



RadBlue Protocol Analyzer Version 13

[Released: 06 DEC 2010]

Questions?

Log on to the RadBlue Forum: <http://radblue.mywowbb.com/>

Release Notes

Release Summary

In this release, we added support for the *optional* Advanced Transcript Analyzer module.

For more information on the features and modifications discussed in this document, see the [RPA User Guide](#).

New Feature

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.

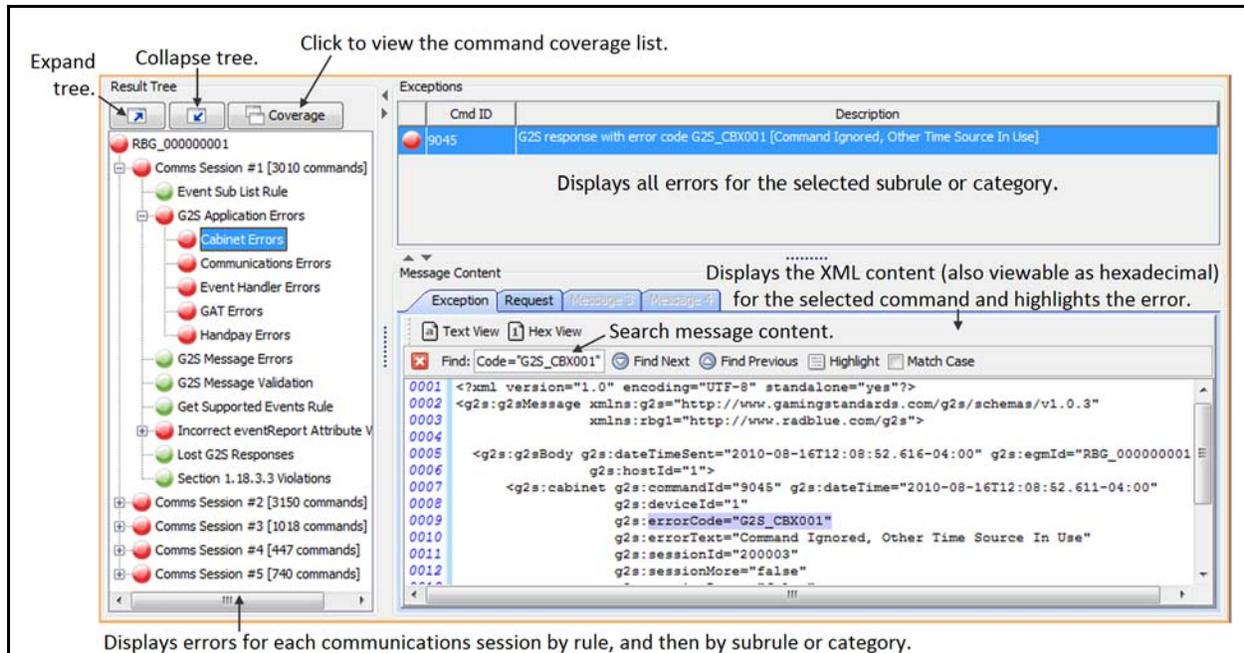
With the current version focusing on event subscriptions, the Advanced Transcript Analyzer validates:

- 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.

For information on purchasing the Advanced Transcript Analyzer, send us an [email](#) or give Russ Ristine a call at +1.775.329.0990.

Review the Advanced Transcript Analyzer Layout

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



Get Started Analyzing Command Data

1. From the Transcript layout, click the **Analyze** drop-down arrow, and select **Advanced**.
2. Double-click an EGM to display its information.

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.

Under each Comms Session, errors are grouped by rules, and then by subrules and categories.

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 or rule violations.

3. Look for red and yellow status icons. (If you only see green - Congratulations! Close the tool and take a well-deserved break.)
4. Double-click a red- or yellow-status **Comms Session** to expand it.

5. Double-click a red- or yellow-status rule to expand it

Note that, if a rule has no errors or warnings (is green), you cannot drill down into the subrules. The same error may appear more than once if it violates more than one rule.

6. Click a subrule or category to display those errors in the **Exceptions** section.
7. Click any error in the Exceptions section.

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

Transcript Modifications

- Previously, the same filtering options applied to all instances of the Transcript object within the tool. Now, each instance of the Transcript object can be filtered differently.



RadBlue Protocol Analyzer Version 12

[Released: 08 NOV 2010]

Questions?

Log on to the RadBlue Forum: <http://radblue.mywowbb.com/>

Release Notes

Release Summary

In this release, we corrected a minor issue on the Configuration interface.

For more information on the features and modifications discussed in this document, see the [RPA User Guide](#).

User Interface

- The Protocol Name and Version (**Configure > Engine Options > Protocol Options**) now correctly reflect value changes.



RadBlue Protocol Analyzer Version 11

[Released: 02 AUG 2010]

Questions?

Log on to the RadBlue Forum: <http://radblue.mywowbb.com/>

Release Notes

Release Summary

In this release, we corrected a Windows 7 permissions issue that occurred during installation, made some usability enhancements to the transcript and corrected some minor issues.

For more information on the features and modifications discussed in this document, see the [RPA User Guide](#).

Installation Note

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.

Installation Modifications

- A permissions issue that prevented RPA from installing on Windows 7 operating systems has been corrected.

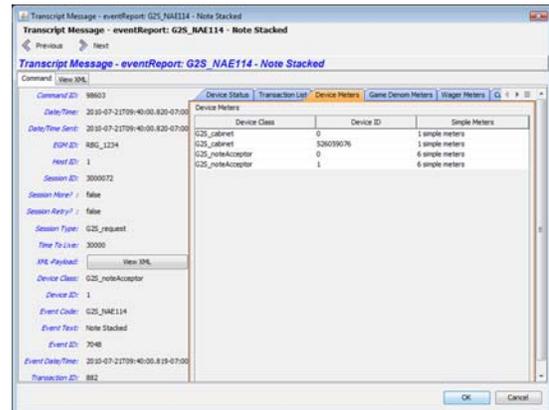
Engine Modifications

- Previously, RPA was not sending messages between the Central system and the Edge system because the `commsOnLine` command from the Central system was not being forwarded to the Edge system at startup. This issue has been corrected.
- The S2S common name has been modified to be the host name from the **MyURL** field on the **Configure > Engine Options** screen. If the MyURL field value is incorrect, "localhost" is used as the common name.

Transcript Modifications

- Previously, when an error was returned in the S2sAck response command, the summary was not displaying the error. The associated error is now displayed in the summary section when an S2SACK.error or communications.commsError response command is received.
- When the Transcript Message window is moved or resized, the tool now retains the new size and position when other rows are selected.
- The rows of the **Device Meters** tab on the eventReport command detail view now automatically resizes all rows so the columns do not need to be resized manually.

If the columns are adjusted, the tool retains the changes when other meter sets are viewed.





RadBlue Protocol Analyzer Version 10

[Released: 07 JUN 2010]

Questions?

Log on to the RadBlue Forum: <http://radblue.mywowbb.com/>

Release Notes

Release Summary

In this release, we added an option that lets you quickly export debug logs when troubleshooting RPA issues and corrected some minor issues.

For more information on the features and modifications discussed in this document, see the [RPA User Guide](#).

Functional Modifications

- A new **Export Debug** option, located on the Debug Log tab, lets you create a .zip file containing all the files that the RadBlue support team needs to troubleshoot product issues. When you click **Export Debug**, a **Debug-[product-x.x.x].zip** file is exported to your computer's desktop.

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

Engine Modifications

- The **S2S Retry** filter in the optional S2S disruptive filters feature has been modified to send an `s2sAck` response command after the command is dropped.

Transcript Modifications

- An issue in which the command filter (**Filter** option) caused some commands not to be displayed in the transcript (making it appear that the commands were not received by the tool) has been corrected.
- Minor spelling errors have been corrected on the `wat.getWatProfile` command view.
- The command view for the `wat.initiateTransfer` command now displays the correct pay method.



RadBlue Protocol Analyzer Version 9

[Released: 07 APR 2010]

Questions?

Log on to the RadBlue Forum: <http://radblue.mywowbb.com/>

Release Notes

Release Summary

In this release, we added support for S2S disruptive filters, added two new engine options and made minor corrections to the Transcript

For more information on the features and modifications discussed in this document, see the [RPA User Guide](#).

Functional Modifications

- Support for S2S Disruptive Filters (*filter set 2*) has been added, which includes the following filters:
 - ♦ **commsOnline filter** - 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.
 - ♦ **resend filter** - The resend filter drops the specified message without sending an `s2sAck` to the originator (so the originator realizes the message was lost).
 - ♦ **retry filter** - The retry filter drops the specified message, but sends an `s2sAck` to the originator (so the originator thinks the message was sent successfully, but then times out when the response message is not received).
 - ♦ **S2S header filter** - This filter changes the *fromSystem* attribute in the `s2sHeader` element from the sending system URL to the RPA URL.
 - ♦ **reply to system filter** - This filter changes the *replyToSystem* attribute in the `s2sHeader` element from original value to the RPA URL.

User Interface Modifications

- Two new parameters have been added to the **Configure > Engine Options** screen:
 - ♦ **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).

Transcript Modifications

- The Transcript has been updated to properly display eventReport event text. Previously, event text would not display if it contained a colon (:).
- The command view for invalid G2S messages now directs the user to view the command XML.



RadBlue Protocol Analyzer Version 8

[Released: 08 MAR 2010]

Questions?

Log on to the RadBlue Forum: <http://radblue.mywowbb.com/>

Release Notes

Release Summary

In this release, we added SSL support, simplified RPA URLs, and added a filter for the `bonus.bonusActivity` command.

For more information on the features and modifications discussed in this document, see the [RPA User Guide](#).

Installation Modifications

- RPA now uses **Java 1.6.0_18** for both Windows and Linux versions. This version of Java *must* be installed on your computer to complete RGS installation. If the installer does not detect this version of Java on your computer, you are prompted to download it
 - ♦ Click **Download** to download and install the new Java version before continuing with the installation.
 - ♦ Click **Locate** to browse to the **java.exe** file for version 1.6.0_18.
 - ♦ Click **Cancel** to exit the installation.

Configuration Modifications

- We've improved the **Configure > Security Options** screen to make using SSL easy. You can choose one of three options:
 - ♦ **Self-Signing** - Create a self-signed certificate from the tool.
 - ♦ **SCEP** - Use SCEP to create a request that is sent to the certificate authority and automatically imports the signed certificate when it becomes available.
 - ♦ **Third-Party** - Create a request that you manually send to the certificate authority, and then manually import the signed certificate into the tool.
- The **Approve all certificates** option under **Configure > Security Options** is now disabled by default. When this option is disabled, you must have a valid certificate from the certificate authority and use an SSL connection (HTTPS).

- The following modifications were made to the **Configure > Engine Options**:

- A **Filter Multicast G2S Bonus Activity from Transcript** option has been added. Enable this option to filter G2S `bonus.bonusActivity` commands from the Transcript and Multicast Transcript *if (and only if) the `bonus.bonusActivity` command is sent via multicast*.
 - The **Emulate RGS** option has been removed.
 - You can now define the inbound and outbound port numbers for both SSL and non-SSL communications in the **IP Address & SOAP Port** section.

Functional Modifications

- RPA now supports SSL messaging. You can configure SSL URLs on the **Engine Options** screen and manage SSL certificates on the **Security Options** screen.

Engine Modifications

- The generation of the `s2sAck` message has been corrected. Previously, this message was not reset with RPA as the originator of the `s2sAck` message.
- Previously, RPA dropped messages with invalid G2S. RPA now handles invalid messages in the same way as valid messages and passes the invalid messages on to the target entity.
- RPA now supports the following S2S schema versions:
 - 1.2.6
 - 1.2.6-igt
 - 1.3.1

User Interface Modifications

- RPA URLs have been simplified. They now use the format: **http[s]://[RPA IP address]:[port]/**

The four URLs used with RPA, for both G2S and S2S, are:

- ♦ Client-to-RPA non-SSL: **http://[RPA IP address]:35101/**
- ♦ Host-to-RPA non-SSL: **http://[RPA IP address]:35111/**
- ♦ Client-to-RPA SSL: **https://[RPA IP address]:35201/**
- ♦ Host-to-RPA SSL: **https://[RPA IP address]:35211/**

Note that the RPA IP address is the network address that the host and client systems use to communicate with RPA. This address is defined in the **Bind To** drop-down on the **Configure > Engine Options** screen, under the **IP Address & SOAP Port** section.

You can view URL information by clicking **Client Side Information** and **Host Side Information** on the main screen.

