1]	bonus.bonus[Data]
50	2008-04-24T09:18:58:838-07:00	2008-04-24T09:18:58:838-07:00	INBOUND	833	723	G2S_request		bonus[1]	bonus.ar.bonus[Data]
51	2008-04-24T09:18:58:900-07:00	2008-04-24T09:18:58:900-07:00	OUTBOUND	2249	723	G2S_response		bonus[1]	bonus.bonus[Data]

[cabinett528059076\]](#)

Serial Number	Date/Time	Date/Time Sent	Direction	Command ID	Session ID	Session Type	Retry?	Device ID	Summary
299	2008-04-24T09:19:09:807-07:00	2008-04-24T09:19:09:807-07:00	INBOUND	895	795	G2S_request		cabinett528059076]	cabinett528059076]
301	2008-04-24T09:19:09:869-07:00	2008-04-24T09:19:09:869-07:00	OUTBOUND	2312	795	G2S_response		cabinett528059076]	cabinett528059076]
303	2008-04-24T09:19:09:853-07:00	2008-04-24T09:19:09:853-07:00	INBOUND	896	796	G2S_request		cabinett528059076]	cabinett528059076]
305	2008-04-24T09:19:09:963-07:00	2008-04-24T09:19:09:963-07:00	OUTBOUND	2313	796	G2S_response		cabinett528059076]	cabinett528059076]
309	2008-04-24T09:19:10:135-07:00	2008-04-24T09:19:10:135-07:00	INBOUND	898	797	G2S_request		cabinett528059076]	cabinett528059076]
311	2008-04-24T09:19:10:197-07:00	2008-04-24T09:19:10:197-07:00	OUTBOUND	2314	797	G2S_response		cabinett528059076]	cabinett528059076]

Device States

Status of each device and any device status changes for the requested time period.

Events

The Events section displays information about events generated by the EGM.

Serial Number	Date Sent	Session ID	Event ID	Transaction ID	Event Device	Event Code	Event Text
1695	2008-04-25T13:05:13.759-07:00	400000	78	1	eventhandler[1]	G2S_EHE101	Event Subscription Changed

G2S ACKs That Have Errors

The G2S ACKs That Have Errors section shows G2S acknowledgement messages containing errors.

Serial Number	Error Code	Error Message
123	G2S_MSX003	Communications Not Online
125	G2S_MSX003	Communications Not Online
144	G2S_MSX003	Communications Not Online
146	G2S_MSX003	Communications Not Online
148	G2S_MSX003	Communications Not Online
150	G2S_MSX003	Communications Not Online
152	G2S_MSX003	Communications Not Online
154	G2S_MSX003	Communications Not Online

Messages

The Messages section displays the actual XML code for messages that appear in the transcript.

The report may rewrite the XML content while formatting this section of the report. In particular, the report may change the XML namespace prefix. However, the XML namespace URI is maintained. Note that unused namespace declarations may not be displayed.

[Message #1](#) communications commsOnLine

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<g2s:g2sMessage xmlns:g2s="http://www.gamingstandards.com/g2s/schemas/v1.0.3">
  <g2s:g2sBody g2s:dateTimeSent="2008-04-24T09:18:52.853-07:00" g2s:egmId="RBG_1234"
    g2s:hostId="1">
    <g2s:communications g2s:commandId="1237" g2s:dateTime="2008-04-24T09:18:52.853-07:00"
      g2s:deviceId="1"
      g2s:errorCode="G2S_none"
      g2s:errorMessage=""
      g2s:sessionId="4000001"
      g2s:sessionMore="false"
      g2s:sessionRetry="false"
      g2s:sessionType="G2S_request"
      g2s:timeToLive="30000">
      <g2s:commsOnLine g2s:deviceChanged="true" g2s:deviceReset="true"
        g2s:egmLocation="http://localhost:38101/RST/api-services/G2SAPI"
        g2s:equipmentType="G2S_egm"
        g2s:metersReset="true"
        g2s:subscriptionLost="true"/>
      </g2s:communications>
    </g2s:g2sBody>
  </g2s:g2sMessage>
```

Meters

The Meters section shows the values of the following meters:

- PCA - Player Cashable Amount (G2S_playerCashableAmt)
- PPA - Player Promo Amount (G2S_playerPromoAmt)
- PNCA - Player Non-Cashable Amount (G2S_playerNonCashAmt)
- GSI - Games Since Initialization (G2S_gamesSinceInitCnt)

Note that this is not a comprehensive list of all possible meters.

Serial Number	Date Sent	Session ID	PCA	PPA	PNCA	GSI	
395	2008-04-25T13:15:17.131-07:00	1006	20.00.000	0.00.000	0.00.000	0	View Message
401	2008-04-25T13:16:18.165-07:00	1007	13.00.000	0.00.000	0.00.000	1	View Message

Sessions

The Sessions section groups sent and received messages. Messages appear in ascending order, by **Session ID**.

A Session ID is a number that is set by the sender of a request, which allows the response to be tied to the original request. While session ID numbers should increase, they don't have to - they must be unique for the number of outstanding messages.

Entries in red indicate incomplete sessions (either no response or too many responses) and are often errors.

Session ID	Messages
723	communications.getDescriptor communications.descriptorList
724	eventHandler.getEventHandlerStatus eventHandler.eventHandlerStatus
725	eventHandler.getSupportedEvents eventHandler.supportedEvents
726	eventHandler.getEventHandlerProfile eventHandler.eventHandlerProfile
727	eventHandler.getEventSub eventHandler.eventSubList
728	eventHandler.setEventHandlerState eventHandler.eventHandlerStatus
729	meters.getMeterSub meters.meterSubList
730	meters.getMeterSub meters.meterSubList
731	bonus.getBonusStatus bonus.bonusStatus

Transcript

The Transcript section shows sent and received messages. Note that since the date is from the G2S message (sent either by the EGM or the host), the date may be incorrect. There are a number of reasons why this occurs. For example:

- the PC clock is incorrect.
- the Network Time Protocol (NTP) is not functioning correctly.
- there are programming errors.

Serial Number	Date/Time	Date/Time Sent	Direction	Command ID	Session ID	Session Type	Reply?	Device ID	Summary
1	2008-04-24T09:38:52.853-07:00	2008-04-24T09:38:52.853-07:00	OUTBOUND	2007	4000000	G2S_request		communicationsC12	communications.commandsList
2	2008-04-24T09:38:54.875-07:00	2008-04-24T09:38:54.963-07:00	INBOUND	821	4000001	G2S_response		communicationsC11	communications.commandsList
3	2008-04-24T09:38:55.463-07:00	2008-04-24T09:38:55.463-07:00	OUTBOUND	2008	4000002	G2S_request		communicationsC12	communications.commandsList
4	2008-04-24T09:38:55.525-07:00	2008-04-24T09:38:55.525-07:00	INBOUND	822	4000003	G2S_response		communicationsC11	communications.commandsList
5	2008-04-24T09:38:55.545-07:00	2008-04-24T09:38:55.545-07:00	INBOUND	823	124	G2S_request		communicationsC12	communications.commandsList
11	2008-04-24T09:38:56.666-07:00	2008-04-24T09:38:56.666-07:00	OUTBOUND	2009	123	G2S_request		communicationsC11	communications.commandsList
14	2008-04-24T09:38:56.244-07:00	2008-04-24T09:38:56.244-07:00	INBOUND	824	124	G2S_request		eventHandlerC11	eventHandler.eventHandlerStatus
15	2008-04-24T09:38:56.322-07:00	2008-04-24T09:38:56.322-07:00	OUTBOUND	2040	124	G2S_response		eventHandlerC11	eventHandler.eventHandlerStatus
16	2008-04-24T09:38:56.438-07:00	2008-04-24T09:38:56.438-07:00	INBOUND	825	125	G2S_request		eventHandlerC11	eventHandler.eventHandlerStatus
19	2008-04-24T09:38:56.463-07:00	2008-04-24T09:38:56.463-07:00	OUTBOUND	2041	125	G2S_response		eventHandlerC11	eventHandler.eventHandlerStatus
22	2008-04-24T09:38:57.713-07:00	2008-04-24T09:38:57.713-07:00	INBOUND	826	126	G2S_request		eventHandlerC11	eventHandler.eventHandlerStatus
23	2008-04-24T09:38:57.744-07:00	2008-04-24T09:38:57.744-07:00	OUTBOUND	2042	126	G2S_response		eventHandlerC11	eventHandler.eventHandlerStatus
26	2008-04-24T09:38:57.838-07:00	2008-04-24T09:38:57.838-07:00	INBOUND	827	127	G2S_request		eventHandlerC11	eventHandler.eventHandlerStatus
27	2008-04-24T09:38:57.885-07:00	2008-04-24T09:38:57.885-07:00	OUTBOUND	2043	127	G2S_response		eventHandlerC11	eventHandler.eventHandlerStatus
28	2008-04-24T09:38:58.040-07:00	2008-04-24T09:38:58.040-07:00	INBOUND	828	128	G2S_request		eventHandlerC11	eventHandler.eventHandlerStatus
31	2008-04-24T09:38:58.228-07:00	2008-04-24T09:38:58.228-07:00	OUTBOUND	2044	128	G2S_response		eventHandlerC11	eventHandler.eventHandlerStatus
34	2008-04-24T09:38:58.307-07:00	2008-04-24T09:38:58.307-07:00	INBOUND	829	129	G2S_request		metersC11	meters.meterSubList
35	2008-04-24T09:38:58.353-07:00	2008-04-24T09:38:58.353-07:00	OUTBOUND	2045	129	G2S_response		metersC11	meters.meterSubList

The **Serial Number** is assigned by the tool. This number corresponds to the order in which the message was received by the application. Use this value to compare the arrival order between any two messages.

The **Date/Time Sent** field is the date and time message that is sent to the host or EGM.

The **Date/Time** field is the date and time message was constructed.

The **Direction** is relative to the application. *Inbound* means a message that came from the other end. *Outbound* is a message that was generated by the application you ran the report from.

The **Retry?** column is blank for first attempts and filled in for retries. This column corresponds to the *sessionRetry* attribute in the G2S message.

Transcript Summary

The Transcript Summary section shows information related to the computer running the installed application.

EGM ID	
OS Architecture	x86
OS Name	Windows XP
OS Version	5.1
OS Patch Level	Service Pack 2
CPU List	pentium_pro+mmx pentium_pro pentium+mmx pentium i486 G86 i86
MAC Addresses	• 00-0F-FE-95-8C-2C
Java Version	1.6.0
JVM Version	1.6.0-b105
Java Home	C:\Program Files\JST-1.1.14-igt\radblue\jre\jre
Username	radblue
Started On	2009-04-24T16:09:07.572-07:00

About the Advanced Transcript Analyzer

The Advanced Transcript Analyzer lets you easily verify that commands being sent by the EGM are semantically valid. Visual cues let you easily discern which events have errors. You can then quickly drill down to the message content level to view the issue.

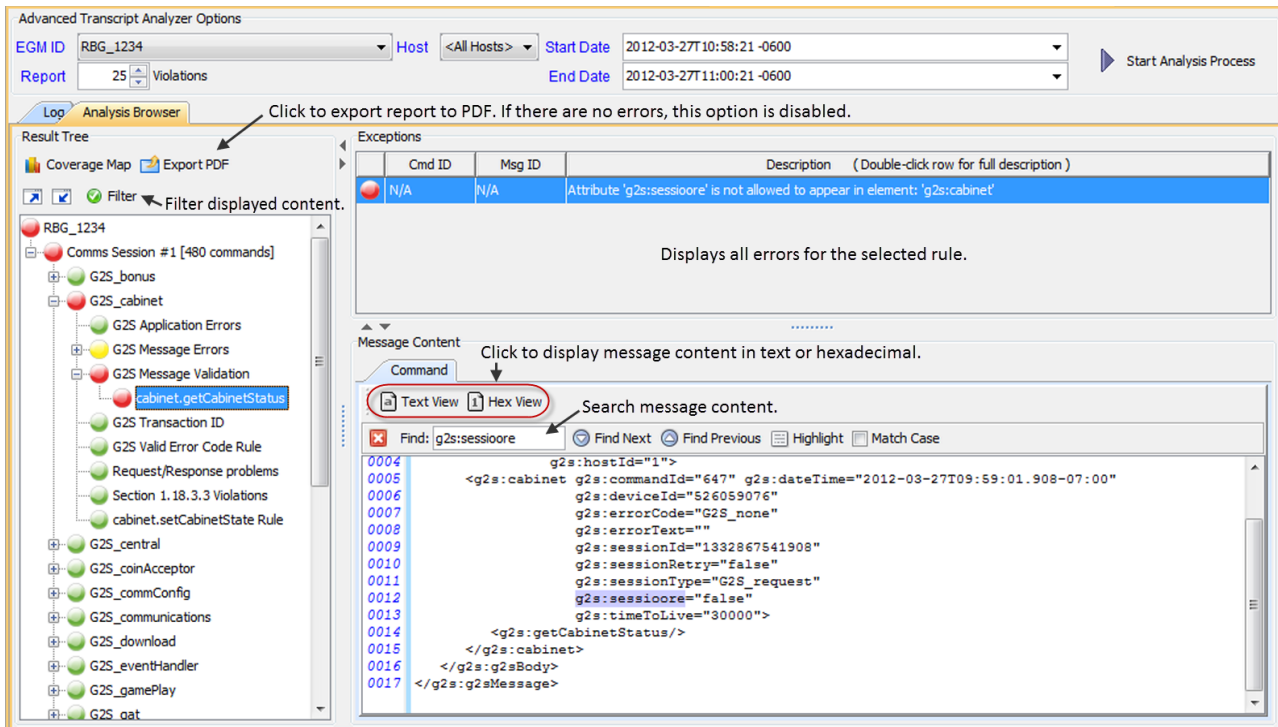
The Advanced Transcript Analyzer validates:

- the event subscription set by the EGM is accurate when compared to the subscription requested by the host.
- every `eventReport` command sent by the EGM to ensure that the EGM has included the associated data agreed upon in the event subscription phase.
- selected attributes in the `eventReport` command to ensure that they properly indicate state transitions as identified by the G2S protocol document.

The Advanced Transcript Analyzer makes it easy for EGM developers and testers to deliver high-quality G2S implementations - and we're continuing to add new areas of investigation (more "rules" to run against your G2S application) to give you the most comprehensive testing possible.

Review the Advanced Transcript Analyzer Layout

The Advanced Transcript Analyzer can be accessed by clicking **Analyze > Advanced** on the Transcript layout.



Errors and warnings are displayed in the **Results Tree** on the left-hand side of the screen. Click the plus sign to drill down to warnings and errors. To narrow the displayed results, click the **Filter** option and choose to display warnings and errors only or specific classes only.

When you click on a command with an error or warning, all violations associated with the command are displayed under **Exceptions**. Click an exception to display the message content, with the violation highlighted, in the **Message Content** section. The **Find** option lets you search the message content. Simply click inside the Find field and start typing.

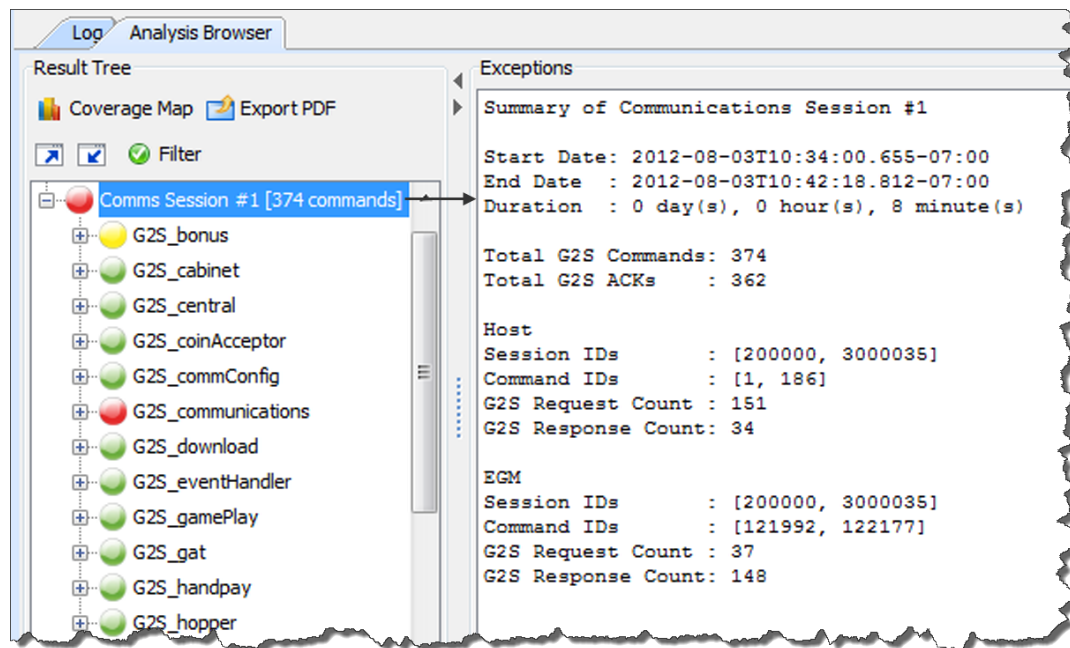
Get Started Analyzing Command Data

From the Transcript layout, click the **Analyze** drop-down arrow, and select **Advanced**.

1. Click the **EGM ID** drop-down arrow, and select the EGM data you want to analyze.
2. Click the Host drop-down arrow, and select the host data you want to analyze or select **All Hosts** to view all host data.
3. Click in the **Report** dialog box, and type or select the number of rule violations you want to view.
4. Select **Ignore keepAlives** if you do not want to include `keepAlive` commands in your analysis.
5. Enter the reporting period date and time in the **Start Date** and **End Date** fields. You can access a calendar to select the date and time by clicking the drop-down arrow. By default, the dates reflect the start and end of the Transcript. If you are using an older version of the Advanced Transcript Analyzer, the default will reflect the current date and time.
6. Click **Start Analysis Process**.

Errors are organized by communication sessions (**Comms Session**). A Comms Session is the period of time between two `commsOnline` commands. Comms Sessions that do not have any significant data do not appear in the Advanced Transcript Analyzer.

When you click to highlight a Comms Session, a summary of that Comms Session displays under Exceptions.



Under each **Comms Session**, errors are grouped by class and then by rules.

A colored status icon appears in front of each grouping to let you know if there are any errors in that group. The colors are defined as follows:

- **Green** - No errors or warnings. You're good to go.
- **Yellow** - Warning. One or more issues that are permissible in the schema, but may cause problems in your implementation.
- **Red** - Error. One or more G2S schema violations.
Look for red and yellow status icons. (If you only see green - Congratulations! Close the tool and take a well-deserved break.)

6. Double-click a red- or yellow-status **Comms Session** to expand it.

7. Double-click a red- or yellow-status class to expand it.

Note: The same error may appear more than once if it violates more than one rule.

8. Click a command to display those errors in the **Exceptions** section.

9. [Resize the Exceptions list](#) as needed by clicking and dragging the sizing bar at the bottom of the list.

10. Click any error in the **Exceptions** section.

The message in which the error occurs is displayed in the **Message Content** section directly below the Exceptions section. The issue within the message (for example, an invalid attribute value) is highlighted.

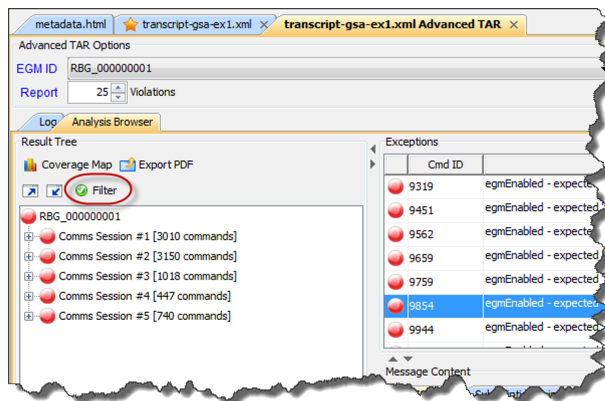
You can use the **Find** option to search for keywords and character strings in the message content. To use the Find option, click inside the **Find** text box, and start typing. Characters in the first matching instance are highlighted in the message content as you type.

- Click **Highlight** to highlight all matching characters.
- Use **Find Next** and **Find Previous** to move from match to match within the message content.
- Select **Match Case** to view only matches in title case as well as character.

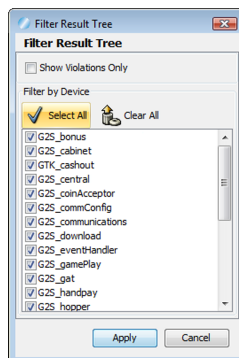
Filter Advanced Transcript Analysis Report

You can filter debug log data from the Advanced Transcript Analysis Report user interface through the Filter option. Choose to view only violations (errors and warnings) or all data for a specific class.

1. From the **transcript-gsa-ex1.xml Advanced TAR** tab, select the **Analysis Browser** tab.



2. Click **Filter**.

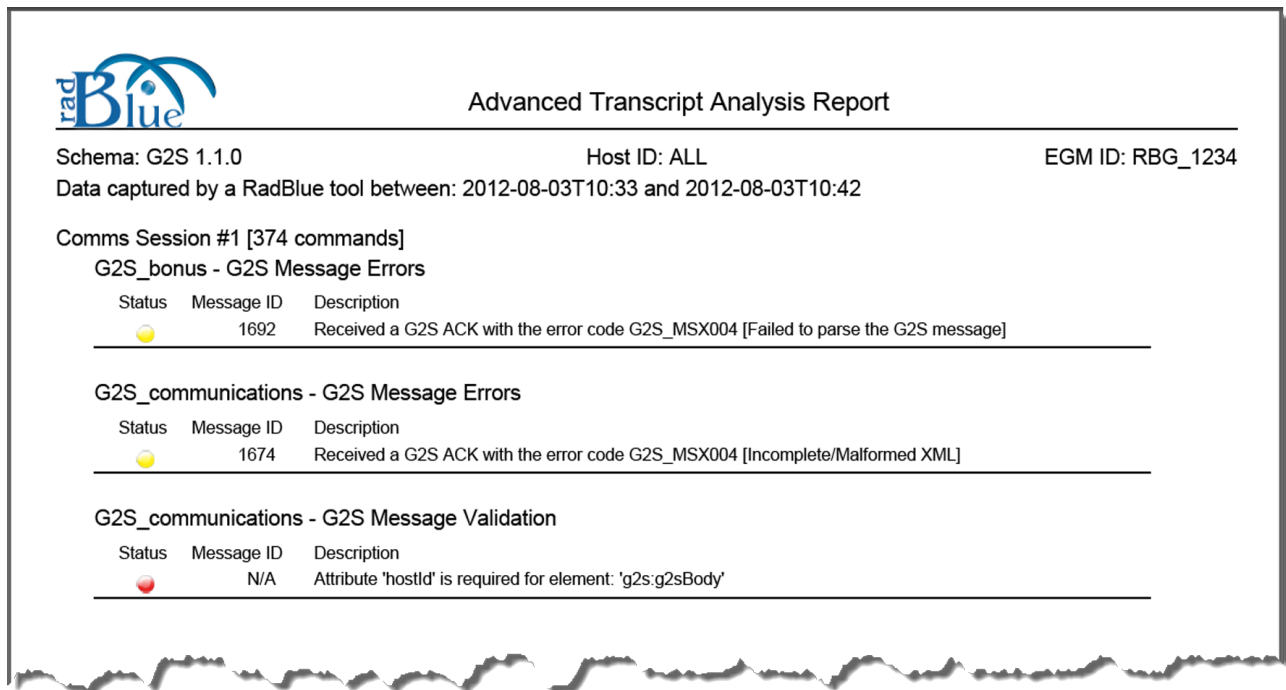


3. Modify the displayed data as required.
 - **Show Violations Only** - Select to display errors and warnings *only*.
 - **Filter by Device** - Select any class to display its data. To omit a class from display, clear its checkbox. By default, all classes are selected. Click **Select All** to select all classes or **Clear All** to clear all classes.
4. Click **Apply** to save and automatically apply your changes.

Generate a PDF of the Advanced Transcript Analysis Report

You can quickly generate a PDF file of all errors and warnings from the currently loaded debug log through the Advanced Transcript Analyzer interface. This option gives you a succinct overview of all issues and allows you to easily share your findings with others. You can choose to generate a report with all errors (complete) or a report that excludes duplicate errors (summary).

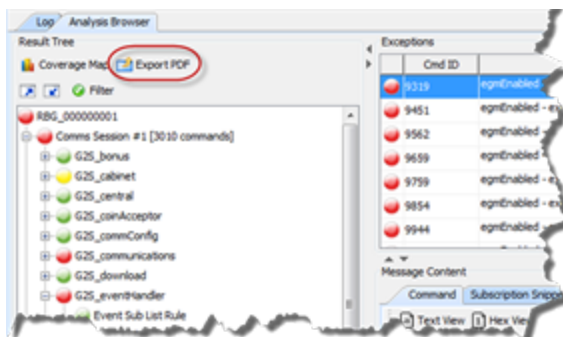
Note that any filters you apply to the Advanced Transcript Analyzer interface are reflected in the report.

A screenshot of the 'Advanced Transcript Analysis Report' interface. The report is titled 'Advanced Transcript Analysis Report' and includes the RadBlue logo. It shows metadata such as 'Schema: G2S 1.1.0', 'Host ID: ALL', and 'EGM ID: RBG_1234'. The data capture period is '2012-08-03T10:33 and 2012-08-03T10:42'. The report is for 'Comms Session #1 [374 commands]'. It lists three sections of errors: 'G2S_bonus - G2S Message Errors' with one error (Message ID 1692), 'G2S_communications - G2S Message Errors' with one error (Message ID 1674), and 'G2S_communications - G2S Message Validation' with one error (Message ID N/A). Each error entry includes a status icon (yellow for message errors, red for validation errors) and a description.

Status	Message ID	Description
Yellow circle	1692	Received a G2S ACK with the error code G2S_MSX004 [Failed to parse the G2S message]
Yellow circle	1674	Received a G2S ACK with the error code G2S_MSX004 [Incomplete/Malformed XML]
Red circle	N/A	Attribute 'hostId' is required for element: 'g2s:g2sBody'

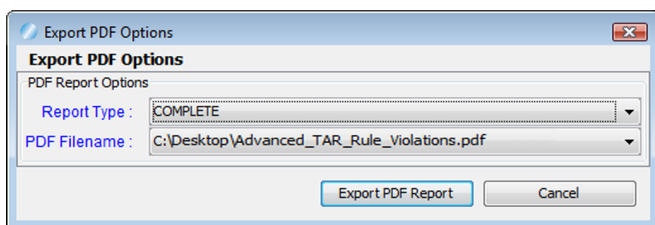
Sample Summary Report

1. From the Advanced Transcript Analyzer screen, select the **Analysis Browser** tab.

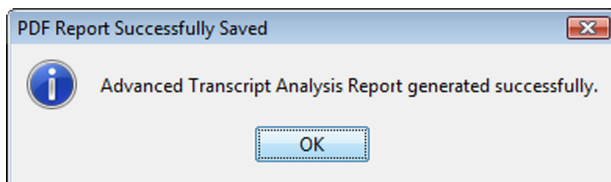


2. Under the **Result Tree**, click **Export PDF**.

Note: If there are no errors in the imported debug log, the **Export PDF** option is disabled.



3. Click the **Report Type** drop-down arrow, and choose whether to generate all errors, including duplicate errors (**COMPLETE**), or one incident, of each error type, per comms session (**SUMMARY**).
4. Click the **PDF Filename** drop-down arrow.
5. Navigate to the location you want the file output to, and type a new file name as needed.
6. Click **Open**.
7. Click **Export PDF Report**.



8. Click **OK**.

A PDF file with the name you entered is created in the specified location.

Working with the Multicast Transcript

The Multicast Transcript displays multicast messages that are sent between the host and EGM. Note that G2S commands contained in multicast messages can also be viewed through the Transcript. However, the Transcript does not display multicast wrapper information.

At the top of the Multicast Transcript Control screen are several options:

- **Load** - Load transcript messages from the database so you can work with them through the user interface. See [Load Messages into the Multicast Transcript](#).
- **Search Content** - Search through the contents of all displayed messages in this transcript instance for the entered text pattern (case sensitive). Clicking on a row in the returned list gives you access to the HTTP header and message contents of the selected message. See [Search the Content of a Multicast Message](#).
- **Clear Display** - Clears the displayed messages in this instance of the transcript control. See [Clear the Multicast Transcript Display](#).
- **Clear DB** - Clears all records of this type in the database for this instance of the tool. See [Clear the Multicast Transcript Database](#).
- **Clear Multicast Listeners** - *RPA only*. Clears all endpoint multicast listeners, which are persisted in RPA. See [Clear the Multicast Listeners](#).

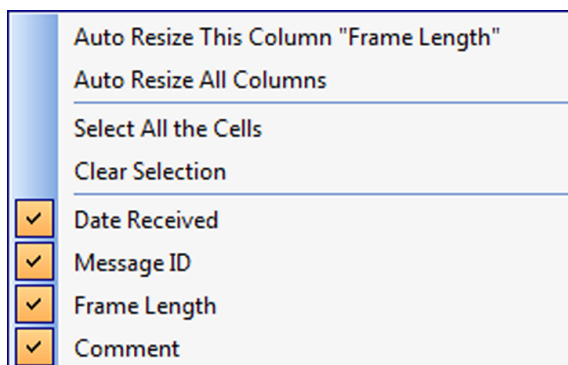
The size limit of the multicast transcript is 4MB. If this limit is reached, messages beyond the limit are not stored in the transcript database, and an informational message displays in the [debug log](#).

Multicast Transcript Column Headers

The following columns are available in the Multicast Transcript:

- **Date Received** - Date and time message is received by the tool.
- **Message ID** - Identification number of the message.
- **Frame Length** - Length of the frame contents.
- **Comment** - Indicates an invalid UMAC (Message Authentication Code using Universal Hashing) or an invalid frame length if an error occurs. If the message is valid, this field is blank.

You can slide the columns around to rearrange their order. To move a column header, left-click and hold while you move the column to its new location. You can also click any column to re-sort it, or use CTRL + left-click to sort on multiple columns.



If you right-click on a column header, a menu displays that allows you to automatically resize one or all columns (based on the displayed data in the columns), as well as to indicate which columns you would like to display.

Clicking on any column header causes the data to be sorted using that header. Click once to sort the column in ascending order. Click a again to sort the column in descending order. The third click clears the sort.

If you want to sort on multiple columns, use the CTRL key when clicking the column headers.

Filter Multicast Transcript Records Quickly

Just below the transcript options is a magnifying glass and entry field that allows you to filter messages based on entered data.

Clicking on the magnifying glass gives you a menu that you can use to provide additional selection criteria.

This powerful tool allows you to immediately view any set of messages that you can imagine, limited only by the data displayed in the columns.

Load Messages into the Multicast Transcript

The Load option loads a set of data from the tool's database that you can work with in the Multicast Transcript Control screen.

If you are using RGS, be sure the EGM for which you want to view information is selected.

1. Click **Load** to load a set of data from the database.
2. Enter the number of messages (rows) you want to view by using the arrows or by typing the number into the combo box.

3. Note that the line numbering begins at zero, so what is displayed is the number of rows entered minus one. For example, if you load 15 rows, 0-14 would be displayed.
4. Click **Load**.

Receive Real-Time Data in the Multicast Transcript

If you select **Realtime Update**, the screen updates dynamically as messages are processed by the tool. However, real-time updating can cause application slowdown.

View the Content of a Multicast Message

By double-clicking on any row, you can examine the details of the multicast message. The multicast message detail view lets you switch between a text and a hexadecimal view. You can also browse through the multicast transcript list while in detail view.

A "secret" search utility helps you find keywords within the message. Simply click in the window where the XML is displayed and start typing. The tool instantly jumps to the first match of the entered string. The up and down arrows will move you to the next or previous match of the entered string. This feature becomes very handy when you want to find data in large XML messages. The search utility works whether you are displaying hexadecimal or text.

To view the content of a multicast message:

1. Double-click the message you want to view.

Several fields provide you with information about the selected message.

- **Date Received** - Date and time message is received by the tool.
- **Multicast Location** - Multicast address or other transport-specific parameters.
- **Current Key** - Key used to authenticate message.
- **UMAC** - Message Authentication Code using Universal hashing.
- **UMAC Nonces** - The core security requirement of the UMAC is the notion of the nonce. MTP nonces are a combination of (Message ID + Frame Index + 0x0 + 0x0).
- **Message ID** - Identification number of the message.
- **Frame Index** - Index number of the frame.
- **Total Frame Count** - Total number of frames in message.
- **Frame Length** - Length of the frame contents.
- **Comment** - Indicates an invalid UMAC or an invalid frame length. If the message is valid, this field is blank

2. On the Message tab, click **Text View** to view the message in either text format, or click Hex View to view the message in hexadecimal format.
3. Click **Ciphertext** to view the message payload. If the message is encrypted, the information displays in hexadecimal format.
4. Click **Previous** and **Next** to navigate through the Multicast transcript list while in message detail view.
5. Click **OK** to return to the multicast transcript.

Search the Content of a Multicast Message

The Search Content option lets you search for keywords within all messages currently displayed in the Multicast transcript.

1. Click **Search Content**.
2. Type the information you want to search on.
3. Click **Proceed**, or click **Cancel** to return to the Multicast Transcript Control. A pop-up window displays all messages containing the text you entered.
4. Click any message to display the Multicast message details along with the XML message text and frame payload.
5. Click **Back** to return to the Multicast Transcript Control.

Clear the Multicast Transcript Display

The Clear Display option lets you clear all messages from the Multicast transcript. This option does not remove messages from the Multicast transcript database.

1. Click **Clear Display** to remove all messages from the current view.

Clear the Multicast Transcript Database

The Clear DB option lets you remove all messages from the Multicast transcript database. Note that this action cannot be undone.

1. Click **Clear DB**.
2. Click **Yes** to remove all data from the transcript database, or click **No** to return to the transcript without clearing the database.

Clear the Multicast Listeners

The Clear Multicast Listeners option lets you remove all endpoint multicast listeners from the Multicast transcript database. Note that this action cannot be undone.

1. Click **Clear Multicast Listeners**.
2. Click **Yes** to remove all endpoint multicast listeners, or click **No** to return to the transcript without removing the listeners.

About Watchables

The Watchables object lets you look for a specific attribute or even a specific value in that attribute. Simply specify a query to watch for particular attributes occurring in the XML stream that flows into and out of the application.

The Watchables feature is based on XML Path Language (XPath) queries. A Watchable will select all messages that meet the XPath criteria. With RadBlue Watchables, you can select from a list of pre-defined XPath criteria, modify the criteria of an existing XPath query, or create your own XPath query.

Watchables			
<input type="checkbox"/> Select Watchable <input type="button" value="New Watchable"/> <input type="button" value="Edit Watchable"/> <input type="button" value="Delete Watchable"/> <input type="button" value="Copy Watchable"/> <input type="button" value="Clear All"/>			
Query Name	Match Found	Time Stamp	
<input checked="" type="checkbox"/> meters@commandId	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters@dateTime	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters@deviceId	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters@errorCode	matched	2008-07-21T09:01:03.844-07:00	
<input checked="" type="checkbox"/> meters@errorText	matched	2008-07-21T09:01:03.782-07:00	
<input checked="" type="checkbox"/> meters@sessionId	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters@sessionMore	matched	2008-07-21T09:01:03.782-07:00	
<input checked="" type="checkbox"/> meters@sessionRetry	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters@sessionType	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters@timeToLive	matched	2008-07-21T09:01:03.782-07:00	
<input checked="" type="checkbox"/> meters.clearMeterSub@meterSubType	no match		
<input checked="" type="checkbox"/> meters.getMeterSub@meterSubType	no match		
<input checked="" type="checkbox"/> meters.meterInfo@meterDateTime	no match		
<input checked="" type="checkbox"/> meters.meterInfo@meterInfoType	no match		
<input checked="" type="checkbox"/> meters.meterSubList@eodBase	matched	2008-07-21T09:01:03.797-07:00	
<input checked="" type="checkbox"/> meters.meterSubList@meterSubType	matched	2008-07-21T09:01:03.813-07:00	
<input checked="" type="checkbox"/> meters.meterSubList@periodicBase	matched	2008-07-21T09:01:03.829-07:00	
<input checked="" type="checkbox"/> meters.meterSubList@periodicInterval	matched	2008-07-21T09:01:03.813-07:00	
<input checked="" type="checkbox"/> meters.setMeterSub@eodBase	matched	2008-07-21T09:01:03.657-07:00	
<input checked="" type="checkbox"/> meters.setMeterSub@meterSubType	matched	2008-07-21T09:01:03.719-07:00	
<input checked="" type="checkbox"/> meters.setMeterSub@periodicBase	matched	2008-07-21T09:01:03.719-07:00	
<input checked="" type="checkbox"/> meters.setMeterSub@periodicInterval	matched	2008-07-21T09:01:03.110-07:00	

About XPath Expressions

The basic XPath expression for RadBlue tools contains a message and a body element. These elements must be defined in the expression. You can then use class, message, attribute name and attribute value elements to track specific messages and their content.

XPath Expression Format

/g2s:g2sMessage/g2s:g2sBody/g2s:cabinet/g2s:cabinetStatus/@g2s:denomId="526059076"

g2s:g2sMessage	g2s:g2sBody	g2s:cabinet	g2s:cabinetStatus	@g2s:denomId	= "526059076"
message	body	class	message type	attribute name	attribute value

Sample XPath Expressions

Watchable	XPath Expression
EGM ID	/g2s:g2sMessage/g2s:g2sBody/@g2s:egmId
Specific EGM ID	/g2s:g2sMessage/g2s:g2sBody/@g2s:egmId="RBG_12345"
Comms State	/g2s:g2sMessage/g2s:g2sBody/g2s:communications/g2s:commsStatus/@g2s:commsState
EGM Location	/g2s:g2sMessage/g2s:g2sBody/g2s:communications/g2s:commsOnLine/@g2s:egmLocation
Paytable ID	/g2s:g2sMessage/g2s:g2sBody/g2s:cabinet/g2s:cabinetStatus/@g2s:paytableId
Theme ID	/g2s:g2sMessage/g2s:g2sBody/g2s:cabinet/g2s:cabinetStatus/@g2s:themeld
Cabinet Status	/g2s:g2sMessage/g2s:g2sBody/g2s:eventHandler/g2s:eventReport/g2s:deviceList/g2s:statusInfo/g2s:cabinetStatus

XPath References

- World Wide Web Consortium (W3C), XPath 2.0 web site: <http://www.w3.org/TR/xpath20/>
- Kay, Michael. *XPath 2.0 Programmer's Reference (Programmer to Programmer)*. Indianapolis, IN: Wiley Publishing, Inc., 2004.

Boolean Expression Usage

XPath allows boolean expressions. For example:

```
if ( count (/g2s:g2sMessage/g2s:g2sBody/g2s:eventHandler/g2s:eventReport/  
g2s:meterList/g2s:meterInfo[2]/g2s:deviceMeters[1]/g2s:* ) = 1 ) then true() else false()
```

The above sample expression tracks messages that contain one, and only one, deviceMeter element under a second meterInfo element. Note that the asterisk (*) indicates that the value of deviceMeters can match anything in that element.

Clear All Watchable Data

Click Clear All to remove all of the matched data from the display.

Copy a Watchable

Copy Watchable allows you to make a copy of one of the queries, in case you want to modify your query just a bit more, but don't want to lose the prior one.

1. Select the watchable you want to copy from the list of active queries.
2. Click **Copy Watchable**.



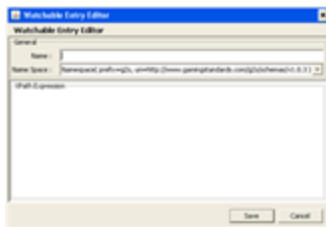
3. Click in the **Name** dialog box, and type a new name for the Watchable.
4. Click **Save**.

Create a New Watchable

Use New Watchable to write your own XPath expressions to further refine your search. For example, you can look for a particular value in a particular attribute (`../@g2s:deviceClass="G2S_all"`).

The XPath specification is available online through the World Wide Web Consortium (W3C). When creating a new Watchable, note that the Watchable namespace must correspond to the GSA schema that the Watchable applies to.

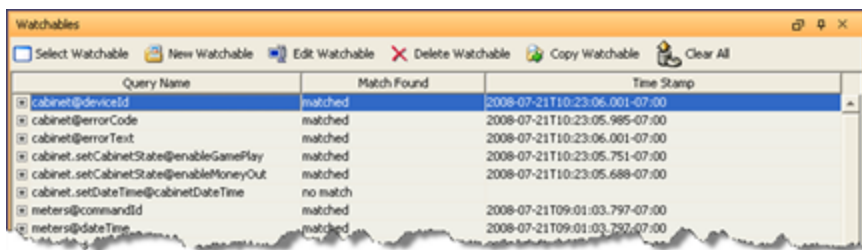
1. Click **New Watchable**.



2. Type the **Name** of the new Watchable.
3. Click the drop-down arrow, and select a **Name Space** for the new Watchable. The namespace provides context for the query.
4. Type the XPath query in the **XPath Expression** text box.
5. Click **Save** to make the newly created Watchable available in the Watchable list.

Delete a Watchable

1. Select the watchable you want to delete from the list of active queries.



2. Click **Delete Watchable**.

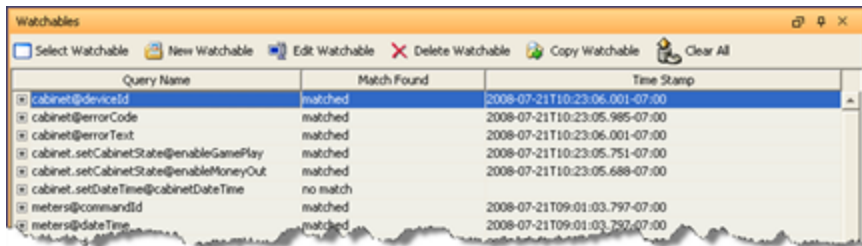


3. Click **Yes** to delete the selected XPath query.

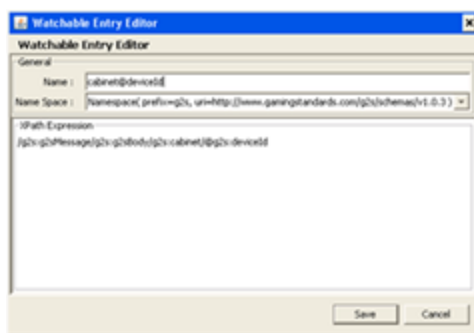
Edit a Watchable

Edit Watchable allows you to modify the name or expression of the selected XPath query. Note that you must restart the tool before your changes will take effect.

1. Select the watchable you want to edit from the list of active queries.



2. Click **Edit Watchable**.

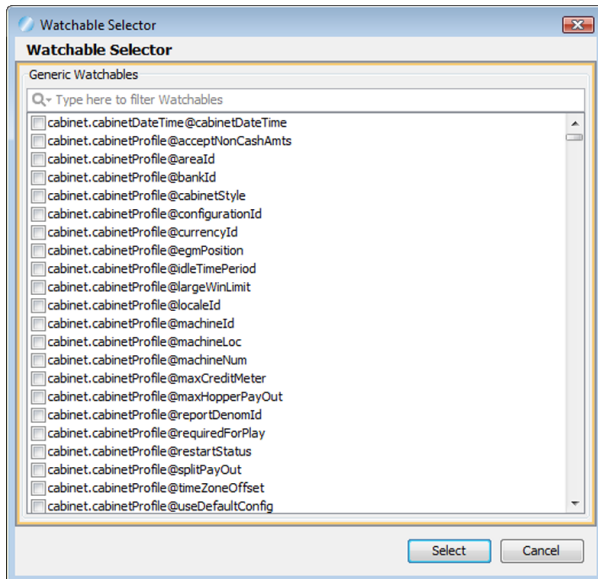


3. Modify the selected Watchable as needed.
4. Click **Save**.

Select Attribute(s) to Track in Watchables

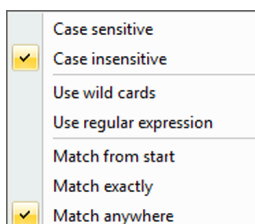
Select Watchable provides a searchable list of all standard attributes in G2S or S2S. Once you select the Watchable criteria, all messages from that point forward will be matched against the Watchable to see if it should be displayed.

1. Click **Select Watchable**.



2. Select the attribute(s) you want to track.

You can quickly filter the available attributes by clicking in the text box at the top of the screen and typing a keyword or characters. To configure additional selection criteria, click the magnifying glass to the left of the text box.



2. Click **Select** to add the selected attribute(s) to the list of attributes that the application is tracking.

The tool creates a sample XPath query that can then be modified. See [Create a New Watchable](#).

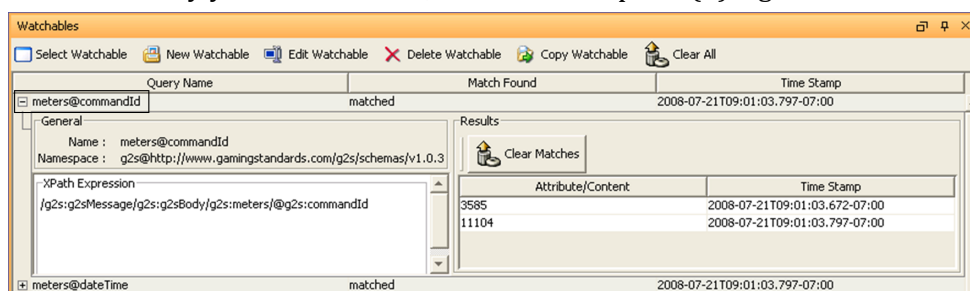
View a Watchable

For each query, the XPath expression, attribute, and date received are displayed. If no commands were received with the attribute specified in a specific query, “no match” is displayed.

For some of the more complex commands, such as the meterInfo command, the application provides tabs and tables for easy navigation.

First, select a meter group (GameDenom, Device, Currency, or Wager) and then select the individual device whose meters you want to examine from the list of those reported by the EGM. By clicking the “plus” (+) sign, you cause the list of the devices meters to be expanded as per the above example. For long meter lists, a scroll bar is provided on the right to easily move through the list.

1. Select the entry you want to view, and click the “plus” (+) sign in front of the entry.

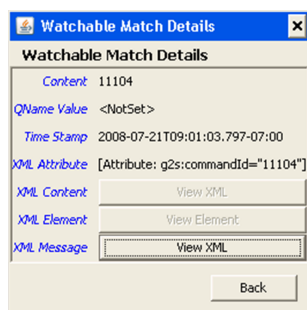


General

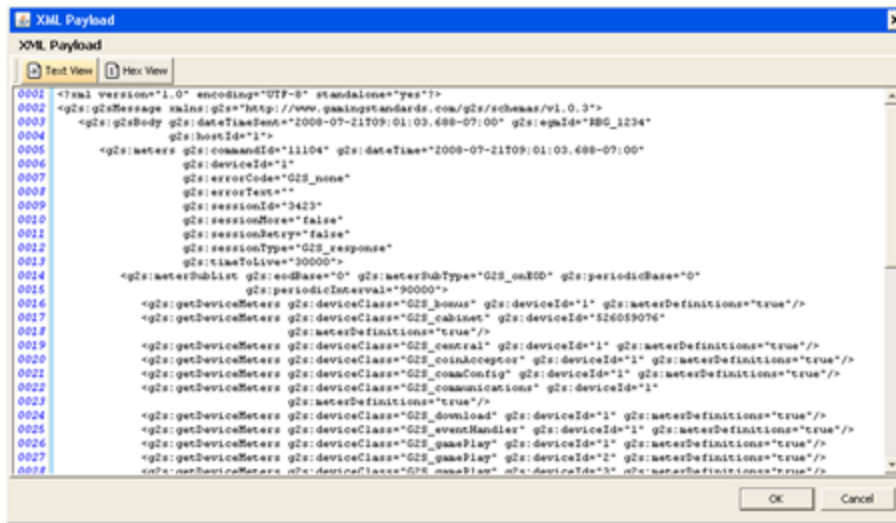
- **Name** - Watchable designation.
- **Namespace** - Namespace that was used in the XPath expression.
- **XPath Expression** - XPath query that the attribute or message content is matched to.

Results

- **Attribute/Content** - Attribute or message content of the matched XPath query.
 - **Time Stamp** - Time and date the message was sent.
2. In the **Results** section, double-click the message you want to view.



3. To view the message's XML content, click **View XML**.



4. To view the message content in hexadecimal format, click **Hex View**.

About the Debug Console

The Debug Console displays all informational, warning and critical errors that occur in the tool. Any of the following message types may appear in the Debug Console:

- **INFO** - Messages that do not impact the system, but may be useful to know. INFO messages appear in black type.
- **DEBUG** - Fine-grained informational events that are useful in troubleshooting. DEBUG messages appear in black.
- **ERROR** - Messages related to program errors. ERROR messages appear in red.
- **FATAL** - Designates a severe error events that will presumably lead the application to abort. FATAL messages appear in red.
- **UNKNOWN** - Messages that have not been assigned a logging designation. UNKNOWN messages appear in pink.
- **WARN** - Messages that indicate potentially harmful situations. WARN messages appear in blue.

You can clear the debug log and filter the debug log display (selectively display messages by warning level) as needed.

The information displayed in the Debug Console is written to a text file ([**tool name**].txt), located in the tool's logs directory.

You can specify the maximum number of lines included in the log through the Configure option under Tools on the menu bar.

1. Go to: **Tools > Configure > Desktop Options > Max Logger Lines**
2. Click **Desktop Options**.
3. In the **Max Logger Lines** field, type or select the maximum number of lines in the Debug Console.
4. Click **OK**.

Clear the Debug Log Display

To clear the Debug Console display, click **Clear Log**.

Note that this option clears the display only, and not the text file associated with the Debug Log ([**tool name**].txt, located in the tool's logs directory).

Filter Debug Messages

The Filter option lets you specify the type(s) of messages you want displayed in the Debug Console.

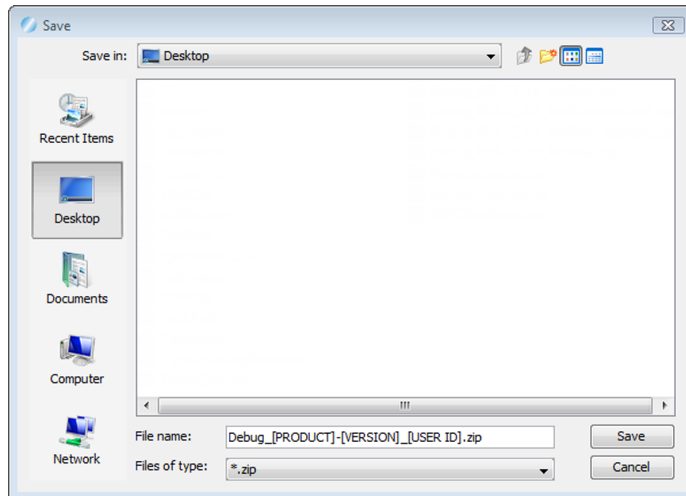
To filter Debug Console messages:

1. From the Debug Console, click **Filter**. The Logging Filter screen appears.
2. Click **Select All** to select all message types.
or
1. Click **Clear All** to clear all boxes, and select the message types you want to display.
2. Click **Apply** for your changes to take effect, or click **Cancel** to exit the Logging Filter without applying any changes.

What to Do If You Can't Resolve an Error

The Export Debug option lets you create a ZIP file containing all the files that the RadBlue support team needs to troubleshoot product issues or for use in the [RadBlue Analysis Suite \(RAS\)](#). The ZIP file includes data from the time the tool was started to the time you select the Export Debug option.

1. Go to **File > Export Debug**.



2. A **Debug-[product-x.x.x]_[user ID].zip** file is exported to your computer's desktop.
3. Attach the ZIP file to an email, along with a description of the issue, and send it to support@radblue.com.

or

Go to www.radblue.com/support, complete the support form, attach the ZIP file and send.

You will be contacted about your support issue within one business day.

Configuring Desktop Options

Desktop Options define default application views, which are comprised of one or more available controls. This screen also allows you to define the amount of data displayed in specific transcripts and views.

Data Management

This section allows you to specify the amount of data used for various transcripts and views. Increasing the data sizes increases the memory used by the tool.

- **Max G2S Transcript Messages** - Maximum number of G2S transcript messages displayed.
- **Max Soap Transcript Messages** - Maximum number of SOAP transcript messages displayed.
- **Max Logger Lines** - Maximum number of lines in the Debug Console stored in the database.
- **Max Watcher Data Versions** - Maximum number of matches for each Watchable stored in the database.

Configuring RPA Engine Options

Engine Options allow you to automate some functions of the RPA engine. Engine options are grouped functionally: [General](#), [Transport](#), [Transcript Filters](#), [Database](#) and [G2S Endpoints](#). Click any tab to view the options for that group.

The screenshot displays the 'Engine Options' configuration window with the 'Transport' tab selected. The window has a dark blue header with the title 'Engine Options'. Below the header are five tabs: 'General', 'Transport' (highlighted in yellow), 'Transcript Filters', 'Database', and 'G2S Endpoints'. The 'Transport' tab contains several configuration sections:

- IP Address & SOAP Port:** A 'Bind To' dropdown menu is set to '172.16.53.60'. Below it are four text input fields: 'Inbound SOAP Port' (35101), 'Inbound SSL SOAP Port' (35201), 'Outbound SOAP Port' (35111), and 'Outbound SSL SOAP Port' (35211). Each of these fields has a blue question mark icon to its right.
- Multiple Client Host Ports:** A checkbox labeled 'Enable' is currently unchecked, with a blue question mark icon to its right.
- From URLs:** Two text input fields: 'From URL' (http://172.16.53.60:35111) and 'SSL From URL' (https://172.16.53.60:35211), each with a blue question mark icon to its right.
- Enable Client Side GZIP:** A checkbox is unchecked, with a blue question mark icon to its right.
- Enable Host Side GZIP:** A checkbox is unchecked, with a blue question mark icon to its right.
- HTTP Connection Timeout:** A text input field containing '5000', with a blue question mark icon to its right.
- HTTP Receive Timeout:** A text input field containing '5000', with a blue question mark icon to its right.

RPA Engine Options screen.

General

From the General tab on the Engine Options configuration screen, you can define the protocol, schema location and the schema version used by RPA.

- **Protocol Name** - Click the drop-down arrow, and select either the G2S or S2S protocol. This setting is used to create the Schema Location.
- **Schema Location** - The Schema Location field is automatically populated based on the Protocol Name and Version values.
- **Version** - Click the drop-down, and select the G2S or S2S version you want to use. This setting is used to create the Schema Location.

Transport

From the Transport tab on the Engine Options configuration screen, you can define RPA settings related to message transport.

- **Bind To** - Click the drop-down arrow, and select the IP Address that you want RPA to use for communications. If the RPA, EGM and host are all running on the same computer, select 127.0.0.1 (localhost).
- **Enable Client Side GZIP** - Select to enable GZIP support on the client side.
- **Enable Host Side GZIP** - Select to enable GZIP support on the host side.
- **From URL** - The URL that RPA is listening on for responses from the host. This value is automatically calculated based on the values you enter in the Bind To, SOAP Port and Protocol Name fields.

Note: After making configuration changes that affect the URL, you should restart the Protocol Analyzer to make sure the web service is properly configured.

- **HTTP Connection Timeout** - Type the maximum time, in milliseconds, before the HTTP connection times out. The default is five seconds (**5000** milliseconds).
- **HTTP Receive Timeout** - Type the maximum time, in milliseconds, for the G2S ACK to be received. The default is five seconds (**5000** milliseconds).
- **Inbound SOAP Port** - Enter the port that you want RPA to use for inbound communications. We recommend that you do not change the SOAP port value unless you have a port conflict.
- **Inbound SSL SOAP Port** - Enter the port that you want RPA to use for inbound SSL-enabled communications. This port number is used when you select SSL Enabled on the Host Side Information screen and when the EGM uses SSL.
- **Multiple Client Host Ports** - Select this option if you want RPA to start multiple G2S servers with unique port numbers to which the EGM can connect. Once selected, the **Inbound SOAP Port** field and **Inbound SSL SOAP Port** field display ending port number values that are determined by adding four to the user-entered port value. For example, if the **Inbound SOAP Port** value is **35101**, the ending port number will be **35105**. You can view all unique client URLs by clicking **Show URL(s)** on the RPA layout.

Note: RPA does not verify that the user has properly configured the EGM for multiple hosts.
- **Outbound SOAP Port** - Enter the port that you want RPA to use for outbound communications. We recommend that you do not change the SOAP port unless you have a port conflict.
- **Outbound SSL SOAP Port** - Enter the port that you want RPA to use for outbound SSL-enabled communications. This port number is used when you select SSL Enabled on the Host Side Information screen and when the EGM uses SSL.

- **SSL From URL** - The URL for SSL-enabled messaging that RPA is listening on for responses from the host. This value is automatically calculated based on the values you enter in the Bind To, SSL SOAP Port and Protocol Name fields.

Transcript Filters

From the Transcript Filters tab on the Engine Options configuration screen, you can filter the specified commands from RPA.

- **Filter G2S ACKs from Transcripts** - Select to filter `g2sack` commands from the Transcript database. If this option is selected, `g2sack` commands do not appear on the Message Transcript.
- **Filter G2S Keep Alives from Transcript** - Select to filter `keepAlive` commands from the Transcript database. If this option is selected, `keepAlive` commands do not appear on the Message Transcript.
- **Filter G2S Set Progressive Values from Transcript** - Select to filter `G2S setProgressiveValue` commands from the Transcript database. If this option is selected, `setProgressiveValue` commands do not appear on the Message Transcript.
- **Filter Multicast G2S Bonus Activity from Transcript** - Select to filter `G2S bonus.bonusActivity` commands from the Message Transcript and Multicast Transcript *if (and only if) the `bonus.bonusActivity` command is sent using multicast.*

Database

From the Database tab on the Engine Options configuration screen, you can define settings for RPA databases.

- **Enable General Transcript Analyzer** - Select to enable the EGM Transcript Analysis Report (**Transcripts > Analyze > General**).
Once selected, configure the number of records to save for use with the EGM Transcript Analysis Report.
Increasing the number of records, increases disk use. Clear this option to improve performance.
- **Save Transcript Messages to Database** - Select this option to save the defined number of messages in the Message, SOAP and Multicast transcripts to the transcript database. Save transcript records in the database only if you want them to remain between runs of the tool or after you clear the transcript display.
Saving a large number of transcript messages affects performance. By default, this option is disabled.

G2S Endpoints

From the G2S Endpoints tab you can manage EGM and G2S host *endpoints*. An *endpoint* is the network location to which RPA forwards messages, defined by a URL. You must add G2S host endpoints, but EGM endpoints are added automatically as RPA receives `commsOnline` commands. RPA allows up to five (5) endpoints *each* for EGMs and G2S hosts.

You can edit the URL description and delete EGM endpoints as needed. G2S Host endpoints can be added, edited or deleted. **Inactive Timeout** automatically deletes an EGM endpoint that has no activity after the defined time.

Note: The endpoint screen you see (G2S or S2S) depends on the selected protocol. If you do not see the G2S Endpoints tab, go to the [General](#) tab and select the **G2S** protocol.

The screenshot shows the 'Engine Options' dialog box with the 'G2S Endpoints' tab selected. The 'EGM Endpoints' section has buttons for 'Edit', 'Remove', and 'Remove All', and an 'Inactive Timeout' set to 05:00. Below is a table with 4 columns: EGM ID, Host ID, EGM URL, and Description. The 'G2S Host Endpoints' section has buttons for 'Add', 'Remove', and 'Edit'. Below is a table with 4 columns: ID, URL, Description, and SSL.

EGM ID	Host ID	EGM URL	Description
RBG_1234	1	http://172.16.53.150:38102/RST/api-services/G2SAPI	UNKNOWN
RBG_4321	1	http://172.16.53.150:38102/RST/api-services/G2SAPI	UNKNOWN
RBG_1234	17	http://172.16.53.150:38102/RST/api-services/G2SAPI	UNKNOWN

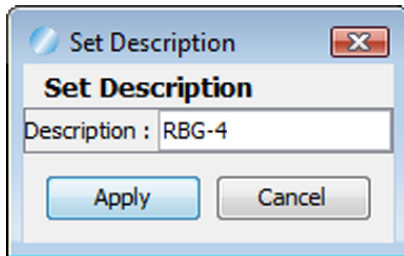
ID	URL	Description	SSL
1	http://localhost:31101/RGS/api-services/G2SHost	RGS	Enabled
17	http://localhost:31101/RGS/api-services/G2SHost	RGS	Enabled

Edit EGM Endpoints

From the G2S Endpoints tab, you can delete or edit the description of any URL in the EGM endpoint list.

To edit an EGM endpoint:

1. Click to select the endpoint you want to edit.
2. Click **Edit**.



3. Type a new description for the selected endpoint. The default value is **UNKNOWN**.
4. Click **Save**.

Delete a G2S Endpoint

You can delete an EGM endpoint or G2S host endpoint by selecting the endpoint you want to delete and clicking **Remove**. To delete all EGM endpoints, click **Remove All**.

Set EGM Endpoint Timeout

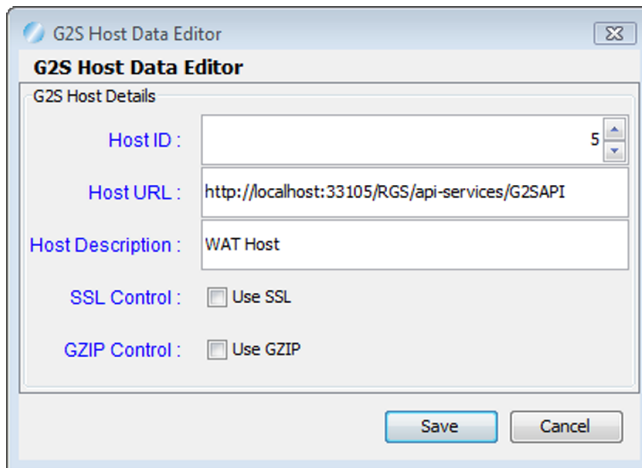
Using the **Inactive Timeout** option to automatically delete EGM endpoints from which RPA has not received a message after a specified amount of time (for example five minutes). To set the Inactive Timeout, select or type the minutes and seconds (mm:ss) you want RPA to wait before removing an EGM endpoint from the list.

Add a G2S Host Endpoint

The G2S host endpoint is the URL to which RPA sends messages. You can add up to five (5) G2S host endpoints to RPA. If you try to add a sixth endpoint, an error displays.

To add a G2S host endpoint:

1. Click **Add**.

The screenshot shows a dialog box titled "G2S Host Data Editor". Inside, there is a section labeled "G2S Host Details". It contains five fields: "Host ID" with a dropdown menu showing the number "5"; "Host URL" with the text "http://localhost:33105/RGS/api-services/G2SAPI"; "Host Description" with the text "WAT Host"; "SSL Control" with a checkbox labeled "Use SSL"; and "GZIP Control" with a checkbox labeled "Use GZIP". At the bottom of the dialog are two buttons: "Save" and "Cancel".

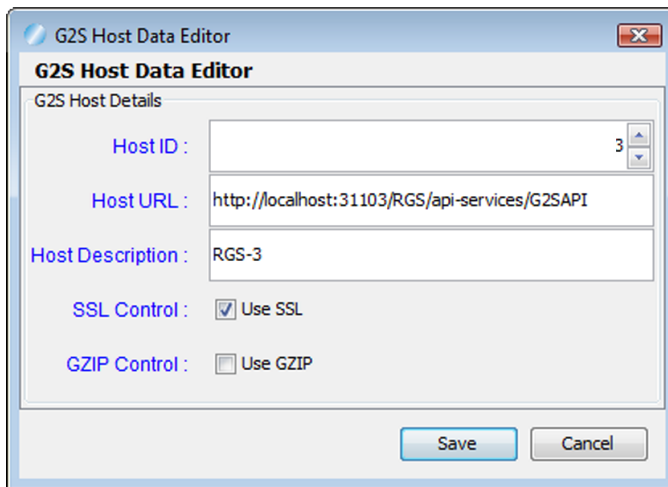
3. Modify the G2S host information as needed.
 - **Host ID** - Type or select the host identifier.
 - **Host URL** - Type the G2S host system URL. This is the location to which RPA forwards messages from the G2S.
 - **Host Description** - Type a description of the defined client URL.
 - **SSL Control** - Select to enable SSL for messages forwarded to the defined URL.
 - **GZIP Control** - Select to enable GZIP for messages forwarded to the defined URL.
4. Click **Save**. The new endpoint is added to the G2S Host Endpoints list.

Edit a G2S Host Endpoint

The G2S host endpoint is the URL to which RPA sends messages. You can edit any of the G2S host endpoint settings as needed. Endpoint changes take effect immediately.

To add a G2S host endpoint:

1. Click to select the endpoint you want to edit.
2. Click **Edit**.



The screenshot shows a dialog box titled "G2S Host Data Editor". Inside, there is a section labeled "G2S Host Details" with the following fields and controls:

- Host ID :** A text box containing the number "3" with a small up/down arrow icon to its right.
- Host URL :** A text box containing the URL "http://localhost:31103/RGS/api-services/G2SAPI".
- Host Description :** A text box containing the text "RGS-3".
- SSL Control :** A checkbox labeled "Use SSL" which is currently checked.
- GZIP Control :** A checkbox labeled "Use GZIP" which is currently unchecked.

At the bottom of the dialog box are two buttons: "Save" and "Cancel".

3. Modify the G2S host information as needed.
 - **Host ID** - Type or select the host identifier.
 - **Host URL** - Type the G2S host system URL. This is the location to which RPA forwards messages from the G2S.
 - **Host Description** - Type a description of the defined client URL.
 - **SSL Control** - Select to enable SSL for messages forwarded to the defined URL.
 - **GZIP Control** - Select to enable GZIP for messages forwarded to the defined URL.
4. Click **Save**. The new endpoint is added to the G2S Host Endpoints list.

S2S Endpoints

From the S2S Endpoints tab you can manage S2S client and host *endpoints*. An *endpoint* is the network location to which RPA forwards messages, defined by a URL. Client and host endpoints are added automatically as RPA receives `commsOnline` commands. However, you can edit any endpoint as needed. RPA allows one endpoint *each* for S2S clients and hosts.

Note: The endpoint screen you see (G2S or S2S) depends on the selected protocol. If you do not see the S2S Endpoints tab, go to the [General](#) tab and select the **S2S** protocol.

Engine Options

General Transport Transcript Filters Database **S2S Endpoints**

S2S Client Endpoint

Edit

Client URL	Description	SSL
http://localhost:44101/RSS/api-services/S2SAPI	S2S Edge	Disabled

S2S Host Endpoint

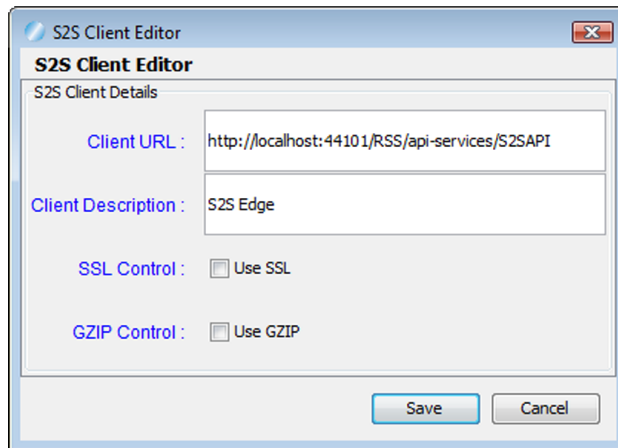
Edit

Host URL	Description	SSL
http://localhost:44102/RSS/api-services/S2SAPI	S2S Central	Disabled

Edit the S2S Client Endpoint

The S2S client endpoint is the URL to which RPA sends messages. To edit the S2S client endpoint:

1. Click to select the endpoint you want to edit.
2. Click **Edit**.

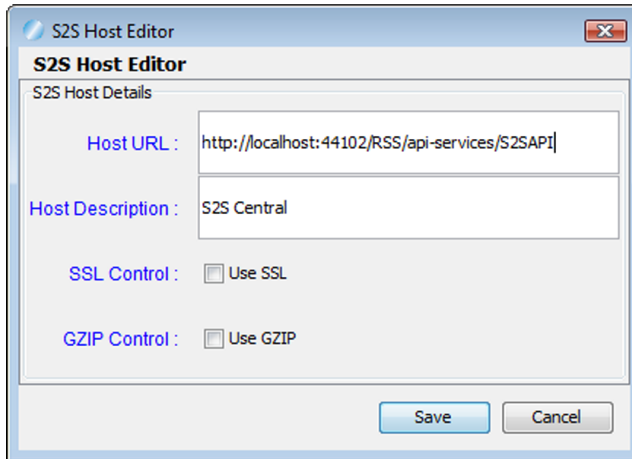


3. Modify the S2S endpoint client details as needed.
 - **Client URL** - Type the S2S client system URL. This is the location to which RPA forwards messages from the S2S host.
 - **Client Description** - Type a description of the defined client URL.
 - **SSL Control** - Select to enable SSL for messages forwarded to the defined URL.
 - **GZIP Control** - Select to enable GZIP for messages forwarded to the defined URL.
4. Click **Save**.

Edit the S2S Host Endpoint

The S2S host endpoint is the URL to which RPA sends messages. To edit the S2S host endpoint:

1. Click to select the endpoint you want to edit.
2. Click **Edit**.



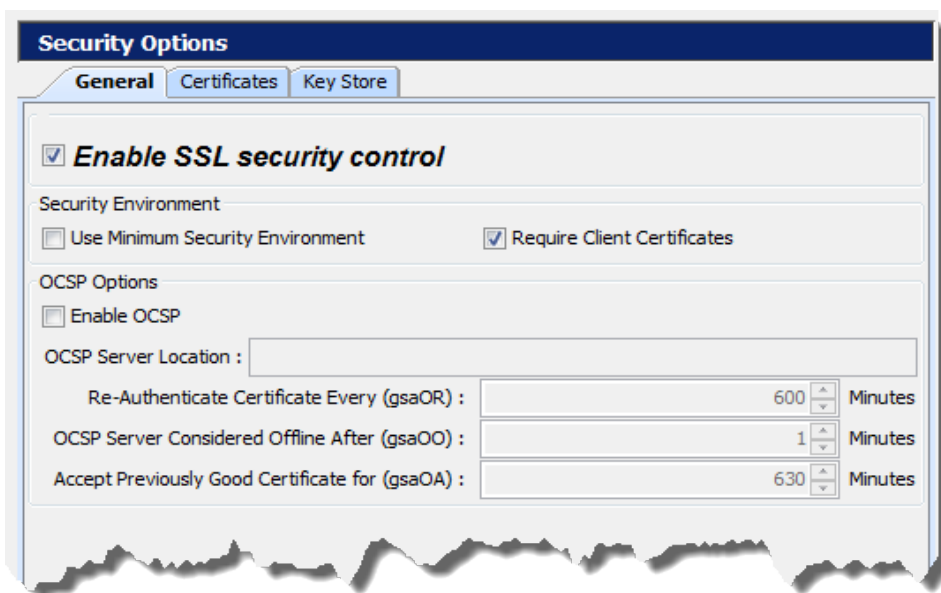
3. Modify the S2S endpoint client details as needed.
 - **Client URL** - Type the S2S host system URL. This is the location to which RPA forwards messages from the S2S client.
 - **Client Description** - Type a description of the defined host URL.
 - **SSL Control** - Select to enable SSL for messages forwarded to the defined URL.
 - **GZIP Control** - Select to enable GZIP for messages forwarded to the defined URL.
4. Click **Save**.

Configure Security Options

From Security Options, you can enable and configure Secure Socket Layer (SSL) encryption information.

- [Enable and configure Online Certificate Status Protocol \(OCSP\) options](#)
- [Create and import signed certificates into the tool](#)
- [Manage installed keystore files](#)

Note: SSL configuration, including the Security Options screen, is not available in the Student Edition of the tool.



To use SSL security, you must select Enable SSL security control. You then have the option to select **Approve All Certificates** if you want to use SSL encryption, but are not concerned with the validity of the certificate authority.

If this option is cleared, the tool performs validity checking when an entity (for example, an EGM) initiates communications. The validity check includes:

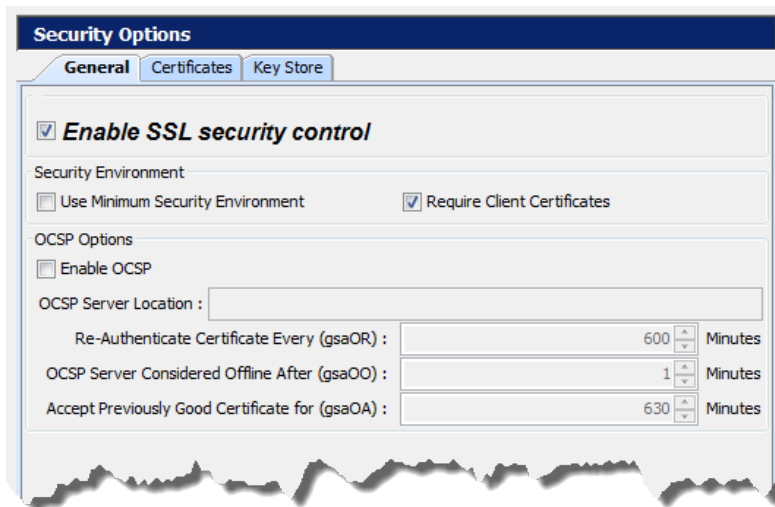
- *Signed by trusted certificate authority?*
- *Is current time/date within the period of validity (effective and expired date)?*
- *Is issuer signature correct?*

When you make a change to the Security Options screen, you are prompted to restart the tool before your changes take effect.

Configure General Security Options

From the General tab, you can enable SSL in the tool, choose to approve all certificates, and [configure OCSF options](#).

1. From **Tools > Configure > Security Options**.
2. Click **General**.



3. Select **Enable SSL security control** to use SSL encryption with the tool. This option must be selected to configure all additional security options.
4. Select **Use Minimum Security Environment** to enable minimum security option when testing. When you enable this option:
 - The **Transport Layer Security (TLS) 1.0** is the *only* supported protocol for client-side TLS sessions. Note that host-side sessions are not restricted.
 - The only supported cipher suite is `SSL_RSA_WITH_3DES_EDE_CBC_SHA` for both client-side and host-side TLS sessions.
5. Select **Require Client Certificate** if the other endpoint must have a certificate or it fails authentication. If this option is cleared, the other endpoint is not asked to send its client certificate. By default, this option is selected.
6. [Enable and configure OCSF options](#).
7. Once all security options have been configured, click **OK**.

Enable and Configure OCSP

You can configure the Online Certificate Status Protocol (OCSP) options to check to see whether the certificate has been revoked.

If a certificate does not pass any validity check, an error is generated and the attempted connection will fail. You can view the error in the debug log.

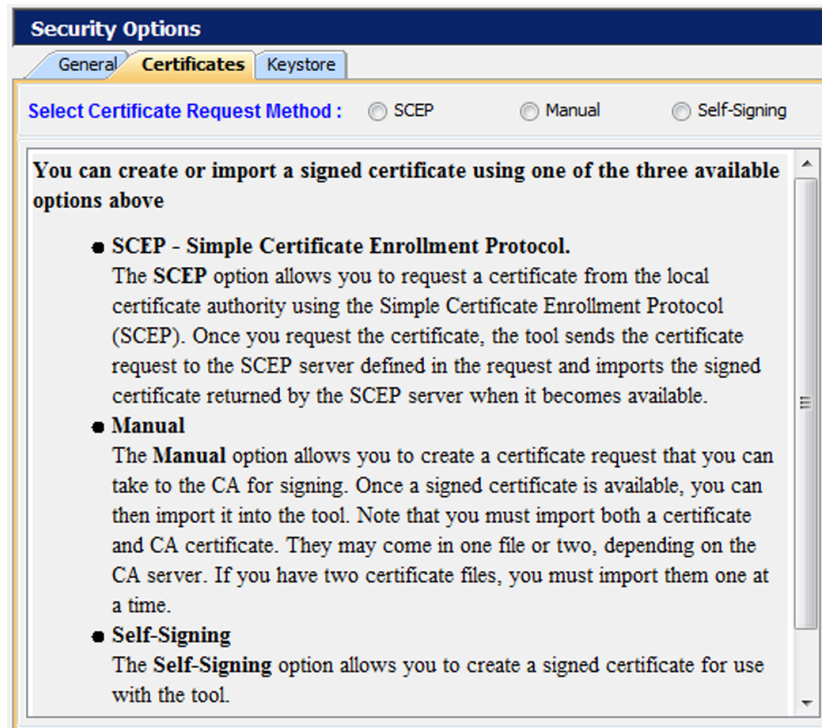
When you enable OCSP, you must configure the following options:

- **OCSP Server Location** - Type the URL location of the OCSP responder.
- **OCSP Server Considered Offline After (gsaOO) x Minutes** - Type or select the minimum period, in minutes, that the tool will attempt to authenticate a certificate from an OCSP server. Zero (0) disables this setting.
- **Re-Authenticate Certificate Every (gsaOR) x Minutes** - Type or select the maximum time, in minutes, that the tool can use a certificate without re-authenticating it.
- **Accept Previously Good Certificate for (gsaOA) x Minutes** - Type or select the maximum time, in minutes, that the tool can use a good certificate when OCSP servers are offline. Note that the gsaOA value should be greater period than the gsaOR value; The difference between gsaOR and gsaOA is the “accept offline” period.

Create or Import a Signed Certificate

You can create or import a signed certificate using one of three available options:

- [Use SCEP to Request a Certificate](#)
- [Load a Manual Certificate](#)
- [Load a Self-Signing Certificate](#)



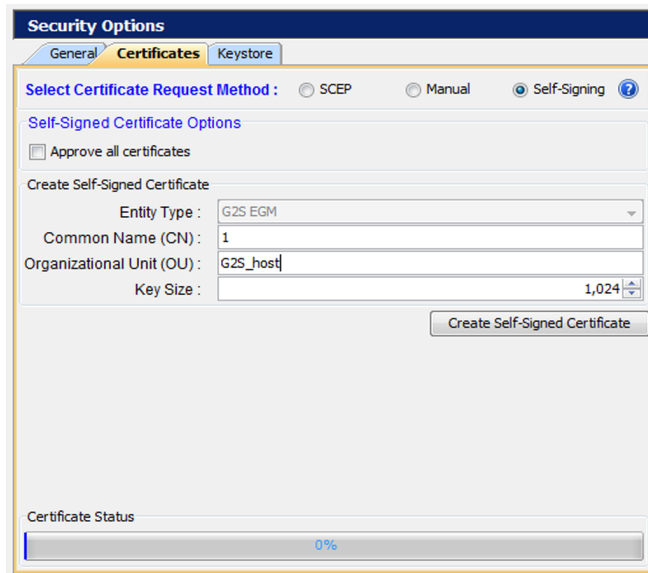
To access the certificate options:

1. From the menu bar, click **Tools**.
2. Select **Configuration**.
3. Click **Security Options** to display the Security Options screen.
4. Click the **Certificates** tab.

Load a Self-Signing Certificate

The Certificates tab allows you to create a signed certificate for use with the tool.

1. From **Tools > Configure > Security Options**.
2. Click **Certificates**.
3. Select **Self-Signing** as the **Certificate Request Method**.



The screenshot shows the 'Security Options' dialog box with the 'Certificates' tab selected. Under 'Select Certificate Request Method', 'Self-Signing' is chosen. The 'Self-Signed Certificate Options' section includes a checkbox for 'Approve all certificates' which is currently unchecked. Below this, the 'Create Self-Signed Certificate' section has fields for 'Entity Type' (set to 'G2S EGM'), 'Common Name (CN)' (set to '1'), 'Organizational Unit (OU)' (set to 'G2S_host'), and 'Key Size' (set to '1,024'). A 'Create Self-Signed Certificate' button is at the bottom right of this section. At the bottom of the dialog, a 'Certificate Status' bar shows '0%'.

4. Select **Approve all certificates** to use SSL encryption without validating the certificate authority.

If this option is cleared, the tool performs validity checking when an entity (for example, an EGM) initiates communications. The validity check includes:

- Signed by *trusted* certificate authority?
 - Is current time/date within the period of validity (effective and expired date)?
 - Is issuer signature correct?
5. Configure certificate options as required.
 - **Entity Type** - Indicates the role of the tool: G2S Host (RGS), G2S EGM Proxy (RPA), G2S EGM (RST), Other G2S, or S2S Server (RSS). This information is determined by the tool. This field is *read-only*.
 - **Common Name** - Type the tool's common name. In the case of an EGM, the common name would be the EGM identifier. The tool will attempt to set this value.

- **Organizational Unit** - Type the organizational unit (role) of the tool: G2S_host, G2S_egmProxy, G2S_egm, or Other G2S. By default, this field is populated with a value that corresponds to the Entity Type.
 - **Key Size** - Click the drop-down arrow, and select the size of the key pair supported by your network environment.
6. Click to **Create Self-Signed Certificate** to generate a self-signed certificate based on the certificate options you completed.
 7. When the **Certificate Status** bar reads **100% Done!**, you have successfully a signed certificate and can now use SSL messaging with the tool.

Use SCEP to Request a Certificate

The SCEP option lets you request a certificate from the local certificate authority using the Simple Certificate Enrollment Protocol (SCEP). Once you request the certificate, the tool sends the certificate request to the SCEP server defined in the request and imports the signed certificate returned by the SCEP server when it becomes available.

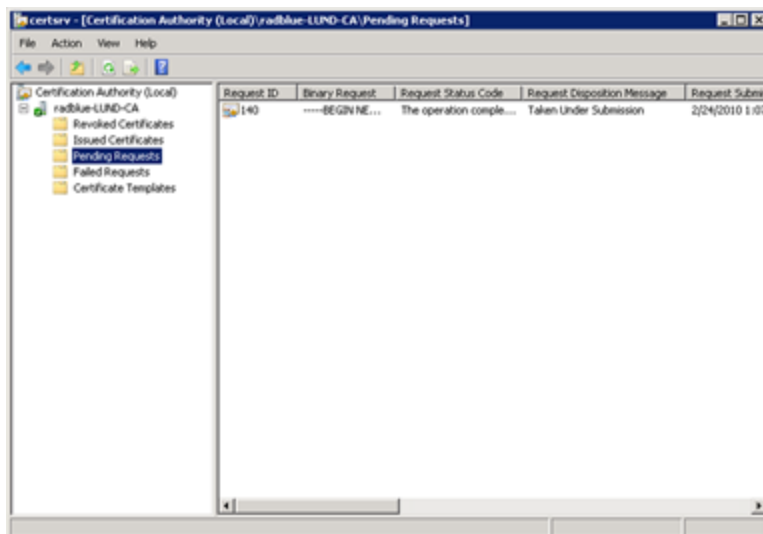
1. From **Tools > Configure > Security Options**.
2. Click **Certificates**.
3. Select **SCEP** as the **Certificate Request Method**.
4. Configure SCEP options as required. The values related to the certificate authority (CA) are available from the CA provider.
 - **SCEP Server Location** - Type the network location of the certificate authority to which you want to send your certificate request.
 - **Pre-Shared Secret Enabled?** - Select if you want to include a pre-shared secret in the certificate request.
 - **Pre-Shared Secret** - Type the pre-shared password that you want to include in the certificate request.
 - **User Name Enabled?** - Select to include the user name in the certificate authority request.
 - **User Name** - Type the user name used by the certificate manager. Depending on your SCEP implementation, the user name may be included in the transaction ID or as part of the Certificate Signing Request (CSR) as the Common Name (CN).
 - **Use User Name as Common Name?** - Select if the user name is the same as the common name.
 - **Common Name** - Type the tool's common name. In the case of an EGM, the common name would be the EGM identifier. The default is **-1**. When setting the Common Name in RPA, this value must equal the host ID that RPA proxies.
 - **CA Identity Enabled?** - Select to include the identifier of the certificate authority in the request.
 - **CA Identity** - Type the identifier of the certificate authority to which the request will be sent.
 - **Entity Type** - Click the drop-down arrow, and select the role of the tool: G2S Host, G2S EGM Proxy, G2S EGM, Other G2S.
 - **Organization Unit** - Type the organizational unit (role) of the tool: G2S_host, G2S_egmProxy, G2S_egm, or Other G2S. By default, this field is populated with a value that corresponds to the Entity Type.
 - **Key Size** - Click the drop-down arrow, and select the size of the key pair supported by your network environment. (1024 is generally the most commonly accepted key size.)

- **SCEP Server Polling Interval** - Type or select the interval, in milliseconds, in which the tool polls the certificate server until the tool's certificate request is approved.
 - **Request SCEP Server Capabilities** - Select to request the options supported by the certificate authority server.
 - **Request Certificate** - Click to request a certificate from the SCEP certificate authority server.
5. Click **Request Certificate**.

The request certificate is sent to the SCEP server. The tool polls the SCEP server location defined in step 4 until a signed certificate is issued.

If the CA is using Microsoft Active Directory Certificate Services, follow these steps to issue a signed certificate on the CA:

- From the computer where Microsoft Active Directory Certificate Services is installed, go to:
Start > Administrative Tools > Certification Authority



- Expand the server name, and click **Pending Requests**.
- Click to highlight the certificate request.
- Right-click the entry, and select **All Tasks > Issue**. When the certificate is issued, it disappears from the list.

Once the certificate is signed, the RadBlue tool imports it the next time a poll is performed.

When the **Certificate Status** bar reads **100% Done!**, you have successfully imported the required certificate and can now use SSL messaging with the tool.

Load a Third-Party Certificate

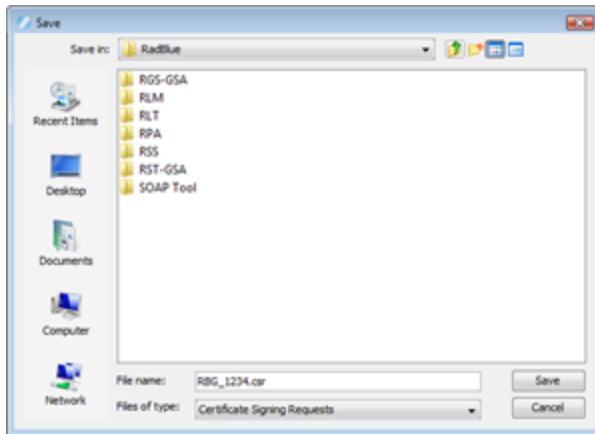
From the Certificates tab, you can create a certificate request that you can take to a certificate authority (CA) for signing. Once a signed certificate is available, you can then import it into the tool. Note that you must import both a certificate and CA certificate. They may come in one file or two, depending on the CA server. If you have two certificate files, you must import them one at a time.

1. From **Tools > Configure > Security Options**.
2. Click **Certificates**.
3. Select **Manual** as the **Certificate Request Method**.

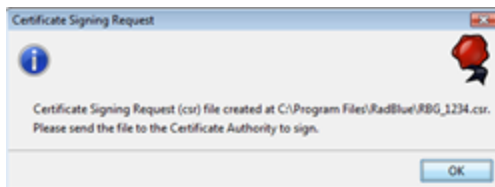
The screenshot shows the 'Security Options' dialog box with the 'Certificates' tab selected. Under 'Select Certificate Request Method', the 'Manual' option is chosen. The 'Manual Certificate Signing Request Options' section contains the following fields: 'Entity Type' (G2S Host), 'Common Name (CN)' (3), 'Organizational Unit (OU)' (G2S_host), and 'Key Size' (1,024). A 'Create Signing Request' button is located below these fields. The 'Import Certificate' section includes a 'Certificate Location' text box, a 'Browse' button, and an 'Import Certificate' button. At the bottom, the 'Certificate Status' bar displays '0% - Create a New Signing Request'.

5. Create a signing request by configuring the following fields with your request-specific information:
 - **Entity Type** - Click the drop-down arrow, and select the role of the tool: G2S Host, G2S EGM Proxy, G2S EGM, Other G2S.
 - **Common Name** - Type the tool's common name. In the case of an EGM, the common name would be the EGM identifier.
 - **Organizational Unit** - Type the organizational unit (role) of the tool: G2S_host, G2S_egmProxy, G2S_egm, or Other G2S. By default, this field is populated with a value that corresponds to the Entity Type.
 - **Key Size** - Click the drop-down arrow, and select the size of the key pair supported by your network environment.

2. Click **Create Signing Request** to generate a signing request.



3. Navigate to the location where you want to save the certificate request file.
4. Modify the file name and file type as required.
5. Click **Save**.



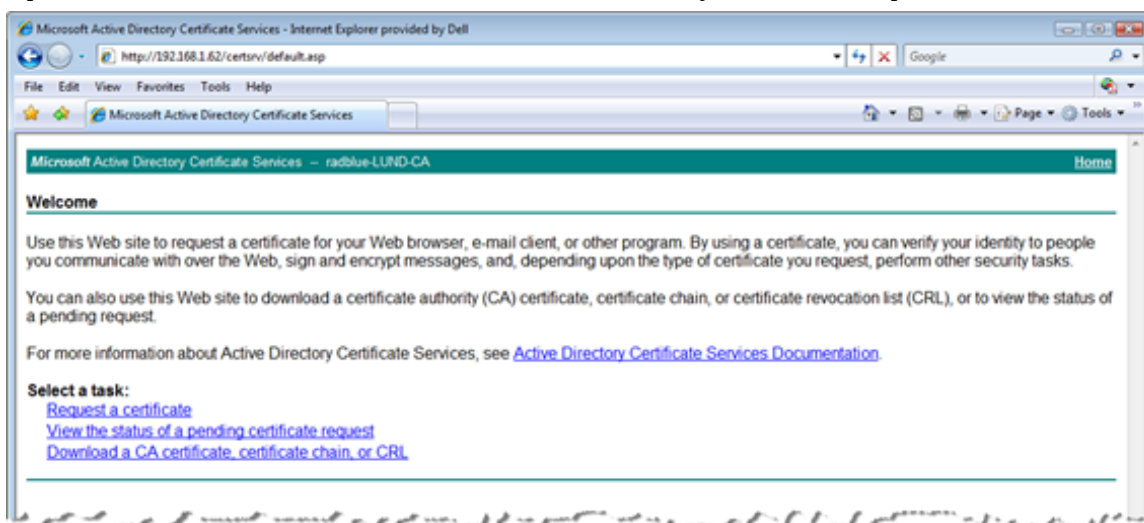
6. Click **OK**.
Notice that the Certificate Status is updated.
7. Depending on the certificate authority you are using, you must now use the certificate request you created to obtain a signed certificate from a certificate authority. For an example of how to obtain a signed certificate from Microsoft Active Directory Certificate Services, see [Obtaining a Signed Certificate Using Microsoft Active Directory Certificate Services](#).
8. Once you have a signed certificate that you can access, type the **Certificate Location** or click **Browse** to navigate to the signed certificate location.
9. Select the signed certificate file, and click **Open**.
10. Click **Import Certificate** to import the signed certificate.
11. If you have an additional certificate, repeat steps 8 through 10.
12. When the **Certificate Status** bar reads **100% Done!**, you have successfully imported the required certificate(s) and can now use SSL messaging with the tool.

Obtain a Signed Certificate Using Microsoft Active Directory Certificate Services

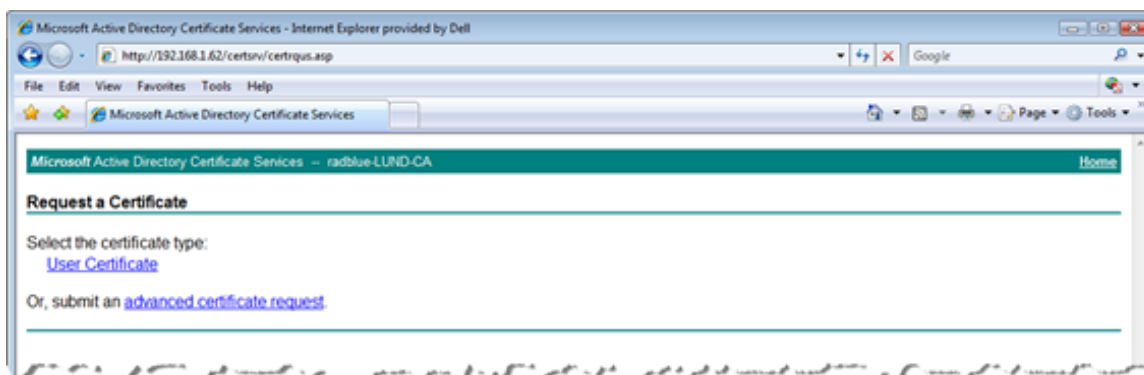
The following procedure is intended to provide an understanding of the process you may go through to create a signed certificate. Microsoft Active Directory Certificate Services is only one of many certificate authority programs. Your individual process may vary greatly depending on the certificate authority program you are using.

This procedure assumes that a certificate request has been created through the [Third-Party](#) tab on the Security Options screen.

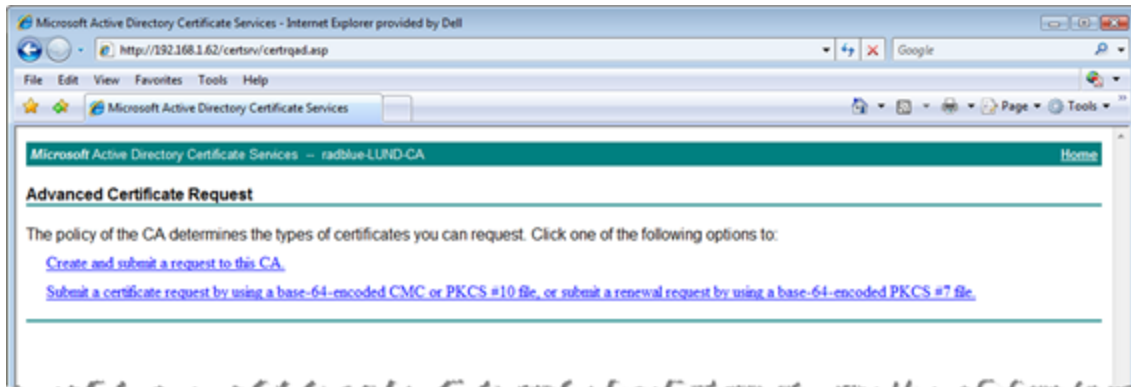
1. Open the certificate request file in Notepad or Wordpad, and click anywhere inside the content.
2. Perform a **CTRL+a** to highlight all content and a **CTRL+c** to copy the content.
3. Open an Internet browser, enter the certificate authority location, and press **Enter**.



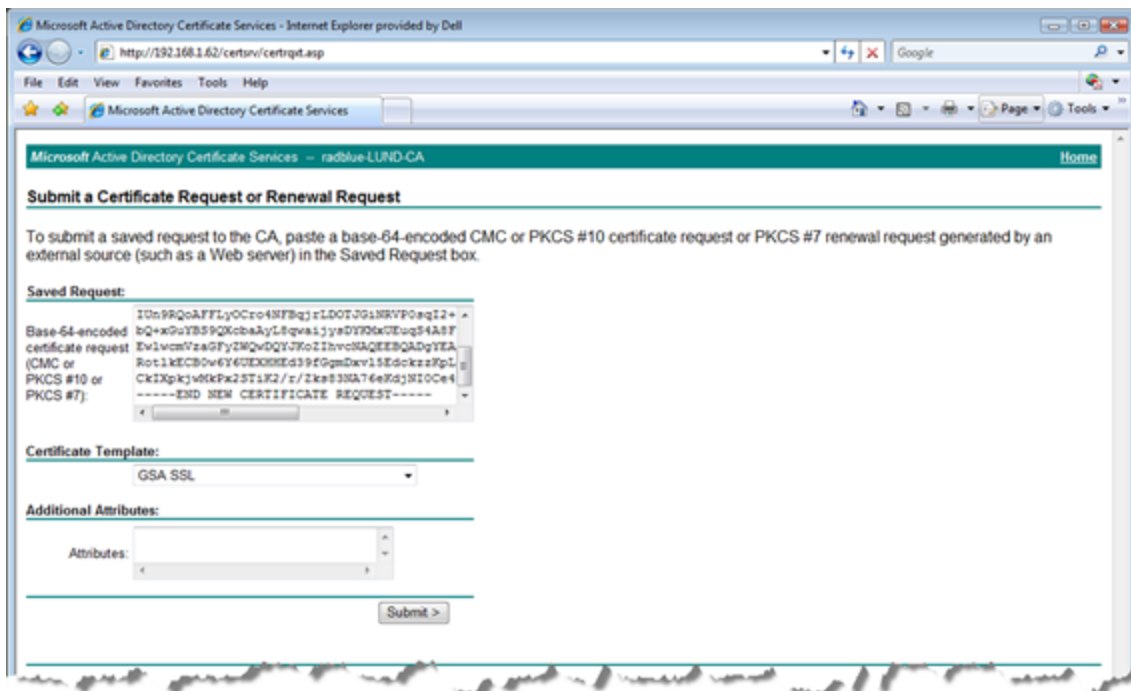
4. Click **Request a certificate**.



5. Click **advanced certificate request**.

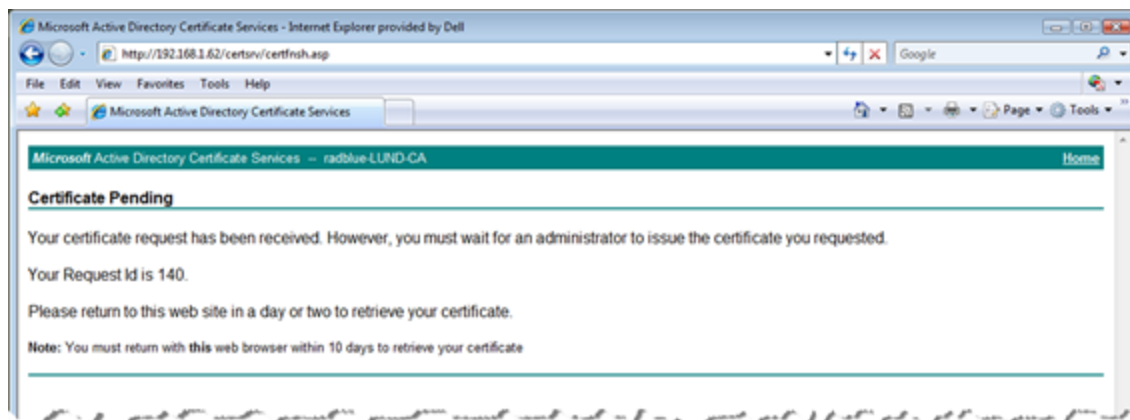


6. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-54-encoded PKC #7 file**.



7. Click inside the **Base-64-encoded. . .** field and paste the certificate request content that you copied in step 2.
8. Click the **Certificate Template** drop-down arrow, and select the certificate template you use. In this example, we selected **GSA SSL**.

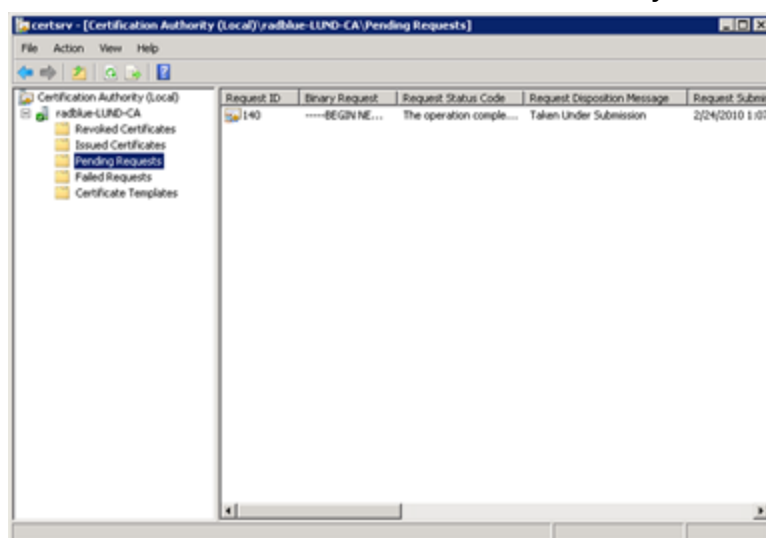
9. Click **Submit**.



10. Note the **Request ID**. In this case, the Request ID is **140**.

11. Minimize, but do not close, the browser.

12. From the computer where Microsoft Active Directory Certificate Services is installed, go to: **Start > Administrative Tools > Certification Authority**



13. Expand the server name, and click **Pending Requests**.

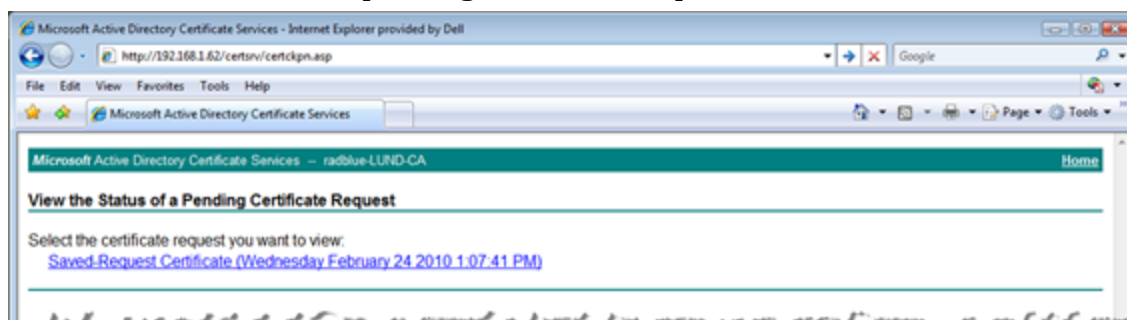
14. Click to highlight **Request ID 140**.

15. Right-click the entry, and select **All Tasks > Issue**. When the certificate is issued, it disappears from the list.

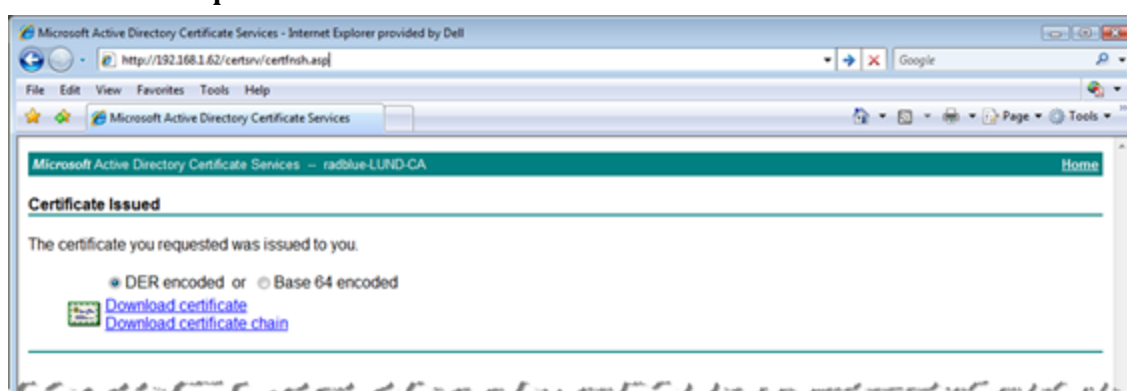
16. Maximize the browser window.

17. Click the **Home** link on the right-hand side of the page.

18. Click **View the status of a pending certificate request**.



19. Click **Saved-Request Certificate**.



20. Click **Download certificate chain** to download both parts of the signed certificate (certificate and CA certificate) as a single file. This is the recommended method because you only have one certificate to import into the tool.
If you want to create two separate files, click **Download certificate** to download the signed certificate file. Then, return to the home page and click **Download a CA certificate, certificate chain, or CRL**. Click **Download a CA certificate** to download the signed CA certificate file.
21. Once you have downloaded the certificate(s), open the tool and go to: **Configure > Security Options**
22. Select the **Third-Party** tab.
23. Click **Browse**, navigate to the signed certificate file, and click **Save**.
24. Click **Import Certificate** to import the selected certificate.
25. If you have an additional certificate, repeat steps 23 and 24.

Manage Key Store Options

From the Key Store tab, you can select the type of key store file you want to use and manage installed key store files.

1. From the menu bar, click **Tools**, and select **Configure** to launch the Configuration screen.
2. Click **Security Options**.
3. Click the **Key Store** tab.
4. Click the **Select Key Store File** drop-down arrow, and select the type of key store file you want to use with the tool.
Note: To update the available key store file types in the list, click **Refresh**.
6. To set the currently used certificate, click to highlight an installed certificate from the list and click **Set As Default**. The default value for this field is **<not set>**.
7. To remove an installed certificate, click to highlight the certificate, and click **Remove**.
8. To view the content of a certificate, click to highlight the certificate, and click **View**.

Import a PKCS #12 File

A PKCS #12 file is used to store multiple cryptography objects within a single file. The file commonly bundles a private key, with its X.509 certificate, or bundles all members of a chain of trust. The filename extension for PKCS #12 files is **P12** or **PFX**.

The **Import PKCS #12 File** option lets you quickly import the certificates stored in a P12 or PFX file into the tool's **client.jks** and **trusted.jks**. All certificates in the PKCS #12 file are imported to client.jks. Only non-key-entry certificates are imported to trusted.jks. Once the certificates are successfully imported, they can be viewed from the Key Store tab.

To import a PKCS #12 file:

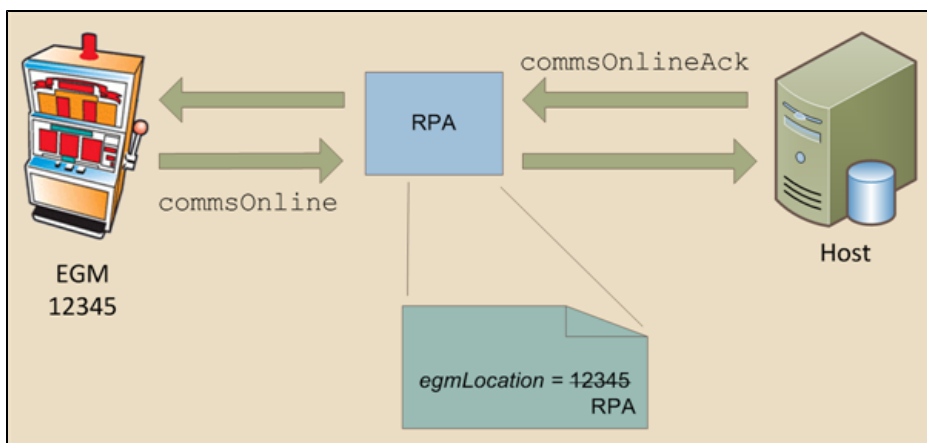
1. Under the **Import PKCS #12 File** section on the **Key Store** tab, and click **Browse**.
2. Navigate to the **P12** or **PFX** file you want to import, and click **Open**.
3. Type the file password.
4. Click **Import**.

The imported files are added to the list of key store files on the Key Store tab. Remember to use the **Select Key Store File** drop-down to switch between Trusted Key Store files and Client Key Store files.

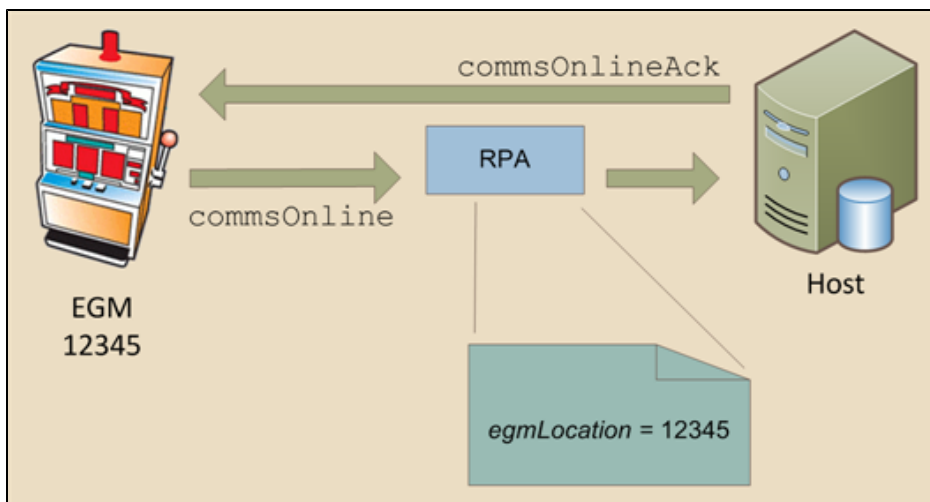
Configure Filter Options

Filter Options allows you to individually enable/disable each of the filters employed in RPA. Filters are small modules that act on the individual messages as they flow through RPA (in-line processing). Whether a filter is enabled or disabled determines what changes, if any, are made to the affected message. Filters can modify the original Simple Object Access Protocol (SOAP) message.

- CommsOnline Filter** - For G2S messaging. Select to enable the commsOnline filter. If selected, the *egmLocation* attribute in the `commsOnline` message is changed from the EGM's location to the RPA's location. For example:

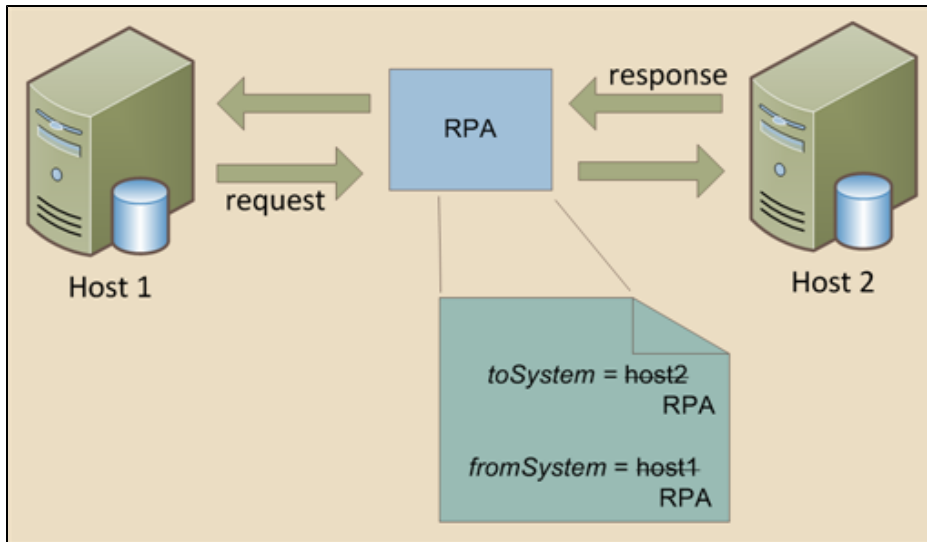


If this filter is cleared, the host bypasses RPA and communicates with the EGM directly. For example:

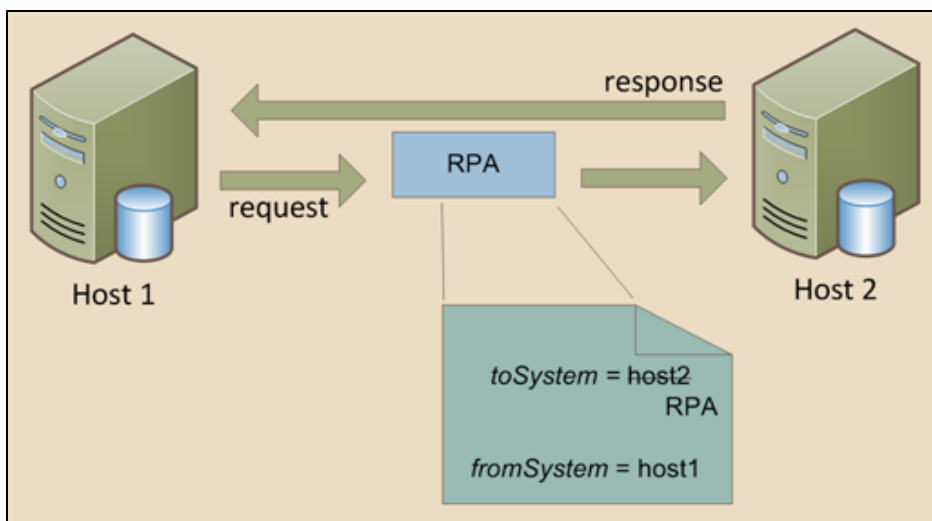


- S2S Header Filters** - For S2S messaging. Click to enable the s2sHeader filter. If selected, RPA modifies the *toSystem* and *fromSystem* attributes of S2S messages to the RPA location. This

allows messages to be directed through RPA. For example:



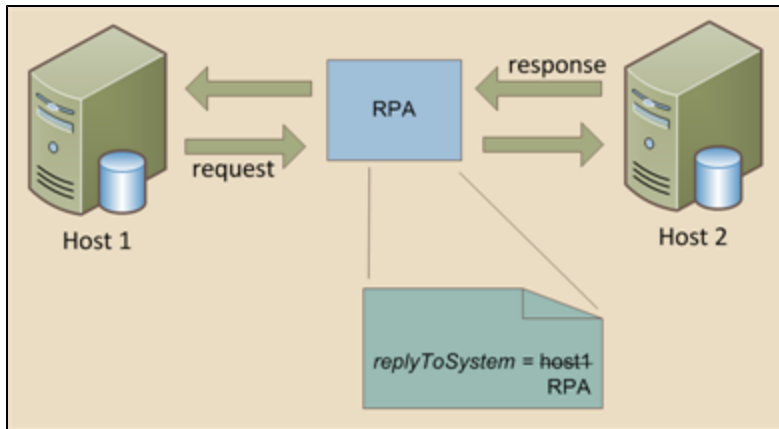
If this filter is cleared, S2S responses are sent directly to the recipient, rather than through RPA. For example:



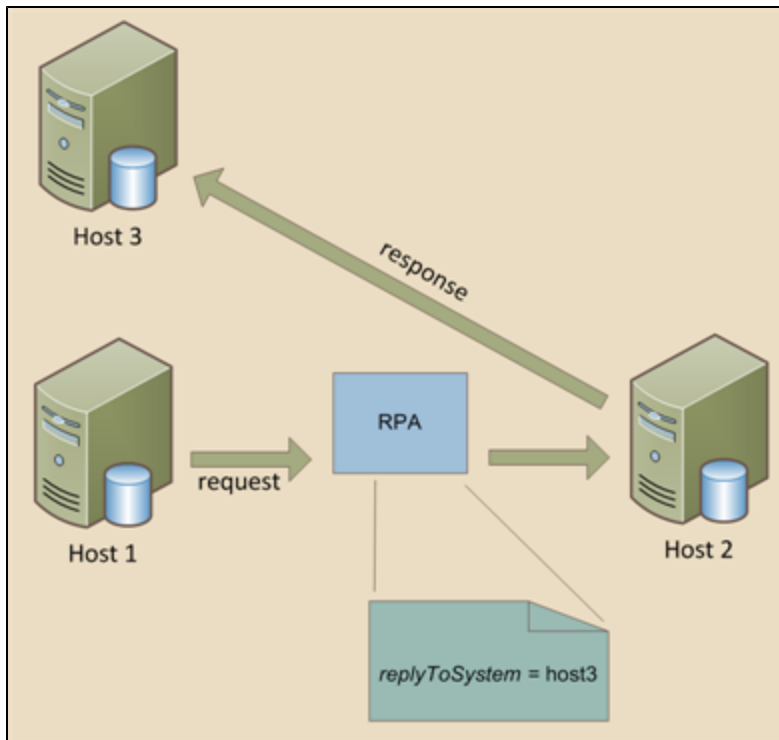
Note that deselecting this filter may cause confusion for host systems because responses go directly to the client while requests are routed through RPA.

- **S2S Reply to System Filter** - For S2S messaging. Click to enable the filter for messages containing the *replyToSystem* attribute. If the *replyToSystem* attribute is not set, no additional processing occurs.

If this filter is selected and the host that RPA is communicating with is in the *replyToSystem* field, RPA changes the *replyToSystem* value to the RPA location. For example:



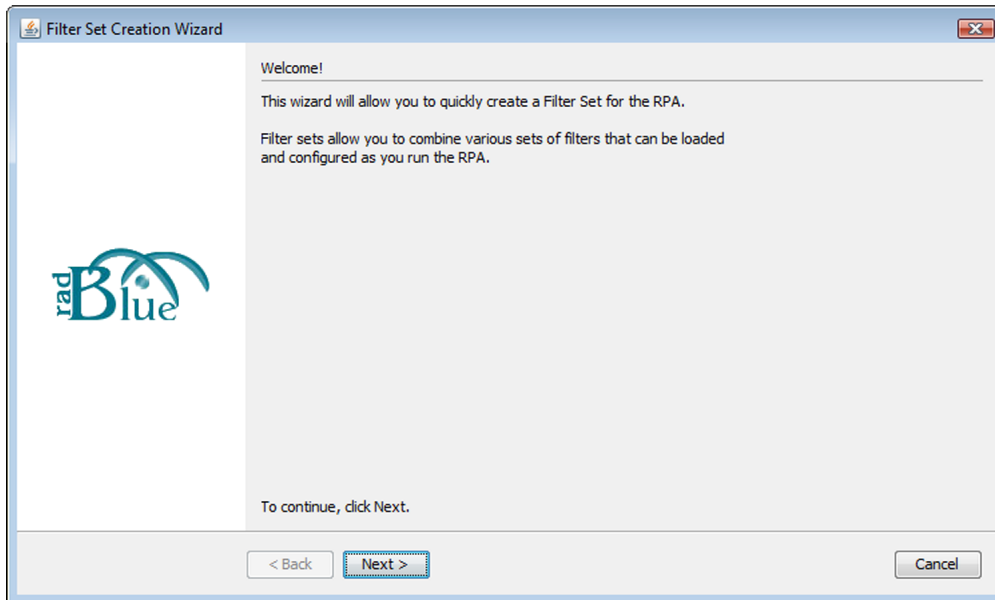
If this filter is selected and the host that RPA is communicating with is not in the *replyToSystem* field, RPA does not modify the message. For example:



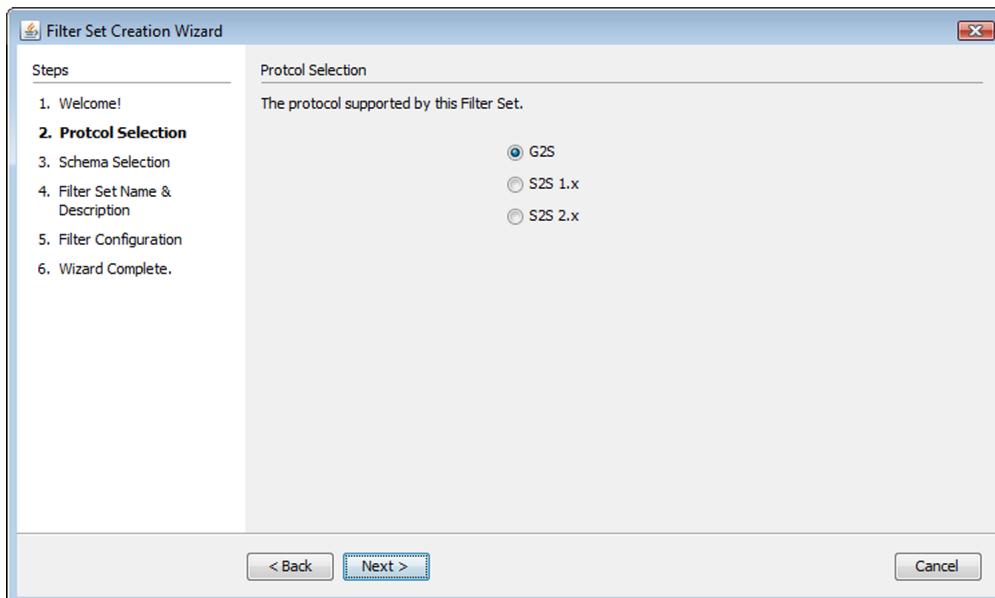
Add a Filter Set

The **Add Set** option launches the **Filter Set Creation Wizard**, which lets you define a new filter set.

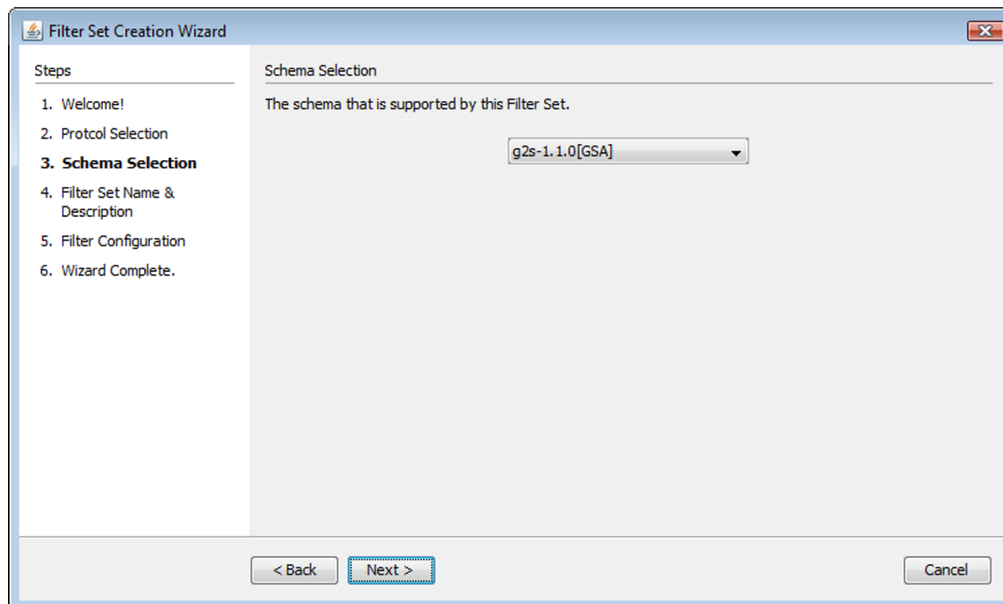
1. Click **Add Set**.



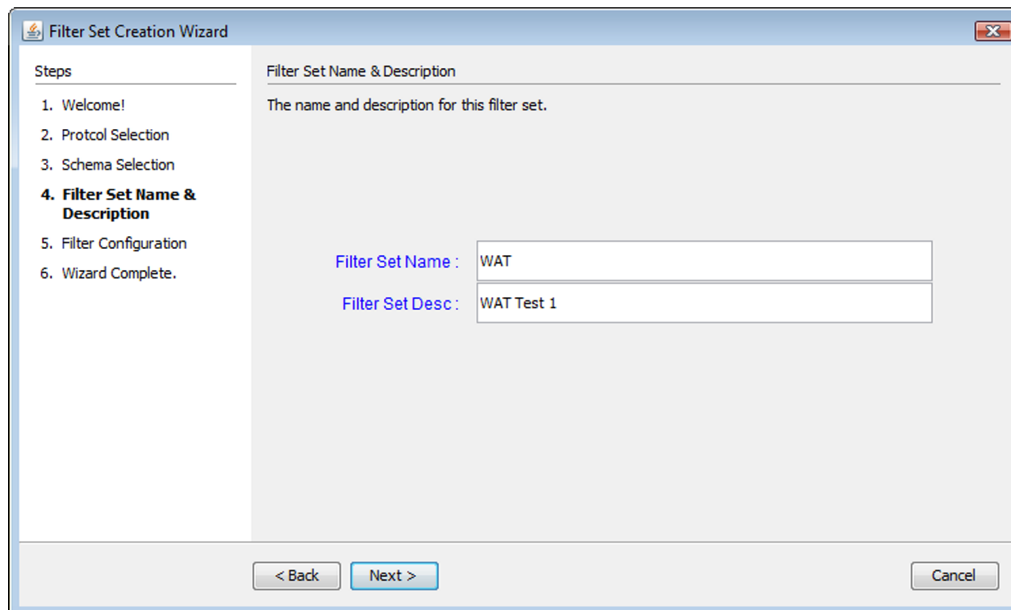
2. Click **Next**.



3. Click the protocol version you want associated with the filter set.
4. Click **Next**.

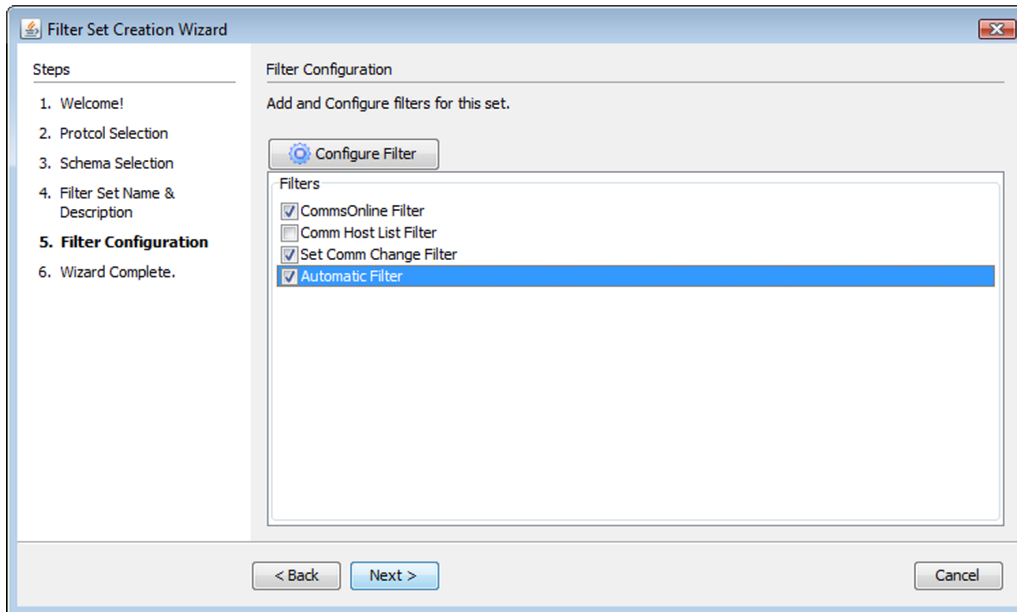


5. Click the drop-down arrow, and select the schema you want associated with the filter set.
6. Click **Next**.



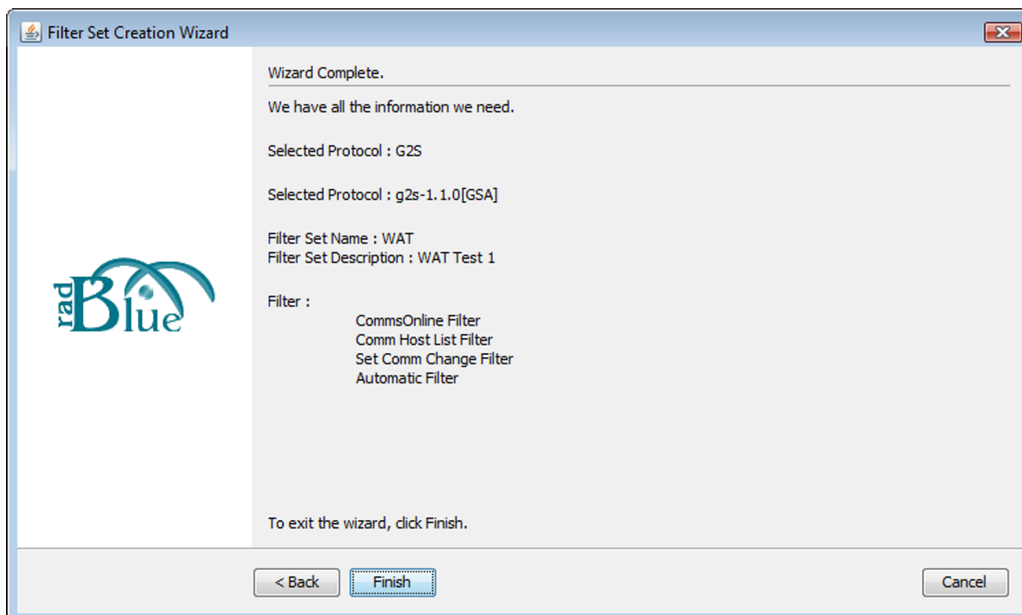
7. Type a name for the filter set.
8. Type a description for the filter set.

9. Click **Next**.



10. Select the filters you want used for the filter set.

11. *For Automatic Filters only*, click **Configure Filter** to configure the automatic filters in the filter set. See [Configure Automatic Filters](#) for more information.

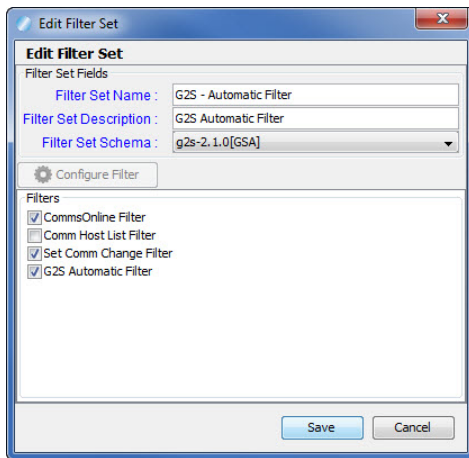


12. Click **Finish** to add the filter set to the Filter Options list.

Edit a Filter Set

You can edit a filter set through [Filter Options](#) on the RPA Configuration screen.

1. From the RPA menu bar, go to: **Tools > Configure > Filter Options**
2. Select the filter set you want to edit, and click **Edit Set**.



3. Modify the filter set, the selected [filter sets](#) or the [automatic filters](#) as needed.
4. Click **Save**.

Set or Clear the Default Filter

To make a filter set the default, click to highlight the filter set and click **Set Default**. The selected filter set name appears in the **Default Filter Set** field.

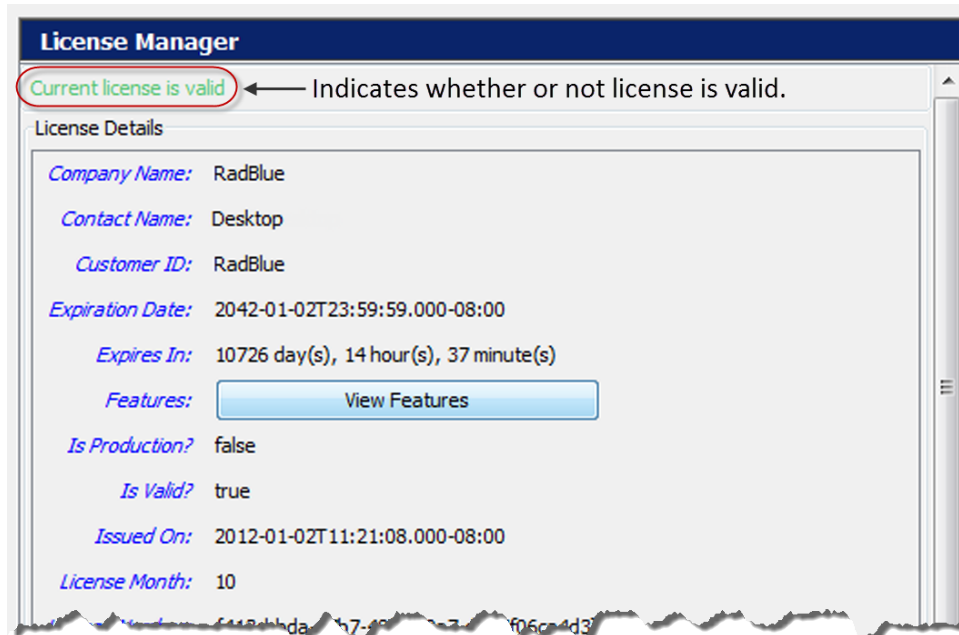
To clear the default filter set, click **Clear Default**.

Delete a Filter Set

To delete a filter set, click to highlight the set you want to delete and click **Remove Set**.

Configure License Manager Options

License Manager displays current licensing information, including the product features available under the license. The New License File option allows you to upload a new license file for the product.



License Details

- **Company Name** - Name of organization that purchased this license.
- **Contact Name** - Name of person license was issued to.
- **Customer ID** - Unique company identifier.
- **Expiration Date** - Date that tool becomes invalid.
- **Expires In** - Time left until license expiration.
- **Features** - Click **View Features** to see which features are enabled for your license.
- **Is Production?** - **True** indicates that the license is a fully licensed version.
- **Is Valid?** - **True** indicates that the license is valid; **False** indicates that the license is invalid.
- **Issued On** - Date of license issuance.
- **License Number** - Unique license identifier.
- **License Month** - Month that license expires.
- **License Year** - Year for which license is valid.
- **Load Message** - Status of license upload.

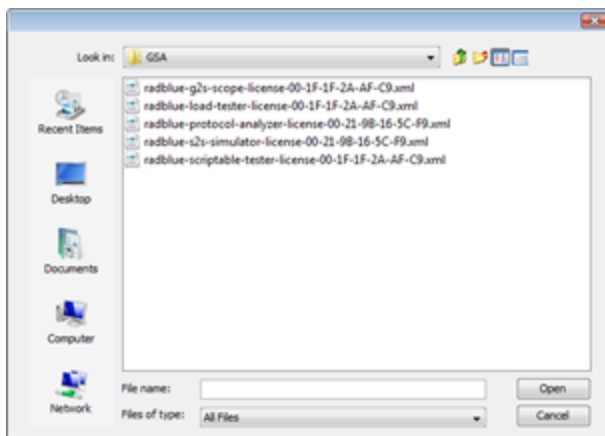
- **Location ID** - Location of purchasing organization.
- **MAC Address** - Physical address of computer on which the tool is installed.
- **Product Line Key** - Unique identifier of installed tool.
- **Product Name** - Name of licensed RadBlue product.

Load a New License File

To use the latest version of the tool, you may periodically need to update your license.

To load a new license:

1. Click the drop-down arrow.



2. Navigate to the new license file.
3. Highlight the new license file, and click **Open**.
4. Click **Apply** or **OK** to install the new license.

A

advanced transcript analyzer

about 103

filter 107

interface 104

print 108

start analyzing 105

C

client keystore 156

client.jks 156

configuration

desktop 131

filter 158

keystore 156

license 165

security 147

D

debug log

about 127

clear 128

filter 128

getting support 129

unresolved errors 129

default alias 156

desktop options 131

E

eventReport 103

F

filter options 158

G

getting support 129

K

keystore

client 156

default alias 156

remove certificate 156

trusted 156

view certificate 156

keystore options 156

L

license manager 165

load new license 166

load new license 166

M

message transcript

about 83

- add comment 93
- clear database 96
- clear display 96
- column description 85
- compare messages 88
- load messages 87
- search message content 90
- view command objects 91
- what are you looking for? 86
- Microsoft active directory certificate services 153
- multicast transcript
 - about 111
 - clear database 114
 - clear display 114
 - clear listeners 115
 - column descriptions 111
 - filter messages 112
 - load messages 112
 - receive real-time data 113
 - search message content 114
 - view message content 113

O

- ocsp 145
- options
 - desktop 131

- filter 158
- license 165
- security 147

P

- pkcs #12 file 157

S

- scep 149
- security options
 - about 147
 - enable ocsp 145
 - load a third-party certificate 151
 - load self-signing certificate 147
 - Microsoft active directory certificate services 153
 - scep 149
- support 129

T

- transcript
 - add comment 93
- transcript analysis report
 - about 97
 - device commands 99
 - device state 99
 - events 99
 - g2sAck errors 99
 - generate 98

- messages 100
- meters 100
- navigating 98
- sessions 101
- transcript 101
- transcript summary 102
- transcript, message
 - about 83
 - add comment 93
 - clear database 96
 - clear display 96
 - column descriptions 85
 - compare messages 88
 - load messages 87
 - search message content 90
 - view command objects 91
 - what are you looking for? 86
- transcript, multicast
 - about 111
 - clear database 114
 - clear display 114
 - clear listeners 115
 - column descriptions 111
 - filter messages 112
 - load messages 112
 - receive real-time data 113

- search message content 114
- view message content 113
- troubleshooting 127
- trusted keystore 156
- trusted.jks 156

W

- watchables
 - about 117
 - about xpath expressions 118
 - boolean expression usage 119
 - clear all data 119
 - copy 120
 - create 121
 - delete 121
 - edit 122
 - sample xpath expressions 118
 - select attributes 123
 - view 124
 - xpath expression format 118
 - xpath references 118

X

- xpath expressions
 - about 118
 - boolean expression usage 119
 - format 118

references 118

sample 118