

radblue

RSS 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.

RSS User Guide	1
About RadBlue	3
Contents	5
Chapter 1: Installing RSS	11
11	11
About the RSS Install	11
Pre-installation Requirements	11
Computer Requirements	11
Install RSS on Windows	12
Uninstall RSS	13
Chapter 2: Getting Started	15
About RSS	15
Supported S2S Classes	16
Additional Resources	17
Supported GSA Versions	17
The RSS User Interface	18
Menu Bar (1)	18
Tools	20
Help	20
Layout Tabs (2)	20
Control Panel (3)	21
Object Window (4)	21
Floor Tabs (5)	21
RSS Configuration Overview	22

Chapter 3: Using RSS	23
Emulate an Edge Server	23
Emulate a Central Host Server	25
Change the S2S Protocol Version	26
Create or Edit a Custom Command	28
Load a Custom Command	32
Send Raw XML	34
Reload XML Files	34
Chapter 4: Using IGT Extensions	35
About IGT S2S GAT Extensions	35
Using S2S GAT Extensions	36
Get List of Components (S2S Edge Server)	36
Verify Components (S2S Edge Server)	37
Request Verification Status of a Component (S2S Edge Server)	38
Send Verification Result (S2S Central Host)	39
Change Available Components (S2S Central Host)	40
Sample GAT-COMPONENT.XML File	40
Chapter 5: Using the Message Transcript	41
Working with the Message Transcript	41
Transcript Column Headers	42
Filter Transcript Messages Using the Quick Filter	43
What Are You Looking for in the Transcript?	43
Load Messages into the Transcript	44
Compare Messages in the Transcript	45
Filter Messages in the Transcript	46
Search the Content of Transcript Messages	47

View Message Details	48
Add a Comment to a Transcript Message	49
Clear the Transcript Display	50
Chapter 6: Using the SOAP Transcript	51
About SOAP Messages	51
Working with the SOAP Transcript	52
SOAP Transcript Column Headers	53
Filter SOAP Transcript Messages Using the Quick Filter	54
What Are You Looking for in the SOAP Transcript?	54
View the Content of a SOAP Message	54
Search the Content of a SOAP Message	58
Clear the SOAP Transcript Display	59
Clear the SOAP Transcript Database	59
Chapter 7: Using Watchables	61
About Watchables	61
About XPath Expressions	62
XPath Expression Format	62
Sample XPath Expressions	62
XPath References	62
Boolean Expression Usage	63
Clear All Watchable Data	63
Copy a Watchable	64
Create a New Watchable	65
Delete a Watchable	65
Edit a Watchable	66
Select Attribute(s) to Track in Watchables	67

View a Watchable	68
Appendix A: Troubleshooting	71
About the Debug Console	71
Clear the Debug Log Display	72
Filter Debug Log Messages	72
What to Do If You Can't Resolve an Error	73
Appendix B: Customizing RSS	75
Configure Desktop Options	75
Configuring RSS Engine Options	76
Database	76
Transport	77
Configuring Namespace Options	78
Add a Namespace	78
Remove a Namespace	78
Configure Security Options	79
Configure General Security Options	80
Enable and Configure OCSP	81
Create or Import a Signed Certificate	82
Use SCEP to Request a Certificate	83
Load a Third-Party Certificate	85
Obtain a Signed Certificate Using Microsoft Active Directory Certificate Services	87
Load a Self-Signing Certificate	91
Manage Key Store Options	92
Import a PKCS #12 File	92
Configure License Manager Options	94
Load a New License File	95

Index	97
--------------------	-----------

About the RSS Install

RSS is only supported on Windows (Vista or 7).

Pre-installation Requirements

1. You must have the RSS license file on your computer prior to installing RSS . If you are using a special version of RSS , you must have a license for that version. If you have not received an RSS license file, contact [RadBlue Support](#).
2. Install Microsoft .NET Framework to use RSS. Download the .NET Framework application and follow the Microsoft .NET Framework installation instructions.
<http://www.microsoft.com/Net/Download.aspx>
3. If your computer does not have the latest required version of Java installed, you are prompted to download and run the Java installer, or to navigate to the correct Java version.

Computer Requirements

The minimum requirements for computers running the simulator are:

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

Install RSS on Windows

Follow these steps to install RSS.

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

6. Click **Browse**, and navigate to the location of the RSS license file.

Note: For version 34 and higher, if you install a version of RSS 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 RSS over a previous installation. All components of the previous installation are removed by the installer except the license file and any backup files.

9. Select the **Start Menu folder** for RSS.

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 RSS, select **Don't create a Start Menu** folder.

10. Click **Finish**.
11. Double-click the **RSS Central** desktop icon to launch the S2S central host simulator.
12. Double-click the **RSS Edge** desktop icon to launch the S2S EGM, kiosk or host simulator.

Uninstall RSS

You can uninstall RSS through the **Uninstall** option (**Start > All Programs > RadBlue S2S Simulator**) or by running the **uninstall.exe** file in the RSS installation directory.

When RSS is uninstalled, a backup folder is created in the RSS directory that saves the installation's security and configuration parameters. When a subsequent RSS 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.

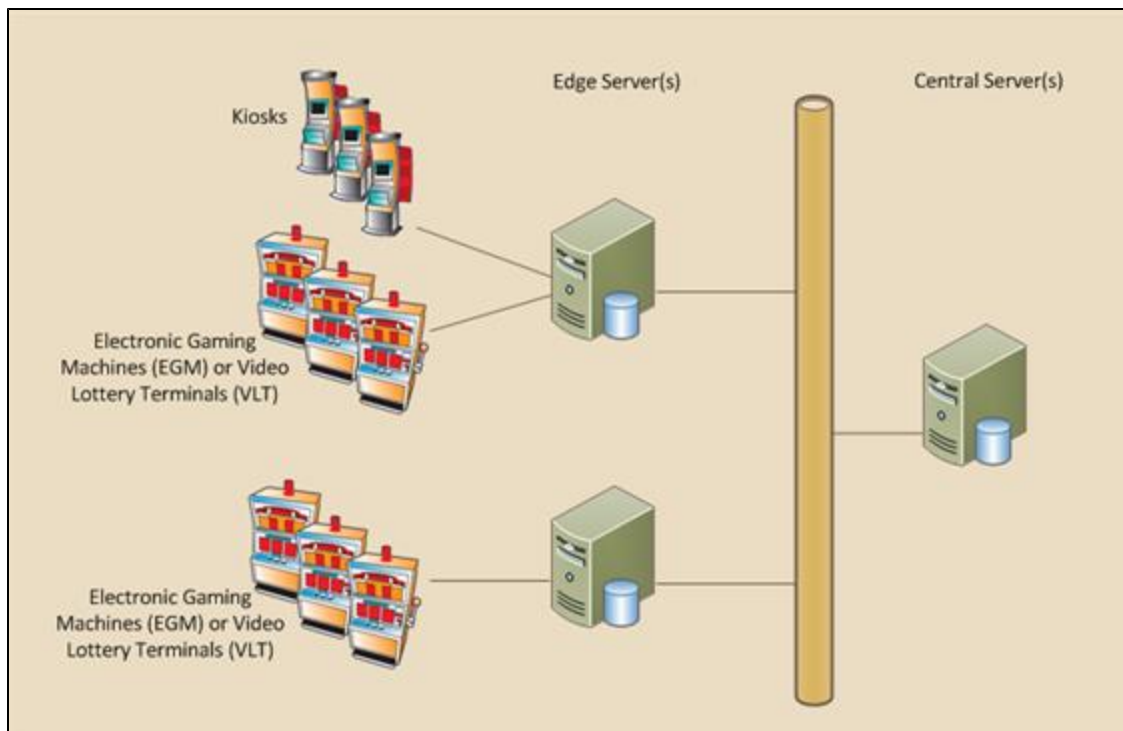
The backup folder is located in the RSS installation directory. The following files are saved in the backup folder:

- All Java Keystore Files (JKS)
- Edge scep_config.xml
- Edge security_manager.xml
- Edge webserver.xml
- Edge Derby Port
- Central scep_config.xml
- Central security_manager.xml
- Central webserver.xml
- Central Derby Port

About RSS

The RadBlue S2S Simulator (RSS) lets you simulate either endpoint for communications between an S2S central host ("Central") and another S2S server ("Edge"), which communicates with Electronic Gaming Machines (EGMs), Video Lottery Terminals (VLTs), and kiosks.

Edge servers typically provide central game determination or other functions for a subset (or all) of the EGMs (and other devices) on the gaming floor.



In Class II (central determination) environments, data captured by multiple Edge servers is consolidated onto a "Central server," which are larger servers where the centralized databases and consolidating applications reside. Through a centralized voucher database, a voucher generated on one manufacturer's EGM can be redeemed on another EGM from a different manufacturer. In addition, the Central server provides a consistent player tracking feed, a single accounting report, a single voucher redemption terminal at each cashier position, ticket redemption kiosks, and all of the other benefits that come from having centralized databases.

The Edge server and Central Server enables the user to generate any valid command in the implemented classes to stimulate the system under test.

Supported S2S Classes

The table below lists the supported S2S classes.

Note: In all cases, the other entity (either Edge or Central) will respond to a request in these classes.

Additional S2S classes and commands can be added as needed. [Contact RadBlue](#) for more information.

Class	You can send commands from. . .	Description
accountingMeter	Edge and Central	Provides a way for a client system to receive accounting meter information from the host system.
communications	Edge and Central	Edge server initiates communications with the central server, and then sends a variety of commands to report status changes in the communications class.
comp	Edge and Central	Can issue comp requests to the Central system.
configuration	Edge and Central	The Edge server can request configuration information from the Central server for several classes.
eventFilter	Edge and Central	Manages event subscription information.
fillCredit	Edge and Central	Send a fillCredit issuance command from the Edge server, or send a fillCreditInfo message from the Central server.
financialTransaction	Edge only	Post and void financial transactions, request cash balances and request financial transaction histories.
gat	Edge and Central	Authentication based on regulatory requirements.
handpay	Edge only	Initiate Edge server requests from handpay data.
infoUpdate	Edge and Central	Subscribe to infoUpdate from the Edge server. Send infoUpdate commands from the Central server.
jackpot	Edge and Central	Table game jackpot transactions and jackpot information requests between systems.
marker	Edge and Central	Issue a marker or voucher from the Edge server, or send an update from the Central server.
openClose	Edge and Central	Open, post and close a table's chip inventory from the Edge server.
patron	Edge and Central	Player management messages sent between a server and a patron data warehouse system.
player	Edge only	Communication of carded player gaming activity to central player tracking system.

Class	You can send commands from. . .	Description
playerRating	Edge and Central	Start a rating, update a rating, close a rating and void a rating from the Edge server. Use the Central server to send the ratingInfo command.
registerClient	Edge only	Edge server replicates data about any of its clients (including EGMs) to the central server.
voucher	Edge only	Communication to central voucher system to add and redeem gaming vouchers.
wat	Edge only	From the Edge server, you can request WAT funds, get an account balance and transfer WAT funds.

Additional Resources

- [RSS Release Notes](#)

Supported GSA Versions

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

Protocol	Versions	
S2S	1.3.1	1.4.2

The RSS User Interface

Let's take a look at the RSS Interface.

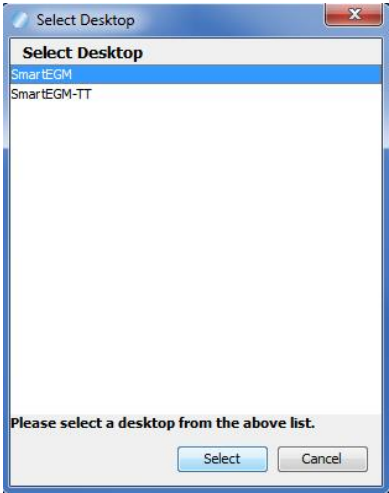
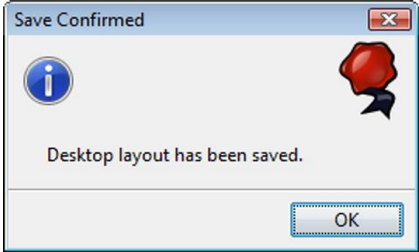
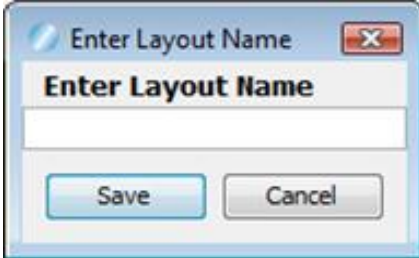
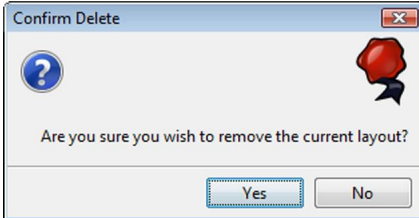


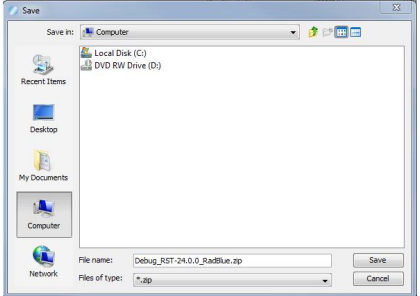
Menu Bar (1)

From the menu bar you can access product options.

File

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>	<p>The dialog box titled 'Enter Desktop Name' has a text input field and 'Save' and 'Cancel' buttons.</p>

Option	Description	Screen
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>	
Add Layout	<p>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.</p>	
Remove Layout	<p>Select to delete the currently displayed layout.</p> <p>Click Yes to delete the layout.</p>	

Option	Description	Screen
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

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

Layout Tabs (2)

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).

Layout Tab	Description
ScriptControl	Lets you change the script for testing. The Script File field displays the currently selected S2S script. A script configures the RSS to emulate either a Central or Edge server, and specifies the version of S2S is being supported.
Transcripts	Lets you see messages, in real-time, as they are sent and received.
Watchables	Allows you to search for a specific attribute or value in that attribute. This feature is based on XML Path Language queries.
Debug Console	Shows all informational, warning, and critical errors that occur in the tool.

Control Panel (3)

Each tab shows unique controls:

- ScriptControl tab - start and stop the script.
- Transcripts tab - manage S2S transcripts, such as: load, filter, and clear.
- Watchable tab - monitor specific attributes and attribute values.
- Debug Console tab - see messages and their status.

Object Window (4)

The object window displays content associated with the selected tab. In this example, you see the **Available S2S Commands** - Commands that can be sent by RSS. The commands displayed depend on whether RSS is running as a Central or Edge server script.

Floor Tabs (5)

Open/Close - The floor tab displays objects that you can drag and drop onto the *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: Script, Display, 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.

RSS Configuration Overview

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

1. Start the RSS Edge Server by double-clicking the desktop icon.
2. Start the RSS Host Server by double-clicking the desktop icon.
3. Configure RSS Startup Options:
 - [Desktop Options](#)
 - [Engine Options](#)
 - [Namespace Options](#)
 - [Security Options](#)
 - [License Manager Options](#)

Emulate an Edge Server

The Edge server lets you send S2S commands to a central host server as an EGM, kiosk or cashier. Before you start sending commands, you must configure the Edge server. Use the Message Transcript to see all sent and received commands.

You can reset the From System and To System fields by clicking **Reset**.

Delete History removes information stored locally for the user interface. This option should be used only, at the direction of RadBlue support, during troubleshooting.

1. Double-click the **RSS Edge** desktop icon.

2. Configure the **S2S Edge script** as required.

If you are using Central and Edge together, they are configured by default to communicate with one another. No configuration changes are required.

- **Vendor ID** - Type the Edge server's 3-letter vendor identifier. This identifier is available through the Gaming Standards Association (GSA).
- **Vendor Name** - Type the Edge server's vendor name.
- **Client ID** - Type a unique identifier for the Edge server.
- **Client Type** - Click to select whether the Edge will act as an EGM, kiosk or cashier.
- **Property ID** - Type a property identifier for the client
- **From System** - Type the URL of the Edge server.
- **To System** - Type the URL of the Central server.

3. Click **Start Script**.



4. The interface lists commands, by class, that are supported by the RSS Edge.
5. Click the link for the command you want to send.
6. Enter command parameters, if any, as required. For information on S2S commands, see the [S2S Message Protocol](#).
7. Click **Send Command**, or click **Cancel** to return to the main screen.
8. Use the Transcript object to view commands and their responses. See Working with the Transcript.

Emulate a Central Host Server

The Central host server lets you send S2S commands to an Edge server (EGM, kiosk or cashier). Use the [Message Transcript](#) to see all sent and received commands.

Delete Browser History removes information stored locally for the user interface. This option should be used during troubleshooting, at the direction of RadBlue support *only*.

1. Double-click the **RSS Central** desktop icon.

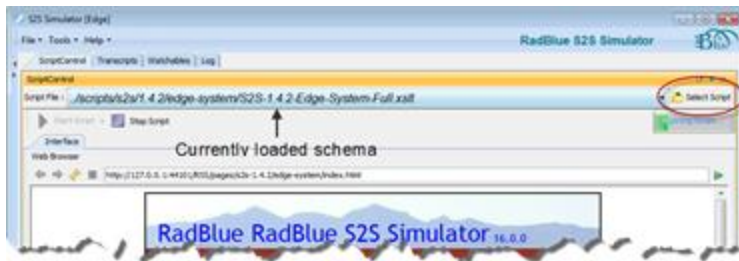


2. Click **Start Script**. The interface lists commands, by class, that are supported by the RSS Central.
3. Click the link for the command you want to send.
4. Enter command parameters, if any, as required. For information on S2S commands and attribute descriptions, see the [S2S Message Protocol](#).
5. Click **Send Command**, or click **Cancel** to return to the main screen.
6. Use the [Message Transcript](#) to view commands and their responses.

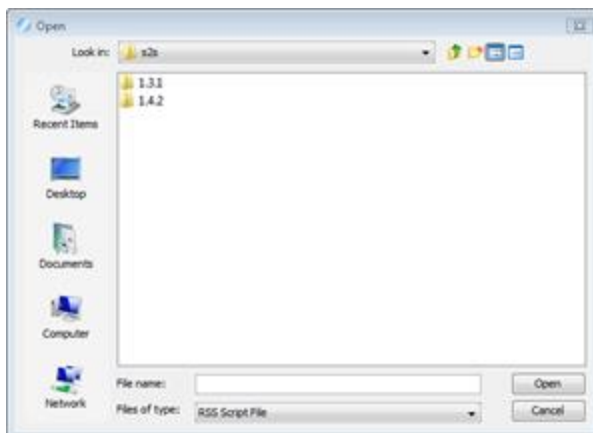
Change the S2S Protocol Version

RSS supports S2S 1.3.1, 1.4.2 and 1.5.0 for both Edge and Central Host. You can change the protocol version through the **Select Script** option.

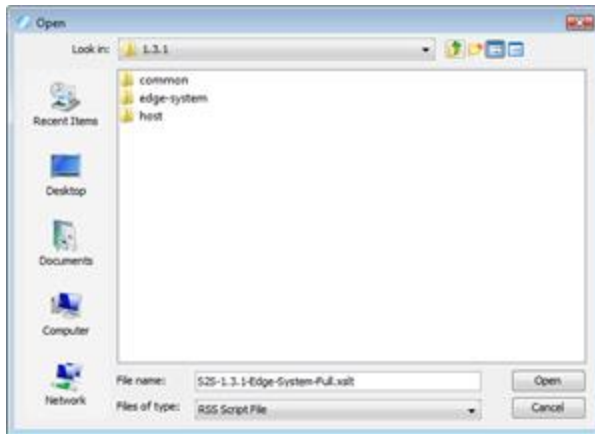
1. Click **ScriptControl**.



2. Note the currently loaded protocol in the **Script File** field.
3. Click **Select Script**.
4. Click the "up" arrow, to the right of the folder drop-down, to the **s2s** folder.



4. Select the protocol version you want to load. For this example, we chose version 1.3.1.



5. Depending on which endpoint you are using, select either **edge-system** or **host**.
6. Select the **XSLT** file.
7. Click **Open**.

Create or Edit a Custom Command

You can customize the content of certain S2S commands by editing the associated XML file (or by using **Save As** while editing to create a new command file). If you are testing *your own* commands, you can add your own elements and attributes in a custom namespace. When the custom command information is sent by RSS, the command ID, session ID and date/time values are updated automatically.

Note that each file contains only one command *except for* the `patron.patronInfo` command, in which a single file can contain multiple unique patron identifiers.

You can customize the following commands:

accounting	Edge/Central	Request/Response
accountingMeters.getMeters	Central	Request
accountingMeters.meterInfo	Edge	Response
accountingMeters.meterSubList	Edge	Response
accountingMeters.setMeterSub	Central	Request
accountingMeters.supportedMeters	Edge	Response

comp	Edge/Central	Request/Response
comp.compAvailabilityList	Central	Response
comp.compInfo	Central	Response
comp.compInfoList	Central	Response
comp.compInfoReq	Edge	Request
comp.getComp	Edge	Request
comp.getCompAvailability	Edge	Request
comp.getKeyPair	Edge	Request
comp.issueCompReq	Edge	Request
comp.keyPair	Central	Response
comp.redeemCompReq	Edge	Request
comp.voidCompReq	Edge	Request

eventFilter	Edge/Central	Request/Response
eventFilter.eventById	Edge	Response
eventFilter.setEventSubById	Central	Request
eventFilter.supportedEvents	Edge	Response

gat	Edge/Central	Request/Response
gat.componentList		
gat.doVerification	Central	Request
gat.verificationResult	Edge	Response
gat.verificationStatus	Edge	Response

infoUpdate	Edge/Central	Request/Response
infoUpdate.hostInfoUpdateList	Edge	Response
infoUpdate.infoUpdateData	Edge	Request
infoUpdate.infoUpdateSubList	Edge	Response
infoUpdate.setInfoUpdateSubList	Central	Request

jackpot	Edge/Central	Request/Response
jackpot.issueJackpotReq	Edge	Request
jackpot.jackpotInfo	Central	Response
jackpot.redeemJackpotReq	Edge	Request
jackpot.voidJackpotReq	Edge	Request

patron	Edge/Central	Request/Response
patron.patronInfo	Central	Response

registerClient	Edge/Central	Request/Response
registerClient.clientIdsByTypeList	Edge	Response
registerClient.clientRegistrationInfo	Edge	Response
registerClient.clientRegistrationInfoList	Edge	Response
registerClient.getClientRegistrationList	Central	Request
registerClient.setClientRegistration	Central	Request

voucher	Edge/Central	Request/Response
voucher.ackVoucher		
voucher.authorizeVoucher	Central	Response
voucher.commitVoucher	Edge	Request
voucher.issueVoucher	Edge	Request
voucher.redeemVoucher	Edge	Request
voucher.requestVoucherActivity	Edge	Request
voucher.setVoucherConfig	Central	Request
voucher.validationIdList	Central	Response
voucher.voucherActivityList	Central	Response

voucher	Edge/Central	Request/Response
voucher.voucherActivityRptTransferred	Central	Response
voucher.voucherConfig	Edge or Central	Response
voucher.voucherLogList	Edge	Response
voucher.voucherLogStatus	Edge	Response
voucher.voucherStatusInfo	Edge	Response

wat	Edge/Central	Request/Response
wat.authorizeTransfer	Central	Response
wat.commitTransfer	Edge	Request
wat.getKeyPair	Edge	Request
wat.getWatAccounts	Edge	Request
wat.getWatBalance	Edge	Request
wat.keyPair	Central	Response
wat.requestTransfer	Edge	Request
wat.watAccountList	Central	Response
wat.watBalance	Central	Response
wat.watLogList	Edge	Response
wat.watLogStatus	Edge	Response
wat.watStatus	Edge	Response

For information on the content of each command, see the [S2S Message Protocol](#).

To customize a command file:

1. Navigate to the RSS installation directory, and open the **rss-data** folder.
2. Right-click the XML command file you want to edit, and select **Open With > WordPad** or open the file with the XML editor of your choice. For this example, we selected the **infoUpdate.infoUpdateData-001.xml** file.
3. Modify the message content as required. You can cut and paste the XML content of the same S2S command directly from the [Message Transcript](#) into the XML file.

Note: All elements and attributes in the XML file must be valid, against the selected S2S schema, for the specified command. Otherwise, an error is generated when the command is sent by RSS.

4. Click **File > Save**.

or

Click **Save As**, and type a new file name.

Note: If an XML file does not use the naming convention **[class].[command]-[yourDescription]**, it will not display in the XML file list. For example:
accountingMeters.meterInfo-MyCommand.xml.

4. Close the file.
5. Go to the RSS, and click [Reload XML](#) to load your changes.
6. [Load and send your custom command\(s\)](#).

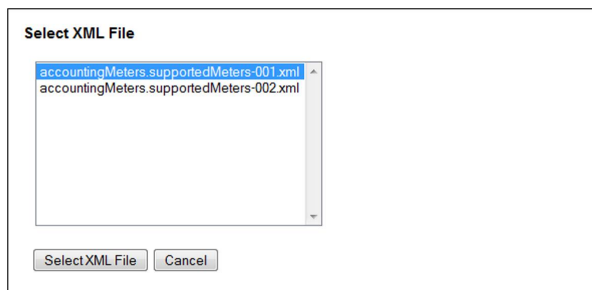
Load a Custom Command

There are two types of custom commands in RSS: response commands that are sent automatically when the corresponding request command is received by RSS and request commands that you send manually through the RSS interface.

1. From the main screen, click [Reload XML Files](#) to ensure you have the latest version of all XML files.
2. Click to select a custom command. For example:



2. Click **Change** to select a different XML file.



3. Select the XML file you want to use, and click **Select XML File**.

Note: If an XML file does not use the naming convention **[class].[command]-[yourDescription]**, it will not display in the XML file list. For example:
accountingMeters.meterInfo-MyCommand.xml.

4. Depending on the command you have selected, click **Save Configuration** or **Send Command**.

Send Raw XML

The Send Raw XML option lets you send any content to an S2S endpoint over an S2S connection. RSS does no additional wrapping of the message, but rather, sends exactly what you have entered to the endpoint.

1. Click **Send Raw XML**.



2. Click inside the text box.
3. Type or paste the message content into the text box.
4. If you do not want the S2S content validated by RSS, clear the **Validate XML?** checkbox.
5. Click **Send Raw XML** to send the message.

Reload XML Files

You can [customize an S2S command](#) by editing its associated XML. Once you've updated an XML file, click the Reload XML Files option to reload all XML files.

About IGT S2S GAT Extensions

S2S GAT has been added to the S2S Central Host (SDDP/download server) and S2S Edge (SMP/sb Director) simulators.

The following GAT commands have been added to the S2S Edge simulator:

- **gat.getComponentList** - request a list of components from the S2S Central Host.
- **gat.doVerification** - request verification of specified component from the S2S Central Host.
- **gat.getVerificationStatus** - request status of component verification from the S2S Central Host.

The GAT command, `gat.verificationResult`, has been added to the S2S Central Host simulator. This command is used to create and send a verification result message.

GAT functionality is supported in both the S2S Central Host and S2S Edge XSLT scripts. For the S2S Central Host, the new script is:

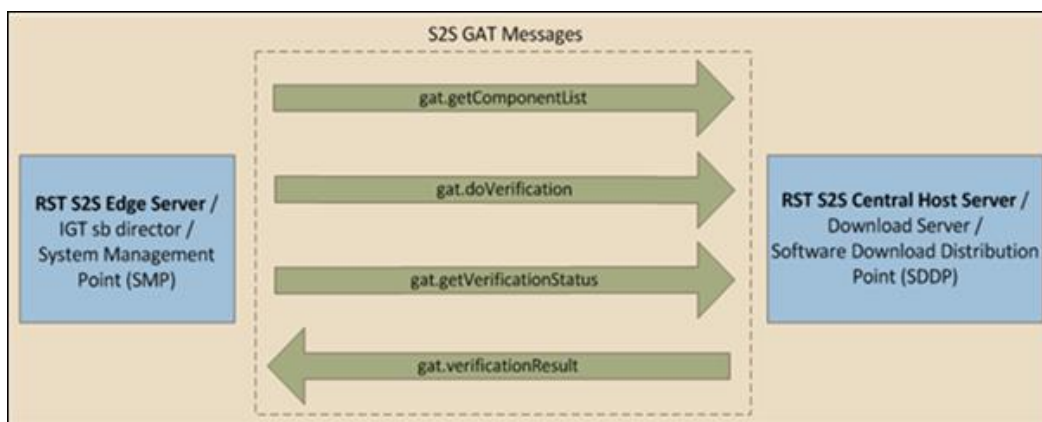
..\radblue\gsa\script\scripts\s2s\1.2.6-igt\host\S2S-1.2.6-Edge-System-Full.xslt

For the S2S Edge simulator, the new script is:

..\radblue\gsa\script\scripts\s2s\1.2.6-igt\edge-system\S2S-1.2.6-Host-Full.xslt

Using S2S GAT Extensions

To examine S2S GAT extensions on one PC, you must install and run two separate instances of the RadBlue S2S Simulator: one to act as the Central Host simulator and one to act as the Edge simulator. Of course, either simulator can be used to test an actual server.



S2S GAT messaging flow

Get List of Components (S2S Edge Server)

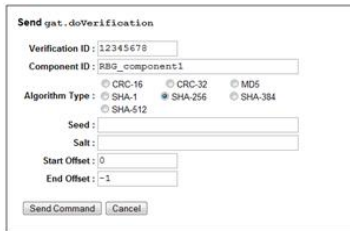
1. Click **gat.getComponentList**.



2. Select the types of components you want to request.
3. Click **Send Command**.
4. Select the **Transcript** object, and double-click the **gat.componentList** message to view the response.

Verify Components (S2S Edge Server)

1. Click **gat.doVerification**.



Send gat.doVerification

Verification ID: 12345678

Component ID: RSG_component1

Algorithm Type: ☐ CRC-16 ☐ CRC-32 ☐ MD5 ☒ SHA-1 ☐ SHA-256 ☐ SHA-384 ☐ SHA-512

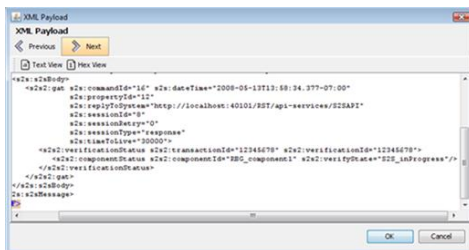
Seed:

Salt:

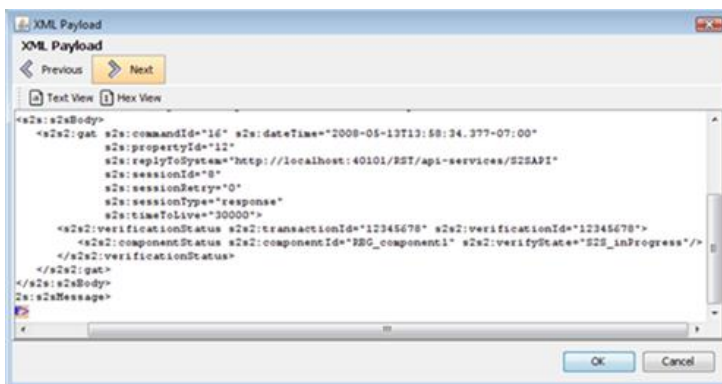
Start Offset: 0

End Offset: -1

2. Enter the identification and verification information for the component you want to verify.
For component information, select the **Transcript** object, and double-click the **gat.componentList**. For example:



3. Click **Send Command**.
4. Select the **Transcript** object, and double-click the **gat.verificationStatus** message to view the response. For example:



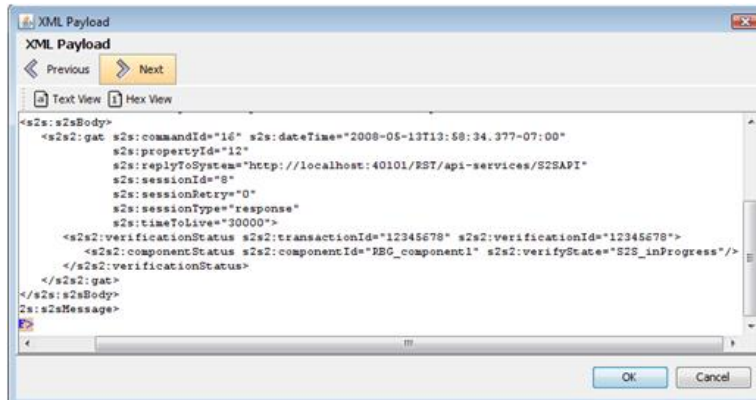
Request Verification Status of a Component (S2S Edge Server)

1. Click **gat.getVerificationStatus**.



A dialog box titled "Send gat.getVerificationStatus". It contains two input fields: "Verification ID" with the value "12345678" and "Transaction ID" which is empty. At the bottom are two buttons: "Send Command" and "Cancel".

2. Enter the transaction identification number (**Transaction ID**) of the component for which you are requesting status information. The default Transaction ID is **12345678**.
3. Click **Send Command**.
4. Select the **Transcript** object, and double-click the **gat.verificationStatus** message to view the response. For example:



Send Verification Result (S2S Central Host)

1. Click **gat.verificationResult** from the GAT (IGT) section of the S2S Central Host.

Send gat.verificationResult

Verification ID: 12345678

Transaction ID: 12345678

Component ID: RBG_Component1

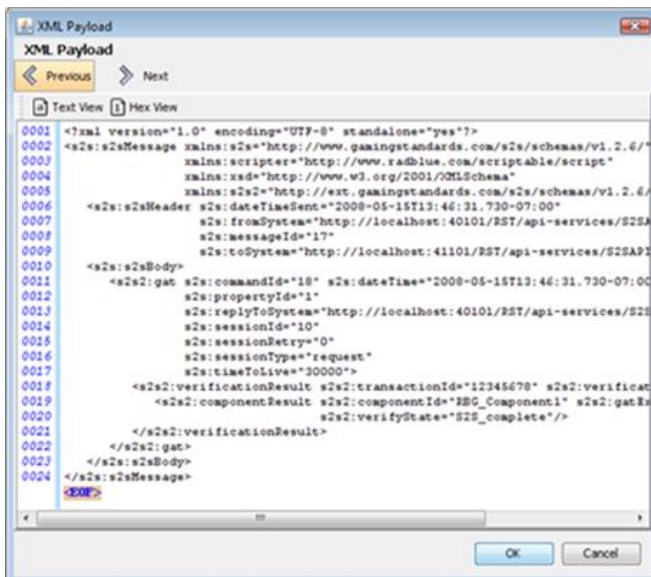
Verify State: ☒ Complete ☐ Queued ☐ In Progress
☐ Error ☐ Passed ☐ Failed

GAT Exec:

Verify Result:

Send Command Cancel

- **Verification ID**, **Transaction ID**, and **Component ID** are automatically completed with the information sent in the **gat.doVerification** or **gat.getVerificationStatus** commands from the S2S Edge server.
 - **Verify State** - Select the state of the specified component.
 - **GAT Exec** - Enter the GAT host procedure used to analyze the verification results.
 - **Verify Result** - Enter the result of the verification request.
2. Click **Send Command**.
 3. From the S2S Edge simulator, select the **Transcript** object, and double-click the **gat.verificationResult** message to view the response. For example:



Change Available Components (S2S Central Host)

You can change the available components returned by the S2S Central Host simulator by modifying the **gat-components.xml** file that is located in the RST directory. Any changes made to the file must comply with the S2S protocol.

1. Navigate to the following folder:
..\radblue\gsa\script\scripts\s2s\1.2.6-igt\host
1. Right-click **gat-components.xml**, and select **Edit**.
2. Modify the component information as needed.
3. **Save** and **Close** the file. File changes take effect the next time the component list is requested.

Sample GAT-COMPONENT.XML File

```
<components>
Component 1

  <component id="RBG_component1" type="G2S_package"
  description="Description" size="12345678">
    <algorithm type="S2S_SHA256" seed="true" salt="false" offsets="true" />
    <algorithm type="S2S_SHA512" seed="true" salt="false" offsets="true" />
Component 2

  </component>
  <component id="RBG_component2" type="G2S_module"
  description="Description" size="12345678">
    <algorithm type="S2S_SHA256" seed="true" salt="false" offsets="true" />
    <algorithm type="S2S_SHA512" seed="true" salt="false" offsets="true" />
Component 3

  </component>
  <component id="RBG_component3" type="G2S_software"
  description="Description" size="12345678">
    <algorithm type="S2S_SHA256" seed="true" salt="false" offsets="true" />
    <algorithm type="S2S_SHA512" seed="true" salt="false" offsets="true" />
  ...
</components>
```


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:

- [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.

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.
- **From Location** - Identifier of entity (for example, EGM or host) that sent 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.
- **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.

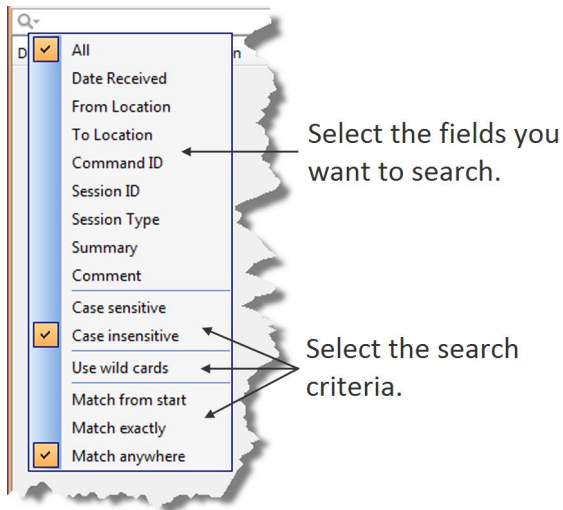
If you right-click on a column header, a menu displays that allows you to automatically resize one or all columns (based on the displayed data in the columns), as well as to indicate which columns you would like to display.

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?

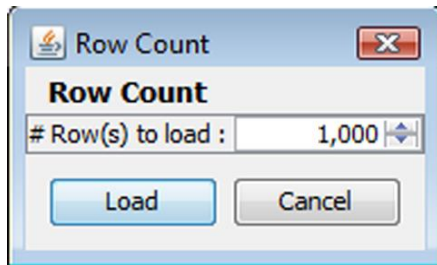
- *Are the correct commands being sent?*
For example, is the `commsOnLine` command being sent during startup?
- *Are messages being acknowledged* (for example, with a `g2sAck` as well as a message acknowledgements?
- *Are there correct request-response pairs?*
For example, if a `communications.getDescriptor` 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**.

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.

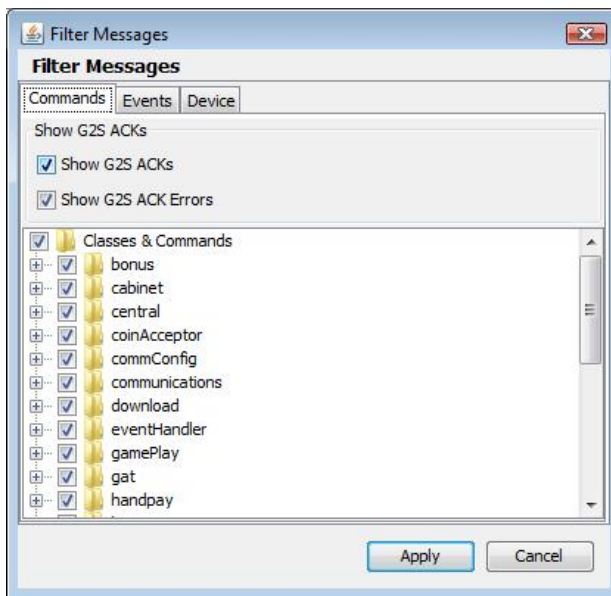
The **Command** tab displays command information in an easy-to-read format along with any meters.

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 **Filters**. The Filter Messages screen displays with three tabs: Commands, Events and Device.

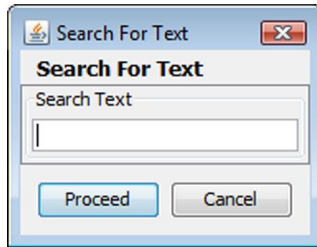


2. On each tab, select the check box of the commands, events and devices you want to display in the Transcript, and clear the check box of the commands, events and devices you want to hide. By default, the `g2sAck` command is cleared (does not display).
3. Click **OK**. Your changes take effect immediately.

Search the Content of Transcript Messages

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

1. Click **Search Content**.



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

View Message Details

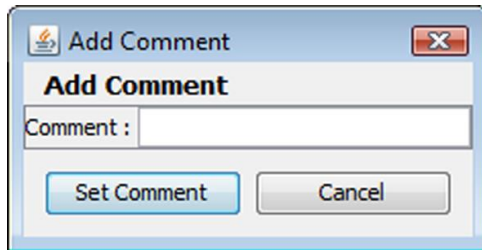
By double-clicking on any row, you can examine the details of the command in that row. The message detail view lets you switch between a text and a hexadecimal view. You can also browse through the transcript list while in detail view.

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.

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.

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.

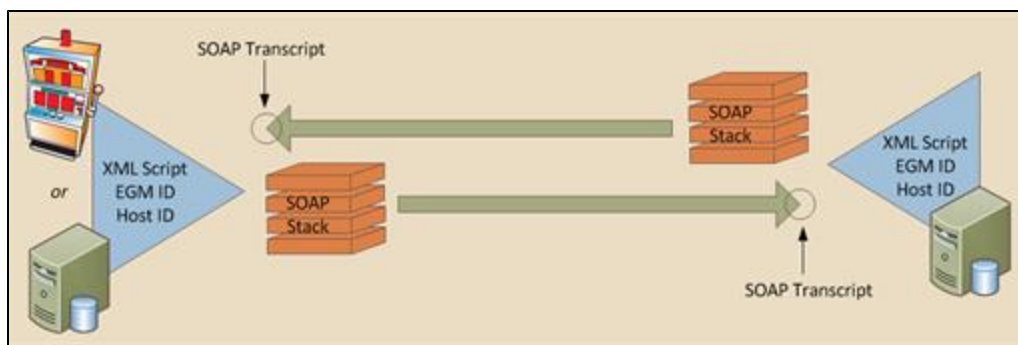
Clear the Transcript Display

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

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

About SOAP Messages

Simple Object Access Protocol (SOAP) is an XML-based protocol for transporting information in a decentralized, distributed environment. A SOAP message consists of a mandatory SOAP envelope, an optional SOAP header, and a mandatory SOAP body. G2S or S2S message content is contained within the body.



SOAP message flow.

- **Envelope** - Top element of the XML document representing the message.
- **Header** - Generic mechanism for adding features to a SOAP message in a decentralized manner without prior agreement between the communicating parties. SOAP defines a few attributes that can be used to indicate who should deal with a feature and whether it is optional or mandatory.
- **Body** - Container for mandatory information intended for the ultimate recipient of the message. SOAP defines one element for the body, which is the Fault element used for reporting errors.

The SOAP Transcript lets you view SOAP-encapsulated messages as they come off the SOAP stack.

Working with the SOAP Transcript

The SOAP Transcript lets you view inbound SOAP-encapsulated messages as they come off the SOAP stack. Here, you can see details of the SOAP wrapper around the messages plus the messages themselves. Primarily, this transcript shows you how the endpoint (for example, an EGM or host) constructed the SOAP around the message. It is used to debug connection issues at startup. SOAP faults display in the SOAP Transcript and are noted in the Summary column as *SOAP Exceptions*.

The SOAP Transcript has several options that allow you to view SOAP information. Use the detail view to see the SOAP wrapper and the message it contains.

At the top of the SOAP Transcript screen are several options:

- **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 SOAP Message](#).
- **Clear Display** - Clears the displayed messages in this instance of the Transcript. See [Clear the SOAP Transcript Display](#).
- **Clear DB** - Clears all records of this type in the database for this instance of the tool. See [Clear the SOAP Transcript Database](#).

The size limit of the SOAP 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](#).

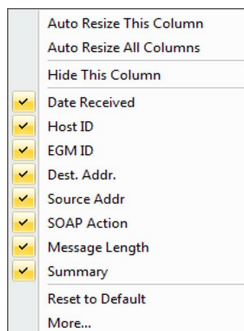
For more information on SOAP messages, see [About SOAP Messages](#).

SOAP Transcript Column Headers

The following columns are available in the SOAP Transcript:

- **Date Received** - Date and time message was received by the tool.
- **Host ID** - Unique identifier of the host.
- **EGM ID** - Unique identifier of the EGM.
- **Dest. Addr.** - Destination Address. URL of the application that the message is sent to.
- **Source Addr** - Source Address. URL of the application that the message was sent from.
- **SOAP Action** - HTTP header value from the SOAP message. If you are having an issue with the SOAP connection, look at the SOAP Action column and verify that the values are consistent with GSA guidelines.
- **Message Length** - Number of bytes in the SOAP message.
- **Summary** - Actual G2S or S2S command within the SOAP 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.

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.



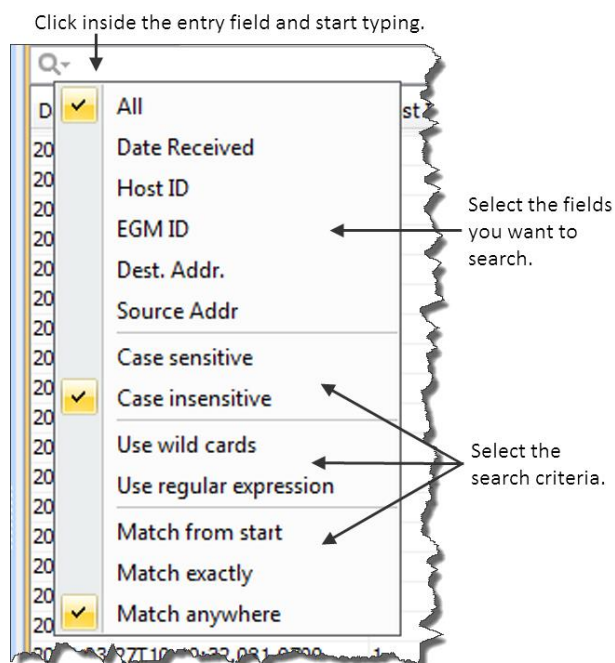
If you right-click on a column header, a menu displays that allows you to automatically resize one or all columns (based on the displayed data in the columns), as well as to indicate which columns you would like to display.

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 SOAP Transcript Messages Using the Quick Filter

Just below the SOAP 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 SOAP Transcript?

The SOAP Transcript lets you view SOAP-encapsulated messages, as they come off the SOAP stack. Primarily, this transcript shows you how the EGM, Central server or Edge server constructs the SOAP around the message. Use the detail view to see the SOAP wrapper and the message it contains.

View the Content of a SOAP Message

By double-clicking on any row, you can examine the details of the SOAP message. The SOAP message detail view lets you switch between a text view of the SOAP wrapper, a hexadecimal view of the SOAP

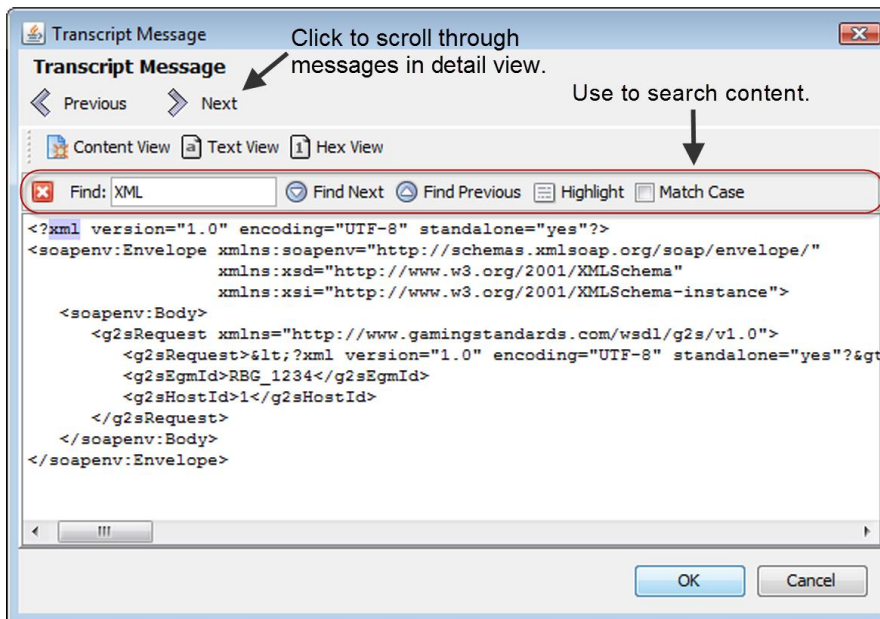
wrapper and the message's XML content. You can also browse through the SOAP transcript list while in detail view.

The Find option lets you search for text strings and keywords within the message. Simply click in the Find text box and start typing. The tool instantly jumps to the first match of the entered string. This feature becomes very handy when you want to find data in large XML messages.

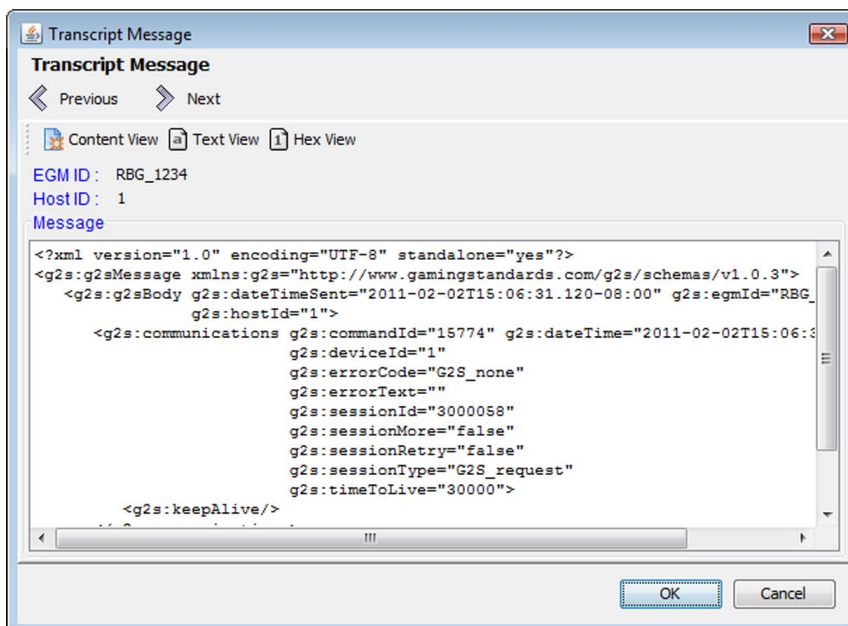
- Use **Find Next** and **Find Previous** to move to the next or previous match of the entered string.
- Click **Highlight** to highlight all instances of the text string or keyword in the message.
- Select **Match Case** if you want to find only a text string or keyword with a specific case (capital or lower case letters).

To view the content of a SOAP message:

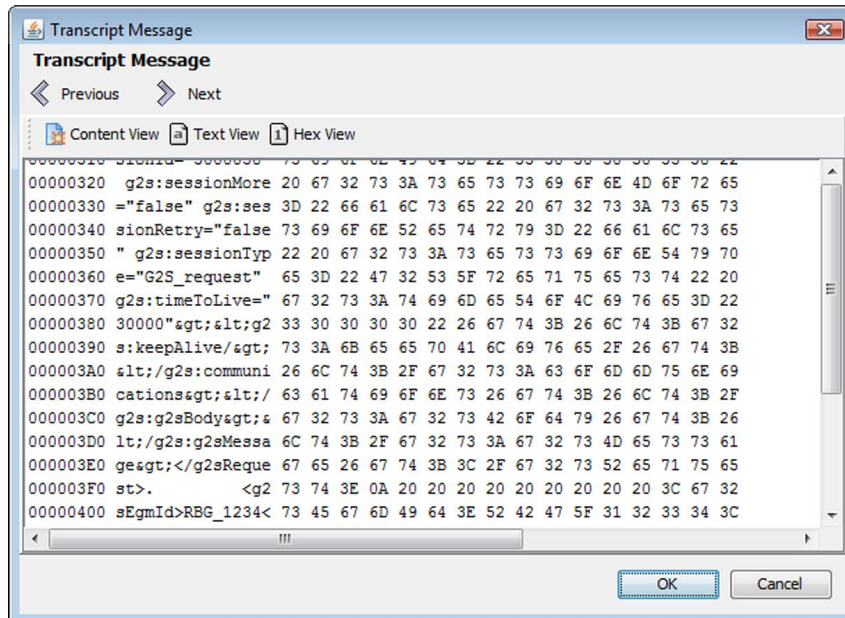
1. Double-click the message you want to view.
2. Click **Text View** to see the SOAP message details as text.



3. Click **Content View** to view the message content.



4. Click **Hex View** to see the SOAP message details as hexadecimal.



5. Click **OK** to return to the SOAP Transcript. Click **Previous** and **Next** to navigate through the SOAP transcript list while in message detail view.
6. Click **OK** to return to the SOAP transcript.

Search the Content of a SOAP Message

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

1. Type the information you want to search on.



2. Click **Proceed**, or click **Cancel** to return to the SOAP Transcript. A pop-up window displays all messages containing the text you entered.

Date Received	SOAP Type	Dest. Addr.	Source Addr.	Message Length
2009-08-06T20:14:28.9...	Request	127.0.0.1:31301	127.0.0.1:50327	14065
2009-08-06T20:14:32.5...	Request	127.0.0.1:31301	127.0.0.1:50327	9690
2009-08-06T20:14:34.3...	Request	127.0.0.1:31301	127.0.0.1:50327	57568
2009-08-06T20:14:38.7...	Request	127.0.0.1:31301	127.0.0.1:50327	37130
2009-08-06T20:14:39.0...	Request	127.0.0.1:31301	127.0.0.1:50327	1799
2009-08-06T20:14:40.3...	Request	127.0.0.1:31301	127.0.0.1:50327	185783
2009-08-06T20:14:42.4...	Request	127.0.0.1:31301	127.0.0.1:50327	1002
2009-08-06T20:14:42.4...	Request	127.0.0.1:31301	127.0.0.1:50327	1046
2009-08-06T20:14:42.4...	Request	127.0.0.1:31301	127.0.0.1:50327	1884
2009-08-06T20:14:42.5...	Request	127.0.0.1:31301	127.0.0.1:50327	1118
2009-08-06T20:14:42.6...	Request	127.0.0.1:31301	127.0.0.1:50327	1118
2009-08-06T20:14:43.2...	Request	127.0.0.1:31301	127.0.0.1:50327	37130
2009-08-06T20:14:47.6...	Request	127.0.0.1:31301	127.0.0.1:50327	1113
2009-08-06T20:24:47.7...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T20:34:47.8...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T20:44:47.9...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T20:54:48.1...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:04:48.3...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:14:48.4...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:24:48.6...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:34:48.7...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:44:48.9...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:54:49.0...	Request	127.0.0.1:31301	127.0.0.1:50327	1124
2009-08-06T11:54:49.1...	Request	127.0.0.1:31301	127.0.0.1:50327	1124

3. Click any message to display the SOAP envelope along with the XML message text.
4. Click **Back** to return to the SOAP Transcript.

Clear the SOAP Transcript Display

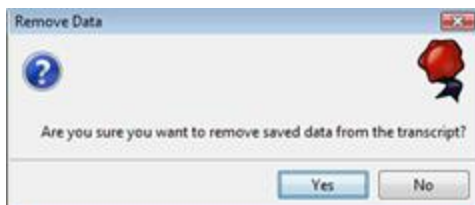
The Clear Display option lets you clear all messages from the SOAP transcript. This option does not remove messages from the SOAP Transcript database.

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

Clear the SOAP Transcript Database

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

1. Click **Clear DB**.



2. Click **Yes** to remove all data from the SOAP Transcript database, or click **No** to return to the Transcript without clearing the database.

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 type="checkbox"/> meters@commandId	matched	2008-07-21T09:01:03.797-07:00	
<input type="checkbox"/> meters@dateTime	matched	2008-07-21T09:01:03.797-07:00	
<input type="checkbox"/> meters@deviceId	matched	2008-07-21T09:01:03.797-07:00	
<input type="checkbox"/> meters@errorCode	matched	2008-07-21T09:01:03.844-07:00	
<input type="checkbox"/> meters@errorText	matched	2008-07-21T09:01:03.782-07:00	
<input type="checkbox"/> meters@sessionId	matched	2008-07-21T09:01:03.797-07:00	
<input type="checkbox"/> meters@sessionMore	matched	2008-07-21T09:01:03.782-07:00	
<input type="checkbox"/> meters@sessionRetry	matched	2008-07-21T09:01:03.797-07:00	
<input type="checkbox"/> meters@sessionType	matched	2008-07-21T09:01:03.797-07:00	
<input type="checkbox"/> meters@timeToLive	matched	2008-07-21T09:01:03.782-07:00	
<input type="checkbox"/> meters.clearMeterSub@meterSubType	no match		
<input type="checkbox"/> meters.getMeterSub@meterSubType	no match		
<input type="checkbox"/> meters.meterInfo@meterDateTime	no match		
<input type="checkbox"/> meters.meterInfo@meterInfoType	no match		
<input 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 type="checkbox"/> meters.meterSubList@periodicBase	matched	2008-07-21T09:01:03.829-07:00	
<input type="checkbox"/> meters.meterSubList@periodicInterval	matched	2008-07-21T09:01:03.813-07:00	
<input type="checkbox"/> meters.setMeterSub@eodBase	matched	2008-07-21T09:01:03.657-07:00	
<input type="checkbox"/> meters.setMeterSub@meterSubType	matched	2008-07-21T09:01:03.719-07:00	
<input type="checkbox"/> meters.setMeterSub@periodicBase	matched	2008-07-21T09:01:03.719-07:00	
<input 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.

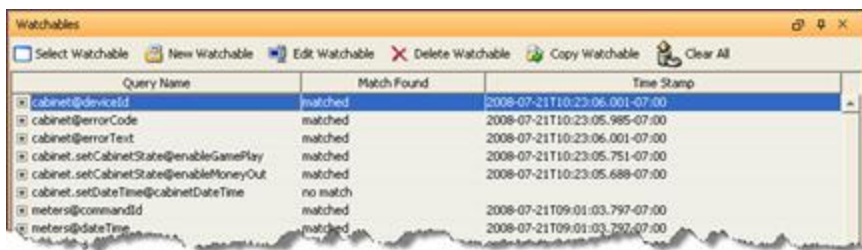
1. Click **New Watchable**.



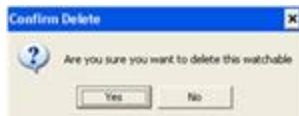
2. Type the **Name** of the new Watchable.
3. Click the drop-down arrow, and select a **Name Space** for the new Watchable. The namespace provides context for the query.
4. Type the XPath query in the **XPath Expression** text box.
5. Click **Save** to make the newly created Watchable available in the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

Delete a Watchable

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



2. Click **Delete Watchable**.

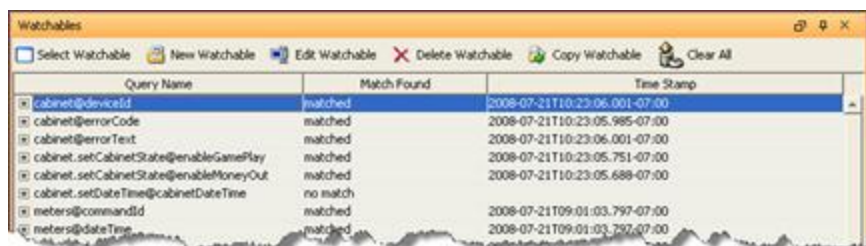


3. Click **Yes** to delete the selected XPath query.

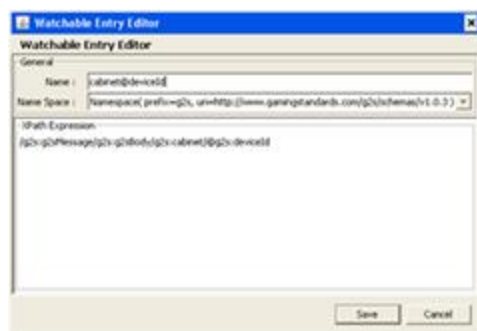
Edit a Watchable

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**.

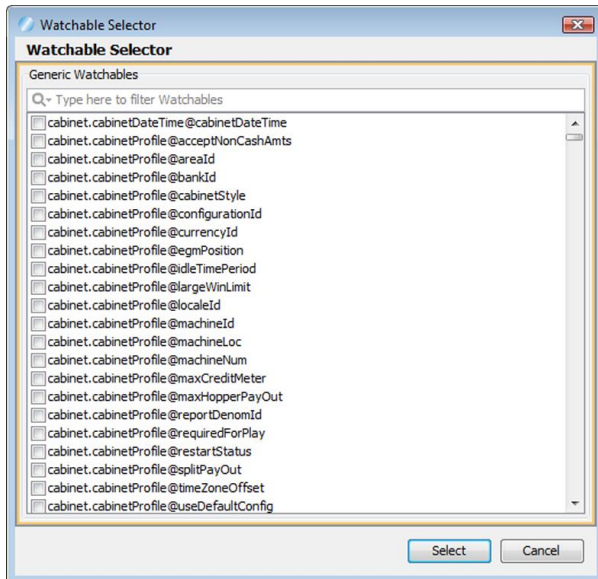


3. Modify the selected Watchable as needed.
4. Click **Save**.

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](#).

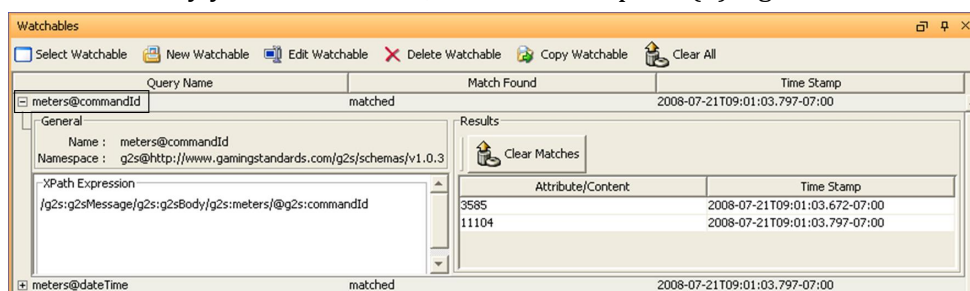
View a Watchable

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.

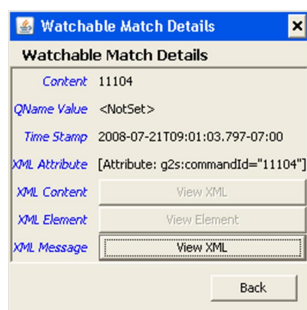


General

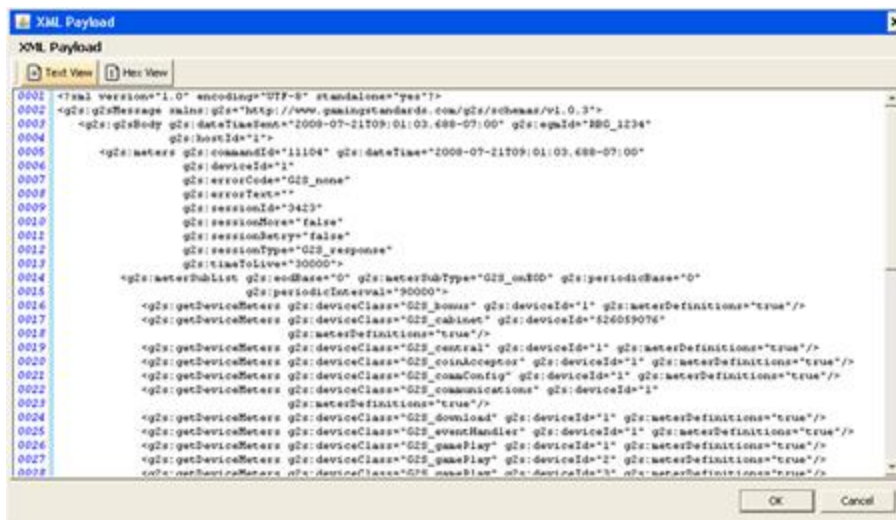
- **Name** - Watchable designation.
- **Namespace** - Namespace that was used in the XPath expression.
- **XPath Expression** - XPath query that the attribute or message content is matched to.

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 Log 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 Log Messages

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

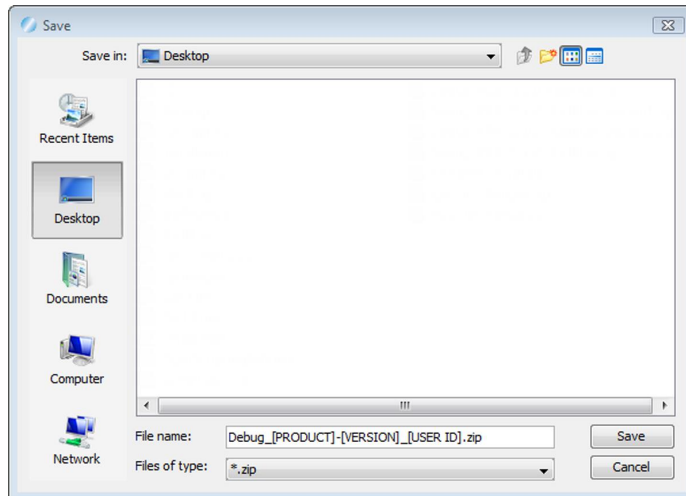
To filter Debug Console messages:

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. Attached 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.

Configure 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.

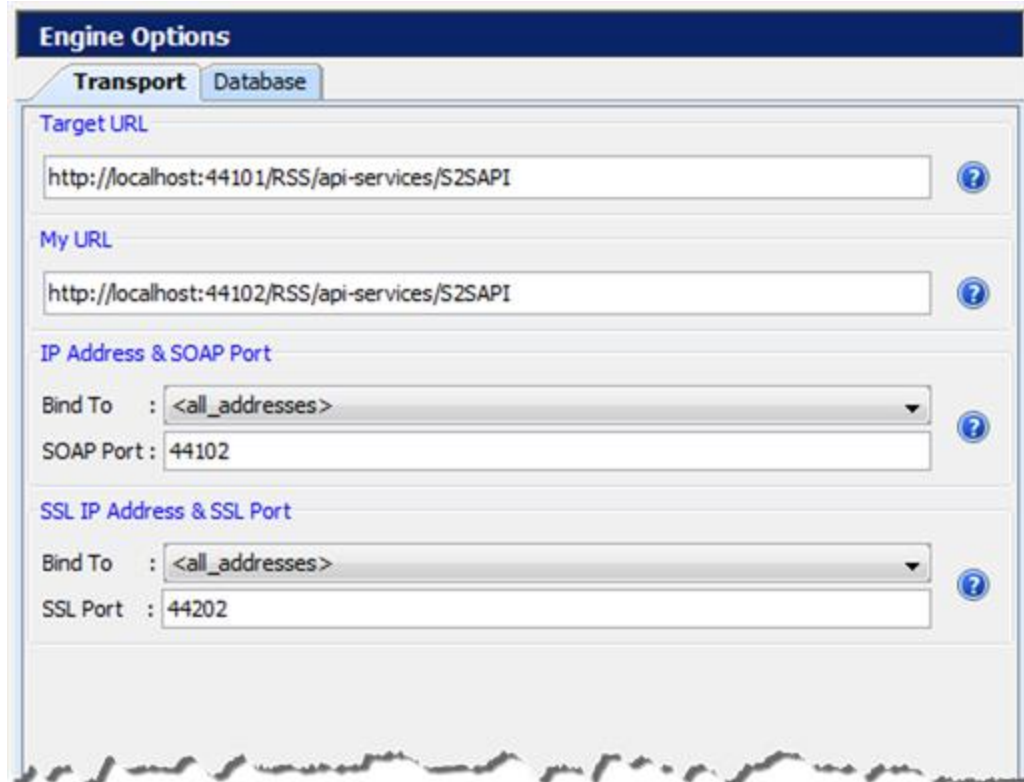
Transcript and Log Messages Displayed

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 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 RSS Engine Options

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



The screenshot shows 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 two tabs: 'Transport' (active) and 'Database'. The 'Transport' tab contains several sections with input fields and dropdown menus, each accompanied by a help icon (a blue circle with a white question mark). The sections are: 'Target URL' with a text field containing 'http://localhost:44101/RSS/api-services/S2SAPI'; 'My URL' with a text field containing 'http://localhost:44102/RSS/api-services/S2SAPI'; 'IP Address & SOAP Port' with a 'Bind To' dropdown menu set to '<all_addresses>' and a 'SOAP Port' text field containing '44102'; and 'SSL IP Address & SSL Port' with a 'Bind To' dropdown menu set to '<all_addresses>' and an 'SSL Port' text field containing '44202'.

RSS Engine Options screen.

Database

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

- **Clear Transcript Messages on Startup** - Select this option to clear the transcript database each time RSS is launched.
- **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.

Transport

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

- **Bind To** - Click the drop-down arrow, and select the IP Address that you want RSS to use for communications.
- **My URL** - Enter the network location of the RSS (Edge or Central) that you are using.
- **SOAP Port** - Enter the port that you want RSS 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 RSS to use for SSL-enabled communications.
- **Target URL** - Enter the network location of the target entity (where you are sending commands).

Configuring Namespace Options

Namespace Options provides you with a list of valid schemas, based on your license, that the application validates against. You can also add or remove custom schemas as needed.

Add a Namespace

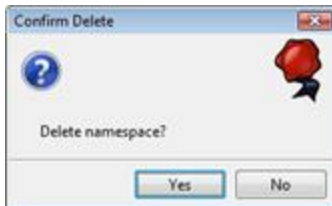
Use the Add Namespace option to add custom schemas to the list of valid schemas.

1. Click **Add Namespace**.
2. Enter the GSA protocol type (**S2S** or **G2S**) in the Namespace Prefix box.
3. Enter the location of the new schema in the Namespace URI box.
4. Click **Save**.
5. Click **Apply** on the main Configuration screen.

Remove a Namespace

Use the Remove Namespace option to remove custom schemas from the list of valid schemas.

1. Highlight the namespace you want to delete.
2. Click **Remove Namespace**.



3. Click **Yes** to remove the selected namespace from the list.
4. Click **Apply** on the main Configuration screen.

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:

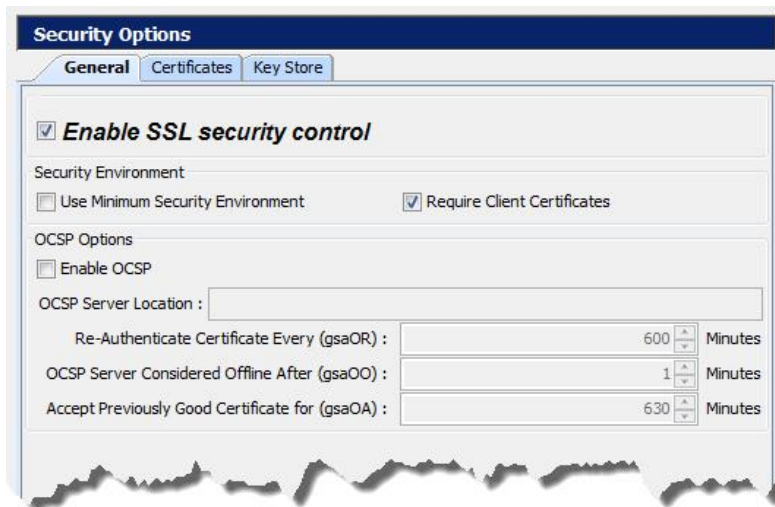
- *Signed by trusted certificate authority?*
- *Is current time/date within the period of validity (effective and expired date)?*
- *Is issuer signature correct?*

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.

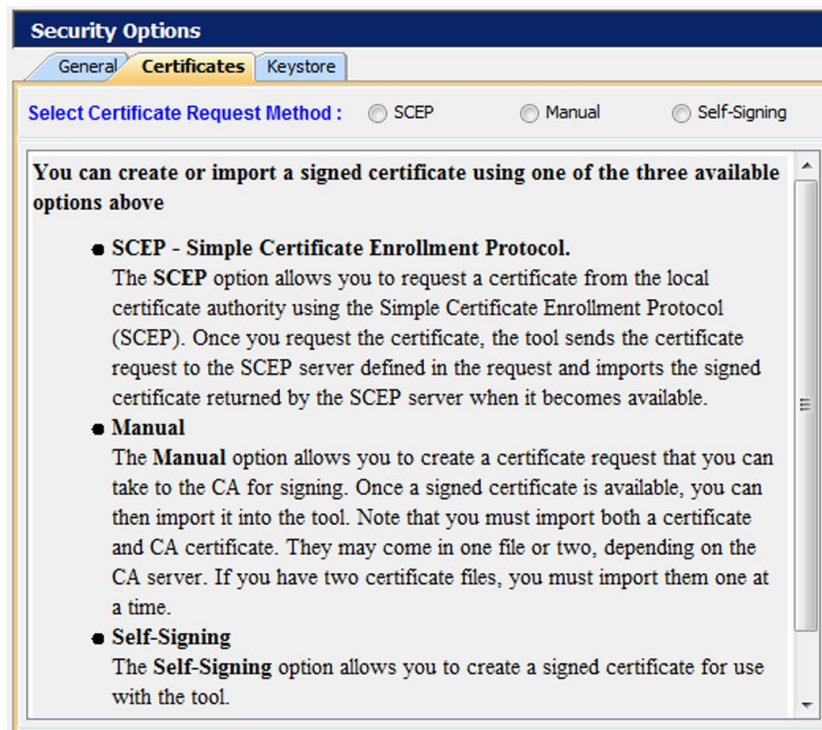
When you enable OCSP, you must configure the following options:

- **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.

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.

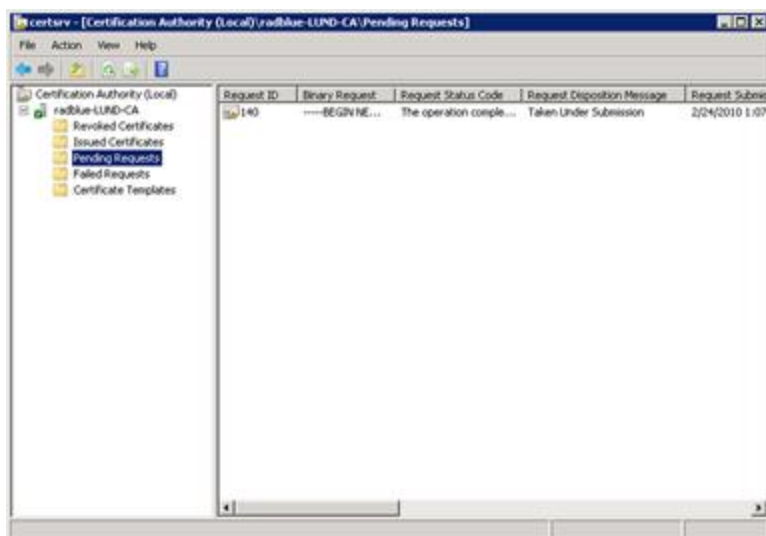
1. From **Tools > Configure > Security Options**.
2. Click **Certificates**.
3. Select **SCEP** as the **Certificate Request Method**.
4. Configure SCEP options as required. The values related to the certificate authority (CA) are available from the CA provider.
 - **SCEP Server Location** - Type the 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**.
 - **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.

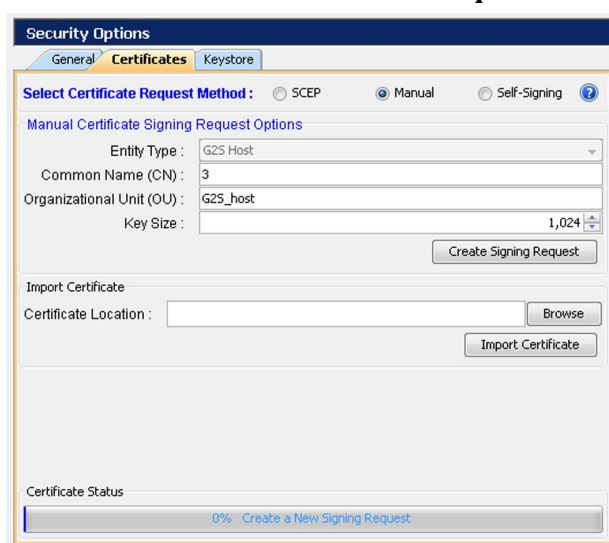
Once the certificate is signed, the RadBlue tool imports it the next time a poll is performed.

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.

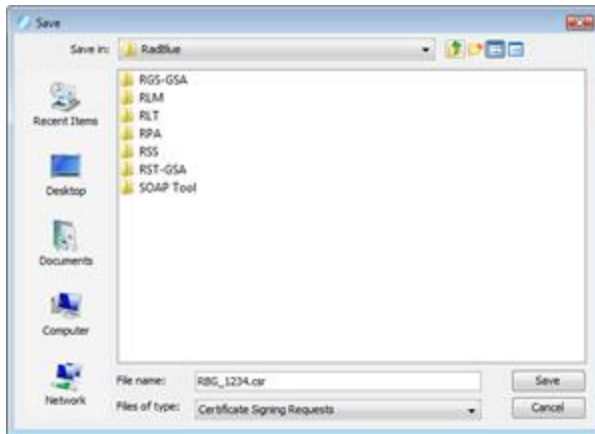
1. From **Tools > Configure > Security Options**.
2. Click **Certificates**.
3. Select **Manual** as the **Certificate Request Method**.



The screenshot shows the 'Security Options' dialog box with the 'Certificates' tab selected. Under 'Select Certificate Request Method', the 'Manual' radio button 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). There is a 'Create Signing Request' button. Below this is the 'Import Certificate' section with a 'Certificate Location' field, a 'Browse' button, and an 'Import Certificate' button. At the bottom, a 'Certificate Status' bar shows '0%' and a link to '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**.



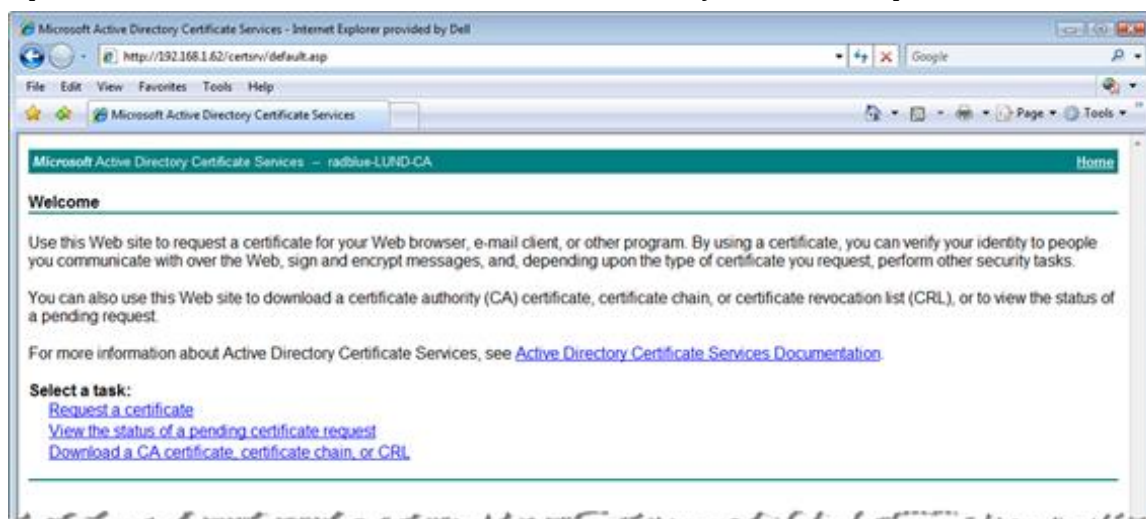
6. Click **OK**.
Notice that the Certificate Status is updated.
7. Depending on the certificate authority you are using, you must now use the certificate request you created to obtain a signed certificate from a certificate authority. For an example of how to obtain a signed certificate from Microsoft 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

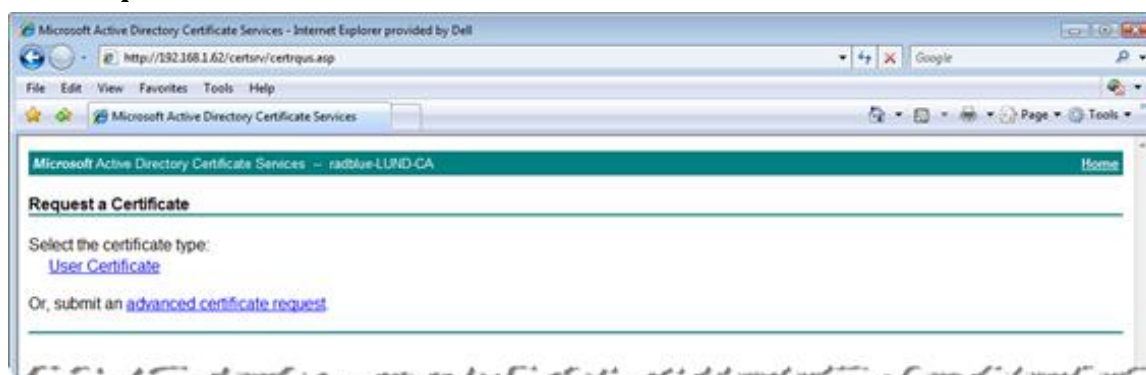
The following procedure is intended to provide an understanding of the process you may go through to create a signed certificate. Microsoft Active Directory Certificate Services is only one of many certificate authority programs. Your individual process may vary greatly depending on the certificate authority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

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

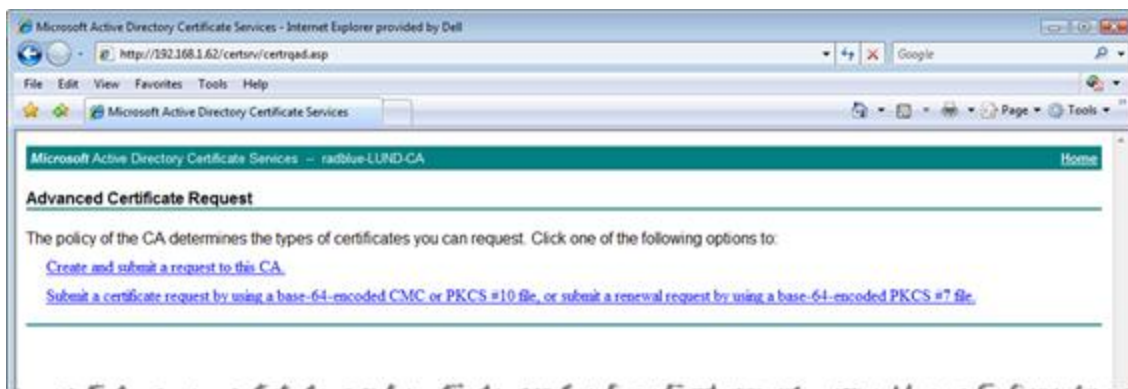
1. Open the certificate request file in Notepad or Wordpad, and click anywhere inside the content.
2. Perform a **CTRL+a** to highlight all content and a **CTRL+c** to copy the content.
3. Open an Internet browser, enter the certificate authority location, and press **Enter**.



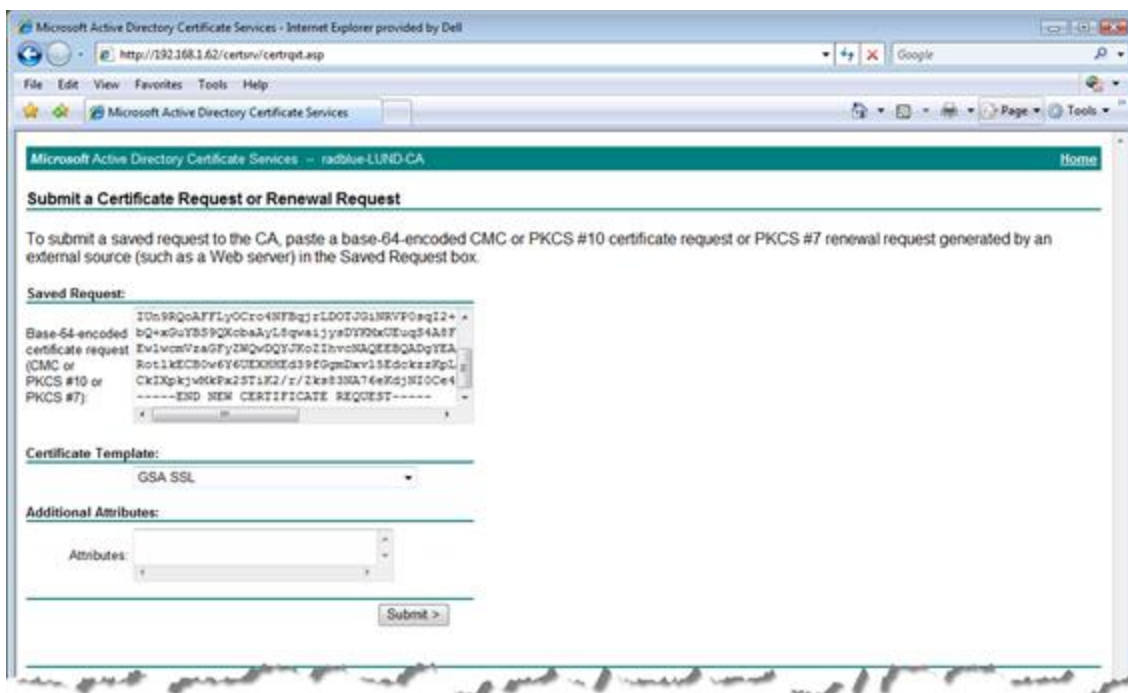
4. Click **Request a certificate**.



5. Click **advanced certificate request**.



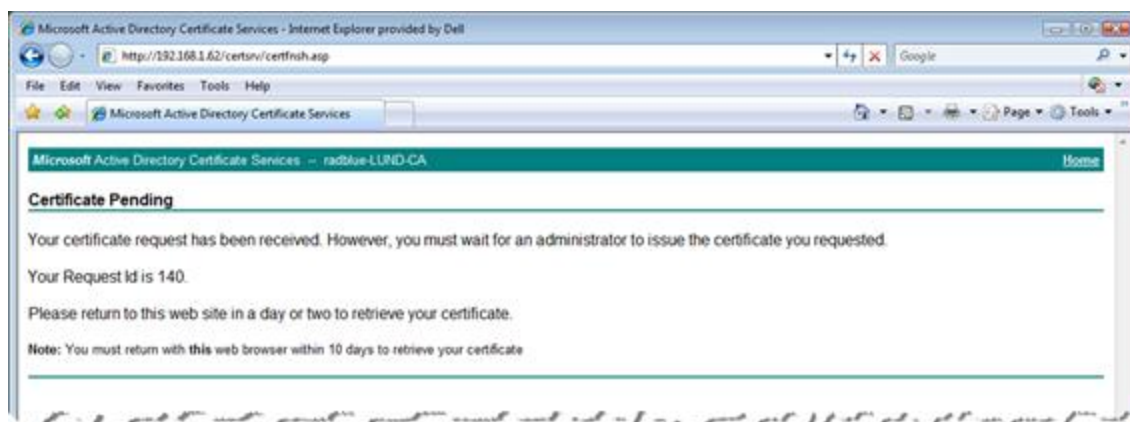
6. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-54-encoded PKC #7 file**.



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**.

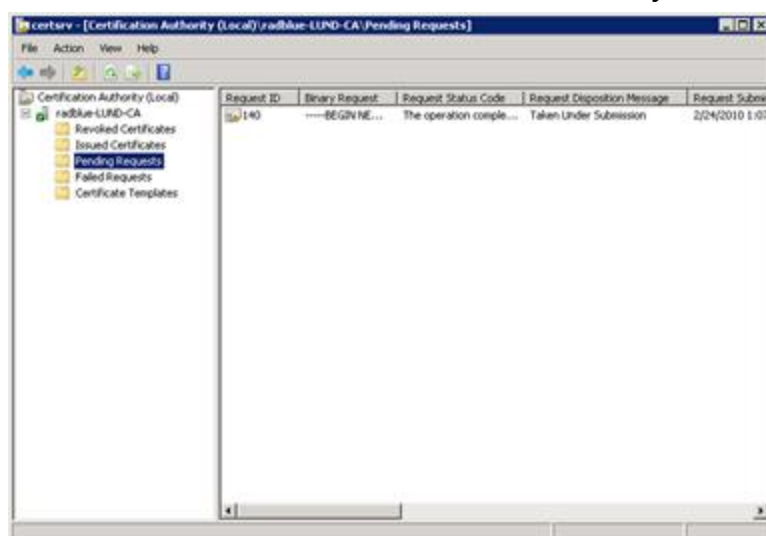
9. Click **Submit**.



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**.

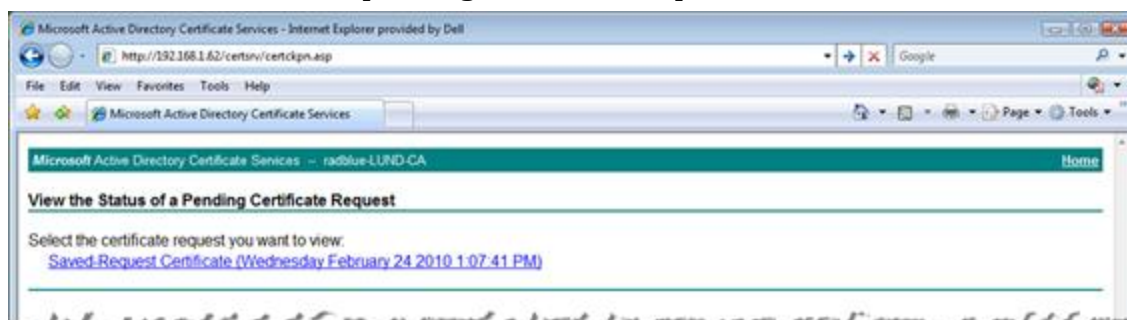
14. Click to highlight **Request ID 140**.

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

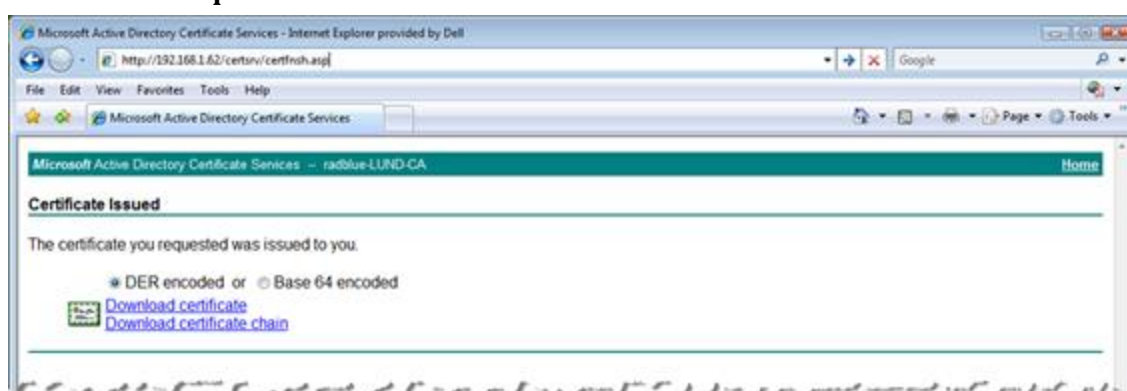
16. Maximize the browser window.

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.

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. The 'Select Certificate Request Method' section has three radio buttons: 'SCEP', 'Manual', and 'Self-Signing', with 'Self-Signing' being the selected option. Below this, the 'Self-Signed Certificate Options' section contains a checkbox for 'Approve all certificates' which is checked. The 'Create Self-Signed Certificate' section has four fields: 'Entity Type' (a dropdown menu showing 'G2S EGM'), 'Common Name (CN)' (a text box with '1'), 'Organizational Unit (OU)' (a text box with 'G2S_host'), and 'Key Size' (a dropdown menu showing '1,024'). A 'Create Self-Signed Certificate' button is located at the bottom right of this section. At the very bottom of the dialog, there is a 'Certificate Status' bar showing '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.

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.

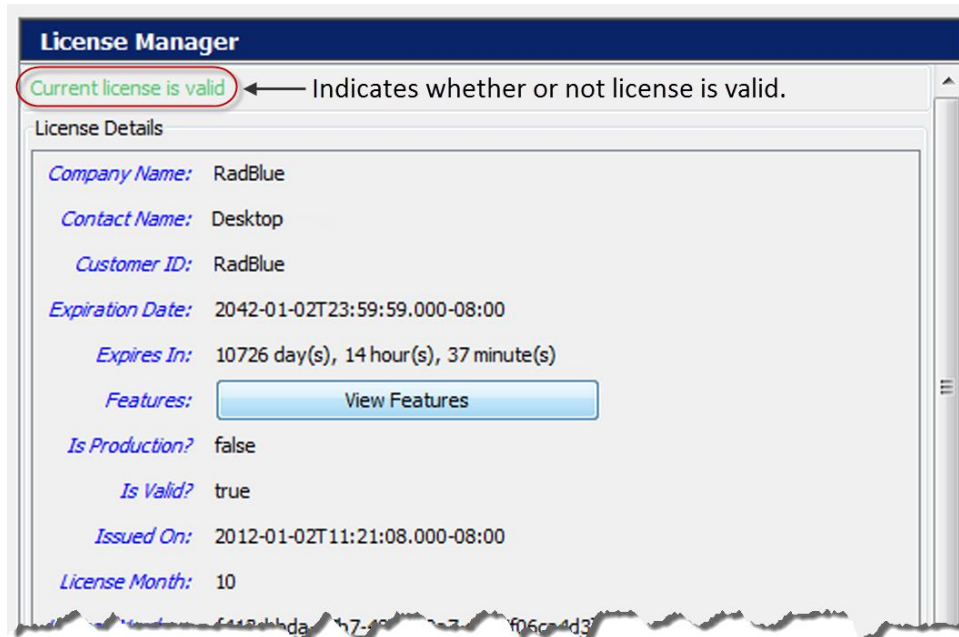
To import a PKCS #12 file:

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 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.

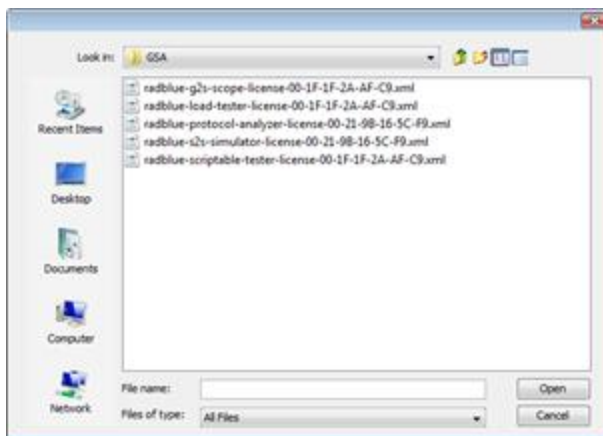
- **Location ID** - Location of purchasing organization.
- **MAC Address** - Physical address of computer on which the tool is installed.
- **Product Line Key** - Unique identifier of installed tool.
- **Product Name** - Name of licensed RadBlue product.

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

accountingMeter 16

additonal resources 17

C

central host server 25

client keystore 92

client.jks 92

communications 16

comp 16

configuration 16

 desktop 75

 engine 76

 keystore 92

 license 94

 namespace 78

 security 91

custom command

 load 32

 reload xml file 34

D

debug log

 about 71

 clear 72

 filter 72

 getting support 73

 unresolved errors 73

default alias 92

desktop options 75

E

edge server 23

engine options 76

eventFilter 16

F

fillCredit 16

financialTransaction 16

G

gat 16

getting support 73

H

handpay 16

I

infoUpdate 16

installation

 windows operating system 11

interface 18

J

jackpot 16

K

keystore

client 92

default alias 92

remove certificate 92

trusted 92

view certificate 92

keystore options 92

L

license manager 94

load new license 95

load new license 95

M

marker 16

message transcript

about 41

add comment 49

clear display 50

column description 42

compare messages 45

load messages 44

search message content 47

view message details 48

what are you looking for? 43

Microsoft active directory certificate
services 87

N

namespace option

about 78

add 78

remove 78

O

ocsp 81

openClose 16

options

desktop 75

engine 76

license 94

namespace 78

security 91

P

patron 16

pkcs #12 file 92

player 16

playerRating 16

protocol version 26

R

registerClient 16

release notes 17

reload xml file 34

rss

central host server 25

create xml file 28

edge server 23

edit xml file 28

install 11

interface 18

load custom command 32

send raw xml 34

S

s2s

change protocol version 26

supported classes 16

scep 83

security options

about 91

enable ocsp 81

load a third-party certificate 85

load self-signing certificate 91

Microsoft active directory certificate
services 87

scep 83

send raw xml 34

soap transcript

about 52

about soap messages 51

clear database 59

clear display 59

column descriptions 53

filter messages 54

search message content 58

view message content 54

what are you looking for? 54

support 73

supported s2s classes 16

T

transcript

add comment 49

transcript, message

about 41, 52

add comment 49

clear display 50

column descriptions 42

compare messages 45

load messages 44

search message content 47

view message details 48

what are you looking for? 43

transcript, soap

about soap messages 51

clear database 59
clear display 59
column descriptions 53
filter messages 54
search message content 58
view message content 54
what are you looking for? 54
troubleshooting 71
trusted keystore 92
trusted.jks 92

V

voucher 16

W

wat 16
watchables
 about 61
 about xpath expressions 62
 boolean expression usage 63
 clear all data 63
 copy 64
 create 65
 delete 65
 edit 66
 sample xpath expressions 62
 select attributes 67

view 68
xpath expression format 62
xpath references 62

X

xml file 28, 32
xpath expressions
 about 62
 boolean expression usage 63
 format 62
 references 62
 sample 62