RapidResponse Administration Guide

1904

kinaxis®
RapidResponse®

All Specifications, claims, features, representations, and/or comparisons provided are correct to the best of our knowledge as of the date of publication, but are subject to change without notice. While we will always strive to ensure our documentation is accurate and complete, this document may also contain errors and omissions of which we are not aware.

THIS INFORMATION IS PROVIDED BY KINAXIS ON AN "AS IS" BASIS, WITHOUT ANY OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABLE QUALITY, SATISFACTORY QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THOSE ARISING BY LAW, STATUTE, USAGE OF TRADE, COURSE OF DEALING OR OTHERWISE. YOU ASSUME THE ENTIRE RISK AS TO THE RESULTS OF THE INFORMATION PROVIDED. WE SHALL HAVE NO LIABILITY TO YOU OR ANY OTHER PERSON OR ENTITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR PROFIT, LOST OR DAMAGED DATA OR OTHER COMMERCIAL OR ECONOMIC LOSS, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR THEY ARE FORESEEABLE. WE ARE ALSO NOT RESPONSIBLE FOR CLAIMS BY A THIRD PARTY. OUR MAXIMUM AGGREGATE LIABILITY TO YOU AND THAT OF OUR DEALERS AND SUPPLIERS SHALL NOT EXCEED THE COSTS PAID BY YOU TO PURCHASE THIS DOCUMENT. SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. All product, font and company names are trademarks or registered trademarks of their respective owners, and use of them does not imply any affiliation with or endorsement by them.

Copyright © 2009-2019 Kinaxis Inc. All rights reserved. This document may not be reproduced or transmitted in any form (whether now known or hereinafter discovered or developed), in whole or in part, without the express prior written consent of Kinaxis.

Kinaxis RapidResponse contains technology which is protected under US Patents #7,610,212, #7,698,348, #7,945,466, #8,015,044, #9,292,573, and #9,710,501 by the United States Patent and Trademark Office. It is also protected under the Japan Patent Office, Japanese patent #4393993 and the Intellectual Property India Office, patents #255768 and #279101. Other patents are pending.

This document may include examples of fictitious companies, products, Web addresses, email addresses, and people. No association with any real company, product, Web address, email address, and person is intended or should be inferred.

RapidResponse Administration Guide E76450-20162

Date of Publication: Monday, August 19, 2019

Printed in Canada.

Support: support@kinaxis.com

Web site: http://www.kinaxis.com

Contents

Part 1: Overview **13**

CHAPTER 1: Welcome **15**
On-Premises versus On-Demand 15
CHAPTER 2: About Kinaxis **19**
Customer Support 19
CHAPTER 3: Accessing help and documentation **21**
Determining which help system or guide to use 22
Documentation conventions 24
Finding the content you need in HTML help 24
Your feedback 25
Help embedded in resources 25
Other ways to learn about RapidResponse 31
CHAPTER 4: RapidResponse administration roles **33**
Administration overview 33
Master Administrator user account for On-Premises 34
System administrator responsibilities 34
User administrator responsibilities 35
Data administrator responsibilities 36
Permission to modify data integration settings 36
Administration pane permissions 37
Determining administrator permissions 41
Assigning administrator permissions 41
Configuring administrator permissions 43
Test systems for the On-Demand service 43
CHAPTER 5: Security and infrastructure **45**
User security 45
System auditing 51
On-Demand service infrastructure 51
Data security in the On-Demand service 54
Systems used by the On-Demand service 55
On-Demand service security policies and information 57
On-Demand service operational policies 60
CHAPTER 6: International character set support **65**
CHAPTER 7: New and changed in RapidResponse **67**
2019 administration changes 67
2018 administration changes 73

2017 administration changes 82
2016 administration changes 86
CHAPTER 8: Configuration changes managed by Kinaxis for On-Demand 95
RapidResponse system settings 95
RapidResponse interface customization 96
RapidResponse data settings 96
Email server settings 96

Part 2: Installation for On-Premises 97

CHAPTER 9: RapidResponse installation overview 99
RapidResponse application components 99
Data configuration 100
RapidResponse installation process 101
Overview of complete installation 102
System requirements for RapidResponse 104
CHAPTER 10: Installing RapidResponse Server 109
Preparing to install RapidResponse Server 109
Installing RapidResponse Server 111
Uninstalling RapidResponse Server 112
CHAPTER 11: Installing RapidResponse Application Server 113
Preparing to install RapidResponse Application Server 114
Installing RapidResponse Application Server 118
RapidResponse Application Server post-installation procedures 120
Testing the RapidResponse installation 122
Importing license keys 124
RapidResponse Application Server folder structure 124
Providing external access to RapidResponse 125
Uninstalling RapidResponse Application Server 127
CHAPTER 12: Installing RapidResponse applications 129
Preparing to install RapidResponse applications 130
Installing RapidResponse applications 130
Installing Capacity Planning (CRP) 131
Uninstalling Capacity Planning (CRP) 132
Capacity Planning (CRP) components 133
Installing Engineering Change Manager 133
Uninstalling Engineering Change Manager 134
Engineering Change Manager components 135
CHAPTER 13: Initial configuration steps 137

Part 3: Upgrading RapidResponse 139

CHAPTER 14: RapidResponse upgrade process overview 141
Learning more about new and changed features 141
Data model calculations after upgrading 142
Preparing to upgrade (On-Premises) 143
RapidResponse upgrade steps (On-Premises) 150
Upgrading RapidResponse with Service Updates 152
Post-update considerations 154
Post-upgrade considerations 155

Data model settings and log files 156
Query Language syntax and compatibility levels 156
Running DataIntegrityCheck after upgrading 160
Dashboard upgrade from RapidResponse 11.0 161
Web server URL configuration 162
Configuration file for Application Server 162
XML deprecation in workbook properties 163
Replacing chained alerts and scheduled tasks 165
Macros 168
Changes to perspectives 169
Record identification fields 169
Non-unique scenario names 170
Replacing optional keys with key fields 174
Specifying whether key reference fields are modifiable 175
CHAPTER 15: Upgrading RapidResponse Server 177
Requirements 178
Migrating from Intel Itanium servers 178
Migrating from Windows Server 2003/2008 servers 179
Stopping RapidResponse services 180
Upgrading RapidResponse Server 181
Upgrading application components 184
Upgrading the RapidResponse ServiceHost service 185
Reviewing the upgrade log files 185
Setting up the RapidResponse Server service 186
CHAPTER 16: Upgrading RapidResponse Application Server 189
Preparing to upgrade Application Server 189
Upgrading RapidResponse Application Server 190
Recovering files in case of upgrade failure 193
Reviewing the upgrade log files 193
Testing the Application Server upgrade 194
CHAPTER 17: Upgrading RapidResponse applications 195
Upgrading applications 195
Predefined resource changes during upgrade 196
Post-upgrade considerations (On-Premises) 198
Upgrading application resources (On-Premises) 198
Upgrading applications through Service Updates 200
Applying Service Updates 201
CHAPTER 18: Converting standard tables to vector data 203
Analyzing vector data for key uniqueness 205
Analyzing resources and data for vector upgrade issues 207
Analyzing vector data for currency issues 210
Analyzing vector data for record header issues 213
Converting tables to contain vector data 214
Vector data considerations after upgrading 214
Analyzing vector data origin issues 215
CHAPTER 19: Upgrading RapidResponse OpenAPI applications 217
How to upgrade OpenAPI 217
CHAPTER 20: Preparing to transition away from RapidResponse OpenAPI 219
Support for OpenAPI to be discontinued 219

System requirements for OpenAPI logging 220
Installing the OpenAPI Service Update for new logging capability 220
Enabling OpenAPI detailed logging 220
Sending log files to Kinaxis 223

Part 4: Server management for On-Premises environments 225

CHAPTER 21: RapidResponse Server management 227
RapidResponse Windows Services 227
RapidResponse Console 235
Authenticating RapidResponse Server 239
Reviewing RapidResponse Server activity 239
Troubleshooting RapidResponse Server 241
Internal errors and system crashes 244
RapidResponse Server folder structure 249
Archiving RapidResponse package files 252
Performance impacts from scans and agents 255
CHAPTER 22: RapidResponse system memory and monitoring 259
Understanding hardware requirements 259
RapidResponse system memory usage 260
Monitoring input data growth 263
Calculations and system memory 265
Query monitoring and management tools 267
Scenario memory consumption 270
Monitoring CPU usage 271
CHAPTER 23: RapidResponse Server settings 273
Importing license keys 273
Site licensing 274
Configuring email support 276
Automatic deletion of system records 277
RapidResponse locale settings 281
RapidResponse and TCP/IP ports 283
Setting the MRPDate calculation 286
Renaming RapidResponse Server 287
CHAPTER 24: RapidResponse Server failover clustering 289
Failover clustering overview 290
Setting up the failover cluster configuration 294
Database folders in a failover cluster 299
Determining which server is active 301
Managing servers in a failover cluster configuration 304
Failover and logging 304
Applying Service Updates and upgrading 305
CHAPTER 25: Monitoring RapidResponse system availability 307
Running the end-to-end test 307
CHAPTER 26: Managing the RapidResponse database 309
RapidResponse database content 309
Location of stored database files 310
Database files and operations 311
Disk space warnings 314
Backing up RapidResponse program files 314

Backing up and restoring the RapidResponse database 315
Rolling back the RapidResponse database 318
Archiving the RapidResponse database files 324
RapidResponse database integrity 327
CHAPTER 27: Data persistence 329
Automatic data persistence 330
Defining data persistence rules for a scenario 330
Logging of persistence operations 333
CHAPTER 28: Automatic RapidResponse Server operations 335
Automatic server operations with webplnSC 335
Automatic server operations with ServerCommand 339
CHAPTER 29: Server exit applications 343
Overview of server exits 343
Server exits for server operations 344
Environment variables 344
Registering server exits 346
Running server exits and error codes 347
Server exit for scenario operations 349
CHAPTER 30: Registry Settings for RapidResponse Server 351
Location of registry settings 351
CHAPTER 31: Monitoring your environment with the RapidResponse Log Service 367
Log collection architecture 368
Data collected by the Performance Monitor Service 370
System requirements for the RapidResponse Log Service 372
Installing the RapidResponse Log Service 372
Configuring RapidResponse to provide log information 374
Installing and configuring the Performance Monitor Service 375

Part 5: System management for On-Premises and On-Demand environments 379

CHAPTER 32: Commands and scheduling system tasks 381
Predefined scheduled system tasks 381
RapidResponse system commands 384
Capture command 385
Checkpoint command 386
Condense command 387
CreateDataPackage command 388
DataExpiry command 389
DataImport command 390
DataIntegrityCheck command 391
DataSynchronize command 393
DataUpdate command 395
DeleteData command 402
DeleteEnterpriseData command 403
DeleteFiles command 403
ExtractData command 403
ExtractNetChangeData command 404
FilterTT command 406
PruneFiles command 406
Restart command 407

RunAddin command ... 407
ScenarioCommit command ... 408
ScenarioReset command ... 408
ScenarioUpdate command ... 409
Snapshot command ... 409
VersionReclaim command ... 411
VersionReclaimSweep command ... 411
Scheduling RapidResponse commands ... 412
Using commands and scheduled system tasks ... 415
Run-time windows for scheduled system tasks ... 417
Turning off all scheduled system tasks ... 418
Logged messages for scheduled tasks ... 418
CHAPTER 33: Reviewing system status and operation logs ... 421
Message notifications ... 421
System administration logs ... 423
Bulletin board information for users ... 441
Data import and data update logs ... 442
Automation logging ... 448
Text logging for alerts ... 461
RapidResponse text-based log files ... 462
Server.log file ... 464
Heartbeat.log file ... 470
Performance.log file ... 473
QueryHistory.log file ... 474
SecurityAudit.log file ... 477
Viewing log data in the Central Log Collector ... 479
CHAPTER 34: RapidResponse system workbooks reference ... 481
Standard system workbooks ... 482
RapidResponse System Data workbook ... 486

Part 6: User administration ... 491

CHAPTER 35: Best practices for setting up user accounts ... 493
About predefined groups ... 493
Predefined user groups ... 494
CHAPTER 36: Guidelines for group setup and user experiences ... 503
Guidelines for initial custom group setup ... 503
User experiences ... 504
Planning the group structure ... 510
CHAPTER 37: Creating groups ... 513
Creating a group ... 513
Assigning and removing permissions ... 517
Assigning resources ... 529
Assigning scenarios ... 533
Scenario permissions in collaboration ... 535
System groups ... 537
CHAPTER 38: Creating user accounts ... 539
Understanding user accounts and license types ... 539
Types of RapidResponse users ... 541
System requirements for users ... 541

Creating users 548
Adding users to groups 554
Assigning and removing permissions for a user 554
Limiting visibility of user information 556
Specifying default data formats for users 559
Setting profile pictures 560
Automatically opening resources upon sign in 562
CHAPTER 39: Managing groups and users 565
Managing groups 565
Managing users 569
CHAPTER 40: Reviewing resource assignments 575
About the Resource Permissions workbook 575
Understanding access permissions 579
Reviewing resource assignments by group 582
Reviewing resource assignments by user 585
Reviewing resource assignments by resource 587
Example: Investigating a resource assignment 590
CHAPTER 41: User account maintenance and troubleshooting 593
Communicating with users 593
Monitoring sign-in activities 595
Monitoring user and group changes 596
Monitoring user adoption 598
Unlocking a user account 599
Disconnecting users from RapidResponse 601
Resolving RapidResponse error messages 602
Monitoring and canceling problematic queries 603
RapidResponse Application Server Event Log 606
Monitoring RapidResponse connection speed 607

Part 7: RapidResponse client administration 609

CHAPTER 42: Customizing the RapidResponse client 611
Changing the session expiry setting 611
Extending web client sign in durations 612
Customizing help and documentation settings 613
Setting the sign-in notice 614
Displaying profile pictures 617
Customizing the workbook link menu 618
Setting the maximum number of command errors logged 623
Adding custom links 624
Enabling the Reference Part toggle 628
Specifying display names for calendars 629
Adjusting calendars for bucketing 630
Specifying the separator for split orders 631
Configuring column headers 631
Configuring status bar identification text 632
Specifying the AND operator for feature lists 632
Defining integrated project management settings 633
Defining process orchestration settings 634
Configuring responsibility 635

Specifying the annual plan target scenario 636
Specifying whether historical data is editable 637
Configuring add-ins 638
Configuring data origin for record modifications 641
CHAPTER 43: Customizing RapidResponse user settings 643
Configuring printed report settings 643
Setting password security options 648
Setting Message Center options 650
Setting file size limits for importing data 653
Specifying email settings 655
Setting the worksheet record limit 657
Setting the record deletion warning threshold 659
Changing image upload size limits 660
Setting hierarchy limits 660
Options for importing Excel data to scenarios 662
Making data formats available to users and resource authors 663
Turning unsaved workbook changes warning on or off 668
Defining time zones 669
Overriding the Everyday calendar name 671
Configuring settings for automation tasks 671
Specifying file location folders 676
Migrating user groups 677
CHAPTER 44: Creating and managing currencies 683
About currencies 683
Overview of adding or creating a currency 684
Adding standard currencies 684
Currency codes 685
Creating currencies 686
Managing currencies 686
Currency conversions 687
Managing conversion rates 689
CHAPTER 45: Configuring unit conversions 695
Defining units of measure 695
Creating unit categories 700
CHAPTER 46: Scenario management 703
RapidResponse database and scenarios 703
Scenario data changes and memory consumption 704
Updating scenarios 707
Administrator tools for scenario management 708
Committing data to the root scenario 717
Renaming the root scenario 719
Creating scenario hierarchies 719
Scheduling scenario updates 724
Scenario perspectives 725
CHAPTER 47: Managing RapidResponse resources 739
Administrator access to resources 739
Managing version control 741
Allowing web service and server calls from workbooks 744
Reviewing the Check In Log 745

Monitoring resource usage 746
Managing process instances 750
Monitoring and canceling scripts 750
Retrieving predefined workbooks 751
Migrating RapidResponse resources 752
Caching worksheet results 763
Forms included in RapidResponse 765
Running automation tasks 767
Unlocking automation resources 769
Responding to a scenario 771
Managing global resource tags 772
CHAPTER 48: Tracking and managing adaptive collaborations 775
Administrator tools for collaboration management 775
CHAPTER 49: Application configuration and settings 777
Configuring S&OP application resources 777
S&OP resources and calculations 777
S&OP data modification scheduled tasks 782
Configuring other application settings 783
Configuring supporting resources 785
Data Integrity - Material workbook and metrics 785
Line of Balance workbooks 786
Clear to Build workbook 786
Attribute Rules workbook 786
Kanban Manager workbook 786
Allotment Overrides workbook 786
Risk/Opportunity Assessment workbook 792
Multi-enterprise workbooks 792
Inventory Analysis workbook 792
Configuring Self-Healing Supply Chain resources 792
Self-Healing Supply Chain scenario structure 793
Self-Healing Supply Chain control fields 796
Self-Healing Supply Chain automation tasks 798
Self-Healing Supply Chain users and groups 801
CHAPTER 50: Predefined resource and tool settings 807
Model, unit, and pool information 807
Attribute Rules workbook 807
CHAPTER 50: Configuring RapidResponse maps 811
Setting up access to maps 812
Mapping requirements 812
Set up access to the mapping service 812
Configuring geocode data for maps 813
CHAPTER 51: Supplier collaboration setup 815
Supplier collaboration overview 815
Automated data flows 817
Scenario setup for supplier collaboration 820
Supplier collaboration predefined resources 822
Adding a new supplier and users 825
Adding a new buyer user 828

CHAPTER 52: Data change tracking and record identification **829**
Configuring data change tracking 829
Deleting data change records 833
CHAPTER 53: Configuring single sign-in for On-Premises **835**
About single sign-in 835
Implementing single sign-in for RapidResponse 843
Integrating RapidResponse with an existing single sign-in environment 847
Implementing single sign-in using SAML2 855
Allowing users to use prompted sign in 860
CHAPTER 54: Configuring single sign-in for On-Demand **863**
About single sign-in 863
Implementing single sign-in 865

Part 8: Data Publishing **869**

CHAPTER 55: Setting up for data publishing for On-Premises **871**
RapidResponse-to-RapidResponse connection 871
Steps to configure data publishing 873
Creating the publisher ID record 873
Data required for publishing 874
Installing the Data Transfer Client for data publishing 875
Moving data to the Data Transfer Client computer 881
Configuring global data transfer settings 881
Configuring data feeds and file locations 882
Defining and configuring subscribers 885
Providing users with data publishing resources and permissions 887
CHAPTER 56: Setting up for data publishing for On-Demand **889**
RapidResponse-to-RapidResponse connection 889
Summary of initial setup steps 890
Data required for publishing 891
Defining subscribers 892
Providing users with data publishing resources and permissions 893

Part 9: Configuring RapidResponse subscribers (On-Premises only) **895**

CHAPTER 57: RapidResponse-to-RapidResponse connection **897**
The RapidResponse-to-RapidResponse connection 897
Steps in configuring the RapidResponse-to-RapidResponse connection 898
CHAPTER 58: Installing and configuring GlobalSCAPE software **901**
Installing the GlobalSCAPE EFT & DMZ Gateway Servers 901
Configuring the GlobalSCAPE EFT Server 903
CHAPTER 59: Installing and configuring Copy Command **907**
Installing Copy Command 907
Configuring the GlobalSCAPE EFT Server to run Copy Command 908
Logging 909
CHAPTER 60: Adding publishers **911**
Creating a new user account 911
Adding a publisher as a data source 912

Index **913**

Part 1: Overview

- "Welcome " on page 15
- "About Kinaxis" on page 19
- "Accessing help and documentation" on page 21
- "RapidResponse administration roles" on page 33
- "Security and infrastructure" on page 45
- "International character set support" on page 65
- "New and changed in RapidResponse" on page 67
- "Configuration changes managed by Kinaxis for On-Demand" on page 95

CHAPTER 1: Welcome

Thank you for choosing and using RapidResponse® from Kinaxis®. RapidResponse helps manufacturers manage increasing business complexity and achieve operations performance breakthroughs with its proven solution for demand and supply chain planning, monitoring and response.

This guide explains all RapidResponse administration tasks and processes from managing the entire system to managing user accounts.

RapidResponse supports three types of administrators: system, user, and data. This guide includes information for the three types of administrators which means you might not need all the information in this guide depending on the type of administrator you are. In each section of the guide you will find a note or comment indicating which type of administrator the information is relevant to. For more information about administrator types, see "RapidResponse administration roles" on page 33.

Data administrators should review this document. However, much of the information directly related to their roles is discussed in the *RapidResponse Data Integration Guide*.

On-Premises versus On-Demand

RapidResponse is available as an On-Premises installation and the On-Demand RapidResponse service (sometimes called SaaS or Software as a Service). From a user's perspective, using either type of RapidResponse is almost identical.

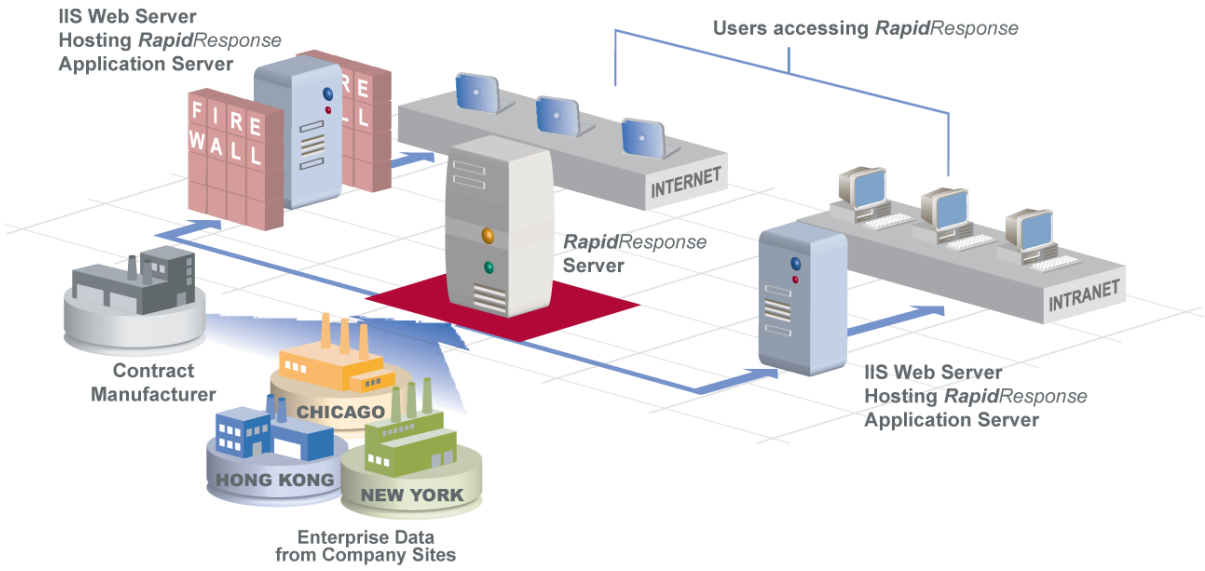
Some administration tasks and processes differ depending on whether you are using On-Premises RapidResponse or the On-Demand RapidResponse service. This guide explicitly notes differences in processes and procedures for the different environments.

On-Demand RapidResponse administrators do not have access to tools, commands, or functionality that might disrupt the RapidResponse service. For example, On-Demand RapidResponse administrators cannot stop the RapidResponse service.

If your company uses a RapidResponse test environment you have the same tools, functionality, and permissions as On-Premises RapidResponse administrators. It is in the RapidResponse test environment where changes to the RapidResponse system can be made and then later applied to the RapidResponse production environment with the assistance of Kinaxis Customer Support. For more information, see "Configuration changes managed by Kinaxis for On-Demand" on page 95.

On-Premises RapidResponse

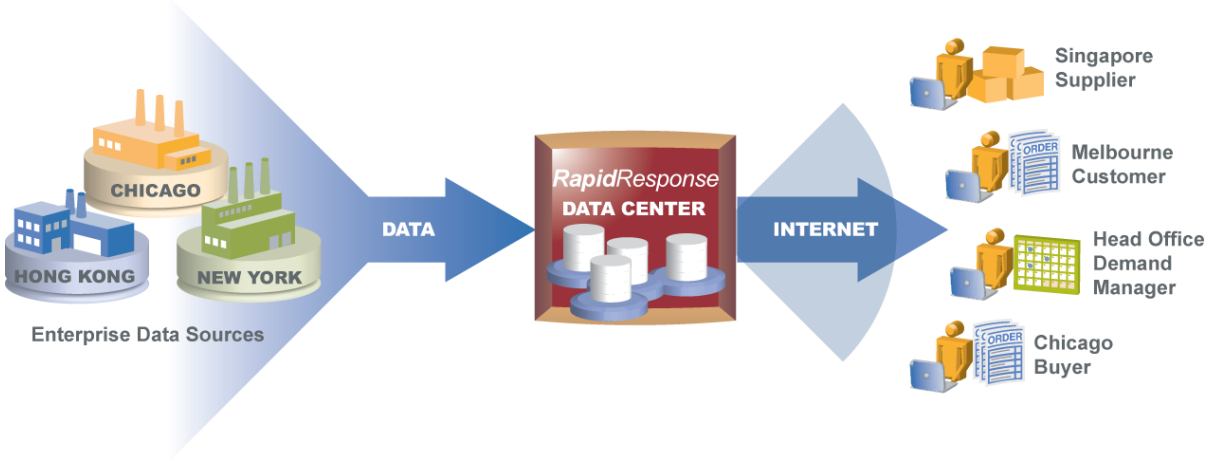
With the On-Premises installation of RapidResponse, enterprise data is integrated into the RapidResponse Server on a computer that the your company manages. Your company is responsible for data extracts, managing the RapidResponse database, configuring RapidResponse, and the connectivity of all users. Users connect to RapidResponse over their intranet or the Internet. The following illustration is an example of a typical On-Premises installation of RapidResponse.



On-Demand RapidResponse service

With the On-Demand RapidResponse, your company is responsible for extracting data from enterprise systems. However, instead of sending the data to one of your servers hosting RapidResponse, the data is sent over the Internet to the RapidResponse Data Center which is hosted by Kinaxis.

Your company is responsible for sending the data to the RapidResponse Data Center in the correct format, and is also responsible for most of the RapidResponse client configuration and user management. However, companies that deploy the On-Demand RapidResponse service are not responsible for hardware that hosts RapidResponse applications or the detailed system administration expertise—Kinaxis personnel handles the complex administrative tasks. The following illustrates the typical On-Demand RapidResponse service setup.


CHICAGO
HONG KONG
NEW YORK
Enterprise Data Sources
DATA
RapidResponse
DATA CENTER
INTERNET
Singapore
Supplier
Melbourne
Customer
Head Office
Demand
Manager
Chicago
Buyer

CHAPTER 2: About Kinaxis

Kinaxis® delivers cloud-based S&OP and supply chain applications for discrete manufacturers and brand owners with complex supply chain networks and volatile business environments.

Leaders across multiple industry verticals, including A&D, Automotive, High Tech, Industrial and Life Sciences rely on RapidResponse® applications to create a foundation for concurrent planning, continuous performance monitoring, and coordinated responses to plan variances across multiple areas of the business. All founded on a single product, RapidResponse's configurable applications encompass a full spectrum of supply chain processes, including such functions as S&OP, supply planning, capacity planning, demand planning, inventory management, MPS, and order fulfillment.

As a result, Kinaxis customers have replaced disparate planning and performance management tools and are realizing significant operations performance breakthroughs in planning cycles, supply chain response times and decision accuracy. From a single product, customers are able to easily model varying supply chain conditions to make both long-term and real-time demand and supply balancing decisions quickly, collaboratively, and in line with the shared business objectives of multiple stakeholders.

For more information, visit www.kinaxis.com or the Kinaxis Knowledge Network at http://knowledge.kinaxis.com/.

Customer Support

The Kinaxis Customer Support team understands demand and supply chain planning, monitoring and response, and is experienced in applying RapidResponse to real-world business scenarios. Areas of expertise include:

- RapidResponse functionality
- Data extraction and mapping issues
- Technical software compatibility
- Coordination of integration
- Product implementation

If you are a key support contact, you can submit support cases. To submit a support case, log into the Kinaxis Knowledge Network. You can also contact Kinaxis Customer Support by phoning 1-866-463-7877 or by sending a message to support@kinaxis.com.

Kinaxis Knowledge Network

The Kinaxis Knowledge Network is the place to find knowledge about RapidResponse. In one site, you can:

- Search all knowledge about RapidResponse, including product documentation, knowledge base articles, and threaded discussions about common questions.
- Review your company's Customer Support requests (and, if you are a key support contact, create new Support requests).
- Engage with a community of RapidResponse experts in the Discussion Groups.

Go to https://knowledge.kinaxis.com and log in today. You can also access the Kinaxis Knowledge Network from RapidResponse by clicking **Kinaxis Knowledge Network** on the **Help** menu.

CHAPTER 3: Accessing help and documentation

Determining which help system or guide to use 22
Documentation conventions 24
Finding the content you need in HTML help 24
Your feedback 25
Help embedded in resources 25
Other ways to learn about RapidResponse 31

The RapidResponse documentation set includes several different help systems and guides, each dealing with a different area of knowledge. Help for individual resources, such as workbooks is also available.

In addition to the RapidResponse documentation, you can access a variety of other resources to help you learn about the capabilities and features in RapidResponse. These include an online community where you can view how-to videos and find advice, a mailing list that you can use to keep up to date on supply chain news and upcoming events, and instructor-led training courses.

Accessing RapidResponse help systems and guides

You can access RapidResponse help systems and guides two ways:

- Access documentation directly from the Help menu in RapidResponse.
- For links to all of the available help systems and guides, see "Determining which help system or guide to use" on page 22.

Account permissions and the contents of your Help menu

The list of options you see when you click the Help menu in RapidResponse depends on the permissions associated with your RapidResponse account. The more permissions you have in RapidResponse, the more options you see on the menu. For example, resource authors have more permission than general users.

Links to documentation that you are less likely to need, based on your permissions, are not shown on the Help menu. For example, users without administrator permissions do not see Administration Help.

Documentation formats

Most RapidResponse documentation resources are available as both HTML help systems and PDF documents. Some documentation is only available in PDF format.

HTML help systems are optimized for viewing in a web browser. While it is possible to print individual topics from HTML help, you will get better results if you print the topic or topics from the equivalent PDF guide.

PDF guides are optimized for printing. They can be viewed and printed using Adobe Reader®. You can download Adobe Reader from the Adobe site at www.adobe.com.

Accessing help for RapidResponse resources

Help is often available in the RapidResponse application window for individual resources of the following types:

- Dashboards and widgets
- Worksheets and workbooks
- Scorecards
- Forms
- Scripts
- Responsibility definitions

For more information, see "Help embedded in resources" on page 25.

Determining which help system or guide to use

The RapidResponse documentation set includes several help systems and guides, each dealing with a different area of knowledge. The following table summarizes the available documentation, some of which you can access from the Help menu in RapidResponse.

Title	Description
RapidResponse User Guide	This guide provides Java client users with basic reference and procedural information. It covers topics such as viewing data, modifying data as part of simulation, solving business problems, and customizing the user interface.
RapidResponse User Guide (Web Client)	This guide provides information on how to view and edit data in the web client.
RapidResponse Applications Guide	Practical ways to use RapidResponse and the applications that can be deployed to support business processes and make decisions. It also includes instructions aimed at RapidResponse administrators that outline how to install and configure applications.
RapidResponse Fundamental Concepts Guide	RapidResponse product overview, which includes key capabilities and the deployment methodology.
RapidResponse Resource Authoring Guide	This guide provides information on creating and managing resources, such as dashboards, workbooks, and filters. Detailed information about RapidResponse Query language is also included.

Title	Description
RapidResponse Analytic and Data Model Guide	Description of the RapidResponse data model and associated analytics. All tables and fields in the data model are listed and described. This guide also notes changes to the data model corresponding to the RapidResponse release.
Data model posters	A series of posters illustrating the structure of tables and fields in RapidResponse, and the relationships between fields. For more information, see "Data Model Posters" on page 23.
RapidResponse Administration Guide	Information for administrators, covering installation, upgrades, maintenance, system settings, and user administration.
RapidResponse Scripting Guide	Information about building custom applications using scripting language objects, functions, and methods to automate some RapidResponse processes.
RapidResponse Web Services Guide	Information on using RapidResponse Web services to create users, resources, and Web service client programs.
RapidResponse Data Integration Guide	Information about integrating enterprise data sources with RapidResponse, including mapping data from source tables and fields, customizing the RapidResponse database, extracting data from enterprise sources, performing data updates to bring new and updated data into RapidResponse, moving data between RapidResponse instances, and moving data changes between RapidResponse and business partners in real-time.
Global Help	If you are not sure which help system contains the information you need, you can search for it in this help system, which includes information from all of the other help systems.
RapidResponse Release Summary	The latest release summary outlines all of the changes that have been made in RapidResponse 1904, including new features and defect resolutions in service updates. Release summaries can be found in the Kinaxis Knowledge Network in the Documentation Center.
Custom Help	Your company might have also created custom help specific to your RapidResponse implementation.

The permissions associated with your RapidResponse account affect the list of guides that you can access from the Help menu. For more information, see "Account permissions and the contents of your Help menu" on page 21.

Data Model Posters

Users who have permission to create resources such as workbooks and dashboards have access to the following posters on their RapidResponse Help menus:

- *RapidResponse Data Model for Import poster*—displays the relationship between the tables and fields used in the RapidResponse data import process.
- *RapidResponse Calculated Data Model poster*—displays the relationship between the main RapidResponse database calculated tables and fields. Calculated fields in the RapidResponse data model input tables are also displayed.
- *RapidResponse Sales & Operations Planning poster* —displays the relationship between the tables used to support the Sales & Operations Planning application.

- *RapidResponse Inventory Planning and Optimization poster* —displays the relationship between the tables used to support Inventory Planning and Optimization application.
- *RapidResponse Integrated Project Management poster* —displays the relationship between the tables used to support Integrated Project Management application.
- *RapidResponse Historical Supply poster* and *RapidResponse Historical Demand poster*—displays the relationship between all tables (input, control, and calculated) that are used to store historical supply data and historical demand data, respectively.

Documentation conventions

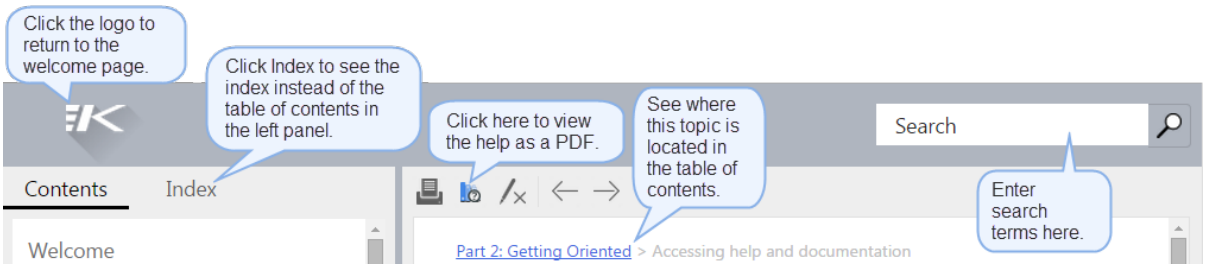
To help you quickly locate and interpret information, Kinaxis guides use conventions noted in the following table.

	Convention	Description
	bold	Bold is used for user-interface elements in procedures. For example: On the **File** menu, click **New**.
	italic	Italic is used when citing other documents. For example: For more information, see the *RapidResponse Administration Guide*.
	`Courier New`	Courier New is used for programming examples and text that is entered in Microsoft Windows Command Prompt window or command lines.
	Caution:	Identifies a caution message (critical information).
	Note:	Identifies a note.
	Tip:	Identifies a tip.

If you are using a Mac OS, procedures that use the Windows CTRL key should be replaced with the Mac OS Command key.

Finding the content you need in HTML help

You can find information in any RapidResponse HTML help system by searching or by browsing in the contents or the index.



Searching the help

You can find the information you require by entering a term in the Search box. You can also refine your search by using AND or OR to search for a combination of words, and you can put quotation marks around your search word or phrase to search for that exact phrasing only. For example, "sort" would return any topics with the word "sort", but not the words "sorted" or "sorting".

▸Search for content

- Type a search term in the search bar and then click .

Note: If you do not want the words you searched for highlighted in the help topic, click **Remove Highlights** .

Tip: If the browser window is small, the search bar might not be displayed. To see a search bar click or enlarge the window.

Browsing the contents and the index

You can also find information by browsing in either of these panes:

- **Contents**—Browse through the topics in the table of contents.
- **Index**—Find a topic through the index. Scroll through the index or type a word or phrase in the Search Index box to find an index entry.

Tip: If the browser window is small, the Contents and Index panes might not be displayed. To see them, click or enlarge the window.

Your feedback

Kinaxis Inc. takes great pride in developing user-friendly applications and we hope that our documentation resources ensure a high level of usability. We welcome your feedback about the help topics you access.

If you have comments or suggestions about Kinaxis documentation or training materials, you can email them to learning-techsupport@kinaxis.com.

Help embedded in resources

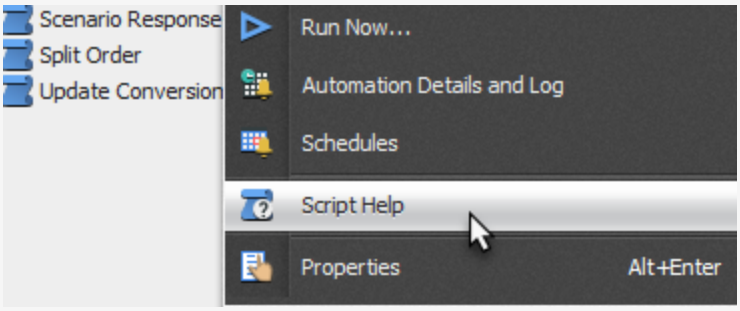
Many openable RapidResponse resources have help embedded within the resource. The form the help takes depends on the type of resource.

When help is available for a resource, you can view it from the open resource. You can also view the help for some types of resources from the Explorer, without having to open the resource first. These resources include workbooks, scorecards, widgets, forms, and scripts. Viewing resource help from the Explorer can help you to determine whether a resource is the right one to use, without having to wait for it to load.

▸View resource help without opening the resource

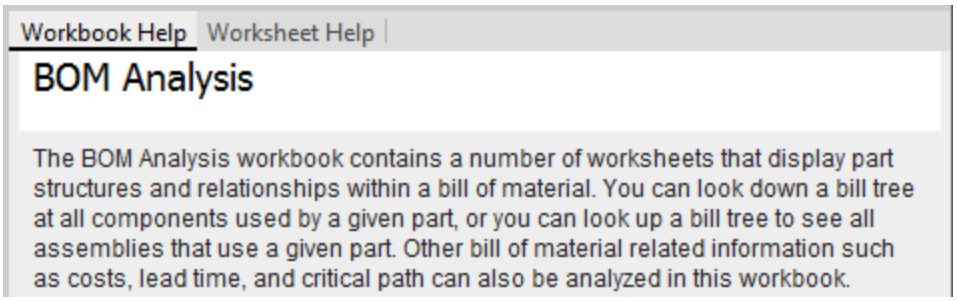
- In the **Explorer**, select a resource and then click beside the name of the resource.

Tip: You can also view resource help from the Explorer by right-clicking the name of the resource and then selecting the Help option for the resource from the menu. For example, to view help for a script, click Script Help.



View and print worksheet and workbook help

RapidResponse worksheets can include a help page that is displayed in a pane on the right-hand side of the worksheet. Workbooks might also include a help page, in which case, the help pane includes two tabs: Workbook Help and Worksheet Help.



▸Show or hide the help pane

- On the **Help** menu, click **Show Workbook/Worksheet Help**.

Note: This command is not available for workbooks that do not have workbook help or help for at least one worksheet defined.

Tip: You can also show or hide the help pane by clicking **Show Workbook/Worksheet Help** on the toolbar.

▸Print the worksheet or workbook help

You can print the worksheet or workbook help when the help pane is displayed.

1. On the **File** menu, click **Print**.
2. Click **Worksheet help** or **Workbook Help**, and then click **OK**.

Note: The worksheet and workbook help are printed as they appear in the help pane. Widen the help pane before printing to maximize the amount of information printed on a page.

Tip: You can also print the worksheet help by right-clicking in the help pane, and then clicking **Print**.

View and print scorecard help

Each scorecard in RapidResponse includes a help page that is displayed in a pane on the right-hand side of the scorecard. You can show and hide the scorecard help pane.

- On the **Help** menu, click **Show Scorecard Help**.

Note: This command is available only for scorecards that have help defined.

Tip: You can also show or hide the scorecard help pane by clicking **Show Scorecard Help** on the toolbar.

▸Print the scorecard help

You can print the scorecard help when it is displayed.

1. On the **File** menu, click **Print**.
2. Click **Scorecard help**, and then click **OK**.

Note: The scorecard help is printed as it appears in the help pane. Widen the worksheet help pane before printing to maximize the amount of information printed on a page.

Tip: You can also print the scorecard help by right-clicking in the help pane, and then clicking **Print**.

View dashboard and widget help

Dashboard help is often available for a dashboard as a whole, and you might also be able to view help for individual widgets.

Dashboard help

Some dashboards might have an Information tab with a text widget that shows dashboard help. Dashboard help contains information about how the dashboard is intended to be used, and can include links to related resources, websites, or help videos.

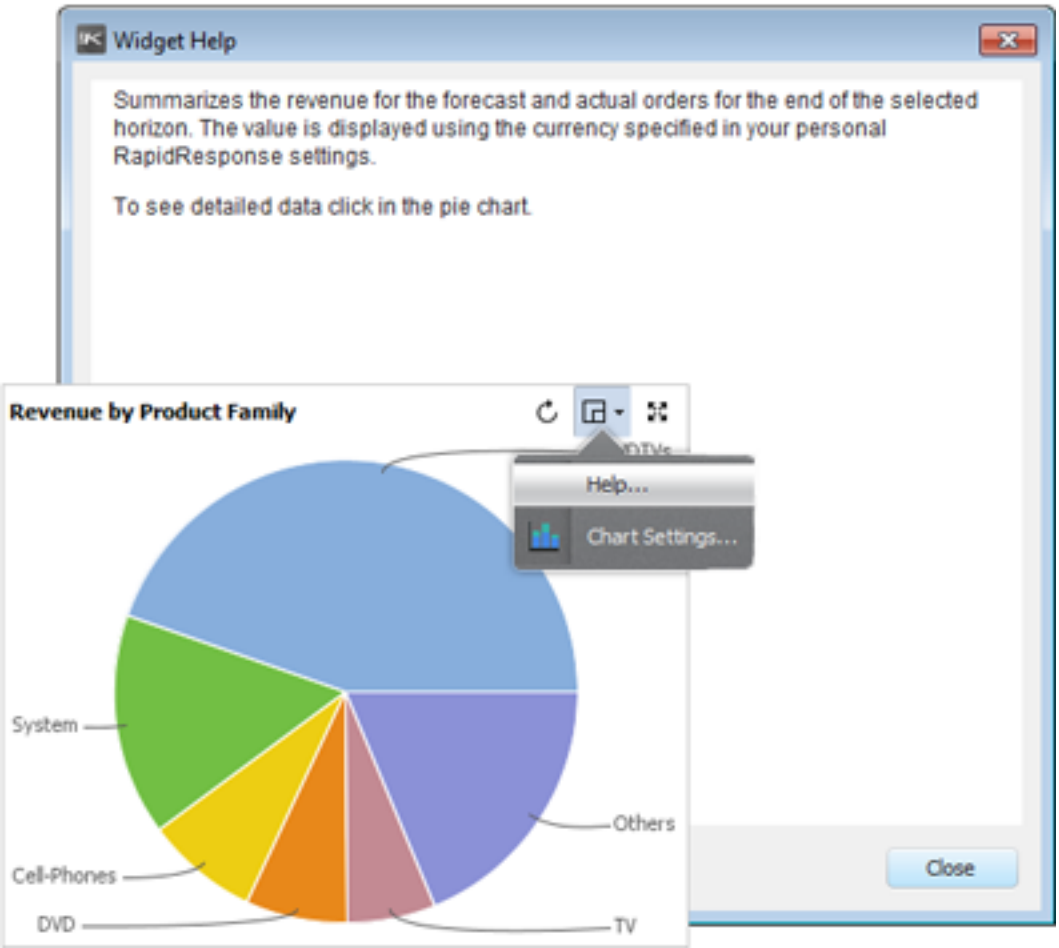
Widget help

Most widgets on dashboards that are supplied with RapidResponse have widget help, and some custom widgets might also include help. Widget help typically describes the metrics displayed in a widget, and might include links to other resources such as workbooks and websites. You can access help for widgets directly from the widget controls on a widget on your dashboard.

▸View widget help

- On a widget title bar, click **Actions** ◲, and then click **Help**.

  The widget help displays in a dialog box.

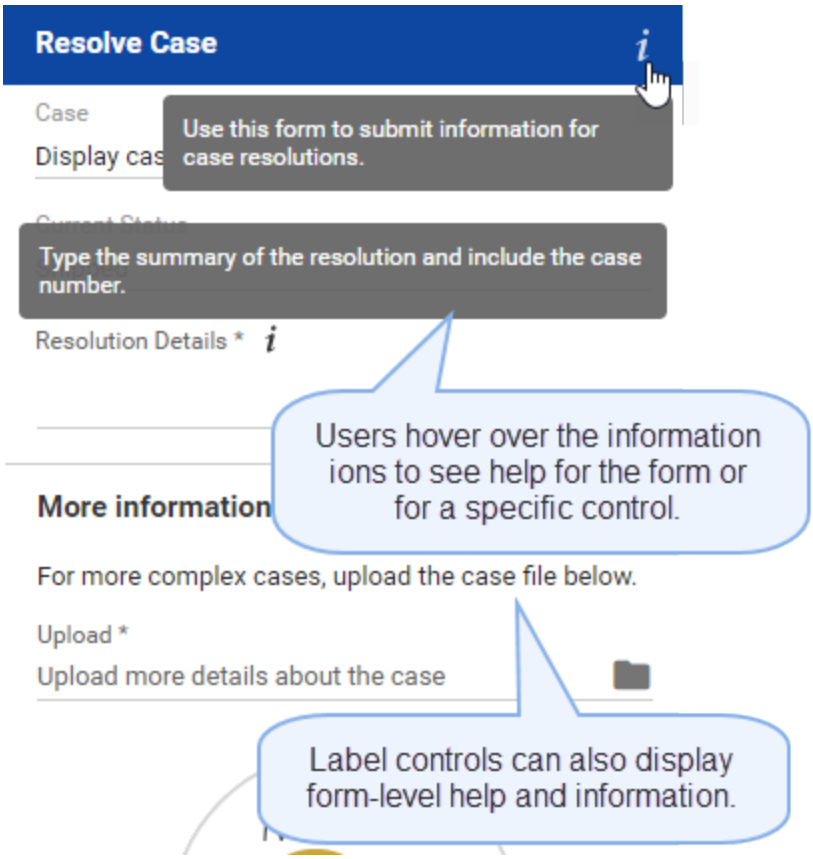


View form help

Forms can display three types of help: contextual help directly on the form, form pop-up help, and field pop-up help.

Both contextual help and form pop-up help might describe the purpose of the form, how to use it, or what happens when the form is run. Contextual help displays right on the form. Form pop-up help displays when you hover over the information icon in the top right corner of the form.

Individual fields on a form might also display help specific to the field, such as what types of values it accepts.



▸View pop-up help for a form

1. On the form, point to the information icon in the upper right corner of the form
   Form help displays below the form title bar.
2. Point away from the information icon to close the help

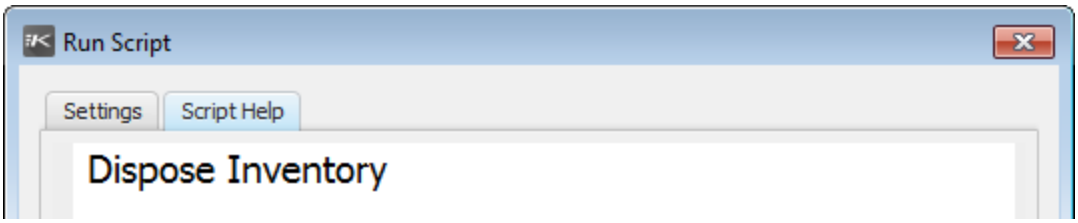
Note: Forms only display the information icon when there is help available in the form.

▸View pop-up help for a field

1. Point to the field you want to view help for.
   Only fields with help display next to the field title
2. Point to the information icon on the field.
   Help for the field displays above or below the field.
3. Point away from the information icon to close the help.

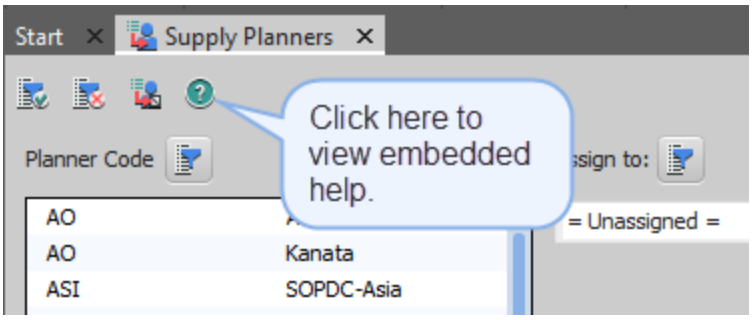
View script help

Some scripts might have embedded help. If a script has embedded help, a Script Help tab is shown when you run the script.



View help for a responsibility definition

You might be able to access embedded help for an open responsibility definition. If help is available, a Responsibility Help button is available near the top left of the tab.



Resources without embedded help

Some types of resources, such as filters, cannot have embedded help, and not every resource that could have embedded help does have embedded help. Resource authors decide whether or not to include help when they create new resources that can have embedded help.

Sometimes, the information needed to use that resource might be available elsewhere. For example, if you access a dashboard by opening it from a task flow, the information you need to understand the purpose of the dashboard might be included in the task flow. Another example is a custom resource created for your company, which might be documented in company procedures that are maintained outside of RapidResponse.

Other ways to learn about RapidResponse

In addition to the RapidResponse documentation set, there are several other ways to learn about RapidResponse.

Kinaxis Knowledge Network

Visit the Kinaxis Knowledge Network at knowledge.kinaxis.com to access features including:

- Upgrade Center—Learn what's new in each version of RapidResponse.
- Training videos—Familiarize yourself with the basic capabilities of RapidResponse by taking an introductory course, delivered as a series of short videos. You can also view videos on some more advanced topics.
- Discussion Forums—Discuss RapidResponse with other users.
- Blogs—Learn how others are using RapidResponse and solving supply chain problems.

Some content is only available after you create a Kinaxis Knowledge Network user account and sign in.

News mailing list

Subscribe to the mailing list to stay up-to-date on news and upcoming supply chain events, such as Kinexions, the annual Kinaxis training and user conference. You can find the subscription form at http://info.kinaxis.com/customer-subscription-page.

Training courses

Kinaxis offers instructor-led courses and self-paced online training courses to help you develop in-depth RapidResponse knowledge. Instructor-led courses are usually delivered online in a virtual classroom, but on-site instruction can also be arranged. To see a list of available courses, visit https://www2.kinaxis.com/rapidresponse-training/courses.cfm.

CHAPTER 4: RapidResponse administration roles

Administration overview 33
Master Administrator user account for On-Premises 34
System administrator responsibilities 34
User administrator responsibilities 35
Data administrator responsibilities 36
Permission to modify data integration settings 36
Administration pane permissions 37
Determining administrator permissions 41
Assigning administrator permissions 41
Configuring administrator permissions 43
Test systems for the On-Demand service 43

RapidResponse supports three types of administrator roles—system, user, and data. It is expected that more than one person at your company fills each administrator role. This chapter discusses the role of each type of administrator, as well as the prerequisite skills and knowledge each is assumed to have. It also outlines the RapidResponse permission levels associated with each administrator type.

Administration overview

Each administrator is a member of a group that provides the administrative capabilities and permissions, as well as resources and user permissions. The administrative groups that are included with RapidResponse can be modified, or you can create your own groups and grant them administrator permissions. For information about creating groups, see "Best practices for setting up user accounts" on page 493. For information about modifying administrative groups, see "Managing groups and users" on page 565.

The administrator groups included with RapidResponse are by default granted every user permission available. As well, these groups have access to all the panes available in the RapidResponse client and can view all the shared workbooks, filters, scorecards, alerts, and task flows available to users in RapidResponse. You can customize the user permissions granted to administrators. For more information about user permissions, see "Creating groups" on page 513. For more information about customizing administrator permissions, see "Assigning administrator permissions" on page 41.

Each administrator consumes a user license. Administrators who also use RapidResponse for response management tasks are expected to use one account for all of their RapidResponse activities, and not to have separate user accounts for their administration role and their user role.

Master Administrator user account for On-Premises

RapidResponse includes access to the Master Administrator user account in On-Premises environments. This account uses **Admin** as the user ID. Because there must always be at least one user with administrator permissions, the Master Administrator is a system account and cannot be deleted.

Only the Master Administrator user can initially create other user accounts (either general users or administrators). Once created, system or user administrators can then create other user accounts. System administrators can also place users in administrator groups.

It is important that only one or two people within your organization have access to the Master Administrator user account. However, this account should not be used for daily administrative tasks.

After installation or setup of RapidResponse, the first sign in to RapidResponse is performed using the Master Administrator account, with the password specified during the RapidResponse Server installation. The password is provided by Kinaxis Customer Support.

Only the Master Administrator user can change the account's password. It is recommended that you change this password periodically for security purposes. To change the password, sign in to RapidResponse as the Master Administrator, and then change the password using the **Change Password** command on the **Tools** menu. For more information, see the *RapidResponse User Guide*.

The Master Administrator account also has an associated email address. This email address receives status and error notifications, such as a scheduled operation failing, from RapidResponse. The email account associated with the Master Administrator account should be reviewed on a daily basis. For more information, see "To change the Master Administrator user email address" on page 422.

System administrator responsibilities

System administrators have all the access, permissions, and rights of user and data administrators. In addition, system administrators are responsible for global RapidResponse system settings and configuration.

System administrators must be members of the System Administrators group, or any other group that has system administrator permissions.

Note: Only system administrators can create or modify user accounts with data or user administrator permissions.

RapidResponse system administrators are responsible for some of the following tasks:

- Installing and configuring the RapidResponse Data Transfer Client.
- Customizing RapidResponse data formats and print settings.
- Contacting Kinaxis Customer Support for additional customization and configuration. For more information, see "Configuration changes managed by Kinaxis for On-Demand" on page 95.
- Installing and upgrading RapidResponse software. For more information see, "Part 2: Installation for On-Premises" on page 97 and "Part 3: Upgrading RapidResponse" on page 139.
- Customizing permissions granted to administrator groups. For more information, see "Configuring administrator permissions" on page 43.

- Creating user accounts and placing them in the user administrator and data administrator groups. For more information, see "Creating user accounts" on page 539.
- Installing and configuring hardware, including servers, operating systems, and networking connectivity.
- Monitoring day-to-day system uptime, performance, and log files. For more information, see "Reviewing system status and operation logs" on page 421.
- Monitoring day-to-day data import and data update log files. For more information, see "Reviewing system status and operation logs" on page 421.
- Monitoring system memory consumption and deleting unused scenarios. For more information, see "RapidResponse system memory and monitoring" on page 259.
- Managing and modifying system and data configuration settings.
- Managing and backing up the RapidResponse database and files required to restore RapidResponse in case of a disk crash or system failure. For more information, see "Managing the RapidResponse database" on page 309.

Depending on their responsibilities, it is expected that RapidResponse system administrators have some of the following skills or characteristics:

- Typically a hardware IT analyst or network administrator.
- Understands the network environment including the mail server environment.
- Experienced in installing Microsoft operating systems and various software packages.
- Understands the architecture of RapidResponse components.

For a detailed list of all permissions given to system administrators, see "Administration pane permissions" on page 37.

User administrator responsibilities

User administrators are responsible for creating and managing general user accounts. This includes assigning group memberships, providing site access, and managing resources such as workbooks, task flows, and filters. User administrators cannot create or modify other administrator accounts.

User administrators must be members of the User Administrators group, or any other group that has user administrator permissions.

A “super”, or very experienced, RapidResponse user sometimes fills the user administrator role. A RapidResponse user administrator might be responsible for some of the following tasks:

- Providing first line user support for RapidResponse users.
- Creating users and groups. This covers the primary user administration tasks and is discussed in "Part 6: User administration" on page 491.
- Providing users resources and permissions to view data and simulate business scenarios. For more information, see "Creating groups" on page 513.
- Canceling queries. For more information, see "Monitoring and canceling problematic queries " on page 603.
- Troubleshooting sign in and workbook opening issue. For more information, see "Resolving RapidResponse error messages" on page 602.
- Contacting Kinaxis Customer Support for additional customization and configuration. For more information, see "Configuration changes managed by Kinaxis for On-Demand" on page 95.

It is expected that more than one person fills the user administration role. Depending on their responsibilities, it is expected that user administrators have some of the following skills or characteristics:

- Typically is part of an IT help desk.
- Understands the basic RapidResponse user experience.
- Is experienced in handling user inquiries and issues.

For a detailed list of all permissions available to user administrators in the Administration pane, see "Administration pane permissions" on page 37.

Data administrator responsibilities

Data Administrators are primarily responsible for loading data (in text files and Microsoft Excel® files) into the RapidResponse database. Data administrators are also responsible for configuring how RapidResponse analytics perform calculations, customizing the data model, creating and managing sites, monitoring the data import and update processes, and publishing data to RapidResponse subscribers. Data administrators cannot create or modify user accounts. For more information about these tasks, the *RapidResponse Data Integration Guide*.

Data administrators must be members of the Data Administrators group, or any other group that has data administrator permissions.

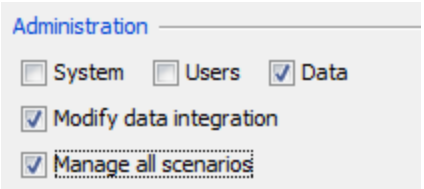
It is expected that more than one person fills the data administration role. Depending on their responsibilities, it is expected that data administrators have some of the following skills or characteristics:

- Understands database concepts and the enterprise data system.
- Understands the architecture of RapidResponse components.
- Is knowledgeable about the RapidResponse data model.
- Understands the basic RapidResponse user experience.
- Experienced in handling user inquiries and issues.

For a detailed list of all permissions available to data administrators in the Administration pane, see "Administration pane permissions" on page 37.

Permission to modify data integration settings

When assigning system or data administration permissions to a user, you can specify whether the administrator will have permissions to make changes to data integration settings. The following illustration shows the Administration section of the User Properties dialog box.



Making changes to RapidResponse data integration settings can potentially destabilize or bring down the RapidResponse system. For this reason, you should carefully consider who will have permissions to change data integration settings.

The **Modify data integration** permission controls the following RapidResponse data settings:

- **Sites**—At least one site is configured for your company during the initial RapidResponse integration. Subsequently, you can add and define new sites in RapidResponse.
- **Data Sources and Mapping**—Changes the data sources or data files used to provide data for RapidResponse input tables, or adds a new data source to provide data for a new site.
- **Data Model**—Using the Data Model dialog box, adds new custom tables or fields to the RapidResponse data model. These can be used to hold data not stored in the standard data model. The Data Model dialog box can also be used to modify properties of custom or standard RapidResponse tables and fields. For example, you can modify the default value used for a field when no value is provided, or you can set whether a given record allows automatic record creation.
- **Data Persistence**—Defines new data persistence rules. These are used to preserve specified data from a given scenario during a data import.

For more information about these settings and tasks, see the *RapidResponse Data Integration Guide*.

If a system or data administrator does not have modification permissions, then they will only be able to view (read-only mode) these data integration settings. System and data administrators without the **Modify data integration** permission can still import or export integration packages (.IPK files), but the **Data sources and mapping** and **Data model namespaces** options will not be available when selecting the settings to include when exporting or importing.

Note: Although On-Demand administrators might have permission to modify data integration settings, they still require the assistance of Kinaxis Customer Support to apply changes to RapidResponse. For example, administrators can customize the data model but cannot apply the changes themselves. For more information, see "Configuration changes managed by Kinaxis for On-Demand" on page 95.

Administration pane permissions

All RapidResponse administrators have access to the Administration pane. However, the items available in the Administration pane differ depending on the administrator group or groups the user belongs to (system, user, or data).

Permission	User	Data	System
User accounts			
Users and Groups	•		•
User Profile Variables	•		•
Site Permissions	•		•

Permission	User	Data	System
Resource Permissions	•		•
Communication			
Send Broadcast Message	•	•	•
Message Center and Email			•
Data			
Control Sets		•	•
Currencies		•	•
Data Model		•	•
Data Origin		•	•
Data Persistence Rules		•	•
Perspectives		•	•
Sites		•	•
Data Integration			
Data Sources and Mapping		•	•
Integration Utilities		•	•
Tolerance and Error Settings		•	•
Business Message Definitions[1]		•	•
Configure Real-time Integration Services (On-Premises only)		•	•
Configure Integration Platform Services		•	•

Permission	User	Data	System
Real-time Integration Service Endpoints[1]		•	•
Real-time Message Log[3]		•	•
Data Integration Toolkit[2]			
Data Integration Center		•	•
Source System Configuration		•	•
Mapping Specification		•	•
System monitoring			
Administration Log		•	•
Application Server Event Log (On-Premises only)	•*	•*	•
Automation Log	•	•	•
Collaborations	•		•
Business Message Log[1]		•	•
Data Extract Log		•	•
Data Import and Update Log		•	•
Query Manager	•		•
Real-time Integration Service Status[1]		•	•
Resources	•	•	•
Resource Check In Log	•	•	
Scenarios	•	•	•

Permission	User	Data	System
Server Performance History			•
Sign-in Log	•		•
System Utilities	•	•	•
System settings			
Application Settings	•	•	•
Configuration			•
Data Formats		•	•
Data Publishing Setup		•	•
Global Settings			•
Help Settings			•
Licenses		•	
Map Visualization Setup			•
Password Security Policies			•
Print Settings			•
Scheduled System Tasks		•	•
Sign-in notice			•
Tags	•	•	•
Time Zones		•	•

Permission	User	Data	System
Workbook Links			•
Web Services			
Change Data Capture Setup		•	•
Web Services Log		•	•

* Indicates a permission is required.

[1] Indicates only available if the RapidResponse Real-time Integration Service has been configured.

[2] Indicates only available if the RapidResponse Integration Toolkit has been installed.

[3] Indicates only available if the Real-time Integration Platform has been configured.

Determining administrator permissions

If you are a system or user administrator, you can determine who has been assigned administrator permissions. This might be useful when performing system audits.

▸To review which users have administrator permissions

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** tab.
3. Review the **Administrator** column. This column indicates administrator type.

Tip: You can filter the **Users** tab to show only administrators by typing **NOT ' '** in the search row.

Assigning administrator permissions

If you are a system administrator, you can assign administrator permissions to groups and users. Assigning any of the administrator permissions also automatically grants access to all shared resources, and assigns authoring and sharing permission for every type of resource, but you can modify these permissions.

By default, none of the three administrator groups allows administrators to modify data integration settings or manage all scenarios in the RapidResponse system.

Without the data integration permission, administrators can only view (read-only) data integration settings. For more information, see "Permission to modify data integration settings" on page 36.

The Manage All Scenarios permission allows administrators to modify shared scenarios (including those not shared to the administrator), delete any shared or private scenario, and give any shared scenario to another user.

Administrator permissions should be granted through group memberships.

▸To assign administrator permissions to a user

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select the user you want to assign administrator permissions to.
3. Click **Properties** on the Users and Groups toolbar.
4. Click the **Group Memberships** tab.
5. Click **Select Groups**.
6. In the list, select the administration group to which you want to add the user, and then click **Member Of**. By default, RapidResponse includes three administration groups (or roles):
   - **System Administrators**—Grants system administrator permissions, as discussed in "System administrator responsibilities" on page 34.
   - **User Administrators**—Grants user administrator permissions, as discussed in "User administrator responsibilities" on page 35.
   - **Data Administrators**—Grants data administrator permissions, as discussed in "Data administrator responsibilities" on page 36.
7. Click **OK**.
8. Click **OK**.

Tip: You can also assign these permissions to a new group to create an administrative group, and then grant only the permissions you want the group to have. For more information, see "Managing groups and users" on page 565.

▸To assign other administrator permissions

1. Ensure the user is included in one of the administrator roles.
2. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
3. On the **Users** tab, select the user you want to assign the data modification permissions to.
4. Click **Properties** on the Users and Groups toolbar.
5. Click the **Permissions** tab.
6. Select **Modify data integration** to allow system and data administrators to be able to modify RapidResponse data integration settings. For more information, see "Permission to modify data integration settings" on page 36.
7. Select **Manage all scenarios** to allow administrators to modify shared scenarios (including those not shared to the administrator), delete any shared or private scenario, and give any shared scenario to another user.
8. Click **OK**.

Configuring administrator permissions

The administrator groups included with RapidResponse are granted every user permission. If necessary, you can modify the administrator groups to deny some permissions you do not want administrators to have. For example, you might not want user administrators to override the worksheet record limit, or data administrators to retrieve predefined resources.

By modifying administrator groups or creating groups with administrative permissions, you can create groups of administrators that have different permissions. For example, if you create a group and grant it data administrator permissions, you can have data administrators with every user permission (from the predefined Data Administrators group) and data administrators with whatever permission you assign to the new group.

Test systems for the On-Demand service

Administrators using the RapidResponse On-Demand service usually have access to a test system. This is a separate instance of RapidResponse beyond the production environment. When customizing your RapidResponse data integration, it is strongly recommended to first make all changes in a RapidResponse test environment. It allows you to make and test changes to integration data without fear of causing errors in production or disrupting your RapidResponse user community. The data integration changes made on the test system can then be applied to the RapidResponse production environment with the assistance of Kinaxis Customer Support.

In a RapidResponse test environment, system and data administrators the modify data integration permission can apply data customizations and restart RapidResponse so the customizations are applied.

For more information, see the *RapidResponse Data Integration Guide*.

CHAPTER 5: Security and infrastructure

User security 45
System auditing 51
On-Demand service infrastructure 51
Data security in the On-Demand service 54
Systems used by the On-Demand service 55
On-Demand service security policies and information 57
On-Demand service operational policies 60

RapidResponse® from Kinaxis® uses the most advanced technology for Internet security available today. Whenever you access your supply chain information all communication is encrypted. Your data is safe, secure and available only to registered users.

The following list highlights some of the benefits of using the On-Demand RapidResponse service:

- World-class connectivity to very large data centers.
- Certified to robust industry security standards.
- Guaranteed system administration performance provided by Kinaxis.
- Quarterly system health checks and system usage reporting.
- Managed software and hardware upgrades.
- This section describes RapidResponse security and the On-Demand service infrastructure items in more detail.

User security

Customer administrators determine authorization and read and write data access rights of each user using standard application security features that include a hierarchical user/group model.

The RapidResponse Server database maintains a secure store of user names and passwords. The RapidResponse Application Server connects to the RapidResponse Server using HTTP on a secure internal network. No end user has a direct connection to a RapidResponse Server. All access is brokered by the RapidResponse Application Server.

Changes in RapidResponse 2016.2

In RapidResponse 2015.3 (and earlier), the RapidResponse Application Server communicated with RapidResponse Server using RPC over TCP/IP.

User IDs and signing into RapidResponse

RapidResponse requires a company ID, user ID, and password to authenticate a user's identity when signing in.

The RapidResponse On-Demand service sign-in page is presented over a secure channel and is available at https://rapidresponse.kinaxis.com/.

The sign in page is HTML form-based. The RapidResponse system does not reveal to the user the reason for sign-in failure because that information could be used to determine user credentials. The sign-in information is transmitted from the client to the RapidResponse Application Server using HTTPS/TLS encryption. RapidResponse users require a system where the operating system and browser support this level of encryption. After validation and successful sign-in, RapidResponse generates a non-persistent session cookie which is used to connect the user with the appropriate data instance.

It is important that passwords are kept secret and are sufficiently complex. Password complexity can be enforced in RapidResponse.

A user ID and initial Password for the initial customer administrator is supplied by Kinaxis. A password change is required to be performed by that administrator on initial sign in. All additional users are defined and maintained exclusively by customer administrators, not by Kinaxis.

The SAML 2.0 Web SSO Profile is supported for federated authentication.

For more information, see " Managing users" on page 569.

HTTPS protocol for RapidResponse clients

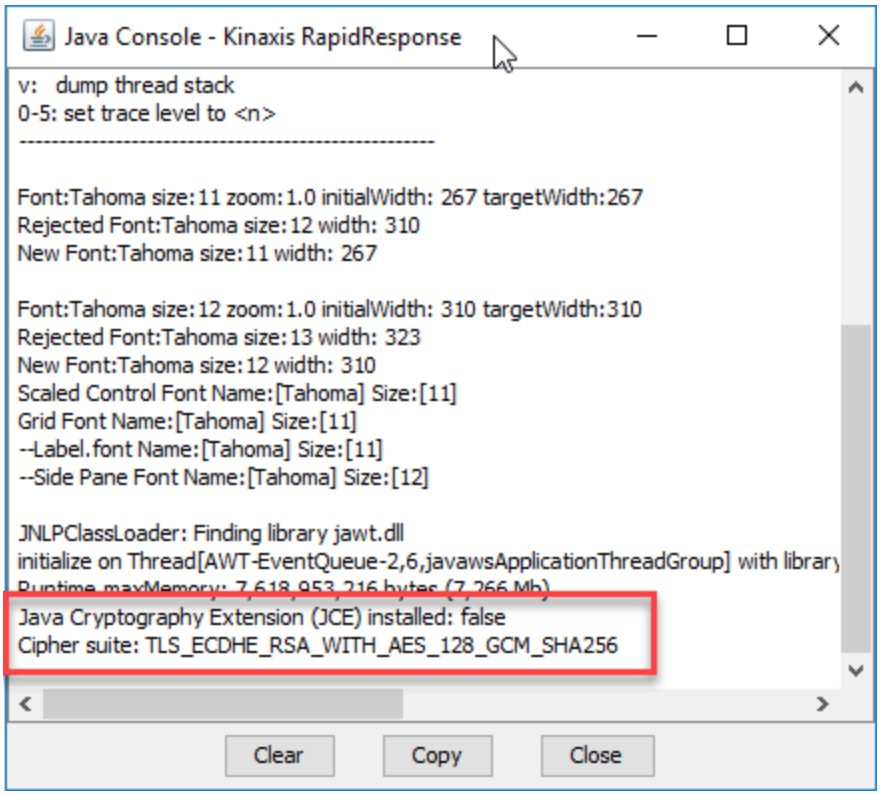
The HTTPS protocol provides secure and encrypted communication between RapidResponse users and the RapidResponse Data Center. All data transmitted between a RapidResponse client and the Data Center is encrypted using Transport Security Layer (TLS). Public key encryption that utilizes certificates from a trusted authority enables secure communication.

The HTTPS protocol provides secure and encrypted communication between RapidResponse users and RapidResponse Application Server. To secure communications, On-Premises RapidResponse administrators need to generate and install a certificate. For more information, see "To generate and install SSL certificates in Windows Server 2012 (IIS 8)" on page 126.

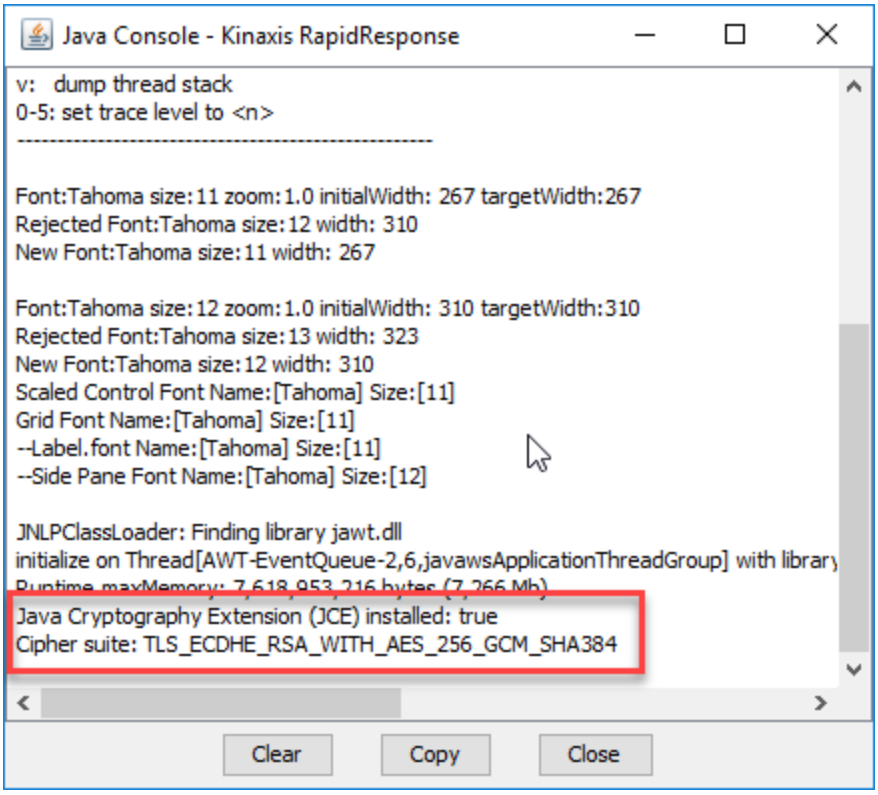
Java client support for 256-bit encryption

The default for the Java Client is 128-bit encryption. In order to use 256-cit encryption, the unlimited strength Java Cryptographic Extensions (JCE) need to be installed. JCE version 8 can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166

To validate that the Java client is connected at 256-bit after installing JCE, output the cipher information in the Java console as shown in the following illustrations:


Java Console - Kinaxis RapidResponse
v: dump thread stack
0-5: set trace level to <n>

Font:Tahoma size:11 zoom:1.0 initialWidth: 267 targetWidth:267
Rejected Font:Tahoma size:12 width: 310
New Font:Tahoma size:11 width: 267
Font:Tahoma size:12 zoom:1.0 initialWidth: 310 targetWidth:310
Rejected Font:Tahoma size:13 width: 323
New Font:Tahoma size:12 width: 310
Scaled Control Font Name:[Tahoma] Size:[11]
Grid Font Name:[Tahoma] Size:[11]
--Label.font Name:[Tahoma] Size:[11]
--Side Pane Font Name:[Tahoma] Size:[12]
JNLPClassLoader: Finding library jawt.dll
initialize on Thread[AWT-EventQueue-2,6,javawsApplicationThreadGroup] with library
Java Cryptography Extension (JCE) installed: false
Cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Clear
Copy
Close


Java Console - Kinaxis RapidResponse
v: dump thread stack
0-5: set trace level to <n>

Font:Tahoma size:11 zoom:1.0 initialWidth: 267 targetWidth:267
Rejected Font:Tahoma size:12 width: 310
New Font:Tahoma size:11 width: 267
Font:Tahoma size:12 zoom:1.0 initialWidth: 310 targetWidth:310
Rejected Font:Tahoma size:13 width: 323
New Font:Tahoma size:12 width: 310
Scaled Control Font Name:[Tahoma] Size:[11]
Grid Font Name:[Tahoma] Size:[11]
--Label.font Name:[Tahoma] Size:[11]
--Side Pane Font Name:[Tahoma] Size:[12]
JNLPClassLoader: Finding library jawt.dll
initialize on Thread[AWT-EventQueue-2,6,javawsApplicationThreadGroup] with library
Java Cryptography Extension (JCE) installed: true
Cipher suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Clear
Copy
Close

Password encryption

Passwords are encrypted and only the encrypted password is stored in the RapidResponse database. If a user forgets their password, an administrator can reset it to a new value.

User passwords are stored using a one-way salted hash based on a PBKDF2 (Password-Based Key Derivation Function 2)-compliant key using a HMAC-SHA256 scheme.

If your company chooses to use the SAML 2.0 Single Sign On capability, your company's authentication mechanism supersedes the user password management capability described above.

Changes in RapidResponse 2016.2

RapidResponse 2016.2 changed the algorithm used to hash passwords in the RapidResponse database from SHA1 to SHA256. Supporting SHA256 for password hashing aligns with industry best practices. When new passwords are created in RapidResponse 2016.2, SHA256 will be used. Upon upgrade to RapidResponse 2016.2, an existing password will remain hashed with SHA1 until the password is changed.

If your company's corporate security policies require the use of SHA256 for password hashes, consider changing or setting up the **Maximum password age** security policy to force users to change their password. For example, if you set this to 90 days, within three months all your users will be using passwords hashed with SHA256. For more information, see "Setting password security options" on page 648.

If you must immediately implement SHA256 for password hashes, contact Kinaxis Support for recommendations on re-hashing user passwords.

Password policies

User administrators have access to the following password policy options (maintained by the administrator, not Kinaxis):

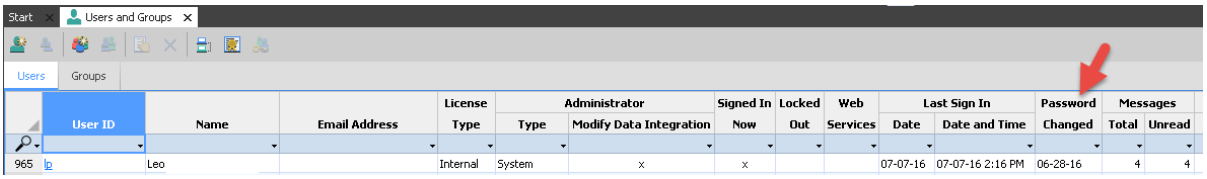
- User lock-out after a specified number of sign in attempts
- Automatic password expiry (force a password change after a specified number of days)
- Minimum password length
- Minimum password complexity
- Password re-use exclusions

For more information, see "Setting password security options" on page 648.

Password age

From the **Users** worksheet in the **User and Groups** workbook, you can review the last time a password was changed for a user. This information can be useful in better understanding password usage and policies. It could also be used in conjunction with the **Maximum password age** security policy.

You can create an alerts based on the **Users** worksheet. Consider creating an alert that reports passwords that exceed a date age threshold.



For more information, see "Setting password security options" on page 648.

Changes in RapidResponse 2016.2

The Password Changed column was introduced in RapidResponse 2016.2

User permissions and data visibility

RapidResponse includes administrative tools that restrict access to data to maintain data confidentiality and control over the type and extent of information accessed by users. RapidResponse administrators grant user permissions that are used to control access to tools and functionality including the ability to:

- Edit data and simulate business scenarios.
- Create resources to view and manipulate data.
- Share data with other users.

By controlling the user experience, RapidResponse administrators can limit what a user can see or do in the system ensuring users only have access to data for which they are responsible. For example, an administrator would provide different permissions to an internal user than she would provide to an external user such as a supplier or customer. For more information, see "Creating groups" on page 513.

Monitoring sign-in activities

Administrators can track and review information about sign-in activity in RapidResponse, which can be especially important if externally-based users, such as customers and suppliers, can access your RapidResponse system. The sign-in activities of users can potentially alert you to possible sign-in attempts by unauthorized users. For example, you can look for multiple failed sign-in attempts or sign-ins by users who you know are away from the office and not able to access the system.

Administrators can review:

- Unsuccessful sign-in attempts
- Unsuccessful sign-in attempts due to the use of invalid User IDs
- Successful sign-ins
- Users locked out of their accounts

For more information, see "Monitoring sign-in activities" on page 595.

Session expiry (time-out settings)

A user's RapidResponse session automatically expires if it is inactive for four hours (240 minutes). If this occurs, the user loses unsaved data and resource changes and will need to re-sign into RapidResponse. The default time setting can be changed. For more information about changing this setting, see "Changing the session expiry setting" on page 611.

RapidResponse Console administrative tool

The web-based RapidResponse Console is a multipurpose administration tool available to RapidResponse system administrators (On-Premises only) to assist in the management and monitoring of the RapidResponse system. This tool can be configured to use HTTPS instead of HTTP to secure communications. For more information, see "RapidResponse Console security settings" on page 237

Changes in RapidResponse 2016.2

As of version 2016.2, the RapidResponse Console supports secured authentication using HTTPS. By switching to HTTPS from HTTP, you can secure the connection between the RapidResponse Console (in a browser) and RapidResponse Server by encrypting all communication. For example, you might want to ensure user names and passwords are encrypted. Using HTTPS also encrypts all data transfers to the browser.

Session and cookie management

RapidResponse constructs and manages each RapidResponse session using a non-persistent cookie. Cookies are protected by:

- A 256-bit SHA-256 hash for validation (to prevent tampering)
- The cookie value is encrypted using a 256-bit AES key.

Phishing attacks and other malicious actions

Some messages that are sent from RapidResponse contain links to sign into the user's RapidResponse account. These links can help users quickly sign in, see the most up to date information, and take necessary actions. It is possible, however, that unauthorized third parties could attempt to steal RapidResponse account information using a phishing attack—an email message that is intended to look like it comes from your company's RapidResponse server, but directs the user to a fake instance of the RapidResponse sign-in page or another website that exists for the purpose of collecting account information.

If users have concerns about the authenticity of a RapidResponse message, they should not click any of its links. Instead, users should open their web browser and sign in to RapidResponse directly from there, or contact their RapidResponse administrator.

RapidResponse administrators should ensure their users are educated about phishing attacks and other malicious actions.

System auditing

RapidResponse includes several auditing tools that can be used by Kinaxis and customer administrators to better understand system and data changes and potential security issues.

Data change tracking

All user data changes applied to the RapidResponse Server database are logged including a user name and a timestamp. For more information, see "Data change tracking and record identification" on page 829.

Auditing system changes

Changes made in RapidResponse that can impact system security are logged in the Security Audit worksheet. Administrators can use the information reported in this worksheet to monitor the key security controls of your RapidResponse system and to perform security audits.

This worksheet logs the following types of changes:

- System configuration changes
- User changes
- Group changes
- Permission changes
- Resource dependency changes
- Profile variable changes

For more information, see "Security Audit worksheet" on page 430.

On-Demand service auditing

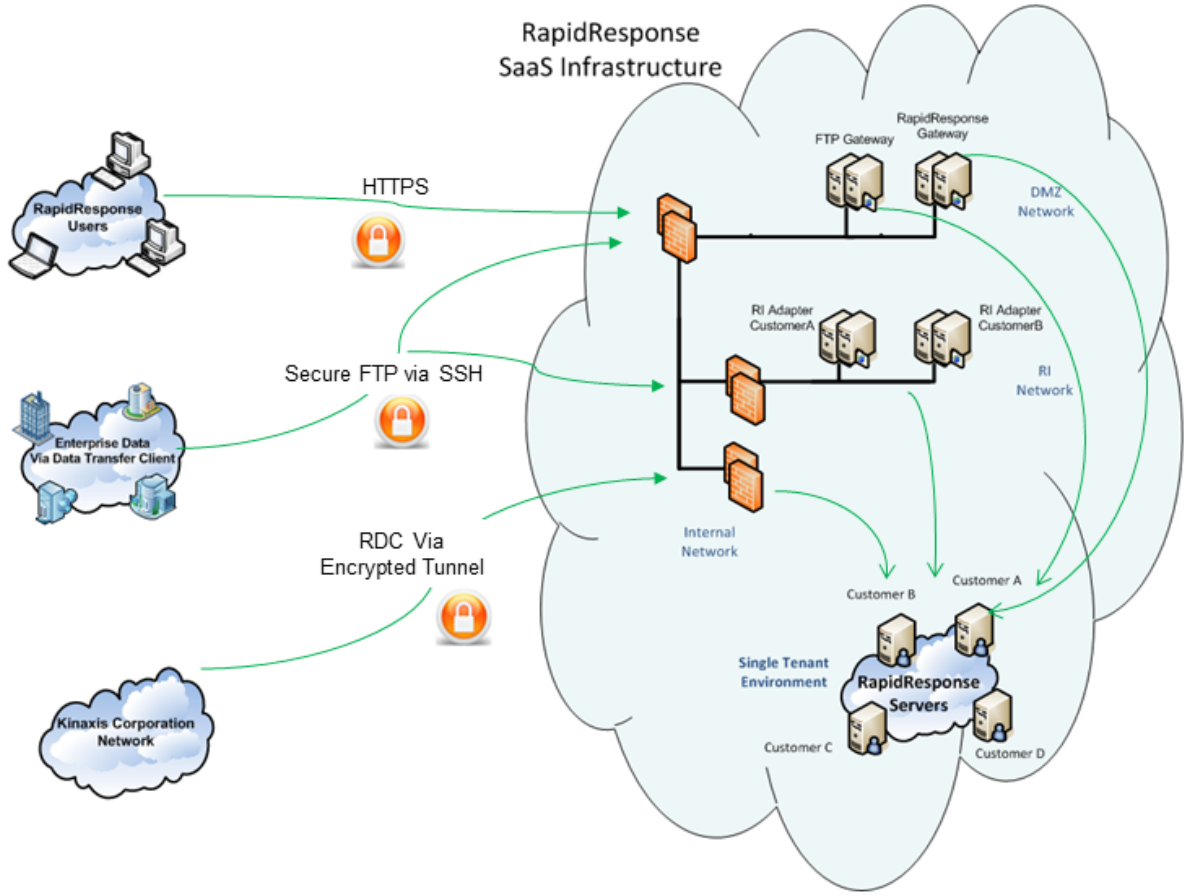
Server access, network access, firewall traffic, intrusion detection, system backup, FTP data traffic, system utilization and numerous application logs are regularly reviewed. Certain logs are collected and analyzed in an automated fashion and alerts are automatically generated for specific events.

On-Demand service infrastructure

RapidResponse is protected using a layered 'defense in depth' methodology. All traffic must traverse multiple firewalls, intrusion detection and prevention technology, and gateway servers. The entire infrastructure has been designed with security as a founding principle. This section describes the On-Demand service infrastructure.

All data is transmitted using the SFTP (SSH) protocol. It is immediately housed on a unique and dedicated customer environment. There are no shared database services whatsoever.

The following illustration represents the infrastructure.



ISP Service

The ISP service used by the On-Demand service has the following characteristics:

- Network-Based Route Optimization—Redundant, high speed connection to all major Internet backbones.
- Premise-Based Route Optimization—Flow control intelligently routes traffic flow for performance across multiple Network Service Provider links.
- Data traffic managed through private network access points

The hosting centers for this service provide highly reliable, highly scalable and high performance connectivity to the Internet. With around the clock monitoring of customer and infrastructure traffic, a scalable infrastructure and disciplined systems management of network elements, the centers provide multi-carrier Internet connectivity that eliminates the risk of single vendor network solutions.

Multiple high speed connections are (100 Mb cross connect) connected to the Internet via separate switch/routers. The connections have no single common point of failure. They enter the buildings through physically distinct telecommunications provider entrances. The ISP Service is monitored by separate network operation centers with 24x7x365 coverage.

Database Server Services

Database server services are provided by a proprietary in-memory database within the RapidResponse Server. Data (including user names and passwords) is stored in a dedicated RapidResponse Server database on a dedicated virtual server for each customer.

Data Storage Format

All customer data is stored within a RapidResponse Server database. In-memory and disk images of the database are synchronized in real-time.

Web client to RapidResponse Application Server communication

The communication between the web client and the RapidResponse Application Server (the web or application server) is through a combination of Web Services (SOAP/REST) and HTML over a secure HTTPS connection.

The RapidResponse clients (the Java client and the web client) are designed to be a light-weight clients that minimize the data is transferred (bandwidth used) over your network.

Java client considerations

The amount of data transferred from the Web server to a RapidResponse client over HTTPS (or HTTP) is dependent on how active a user is and the amount of data in the resources (dashboards, workbooks, scorecards, and so on) that they open.

For example, about 100 KB of data is transferred from the Web server to the client when signing in. However, the more resources the user has access to, the more data that is transferred.

Most operations use about 1 to 5 KB of data. Opening a worksheet is usually about 10 KB and another 10 KB for every 64 rows of data the user scrolls through. However, this is dependent on the number of columns. When a user is inactive, about 500 bytes of data are transferred every five minutes.

Web client considerations

RapidResponse users on the web client can access the RapidResponse system over Wi-Fi or over a wireless data connection (cellular). Although the web client is designed to be light-weight, user administrators should be aware of the data transfer considerations, especially over wireless data connections.

Here are some examples of data transfers when using the web client:

- The main page listing dashboards, scorecards, and forms (18 total in test) without thumbnails is about 4 MB.
- Dashboard thumbnails average about 0.3 MB.
- Each dashboard tab averages about 0.8 MB.

These are estimates are dependent on the number and complexity of dashboards, scorecards, and forms. You might want to test the data transfer of your own RapidResponse resources for more accurate estimates.

Encryption of communication between RapidResponse Server and RapidResponse Application Server

If RapidResponse Server (data server) and RapidResponse Application Server (web server) are not installed on the same computer, communication is facilitated using a network LAN connection. This communication between the two systems can be encrypted.

RapidResponse system administrator for On-Premises RapidResponse systems can control whether the communication on the network between RapidResponse Server and RapidResponse Application Server is encrypted. By default, it is not. For more information, see "Encrypting communication between RapidResponse Server and RapidResponse Application Server" on page 284.

Changes in RapidResponse 2016.2

RapidResponse 2016.2 introduced the ability to encrypt the communication between RapidResponse Server and RapidResponse Application Server.

Other infrastructure details

- The RapidResponse Application Server uses the .NET Common Language Runtime (CLR) which is a managed execution environment that contains specific safeguards against buffer overflows causing code execution.
- No security depends on hidden fields.
- All parameters are validated by the application.
- The service does not use SQL. The RapidResponse Server does not support execution of operating system level commands.
- The RapidResponse Application Server code is compiled and stripped of comments by the compiler. HTML comments are only used to document the third-party libraries included in the web client. This information is benign and available by examining the links themselves.

Data security in the On-Demand service

This section provides an overview of the security related to transferring data from enterprise system to the RapidResponse On-Demand service.

Data Transfer service

The bulk data transfer service encrypts all traffic using the SFTP (SSH) protocol. Data is transferred directly to a customer's data server and never touches down outside the double firewall architecture. This service is facilitated by installing and running a Kinaxis-supplied Data Transfer Client.

Real time data transaction services are provided through a messaging system which facilitates interaction between diverse operating systems and applications across internal and external networked computer systems.

Transferring data

A secure implementation is used to transfer data between the RapidResponse Data Transfer Client and the RapidResponse Data Center in order to both protect and ensure the integrity of your company's data.

All data transfers are done over connections secured using SFTP (SSH) and connections are encrypted using strong ciphers and 128 bit keys.

Once each extract file is transferred to the Data Center, its integrity on the FTP Server is verified to ensure the file was transferred accurately, and it is automatically retransmitted if necessary. For more information about transferring data, see the *RapidResponse Data Integration Guide*.

Systems used by the On-Demand service

This section describes the systems, tools, and applications used by the RapidResponse On-Demand service.

DNS Services

For redundancy purposes, the RapidResponse On-Demand service uses multiple Tier 1 DNS services with the following characteristics:

- Proprietary, industry-leading network platform
- Large global networks using BGP and IP Anycast
- Carrier-class, highly redundant network nodes
- 100 percent uptime service-level agreement
- Nameserver segmentation for greater security and protection from DDoS attack impact across the network
- Add-on dedicated resolvers and nameserver segmentation for increased performance and security
- DNSSEC and IPv6 compliant

Operating system baselines

All new equipment is loaded with tested and proven operating system baselines. These images contain hardened operating systems with all non-essential services disabled.

Operating system updates

Operating system updates related to security are reviewed as they become available and applied as needed after testing. Updates will be applied in a maintenance window unless the severity requires immediate attention.

System Redundancies

All equipment used to deliver the service, including load balancers, firewalls, gateways, switches is operated in redundant, n+1 architecture.

Backup services

The backup software used provides integrated automated backup, restore, archive, storage management, and business continuity functions. A database keeps track of all backups and where they are located.

Virus and malware protection

The On-Demand service uses on-access antivirus/malware detection with a central reporting and management infrastructure. Virus definition files are automatically distributed and enforced. Any non-compliant systems (due to out of date DAT or detected viruses) are automatically detected and remediated as part of a regular log review process. The application does not support the processing of incoming email. The application might send attachments but never with executable content. Data transfer functionality includes the refusal of file types that may exploit system vulnerabilities.

Intrusion prevention systems

The On-Demand service uses a sophisticated inline-IPS that scans all packets looking for unique signatures or patterns, and proactively detects and drops suspect traffic. The IPS signatures are regularly updated to ensure accuracy of detection and protection against zero-day exploits. Logs are regularly monitored and action taken when suspect traffic patterns are detected.

Firewalls and network security

Kinaxis leverages industry leading SSL Load balancers and firewall appliances to ensure that only legitimate traffic is serviced in a secure and efficient manner. Privacy of confidential data is secured at the network/firewall layer by restricting traffic on secure connections such as HTTPS for interactive users and encrypted SFTP (SSH) data transmissions for bulk file transfers.

Monitoring Services

All network devices, server hardware, services, performance counters, and most application processes, including end-to-end application tests, are monitored using dedicated monitoring software. Service accessibility and general responsiveness is also monitored and tracked by a separate monitoring service from locations around the world.

Communication Protocols

The following is a list of communications protocols used within the On-Demand service:

- External Internet Layer: HTTP, HTTPS, SFTP (SSH), and AS2 (HTTPS)
- Internal Network Layer: HTTP and HTTPS

All in-coming ports not required by the service are disabled

Changes in RapidResponse 2016.2

In RapidResponse 2015.3 (and earlier), the Internal Network Layer supported HTTP, TCP, RPC, and IPsec.

On-Demand service security policies and information

This section describes the security policies used by the RapidResponse On-Demand service.

Internal fraud protection

Kinaxis has the following procedures in place to protect against internal fraud:

- Employees have all signed and adhere to a code of conduct, including a non-disclosure agreement which protects the confidentiality of customer information and data.
- Access to the hosting environment (both physical and network) is restricted to the Service Operations team only.
- Kinaxis staff cannot access user passwords.

- System logs are monitored on a regular basis.
- Regular internal security reviews are performed.

Kinaxis hosting systems administration security

Kinaxis administrator access to each RapidResponse instance follows a strictly controlled group privileges methodology using a "minimum need to access" principle. Kinaxis administrator accounts/passwords follow these rules:

- User lock-out after a specified number of sign in attempts
- Automatic password expiry (force a password change after a specified number of days)
- Minimum password length
- Minimum password complexity
- Password re-use exclusions

Administration access is segmented into the following groups:

- Support Services
- Hosting Services

All administration activities are logged and all infrastructure modifications are documented and maintained in an asset management database.

Physical Security

Kinaxis has outsourced its data center requirements using a co-location model at multiple locations. Kinaxis owns and operates all equipment, and the service provider is responsible for physical security and environmental controls. Facility access is monitored by video surveillance and on-site personnel. Access to individual tenant cages is reliant on multiple factors, at least one being biometric. Access to the Data Center is limited to authorized personnel based on job function, and physical security access permissions are reviewed quarterly by Kinaxis management.

All the Kinaxis data center locations employ UPS power systems and generator backup, air conditioning systems, fire detection and suppression systems, and environmental monitoring and alert notification systems.

Key management

Keys such as SSH keys and SSL certificates passwords are stored in a network accessible Privileged Identity Management platform that supports high availability, auditing, and AES-256 bit encryption of all content at all times.

Security incident handling

Kinaxis has implemented a formal Security Incident Response Policy. Security incidents are detected and reported from various sources including employees, contractors, customers, Security Operations Center, business partners, and hosting providers as examples. Security incidents are tracked in an online system, classified based on severity and managed following a defined procedure. Customers are notified of security incidents that affect them or if there is action on their part to address a security related issue. Escalation procedures are in place to ensure incidents are handled within defined timelines. Security incidents reported from customers should follow the standard support process with appropriate prioritization based on the severity of the incident.

Data confidentiality

Customer data is treated as confidential in accordance with the executed non-disclosure agreement and/or the confidentiality obligations as stated in your RapidResponse SaaS Agreement.

Remote systems management

Remote systems management is enabled using VPN technology. VPN access to the hosting facilities must be approved by the Director of Global Support and is limited to designated Service Operations personnel.

Remote administration is performed using tools and commands designed for RapidResponse, over a secure VPN access, from secure machines.

Cross-site scripting

All content is validated and properly encoded by the client application before it is displayed to the end user. RapidResponse does not permit the end user to insert script code into any view.

Application requests always authenticated

Security is enforced by the application. With the exception of static content, every application request requires authentication. Static content is limited to the logon page, help, user guides, images, style sheets, and redistributable scripts and Java archives.

Other security policies

The following security policies are put in place for all On-Demand instances of RapidResponse:

- Third-party Security Incident and Event Management (SIEM) is always enabled for continuous log review and threat detection.
- Automated third-party network vulnerability scanning is scheduled regularly.
- Security policy documentation is included in Kinaxis service operations manuals and Kinaxis corporate policy documents.

On-Demand service operational policies

The following section describes the operational policies of the On-Demand RapidResponse service.

Hosting

Kinaxis has contracted with leading global providers of top tier data center services to provide the base level infrastructure for the RapidResponse On-Demand service.

In this model, the co-location partner provides:

- Hosting center resources and 24x7x365 physical security including continuously manned entrances requiring biometric scanners and secure badge access, 24-hour roaming and video surveillance with real-time monitoring
- Systems infrastructure (rack space, temperature/humidity controls, fire detection and suppression, consideration of earthquake and extreme weather events)
- Uninterruptible electrical power (redundant feeds) with generator backup
- State of the art HVAC with strict temperature and humidity ranges.
- VESDA very early smoke detection with pre-action dry-pipe water sprinkler systems in multi-zone configurations

In addition, Kinaxis has contracted with industry leading ISP providers to provide high-performance connectivity. The ISP partner provides:

- Multiple redundant (using separate data vaults) 100 Mb cross connects
- 7x24x365 Network Operations Center
- High performance, optimized network using up to eight different network service providers as well as private network access points.

Kinaxis provides:

- RapidResponse application provisioning
- RapidResponse application maintenance
- Data integration and synchronization services
- RapidResponse application monitoring including thresholds, logs and processes
- Remote on-demand service monitoring of availability and performance
- Customer support services including a 24x7x365 emergency call center
- Additional administration and change request services
- Public domain name services

- Online community for incident reporting and a knowledge base of key articles
  - Online documentation updates
  - Training services
  - Product discussion forum providing an opportunity for customers and Kinaxis employees to share ideas, best practices, and help each other achieve the greatest value from the service.
- Equipment provisioning
- Equipment maintenance
- Systems installation and configuration (servers, firewall, network, storage)
- Systems management (operating system provisioning and updates including security updates, virus and intrusion detection, vulnerability scanning, system backups, system and application monitoring, firewall and switch management)

Outage escalation

In the event of an outage, Service Operations personnel are alerted immediately. Further escalation to the Director, Global Support Services; Director, Infrastructure and Data Center Operations; SVP, Customer Success Operations occurs as required.

Outage tracking and reporting

Outage tracking and reporting are provided through a web based trouble ticket tracking system.

Data backup

Kinaxis leverages a number of backup technologies to ensure recoverability of customer data and meet recovery time objectives/recovery point objectives. Application backups begin with a native RapidResponse backup package creation process, followed by the use compression and AES-256 bit encryption, and finally replication of encrypted/compressed data to offsite location.

Backups are performed at least once every 24 hours and are retained for 30 calendar days. In addition, a monthly backup is retained for one year. No tapes are used.

Change management

Kinaxis has a formalized change management process in place which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The Service Operations management team meets regularly to review and schedule changes to the RapidResponse hosting environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Necessary approvals are obtained and documented as soon as possible.

Changes to infrastructure and software are developed and tested in a separate test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.

Kinaxis uses a standardized server build checklist to help secure its servers, as well as conducting monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with the Kinaxis patch management process.

Capacity planning

Server and network loading is constantly monitored to ensure that there is adequate capacity available to meet current and anticipated future demands. Additional resources are added as needed and where applicable.

Patch management

Kinaxis follows a patch management process that includes four major processes:

1. "Collecting Information", where announcements about security vulnerability are reviewed.
2. "Assessing Risks", where Kinaxis analyzes risks identified through the collected security vulnerability information.
3. "Applying the Security Update Program", where Kinaxis tests and apply the security up-date program.
4. "Monitoring the Result", where Kinaxis checks that all the necessary security update programs have been applied.

The Kinaxis On-Demand service leverages hardened OS images where only essential services are enabled. Patches that have been classified as critical and applicable to the service are applied during a scheduled maintenance window unless the severity requires immediate attention. Patches that have been assessed and deemed applicable but non-critical are applied quarterly or as part of the subsequent service pack install.

Certification

Kinaxis has completed a SSAE 16 SOC 2 examination of the RapidResponse On-Demand Service. This indicates that the selected processes, procedures and controls have been formally evaluated and tested by an independent accounting and auditing firm. The examination included the controls related to security monitoring, change management, service delivery, support services, backup and environmental controls, logical and physical access.

Quarterly service health check reports

Reports are generated for each customer every quarter which include:

1. Service Level Agreement performance,
2. Response time performance,
3. Average weekly user load,
4. Data integrity
5. Top accessed resources
6. Number of reports generated (User initiated/Alert initiated)

Disaster recovery

The standard objectives for recovery in the event of a disaster are:

- Recovery Point: 24 hours.
- Recovery Time: 24 hours.

Production site recovery methodology

The RapidResponse On-Demand service has deployed multiple geographically diverse alternate data centers.

Kinaxis performs remote data replication (disk to disk) of all encrypted production backup files between alternate sites. In the event of a disaster, all of the required virtual machines would be re-imaged with production information and production service re-stored. This recovery plan is reviewed and tested annually.

Scheduled system reviews

Systems utilization and numerous application logs are reviewed on a regular basis. The data center facility is monitored by an on-site command center on a 24x7x365 basis. Critical conditions result in the generation of an automated alert and immediate human engagement.

Application Instrumentation

Service availability is monitored using automated end to end tests through the Internet. All key sub-services are monitored on a regular basis using automated processes that include alert generation. The service availability and responsiveness are also continuously monitored by a separate secondary monitoring service with tests run from various representative geographic locations.

CHAPTER 6: International character set support

The RapidResponse visibility capabilities make global information distribution much more effective, allowing employees and business contacts in various locations to access data quickly. With RapidResponse, customers and suppliers across the globe can easily and securely access key data they require. Because you can deploy a single instance of RapidResponse to support your entire multinational company, RapidResponse needs to support international character sets.

RapidResponse database

Data is imported in RapidResponse using data files (text or Microsoft Excel files). The files can be in Unicode or coded format (single-byte and double-byte). Once the data is imported, it is converted into and stored as Unicode format.

RapidResponse client

Globally deploying RapidResponse in a multilingual environment is straightforward; RapidResponse Server supports one or more installations of RapidResponse Application Server. Users connect to a RapidResponse Application Server to access the RapidResponse client.

The RapidResponse client is a Java Web Start application (based on the Java Runtime Environment). The JRE fully supports Unicode formatting.

Data can be exported from the RapidResponse client into the local code page format or as Unicode.

RapidResponse administration

If you have deployed RapidResponse across countries that use different languages and character sets, you should be aware that across an entire RapidResponse system, only one font can be used as the default font for all printed reports (generated in PDF format). For information about setting a font, see "Configuring printed report settings" on page 643.

In addition, the locale that is set on the computer on which RapidResponse Server is installed affects the way RapidResponse Server handles data. For example, different locale settings have different methods of sorting query data. You can set a different locale for RapidResponse Server from the one specified on the computer on which RapidResponse Server is installed. For more information, see "RapidResponse locale settings" on page 281.

CHAPTER 7: New and changed in RapidResponse

2019 administration changes **67**
2018 administration changes **73**
2017 administration changes **82**
2016 administration changes **86**

This chapter outlines significant new features and enhancements to RapidResponse that should be reviewed by RapidResponse administrators. Data administrators should also review the *RapidResponse Data Integration Guide* for new and changed features.

There are similar chapters in other guides. For more information, see "Determining which help system or guide to use" on page 22.

Before the upgrade process is started, it is recommended you review the all the new and changed features included in the latest version of RapidResponse. You can learn more about the new features and changes included in RapidResponse from the *RapidResponse Release Summary Guide*.

This document is available for download from the Kinaxis Knowledge Network and summarizes the changes to RapidResponse. It contains a compilation of changes gathered from every RapidResponse guide and help system. It also contains lists of defects resolved in each version.

▸To access the *RapidResponse Release Summary Guide*

1. On the **Help** menu, click **Kinaxis Knowledge Network**.
2. Sign into the Kinaxis Knowledge Network.

   You can create a new Kinaxis Knowledge Network account if you do not have one. An account is required.
3. On the **Knowledge** menu, click **Documentation**.
4. Under **Release Summary Documents**, select a release to download the PDF document.

Tip: You can also find release summary content in the *Global Help* system.

2019 administration changes

The following 2019 releases include changes to RapidResponse administration:

- "Service Update 1904" on page 68
- "Service Update 1903" on page 69
- "Service Update 1902" on page 70
- "Service Update 1901" on page 71
- "Version 2016.2, Service Update 30" on page 71
- "Version 2016.2, Service Update 29" on page 72
- "Version 2016.2, Service Update 28" on page 72
- "Version 2016.2, Service Update 27" on page 72

Service Update 1904

Allowing users to edit historical data

If your company has business processes that require editing or inserting data in historical tables, you can now allow general users to edit this data. This replaces the previous behavior of only allowing administrators to edit historical data, and for processes that require historical data changes, allows the users who execute the process to modify the required data. For more information, see "Specifying whether historical data is editable" on page 637.

Automatic scenario deletion

If you are using the On-Demand RapidResponse Service or have configured a scenario deletion limit, you and the scenario owner can now be notified of scenarios that are approaching the deletion age. You can configure how many days before deletion the notifications are sent, and notifications are repeated every day until either the scenario is deleted or accessed.

Notifications include lists of all scenarios that are due to be deleted, and indicate in how many days the scenario will be deleted. For more information, see "Automatically deleting unused scenarios" on page 712.

Input field limits in tables

Tables are now limited to a maximum number of input fields. Very large tables can degrade performance when loading or working with data, and limiting the table size ensures tables contain the information needed but do not cause issues when running queries on that data.

This limit applies only to input fields, which are populated with data from your data sources or user action. Calculated, notes, and set fields are not affected.

If a table is larger than the limit, RapidResponse does not start. To prevent this, you should split very large tables into multiple related tables, and use references to keep records aligned between the tables. This can also improve your table design if the same field values are used for multiple records. For more information about data model design, see the *RapidResponse Data Integration Guide*.

This limit might cause issues if you have defined tables with more than 700 input fields. For more information, see "Post-update considerations" on page 154.

Service Update 1903

Running automation tasks

All alerts and scheduled tasks now run by executing queries using multi-threaded execution. This ensures all queries required for alerts and scheduled tasks execute using as many of the available CPU cores as possible. This improves performance by running each automation task using the available threads, and by running automation tasks concurrently by executing on different threads. This replaces the previous behavior of executing every scheduled automation task query on the same thread in sequence.

Scheduled automation tasks and automation tasks run interactively by users share the available threads, and a scheduler balances the threads so they are available to both types of automation tasks. This ensures interactive tasks have access to threads to perform their operations, and maintains threads to execute the scheduled automation tasks at the same time. Interactive queries are provided with more threads than scheduled queries, which ensures users' tasks do not wait for a scheduled query to complete.

RapidResponse 2016.2 Service Update 8 introduced an option in the alert and scheduled task properties to use multi-threaded execution for scheduled queries. Now that all automation tasks run with multi-threaded execution, the **Improve execution performance** check box is removed from the **Alert Properties** and **Scheduled Task Properties** dialog boxes.

For more information, see "Configuring RapidResponse Service Host" on page 234.

Because this affects how queries run, after applying this Service Update you should monitor CPU usage to determine if your alert queries are consuming excess resources. For more information, see "Monitoring CPU usage" on page 271

New license key for Self-Healing Supply Chain

Users of the Self-Healing Supply Chain will now require the SelfHealingSupplyChain license key. As of Service Update G1903, the SelfHealingLT license key has been deprecated.

For more information, see "Configuring Self-Healing Supply Chain resources" on page 792.

Support for Yields added to the Self-Healing Supply Chain automation

Users of the Self-Healing Supply Chain can now monitor and heal yield forecasts using the Self-Healing Supply Chain. Automation chains, control tables, users and groups have been updated to support both lead time and yield use cases.

- There are now three automation chains supporting the Self-Healing Supply Chain:
  - Self-Healing Common - performs common setup and triggers the lead time and yield automation chains.
  - Self-Healing Lead Time - performs the actions associated with healing lead time parameters.
  - Self-Healing Yield - performs the actions associated with healing yield parameters.
- The ML Lead Time User group has been renamed to **ML Self-Healing Users**.

For more information, see "Self-Healing Supply Chain automation tasks" on page 798, "Self-Healing Supply Chain control fields" on page 796, and "Self-Healing Supply Chain users and groups" on page 801.

Renamed scenarios to support the Self-Healing Supply Chain

The scenarios used by the Self-Healing Supply Chain have been renamed to better reflect their purpose:

- Approved Actions remains unchanged.
- SH Current Plan is now **Self-Healing Current Plan**.
- LT Upload is now **Self-Healing Upload**.
- LT Load is now **Self-Healing Load**.
- SH Current Performance is now **As Designed by Self-Healing**.
- SH Suggested Plan is now **As Demonstrated by Self-Healing**.
- SH Working Plan is now **Self-Healing Working Plan.**.

For more information, see "Self-Healing Supply Chain scenario structure" on page 793.

Service Update 1902

Accepted URLs for web service and server calls

Workbook definitions can contain web service and server calls, defined in the Advanced configuration using custom XML. New options in Global Settings limit the URLs that these calls can use, allowing only those that are included in the accepted lists. For more information, see "Allowing web service and server calls from workbooks" on page 744.

New method for deleting collaborations

A scripting method is now available for deleting collaborations. This method can be used by system and user administrators. For more information, see the *RapidResponse Scripting Guide*.

Locked automation resources

Now, when an alert, scheduled task, or automation chain is given to a different user, it is locked and cannot run until its owner or an administrator unlocks it. This new requirement helps to prevent automation resources from running using inappropriate permissions and data settings. If you are asked to unlock an automation resource, it is good practice to review the properties of the resource and consider the permissions of the resource owner before you unlock it.

For more information, see "Unlocking automation resources" on page 769.

Running automation tasks

Automation tasks that are run by multiple users now ensure each requested run is scheduled individually. This replaces the previous behavior of adding the automation task to the execution queue, which allowed only one user to run the automation task because the task could only be marked for execution once within the alerting service's polling interval. Each user's execution is now queued individually, which ensures each user runs the automation task as expected.

Service Update 1901

Version numbering

As of this version of RapidResponse, the version numbering now reflects which release number of the year the version is. This supports the continuous delivery of RapidResponse, and allows you to correlate the version number of your RapidResponse installation with the order of releases for that year.

For example, RapidResponse G1901 is the first release of 2019 using this version numbering.

The letter designation in the version number (G) is used to identify the major platform version.

Size limits on image uploads

To optimize system performance, RapidResponse now limits the size of images that users can upload to the image library. System administrators can adjust the size limits if necessary.

Images that are already in the image library are not affected by this change.

For more information, see "Changing image upload size limits" on page 660.

Server authentication

All communication between RapidResponse Server and each instance of RapidResponse Application Server is now authenticated using public and private keys. This improves security by ensuring only requests from registered and authenticated sources are processed.

RapidResponse Application Server instances are registered on installation, however, if you are using On-Premises RapidResponse, in some cases you might need to update the key or re-register a server. In this case, a utility is provided that you can run to create a new key for an Application Server. For more information, see "Authenticating RapidResponse Server" on page 239.

Version 2016.2, Service Update 30

Users warned about performance impact when deleting records

Users are now warned about the potential performance impact if they try to delete a very large number of records in a worksheet. They can choose whether to delete the records anyway or cancel the action. A new global setting allows system administrators to specify the number of records that a user must try to delete before being warned. For more information, see "Setting the record deletion warning threshold" on page 659.

New visibility into data quality

The Adoption Dashboard now tracks data with possible integrity issues. You can view the types of issues at each site or the total issues charted by site. For more information, see "Monitoring user adoption" on page 598.

Restarting RapidResponse services

When you restart RapidResponse Server, the Powershell command added in RapidResponse 2016.2 Service Update 28 is no longer required. The RapidResponse Server service now performs the operations the Powershell command was performing, and the service restarts without requiring additional processing. For more information, see "Stopping RapidResponse services" on page 229.

Version 2016.2, Service Update 29

Diagnostic files

For On-Premises RapidResponse, in the event of a RapidResponse Server crash, the limited dump file created for the diagnostic package is now generated within a specific time window. This ensures the limited dump file creation is completed within a predictable time window, and reduces the time RapidResponse Server is not accessible to users. If the time window expires before the file is complete, a partial file is created, which ensures you receive some information about the server state and the crash issue. For more information, see "Internal errors and system crashes" on page 244.

Version 2016.2, Service Update 28

Reporting changes to scheduled system tasks

Changes made to scheduled system tasks and the arguments passed to them are now reported in the Security Audit worksheet of the Administration Log workbook. This allows you to track changes to system tasks, including the change made and the user who made the change. For more information, see "Security Audit worksheet" on page 430.

Restarting RapidResponse services

For On-Premises RapidResponse, when you restart RapidResponse as part of a data model update or for scheduled maintenance, the RapidResponse service now restarts by executing a Powershell command that restarts the RapidResponse service. This replaces the previous behavior of using RapidResponse Server processes to stop, monitor, and restart the RapidResponse Server service. This reduces memory consumption by ensuring only one RapidResponse Server process is active at one time.

When you upgrade to RapidResponse 2016.2 Service Update 28, you must ensure Powershell command execution is permitted in your environment. Otherwise the restart process might not function as expected. For more information, see "Stopping RapidResponse services" on page 229.

Version 2016.2, Service Update 27

Reorganized permissions in User Properties and Group Properties

Over the years, the number of permissions that can be granted to users and groups has grown. To better display the expanded set of permissions, the User Properties and Group Properties dialog boxes have been reorganized.

- Authoring permissions, which were previously listed on the Permissions tab, have been moved to a new Authoring tab.
- The remaining permissions have been reorganized into categories that better describe the current set of permissions.

For more information, see "Assigning and removing permissions" on page 517.

Null references in data updates

When you bring data into RapidResponse using the DataUpdate or DataSynchronize command, you can now control how null and blank reference field values are handled during the data update or synchronization process. The new behavior requires every key field in the reference, both base fields and reference fields, to contain a null value for the reference to be considered null. This ensures references are interpreted correctly in the case the reference contains only reference key values.

Using the previous behavior, a reference was considered null if its base key field values were blank or null. To prevent this change from affecting your data or processes, the new behavior is used only if you enable it. For more information, see "Specifying how references are considered null" on page 401.

Using a proxy with the RapidResponse Log Service

Local Log Aggregator version 4.5 has been released. This new version allows logs to be forwarded from On Premises systems using an HTTP proxy. To make this possible, some changes have been made to the installation procedure. For more information, see "Installing the RapidResponse Log Service" on page 372.

2018 administration changes

The following 2018 releases include changes to RapidResponse administration:

- "Version 2016.2, Service Update 26" on page 74
- "Version 2016.2, Service Update 25" on page 76
- "Version 2016.2, Service Update 24" on page 76
- "Version 2016.2, Service Update 23" on page 76
- "Version 2016.2, Service Update 21" on page 76
- "Version 2016.2, Service Update 20" on page 78
- "Version 2016.2, Service Update 19.2" on page 79
- "Version 2016.2, Service Update 19" on page 79
- "Version 2016.2, Service Update 18" on page 80
- "Version 2016.2, Service Update 16" on page 81
- "Version 2016.2, Service Update 15" on page 82

Version 2016.2, Service Update 26

Changes to user licenses

A new type of user, named Light, has been added and the permissions available to Report users have changed.

Light users

Light users can sign in to RapidResponse and take any action that does not require a permission. They can also be given the following permissions:

- override the worksheet record limit
- use Message Center and the Start page.
- have passwords that never expire or cannot be changed.
- create private filters (static and expression-based).
- add users to collaborations.
- send resource links.
- edit data in shared scenarios.
- import data into scenarios.

For example, managers who do not create scenarios to edit data but need to view data and collaborate with others in RapidResponse can be Light users.

Report users

In Service Updates 21-25, Report users could send resource links and import data into scenarios. These two permissions can now only be granted to Light and Full users.

For more information about the user types, see "Understanding user accounts and license types" on page 539.

Upgrade behavior

Upon upgrade from RapidResponse 2016.2 Service update 20 or earlier, any External users are converted to Light users.

If you are upgrading from Service Update 21 through 25, any previously existing External users were converted to Report users in a previous upgrade, but there was no change in functionality. Upon upgrade to Service Update 26, these Report users are converted to Light users, and can now be granted more permissions.

The following table shows how license types have changed in recent service updates.

License Key Name (Visible to On-Premises customers in the License Keys list)	User License Type Label		
	Pre-Service Update 21	Service Updates 21-25	Service Update 26
NamedUserInternal	Internal	Full	Full
NamedUserExternal	External	Report	Light

License Key Name (Visible to On-Premises customers in the License Keys list)	User License Type Label		
	Pre-Service Update 21	Service Updates 21-25	Service Update 26
Report	N/A	N/A	Report
NamedUserAlert	Alert	Alert	Alert

To prevent External or Report users from accidentally gaining new permissions that you did not intend to give them when they are converted to Light users, these users remain in the External Users Group. If you want Light users to be able to create filters, send resource links, or add users to collaborations, grant the desired permissions to the External Users group first. Save your changes. This stops the group membership from actively preventing these users from having these permissions. If you do not want all members of the group to have these permissions, clear the check boxes for these permissions and save your changes again.

For information about user groups, see "Managing groups" on page 565.

Limiting access to names and contact information

You can now limit the visibility of users' names and contact information to selected users. This makes it possible for you to give someone access to a RapidResponse system without giving them access to the other users' personal information. For example, you can provide your suppliers with access to your RapidResponse system to collaborate and plan, without showing information that enables them to identify each other.

There are three visibility levels to choose from:

Visibility level	Can see information about
All (default)	All users
Limited	Users with the All visibility level
None	Self only

Upon upgrade, Light users (who might have been Report or External users before upgrade) are assigned a visibility level of None. Full or System users are assigned a visibility level of All. You can change a user's visibility level after the upgrade is complete.

For more information, see "Limiting visibility of user information" on page 556.

Security audit enhancements

Additional items are now recorded in the Security Audit worksheet, which allows you to monitor changes to currencies, data formats, resource tags, and data tolerance tests. New logging categories are available for each of these areas, and any changes are recorded along with the user that made the change. You can use this information to detect changes to the system and verify the change was legitimate. For more information, see "Security Audit worksheet" on page 430

Version 2016.2, Service Update 25

Email retry limits

If email messages cannot be sent from RapidResponse, the message is now retried for up to seven days. Messages that cannot be re-sent after this period are automatically deleted. This ensures that any email messages that are undeliverable are removed, and do not occupy excessive disk space. For more information, see "Configuring email support" on page 276.

Diagnostic files

For On-Premises RapidResponse, in the event of a RapidResponse Server crash, you can now retrieve registry settings for your RapidResponse Server as part of the diagnostic package. This information can assist with diagnosing problems, and can be provided to Kinaxis Customer Support to help reproduce issues. For more information, see "Internal errors and system crashes" on page 244.

Version 2016.2, Service Update 24

Multi-threaded queries for scheduled tasks that run scripts

System and data administrators can now reduce the execution time for scheduled tasks that run scripts. This is done by enabling the tasks to use multi-threaded queries.

For more information, see "Monitoring resource usage" on page 746.

Note: This option became available for some other types of automation tasks in Service Update 8.

Version 2016.2, Service Update 23

Scenario name change for the Self-Healing Supply Chain

A prefix has been added to the scenarios used by the Self-Healing Supply Chain (SH Current Plan, SH Suggested Plan, SH Current Performance, and SH Working Plan). If you are upgrading from an older version of RapidResponse, you will need to delete the Current Plan scenario and its children before applying the Self Healing Supply Chain.rpk file, and then run the ML Service User script after the upgrade to create the necessary scenarios.

Version 2016.2, Service Update 21

Version 2016.2, Renamed user license types

Two of the user license types have been renamed:

Old name	New name
Internal	Full
External (also known as Light Access)	Report

This change reflects the fact that users external to the organization that owns the RapidResponse system sometimes require extensive permissions, while some users within the organization might only need to use basic functions, such as viewing reports.

For more information about the user types, see "Understanding user accounts and license types" on page 539.

On upgrade, existing licenses are renamed, but continue to function the same way as they did in Service Update 20. A future service update will introduce a new user type.

Java 10 support

The Java client and the RapidResponse Application Server can now run using Oracle Java Runtime Environment (JRE) 8 or 10.

For more information, see "Java client requirements" on page 541 and "Java Runtime Environment (JRE)" on page 118.

Note: Users might see the following warning when they run the Java client using Java 10: `Java Web Start and Java Plug-in are deprecated and will be considered for removal in a future Java release. Please contact the developer of this content "Kinaxis Inc." and request an update for this program`. No action is required by users or administrators in response to this warning. RapidResponse is updated frequently and will be compatible with future versions of the Java Runtime Environment.

Installation and upgrade changes

If you are installing or upgrading RapidResponse components, the process now allows you to specify the components you want to install, and they are installed as a single operation. This replaces the previous behavior of requiring a separate installation program for each component. You can use this installation process to install RapidResponse Server and its required components, install RapidResponse Server and Application Server on the same computer, or install several applications in a single operation. For example, you can install the S&OP application, Inventory Manager application, and Engineering Change Manager in a single installation operation.

As the installation or upgrade process runs, you are prompted to specify options for components as required. Any options that are required by multiple components, such as the RapidResponse Server name, are required only once and reused for every additional component in the process that requires them.

For more information, see "RapidResponse installation process" on page 101 or "RapidResponse upgrade steps (On-Premises)" on page 150.

This new installation process no longer requires you to install the RapidResponse supplemental application components before installing the RapidResponse Application Server. These components are now automatically installed as part of the RapidResponse Server installation. However, if you are upgrading to RapidResponse 2016.2 Service Update 21 (or later) by applying a Service Update and have not upgraded RapidResponse server, you must separately upgrade the supplemental application

components and the RapidResponse ServiceHost service. For more information, see "Upgrading application components" on page 184 and "Upgrading the RapidResponse ServiceHost service" on page 185.

Configuring Self-Healing Supply Chain (On-Demand)

A machine learning service is deployed for the new Self-Healing Lead Time capability of the RapidResponse Self-Healing Supply Chain. The Self-Healing Lead Time capability introduces new resources that require specific configuration settings to automatically detect and correct inaccurate lead time assumptions. If you are using the Self-Healing Lead Time capability, you can modify application settings to better meet the needs of RapidResponse users.

For more information, see "Configuring Self-Healing Supply Chain resources" on page 792.

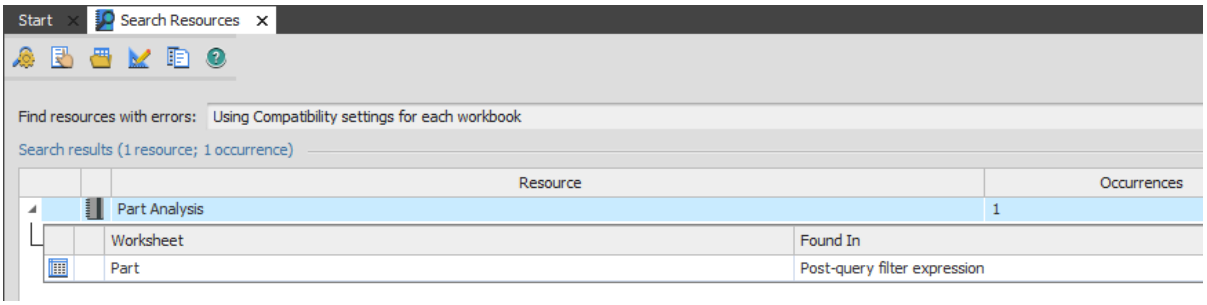
Version 2016.2, Service Update 20

Query expression encapsulation

Column and filter expressions are now automatically encapsulated, which provides more reliable error reporting and allows workbook authors to define columns that use other column expressions with fewer restrictions on how those columns must be positioned.

This change also limits support for worksheets that contain a post-query filter expression. Upon upgrading to Service Update 20, post-query filter expressions that return a Boolean value are encapsulated, and continue to perform the filtering they define. Expressions that do not return a Boolean value are used for extra processing of the result set, are no longer valid, and are reported as errors.

You can locate any worksheets that contain post-query filter expressions that do not return Boolean values by searching for resources that contain errors, as shown in the following illustration.



You must replace these expressions with a composite worksheet that performs the required filtering or processing to view data in the worksheet. For more information, see the *RapidResponse Resource Authoring Guide*.

For an example of an encapsulated query, see "Monitoring and canceling problematic queries " on page 603.

Warn workbook authors before discarding unsaved changes

By default, workbook authors are now warned of unsaved changes that might otherwise be accidentally discarded. This could occur if, for example, they click Cancel instead of Save after changing workbook properties.

This feature can be turned off. For more information, see "Turning unsaved workbook changes warning on or off" on page 668.

Version 2016.2, Service Update 19.2

Removal of maxRequestLength attribute from non-root Web.config

The **maxRequestLength** attribute in the **Web.config** file can be used to limit the size of files that can be imported into a scenario or uploaded for preview before inclusion in the data import process.

Previously, this attribute could be specified in **\Program Files\Kinaxis\RapidResponse\web\Web.config**, as well as in non-root **Web.config** files located in the following locations:

- Program Files\Kinaxis\RapidResponse\web\en\IntegrationModule
- Program Files\Kinaxis\RapidResponse\web\en\WorkbookModule\Extensions\Import

This created potential upgrade issues as if the attribute in these files was modified, it was then reset to its default value when installing a new service update (which could in turn impact certain import operations). As a result, support for this attribute has been removed from the non-root Web.config files in the two locations listed above. These files now always inherit their **maxRequestLength** attribute value from the **Web.config** file in **\Program Files\Kinaxis\RapidResponse\web**.

For information about how this attribute is used, see "Setting file size limits for importing data" on page 653.

Version 2016.2, Service Update 19

Preserving configurations on upgrade

When you perform a RapidResponse upgrade, either from version 2015.3 (or earlier) or by applying a Service Update, some of your configurations are now automatically preserved during the upgrade. This replaces the previous behavior of always resetting configurations to their default settings, and allows you to resume using RapidResponse more quickly after performing the upgrade.

The settings preserved depend on the version you are upgrading from and the configurations you have made. You might see any of the following:

- Custom email footers are now always preserved.
- When applying a Service Update, predefined user groups are not reset with their default resources and permissions.
- When applying a Service Update, the Application Server's web configuration is now preserved. For more information, see "Configuration file for Application Server" on page 162.

- When upgrading from RapidResponse 2015.3 or applying a Service Update, if you have configured the user account the RapidResponse ServiceHost service runs with, that user account is preserved.
- Customizations in your Internet Information Services (IIS) configurations are now always preserved.

Extending web client sign on credentials

You can now extend sign in durations for users on the web client. This enables users to remain signed in for longer and to easily open and close browser windows without having to re-sign into the client. For more information, see "Extending web client sign in durations" on page 612.

A new worksheet is available in the RapidResponse User Administration workbook to view and manage the tokens granted for these extended sign in durations. For more information, see "To view or delete authentication tokens" on page 613.

Changes to user license validation

Changes have been made to user license validation. Most RapidResponse systems will not behave differently as a result of this change. However, in systems with certain non-recommended configurations, upgrading to Version 2016.2 Service Update 19 might result in changes to permissions for external users. For more information about external user permissions, contact Kinaxis Customer Support.

Viewing user adoption metrics

You can now view user sign in activity and communications, and part and constraint responsibility assignments using the Adoption Dashboard. For more information, see "Monitoring user adoption" on page 598.

Version 2016.2, Service Update 18

Installing and upgrading application components

When you install or upgrade your RapidResponse instance, an additional installation program is provided, which provides namespaces and tables required for the applications your company uses. This allows you to upgrade the applications you use and the Application Server separately from upgrading your RapidResponse Server. This ensures you can update the applications or install Service Updates to correct issues, without requiring you to perform a full Server upgrade. For more information, see "Upgrading application components" on page 184.

Upgrading RapidResponse with Service Updates

Service Updates are used to correct issues and provide additional functionality between RapidResponse versions. These updates are now provided as upgrade programs, which streamlines the installation process and allows you to preserve settings between updates. This ensures your RapidResponse system functions identically after the update, and improves update time by not requiring you to re-apply your configurations.

In addition, Service Updates can now be applied separately to RapidResponse Server and RapidResponse Application server. This allows you to apply corrections and update applications without requiring a corresponding update on your RapidResponse Server, and ensures

For more information, see "Installing RapidResponse documentation resources" on page 121.

Documentation resources are no longer installed

When installing the On-Premises version of RapidResponse Server and RapidResponse Application Server, documentation resources (help systems and PDF files) are no longer installed. This change should not typically be noticeable to users as, by default, RapidResponse documentation resources are provided from an Internet location hosted by Kinaxis. This is the recommended configuration as it ensures access to continually updated information that reflects the latest product changes as well as corrective content.

However, if you have configured RapidResponse to always use these locally installed resources, or want to ensure users have access to RapidResponse documentation even when they lack Internet access, then you can download and manually install updated documentation and help. For more information, see "Upgrading application components" on page 184.

Importing scenarios in resource packages

You can now include shared scenarios in resource packages to enable easy migration between systems. This ensures that resources in the package have the scenarios they require and allows you to share multiple scenarios with users. For more information, see "Migrating RapidResponse resources" on page 752.

Monitoring memory consumption

You can now modify how often memory consumption alarms run to notify you of high or growing memory usage. This replaces the previous behavior of running the alarm once per day, and allows you to monitor your memory usage more closely by receiving notifications multiple times per day. For more information, see "Monitoring input data growth" on page 263.

Version 2016.2, Service Update 16

Password complexity requirements

You can now enforce more strict password complexity rules. Previously, password complexity required two types of characters: letters, numbers, or symbols. Now, you can enforce passwords that require four types of characters: upper-case letters, lower-case letters, numbers, and symbols.

When you upgrade to RapidResponse 2016 Service Update 16, your existing password complexity rule is applied, and you can select the new option. When you change the complexity rule, users can continue to use their existing passwords. The new rules are enforced the next time a user changes their password. For more information, see "Setting password security options" on page 648.

Granting user permissions

If you are a user administrator, you can now assign permissions that you do not have. This replaces the previous behavior of requiring you to have permissions to be able to assign them, and allows you to create users with the permission they require regardless of your own permissions. For example, if you do not have permission to create processes, you can now allow a user or group to create and share processes.

However, you can assign system administration permissions only if you are a system administrator.

For more information, see "Assigning and removing permissions" on page 517.

Performance Monitor Service available On-Premises

The Performance Monitor Service, which is used to monitor system performance and collect logs for archiving, is now available for On-Premises implementations of RapidResponse. It has long been included with On-Demand implementations.

You can install this service if you want Kinaxis Customer Support to have more information to help you resolve issues or if you want to be able to see additional information about your RapidResponse implementation on the Central Log Collector system.

For more information, see "Performance Monitor Service" on page 368.

Version 2016.2, Service Update 15

Enhanced resource permissions

System and user administrators are now able to grant author and administrative permissions to users that are not the resource owner. This gives non-owners the ability to check in and out, share, edit, and delete resources without being an administrator. For more information, see Managing groups and users.

Identifying missing scenarios in resource packages

Any missing scenarios required by a resource in a resource package are now identified when the resource package is imported. This ensures that all resources in the package work as expected for users. For more information, see "Identifying missing scenarios" on page 760

2017 administration changes

The following 2017 releases include changes to RapidResponse administration:

- "Version 2016.2, Service Update 14" on page 83
- "Version 2016.2, Service Update 13" on page 83
- "Version 2016.2, Service Update 12" on page 83
- "Version 2016.2, Service Update 11" on page 84
- "Version 2016.2, Service Update 10" on page 84
- "Version 2016.2, Service Update 9" on page 84
- "Version 2016.2, Service Update 8" on page 85
- "Version 2016.2, Service Update 7" on page 85
- "Version 2016.2, Service Update 6" on page 85
- "Version 2016.2, Service Update 5" on page 85

Version 2016.2, Service Update 14

Updated RapidResponse System Data workbook

The RapidResponse System Data workbook now includes additional worksheets. You can now use the workbook to report group membership details for users and groups, resource and permission details for users and groups, and resource usage details. For more information, see "RapidResponse System Data workbook" on page 486.

User accounts for accessing web services

A web service client can be used to execute queries in RapidResponse. Access to this capability is controlled by a new permission that is available only to web service user accounts. You can assign the permission to execute external queries to a single user to allow a web service client to update data records using the web service. For more information, see "Assigning and removing permissions" on page 517.

Version 2016.2, Service Update 13

RapidResponse system requirements

RapidResponse Server and RapidResponse Application Server now support Microsoft Windows Server 2016 (Standard and Datacenter editions). This new server includes many new features and enhancements. For more information, see "System requirements for RapidResponse" on page 104.

Version 2016.2, Service Update 12

Converting units of measure

You can now define conversion rates for units of measure, which allows you to view quantities in different units in workbooks. You can also define categories for measures, which allows you to define conversions between similar units at different scales, and ensure the units available in a workbook are compatible and produce meaningful results.

For more information, see "Configuring unit conversions" on page 695.

Single sign-in authentication

If you use a SAML2 single sign-in solution, the certificate signing component used by the single sign-in interface has been updated to improve security. However, if you sign authentication requests, the new certificate signing requirements are not compatible with signed certificates generated by the previous SAML2 configuration.

To continue to use SAML2 single sign-in, you must update the certificate signing algorthim using the `SSIConfig.exe` utility.

For more information, see "Updating a SAML2 configuration" on page 859.

Version 2016.2, Service Update 11

Users for single sign-in

If you have implemented a single sign-in (SSI) solution, you can now specify whether users are permitted to sign in only using SSI, or whether they are able to sign in with their user name and password. By allowing users to sign in only with SSI, you can ensure the user credentials are managed only by your SSI infrastructure, which can improve security by not allowing users to sign in as other users if their passwords are known.

If you allow a user to sign in only using SSI, you cannot specify the user's password, and the user cannot change their password in RapidResponse. For more information, see "Creating users" on page 548.

Version 2016.2, Service Update 10

Migrating user groups

You can now create user group packages to migrate user groups between instances of RapidResponse. For example, you can move a user group package from a test system to a production system. User group packages include the user groups and their permissions.

System and user administrators can migrate user groups, however it is recommended that system administrators manage the process. For more information, see "Migrating user groups" on page 677.

Version 2016.2, Service Update 9

RapidResponse maps

Configure access to the mapping service

RapidResponse maps are a new type of data visualization that display in workbooks and dashboards. For users in an On-Premises environment to view data in maps, access to the mapping service must be configured and a new license key for mapping has to be imported. For more information, see "Configuring RapidResponse maps" on page 811.

Geocodes

Geocodes are a new formatting option for string columns that display complete street addresses. The string value is converted to a set of latitude and longitude coordinates that can be used to identify precise locations on the map. Geocode columns are typically used to display manufacturing and distribution sites on a RapidResponse map. For more information, see "Configuring geocode data for maps" on page 813.

Version 2016.2, Service Update 8

Improve performance of automation tasks using multi-threaded queries

System and data administrators can now reduce the execution time for some automation tasks by enabling the tasks to use multi-threaded queries. This option is available for alerts and scheduled tasks that modify data.

For more information, see "Monitoring resource usage" on page 746.

Version 2016.2, Service Update 7

Server restart performance

When you restart the server after applying data model changes, your changes might be stored as a database DFS segment that contains only the modified tables, depending on the nature of the data model change. The database file is then copied into memory and used to apply the data model changes. This replaces the previous behavior of creating a copy of the entire database and reading it into memory to apply all data model changes, and can improve system performance when the server restarts. For more information, see "DFS folders" on page 312.

Version 2016.2, Service Update 6

Adding a scorecard to a resource package also adds metric workbooks

When you add a scorecard to a resource package, the metric workbooks required by the scorecard are now automatically included in the resource package as dependent resources.

Version 2016.2, Service Update 5

New library system workbook

The RapidResponse System Data workbook has been added and is available to system administrators. This workbook is a library system workbook that contains worksheets displaying data from system tables. For example, worksheets in this workbook expose system data such as scenario information, query history, data import and update logs, server operations and logs, user and group details, and user sign-in information.

The raw worksheets in this workbook can then be used by system administrators to build their own workbooks reporting details of system data as they best see fit. For example, formatting can be applied, columns can be moved or removed, and worksheet views can be joined in composites. The workbooks that system administrators create based on the data views provided in this workbook can then be shared to other users, both administrators or non-administrators.

Library workbooks can only be opened by the owner of the workbook, or an administrator, who also has library workbook authoring permission.

Note that the data presented in worksheets in the RapidResponse System Data workbook is not editable, and this workbook is provided only to allow creating custom views into your organization's system data.

For more information, see "RapidResponse System Data workbook" on page 486.

2016 administration changes

The following 2016 release includes changes to RapidResponse administration.

Note: Features that were added in versions of RapidResponse prior to 2016.2 are not included in this list of changes.

Version 2016.2 Initial release

Improved RapidResponse system performance

RapidResponse 2016.2 makes better use of existing multi-core and multi-CPU server hardware to improve the overall system performance of queries against the RapidResponse database. Internally, RapidResponse breaks queries into smaller chunks that can be run simultaneously against the existing server hardware.

With RapidResponse 2016.2, most query operations complete in less time. This should be noticeable to RapidResponse users of query-intensive resources. For example, most worksheets will open and recalculate faster than before.

Administrators do not need to make changes to their systems to take advantage of these improvements. However, system administrators (On-Premises) should continue to monitor their RapidResponse systems and determine when hardware such as CPU or system memory needs to be adjusted to accommodate higher loads. For more information about monitoring and managing your RapidResponse system, see "Query monitoring and management tools" on page 267and "RapidResponse system memory usage" on page 260.

The changes to query operations introduced two changes to RapidResponse system logging. A new line has been added to the Heartbeat section in the **Server.log** file and a new column has been added to the **QueryHistory.log** file named **QE3Status**. For more information, see "Heartbeat messages" on page 465 and " QueryHistory.log file" on page 474.

Data scalability improvements

The system memory utilization of RapidResponse 2016.2 has been improved. RapidResponse has now been tested on systems with 3 TB (3,072 GB) of system memory. RapidResponse 2015.3 and 2014.4 had only been tested to run with 2 TB (2,048 GB) of system memory. With this change, you can now load even more data into RapidResponse (provided your system supports the increased memory). This increased data capacity can create new opportunities for expanding the relevant application areas of RapidResponse across your business. To better understand input memory usage, see "RapidResponse system memory usage" on page 260.

In RapidResponse, each record in an input table has a unique identifier, known as a RecordId. Data scalability improvements in the RapidResponse Server have effectively removed limitations on the input records. In RapidResponse 2015.3 (and earlier) limited the RecordIds to 4 billion per input table. This limitation no longer applies in RapidResponse 2016.2. This increased data capacity can create new opportunities for expanding the relevant application areas of RapidResponse across your business. For more information about RecordId, see the *RapidResponse Resource Authoring Guide*.

Once an input table uses about 3 billion RecordIds, RapidResponse converts the internal storage addressing from 32-bit to 64-bit. This can result in a small increase in system memory usage. For more information about RecordIDs and their storage, see "RecordId usage" on page 467.

The size of your input data is still limited by your allocated system memory and your acceptable system performance levels. Extra input data can result in slower start up times as it takes longer to load the database. Depending on your system setup, extra data might also slow overall system performance.

If your company is using RapidResponse in an On-Premises setup, you might need to increase the system memory on the computer hosting the RapidResponse system to take advantage of this increased data capacity. Other hardware specifications might also need to be enhanced.

Read-only reference key fields

Reference key fields in tables can no longer have their values edited. This replaces the previous behavior of allowing processes to modify the values in reference keys, and ensures processes do not create duplicate records in tables.

Upon upgrading to RapidResponse 2016.2 (or later), a processing rule is inserted to allow the previous behavior to continue. However, you should replace any processes that modify the reference key fields, and then modify the processing rule to not allow the reference keys to be modified.

For more information, see "Specifying whether key reference fields are modifiable" on page 175 and "Testing workbooks for modifications to reference keys" on page 146.

Password encryption

Passwords are encrypted and only the encrypted password is stored in the RapidResponse database. RapidResponse 2016.2 changed the algorithm used to hash passwords in the RapidResponse database from PBKDF2-compliant key SHA1 to SHA256. Supporting SHA256 for password hashing aligns with industry best practices. When new passwords are created in RapidResponse 2016.2, SHA256 will be used. Upon upgrade to RapidResponse 2016.2, an existing password will remain hashed with SHA1 until the password is changed.

If your company's corporate security policies require the use of SHA256 for password hashes, consider changing or setting up the **Maximum password age** security policy to force users to change their password. For example, if you set this to 90 days, within three months all your users will be using passwords hashed with SHA256. For more information, see "Setting password security options" on page 648.

If you must immediately implement SHA256 for password hashes, contact Kinaxis Support for recommendations on re-hashing user passwords.

For more information, see "User security" on page 45.

TCP/IP ports changes and encryption for On-Premises RapidResponse

The RapidResponse Server is bound to a specific TCP/IP port and it must be open for inbound requests. RapidResponse Server uses this port to communicate with other RapidResponse components. The

default setting is port 14600. As of RapidResponse 2016.2, two other TCP/IP ports must also be opened for inbound requests on the computer where RapidResponse Server is installed. RapidResponse Server uses these port to communicate with RapidResponse Application Server. These two ports need to be 2 and 3 port numbers greater than the port number used by RapidResponse Server to communicate with other RapidResponse components. For example, if the port number is 14600 then you must also open 14602 and 14603 to inbound requests from RapidResponse Application Server. For more information, see "RapidResponse and TCP/IP ports" on page 283.

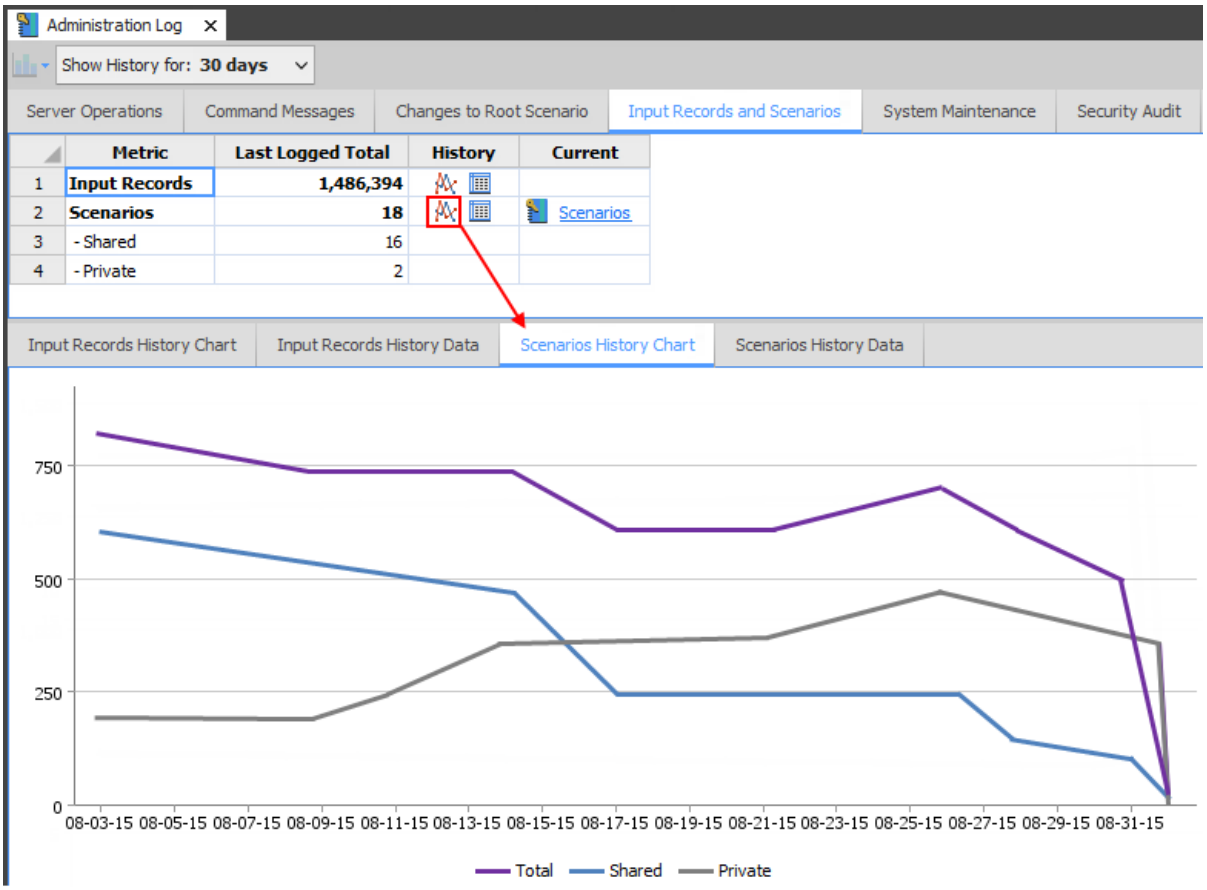
In a typical RapidResponse system, RapidResponse Application Server is not installed on the same computer as RapidResponse Server. It use a network LAN connection to communicate with RapidResponse Server. As of RapidResponse 2016.2, you can encrypt the communication between RapidResponse Server and RapidResponse Application Server to improve your internal network security. For more information, see "Encrypting communication between RapidResponse Server and RapidResponse Application Server" on page 284.

Maintain system performance with logging of data metrics

As input data grows, it consumes more system memory. An excessively large amount of input data can negatively impact system performance. Similarly, scenarios can contribute to excessive system memory usage. The new Input Records and Scenarios worksheet in the Administration Log workbook can help you maintain the performance of your RapidResponse system by logging the following metrics:

- The number of input records in data tables in the root scenario.
- The number of scenarios on your RapidResponse system. This includes shared and private scenarios.

The worksheet provides links to history worksheets, where you can view metric history as individual logged values or as a line chart. You can display up to approximately three years of metric history.



The metric totals are logged daily by the new Write Administration Metrics scheduled task, which must be configured before data is logged in this worksheet. For more information about generating metric data or the Input Records and Scenarios worksheet, see "Input Records and Scenarios worksheet" on page 425.

Additionally, the Scenarios workbook includes the new Scenario Metrics worksheet, which provides the same scenario data as the Input Records and Scenarios worksheet. For more information about the Scenarios workbook, see "Administrator tools for scenario management" on page 708.

Profile variable and macro changes logged in the Security Audit worksheet

The Security Audit worksheet in the Administration Log system workbook logs changes made in RapidResponse that can impact system security. This worksheet now logs profile variable and macro changes in addition to system configuration, user, group, permission, and resource dependency modifications.

Administration Log

Show: **Profile Variable Changes** | Description

Server Operations | Command Messages | Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit

	Date	Changed By		Type of Change	Description
		User ID	Name		
1	06-09-16 3:33 PM	tbrennan	Theo Brennan	User Variable	UserVariable Context=RapidResponse|Name=FulfillmentOrderLink|User=Order Fulfillment changed
2	06-09-16 3:33 PM	tbrennan	Theo Brennan	User Variable	UserVariable Context=RapidResponse|Name=FulfillmentOrderLink|User=Order Fulfillment changed
3	06-09-16 3:33 PM	tbrennan	Theo Brennan	User Variable	UserVariable Context=RapidResponse|Name=FulfillmentOrderLink|User=Order Fulfillment changed
4	06-09-16 3:33 PM	tbrennan	Theo Brennan	User Variable	UserVariable Context=RapidResponse|Name=FulfillmentOrderLink|User=Order Fulfillment added

Server Operations | Command Messages | Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit

	Date	Changed By		Type of Change	Description
		User ID	Name		
1	08-15-16 1:20 PM	rfox	Rachel Fox	Macro	Macro Name=MarketingFcst_EvaluationHorizonStart changed
2	08-15-16 1:19 PM	rfox	Rachel Fox	Macro	Macro Name=PlannedOrderAction3 deleted

For more information, see "Security Audit worksheet" on page 430.

If you are using an On-Premises RapidResponse system, profile variable and macro changes are also recorded in a text-based log file named **SecurityAudit.log**. For more information, see "SecurityAudit.log file" on page 477.

New version reclaim system command

RapidResponse 2016.2 introduces the VersionReclaimSweep command. This command is used to clean up the internal version structure used to support scenarios. The version reclaim process reduces the size the RapidResponse database and frees system memory. This command is similar to the VersionReclaim command that was no longer supported as of RapidResponse 2014.1.

When the VersionReclaimSweep command runs, it write-locks the RapidResponse database. As such, it should only be run during low user activity periods.

Before running this command, run the Condense command. For more information, see "Condense command" on page 387. It is also recommended that this command be run after upgrading RapidResponse to a newer version.

This command is not available to data administrators and it is not available in On-Demand RapidResponse systems.

A default scheduled system task is available for this command named **Version Reclaim Sweep**. By default, this task is not enabled. For more information, see "Predefined scheduled system tasks" on page 381.

For more information about this command, see "VersionReclaimSweep command" on page 411.

Improved security for the RapidResponse Console

The web-based RapidResponse Console is a multipurpose administration tool available to RapidResponse system administrators (On-Premises only) to assist in the management and monitoring of the RapidResponse system.

The RapidResponse Console now supports secured communication using HTTPS. By switching to HTTPS from HTTP, you can secure the connection between the RapidResponse Console (in a browser) and RapidResponse Server by encrypting all communication.

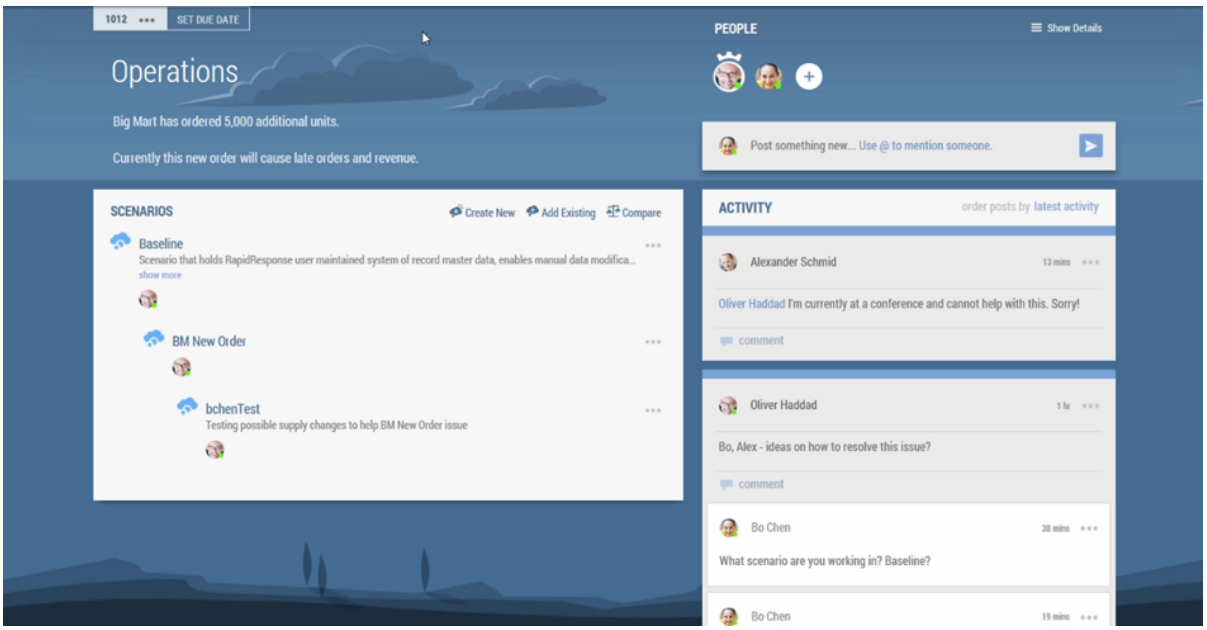
For more information, see "RapidResponse Console security settings" on page 237.

Archiving database and package files (On-Premises)

In addition to creating and storing backup copies of the RapidResponse database, you can now use RapidResponse to create an archive of the individual database files. By archiving database files, you can more easily rollback the database in case of a system failure or a corrupted database. The new archiving feature can also be used to create an archive of RapidResponse package files. This can help when rolling back your database or when troubleshooting and working with Kinaxis Customer Support. For more information about archiving, see "Archiving the RapidResponse database files" on page 324 and "Archiving RapidResponse package files" on page 252.

New way for users to collaborate

Users have a new way to collaborate in RapidResponse that allows them to communicate securely, share simulated data in scenarios, and compare solutions in a single interface. Adaptive Collaboration also allows users to include links to resources and annotated screenshots directly in the collaboration to provide more comprehensive details about the data and their proposed solutions. Available in both the Java client and the web client, collaborations have the same interface in both clients with some additional features available in the Java client.



On upgrade, all users have access to adaptive collaborations. The **Add users to collaborations** permission has been added and it controls whether a user can access to the entire RapidResponse user list and can add other users to collaborations. The permission is not enabled for users with External license types, however those external users can still participate in collaborations. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list. For more information about the External user type, see "Understanding user accounts and license types" on page 539. For more information about permissions, see "Assigning and removing permissions" on page 517.

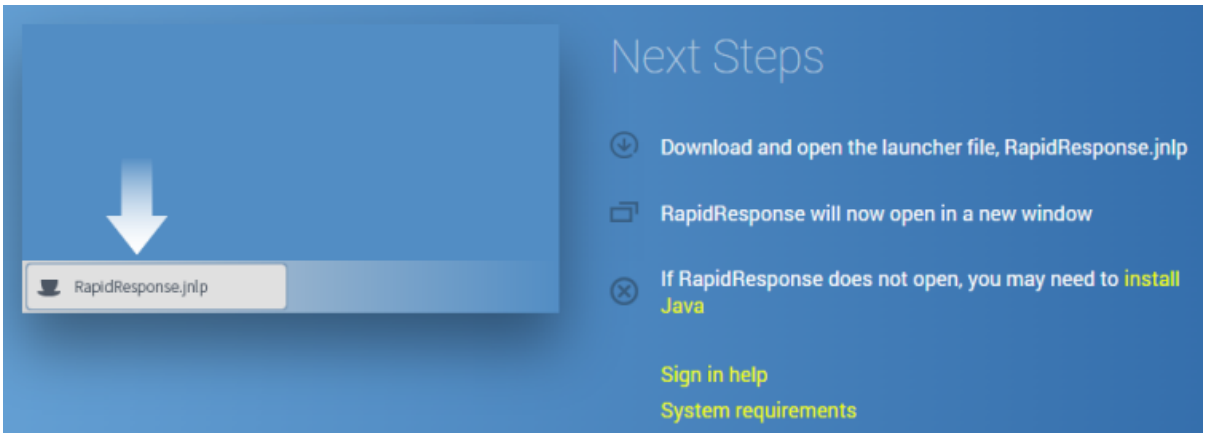
Users determine if other collaboration participants can modify or only view the data in collaboration scenarios. For more information, see "Scenario permissions in collaboration" on page 535.

Tracking collaborations

The Collaborations workbook, available to user and system administrators, tracks all open and archived collaborations in the system. From the Collaborations workbook you can open and view the collaborations and permanently delete all content in a collaboration. Scenarios and resources used in the collaboration are not deleted from the system and still remain accessible to users. For more information, see "Tracking and managing adaptive collaborations" on page 775.

A more user-friendly sign-in page

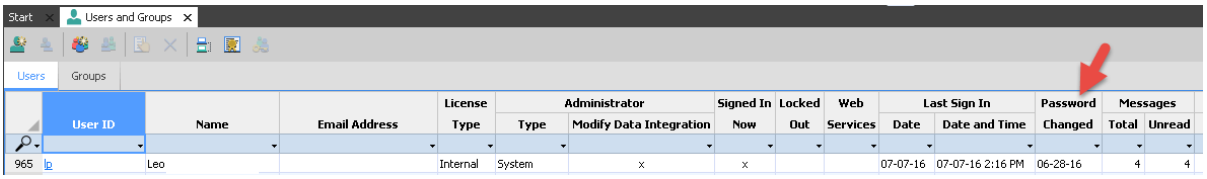
The RapidResponse sign-in page has been improved: it now provides browser-specific instructions to guide users through opening the JNLP file and launching the Java client. It also provides links that users might find useful: a link to download the latest version of Java, a link to more detailed sign-in help, and a link to RapidResponse system requirements.



For more information, see the *RapidResponse User Guide*.

Password changed information

The **Users** worksheet in the **User and Groups** workbook available to Administrators includes a new column that notes the last time a user's password was changed. Passwords can be changed by user administrators or by the user if they have permission to do so.



User ID	Name	Email Address	License Type	Administrator Type	Administrator Modify Data Integration	Signed In Now	Locked Out	Web Services	Last Sign In Date	Last Sign In Date and Time	Password Changed	Messages Total	Messages Unread
965 lo	Leo		Internal	System	x	x			07-07-16	07-07-16 2:16 PM	06-28-16	4	4

This information can be useful in better understanding password usage and policies. It could also be used in conjunction with the **Maximum password age** security policy.

You can create an alerts based on the **Users** worksheet. Consider creating an alert that reports passwords that exceed a date age threshold. For more information, see "Setting password security options" on page 648.

System requirement changes for Java client users

The Java client runs as a standalone Java Web Start application but is started from a Web browser and requires a supported Oracle Java Runtime Environment (JRE).

The Java client is now supported on Microsoft's newest operating system, Windows 10 (32-bit and 64-bit). In addition, RapidResponse can now be started using the Microsoft Edge browser.

Mac OS users can use theJava client with Mac OS X 10.11 (El Capitan) however Mac OS X 10.9 (Mavericks) is no longer supported.

It is strongly recommended that user systems have the latest service updates and patches applied to operating systems, browsers, and JREs to maintain system performance and security.

For more information, see "System requirements for users" on page 541.

System requirement changes for RapidResponse web client users

In addition to mobile devices, the web client can also be used with desktop browsers that support HTML5. RapidResponse 2016.2 now supports the Microsoft Edge browser.

For more information, see "System requirements for users" on page 541 and "Web client requirements" on page 547.

CHAPTER 8: Configuration changes managed by Kinaxis for On-Demand

This section applies to the On-Demand service only.

RapidResponse system settings 95
RapidResponse interface customization 96
RapidResponse data settings 96
Email server settings 96

In addition to the RapidResponse setup, configuration, and maintenance procedures outlined in this guide, additional configuration and maintenance services can be procured from Kinaxis Customer Support. This chapter outlines the services.

Note: If your company uses a RapidResponse test environment you have the same tools, functionality, and permissions as On-Premises RapidResponse administrators.

RapidResponse system settings

- Change system settings, such as the frequency with which RapidResponse data is updated or in-memory data is transferred to a permanent file.
- Change the limit of parts loaded into the Part control, which is available in some worksheets.
- Configure RapidResponse to automatically delete certain records after a specified period of time.
- Change the name of the Everyday calendar.
- Configure RapidResponse to export reports to a file location at the RapidResponse Data Center (from which they can subsequently be transferred to your company's network).
- Change the maximum file size of attachments in Message Center.
- Configure memory settings for users.
- Configure the expiry time for inactive sessions.
- Change the worksheet record limit.
- Configure single sign-in for users, which allows users to access RapidResponse without providing their user name and password. Single sign-in requires an identity provider that supports the SAML 2.0 SSO Web profile. You must work with Kinaxis Customer Support to integrate RapidResponse with your identity provider. For more information, see "Configuring single sign-in for On-Demand" on page 863.

RapidResponse interface customization

- Configure add-in applications that can be run from the Add-ins pane. For more information about add-in applications, see the *RapidResponse User Guide*.
- Add links to internal or external websites or external applications to the Extensions pane. For more information about the Extensions pane, see the *RapidResponse User Guide*. An interface to control users' access to the links can also be created.

RapidResponse data settings

- Change settings in control tables to determine how RapidResponse generates calculated data.
- Restart RapidResponse to add new tables to the RapidResponse data model or add fields to existing tables. These can be used to hold data that is not stored in the standard data model.
- Change the extract sources used to provide updated data for RapidResponse input tables.
- Specify an alternate data source to provide data for input tables.
- Save specified data during a data import. Typically, this is used for data maintained only in RapidResponse and not provided by the extract source.
- Add default records to input tables if needed to preserve referential integrity (for example, when mapping a fixed value to a reference field where the value is not found in the referenced table).
- Define an additional data source.
- Move integration settings from test servers to production.
- Restore data packages to roll back data model changes.
- Convert tables to contain vector data.

Email server settings

To prevent email messages sent by RapidResponse from being marked as spam, Kinaxis Customer Support might ask the following questions and discuss the following options with you:

- Does your email server use the Sender Policy Framework (SPF) to publish a list of trusted servers?
  If no, email messages sent from RapidResponse will not be marked as spam.
  If yes, continue to the next question.
- Can you add the Kinaxis mail server to the list of trusted servers?
  If yes, Kinaxis Customer Support will provide the mail server address.
  If no, continue to the next question.

Part 2: Installation for On-Premises

- "RapidResponse installation overview" on page 99
- "Installing RapidResponse Server" on page 109
- "Installing RapidResponse Application Server" on page 113
- "Installing RapidResponse applications" on page 129
- "Initial configuration steps" on page 137

CHAPTER 9: RapidResponse installation overview

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

This section applies to RapidResponse 2016.2 Service Update 21. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

RapidResponse application components 99
Data configuration 100
RapidResponse installation process 101
Overview of complete installation 102
System requirements for RapidResponse 104

This chapter describes the RapidResponse application components and outlines the general steps to install RapidResponse. These steps should be followed in the sequence noted. If you already have RapidResponse installed and want to upgrade, see"Part 3: Upgrading RapidResponse" on page 139.

RapidResponse application components

RapidResponse includes the following application components:

- **RapidResponse Server**—includes the analytics engine and a proprietary in-memory database that connects to a full range of enterprise applications, to perform multi-scenario what-if analyses on data. RapidResponse Server is installed before other RapidResponse components.

  RapidResponse Server is supported on 64-bit Intel Xeon computers. For more information about system requirements, see "RapidResponse Server" on page 104.

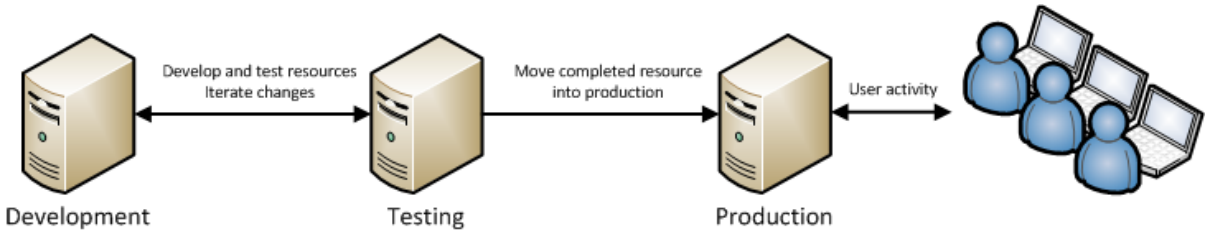
- **RapidResponse Application Server**—provides the client applications that RapidResponse users to sign into. RapidResponse Application Server is installed after RapidResponse Server and resides on a Web server on the same local area network as RapidResponse Server.

  RapidResponse Application Server resides on Web servers that support Microsoft Internet Information Services (IIS). Often, two instances of the application are installed. One instance is for internal network users on the intranet. The other is for external users (for example, a company's suppliers) who access RapidResponse over the Internet.

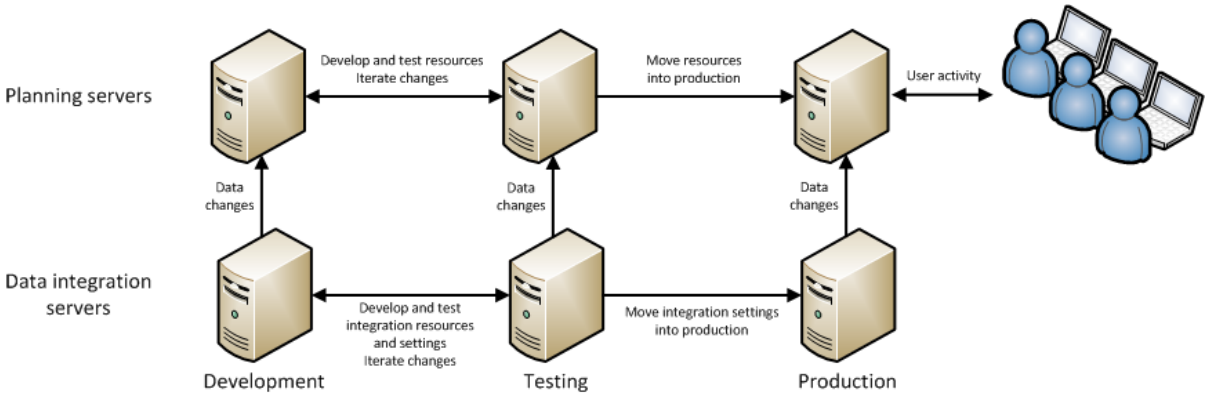
- **RapidResponse Data Integration Server**—a separate instance of RapidResponse Server and Application Server that is used only for performing data integrations. Another RapidResponse instance, called the planning server, must be provided for users to sign in to, and data from the data

integration server is periodically moved to the planning server. For more information, see the *RapidResponse Data Integration Guide*. This configuration is available only if one was configured for you, and is no longer a recommended configuration.

Depending on your requirements, you might require additional RapidResponse instances. For example, one RapidResponse instance could be provided for developing resources and processes, one for testing those resources, and a last for putting the resources into production. By using multiple systems for the development process, you can ensure the development and testing do not interfere with your operations.

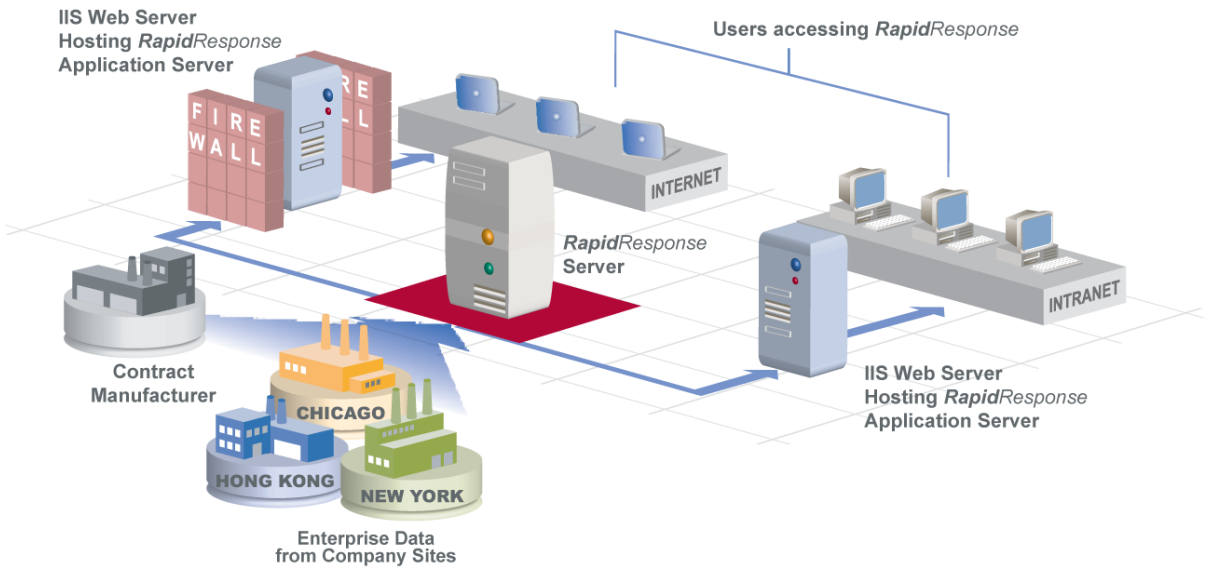


If you are using multiple servers in this way, you can allow external access only to the production server. As resources are developed and tested, you can make them available to both internal and external users. If you are have also been provided with a data integration server, you can use the multiple server configuration to create and test data integration settings before moving them into production. The development and test systems for the data integration server can also be used to perform data mappings to be used in the development and test systems for the planning server.



Data configuration

The following illustration shows data being imported from an enterprise data source, such as an ERP or MRP system, into the RapidResponse Server. Users can then connect to the data using a Web-based client through the RapidResponse Application Server.



RapidResponse installation process

You can install RapidResponse by either individually installing components, or by using the installation program to install each component in a single operation. The single installation operation installs all components on the same computer, and manages the individual components seamlessly. If you install components separately, you can install them on separate computers, and configure the connections between them. You can also install several components together on separate computers by running the installation process on each computer. This section assumes RapidResponse Server and RapidResponse Application Server are installed on separate computers.

The RapidResponse installation process has the following steps.

1. Install RapidResponse Server, supplemental components, and the ServiceHost service. For more information, see"Installing RapidResponse Server" on page 109.
2. Install RapidResponse Application Server. For more information, see "Installing RapidResponse Application Server" on page 113.
3. Sign in to RapidResponse and import license keys. For more information, see "Importing license keys" on page 124.
4. Install RapidResponse applications and predefined resources. For more information, see "Installing RapidResponse applications" on page 129.

After completing the installation process, review "Initial configuration steps" on page 137. You can also import data into RapidResponse provided that Kinaxis services has completed the data integration process.

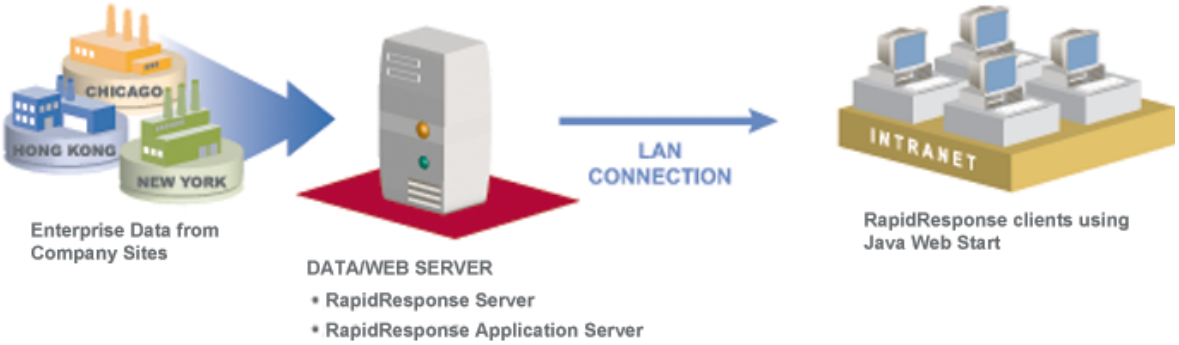
Note: For more information about RapidResponse applications, see "Installing RapidResponse applications" on page 130 and the *RapidResponse Applications Guide*.

Overview of complete installation

This section provides diagrams of various views of RapidResponse architecture. These diagrams are for illustration purposes only; your own installation architecture is dependent on your hardware, software, network, and security settings.

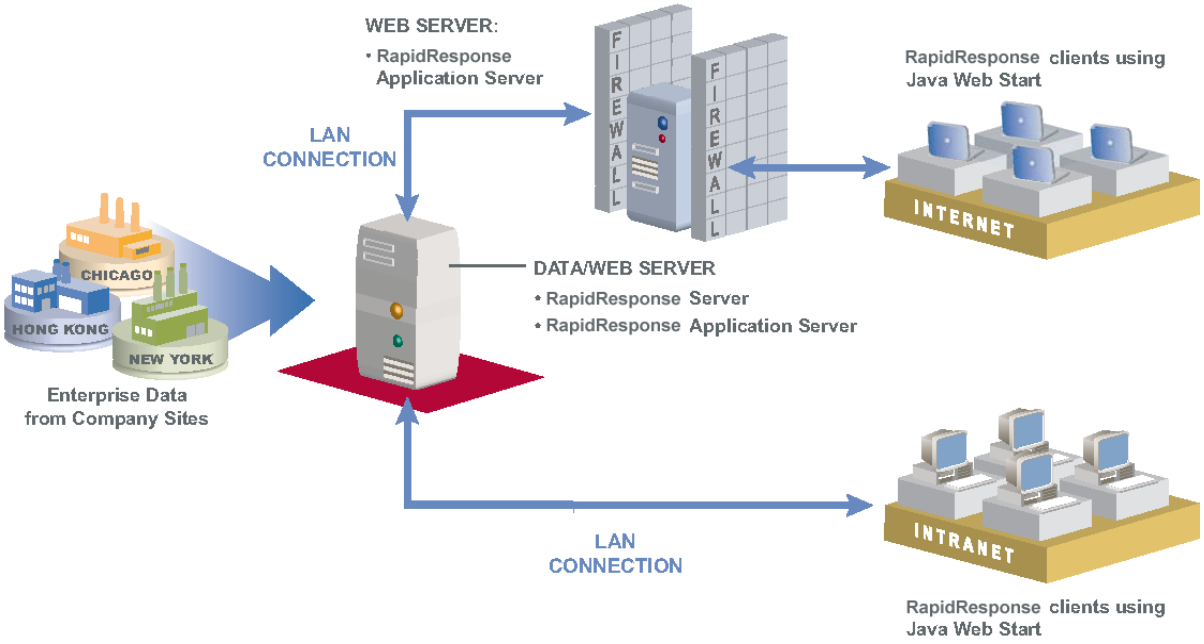
One instance of RapidResponse Application Server

In this diagram, RapidResponse Application Server is installed on the same computer as RapidResponse Server. This instance is used by internal RapidResponse users on the intranet. This configuration does not support users accessing RapidResponse from the Internet. Internet access to RapidResponse should only be provided when the Application Server is behind a firewall.



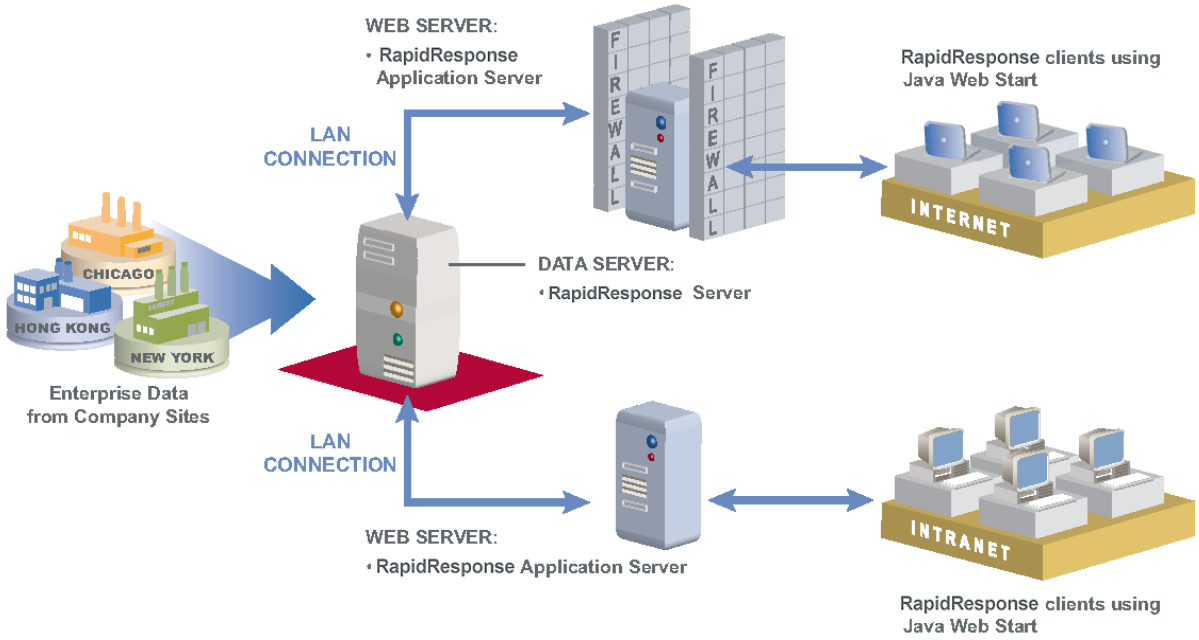
Two instances of RapidResponse Application Server

In this diagram, RapidResponse Application Server is installed on the same computer as RapidResponse Server. This instance is used by internal RapidResponse users on the intranet. The other instance is installed on a computer that provides firewall protection for users accessing RapidResponse from the Internet.



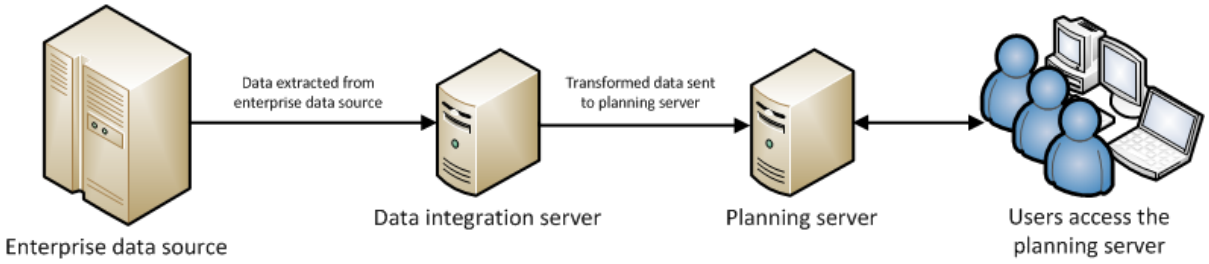
RapidResponse Application Server on two separate servers

In this diagram, RapidResponse Application Server is installed on two other computers; one outside the firewall and the other for internal users. Neither instance is with the same computer as RapidResponse Server and both servers have a LAN connection to RapidResponse Server. This configuration supports users accessing RapidResponse from the Internet.



RapidResponse data integration server

In this diagram, a RapidResponse data integration server is installed on one instance of RapidResponse Server and RapidResponse Application Server, and feeds data to a planning server, which is another instance of RapidResponse Server and RapidResponse Application Server that users sign in to.



System requirements for RapidResponse

This section outlines the system requirements and recommendations for the On-Premises RapidResponse. The requirements noted should be taken as minimum requirements. If you need assistance determining your system requirements, contact Kinaxis Customer Support. For more information, see "Customer Support" on page 19.

Overall system recommendations

This section describes the system requirements for the RapidResponse system. For RapidResponse client system requirements, see "System requirements for users" on page 541. The system requirements for the data integration applications and components are described in the *RapidResponse Data Integration Guide*.

RapidResponse Server

The minimum RapidResponse Server system requirements are described in the following table. However, your actual requirements depend on several factors including the size of your data and the number of users. Contact Kinaxis Customer Support for assistance in determining your actual system requirements. For more information, see "Customer Support" on page 19.

Requirement	Supported and Verified
Server/Processor	Intel® Xeon™ 64-bit, 4-way, 3.0 GHz (supporting Intel Extended Memory 64 Technology or EM64T)
Operating System	Microsoft Windows Server 2016 Standard with Desktop Experience Microsoft Windows Server 2016 Datacenter with Desktop Experience Microsoft Windows Server 2012 Standard (Server with a GUI) Microsoft Windows Server 2012 R2 Standard (Server with a GUI) Microsoft Windows Server 2012 Datacenter (Server with a GUI) Microsoft Windows Server 2012 R2 Datacenter (Server with a GUI) **Notes:** • In addition to the using the correct Windows Service Pack (SP), it is advisable that the operating system also include the latest Windows Updates. • RapidResponse does not support Server Core installations (no GUI). • Support for Microsoft Windows Server 2016 is available as of RapidResponse 2016.2 Service Update 13.
Operating system components	Microsoft .NET Framework 4.5 Microsoft .NET Framework 4.6.2 Microsoft Visual C++ Redistributable (x86) - 14.0.24215 Microsoft Visual C++ Redistributable (x64) - 14.0.24215 .NET Framework is usually included by default with the operating system. However, it is also included in the installation program or can also be downloaded from https://www.microsoft.com/net/download/framework.
System memory	8 GB RapidResponse has been tested on systems with 3 TB (3,072 GB) of system memory. To expand beyond 1 TB (1,024 GB) of system memory, contact Kinaxis Customer Support. For information about memory settings, see "RapidResponse system memory usage" on page 260.
Drive space	Three 36-GB disks It is recommended that RapidResponse Server be installed on a separate drive (physical) from the Windows operating system. It is also recommended that the default locations for the Dumps folder and the Packages folder be on different physical drives. In all, this configuration requires three physical drives.
Monitor	1024 x 768 minimum resolution

RapidResponse Application Server

RapidResponse Application Server must be installed on a server that includes a Web server. It can be installed on the same server where RapidResponse Server resides. However, before installing both applications on the same server contact Kinaxis Customer Support to discuss performance and memory issues.

You should also contact Customer Services for assistance in determining your actual system requirements. For more information, see "Customer Support" on page 19.

Requirement	Supported and Verified
Server/Processor	Intel Xeon 64-bit, 2-way, 3.0 GHz (supporting Intel Extended Memory 64 Technology or EM64T)
Operating System	Microsoft Windows Server 2016 Standard with Desktop Experience Microsoft Windows Server 2016 Datacenter with Desktop Experience Microsoft Windows Server 2012 Standard (Server with a GUI) Microsoft Windows Server 2012 R2 Standard (Server with a GUI) Microsoft Windows Server 2012 Datacenter (Server with a GUI) Microsoft Windows Server 2012 R2 Datacenter (Server with a GUI) **Note:** In addition to the using the correct Windows Service Pack (SP), it is advisable that the operating system also include the latest Windows Updates. **Note:** RapidResponse does not support Server Core installations (no GUI). **Note:** Support for Microsoft Windows Server 2016 is available as of RapidResponse 2016.2 Service Update 13.
Operating system components	Microsoft .NET Framework 4.5 Included in the installation program but can also be downloaded from http://msdn2.microsoft.com/en-us/netframework/default.aspx.
Java Runtime Environment (JRE) —64-bit version	Oracle Java Runtime Environment (JRE), version 8 or 10 (all updates) You can test the version of the JRE you are using by visiting http://www.java.com/en/download/help/testvm.xml. You can also download the latest version of the JRE by visiting http://www.java.com/en/. **Note:** To protect your system from potential security threats, it is recommended that you use an up-to-date version of JRE 8. As of 2019, updates to Java 8 require a maintenance contract with Oracle.
Physical memory	8 GB of RAM
Disk space	two 36-GB disks
Web Server	Microsoft Internet Information Services (IIS), Version 8 (and later)

Virtualization

RapidResponse supports virtualization technology from the leading provider, VMware, Inc.

By using virtualization technology, you can:

- Reduce your requirements and investments in server infrastructure. For example, you might not need to have dedicated standby equipment to support RapidResponse.
- Increase the utilization of existing hardware.
- Simplify backup and recovery procedures for RapidResponse.

RapidResponse Server and RapidResponse Application Server can be installed on an operating system that runs on VMware ESX Server 5.1, VMware vCenter 5.1, or VMware vSphere 5.5 and 6.0.

There are known memory allocation limits for virtual machines with specific versions of applications. Please ensure your VMware version is capable of supporting the memory requirements for your RapidResponse configuration.

For more information about virtualization, visit www.vmware.com.

CHAPTER 10: Installing RapidResponse Server

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

This section applies to RapidResponse 2016.2 Service Update 21. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

Preparing to install RapidResponse Server 109
Installing RapidResponse Server 111
Uninstalling RapidResponse Server 112

RapidResponse Server includes the analytics engine and a proprietary in-memory database that connects to a full range of enterprise applications, to perform multi-scenario what-if analyses on data. RapidResponse Server is installed before other RapidResponse application components.

This chapter explains how to install RapidResponse Server for the first time or on a different server. Included is a description of how to install, set up, and uninstall the RapidResponse Server.

The RapidResponse DVD (or the RapidResponse installation image) includes the RapidResponse Server installation program. An easy-to-use setup wizard leads you through the installation process.

Preparing to install RapidResponse Server

You should prepare before installing RapidResponse Server. To prepare, you will need to verify some RapidResponse configuration items and be able to provide this information. This section outlines how to prepare for installing RapidResponse Server.

System requirements

Confirm that the computer where RapidResponse Server will be installed meets the minimum system requirements.

It is recommended that more than one physical drive be available. RapidResponse Server should be installed on a separate drive (physical) from the Windows operating system. A third physical drive should be used for data backups and diagnostic files to improve system performance.

If you need assistance determining the appropriate hardware configuration for your enterprise, contact Kinaxis Customer Support. For more information, see "System requirements for RapidResponse" on page 104.

It is recommended that more than one physical drive be available. RapidResponse Server should be installed on a separate drive (physical) from the Windows operating system.

Installation license key (serial) number

An installation license key is required to install RapidResponse Server. Kinaxis Customer Support provides you this key.

TCP/IP ports and RapidResponse Server

The RapidResponse Server is bound to a specific TCP/IP port and it must be open for inbound requests. RapidResponse Server uses this port to communicate with other RapidResponse components.

A default port number (14600) is provided during the RapidResponse Server installation program. You have the option of choosing an alternative port number between 1024 and 65535. This port cannot already be assigned.

Before installing RapidResponse Application Server, two other TCP/IP ports must also be opened for inbound requests on the computer where RapidResponse Server is installed. RapidResponse Server uses these port to communicate with RapidResponse Application Server. These two ports need to be 2 and 3 port numbers greater than the port number used by RapidResponse Server to communicate with other RapidResponse components. For example, if the port number is 14600 then you must also open 14602 and 14603 to inbound requests from RapidResponse Application Server.

You can also change the port number after you install RapidResponse Server. For more information, see "RapidResponse and TCP/IP ports" on page 283.

Using a specific port number provides enhanced security for those installations that need to access RapidResponse Server through a firewall.

Failover cluster configuration

RapidResponse Server failover clustering is an optional capability that is designed to reduce system downtime when RapidResponse Server is stopped for maintenance or crashes unexpectedly.

To help improve system availability, consider deploying the optional failover cluster configuration for your RapidResponse system. When a scheduled or unscheduled RapidResponse Server outage occurs, a second server (a standby) automatically takes over from the active server. The two servers share the same RapidResponse database.

After RapidResponse Server has been installed and the data integration tasks have been completed, consider deploying the failover cluster configuration. If you have configured a separate data integration server, the folders that are shared between the servers in the failover cluster must be configured to be updated by the data integration server.

For more information, see "RapidResponse Server failover clustering" on page 289.

Installing RapidResponse Server

The following procedure outlines the steps necessary for a successful installation of RapidResponse Server.

▸To install RapidResponse Server

1. Log on as a Windows Server administrator on the computer where RapidResponse Server will be installed, and then in the RapidResponse installation image, double-click the **EasyInstaller.exe** file.
2. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
3. Click **Next**.
4. On the **Customize** tab, do the following:
   - Ensure the **RapidResponse Server** check box is selected.
   - Clear the **RapidResponse Application Server** check box.
     If you are installing RapidResponse Server and RapidResponse Application Server on the same computer, leave this check box selected.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
5. If you are prompted to install required software components (such as RapidResponse OpenAPI, Windows Installer, and Microsoft Visual C++ components), click **Install** and follow the subsequent installation instructions. You might be then prompted to restart the computer. If so, you will need to restart the installation program. If not, go to the next step.
6. Review the information on the **Welcome** screen and click **Next**.
7. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
8. On the **Customer Information** screen, do the following:
   - Type your name and the name of your company in the appropriate boxes.
   - Type the serial number exactly as provided by Kinaxis Customer Support.
   - Click **Next**.
9. On the **Port Numbers** screen, type a TCP/IP port number for the RapidResponse Server or accept the default value (14600) and then click **Next**. The RapidResponse Server is bound to a specific port and it must be open for inbound requests other RapidResponse components. For more information, see "TCP/IP ports and RapidResponse Server" on page 110.

   The port number must be between 1024 and 65535 and cannot already be assigned. The port number can be modified after the installation is complete. For more information, see "RapidResponse and TCP/IP ports" on page 283.
10. On the **Destination Folder** screen, choose the location where you want to install RapidResponse Server or accept the default.

    It is recommended that RapidResponse Server be installed on a separate drive (physical) from the Windows operating system.
11. On the **Database Folder** screen, specify the location where the RapidResponse database files will be stored or accept the default location of **C:\RapidResponse\Data**. Click **Next**.

    The folder name chosen on this screen will have the **\Data** sub-folder appended to it. For example, **C:\RapidResponse\Data.**

If you are running virus-scanning applications on the computer where the RapidResponse database is stored, ensure the database folder is excluded from the virus scan operation. Scanning the database folder can result in file locks being placed on RapidResponse database files.

After RapidResponse Server installation, you can change the Data storage folder. For more information, see "Location of stored database files" on page 310.

12. On the **Select Program Folder** screen, you can either accept the suggested folder name, type a new folder name, or select one from the **Existing Folders** list. Click **Next**.
13. Click **Install** to start the installation.
14. When the components are done installing, click **Next**.
15. If any components failed to install, click **Open Log File** to review the errors.
16. Click **Finish**.
17. If the **Restart Windows** screen displays, select an option and click **Finish**.

Uninstalling RapidResponse Server

If you no longer want to use RapidResponse Server on a specific computer, you can uninstall it. If you want to use RapidResponse Server again on the same server, you must re-install from the RapidResponse DVD or the RapidResponse installation image.

The RapidResponse Server uninstall program doesn't remove data or RapidResponse resources. This information is preserved in the **C:\RapidResponse\Data** folder.

▸To uninstall RapidResponse Server

1. Stop the RapidResponse Server service. Sign into RapidResponse Console. For more information, see "To sign in to RapidResponse Console" on page 230.
2. Click the **Actions** menu.
3. Click **Stop Service**.
4. Stop all other RapidResponse services from the **Windows Services** dialog box. This includes RapidResponse Server Monitor, RapidResponse Service Host, and RapidResponse Utility Server.

   For more information about RapidResponse services, see "RapidResponse Windows Services" on page 227.

   - In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
   - Click a RapidResponse service name. For example, **RapidResponse Service Host**.
   - On the **General** menu, click **Pause** (if available) and then click **Stop**. Repeat this step for each RapidResponse service.
5. In the Microsoft Windows Control Panel, double-click **Add or Remove Programs**.
6. In the **Currently Installed Programs** window, choose **Kinaxis RapidResponse Server**, and click the **Change/Remove** button.
7. Click **Yes** to confirm your choice.
8. When the uninstall is complete, click **OK**.

CHAPTER 11: Installing RapidResponse Application Server

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

This section applies to RapidResponse 2016.2 Service Update 21. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

Preparing to install RapidResponse Application Server 114
Installing RapidResponse Application Server 118
RapidResponse Application Server post-installation procedures 120
Testing the RapidResponse installation 122
Importing license keys 124
RapidResponse Application Server folder structure 124
Providing external access to RapidResponse 125
Uninstalling RapidResponse Application Server 127

RapidResponse Application Server provides the clients that RapidResponse users sign into. Users can sign into the Java client or the HTML5-based web client.

RapidResponse Application Server is installed after RapidResponse Server and resides on a Web server on the same local area network as RapidResponse Server.

RapidResponse Application Server can be installed on more than one Web server computer. Each instance can connect with a common RapidResponse Server. For example, you might want to install RapidResponse Application Server on a Web server computer for intranet users and on another Web server computer for Internet users.

This chapter describes how to install RapidResponse Application Server for the first time (or on a different server). Included is a description of how to prepare, set up, and uninstall RapidResponse Application Server. An easy-to-use setup wizard leads you through the installation process.

If you're upgrading RapidResponse Application Server, skip this chapter and see "Upgrading RapidResponse Application Server" on page 189.

Preparing to install RapidResponse Application Server

You should prepare before installing RapidResponse Application Server. To prepare, you will need to verify some RapidResponse configuration items and be able to provide information. This section outlines how to prepare for installing Application Server.

Windows Server 2012 settings

RapidResponse Application Server is installed on a computer running Windows Server 2012. This computer must meet the minimum system requirements. For more information, see "System requirements for RapidResponse" on page 104.

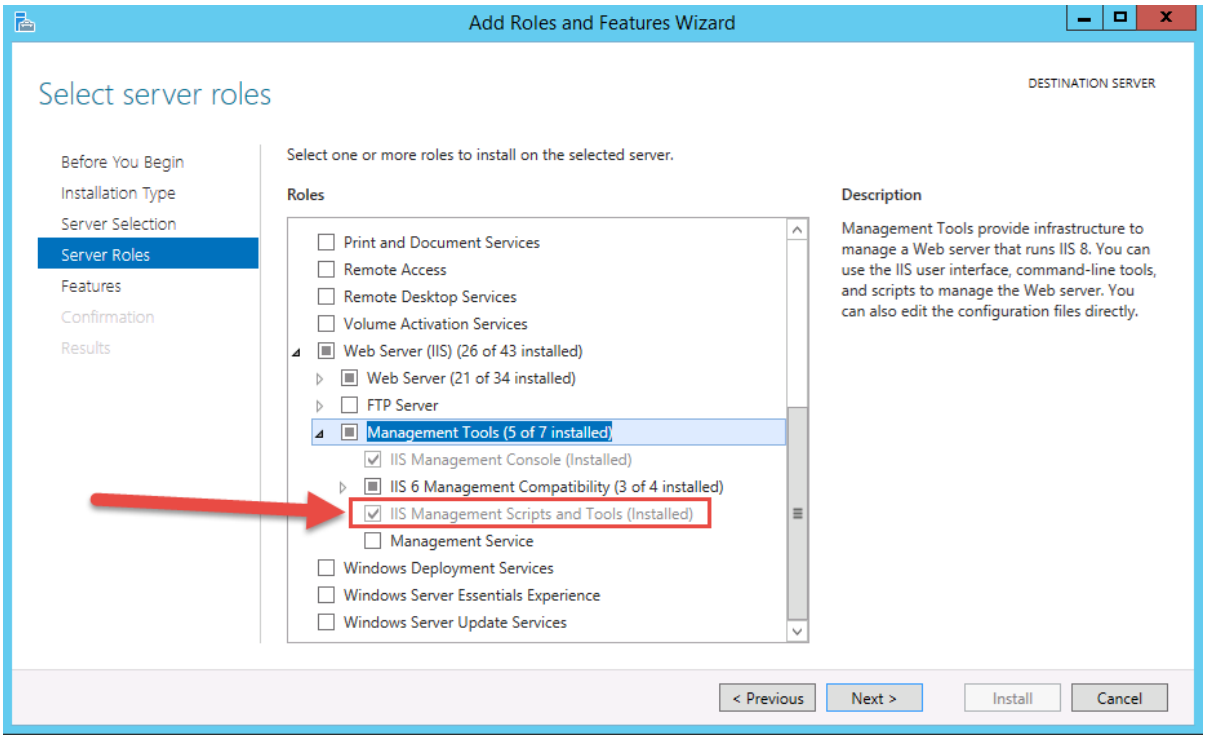
In addition, the following Windows Server 2012 settings must be configured.

- Microsoft Internet Information Services
- IIS Manager and Feature Delegation
- Web Server (IIS) and WCF (Windows Communication Foundation) Services

This section further discusses these settings.

Microsoft Internet Information Services (IIS)

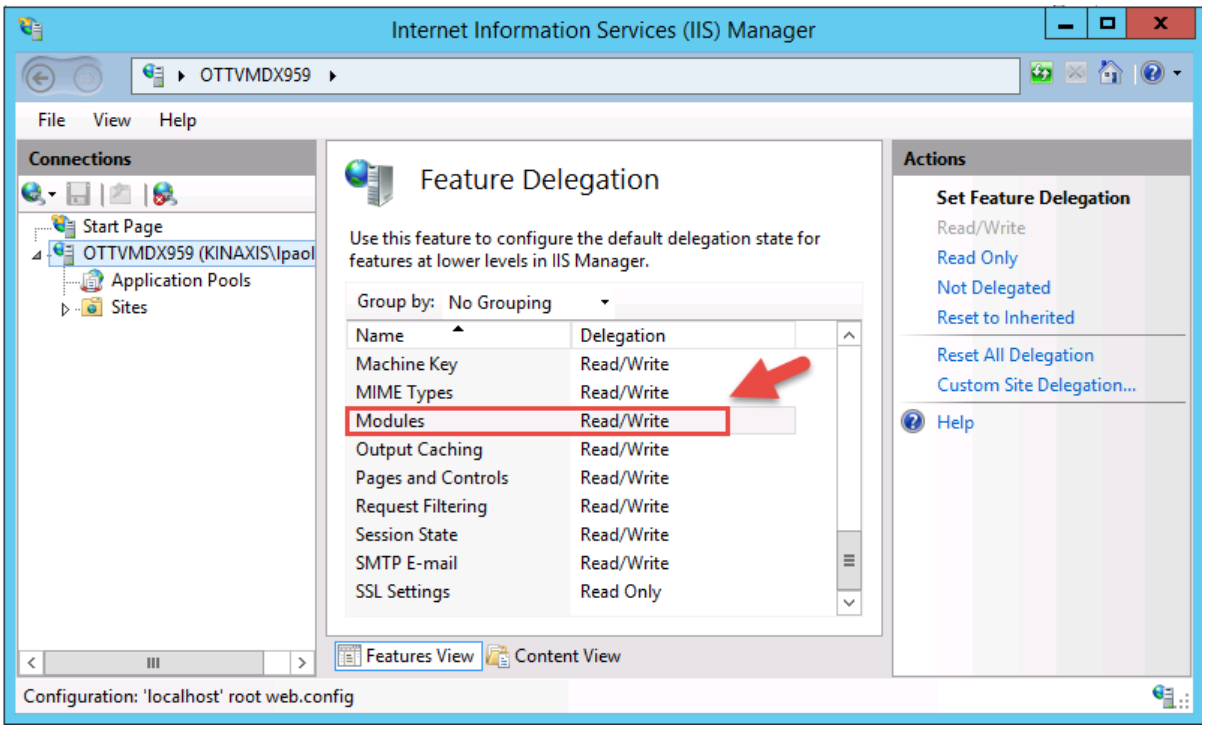
RapidResponse Application Server requires that Microsoft Internet Information Services (IIS) be installed and that **ISS Management Scripts and Tools** feature is turned on. For more information, see the Windows Server Help.



IIS addresses many of the potential security concerns of transmitting data across the Internet or an intranet. Your company, however, needs to take appropriate measures such as ensuring appropriate network configurations (for example, firewalls) are in place and the Web server operating system meets the RapidResponse system requirements.

IIS Manager and Feature Delegation

The IIS Manager includes the Feature Delegation page. From this page you can configure the delegation state for sites and applications on your Web server. RapidResponse requires that the **Modules** element must be set to **Read/Write**.



Web Server (IIS) settings and WCF (Windows Communication Foundation) Services

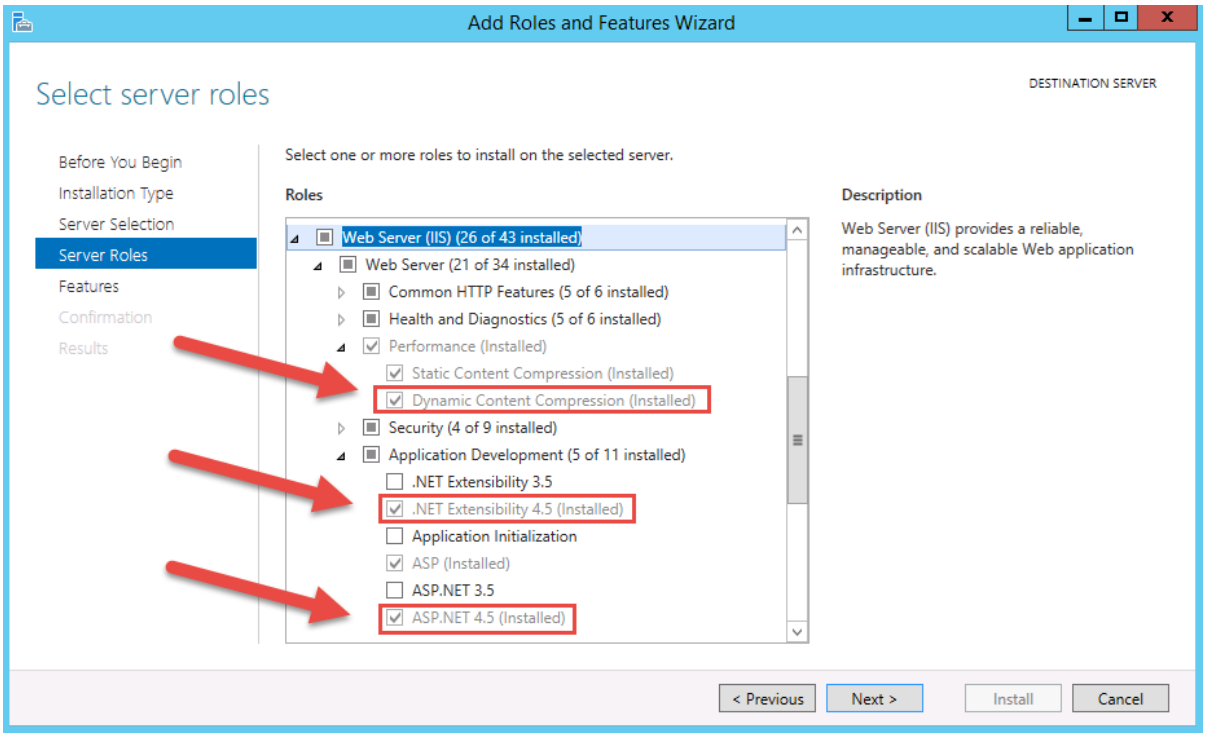
To run RapidResponse Application Server, the following Web Server (IIS) settings must be enabled:

- ASP.NET 4.5
- .NET Extensibility 4.5 (or 4.6)
- Dynamic Content Compression

In addition, WCF Services must be enabled.

▸To set Web Server (IIS) and WCF settings

1. Run **Server Manager**.
2. From the **Manage** menu, click **Add Roles and Features**.
3. On **Add Role or Feature Wizard** dialog, click **Server Selection** in the list of pages.
4. Select the server you are working with and click **Next**.
5. In the **Roles** box, under **Web Server (IIS),** and then select **Web Server**.
6. Select **Performance** and then select **Dynamic Content Compression**.
7. Under **Web Server**, select **Application Development**, then select **.NET Extensibility 4.5** and **ASP.NET 4.5**.
8. Click **Next**.
9. In the **Features** box, under **.NET Framework 4.5 Features**, select **WCF Services**.
10. Click **Next**.
11. Click **Install**.



RapidResponse uses an IIS Application Pool that uses a Network Service account. Changing this identity is not recommended or supported.

RapidResponse Server

Before installing, ensure that a compatible version of RapidResponse Server is running, and there is LAN connection between the computer where RapidResponse Server is installed and the computer where RapidResponse Application Server will be installed.

You will need to provide the computer name or the IP address of the computer on which RapidResponse Server is installed. If you're not sure of the computer name, refer to the **Computer Name** identified in the **System** option of the Windows **Control Panel**.

Master Administrator user password

The RapidResponse Master Administrator user (Admin user) password is required so that the installation program can make the required changes to the RapidResponse data files. The Master Administrator user cannot be signed into RapidResponse during the installation process.

TCP/IP ports and RapidResponse Application Server

The RapidResponse Server is bound to a specific TCP/IP port and it must be open for inbound requests. RapidResponse Server uses this port to communicate with other RapidResponse components.

A default port number (14600) is provided during the RapidResponse Server installation program. You have the option of choosing an alternative port number between 1024 and 65535. This port cannot already be assigned.

Before installing RapidResponse Application Server, two other TCP/IP ports must also be opened for inbound requests on the computer where RapidResponse Server is installed. RapidResponse Server uses these port to communicate with RapidResponse Application Server. These two ports need to be 2 and 3 port numbers greater than the port number used by RapidResponse Server to communicate with other RapidResponse components. For example, if the port number is 14600 then you must also open 14602 and 14603 to inbound requests from RapidResponse Application Server.

You can also change the port number after you install RapidResponse Server. For more information, see "RapidResponse and TCP/IP ports" on page 283.

Java Runtime Environment (JRE)

RapidResponse Application Server requires a 64-bit Oracle Java Runtime Environment (JRE), version 8 or 10. If a supported JRE is not installed, you are presented, when installing, with instructions on how to download and install a supported JRE. You can also download the latest version of the JRE by visiting http://www.java.com/en/.

Note: RapidResponse Real-time Integration Service and the Data Transfer Client require JRE 8. If you are installing the RapidResponse Application Server on the same computer as either of these components, JRE 8 must be installed.

Installing RapidResponse Application Server

The RapidResponse Application Server installation adds files to the RapidResponse Server and the Web server computer(s). In addition, it automatically configures a number of services. A successful installation does the following:

- Installs RapidResponse Application Server on a Web server computer.
- Creates the registry keys required to support RapidResponse Application Server.
- Installs RapidResponse OpenAPI (if not already installed).
- Creates the required virtual directories.

The following procedure outlines the steps necessary for a successful installation of RapidResponse Application Server. If you receive error messages during the installation regarding connections between RapidResponse Server and RapidResponse Application Server, see "Troubleshooting RapidResponse framework connectivity" on page 123.

▸To install RapidResponse Application Server

1. Log on as a Windows Server administrator on the computer where RapidResponse Application Server will be installed, and then in the RapidResponse installation image, double-click the **EasyInstaller.exe** file.
2. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.

3. Click **Next**.
4. On the **Customize** tab, do the following:
   - Clear the **RapidResponse Server** check box.
   - Ensure the **RapidResponse Application Server** check box is selected.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
5. If you are prompted to install required software components (such as RapidResponse OpenAPI, Windows Installer, and Microsoft Visual C++ components), click **Install** and follow the subsequent installation instructions. You might be then prompted to restart the computer. If so, you will need to restart the installation program. If not, go to the next step.
6. Review the information on the **Welcome** screen and click **Next**.
7. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
8. On the **RapidResponse Server** screen, do one of the following in the **Computer Name** box:
   - If RapidResponse Server is in the same domain as the Web server, type the computer name or the IP address of the computer on which RapidResponse Server is installed.
   - If RapidResponse Server is not in the same domain as the Web server, type the IP address of the computer on which RapidResponse Server is installed.
   - In the **RapidResponse Server Port box**, accept the default port or type the port number RapidResponse Server uses to communicate with other RapidResponse components. For more information, see "TCP/IP ports and RapidResponse Application Server" on page 117.
   - In the **Admin Password** box type the RapidResponse Master Administrator (Admin user) password.
   - Click **Next**.
9. On the **RapidResponse Web Site** screen, in the Web Site box, choose the Web site for RapidResponse. This site is typically named **Default Web Site** if the Web server has only one Web site.

   In the **Virtual Directory Name** box, type the name of the virtual directory to be used by RapidResponse or accept the default.
10. On the **Destination Folder** screen, choose the location where you want to install RapidResponse Application Server or accept the default, and then click **Next**.
11. On the **Select Program Folder** screen, you can either accept the suggested folder name, type a new folder name, or select one from the **Existing Folders** list. Click **Next**.
12. On the **Ready to Install the Program** screen, click **Install**. The installation process begins.
13. When the components are done installing, click **Next**.
14. If any components failed to install, click **Open Log File** to review the errors.
15. Click **Finish**.
16. If the **Restart Windows** screen displays, select an option and click **Finish**.
17. Review the RapidResponse Application Server installation log files in the **C:\Program Files\Kinaxis\RapidResponse\Logs** folder. For more information about the log files, see "Reviewing system status and operation logs" on page 421.
18. After completing the Application Server installation, you need to test that it installed properly and then import the license keys. For more information, see "Testing the RapidResponse installation" on page 122 and "Importing license keys" on page 124.

Notes:

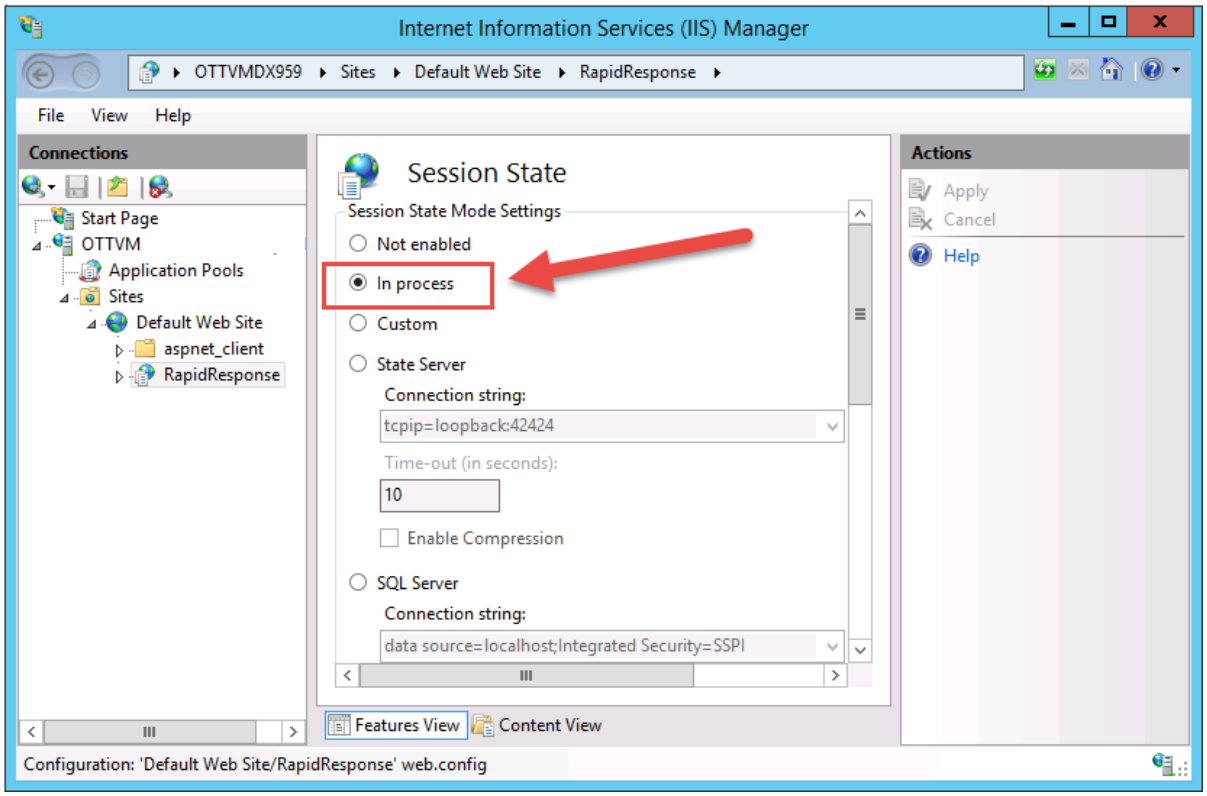
- RapidResponse Application Server can be installed on more than one Web server computer. Each instance can connect with a common RapidResponse Server. For example, you might want to install RapidResponse Application Server on a Web server computer for intranet users and on another Web server computer for Internet users.
- If you sign into RapidResponse after installation and before data has been loaded into the RapidResponse database, you will see only the Scenarios and Administration panes. This is due to not having any sites yet defined in RapidResponse. At least one site must be added to see the full RapidResponse interface.

RapidResponse Application Server post-installation procedures

After installing RapidResponse Application Server, review the following post-installation procedures.

Session State for IIS Manager

RapidResponse Application Server requires Microsoft Internet Information Services (IIS). The Session State Mode setting for RapidResponse in IIS Manager must be set to **In Process**.



Installing RapidResponse documentation resources

By default, the On-Premises version of RapidResponse relies on Internet-based documentation resources (Help systems and PDF files) hosted by Kinaxis. These resources are continually updated to reflect functionality introduced in new service updates, as well as for documentation corrections and improvements. RapidResponse users can also provide comments in these hosted help topics, see comments other users have made, and rate individual topics.

If necessary, a .Zip file containing all documentation resources for the version of RapidResponse you installed is available from the same location where you accessed the RapidResponse installation program and files. The contents of this file can then be extracted into the existing **Docs** and **Help** folders in the **Program Files\Kinaxis\RapidResponse\Web\en** directory (by default, these two folders are empty other than for a copy of the *RapidResponse Administration Guide*).

Administrators can then specify that users always access the Help resources hosted on the RapidResponse Application Server system (rather than those hosted by Kinaxis). Typically, this would only be done if your users aren't ever expected to have Internet access. Additionally, if RapidResponse is configured so that users access the documentation resources hosted by Kinaxis, then the resources installed on the RapidResponse Application Server are only used in cases where those users are offline or temporarily without internet access.

1. In the directory containing the RapidResponse installation files, browse to the **Rollup\Docs** folder.
2. Copy the **RRDocs.zip** file.
3. Paste the **RRDocs.zip** file to a location on the system where the RapidResponse Application Server is installed (for example, the Desktop).
4. Start the application you want to use to unzip and extract the contents of the **RRDocs.zip** file (for example, WinZip). This application must be run using the **Run As administrator** option to enable extracting and writing files to the **Help** and **Docs** folders.
5. In WinZip (or similar tool), open the **RRDocs.zip** file.
6. Unzip the contents of the **RRDocs.zip** file to the following directory:
   Program Files\Kinaxis\RapidResponse\en
7. During the extraction process, Help files and PDFs in the Zip file are copied to the **Help** and **Docs** folders respectively. When prompted during this process, you should replace the existing copy of the *RapidResponse Administration Guide*.

Notes:

- Each time you apply a RapidResponse Service Update, the contents of the **Help** and **Docs** folders are deleted. You can then follow the steps above to install the documentation resources for that particular Service Update.
- If you do not use the **Run As Administrator** option to start WinZip, an error will be generated when you attempt to extract files to the **Help** and **Docs** folders. In this case, you can still extract the files to another folder location (such as, on the Desktop) and then manually copy them to the **Help** and **Docs** folders.
- Optionally, the contents of the **Docs** folder in the **RRDocs.zip** file can also be extracted to the **RapidResponse/Docs** folder on the system where RapidResponse Server is installed. In earlier versions of RapidResponse, all RapidResponse PDF Guides were installed to this location (however,

Testing the RapidResponse installation

After completing the RapidResponse installation, you need to test whether it was properly installed. To test the installation you need to start RapidResponse Server and test whether you can sign into RapidResponse. By signing into RapidResponse you are testing whether RapidResponse Server and RapidResponse Application Server (known together as the RapidResponse framework) are properly communicating. If you encounter connectivity problems from RapidResponse Application Server to RapidResponse Server, see "Troubleshooting RapidResponse framework connectivity" on page 123.

Starting RapidResponse Server

RapidResponse runs as Microsoft Windows services and the main service is RapidResponse Server. After completing the RapidResponse installation, test whether you can start the RapidResponse Server service. For more information about the services, see "RapidResponse Windows Services" on page 227.

To start RapidResponse Server, you must use the computer where RapidResponse Server is installed, or access the computer using Microsoft Windows Remote Desktop Connection.

You have two options to start RapidResponse Server.

▸To start RapidResponse Server service from Windows Control Panel

1. Log on as an administrator to the computer where RapidResponse Server is installed.
2. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
3. Click **RapidResponse Server** in the Services pane.
4. On the **General** menu, click **Start**.

Note: You can use the Microsoft Windows Services dialog box to have this service automatically start when the computer where RapidResponse Server is installed is started.

▸To start RapidResponse Server service from Windows Start Menu

1. Log on as an administrator to the computer where RapidResponse Server is installed.
2. From the Microsoft Windows **Start** menu, point to **All Programs**, **RapidResponse**, and then click **Start RapidResponse Server**.

Signing into RapidResponse

You can test the installation by signing in to RapidResponse through a supported Web browser. The URL for signing in to RapidResponse is established during the installation. It is **Web Server Name/rapidresponse**. For example, if your Web server is named server99, the URL is **http://server99/rapidresponse**.

When testing, sign into RapidResponse as the Master Administrator (Admin user). The initial Master Administrator password is provided by Kinaxis Customer Support. For more information about this account, see "Master Administrator user account for On-Premises" on page 34.

▸To sign in to RapidResponse

1. Open a Web browser.
2. Type the **RapidResponse** URL into the Address box of the browser.
3. On the **RapidResponse Sign In** page, do the following:
   - In the **User ID** box, type **Admin**.
   - In the **Password** box, type the Admin user password. The password is case sensitive.
   - Click **Go**.

Troubleshooting RapidResponse framework connectivity

When installing or running RapidResponse Application Server, you might receive an error message indicating that a connection to the RapidResponse Server could not be made. The possible causes of and solutions to this problem vary depending on whether the RapidResponse Server is in the same domain as the Web server computer.

The following table describes possible causes for the error message when the RapidResponse Server is not in the same domain as the Web server.

Possible Cause	Solution
The computer on which the RapidResponse Server is installed is down.	Check the computer and make sure it is running.
RapidResponse Server is not installed on the computer you specified during installation.	Check that the name of the computer you specified is correct. To find out which port number RapidResponse Server is using, you can look in **Server.log**. Check to see if the RapidResponse Server has actually been installed on this server. For more information about the log file, see " Server.log file" on page 464.
The RapidResponse Server is installed on the computer you specified, but is not running.	Start RapidResponse Server.

The following table describes possible causes for the error message when the RapidResponse Server is in the same domain as the Web server.

Possible Cause	Solution
The installation can't find the RapidResponse Server computer.	Check to see that the specified server name is correct.
The installation can't find the RapidResponse Server.	Check to see that the RapidResponse Server is installed on the specified computer.
The RapidResponse Server is installed on the computer you specified, but is not running on the specified port.	Check that the name of the computer you specified is correct. To find out which port number RapidResponse Server is using, look in **Server.log**. For more information about the log file, see " Server.log file" on page 464.
The RapidResponse Server is not running.	Start RapidResponse Server.

Importing license keys

License keys are used to enable RapidResponse functionality, and to specify the number of user accounts and sites that RapidResponse can support. The license key file is provided by Kinaxis Customer Support.

Kinaxis Customer Support generates the license keys and the keys are only compatible with a specific computer based on the computer's server ID. You need to provide Kinaxis Customer Support with the server ID of the computer where RapidResponse Server is installed.

When you import a license key file, the existing license keys are replaced.

RapidResponse license keys use expiry dates. Fifteen days prior to the keys expiring, system administrators receive a warning. If you receive a warning, you should immediately contact Kinaxis Customer Support.

▸To determine the computer's server ID

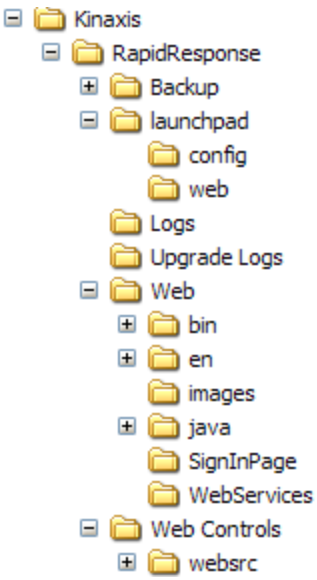
1. Open a Windows command window on the computer where RapidResponse Server is installed.
2. Go to the **C:\RapidResponse\Program** folder.
3. Type **getserverid.exe** and press **ENTER**.
4. The command generates information in the following format:
   Server ID is >1234567890<.
5. Send the Server ID information to Kinaxis Customer Support (support@kinaxis.com).

▸To import license keys

1. Sign into RapidResponse.
2. In the **Administration** pane, under **System Settings**, click **Licenses**.
3. Click **Browse**.
4. Locate the license keys file, and then click **Open**.
5. Click **Import License Keys**.

RapidResponse Application Server folder structure

The RapidResponse Application Server folder structure is shown in the following illustration:

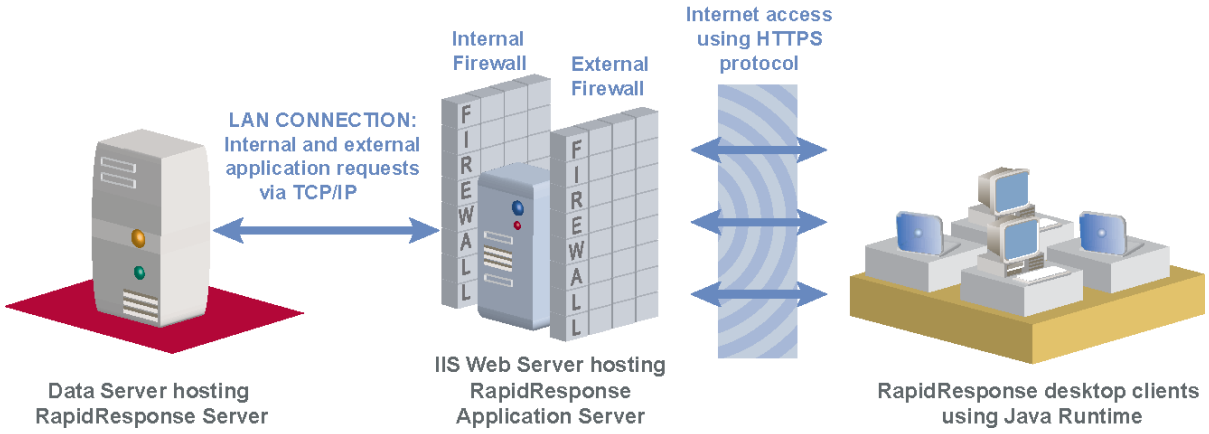


For information about backing up RapidResponse folders and files, see "Backing up RapidResponse program files" on page 314.

Providing external access to RapidResponse

You can give access to RapidResponse to users outside of your internal network; that is, users who access it across the Internet. You can choose the resources that you make available to external users, and you can also specify the type of access. This allows you to provide critical information to key players in your supply chain in a secure manner.

The HTTPS protocol provides secure and encrypted communication between RapidResponse users outside of your internal network and the RapidResponse Application Server. As shown in the following illustration, you should install RapidResponse Application Server on a system outside of your internal firewall.



When RapidResponse uses the HTTPS protocol, all data transmitted between a RapidResponse client and the RapidResponse Application Server is encrypted using either Secure Sockets Layer (SSL) or

Transport Layer Security (TLS). Kinaxis recommends using TLS. Public key encryption that utilizes certificates from a trusted authority enables the SSL communication between RapidResponse clients and RapidResponse. To secure communications, RapidResponse administrators need to generate and install a certificate. For more information, see "To generate and install SSL certificates in Windows Server 2012 (IIS 8)" on page 126.

To provide RapidResponse access to those outside of your internal network, you should install RapidResponse on a computer outside of your internal firewall (that is, in the DMZ). This computer requires that inbound TCP port 443 be open for HTTPS connectivity between a RapidResponse client and RapidResponse Application Server. If you are using HTTP, then port 80 needs to be open.

For more information about RapidResponse security, see "Security and infrastructure" on page 45.

Securing communication with certificates

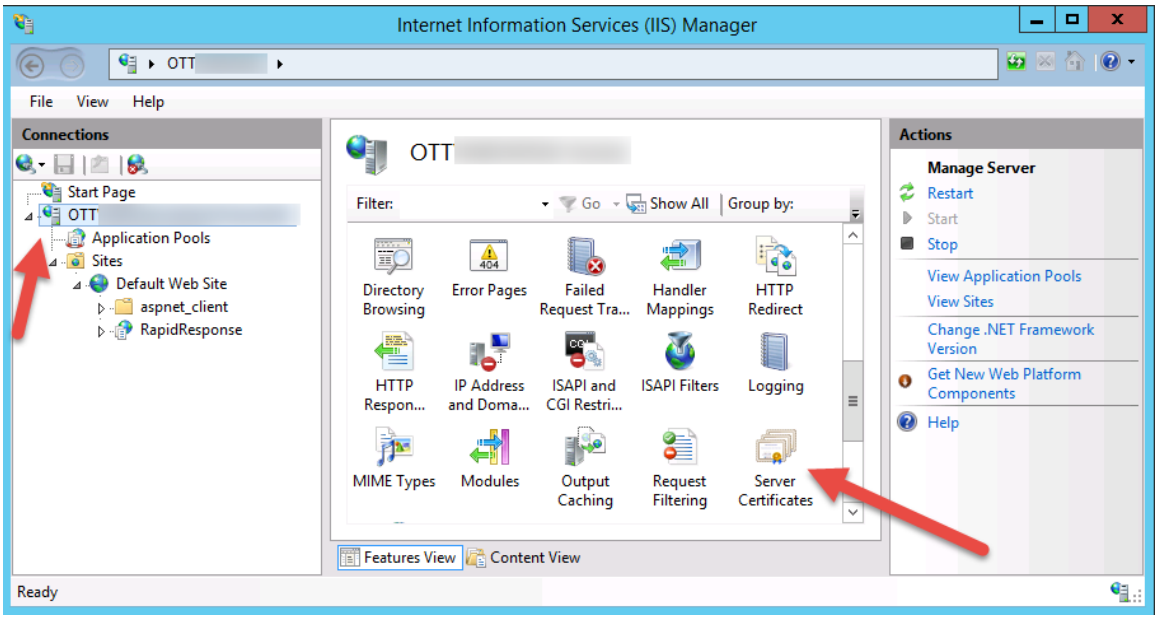
RapidResponse can use the HTTPS communications protocol to help ensure secure communications. This means that all data transmitted between a RapidResponse client and the RapidResponse Application Server is encrypted using HTTPS. Public key encryption that utilizes certificates from a trusted authority enables secure communication between RapidResponse clients and RapidResponse. In order for your IIS Web server to secure communications, you need to generate and install a certificate for it.

Public Key Encryption uses two separate keys. A message encrypted with either of the keys can only be decrypted with the other. A trusted certifying authority issues these public keys along with an attached description of the owner and issuing authority. This package is known as a certificate.

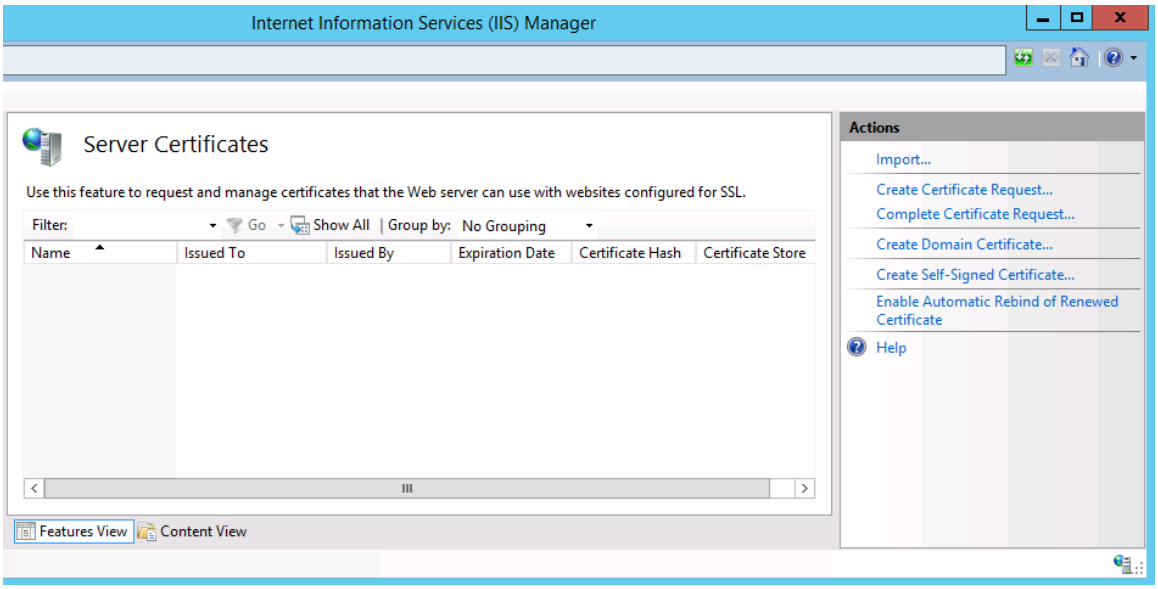
When the browser requests a secure connection to a secure site, IIS returns a certificate. A certifying authority stamps the certificate. It contains the identity of the certificate holder, their domain name and the public key. The browser then presents the information to the user. The certificate's public key is used by the browser to safely send the symmetric encryption key that it has made up for this secure connection.

▸To generate and install SSL certificates in Windows Server 2012 (IIS 8)

1. Open **Internet Information Services (IIS) Manager** on the computer where RapidResponse Server is installed.
2. Select the server and double-click **Server Certificates**.



3. From the **Actions** panel, import a certificate or create a certificate request. If you have generated the new request, you will need to send the request to the appropriate authority of your choice. When you receive the authorized certificate, you must install it. If you need more assistance, see the Microsoft Server documentation.



Once you have successfully installed the authorized certificate, users will see a message notifying them that they are using a secure connection.

Uninstalling RapidResponse Application Server

RapidResponse Application Server is removed from a Web server computer using the Windows Control Panel. The RapidResponse Application Server uninstall program does not remove data or RapidResponse resources. This information is preserved in the **C:\Program Files\Kinaxis\RapidResponse** folder.

▸To uninstall RapidResponse Application Server

1. In the Microsoft Windows Control Panel, double-click **Add/Remove Programs**.
2. In the **Currently Installed Programs** window, choose **Kinaxis RapidResponse Application Server**, and click the **Remove** button.
3. Click **Yes** to confirm your choice.
4. When the uninstall is complete, click **OK**.

CHAPTER 12: Installing RapidResponse applications

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

This section applies to RapidResponse 2016.2 Service Update 21. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

Preparing to install RapidResponse applications 130
Installing RapidResponse applications 130
Installing Capacity Planning (CRP) 131
Installing Engineering Change Manager 133

This section describes how to install RapidResponse applications and the options available to you during the installation. If you are upgrading RapidResponse, skip this chapter and see "Upgrading RapidResponse applications" on page 195.

Each application is composed of a variety of predefined RapidResponse resources. The predefined resources are installed and stored in the RapidResponse database and are available to use from the RapidResponse client. Predefined resources include:

- Dashboards and widgets
- Workbooks
- Scorecards
- Processes and task flows
- Filters and hierarchies
- Alerts and scheduled tasks
- Insert definitions
- Forms
- Responsibilities

For a complete list and discussion of RapidResponse applications, see the *RapidResponse Applications Guide*.

Preparing to install RapidResponse applications

Before installing RapidResponse applications, you should verify the following RapidResponse configuration items.

RapidResponse Server

You must provide the computer name or the IP address of the computer on which RapidResponse Server is installed. If you are not sure of the computer name, refer to the Computer Name that is identified in the System option of the Microsoft Windows Control Panel.

Port numbers

If you do not accept the defaults, you must enter the port numbers for RapidResponse Server. The port is used to communicate with other RapidResponse components.

Master Administrator user password

The Master Administrator user (Admin user) password is required so that the installation program can make the required changes to the RapidResponse data files. The Master Administrator user cannot be signed into RapidResponse during the installation process.

Installing RapidResponse applications

During the installation of predefined resources, you are prompted to select the appropriate resources. If you are not certain what to choose, select all of the resources.

The RapidResponse Resource Installer installs the predefined resources to the RapidResponse database as objects, and then shares them to predefined user groups. You can optionally install the Capacity Planning and Engineering Change Manager applications as part of this process. If you select to install these applications, they are installed after any applications you specify in the RapidResponse Resource Installer.

▸To install RapidResponse applications

1. Log on to a computer where RapidResponse Application Server is installed
2. In the RapidResponse installation image, double-click the **EasyInstaller.exe** file.
3. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
4. Click **Next**.

5. On the **Customize** tab, do the following:
   - Clear the **RapidResponse Server** check box.
   - Clear the **RapidResponse Application Server** check box.
   - Select the **RapidResponse Applications** check box.
   - Optionally, select the **RapidResponse Capacity Planning** check box if you are using the Capacity Planning application.
   - Optionally, select the **RapidResponse Engineering Change Manager** check box if you are using the Engineering Change Manager application.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
6. On the **Welcome** screen, review the information, and then click **Next**.
7. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
8. On the **RapidResponse Server** screen, in the **Computer Name** box, do one of the following:
   - If RapidResponse Server is in the same domain as the Web server, type the computer name or the IP address of the computer on which RapidResponse Server is installed.
   - If RapidResponse Server is not in the same domain as the Web server, type the IP address of the computer on which RapidResponse Server is installed.
9. In the **RapidResponse Server Port** box, accept the default port or type the port number that RapidResponse Server uses to communicate with other RapidResponse components, including Application Server.
10. In the **AdminPassword** box, type the Master Administrator (Admin user) password.
11. Click **Next**.
12. On the **Custom Setup** screen, click the icon beside the application name, and then click **This feature, and all subfeatures will be installed on local hard drive**. Also, ensure that the **Common Resources** and **Others** entries in the list are selected to be installed.
13. Click **Next**.
14. On the **Ready to Install the Program** screen, click **Install**. The installation process begins.
15. Click **Finish**.
16. When the components are done installing, click **Next**.
17. If any components failed to install, click **Open Log File** to review the errors.
18. Click **Finish**.

Note: Although the Microsoft Windows Control Panel indicates that you can remove the **Kinaxis RapidResponse Resource Installer**, removing this item deletes only the program that installs the predefined resources to the RapidResponse database. The actual resources remain in the RapidResponse database. To remove the resources, you must delete them using the RapidResponse client.

Installing Capacity Planning (CRP)

This section applies only if you are installing Capacity Planning individually, and not as part of the overall installation process. If you have included Capacity Planning with other application installations, the required settings are already specified and you do not require any additional configuration. For more information, see "Installing RapidResponse applications" on page 130.

This application helps you to identify work centers that are over or under-utilized, manage resource loading, and balance demand with the most efficient use of resources over time. It consists of analytic calculations, tables, and predefined resources including workbooks.

The Capacity Planning (CRP) installation adds files to the RapidResponse Server and RapidResponse Application Server computers, and automatically configures default settings.

▸To install RapidResponse Capacity Planning (CRP)

1. Log on to a computer where RapidResponse Application Server is installed
2. In the RapidResponse installation image, double-click the **EasyInstaller.exe** file.
3. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
4. Click **Next**.
5. On the **Configuration** tab, do the following:
   - Clear the **RapidResponse Server** check box.
   - Clear the **RapidResponse Application Server** check box.
   - Select the **RapidResponse Capacity Planning** check box.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
6. Review the information on the **Welcome** screen, and click **Next**.
7. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
8. On the **RapidResponse Server** screen, do one of the following in the **Computer Name** box:
   - If RapidResponse Server is in the same domain as the Web server, type the computer name or the IP address of the computer on which RapidResponse Server is installed.
   - If RapidResponse Server is not in the same domain as the Web server, type the IP address of the computer on which RapidResponse Server is installed.
9. In the **RapidResponse Server Port** box, accept the default port, or type the port number that RapidResponse Server uses to communicate with other RapidResponse components, including Application Server.
10. In the **Admin Password** box, type the Master Administrator (Admin user) password.
11. Click **Next**.
12. On the **Ready to Install the Program** screen, click **Install**. The installation process begins.
13. When the components are done installing, click **Next**.
14. If any components failed to install, click **Open Log File** to review the errors.
15. Click **Finish**.
16. If the **Restart Windows** screen appears, select an option and click **Finish**.

Uninstalling Capacity Planning (CRP)

RapidResponse Capacity Manager is uninstalled using the Microsoft Windows Control Panel. The uninstall program does not remove data or RapidResponse resources. This information is preserved in the **C:\Program Files\Kinaxis\RapidResponse** folder.

▸**Uninstall RapidResponse Capacity Planning (CRP)**

1. In the Windows Control Panel, double-click **Add/Remove Programs**.
2. In the **Currently Installed Programs** window, choose **Kinaxis RapidResponse Capacity Planning (CRP)**, and click **Remove**.
3. Click **Yes** to confirm your choice.
4. When the uninstall is complete, click **OK**.

Capacity Planning (CRP) components

Capacity Manager consists of analytic calculations, tables, and predefined resources, including the following workbooks:

- CRP Analysis - Labor
- CRP Analysis - Machine
- CRP Master Data
- CRP Sheet - Labor
- CRP Sheet - Machine
- Work Center Properties

Capacity Manager includes the All Work Centers filter and the Capacity Manager user group that provides access to all the resources.

If Capacity Manager is not installed, database tables and fields that are associated with it are not available in the RapidResponse client. Workbook authors cannot create a report based on a table that is not available or use a field that references a table that is not available.

You can install Capacity Manager to use the optional Capacity Manager analytics to calculate. If it is not installed, the calculated fields that are associated with Capacity Manager remain empty.

For more information about the calculations, see the *RapidResponse Analytic and Data Model Guide*. For more information about using Capacity Manager to solve business problems, see the the *RapidResponse Applications Guide*.

Installing Engineering Change Manager

This section applies only if you are installing Engineering Change Manager individually, and not as part of the overall installation process. If you have included Engineering Change Manager with other application installations, the required settings are already specified and you do not require any additional configuration. For more information, see "Installing RapidResponse applications" on page 130.

Engineering Change Manager helps you analyze engineering changes to determine the best date at which to introduce an engineering change. Choosing the right date can lower the cost of implementing an engineering change; it can help you reduce excess or obsolete inventory, and ensure that customer satisfaction by eliminating late orders.

The RapidResponse Engineering Change Manager installation adds files to the RapidResponse Server and RapidResponse Application Server computers, and automatically configures default settings.

You will need the following information:

- **RapidResponse Server**—The computer name or the IP address of the computer on which RapidResponse Server is installed. If you are not sure of the computer name, refer to the Computer Name that is identified in the System option of the Microsoft Windows Control Panel.
- **Port numbers**—Port numbers for RapidResponse Server. The port is used to communicate with other RapidResponse components.
- **Master Administrator user password**—The Master Administrator user (Admin user) password is required so that the installation program can make the required changes to the RapidResponse data files. The Master Administrator user cannot be signed into RapidResponse during the installation process.

▸To install RapidResponse Engineering Change Manager

1. Log on to a computer where RapidResponse Application Server is installed
2. In the RapidResponse installation image, double-click the **EasyInstaller.exe** file.
3. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
4. Click **Next**.
5. On the **Configuration** tab, do the following:
   - Clear the **RapidResponse Server** check box.
   - Clear the **RapidResponse Application Server** check box.
   - Select the **RapidResponse Engineering Change Manager** check box.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
6. Review the information on the **Welcome** screen, and click **Next**.
7. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
8. On the **RapidResponse Server** screen, do one of the following in the **Computer Name** box:
   - If RapidResponse Server is in the same domain as the Web server, type the computer name or the IP address of the computer on which RapidResponse Server is installed.
   - If RapidResponse Server is not in the same domain as the Web server, type the IP address of the computer on which RapidResponse Server is installed.
9. In the **RapidResponse Server Port** box, accept the default port or type the port number that RapidResponse Server uses to communicate with other RapidResponse components, including Application Server.
10. In the **AdminPassword** box, type the Master Administrator (Admin user) password.
11. Click **Next**.
12. On the **Ready to Install the Program** screen, click **Install**. The installation process begins.
13. When the components are done installing, click **Next**.
14. If any components failed to install, click **Open Log File** to review the errors.
15. Click **Finish**.
16. If the **Restart Windows** screen appears, select an option and click **Finish**.

Uninstalling Engineering Change Manager

RapidResponse Engineering Change Manager is uninstalled using the Microsoft Windows Control Panel. The uninstall program does not remove data or RapidResponse resources. This information is

preserved in the **C:\Program Files\Kinaxis\RapidResponse** folder.

▸Uninstall RapidResponse Engineering Change Manager

1. In the Windows Control Panel, double-click **Add/Remove Programs**.
2. In the **Currently Installed Programs** window, choose **Kinaxis RapidResponse Engineering Change Manager**, and click **Remove**.
3. Click **Yes** to confirm your choice.
4. When the uninstall is complete, click **OK**.

Engineering Change Manager components

Engineering Change Manager includes the following workbooks:

- Engineering Change Data
- Engineering Change Manager
- Engineering Change Metrics

Calculations are performed in the workbooks. Also included is the Engineering Change Manager user group, which provides access to all the resources.

For more information about using Engineering Change Manager to solve business problems, see the *RapidResponse Applications Guide*

CHAPTER 13: Initial configuration steps

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

After installing RapidResponse, it needs to be configured to meet the unique needs of your company. This chapter provides an overview of all the administrative tasks that need to be performed after installing RapidResponse and before rolling it out to your user community.

You do not need to review this section if you are upgrading to RapidResponse. For more information about upgrading, see "Part 3: Upgrading RapidResponse" on page 139.

1. Reset the Master Administrator (Admin user) password. To change the password, sign in to RapidResponse as the Master Administrator user, and then change the password using the **Change Password** command on the **Tools** menu. For more information, see the *RapidResponse Help*. For more information about changing other account settings, see "Part 6: User administration" on page 491.
2. Set the email address for the Master Administrator user account. This email address receives status, warning, and error messages from RapidResponse. For more information, see "Message notifications" on page 421.
3. Specify an email server to support email functionality available in RapidResponse. As well, you might need to open port 25 to support email from RapidResponse. For more information, see "Configuring email support" on page 276.
4. Add any currencies that your company uses. One of these currencies must be set as the base currency, which is the default currency for all users, and is used as the basis for all currency conversions. For more information, see "Managing currencies" on page 686.
5. Create user groups, and user accounts for those who will be accessing RapidResponse. For more information, see "Managing groups and users" on page 565.
6. Define time zones for RapidResponse. In order for RapidResponse to recognize time zones, you must define them. You should define time zones that are relevant to your company, sites, and customers. For more information, see "Defining time zones" on page 669.
7. Optionally, customize the environment for RapidResponse users. Many customization options exist including (but not limited to):
   - Configuring printed report settings
   - Setting password security options
   - Setting the Message Center message limit
   - Specifying email settings
   - Setting the worksheet record limit
   - Setting default data formats for new users

- Making data formats available to users
- Overriding the Everyday calendar name
- Setting limits for the Part control
- Customizing the link menu

Review "Customizing RapidResponse user settings" on page 643 for more information.

8. Optionally, enable single sign-in for all users. For more information, see " Configuring single sign-in for On-Premises" on page 835.
9. The Master Administrator (Admin) user should enable the **Input Data Memory Load** and **CPU Usage** alerts. These alerts are to create reports to help monitor the RapidResponse system. For more information about these alerts, see "Monitoring input data growth" on page 263 and "Monitoring CPU usage" on page 271.
10. Set up alerts if your company will be monitoring data or automatically creating customized reports. For more information, see "Configuring settings for automation tasks" on page 671.
11. Modify the settings for some predefined resources. By modifying the settings, you can better meet the needs of your users. For more information, see "Predefined resource and tool settings" on page 807.
12. Modify the default folder locations in the RapidResponse program folder. For more information, see "RapidResponse Server folder structure" on page 249.
13. If you require a specific user account for the RapidResponse Service Host, in the Windows Services configuration, specify the user account to use for the RapidResponse Service Host.

Once you complete these configuration steps you should provide the RapidResponse URL to your RapidResponse users. You should also review other sections of this guide for server, data, and user administration tasks, settings, and processes.

Part 3: Upgrading RapidResponse

- "RapidResponse upgrade process overview" on page 141
- "Upgrading RapidResponse Server" on page 177
- "Upgrading RapidResponse Application Server" on page 189
- "Upgrading RapidResponse applications" on page 195
- "Converting standard tables to vector data" on page 203
- "Upgrading RapidResponse OpenAPI applications" on page 217
- "Preparing to transition away from RapidResponse OpenAPI" on page 219

CHAPTER 14: RapidResponse upgrade process overview

This section applies to RapidResponse 2016.2 Service Update 21 and later. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

Learning more about new and changed features 141
Data model calculations after upgrading 142
Preparing to upgrade (On-Premises) 143
RapidResponse upgrade steps (On-Premises) 150
Upgrading RapidResponse with Service Updates 152
Post-update considerations 154
Post-upgrade considerations 155

This chapter provides an overview of the RapidResponse upgrade process. The upgrade program manages the upgrade to the current version of RapidResponse from version 11.0 or later. If you are upgrading from a version earlier than 11.0, you should first upgrade to version 11.0 and then upgrade to the current version. For more information, contact Kinaxis Customer Support.

On-Demand: Kinaxis Customer Support performs the upgrade process for your company's RapidResponse Service. The relevant sections in this chapter should be reviewed before the upgrade process is completed to better prepare for changes.

Learning more about new and changed features

Before the upgrade process is started, it is recommended you review the new changed features included in the latest version of RapidResponse.

- Many changes that affect administration are discussed in "New and changed in RapidResponse" on page 67.
- You can learn more about all new features and changes included in RapidResponse from the *RapidResponse Release Summary Guide*.

The *RapidResponse Release Summary Guide*

A new version of the *RapidResponse Release Summary Guide* is released with each new version of RapidResponse, including service updates.

This document is available for download from the Kinaxis Knowledge Network and summarizes the changes to RapidResponse. It contains a compilation of changes gathered from every RapidResponse guide and help system. It also contains lists of defects resolved in each version. These lists are not available in other documentation.

▸To access the *RapidResponse Release Summary Guide*

1. On the **Help** menu, click **Kinaxis Knowledge Network**.
2. Sign into the Kinaxis Knowledge Network.

   You can create a new Kinaxis Knowledge Network account if you do not have one. An account is required.
3. On the **Support** menu, click **Support Overview**.
4. Click **Downloads**.
5. Select the newest release under the **Downloads -RapidResponse 1904** heading, and then click the download link for the RapidResponse Release Summary PDF document.

Data model calculations after upgrading

All new data model analytics or changes to existing analytics are designed to allow backwards compatibility with existing configurations; that is, the changes will not impact the results RapidResponse was previously generating. The default settings for each of the new configurable data model features are set so that the calculated results from RapidResponse after upgrade are the same as the results before upgrade.

During the upgrade, you need to compare the “before” and “after” calculation results. Kinaxis has performed this activity on a number of customer data sets as part of our quality assurance efforts. As part of the comparison process you might notice differences in results. These result differences are considered “explainable” and can be attributed to corrected defects in the data model analytic calculations.

When comparing or validating results, you should review three top-level parts to ensure independent demand available dates align.

After you upgrade, all queries, data in custom applications, and inserts continue to be compatible with the new data model; that is, errors are not generated.

The following changes can occur in the data model after an upgrade:

- A field is moved from one table to another.
- A field is deleted from a table.
- A field is added to a table.
- A table is added.

Fields that have been moved or removed in the upgraded data model are still available; however, they are read-only.

Fields that have been added to the data model are given default values to ensure that operations function. The default value for a given field can be viewed in the Data Model dialog box by accessing the field’s properties. This dialog box can be accessed from the RapidResponse **Administration** pane by clicking **Data Model** under the **Data** section. If necessary, you can specify a different default value to override the initial default.

See the “Data model change summary” section in the *RapidResponse Analytic and Data Model Guide* for information about changes.

Preparing to upgrade (On-Premises)

This topic only applies to the On-Premises version of RapidResponse.

From a high-level perspective, the RapidResponse upgrade process is straight forward: you upgrade the RapidResponse components and the database is automatically upgraded to match the new components. In practice, several major steps and processes must be completely followed after careful planning. As well, the upgrade process should first be performed in a RapidResponse test environment. This is a separately installed instance of RapidResponse beyond your production environment. For more information about creating test environments, see "Set up the RapidResponse test environment" on page 148.

The amount of time required to upgrade a RapidResponse system is highly dependent on database size and the number of resources (dashboards, workbooks, and so on). The larger the initial database, the longer the overall upgrade process will take as it might require multiple restarts of RapidResponse Server.

The upgrade process also requires that RapidResponse Server be restarted multiple times. In some cases, this could make the upgrade process very time consuming. For example, if your database takes one hour to load and the upgrade process requires four restarts, then the process will take more than four hours to complete.

This section describes the general steps to upgrading RapidResponse. After reviewing this material, create an upgrade plan. This section explains the steps for preparing to upgrade RapidResponse. The following topics are discussed:

- "RapidResponse installation program and serial number" on page 143
- "Review system requirements" on page 144
- "Delete unused resources and users" on page 144
- "RapidResponse TCP/IP ports" on page 144
- "Delete unused scenarios and update scenarios" on page 145
- "Testing custom fields for period (.) character" on page 145
- "Testing workbooks for modifications to reference keys" on page 146
- "Review tables that contain vector data" on page 148
- "Apply pending data model changes" on page 148
- "Set up the RapidResponse test environment" on page 148
- "Disable data automation tools" on page 149

RapidResponse installation program and serial number

To upgrade, you require the RapidResponse installation program. The installation program is available in two formats:

- The RapidResponse DVD which is available from the Kinaxis Customer Support group.
- As an installation image. This is available for download from the Kinaxis Secure FTP site.

To upgrade, you also require new RapidResponse serial numbers for your production and test environments. To receive these numbers, contact Kinaxis Customer Support at support@kinaxis.com.

Review system requirements

You need to confirm that the computers where RapidResponse Server and RapidResponse Application Server are currently installed meet the latest system requirements before upgrading. For more information, see "System requirements for RapidResponse" on page 104.

During the RapidResponse Server upgrade, the database temporarily consumes more space on disk. Once the upgrade is completed, the database returns to its original size.If you are upgrading from RapidResponse 11.0 (and later) to 2014.1 (or later), expect the database to grow by a factor of three during the upgrade.

Kinaxis recommends that before upgrading, you review the current size of the database. The RapidResponse database is stored in the **C:\RapidResponse\Data** folder. Consider adding more disk space before upgrading if the current disk does not meet the requirements of the upgrade process.

The RapidResponse 11.0 (and later) database is stored in DFS folders in the Data folder. For more information about the database, see "Managing the RapidResponse database" on page 309.

When upgrading to RapidResponse 2014.1 (and later), you should also review the amount of system memory available on the computer where RapidResponse Server is installed.

The RapidResponse Server upgrade process requires that the system memory be at least four times the size as the RapidResponse database. For example, if the size of the database on disk is 50 GB then the system requires at least 200 GB of system memory to complete the upgrade. If you are upgrading from RapidResponse 11.0 (or earlier), the system memory should be at least five times the size as the database.

Your actual requirements depend on several factors including the size of your data and the number of users. Contact Kinaxis Customer Support for assistance in determining your actual system requirements. For more information, see "Customer Support" on page 19.

Delete unused resources and users

To help the RapidResponse upgrade program run efficiently, you should delete any unused resources (such as dashboards and workbooks) and users no longer using the system. This also helps to save system memory and improves the upgrade process. For information about understanding which resources are no longer being used, see "Monitoring resource usage" on page 746. For information about deleting user accounts no longer in use, see "Deleting user accounts" on page 573.

RapidResponse TCP/IP ports

The RapidResponse Server is bound to a specific TCP/IP port and it must be open for inbound requests. RapidResponse Server uses this port to communicate with other RapidResponse components. The default setting is port 14600.

As of RapidResponse 2016.2, two other TCP/IP ports must also be opened for inbound requests on the computer where RapidResponse Server is installed. RapidResponse Server uses these port to

communicate with RapidResponse Application Server. These two ports need to be 2 and 3 port numbers greater than the port number used by RapidResponse Server to communicate with other RapidResponse components. For example, if the port number is 14600 then you must also open 14602 and 14603 to inbound requests from RapidResponse Application Server.

For more information, see "RapidResponse and TCP/IP ports" on page 283.

Delete unused scenarios and update scenarios

By deleting unused scenarios and updating historical (out-of-date) scenarios, you can improve the database upgrade process and shorten the processing. For more information about scenario management, see "Scenario management" on page 703.

Testing custom fields for period (.) character

As of RapidResponse 9.0, data administrators could not create new custom fields that used the period (.) character. Field names can only consist of alphanumeric characters (a-z, 0-9) and underscores (_). The first character must be alphabetic.

RapidResponse continued to support field names that included the period character up to version 2014.2. As of RapidResponse 2014.4, the period character in custom field names is no longer supported. Before upgrading to RapidResponse 2014.4 (or later) from RapidResponse 2014.2 (or earlier), you must rename fields that contain the period character before upgrading or data will be lost.

If your system contains fields with the period character, it is likely they will be Set fields. These set fields can be simply renamed without impacting your system. For more information about customizing the data model, see the *RapidResponse Data Integration Guide*.

If your system includes fields other than the Set type with the period character, you must contact Kinaxis Customer Support to further discuss your upgrade options.

The **PreUpgradeAnalyzer** utility can be used to test whether any custom fields are using the period character. To access this utility, go to https://knowledge.kinaxis.com/s/article/Analyzingresourcesanddataforvectorupgradeissues53745 and click on **PreUpgradeAnalyzer** in the Files section. A version of this utility is available for each RapidResponse version, so you must ensure you use the specific utility designed for the RapidResponse version you are upgrading from.

The **PreUpgradeAnalyzer** utility takes a configurable XML file that specifies the RapidResponse Server name and other configuration settings. The results of the utility's analysis is a Microsoft Excel workbook. You can specify the location this file is saved and its name in the configuration file.

▸To configure the upgrade utility

1. Extract the utility's **.zip** file into a folder of your choice.
2. Using Windows Explorer, navigate the to location you extracted the **.zip** file.
3. Edit the **config.xml** file.

4. Specify the following options as required.

Element	Required	Description
server	Yes	The RapidResponse Server name. For example, `<server>localhost</server>`
adminPassword	Yes	The password for the Master Administrator user account (Admin user). For example, `<adminPassword>P45sW0rD</adminPassword>`
outputFolder	No	Optionally, the folder to save the results file in. For example, `<outputFolder>..\ResultReports</outputFolder>`
outputFile	No	Optionally, the name of the Microsoft Excel workbook the analysis is saved in. For example, `<outputFile>UpgradeReport</outputFile>`

   You can also change the configuration file's name, copy the **config.xml** file to create additional sets of configuration options, or create a configuration file by creating a new document and specifying the elements listed above.
5. Save your changes.

▸To analyze resources for upgrade issues

1. In Windows Explorer, navigate the to location you extracted the **.zip** file.
2. Modify the configuration file to set the `<errorsOnly>` element to **false**. Save your changes.
3. Open a Command Prompt window.
4. Navigate the to location you extracted the **.zip** file.
5. Run the following command:
   `PreUpgradeAnalyzer_version.exe configuration`
   where `version` is the version of RapidResponse you are upgrading from, and `configuration` is the name of the configuration file. For example, if you are upgrading from RapidResponse 2014.1, you would specify the version argument as `2014.1`.
   In some cases, a RapidResponse Service Update introduces a significant change that requires a new version of the PreUpgradeAnalyzer utility. In this case, the Service Update level that requires the new version of the utility is indicated in the `version` value, separated from the version number by an underscore. For example, RapidResponse 2016.2 Service Update 5 introduced significant changes to RapidResponse's infrastructure, so the `version` value to analyze an upgrade to a version later than Service Update 5 is `2016.2_5`.
6. When the utility completes, open the Microsoft Excel workbook.
7. The **Illegal field names** worksheet in the workbook lists any field names that include the period character. Review this worksheet.

Testing workbooks for modifications to reference keys

As of RapidResponse 2016.2, reference key fields on tables cannot be modified. Any resources or processes that depend on modifying a value in a reference key field must be reviewed and modified to ensure the process can continue. These processes should be replaced to prevent modifications from producing duplicate records in the table.

The **PreUpgradeAnalyzer** utility can be used to test whether any resource perform modifications on values in reference key fields. This utility is available for download from the Kinaxis Knowledge Network. A version of this utility is available for each RapidResponse version, so you must ensure you use the specific utility designed for the RapidResponse version you are upgrading from. To access this utility, go to https://knowledge.kinaxis.com/s/article/Analyzingresourcesanddataforvectorupgradeissues53745 and click on **PreUpgradeAnalyzer** in the Files section.

The **PreUpgradeAnalyzer** utility takes a configurable XML file that specifies the RapidResponse Server name and other configuration settings. The results of the utility's analysis is a Microsoft Excel workbook. You can specify the location this file is saved and its name in the configuration file.

▸To configure the upgrade utility

1. Extract the utility's **.zip** file into a folder of your choice.
2. Using Windows Explorer, navigate the to location you extracted the **.zip** file.
3. Edit the **config.xml** file.
4. Specify the following options as required.

Element	Required	Description
server	Yes	The RapidResponse Server name. For example, `<server>localhost</server>`
adminPassword	Yes	The password for the Master Administrator user account (Admin user). For example, `<adminPassword>P45sW0rD</adminPassword>`
outputFolder	No	Optionally, the folder to save the results file in. For example, `<outputFolder>..\ResultReports</outputFolder>`
outputFile	No	Optionally, the name of the Microsoft Excel workbook the analysis is saved in. For example, `<outputFile>UpgradeReport</outputFile>`

   You can also change the configuration file's name, copy the **config.xml** file to create additional sets of configuration options, or create a configuration file by creating a new document and specifying the elements listed above.
5. Save your changes.

▸To analyze resources for upgrade issues

1. In Windows Explorer, navigate the to location you extracted the **.zip** file.
2. Modify the configuration file to set the `<errorsOnly>` element to **false**. Save your changes.
3. Open a Command Prompt window.
4. Navigate the to location you extracted the **.zip** file.
5. Run the following command:

   ```
   PreUpgradeAnalyzer_version.exe configuration
   ```

   where `version` is the version of RapidResponse you are upgrading from, and `configuration` is the name of the configuration file. For example, if you are upgrading from RapidResponse 2014.1, you would specify the version argument as `2014.1`.

   In some cases, a RapidResponse Service Update introduces a significant change that requires a new version of the PreUpgradeAnalyzer utility. In this case, the Service Update level that requires

the new version of the utility is indicated in the `version` value, separated from the version number by an underscore. For example, RapidResponse 2016.2 Service Update 5 introduced significant changes to RapidResponse's infrastructure, so the `version` value to analyze an upgrade to a version later than Service Update 5 is `2016.2_5`.

6. When the utility completes, open the Microsoft Excel workbook.
7. The **Key Reference Modifications** worksheet in the workbook lists any workbooks that contain a modification on a reference key field and the worksheet they are performed by. Review this worksheet.

For information about managing these modifiable reference key fields, see "Specifying whether key reference fields are modifiable" on page 175.

Review tables that contain vector data

Depending on how you have configured your data model, your tables that contain vector data might contain more than eight key fields. Upon upgrading to RapidResponse 2015.3 (or later), only eight fields can be used as keys. In this case, a set of eight key fields will be assigned, which might not be the fields you require as keys. In this case, your custom vector data might not be valid.

Before beginning the upgrade process, you must review your data model and modify tables to ensure all vectors contain eight or fewer key fields. For more information, see the *RapidResponse Data Integration Guide*.

Apply pending data model changes

Pending data model changes are lost when upgrading RapidResponse. Before upgrading you should review whether you have any pending data model changes. If so, decide whether you want to apply them. For more information, see the *RapidResponse Data Integration Guide*.

Set up the RapidResponse test environment

Before beginning the upgrade process, you must ensure your RapidResponse test environment is set up to reflect the current state of your RapidResponse production environment from both an application software and data perspective.

The RapidResponse application software should be identical in both environments including service packs and hot fixes.

As well, the following folders (if they exist), should be copied from the production environment to the test environment:

- **C:\RapidResponse\Configuration**
- **C:\RapidResponse\Integration**

Data must be copied from your production environment to your test environment as a data package (also used in the data backup process). The following procedures explain how to create a data package and how to load it onto the RapidResponse test environment.

▶To manually create a data package

1. Sign in to your RapidResponse production environment.
2. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
3. In the **Scheduled System Tasks** worksheet, click anywhere in a row that contains **CreateDataPackage** in the Command column.
4. Click **Run Task Now** ▶.
5. Click **Yes** to confirm you want to run the task.

   By default, a file named in the format **backup_*ServerName_timestamp*.pkg** is saved. By default, this file is stored in **C:\RapidResponse\Packages** folder. However, the file name and location can be customized as described in "CreateDataPackage command" on page 388.

▶To load the RapidResponse data package

1. Ensure the RapidResponse Server is stopped. For more information, see "RapidResponse Windows Services" on page 227.
2. Delete the existing RapidResponse database from the test environment so the data package from the RapidResponse production environment can be loaded and any other **.pkg** files. You can delete the existing **DFS** and **XACT** database folders and files from the **C:\RapidResponse\Data** folder.
3. If it exists, delete the **xact.log** file from the **C:\RapidResponse\Data** folder.
4. Navigate to the folder or location where the **CreateDataPackage** command (from your production environment) saved the backup files package. This might be in the **C:\RapidResponse\Data** or **C:\RapidResponse\Packages** folder.
5. Copy and paste the backup files package into the **C:\RapidResponse\Data** folder on your test environment.
6. Restart RapidResponse Server.

   After decompressing the backup database package, RapidResponse Server uses the backed up database archive.

Note: For more information about stopping and starting the RapidResponse Server service, see "RapidResponse Windows Services" on page 227.

Disable data automation tools

The first thing you should do after properly setting up your RapidResponse test environment is to disable all RapidResponse scheduled processes, if applicable, including:

- **Alerts, Automation Chains, and Scheduled Tasks**—to prevent messages and reports from being sent, and scheduled data modifications from being performed from the system. For more information, see "Alert overrides in a development environment" on page 675.
- **Data publishing**—to prevent data from being sent to RapidResponse data subscribers, remove the data publisher configuration ID record. For more information, see "Creating the publisher ID record" on page 873.
- **RapidResponse system scheduled tasks**—to prevent data from being imported and other RapidResponse tasks from being run, ensure all RapidResponse scheduled tasks are disabled by

setting the **Enable?** column to **N** in the **Scheduled System Tasks** workbook for each task. For more information, see " Scheduling RapidResponse commands" on page 412.

Notes:

- You should also disable any automated custom scripts and RapidResponse OpenAPI programs before continuing the upgrade process. You might also want to contact Kinaxis Customer Support for assistance.
- RapidResponse stores records detailing user-initiated changes (inserts, deletions, and modifications) made to data in RapidResponse scenarios. This data is stored in the DataChange table which is fully described in the *RapidResponse Analytic and Data Model Guide*. During a RapidResponse Server restart, records that exceed a specified threshold (in days) are deleted. The default is 45 days. If you are testing a server upgrade, consider changing this setting to a high number (for example, 999) to avoid processing during the RapidResponse Server startup. For more information, see " Automatic deletion of system records" on page 277.

RapidResponse upgrade steps (On-Premises)

This topic only applies to the On-Premises version of RapidResponse.

This section describes the steps you must follow to properly upgrade RapidResponse. In many cases, these steps are cross referenced to other sections or chapters in this document and require you to jump to those sections or chapters and then come back to the steps in this section.

Before beginning the upgrade process, review all the steps to better understand the process. You should consider this list a checklist of all the steps you will need to perform to complete the upgrade.

1. Upgrade RapidResponse Server in the RapidResponse test environment. For more information, see "Upgrading RapidResponse Server" on page 177.
2. Upgrade the RapidResponse Application Server in the RapidResponse test environment. For more information, see"Upgrading RapidResponse Application Server" on page 189.
3. RapidResponse 2014.4 introduced vector series data in standard and custom tables. This reduced memory consumption because the vector records are not stored as full records, so they do not have the full memory overhead for a record and require the same memory as a single field. If your company has not already started using vector series data, consider this optional upgrade step. For more information, see "Converting standard tables to vector data" on page 203.
4. Upgrade RapidResponse applications and predefined resources (dashboards, workbooks, scorecards, and so on) in the RapidResponse test environment. For more information, see "Upgrading RapidResponse applications" on page 195.
5. Each upgraded predefined resource on the test system should be reviewed and tested to confirm it is working as expected and returning the expected results. If your company had previously modified predefined resources you might want to apply the same modifications to the upgraded resources.
6. Validate custom resources and applications, and results on the test system. For more information, review see"Data model calculations after upgrading" on page 142 in this chapter. Once you are satisfied with the results on the test system, continue the upgrade process.
7. If your company is either publishing RapidResponse data or subscribing to another company's data publishing process, you need to make workbook changes (and configuration changes in some cases) in the test environment. For more information, see "Setting up for data publishing

for On-Premises" on page 871" and Part 9: Configuring RapidResponse subscribers (On-Premises only)".

> **Caution:** After completing these steps, you can now start working on the RapidResponse production environment. However, if a significant amount of time has elapsed since you began working on the upgrade process in the test environment and changes have been made to the production environment's data integration configuration settings, then you should start the process again. For example, if you have changed control table settings or you import control table data that often changes, start the process again.

8. You will begin working in the RapidResponse production environment. Before you begin this portion of the upgrade process, notify your user community that RapidResponse will not be available. All users need to be signed out of RapidResponse and the computer hosting RapidResponse Server should be taken out of service.
9. Copy the data package from the test environment to the production environment. This step is similar to the moving the data package from the production environment to the test environment. For more information, see "Set up the RapidResponse test environment" on page 148.
10. Disable all RapidResponse scheduled processes, if applicable, including:
    - **Alerts, Automation Chains, and Scheduled Tasks**—to prevent messages and reports from being sent, and scheduled data modifications from being performed. For more information, see"Alert overrides in a development environment" on page 675.
    - **Data publishing**—to prevent data from being sent to RapidResponse data subscribers remove the data publisher configuration ID record. For more information, see"Creating the publisher ID record" on page 873.
    - **RapidResponse system scheduled tasks**—to prevent data from being imported and other RapidResponse tasks from being run, disable all RapidResponse scheduled tasks by setting the **Enable?** column to **N** in the Scheduled System Tasks worksheet (Scheduled System Tasks workbook) for each task. For more information, see " Scheduling RapidResponse commands" on page 412.

      You can also turn off all system scheduled tasks by using a Windows registry key. For more information, see "Turning off all scheduled system tasks" on page 418.
    - **Custom scripts and programs**—disable any automated custom scripts and RapidResponse OpenAPI programs.
    - **Data extraction programs**—to prevent enterprise data from being sent to the RapidResponse data extract folders. This is an important step because you might need to change the RapidResponse data extract folder structure.
11. Upgrade RapidResponse Server in the RapidResponse production environment. For more information, see "Upgrading RapidResponse Server" on page 177.
12. Upgrade the RapidResponse Application Server in the RapidResponse production environment. For more information, see "Upgrading RapidResponse Application Server" on page 189.
13. If applicable, upgrade custom applications. Contact Kinaxis Customer Support for more information about upgrading custom applications. If your maintenance agreement includes upgrade of custom applications, contact Kinaxis Customer Support to schedule the upgrade.
14. If your company is either publishing RapidResponse data or subscribing to another company's data publishing process, you need to make workbook changes (and configuration changes in some cases) in the test environment. For more information, see "Setting up for data publishing for On-Premises" on page 871" and Part 9: Configuring RapidResponse subscribers (On-Premises only)".

15. Enable all the processes that were disabled in step 10 including:
    - Alerts, Automation Chains, and Scheduled Tasks
    - Data publishing
    - RapidResponse system scheduled tasks
    - All custom Windows-scheduled tasks
    - Custom scripts and programs
    - Data extraction programs
16. If applicable, upgrade RapidResponse OpenAPI on computers that have custom RapidResponse applications. RapidResponse OpenAPI is used by custom applications to communicate with and retrieve data from RapidResponse Server.

    Only version 10.0 (or later) of RapidResponse OpenAPI is compatible with the current version of RapidResponse Server. The setup program can be downloaded by users. For more information, see "Upgrading RapidResponse OpenAPI applications" on page 217.
17. If applicable, review data publishing and subscribing processes and resources. For more information, see "Setting up for data publishing for On-Premises" on page 871" and Part 9: Configuring RapidResponse subscribers (On-Premises only)".
18. If applicable, modify file locations to allow alerts to write and modify files. For more information, see "Specify storage folders for alert-generated reports" on page 672.
19. If applicable, in the Windows Services configuration, specify the user account the RapidResponse Service Host uses to sign in to RapidResponse and run alerts, scheduled tasks, and automation tasks.

Upgrading RapidResponse with Service Updates

RapidResponse Service Updates are provided by Kinaxis to address issues and provide additional functionality. Service Updates are delivered monthly, and allow you to keep your RapidResponse instance continuously up to date. Each Service Update can contain enhancements, resolved issues, and security updates.

A Service Update is available from Kinaxis Customer Support, and typically includes changes for multiple RapidResponse components, including RapidResponse Server, RapidResponse Application Server, and RapidResponse applications. You can choose which components to update, however, some components depend on others to continue to function as expected. For example, changes to resources depend on the corresponding changes to the RapidResponse Application Server, so these must have the same Service Update applied. However, RapidResponse Server and Application Server can have different Service Updates applied, as long as the RapidResponse Server Service Update version is not greater than the Application Server version. It is recommended you apply updates to all RapidResponse components included in a Service Update.

You should save the installation image to a location on the computers that RapidResponse Server and RapidResponse Application Server are installed on.

Before you apply a Service Update, you should Run the Capture command to save your transactions, and create a backup data package in case you need to restore your data. These ensure the Service Update is applied to stable data, and provides the means to recover if issues are encountered during the upgrade process. For more information, see "Predefined scheduled system tasks" on page 381.

If you are using a failover cluster, before applying a Service Update to the active server, you must stop any standby servers before starting the Service Update process. Otherwise the standby server is activated, and the upgraded server cannot apply data model changes introduced in the Service Update because the standby server cannot apply data model changes.

After applying the Service Update to the active server, you must also apply the Service Update to the standby server before restarting it. For more information about failover, see "RapidResponse Server failover clustering" on page 289.

Service Update content is provided in installation programs, which you can install similarly to other upgrades you might perform. For more information, see "Upgrading RapidResponse Server with Service Updates" on page 182 and "Upgrading RapidResponse Application Server with Service Updates" on page 192.

Updates applied to RapidResponse Server also update the supplemental application components and the ServiceHost service. If you do not apply the Service Update to RapidResponse Server, you must upgrade these components by running their installation programs.

Service Update content for applications and resources is provided in resource package (.RPK) files that contain updated resources for RapidResponse applications. You must import the content of these resource packages to update the resources, instead of running the resource installation program. For more information, see "Upgrading application resources (On-Premises)" on page 198.

▸To apply Service Update content to RapidResponse components

1. Run the **Capture** scheduled system task. For more information, see "Predefined scheduled system tasks" on page 381.
2. Run the **Create Backup** scheduled system task. For more information, see "Predefined scheduled system tasks" on page 381.
3. Apply the Service Update to RapidResponse Server (optional). For more information, see "Upgrading RapidResponse Server with Service Updates" on page 182.
4. If you did not apply the Service Update to RapidResponse Server, do the following:
   - Run the application supplemental installer (required). For more information, see "Upgrading application components" on page 184.
   - Run the ServiceHost service installer (required). For more information, see "Upgrading the RapidResponse ServiceHost service" on page 185.
5. Apply the Service Update to RapidResponse Application Server (required). For more information, see "Upgrading RapidResponse Application Server with Service Updates" on page 192
6. Import resource packages for each required application (optional but recommended). For more information, see "Upgrading applications through Service Updates" on page 200.

Updating resources in Service Updates

Updates to an existing and installed application can be applied by importing a resource package (.RPK file). A resource package for each application contains resources of many types to support a given application or area, including linked or dependent resources that the application depends on. For more information, see "Upgrading applications through Service Updates" on page 200.

Reverting Service Updates

If, after the service update installation, there is a need to revert to the previously installed version of RapidResponse, all RapidResponse components should be uninstalled and the previous version reinstalled. If you are using Single-Sign On (SSO), this will also need to be re-configured. For complete information about installing and uninstalling RapidResponse components, see "RapidResponse installation overview" on page 99.

Once the prior version is reinstalled, scripts can be run that restore various backed up RapidResponse Server configuration files (for example, Server registry) and RapidResponse Application Server configuration files (for example, Web.config) to their prior state.

▸To revert to backed up RapidResponse Server configuration files

1. Browse to the **RapidResponse\Backup** folder.
2. Right-click the **RR_Restore.ps1** file and select **Run with Power Shell**.
3. Do one of the following:
   - To restore from the latest (or only) datetime-stamped folder, press **Enter**.
   - To restore from a specific datetime-stamped folder (if more than one), type in the name of the folder seen under **RapidResponse\Backup**.

▸To revert to backed up RapidResponse Application Server configuration files

1. Browse to the **Program Files\Kinaxis\RapidResponse\Backup** folder.
2. Right-click the **RR_Restore.ps1** file and select **Run with Power Shell**.
3. Do one of the following:
   - To restore from the latest (or only) datetime-stamped folder, press **Enter**.
   - To restore from a specific datetime-stamped folder (if more than one), type in the name of the folder seen under **Program Files\Kinaxis\RapidResponse\Backup**.

Post-update considerations

When you apply a Service Update, your configurations are preserved during the update process.

This section describes modifications in specific Service Updates that might have an impact on your operations.

Table size after applying Service Update 1904

Service Update 1904 introduces a limit to the number of input fields allowed in a table. If you have a table with more than 700 input fields, the server is unable to start after applying this Service Update. To resolve this, you can adjust the **InputFieldLimit** registry setting to a size that accommodates your table. For more information, see "Location of registry settings" on page 351.

Tables this large are not recommended, and you should also revise your tables to limit the number of fields, which also assists with reducing memory consumption and improving the usability of your database. Smaller tables allow you to focus the table on specific data. By creating several smaller tables with references you can define records that are stored once and reused across several tables, instead of

duplicating the same data values in every record in a large table. For more information about designing tables, see the *RapidResponse Data Integration Guide*.

Post-upgrade considerations

This section discusses changes that some administrators might need to make to the RapidResponse production environment after completing the upgrade process. These include:

- Review the data model settings and log files. For more information, see "Data model settings and log files" on page 156.
- The RapidResponse Query Language is used when writing query expressions that return data from the RapidResponse database for use in resources such as workbooks. New versions of RapidResponse sometimes include changes to the RapidResponse Query Language. In some cases, this includes changes meant to reduce or prevent occurrences of ambiguous syntax that could result in unintended or unexpected results. When such changes are made, a new compatibility level is introduced. Each new compatibility level defines a set of syntax which was previously valid, but has since been deemed ambiguous and returns an error. After upgrading, use the Search Resources Settings dialog box to find workbooks that do not validate against a particular compatibility level. For more information, see "Query Language syntax and compatibility levels" on page 156.
- The **VersionReclaimSweep** system command is used to clean up the internal version structure used to support scenarios. The version reclaim process reduces the size the RapidResponse database and frees system memory. It is recommended that this command be run after upgrading RapidResponse to a newer version. For more information, see "VersionReclaimSweep command" on page 411.
- The **DataIntegrityCheck** system command performs a test on the RapidResponse database for invalid references and inconsistent counts in scenarios. It is recommended that this command be run after upgrading RapidResponse to a newer version. For more information, see "Running DataIntegrityCheck after upgrading" on page 160.
- If you are upgrading from RapidResponse 11.0, decide whether customized copies of predefined dashboards should be kept. For more information, see "Dashboard upgrade from RapidResponse 11.0" on page 161.
- If you are upgrading from RapidResponse 11.1 (or earlier), provide the URL that users use to sign into RapidResponse. For more information, see "Web server URL configuration" on page 162.
- If you are using the On-Premises version of RapidResponse and you have been using customization settings, you might want to copy these settings into the new **web.config** file. For more information, see "Configuration file for Application Server" on page 162.
- If you are using the On-Premises version of RapidResponse, consider updating workbooks to avoid using XML-based Select controls. For more information, see "XML deprecation in workbook properties" on page 163.
- If you are upgrading from RapidResponse 2013.4 (or earlier), replace chained alerts and scheduled tasks with automation chains. For more information, see "Replacing chained alerts and scheduled tasks" on page 165.
- If you are upgrading from RapidResponse 11.0, it is recommended that you manually edit some macros to match the expressions used in the newer version of RapidResponse. For more information, see "Macros" on page 168.
- If you are upgrading from RapidResponse 2013.4 (or later), review the Hidden Data Changes worksheet and consider scheduling the Perspective - Hidden Data Changes alert to run automatically. For more information, see "Changes to perspectives" on page 169.

- If you are upgrading from RapidResponse 2014.4 (or earlier), activate the non-unique scenario name feature once you have reviewed resource and system settings for compatibility. For more information, see "Non-unique scenario names" on page 170.
- If you are upgrading from RapidResponse 2014.4 (or earlier) and have enabled optional keys on the Allocation, BillOfMaterial, OnHand, or Operation tables, replace the optional keys with any key fields you want to use for identifying records. For more information, see "Replacing optional keys with key fields" on page 174.
- If you are upgrading to RapidResponse 2015.3 (or earlier), you might have processes that modify reference key fields in tables. These fields are read-only for RapidResponse 2016.2 (or later), however, upon upgrading, a processing rule is added to the RapidResponse Administration workbook that allows these values to remain modifiable. It is recommended you make all reference key fields read-only by replacing the operations that modify the key fields with an operation that inserts a new record with the required value and deleting the existing record. For more information, see "Specifying whether key reference fields are modifiable" on page 175.

Data model settings and log files

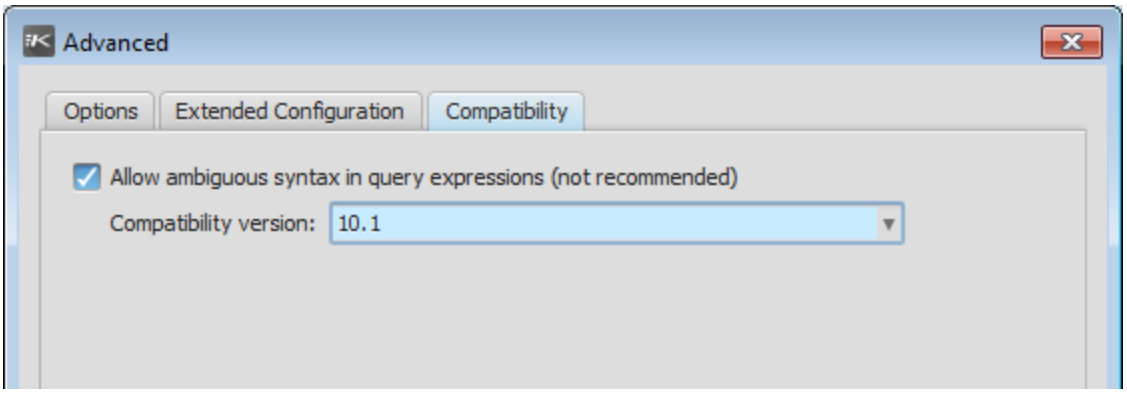
After completing the upgrade process, review the "Data Model Change Summary" section in the *RapidResponse Analytic and Data Model Guide*. This section outlines changes to the data model, including new and modified tables and fields, and outlines the changes to the analytics. It might also describe changes you need to make to your data integration settings.

Log files

If you are using the On-Premises version of RapidResponse, all log files are stored in the **C:\RapidResponse\Logs** folder on the same computer as RapidResponse Server. The **Logs** folder location cannot be customized; that is, the Logs folder can only be a sub-folder to the main RapidResponse folder. If you have any scripts or batch files that rely on log files, make the necessary adjustments. For more information, see "Reviewing system status and operation logs" on page 421.

Query Language syntax and compatibility levels

The RapidResponse Query Language is used when writing query expressions that return data from the RapidResponse database for use in resources such as workbooks. New versions of RapidResponse sometimes include changes to the RapidResponse Query Language. In some cases, this includes changes meant to reduce or prevent occurrences of ambiguous syntax that could result in unintended or unexpected results. When such changes are made, a new compatibility level is introduced. Each new compatibility level defines a set of syntax which was previously valid, but has since been deemed ambiguous and returns an error. As shown in the following illustration, compatibility levels can be viewed or set on a workbook by workbook basis within the Workbook Properties' Advanced dialog box.



All new workbooks are automatically set to the latest compatibility level, and it is recommended that all workbooks use that latest compatibility level. However, to avoid breaking existing resources, or in cases where the older ambiguous syntax is truly required, an earlier compatibility level can be used. The following compatibility levels are supported in RapidResponse:

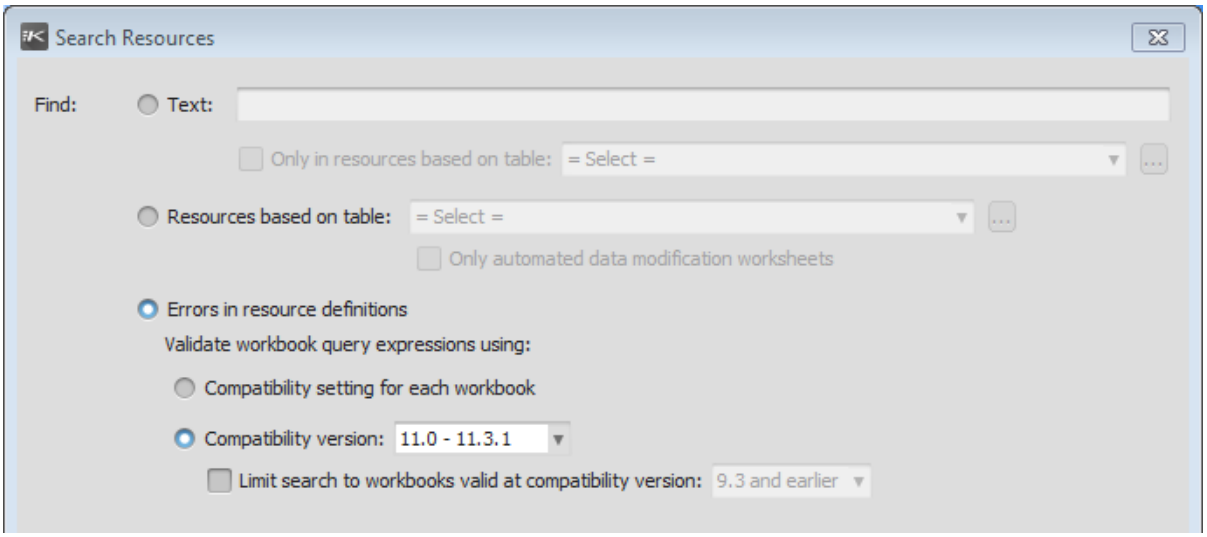
- 2014.1 and later
- 11.0 — 11.3.1
- 10.1
- 9.4 — 10.0
- 9.3 and earlier

During a RapidResponse upgrade, the upgrade program attempts to set all workbooks in your system to the latest compatibility level. However, if any workbooks are found containing worksheets that do not validate against the latest compatibility level, then the workbooks are set to the highest compatibility level against which they do validate.

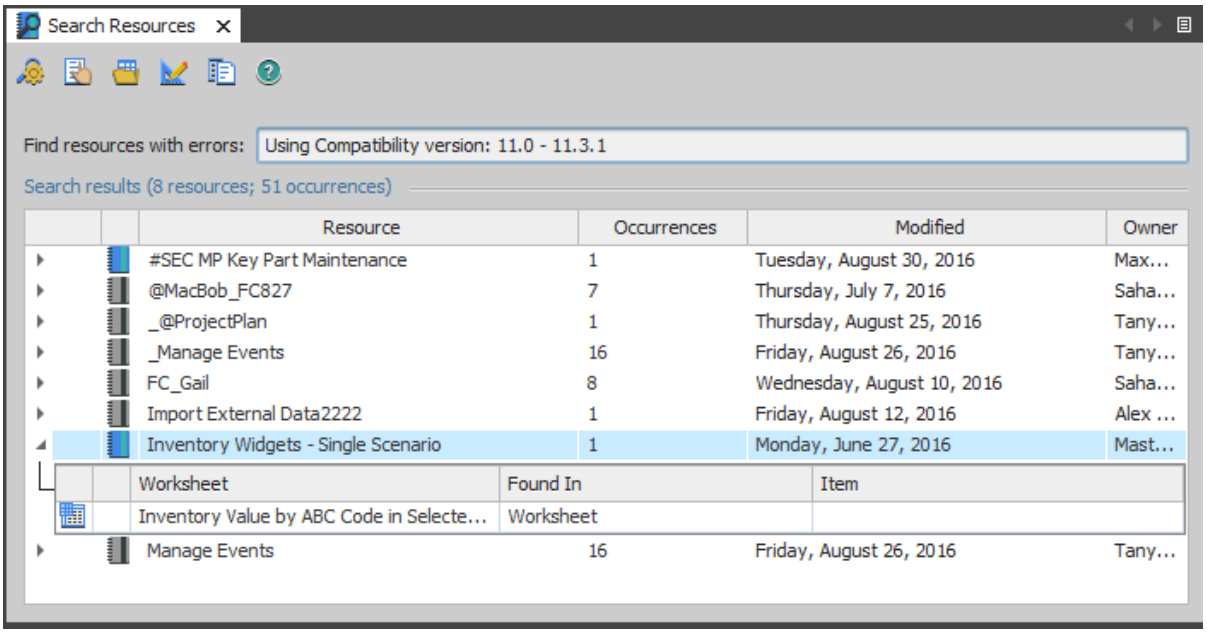
On-Premises: A log of those workbooks is kept in the **Upgrade x.y.z.log** file, and this file should be reviewed after completing the RapidResponse Application Server upgrade to determine which workbooks contain ambiguous syntax.

It is then recommended that you modify the column and filter expressions in those workbooks so that they do validate against the latest compatibility level, and then manually set each to the latest compatibility level.

After upgrading, you can also use the Search Resources Settings dialog box to find workbooks that do not validate against a particular compatibility level. For example, you might typically search for workbooks that do not validate at the latest compatibility level. As shown in the following illustration, you can also restrict this search to only workbooks that did validate against an earlier compatibility level. For example, you can search for workbooks that fail validation at the latest compatibility level but which did validate at the previous compatibility level. This lets you focus on those workbooks which have syntax issues introduced by the most recent upgrade, while ignoring those with long standing issues you might no longer be concerned with.



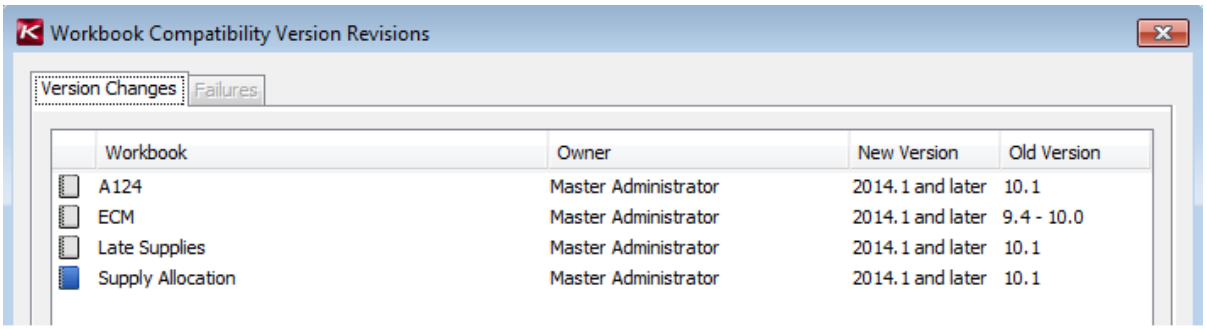
After specifying the type of validation issues you want to search for, the results are then shown on the Search Resources tab. For each workbook with a validation error, you can see the specific worksheet, column, or filter that had the issue and potentially link directly to the expression with the problematic syntax. From there you can fix the expression and update the workbook's compatibility level as required. The following illustration shows a list of workbooks that failed validation.



Occasionally, validation errors reported across many different workbooks might be resolved by a single property change in RapidResponse. For example, Version 11.0 introduced a new money data type and many standard fields in the RapidResponse data model were changed from being quantities to being money. As a result, certain existing expressions which combine these money fields (previously quantities) with custom quantity fields do not validate at the latest compatibility level until the custom fields are changed to use the money data type. Once this change is made, however, many workbooks can potentially be upgraded to the Version 11.0 compatibility level. To reduce the effort in manually

updating each of these workbook's compatibility levels, you can use a utility in the Resources workbook that automatically updates all workbooks in RapidResponse to the latest compatibility level against which they validate. The modified workbooks are then reported in the Workbook Compatibility Version Revisions dialog box.

The following illustration shows a list of workbooks automatically upgraded to higher compatibility level.



Any resources that cannot be upgraded because they are checked out are listed on the Failures tab. If necessary, you can discard the author's check out and perform the resource upgrade again. For more information, see "Discarding a resource check out" on page 743.

> **Note:** For more information about changes to the RapidResponse Query Language, compatibility levels, and modifying worksheets that use ambiguous syntax, see the *RapidResponse Resource Authoring Guide*.

▸To search for workbooks that fail validation against a specified compatibility level

1. From the **Tools** menu, click **Search Resources**.
2. In the **Find** area, click **Errors in resource definitions**.
3. Click **Compatibility version** and then select the compatibility level to validate against by choosing one of the following from the list:
   - **2014.1 and later**
   - **11.0 — 11.3.1**
   - **10.1**
   - **9.4 — 10.0**
   - **9.3 and earlier**

   For example, if you wanted to validate against the latest compatibility level, select **2014.1 and later**.
4. Optionally, if you only want to validate those workbooks that pass validation against an earlier compatibility level, select the **Limit search to workbooks valid at compatibility** level check box and then select a compatibility level from the list. Valid options are:
   - **11.0 — 11.3.1**
   - **10.1**
   - **9.4 — 10.0**
   - **9.3 and earlier**

For example, if you only wanted to search for workbooks that fail validation because of changes introduced at the latest compatibility level, select **11.0 — 11.3.1** from the list.

5. Click **Search**.

   All workbooks that failed validation against the specified Query Language compatibility level are shown in the Search Resources window, and each worksheet within it that failed validation is shown underneath.

6. If you want to fix a workbook so that it validates against the latest query compatibility level, do the following:
   - In the **Search Resources** window, expand the workbook and double-click a worksheet.
   - When prompted to set the workbook to the latest query compatibility level, click **Yes** to allow RapidResponse to open the Worksheet Properties dialog and set focus to the area of the worksheet with the validation error. If you click **No**, RapidResponse opens the worksheet but does not place focus on the error.
   - In the **Worksheet Properties** dialog box, fix the identified error to which RapidResponse has set focus.
   - Repeat for any other worksheets identified in the **Search Results** dialog box.

Note: If you do not receive a prompt to change the workbook's query compatibility level, this indicates that either the error being reported would exist regardless of the query compatibility level being searched, or that workbook's query compatibility level has previously been set to a level against which it does not validate.

▸To upgrade all workbooks to the latest compatibility level at which they validate

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click the **Workbooks** tab.
3. On the workbook toolbar, click **Increase Workbook Compatibility Version** .
4. Click **Yes** when prompted.

   The **Workbook Compatibility Version Revisions** dialog box displays the details of each workbook whose compatibility level was updated.

Running DataIntegrityCheck after upgrading

The DataIntegrityCheck system command performs a test on the RapidResponse database for invalid references and inconsistent counts in scenarios. It is recommended that this command be run after upgrading RapidResponse to a newer version. For more information about this command, see "DataIntegrityCheck command" on page 391. For more information about running system commands, see "Using commands and scheduled system tasks" on page 415.

The execution of the DataIntegrityCheck system command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423. In addition, issues are written to the **Server.log** log file and a message is sent to all system administrators.

After upgrading to RapidResponse 2016.2 (or later) from 2015.3 (or earlier), running the **DataIntegrityCheck** command can return the following message:

```
Duplicate record on Table 'System::UserVariable
```

If this message is returned then your system has duplicate profile variables. RapidResponse workbooks can be customized for different users or groups through the use of profile variables. Profile variables let you create one report that can be sent to multiple users with different information needs. For example, you can create a profile variable and assign it to each of your suppliers.

You can review the duplicate profile variables in the Macros and Profile Variables workbook. To open this workbook, from the **Administration** pane, under **User Accounts**, click **User Profile Variables**. Delete the duplicates in the **Profile Variables** worksheet. You should delete the profile variables that are not being used by RapidResponse. If you cannot determine which profile variables to delete or you cannot find the duplicate profile variables (they might be filtered out of the worksheet), then contact Kinaxis Customer Support for further assistance.

You should contact Kinaxis Customer Support for assistance if any other warnings or errors occur after running the DataIntegrityCheck system command.

Dashboard upgrade from RapidResponse 11.0

Because of changes in the underlying dashboard technologies, upgrading from RapidResponse 11.0 impacts pre-existing dashboards. The upgrade program converts the format of existing dashboards to a new internal format.

If users of the predefined dashboards had modified the layout, then upgrade program creates a copy of the modified dashboard retaining the changes. User layout changes can include resizing widgets, adding widgets from the tray, and removing widgets from a dashboard.

The RapidResponse Master Administrator owns all predefined resources including dashboards and might need to manually perform some actions after the RapidResponse upgrade is completed. System administrators can also perform these actions.

This section describes the conversion process and is dependent on the state of dashboard at the time of the RapidResponse upgrade.

1. The original predefined dashboard is converted into the new format and retains the original name. It also maintains the original sharing properties so that all users who had access to the dashboard continue to have access. However, user preferences such as bucket settings, chart settings, and hidden columns are reset to the original dashboard preference settings. Preferences are not reset if users who had access to the dashboard did not modify their personal layouts.
2. For each user who changed the layout of the predefined shared dashboard, the upgrade program creates a new shared dashboard.

   For example, assume two users (User1 and User2) modified the layout of a predefined dashboard. The upgrade program creates MyDashboard_UserID1 and MyDashboard_UserID2 dashboards. The MyDashboard_UserID1 dashboard is owned by the Master Administrator and is shared with User 1 (and all administrators). The MyDashboard_UserID2 dashboard is also owned by the Master Administrator is shared with User 2 (and all administrators).

After the upgrade, the Master Administrator (or other administrators) needs to work with individual users and determine whether the user should be using the dashboard with the original layout or their customized layout version. To maintain consistency across your organization, administrators might want to delete the shared dashboards with the customized layouts.

The widget preferences are maintained. Preferences include items such as bucket settings, chart settings, and hidden columns.

Note: Some users have a dashboard set to automatically open upon sign in. If a copy of this dashboard is created by the upgrade program, then the copy is set to automatically open upon sign. If you delete the copy, then users might want to reset another dashboard to automatically open upon sign in. Alternately, a user administrator can reset this for users. For more information, see " Automatically opening resources upon sign in" on page 562.

Web server URL configuration

This topic only applies to the On-Premises version of RapidResponse.

RapidResponse 11.2 introduces new functionality to send links to resources, reports, and web addresses using Message Center and email messages. If you are upgrading from RapidResponse 11.1 (or earlier), you must provide the address (or URL) users use to sign into RapidResponse. This information is added to the **Message Center and Email** dialog box. For more information, see "To configure an email server" on page 276.

Configuration file for Application Server

This topic only applies to the On-Premises version of RapidResponse.

The **web.config** configuration file holds customization settings for the Java client. This includes the following settings:

- Single sign on. For more information, see " Configuring single sign-in for On-Premises" on page 835.
- The maximum size of integration package file. For more information, see the *RapidResponse Data Integration Guide*.
- Java Runtime Environment (JRE) memory settings for all users. For more information, see "Memory settings for the Java client" on page 544.
- File size limits for importing data. For more information, see "Setting file size limits for importing data" on page 653.
- Security of communication settings between RapidResponse Server and RapidResponse Application Server. For more information, see "Encrypting communication between RapidResponse Server and RapidResponse Application Server" on page 284.

Upon upgrade, the **web.config** file is replaced with a new version that does not include the customization settings. The original versions of the file with the customization settings is saved as **web.config.bak**.

If your company had applied any customization settings to the web.config, you need to copy them from the **web.config.bak** file to the new version of **web.config**.

The **web.config** file is located in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder on the computer where RapidResponse Application Server is installed. It can be edited with an XML or text editor.

Notes:

- If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of

RapidResponse Application Server is installed.

- If you are upgrading by applying a RapidResponse 2016.2 Service Update, your customizations in the **web.config** file are automatically preserved.

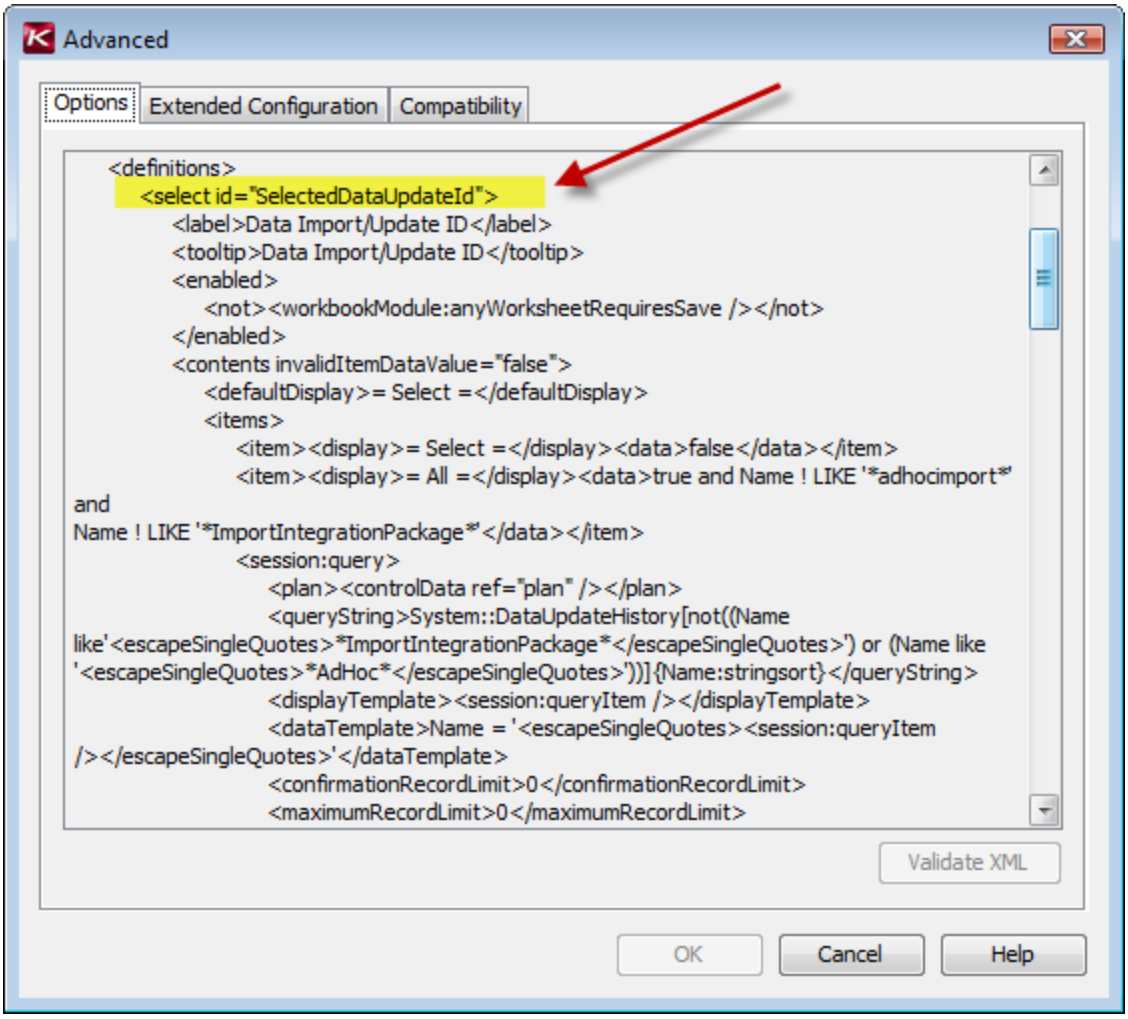
XML deprecation in workbook properties

This topic only applies to the On-Premises version of RapidResponse.

From the General tab of the Workbook Properties dialog box or the Worksheet Properties dialog box, you can clicked the Advanced button to access a dialog box to add XML code. This code customizes workbooks and the worksheets. For example, the XML code can be used to add custom data selection controls.

A future version of RapidResponse will no longer support the use of XML code in workbook definitions. This was announced in RapidResponse 11.2 in the Release Notes. It recommended you do not create or copy workbooks and worksheets that use XML code in the Options tab of the Advanced dialog box.

The following illustration shows an example of the Advanced dialog box with XML code in Options tab.



The XML code was often used to define a Select control. A Select control could be used to add a custom control to a worksheet toolbar to filter data in a special manner or to limit the availability of scenarios. The support for the XML-based Select control might be removed before the general support for XML code in workbooks is removed.

When upgrading to RapidResponse 2013.4 (or later) from RapidResponse 2013.2 (or earlier), messages will be written to the **Upgrade.log** file (available to system administrators) that summarize which workbooks, if any, include an XML-based Select control. The workbooks listed will include predefined workbooks supplied by Kinaxis and custom workbooks.

The **Upgrade.log** file is created when the RapidResponse Server is upgraded. The upgrading of predefined resources occurs after the RapidResponse Server is upgraded and, if you choose to, replaces older versions of predefined workbooks with new versions. The new versions of the predefined workbooks do not include any XML-based Select controls. The replaced workbooks are backed up. For more information about upgrading predefined resources, see the *RapidResponse Applications Guide*.

The predefined resources upgrade might remove all instances of workbooks with the XML-based Select controls. However, there are two cases where workbooks might continue to include XML-based Select controls:

- Custom workbooks.
- Predefined workbooks that have not been replaced by the upgrade program.

Workbooks that include XML-based Select controls continue to function. However, workbook authors are warned when they edit workbooks that include XML-based Select controls.

Disabling workbooks with XML-based Select controls

As an administrator you can choose to disable all workbooks that use XML-based Select controls. Disabled workbooks cannot be opened by RapidResponse users and processes. You might consider this to prevent the propagation of additional workbooks with XML-based Select controls.

▸To disable workbooks with XML-based Select controls

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **ID** box, type **Client_AllowWorkbookXmlControls**.
   - In the **Value** box, type **N**.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.

Note: Set the process rule to **Y** to re-enable the workbooks that include XML-based Select controls.

Replacing XML-based Select controls

In most cases, XML-based Select controls can be replaced by one of the following:

- Workbook filters

  In particular, you might be able to take advantage of list variables for fixed values or filter variables for a control to filter data. Filter variables were introduced in RapidResponse 2013.4.

- Limiting the scenarios available from a workbook. RapidResponse 2014.1 introduced a new workbook property that allows authors to limit the scenarios available to a workbook user.

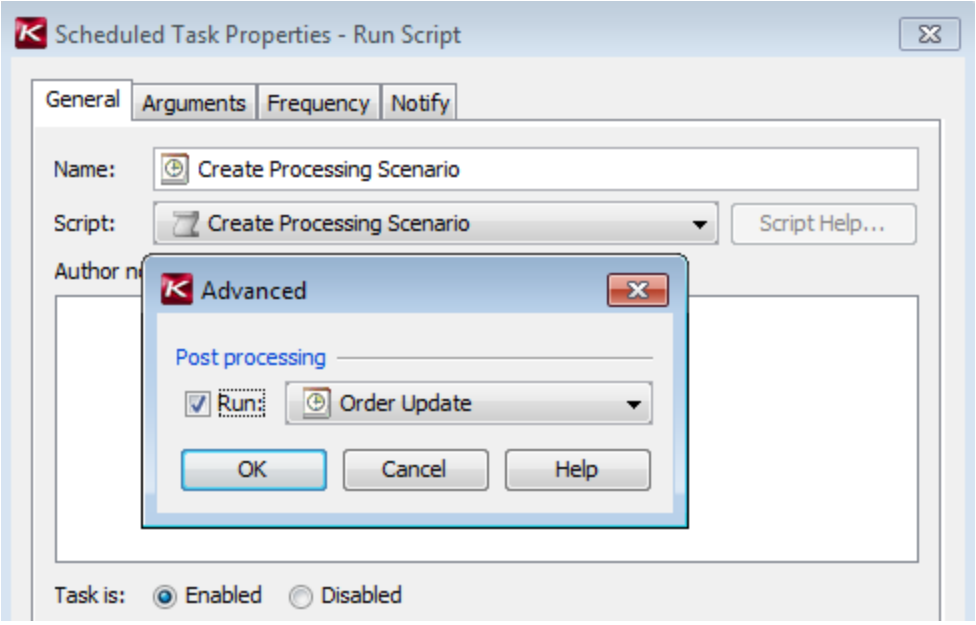
For more information about workbook filters and limiting scenarios, see the *RapidResponse Resource Authoring Guide*.

Replacing chained alerts and scheduled tasks

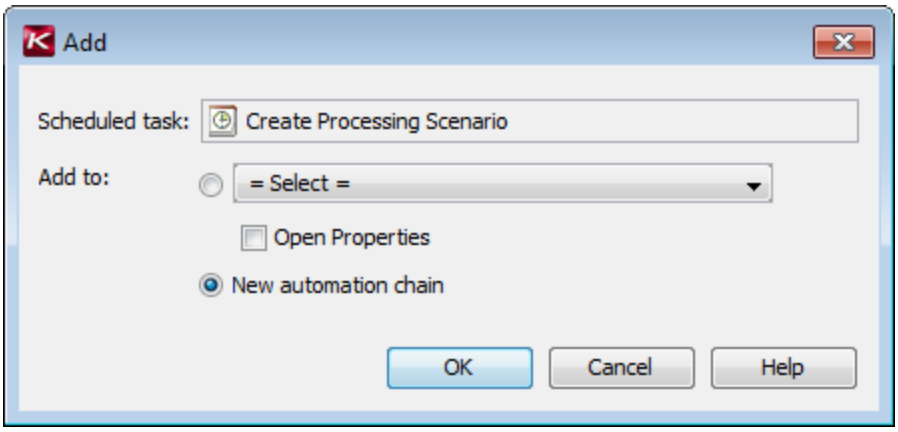
When you upgrade to RapidResponse 2014.1 (or later) from RapidResponse 2013.4 (or earlier), you cannot create new chained alerts or scheduled tasks, which run another alert or scheduled task on completion. Chained alerts created before the upgrade continue to function, but should be replaced with automation chains, which define the alerts and scheduled tasks to run, and the sequence they run in.

Chained alerts and scheduled tasks were created by specifying a post-processing step that runs another alert or scheduled task.

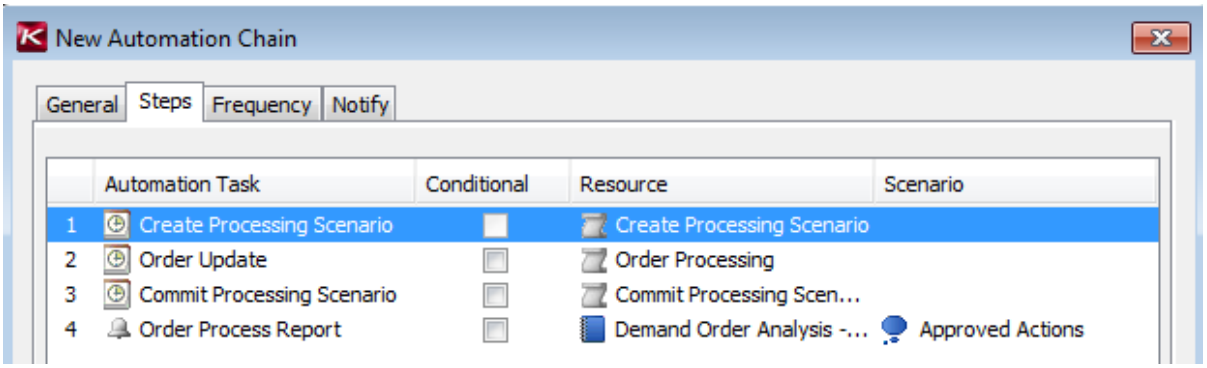
The following illustration shows the post-processing step in RapidResponse 2013.4 (or earlier).



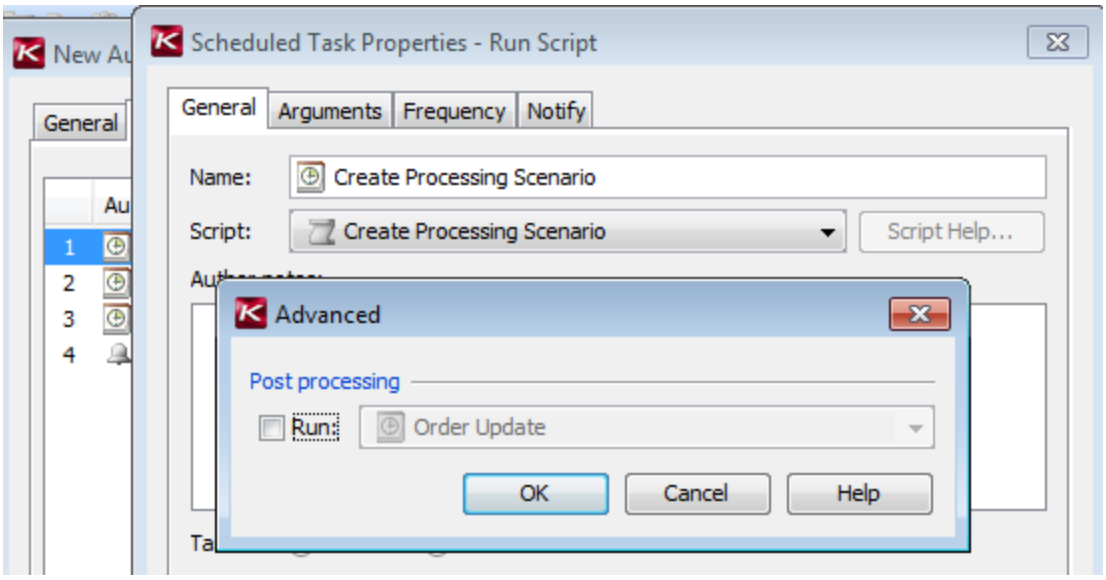
To replace these with automation chains, you can create an automation chain by adding the first alert or scheduled task to a new automation chain. This creates an automation chain with that alert or scheduled task as its first step.



When you add an alert or scheduled task that runs another, each chained alert or scheduled task is automatically added as a step in the automation chain. If version control is turned on in your system, you must check out each step to modify the properties. In the following illustration, all steps have been added to the automation chain.



After adding the steps to the automation chain, you must disable the post-processing in each step of the automation chain. Otherwise, the automation chain does not run.



For information about creating automation chains, see the *RapidResponse User Guide*.

▸To convert a chained alert to an automation chain

1. In the **Explorer**, select the first alert or scheduled task in a chain.
2. On the **Actions** menu, click **Add to Automation Chain**.
3. In the **Add to Automation Chain** dialog box, click **New Automation Chain**, and then click **OK**.
4. In the **New Automation Chain** dialog box, in the **Name** box, type a name for the automation chain.
5. Click the **Steps** tab.
6. For each step, do the following:
   - Select the step.
   - If version control is turned on in your system, click **Check Out**.
   - Click **Properties.**
   - Click **Advanced.**
   - Clear the **Run** check box.
   - Click **OK**.
7. Click **OK**.
8. If you are using resource version control, check in the automation chain.
9. Share the automation chain with the users who require access to it.

Caution: If you have enabled resource versioning, do not revert changes on the alerts or scheduled tasks that are modified to run as part of an automation chain. If the changes are reverted, the automation chain will not be able to run, which might cause processes to not complete.

Note: For information about version control of resources, see the *RapidResponse Resource Authoring Guide*.

Macros

Macros are reusable expressions that can be used in multiple contexts without having to retype the expression.

The upgrade program imports new macros to the RapidResponse database. Existing macros are not automatically modified and are left unchanged. After upgrading it is recommended you manually edit macros to match the expressions used in the newer version of RapidResponse.

Macros can be modified in the Macros and Profile Variables workbook. To open this workbook, from the **Administration** pane, under **User Accounts**, click **User Profile Variables**.

The following table describes the macros that have been modified and the workbooks that use the macros. Ensure you review all macro changes.

These macros were modified in RapidResponse 11.0:

Macro name	Expression	Workbooks
RR_ BOMAltOrphan	`(not has Assembly.PartSources [Type.PlannedOrderSupplyType.Source = 'Make' and BOMAlternate = ^Alternate]) and (not has Assembly.ScheduledReceipts [Order.Type.Source = 'Make' and BOMAlternate = ^Alternate])`	• Data Integrity - Material • Data Integrity Metrics - Material
RR_ BomSubstitutio n	`not IsNull(SubstituteGroup) and SubstituteGroup.Type.ProcessingRule <> 'ignore' and not has SubstituteGroup.BillOfMaterial [assembly.self=^assembly.self & substitutionSequence = 0]`	• Data Integrity - Material • Data Integrity Metrics - Material
RR_IndValue	`((Order.Type.ProcessingRule in 'SalesActual','Regular') and ((((? UnitSellingPrice>0 UnitSellingPrice Part.AverageSellingPrice)*Quantity )>MoneyValue(500000)) or (((? UnitSellingPrice>0 UnitSellingPrice Part.AverageSellingPrice)*Quantity )<MoneyValue(5)) ))`	• Data Integrity - Material • Data Integrity Metrics - Material
RR_PSCost	`(((? Part.UnitOfMeasure.BaseConversion > 0 and SupplierUoM.BaseConversion > 0 Part.UnitOfMeasure.BaseConversion/SupplierUoM.BaseConversion 1.0)* EffUnitCost < (0.5* CONVERTONDATE (Part.StdUnitCost, ASSOCIATEDDATE(EffUnitCost)))) or ((? Part.UnitOfMeasure.BaseConversion > 0 and SupplierUoM.BaseConversion > 0 Part.UnitOfMeasure.BaseConversion/SupplierUoM.BaseConversion 1)* EffUnitCost > (2 * CONVERTONDATE (Part.StdUnitCost, ASSOCIATEDDATE(EffUnitCost)))))`	• Data Integrity - Material • Data Integrity Metrics - Material

Macro name	Expression	Workbooks
RR_ SRPriceRange	`(((Quantity * (? UnitPrice > 0 CONVERTONDATE(UnitPrice, ASSOCIATEDDATE(EffectiveUnitPrice)) PartSource.EffUnitCost)) < MoneyValue(5)) or ((Quantity * (? UnitPrice > 0 CONVERTONDATE(UnitPrice, ASSOCIATEDDATE (EffectiveUnitPrice)) PartSource.EffUnitCost)) > MoneyValue(500000)))`	• Data Integrity - Material • Data Integrity Metrics - Material
RR_SRUnitPrice	`(UnitPrice > 0 and (CONVERTONDATE(UnitPrice, ASSOCIATEDDATE(EffectiveUnitPrice)) < (0.5 * PartSource.EffUnitCost) or CONVERTONDATE(UnitPrice, ASSOCIATEDDATE(EffectiveUnitPrice)) > (2 * PartSource.EffUnitCost)))`	• Data Integrity - Material • Data Integrity Metrics - Material
RR_SRValue	`(EffectiveUnitPrice * Quantity)`	• Multi-Enterprise Managemen t Metrics • Operations Metrics

Changes to perspectives

Scenarios that have perspectives applied can be modified. In fact, users can also modify data that has a perspective applied to it. However, after the data has been modified it is immediately overlaid with the values defined in the perspective definition. The user-modified data will not affect analytic calculations or query results as it is considered hidden.

Prior to RapidResponse 2014.1, user-modified data would not be overlaid by a perspective. It would also be used in analytic calculations or query results. This change might impact your RapidResponse processes or analytic calculations. After upgrading from RapidResponse 2013.4 (or earlier) to RapidResponse 2014.1 (or later), review the Hidden Data Changes worksheet in the Perspectives workbook. This new worksheet identifies changes that have been made to scenario data that are not visible because a perspective value is overlaid.

RapidResponse also includes the **Perspective - Hidden Data Changes** alert which is shared to all system administrators. This alert is based on the Hidden Data Changes worksheet and can be used to notify administrators and users about user-modified data that has been overlaid by a perspective. The alert is unscheduled but administrators should consider scheduling it to run on a weekly or monthly basis.

For more information about perspectives, see "Scenario perspectives" on page 725.

Record identification fields

If you have upgraded to RapidResponse 2014.4 (or later) from RapidResponse 2014.2 (or earlier) and have customized identification fields on tables, the customizations might be defined without a namespace qualification. These customizations are considered invalid in RapidResponse 2014.4 (or later), and must be updated to properly namespace-qualify the fields. These modifications can be performed automatically by opening the Data Model dialog box, and then applying the changes to the active data

model. For more information about customizing the data model, see the *RapidResponse Data Integration Guide*.

▸To update namespaces on identification fields

1. In the **Administration** pane, under **Data**, click **Data Model**.
2. Click **OK**.
3. Click **Yes** to apply changes to the active data model.
4. Click **Apply**, and then click **Yes**.

Non-unique scenario names

In RapidResponse 2014.4 (and earlier), no two scenarios on a RapidResponse system could have the same name, so in most cases, scenarios referred to in resource definitions did not have a scope (private or shared) specified. As of RapidResponse 2015.3, multiple scenarios with the same name can exist, so more that just the name is needed to identify a scenario. The scope, and in some cases the owner's user name, are needed.

If you are upgrading from RapidResponse 2014.4 (or earlier) to RapidResponse 2015.3 (or later), the following steps are recommended.

- Review resources (dashboards, workbooks, and so on) that refer to scenarios and make any necessary changes to ensure that they will continue to function as intended.

  RapidResponse automatically scopes scenarios—that is, identifies them as private or shared—in resource definitions during upgrade. In some cases, it might not assign the correct scope for your purposes, so resource authors and administrators might need to edit resources after upgrade. For more information, see "Updates to resources during upgrade" on page 170.

- Activate the feature to allow non-unique scenario names.

  Before you activate the feature to allow non-unique scenario names, some scripts and scheduled system tasks might also need to be adjusted to account for the possibility of non-unique scenario names and changes to RapidResponse's assumptions about scenarios. For more information, see "Permitting non-unique scenario names" on page 172.

Updates to resources during upgrade

When you upgrade from RapidResponse 2014.4 (and earlier) to 2015.3 (or later), RapidResponse automatically updates existing resources to specify the scopes of scenarios in resource definitions. Scenarios referred to in resource definitions are assumed to be shared unless the following conditions are met:

- The resource is private.
- A shared scenario with the specified name does not exist at the time of upgrade.
- A private scenario with the specified name exists at the time of upgrade.
- Private scenarios are allowed in the context in which the scenario is specified. For example, in a workbook definition, you can only select shared scenarios when you limit the available scenarios, but in a private workbook, you can select a private scenario as the baseline scenario for multi-scenario columns.

If all of the above conditions are met, the resource is scoped as private.

If you are using the On-Premises version of RapidResponse, after upgrading, review the upgrade log file, `C:\RapidResponse\Upgrade Logs\Upgrade (version).tab` to see messages about the resource update process, including errors instances where a scenario named in a resource definition does not exist. If you are using the On-Demand version of RapidResponse, contact your Kinaxis Customer Support for assistance.

It is recommended that resource authors review the resources that they own to determine whether the appropriate scope has been assigned to scenarios in the resource definitions.

The $Scenario# variable

The $Scenario# system variable now returns scenarios in the format

`?(scope):(scenario name)`

instead of only returning scenario names.

During the upgrade process, RapidResponse does not make any automatic changes to expressions where this variable is used. Workbooks that use this variable will often continue to function normally, but there are two situations in which you will see a change in behavior.

- The `$Scenario#` variable is compared to a constant.

  In these cases, you need to change the constant to match the format in which scenario names are now returned by the $Scenario# variable. For example, you might change '`$Scenario1 = Baseline`' to '`$Scenario1 = ?shared:Baseline`' if you want to compare the first comparison scenario selected by the user to a shared scenario named Baseline.

- The scenario returned by $Scenario# is displayed in a worksheet column.

  In these cases, you can do nothing, and allow the scenario name to be displayed in the `?(scope):(scenario name)` format.

  If you only want the name of the scenario to be displayed, you can replace the $Scenario# variable with an expression that returns only the name of the scenario.

  ```
  ScenarioProperty(CanonicalScenarioId($Scenario#), "Name")
  ```

  For example, if you want the name of the scenario used as the baseline in a worksheet to be displayed, replace `$Scenario0` with `ScenarioProperty(CanonicalScenarioId($Scenario0), "Name")`

For more information about the $Scenario# variable, the ScenarioProperty function, and the CanonicalScenarioId function, see the *RapidResponse Resource Authoring Guide*.

Finding workbooks that use $Scenario#

There are two ways to locate workbooks containing the $Scenario# variable.

- In the `Upgrade (version).tab` log file that is created during the upgrade process, you are warned if any workbook definitions include the `$Scenario#` variable. For more information about upgrade logs, see "Reviewing the upgrade log files" on page 193. This log file is only available if you are using the On-Premises version of RapidResponse.
- You can locate shared workbooks that use the $Scenario# variable by selecting Search Resources from the Tools menu, and searching for `$Scenario` in expressions. For more information about searching for resources, see the *RapidResponse Resource Authoring Guide*.

Permitting non-unique scenario names

When you upgrade from RapidResponse 2014.4 (and earlier), a processing rule, named ScenarioNameUnique, is put in place during the upgrade process to prevent users from creating scenarios with non-unique names right away. A system administrator can change or remove this processing rule to permit scenarios with non-unique names.

The following table summarizes the changes in RapidResponse behavior that occur when you change (or remove) the ScenarioNameUnique processing rule.

ScenarioNameUnique = Y	ScenarioNameUnique = N or processing rule is absent
No two scenarios can have the same name.	Multiple scenarios can have the same name.
Scenarios specified in arguments for scheduled system tasks can be shared or private. If no scenario with the specified name exists, the task fails.	Scenarios specified in arguments for scheduled system tasks are assumed to be shared. If a shared scenario with the specified name exists, it is used. If no shared scenario with that name exists, the task fails, whether or not a private scenario with that name exists.
Scenarios named in RapidResponse OpenAPI scripts can have a scope specified, but if no scope is specified, the scenario with the given name is used regardless of scope.	Scenarios named in RapidResponse OpenAPI scripts are assumed to be shared if the scope is not specified. If a private scenario with the given name exists, it is only used if you specify the scope as private.
Scenarios names used by web service clients can have a scope specified, but if no scope is specified, the scenario with the given name is used regardless of scope.	Scenarios names used by web service clients are assumed to be shared if the scope is not specified. If a private scenario with the given name exists, it is only used if you specify the scope as private.

Before you permit non-unique scenario names, consider the following:

- Do any scheduled system tasks use private scenarios? If so, you will need to make changes, such as sharing private scenarios, to get the desired results. For more information about system tasks, see "RapidResponse system commands" on page 384.
- Does your RapidResponse system use external automated processes, including OpenAPI programs or web service clients? If so, any scenarios used in those processes must be shared or the scope must be specified. For more information, see the *RapidResponse Web Services Guide*.
- Will having multiple scenarios with the same name potentially cause new unhandled exceptions in RapidResponse scripts? If so, the scripts might need to be edited. For more information, see the *RapidResponse Scripting Guide*.

If you are using the On-Premises version of RapidResponse, before you permit non-unique scenario names, you can have RapidResponse log each use of an unscoped scenario name that resolves to a private scenario. These might be scenarios used by a scheduled system task, a RapidResponse Open API program, or a web service client . For each occurrence, a message is written to the Server.log file, telling you the name of the private scenario that was used. By tracking the use of unscoped scenario names that resolve to private scenarios, you can determine where you need to make changes—either scoping scenarios as private or sharing scenarios—to avoid errors when you eventually permit non-unique scenario names.

▸Log uses of unscoped scenario names that resolve to private scenarios (On-Premises)

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Select the **Processing Rules** tab of the **RapidResponse Administration** workbook.
3. Click **Insert Record** .
4. In the **Type** field, select **ProcessingRule**.
5. In the **ID** field, type `LogUsesOfUnscopedPrivatePlans`.
6. In the **Value** field, type `Y`, and then save your changes.

   Each time an unscoped scenario name is used, a message is added to the **Server.log** file. For information about viewing the Server.log file, see "RapidResponse text-based log files" on page 462.

Tip: You can change the **Value** of the **LogUsesOfUnscopedPrivatePlans** processing rule to `N`, or delete it, to stop logging uses of unscoped scenario names that resolve to private scenarios.

▸Permit non-unique scenario names

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Select the **Processing Rules** tab of the **RapidResponse Administration** workbook.
3. Change the **Value** of the **ScenarioNameUnique** processing rule to `N`.

Tip: Once you are sure that the system is functioning correctly while allowing non-unique scenario names, you can optionally delete the ScenarioNameUnique processing rule and the LogUsesOfUnscopedPrivatePlans processing rule.

Reverting to unique scenario names

Reverting to unique scenario names is not recommended, though it might be necessary to do so temporarily if permitting non-unique scenario names causes unanticipated problems on your RapidResponse system. Before reverting to unique scenario names, ensure that all existing scenario names are unique. Non-unique scenario names can cause errors, such as RapidResponse OpenAPI scripts or scheduled system tasks performing operations using the wrong scenario.

▸Revert to unique scenario names

1. In the **Administration** pane, under **System Monitoring**, click **Scenarios**.
2. Review the names of the existing scenarios to ensure that they are unique.
3. If multiple scenarios with the same name exist, correct this problem using any of the following methods.
   - Delete scenarios.
   - Rename your private scenarios.
   - Ask other users to rename their private scenarios.
4. In the **Administration** pane, under **System Settings**, click **Configuration**.

5. Select the **Processing Rules** tab of the **RapidResponse Administration** workbook.
6. Change the **Value** of the **ScenarioNameUnique** processing rule to `Y`.

> **Tip:** You can also revert to using unique scenario names by restoring a data package that was created prior to allowing non-unique scenario names. This approach is more reliable, since you cannot accidentally overlook a duplicate scenario name and then encounter errors as a result. However, any changes to data, resources, or settings that were made after the data package was created are lost. For more information, see "Backing up and restoring the RapidResponse database" on page 315.

Replacing optional keys with key fields

If you have upgraded from RapidResponse 2014.4 (or earlier), the key field requirements for tables are modified to allow up to eight key fields on each table, and to allow key fields of many data types. If you have enabled the optional key fields on any of the tables that can optionally contain keys, you can replace the optional keys with key fields of your choice. These tables are:

- Allocation
- BillOfMaterial
- OnHand
- Operation

If you have enabled optional keys on these tables, a BaseKey field and two references are used as keys for the table. These fields are maintained as key fields after upgrading to RapidResponse 2015.3 (or later), however, it is recommended you replace the optional keys with key fields of your choice. This allows you to configure the key fields with data that is more relevant for your company, and allows you to not populate the BaseKey field, which typically does not contain meaningful values.

To replace the optional keys with key fields, you must first disable optional keys on the table, and then modify the fields in the table to specify the key fields.

For more information about key fields and customizing the RapidResponse data model, see the *RapidResponse Data Integration Guide*.

▸To replace optional keys

1. On the **Administration** pane, under **Data**, click **Data Model**.
2. Select the table you want to modify.
3. Click **Table**, and then click **Properties**.
4. In the **Table Properties** dialog box, clear the **Records must be uniquely identified** check box.
5. Click **OK**.
6. In the **Fields** list, do the following for each field you want to use to identify records in the table:
   - Click **Field**, and then click **Properties**.
   - Select the **Key field** check box.
   - Click **OK**.
7. Click **OK**, and then apply your changes to the active data model.

Note: Key fields can be of the String, Reference, Date, DateTime, Time, Integer, and Boolean data types.

Specifying whether key reference fields are modifiable

If you are upgrading to RapidResponse 2016.2 (or later), you might have processes that modify reference key fields in tables. These fields are read-only for RapidResponse 2016.2 (or later), however, upon upgrading, a processing rule is added to the RapidResponse Administration workbook that allows these values to remain modifiable.

The processing rule, ModifyKeyReferences, by default allows all reference key fields to be editable. This allows your processes to continue running if you have not already replaced them. You should replace any process that modifies these reference key values to prevent the processes from creating duplicate records. For tables where the modifiable key values are required, you can modify the processing rule to specify the tables that allow the reference key fields to be editable.

The ModifyKeyReferences processing rule uses a String value to define the tables that can have their reference key values modified. These tables must be namespace-qualified, and separated by commas. You can use wildcards to define multiple tables, for example, `'Mfg::Independent*'` to allow reference key modifications in all tables in the Mfg namespace that begin with Independent.

It is recommended you make all reference key fields read-only by replacing the operations that modify the key fields with an operation that inserts a new record with the required value and deleting the existing record. For more information, see the *RapidResponse Resource Authoring Guide*.

▸To specify the tables that can contain modifiable reference keys

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** worksheet.
3. For the **ModifyKeyReferences** row, in the **Value** column, specify the expression that defines the table or tables you want to allow reference key modifications in.
4. Save your changes.

▸To disallow modifiable reference keys

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** worksheet.
3. Delete the **ModifyKeyReferences** row.
4. Save your changes.

CHAPTER 15: Upgrading RapidResponse Server

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

This section applies to RapidResponse 2016.2 Service Update 21. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

Requirements 178
Migrating from Intel Itanium servers 178
Migrating from Windows Server 2003/2008 servers 179
Stopping RapidResponse services 180
Upgrading RapidResponse Server 181
Upgrading application components 184
Upgrading the RapidResponse ServiceHost service 185
Reviewing the upgrade log files 185
Setting up the RapidResponse Server service 186

This chapter outlines the steps to upgrading RapidResponse Server. The upgrade program manages the upgrade to the current version from version 11.0 or later.

All RapidResponse services are automatically stopped and reinstalled with their default settings as part of the upgrade. If you are upgrading from RapidResponse 2014.4 (or earlier) and have changed the user account the RapidResponse Service Host runs as, you must make the same change following the upgrade.

If you are not upgrading RapidResponse Server, you do not need to review this chapter. For information about installing RapidResponse Server, "Installing RapidResponse Server" on page 109.

Cautions:

- Do not uninstall your existing RapidResponse Server version prior to upgrading RapidResponse Server.
- If you are upgrading by installing a RapidResponse 2016.2 Service Update, do not start RapidResponse Server before you have installed the supplemental application components. The application components include the required tables and namespaces for applications, which are not included in the Server installation. This is interpreted as a data model change, so restarting the server here will remove tables and delete data. For more information, see "Upgrading RapidResponse with Service Updates" on page 152.

Note: The upgrade process requires that RapidResponse Server be restarted multiple times. In some cases, this could make the upgrade process very time consuming. For example, if your database takes one hour to load and the upgrade process requires four restarts, then the RapidResponse Server upgrade process will take more than four hours to complete.

Requirements

You need the following items to upgrade RapidResponse Server.

- **Serial number**

  A serial number is required to install RapidResponse Server. Kinaxis Customer Support provides this number.

- **Master Administrator user password**

  The RapidResponse Master Administrator user (Admin user) password is required so that the upgrade program can make the required changes to the RapidResponse data files. The Master Administrator user cannot be signed into RapidResponse during the installation process.

- **Port numbers**

  If you do not accept the defaults, you will be required to enter the port numbers for RapidResponse Server. The port, specified in the RapidResponse Server installation, is used to communicate with other RapidResponse components.

- **Existing RapidResponse Server name**

  You will need to provide the computer name or the IP address of the computer on which the current RapidResponse Server is installed before upgrading. If you are not sure of the computer name, refer to the **Computer Name** identified in the **System** option of the Windows **Control Panel**.

- **Update RapidResponse license keys**

  Before upgrading, you need to import the new RapidResponse license keys. To receive the license keys, contact Kinaxis Customer Support at support@kinaxis.com. For more information about importing license keys, see "Importing license keys" on page 273.

Migrating from Intel Itanium servers

As of RapidResponse 2013.2, RapidResponse Server is no longer supported on Intel Itanium-based servers. To upgrade, you must migrate RapidResponse Server to a server that meets the current system requirements. You must also migrate the RapidResponse database and reconfigure processes that used your Itanium server such as the FTP destination for data transfers.

Before you begin planning to upgrade RapidResponse Server on the Itanium platform, contact Kinaxis Customer Support to discuss upgrade options. You should also review current system requirements. For more information, see "System requirements for RapidResponse" on page 104.

The following process overview explains how to migrate from an Intel Itanium server.

▸To migrate RapidResponse Server from an Intel Itanium platform

1. Upgrade your current RapidResponse Server installation to RapidResponse 10.0. The upgrade steps are described in the version 10.0 *RapidResponse Administration Guide*.
2. Create a data package. For more information, see "Manually creating a data package" on page 315.
3. Install RapidResponse Server 10.0 on a supported server.
4. Restore the saved data package on the system where you installed the new instance of RapidResponse Server. For more information, see "Restoring data packages" on page 317.
5. Upgrade your new instance of RapidResponse Server to the latest version. For detailed information about upgrading, see "Upgrading RapidResponse Server" on page 181.
6. Reconfigure any processes that were directed to the Intel Itanium server. For example, your data update process might have had data files moved by FTP to the Intel Itanium server.

Migrating from Windows Server 2003/2008 servers

As of RapidResponse 2013.4, RapidResponse Server and RapidResponse Application Server are no longer supported on Microsoft Windows Server 2003 servers.

As of RapidResponse 2015.3, RapidResponse Server and RapidResponse Application Server are no longer supported on Microsoft Windows Server 2008 servers.

To upgrade, you must migrate these RapidResponse components to a server (or servers) that meet the current system requirements. You must also migrate the RapidResponse database and reconfigure processes that used the previous server such as the FTP destination for data transfers.

Before you begin planning to upgrade RapidResponse, contact Kinaxis Customer Support to discuss upgrade options. You should also review current system requirements. For more information, see "System requirements for RapidResponse" on page 104.

The following process overviews explain how to migrate RapidResponse Server and RapidResponse Application Server from Windows Server 2003/2008.

▸To migrate RapidResponse Server from Windows Server 2003/2008

1. Using your current RapidResponse Server, create a data package. For more information, see "Manually creating a data package" on page 315.
2. Using your new server computer, install the same version of RapidResponse Server that you are currently running on your Windows Server 2003/2008 server. You should also install the latest service updates. Contact Kinaxis Customer Support for installation images and service updates.
3. Copy the RapidResponse data package to your new server computer where you re-installed RapidResponse Server.
4. Restore the saved data package on the system where you re-installed RapidResponse Server. For more information, see "Restoring data packages" on page 317.
5. Reconfigure any processes that were directed to the Windows Server 2003/2008 server. For example, your data update process might have had data files moved by FTP to the Windows Server 2003 server.
6. Upgrade your new instance of RapidResponse Server to the latest version. For detailed information about upgrading, see "Upgrading RapidResponse Server" on page 181.

▸To migrate RapidResponse Application Server from Windows Server 2003/2008

1. Using your new server computer, install the same version of RapidResponse Application Server that you are currently running on your Windows Server 2003/2008 server. You should also install the latest service updates. Contact Kinaxis Customer Support for installation images and service updates.
2. Copy the RapidResponse Application Server configuration files from the Windows Server 2003/2008 server to the computer where you re-installed RapidResponse Application Server. For a listing of the configuration files, see "Backing up Application Server configuration files" on page 314.
3. Upgrade your new instance of RapidResponse Application Server to the latest version. For detailed information about upgrading, see "Upgrading RapidResponse Application Server" on page 189.

Stopping RapidResponse services

Before upgrading, you need to stop all RapidResponse services including the RapidResponse Server service.

Before stopping RapidResponse Server, notify your user community that RapidResponse will not be available and all users should be signed out. After stopping RapidResponse Server, calculated results are lost.

Stopping RapidResponse Server service

The steps in this procedure depend on the version of RapidResponse you are upgrading from. If you are upgrading from RapidResponse 10.1 (and earlier), you must checkpoint the service. If you are upgrading from RapidResponse 11.0 (and later), you must condense the RapidResponse database and stop the current RapidResponse Server before you begin the upgrade process.

Running the Condense command creates a new main database file by combining all the DFS folders in the hive. The new file represents the complete database as of the time the operation began. For more information, see "Condense command" on page 387 and "Database files and operations" on page 311.

▸To condense the database and stop the RapidResponse Server service

1. Sign into RapidResponse Console. For more information, see "To sign in to RapidResponse Console" on page 230.
2. Click the **Actions** menu.
3. Click **Condense** and then click the **Condense** button.
4. Wait for the **Results** window to display and then click **Stop Service**.

Stopping RapidResponse services

After you have stopped the RapidResponse Server service, stop the other services.

▸To stop RapidResponse services

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Select a RapidResponse service (other than **RapidResponse Server**).
3. On the **General** menu, click **Stop**.
4. Repeat steps 2 and 3 for other services.

Upgrading RapidResponse Server

This section covers steps 1 and 11 of the general steps to upgrade RapidResponse Server described in "RapidResponse upgrade steps (On-Premises)" on page 150. The RapidResponse Server upgrade program is wizard-like, and similar to the installation program.

This section provides instructions for the case where you are upgrading RapidResponse from a previous version, for example, if you are upgrading from RapidResponse 2015.3 (or earlier) to RapidResponse 2016.2 (or later). If you are upgrading RapidResponse by applying a Service Update, see "Upgrading RapidResponse Server with Service Updates" on page 182.

▸To install RapidResponse Server as an upgrade

1. If applicable, close the RapidResponse Console.
2. Navigate to the installation image, right-click the **EasyInstaller.exe** file and select **Run as administrator**.
3. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
4. Click **Next**.
5. On the **Customize** tab, do the following:
   - Ensure the **RapidResponse Server** check box is selected.
   - Clear the **RapidResponse Application Server** check box.
     If you have installed RapidResponse Server and RapidResponse Application Server on the same computer, leave this check box selected.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
6. If you are prompted to install required software components (such as RapidResponse OpenAPI, Windows Installer, and Microsoft Visual C++ components), click **Install** and follow the subsequent installation instructions. You might be then prompted to restart the computer. If so, you will need to restart the installation program. If not, go to the next step.
7. Review the information on the **Welcome** screen and click **Next**.
8. On the **Software License Agreement** screen, review the conditions of the license agreement, and then click **Yes**.
9. On the **Registration** screen, do the following:
   - Type your name and the name of your company in the appropriate boxes.
   - Type installation license key (serial) number exactly as provided by Kinaxis Customer Support.
   - Click **Next**.
10. On the **Port Numbers** screen, type a TCP/IP port number for the RapidResponse Server or accept the default value (14600) and then click **Next**. The RapidResponse Server is bound to a specific

port and it must be open for inbound requests other RapidResponse components. For more information, see "TCP/IP ports and RapidResponse Server" on page 110.

The port number must be between 1024 and 65535 and cannot already be assigned. The port number can be modified after the installation is complete. For more information, see "RapidResponse and TCP/IP ports" on page 283.

11. On the **Select Destination Folder** screen, choose the location where your current RapidResponse Server is installed and then click **Next**.

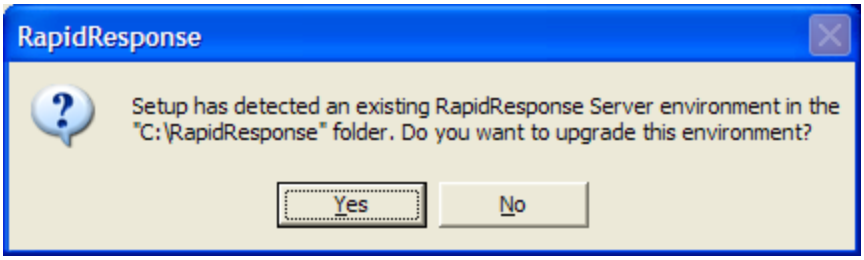
    To upgrade, you must install RapidResponse Server in the same location as the current installation. If you install to a different location on the computer, a new version of RapidResponse Server is installed, and co-exists with your current installation; nothing is upgraded.

12. On the **Select RapidResponse Server Database Location** screen, specify the location for the RapidResponse Server database files. It must be the same location as your current RapidResponse Server database files.

    The folder name chosen on this screen will have the **\Data** sub-folder appended to it. For example, **C:\RapidResponse\Data.**

    If you are running virus-scanning applications on the computer where the RapidResponse database is stored, ensure the database folder is excluded from the virus scan operation. Scanning the database folder can result in file locks being placed on RapidResponse database files.

13. Click **Yes** when the following message box appears:



14. On the **Select Program Folder** screen, you can either accept the suggested folder name, type a new folder name, or select one from the **Existing Folders** list. Click **Next**. The installation begins.
15. The upgrade process begins and might take some time to complete. A dialog box displays confirming the data files were successfully upgraded. Click **OK**.
16. If you are upgrading from RapidResponse 2015.3 (or earlier), select the **Start RapidResponse Server** check box to restart RapidResponse Server.

    If you are upgrading RapidResponse Server by installing a Service Update, leave the **Start RapidResponse Server** check box cleared, and then continue to the next step.

17. When the components are done installing, click **Next**.
18. If any components failed to install, click **Open Log File** to review the errors.
19. Click **Finish**.
20. If the **Restart Windows** screen displays, select an option and click **Finish**.

Upgrading RapidResponse Server with Service Updates

Service Update content for RapidResponse Server is applied using the installation programs. RapidResponse Windows services must be stopped before updating RapidResponse Server, and are automatically restarted following the Service Update process.

The RapidResponse Server upgrade process also updates the supplemental application components and the ServiceHost Service. After running the RapidResponse Server upgrade, you must then upgrade the RapidResponse Application Server. For more information, see "Upgrading RapidResponse Application Server" on page 190.

When you apply a Service Update, a backup of your settings is automatically created in the **RapidResponse\Backup** folder. If necessary, you can revert your RapidResponse Server to your previous version. For more information, see "Reverting Service Updates" on page 154.

▸To apply a Service Update to RapidResponse Server

1. Stop all RapidResponse Windows Services. For more information, see "Stopping RapidResponse services" on page 180.
2. Set the RapidResponse Server service to use the **Startup type** of **Manual**.
3. Navigate to the installation image, right-click the **EasyInstaller.exe** file and select **Run as administrator**.
4. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
5. Click **Next**.
6. On the **Customize** tab, do the following:
   - Ensure the **RapidResponse Server** check box is selected.
   - Clear the **RapidResponse Application Server** check box.
     If you have installed RapidResponse Server and RapidResponse Application Server on the same computer, leave this check box selected.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
7. Review the information on the **Welcome** screen and click **Next**.
8. If you are prompted to install required software components (such as RapidResponse OpenAPI, Microsoft Visual C++ components, or Microsoft .NET Framework), click **Install** and follow the subsequent installation instructions. Note that during installation of specific components, an automatic server reboot might occur without warning.
9. Follow the remainder of the install prompts to apply the RapidResponse Server update.
10. In the **Setup Complete** dialog box, ensure the **Start RapidResponse Server** check box is cleared, and then click **Finish**.
11. When the components are done installing, click **Next**.
12. If any components failed to install, click **Open Log File** to review the errors.
13. Click **Finish**.
14. Set the RapidResponse Server service to use the **Startup type** of **Automatic**.

Recovering data files in case of upgrade failure

When the upgrade program commences, it saves a copy of the RapidResponse database in an archive file named **PreUpgrade*xyx*.pkg** (where xyz represent the version numbers). The archive is stored in the **C:\RapidResponse\Packages** folder and can be used in case the upgrade fails and you need to revert back to the pre-upgrade database.

Similarly, if you are applying a Service Update, the backup package you create during the Service Update process is stored in the **C:\RapidResponse\Packages** folder. This package is named **Backup_*server*_*date-time*.pkg** or **Backup_*server*_*date-time*.zip**, where *server* is the name of the computer, *date* is the date the package was created, and *time* is the time the package was created. If the Service Update process fails, you can restore your previous database by following the same procedures with this package.

The upgrade program might fail in the following situations:

- The administrator running the upgrade is unable to provide the Admin password and chooses to cancel the upgrade program.
- There is an internal failure in the upgrade program.

In either of these situations, the upgrade program recovers the application, but you must manually restore the RapidResponse database.

▸To restore a RapidResponse database archive

1. Ensure the RapidResponse Server is stopped. For more information, see "To stop other RapidResponse Server services" on page 232.
2. Delete the contents of the **C:\RapidResponse\Data** folder.
3. Navigate to the **C:\RapidResponse\Packages** folder.
4. Copy and paste the backup package into the **C:\RapidResponse\Data** folder.
5. Restart RapidResponse Server.

   After decompressing the backup data package, RapidResponse Server uses the backed up database archive.

Upgrading application components

The information in this section applies only if you are upgrading RapidResponse Application Server and have not also upgraded RapidResponse Server . If you upgraded RapidResponse Server, the application components are automatically upgraded.

RapidResponse applications require specific data tables and their corresponding namespaces, which are not included in RapidResponse Server. These tables and namespaces are provided in the supplemental application installer, which allows you to install the required data for predefined resources and any RapidResponse applications your company uses.

Because these tables and namespaces are not part of the RapidResponse Server installation, you can upgrade the applications as new versions are released, without requiring an update to RapidResponse Server. The application components must be updated whenever you upgrade RapidResponse Application Server or apply a Service Update, regardless of whether you have applied an update to RapidResponse Server. Service Updates for application components are applied on the computer where RapidResponse Server is installed.

The application supplemental installer copies new versions of files into RapidResponse Server if they either do not already exist or newer versions are present in the application supplemental installer. If you run the upgrade and the application components have not been updated, no files are copied to RapidResponse Server.

RapidResponse Server restarts at the end of the supplemental application installation if any files have been modified. If no changes were made, the Server does not restart automatically. However, if you have upgraded RapidResponse Server in this case, you must restart the Server manually.

The upgrade process for the supplemental application installer automatically stops RapidResponse Server if it has not already stopped.

▸To apply a Service Update to RapidResponse application components

1. Optionally, stop the **RapidResponse Server** service. For more information, see "Stopping RapidResponse services" on page 180.
2. In the installation image, navigate to the **Rollup\RapidResponseCore\Application Server\Supplemental Installer** folder.
3. Right-click the **setup.exe** file and select **Run as administrator**.
4. Review the information on the **Welcome** screen and click **Next**.
5. On the **Software License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
6. Click **Install** to begin the installation.
7. In the **InstallShield Wizard Completed** screen, click **Finish** to complete the installation. You also have the option to view the Windows Installer Log from this screen.
8. Restart RapidResponse Server if it did not start automatically.

Upgrading the RapidResponse ServiceHost service

The RapidResponse ServiceHost service runs alerts and provides an interface for external processes to interact with RapidResponse. This service can be updated with additional functionality , and can be upgraded similarly to other RapidResponse components.

If you upgrade RapidResponse Server, the ServiceHost service is automatically updated as part of that process. However, if you are upgrading RapidResponse by applying a Service Update and do not upgrade RapidResponse Server, you must upgrade the ServiceHost using a separate installation program.

In addition, you must upgrade the supplemental application components before you upgrade the ServiceHost service. For more information, see "Upgrading application components" on page 184.

▸To upgrade the ServiceHost service

1. In the RapidResponse installation image, navigate to the **Rollup\RapidResponseCore\Server\ServiceHost** folder.
2. Right-click the **ServiceHostSetup.msi** file and select **Run as administrator**.
3. Review the information on the **Welcome** screen and click **Next**.
4. Follow the install prompts to apply the Service Update.

Reviewing the upgrade log files

After upgrading, review the RapidResponse Server upgrade log files in the **C:\RapidResponse\Upgrade Logs** folder. The upgrade log files summarize the changes made to RapidResponse Server. The files might also indicate warnings and errors, and whether you need to perform any manual steps to complete the upgrade. The following lists the log files that are created during the upgrade process:

- ResourceUpgrade.log (Review if ServiceHost does not start)
- RapidResponse Utility.InstallLog
- RapidResponse Utility.InstallState
- RapidResponse Utility Installation.log
- ServiceHostInstaller.log

Setting up the RapidResponse Server service

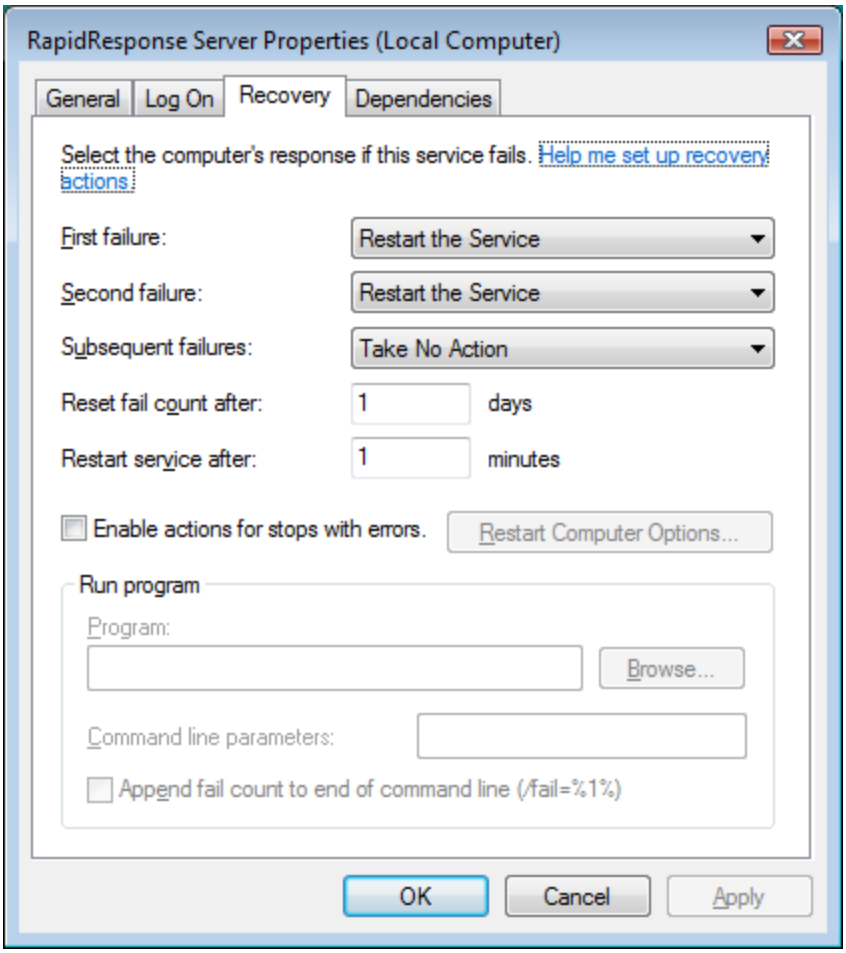
To help ensure optimal system performance, Kinaxis recommends the following RapidResponse Server service settings. The settings are available in the Windows Service Properties dialog box.

General tab

- **Startup Type**—Automatic

Recovery tab

- **First Failure**—Restart the Service
- **Second Failure**—Restart the Service
- **Subsequent Failure**—Take No Action
- **Reset fail count after**—1 days
- **Restart service after**—1 minutes



▸To open the Windows Services dialog box

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Click **RapidResponse Server**.

CHAPTER 16: Upgrading RapidResponse Application Server

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

This section applies to RapidResponse 2016.2 Service Update 21. If you are using a previous version, refer to the Service Update 20 documentation section on the Kinaxis Knowledge Network, available from https://knowledge.kinaxis.com/s/documentation-service-update-20.

Preparing to upgrade Application Server 189
Upgrading RapidResponse Application Server 190
Recovering files in case of upgrade failure 193
Reviewing the upgrade log files 193
Testing the Application Server upgrade 194

This chapter outlines the steps to upgrading RapidResponse Application Server. The upgrade program manages the upgrade to the current version from version 11.0 or later.

If you are not upgrading RapidResponse Application Server, you don't need to review this chapter. For information about installing RapidResponse Application Server, "Installing RapidResponse Application Server" on page 113.

Preparing to upgrade Application Server

RapidResponse Application Server provides the Web-based client that RapidResponse users sign into. You should prepare before upgrading RapidResponse Application Server. To prepare, you will need to verify some RapidResponse configuration items and be able to provide information. This section outlines how to prepare for installing Application Server.

RapidResponse Server

Before upgrading, ensure that a compatible version of RapidResponse Server is running, and there is LAN connection between the computer where RapidResponse Server is installed and the computer where RapidResponse Application Server will be upgraded.

You will need to provide the computer name or the IP address of the computer on which RapidResponse Server is installed. If you're not sure of the computer name, refer to the **Computer Name** identified in the **System** option of the Windows **Control Panel**.

Java Runtime Environment (JRE)

As of RapidResponse 11.0, RapidResponse Application Server required a 64-bit Oracle Java Runtime Environment (JRE). You might need to update to a new JRE if you had been using a 32-bit JRE.

In addition, RapidResponse Application Server 2014.2 (and earlier) supported JRE 6. RapidResponse Application Server 2014.4 supported JRE 7.

As of February 2013, JRE 6 reached the end of its supported life. Support for JRE 7 updates ended in April 2015. When supported life ends, Oracle no longer posts updates which means critical bug fixes and security fixes are no longer available.

To help maintain system security and reliability, RapidResponse Application Server now requires JRE 8. You download the latest version of the JRE by visiting http://www.java.com/en/.

Single sign-in

If you are using single sign-in (SSI), make a copy of the **web.config** file before upgrading. This file is located in the **C:\Program Files\Kinaxis\RapidResponse\web**\ folder. After you complete the upgrade process, copy the single sign-in code from the original **web.config** file to the newly installed file. For more information about SSI, see " Configuring single sign-in for On-Premises" on page 835.

Upgrading RapidResponse Application Server

The following procedure outlines the steps necessary for a successful upgrade of RapidResponse Application Server. The upgrade program installs RapidResponse Application Server into the **C:\Program Files\Kinaxis\RapidResponse** folder.

You must have upgraded application components before upgrading RapidResponse Application Server. For more information, see "Upgrading application components" on page 184.

This section provides instructions for the case where you are upgrading RapidResponse from a previous version, for example, if you are upgrading from RapidResponse 2015.3 (or earlier) to RapidResponse 2016.2 (or later). If you are upgrading RapidResponse by applying a Service Update, see "Upgrading RapidResponse Application Server with Service Updates" on page 192.

▸To upgrade RapidResponse Application Server

1. Navigate to the installation image, right-click the **EasyInstaller.exe** file and select **Run as administrator**.
2. Log on as a Windows Server administrator on the computer where RapidResponse Application Server will be installed, and then in the RapidResponse installation image, double-click the **EasyInstaller.exe** file.
3. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
4. Click **Next**.

5. On the **Customize** tab, do the following:
   - Clear the **RapidResponse Server** check box.
   - Ensure the **RapidResponse Application Server** check box is selected.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
6. If you are prompted to install required software components (such as RapidResponse OpenAPI, Windows Installer, and Microsoft Visual C++ components), click **Install** and follow the subsequent installation instructions. You might be then prompted to restart the computer. If so, you will need to restart the installation program. If not, go to the next step.
7. Review the information on the **Welcome** screen and click **Next**.
8. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
9. On the **RapidResponse Server** screen, do one of the following in the **Computer Name** box:
   - If RapidResponse Server is in the same domain as the Web server, type the computer name or the IP address of the computer on which RapidResponse Server is installed.
   - If RapidResponse Server is not in the same domain as the Web server, type the IP address of the computer on which RapidResponse Server is installed.

   In the **RapidResponse Server Port box**, accept the default port or type the port number RapidResponse Server uses to communicate with other RapidResponse components. For more information, see "TCP/IP ports and RapidResponse Application Server" on page 117.

   In the **Admin Password** box type the RapidResponse Master Administrator (Admin user) password.

   Click **Next**.
10. On the **RapidResponse Web Site** screen, in the Web Site box, choose the Web site for RapidResponse. This site is typically named **Default Web Site** if the Web server has only one Web site.

    In the **Virtual Directory Name** box, type the name of the virtual directory to be used by RapidResponse or accept the default.
11. On the **Destination Folder** screen, choose the location where you want to install RapidResponse Application Server or accept the default, and then click **Next**.
12. On the **Select Program Folder** screen, you can either accept the suggested new folder name, type a new folder name, or select one from the **Existing Folders** list. Click **Next**.
13. On the **Select Base Currency** screen, choose the currency to be used as the system's base currency. This currency is used as the base for currency conversions and is the default currency for new users. Click **Next**.
14. On the **Ready to Install the Program** screen, click **Install**. T
15. When the components are done installing, click **Next**.
16. If any components failed to install, click **Open Log File** to review the errors.
17. Click **Finish**.
18. If the **Restart Windows** screen displays, select an option and click **Finish**.
19. Review the RapidResponse Application Server installation log files in the **C:\Program Files\Kinaxis\RapidResponse\Upgrade Logs** folder.
20. You should test administrative and general user accounts by signing in to RapidResponse through the client as a user, and verifying that all appropriate resources are available. For

example, all users who were in the RapidResponse Application Server administrators group in the previous version of RapidResponse Application Server should see the Administration pane.

21. Import the new software license keys supplied by Kinaxis Customer Support. License keys enable RapidResponse functionality such as optional applications, and specify the number of user accounts and sites that RapidResponse can support. For more information, see "Importing license keys" on page 273.

    You will have different license key sets for your test and production environments.

Note: In some cases, you might be warned of a required restart, but then not be prompted to restart your computer. In this case, you can continue on to the next part of the upgrade process and restart Windows after the upgrade is complete.

Upgrading RapidResponse Application Server with Service Updates

Service Update content for RapidResponse Application Server is applied using the installation programs. You must run the application supplemental installer and Service Update installer prior to running the upgrade, and upgrade applications following the upgrade. For more information, see "Upgrading application components" on page 184, "Upgrading the RapidResponse ServiceHost service" on page 185, and "Upgrading applications through Service Updates" on page 200.

You must stop Internet Information Services (IIS) before running the Service Update installation program, and you must manually restart IIS after the upgrade.

When you apply a Service Update, a backup of your settings is automatically created in the Program Files\Kinaxis\RapidResponse\Backup folder. If necessary, you can revert your RapidResponse Application Server to your previous version. For more information, see "Reverting Service Updates" on page 154.

▸To apply a Service Update to RapidResponse Application Server

1. Stop IIS.
2. Navigate to the installation image, right-click the **EasyInstaller.exe** file and select **Run as administrator**.
3. On the **Start** tab, optionally review the system preparation checklist to ensure you have all required prerequisites.
4. Click **Next**.
5. On the **Customize** tab, do the following:
   - Clear the **RapidResponse Server** check box.
   - Ensure the **RapidResponse Application Server** check box is selected.
   - Optionally, click **Change** to specify a location to save installation log files.
   - Click **Next**.
6. If you are prompted to install required software components (such as RapidResponse OpenAPI, Microsoft Visual C++ components, or Microsoft .NET Framework), click **Install** and follow the subsequent installation instructions. Note that during installation of specific components, an automatic server reboot might occur without warning.
7. Review the information on the **Welcome** screen and click **Next**.
8. Follow the remainder of the install prompts to apply the RapidResponse Application Server update.
9. When the components are done installing, click **Next**.

10. If any components failed to install, click **Open Log File** to review the errors.
11. Click **Finish**.
12. Start IIS.

Notes:

- If your RapidResponse Application Server system included locally installed RapidResponse help resources, these are removed by the Service Update. However, you can download and install updated help resources. For more information, see "Installing RapidResponse documentation resources" on page 121.
- In some cases, you might be warned of a required restart, but then not be prompted to restart your computer. In this case, you can continue on to the next part of the upgrade process and restart Windows after the upgrade is complete.

Recovering files in case of upgrade failure

When the upgrade program commences, saves a copy of the RapidResponse database to protect it from loss or corruption in case the upgrade program fails. The upgrade program might fail in the following situations:

- The administrator running the upgrade is unable to provide the Admin password and chooses to cancel the upgrade program.
- There is an internal failure in the upgrade program.

For information about how to recover from a RapidResponse Application Server upgrade failure, see "Recovering data files in case of upgrade failure" on page 183.

Reviewing the upgrade log files

After upgrading, review the RapidResponse Application Server upgrade log files in the **C:\Program Files\Kinaxis\RapidResponse\Upgrade Logs** folder. The upgrade log files summarize the changes made to RapidResponse Application Server. The files might also indicate warnings and errors, and whether you need to perform any manual steps to complete the upgrade. The following table lists the log files that are created during the upgrade process.

File name	Description
ResourceImport_timestamp.log	Provides a summary of the import of predefined resources including dashboards, workbooks, scorecards, and so.
InsertDefInstaller.log	Notes the insert definitions that are installed during the upgrade.

File name	Description
Upgrade *x.y.z*.log	Provides detailed information about changes to RapidResponse Application Server and resources. The *x.y.z* represent the RapidResponse Application Server version number; for example, 9.3.1. This file is also included in new installations of RapidResponse Application Server.
Upgrade *x.y.z*.tab	Notes summary information about changes applied to RapidResponse resources (dashboards, workbooks, scorecards, task flows, and so on). The information in this file is in a tab-delimited format. Tab-delimited files can be opened in a spreadsheet application like Microsoft Excel for better readability. The *x.y.z* represent the RapidResponse Application Server version number; for example, 9.3.1. This file is also included in new installations of RapidResponse Application Server.

Note: Consider reviewing the information about changes to resources after you upgrade the predefined resources. For more information, see the *RapidResponse Applications Guide*.

Testing the Application Server upgrade

After upgrading, you should test administrative and general user accounts by signing in to RapidResponse as a user, and verifying that all appropriate resources are available. For example, all users who were in an administrator group in the previous version of RapidResponse should see the Administration pane.

CHAPTER 17: Upgrading RapidResponse applications

Upgrading applications 195
Upgrading applications through Service Updates 200

This chapter outlines how to upgrade RapidResponse applications to the latest version using Service Updates. Each application can be upgraded by installing new resources from a resource package, which adds new resources as required and upgrades existing resources.

If you are upgrading from RapidResponse 2015.3 (or earlier) to RapidResponse 2016.2 (or later), this chapter also outlines how the RapidResponse upgrade program upgrades predefined resources (such as dashboards and workbooks). It also discusses how different types of predefined resources are treated during the upgrade and administrator tasks after the predefined resource upgrade is completed.

If you are not upgrading, you do not need to review this chapter. For information about installing RapidResponse predefined resources, see "Installing RapidResponse applications" on page 129.

If you are upgrading to RapidResponse 2016.2, you should also upgrade to Service Update 15, which specifies the baseline for all resources.

Review the *RapidResponse Applications Guide* to see a summary of new predefined resources and an outline of the changes that were made to pre-existing predefined resources after upgrading.

Upgrading applications

This section applies only if you are upgrading RapidResponse to a version earlier than Version 2016.2 Service Update 10. As of Service Update 10, predefined resource upgrades are presented as resource packages (RPK files). It is recommended you upgrade your RapidResponse instance and resources to Version 2016.2 Service Update 15, which is considered the baseline version for predefined resources.

During the RapidResponse resource upgrade, new resources (never previously existing in RapidResponse) are imported to the RapidResponse database and ownership is assigned to the Master Administrator. These resources are then shared with the appropriate predefined user groups.

If you are upgrading RapidResponse by applying a Service Update, the resources are not updated by running the Applications Installer. Instead, you can import resource packages that contain the changes for specific applications. For more information, see "Upgrading applications through Service Updates" on page 200.

Predefined resource changes during upgrade

This topic applies only if you are upgrading RapidResponse to a version earlier than Version 2016.2 Service Update 10. As of Service Update 10, predefined resource upgrades are presented as resource packages (RPK files). It is recommended you upgrade your RapidResponse instance and resources to Version 2016.2 Service Update 15, which is considered the baseline version for predefined resources.

The RapidResponse upgrade program does not treat all predefined resources the same way. In some cases, it attempts to upgrade them, and in other cases, an administrator or resource author must retrieve resources or manually update existing resources.

All RapidResponse resources, including predefined resources, are installed and stored in the RapidResponse database and are available to use from the RapidResponse client.

This section describes how each type of predefined resource is treated during an upgrade and what you can do as part of the upgrade process.

Dashboards and widgets

The dashboard and widget were introduced in RapidResponse 10.1 as new resource types.

All new dashboards and widgets are installed. The upgrade program does the following:

1. New dashboards and widgets are imported into the RapidResponse database, and ownership is assigned to the Master Administrator. These resources are then shared with the appropriate predefined user groups.
2. If you choose to upgrade predefined resources, including dashboards and widgets, all predefined dashboards and widgets are assigned to the Master Administrator and are no longer shared with other users and groups. The resource version number is also appended to the resource name, such as Part Properties_10.0.0.
3. New versions of predefined dashboards and widgets are assigned to the Master Administrator, and are shared to all users and groups to whom they had been shared in the previous version.

Workbooks

The upgrade program does the following:

1. RapidResponse includes a special repository in the RapidResponse database for the original version of all workbooks. All workbooks in the repository are deleted and replaced by the latest versions.
2. New workbooks are imported into the RapidResponse database, and ownership is assigned to the Master Administrator. These workbooks are then shared with the appropriate predefined user groups.
3. If you choose to upgrade predefined resources, including workbooks, all workbooks are assigned to the Master Administrator and are no longer shared with other users and groups. The resource version number is also appended to the resource name, such as Part Properties_10.0.0.
4. New versions of predefined workbooks are assigned to the Master Administrator, and are shared to all users and groups to whom they had been shared in the previous version.

Notes:

- System workbooks support administration functionality and are not directly opened or accessed. Instead, you can open system workbooks by clicking a link in the **Administration** pane. All system workbooks are installed by the upgrade program and cannot be retrieved. The upgrade program overwrites existing system workbooks with the same name. For more information, see the *RapidResponse Applications Guide*.
- RapidResponse 2015.3 introduced the ability to create private and shared versions of a scenario with the same name. If you have upgraded from RapidResponse 2014.4 (or earlier) to RapidResponse 2015.3 (or later), any workbooks you have configured to use specific scenarios must be investigated to ensure the correct scenario is used in all resources.

Scorecards

The upgrade program does the following:

1. New scorecards are imported into the RapidResponse database, and ownership is assigned to the Master Administrator. These scorecards are then shared with the appropriate predefined user groups.
2. If you choose to upgrade predefined resources, including scorecards, all scorecards are assigned to the Master Administrator and are no longer shared with other users and groups. The resource version number is also appended to the resource name, such as Operations_10.0.0.
3. New versions of predefined scorecards are assigned to the Master Administrator, and are shared to all users and groups to whom they had been shared in the previous version.

Processes and task flows

The upgrade program does the following:

1. New processes and task flows are imported into the RapidResponse database, and ownership is assigned to the Master Administrator. These resources are then shared with the appropriate predefined user groups.
2. If you choose to upgrade predefined resources, including processes and task flows, all processes and task flows are assigned to the Master Administrator and are no longer shared with other users and groups. The resource version number is also appended to the resource name, such as Operations_10.0.0.
3. New versions of predefined processes or task flows are assigned to the Master Administrator, and are shared to all users and groups to whom they had been shared in the previous version.

Filters and hierarchies

The upgrade program does the following:

1. New filters and hierarchies are imported into the RapidResponse database and ownership is assigned to the Master Administrator. These resources are then shared with the appropriate

predefined user groups.

2. Existing filters and hierarchies are not changed. After upgrading resources, you should review the resource changes in the the *RapidResponse Applications Guide*. You can edit filters and hierarchies.

Insert definitions

Provided they have the required permissions, users can insert records into worksheets based on any input or control tables in RapidResponse. The fields that the user must fill in to insert the records are defined in an insert definition, which is displayed in the Insert Record dialog box.

For commonly used tables, RapidResponse includes insert definitions that contain the fields that are usually filled for a new record.

The upgrade program does the following:

1. New insert definitions are imported into the RapidResponse database and made available to users.
2. All upgraded predefined insert definitions are renamed with the insert definition's version number appended to the name, such as Part_10.0.0.
3. New versions of predefined insert definitions are imported into the RapidResponse database and made available to users.

Post-upgrade considerations (On-Premises)

This topic only applies to the On-Premises version of RapidResponse.

This topic applies only if you are upgrading RapidResponse to a version earlier than Version 2016.2 Service Update 10. As of Service Update 10, predefined resource upgrades are presented as resource packages (RPK files). It is recommended you upgrade your RapidResponse instance and resources to Version 2016.2 Service Update 15, which is considered the baseline version for predefined resources.

Before you promote the RapidResponse database and resources changes from the test environment to the production environment, review and test each upgraded predefined resource to confirm that they are working as expected and returning the expected results.

If your company uses modified or customized predefined resources, you can apply the same modifications to the new upgraded workbooks.

Caution: If you restore a previous version of a workbook, you could break links or functionality between dashboards and workbooks that are organized in a process flow.

Note: Ensure that you review the the *RapidResponse Applications Guide* to understand the manual changes you make to predefined resources.

Upgrading application resources (On-Premises)

This topic only applies to the On-Premises version of RapidResponse.

This topic applies only if you are upgrading RapidResponse to a version earlier than Version 2016.2 Service Update 10. As of Service Update 10, predefined resource upgrades are presented as resource packages (RPK files). It is recommended you upgrade your RapidResponse instance and resources to Version 2016.2 Service Update 15, which is considered the baseline version for predefined resources. If you are applying a Version 2016.2 Service Update, see "Upgrading applications through Service Updates" on page 200.

During the upgrade process, you can choose to upgrade any of the RapidResponse applications. In addition, you can also upgrade predefined resources that are not part of an application but that might be supporting applications. These are grouped under the following categories:

- Common resources—used to support all the applications and the business problems that they solve.
- Others—do not support any applications but are required for some RapidResponse functionality.

During the applications upgrade process, you are prompted to select the applications that you want to upgrade and install. The RapidResponse Applications Installer installs the application predefined resources to the RapidResponse database as objects. After the installation is complete, the predefined resources are shared to predefined user groups that are included with RapidResponse.

This section provides instructions for the case where you are upgrading RapidResponse from a previous version, for example, if you are upgrading from RapidResponse 2015.3 (or earlier) to RapidResponse 2016.2 (or later). If you are upgrading RapidResponse by applying a Service Update, see "Upgrading applications through Service Updates" on page 200.

▸Upgrade RapidResponse predefined resources

1. Log on to a computer where RapidResponse Application Server is installed, and do one of the following:
   - **DVD installation**—insert the RapidResponse DVD. If a menu does not appear, use Microsoft Windows Explorer to navigate to your DVD drive, and double-click the DVD drive icon.
   - **Image installation**—use Windows Explorer to navigate to the installation image that you downloaded from the Kinaxis Secure FTP, and double-click the **autostart.exe** file.
2. On the main installation screen, from the **Install RapidResponse** section, choose **RapidResponse Applications**.
3. Review the information on the **Welcome** screen, and click **Next**.
4. On the **License Agreement** screen, review the conditions of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
5. On the **RapidResponse Server** screen, do one of the following in the **Computer Name** box:
   - If RapidResponse Server is in the same domain as the Web server, type the computer name or the IP address of the computer on which RapidResponse Server is installed.
   - If RapidResponse Server is not in the same domain as the Web server, type the IP address of the computer on which RapidResponse Server is installed.
6. In the **RapidResponse Server Port** box, accept the default port, or type the port number that RapidResponse Server uses to communicate with other RapidResponse components, including Application Server.
7. In the **AdminPassword** box, type the Master Administrator (Admin) password.
8. Click **Next**.
9. On the **Custom Setup** screen, click the icon beside the application name, and then click **This feature, and all subfeatures will be installed on local hard drive**. Also, ensure that the **Common Resources** and **Others** entries in the list are selected to be installed.

10. Click **Next**.
11. On the **Ready to Install the Program** screen, click **Install**. The installation process begins.
12. Click **Finish.**

Notes:

- Although the Microsoft Windows Control Panel indicates that you can remove the Kinaxis RapidResponse Applications Installer, removing this item deletes only the program that installs the predefined resources to the RapidResponse database. The actual resources remain in the database.
- Due to significant changes in RapidResponse 2013.2, the **Inventory Management** workbook (included in SCM resources) is considered a new resource instead of an upgraded resource. The previous version of the **Inventory Management** workbook is backed up by being assigned to the Master Administrator (Admin) and is no longer shared with other users and groups.

Upgrading applications through Service Updates

Updates to an existing and installed application can only be applied by importing the applicable resource package (.RPK file). Each available resource package contains resources of many types for a given application or area including linked or dependent resources that the application depends on. This allows the existing application components to be overwritten and replaced by the contents of the .RPK file. During the process of updating a given resource package, you might typically be given the option to replace or keep certain existing resources (for example, a linked dependent resource). For more information, see "Importing a resource package" on page 757.

In Version 2016.2 Service Update 15, all application workbooks were updated to ensure that their query expressions comply with a compatibility level being introduced in a future service update (other revisions and bug fixes were also made). The RPKs included in Service Update 15 therefore contain all required resources and dependencies for each application, and are considered a baseline against which all future application updates are made. For example, if a given application was updated in Service Update 16, the corresponding .RPK file would only contain resources reflecting those changes made since Service Update 15. If that same application were updated again in Service Update 17, the corresponding .RPK file would contain resources reflecting all changes made since Service Update 15 (that is, changes made in both Service Update 16 and Service Update 17).

Therefore if upgrading an application from a version earlier than Service Update 15, the application's RPK from Service Update 15 must first be applied before any versions of that RPK from subsequent service updates are applied. Iif needed, these resources can be found on the Kinaxis Knowledge Network in the Support > Downloads area.

Depending on the content available in the Service Update, the following .RPK files might be provided.

File	Description
Aggregate Supply Planning.rpk	Contains updated files for the Aggregate Supply Planning application.
Capacity Planning (Constraints).rpk	Contains updated files for the Capacity Planning (Constraints) application.

File	Description
Capacity Planning (CRP).rpk	Contains updated files for the Capacity Planning (CRP) application.
Demand Planning.rpk	Contains updated files for the Demand Planning (CRP) application.
Distribution Requirement Planning.rpk	Contains updated files for to the Distribution Requirements Planning (DRP) application.
Engineering Change.rpk	Contains updated files for to the Engineering Change application.
Integrated Project Management.rpk	Contains updated files for to the Integrated Project Management application.
Inventory Management.rpk	Contains updated files for to the Inventory Management application.
Inventory Planning and Optimization.rpk	Contains updated files for to the Inventory Planning and Optimization (IPO) application.
Master Production Scheduling.rpk	Contains updated files for to the Master Production Scheduling application.
Order Fulfillment.rpk	Contains updated files for to the Order Fulfillment application.
S&OP.rpk	Contains updated files for to the Sales and Operations Planning (S&OP) application.
Self Healing Supply Chain.rpk	Contains updated files for the Self-Healing Supply Chain (SHSC) application.
Supplier Collaboration.rpk	Contains updated files for to the Supplier Collaboration application.
Non-Application Specific.rpk	Contains updated files that are used by multiple applications or may not be application-specific, such as the Control Tables, Part Properties, or Planning Sheet workbooks.

Applying Service Updates

Service Update content for resources is applied by importing resource packages that contain the updated resources. Resource packages are supplied for each RapidResponse application. For more information, see "Upgrading RapidResponse with Service Updates" on page 152.

If you are adding an application, you must install the relevant resources as described in "Installing RapidResponse applications" on page 130. For subsequent Service Updates, you can update that application by importing its resource package.

▸To apply a Service Update to RapidResponse resources

1. In the directory containing the installation files, browse to the **Rollup/Resources** folder.
2. Copy the **.rpk** file corresponding to the application or resources you want to update.
3. Paste the copied package to a location on the system where RapidResponse Application Server is installed.
4. Sign in to RapidResponse.

5. From the **Go** menu, click **Administration**.
6. Under **System Monitoring**, click **System Utilities**.
7. In the **System Utilities** dialog box, click **Import**.
8. In the **Import Resource Package** dialog box, do the following:
   - Browse to the location where you pasted the **.rpk** file.
   - Select the **.rpk** file.
   - Click **Open**.
9. In the **Import Resource Package** dialog box, review the resources listed on the **Selected Resources** and **Dependent Resources** tabs.

   The **Diff?** column indicates which resources are different from the version in your environment and which are identical.
10. For all modified resources in the RPK for which you want to overwrite the corresponding resource in your RapidResponse environment, ensure **Import version** is selected from the **Action** list.

    The **Import version** option will also overwrite any customizations your organization has made to these resources. Therefore, you can choose to import separate/renamed versions and then compare them against your modified versions before deciding how to proceed or merge the changes.
11. To import a renamed version of a modified resource, do the following:
    - For a given resource, from the **Action list**, click **Rename**.
    - In the **New Name** cell, type a new name for the resource to be imported with.
12. Click **OK** to import the contents of the resource package.
    If you are using the Self-Healing Supply Chain and see a warning about missing scenarios after importing the **Self Healing Supply Chain.rpk** file, run the **ML Service User** script to create the scenarios needed to use the Self-Healing Supply Chain.

CHAPTER 18: Converting standard tables to vector data

Analyzing vector data for key uniqueness 205
Analyzing resources and data for vector upgrade issues 207
Analyzing vector data for currency issues 210
Analyzing vector data for record header issues 213
Converting tables to contain vector data 214
Vector data considerations after upgrading 214
Analyzing vector data origin issues 215

RapidResponse 2014.4 introduced vector series data in standard and custom tables.

Using vectors can help reduce memory consumption. The records in the vector set are represented as a single record in the header table, which stores the references from the vector to the header as a single reference, instead of a separate reference for each vector record. Vector records are not stored as full records, so they do not have the full memory overhead for a record and require the same memory as a single field. In addition, values can be reused across multiple vectors, regardless of which tables the vector sets are defined in.

The records in the vector set are represented as a single record in the header table, which stores the references from the vector to the header as a single reference, instead of a separate reference for each vector record. This reduces memory consumption because the vector records are not stored as full records, so they do not have the full memory overhead for a record and require the same memory as a single field.

Using a vector for date-phased data can improve performance when you are saving changes to many records in a vector set. Changes in a vector set are saved as a single operation, regardless of how many records are in the vector. For example, if a data modification process writes changes over every record in a vector set with 200 records, those changes are saved in a single operation instead of hundreds of individual operations. Similarly, if you are editing summarized data that disaggregates changes into many detail records, using a vector set allows you to save the change to every disaggregated record in a single operation.

Vector sets typically are used to optimize a table structure consisting of header and detail tables. The vector set contains all detail records for each header record.

Conversion process for standard tables

In new installations of RapidResponse (as of version 2014.4), the following five standard tables support vector data series:

- **ForecastDetail**
- **HistoricalDemandActual**
- **HistoricalDemandSeriesDetail**
- **HistoricalSupplyActual**
- **HistoricalSupplySeriesDetail**

If your company is upgrading from RapidResponse 2014.2 (or earlier) to RapidResponse 2014.4 (or later), you can convert the five standard tables to support vector data series. The conversion process can only be executed once you have upgraded to RapidResponse 2014.4 (or later).

The data in the five standard tables must meet several requirements before the conversion process can be applied. Kinaxis provides tools and process to test the requirements. You also have the option to run the tools before you upgrade to be better prepared.

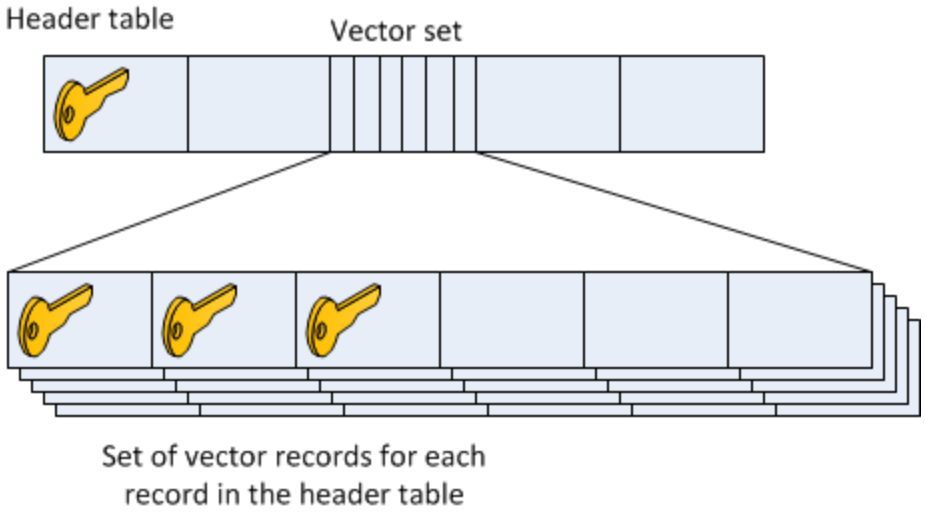
Kinaxis recommends converting the five standard tables to support vector data series so that you can take advantage of performance enhancements. However, the conversion process, in some cases, can be resource intensive.

The rest of this chapter describes the process to convert the five standard tables. If your company is using the On-Premises version of RapidResponse, these steps can be followed as described. If your company is using the On-Demand version, you will need to work with Kinaxis Customer Support to complete the conversion process.

Vector data conversion overview

Tables that can contain vector data have multiple key fields defined to ensure the records in the vector set are unique, and those keys can be of any data type. Vectors are typically used to store date-phased series of data, and should therefore contain a Date key field.

An example of a vector set and its relationship to its owning table is shown in the following illustration.



Before the five standard tables can be converted to support vector data, you must review the data they hold to ensure they meet the following criteria. Conversion resources are available to test tables for possible issues with the conversion to vector data.

- Converted tables cannot contain Notes or Set fields. Before you upgrade to vector data, you should review the tables and remove any custom Notes fields from them. If any tables contain references to these tables, you must remove those reference fields, and redesign the keys for the tables that contained the references if necessary. For more information about modifying tables, see the *RapidResponse Data Integration Guide*.
- Converted tables must contain key fields and uniquely identify records. For more information, see "Analyzing vector data for key uniqueness" on page 205.
- If workbook commands perform operations on worksheets based on the tables that are converted to contain vector data, the changes to the table's key fields might cause the operations to become invalid, and therefore need to be modified. For more information, see "Analyzing resources and data for vector upgrade issues" on page 207.
- Any perspective definition that has been defined on a table that is converted to contain vector data should be modified to use a different table For more information, see "Analyzing resources and data for vector upgrade issues" on page 207.
- Converted tables cannot have a currency attribute. For more information, see "Analyzing vector data for currency issues" on page 210.
- If data updates can delete records in the table, the header records must each be provided from a single data file. For more information, see "Analyzing vector data for record header issues" on page 213.
- If data updates can delete records in the table, all records in the table must have a data origin. For more information about locating and correcting missing origins, see "Analyzing vector data origin issues" on page 215.

Caution: If a table that contains vector data has a Notes field after the upgrade, that field is removed. If a table that contains vector data contains a Set field after the upgrade, the namespace the corresponding reference field is in removed, which deletes all tables and data in that namespace. For more information, see "Analyzing resources and data for vector upgrade issues" on page 207.

Analyzing vector data for key uniqueness

Tables that contain vector data must contain unique records for each header record, and therefore require key fields. The historical tables that are converted to contain vector data do not contain key fields, so prior to the upgrade, you must determine whether adding key fields to the table results in duplicate key values. If the tables contain duplicate fields after converting to vector data, any results form the table should not be used for making decisions because the records used in calculations cannot be predicted. If duplicate keys are found, you can do the following for the table to remove the duplicates:

- Designate additional fields as key fields. Tables that contain vector data can contain any number of base key fields, and fields of any type can be a key. You can also add fields and designate them to be key fields if you require additional fields to identify records in the vector data.
- Merge records that have similar keys. Typically, you can do this if you have specified as many key fields as possible. If you merge records, you must ensure your data update process creates the merged records after converting the tables to contain vector data.

A workbook you can use to find duplicate keys and assess whether adding key fields can resolve issues with duplicate records is available from the Kinaxis Knowledge Network. To access the workbook, go to https://knowledge.kinaxis.com/s/article/Analyzing-your-data-prior-to-converting-standard-tables-to-

vector-data. Click **RapidResponse Vector-related Key analysis** in the Files section to download the workbook.

The workbook reports the number of duplicate records for each header record. You can add columns to the worksheets to represent the fields to be used as keys. By comparing the results of adding the field, you can determine if that key has made records unique, and then continue adding key columns until you cannot add more fields.

Key uniqueness must be checked for each scenario that is used for modifying data, to ensure the correct values are returned in worksheets. You should check the key fields you have added in every scenario, and add key fields or merge records where needed, until all scenarios report unique values for the table.

The owning reference is automatically used as a key field for the vector data, and the fields within the vector set must contain unique values. Additional key fields can be specified according to how the data is structured, or depending on the fields used to transform data. For example, if your data update process performs modifications on the historical data, the fields that are marked as view-only in the automatic data modification worksheets should be considered candidates for key fields.

After establishing the key fields, you must ensure any workbook commands and automatic data modifications in worksheets that are based on the converted tables are still valid. For more information, see "Analyzing resources and data for vector upgrade issues" on page 207.

▸To assess which tables have duplicate key fields

1. Import and open the **RapidResponse Vector-related Key analysis** workbook.
2. For one of the tables that will be converted, click that table's **Grouped** worksheet.
3. In the **Scenario** list, select a scenario to use for the analysis.

   The number of duplicate values for each header record is displayed.
4. To determine which fields are being duplicated, click the link in the **Count** column.

   The **Details** worksheet displays the duplicate values.

▸To test a new key field

1. In the table's **Details** worksheet, open the worksheet properties.
2. In the **Worksheet Properties** dialog box, click the **Columns** tab.
3. Add a column for each field that you want to use as a key.
4. Click **OK**, and then open the properties for the table's **Grouped** worksheet.
5. On the **Columns** tab, add columns for the same fields you added in step 3.
6. On the **Grouping** tab, specify the **Group By** grouping rule for the new columns.
7. Click **OK** twice.
8. Exit design mode and save your changes.
9. In the table's **Grouping** worksheet, if any fields are still duplicated, repeat this procedure until either you have added all fields you can as keys, or no duplicate keys are reported.

   If the table contains duplicates and you have no more fields you can make a key, you should consider merging records to ensure only a single value is returned for a set of key values. This requires you to ensure the duplicated records can be merged, and to modify your data integration to ensure the records are merged.

After you upgrade the tables, you must ensure the changes you have specified are made to the table and your data sources after the upgrade. For more information, see the *RapidResponse Data Integration Guide*.

Analyzing resources and data for vector upgrade issues

Before you can upgrade your RapidResponse system to use vector data, it must be tested for resource and data upgrade issues. If any issues are found, they must be remedied before continuing the upgrade process.

The **PreUpgradeAnalyzer** utility examines your RapidResponse system for three potential upgrade issues:

- "Workbook commands" on page 207
- "Perspectives" on page 207
- "Invalid field types" on page 208

Workbook commands

If workbook commands perform operations on worksheets based on the tables that are converted to contain vector data, the changes to the table's key fields might cause the operations to become invalid, and therefore need to be modified.

For each update operation in workbooks, the source worksheet, destination worksheet, and operations performed by the update are reported. For each modification operation in workbooks, the worksheet the modification is performed on is reported. For each of the table's key fields and the fields you have specified that will become keys after upgrading, the following properties are also reported:

- Is Present—Whether the key field is present in the worksheet. This value is reported for update and modification operations.
- Is Writable—Whether the key field's value is editable. This value is reported for update and modification operations.
- Is Adjacent To Keys—Whether the key field has only other key columns to the left of it in the worksheet. This value is reported only for update operations.

Keys that are editable can represent an issue when the table is converted to contain vector data. Because the key field is editable, a value that results in a duplicate key could be written into that field, leading to invalid results in the vector data. Keys that do not have other key fields beside them can also represent issues, because the key fields are used for grouping records in the worksheets. If a standard field is placed between key fields, the worksheet that performs the data modification is not valid and cannot be used for automatically modifying data.

Perspectives

Any perspective definition that has been defined on a table that is converted to contain vector data should be modified to use a different table. Because perspectives are not valid for vector data, any perspective definition that uses a table that contains vector data is not applicable, and is ignored. If the modifications applied by the perspective are essential, you can define an automatic data modification that modifies the values to match the perspective.

Invalid field types

All Note fields on tables that will be converted to contain vector data are deleted during the upgrade process. For any Set field on the table , the reference field that points to the converted table is no longer a valid field. To ensure data is not invalidated by the upgrade, the namespace and all tables, fields, and data in that namespace are deleted. To prevent this, you must modify any references to the table that will be converted prior to the upgrade.

PreUpgradeAnalyzer utility

The **PreUpgradeAnalyzer** utility examines your RapidResponse system for potential upgrade issues. The utility takes a configurable XML file that specifies the RapidResponse Server name to check and, for each table that is converted, an optional list of custom fields that you will use as a key field for the vector data. The results of the utility's analysis is a Microsoft Excel workbook. You can specify the location this file is saved and its name in the configuration file.

The **PreUpgradeAnalyzer** utility is available from the Kinaxis Knowledge Network. A version of this utility is available for each RapidResponse version, so you must ensure you use the specific utility designed for the RapidResponse version you are upgrading from. For more information and to download this utility, go to https://knowledge.kinaxis.com/s/article/Analyzingresourcesanddataforvectorupgradeissues53745.

▸To configure the upgrade utility

1. Extract the utility's **.zip** file into a folder of your choice.
2. Using Windows Explorer, navigate the to location you extracted the **.zip** file.
3. Edit the **config.xml** file.
4. Specify the following options as required.

Element	Required	Description
server	Yes	The RapidResponse Server name. For example, `<server>localhost</server>`
adminPassword	Yes	The password for the Master Administrator user account (Admin user). For example, `<adminPassword>P45sW0rD</adminPassword>`
outputFolder	No	Optionally, the folder to save the results file in. For example, `<outputFolder>..\ResultReports</outputFolder>`
outputFile	No	Optionally, the name of the Microsoft Excel workbook the analysis is saved in. For example, `<outputFile>UpgradeReport</outputFile>`

Element	Required	Description

keyFields	No	Optionally, the custom fields that will be used as key fields when the tables are converted to vectors. For each item in this list, you must specify the namespace-qualified table name and each field on that table that will be used as a key. For example,
		`<keyFields>`
		`  <table>`
		`  <name>Mfg::HistoricalDemandActual</name>`
		`  <fields>`
		`  <name>User::BatchNumber</name>`
		`  <name>User::LastRunDate</name>`
		`  </fields>`
		`  </table>`
		`</keyFields>`

errorsOnly	No	Optionally, specifies whether only errors are returned in the report. If this value is not included or is set to `true`, only the errors are reported. If this value is included and is set to `false`, all worksheet and field issues are included in the report. For example, `<errorsOnly>false</errorsOnly>`

You can also change the configuration file's name, copy the **config.xml** file to create additional sets of configuration options, or create a configuration file by creating a new document and specifying the elements listed above.

5. Save your changes.

▸To analyze resources for upgrade issues

1. In Windows Explorer, navigate the to location you extracted the **.zip** file.
2. Modify the configuration file to add the `<errorsOnly>` element and set it to **false**. Save your changes.
3. Open a Command Prompt window.
4. Navigate the to location you extracted the **.zip** file.
5. Run the following command:

   `PreUpgradeAnalyzer_version.exe configuration`

   where `version` is the version of RapidResponse you are upgrading from, and `configuration` is the name of the configuration file. For example, if you are upgrading from RapidResponse 2014.1, you would specify the version argument as `2014.1`.

   In some cases, a RapidResponse Service Update introduces a significant change that requires a new version of the PreUpgradeAnalyzer utility. In this case, the Service Update level that requires the new version of the utility is indicated in the `version` value, separated from the version number by an underscore. For example, RapidResponse 2016.2 Service Update 5 introduced significant changes to RapidResponse's infrastructure, so the `version` value to analyze an upgrade to a version later than Service Update 5 is `2016.2_5`.
6. When the utility completes, open the Microsoft Excel workbook.
7. Review the worksheets that have **Upgrade** or **Insert** operations.
8. Modify the configuration file to add key fields as needed, and run the command until all the fields that will be key fields in the converted tables are represented in the report.
9. Modify the configuration file to set the `<errorsOnly>` element to **true**. Save your changes.
10. Run the `PreUpgradeAnalyzer_version` command again.
11. When the utility completes, open the Microsoft Excel workbook.

12. For each reported error, modify the worksheet automation to resolve the error.
13. Run the command again, and repeat these steps until no more errors are reported.

▸To analyze invalid perspectives and fields

1. Open a Command Prompt window.
2. Navigate the to location you extracted the **.zip** file.
3. Run the following command:

   `PreUpgradeAnalyzer_version.exe configuration`

   where `version` is the version of RapidResponse you are upgrading from, and `configuration` is the name of the configuration file. For example, if you are upgrading from RapidResponse 2014.1, you would specify the version argument as `2014.1`.

   In some cases, a RapidResponse Service Update introduces a significant change that requires a new version of the PreUpgradeAnalyzer utility. In this case, the Service Update level that requires the new version of the utility is indicated in the `version` value, separated from the version number by an underscore. For example, RapidResponse 2016.2 Service Update 5 introduced significant changes to RapidResponse's infrastructure, so the `version` value to analyze an upgrade to a version later than Service Update 5 is `2016.2_5`.
4. When the utility completes, open the Microsoft Excel workbook.
5. Review the following worksheets.
   - **Invalid Fields**—Reports all Notes fields in tables that will be converted to contain vector data or all references to these tables.
   - **Invalid Perspectives**—Reports all perspectives that define changes on tables that will be converted to contain vector data.

Analyzing vector data for currency issues

When you convert tables to contain vector data, those tables cannot have currencies defined, and instead inherit their currency attributes from the owning table. Prior to converting the tables to contain vector data, you must ensure the tables do not have a currency defined. You can also analyze your tables to determine if tables have multiple currencies defined, which might indicate issues because all records in a vector must have the same currency for each header.

A workbook named **RapidResponse Vector-related Currency Analysis**, which you can use to analyze the tables to determine if any currency work is required, is available from the Kinaxis Knowledge Network. To access the workbook, go to https://knowledge.kinaxis.com/s/article/Analyzing-your-data-prior-to-converting-standard-tables-to-vector-data. Click **RapidResponse Vector-related Currency Analysis** in the Files section to download the workbook.

- Identify vectors that have currencies defined.
- Analyze how currencies are used in vector data and how the currency can be transitioned to the header records
- Locate data that must be modified to enforce the currency rules

If a table that will be converted to contain vector data has a currency defined, you should typically move that currency expression to the header table. However, if the currency expression results in multiple currencies for a single header, you must modify the expression to ensure a single currency is produced for each header, which results in a single currency for the vector data.

The currency or currencies defined for a table are listed in this worksheet, which can help you determine how the currency is being specified. For example, the currency might be set by a custom field on the table, or by a currency attribute defined on the table. Regardless of how it is specified, the currency must be moved to the owning table, or any other table above this table in the data model.

For headers that report multiple records, you must modify the table to ensure each header has a single currency.

▸To locate currency violations

1. Import and open the **RapidResponse Vector-related Currency Analysis** workbook.
2. Click a table's **Currency Violations** worksheet tab. For example, the **HistoricalDemandActual Currency Violations** worksheet.
3. Select the scenario to analyze data in. This must be a scenario in which records are created in the table you selected.
4. If the worksheet contains no records, this table and scenario require no additional work.

   Otherwise, you must modify the table, as described in "Modifying tables to resolve currency issues" on page 211.
5. Repeat steps 3 and 4 for each scenario that records are created in this table.
6. Repeat this procedure for each table.

▸To determine whether a header has multiple currencies

1. For a table that has a currency defined, click the table's **Grouped** worksheet. For example, if the **HistoricalSupplyActual** table has a currency, click the **HistoricalSupplyActual Grouped** worksheet.
2. Open the worksheet properties.
3. For the **Currency** column, modify the expression to match the converted table's currency expression.
4. Save your changes to the worksheet definition.
5. Click the table's **Currency Violations** worksheet.
6. In the **Scenario** list, select a scenario in which a record has been inserted in the table's header.

   If header records are reported in this worksheet, you must either modify the header creation process to either group data by currency to ensure a single currency is created for each header record, or modify the header table's currency expression to ensure a single currency value is specified. You should also add a currency field to the header table to ensure that field is used in the table's currency expression.

Modifying tables to resolve currency issues

Header records with multiple currencies represent invalid vector data. To resolve these issues, you can do either of the following:

- Modify the table and data update process to ensure a single currency is defined for each header record.
- Configure a process that loads the data into a custom table instead of the vector. You can then create a worksheet that displays this data with a single currency, and then perform an automatic data modification to move the records into the vector.

You must also resolve data issues caused by currencies. Depending on how you want to configure the data, you can define a single currency for the table, or enable multiple currencies for the table, as long as a single currency is used for each header record. The change you make to the data must be made in each scenario that you use for reporting or working with Money values.

If you have data that contains multiple currencies but you want it to use a single currency, you can define a process that copies records to a custom table, changes the currency value for the table, and then copies the modified values back into the table.

To perform this modification, perform the following steps:

1. Choose the currency you want to use, and then identify the records that you must modify the currency for.
2. Create a custom table that contains the following fields:
   - RecordId
   - attribute<Core::Currency>
   - each of the Money fields from the table
3. Modify the currency attribute to match the currency for the table. For example, you could set the table's currency to a specific value.

   This modification typically results in incorrect data values because the value is not modified when the currency is changed. You must convert the value to ensure it is correct, or update your data extraction to bring in records using the new currency, and modify the values as required.
4. Copy the Money values into the table.
5. Delete the custom table.

For more information about managing currencies, see "About currencies" on page 683. For more information about adding and modifying tables and specifying the currency used in tables, see the *RapidResponse Data Integration Guide*.

If you want to use multiple currencies for the table, you can define automatic data modifications that copy records from one header to another with a different currency. To perform this modification, perform the following steps:

1. Identify the currencies you want to use in the table
2. If necessary, create header records that use the required currencies. You can do this by creating an automatic data modification worksheet that updates records in the header table with header values from the table that will be converted to contain vector data, with the new currency specified.
3. For each currency that new headers are created for, do the following:
   - Create worksheets to be used to insert or modify data in the table that will be converted to contain vector data.
   - In those worksheets, add a worksheet filter that locates records in the table and in the header table that have the same currency. For example, the expression `attribute<currency>='USD' and Header has Actuals[attribute<currency><>'USD']` locates records in the table and actual orders in the header table that use the US Dollar currency.
   - Define a modification operation in the worksheet and arrange the columns so the new currency for the header overwrites the current currency.
4. Perform the data modifications on each scenario that requires the changes.

For more information about automatic data modifications, see the *RapidResponse Resource Authoring Guide*.

Analyzing vector data for record header issues

For tables that are converted to contain vector data, if the table is configured to allow data updates to delete data, the vector's header record data must be provided by a single data source. For each header that is updated from multiple sources, you must modify your integration settings to ensure all updates for that header record are brought in from a single source.

If multiple sources update a header record, because the vector records do not have the same source, they are not considered to be the same records. This causes the entire vector to be replaced, which might cause unexpected results or remove records that are needed in processes. If you cannot provide the updates for a header record in a single data source, you might consider splitting the record into multiple header records, which ensures the resulting records are correct.

A workbook named **RapidResponse Vector-related Origin Analysis**, which you can use to determine which tables are updated by multiple sources, is available from the Kinaxis Knowledge Network. To access the workbook, go to https://knowledge.kinaxis.com/s/article/Analyzing-your-data-prior-to-converting-standard-tables-to-vector-data. Click **RapidResponse Vector-related Origin Analysis** in the Files section to download the workbook.

▸To determine the tables and scenarios used for updating data

1. On the **Administration** pane, under **Data**, click **Data Model**.
2. Open the properties of the following tables to determine if any of them have **Insert, modify, and delete records** specified in the **Allow data update to** area:
   - **HistoricalDemandActual**
   - **HistoricalDemandSeriesDetail**
   - **HistoricalSupplyActual**
   - **HistoricalSupplySeriesDetail**
3. Close the **Data Model** dialog box.
4. On the **Administration** pane, under **System Settings**, click **Scheduled system Tasks**.
5. In the **Task Arguments** worksheet, locate any **Scenario** arguments that have been defined for a **DataUpdate** operation.

▸To determine which tables are updated from multiple sources

1. Import and open the **RapidResponse Vector-related Origin Analysis** workbook. You might receive an error when importing this workbook. The error can be ignored.
2. Click the worksheet tab for either the **ForecastDetail** table or any worksheet for the tables that are managed by data updates.
3. In the **Scenarios** list, select the **Enterprise Data** scenario or one of the scenarios that you identified as a data update target.
4. Repeat these steps for all tables that are managed by data updates and scenarios that are data update targets.

If any tables are returned by the worksheets, you should consider changing the table's properties to not delete records during data updates. Otherwise, you can modify your data extract processes to ensure all data for a header comes from a single source. For more information about modifying tables and data sources, see the *RapidResponse Data Integration Guide*.

Converting tables to contain vector data

After you have reviewed the data in the tables to be converted, and made appropriate changes, you can convert the following standard tables to contain vector data:

- **ForecastDetail**
- **HistoricalDemandActual**
- **HistoricalDemandSeriesDetail**
- **HistoricalSupplyActual**
- **HistoricalSupplySeriesDetail**

For more information about the conversion process and data changes, review "Vector data conversion overview" on page 204.

After you convert tables to contain vector data, you cannot revert this change.

If you are using On-Premises RapidResponse, you can convert tables to contain vector data by performing an operation using the RapidResponse Console. If you are using the On-Demand RapidResponse service, Kinaxis Customer Support can perform the table conversion when you are ready for it.

▸To convert tables to contain vector data

1. Sign in to the RapidResponse Console. For more information, see "To sign in to RapidResponse Console" on page 230.
2. Click the **Query** tab.
3. In the **Query** box, type `EnableVectors()`.
4. Click **Submit**.
5. Click the **Actions** tab, and then click **Restart Service**.

Vector data considerations after upgrading

Data change tracking is not available for tables that contain vector data. However, after upgrading you might have workbooks that contain automatic data modifications that are configured to log data changes on worksheets based on the tables that have been converted to contain vector data. In this case, no changes are tracked, but the logging process is still performed. You should modify the workbook commands in these workbooks to not log changes, which can improve performance.

For tables that are converted to contain vector data, you can modify the tables to replace the use of identifier fields with the new key fields. For example, in the ForecastDetail table, typically the Id field was populated using a concatenation of values to ensure the detail records were unique. This process required multiple operations to construct the Id field values and consumed significant amounts of memory. After upgrading, you can use the fields that were used to construct the concatenated values as the keys, which also allows you to stop populating the Id field. After defining other keys, you can hide the Id field. This clears the data from the Id field, which reduces memory consumption. You must have permission to modify the data integration to perform this function.

▸To hide the ForecastDetail.Id field

1. In the **Administration** pane, under **Data**, click **Data Model**.
2. In the **Data Model** dialog box, under **Table**, select the **ForecastDetail** table. You might need to change the selections in the **Show** and **Namespace** lists if the table is not shown.
3. In the **Fields** area, select the **Id** field.
4. Click **Field**, and then click **Properties**.
5. Select the **Hide field** check box.
6. If you want the **Id** field's data values to be deleted, select the **Delete field data on next RapidResponse restart** check box.

For more information about vectors, see the *RapidResponse Analytic and Data Model Guide*. For more information about creating or converting tables to vectors, see the *RapidResponse Data Integration Guide*.

Analyzing vector data origin issues

Each record in a table, aside from the historical tables, has a data origin, which determines how the record was created. The data origin field for a record is populated when you perform a data update. Any records that do not have an origin value are not managed by data updates, and are never deleted during a data update. In this case, the records might result in unexpected data in the record's table. These records without an origin must be manually deleted. For more information about data origins, see "Origin of database records" in the *RapidResponse Data Integration Guide*.

After you convert a table to contain vector data as described in "Converting tables to contain vector data" on page 214, any data origin values for the table are lost, and a new origin field on the vector's owning table is created. This process applies to the ForecastDetail table when you convert it to contain vector data. For any of the historical tables that can be converted to contain vector data, this process applies to the table if it has been configured to allow data updates to manage record lifetimes. The origin value determines whether records that are not presented in a data update are deleted.

After converting the table, you should perform two data updates that bring in all the records you want data updates to manage. The same data files should be used for both of these data updates. The first of these data updates creates the data origins for the records in the table. The second data update deletes all records that are not present in the data files used in the data update. This process ensures that all records provided in a data update have an origin. Any records without an origin will not be managed by data updates, and should be deleted.

A workbook named **Vector Originating Files** is available on the Kinaxis Knowledge Network to report the records that do not have a data origin. You can use this workbook to manage any records with missing origins. To download this workbook, click the following link: https://knowledge.kinaxis.com/s/article/VectorOriginatingFilesworkbook68109.

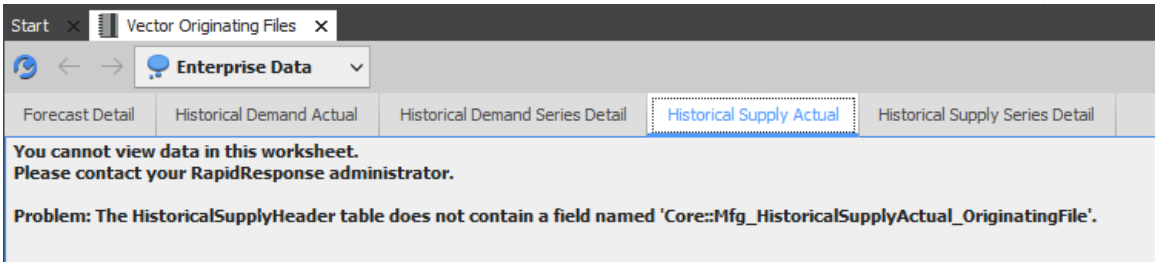
This workbook contains one worksheet for each standard RapidResponse table that can contain vector data. For the tables that allow data updates to manage data, the worksheet displays all records that do not have an OriginatingFile value. These records do not have a data origin and will not be deleted by data updates. You should delete these records.

For more information about allowing data updates to manage data in historical tables and tables that contain vector data, see the *RapidResponse Data Integration Guide*.

▸To analyze vector origins

1. After converting the tables to contain vector data, perform two data updates that bring in all records you want data updates to manage.
2. Import and open the **Vector Originating Files** workbook.
3. In the **Data Settings** dialog box, specify the scenario that your data updates target.
4. In each worksheet that displays data, delete the records reported in the worksheet.

   For any of these tables that do not allow data updates to manage records, the worksheet for that table reports an error, as shown in the following illustration. These errors are expected, and data updates continue to bring in new data for these tables.



If you have upgraded to RapidResponse 2016.2 (or later), the IndependentDemand table's FeatureList field has been modified to be a vector set, represented by a table named IndependentDemandFeatureList. If you are using this table and want data updates to manage the data in it, a separate workbook named **Vector Originating File - FeatureList** is available for analyzing its data origin. To download this workbook, go to https://knowledge.kinaxis.com/s/article/Analyzing-your-data-prior-to-converting-standard-tables-to-vector-data. Click **Vector Originating File - FeatureList** in the Files section.

▸To analyze the IndependentDemandFeatureList table's origin

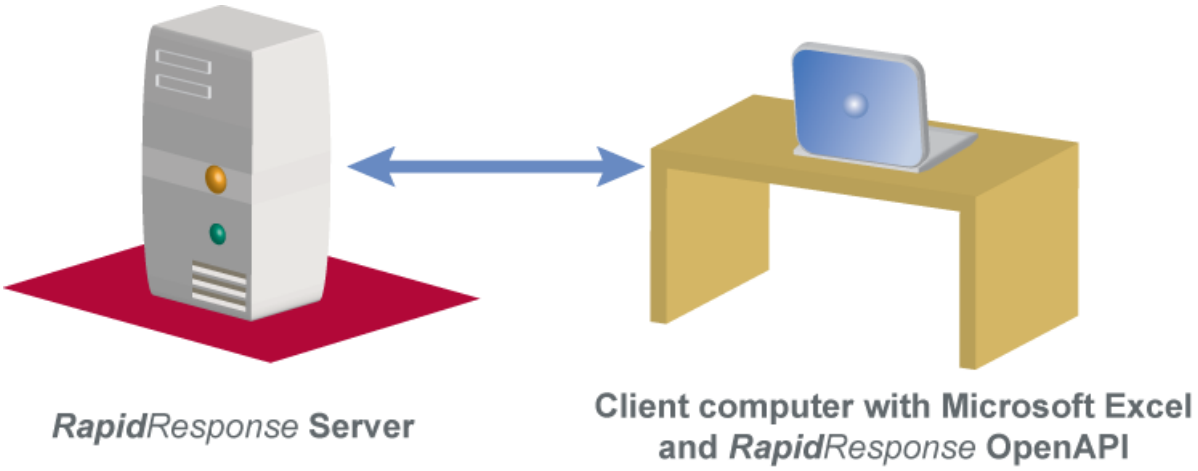
1. After converting the table to contain vector data, perform two data updates that bring all records you want data updates to manage.
2. Import and open the **Vector Originating File - FeatureList** workbook.
3. In the **Data Settings** dialog box, specify the scenario that your data updates target.
4. In the **FeatureList** worksheet, delete the records reported in the worksheet.

CHAPTER 19: Upgrading RapidResponse OpenAPI applications

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

How to upgrade OpenAPI 217

RapidResponse OpenAPI is a set of registered Microsoft COM objects (DLL files) that are used to programmatically access RapidResponse Server. Custom applications can use RapidResponse OpenAPI to retrieve data from RapidResponse Server. For example, a custom application running inside of Microsoft Excel can retrieve data from RapidResponse Server as shown in the following illustration.



How to upgrade OpenAPI

Users can upgrade RapidResponse OpenAPI by downloading the installation program from the RapidResponse Application Server. Alternatively, the installation program is available from the RapidResponse DVD.

▸To upgrade by downloading from RapidResponse Application Server

1. Open a Web browser.
2. Type **http://servername/rapidresponse/en/openapi/setup.exe** into the Address box of the browser where **servername** is the computer where RapidResponse Application Server is installed.
3. Click **Run** or **Open** to start the installation program.
4. Follow the installation program instructions.
5. Click **Finish**.

   If the RapidResponse OpenAPI is already running, you need to reboot the computer to complete the installation.

▸To upgrade RapidResponse OpenAPI using the RapidResponse DVD

1. Insert the RapidResponse DVD into the DVD drive on the client computer where you want to upgrade RapidResponse OpenAPI.

   If a menu does not display, use Windows Explorer to navigate to your DVD drive, and double-click the DVD drive icon to run the RapidResponse DVD.
2. Click **Browse the DVD**.
3. Using Windows Explorer, navigate to the **\Server\OpenAPI** folder on the DVD and double-click one of the following files:
   - **setup.exe** for 32-bit operating systems
   - **setupx64.exe** for x64 operating systems
4. Click **Next**.
5. Click **Finish**.

   If the RapidResponse OpenAPI is already running, you need to reboot the computer to complete the installation.

RapidResponse OpenAPI installation location

On 32-bit operating system computers, RapidResponse OpenAPI is then installed into the **C:\Program Files\Common Files\Kinaxis\openAPI*x_y_z*** folder. In the folder name, ***x*** represents the RapidResponse Server major version number, ***y*** represents the minor version number, and ***z*** represents the release number (for example, **openAPI7_3_5**).

On 64-bit operating system computers, 32-bit and 64-bit versions of RapidResponse OpenAPI are installed in the following folders, respectively:

- **C:\Program Files (x86)\Common Files\Kinaxis\openAPIx_y_z**
- **C:\Program Files\Common Files\Kinaxis\openAPIx_y_z**

CHAPTER 20: Preparing to transition away from RapidResponse OpenAPI

Support for OpenAPI to be discontinued 219
System requirements for OpenAPI logging 220
Installing the OpenAPI Service Update for new logging capability 220
Enabling OpenAPI detailed logging 220
Sending log files to Kinaxis 223

RapidResponse OpenAPI is a set of registered Microsoft COM objects (DLL files) that are used to programmatically access the RapidResponse Server database. Historically, RapidResponse OpenAPI was used for communication between the RapidResponse Application Server and RapidResponse Server.

Additionally, custom applications could be developed to have RapidResponse OpenAPI interact with RapidResponse Server. For example, a custom application running inside of Microsoft Excel can retrieve data from RapidResponse Server.

Custom applications could be created in a variety application development environments that supported COM objects, including Microsoft Visual Basic, Microsoft IIS (Internet Information Server), Microsoft Visual Studio (Visual C++, Visual InterDev, Visual J++, Windows Scripting Host), and Microsoft Office applications using VBA (Visual Basic for Applications), amongst others.

Support for OpenAPI to be discontinued

RapidResponse OpenAPI is more than 15 years old and relies on technology that is suitable only for internal networks. Since 2010, the focus of RapidResponse API maintenance has shifted towards web services such as RapidResponse Web Services, RapidResponse Scripting, and RapidResponse Real-time Integration Service.

Web service client programs can run over the Internet or a local intranet using standard network protocols such as HTTP, HTTPS, and SOAP. RapidResponse web services include methods to read and update data, run scripts, import and export data as well as capture RapidResponse data changes.

A future version of RapidResponse (to be released in 2018) will no longer support RapidResponse OpenAPI.

To help you transition away from OpenAPI, RapidResponse introduces a new detailed OpenAPI logging capability to help you evaluate your exposure to OpenAPI calls and usage patterns. Kinaxis can evaluate the logs and offer instruction and advice on how to migrate to alternative RapidResponse tools.

System requirements for OpenAPI logging

The RapidResponse OpenAPI detail logging capability can only be used on On-Premises systems. This capability cannot be used by customers using the On-Demand RapidResponse service (sometimes called SaaS or Software as a Service).

Installing the OpenAPI Service Update for new logging capability

Instructions for installing service updates are also available from the download site. The RapidResponse OpenAPI service update needs to be installed on the following systems:

- The system where RapidResponse Server is installed. This system might be running OpenAPI Server Exits, Server Add-ins, and batch scripts that leverage OpenAPI.
- If RapidResponse Server and RapidResponse Application Server are installed on different computers, the OpenAPI service update needs to be installed on the computer where RapidResponse Application Server is installed
- If custom OpenAPI applications are being used on client computers (for example, an application running inside of Microsoft Excel that retrieves data from RapidResponse Server), apply the OpenAPI service update to each client computer that uses the custom application.

  On 32-bit operating system computers, RapidResponse OpenAPI is then installed into the **C:\Program Files\Common Files\Kinaxis\openAPIx_y_z** folder. In the folder name, x represents the RapidResponse Server major version number, y represents the minor version number, and z represents the release number (for example, openAPI10_1_0).

  On 64-bit operating system computers, 32-bit and 64-bit versions of RapidResponse OpenAPI are installed in the following folders, respectively:
  - C:\Program Files (x86)\Common Files\Kinaxis\openAPIx_y_z
  - C:\Program Files\Common Files\Kinaxis\openAPIx_y_z

Enabling OpenAPI detailed logging

The OpenAPI detailed logging must be manually enabled on each computer where the OpenAPI service update was installed. The following steps are required to enable logging.

Delete OpenAPI INI and log files

The OpenAPI service update installation creates a file named **OpenAPI-<program>-log.ini** for each OpenAPI program or executable found. Each of these INI files must be manually deleted. In addition, you should also delete existing OpenAPI log files that use the name pattern **OpenAPI-<program>.log** where **<program>** represents the name of the OpenAPI program or executable found.

On the computer where RapidResponse Server is installed, the file is stored in the **C:\RapidResponse\Logs** folder. This is the default location for log files. If your RapidResponse system has been customized, this folder might be in a different location. For more information about customizing the location of the Logs folder, see the RapidResponse Administration Guide.

On the computer where RapidResponse Application Server is installed (if not on the same computer as RapidResponse Server), the INI file is stored in the **C:\RapidResponse\Logs** folder.

On client computers, the INI files are stored in the **C:\RapidResponse\Logs** folder.

Note: The locations of the Logs folder for the Application Server and client computers can also be customized. To do so, follow same procedure used when customizing the location of the Logs folder for RapidResponse Server.

Resetting IIS

After the OpenAPI service update is applied to the computer where RapidResponse Application Server is installed (either standalone or with RapidResponse Server), Internet Information Services (IIS) for Windows® Server must be stopped and started. Once IIS has been restarted, complete the following steps:

1. Sign into the Java client or the web client.
2. Sign out of the client.
3. With a text editor, open the OpenAPI-w3wp-log.ini file (on the computer where RapidResponse Application Server is installed).
4. Add a ! character to the beginning of the following lines:
   - log4j.logger.RapidResponse.OpenAPI.Internal.EntryPoint=DEBUG
   - log4j.logger.RapidResponse.OpenAPI.Internal.Parameters=DEBUG
5. Save the file.
6. Stop and restart IIS.

Caution: Not commenting out the two lines in the INI can significantly impact your system's performance.

Note: Instead of starting with log4j.logger, the lines to edit in the text file might start with log4cplus.logger. This applies to RapidResponse 2014.1 (and later).

Resetting the RapidResponse Service Host service

The RapidResponse Service Host service must be reset after OpenAPI service update is applied. To do so, complete the following steps on the computer where RapidResponse Server is installed.

1. Stop the RapidResponse Service Host service. For more information about stopping this service, see the RapidResponse Administration Guide.
2. With a text editor, open the **OpenAPI-ServiceHost-log.ini** file.
3. Add a ! character to the beginning of the following lines:
   - log4j.logger.RapidResponse.OpenAPI.Internal.EntryPoint=DEBUG
   - log4j.logger.RapidResponse.OpenAPI.Internal.Parameters=DEBUG
4. Save the file.

5. Start the RapidResponse Service Host service. For more information about starting this service, see the RapidResponse Administration Guide.

Caution: Not commenting out the two lines in the INI can significantly impact your system's performance.

Note: Instead of starting with **log4j.logger**, the lines to edit in the text file might start with **log4cplus.logger**. This applies to RapidResponse 2014.1 (and later).

Turn on OpenAPI logging

After the OpenAPI service update has been applied to RapidResponse Server, RapidResponse Application Server (if applicable), and OpenAPI client computers (if applicable), and the other steps have been completed, the OpenAPI detailed logging can be turned on for each computer.

To turn on OpenAPI detailed logging, you must edit Windows Registry on each computer where the OpenAPI service update was applied. RapidResponse registry settings are stored in the main configuration key located in:

HKEY_LOCAL_MACHINE\SOFTWARE\Webplan Inc.\Webplan

OpenAPI logging is enabled when **OpenAPILogging** value is set to 1 (this is a DWORD).

Logging commences once the OpenAPI applications are started (manually or scheduled).

Notes:

- After you change the Windows Registry on the computer where RapidResponse Application Server is installed, you must stop and restart Internet Information Services (IIS).
- If OpenAPI detailed logging is turned on and RapidResponse Application Server is not installed on the same computer as RapidResponse Server, you can expect the Application Server performance to degrade by approximately 5 percent. Performance returns to normal once the OpenAPI detailed logging is turned off.
- After you change the Windows Registry on the computer where RapidResponse Server is installed, you must stop and restart the RapidResponse Service Host service.
- To turn off logging, set the OpenAPILogging value is set to 0. This change must be applied to all computers where OpenAPI logging was turned on including RapidResponse Server, RapidResponse Application Server (if applicable), and OpenAPI client computers (if applicable).

Caution: Improperly modifying the Windows registry can result in system instability. Before modifying the registry, create a backup using the Export tool in the Microsoft Registry Editor. For more information, see the Microsoft Registry Editor Help.

Sending log files to Kinaxis

Once you have determined that all your RapidResponse OpenAPI applications have run, all the log files need to be zipped together and sent to the Kinaxis Customer Support team at support@kinaxis.com.

Before doing so, ensure all your OpenAPI applications have run and exercised all the application functions. To do so, you might need to review your internal processes regarding RapidResponse. Some applications might be scheduled, others might be manually run, and others might run as Server Exit applications (scenario or server operations as the trigger). You might also want to contact your user base to better understand how they are using RapidResponse to help understand the use of OpenAPI applications.

After you have sent your log files to the Kinaxis Customer Support, you can turn off detailed OpenAPI logging. To turn off logging, set the **OpenAPILogging** registry value is set to 0. This change must be applied to all computers where OpenAPI logging was turned on including RapidResponse Server, RapidResponse Application Server, and OpenAPI client computers. You must also restart OpenAPI applications.

Note: Turning off OpenAPI detail logging does not turn off all OpenAPI logging. RapidResponse continues to log standard OpenAPI operations.

Part 4: Server management for On-Premises environments

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

- "RapidResponse Server management" on page 227
- "RapidResponse system memory and monitoring" on page 259
- "RapidResponse Server settings" on page 273
- "RapidResponse Server failover clustering" on page 289
- "Monitoring RapidResponse system availability" on page 307
- "Managing the RapidResponse database" on page 309
- "Data persistence" on page 329
- "Automatic RapidResponse Server operations " on page 335
- "Server exit applications" on page 343
- "Registry Settings for RapidResponse Server" on page 351
- "Monitoring your environment with the RapidResponse Log Service" on page 367

CHAPTER 21: RapidResponse Server management

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

RapidResponse Windows Services 227
RapidResponse Console 235
Authenticating RapidResponse Server 239
Reviewing RapidResponse Server activity 239
Troubleshooting RapidResponse Server 241
Internal errors and system crashes 244
RapidResponse Server folder structure 249
Archiving RapidResponse package files 252
Performance impacts from scans and agents 255

The RapidResponse system runs as Microsoft Windows services. This chapter discusses the services and how to configure them. As a system administrator, you can also use Microsoft Windows and RapidResponse tools to review system activity. This is especially important in troubleshooting cases or to simply maintain RapidResponse service uptime.

RapidResponse Windows Services

RapidResponse runs as Microsoft Windows services. The main services are:

- **RapidResponse Server**—Runs the RapidResponse Server application and is set to start manually. You can use the Microsoft Windows Services dialog box to have this service automatically start when the computer where RapidResponse Server is installed is started. For more information, see "The Windows Services dialog box" on page 232 and "Configuring the RapidResponse Server service" on page 233.
- **RapidResponse Service Host**—Runs all alerts, scheduled tasks, automation chains, and business process notifications for RapidResponse. After the installation of RapidResponse Server, this service is set to automatically start. In some cases, you might need to restart this service manually.

  The RapidResponse Service Host creates a Microsoft Windows user named RapidResponseService. All alerts, scheduled tasks, and automation chains are processed as this user account, and cannot run under any other. The password for this account is set automatically, and must not be changed.

  For more information about Service Host, see "Configuring RapidResponse Service Host" on page 234.

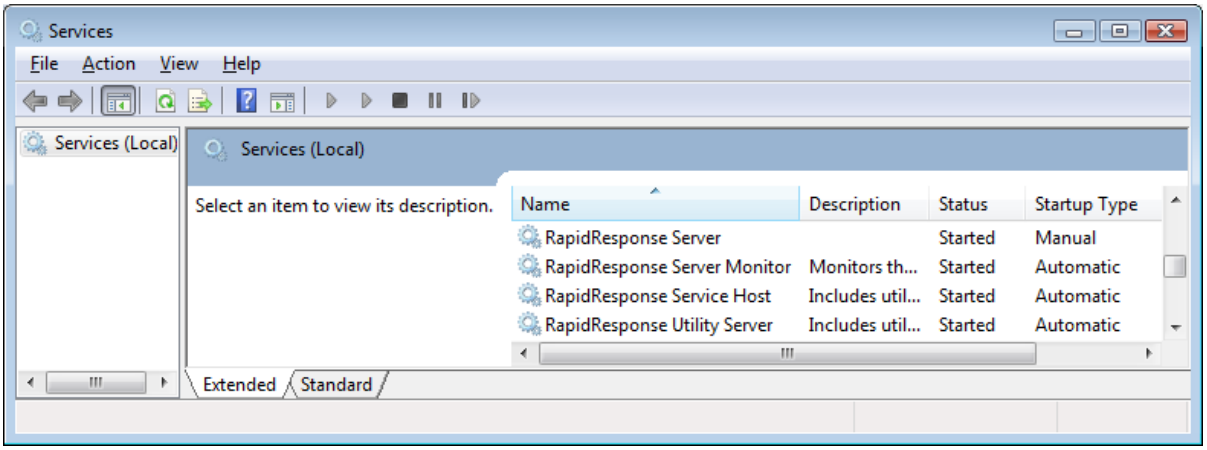
- **RapidResponse Utility Server**—Runs internal utility programs that support RapidResponse. After the installation of RapidResponse Server, this service is set to automatically start. This service is used to send email messages from RapidResponse. For more information, see "Configuring email support" on page 276.
- **RapidResponse Server Monitor**—Monitors the status of the RapidResponse Server service. If the RapidResponse Server service stops unexpectedly or crashes, this service saves debugging information for analysis by Kinaxis Customer Support to help diagnose the problem. After the installation of RapidResponse Server, this service is set to automatically start. Stopping and restarting this service does not stop the RapidResponse Server service. For more information, see "Internal errors and system crashes" on page 244.

All four services should always be started when the entire RapidResponse system is running.

Caution: If you change the user account the RapidResponse Service Host runs under or change the password for the RapidResponseService user account, alerts, scheduled tasks, and automation chains no longer function. If these settings have been changed, you can reset the RapidResponse Service Host settings as described in "Resetting the RapidResponse Service Host" on page 234.

Notes:

- If you publish data to other companies using RapidResponse, you will also have the RapidResponse Data Transfer Client service. If you use RapidResponse Connection Services, you will have RapidResponse Event Manager and RapidResponse Task Manager services on the computers on which they are installed.
- If your company has deployed the optional RapidResponse failover cluster configuration, the RapidResponse services are available on both instances of RapidResponse Server. For more information, see "RapidResponse Server failover clustering" on page 289.



Starting and stopping RapidResponse services

RapidResponse runs as Microsoft Windows services and the main service is RapidResponse Server. This section describes how to start and stop RapidResponse services.

Starting RapidResponse services

In order to work with any of the tools in RapidResponse, RapidResponse Server must be started.

To start RapidResponse Server, you must use the computer where RapidResponse Server is installed, or access the computer using Microsoft Windows Remote Desktop Connection.

When the RapidResponse Server service starts it executes multiple internal steps concurrently. This can lead to significant system memory consumption. In some cases the amount of system memory required to start the RapidResponse Server service is double the standard system memory consumption level.

▸To start the RapidResponse Server service

1. Log on as an administrator to the computer where RapidResponse Server is installed.
2. From the Microsoft Windows **Start** menu, point to **All Programs**, **RapidResponse**, and then click **Start RapidResponse Server**.

Notes:

- You can manually start the RapidResponse Server service through the Microsoft Windows Services dialog box. However, this is not a recommended method as you might receive a time-out error with larger data sets even though RapidResponse Server continues to load the database. For more information, see "The Windows Services dialog box" on page 232.
- You can use the Microsoft Windows Services dialog box to automatically start the RapidResponse Server service when the computer starts. For more information, see "Configuring the RapidResponse Server service" on page 233.
- Starting of the RapidResponse Service service is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

▸To start other RapidResponse services

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Click the service name. For example, **RapidResponse Service Host**.
3. On the **General** menu, click **Start**.

Tip: You can use the Microsoft Windows Services dialog box to have the RapidResponse services automatically start when the computer where RapidResponse Server is installed is started.

Stopping RapidResponse services

You can stop and then restart RapidResponse Server with the data and scenarios that existed prior to the last stoppage. Before you stop RapidResponse Server, you should let users know that RapidResponse will be temporarily unavailable. For more information, see "Communicating with users" on page 593.

The web-based RapidResponse Console is a multipurpose administration tool available to RapidResponse system administrator to assist in the management and monitoring of the RapidResponse system. It is also used to stop the RapidResponse Server service and it can also be used to restart the RapidResponse service.

You can also stop and restart the RapidResponse Server service with the Windows Services dialog box but there are some drawbacks as explained in "The Windows Services dialog box" on page 232.

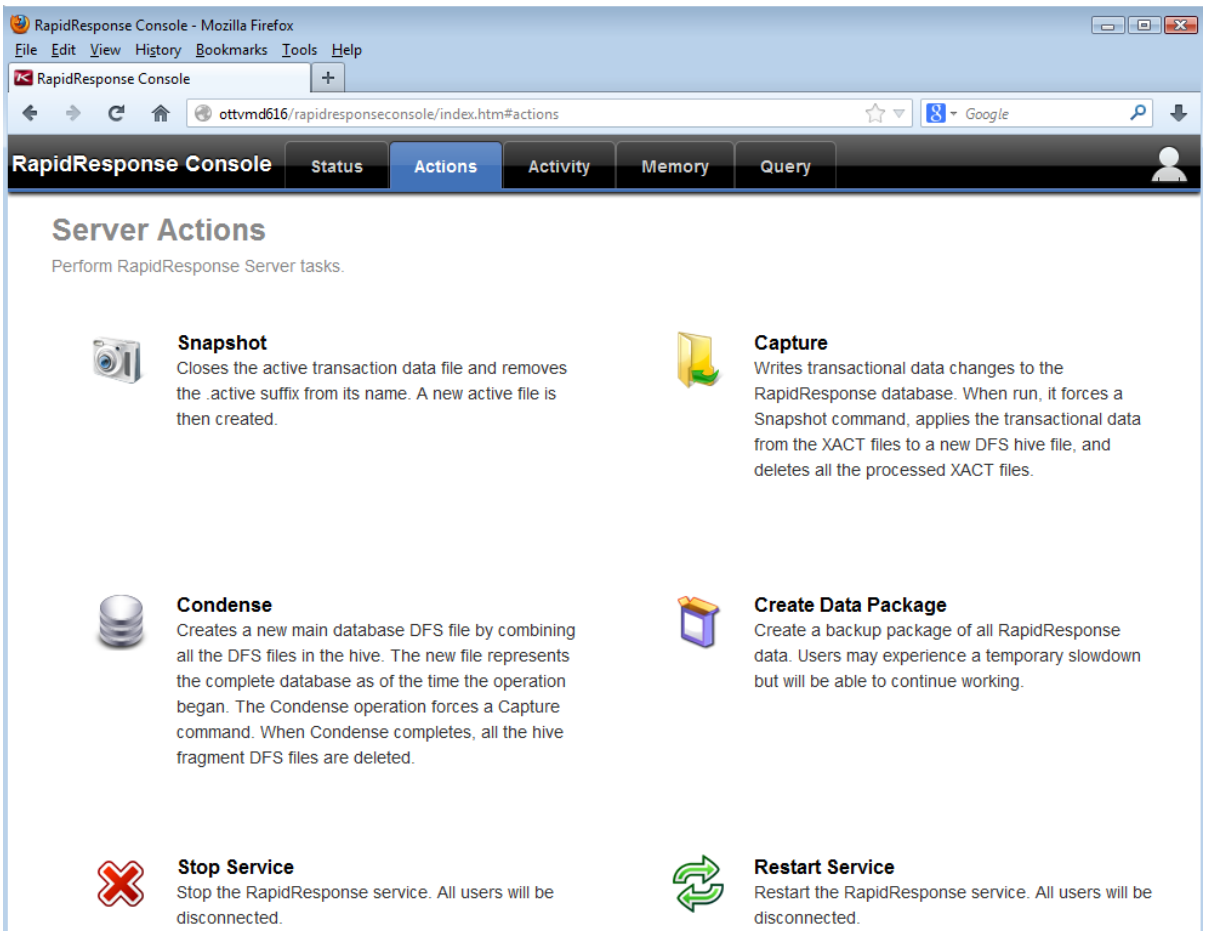
▸To sign in to RapidResponse Console

1. Open a Web browser.
2. Type the **RapidResponse Console** URL into the Address box of the browser.

   The URL for signing in to RapidResponse Console is established during the installation. It is **Server Name/rapidresponseconsole**. For example, if your RapidResponse Server server is named server99, the URL is **http://server99/rapidresponseconsole** or **https://server99/rapidresponseconsole**.
3. On the **RapidResponse Sign In** page, do the following:
   - In the **User ID** box, type your system administrator user ID.
   - In the **Password** box, type your user password. The password is case sensitive.
   - Click **Sign In**.

Notes:

- The RapidResponse Console can be started using HTTP or HTTPS for encrypted communication. This is dependent on how your RapidResponse system is configured. For more information, see "RapidResponse Console security settings" on page 237.
- If you are using Microsoft Internet Explorer 11, you might be disconnected after 15 minutes of inactivity, but not notified that your console session has timed out. In this case, you should reconnect or use another browser.



▸To stop the RapidResponse Server service

1. Sign into RapidResponse Console. For more information, see "To sign in to RapidResponse Console" on page 230.
2. Click the **Actions** menu.
3. Click **Stop Service**.

Notes:

- Stopping of the RapidResponse Server service is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.
- If the RapidResponse Server service is stopped using this procedure, you cannot use the Console to restart the service. Instead, use the Windows **Start** menu. For more information, see "Starting RapidResponse services" on page 229.
- Calculated results, which are stored in-memory, are not maintained when RapidResponse Server is stopped.

▸To stop and restart the RapidResponse Server service in one step

1. Sign into RapidResponse Console. For more information, see "To sign in to RapidResponse Console" on page 230.

2. Click the **Actions** menu.
3. Click **Restart Service**.

Notes:

- Performing a restart signs out all RapidResponse users. When RapidResponse Server is restarted the Capture command is run. This command writes all transactional data to the RapidResponse database. For more information, see "DFS folders" on page 312.
- You can also schedule restarts of the RapidResponse Server with a system scheduled task and the Restart command. For more information, see "RapidResponse system commands" on page 384.
- Restarting RapidResponse from this command does not apply data model changes. For more information about applying data model changes with a restart, see following procedure.

▸To restart the RapidResponse Server service and apply data model changes

1. Sign into the Java client.
2. In the **Administration** pane, under **Data Integration**, click **Integration Utilities**.
3. Select **Apply data model changes**.
4. Click **Restart** and click **Yes** to confirm.

▸To stop other RapidResponse Server services

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Select a RapidResponse service (other than **RapidResponse Server**).
3. On the **General** menu, click **Stop**.

The Windows Services dialog box

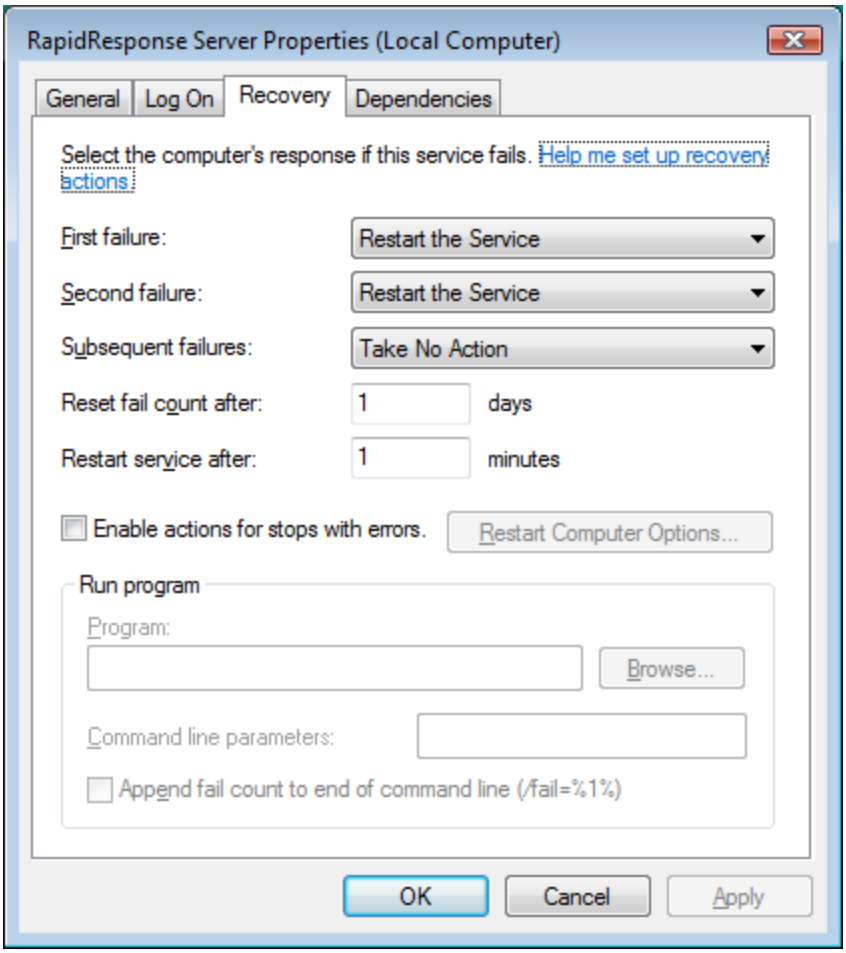
You can also stop and start the RapidResponse Server service using the Microsoft Windows Services dialog box. However, it is not recommended you use this method. Instead, use the RapidResponse Console as described in "Starting and stopping RapidResponse services" on page 228.

Using the Windows Services dialog box can result in an operational issue. When starting RapidResponse, the Windows Services dialog box might return a timeout error with larger data sets. RapidResponse Server, however, continues to load the database and it is ambiguous whether the start operation actually completes.

Tip: You can use the Microsoft Windows Services dialog box to have the RapidResponse Server service automatically start when the computer where RapidResponse Server is installed is started.

Configuring the RapidResponse Server service

Windows services can be set to automatically restart if they unexpectedly stop or fail. The recommended best practice for the RapidResponse Server service is to have it set to restart if it unexpectedly stops or crashes. These settings are available from the Recovery tab in the Windows Services dialog box.



General tab

- **Startup Type**—Automatic

Recovery tab

- **First Failure**—Restart the Service
- **Second Failure**—Restart the Service
- **Subsequent Failure**—Take No Action
- **Reset fail count after**—1 days
- **Restart service after**—1 minutes

▸To open the Windows Services dialog box Recovery tab

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Click **RapidResponse Server**.
3. Click the **Recovery tab.**

If the best practices are followed, RapidResponse Server attempts to restart automatically following a one-minute delay, up to two times in a 24-hour period. If it shuts down a third time within this time period, RapidResponse Server does not automatically restart. If this occurs it is recommended that you investigate the problem before restarting RapidResponse Server.

If the RapidResponse Server service is not stopped normally (that is, a Stop command is not issued), then a Warning message is written to the **Server.log** file. For more information about the log file, see " Server.log file" on page 464.

Upon restart, RapidResponse creates a new version of the **Server.log** file.

Configuring RapidResponse Service Host

RapidResponse administrators can configure and customize the RapidResponse Service Host service settings.

Resetting the RapidResponse Service Host

The RapidResponse Service Host service, by default, runs using the RapidResponseService user account. If the properties of either are modified then alerts, scheduled tasks, business process notifications, and responsibility calculations might not function. If alerts stop functioning or responsibility stops calculating, the likely cause is a change to either the RapidResponse Service Host settings or the RapidResponseService user account. These problems can be corrected by resetting the RapidResponse Service Host settings.

You can use a different user account in place of the RapidResponseService account, however, you must configure this user account with the same permissions required by the RapidResponseService account. For more information, see "To grant permissions to the RapidResponseService user" on page 673.

All procedures assume the RapidResponseService account is used.

▸To reset the RapidResponse Service Host

1. Open a Windows Command Prompt window.
2. Navigate to the **C:\RapidResponse\Program\ServiceHost** folder.
3. Type the following command:
   `servicehostinstaller.exe reset`
4. Press **Enter**.

The RapidResponse Service Host is reinstalled with its default settings, and the RapidResponseService user account is re-created with an automatically-generated password. If you are using a different user account, you must specify that user in the Windows Services configuration.

Changing the number of processor threads used by Service Host

The RapidResponse Service Host service executes the queries for each automation task it runs using multi-threaded execution. This allows the scheduled automation tasks to execute queries using as many threads as required. This also balances the thread usage between all automation tasks in the queue and automation tasks run by users, allowing both types of automation tasks to run simultaneously.

You can specify the number of CPU threads dedicated to RapidResponse Service Host service using the ServiceHost_ThreadCount processing rule. The number of threads used by Service Host is automatically set to the number of CPUs present in the computer where RapidResponse is installed. However, if you want to dedicate threads to executing the users' interactive queries, you should change this setting. Typically, you should adjust this value if you find users' tasks are taking longer than expected to complete.

The ServiceHost_ThreadCount setting cannot be increased above the number of processors. It is recommended to set this to a quarter of the number of CPU cores available, and then you can increase or decrease the value depending on your task performance.

▸To change the number of processor threads

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **ID** box, type **ServiceHost_ThreadCount**.
   - In the **Value** box, type a number less then the number of processors in the computer.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.

Note: To reset the number of threads, delete the ServiceHost_ThreadCount setting.

RapidResponse Console

The web-based RapidResponse Console is a multipurpose administration tool available to RapidResponse system administrators to assist in the management and monitoring of the RapidResponse system. The RapidResponse Console is also used to stop the RapidResponse Server service and to restart the RapidResponse service.

For information about starting RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

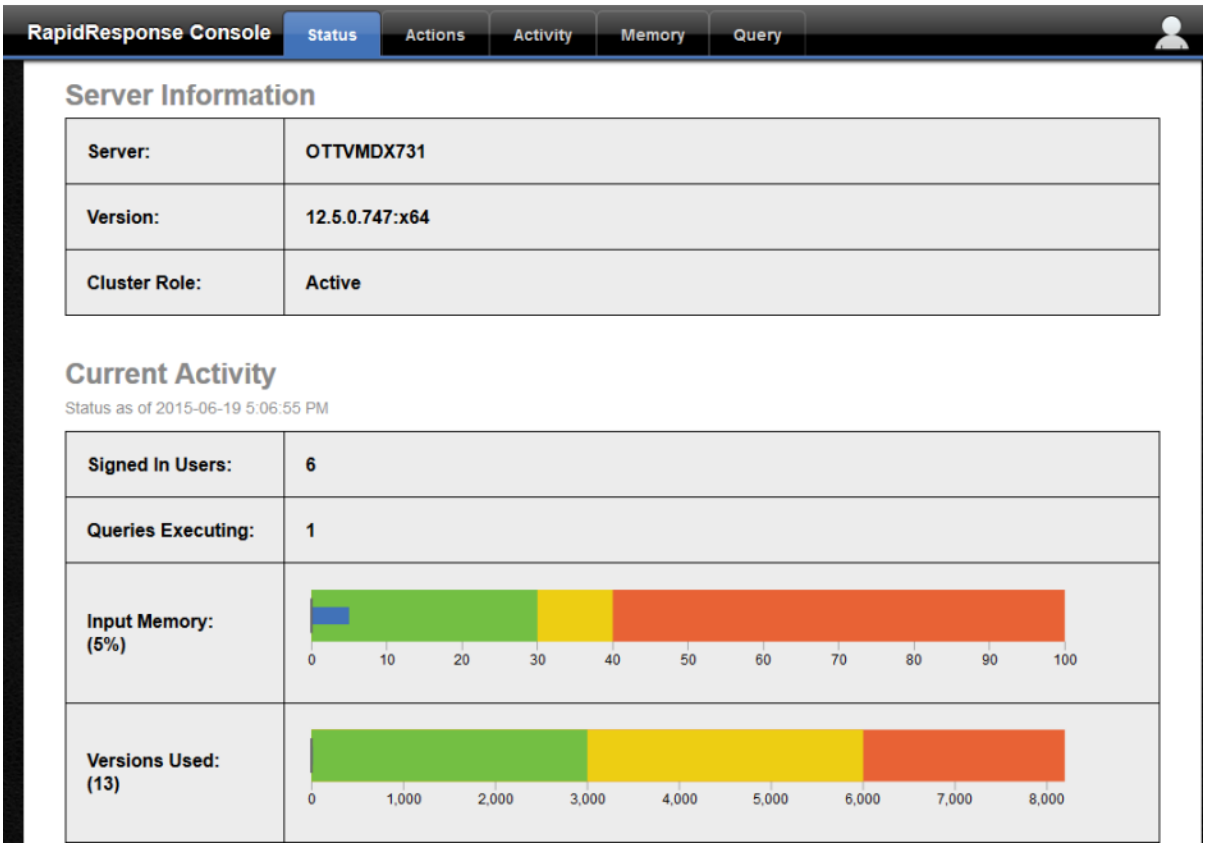
For information about security settings, see "RapidResponse Console security settings" on page 237.

The RapidResponse Console includes the following pages:

- "Status page" on page 236
- "Actions page" on page 236
- "Activity page" on page 237
- "Memory page" on page 237
- "Query page" on page 237

Status page

The Status page provides a quick view of the number of users currently signed in to RapidResponse, the number of queries executing, the amount of memory being consumed by input data, and the number of scenarios in use. The Status page also shows the status of the RapidResponse Server and, if failover clustering has been enabled, whether the RapidResponse Server you are signed in to is in active or standby mode. For more information, see "Determine Server status using RapidResponse Console" on page 301.



Actions page

The Actions page allows you to perform the following actions:

- Run the Snapshot command. For more information, see "Snapshot command" on page 409.
- Run the Condense command. For more information, see "Condense command" on page 387.
- Run the Capture command. For more information, see "Capture command" on page 385.
- Create a data package. For more information, see "Backing up and restoring the RapidResponse database" on page 315.

- Stop or restart the RapidResponse service. For more information, see "Starting and stopping RapidResponse services" on page 228.

Activity page

The Activity page provides detailed information about active RapidResponse tasks and the progress of executing commands. For more information, see "Reviewing RapidResponse Server activity" on page 239.

Memory page

The memory page provides detailed information about the amount of system memory RapidResponse is consuming. For more information, see "System memory details in RapidResponse Console" on page 261.

Query page

The Query page can be used to run queries against the RapidResponse database. For more information, see "Manually running queries against the database" on page 244. For information about queries, see "Query monitoring and management tools" on page 267.

For more information about monitoring active queries using RapidResponse Console, see "System memory details in RapidResponse Console" on page 261. To quickly check the number queries that are executing, view the Status page of the RapidResponse Console.

RapidResponse Console security settings

The URL for signing in to the RapidResponse Console is established during the installation of RapidResponse. It is **Server Name/rapidresponseconsole**. For example, if your RapidResponse Server computer is named **server99**, the default URL is **http://server99/rapidresponseconsole**.

The RapidResponse Console also supports secured communication using HTTPS. By switching to HTTPS, you can secure the connection between the RapidResponse Console (in a browser) and RapidResponse Server by encrypting all communication.

To use HTTPS, you must install a SSL certificate from a trusted authority to secure communication between the RapidResponse Console and RapidResponse Server. For more information about certificates and the RapidResponse system, see "Securing communication with certificates" on page 126.

The computer where RapidResponse is installed must have the inbound TCP port 443 open for HTTPS connectivity between the RapidResponse Console and RapidResponse Server.

To set RapidResponse Console communications to use HTTPS, the **HttpsRapidResponseConsole** Windows registry setting must be set to 1 (DWORD). This key is stored at **HKLM\SOFTWARE\webPLAN Inc.\webPLAN**. For more information about RapidResponse Windows registry settings, see "Registry Settings for RapidResponse Server" on page 351.

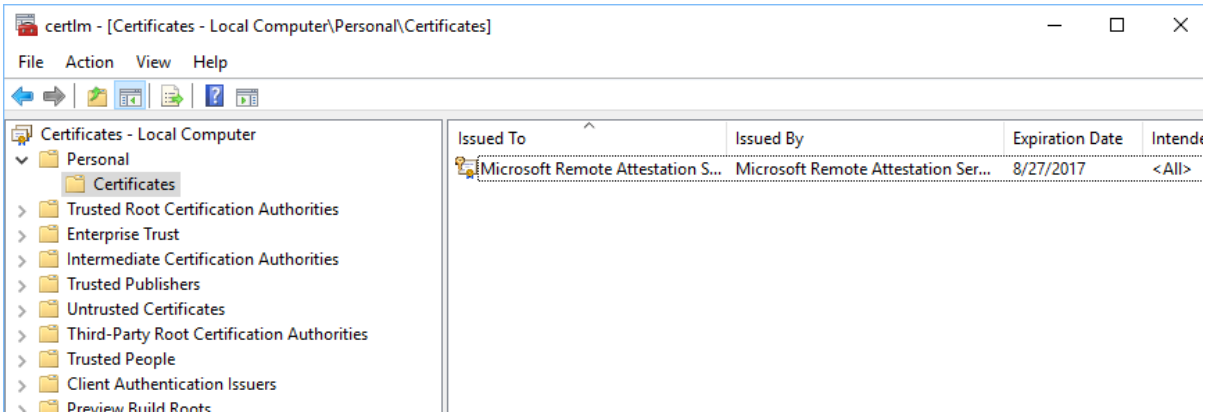
Once the RapidResponse Console is set to use HTTPS, requests to use HTTP are not returned and eventually timeout. If the RapidResponse Server computer is using IIS, you can set up forwarding so that HTTP requests are redirected to the HTTPS endpoint.

> **Note:** Security warnings are returned if the RapidResponse Console is configured to use HTTPS but the SSL certificate is not installed or installed incorrectly.

Certificates when not using IIS

The RapidResponse Console does not require that IIS (Internet Information Services) on the computer where RapidResponse Server is installed. If you are not using IIS on the computer where RapidResponse Server (and RapidResponse Console) is installed, you must manually bind the SSL certificate to port 443.

The first step is to import the certificate. You can use the Windows Certificate Manager (**certlm.msc**) to do this. From the **Action** menu, click **All Tasks** and then click **Import**. Consider storing the certificate in the **Local Computer\Personal\Certificates** folder in the Certificate Manager. However, your own system settings might require you to use a different folder.



The next step is to bind the SSL certificate to port 443. To do so, run a **netsh** command from the Windows command prompt. Here is an example:

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={B43904DF-7378-4805-
B495-EDEE9AA519E4}
```

Where:

- **ipport** specifies the port number.
- **certhash** specifies the certificate's thumbprint. For information about retrieving a certificate's thumbprint, visit the Microsoft Developer Network at https://msdn.microsoft.com/en-us/library/ms734695(v=vs.110).aspx.
- **appid** is a GUID that identifies the owning application. In the case of RapidResponse Console, use B43904DF-7378-4805-B495-EDEE9AA519E4 as the **appid.**

For more information about the **netsh** command, visit the Microsoft Developer Network at https://msdn.microsoft.com/en-us/library/ms733791(v=vs.110).aspx.

Authenticating RapidResponse Server

All communications between RapidResponse Server and the RapidResponse Application Server are authenticated using the Application Server's unique identifier and public key encryption. If you have installed multiple instances of RapidResponse Application Server, each instance has its own client identifier and public key, both of which are used to authenticate the requests from that instance. Any request that does not include the correct client and key is rejected.

If necessary, as the Master Administrator, you can remove or update the public keys associated with any of your RapidResponse Application Server instances. You can manage keys for the server connection using the public key infrastructure configuration program. This utility, PKIConfig.exe, allows you to register and update keys for the server connection.

To update a public key for the Application Server

1. On the computer where RapidResponse Application Server is installed, open a Command Prompt window.
2. Navigate to the **Program Files\Kinaxis\RapidResponse\PKIConfig** folder.
3. Run the **PKIConfig.exe** file with the following parameters:

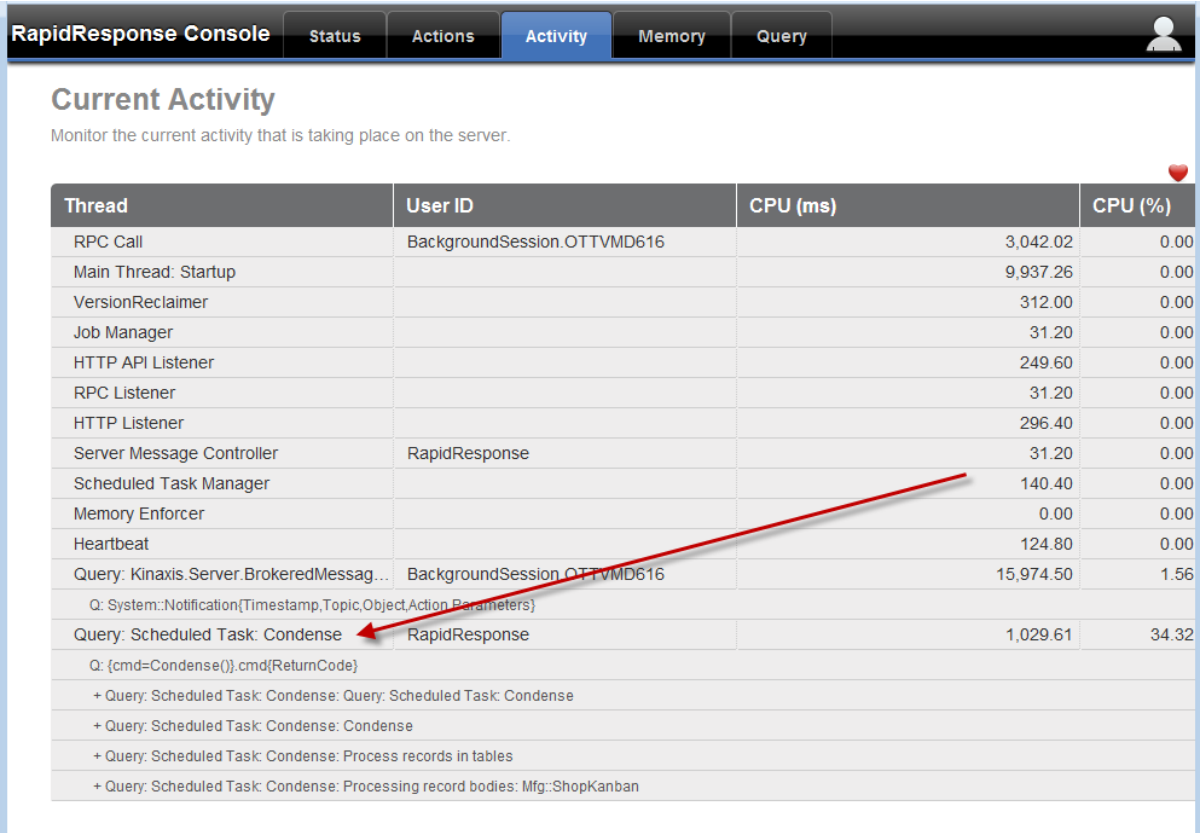
   ```
   PKIConfig.exe -server=ServerName -pwd=AdminPassword -
   registerClient="ApplicationServerClient"
   ```

   where `ServerName` is the computer RapidResponse Server is installed on, `AdminPassword` is the Master Administrator password, and `ApplicationServerClient` is a constant that automatically identifies the Application Server you are authenticating.

Communication between RapidResponse Server and RapidResponse Service Host are also authenticated using keys. However, to re-authenticate a Service Host instance, you must reinstall the Service Host. For more information, see "Installing RapidResponse Server" on page 109.

Reviewing RapidResponse Server activity

The **Activity** page in the RapidResponse Console provides detailed information about active RapidResponse tasks and the progress of executing commands. For example, the Condense command progress is shown in the following illustration.

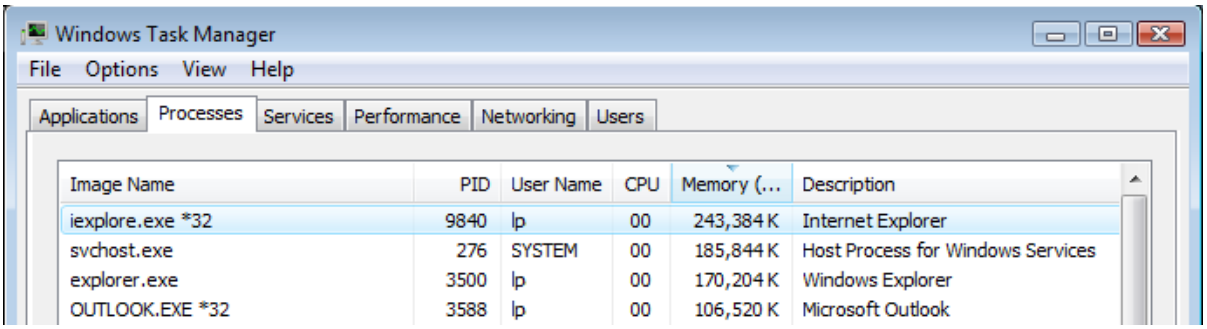


To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

Column	Description
Thread	One of the following: • An active RapidResponse Server internal thread • An executing RapidResponse command • An executing query indicating the active resource (for example, worksheet name).
User ID	The ID of the user who initiated the task. **RapidResponse** indicates the system initiated the task (including Scheduled System Tasks even if run on demand) and blank indicates an active RapidResponse Server internal thread.
CPU	Cumulative CPU usage in seconds.
CPU (%)	Represents the percentage of time the thread was used of a CPU in the past second. It is calculated by reading the CPU time for each thread, waiting one second, and then reading the CPU time again. The difference is expressed as the CPU (%) This can be used to better understand which threads are consuming CPU and which are idle.

Note: The beating heart icon above the CPU (%) column indicates that RapidResponse is active.

The **Activity** page can be considered similar to the Processes tab in the Windows Task Manager.



Troubleshooting RapidResponse Server

RapidResponse system administrators are responsible for maintaining the system for their users. At some point they might be tasked with resolving RapidResponse Server stability issues.

As a RapidResponse system administrator, you might be faced with a situation where RapidResponse stops unexpectedly (also known as a crash) or becomes unresponsive (hangs).

If RapidResponse stops due to hardware issues, you should first consult your company's internal support team before engaging Kinaxis Customer Support.

If RapidResponse stops unexpectedly due to software issues (operating system or RapidResponse system), you might be able to resolve the issue by reviewing the RapidResponse log files, in particular, the **Server.log** file. For more information, see "Reviewing system status and operation logs" on page 421.

If RapidResponse becomes unresponsive (or seems unresponsive), review the **Activity** page in the RapidResponse Console to better understand the status of active RapidResponse tasks and the progress of executing commands. To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

If you cannot diagnose and resolve the issue or if the RapidResponse system repeatedly stops unexpectedly, then you might need the assistance of Kinaxis Customer Support. To properly and efficiently diagnose issues, Kinaxis Customer Support representatives require as much information as possible. RapidResponse includes tools that make it easy to generate system information, and data and log file packages for Kinaxis representatives. They can use these packages to properly and efficiently diagnose system issues.

Manually generating log file packages

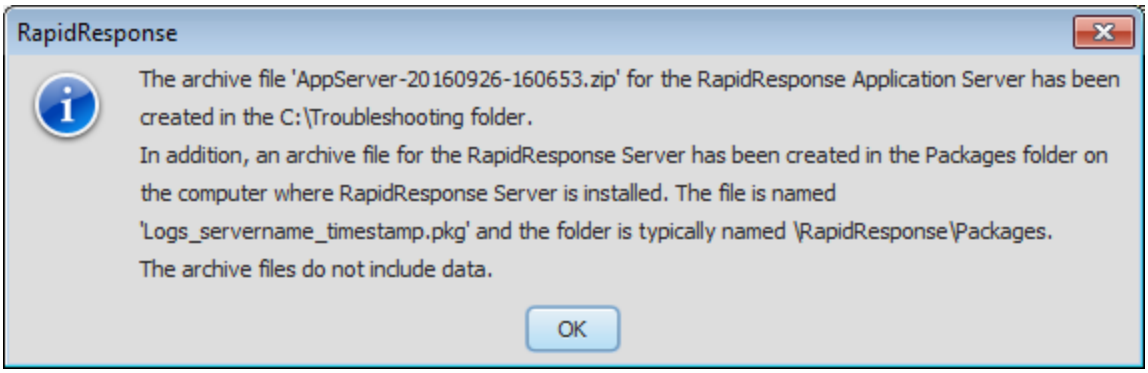
It is likely Kinaxis Customer Support representatives will request log file packages when diagnosing RapidResponse system issues. This is especially true for system stability issues. RapidResponse includes a system utility that generates exactly the information Customer Support representatives require from RapidResponse Server and RapidResponse Application Server. This section explains how to generate the required information.

▸**To manually generate log file packages**

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. In the **System information archive** section, choose a time period that includes the RapidResponse Application Server log files you want to save.
3. Click **Save Archives**.
4. In the **Save Archives** dialog box, specify the location to save the file.
5. In the **File name** box, type a name for the file.

   A time stamp will be automatically appended to the file name you select.
6. A confirmation dialog is displayed that indicates the location where the log file packages for RapidResponse Server and RapidResponse Application Server are saved.

   The RapidResponse Server log package is saved in the **C:\RapidResponse\Packages** folder on the computer where RapidResponse Server is installed and is named **Logs_*servername*_*timestamp*.pkg** or **Logs_servername_*timestamp*.zip**. For example:



Notes:

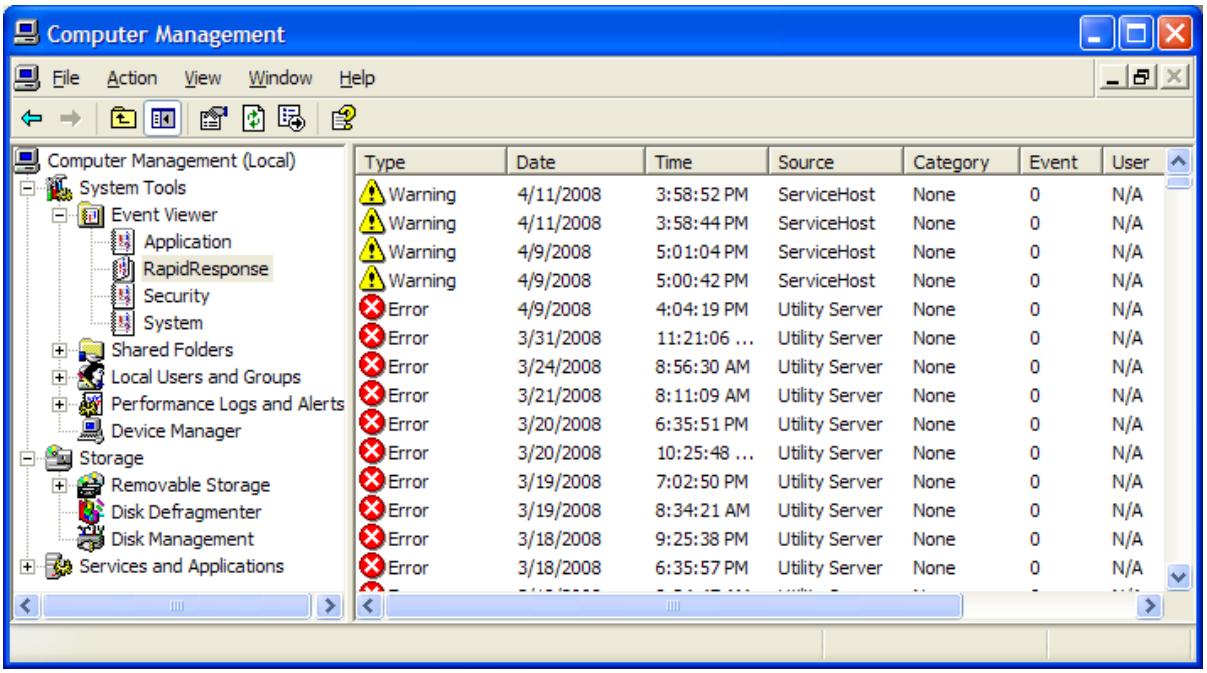
- The log file packages are saved in the compressed format. The RapidResponse Application Server log file package uses the .ZIP extension and the RapidResponse Server log file package uses the .PKG extension.
- For information about decompressing RapidResponse packages (.PKG files), see "Decompressing packages and Packages folder" on page 251.

Information saved in the log file packages

The RapidResponse Server log file package stores every log file in the **C:\RapidResponse\Logs** folder from the computer where RapidResponse Server is installed. The RapidResponse Application Server log file package stores every log file in the **C:\Program Files\Kinaxis\RapidResponse\Logs** folder from the computer where RapidResponse Application Server is installed.

Both packages include a file named **SystemInfo.txt** that includes hardware information (computer name, CPUs, RAM, and available disk space) and software information (operating system and RapidResponse versions).

In addition, the log file packages include exported information available in the Windows Event Log Service for the Application, System, and RapidResponse categories. The Windows Event Log Service records significant system changes, program errors, and user notifications. The Event Logs can be viewed in the Windows Computer Management dialog box. For more information about Event Logs, refer to the *Microsoft Windows Help*. The following image shows the Windows Computer Management dialog box.



Creating the Application Server log file package using a command line

If the RapidResponse client is not available, you can still create a RapidResponse Application Server log file package using a command line executable.

▸To create the log file package using a command line

1. Open a Windows Command window on the computer where RapidResponse Application Server is installed.
2. Change the path to **C:\Program Files\Kinaxis\RapidResponse\CollectArchives**.
3. Type the following command: `CollectArchives.exe` *`folder_filename`*

   where *`folder_filename`* is the folder and filename of the log package.

   For example: `CollectArchives.exe C:\KinaxisSupport\logs.zip`
4. Type ENTER.
5. A confirmation dialog box is displayed indicating where the log package was stored.

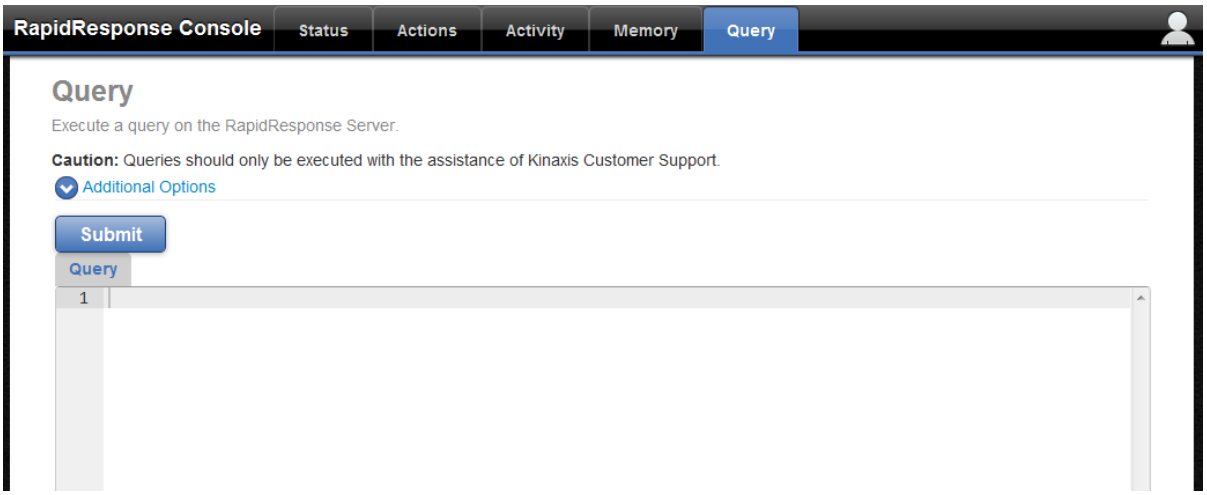
Notes:

- If the *`folder_filename`* parameter is not specified, the log package is saved in the **C:\Program Files\Kinaxis\RapidResponse\SavedArchives** folder.
- Unlike the RapidResponse utility, you cannot control the log file dates using the command line.
- A time stamp is appended to the log package filename.

Manually running queries against the database

The **Query** page in the RapidResponse Console can be used to run queries against the RapidResponse database. This should only be done in troubleshooting situations with the assistance of Kinaxis Customer Support. To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

> **Caution:** Running queries that modify data can potentially corrupt your RapidResponse database. Only do so with the assistance of Kinaxis Customer Support.



Internal errors and system crashes

The RapidResponse Server Monitor service monitors the status of the RapidResponse Server service. After the installation of RapidResponse Server, the RapidResponse Server Monitor service is set to automatically start. For more information about RapidResponse services, see "RapidResponse Windows Services" on page 227.

When an internal error (also called a “handled exception error”) is generated by RapidResponse Server, it attempts to maintain service performance without crashing.

After an internal error is generated, RapidResponse Server Monitor sends a message to the RapidResponse Master Administrator (Admin user) alerting them of potential server stability issues. The message includes an attachment named **exception.xml** that can be used by Kinaxis Customer Support to help diagnose the issue.

RapidResponse Server Monitor also generates a series of diagnostic files when an internal error occurs. These files can also be used by Kinaxis Customer Support to help diagnose the issue.

Like an internal error, a crash of the RapidResponse Server results in Server Monitor sending a message to the RapidResponse Master Administrator (Admin user) which alerts them of the unexpected shutdown. Diagnostic files are also generated.

Diagnostic files

RapidResponse Server Monitor creates diagnostic files after RapidResponse Server generates an internal error or crashes. The diagnostic files are created before the RapidResponse Server service resumes operating in the case of an internal error or restarts in the case of a crash. Through Windows registry settings, system administrators can customize the type of diagnostic files created by RapidResponse Server Monitor.

The following section describes the diagnostic files that might be created.

Automated Server-incident Analysis (ASA) file

An Automated Server-incident Analysis (ASA) files includes stack traces, threads, and other debugging information. This text file uses the naming convention ***timestamp.serverName.*****asa.txt**.

Small dump file

The small dump file contains system information such as call stacks and registers. Small dump files are named ***timestamp.serverName.*****small.txt**.

Limited dump file

The limited dump file contains the same information as the small dump file along with data from the RapidResponse database. These files are usually about 100 MB in size. Limited dump files are named ***timestamp.serverName*****.limited.txt**.

The limited dump file process includes an internal time window, based on your data volumes, which ensures the dump file is written and RapidResponse does not remain inaccessible for an excessive period of time. The writing process ends when the time window expires, and the limited dump file might contain a partial record of the issues.

Full dump file

The full dump file contains more detailed information than the limited dump file. This dump file is generally about the same size as the **RapidResponse.exe** process as displayed in the Windows Task Manager and includes all the data in the RapidResponse database. Full dump files are named ***timestamp.serverName*****.full.txt**.

Registry dump file

The registry dump file contains information about the registry settings applied to RapidResponse Server and RapidResponse Server Monitor. This file is produced only after a RapidResponse Server crash. Registry dump files are named ***timestamp.serverName*****.regdump.txt**

Complete diagnostics package file

The diagnostics package files created by the RapidResponse Server Monitor contains detailed system information. This file uses the following naming convention:

diagnostics.*serverName.timestamp*.pkg or **diagnostics.*serverName.timestamp*.zip**

The complete diagnostics package files include the following:

- Two Automated Server-incident Analysis (ASA) files.
- A small dump file.
- A registry dump file, if applicable.
- The largest available dump file created by the RapidResponse Server Monitor service for this incident.
- The entire contents of the **C:\RapidResponse\Logs** folder.

Optionally, the diagnostics package files can also include the entire contents of the **C:\RapidResponse\Data** folder (excluding any PKG files). You can modify this setting using the **PkgIncludeDataDirectory** Windows registry setting. By default this option is enabled. For more information, see "PkgIncludeDataDirectory" on page 364. The **\Data** folder is not included if the RapidResponse system is using the optional failover cluster configuration. For more information, see "RapidResponse Server failover clustering" on page 289.

Note: Due to its size, including the contents of the **C:\RapidResponse\Data** folder might result in significant time elapsing before RapidResponse Server restarts after a crash.

Diagnostic file storage

By default, dump files are stored in the **Dumps** folder which is a sibling to the **C:\RapidResponse\Data** folder (default installation). As an administrator, you should periodically review this folder and delete old dump files. The default location of the Dumps folder can be changed using the **DumpDirectory** Windows registry setting. For more information, see "DumpDirectory" on page 363

By default, the diagnostics package files are stored in the **C:\RapidResponse\Packages** folder. This is the same location where RapidResponse data package files are stored. Packages are used to back up the RapidResponse database.

Only two diagnostics package files are stored. After a new version is created, the oldest diagnostic package is deleted. Because of this, once a file is no longer needed in this location (for example, it has been sent to Kinaxis Customer Support), you should delete it.

The default storage location of the diagnostic package files can be customized so that they are not stored in the same location as the packages used to back up the RapidResponse database. To do so, use the **PkgDirectory** Windows registry setting. For more information, see "PkgDirectory" on page 364.

By having these folders on different drives you can speed up the operation that are performed within them and more quickly return RapidResponse Server to a running state.

Customizing diagnostic file generation

RapidResponse Server Monitor writes diagnostic files after the RapidResponse Server service generates an internal error or crashes. While writing the files, RapidResponse is not available to users.

While the RapidResponse Server Monitor is creating the diagnostic files, which might take minutes or up to an hour depending on the size of the data and the speed of the computer hardware, it writes messages to the **RRMonitor.log** file. The messages indicate the projected size of the dump file and the current size of the file. Here is an example:

```
2013-01-09 22:14:51 INFO null - RapidResponse: Projected dump file size is:
503 MB. Dump file size so far: 59 MB.
```

```
2013-01-09 22:15:52 INFO null - RapidResponse: Projected dump file size is:
503 MB. Dump file size so far: 191 MB.
```

```
2013-01-09 22:16:53 INFO null - RapidResponse: Projected dump file size is:
503 MB. Dump file size so far: 390 MB.
```

Do not manually stop or restart RapidResponse Server until the **RRMonitor.log** file indicates the diagnostic files are complete. RapidResponse Server will usually restart automatically based on the Windows Services settings.

Note: Due to memory issues, RapidResponse Server might become unresponsive when creating limited or full dump files. If this is the case, RapidResponse Server Monitor terminates writing the dump file and the Automated Server-incident Analysis file (***timestamp*_asa.txt**.). However, the small dump file is still created. The termination is controlled by a time threshold which is controlled by a Windows registry setting named **TimeLimit**. By default, it is set to 300 seconds. For more information, see "TimeLimit" on page 365.

As a system administrator, you can control the diagnostic files created by RapidResponse Service Monitor to limit downtime to RapidResponse users.

By default, RapidResponse Service Monitor will do the following, in order, after an internal error is generated or a crash:

1. Create the **exception.xml** file and send it RapidResponse Master Administrator (Admin user).
2. Create the Automated Server-incident Analysis (ASA) file.
3. Create a small dump file.
4. Optionally, create a limited or full dump file.
5. Create a second copy of the Automated Server-incident Analysis (ASA) file.
6. Optionally, create a full dump file.
7. Create a complete diagnostics package file.

System administrators can modify what happens in the fourth and sixth steps through the use of Windows registry settings. The following registry settings are used to create diagnostic files.

Registry setting	Description	Default
LimitedDumpOnFirstChance	Controls whether a limited dump file is created after an internal error.	0 (off)
LimitedDumpOnFirstChanceAnaltyics	Controls whether a limited dump file is created after an internal error during the execution of analytic calculations.	1 (on)
FullDumpOnFirstChance	Controls whether a full dump file is created after an internal error.	0 (off)
LimitedDumpOnSecondChance	Controls whether a limited dump file is created after a RapidResponse Server crash.	0 (off)
FullDumpOnSecondChance	Controls whether a full dump file is created after a RapidResponse Server crash.	0 (off)

For more information about Windows registry settings, see "Registry Settings for RapidResponse Server" on page 351.

Consider making changes to these Windows registry settings in conjunction with Kinaxis Customer Support. Here are some use cases to consider:

- If Kinaxis Customer Support cannot fully diagnose an internal error they might recommend that you create a full dump on the next error (FullDumpOnFirstChance=1).
- If Kinaxis Customer Support cannot fully diagnose a crash they might recommend that you create a full dump on the next crash (FullDumpOnSecondChance=1).
- If your company is restricted from including your business data in files you send to Kinaxis Customer Support, set all the registry settings to 0.
- If your RapidResponse system is generating many internal errors that impact RapidResponse Server uptime, do not create a limited dump file (LimitedDumpOnFirstChance=0). If you change this setting ensure you create a limited dump(LimitedDumpOnSecondChance=1) or a full dump (FullDumpOnSecondChance=1) if the system crashes.

Customizing the contents of dump files

The limited and full dump files expose your RapidResponse business data to Kinaxis Customer Support. By creating or modifying the **NoTraversal** Windows registry setting, you can specify that the limited and full dump files not include your business data. By default this option is not enabled. For more information, see "NoTraversal" on page 364.

Excluding business data from dump files makes it more difficult to diagnose system issues.

Manually generating diagnostic files

Instead of stopping unexpectedly or crashing, the RapidResponse Server service might become unresponsive (also known as a hung or deadlocked state). In this case, you might need to generate diagnostic system information for use by Kinaxis Customer Support.

Manually generating the diagnostic files, in some cases, can take a significant amount time. During the writing of dump files the RapidResponse system is not available to users. However, generating the Automated Server-incident Analysis (ASA) file allows users to maintain their RapidResponse sessions.

▸To manually generate a complete diagnostics package file

1. From the Microsoft Windows **Start** menu, point to **All Programs, RapidResponse**, **Write Debugging Information**, and then click **Complete Diagnostics Archive**.
2. Click **Yes**.

Notes:

- The diagnostics package file includes a full dump file and a small dump file.
- Writing the Complete Diagnostics Archive might take one to two hours to complete depending on the current RapidResponse process size. During the file creation the RapidResponse system is not available to users.

▸To manually generate a limited dump file

1. From the Microsoft Windows **Start** menu, point to **All Programs, RapidResponse**, **Write Debugging Information**, and then click **Limited Dump File**.
2. Click **Yes**.

Notes:

- This command also creates a small dump file and a Automated Server-incident Analysis (ASA) file.
- Writing the Limited Dump File usually takes one to three minutes to complete. During the file creation the RapidResponse system is not available to users.

▸To manually generate a small dump file

1. From the Microsoft Windows **Start** menu, point to **All Programs, RapidResponse**, **Write Debugging Information**, and then click **Small Dump File**.
2. Click **Yes**.

Notes:

- Writing a small dump file is a very quick process (small number of seconds and usually less than 10 seconds). As such, it can be used repeatedly if requested by support.
- During the file creation the RapidResponse system is not available to users.
- This command also creates a Automated Server-incident Analysis (ASA) file.

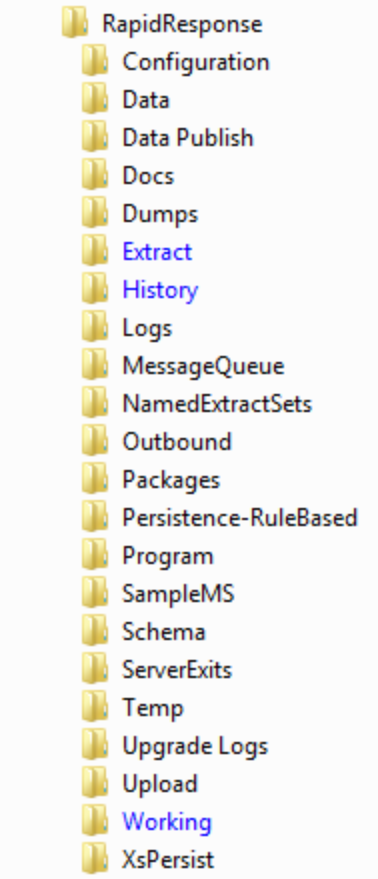
▸To manually generate an Automated Server-incident Analysis (ASA) file

1. From the Microsoft Windows **Start** menu, point to **All Programs, RapidResponse**, **Write Debugging Information**, and then click **Automated Server-incident Analysis File**.
2. Click **Yes**.

RapidResponse Server folder structure

By default, the RapidResponse Server is installed to **C:\RapidResponse**. However, it is recommended that RapidResponse Server should be installed on a separate drive (physical) from the Windows operating system. For example, **D:\RapidResponse**.

The following illustration shows the folder structure created when you install RapidResponse Server:



Note: If your company has deployed the optional RapidResponse Server failover cluster you should review the "Database folders in a failover cluster" on page 299.

The following describes some of the folders created when RapidResponse Server is installed.

- **Configuration**—contains configuration files used by RapidResponse Server. These files should not be edited.
- **Data**—contains files that store the RapidResponse database. These files can be used for backing up and restoring the RapidResponse database. For information about data files, see "RapidResponse database content" on page 309. The files in the Data folder can be archived to another location in case of troubleshooting. For more information, see "Archiving the RapidResponse database files" on page 324.
- **Docs**—contains the RapidResponse documentation in PDF format.
- **Dumps**—contains the dump files created by RapidResponse Server Monitor after RapidResponse Server generates an internal error or crashes. For more information, see "Internal errors and system crashes" on page 244. The default location of this folder can be changed to improve performance. For more information, see "Improve performance by moving default subfolders" on page 251.
- **NamedExtractSets**—used for moving data files between RapidResponse instances, or in the RapidResponse Web Services net change data update process. For more information, see the *RapidResponse Data Integration Guide*.

- **Packages**—stores packages files that use the PKG file extension. This folder stores back up copies of the RapidResponse database, data files, and log files. For more information about this folder, see "Decompressing packages and Packages folder" on page 251. For more information about creating and using these packages, see "Backing up and restoring the RapidResponse database" on page 315.

  By default, this folder also stores the diagnostic files created by RapidResponse Server Monitor after RapidResponse Server generates an internal error or crashes. For more information, see "Internal errors and system crashes" on page 244. The default location of this folder can be changed to improve performance. For more information, see "Improve performance by moving default subfolders" on page 251.

  The files in the Packages folder can be archived to another location in case of troubleshooting. For more information, see "Archiving RapidResponse package files" on page 252.
- **Persistence-RuleBased**—contains data persistence definitions. This folder and the files it contains should not be modified. For more information, see "Data persistence" on page 329.
- **Program**—contains the RapidResponse Server program and system files.
- **SampleMS**—contains RapidResponse Server sample data. The sample data can be used for validating an installation or for training purposes.
- **Temp**—used as a temporary file location for several data import processes and database operations. Upon restart of RapidResponse Server, files older than 48 hours are automatically deleted. This folder usually is empty.

The folders not discussed in this section are generally used in the data import processes or the RapidResponse program upgrade process.

For information about backing up RapidResponse folders and files, see "Backing up RapidResponse program files" on page 314.

Improve performance by moving default subfolders

As noted above, by default, the **Dumps** and **Packages** folders are child folders in **C:\RapidResponse**. It is recommended that the default locations for these folders be moved to different physical drives (not on the same drive as the RapidResponse Server and database, or the Windows operating system).

By having these folders on different drives you can speed up the operation that are performed within them and more quickly return RapidResponse Server to a running state.

The default folder locations can be changed using the Windows registry. For more information see:

- "DumpDirectory" on page 363 (for Dump folder)
- "Packages" on page 359 (for Packages folder and database archives)
- "PkgDirectory" on page 364 (for diagnostics package files that, by default, are stored in the Packages folder)

Decompressing packages and Packages folder

The **C:\RapidResponse\Packages** folder contains compressed archives, or packages, of the RapidResponse database, data files, and log files. It stores packages created by the following processes:

- Database backups. For more information, see "Backing up and restoring the RapidResponse database" on page 315 and "CreateDataPackage command" on page 388.
- Database integrity checks. For more information, see " RapidResponse database integrity" on page 327.
- Diagnostic files for Kinaxis Customer Support. For more information, see "Internal errors and system crashes" on page 244.
- Database backups automatically saved before for upgrading. For more information, see "Recovering data files in case of upgrade failure" on page 183.
- Package of data files that could be used to restore RapidResponse to its state before the data import occurred. The file is named **PreDataImport.pkg** or **PreDataImport.zip**. For more information, see "DataImport command" on page 390 and "DataUpdate command" on page 395.
- Database backups saved before applying data model customizations. For more information about customizing the data model, see the *RapidResponse Data Integration Guide*.

Notes:

- The only compressed archive not stored in the **\Packages** folder is the Last Known Good Data package created with a DataImport command. For more information, see "DataImport command" on page 390.
- The files in the Packages folder can be archived to another location in case of troubleshooting. For more information, see "Archiving RapidResponse package files" on page 252.

If you want to view the contents of a package, you need to decompress it.

▸To decompress a RapidResponse package

1. Open a Windows Command Window on the computer where RapidResponse Server is installed.
2. Navigate to the **C:\RapidResponse\Packages** folder.
3. Specify the decompression command using the following syntax:
   ```
   wpzip PackageName.pkg
   ```
   where **PackageName.pkg** is the name of the compressed package.

Archiving RapidResponse package files

RapidResponse Server stores package files (.PKG or .zip extension) in the **Packages** folder. By default, the **Packages** folder is a child folder in **C:\RapidResponse**. However, the location of the Packages folder can be customized. In fact, it is recommended that you customize the location to improve RapidResponse system performance. For more information, see "Improve performance by moving default subfolders" on page 251.

The RapidResponse system can be set up to archive the contents of the **Packages** folder. By archiving these types of files, you might be able to more easily rollback the database in case of a system failure or a corrupted database. It might also help to archive packages when troubleshooting and working with Kinaxis Customer Support.

RapidResponse supports the following types of package files (.PKG file extension):

- RapidResponse data package files. These types of packages are a complete copy of the RapidResponse database. For more information, see "Backing up and restoring the

RapidResponse database" on page 315.

- RapidResponse backup package files. These types of packages contain a copy of data model tables and customizations, and can be used to recreate these customizations on other systems.
- Log file packages used in troubleshooting situations by Kinaxis Customer Support to help diagnose and understand system issues. For more information, see "Troubleshooting RapidResponse Server" on page 241.
- Diagnostics package files created by the RapidResponse Server Monitor. These files contain detailed system information. For more information, see "Internal errors and system crashes" on page 244. The default storage location of the diagnostic package files can be customized so that they are not stored in the same location as the other package files. To do so, use the **PkgDirectory** Windows registry setting. For more information, see "PkgDirectory" on page 364.

Setting up archiving of package files

To set up the archiving of RapidResponse database files, you must create or a modify a Windows registry setting on the computer where RapidResponse Server is installed. The **Directories\BackUpRoot** setting specifies the folder where the archived files are stored. This setting is specified as an absolute path and **\Packages** is appended to it. For example, if you specify **E:\Archive** then the archived files are stored in **E:\Archive\Packages**. If the **Directories\BackUpRoot** setting is blank or not available then archiving of the database files is turned off.

In addition, the **BackUpPackages** registry setting must be set to 1 to turn on the archiving of package files. For more information, see "BackUpPackages" on page 352.

The **Directories\BackUpRoot** setting also controls the archiving of RapidResponse database files. When this setting is specified, **\Data** is appended to it for a location for database files. For more information about archiving database files, see "Archiving the RapidResponse database files" on page 324. For more information about this Windows registry setting, see "BackUpRoot" on page 357.

It is recommended that the archive folder be on a drive or device separate from the **Data** folder (the RapidResponse database folder). Doing so can improve RapidResponse Server restart time. It is also a best practice not to store the archived files on the same hardware as the **Data** folder in case of catastrophic hardware issues.

The RapidResponse Server service must have read-write access to the network location where the archive folder resides. For example, the archive folder might reside on a SAN or NAS.

Consider storing the archive folder where dump and diagnostic package files are stored. For more information, see "Selecting storage locations for operations" on page 311.

Notes:

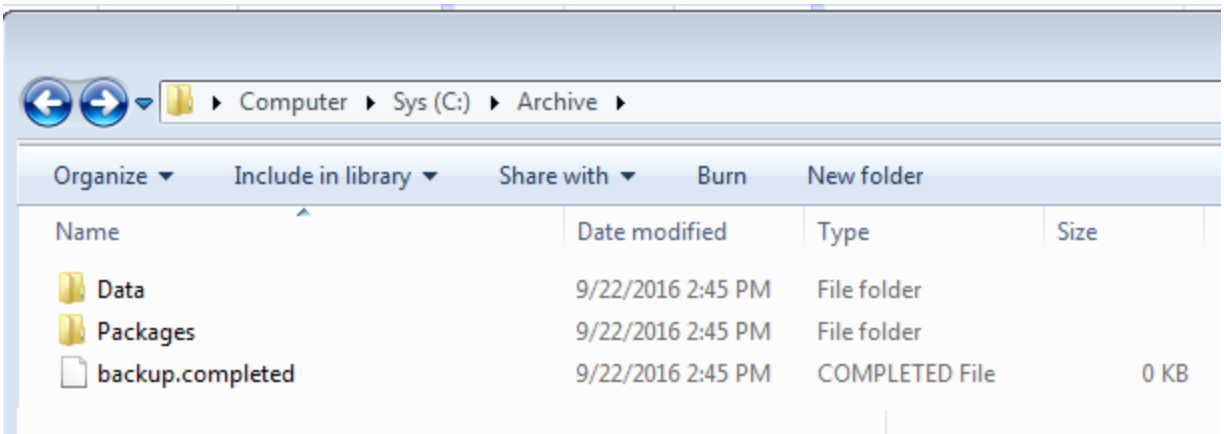
- RapidResponse Server does not need to be restarted after changing the archive folder setting.
- If your company has deployed the optional RapidResponse Server failover configuration, you must ensure that both RapidResponse systems use the same registry key. For more information, see "RapidResponse Server failover clustering" on page 289.

Archive process execution

After being set up, the archive process is automatically executed after the RapidResponse Server service has started. It also executes after the following RapidResponse system commands have completed:

- "CreateDataPackage command" on page 388
- "Restart command" on page 407

The archive folder holds copies of all package files in the folder specified in the **Directories\BackUpRoot** Windows registry setting. The following illustration shows the folder structure if the registry setting is **C:\Archive**.



The following list summarizes the steps RapidResponse executes when running the archive operation.

1. The **backup.completed** file in the archive folder (which specified in the **Directories\BackUpRoot** Windows registry setting) is deleted (if file exists).
2. An empty text file named **backup.inprogress** is created in the archive folder. The existence of this file indicates that RapidResponse is actively creating archive files.
3. Any temporary files that RapidResponse has created in the archive folder are deleted. These files use the **.tmp** extension. Files are in a temporary state until they are fully copied over to the archive folder.
4. Package files that are older than the age deletion threshold are deleted from the archive folder. The default setting is 10,080 minutes (7 days). The threshold setting can be modified. For more information, see "Modifying the age deletion threshold" on page 255.
5. Package files that exist in the archive folder but no longer exist in the Packages folder (**\Packages**) are deleted from the archive folder.
6. All package files in the **Packages** folder are copied to the archive folder. If a package file with the same name already exists in the archive folder, then both versions are retained in the archive folder.
7. A file named **manifest.*timestamp*.json** is created in the archive folder. This text file lists the names of all the package files stored in the Packages folder. This information can be of use when working with Kinaxis Customer Support.
8. The empty text file named **backup.inprogress** is deleted.
9. The **backup.completed** file is created in the archive folder. This file indicates that the archive process has completed. If this file exists, the archive files have been successfully created.

Note: Archiving operations are logged in the **Server.log** file. For more information, see "RapidResponse text-based log files" on page 462.

Modifying the age deletion threshold

When the archive operation executes, it deletes package files that are older than the age deletion threshold. This helps to ensure that disk space will be available for newly archived packages. The default age deletion threshold is 10,080 minutes (7 days). This setting can be modified by editing the **PackageBackUpWindowMinutes** Windows registry setting. For more information, see "PackageBackUpWindowMinutes" on page 355.

The higher the value used in this setting, the more disk space that will be consumed. However, a higher value might provide an opportunity to recover older package files that could be useful in troubleshooting situations. The amount of disk space required might also depend on how often the archiving process is executed which is dependent of the execution of RapidResponse system commands.

Note: If your company has deployed the optional RapidResponse Server failover configuration, you must ensure that both RapidResponse systems use the same registry key. For more information, see "RapidResponse Server failover clustering" on page 289.

Performance impacts from scans and agents

RapidResponse Server, and other applications, that make extensive use of system memory (also known as RAM or physical memory) can experience significant performance issues when scanning tools such as antivirus applications or agents are introduced.

Active file scans of the RapidResponse database and folder scans of the data files can significantly slow RapidResponse operations leading to poor user experiences, system performance issues, and, in some cases, service failures.

It is strongly recommended that scanning tools or agents exclude the following folders from all their processes to avoid file locking conflicts with RapidResponse operations:

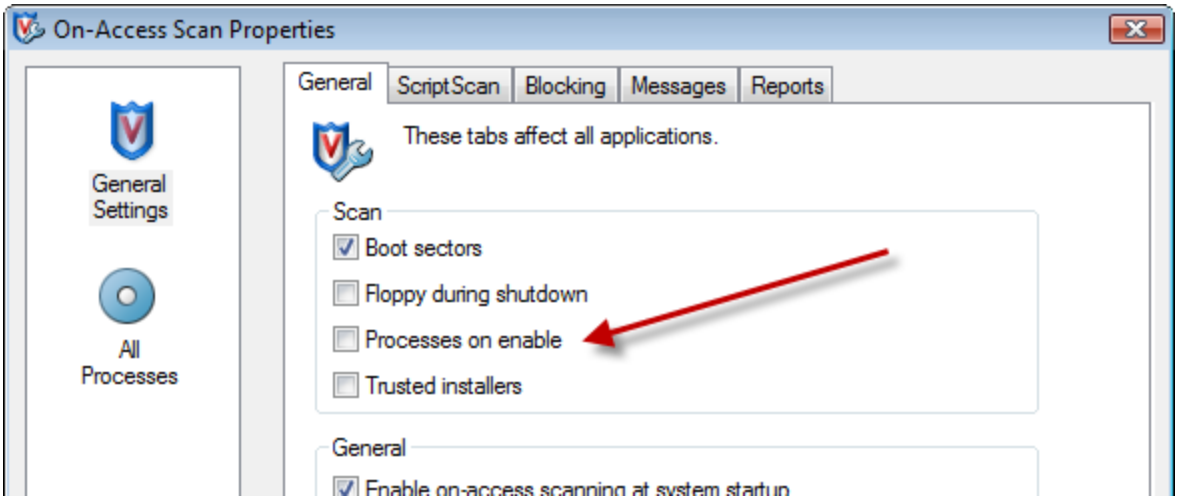
- C:\RapidResponse\Data
- C:\RapidResponse\Extract
- C:\RapidResponse\Packages
- C:\RapidResponse\Working

In addition, scanning tools or agents should exclude the RapidResponse Application Server configuration file (**web.config**) which is stored in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder on the computer where RapidResponse Application Server is installed. The scanning of this file can result in the Microsoft Internet Information Services (IIS) being reset leading to the disconnection of all users from the RapidResponse system.

Example: Maintaining performance with McAfee VirusScan

McAfee VirusScan (VSE) is used by many enterprises including a significant number of companies that have deployed RapidResponse. This section provides an example of how to configure VSE to work with RapidResponse. Although VSE is used in this example, the general process can be applied to other scanning tools and agents that might be running on a computer hosting the RapidResponse system.

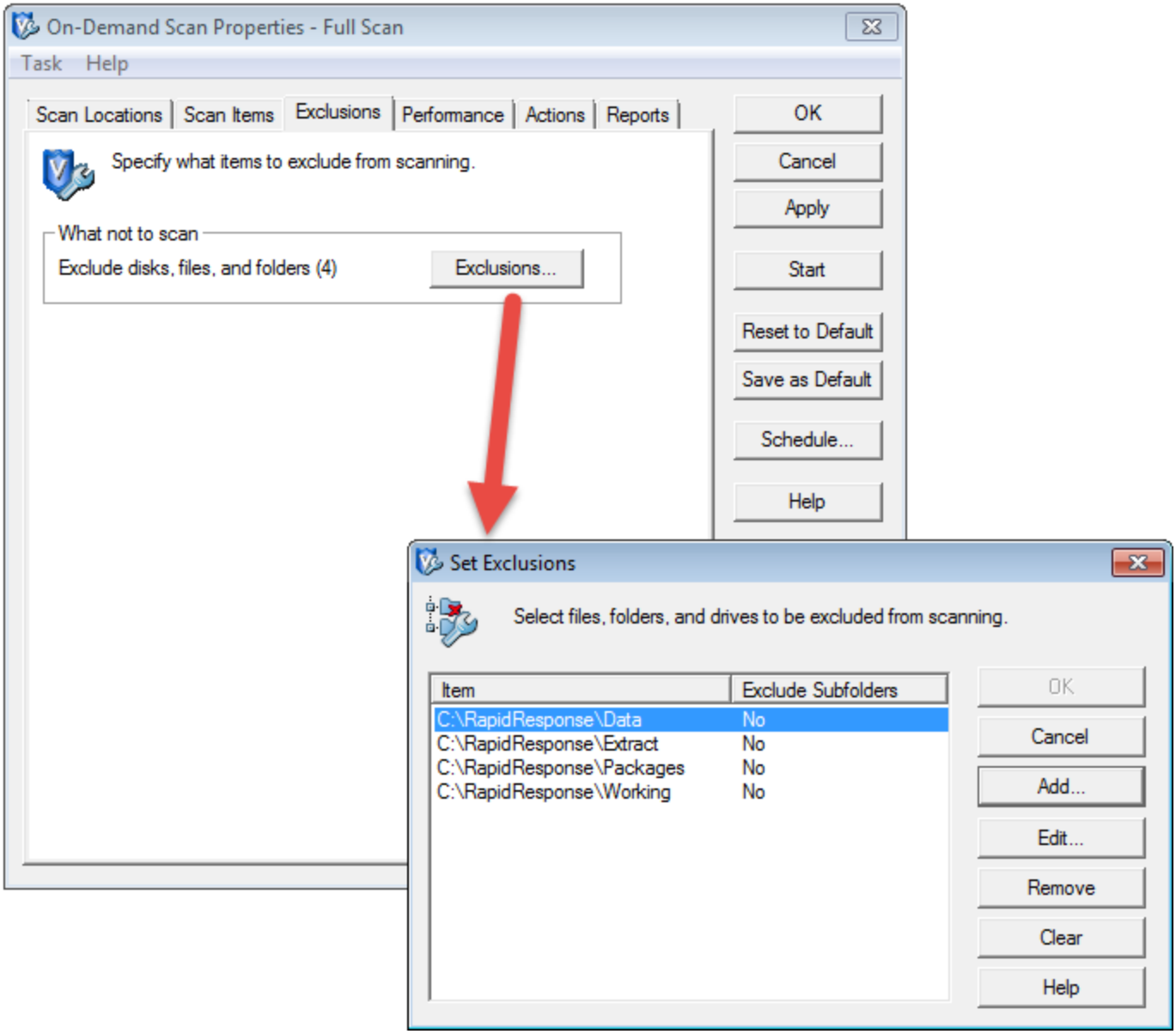
VSE On-Access Scanner includes a setting named **Processes on enable** which scans all running processes. By default it is turned off. The following image shows the setting, on the General tab of the On-Access Scan Properties (McAfee VirusScan Enterprise)



If this setting is turned on, the RapidResponse database, which is held in-memory (system), might become paged out to disk and must be reprocessed into memory with each database request. The paging out to disk is random. However, if it occurs it significantly impacts RapidResponse Server performance if a requested operation requires sufficient amounts of memory. The RapidResponse Server operation in this case needs to access the disk instead of the faster system memory. It is strongly recommended that the **Processes on enable** setting be turned off in environments where McAfee VirusScan Enterprise is used.

For more information about virus scanning and processes, review the Technical Article created by McAfee, Inc. at https://kc.mcafee.com/corporate/index?page=content&id=KB76157.

To prevent the scanning of RapidResponse folders holding the RapidResponse database and data files, set the scanning for exclusions as follows:


On-Demand Scan Properties - Full Scan
Task
Help
Scan Locations
Scan Items
Exclusions
Performance
Actions
Reports
OK
Cancel
Apply
Start
Reset to Default
Save as Default
Schedule...
Help
Specify what items to exclude from scanning.
What not to scan
Exclude disks, files, and folders (4)
Exclusions...
Set Exclusions
Select files, folders, and drives to be excluded from scanning.
Item
Exclude Subfolders
C:\RapidResponse\Data
No
C:\RapidResponse\Extract
No
C:\RapidResponse\Packages
No
C:\RapidResponse\Working
No
OK
Cancel
Add...
Edit...
Remove
Clear
Help

CHAPTER 22: RapidResponse system memory and monitoring

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Understanding hardware requirements 259
RapidResponse system memory usage 260
Monitoring input data growth 263
Calculations and system memory 265
Query monitoring and management tools 267
Scenario memory consumption 270
Monitoring CPU usage 271

RapidResponse system performance is directly tied to the operating system, processing power, and system memory on the computer where RapidResponse Server is installed.

This chapter describes how the RapidResponse Server uses system memory and the system monitoring options available to system administrators.

By monitoring system information on a regular basis, you can avert potential RapidResponse system issues and maintain a high level of system responsiveness. This information is also helpful in diagnosing system performance issues.

Understanding hardware requirements

The number of users RapidResponse can support is dependent on the processing power and the number of processors on the computer where RapidResponse Server is installed. The greater the number of concurrently signed in RapidResponse users, the greater the number of processors the server requires. If the number of RapidResponse users increases significantly, the performance of RapidResponse Server can be negatively impacted.

System memory, sometimes called RAM or physical memory, is used to load RapidResponse input data and perform analytic calculations and queries. If not enough system memory is available, or it is not properly configured, then RapidResponse system performance can be slow, or even unacceptable. For example, if the number of RapidResponse users you are supporting significantly increases, then more analytic calculations and queries are generated. If not enough memory is available, then RapidResponse Server continually swaps available memory amongst users, which results in slow performance.

Kinaxis Customer Support can help you determine your RapidResponse Server hardware requirements. Customer Support considers many factors when recommending system memory including:

- The input data size and the size of the historical data.
- The number of concurrent users.
- The analytics that are heavily used.
- The number of and age of permanent scenarios.

For more information about system requirements, see "System requirements for RapidResponse" on page 104. The rest of this section discusses system memory and how you can monitor and manage RapidResponse system memory settings.

RapidResponse system memory usage

The RapidResponse database is loaded in-memory. As such, it consumes system memory on the computer where RapidResponse Server is installed. RapidResponse runs on Microsoft Windows Server operating systems and can support up to 6 TB (6,144 GB) of system memory. System administrators need to understand how RapidResponse uses system memory and how it should be configured.

RapidResponse Server holds three types of data in-memory:

- **Input**—Imported from enterprise data sources. It also includes data modifications users or automated processes make in scenarios. For more information, see "Monitoring input data growth" on page 263. For more information about scenarios and memory management, see "Scenario memory consumption" on page 270.
- **Calculations**—Computations performed by the RapidResponse Server. This type of data is also known as "analytic calculations". The more complex the calculation, the more system memory required. Cached worksheet results are included in Calculations memory. For more information, see "Calculations and system memory" on page 265 and "Caching worksheet results" on page 763.
- **Queries**—Query results are the records each user works with. As the number of records, or rows, in all users' active worksheets grows, more system memory is consumed.

  Queries run against some tables, depending on the filter, can potentially return hundreds of thousands of records (or even millions). The more complex the query evaluation, the more system memory that is consumed. For example, opening a multi-level composite worksheet or a scenario that includes scenario comparison columns can consume more memory than a worksheet with a simple filter. For more information, see "Query monitoring and management tools" on page 267.

Each of these in-memory data types is further discussed in this chapter.

By default, about 10 GB of the system memory is dedicated to the operating system, the RapidResponse Server service, and the RapidResponse Service Host service. The remainder is available for use by RapidResponse. The more system memory that is available, the better the RapidResponse system performance and user experience.

The Master Administrator (Admin user) is notified if the server's system memory load reaches 90 percent. You can change this setting by creating a **ServerLoadAlertThreshold** value in the Windows Registry. For more information, see "ServerLoadAlertThreshold" on page 356.

Notes:

- If RapidResponse Application Server is installed on the same computer as RapidResponse Server, then 4 GB of system memory is automatically allocated for it.
- On systems with less than 100 GB of system memory, the RapidResponse Server can use up to 90 percent of the system memory. This default memory limit can be overridden by altering

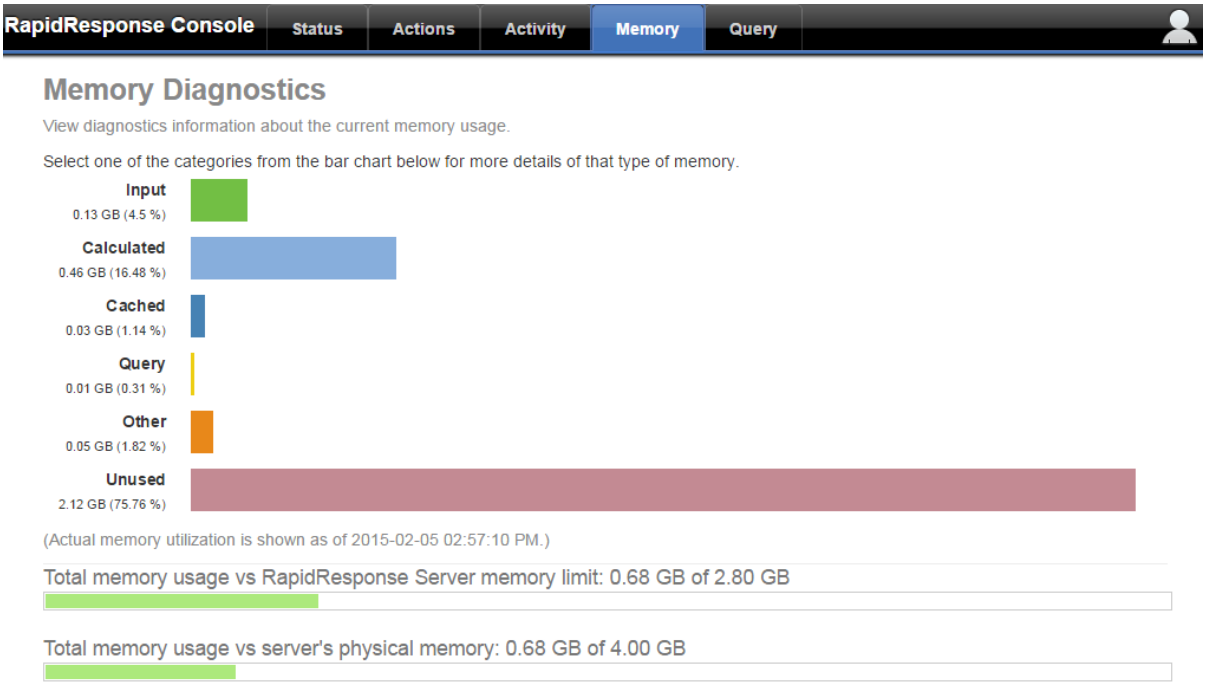
the **MemoryLimit** value in the Windows Registry. For more information, see "MemoryLimit" on page 354.

System memory details in RapidResponse Console

A RapidResponse system administrator should regularly monitor the amount of system memory RapidResponse is consuming. It should also be reviewed when users have performance-related complaints. By reviewing the system memory usage, system administrators can better understand the health of the overall system.

Use the RapidResponse Console to understand system memory usage. This Web-based multi-purpose administration tool is available to RapidResponse system administrators to assist in the management and monitoring of the RapidResponse system. To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

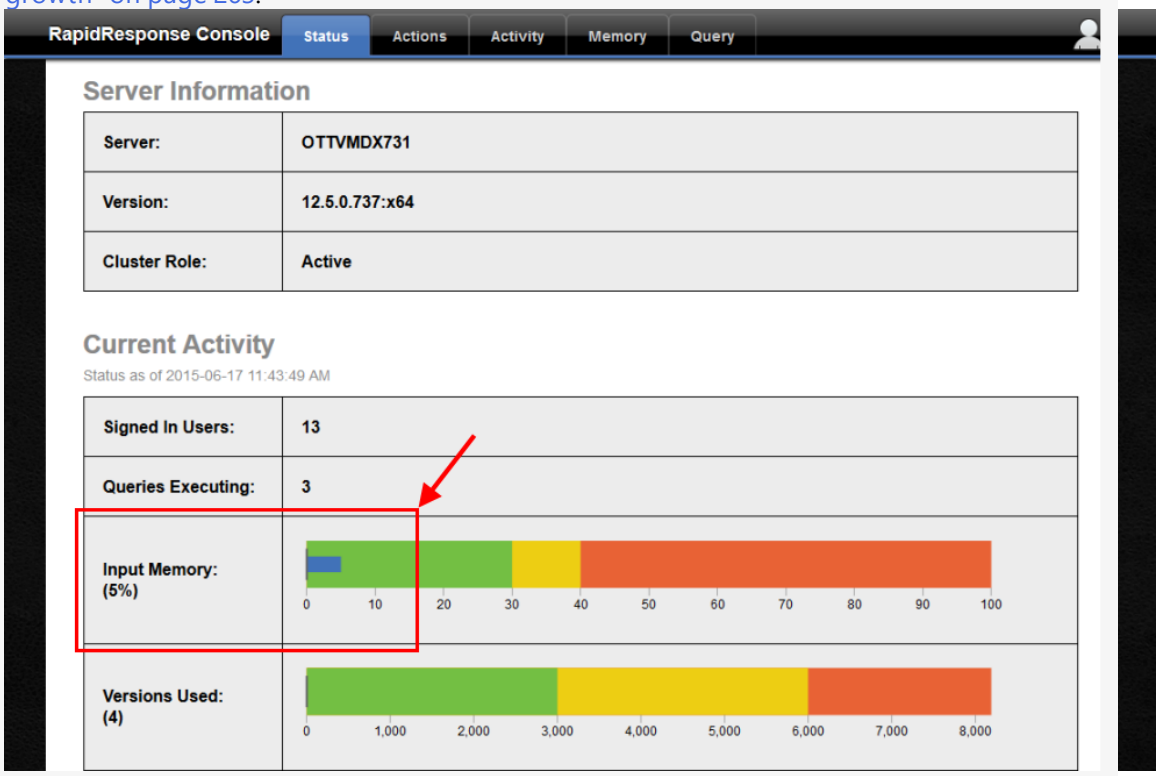
The RapidResponse Console provides detailed information about system memory consumption from the **Memory** page. From the page, you can review a graphical representation of memory consumption showing how system memory is allocated amongst input data, calculations, queries, and other (system overhead). The following illustration provides an example view.



By clicking the Input, Calculated, Cached, and Query bars in the chart on the **Memory** page you can drill for more details about a specific memory category. For example, by clicking the **Input** bar, you are provided with input data information such as the memory consumed by specific tables. This information can help you better understand the state of your RapidResponse system and usage patterns. It can also be useful when discussing issues with Kinaxis Customer Support.

Notes:

- In some cases, due to data complexities, you might notice an inconsistency between the summary bar chart and the detailed data. This is likely to be meaningful only with smaller databases or few calculated results or queries. Regardless, the information should still be considered valuable when managing and monitoring the RapidResponse system. You can also review the Windows Task Manager for more information about system memory usage.
- If your RapidResponse Server was installed on a drive other than **C:**, you might experience an error when accessing the Memory page in RapidResponse Console. To correct the error, create a folder named **C:\RapidResponse\Temp** on the computer where RapidResponse Server is installed.
- The Status page on the RapidResponse Console provides a quick view of the amount of memory being consumed by input data. It is important to quickly understand when too much input memory is being consumed. For more information, see "Monitoring input data growth" on page 263.



Server.log file

You can also determine how much system memory is allocated to RapidResponse Server by reviewing the **Server.log** file. This file contains a line similar to the following that indicates system memory allocation:

```
2008-05-06 09:21:54 INFO null - Memory limit: 1565MB
```

Additionally, every 15 minutes, RapidResponse Server writes a *heartbeat*, or status, message to **Server.log**. Each heartbeat message contains detailed information about how system memory is being consumed by RapidResponse, the amount of system memory consumed by input data, and the amount of system memory consumed by queries. For more information about the **Server.log** file, see " Server.log file" on page 464.

Monitoring input data growth

Monitoring the growth of input data is a key responsibility of RapidResponse system administrators. As input data grows it consumes more system memory. If input data grows too big, it can consume a significant portion of system memory and, in turn, negatively impact RapidResponse system performance.

To aid in this monitoring responsibility, RapidResponse includes alarms and a report as discussed in this section. You can use the RapidResponse Console to review system memory consumption of input data. For more information, see "System memory details in RapidResponse Console" on page 261.

Additionally, the Input Records and Scenarios worksheet in the Administration Log workbook provides current and historical information about the total number of input records in data tables in the root scenario. For more information, see "Input Records and Scenarios worksheet" on page 425.

Alarms

RapidResponse includes three alarms that notify through Message Center messages the Master Administrator (Admin user) of input data growth. The message alarms include the following subject line: **RapidResponse Alarm: Input Memory use**.

If any of these alarms are triggered, system administrators should investigate possible causes or contact Kinaxis Customer Support.

Alarm	Description
Cautionary for input data load	Triggered if RapidResponse input data consumes more than a specified amount of system memory (expressed as a percentage). Default: 33
Critical for input data load	Triggered if RapidResponse input data consumes more than a specified amount of system memory (expressed as a percentage). Default: 50
Growing input data load	RapidResponse compares the percentage of system memory consumed by input data to the lowest historical value (or a specified value) in the previous 90 days. If the current value is 5 percent greater than the lowest historical value (baseline), an alarm is triggered. Default floor value: 20

By default, RapidResponse reviews input data memory consumption once per day at 8 AM. You can modify how often you want to be notified of data consumption issues by changing the frequency on which the memory alarm runs. When you specify a frequency for the memory alarm, it is used after the alarm runs the next day.

▸To modify the input data alarm thresholds

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Database** category.
3. In one of the following boxes, type a value (represented as a percentage):

- Alarm - Cautionary for input data load
- Alarm - Critical for input data load
- Alarm - Growing input data load

These settings are fully described in the **Global Settings** dialog box or in the table immediately before this procedure.

4. Click **OK**.
5. Restart the RapidResponse Server. It can be restarted using the Scheduled System Tasks workbook or the RapidResponse Console. For more information see, "Commands and scheduling system tasks" on page 381 or "To stop and restart the RapidResponse Server service in one step" on page 231.

Note: To turn off an alarm, clear its setting in the **Global Settings** dialog box.

▸To specify how often the input data alarm runs

1. In the **Administration pane**, under **System Settings**, click **Configuration**.
2. In the **RapidResponse Configuration** workbook, click the **Other Settings** worksheet.
3. Insert the following record:
   - **Type**—ProcessingRule
   - **Name**—MemAlarmPeriod
   - **Value**—How frequently to check memory consumption, in milliseconds (ms).

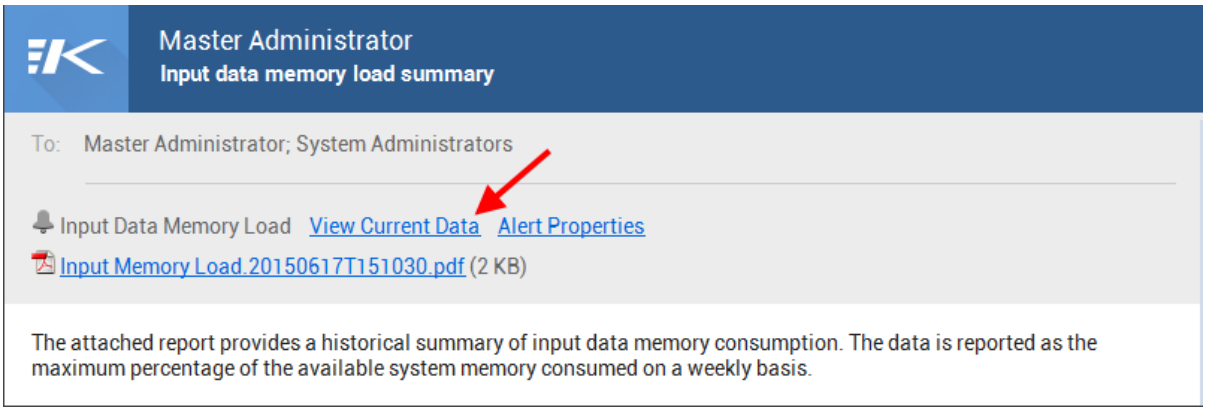
Note: By default, the memory alarm period is set to 86400000 ms, which is 24 hours.

Weekly report

RapidResponse uses a predefined alert to send a weekly report of the maximum percentage of the available system memory consumed by input data on a weekly basis. The report provides a historical summary of input data memory consumption and is sent to all system administrators.

By monitoring this information on a regular basis, you can avert potential RapidResponse system issues and maintain a high level of system responsiveness. This information is also helpful in diagnosing system performance issues.

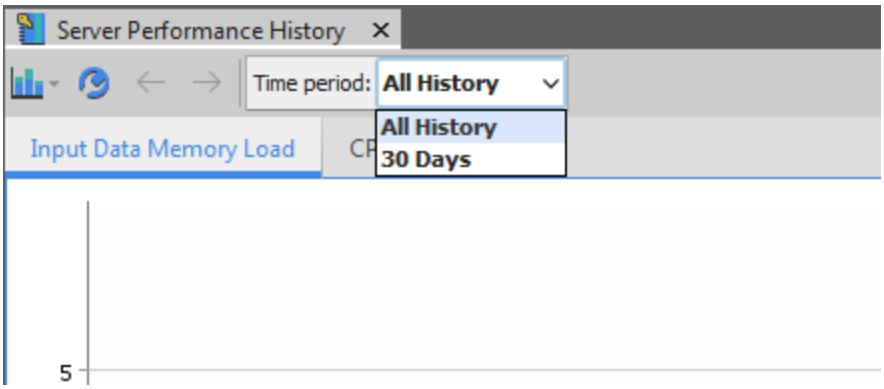
The message also includes a link to a graphical representation of the input data memory load statistics. To view the chart, click **View Current Data**.



Alternatively, this information is also available from the Administration pane (under **System Monitoring**, click **Server Performance History** and open the **Input Data Memory Load** worksheet). Two input data memory load charts are available:

- last 30 days using the daily highs
- all history using the weekly highs

The following image shows the Input Data Memory Load worksheet in Server Performance workbook.



The **Input Data Memory Load** alert that creates the report can be modified to change the reporting interval, recipients, and other properties. Modifications can only be performed by the Master Administrator (Admin) user.

Note: By default, this alert is not enabled upon installation of RapidResponse.

Calculations and system memory

RapidResponse Server caches calculations in memory to ensure a high level of performance for users. Calculations include both analytic results and, if worksheet caching is turned on, worksheet results. For more information, see "Caching worksheet results" on page 763.

Stored results are maintained for as long as possible to prevent a recalculation if the results are required again. You can specify which scenarios RapidResponse should prioritize when deciding which cached

results to keep and which ones to discard. For more information, see "Setting scenario priority" on page 714. Intermediate results are maintained in memory while the computations are being executed.

You can use the RapidResponse Console to monitor the impact of calculations on system memory. For more information, see "System memory details in RapidResponse Console" on page 261.

RapidResponse Server imposes a limit on its use of system memory to save certain results that it has calculated. This is done for two reasons:

- To keep memory available for other purposes.
- To prevent RapidResponse Server from storing so many cached calculations that it would exceed the amount of system memory in the computer, causing the operating system to swap memory pages out to disk.

This limit is not a hard limit on the size of the RapidResponse Server process. Rather, it represents the point at which RapidResponse Server will begin to reuse some of the memory that has been allocated to calculated results.

The RapidResponse Master Administrator (Admin user) is notified with a message if insufficient memory is available for calculated results. The following is an example of the message:

```
Subject: Insufficient Memory for Calculated Results
The amount of memory available for calculated results is insufficient.
Recommendation: Cancel any active queries which are using a large amount of
memory, and end any user activities which are using a large amount of memory.
```

To remedy this situation, do one of the following:

- Cancel active queries. For more information see, "To cancel an active query" on page 605.
- End activity for some users. For more information see, "To view recent query history" on page 605.

Memory settings for calculations

RapidResponse analytic calculations use memory pools for storing input data and results, and holding intermediate results. Stored results are maintained as long as possible to prevent recalculation in the event they are required again. Intermediate results are maintained in a memory pool while they are being recalculated.

Unusual or erroneous data can cause a RapidResponse analytic to consume an excessive amount of memory. To prevent analytics from consuming all system memory, RapidResponse limits any single analytic result (for example, the netting results for a single part) to 4,096 MB (4 GB).

If the memory limit is exceeded, the query is immediately canceled. A warning message is written to the **Server.log** file and a message is sent to RapidResponse system administrators. The RapidResponse user that generated the query by opening a workbook is warned an error occurred and to contact their RapidResponse administrator.

For information about memory pool statistics in RapidResponse, see "Heartbeat.log file" on page 470.

▸To change the calculation memory pool limit

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.

4. In the **Insert Record** dialog box, do the following:
   - In the **Id** box, type **AnalyticMemoryLimitMB**.
   - In the **Value** box, type the memory pool limit (MB).
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.
6. Sign out and back into RapidResponse so that the changes take effect.

Caution: If you override this limit, it will not be updated upon upgrade if the default is modified.

Setting analytic cache limits

You can specify the size of the analytics cache memory limit, which is the amount of memory available to each processor thread used to calculate an analytic result. This allows the analytics performing the calculation to share and reuse partial results between different calculations. This value is specified in megabytes, and by default, is set to 2000 MB.

The default value for this setting will typically be sufficient for most environments. However, this limit might be exceeded and require changing in certain situations. For example, this might typically occur when the FlatBillDown and FlatBillUp tables are used in filtering or in queries that are run against all parts in the database. These are not recommended practices, but if unavoidable, the queries might run out of memory and require modifications to the limit.

Any changes from the default value should only be done in close consultation with Kinaxis customer personnel.

▸To change the analytic cache limit

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **Id** box, type **AlgorithmCacheMemoryLimitMB**.
   - In the **Value** box, type the cache memory limit (MB).
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.
6. Sign out and back into RapidResponse so that the changes take effect.

Query monitoring and management tools

A query is performed when a RapidResponse user requests a set of database records. For example, when a user opens a workbook, a query is executed to retrieve the records to display in the active worksheet.

The query consumes system memory during the evaluation. The more complex the evaluation, the more system memory is consumed. RapidResponse Server caches query results in memory to ensure a high level of performance for users.

The following RapidResponse database tables are often associated with high system memory usage:

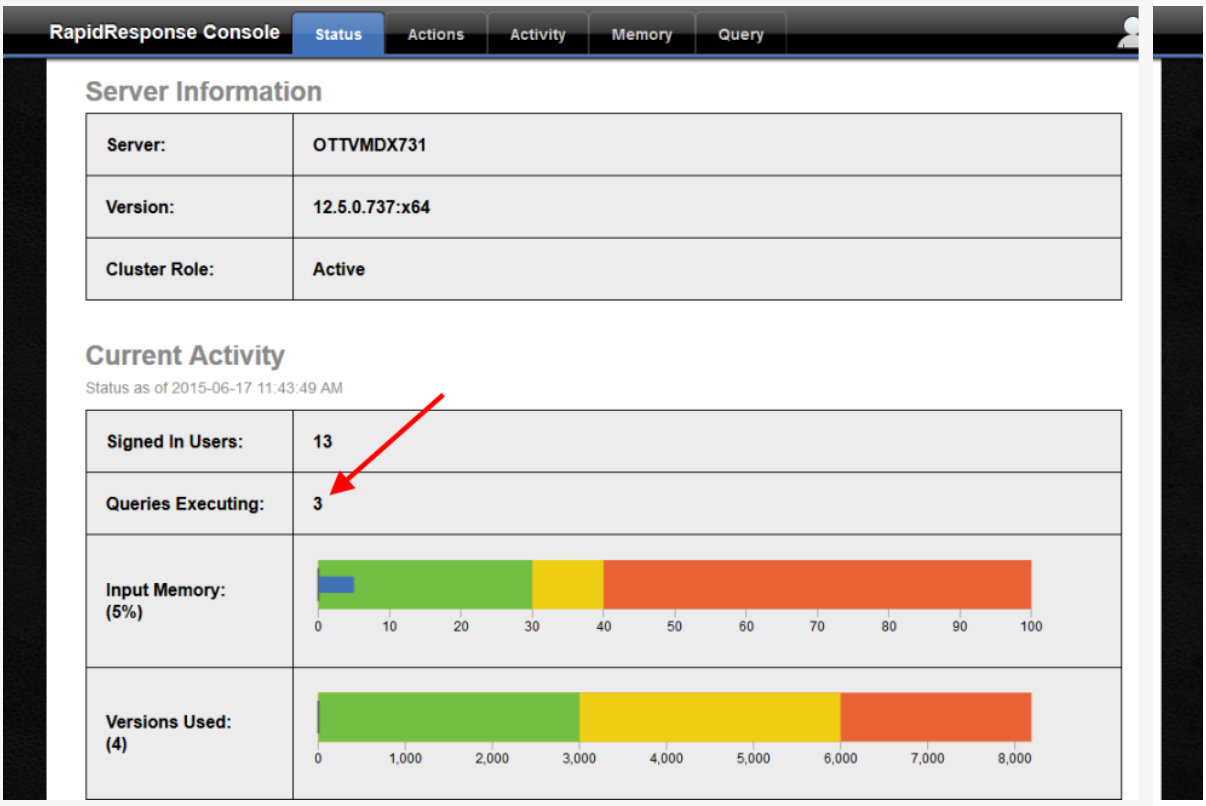
- **Part**—stores part information
- **ScheduledReceipt**—stores all work orders and purchase orders
- **IndependentDemand**—stores all customer orders and forecasts
- **PlannedOrder**—stores planned, or recommended, order information

This section describes the tools and settings to help monitor and manage query evaluations and results.

System and user administrators also have access to the Query Manager to help manage queries. For more information, see "Monitoring and canceling problematic queries " on page 603.

You can use the RapidResponse Console to monitor the active queries and to run a query against the RapidResponse database. For more information, see "System memory details in RapidResponse Console" on page 261 and "Manually running queries against the database" on page 244.

Note: The Status page on the RapidResponse Console provides a quick view of the number of queries executing. The following illustration shows the Status page, which displays the number of queries executing.



Query memory usage alarm

The RapidResponse Master Administrator (Admin user) is notified with a message if 20 percent of the system memory on the computer where RapidResponse Server is installed is used to generate query results. For example, on a system that has 128 GB of system memory, the maximum is 24 GB before a notification is sent.

The following is an example of the error message that high query memory usage generates:

```
Subject: Excessive Query Memory
An excessive amount of the RapidResponse Server's memory is being used for
query results. Users should close large queries. Users consuming the largest
amounts are:
Allison : 8400 KB
Bhanu : 7300 KB
```

You can change the threshold setting by creating a **QueryMemoryAlertThreshold** value in the Windows Registry. For more information, see "QueryMemoryAlertThreshold" on page 355.

Canceling queries

RapidResponse administrators can cancel queries that negatively impact RapidResponse performance. For more information, see "Monitoring and canceling problematic queries " on page 603.

When there is a heavy system memory load on RapidResponse Server, queries might be truncated. When this occurs, a message is written to the Event Log and to **Server.log**. The message is logged only the first time a query is truncated, during the period that RapidResponse Server is running. The message is: **Query truncated at <number> records, due to a memory load of <number>%**.

To protect system performance and stability, RapidResponse automatically cancels query evaluations that use more than 50 percent of the available system memory (excluding the system memory allocated to input data). In determining the amount of system memory used by the query evaluation, RapidResponse includes the final result, intermediate results, and nested query results.

If the system memory threshold is exceeded, a warning message is written to the **Server.log** file and a message is sent to RapidResponse system administrators. The information in the log file helps RapidResponse administrators understand why the query was canceled. The user who initiated the query does not receive notice that her query was canceled.

The 50 percent system memory limit is a default setting and can be changed.

▸To change the threshold for automatically canceling queries

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **Id** box, type **QueryMemoryLimit**.
   - In the **Value** box, type one of the following:
     - The percentage of the system memory. To specify a percentage, enter a number followed by a percent sign. For example, **40%**.
     - An absolute system memory limit in megabytes (MB).
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.
6. Sign out and back into RapidResponse so that the changes take effect.

Invalidation of results and query performance

By default, RapidResponse does not recalculate all stored results in a scenario when changes are made to data; that is, only some calculated results are discarded (or invalidated) as necessary. This avoids recalculation of some results. However, depending on factors such as product structure or data size, the selective invalidation of calculated results might result in slower runtime.

This setting can be changed so that all results are recalculated after a change to data (excluding custom fields and notes). This might result in faster query performance. However, in some cases, especially where the system is heavily used for what-if processing, performance might degrade.

You can change this setting by creating a **InvalidateAll** value in the Windows Registry. For more information, see "InvalidateAll" on page 353.

Scenario memory consumption

Input data from enterprise data sources is represented in RapidResponse as the Enterprise Data scenario (sometimes called the root scenario). All other scenarios in RapidResponse are based on this scenario and together they can consume a significant portion of system memory. If too much system memory is used, RapidResponse system performance can be adversely affected. As such, it is important to understand how scenarios contribute to memory consumption.

RapidResponse uses a versioned database and every scenario can be considered a copy of its parent. Creating a child scenario does not copy all the data from its parent. Instead, the scenarios are linked; the parent and child scenarios share the same database records except for the unique records due to modifications, deletions, and insertions in the parent or child scenario. Changing data in a child scenario creates a new and unique record relative to its parent and adds another record to the RapidResponse database.

Unless the data in a child scenario changes significantly, child scenarios use significantly less memory than their parent. However, as child scenarios become more out-of-date with the data in their parent, their memory usage can considerably increase.

Scenarios internally are built out of *versions*. The number of versions a scenario requires depends on its relationship with other scenarios in the system. RapidResponse can support up to 8,192 versions. While data is being modified (transactions), the changes are stored internally in versions. As data and scenarios change, RapidResponse continuously manages the versions by collapsing and deleting versions that are no longer required.

RapidResponse Server does not automatically manage scenarios that might contribute to excessive system memory usage. The two most obvious contributors are scenarios that are no longer being used and historical scenarios that are not being updated. The RapidResponse system provides administrators the tools to manage these types of scenarios and monitor overall scenario usage.

The Scenarios workbook lists all private and shared scenarios available in RapidResponse. You can view information about any scenario, such as whether the scenario is shared, the scenario's owner, when it was last used, or whether it is permanent. You can also delete scenarios from this workbook. For more information, see "Administrator tools for scenario management" on page 708.

The Input Records and Scenarios worksheet in the Administration Log workbook provides current and historical information about the total number of private and public scenarios on your RapidResponse system. For more information, see "Input Records and Scenarios worksheet" on page 425.

In some cases, a record can consume a version, but not be visible in any scenario. This typically happens when a record is deleted in one scenario and modified in another, and the deletion is then updated into the modification scenario. This deletes the record, however, the modification still consumes a version and resides in memory. These invisible records can consume significant memory and increase the size of the RapidResponse database over time. These records can be automatically cleaned up by the VersionReclaim and VersionReclaimSweep commands. For more information, see "VersionReclaim command" on page 411 and "VersionReclaimSweep command" on page 411.

For more information about scenarios, memory consumption, and scenario management, see "Scenario management" on page 703 and " Scenario data changes and memory consumption" on page 704.

Monitoring CPU usage

RapidResponse uses a predefined alert to send a weekly report showing the RapidResponse CPU usage on the computer where it is installed. The data is reported as the number of CPU seconds consumed for the last seven days using 4-hour intervals and the report is sent to all system administrators.

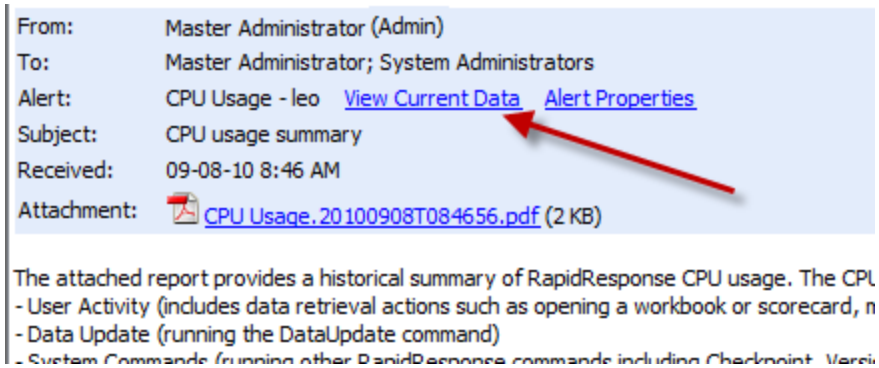
The report provides a historical summary of RapidResponse CPU usage. The CPU usage information is broken into three categories:

- **User Activity**—includes data retrieval actions such as opening a workbook or scorecard, modifying data, scenario management and so on.
- **Data Update**—running the DataUpdate command.
- **System Commands**—running other RapidResponse commands including Capture, DataExpiry, and so on.

By monitoring this information on a regular basis, you can avert potential RapidResponse system issues and maintain a high level of system responsiveness. This information is also helpful in diagnosing system performance issues.

If this report indicates high levels of CPU usage that are impacting users, your alerts might be consuming excess CPU time in periods of high user activity. To prevent alert queries from consuming resources required by users, you can adjust the number of worker threads the RapidResponse Service Host service is allowed to use for executing queries. This allows you to dedicate more threads to user processes. For more information, see "Configuring RapidResponse Service Host" on page 234

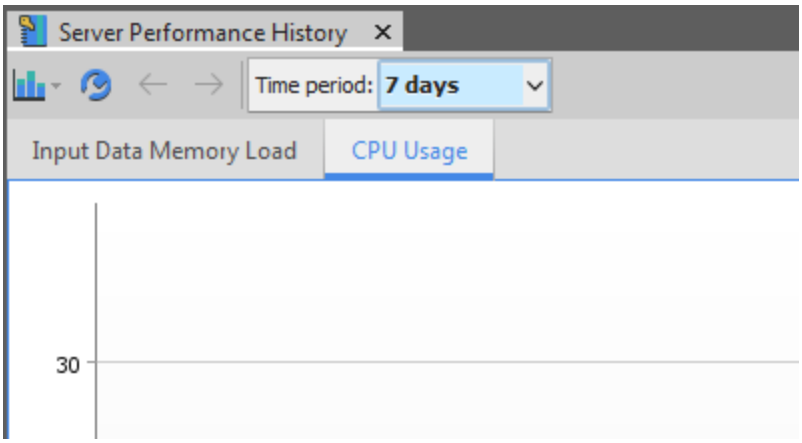
The message also includes a link to a graphical representation of the CPU usage statistics. To view the chart, click **View Current Data**.



Alternatively, this information is also available from the Administration pane (under **System Monitoring**, click **Server Performance History** and open the **CPU Usage** worksheet). Three CPU usage charts are available:

- last 12 hours using 15-minute intervals
- last 24 hours using 30-minute intervals
- last 7 days using 4-hour intervals

The following image shows the CPU usage worksheet in Server Performance workbook.



The **CPU Usage** alert that creates the report can be modified to change the reporting interval, recipients, and other properties. Modifications can only be performed by the Master Administrator (Admin) user.

Note: By default, this alert is not enabled upon installation of RapidResponse.

CHAPTER 23: RapidResponse Server settings

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Importing license keys 273
Site licensing 274
Configuring email support 276
Automatic deletion of system records 277
RapidResponse locale settings 281
RapidResponse and TCP/IP ports 283
Setting the MRPDate calculation 286
Renaming RapidResponse Server 287

During the initial RapidResponse setup and integration, RapidResponse Server settings were configured; however, you might need to modify these settings, depending on your company's requirements.

For example, to ensure optimum RapidResponse Server performance you need to manage the deletion of system records. Or you can change RapidResponse port numbers to allow communication between various RapidResponse components and open specific ports to provide external users access to RapidResponse.

Importing license keys

License keys are used to enable RapidResponse functionality, and to specify the number of user accounts and sites that RapidResponse can support. The license key file is provided by Kinaxis Customer Support.

Kinaxis Customer Support generates the license keys and the keys are only compatible with a specific computer based on the computer's server ID. You need to provide Kinaxis Customer Support with the server ID of the computer where RapidResponse Server is installed.

When you import a license key file, the existing license keys are replaced.

RapidResponse license keys use expiry dates. Fifteen days prior to the keys expiring, system administrators receive a warning. If you receive a warning, you should immediately contact Kinaxis Customer Support.

▸To determine the computer's server ID

1. Open a Windows command window on the computer where RapidResponse Server is installed.
2. Go to the **C:\RapidResponse\Program** folder.
3. Type **getserverid.exe** and press **ENTER**.
4. The command generates information in the following format:
   Server ID is >1234567890<.
5. Send the Server ID information to Kinaxis Customer Support (support@kinaxis.com).

▸To import license keys

1. In the **Administration** pane, under **System Settings**, click **Licenses**.
2. Click **Browse**.
3. Locate the license keys file, and then click **Open**.
4. Click **Import License Keys**.

Notes:

- You can review which RapidResponse capabilities are available by clicking **License Keys**.
- For information about checking how many user licenses are available, see "Reviewing user license information" on page 541.

Site licensing

All parts in the RapidResponse database are associated with a site. The combination of the part's name and its site, make the part unique. While multiple sites could carry the same part and use the identical name to identify it, the part is considered unique in each different site. The same is true of constraints and work centers.

Sites are used to identify data sources. Data sources can include your company's enterprise system (for example, ERP), data feeds from your customers and suppliers, and other databases. RapidResponse can use sites to model a source of supply, demand, or both. Supply and demand from each site is segregated from other sites. For more information, see the *RapidResponse Data Integration Guide*.

RapidResponse supports two types of sites: manufacturing/physical and inventory/logical.

Manufacturing/Physical

A manufacturing/physical site is an individual location within a company (or a company's subsidiary or a company's third-party manufacturing facilities) that segregates its supply and demand from other locations, for example, a plant, a specific geographic location, and so on. Typically, manufacturing, assembly of products, or both occur at this type of site.

Data from manufacturing/physical sites is used to model supply and demand, and model the building of supply to support demand. The part data associated with manufacturing/physical sites includes a BOM structure.

Enterprise data sources are often used as a site identifiers.

Inventory/Logical

Inventory/logical sites are used to identify units, such as business units and inventory hubs. An inventory/logical site is often an inventory location, and it segregates its supply and demand from other locations. Examples include retail site, hub, VMI, and order consolidation.

These types of sites are primarily used to model a source of supply, demand, or both.

The part data associated with the inventory/logical site type does not involve transformation of one part into another (for example, processing, assembly, and so on) and should not include any BOM structures. RapidResponse analytics (including netting) must not be used in modeling exercises that explode BOM structures.

Licenses

Every RapidResponse instance has at least one manufacturing/physical site. Typically, RapidResponse deployments include additional manufacturing/physical and inventory/logical sites. RapidResponse limits the number of sites that can be used through licensing.

Site licenses are monitored during a data update or data import process. If the site limit is exceeded, the data update is not performed. If the site limit is exceeded during a data import, the import is not performed and RapidResponse Server is stopped. To restart RapidResponse Server, restore the latest RapidResponse database. For more information about the RapidResponse database, and restarting RapidResponse, see "RapidResponse database content" on page 309 and "RapidResponse Windows Services" on page 227.

Additionally, the Master Administrator (Admin user) is notified if RapidResponse consumes more sites than your company has licensed. To resolve this issue, modify your company's extract data or contact Kinaxis Customer Support to acquire additional licenses.

For more information about adding, see the *RapidResponse Data Integration Guide*.

▸To review site license status

1. In the **Administration** pane, under **System Settings**, click **Licenses**.
2. In the **Users and Sites** area, click **View License Details**.
3. Click the **Sites** tab and review the information.

Notes:

- Depending on your license agreement, you might not see the **Users and Sites** section of the **Licenses** dialog box.
- The site licenses have an expiry date and must be renewed. RapidResponse monitors the status of both site type licenses, and 15 days before the expiry date, the Master Administrator (Admin user) receives an email message notification as a reminder.

Configuring email support

RapidResponse sends email messages to administrators and to users (alarms, alerts, and messages from Message Center). To support this functionality, you must specify an email server and provide the email address of each user who will use the email functions in RapidResponse.

The RapidResponse Utility Server service sends emails using the settings you have specified. If an email cannot be sent, it is retried for up to seven days. Messages older than seven days are not sent. When the Utility Server restarts, any messages that could not be sent and that are older than seven days are deleted automatically.

To set up email messaging, RapidResponse requires:

- A properly installed and configured SMTP-compliant email server.
- The RapidResponse Utility Server service accesses the email server to send email notifications. The Utility Server uses an outbound connection on TCP port 25. This port must be opened in the firewall. In addition, you might need to configure virus scanning applications to allow outbound SMTP email. For example, McAfee VirusScan includes a tool that blocks mail from third-party email applications. For more information, see https://kc.mcafee.com/corporate/index?page=content&id=KB50707. For more information about the RapidResponse Utility Server service, see "RapidResponse Windows Services" on page 227.
- MAPI compliant email client.

This topic applies only to administrators using an **On-Premises** system.

Before configuring an email server, you must do the following:

- Specify an email address for the Master Administrator (Admin) user account. For more information, see "Master Administrator message notifications" on page 422.
- Specify the RapidResponse default email address. This address is used as the From address in email messages origination from the RapidResponse system such as alarms, warnings or status messages (as opposed to user generated messages). For more information, see "Specifying a default email address" on page 656.

As part of the email configuration process, you must also provide the address (or URL) users use to sign into RapidResponse.

▸To configure an email server

1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. In the **Message Center and Email** dialog box, type the name of your organization's email server in the **Email server** box. The name is case sensitive.
3. In the **Web server URL** box, type the address of the RapidResponse Application Server. This is the address that users use to sign into RapidResponse. For example, **http://*computername*/rapidresponse**.

   This address is used to support the functionality that send links to resources, reports, and web addresses using Message Center and email messages.

Notes:

- Email addresses specified within RapidResponse must be known to the designated email server.

- RapidResponse system administrators can configure email settings such as standard footers and whether to disable file attachments. For more information, see "Specifying email settings" on page 655.
- To receive attachments with alert notifications, email clients that can process MIME-standard attachments are required. For more information about alerts, see "Configuring settings for automation tasks" on page 671.
- An email address is required for each user who requires email support. For information about defining email addresses for individual users, see "Editing user accounts" on page 570.
- Unsent email is stored by the Utility Server for up to seven days. Messages that cannot be sent in this period, or any messages older than seven days are deleted.

Automatic deletion of system records

RapidResponse logs information about various activities such as user sign-in attempts, data changes, messages, and more. This information is stored in the RapidResponse database as system records. Over time, these system records can grow in size and potentially consume significant amounts of memory. To prevent excessive growth of these system records, the RapidResponse DataExpiry command deletes older records.

The DataExpiry command determines whether data has exceeded the age deletion threshold and, if it has, deletes it from the RapidResponse database. By default, the DataExpiry command is scheduled to run daily as the Auto-Delete scheduled task but it needs to be turned on. For more information, see "DataExpiry command" on page 389 and " Scheduling RapidResponse commands" on page 412.

You can customize the age deletion threshold for each system record type. You can also customize which system record types are deleted by the DataExpiry command.

The following table notes the system records that can be deleted and the default age of the data before it is deleted.

System records	Description	Age deletion threshold (days)
Administration log records	Stores summary information about: • Executions of RapidResponse commands and scheduled tasks. • Applications of RapidResponse data model customizations and changes. • Restart of the RapidResponse system. These records are displayed in the Server Operations worksheet in the Administration Log workbook. For more information, see "Server Operations worksheet" on page 424. Administration log records also include changes related to key security controls of your RapidResponse system. These records are displayed in the Security Audit worksheet in the Administration Log workbook. For more information, see "Security Audit worksheet" on page 430.	45
Alert and scheduled task log records	Stores records detailing successful and failed alert and scheduled task (modify data) execution, including reasons for failures. For scheduled tasks that modify data, RapidResponse also logs the changes made to records (inserts, modified, and deletes). For more information, see "Automation logging" on page 448.	14
Command log records	Stores the detailed log messages associated with the execution of RapidResponse commands. The commands are usually run as scheduled system tasks. These records are displayed in the Command Messages worksheet in the Administration Log workbook. For more information, see "Command Messages worksheet" on page 424.	14

System records	Description	Age deletion threshold (days)
Data change records	Stores records detailing user-initiated changes (inserts, deletions, and modifications) made to data in RapidResponse scenarios. These records are available for display in the Data Import and Update Log workbook, which is available to data and system administrators. Data change information is stored in the following tables: • DataChange • DataChange_Historical • DataChange_Local • DataChange_PendingUpdate All are fully described in the *RapidResponse Analytic and Data Model Guide*. The DataChange table is used in the Changes to Root Scenario worksheet in the Administration Log workbook. For more information, see "Changes to Root Scenario worksheet" on page 425. The DataChange worksheets populate the following tabs in the Scenario Properties window: • **Inherited Data Changes** tab (DataChange_Historical table) • **Pending Updates** tab (DataChange_PendingUpdate table) • **Data Changes (Pending Commits)** tab (DataChange_Local table) For more information about configuring data change tracking, see "Configuring data change tracking" on page 829. **Note:** A data import deletes all existing records. **Note:** Unlike the system records, the DataChange records are only deleted once the RapidResponse Server is restarted and the age threshold is exceeded. **Note:** If you are testing a RapidResponse Server upgrade, consider changing this setting to a high number (for example, 999) to avoid processing during the startup process.	45

System records	Description	Age deletion threshold (days)
Data metric log records	Stores records of the number of input records in data tables in the root scenario and the number of scenarios, shared and private, on your system. These totals are typically logged daily by a scheduled task that is owned by the Master Administrator. This data is available to administrators in the Input Records and Scenarios worksheet in the Administration Log system workbook and the Scenario Metrics worksheet in the Scenarios system workbook. For more information, see "Input Records and Scenarios worksheet" on page 425.	1130
Data update log records	Stores records detailing operations performed during data import and data updates. For more information, see "Data import and data update logs" on page 442. If these records are automatically deleted, the data update history folders can also be deleted, and can override the deletion rule specified for the folders. These folder deletions are reported in the server log, so to prevent unnecessary log entries, you can set this value to the same value as the data update history folder deletion rule. For more information, see the *RapidResponse Data Integration Guide*.	14
Excel import configuration records	Stores records detailing how data is imported from a Microsoft Excel file into a scenario. For more information, see the *RapidResponse Data Integration Guide*.	45
Links in messages	Stores the links to resources, reports, and web addresses in messages (and email messages). For more information, see "Setting Message Center options" on page 650.	45
Messages	Stores records detailing messages delivered to each user's Message Center. For more information, see "Setting Message Center options" on page 650.	45
Real-time data update history	Stores records detailing the results of data updates performed by bringing in grouped messages through the Real-time Integration Platform.	45
Real-time Message Log workbook	Stores records detailing messages sent and received by the Real-time Integration Platform.	45

System records	Description	Age deletion threshold (days)
Sign-in log records	Stores records detailing successful and failed sign-in attempts to RapidResponse. For more information about sign-in logging, see "Monitoring sign-in activities" on page 595.	45
Workbook command log records	Stores records detailing workbook commands that have been run interactively. This information includes when the command was run, which user ran the command, which scenario was changed by the command, and which worksheets were modified by the command. It also includes details about the records that were modified by data modification commands and the errors that occurred. These records are displayed in the Workbook Command Log worksheets in the Automation Log and the Automation Details and Log workbooks. For more information about workbook command logging, see "Workbook Command Log worksheet" on page 454.	14

▸To change the age deletion threshold for system records

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. Click the **Auto-delete Configuration** tab.
3. Locate the specific record type you want to change and in the **Maximum Record Age** column type in the number of days to preserve the system records.

Caution: Setting the age deletion threshold too low can result in users having an incomplete set of records to work with. This is especially true for data change records.

▸To disable automatic data deletion for a specific record type

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. Click the **Auto-delete Configuration** tab.
3. Locate the specific record type, and in the **Auto-delete enabled?** column set the value to **N**.

Caution: Disabling the automatic deletion of specific record types can lead to excessive growth of system records which can consume significant amounts of system memory.

RapidResponse locale settings

A locale is a collection of region-related, user-preference information used by your computer. The locale that is set on the computer on which RapidResponse Server is installed affects the way RapidResponse

Server handles data. For example, different locale settings have different methods of sorting query data.

You can set a different locale for RapidResponse Server from the one specified on the computer on which RapidResponse Server is installed. When setting a locale, you must provide a valid LCID number. The LCID number is a 4-digit hexadecimal number that represents the version of the language to use for the locale settings. The following table provides an example of some valid <LCID> values you can use.

Locale	LCID number (hexadecimal)
Chinese (Singapore)	1004
Chinese (Taiwan)	0404
Chinese (Hong Kong SAR)	0c04
Chinese (Macao SAR)	1404
Dutch (Netherlands)	0413
English (United States)	0409
Finnish	040b
French (France)	040c
German (Germany)	0407
Japanese	0411
Korean	0412
Spanish (Spain - Modern Sort)	0c0a
Spanish (Spain - Traditional Sort)	040a
Spanish (Latin America)	e40a
Spanish (Mexico)	080a

For a complete listing of the LCID numbers for setting the system locale, refer to the Microsoft Developer's Network (MSDN) library, at http://msdn.microsoft.com/library/default.aspx.

For more information about RapidResponse and locales, see "International character set support" on page 65.

▸To set the locale in the Configuration table

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **Id** box, type **ServerLocale**.
   - In the **Value** box, type a valid LCID number.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.
6. Sign out and back into RapidResponse so that the changes take effect.

Logged locale messages

If the locale setting in RapidResponse Server is valid, the following message is logged in **Server.log**:

```
The locale that will be used is: <LCID> (<description>)
```

If the locale that you have set is invalid on your system, the following message is logged in **Server.log**:

```
The LCID value "<LCID>" provided in the Configuration table is not a valid
LCID for this machine. The system locale will be used: <LCID>(<description>)
```

For more information about the log file, see " Server.log file" on page 464.

RapidResponse and TCP/IP ports

The RapidResponse Server is bound to a specific TCP/IP port and it must be open for inbound requests. RapidResponse Server uses this port to communicate with other RapidResponse components.

A default port number (14600) is provided during the RapidResponse Server installation program. You have the option of choosing an alternative port number between 1024 and 65535. This port cannot already be assigned.

Before RapidResponse Application Server is installed, two other TCP/IP ports must also be opened for inbound requests on the computer where RapidResponse Server is installed. RapidResponse Server uses these port to communicate with RapidResponse Application Server. These two ports need to be 2 and 3 port numbers greater than the port number used by RapidResponse Server to communicate with other RapidResponse components. For example, if the port number is 14600 then you must also open 14602 and 14603 to inbound requests from RapidResponse Application Server.

If you want to verify which port RapidResponse Server is using, review the **Server.log** file. Alternatively, you can review the port registry setting in **HKEY_LOCAL MACHINE\SOFTWARE\Webplan Inc**. For more information about this Windows registry setting, see "Port" on page 355.

In the event that you subsequently need to change the RapidResponse Server port number, follow the steps outlined below.

▸To change the RapidResponse Server port number

1. Stop the RapidResponse Server service.
   For more information see "RapidResponse Windows Services" on page 227.
2. Open a Windows Command window.
3. Change the path to RapidResponse Server folder.
   If you used the default location this is **C:\RapidResponse\Program**, (where **C:** is the drive where RapidResponse Server is installed).
4. Type the following command: `servername -install -Pn`
   where **`servername`** is the name of the RapidResponse Server executable and ***n*** is the port number. You can enter a value from 1024 to 65535.
5. The service is now installed on the new port.
6. Ensure the two ports required by RapidResponse Application Server on the RapidResponse Server computer are open for inbound requests. These two ports need to be 2 and 3 port

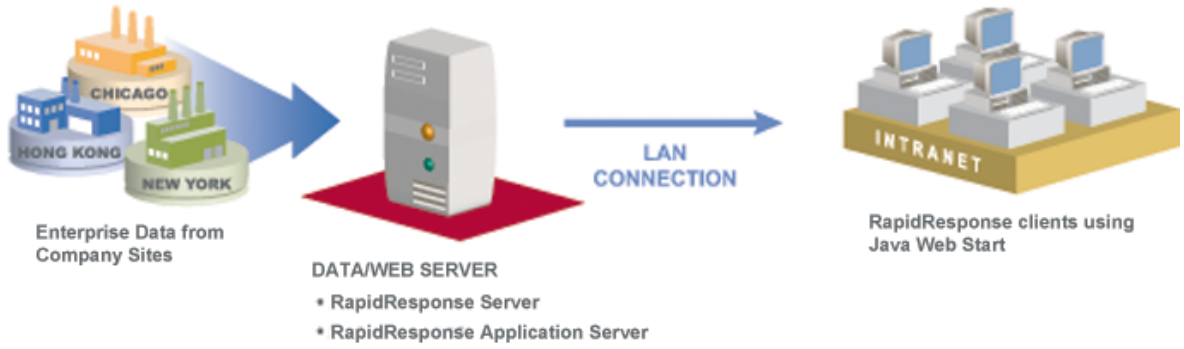
numbers greater than the port number used by RapidResponse Server to communicate with other RapidResponse components.

Note: All clients outside the firewall will need to append their server logon string with a colon and the new port number. For example: **YourServer:1457**.

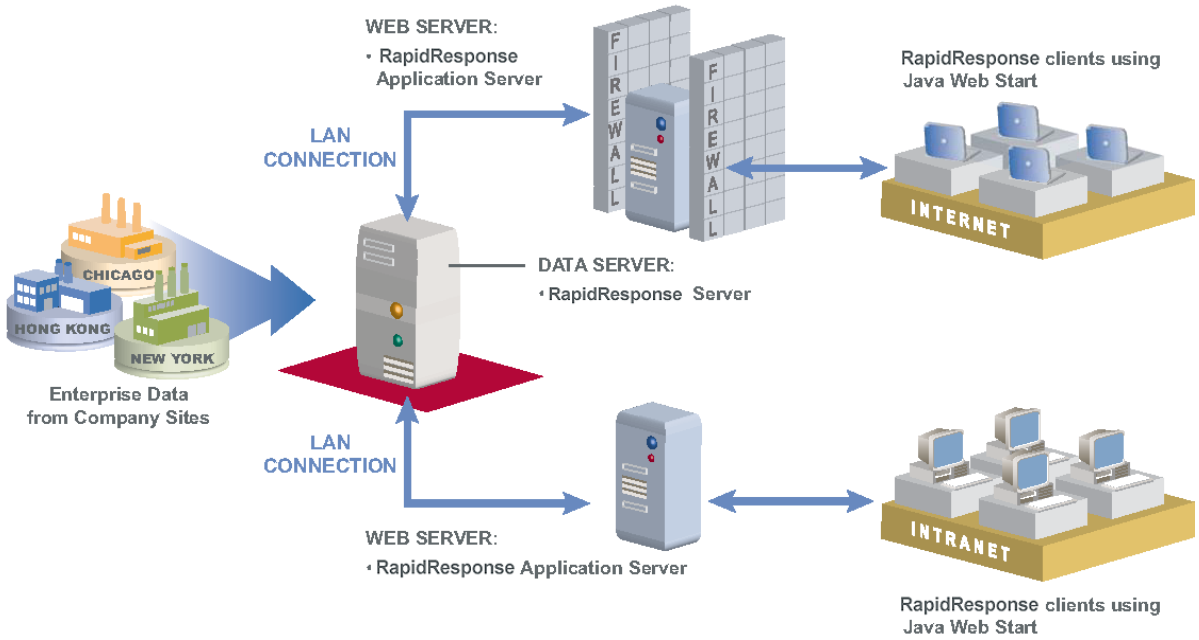
Note: No spaces are allowed on either side of the colon.

Encrypting communication between RapidResponse Server and RapidResponse Application Server

A RapidResponse system can be configured where RapidResponse Application Server is installed on the same computer as RapidResponse Server. This instance is used by internal RapidResponse users on the intranet. This configuration does not support users accessing RapidResponse from the Internet. Internet access to RapidResponse should only be provided when the Application Server is behind a firewall.



A more typical configuration is where RapidResponse Application Server is not installed on the same computer as RapidResponse Server. In the following diagram, RapidResponse Application Server is installed on two other computers; one outside the firewall and the other for internal users. Neither instance is with the same computer as RapidResponse Server and both servers have a network connection to RapidResponse Server. This configuration supports users accessing RapidResponse from the Internet.



As a RapidResponse system administrator, you can control whether the communication on your network between RapidResponse Server and RapidResponse Application Server is encrypted. By default, it is not.

▸To change the encryption setting for RapidResponse communication

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. On the computer where RapidResponse Application Server is installed, open the **Web.config** file located in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder with an XML or text editor.
2. Locate one of the following lines in the file **Web.config** file:
```
<server ipaddr="localhost" apiProtocol="FlatBuffer" encrypted="true">
<server ipaddr="localhost" apiProtocol="FlatBuffer" encrypted="false">
```
3. To turn on encryption, the encrypted value must be set to **true**. To turn off encryption, the encrypted value must be set to **false**.
4. Save the **Web.config** file.

Note: If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of RapidResponse Application Server is installed.

Setting the MRPDate calculation

By default, the MRPDate, also called the planning date, is the date on which data was last updated in RapidResponse, and represents the first date on which planning data can be modified.

The MRPDate is used by RapidResponse analytics to determine time fences, to determine if an order is late or inside lead time, and can be used as the first date in a bucketed crosstab worksheet.

If your company is using multiple sites, data is likely imported into RapidResponse on a different schedule for each site. For example, the data for site Chicago might be imported every Wednesday, while the data for site Taipei is imported every day. In a multi-site RapidResponse installation, the MRPDate will typically be either of the following:

- The date of the latest data update. In this case, the MRPDate would be updated each time data from one of the sites is imported. This is the default and most common setting. If you do not see an MRPDateCalculation record in the Configuration worksheet of the Administration workbook, this is the setting used by your RapidResponse system. It is represented by the following expression:
  ```
  PlanningCalendars[rundate.firstdate > 1970-01-01 & rundate.firstdate <>
  future & rundate.firstdate <> undefined]{rundate.firstdate}group{max}
  ```
- The date of the oldest data update in a sequence of site data updates.

You can configure how the MRPDate is calculated. You can specify either of the options listed above, or use another configuration if required by your company. Typically, this is done during the RapidResponse integration.

▸To change the MRPDate calculation

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **ID** box, type **MRPDateCalculation**.
   - To use the date of the latest data update, in the **Value** box, type:
     ```
     PlanningCalendars[rundate.firstdate > 1970-01-01 & rundate.firstdate
     <> future & rundate.firstdate <> undefined]{rundate.firstdate}group
     {max}
     ```
     This calculation is the default if not specified.
   - To use the date of the oldest data update, in the **Value** box, type:
     ```
     PlanningCalendars[rundate.firstdate > 1970-01-01 & rundate.firstdate
     <> future & rundate.firstdate <> undefined]{rundate.firstdate}group
     {min}
     ```
   - To use another date, type the expression in the **Value** box.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.
6. Sign out and back into RapidResponse so that the changes take effect.

Renaming RapidResponse Server

In some cases, you might need to change the name of the computer RapidResponse Server runs on. Data packages, server logs, and transactional data files are all named using the Server name, and these items are impacted if the name must be changed.

If the RapidResponse Server is renamed, any existing logs or data hives are maintained and considered to be part of a failover configuration, even if there is only the single server. For more information about failover, see "RapidResponse Server failover clustering" on page 289. Failover clustering can impact system performance on system startup, because the system must check if the other server or servers are running before this instance can start.

Transactional data files are stored in the **RapidResponse\Data** folder, and record every transaction performed in RapidResponse in sequential order. If the Server name changes, a new set of files is created, and the old set is obsolete, but is maintained. The obsolete set of files is considered a second RapidResponse Server's data transactions, and is kept to accommodate a failover structure.

If RapidResponse server is renamed, the obsolete server names are maintained in the server.log file.

If you must rename the RapidResponse Server, you must also modify your Application Server configuration to locate the new Server.

▸To prepare to rename a RapidResponse Server

1. Shut down the server by stopping the **RapidResponse Server** service.
2. Delete all Heartbeat and Server xml files from the **ServerComm** folder.
3. Rename the server.
4. Start the server by starting the **RapidResponse Server** service.

▸To configure RapidResponse Application Server

1. In the **C:\Program Files\Kinaxis\RapidResponse\Web** folder, edit the **web.config** file.
2. Locate the **Server.ipaddr** attribute.
3. Change the attribute value to the new RapidResponse Server name.
4. Save your changes.

CHAPTER 24: RapidResponse Server failover clustering

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Failover clustering overview 290
Setting up the failover cluster configuration 294
Database folders in a failover cluster 299
Determining which server is active 301
Managing servers in a failover cluster configuration 304
Failover and logging 304
Applying Service Updates and upgrading 305

RapidResponse Server failover clustering is an optional capability that is designed to reduce system downtime when RapidResponse Server is stopped for maintenance or crashes unexpectedly. Failover clustering is also known as "server resiliency".

There are times that RapidResponse Server must be stopped. For example, a scheduled weekly restart stops the RapidResponse Server and flushes system memory to maintain high-performance levels. However, while the system is stopped and restarted, RapidResponse users are prevented from accessing the system and their data. Depending on the size of the database, RapidResponse users can be denied system access for an hour or more while the database is reloaded into memory after restarting.

Applying Service Updates to RapidResponse Server also stops the system and prevents RapidResponse users from getting to their work. For more information, see "Upgrading RapidResponse with Service Updates" on page 152.

There are other cases where RapidResponse Server can stop unexpectedly. For example, an operating system or RapidResponse software crash can bring the system down. Unlike a system restart, a software crash could happen at a peak usage time and dramatically impact productivity.

A hardware failure, like a software crash, also brings down RapidResponse Server and the entire system. However, unlike a software crash, the system might not be recoverable until the hardware issue is resolved.

To help improve system availability, consider deploying the optional failover cluster configuration for your RapidResponse system. When a scheduled or unscheduled RapidResponse Server outage occurs, a second server (a standby) automatically takes over from the active server. The two servers share the same RapidResponse database.

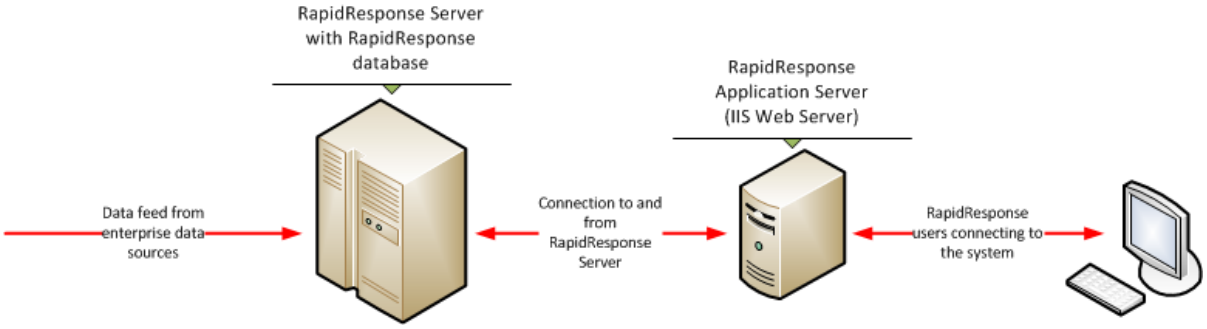
Failover clustering overview

RapidResponse Server failover clustering is an optional RapidResponse capability that is designed to improve system uptime (high-availability of the system) by allowing two computers to simultaneously run RapidResponse Server. The failover clustering capability does not rely on the Microsoft Cluster Server (MSCS) nor does it provide parallel computing power.

Network setup

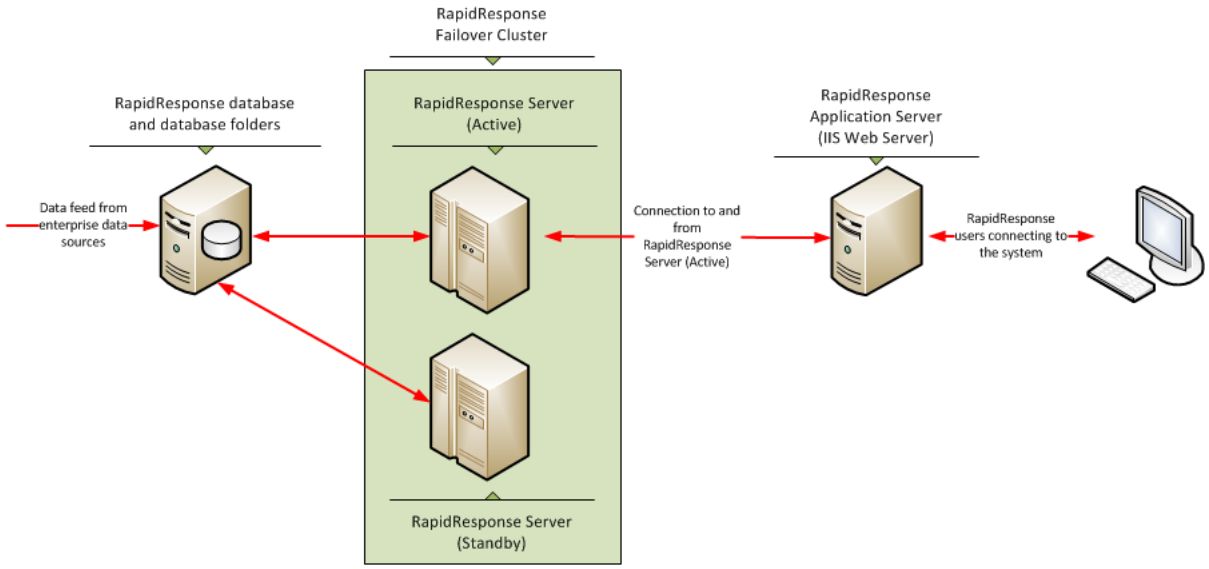
This section describes the failover clustering network setup.

The following illustration provides an example of a standard RapidResponse network set up without failover clustering.



This illustration provides a logically separated view of the RapidResponse network setup. Your RapidResponse set up might be different. For example, the RapidResponse database can be on a different drive from the RapidResponse program and executables. Or it might be located on a different computer or device in the same network. In addition, the RapidResponse Application Server might be installed on the same computer as the RapidResponse Server.

The following illustration shows an example of a RapidResponse network setup with failover clustering deployed.

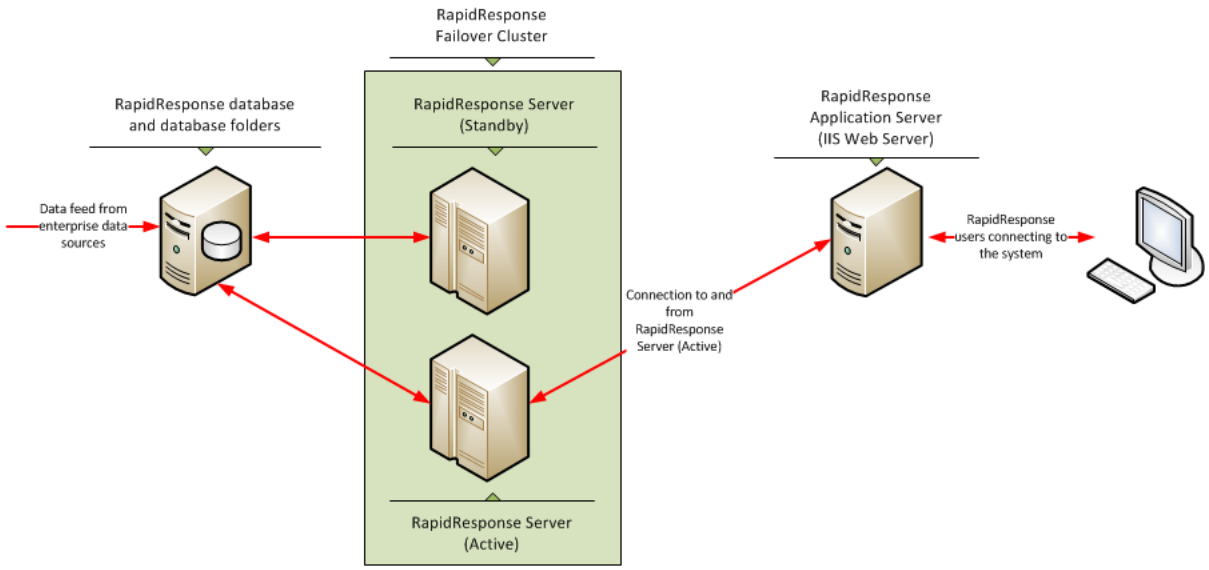


The illustration shows the two instances of RapidResponse Server sharing access to the RapidResponse database.

The RapidResponse Application Server communicates only with the active RapidResponse Server. The active server communicates with the RapidResponse database in a read-write mode. The standby server only communicates with the RapidResponse database in a read-only mode.

The standby server uses the same data as the active server and continually updates as the RapidResponse database is updated.

The following illustration is similar to the previous. Once again the RapidResponse Application Server communicates only with the active RapidResponse Server. In this case, the active and standby systems have switched.



Again, these diagrams provide a logically separated view of the RapidResponse network setup. Your setup can be different. For example, the data feed might come from a data integration server, which is configured to store data in the shared database location. The RapidResponse database and database folders might reside on the same computer that a RapidResponse Server instance resides on but on a separate drive from the RapidResponse programs. However, this type of setup takes away from the failover capabilities in the case of a hardware failure on the computer where both reside.

Note: Each RapidResponse Server instance also includes three other Windows services: RapidResponse Service Host, RapidResponse Utility Server, and RapidResponse Server Monitor. For more information about the RapidResponse Windows services, see "RapidResponse Server management" on page 227.

Failover processing

The RapidResponse failover clustering configuration requires two computers running RapidResponse Server. As long as RapidResponse Server is started on both computers in the failover cluster then RapidResponse failover process is operational.

When failover clustering is deployed, the active server is accessed by RapidResponse users who can perform read-write operations. The standby server cannot be accessed by the RapidResponse Application Server and RapidResponse users. The standby server continually updates as the RapidResponse database is updated. It runs with the latest data changes as they are written to the database.

The active RapidResponse Server can be stopped in several ways including:

- Manually stopped
- Automatically stopped with scripts or scheduled tasks.
- Software crashes (operating system or RapidResponse Server faults)
- Hardware crashes

When the active RapidResponse Server stops, the following occurs:

1. All active RapidResponse user sessions (and processes) are terminated. Unsaved data changes created by users are lost.
2. After a short time (usually less than a minute), the standby server becomes the active server. A message is sent to all RapidResponse system administrators informing them of the change. The message is available in Message Center. By default, the Master Administrator and system administrators have messages in RapidResponse Message Center automatically forwarded to their email accounts.
3. Once the new active server has completed loading any outstanding transactional data changes, it can be accessed by the RapidResponse Application Server. For more information about how the database handles transactions, see "Database files and operations" on page 311.

RapidResponse users can now sign into the system.

When a standby server starts, the following occurs:

1. A standby server starts by loading all of the data from the DFS folders in the Data folder (ignoring the XACT files).

2. At this point the standby server has reached the state that the primary server had at some point in the past.
3. The standby takes note of the last transaction ID that is reflected in the latest DFS.
4. The standby then authenticates itself, and subscribes to the transaction steam.
5. Upon opening the stream, it begins reading transactions. It ignores any transactions that are already included in the loaded DFS (when the transaction ID is less than or equal to the "last transaction ID").
6. Later transactions are processed into its own in-memory database.

In this way, the standby's in-memory database is continually updated to hold the same input data as the primary.

Note: Performing a full data import or applying data model changes can result in the restart of RapidResponse Server. In these two specific cases, failover server switching is turned off.

Restarting the former active server

To re-engage the RapidResponse failover system, the former active server must be restarted to become the standby server.

If the stopped RapidResponse Server was manually or automatically stopped, restart it.

If the RapidResponse Server was stopped or failed due to software or hardware issues, and auto-restart best practices are being followed, RapidResponse Server attempts to restart automatically following a one-minute delay, up to two times in a 24-hour period. If it shuts down a third time within this time period, RapidResponse Server does not automatically restart. If this occurs it is recommended that you investigate the problem before restarting RapidResponse Server. For more information about best practices and automatically restarting Windows services, see "Configuring the RapidResponse Server service" on page 233.

If your company has not set RapidResponse Server to automatically restart if the Windows service unexpectedly stops or fails then it should be manually restarted.

Note: If the RapidResponse Server service is not stopped normally (that is, a Stop command is not issued), then a Warning message is written to the **Server.log** file. Upon restart, RapidResponse closes the existing log file and creates a new file named **Server.*timestamp*.log** where the timestamp is in the **yymmdd-hhmmss** format. For more information about server logging in a failover cluster configuration, see "Failover and logging" on page 304.

System requirements for failover cluster

To set up the failover cluster, both computers should have the same performance characteristics. Characteristics can include memory, CPU, and disk access rates. If the computers are not similar then performance differences might be noticed by RapidResponse users. The RapidResponse system does not report specification or performance differences.

The two computers in the failover cluster need to be on the same network along with the computer hosting the RapidResponse database.

It is also recommended that the two computers use synchronized clocks to avoid ambiguity about timestamps when reviewing logs and other time-based tools.

Setting up the failover cluster configuration

Before setting up the failover cluster configuration, your enterprise systems should already be set up to send data files to your RapidResponse system. The data should also be validated to ensure RapidResponse calculations are similar to the results generated by your enterprise system. This is considered the initial RapidResponse data integration step.

Trying to set up the RapidResponse failover cluster before the initial data integration steps have been completed will slow down the data integration process.

This section describes the process of setting up the RapidResponse failover cluster.

License keys (Step 1)

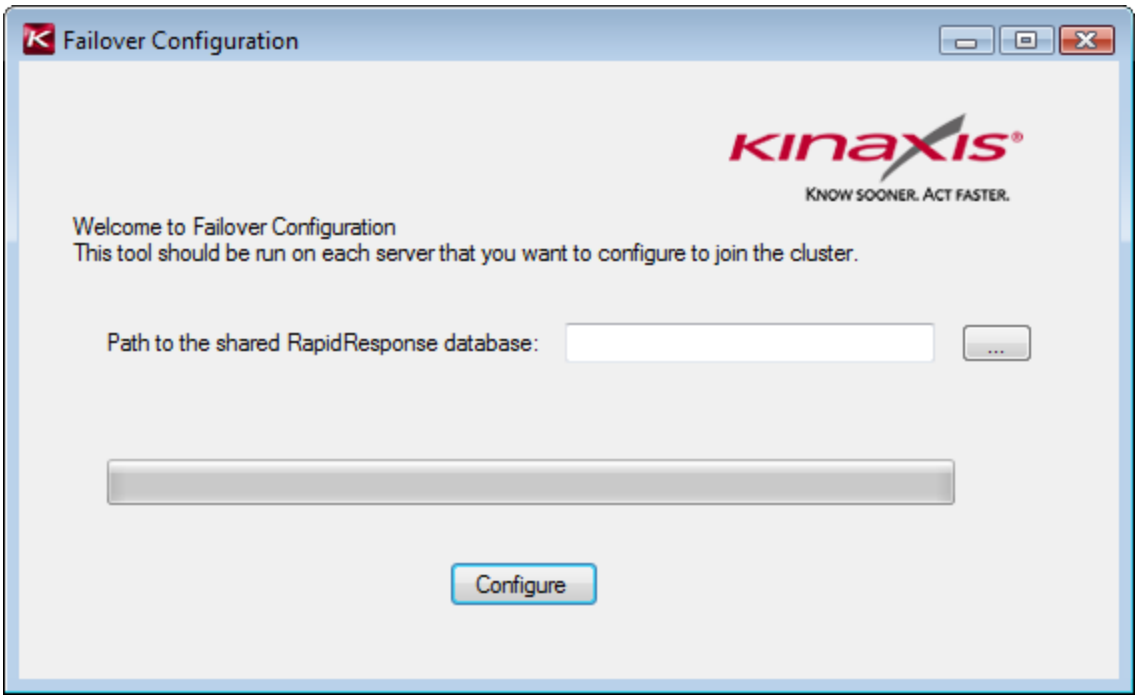
RapidResponse Server failover clustering is an optional capability. It requires license keys to enable it. Contact Kinaxis Customer Support for a new set of license keys for your current instance of the RapidResponse Server and for the second computer. For more information about installing license keys, see "Importing license keys" on page 273.

Stop RapidResponse Server and all data feeds (Step 2)

RapidResponse Server must be stopped. For more information, see "Starting and stopping RapidResponse services" on page 228. The enterprise data extraction programs and any other programs that send data to RapidResponse must also be stopped.

Copy the database folders to shared location (Step 3)

The database folders need to be moved to a location that both instances of the RapidResponse Server can access. The Failover Configuration program copies the database folders from the computer where RapidResponse Server is installed to the computer (or drive) where the shared RapidResponse database and database folders will reside. For more information about the database folders in a failover cluster, see "Database folders in a failover cluster" on page 299. The following image shows the Failover Configuration program.



1. On the computer where RapidResponse Server is installed, open the **C:\RapidResponse\Program** folder with Windows Explorer.
2. Double-click the **FailoverConfig.exe** file.
3. Click the **Browse** button (...) and navigate to the network location where the database and the database folders will reside.
4. Click **Configure**.
5. Click **Ok**.

After this program has completed, the database folders are copied to the specified location. The original database folders are renamed **obsolete.foldername**. The program also modifies the Windows registry and restarts RapidResponse Server when complete.

Notes:

- The RapidResponse Server service must have read-write access to the network location where the database folders resides. For example, the folders might reside on a SAN or NAS.
- The RapidResponse Server Monitor service must have network (read-write) access to the **ServerComm** folder. For more information about folders used in the configuration, see "Database folders in a failover cluster" on page 299. For more information about the Server Monitor service, see "Internal errors and system crashes" on page 244.

Reset the data extraction and data feeds (Step 4)

The data extraction programs can be restarted. However, the programs that send data to RapidResponse Server must be first modified to send data to the new database folder location. For more

information about the database folders in a failover cluster, see "Database folders in a failover cluster" on page 299.

Install RapidResponse Server on the second computer (Step 5)

RapidResponse Server is to be installed on the second computer in the failover cluster. When installing, use the same set of license keys provided by Kinaxis Customer Support. The second computer should have the same version of RapidResponse Server as the first computer (including service updates). The second computer does not require that the data feeds be enabled.

Second RapidResponse Server access to database (Step 6)

The second instance of RapidResponse Server needs to be configured to access the shared RapidResponse database and database folders.

1. Start RapidResponse Server. For more information, see "Starting and stopping RapidResponse services" on page 228.
2. Run the Failover Configuration program from the second computer where RapidResponse Server is installed. For more information, see "Copy the database folders to shared location (Step 3)" on page 294.
3. After the Failover Configuration program completed, the second instance of RapidResponse Server stops. Restart it to put it into failover mode. For more information, see "Starting and stopping RapidResponse services" on page 228.

RapidResponse Application Server configuration (Step 7)

The RapidResponse Application Server needs to be configured to access both instances of RapidResponse Server in the failover cluster. Upon completing the following steps, the Application Server is configured to only access the active RapidResponse Server.

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Open a Windows Command window on the computer where RapidResponse Application Server is installed.
2. Change the path to **C:\Program Files\Kinaxis\RapidResponse\WebConfig**.
3. Type the following command:

   ```
   WebConfig.exe RapidResponse -AdminPWD=<password> -
   server=machine1;machine2
   ```

   Where **password** is the RapidResponse password for the Master Administrator (Admin user) and **machine1** and **machine2** represent the full computer names of the RapidResponse Server installations.

The executable confirms that the two RapidResponse Server names are valid and are in the failover cluster. Running this command modifies the **web.config** file located in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder. The server element in the RapidResponse section includes the two full computer names. For example:

```
<RapidResponse>
     <server ipaddr="machine1;machine2 :14600"
</RapidResponse>
```

Note: RapidResponse Application Server can be installed on more than one Web server computer. Each instance can connect with a common RapidResponse Server. For example, you might want to install RapidResponse Application Server on a Web server computer for intranet users and on another Web server computer for Internet users. If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of RapidResponse Application Server is installed.

Modifying the system restart settings (Step 8)

A significant benefit of deploying the failover configuration is the potential reduction in system downtime.

Restarting RapidResponse Server requires that the RapidResponse database be reloaded. With large data sets, this sometimes results in the RapidResponse system being unavailable to users for an hour or more. This tends to be more problematic when RapidResponse is deployed globally and there are few daily time windows when the system is being used lightly.

The recommended best practice is to restart RapidResponse Server on at least a weekly basis. Restarting improves performance by releasing resources that are no longer being used from the system memory.

When the failover configuration is deployed, the restarting of RapidResponse Server does not result in significant system downtime. The following table provides an outline of the order of operations that are automatically followed when a RapidResponse Server restart is initiated.

	Server 1	Server 2
1	• Running as the Active Server.	• Running as the Standby Server.
2	• RapidResponse Server stops when Restart command issued. • All user sessions are terminated.	
3		• Automatically starts running as the Active Server. • Users can sign into system once database is reloaded.
4	• RapidResponse Server is restarted and database is loaded. • Starts running as the Standby Server.	

Consider reviewing when the Restart command is scheduled to run. Due to the reduction in system downtime, you might want to increase the frequency or change the schedule. For more information about scheduled system tasks, see "Commands and scheduling system tasks" on page 381.

Failover configuration and OpenAPI (Step 9)

If your RapidResponse system is using the RapidResponse OpenAPI, review this section. If not, it can be skipped.

RapidResponse OpenAPI is a set of registered Microsoft COM objects that are used to programmatically access RapidResponse Server and the RapidResponse database.

If you deploy the optional failover configuration, you might need to modify existing RapidResponse OpenAPI scripts. The **GetSession15** method now supports multiple RapidResponse Servers. The previous syntax was:

```
Object.GetSession15(ServerName)
```

Where **Object** was a valid Distribution object and **ServerName** was the name or IP address of the RapidResponse Server.

The syntax to use when deploying the failover configuration is:

```
Object.GetSession15(ServerName1; ServerName1)
```

The method attempts to create a session on the first specified server. If unsuccessful, it tries the second. Once the session is created, the method then determines which RapidResponse Server is considered active.

The following example shows how to set a Session object using the GetSession15 syntax with two RapidResponse Servers.

```
Set session= Dist.GetSession15("MyServer1;MyServer2")
```

If ports need to be specified the format for the previous example can be one of the following:

```
Set session= Dist.GetSession15("MyServer1:14600;MyServer2:14601")
Set session= Dist.GetSession15("MyServer1;MyServer2:14600")
```

Although RapidResponse continues to support the OpenAPI programming extensions (and server exits), they are no longer being promoted. It is not recommended that you extend the use of these tools. Consider alternatives to automate operations and customize processes including:

- RapidResponse Scripts—For more information, see the *RapidResponse Scripting Guide*.
- Workbook commands to modify data—For more information, see the *RapidResponse Resource Authoring Guide*.
- Forms to guide users through data entry or other tasks—For more information, see the *RapidResponse Resource Authoring Guide*.
- RapidResponse scheduled system tasks—For more information, see "Commands and scheduling system tasks" on page 381.

Failover configuration with folder paths (Step 10)

If you deploy the failover configuration, you might need to update the absolute folder paths used by three RapidResponse tools. The folder paths might need to point to the shared folder system in the failover cluster for the following:

- The Path field on ServerExit records. For more information, see "To register a server exit application" on page 346.
- The network locations for add-ins. For more information, see "Registering the add-in's network location" on page 638.
- If your company is using data publishing to send data to subscribers, a folder named **DataPublishRoot** is defined using a configuration record. You can modify the default location from the **File Locations** worksheet in the **RapidResponse Administration** workbook. To open this workbook, in the **Administration** pane, under **System Settings**, click **Configuration**. For more information, see "Moving data to the Data Transfer Client computer" on page 881.
- If your company is using data publishing to send data to subscribers, the folder where data is extracted to for each subscriber in a Data Publish setup. For more information, see "Moving data to the Data Transfer Client computer" on page 881.

Database folders in a failover cluster

When setting up the RapidResponse Server failover cluster, the Failover Configuration program moves database folders (and other supporting folders) to a location that both instances of the RapidResponse Server can access. The folders that are moved originally resided in the **C:\RapidResponse** folder on the computer where the original instance of RapidResponse Server was installed (this is the default configuration).

The following folders are shared and accessed by both RapidResponse Server instances in a failover cluster:

Folder name	Description
Data	Contains files that store the RapidResponse database. These files can be used for backing up and restoring the RapidResponse database. For information about data files, see "RapidResponse database content" on page 309.
Data Publish	In a RapidResponse-to-RapidResponse connection, contract manufacturers (publishers) publish relevant data from RapidResponse and send it to brand owners (subscribers). This folder is used in the process. For more information about data publishing, see "Setting up for data publishing for On-Premises" on page 871 and "RapidResponse-to-RapidResponse connection" on page 897.
Extract	Holds the data text files extracted from the enterprise data sources and Microsoft Excel files. This folder includes subfolders for each data source RapidResponse is expected to support. The subfolders are specified during the data integration process and the data extraction process creates new versions of the folders that hold the data source data. If you are using a data integration server, this folder holds the data text files extracted from your enterprise data sources and updated into the data integration server. Data to be updated on the planning server is stored in the NamedExtractSets folder. For more information, see the *RapidResponse Data Integration Guide*

Folder name	Description
History	Holds information about completed data imports and data updates. For more information, see the *RapidResponse Data Integration Guide*.
MessageQueue	Stores internal server messages used for coordinating RapidResponse Server operations.
NamedExtractSets	Used for moving data between RapidResponse instances. This folder is used for both full and net change extracts, and is used by the DataSynchronize process. For more information, see "DataSynchronize command" on page 393. If you are using a data integration server, this folder is used for making data extracted from the data integration server available to a planning server. For more information, see the *RapidResponse Data Integration Guide*. Also used in the RapidResponse web services net change data update process. For more information, see the *RapidResponse Web Services Guide*.
Packages	Stores two different types of archive files (or packages) that use the PKG file extension. This folder stores back up copies of the RapidResponse database. For more information about creating and using these packages, see "Backing up and restoring the RapidResponse database" on page 315. This folder also stores the diagnostic files created by RapidResponse Server Monitor after RapidResponse Server generates an internal error or crashes. For more information, see "Internal errors and system crashes" on page 244. The default location for these types of files can be changed to improve performance. For more information, see "Improve performance by moving default subfolders" on page 251.
ServerExits	Storage location for server exit applications. For more information, see "Server exit applications" on page 343.
ServerComm	This folder stores the files used to synchronize the RapidResponse Servers in a cluster. For more information, see "ServerComm folder" on page 303. The RapidResponse Server Monitor service must have network (read-write) access to the **ServerComm** folder. For more information about the Server Monitor service, see "Internal errors and system crashes" on page 244. **Note:** This folder is only used if a RapidResponse Server failover cluster has been implemented.

The following folders are located on both instances of RapidResponse Server:

- Configuration
- Docs
- Dumps
- Logs

  Both instances of RapidResponse Server in a failover configuration create their own text-based log files including **Server.log**. For more information about these files, see "RapidResponse text-based log files" on page 462. Also see "Failover and logging" on page 304.
- Persistence-RuleBased
- Program
- Schema
- Temp
- Upgrade Logs
- Working

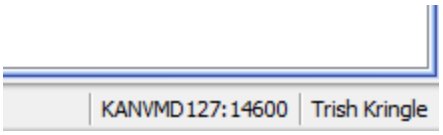
For more information about the RapidResponse folder structure when not using a failover cluster, see "RapidResponse Server folder structure" on page 249.

Determining which server is active

RapidResponse administrators and users cannot sign in to a RapidResponse Server when it is in standby mode.

Administrators have options to determine if the RapidResponse failover cluster is operational, and the active and standby status of the RapidResponse Server instances.

The easiest way to determine the name of the active RapidResponse Server is to review the status bar in the RapidResponse client. It shows the name of the signed in user and the RapidResponse Server the client is accessing, as shown in the following image.

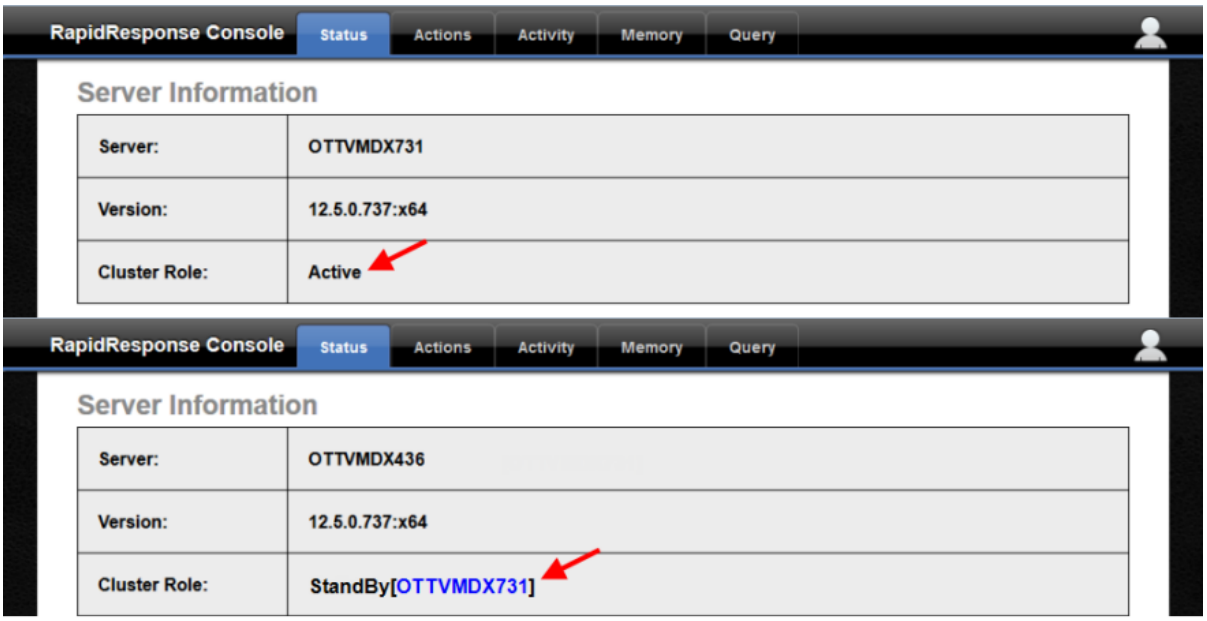


However, this does not confirm whether the second instance of RapidResponse Server is actually in standby mode and not stopped. For information about customizing the status bar, see "Configuring status bar identification text" on page 632.

You have three options to determine the status of the active and standby RapidResponse Servers.

Determine Server status using RapidResponse Console

System administrators can use the RapidResponse Console to determine the status of a RapidResponse Server. If failover clustering has been enabled, the Status page in the Console indicates whether the RapidResponse Server you are signed in to is in active or standby mode.



If in standby mode, you can click the hyperlink to open the RapidResponse Console for the active RapidResponse Server.

For information about signing in to RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

Run a query in RapidResponse Console

The **Query** page in the RapidResponse Console can be used to run queries against the RapidResponse database. You can run a query (read-only) that returns the status of both RapidResponse Servers in the failover cluster.

The query to submit is as follows:

```
Clusterinfo {machinename, effrole, isself}
```

The query returns the status of the two RapidResponse Servers in the failover cluster. The following image includes query results that show active and standby modes.

In the previous example, it shows one server is active and the other is in standby mode (the **effrole** column). The **isself** column indicates which RapidResponse Server instance the RapidResponse Console is using. The following example shows that one server is in active mode and the other server has stopped (expired).

For more information about queries and RapidResponse Console, see "Manually running queries against the database" on page 244.

ServerComm folder

The servers in a failover cluster will share access to certain file system folders. A key one is the ServerComm folder. Among other things, it provides a location for servers to tell each other their names.

When starting, a server uses the files in ServerComm, as well as direct communication to the other server via UDP, to decide which server will be the primary server and which will be the standby. Once a server has become the primary, it establishes a pair of http endpoints. One is used by any aspiring standby server to authenticate that it has the required permissions. The second endpoint provides a stream of transactions.

The ServerComm folder resides in the RapidResponse database folder set. This folder stores the files used to synchronize the RapidResponse Servers in a cluster. Included in this folder are two files with the following names:

- Server-*machine1*.xml
- Server-*machine2*.xml

The *machine* represents the computer name of a RapidResponse Server in the failover cluster.

Each file includes a role element which can be reviewed to determine which server is active. For example, the files might contain one of the following lines:

- `<Role>Active</Role>`
- `<Role>Standby</Role>`

The RapidResponse Server Monitor service must have network (read-write) access to the **ServerComm** folder. For more information, see "Database folders in a failover cluster" on page 299. For more information about the Server Monitor service, see "Internal errors and system crashes" on page 244.

Note: The actual inter-server communication is done via UDP datagrams. The files in ServerComm are duplicates of this information, provided primarily for diagnostic purposes.

Managing servers in a failover cluster configuration

Managing the RapidResponse Server instances in a failover cluster configuration is not very different than managing a single instance. However, there are some administration tasks that impact the overall system that administrators need to understand.

Server management task	Description and impact
Starting a RapidResponse Server instance	When a RapidResponse Server in the cluster is restarted, it tests whether the other server is running. If another server is running, it goes into standby mode. If not, it becomes the active server.
Stop the RapidResponse Server standby instance	From the standby computer, follow the standard procedure to stop RapidResponse Server as described "Starting and stopping RapidResponse services" on page 228. If the standby RapidResponse Server instance is stopped then the entire RapidResponse system will stop if the active RapidResponse Server instance stops.
Stop the RapidResponse Server active instance	From the active computer, follow the standard procedure to stop RapidResponse Server as described "Starting and stopping RapidResponse services" on page 228. After a short time (usually less than a minute), the standby RapidResponse Server instance is becomes the active instance.
Monitoring responsiveness of RapidResponse system	A failover is not triggered if the active RapidResponse Server becomes unresponsive but does not stop (or crash). If your company is monitoring the RapidResponse system availability using an end-to-end test then system administrators might be alerted that the active server is unresponsive. If alerted, they can manually trigger the failover by stopping the active non-responsive server. For more information about monitoring the RapidResponse system, see "Monitoring RapidResponse system availability" on page 307.

Failover and logging

RapidResponse Server uses several text-based logs files to track system diagnostics information including **Server.log** and **QueryHistory.log**. For more information about the log files, see "RapidResponse text-based log files" on page 462.

All log files are stored in the **C:\RapidResponse\Logs** folder on the same computer as the RapidResponse Server program files. The **Logs** folder location cannot be customized; that is, the **Logs** folder can only be a subfolder to the main RapidResponse folder.

If your company has deployed the failover cluster configuration, the **Logs** folder on both RapidResponse Server systems might need to be reviewed.

System and data import status messages are written to the **Server.log** file. Messages about failover cluster status messages are also written including transition messages. For example, when a server

transitions from standby to active, a message is written. However, the messages do not distinguish between scheduled failover and an unscheduled failover.

If you are diagnosing RapidResponse system issues with Kinaxis Customer Support representatives, it is likely they will request log file packages. RapidResponse includes a system utility that generates exactly the information Customer Support representatives require from RapidResponse Server and RapidResponse Application Server logs. If your company has deployed the failover cluster configuration, the utility generates the file using the log files from only the active server. For more information about the utility, see "To manually generate log file packages" on page 242.

RapidResponse includes other diagnostic tools that use the RapidResponse Server log files. These tools also use the log files from the active server. For more information, see "Diagnostic files" on page 245.

Applying Service Updates and upgrading

To apply Service Updates, the RapidResponse Server must be stopped and RapidResponse users are prevented from signing into the system. By deploying the failover cluster configuration, you can reduce the amount of system downtime and maintain a high level of user uptime during the Service Update process.

The following table provides an outline of the order of operations that should be followed when applying most Service Updates. The items marked with **ACTION** are steps that need to be executed by system administrators.

	Server 1	Server 2
1	• Running as the Active Server.	• Running as the Standby Server.
2		• **ACTION**: Stop RapidResponse Server.
3		• **ACTION**: Apply the Service Update to all components.
4		• **ACTION**: Start RapidResponse Server. • Running as the Standby Server. • Loads RapidResponse database after confirming compatibility.
5	• **ACTION**: Stop RapidResponse Server.	
6		• Starts running as the Active Server.
7	• **ACTION**: Apply the Service Update to all components.	
8	• **ACTION**: Start RapidResponse Server. • Starts running as the Standby Server. • Loads RapidResponse database after confirming compatibility.	

For more information about applying Service Updates to RapidResponse components, see "Upgrading RapidResponse with Service Updates" on page 152.

The process for upgrading RapidResponse Server is somewhat different than the process for applying Service Updates.

Both instances of RapidResponse Server in a failover cluster configuration need to access the same database. The active server accesses the database in read-write mode and the standby server in read-only mode. As the RapidResponse Server upgrade process changes the database structure, both instances of RapidResponse Server cannot run at the same time if only one instance has been upgraded. In addition to upgrading RapidResponse Server, you must upgrade the application supplemental components and RapidResponse Application Server. For more information, see "RapidResponse upgrade process overview" on page 141

To reduce system downtime, a strict order of operations should be followed when upgrading RapidResponse Server.

Note: Some Service Updates, like upgrades, also change the database structure. The notes supplied with Service Updates indicate whether the database structure changes.

	Server 1	Server 2
1	• Running as the Active Server.	• Running as the Standby Server.
2		• **ACTION**: Stop RapidResponse Server.
3		• **ACTION**: Upgrade RapidResponse components (or apply the Service Update). Upgrade process cannot upgrade database because standby instance has read-only permissions.
4		• Upgrade process attempts to start RapidResponse Server standby instance. • RapidResponse Server does not start because the database is not compatible with the new RapidResponse Server application that has been upgraded. • Only Server 1 is running as the active RapidResponse Server.
5	• **ACTION**: Stop RapidResponse Server. **Note:** Both RapidResponse Servers stopped and users cannot access the system.	
6	• **ACTION**: Upgrade RapidResponse components (or apply the Service Update). • The RapidResponse Server application and the database are upgraded.	
7	• **ACTION**: Start RapidResponse Server. • Loads RapidResponse database. • Running as the Active Server.	
8		• **ACTION**: Start RapidResponse Server. • Loads RapidResponse database after confirming compatibility. • Running as the Standby Server.

CHAPTER 25: Monitoring RapidResponse system availability

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Running the end-to-end test 307

You can test your RapidResponse instance to determine if it is accessible, using the end-to-end test. The end-to-end test attempts to sign in to RapidResponse and optionally, perform a query. If the sign in is successful, the test returns a success message, indicating that RapidResponse is available for users to sign in.

If the end-to-end test is successful and a query is performed, the time required to perform the test query can also be returned. An available server with poor timing numbers could indicate the server is busy or is running a resource-intensive process. In this case, users should not sign in until the process has completed.

Running the end-to-end test

The end-to-end test is an HTTP request that, by default, attempts to sign in to RapidResponse and execute a query. If the sign in and the query are successful, the end-to-end test returns a success message and the time required to sign in and perform the query, both in milliseconds.

You can perform the end-to-end test either in a web browser or using a web service, depending on your requirements. For example, you might run the end-to-end test request by typing the HTTP request or clicking a link in your web browser to determine if you can sign in. You might run the end-to-end test using an HTTP client to automatically send notifications to users if RapidResponse is either not available or if a resource-intensive process is running.

This section discusses the HTTP request that performs the end-to-end test and its parameters.

Depending on how you want to use the end-to-end test, you can optionally not perform the query, or you can optionally not return the timing information. You specify the options as HTTP query parameters on the request that performs the end-to-end test.

Parameter	Description
mode	Specifies how the sign in test is performed. whether a query is performed after the end-to-end test signs in to RapidResponse. Valid values are: • 0—The end-to-end test attempts to sign in, perform a query, and then sign out. • 1—The end-to-end test first determines whether RapidResponse is accepting sign ins. If sign in is not allowed, reports success. Otherwise, attempts to sign in and perform the query.
nostats	Specifies whether the returned message contains timing information. If this parameter is provided, only the status is reported. Otherwise, the status and times required to sign in and perform the query are reported

The end-to-end test returns an HTTP code 200 (OK) if the end-to-end test can access RapidResponse. Depending on the specified `mode`, the success code is returned if the test can sign in to RapidResponse successfully and perform the query, or if it can connect but is not allowed to sign in.

If the end-to-end test cannot sign in or cannot access RapidResponse (depending on the `mode`), it returns an HTTP code 500 (Server Error). The end-to-end test has a 180 second timeout, and if the time is exceeded, error 500 is returned and the end-to-end test fails. For more information about HTTP codes, visit http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html.

To run the end-to-end test, perform the following HTTP GET request to the computer the RapidResponse Application Server is installed on:

```
http://host/RapidResponse/EndToEndTest.ashx
```

where `host` is the computer RapidResponse Application Server is installed on.

To specify parameters for the end-to-end test, add an HTTP query string to the request. The query string is denoted with a question mark (?), and specifies values for the query parameters, separated by ampersands (&). For example,

```
http://host/RapidResponse/EndToEndTest.ashx?mode=1&nostats
```

This request signs in to RapidResponse, reports success even if sign-in is not available, and returns only the success message.

CHAPTER 26: Managing the RapidResponse database

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

RapidResponse database content 309
Location of stored database files 310
Database files and operations 311
Disk space warnings 314
Backing up RapidResponse program files 314
Backing up and restoring the RapidResponse database 315
Rolling back the RapidResponse database 318
Archiving the RapidResponse database files 324
RapidResponse database integrity 327

As a RapidResponse administrator, you might be responsible for managing the RapidResponse database files. These files store RapidResponse data and resources and should not be confused with data text files or Microsoft Excel files that are imported into RapidResponse. For information about importing and updating data, see the *RapidResponse Data Integration Guide*.

This chapter describes the RapidResponse database files and provides instructions about moving data from memory into permanent files. It also discusses how to verify the integrity of the RapidResponse database and provides instructions on backing up the RapidResponse database and program files.

RapidResponse database content

The RapidResponse database is loaded in-memory. It is also stored, or backed up, to disk and is loaded when the RapidResponse Server service starts. The following table describes the data stored in the RapidResponse database files.

Item	Description
Imported data	Data imported from your enterprise data sources (which can include customer and supplier data). During each data update the database is modified.
Data modifications	Includes records that have been inserted, deleted, or modified by users or automated processes.

Item	Description
Scenarios	A scenario is stored in the RapidResponse database as a single record and not a complete duplicate of its parent scenario in terms of records and size. Changing a record in a scenario results in a single record being added to the RapidResponse database. For more information about how scenarios are stored, see "Scenario memory consumption" on page 270.
System records	System tables hold information used internally by RapidResponse, such as user information, system settings, or any other information that is not directly used in calculations or imported from an enterprise system.
Resource definitions	Dashboard, workbook, filter, and other resource definitions, along with Message Center messages are stored in the database.

Location of stored database files

During the RapidResponse Server installation process, the storage location of the RapidResponse database files is specified. The default location is the **C:\RapidResponse\Data** folder. The executables folder must reside on an internal disk. The **Data** folder, however, can reside in a variety of locations or hardware configurations including:

- Same internal hard disk as the executables folder
- On a hard disk separate from the executables folder
- SAN (storage area network)
- NAS (network attached storage)

Notes:

- The RapidResponse Server service must have read-write access to the network location where the **Data** folder resides. For example, the **Data** folder might reside on a SAN or NAS.
- If your company has deployed the optional RapidResponse failover cluster configuration, the location of the stored database files are shared between both instances of RapidResponse Server. For more information, see "RapidResponse Server failover clustering" on page 289.

Hardware and operation responsiveness

The speed of some RapidResponse Server operations that use the stored database files (for example, starting) is affected by the performance of the deployed storage hardware. Kinaxis has tested three RapidResponse Server operations against disks of varying performance levels to determine whether deploying faster hardware improves operational performance. The following table summarizes the results.

Server Operations	Performance notes
Starting RapidResponse Server service and loading the stored database files. For more information, see "Starting and stopping RapidResponse services" on page 228.	Deploying a faster hard disk does not improve performance.
Creating an archive, or package, of the RapidResponse database files. For more information, see "CreateDataPackage command" on page 388.	Deploying a faster hard disk does not significantly improve performance.
Generating dump and complete diagnostics package files. For more information, see " Automatic deletion of system records" on page 277.	Deploying a faster hard disk can significantly improve performance. Consider deploying a high-performance hard disk if you often generate diagnostic package files.

Note: You might not experience similar performance improvements due to other hardware or network differences.

Selecting storage locations for operations

During the installation of RapidResponse Server, the **Data** folder is created based on information supplied by the person installing RapidResponse. The default location is **C:\RapidResponse\Data**.

After the installation, you can change the storage location of the **Data** folder by modifying a Windows registry setting. For more information, see "DataBackUpWindowMinutes" on page 352. If your company has deployed the optional RapidResponse Server failover configuration, you cannot use this setting. For more information, see "RapidResponse Server failover clustering" on page 289.

Additionally, during the installation of RapidResponse Server, storage folders for dump and diagnostic package files are also created. These folders are parallel to the **Data** folder. For example, **C:\RapidResponse\Dumps** and **C:\RapidResponse\Packages.**

These storage locations can also be changed using Windows registry settings. In fact, by having the diagnostic package files folder on a drive or device separate from the **Data** folder, you can improve RapidResponse Server restart time. For more information about changing the drive and folder, see "PkgDirectory" on page 364 and "DumpDirectory" on page 363.

Database files and operations

The RapidResponse database is loaded in-memory when the RapidResponse Server is started. The stored RapidResponse database includes, at minimum, an XACT file and a DFS folder.

XACT files

As users or automated processes (for example, scheduled tasks) modify data or resources, the changes are stored in-memory. The changes are also written to transactional database files named XACT. This helps to maintain system performance and makes the changes available for recovery in case of system failure.

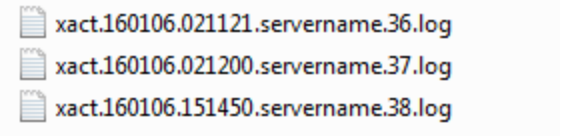
The XACT files are stored in the **C:\RapidResponse\Data** folder (default location). The data changes are subsequently written to the RapidResponse database by a RapidResponse Server command named **Capture**.

Transactional data can be broken into multiple files so multiple XACT files can exist and each file is named **xact.*timestamp.servername*.sequence.log**. For example:

```
xact.160114.021121.server1792.36.log
```

The timestamp indicates when the file was created.

The following is an example of three transaction files created over three days.



The XACT file with the latest timestamp is considered the active transaction file. Each transaction data file contains the full set of transactions that have been executed between the time it was created and the time it was closed. The transaction data files that are not active cannot accept changes.

Running the **Snapshot** command closes the active transaction data file. A new active file is then created. Once the transaction data files are written to the RapidResponse database, the files are deleted and a new active transaction data file is created.

The use of multiple transaction data files is integral to a disaster recovery strategy. For more information, see "Snapshot command" on page 409.

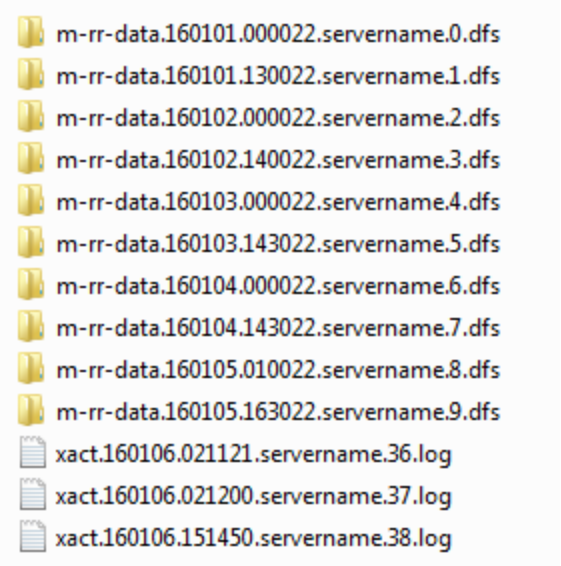
Note: If the total size of the transaction data files (XACT files) exceeds 1 GB, the Capture command automatically runs and a new active transaction data file is created.

DFS folders

Other than the transactional data in the XACT files, RapidResponse data is stored in DFS folders in the **C:\RapidResponse\Data** folder (default location). The RapidResponse database includes one or more DFS folders. The folders are named **m-rr- data.*timestamp.ServerName*.sequence.dfs**. For example:

m-rr-data.160101.000022.servername.0.dfs

The oldest DFS folder is the main folder in the series, or hive. The main (first) folder embodies a complete copy of the RapidResponse database at the exact time of the timestamp. In the following example, the first folder listed is the main hive folder.



Additional DFS folders might exist and are considered 'hive fragments'. These have timestamps and names that are later than the main hive folder. These DFS folders make up an ordered series of transactional data changes. When considered as a whole, the DFS folders are the complete database as of the timestamp of the latest DFS folder.

Once DFS folders have been created, they are never written to again. All transactions contributing to a given DFS file were executed before the timestamp in the folder name.

A new hive fragment DFS folder (not the main DFS folder) is created when transactional data changes (XACT files) are applied to the RapidResponse database by the Capture command. When run, it forces a Snapshot command, applies the transactional data from the XACT files to a new DFS hive folder, and deletes all the processed XACT files. A new active transaction file is then created (**xact.*timestamp.servername*.sequence.log**).

As of RapidResponse 2016.2 Service Update 7, new DFS segments can also be created when you make data model changes. This is a change from the previous behavior, where a data model change copied the entire database into memory so the new data model can be applied when the server restarts. Now, changes such as adding fields to tables or adding tables can be applied as a new DFS segment, which copies only the changes into memory, and can improve performance on server start up. However, not all data model changes can make use of this behavior. For example, adding key fields to a table still requires a full database copy to ensure the proper data is represented in the database after the server restarts.

The RapidResponse Server command Condense creates a new main database folder by combining all the DFS folders in the hive. When run, it forces a Capture command. After the condense operation completes, the earlier hive fragment DFS folders are deleted and the new main DFS folder contains the complete database as of the time the operation began.

For more information, see "Capture command" on page 385 and "Condense command" on page 387.

Note: You might notice TMP files in the Data folder. These files are transient and are created by the Capture and Condense command operations. During normal operations, these files are automatically renamed with a DFS extension. In case of a system crash, the TMP files can be safely deleted without any risk of corruption or data-loss.

Disk space warnings

RapidResponse warns systems administrators when available disk space, where the RapidResponse database is stored, falls below a specified threshold.

The threshold is calculated as the size of the main RapidResponse database folder multiplied by the number specified by a RapidResponse system administrator. For example, if the main database folder is 12 GB and the number is set to 3, a warning is generated if the free disk space is less than 36 GB.

The warning is sent as an email message to system administrators and is also written to the **Server.log** file. For more information about the log file, see " Server.log file" on page 464.

The RapidResponse Server tests the disk space every 10 minutes.

> **Tip:** If you often receive disk space warnings, consider running the Condense command more frequently. For more information, see "Condense command" on page 387.

▸To change the disk space threshold warning

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Database** category.
3. In the **Disk space threshold warning** box, type a number. This number is multiplied by the size of the main RapidResponse database folder.

   The default setting is 2.

Backing up RapidResponse program files

As part of the regular RapidResponse maintenance, a RapidResponse system administrator should regularly back up the RapidResponse program and configuration files to restore the system in the event of a system failure. The back up process for the RapidResponse Server program files and the RapidResponse Application Server configuration files can be automated through batch or script files. For information about backing up the RapidResponse database, see "Backing up and restoring the RapidResponse database" on page 315.

Backing up RapidResponse Server files

As part of the regular RapidResponse maintenance, an administrator should regularly back up the RapidResponse Server program files and raw data files (text or Microsoft Excel files). To create a backup of the RapidResponse Server files, create a copy of the **C:\RapidResponse** folder excluding the **C:\RapidResponse\Data** subfolder.

Backing up Application Server configuration files

As part of the regular RapidResponse maintenance, an administrator should regularly back up the following RapidResponse Application Server configuration files. The files to back up are in XML format, and multiple XML files might exist in the following folders.

In case of system failure, these files can be restored to return RapidResponse Application Server to its previous state.

- C:\Program Files\Kinaxis\RapidResponse\Web\Web.config (file)
- C:\Program Files\Kinaxis\RapidResponse\Web\en\common\config
- C:\Program Files\Kinaxis\RapidResponse\Web\en\config\Client
- C:\Program Files\Kinaxis\RapidResponse\Web\en\config\Client\extensions
- C:\Program Files\Kinaxis\RapidResponse\Web\en\config\extensions
- C:\Program Files\Kinaxis\RapidResponse\Web\en\config\ecaanalysis

Note: If your company has installed RapidResponse Application Server on more than one computer (for example, Internet and intranet deployment), then you should back up each instance of the program files.

Backing up and restoring the RapidResponse database

To back up data against the occurrence of a system failure (for example, disk crash or power failure), you need to regularly store backup copies of the RapidResponse database.

RapidResponse includes the CreateBackup scheduled task which runs the RapidResponse CreateDataPackage command. This command creates an archive, or data package, of the RapidResponse database in the **C:\RapidResponse\Packages** folder. A system administrator should schedule the **CreateBackup** task to run at a regular interval. For more information, see "To create or modify a RapidResponse scheduled task" on page 416.

The default folder where data packages are stored can be modified with a command argument or by changing a Windows registry setting. For more information about the command, see "CreateDataPackage command" on page 388. For more information about the Windows registry setting, see "Packages" on page 359.

Data packages can also be used to move data and configuration settings from a test server to a production server.

Note: Some RapidResponse operations performed in an unintended manner can lead to data loss or a corrupted RapidResponse database. System operations or processes can result in your system becoming unresponsive or unable to start. In this case, you might want to roll back your RapidResponse database to an earlier point in time to resolve your data or system issues. Ideally, this can be done with a minimum loss of data. This can also be a key to your disaster recovery strategy. For more information, see "Rolling back the RapidResponse database" on page 318.

Manually creating a data package

Three options are available to manually create a RapidResponse data package. You might want to do this if you are moving data from a test server to a production server or you need to send a data package

to Kinaxis Customer Support.

- Running the CreateDataPackage command from the Scheduled task page. The command can be run by system or data administrators.
- Running the RapidResponse System Utilities. This dialog box is only available to RapidResponse system administrators.
- Running the RapidResponse Console. You do not need to have the RapidResponse client running to use this method. However, only a RapidResponse system administrator can use this method.

Like the CreateBackup scheduled task, all three methods for manually creating a data package save the package in the **C:\RapidResponse\Packages** folder on the computer where RapidResponse Server is installed and use the name **Backup_*servername*_*timestamp*.pkg**.

Note: During a Create Data Package operation, signed in RapidResponse users might experience a temporary performance slowdown.

▸To manually create a data package with a command

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. In the Scheduled System Tasks worksheet, click anywhere in a row that contains **CreateDataPackage** in the **Command** column.
3. Click **Run Task Now**.
4. Click **Yes** to confirm you want to run the task.

▸To manually create a data package with the RapidResponse utility

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. In the **Data Package** section, click **Data Package**.
3. Click **OK** after confirming the package's creation.

Note: The System Utilities dialog box is only available to system administrators.

▸To manually create a data package using RapidResponse Console

1. Sign into RapidResponse Console. For more information, see "To sign in to RapidResponse Console" on page 230.
2. Click the **Actions** menu.
3. Click **Create Data Package**.
4. Click **Create Data Package** again.

   After the data package is created a **Results** dialog box is displayed which indicates data package statistics, and file size and location.

Managing saved data packages

The CreateBackup schedule task that creates data packages is scheduled, by default, to run every day. Creating a backup package daily could use a significant portion of hard disk space on the

RapidResponse Server computer. Without enough free disk space, RapidResponse Server functions such as database collapsing might not properly execute. As such, it is important to manage the number of data packages saved to ensure they do not consume all the free disk space.

RapidResponse includes the Prune Backup Packages scheduled task to help manage the number of data packages. By default, this task is scheduled to run each day and it deletes all saved data packages except for the two most recently created.

For more information about this scheduled task, see "Prune Backup Packages" on page 383.

Restoring data packages

Administrators might need to restore data packages due to system failure or to move data and configuration settings from one RapidResponse system to another (for example, test system to a production system).

Caution: Ensure that when you restore a data package that it was created using a RapidResponse system that uses the same version as the system where the package is being restored. For example, you cannot create a data package using RapidResponse 2015.3 and restore it on a RapidResponse 2016.2 system. In addition, the system that creates the data package and the system that loads the data package must have the same service updates applied. You should also be aware that you might not receive an error if you attempt to restore data package that was created on a system that used a different RapidResponse version.

▸To restore a RapidResponse data package

The first two steps apply to the computer where the data package will be loaded.

1. Ensure RapidResponse Server is stopped on the computer. For more information, see "To stop other RapidResponse Server services" on page 232.
2. Delete all contents of the **C:\RapidResponse\Data** folder.
3. On the computer where the backup package was created, navigate to the folder or location where the **CreateDataPackage** command saved the backup package. By default, this is **C:\RapidResponse\Packages**. Copy the backup package file.
4. Paste the backup package file into the **C:\RapidResponse\Data** folder on the computer where the data package will be loaded.
5. Restart RapidResponse Server.

   After decompressing the backup data package, RapidResponse Server uses the backed up data package.

6. Sign into RapidResponse as the Master Administrator (Admin user).
7. If the restored the data package was created on another computer (for example, a test system), you must import the RapidResponse license keys. The license keys are only compatible with a specific computer based on the computer's server ID. For more information, see "Importing license keys" on page 273.

Note: Restoring a data package also loads selected files and folders into the **C:\RapidResponse\History** folder to ensure the integrity of the database logs is maintained.

▸To decompress a RapidResponse data package

1. Open a Windows Command Window on the computer where RapidResponse Server is installed.
2. Navigate to the **C:\RapidResponse\Packages** folder.
3. Specify the decompression command using the following syntax:
   `wpzip PackageName.pkg`

   where **PackageName.pkg** is the name of the compressed package.

Rolling back the RapidResponse database

As a RapidResponse system administrator (On-Premises), you might be responsible for the RapidResponse database. You might also be responsible for the entire system.

Some RapidResponse operations performed in an unintended manner can lead to data loss or a corrupted RapidResponse database. System operations or processes can result in your system becoming unresponsive or unable to start.

By rolling back or restoring your RapidResponse database to an earlier point in time, you might be able to resolve your data or system issues. Ideally, this can be done with a minimum loss of data. This can also be a key to your disaster recovery strategy.

This section demonstrates a variety of use cases and the steps or processes to roll back your database while minimizing data loss. The following use cases are discussed:

- "Customizing the data model resulted in data loss" on page 319
- "RapidResponse Server cannot start due to corrupted data" on page 320
- "Operations made unintended changes – restore using the database folders" on page 322
- "Operations made unintended changes – restore using a data package" on page 323

Before reviewing this section, ensure you understand how the RapidResponse database files are organized and managed. For more information, see "Database files and operations" on page 311. The second and third use cases require this information.

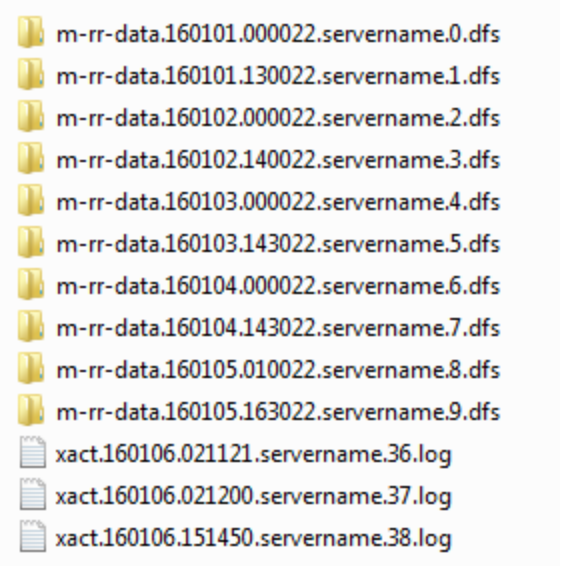
As a reminder, the RapidResponse database is stored in the **C:\RapidResponse\Data** folder. The RapidResponse database includes one or more DFS folders. The folders are named **m-rr-data.*timestamp.ServerName*.sequence.dfs**. For example:

m-rr-data.160101.000022.servername.0.dfs

The timestamp uses the following format:

yymmdd.hhmmss

The oldest DFS folder is the main folder in the series, or hive. The main folder embodies a complete copy of the RapidResponse database at the exact time of the timestamp. In the following example, the first folder listed is the main hive folder.



Additional DFS folders might exist and are considered 'hive fragments' and have timestamps and names that are later than the main hive folder. These DFS folders make up an ordered series of transactional data changes. When considered as a whole, the DFS folders are the complete database as of the timestamp of the latest DFS folder. Once DFS folders have been created, they are never written to again.

The XACT files contain RapidResponse transaction data. As users or automated processes (for example, scheduled tasks) modify data or resources, the changes are stored in-memory and in XACT transactional data files. The transactional data changes are subsequently written to a new RapidResponse database fragment (DFS hive folder) by a RapidResponse Server command named **Capture**. For more information about this command, see "Capture command" on page 385.

If you have turned on the archiving of database files, consider using them as part of the rollback process. For more information, see "Archiving the RapidResponse database files" on page 324.

Customizing the data model resulted in data loss

Applying changes to your data model can inadvertently result in data loss. For example, if you delete tables or fields from the data model then the data stored in these fields is also deleted. In cases where data is deleted from a table that is referenced from another table, if the reference is not nullable, data will be deleted from both tables. This is often unexpected.

As a system administrator, you can roll back (restore) your RapidResponse system to its state before the data model changes were applied.

Immediately before applying data model changes to the database, RapidResponse saves a copy of the RapidResponse database. The RapidResponse database stores data and configuration settings including the data model.

The database is saved in a data package file named **PreTransform_*ServerName-timestamp*.pkg** or **PreTransform_*ServerName-timestamp*.zip** in the **C:\RapidResponse\Packages** folder (default setting). The date and time specified in the file name is based on the local time on the RapidResponse Server.

▸To restore a RapidResponse data package

The first two steps apply to the computer where the data package will be loaded.

1. Ensure RapidResponse Server is stopped.
2. Delete the contents of the **C:\RapidResponse\Data** folder.
3. Navigate to the folder or location where RapidResponse data packages are saved. By default, packages are stored in the **C:\RapidResponse\Packages** folder. Copy the **PreTransform** package file.
4. Paste the **PreTransform** package file into the **C:\RapidResponse\Data** folder on the computer where RapidResponse Server is stopped.
5. Restart RapidResponse Server.

   RapidResponse Server loads the data package after automatically decompressing it.

For information about customizing the data model, see the *RapidResponse Data Integration Guide*.

RapidResponse Server cannot start due to corrupted data

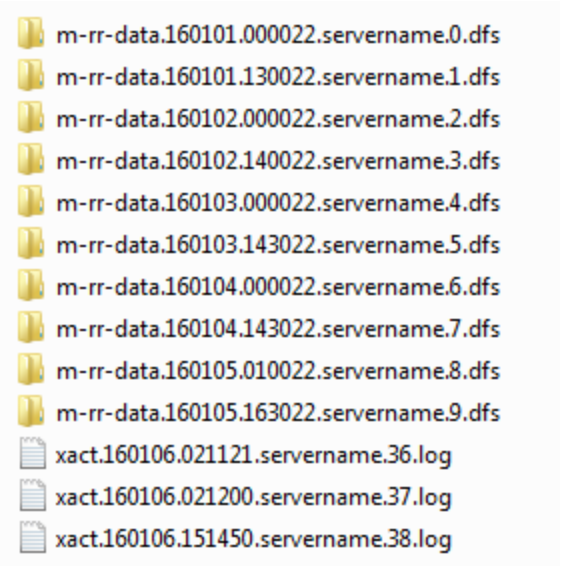
In this case, you cannot start RapidResponse Server. You understand that there might have been significant data integration and process changes over the past few days. You suspect the database might be corrupted.

To remedy the situation, you can try to restart RapidResponse Server and reload the database using an iterative testing approach. This approach can be somewhat time consuming but it can minimize data loss.

Using this approach, you attempt to load as many time-based database fragments as you can until an error is encountered, or RapidResponse Server cannot start or becomes unresponsive.

The iterative approach begins with first attempting to load the main folder fragment (0.DFS). If that fragment loads then you load more and more fragments until the process fails and no other DFS folders can be loaded.

The following procedure shows the process in action and it is based on RapidResponse database with 12 DFS files and three XACT files shown in the following illustration.

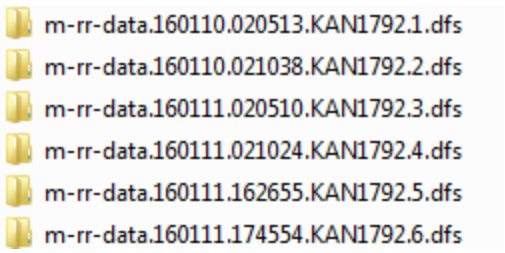


▸To iteratively load the RapidResponse database

1. Stop RapidResponse Server if it is running.
2. Create a **TempData** folder at the same level as the **C:\RapidResponse\Data** folder.
3. Move all DFS folders and XACT files except **0.DFS** from the **Data** folder to the **TempData**.
4. Start RapidResponse Server. This step attempts to load the main folder in the DFS series.
5. Do one of the following:
   - If RapidResponse Server does not start and load the database then you cannot move forward with this process. In this case, you might need to try loading a saved data package. For more information, see "Operations made unintended changes – restore using a data package" on page 323.
   - If RapidResponse Server did start and load the database then you move forward with this process. The loading the **0.DFS** confirms that this portion of the database does not contain issues that would prevent it from loading.

The rest of this process is repetitive. You attempt to load as many DFS files (in order from oldest to newest) as you can through an iterative testing process.

1. Stop RapidResponse Server.
2. Delete the XACT file in the **C:\RapidResponse\Data** folder. This file is created each time RapidResponse Server starts if an XACT file does not already exist.
3. Copy about half of the DFS files from the **TempData** folder to the **Data** folder. The earliest folders (lowest numbered) must be selected. For example, **1.DFS**, **2.DFS**, and so on. In the first iteration using the current example, use these folders:



4. Start RapidResponse Server.
5. Do one of the following:
   - If RapidResponse Server starts and the data loads then repeat this process and load another half of the remaining files.
   - If RapidResponse Server does not start or the data does not load then complete the following steps.
6. Stop RapidResponse Server if it is running.
7. Remove half the files that were previously copied to the Data folder. In the first iteration of the current example, the 4.DFS, 5.DFS, and 6.DFS files would be used.
8. Start RapidResponse Server.
9. Repeat Step 5.

Continue this iterative testing process until you can no longer load any more DFS files.

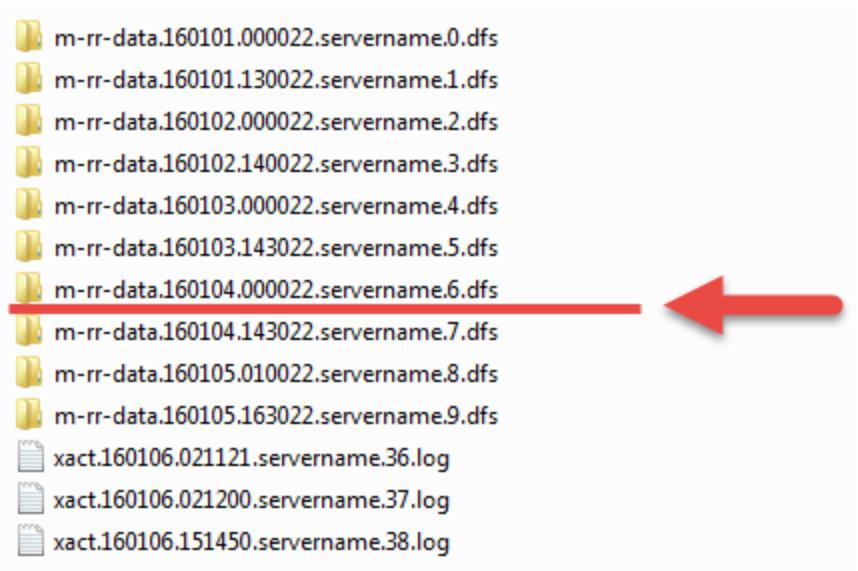
Take note of the timestamp on the last DFS file (highest number). This will help you understand the date and time cutoff where data has been lost and will help in further recovery.

Operations made unintended changes – restore using the database folders

In this case, your users complain that their RapidResponse data is not correct. After investigating you determine that the data became corrupted after a new data feed was added for a new site. The first data feed from the new site was loaded January 4 at 10 A.M.

Your company has been following standard best practices and has been capturing transactions and condensing the database on a scheduled basis. For more information, see "Commands and scheduling system tasks" on page 381.

The **Data** folder contains the following folders and XACT files.



The folders and files are sorted name. Because the file names are based on timestamps, the folder is also sorted by date and time (with the oldest at the top).

The red line and arrow highlight is placed before the DFS folder created on January 4 at 2.30.22 P.M. (or 143022). This information will be used in the process to roll back the database.

▸To rollback the database using the database folders

1. Stop RapidResponse Server.
2. Navigate to the **C:\RapidResponse\Data** folder.
3. Sort the contents of the folder by name (ascending). This will result in the oldest DFS folder (the main folder) being sorted at the top as shown in the previous illustration.
4. Delete all DFS folders that have a timestamp later than when problem was introduced. In this use case the data problem was introduced January 4 at 10 A.M. The **7.DFS**, **8.DFS**, and **9.DFS** folders should be deleted.
   - If the database was corrupted before the creation date of the oldest DFS folder (main folder of the hive) this procedure will not work for you. Instead review the data package process. For

more information, see "Operations made unintended changes – restore using a data package" on page 323.

5. Delete all transactional data (XACT files).
6. Start RapidResponse Server.

To minimize data loss, consider copying data files from the **\History** folder and reloading them into the **\Extract** folder so they can be re-imported into the RapidResponse database. Do not include the data files used to update the problematic site.

Operations made unintended changes – restore using a data package

This process can be followed if you are unable to use the other processes in this section.

In this case, your users complain that their RapidResponse data is not correct. After investigating you determine that the data became corrupted after a new data feed was added for a new site. The first data feed from the new site was January 4 at 10 A.M. (two days earlier).

Your company has been following standard best practices and has been creating a backup of the database on a daily basis using the **CreateDataPackage** system command. For more information, see "CreateDataPackage command" on page 388.

After further investigation, you decide the best course of action is to restore the RapidResponse database using the data package created on January 4 at 2 A.M. (eight hours before the first data feed from the problematic site).

To restore the database without data from the new site, you need to execute the following tasks:

1. Record all system configuration changes made in the last two days.
2. Capture all the files used in the data update process since January 4 at 2 A.M (except those from the problematic site).
3. Load the RapidResponse data package created on January 4 at 2 A.M.
4. Re-apply all system configuration changes made in the last two days (if applicable).
5. Run a DataUpdate command with the captured files used in the data update process.

After completing these tasks, your RapidResponse database will be up to date with a minimum loss of data. Data from the new problematic site will not be loaded or available to your RapidResponse users.

The following section describes these five tasks in more detail.

Record all system configuration changes (Step 1)

Almost all system configuration changes are recorded in RapidResponse and are available for review in the Administration Log workbook (available from the Administration pane). For more information, see " System administration logs" on page 423.

The **Security Audit** worksheet displays configuration, user and group, and permission changes. The **Changes to Root Scenario** worksheet displays all data changes that have been committed to the root scenario. It also identifies the user who made each change, and shows the table and field values affected by the change.

Record or export all data in these worksheets since January 4 at 2 A.M. (the date and time when the data package was created). Using a search on the Date column is an easy way to filter the data in the worksheets.

Capture all the files used in the data update (Step 2)

In this step, copy all the data files from the **\History** folder that were used in the data update processes since January 4 at 2 A.M. (the date and time when the data package was created). Do not include the data files used to update the problematic site.

For more information about the data flow in the Data Update process, see the *RapidResponse Data Integration Guide*.

Load the saved RapidResponse data package (Step 3)

In this step, you load the RapidResponse data package created on January 4 at 2 A.M. For detailed information about how to perform this action, see "Restoring data packages" on page 317.

Re-apply all system configuration changes (Step 4)

If any system configuration changes had been made in the last two days they should be made again. These changes were recorded in Step 2 and were available in the Administration Log workbook.

Run a DataUpdate command with the captured files (Step 5)

In this step, you reload the data files used in the data update process that were captured in Step 2. These files need to be copied to the **\Extract** folder. Once copied to the folder then run a DataUpdate command.

For more information about the data flow in the Data Update process, see the *RapidResponse Data Integration Guide*.

Archiving the RapidResponse database files

In addition to creating and storing backup copies of the RapidResponse database, you can create an archive of the individual database files. By archiving database files, you can more easily rollback the database in case of a system failure or a corrupted database. For more information about backups and rolling back the database, see "Backing up and restoring the RapidResponse database" on page 315 and "Rolling back the RapidResponse database" on page 318.

Database folders and files used in archiving process

The RapidResponse database is stored as **DFS** folders and **XACT** files (transaction files). The folders and files are stored in the **\Data** folder. The archiving process copies the contents of the **\Data** folder to another location. For more information about the RapidResponse database, see "Database files and operations" on page 311. The RapidResponse archiving process automatically manages the life cycle of the stored database files by deleting files older than a specified age deletion threshold.

Setting up archiving

To set up the archiving of RapidResponse database files, you must create or a modify a Windows registry setting on the computer where RapidResponse Server is installed. The **Directories\BackUpRoot** setting specifies the folder where the archived files are stored. This setting is specified as an absolute path and **\Data** is appended to it. For example, if you specify **E:\Archive** then the archived files are stored in **E:\Archive\Data**. If the **Directories\BackUpRoot** setting is blank or not available then archiving of the database files is turned off.

The **Directories\BackUpRoot** setting also controls the archiving of RapidResponse package files. When this setting is specified, **\Packages** is appended to it for a location for package files. For more information about archiving packages, see "Archiving RapidResponse package files" on page 252. For more information about this Windows registry setting, see "BackUpRoot" on page 357.

It is recommended that the archive folder be on a drive or device separate from the **Data** folder (the RapidResponse database folder). Doing so can improve RapidResponse Server restart time. It is also a best practice not to store the archived files on the same hardware as the **Data** folder in case of catastrophic hardware issues.

The RapidResponse Server service must have read-write access to the network location where the archive folder resides. For example, the archive folder might reside on a SAN or NAS.

Consider storing the archive folder where dump and diagnostic package files are stored. For more information, see "Selecting storage locations for operations" on page 311.

Notes:

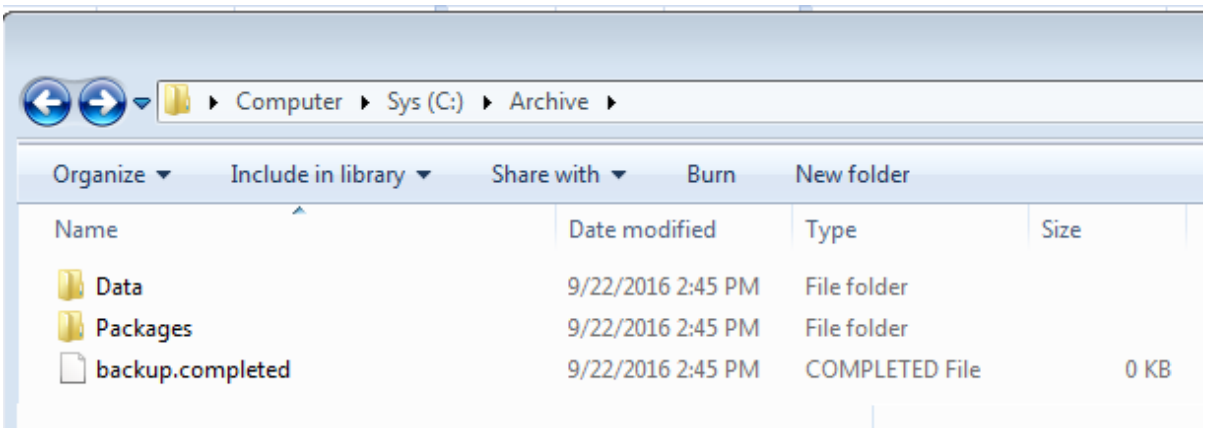
- RapidResponse Server does not need to be restarted after changing the archive folder setting.
- If your company has deployed the optional RapidResponse Server failover configuration, you must ensure that both RapidResponse systems use the same registry key. For more information, see "RapidResponse Server failover clustering" on page 289.

Archive process execution

After being set up, the archive process is automatically executed after the RapidResponse Server service has started. It also executes after the following RapidResponse system commands have completed:

- "Capture command" on page 385
- "Condense command" on page 387
- "Restart command" on page 407
- "Snapshot command" on page 409

The archive folder holds copies of all **DFS** folders and **XACT** files in the folder specified in the **Directories\BackUpRoot** Windows registry setting. The following illustration shows the folder structure if the registry setting is **C:\Archive**.



The following list summarizes the steps RapidResponse executes when running the archive operation.

1. The **backup.completed** file in the archive folder (which specified in the **Directories\BackUpRoot** Windows registry setting) is deleted (if file exists).
2. An empty text file named **backup.inprogress** is created in the archive folder. The existence of this file indicates that RapidResponse is actively creating archive files.
3. Any temporary files that RapidResponse has created in the archive folder are deleted. These files use the **.tmp** extension. Files are in a temporary state until they are fully copied over to the archive folder.
4. **DFS** folders and **XACT** files that are older than the age deletion threshold are deleted from the archive folder. The default setting is 120 minutes (two hours). The threshold setting can be modified. For more information, see "Modifying the age deletion threshold" on page 326.
5. All **DFS** folders and **XACT** files in the RapidResponse database folder (**\Data**) are copied to the archive folder. If a folder or file with the same name already exists in the archive folder, the new file or folder is retained in the archive folder.
6. A file named **manifest.*timestamp*.json** is created in the archive folder. This text file lists the names of all the **DFS** folders and **XACT** files that make up a complete copy of the RapidResponse database. This information can be of use when working with Kinaxis Customer Support or when you want to roll back the RapidResponse database. For more information, see "Rolling back the RapidResponse database" on page 318.
7. The empty text file named **backup.inprogress** is deleted.
8. The **backup.completed** file is created in the archive folder. This file indicates that the archive process has completed. If this file exists, the archive files have been successfully created.

Note: Archiving operations are logged in the **Server.log** file. For more information, see "RapidResponse text-based log files" on page 462.

Modifying the age deletion threshold

When the archive operation executes, it deletes **DFS** folders and **XACT** files that are older than the age deletion threshold. This helps to ensure that disk space will be available for newly archived folders and files. The default age deletion threshold is 120 minutes (two hours). This setting can be modified by

editing the **DataBackUpWindowMinutes** Windows registry setting. For more information, see "DataBackUpWindowMinutes" on page 352.

The higher the value used in this setting, the more disk space that will be consumed. However, a higher value might provide an opportunity to roll back the database further in time. The amount of disk space required might also depend on how often the archiving process is executed which is dependent of the execution of RapidResponse system commands.

Note: If your company has deployed the optional RapidResponse Server failover configuration, you must ensure that both RapidResponse systems use the same registry key. For more information, see "RapidResponse Server failover clustering" on page 289.

RapidResponse database integrity

RapidResponse can check the database for invalid references and inconsistent counts in scenarios. This procedure is called a data integrity check and can alert you in advance of potential operational problems with RapidResponse. Taking a proactive approach, rather than waiting for a system problem or failure, can potentially and significantly reduce system downtime.

Potential problems could include any of the following:

- Inaccurate resource reporting
- Potential performance degradation
- Potential for complex data remediation
- Risk to system stability
- Accuracy of analytic results

RapidResponse includes a default scheduled task that runs once each day and executes the RapidResponse **DataIntegrityCheck** command. For more information about setting up database integrity checks, see "DataIntegrityCheck command" on page 391.

You have four options to control how a database integrity check is performed to reduce the verification processing time and improve system performance.

- You can control whether the database integrity check stops after detecting one problematic scenario by changing the **IntegrityCheckMaxProblemPlans** values in the Windows Registry. For more information, see "IntegrityCheckMaxProblemPlans" on page 353.
- You can change the number of scenarios that are verified by modifying the DataIntegrityCheck command's MaxPlan setting. For more information, see "DataIntegrityCheck command" on page 391.
- You can modify the depth of scenarios in the scenario tree that are verified with the DataIntegrityCheck command's MaxPlanDepth setting. For example, the depth of the Enterprise Data (root) scenario is 0 and any direct children of this scenario are considered to be at a depth of 1 in the scenario tree. For more information, see "DataIntegrityCheck command" on page 391.
- The Data Integrity Check command can be configured to block four types of tests on a scenario-by-scenario basis. By blocking some tests you can improve the Data Integrity Check command performance. For more information, see "Blocking specific tests" on page 392.

Detection of database integrity errors

If a problem is detected during the verification process, RapidResponse Server writes an error message to the **Server.log** file and sends a message to the RapidResponse Master Administrator (Admin user). For more information about the log file, see " Server.log file" on page 464.

If an error is detected by the Data Integrity Check, it is strongly recommended that you send a data package file to Kinaxis Customer Support for analysis. For more information, see "Customer Support" on page 19.

You should also disable the running of the Database Integrity Check scheduled task until the error is resolved. This will prevent unnecessary messages from being delivered.

CHAPTER 27: Data persistence

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Automatic data persistence 330
Defining data persistence rules for a scenario 330
Logging of persistence operations 333

In a typical RapidResponse configuration, a data import is performed only once and then the data update process is used to refresh the RapidResponse data with changes from the enterprise system. However, there are cases where you might want to re-import data (by performing a data import). For example, you might want to perform a data import to reset the RapidResponse database.

During a data import, input data in the root scenario is replaced with data from the enterprise data sources, and all scenarios derived from the root scenario, except scenarios set as permanent, are deleted. By default, select data in RapidResponse is automatically persisted (saved) in the enterprise data scenario and then restored during the data import process. This includes most data that is considered to be maintained exclusively in RapidResponse.

In some cases, though, you might want to persist (save) other input data within a specific scenario (other than the root) so that it can be automatically restored when the next data import occurs. A typical use of persistence is to save data that is maintained only in the RapidResponse data model, and does not exist in the enterprise data source. For example, you might have data in the Constraint table, or in a custom table or field, that you are maintaining in a given scenario and which does not exist in the enterprise data source. By persisting this data, you can preserve it rather than losing it during the next data import.

Notes:

- To perform the procedures described in this chapter, you must be a system or data administrator that has permission to modify data integration settings. If an administrator does not have this permission then they can only view the data integration settings described in this chapter. For more information about the modify permission, see "Permission to modify data integration settings" on page 36.
- Before performing the procedures described in this chapter, it is highly recommended you review and understand the information in the *RapidResponse Data Integration Guide*. It provides an overview of the data integration change process and how to move changes from RapidResponse test systems to RapidResponse production environments.

Automatic data persistence

By default, certain data in RapidResponse is automatically persisted during a data import. For the most part, this is data maintained only in RapidResponse (system of record) and does exist in your enterprise data sources. It includes the following:

- All data in historical tables (each historical data extract is assumed to contain only new historical data). For more information on historical data, see the *RapidResponse Data Integration Guide*.
- Data integration settings.
- Records that have been inserted or modified by RapidResponse users and then committed to the root scenario.
- Automatically created records that have been subsequently modified by RapidResponse users and then committed to the root scenario.

You can identify all user-created (or modified) records that RapidResponse persists because they have been committed to the root scenario.

▸To identify records to be automatically persisted in the root scenario

1. In the **Administration** pane, under **Data**, click **Data Origin**.
2. Click the **Data Originating in RapidResponse** worksheet.
3. From the **Scenario** list, select the root scenario (by default, this scenario is named **Enterprise Data**).
4. From the **Origin** list, select **User**.
5. From the **Table** list, select **All**.

   To see just the records that will be automatically persisted from a specific table, select it from the **Table** list.

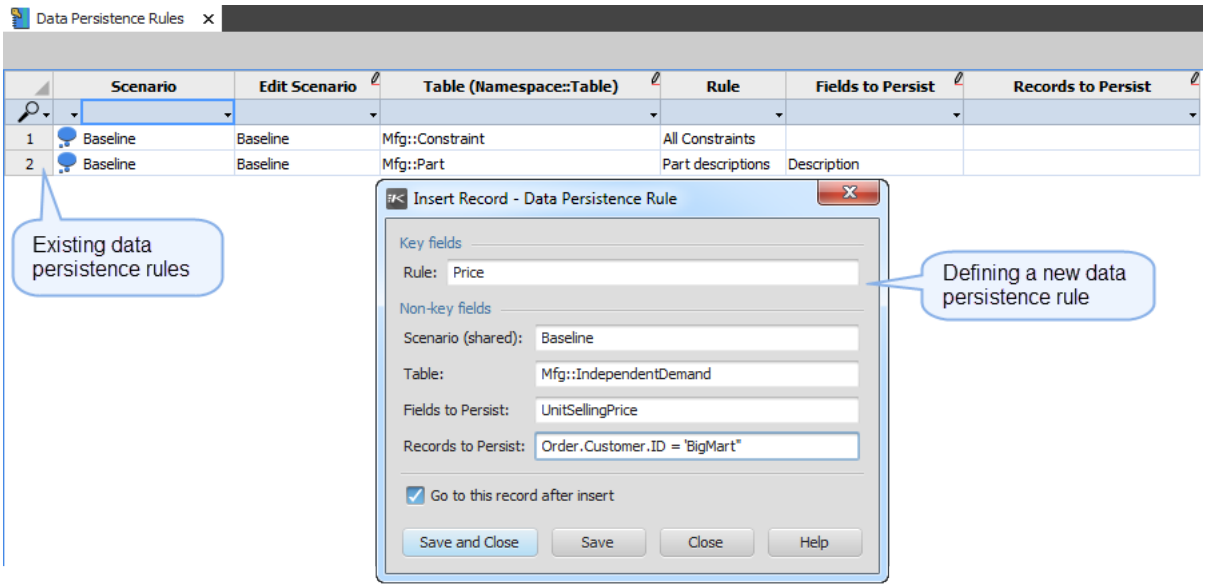
▸Reviewing data changes in the root scenario

1. In the **Administration** pane, under **System Monitoring**, click **Administration Log**.
2. Click the **Changes to Root scenario** worksheet.

Note: For more information about the **Changes to Root scenario** worksheet, see Administration Log's workbook help.

Defining data persistence rules for a scenario

Data persistence is configured by adding one or more data persistence rules. These rules are defined using the Data Persistence Rules worksheet as shown in the following illustration.



Each data persistence rule identifies the scenario that data is to be persisted in. Ensure that any scenario you are defining persistence rules for has been configured as a permanent scenario. To be permanent, a scenario must first be shared. Any scenario that is not permanent is deleted during a data import and therefore unable to have its data persisted. For more information about permanent scenarios, see " Creating scenario hierarchies" on page 719.

Data persistence rules also identify the table in which data is to be persisted and how records in that table should be persisted. You can either persist entire records or just select fields on a record. For example, if you are storing records in the Constraint table that are not in your enterprise data source, you might want to persist those Constraint records in their entirety. Alternatively, if you have added custom fields to the Part table that don't exist in your enterprise data source, you might want to persist just those field values on Part records.

Optionally, if you only want a given persistence rule to apply to specific records in a table, you can add a filter expression that identifies those records.

Caution: It is assumed the following procedure will be completed and verified in a RapidResponse test environment as discussed in the *RapidResponse Data Integration Guide*. After verifying and accepting the changes, the data integration settings can be moved to your production environment. For more information, see the *RapidResponse Data Integration Guide*.

▸To define a data persistence rule

1. In the **Administration** pane, under **Data**, click **Data Persistence Rules**.
2. On the **Edit** menu, click **Insert Record**.
3. In the **Insert Record** dialog box, specify the following:
   - **Rule**—a unique name for this data persistence rule.
   - **Scenario (shared)**—the scenario in which data is to be persisted. It should be a scenario that has been configured as permanent. This ensures the scenario is not deleted during a subsequent data import. For more information, see " Creating scenario hierarchies" on page 719.

- **Table**—the name of the table containing data to be persisted. This can be any standard or custom input table. The table should be specified along with its namespace in the format `Namespace::Table` (for example, `Mfg::Constraint`).
- **Fields to Persist**—identifies the fields to be persisted in this table. If you want to persist records in their entirety, this box should be left blank. However, if you want to persist only specific fields, they should be specified in a comma delimited list. Note that if persisting a field defined in a different namespace than its table, the field must be specified along with its namespace in the format `Namespace::Field` (for example, `Xyz::Region`).
- **Records to Persist**— identifies the records in the table to apply the persistence rule to. If you want all records in the table to be persisted, leave this box blank. However, if you want only specific records in the table to be persisted, type a RapidResponse filter expression to identify those records. The expression must be valid on the table data is being persisted from.

  No validation is performed on query expressions entered in the **Records to Persist** field. Therefore, if adding a filter expression to persist only select records from a table, its recommended that you first create the query expression you want to use in a worksheet. This allows you to both validate the syntax of the query expression and ensure it returns the desired records. For more information, see "To test the query expression used to persist selective records" on page 333.

4. Do one of the following:
   - Click **Save and Close** to save the persistence rule and return to the **Data Persistence Rules** worksheet.
   - Click **Save** to save the persistence rule and specify a persistence rule for another table and scenario combination.

Note: The **Fields to Persist** field must be left blank for any table that does not have key fields (for example, the BillOfMaterial table). Persistence on such tables can only be applied to entire records.

Examples

1. To create a rule that persists all Constraint table records in the “Today” scenario, specify the following values:
   - **Scenario**—Today
   - **Table**—Mfg::Constraint
   - **Fields to Persist**—<leave blank>
   - **Records to Persist**—<leave blank>
2. To create a rule that persists Supplier table records in the “Working” scenario where the supplier is either “Allied” or “CVM”, specify the following value:
   - **Scenario**—Working
   - **Table**—Mfg::Supplier
   - **Fields to Persist**—<leave blank>
   - **Records to Persist**—ID in ('Allied', 'CVM')
3. To create a rule that persists the “Name” and “CustomerGroup” fields on all Customer table records in the “Actions” scenario, specify the following values:

- **Scenario**—Actions
- **Table**—Mfg::Customer
- **Fields to Persist**—Name, CustomerGroup
- **Records to Persist**—<leave blank>

4. To create a rule that persists the UnitSellingPrice field in IndependentDemand table records in the "Today" scenario where the customer is "BigMart", specify the following values:
   - **Scenario**—Today
   - **Table**—Mfg::IndependentDemand
   - **Fields to Persist**—UnitSellingPrice
   - **Records to Persist**— Order.Customer = 'BigMart'

▸To test the query expression used to persist selective records

1. Open or create a new private workbook, and create a new worksheet within it (your user account must have workbook authoring privileges to do this).
2. In the **New Worksheet** dialog box, ensure to do the following:
   - On the **General** tab, from the **Table** list select the table from which data will be persisted.
   - On the **Filtering** tab, type a RapidResponse query expression that defines the records you want persisted from the table. You can verify the syntax in the expression by clicking **Validate Expression**.
   - On the **Columns** tab, add columns which will allow you to easily verify that the desired records are being returned.
3. When you have finished defining the new worksheet, click OK to close the New Worksheet dialog box, and open the worksheet.
4. Ensure the worksheet returns the desired records (that is, records representative of those which you want persisted). If it does not, modify the worksheet's filter expression to return the desired records.

Note: For complete information on creating workbooks and worksheets, see the RapidResponse Help.

Tip: You can copy the filter expression from the Filtering tab in RapidResponse, and then paste it in the **Records to Persist** field in the **Insert Record** dialog box.

Logging of persistence operations

For troubleshooting purposes, RapidResponse logs data persistence operations. Logged information is available to data and system administrators from the Data Import and Update Log workbook in the RapidResponse client.

▸To view logged data persistence information

1. In the **Administration** pane, under **System Monitoring**, click **Data Import and Update Log**.
2. Click the tab of the worksheet you want to review.
3. Optionally, select a data persistence rule operation from the **Data Import/Update ID** list.

Data persistence operations are listed using the following formats:
timestamp*.DataImport.Persist.Insert.*persistence-rule-name
timestamp*.DataImport.Persist.Update.*persistence-rule-name

Because data persistence is applied immediately after a data import, the data persistence operations are listed immediately after a data import in the list.

For detailed information about data logging information, see "Data import and data update logs" on page 442.

System and data folders

This topic only applies to the **On-Premises** version of RapidResponse.

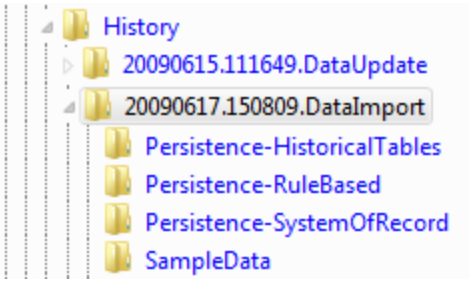
This section describes the system and data folders used in data persistence operations.

Data persistence rules, which are created in Data Persistence Rules workbook, are saved in the **C:\RapidResponse\Persistence-RuleBased folder.** This folder and the files it contains should not be modified.

The **C:\RapidResponse\History*timestamp*.DataImport** folder also contains three folders related to data persistence.

- **Persistence-SystemOfRecord**—contains records committed to the root scenario.
- **Persistence-HistoricalTables**—contains historical table records stored in the root scenario.
- **Persistence-RuleBased**—contains the same persistence rules stored in the C:\RapidResponse**Persistence-RuleBased folder.**

The following image shows a History folder example with persistence subfolders.



CHAPTER 28: Automatic RapidResponse Server operations

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Automatic server operations with webplnSC 335
Automatic server operations with ServerCommand 339

You can automate server operations from outside of RapidResponse. The operations you can perform are similar to those performed with scheduled tasks, but are run from the operating system instead of from RapidResponse.

You can use automatic server operations to control RapidResponse Server when it is not running, to perform an operation without signing in to RapidResponse, or to perform the same operation as a scheduled task outside of its time window.

Automatic server operations with webplnSC

webplnSC is an application that you can use to control RapidResponse Server. You can use webplnSC from the Command window in Microsoft Windows, or you can include any of the webplnSC commands in batch files that you schedule to run at specific times. webplnSC provides feedback through status and error codes that you can test to conditionally branch a program.

Note: In addition to using **webplnSC** to control RapidResponse Server, you can also use RapidResponse commands to perform similar operations. For more information, see "Commands and scheduling system tasks" on page 381.

Setting automatic server operations

You can use webplnSC to perform the following RapidResponse Server operations:

- Check whether RapidResponse Server is running or stopped (server status)
- Stop RapidResponse Server
- Restore the previous RapidResponse Server session

You need Windows administrator privileges for all tasks except checking the RapidResponse Server status.

Some of the server operations discussed in this section make RapidResponse unavailable to users. You can inform users of any scheduled maintenance that impacts them ahead of time. For more information, see "Communicating with users" on page 593.

The following tables summarize and describe the commands you can use to automatically control RapidResponse Server using webplnSC.

Task	Command	Description
Check the status of RapidResponse Server	`webplnsc [\\server name] status`	Returns the current status of RapidResponse Server. The status can be: • **Stopped—**RapidResponse Server is not running • **Running—**normal operation • **Restoring/Importing—**a session is being restored • **Shutdown—**RapidResponse Server is being shut down • **Checkpoint—**a checkpoint is in progress For remote operations, use the \\server name. The "\\" is required.
Checkpoint RapidResponse Server	`webplnsc [\\server name] checkpoint`	Performs a checkpoint. For remote operations, use the \\server name. The "\\" is required. **Note:** As of RapidResponse 11.0, this command is no longer supported in webplnSC.
Stop RapidResponse Server, with a checkpoint	`webplnsc [\\server name] shutdown`	Performs a checkpoint then stops RapidResponse Server. For remote operations, use the \\server name. The "\\" is required. **Note:** As of RapidResponse 11.0, this command no longer supports a checkpoint.
Stop RapidResponse Server, with no checkpoint	`webplnsc [\\server name] shutdown -nocheckpoint`	Stops RapidResponse Server. A checkpoint is not performed. For remote operations, use the \\server name. The "\\" is required.

Task	Command	Description
Restore the last RapidResponse Server session	`webplnsc [\\server name] restore`	Starts RapidResponse Server and restores the last session. For remote operations, use the \\server name. The "\\" is required.
Import data	`webplnsc [\\server name] import [-source=<mapfilepath>]`	**Note:** As of RapidResponse 9.2, this command no longer works and returns an initialization error. Starts RapidResponse Server and imports enterprise data. If the server is already running, then it is shut down first. This ensures that a checkpoint is done before the import takes place. The **-source** option specifies the full path name to the map file to be used for importing. For remote operations, the path name is relative to the remote server. If the **–source** option is not used, then the map file located in the registry is used. The path name can be any valid DOS path. It can include static strings, batch program arguments and environment variables. For remote operations, use the \\server name. The "\\" is required.

For more information about the structure of webplnSC commands, see "Structure of webplnSC commands" on page 337.

▸To control RapidResponse Server using webplnSC commands

1. Log on to Microsoft Windows as the Administrator.
2. Open a Command window.
3. Navigate to the **C:\RapidResponse\Program** folder.
4. Type the webplnSC command.

Tip: You can also create a batch program that includes the webplnSC commands that you want to run. You can use the command **if errorlevel** instruction to branch the program according to the return and error codes that webplnSC provides.

Structure of webplnSC commands

A command that you use to control RapidResponse Server using webplnSC looks like this:

```
webplnSC [\\servername]<command> [options]
```

The following table describes the parts of the webplnSC command.

Part of the command	Description
\\servername	Optional. Specifies the name of the server when you want to run the commands on a remote server. The server name must be preceded by "\\". If blank, the local computer is used.
Command	Specifies RapidResponse Server control command to be issued. Valid commands are: • **Restore**—starts RapidResponse Server and restores the last session • **Import**—starts RapidResponse Server and imports enterprise data. The map file used for the import depends upon whether a map file path was specified on the console application. If no map file is entered after the switch then the map file located in the registry is used. If RapidResponse Server is "running" then the server will be shutdown first. **Note:** As of RapidResponse 9.2, this command no longer works and returns an initialization error. • **Shutdown**—stops RapidResponse Server. • **Status**—returns the current state of RapidResponse Server
Options	• **-source=<mapfilepath>**—used with the **Import** command. Indicates the full path name to the map file. The path name should be any valid DOS path. The path name can include static strings, batch program arguments, and environment variables. **Note:** As of RapidResponse 9.2, this option no longer works and returns an initialization error.

Error and status codes in webplnSC

webplnSC returns two types of codes:

- **Status codes**—indicate the current status of RapidResponse Server
- **Error codes**—indicate why a specific command cannot be carried out

The codes provide feedback about the operations taking place. You can use the codes in batch programs to branch according to the results of tasks carried out.

The following tables summarize the status codes and error codes generated by the webplnSC application.

Status Code	RapidResponse Server Status
1	Stopped
2	Restoring or Importing
3	Shutting Down
4	Running
5, 6, or 7	Checkpointing

Error Code	Description
11	Invalid command syntax
12	Account does not have administrator privileges
13	Server Not Found
14	RapidResponse service name is invalid
15	RapidResponse service has been disabled
16	RapidResponse service executable cannot be found
21	RapidResponse Server is not running
22	RapidResponse Server is already running
23	RapidResponse Server is currently restoring
24	RapidResponse Server is currently performing a checkpoint
31	Error occurred during Startup - Service specific error
32	Error occurred during Startup (could not start RPC Listener)
33	Error occurred during Startup (Init Engine failed). See the Event Log.
41	Error occurred during Import. See the Event Log and the **Server.log** file. For more information about the log file, see " Server.log file" on page 464. **Note:** As of RapidResponse 9.2, you can no longer use webplnSC to import data.
> 1000	Other Service Errors

Automatic server operations with ServerCommand

ServerCommand is a Windows scripting file that you can use to perform operations on RapidResponse Server without signing in to RapidResponse. You can run ServerCommand scripts from a Microsoft Windows command window, or in a batch file. The **ServerCommand.wsf** file is located, by default, in the **C:\RapidResponse\Program** folder.

Prior to RapidResponse 9.2, ServerCommand was called ceocommand. If you have existing scripts that use the ceocommand naming, they will continue to function, but it is recommended you convert them to use ServerCommand instead to ensure they continue to work in future releases.

Running commands with ServerCommand

The ServerCommand script can run any of the standard RapidResponse commands. For a complete list of commands, see "Commands and scheduling system tasks" on page 381.

For example, you can use ServerCommand to perform a data update, create a backup, or update a scenario. You must specify parameter values for each command that requires them.

ServerCommand requires a connection to a running RapidResponse Server, and accesses the server using the user account and password you specify in the command parameters. If you do not want the command to sign in as a user, you can specify the Master Administrator password without a user name.

If you run as a command using your user name and password, you must not be signed in to RapidResponse. Otherwise, the command fails to run. This restriction does not apply if you run a command using the Master Administrator password. In this case, the command runs even if the Master Administrator is signed in.

If the command generates a result, the result is output to the Windows command window when the command is complete. However, you can choose to output the results to a log file instead. If you are performing the operation with a batch file, you should log the results so they can be reviewed.

Structure of ServerCommand commands

A command that you use to control RapidResponse Server using ServerCommand looks like this:

```
[cscript] C:\RapidResponse\Program\ServerCommand.wsf
[/user:"user_ID"] /password:"user_password"
/command:"command_name" [/parameters]
[/path:>"file_path\filename.txt"]
```

The following table explains each element of the ServerCommand command.

Element	Description
cscript	Optional element that writes the output of the command to a file.
/user:	Optional element that specifies the user ServerCommand signs in as to run the command. If this element is not specified, ServerCommand signs in as the Master Administrator account.
/password:	Required element that specifies the password of the user ServerCommand signs in as to run the command. If you did not specify a /user: element, this must be the Master Administrator password.
/command:	Required element that specifies the command that ServerCommand runs. For a list of commands, see "RapidResponse system commands" on page 384.
/parameters	If the command requires parameters, specifies each parameter and the value passed to the command, in the format `/parameter_name:"value"`
/path:	Optional element that specifies the folder that contains the file that the result of the command is written to. This element is required only if the cscript element is used, and must refer to a fully-resolvable file path, either on a local hard drive or a network drive.
>	Specifies the name of the file that the result of the command is written to. This element must follow the folder specified in the /path: element. If the file does not exist, it is created.

The arguments can be specified in any order.

Examples of ServerCommand commands

Suppose you want to update your scenario named Hourly Changes with changes from its parent every hour. You can create a batch file that performs the ScenarioUpdate command using ServerCommand.

The ServerCommand line for this batch file would be:

```
C:\RapidResponse\Program\ServerCommand.wsf /user:"yourname"
/password:"yourpassword" /command:"ScenarioUpdate"
/scenario:"Hourly Changes"
```

When the batch file runs, the Hourly Changes scenario is updated.

You could also write a batch file to perform a data update that only inserts and modifies records in the RapidResponse database, limits the number of record changes in each data file to 100, and writes the result of the data update operation to a log file. You can do this using ServerCommand to run the DataUpdate command with the parameters specified in the following line:

```
cscript C:\RapidResponse\Program\ServerCommand.wsf /password:"adminpassword"
/command:"DataUpdate" /MaxRecords:"100" /AllowDeletes:"False"
/path:>"C:\Logs\CommandLog.log"
```

When the batch file runs, new and modified records are brought in to RapidResponse from the enterprise data sources. The result of the operation is then written to the **CommandLog.log** file in the **C:\Logs** folder.

For more information about the ScenarioUpdate and DataUpdate commands, see "RapidResponse system commands" on page 384.

CHAPTER 29: Server exit applications

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Overview of server exits 343
Server exits for server operations 344
Environment variables 344
Registering server exits 346
Running server exits and error codes 347
Server exit for scenario operations 349

Server exits are RapidResponse OpenAPI applications that execute in response to a RapidResponse Server event. For example, you can create a server exit application that creates a customized log file each time the DataUpdate server command is run.

Note: Although RapidResponse continues to support the OpenAPI programming extensions and server exits, they are no longer being promoted. It is not recommended that you extend the use of these tools. Consider using RapidResponse scripts to automate operations and customize processes. For more information, see the *RapidResponse Scripting Guide*.

Overview of server exits

In many RapidResponse implementations, RapidResponse Server is only one component in a larger execution system. Because execution systems can be comprised of a variety of different business process oriented applications, effective communication needs to exist amongst these multiple systems.

A number of RapidResponse Server operations are considered essential events that must be communicated to other systems within the execution environment. This includes:

- Automatically updating the enterprise system.
- Integrating work-flow applications and other systems with RapidResponse specific information.

Using RapidResponse Server's ability to support server exit applications, you can configure any desired communication with these execution systems directly through the OpenAPI framework.

Server exits for server operations

A server exit application based on a server operation is performed in addition to normal RapidResponse Server functionality. You can only have one server exit application based on a specific server operation. For example, there can only be one server exit application based on a **ServerPostImport** operation.

When a server exit application based on a server operation executes, the following occurs:

- RapidResponse Server passes environment variables to the server exit application.
- RapidResponse Server executes the server exit application.
- RapidResponse Server performs normal functionality after the server exit application is finished executing.

A server exit application can be based on one of the following operations.

Server Operations	Description
ServerDataUpdate	Runs when a data update is completed after running the DataUpdate command or when a user commits a pending data update. This server exit operation can only be used with the data update process introduced in RapidResponse 8.2.
ServerPostImport	Runs after new data is imported into RapidResponse Server, the transaction-recovery is completed, and the selective persistence process has executed (if applicable) but before any users are allowed to sign in. During this server operation, the root scenario is editable. It is strongly recommended that you do not amend the root scenario. If you do, a data update might not work properly.
ServerPostRestore	Runs after data is restored to RapidResponse Server and transaction-recovery is done. During this Server operation, it is possible for users to sign in to RapidResponse Server.

RapidResponse 2014.1 (and later) no longer support the following server exits for server operations:

- ServerCheckPoint
- ServerPostDataLoad
- ServerPostImportSelPersist
- ServerPreLoad
- ServerPreDataUpdate
- TransactionImport

In addition, server exits for scenario operations are no longer supported. For reference information about this server exit type, see "Server exit for scenario operations" on page 349.

Environment variables

When a server exit application runs, RapidResponse Server passes environment variables to it. Environment variables store system data such as a user ID and password. You can use environment variables to achieve specific tasks such as connecting to RapidResponse Server or getting the name of a scenario that has been given to another RapidResponse user.

The following two objects are used to work with environment variables:

- WshShell
- WshEnvironment

WshShell object

A **WshShell** object is responsible for starting new processes, creating shortcuts on the Windows desktop, and handling Windows environment variables. You can use the **CreateObject()** function to create a **WshShell** object. The syntax to create a **WshShel**l object is:

```
Set myWshShellOb = CreateObject("Wscript.Shell")
```

WshEnvironment object

After you create a **WshShell** object, you can create a **WshEnvironment** object. A **WshEnvironment** object is used to get the value of an environment variable.

You can use the **WshShell** object's **Environment** method to create a **WshEnvironment** object. The syntax to create a **WshEnvironment** object is:

```
Set myWshEnvironmentOb = myWshShellOb.Environment("PROCESS")
```

You must specify **PROCESS** as the parameter value to access environment values passed to the server exit application.

You can use the **WshEnvironment** object's **Item** property to retrieve the value of an environment variable. For example, you can retrieve the value of the **User_ID** environment variable to get the current user signed onto RapidResponse Server. The syntax is:

```
UserId = myWshEnvironmentOb.Item("USER_ID")
```

The following table lists all environment variables passed to a server exit application.

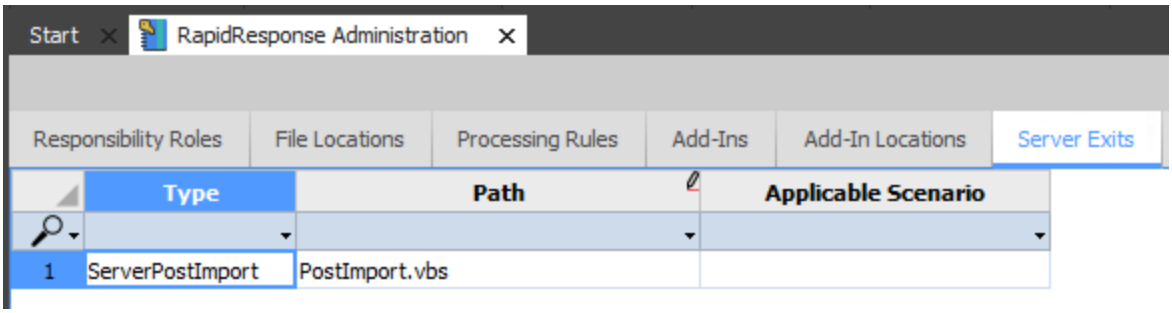
Environment variable	Description
DATA_UPDATE_KEY	The Name field of the DataUpdateHistory system table. This table is used to populate the Data Update Summary worksheet in the RapidResponse Data Update Log workbook.
EXIT_NAME	The name of the server exit application being executed.
SERVER_ID	IP address or network name of RapidResponse Server.
RAPIDRESPONSE_ROOT	The root ID of RapidResponse Server.
SESSION_ID	The name of RapidResponse Server executing the server exit application. If there are multiple versions of RapidResponse Server on the same computer, a colon (:) and the server number appear after the server name. For example: `rrserver : 2`
SESSION_PASSWORD	The session password for the current user. It is used to create another session.
USER_ID	The user ID of the user who is currently logged onto RapidResponse Server. For server operations, this is the user ID of a RapidResponse system administrator.

Note: For more information about the **WshShell** or the **WshEnvironment** objects, see Microsoft's MSDN online help.

Registering server exits

After you create a server exit application, you need to register it before you can run it. To register, create an entry in the Server Exits worksheet in the RapidResponse Administration workbook. If you do not register the server exit, the operation is performed in the normal manner.

The following figure shows a **Server Exits** worksheet with the **PostImport.vbs** application registered.



▸To register a server exit application

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Server Exits** worksheet tab.
3. On the **Edit** menu, click **Insert Record**.
4. From the **Type** list box, choose the server exit type.
5. In the **Path** box, type the path on the computer where RapidResponse Server is installed that is relative to the server exit's directory.

   If this entry does not exist, the path is relative to RapidResponse Server's program directory.

   For example: the server exit application is **GeneralCommit.vbs**

   The base path is described in the registry under this key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Webplan Inc.\Webplan\Directories

   It has a string value entry called ServerExits.
6. Click **Save** to insert the record or click **Save and Close** to insert the record and close the **Insert** dialog box.

Notes:

- If you enter a value in the Applicable Scenario Name column for a server exit application, RapidResponse Server does not notify you of the error while you are in the Server Exits worksheet. Rather, a message appears in **Server.log**. For more information about the log file, see " Server.log file" on page 464.
- You can also remove server exit applications from your system. When you remove a server exit application, processing controlled by that server exit reverts to normal.

Running server exits and error codes

A server exit application based on a scenario operation replaces RapidResponse Server functionality. A server exit application based on a server operation is performed in addition to RapidResponse Server functionality.

You can run a registered server exit application by invoking a specific process. For example, assume you have registered a server exit application based on a **PlanCommit** operation. You can run this application by committing a child scenario to a specific scenario (the scenario is defined when a server exit application is registered).

Error messages for server exit applications

If an error is encountered during the execution of a server exit application, RapidResponse Server logs an error message in **Server.log** file. For example:

```
Error returned from ServerCheckPoint exit: Error code 16.
```

Where, **ServerCheckPoint** is the server operation, and **16** is the associated error code.

When a server exit application encounters an error, RapidResponse Server creates an error value. This value is displayed by RapidResponse. There are two sets of error codes:

- error messages for server applications
- error messages for scenario operations

The error messages described in this section relates to both types of server exit applications (scenario and server operations). The following table lists server exit application error messages.

Error Message	Description
Return code of 24	A user-defined error will only have meaning if the server exit application sends a message to the parent (for example, the RapidResponse client or OpenAPI application that caused the server exit to run).
Scenario operation originates at RapidResponse client and has a return code of 24	RapidResponse client checks for any messages sent by the server exit application and displays a message box to the user.
Scenario operation originates from an OpenAPI method call.	To retrieve a server exit message, call the **ReceiveMessageFromChild()** method.
Server operation	An error message produced by RapidResponse Server is passed to the **server.log** file.

Error codes for scenario operations

The error codes described in this section relate to server exit applications based on scenario operations.

The following table lists error codes for scenario operations.

Return Code	Description
0	OK, no error.
1	Not signed in.
2	Too many scenarios.
3	User is not the owner.
4	Scenario is shared.
5	Scenario is not up-to-date.
6	User does not have write permissions for the scenario.
7	Scenario has child scenarios.
8	Illegal operation for scenario with child scenarios.
9	Invalid user ID or Password.
10	The user is already signed in.
11	Not connected to RapidResponse Server.
12	Concurrent user limit.
13	Cannot perform operation because name is not unique.
14	Scenario is being used by queries.
15	Scenario has child scenarios.
16	Do not have access to parent scenario.
17	Scenario does not exist.
18	Scenario is not private.
19	Scenario is a scheduled scenario.
20	Scenario is an internal scenario type.
21	Parent scenario needs to be updated.
22	No such user.
23	Feature is not licensed.
24	User defined error.
25	Attempting to change the value of a constant variable.
26	Attempting to change the context to one that does not exist.
27	The server is unable to create a UUID when trying to commit a scenario.
28	The server could not process the commit because there was an event.
29	Attempting to change the context to one that does not exist.
30	Attempting to change the context when it is not permitted.
31	Attempting to sign in as a child session after the parent session.

Return Code	Description
32	Attempting to set the time zone to one that does not exist.
33	The licensing for RapidResponse Server has expired.
34	The clock for the server was set back.

Server exit for scenario operations

Caution: RapidResponse 2014.1 no longer supports server exits for scenario operations. The information in this section is supplied for reference purposes only.

A server exit application based on a scenario operation is performed instead of normal RapidResponse Server functionality. For example, when you give a scenario to another user using RapidResponse, the scenario is given to the specified user. This represents normal RapidResponse Server functionality. However, you can create a server exit application that overrides this functionality.

There can only be one server exit application based on a specific scenario per scenario operation. For example, only one PlanGive server exit application can be based on a scenario named **MyPrivateScenario**.

Assume that **MyPrivateScenario** is associated with a server exit application named **GiveAllPlans**. When a scenario operation occurs (for example, **MyPrivateScenario** is given to another RapidResponse user), RapidResponse Server performs the following:

- Determines if the scenario is associated with a server exit application (in this example, **MyPrivateScenario** is associated with **GiveAllPlans**).
- If the scenario is associated with a server exit application, RapidResponse Server executes the application (in this example, RapidResponse Server executes **GiveAllPlans**). If not, RapidResponse Server performs normal functionality (for example, RapidResponse Server will give **MyPrivateScenario** to another RapidResponse user).
- Passes environment variables to the server exit application (in this example, RapidResponse Server passes environment variables to **GiveAllPlans**). For information about environment variables, see "Environment variables" on page 344.

A server exit application can be based on the following scenario operations.

Scenario operations	Description
PlanCommit	Runs when a child scenario of one of the listed scenarios is committed.
PlanDelete	Runs when the scenario being deleted is one of the listed scenarios.
PlanGive	Runs when the scenario being given is one of the listed scenarios.
PlanPublish	Runs when the scenario being shared is one of the listed scenarios.
PlanUpdate	Runs when the scenario being updated is one of the listed scenarios.

There are OpenAPI methods that affect how server exit applications based on scenario operations behave. For example, assume you create a server exit application based on a **PlanCommit** operation. The **Session** object's **CommitPlan()** method should be used as part of the server exit application's business logic.

Consider the following scenario:

- You create a server exit application based on a **PlanCommit** operation.
- The server exit application calls **CommitPlan()**.
- You commit a scenario using the RapidResponse client which results in the server exit application being executed.
- When the **CommitPlan()** method is executed, the server exit application is executed again and so on. This creates a recursive server exit loop.

Each time the server exit application is executed, **CommitPlan()** is called and the server exit application is executed again. To avoid this situation, you can change the value of the **ByPassServerExit** parameter (a parameter of **CommitPlan()**) to **True**. This results in the server exit application being ignored. If you set **ByPassServerExit** to **False**, then a recursive server exit loop occurs.

CHAPTER 30: Registry Settings for RapidResponse Server

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Location of registry settings 351

The Windows registry on the computer where RapidResponse Server is installed includes many RapidResponse Server settings. For example, the settings that specify how RapidResponse Server manages memory are stored in the Windows registry. The RapidResponse Server registry settings can be used to optimize how RapidResponse Server performs. This chapter provides a summary of RapidResponse Server registry settings.

Cautions:

- Although the Windows registry is where many RapidResponse Server settings are stored, it is advised to use the RapidResponse client, either through workbooks or the Administration pane to modify RapidResponse Server settings.
- Improperly modifying the Windows registry can result in system instability. Before modifying the registry, create a backup using the Export tool in the Microsoft Registry Editor. For more information, see the Microsoft Registry Editor Help.

Note: If you have deployed the optional RapidResponse Server failover cluster configuration, you might need to make changes in each registry system on the two RapidResponse Server instances. For more information about failover clustering, see "RapidResponse Server failover clustering" on page 289.

Location of registry settings

RapidResponse Server registry settings are stored in the main configuration key located in:

HKEY_LOCAL_MACHINE\SOFTWARE\Webplan Inc.\Webplan

You will also notice that some registry settings are also stored in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Webplan Inc.\Webplan

Settings in the **Wow6432Node** key must not be modified.

▸**To open the Microsoft Registry Editor**

1. From the Windows **Start** Menu, choose **Run**.
2. In the **Open** box, type **regedit** and click **OK**.

Note: If you change a RapidResponse Server registry setting, you must stop and restart RapidResponse Server before the change becomes effective.

Keys	Value	Type	Description
Webplan	(Default)	String	Internal RapidResponse Server Setting. Do not change.
Webplan	AdminEMail	String	Specifies the Admin user's email address **Default:** None
Webplan	BackUpPackages	DWORD	Specifies whether RapidResponse stores archived copies of RapidResponse package files. For more information about archiving, see "Archiving RapidResponse package files" on page 252. **0**: Off (default if not specified). **1**: On In addition to turning this setting on, the **BackUpRoot** registry setting must also be enabled to archive package files. For more information, see "BackUpRoot" on page 357. **Note:** Changing this setting does not require the restart of RapidResponse Server. **Note:** If your company has deployed the optional RapidResponse Server failover configuration, you cannot use this setting. For more information, see "RapidResponse Server failover clustering" on page 289.
Webplan	DataBackUpWindowMinutes	DWORD	When archiving of database files is turned on, specifies the minimum duration to store the database files in the archive folder. For more information about archiving, see "Archiving the RapidResponse database files" on page 324. This setting is specified in minutes. If archiving is turned on and this setting is not specified, then the default is used (120 minutes). **Note:** Changing this setting does not require the restart of RapidResponse Server. **Note:** If your company has deployed the optional RapidResponse Server failover configuration, you cannot use this setting. For more information, see "RapidResponse Server failover clustering" on page 289.

Keys	Value	Type	Description
Webplan	HttpsRapidResponseConsole	DWORD	Specifies whether communication between the RapidResponse Console and RapidResponse Server should be encrypted. **0**: HTTP (default if not specified). **1**: HTTPS For more information, see "RapidResponse Console security settings" on page 237.
Webplan	InputFieldLimit	DWORD	Specifies the maximum number of input fields allowed in a table. This limit does not include calculated, notes, or set fields. You can specify a maximum of 1000 input fields, however, tables this large are not recommended. **Default**: 700
Webplan	IntegrityCheckMax ProblemPlans	DWORD	Specifies the number of problematic scenarios that can be detected before the database verification process stops. If this Registry key is not present, by default, the value is set to 1.
Webplan	InvalidateAll	DWORD	Specifies whether all calculated results for a scenario will be discarded, or invalidated, when any data in the scenario is changed. By invalidating the results, data can be saved more quickly but this might result in slower query performance. **0**: selected invalidation (default if not specified). **1**: invalidate all
Webplan	MailServer	String	Specifies the email server used by RapidResponse Server. **Default:** None

Keys	Value	Type	Description
Webplan	MemoryLimit	DWORD	Specifies the number of megabytes to be used as the server memory limit. It can be set to any value, up to the process size limit imposed by the operating system. If the value is too high, or if the registry entry is not a DWORD, the registry entry will be ignored. A message is written in the **Server.log** file upon startup, which reports the memory limit that is used. **Default:** The default difference between the physical memory and the memory limit is fixed at 10 GB (so, the RapidResponse Server uses the amount of physical memory minus 10 GB). In systems with less than 100 GB of physical space, the RapidResponse server calculates a limit of 90 percent of system memory. It is recommended that you do not leave the memory limit at the default setting. For more information, see "RapidResponse system memory usage" on page 260.
Webplan	MemoryModel	DWORD	Specifies a limit to the amount of physical memory RapidResponse Server can use. **32**: Sets physical memory limit to 32 GB. **64**: Sets physical memory limit to 64 GB. **128**: Sets physical memory limit to 128 GB. **Note:** As of RapidResponse 10.1, this setting is ignored.
Webplan	OpenAPILogging	DWORD	Specifies whether detailed OpenAPI logging is turned on. **0**: Off (default if not specified). **1**: On For more information, see "Enabling OpenAPI detailed logging" on page 220.

Keys	Value	Type	Description
Webplan	PackageBackUpWindowMinutes	DWORD	When archiving of database files is turned on, specifies the minimum duration to store package files in the archive folder. For more information about archiving, see "Archiving the RapidResponse database files" on page 324. This setting is specified in minutes. If archiving is turned on and this setting is not specified, then the default is used (10,080 minutes or one week). **Note:** Changing this setting does not require the restart of RapidResponse Server. **Note:** If your company has deployed the optional RapidResponse Server failover configuration, you cannot use this setting. For more information, see "RapidResponse Server failover clustering" on page 289.
Webplan	Port	String	The RapidResponse Server is bound to a specific TCP/IP port and it must be open for inbound requests. RapidResponse Server uses this port to communicate with other RapidResponse components. This registry setting specified the port RapidResponse Server uses. The port number can be any value from 1024 to 65535. The port number is originally specified during the RapidResponse Server installation. For information about changing he port number, see "RapidResponse and TCP/IP ports" on page 283.
Webplan	QueryMemoryAlert Threshold	DWORD	Specifies the amount of memory (in MB) used before a message to the master administrator (Admin user) is automatically generated. A message might be sent in cases where users are consuming a large amount of memory while running queries. The alert message is also written to the Event log. If this Registry key does not exist, by default, the master administrator is notified if 10 percent of the usable memory on the computer where RapidResponse Server is installed is used to generate query results.

Keys	Value	Type	Description
Webplan	RunScheduledTasks	DWORD	Specifies whether scheduled system tasks should be turned off or on. Setting **RunScheduledTasks** to 0 prevents scheduled system tasks from running on a schedule. However, it does not prevent scheduled system tasks from being run on demand. In addition, f a scheduled system task is manually triggered to run while scheduled tasks are turned off, a message will be logged in the Server.log file Deleting the **RunScheduledTasks** registry setting or setting it to a value other than 0 turns the scheduled system tasks back on. For more information, see "Turning off all scheduled system tasks" on page 418. By default, this Registry key does not exist.
Webplan	ServerLoadAlert Threshold	DWORD	Specifies the percentage of Server memory load used before an email alert to the Master Administrator (Admin user) is automatically generated. The alert message is also written to the Event log. If this Registry key is not present, by default, the Admin user is notified if the Server load reaches 90 percent. This Registry setting must be a number between one and 100.
Webplan\ *n.n.n*	(Default)	String	*n.n.n* represents the RapidResponse Server version number (for example, 9.5.0). Multiple versions of this key might exist depending on the number of RapidResponse Server upgrades. Do not change the key or value.
Webplan\ Database	Server	String	Specifies the location of an SQL Server that RapidResponse might use. The default is **localhost**.
Webplan\ DataLoad	DataSource	String	Specifies connect string for dataload; text file or relational database. This value is used when the **-import** parameter is used with the Windows Service dialog box for RapidResponse Server. **Note:** As of version 9.2, this setting is ignored.
Webplan\ DataLoad	EmailAttachment	DWORD	Specifies whether the email notification of the log file associated with data import includes an attachment of the log file itself. **0:** No attachment (default). **1:** Attachment of log file in email notification.

Keys	Value	Type	Description
Webplan\ DataLoad	EmailWho	String	Specifies the name of the email recipient for email notification of the log file associated with data import. When the value is empty, email notification is disabled. An empty value is the default.
Webplan\ DataLoad	ErrorLimit	DWORD	Specifies the number errors to log for each data text file that is imported. **Note:** As of version 9.2, this setting is ignored. For more information about limiting error logging, see "Limiting errors and warnings" on page 445.
Webplan\ Directories	Backup	String	Specifies drive and folder where RapidResponse stores a compressed backup file of the database. If this Registry key does not exist, the files are stored in the **\Backup** subfolder of the folder specified in the **Root** directory registry key. For more information about this key, see "RootShared" on page 360. If using this setting, the specified folder must already exist; RapidResponse cannot create it. **Note:** As of version 9.2, this setting is ignored.
Webplan\ Directories	BackUpRoot	String	Specifies the drive and folder where RapidResponse stores archived copies of the RapidResponse database and package files. For more information about archiving, see "Archiving the RapidResponse database files" on page 324 and "Archiving RapidResponse package files" on page 252. If this setting is empty or does not exist then archiving is turned off. **Note:** Changing this setting does not require the restart of RapidResponse Server. **Note:** If your company has deployed the optional RapidResponse Server failover configuration, you cannot use this setting. For more information, see "RapidResponse Server failover clustering" on page 289.

Keys	Value	Type	Description
Webplan\ Directories	Data	String	Specifies drive and folder where RapidResponse database is stored. If this Registry key does not exist, the files are stored in the **\Data** subfolder of the folder specified in the **Root** directory registry key. For more information about this key, see "RootShared" on page 360. If using this setting, the specified folder must already exist; RapidResponse cannot create it. **Note:** If your company has deployed the optional RapidResponse Server failover configuration, you cannot use this setting. For more information, see "RapidResponse Server failover clustering" on page 289.
Webplan\ Directories	MaxBackupFiles	DWORD	Specifies the maximum number of backup files that can be saved in the folder specified in the Backup Registry value. It can be set to a value between 0 and 255. If not specified, the default is 0. **Note:** As of version 9.2, this setting is ignored.

Keys	Value	Type	Description
Webplan\ Directories	Packages	String	Specifies the folder where the RapidResponse data package files are stored. Packages are used to back up the RapidResponse database. For more information, see "Backing up and restoring the RapidResponse database" on page 315. The specified folder where data packages are stored also stores other types packages including: • Log file packages used in troubleshooting situations by Kinaxis Customer Support. For more information, see "Troubleshooting RapidResponse Server" on page 241. • Diagnostics package files created by the RapidResponse Server Monitor. These files contain detailed system information. For more information, see "Internal errors and system crashes" on page 244. **Note:** The default storage location of the diagnostic package files can be customized so that they are not stored in the same location as the packages used to back up the RapidResponse database. To do so, use the **PkgDirectory** Windows registry setting. For more information, see "PkgDirectory" on page 364. If this Registry key does not exist, the files are stored in the **\Packages** subfolder of the folder specified in the **Root** directory registry key. For more information about this key, see "RootShared" on page 360. If using this setting, the specified folder must already exist; RapidResponse cannot create it. It is recommended that the default location for the **Packages** folder be moved to different physical drives (not on the same drive as the RapidResponse Server and database). For more information, see "Improve performance by moving default subfolders" on page 251. **Note:** If your RapidResponse installation is using the failover configuration, ensure this folder is available to both instances of the RapidResponse Server. For more information, see "RapidResponse Server failover clustering" on page 289.

Keys	Value	Type	Description
Webplan\ Directories	Program	String	Specifies the folder where the RapidResponse Server program is installed. This entry should not be modified. If this Registry key does not exist, the files are stored in the **\Program** subfolder of the folder specified in the **Root** directory registry key. For more information about this key, see "RootShared" on page 360. If using this setting, the specified folder must already exist; RapidResponse cannot create it.
Webplan\ Directories	Root	String	Specifies the folder where RapidResponse program and data subfolders are stored. The location was originally specified during the RapidResponse Server installation. The default location is **C:\RapidResponse**. The location of some of the subfolders can be modified by changing the registry setting for the other **Webplan\Directory** keys. This list includes: • "Backup" on page 357 • "DataBackUpWindowMinutes" on page 352 • "Packages" on page 359 • "Program" on page 360 • "ServerExits" on page 361 **Note:** If your company is using the optional RapidResponse failover configuration, this setting is overridden by the **RootShared** registry key. For more information, see "RapidResponse Server failover clustering" on page 289
Webplan\ Directories	RootShared	String	This setting is only used if your company is using the optional RapidResponse failover configuration. It specifies the folder where RapidResponse program and data subfolders are stored for each instance of RapidResponse Server in the failover cluster. The location was originally specified during the execution of the Failover Configuration program. For more information, see "RapidResponse Server failover clustering" on page 289.

Keys	Value	Type	Description
Webplan\ Directories	ServerExits	String	Specifies the path of the RapidResponse Server to Server Exit executables. The path is relative to the ServerExits folder. If this Registry key does not exist, the files are stored in the **\ServerExits** subfolder of the folder specified in the **Root** directory registry key. For more information about this key, see "RootShared" on page 360. For more information about server exits, see "Server exit applications" on page 343. **Note:** If your RapidResponse installation is using the failover configuration, ensure this folder is available to both instances of the RapidResponse Server. For more information, see "RapidResponse Server failover clustering" on page 289.
Webplan\ Directories\ LastUsed			The multiple values in the LastUsed key hold the location of various folder locations used by RapidResponse such as the location for log files.
Webplan\ LogFlags	import	DWORD	Specifies whether to log data import information. **0**: errors are not logged **1**: errors are logged **(default)**
Webplan\ LogFlags	Query	DWORD	As of RapidResponse 8.1, this registry setting is ignored. It used to specify whether to log each query against the RapidResponse database.
Webplan\ LogFlags	SeparateLogs	DWORD	As of RapidResponse 8.1, this registry setting is ignored. This setting used to specifies the file where RapidResponse Server would write information during the data import process.
Webplan\ LogFlags	truncateOnOpen	DWORD	As of RapidResponse 8.1, this registry setting is ignored. It used to specify whether to empty the Server.log file after restoring RapidResponse.
Webplan\ Network	Protocol	String	Key is added when RapidResponse Desktop is installed on the same computer as RapidResponse Server. Indicates the protocol RapidResponse Desktop uses to communicate with RapidResponse Server. Valid values: **ncacn_ip_tcp**: TCP/IP **ncacn_np**: Named pipes

Keys	Value	Type	Description
Webplan\ Overrides	EmailOverride	String	Specifies an alternate email address for alerts to send email to. This setting overrides the "To", "CC" and "BCC" addresses (if present) used by the alert. This option can be used in a test or development environment. For more information, see "Alert overrides in a development environment" on page 675.
Webplan\ Overrides	SupplyAgentExport Override	String	Specifies a folder location for the file export location specified in the Delivery tab of the New Alert or Alert Properties dialog boxes. This option can be used in a test or development environment. When specifying, use the complete path to the alternate folder location. This registry value is overridden by the AlertService_ExportDirectoryOverride setting introduced in version 9.0. For more information, see "Overriding the file export location" on page 676.
Webplan\ Overrides	SupplyAgentThreadOverride	DWORD	Specifies the number of processor threads dedicated to alerts. This option can be used in a test or development environment. If not specified, the default is the number of processors present in the computer RapidResponse is installed on. This registry value is overridden by the ServiceHost_ThreadCount setting introduced in version 9.0. For more information, see "Configuring RapidResponse Service Host" on page 234.
Webplan\ RRMonitor	AsaOnlyOnFirstChance	DWORD	Controls whether only an Automated Server-incident Analysis (ASA) diagnostic file is created when an exception is throw by RapidResponse Server. **0**: Creates the ASA file along with the other diagnostic files (default). **1**: Create only the ASA file. If set to **1**, the other registry settings regarding diagnostic files to create are ignored. For more information, see "Improve performance by moving default subfolders" on page 251.

Keys	Value	Type	Description
Webplan\ RRMonitor	DumpDirectory	String	Specifies drive and folder where RapidResponse Server Monitor stores dump files. For more information, see "Internal errors and system crashes" on page 244. If this Registry key does not exist, the dump files are stored in the **C:\RapidResponse\Dumps** folder (default installation). The specified folder must already exist; RapidResponse cannot create it. It is recommended that the default location for the **Dump** folder be moved to different physical drives (not on the same drive as the RapidResponse Server and database). For more information, see "Improve performance by moving default subfolders" on page 251.
Webplan\ RRMonitor	FullDumpOnFirst Chance	DWORD	Controls whether a full dump file is created after an internal error. **0**: Do not create **(default).** **1**: Create the file. For more information, see "Internal errors and system crashes" on page 244.
Webplan\ RRMonitor	FullDumpOnSecondChance	DWORD	Controls whether a full dump file is created after a RapidResponse Server crash. **0**: Do not create **(default).** **1**: Create the file. For more information, see "Internal errors and system crashes" on page 244.
Webplan\ RRMonitor	LimitedDumpOn FirstChance	DWORD	Controls whether a limited dump file is created after an internal error. **0**: Do not create**(default)**. **1**: Create the file. For more information, see "Internal errors and system crashes" on page 244.
Webplan\ RRMonitor	LimitedDumpOn FirstChanceAnalytics	DWORD	Controls whether a limited dump file is created after an internal error. **0**: Do not create**.** **1**: Create the file **(default)**. For more information, see "Internal errors and system crashes" on page 244.
Webplan\ RRMonitor	LimitedDumpOn SecondChance	DWORD	Controls whether a limited dump file is created after a RapidResponse Server crash. **0**: Do not create **(default).** **1**: Create the file. For more information, see "Internal errors and system crashes" on page 244.

Keys	Value	Type	Description
Webplan\ RRMonitor	NoTraversal	DWORD	Specifies whether to include RapidResponse business data in limited and full dump files. **0**: Include the business data **(default).** **1**: Do not include the business data. For more information, see "Internal errors and system crashes" on page 244.
Webplan\ RRMonitor	PkgDirectory	String	Specifies drive and folder where RapidResponse Server Monitor stores diagnostic package files. For more information, see "Internal errors and system crashes" on page 244. If this Registry key does not exist, the diagnostic package files are stored in the **C:\RapidResponse\Packages** folder (default installation). The specified folder must already exist; RapidResponse cannot create it. It is recommended that the default location for the **Packages** folder be moved to different physical drives (not on the same drive as the RapidResponse Server and database). For more information, see "Improve performance by moving default subfolders" on page 251.
Webplan\ RRMonitor	PkgIncludeData Directory	DWORD	Specifies whether to include the entire contents of the **C:\RapidResponse\Data** folder (excluding any PKG files) in complete diagnostic packages. **0**: do not include **1**: include **(default)** For more information, see "Internal errors and system crashes" on page 244.
Webplan\ RRMonitor	PkgIncludeFull Dump	DWORD	Specifies whether the dump file contains more detailed information than the standard dump file created by the RapidResponse Server Monitor service. **0**: standard information **1**: detailed information **(default)** For more information, see "Internal errors and system crashes" on page 244. **Note:** As of RapidResponse 10.1, this setting is ignored.

Keys	Value	Type	Description
Webplan\ RRMonitor	TimeLimit	DWORD	Specifies the time limit to create limited and full dump files. If the time limit is exceeded, only the small dump file is created. The default setting is 300 seconds. If set to 10 (or less), the default value is used. For more information, see "Internal errors and system crashes" on page 244.
Webplan\ ServerConfiguration\ ProcessingRule	ApplyEnvSuffixToEmailSubject	String	Specifies whether to include the name of the computer where RapidResponse Server is installed in email messages generated by RapidResponse. The computer name is appended to the subject of the message. **Y**: append computer name. If blank or any other string, the computer name is not appended. This is the default. This setting can be controlled from the RapidResponse client. For more information, see "Specifying email settings" on page 655.

CHAPTER 31: Monitoring your environment with the RapidResponse Log Service

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Log collection architecture 368
Data collected by the Performance Monitor Service 370
System requirements for the RapidResponse Log Service 372
Installing the RapidResponse Log Service 372
Configuring RapidResponse to provide log information 374
Installing and configuring the Performance Monitor Service 375

The RapidResponse Log Service and the Performance Monitor Service can be used to send logs from your RapidResponse implementation to Kinaxis to be archived. This information can help with troubleshooting and decision making.

RapidResponse Log Service

RapidResponse records logs of operations that are performed. Typically these logs are stored on the computer RapidResponse is installed on, and are overwritten over time. For more information about logs, see "Reviewing system status and operation logs" on page 421.

You can also configure an optional service that records your log entries in a central health monitoring service at the Kinaxis Data Center. This service allows Kinaxis Customer Support to maintain records of your server operations, and provide reports of activities and make recommendations for process changes or maintenance.

The RapidResponse Log Service is installed on a computer in the same network as your RapidResponse Server and RapidResponse Application Server installations. Log entries are sent to Kinaxis continuously through a secure TCP or HTTPS port and encrypted using certificates you generated and exchanged with Kinaxis Customer Support. If required, you can send logs to Kinaxis using a proxy server. All information sent to Kinaxis is also recorded in your log files.

Configuring the RapidResponse Log Service requires assistance from Kinaxis Customer Support to ensure your environment is monitored. A public key is generated after installing the RapidResponse Log Service, which Kinaxis Customer Support requires to enable reporting and monitoring for your logs. In addition, you require the location of the Global Log Aggregator, which the RapidResponse Log Service sends log information to. This location is provided by Kinaxis Customer Support. For more information, see "Installing the RapidResponse Log Service" on page 372.

After installing and configuring the RapidResponse Log Service, log entries are automatically sent to Kinaxis, and reports can be sent to you as required.

In addition to the logs collected by the RapidResponse Log Service, you can collect data relevant to the performance your RapidResponse system using the Performance Monitor Service. This is an optional component that can be installed separately from the RapidResponse Log Service, but which requires the RapidResponse Log Service to function.

Performance Monitor Service

This information gathered by this service can be used in the following ways:

- RapidResponse administrators from your company can view the data to better understand usage and performance trends for your RapidResponse implementation.
- Support agents at Kinaxis can use the data to diagnose problems. Much of the information collected is included in logs that you would otherwise have to send to support to get complex issues diagnosed. The advantages of using the Performance Monitor Service are that support already has the information when you contact them, and they can view archived logs to see what was happening before the problem started.
- Developers at Kinaxis can use the data to understand which customers might be affected by a new or changed feature and what improvements would be useful for the most customers.

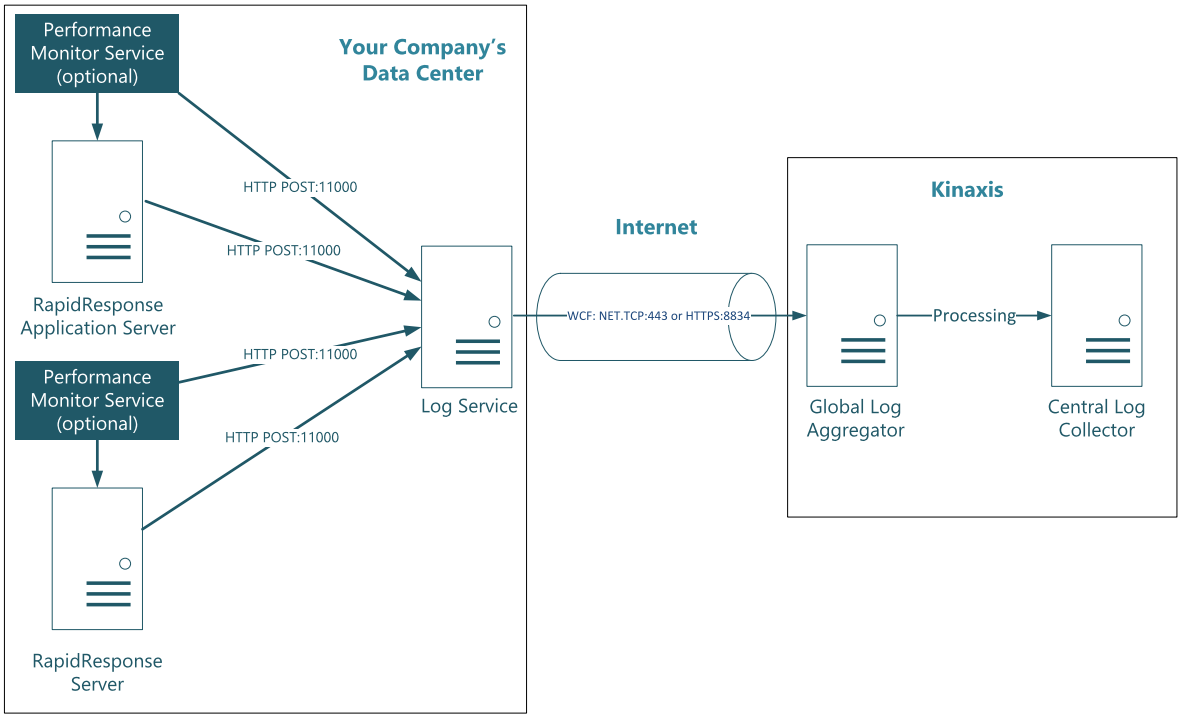
Note: The data collected by the Performance Monitoring Service do not contain enough information to enable anyone to reconstruct your company's planning data. For more information about what is contained in these logs, see "Data collected by the Performance Monitor Service" on page 370.

Viewing data collected by the Performance Monitor Service

The log files are intended to be processed before you view them. For more information, see "Viewing log data in the Central Log Collector" on page 479.

Log collection architecture

The following diagram shows how logs are collected and transmitted when you use the RapidResponse Log Service and the Performance Monitor Service.



Creating logs

RapidResponse Server and RapidResponse Application Server both generate log files. For more information about these log files, see "Reviewing system status and operation logs" on page 421.

The Performance Monitor Service is an optional Windows service that can be installed alongside RapidResponse Server and RapidResponse Application Server. It schedules a collection of plug-ins to gather information related to system performance and write it to log files. For information about the plug-ins and what they collect, see "Data collected by the Performance Monitor Service" on page 370.

Aggregating and forwarding logs

The RapidResponse Log Service aggregates logs collected by RapidResponse Server, RapidResponse Application Server, and the Performance Monitor Service. It then sends them to the Global Log Aggregator Service at Kinaxis, using a secure channel over the Internet. Optionally, a proxy server can be used to forward the logs. Logs from many other RapidResponse systems are also collected by the Global Log Aggregator Service.

Processing and archiving logs

Kinaxis processes logs and then stores the information for one year. Selected data from the logs are made available in reports on the Central Log Collector system. These reports can be viewed by administrators from your company and authorized Kinaxis employees. For more information, see "Viewing log data in the Central Log Collector" on page 479.

Data collected by the Performance Monitor Service

Plug-ins run by the Performance Monitor Service each collect a different type of data. They are run on different schedules, depending on how often it makes sense to collect that type of data.

The following plug-ins are run by this service:

Name	Captures information about...	Frequency
Performance CounterPlugin	RapidResponse's use of system resources, such as memory and processors.	15 minutes
MemoryAnalysis	Memory usage within RapidResponse, including: • How much memory is used out of each pool. • The maximum memory available for each pool.	1 hour
TableInfo	RapidResponse table metadata, such as: • Number of records in the table • How much memory is used by the table	1 hour
ScenarioStats	Scenario information for each scenario, such as: • Name • Parent scenario • Owner • Dates of most recent update, commit, and reset activity • When the scenario was created and (if applicable) shared • How many times a query has been run using this scenario	1 hour
RapidResponse VersionNumbers	The version numbers of RapidResponse components: • RapidResponse Server • RapidResponse Application Server • RapidResponse Service Host • RapidResponse Server Monitor	12 hours
HardwareInfo	The hardware specifications and operating system of the machine that RapidResponse is running on.	1 day
LicenseDetails	• License keys • User licenses • Site licenses	1 day
AnalyticsDetails	How long it takes to calculate the following analytics and how many results are returned: • Netting • Activity • CTP • CTPActivity • FLP	1 day

Name	Captures information about...	Frequency
UserMetaData	Registered users. The following data are collected for each user: • Name • License type • Country • Location • Membership in the External user group	1 day
Scheduled TaskMonitor	Information about scheduled system tasks. In RapidResponse, this information can be viewed in the Scheduled System Tasks workbook.	1 day
RegistrySettings	Windows registry keys related to RapidResponse. Determines whether RapidResponse data is stored on a network share, and if so, what the UNC path of the Data folder is.	1 day
Processing RulesPlugin	Processing rules. In RapidResponse, these processing rules can be viewed in the RapidResponse Administration workbook, on the Processing Rules worksheet.	1 day
SSOEnabledPlugin	Whether SSO is enabled. If SSO is enabled, the plugin looks for configuration information, such as whether the certificate is embedded or contained in a file.	1 day
CustomerExtract	Usage patterns, including: • How many resources of different types exist on your system. • Which RapidResponse applications are used. • Which analytics are used. • The numbers of records in some tables in the root scenario. • Numbers of users and groups of different types. • How often certain analytics are used.	2 days
QE2Fallback	Attributes that are defined by expressions that are not compatible with the multi-threaded version of the query engine. These expressions cause RapidResponse to fall back to an older version of the query engine that does not support multi-threading. This can have a negative impact on performance.	2 days
UserPermissions	Information about permissions granted to the External user group.	2 days
Workbook Features	Information about individual resources, such as workbooks or filters, that exist in the system. This includes general information such as who owns the resource, how many times it has been used, and how it is configured. Configuration information is limited to statistics about which options are selected in resource properties. For example, the number of conditionally hidden worksheets in a workbook is recorded. Details, such as the expressions used to determine whether worksheets are hidden, are not collected.	10 days

Note: Frequency intervals start from the time the RapidResponse Performance Monitor Service is started. If the service is unable to connect to RapidResponse, it tries again during the next run interval.

System requirements for the RapidResponse Log Service

The RapidResponse Log Service requires the following.

Requirement	Supported and Verified
Operating System	Microsoft Windows 7 SP1 (64-bit) Microsoft Windows 8 (64-bit) Microsoft Windows 8.1 (64-bit) Microsoft Windows 10 (64-bit) **Note:** In addition to the using the correct Windows Service Pack (SP), it is advisable that the operating system also include the latest Windows Updates.
Processor	1.5 GHz with two cores
Physical memory	2 GB of RAM
Disk space	7 GB per RapidResponse installation being monitored
Operating system components	Microsoft .NET Framework 4.5 Can be downloaded from http://msdn2.microsoft.com/en-us/netframework/default.aspx.

Ports required for the RapidResponse Log Service

The RapidResponse Log Service collects log entries from each instance of RapidResponse Server and RapidResponse Application Server you have configured. The log entries are sent across your network to the RapidResponse Log Service over HTTP port 11000. You must ensure this port is open between each computer you have installed RapidResponse Server or RapidResponse Application Server on and the computer you have installed the RapidResponse Log Service on.

The RapidResponse Log Service also connects to the global log collection system at the Kinaxis Data Center using one of the following ports, depending on the protocol you select when you install the Log Service:

- 8834 (NET.TCP)
- 443 (HTTPS)

The data passed to the Kinaxis Data Center is encrypted using a certificate generated when you install the RapidResponse Log Service. Ensure that the required port is opened to allow Kinaxis Customer Support to monitor your logs and perform health monitoring operations.

Installing the RapidResponse Log Service

The RapidResponse Log Service should be installed on a separate computer or virtual machine in the same network as your RapidResponse Server and RapidResponse Application server installations. The RapidResponse Log Service requires information from Kinaxis Customer Support, and produces a public key that Kinaxis Customer Support requires to enable monitoring and reporting for your log entries.

▸Install the RapidResponse Log Service

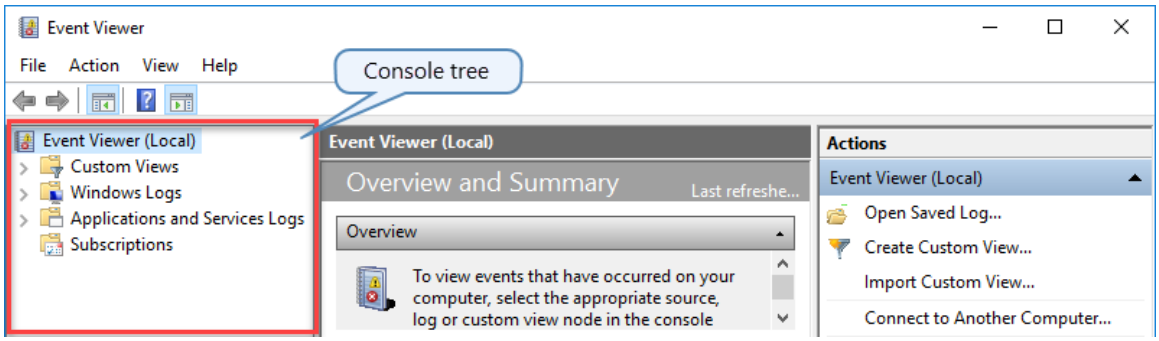
1. Log on as a Windows administrator on the computer you will be installing the RapidResponse Log Service on.
2. To obtain the installation file, download the installation file from https://knowledge.kinaxis.com/s/article/Monitoring-your-environment-with-the-RapidResponse-Log-Service-Component-Download.
3. Unzip the installation file, browse to the **LogService** folder, and then run **setup.msi**.
4. On the **Welcome** screen, click **Next**.
5. On the **License Agreement** screen, review the information. Select **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Destination Folder** screen, optionally specify a folder to install the RapidResponse Log Service in, or use the default. Click **Next**.
7. On the **Temporary Folder** screen, specify the location the RapidResponse Log Service stores log files in before they are sent to the Kinaxis Data Center. Click **Next**.
8. On the **Data Center Information** screen, specify your **Customer Name** and the address for the **Global Log Aggregator**. Contact Kinaxis Customer Support to obtain this information. Ensure you specify the information exactly as it is provided, otherwise the RapidResponse Log Service might not be able to communicate with the Data Center.
9. Optionally, if you want to use a proxy server to forward logs to the Global Log Aggregator, select **Use HTTPS instead of TCP** and then specify the address of your proxy server in the **HTTP Proxy Server** box.
10. Click **Next**.
11. Click **Install**.

▸Validate the Installation of the Log Service

After installing the Log Service, follow these steps to check that the installation was successful. If the installation was not successful, contact Kinaxis Customer Support for help.

1. Check that the Log Service is started.
   - Open the **Services** pane (part of the Microsoft Management Console.)
   - Ensure that status of **RapidResponse Log Service** is **Running**. If it is not running, select the service in the list and then click **Start**.

     If the service is not running and cannot be started, the installation was not successful.
2. Check for error events in Windows logs.
   - Open the **Event Viewer** pane (part of the Microsoft Management Console).
   - Ensure that the console tree is displayed. If you do not see the console tree, click **View** > **Customize** and then select **Console tree**.



- In the Console tree, expand the **Applications and Services Logs** node and then click **RapidResponse**. Check for any errors with the **LocalLogAggregationService** source.

  If there are errors, the installation was probably not successful. Review any error messages, check that you have completed all of the steps in the installation procedure, and ensure that your firewall configuration does not interfere with the service. For information, see "Ports required for the RapidResponse Log Service" on page 372.

3. While RapidResponse and the Log Service are running, in Windows Explorer, open the folder that you specified on the Temporary Folder screen. If the Log Service is working correctly, files with names that begin with the customer name that you specified on the Data Center Information screen during installation will be added and then removed from this folder every few seconds.

▸Provide the public key to Kinaxis Customer Support

1. Navigate to the folder you installed the RapidResponse Log Service in.

   By default, this is **C:\Program Files\Kinaxis\RapidResponse Log Service**
2. Locate a certificate file named **Kinaxis_LLA_<CompanyName>_<MachineName>.cer**.
3. Add this file to an encrypted .zip file, and specify a password for the file.
4. Contact Kinaxis Customer Support for instructions on where to send this file, and to communicate the password.

Configuring RapidResponse to provide log information

After installing the RapidResponse Log Service, you can configure each instance of RapidResponse Server or RapidResponse Application Server to send log files to the RapidResponse Log Service. This is done using the RapidResponse Log Service Configurator utility provided on the Kinaxis Knowledge Network.

The configuration requires the location of the RapidResponse Log Service, the folders the server logs, the Application Server, and the RapidResponse Service Host service are stored in, and a folder used to store the logs before they are sent to the RapidResponse Log Service. This folder can be created automatically during the configuration process.

The folder you specify for sending the log files to the RapidResponse Log Service should be used only for storing the log files that are sent. Folders for each type of log file the RapidResponse Log Service sends are created automatically in this folder.

After you configure the log folders, you can review a log output to verify the configuration is correct. This output is provided in the folder you run the RapidResponse Log Service Configurator from.

The RapidResponse Log Service Configurator restarts the RapidResponse Application Server and RapidResponse Service Host during the configuration process. Any users who are signed in to RapidResponse when you configure the log service are disconnected.

▸To configure a RapidResponse instance to send logs

1. Log on as a Windows administrator on the computer you have installed RapidResponse Server or RapidResponse Application Server on.
2. Download the RapidResponse Log Service Configurator utility from the Kinaxis Knowledge Network.
3. Run the RapidResponse Log Service Configurator utility.
4. In the **RapidResponse Log Service** box, specify the name of the computer the RapidResponse Log Service is installed on.
5. In the **Server Logs Directory** box, specify the folder RapidResponse Server stores its log files in. By default, this is the **RapidResponse\Logs** folder.
6. In the **ServiceHost Directory** box, specify the location the RapidResponse Service Host service is installed in. By default, this is the **RapidResponse\Program\ServiceHost** folder.
7. In the **App Server Directory** box, specify the folder the RapidResponse Application server is installed in. By default, this is the **Program Files\Kinaxis\RapidResponse\Web** folder.
8. In the **Temp Log Directory**, specify the folder the logs are stored in before they are sent to the RapidResponse Log Service.
9. Click **Save and Run**.

▸To review the configuration

1. Navigate to the folder you ran the RapidResponse Log Service Configurator utility from.
2. Open the log file in a text editor.
3. If errors are reported, run the configuration utility again and specify the correct options.

Installing and configuring the Performance Monitor Service

The Performance Monitor Service is an optional Windows service that logs information related to system performance on RapidResponse Application Server and RapidResponse Server installations. For more information, see "Performance Monitor Service" on page 368.

If both the RapidResponse Application Server and the RapidResponse Server components are installed on the same computer, you only need to install the Performance Monitor Service once on that computer. If the components are installed on different computers, though, the Performance Monitor Service needs to be installed on each of them.

Before installing the Performance Monitor Service:

- RapidResponse Log Service needs to be installed on a computer in the same network as your RapidResponse Server and RapidResponse Application Server installations.
- Microsoft .NET Framework version 4.5.2 or later needs to be installed on the server where you are going to install the Performance Monitor Service. It can be downloaded from http://msdn2.microsoft.com/en-us/netframework/default.aspx.

▸Install the Performance Monitor Service

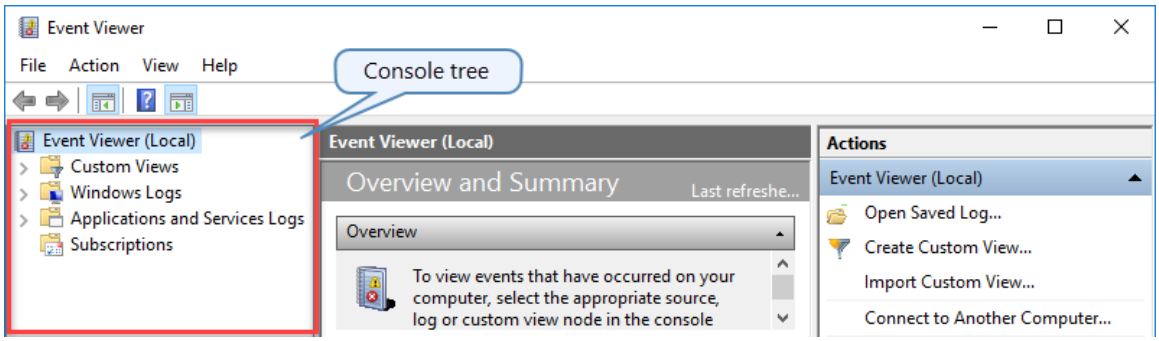
1. To obtain the necessary files, download the zipped installation file from https://knowledge.kinaxis.com/s/article/Monitoring-your-environment-with-the-RapidResponse-Log-Service-Component-Download. Unzip the folder and place the contents on the server where you are installing the Performance Monitor Service.
2. Run **PerfMonSetup.msi** as an administrator.
3. In the **Kinaxis RapidResponse Performance Monitor Setup** dialog box, provide the following information:
   - **Log Folder**—the path where the service stores logs that it generates if it cannot connect to the Log Service.
   - **Server Address**—The server name or IP address of the computer hosting the Log Service.
   - **Server Port**—The port used by the Log Service to receive logs (typically 11000).
4. Click **Next** and then click **Finish**.
5. Validate the installation of the Performance Monitor Service to ensure that it is installed correctly. For more information, see "Validate the Installation of the Performance Monitor Service" on page 376.

▸Validate the Installation of the Performance Monitor Service

After installing the Performance Monitor Service, follow these steps to check that the installation was successful. If the installation was not successful, contact Kinaxis Customer Support for help.

1. Check that the Performance Monitor Service is started.
   - Open the **Services** pane (part of the Microsoft Management Console.)
   - Ensure that status of RapidResponse Performance Monitor Service (**RapidResponse PerfMonitor Service**) is **Running**. If it is not running, select the service in the list and then click **Start**.

     If the service is not running and cannot be started, the installation was not successful.
2. Check for error events in Windows logs.
   - Open the **Event Viewer** pane (part of the Microsoft Management Console).
   - Ensure that the console tree is displayed. If you do not see the console tree, click **View** > **Customize** and then select **Console tree**.



   - In the Console tree, expand the **Applications and Services Logs** node and then click **RapidResponse**. Check for any errors with the **PerfMonitorService** source. If there are any errors, the installation was not successful.

▸Configure the Performance Monitor Service

After installing the Performance Monitor Service, specify the scenario that the AnalyticsDetails plug-in will use to determine how long it takes to calculate key analytics. Choose the shared scenario that best represents your complete data and analytic usages, primarily used by the majority of users for daily planning. If you are not sure which scenario to use, refer to the Scenarios workbook for scenario usage statistics.

1. In the **Administration** pane, under **User Accounts**, select **User Profile Variables**.
2. In the **Profile Variables** worksheet of the **Macros and Profile Variables** workbook, insert a new record. Use the following data values:
   - **User ID or Group**: All Users
   - **Variable Name**: AnalyticE2EScenario
   - **Type:** Permanent
   - **Data Value**: <The name of your chosen scenario>
   - **Display Value**: <The name of your chosen scenario>

Notes:

- Because only shared scenarios can be used by the AnalyticsDetails plug-in, you do not need to specify the scope of the scenario. The name by itself is sufficient.
- If the AnalyticE2EScenario profile variable is not specified or is not valid, the AnalyticsDetails plug-in uses the root scenario for its calculations.

Part 5: System management for On-Premises and On-Demand environments

- "Commands and scheduling system tasks" on page 381
- "Reviewing system status and operation logs" on page 421
- "RapidResponse system workbooks reference" on page 481

CHAPTER 32: Commands and scheduling system tasks

Predefined scheduled system tasks 381
RapidResponse system commands 384
Scheduling RapidResponse commands 412
Using commands and scheduled system tasks 415
Run-time windows for scheduled system tasks 417
Turning off all scheduled system tasks 418
Logged messages for scheduled tasks 418

RapidResponse includes preconfigured scheduled system tasks that run RapidResponse commands. Most of the commands are related to data management operations and are managed through the Administration pane of the RapidResponse client.

On-Demand: Some RapidResponse commands are only available to the Master Administrator at Kinaxis. However, when using a RapidResponse test environment, RapidResponse administrators have the same tools, functionality, and permissions as the Master Administrator at Kinaxis.

Predefined scheduled system tasks

RapidResponse includes predefined scheduled system tasks. The number of tasks is dependent on whether you are using an on-demand or on-premises version of RapidResponse.

Each scheduled task runs a RapidResponse command. For more information about the commands associated with each scheduled task, see "RapidResponse system commands" on page 384. The following table provides an overview of the scheduled task included with RapidResponse.

On-Demand: System and data administrators might not have access to all scheduled system tasks available with RapidResponse. Some scheduled system tasks such as data import are only available to the Master Administrator at Kinaxis. However, when using a RapidResponse test environment, RapidResponse administrators have the same tools, functionality, and permissions as the Master Administrator at Kinaxis.

On-Premises: System administrators can view, run, and edit all predefined scheduled system tasks. Data administrators can only view, run, or edit some scheduled system tasks.

Some of the tasks discussed in this section make RapidResponse unavailable to users. You can inform users of any scheduled maintenance that impacts them ahead of time. For more information, see "Communicating with users" on page 593.

The following tables lists the default scheduled tasks available in RapidResponse. If you are using an On-Demand system then only the Data Update task is available.

Predefined scheduled system tasks	Task description (and RapidResponse command)
Auto-delete	Determines whether data in some system tables has exceeded the age deletion threshold, and if it has, deletes it from the RapidResponse database. **Caution:** Disabling this task can lead to the excessive growth of system records which can consume significant amounts of system memory. **Note:** Not available to data administrators. **RapidResponse command:** "DataExpiry command" on page 389
Capture	Writes transactional data changes to the RapidResponse database, which includes one or more DFS folders. When run, it forces a Snapshot command, applies the transactional data from the XACT database files to a new DFS hive folder, and deletes all the processed XACT files. A new active transaction file is then created. **Note:** Not available to data administrators. **RapidResponse command:** "Capture command" on page 385
Condense	Creates a new main database file by combining all the DFS folder in the hive. The new file represents the complete database as of the time the operation began. **Note:** Not available to data administrators. **RapidResponse command:** "Condense command" on page 387
Checkpoint and Version Reclaim	As of RapidResponse 11.0, the Checkpoint command has been replaced by the following commands: • "Snapshot command" on page 409 • "Capture command" on page 385 • "Condense command" on page 387 On upgrade to RapidResponse 11.0 (or later) from RapidResponse 10.1 (or earlier), all scheduled tasks that use the Checkpoint command are disabled. The Checkpoint command continues to function but it is strongly recommended it no longer be used. Running the Checkpoint command is the equivalent to running the Capture command. For more information, see "Checkpoint command" on page 386.
Create Backup	Creates a backup of the RapidResponse database. This data backup, or data package, can be used to move data and configuration settings from a test server to a production server or to restore data files in the case of disk crash or power failure. This task is automatically enabled after RapidResponse is installed. If deleted, RapidResponse recreates and re-enables it the next time it starts. If this task is disabled, RapidResponse does not re-enable it. **RapidResponse command:** "CreateDataPackage command" on page 388

Predefined scheduled system tasks	Task description (and RapidResponse command)
Data Import (delete non-permanent scenarios)	Imports a complete enterprise data set into RapidResponse. This task relies on the data import and data update processes being configured as explained in the *RapidResponse Data Integration Guide*. **Caution:** Performing a data import overwrites the Enterprise Data (root scenario) and Approved Actions scenarios with new data. Any child scenarios of these scenarios are deleted and users must create new scenarios. **RapidResponse command:** "DataImport command" on page 390
Data Update	Initiates the data update process as described in the *RapidResponse Data Integration Guide*. **RapidResponse command:** "DataUpdate command" on page 395
Database Integrity Check	Performs a test on the RapidResponse database for invalid references and inconsistent counts. This task is automatically enabled after RapidResponse is installed. If deleted, RapidResponse recreates and re-enables it the next time it starts. If this task is disabled, RapidResponse does not re-enable it. This task is also part of the DIC group of scheduled system tasks. By having Database Integrity Check scheduled task part of a different group than the other default scheduled system tasks, it can run concurrently with other commands including Restart, and CreateDataPackage. For more information, see "Running scheduled tasks concurrently" on page 417. **Note:** If a database error is discovered, you should disable the running of this task until the problem is resolved. This will prevent unnecessary messages from being delivered and data packages from being created. **Note:** Not available to data administrators. **RapidResponse command:** "DataIntegrityCheck command" on page 391
Prune Backup Packages	Deletes all saved backup data packages except for the two most recently created. The Create Backup schedule task that creates data packages is scheduled, by default, to run every day. Creating a backup package daily could use a significant portion of hard disk space on the RapidResponse Server computer. Without enough free disk space, RapidResponse Server commands such as Condense might not properly execute. As such, it is important to manage the number of data packages saved to ensure they do not consume all the free disk space. **RapidResponse command:** "PruneFiles command" on page 406
Restart	Runs the Capture command, and then stops and restarts RapidResponse Server. **RapidResponse command:** "Restart command" on page 407

Predefined scheduled system tasks	Task description (and RapidResponse command)
Snapshot	Running the **Snapshot** command closes the active transaction data file. A new active file is then created. The XACT file with the latest timestamp is considered the active transaction file. Each transaction data file contains the full set of transactions that have been executed between the time it was created and the time it was closed. The transaction data files that are not active cannot accept changes. **Note:** Not available to data administrators. **RapidResponse command:** "Snapshot command" on page 409
Version Reclaim Sweep	Running the **VersionReclaimSweep** command cleans up the internal version structure used to support scenarios. The version reclaim process reduces the size the RapidResponse database and frees system memory. When the **VersionReclaimSweep** command runs, it write-locks the RapidResponse database. As such, it should only be run during low user activity periods. Before running this command, run the Condense command. For more information, see "Condense command" on page 387. **Note:** Not available to data administrators. **RapidResponse command:** "VersionReclaimSweep command" on page 411

Not all these tasks are automatically enabled during the RapidResponse installation or integration. You can modify the properties of each task including schedule time and command arguments.

RapidResponse system commands

RapidResponse system commands can be configured to run automatically as a scheduled task or on demand. Some of the RapidResponse commands take arguments that are used to specify how the command should perform. For more information about running a command on demand, see "To run a RapidResponse command/scheduled task on demand" on page 416. For more information about scheduling a command, see "To create or modify a RapidResponse scheduled task" on page 416.

The following commands are available in On-Demand and On-Premises RapidResponse systems.

- "DataSynchronize command" on page 393
- "DataUpdate command" on page 395
- "DeleteData command" on page 402
- "DeleteEnterpriseData command" on page 403
- "ExtractData command" on page 403
- "ExtractNetChangeData command" on page 404
- "ScenarioCommit command" on page 408
- "ScenarioReset command" on page 408
- "ScenarioUpdate command" on page 409

The following commands are available in On-Premises RapidResponse systems only.

- "Capture command" on page 385
- "Checkpoint command" on page 386
- "Condense command" on page 387
- "CreateDataPackage command" on page 388
- "DataExpiry command" on page 389
- "DataImport command" on page 390
- "DataIntegrityCheck command" on page 391
- "DeleteFiles command" on page 403
- "FilterTT command" on page 406
- "PruneFiles command" on page 406
- "Restart command" on page 407
- "RunAddin command" on page 407
- "Snapshot command" on page 409
- "VersionReclaim command" on page 411
- "VersionReclaimSweep command" on page 411

Notes:

- Some commands can also be run using a script. For more information, see the *RapidResponse Scripting Guide*.
- Commands can also be run in a Microsoft Windows command window or batch file by using the **ServerCommand** command. For more information, see "Automatic server operations with ServerCommand" on page 339.
- All scenarios specified in command arguments are assumed to be shared.

Capture command

The Capture command writes transactional data changes to the RapidResponse database, which includes one or more DFS folders. When run, it forces a Snapshot command, applies the transactional data from the XACT files to a new single DFS hive folder (also called a *database fragment*) , and deletes all the processed XACT files. A new active transaction file is then created.

If the total size of the transaction data files (XACT files) exceeds 1 GB, the Capture command automatically runs and a new active transaction data file is created.

The Capture command also runs when the RapidResponse Server service is started.

It is recommended that the Capture command be scheduled to run once a day during the lightest system load. The Capture operation has no direct impact on RapidResponse users or other RapidResponse Server tasks. Users can run queries (for example, open reports), create scenarios, and change data. System operations such as data update are not impeded.

For more information about DFS folders and the Condense command, see "DFS folders" on page 312.

This command is not available to data administrators. This command is available for use in RapidResponse scripts. For more information, see the **executeCapture** method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Notes:

- This command is not available in On-Demand RapidResponse systems.
- If the total size of the transaction data files (XACT files) exceeds 1 GB, the Capture command automatically runs and a new active transaction data file is created.

Checkpoint command

As of RapidResponse 11.0, the Checkpoint command has been replaced by the following commands:

- "Snapshot command" on page 409
- "Capture command" on page 385
- "Condense command" on page 387

On upgrade to RapidResponse 11.0 (or later) from RapidResponse 10.1 (or earlier), all scheduled tasks that use the Checkpoint command are disabled.

The Checkpoint command continues to function but it is strongly recommended it no longer be used.

Upgrade notes

The following summarizes other changes related to the replacement of the Checkpoint command.

- The Checkpoint command no longer supports the optional running of a scenario version reclaim. If you had been using this option, consider scheduling the VersionReclaim command. For more information, see "VersionReclaim command" on page 411.
- Prior to RapidResponse 11.0, clicking the Pause button for RapidResponse Server in the Windows Services dialog box ran the Checkpoint command. The Pause button remain active but does not execute any actions. For more information, see "The Windows Services dialog box" on page 232
- The Checkpoint command in webplanSC is no longer supported. If you had been using the command from the Windows Command window or batch scripts, consider converting these processes to ServerCommand operations using the new commands. For more information see, "Automatic RapidResponse Server operations " on page 335.
- The Restart command in webplanSC no longer performs a checkpoint prior to stopping the RapidResponse Server. For more information see, "Automatic server operations with webplnSC" on page 335.
- The RapidResponse Script method **executeCheckpoint** continues to function. It is recommended you modify existing scripts to use **executeCapture**. For more information, see the *RapidResponse Scripting Guide*.
- If you are still using RapidResponse OpenAPI, you need to be aware the ServerCheckpoint server exit no longer functions and the CheckpointServer session method runs a Capture command.

Previous description of Checkpoint command (RapidResponse 10.1)

Changes made to RapidResponse data and resources, such as workbooks or filters, are saved in-memory. These transactional changes are also saved in a temporary location in the **m-rr-data.*timestamp*.ifs** database file so that they are available for recovery in case of a system failure.

The Checkpoint command moves the transactional data changes from in-memory to the **m-rr-data.*timestamp*.ifs** and **d-rr-data.ifs** database files.

The Checkpoint command can be configured through arguments to do a scenario version reclaim (the **Checkpoint and Version Reclaim** scheduled task is configured to do so).

This command is not available to data administrators. This command is available for use in RapidResponse scripts. For more information, see the **executeCheckpoint** method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Argument	Description	Value
forceVersion Reclaim	Optional argument that specifies whether to perform a version reclaim when checkpointing.	**0**—disables the version reclaim option (default if not present). **1**—enables the version reclaim option.

Note: This command is not available in On-Demand RapidResponse systems.

Condense command

The Condense command creates a new main database file by combining all the DFS folders in the hive. The new file represents the complete database as of the time the operation began. When the Condense operation begins, it forces a Capture command. When Condense completes, all the previously created DFS folders are deleted.

Running the Condense command can significantly reduce the amount of disk space in use.

It is recommended that the Condense command be scheduled to run once a week before the RapidResponse Server is scheduled to be restarted.

However, if your company has many data changes (either in the enterprise system or in the RapidResponse database), you might want to run the Condense command more frequently. System administrators are warned when available disk space falls below a configured threshold. For more information, see "Disk space warnings" on page 314.

The Condense operation has no direct impact on RapidResponse users or other RapidResponse Server tasks. Users can run queries, create scenarios, make changes to data. System operations such as data update are not impeded. However, the Condense command does make heavy use of system memory.

For more information about DFS folders and the Condense command, see "DFS folders" on page 312.

This command is not available to data administrators. This command is available for use in RapidResponse scripts. For more information, see the **executeCondense** method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Note: This command is not available in On-Demand RapidResponse systems.

CreateDataPackage command

This command creates an archive, or package, of the RapidResponse database files. This can be used to move data from a test server to a production server, from a production server to a test server, or to restore data files in the case of disk crash or power failure.

This command backs up the following files and folders:

- C:\RapidResponse\Data
- C:\RapidResponse\Logs
- C:\RapidResponse\History
- manifest file

The manifest file includes the name of the RapidResponse Server, the server ID, the date and time the package was created, and the full path names, time stamps, and sizes of the other files in the package.

The backup files, by default, are stored in a compressed file named **backup_*ServerName*_YYMMDD-HHMMSS.pkg**. The date and time specified in the file name is based on the local time on the RapidResponse Server.

If you are restoring a system using a package, you can use either a data or archive package. If you have loaded multiple packages, the file with the latest timestamp is used to restore the database. The data loaded from a data or archive package is identical, but the archive package provides the history of your data and system.

The files in the package file are compressed by about 80 to 90 per cent. You should ensure you have enough disk available for the package files. For information about decompressing packages, see "Decompressing packages and Packages folder" on page 251.

The Create Backup scheduled task that creates data packages is scheduled, by default, to run every day. Consider using the PruneFiles command to delete older versions or no longer needed versions to save hard disk space. For more information, see "PruneFiles command" on page 406.

This command is available for use in RapidResponse scripts. For more information, see the executeCreateDataPackage method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

For more information about archiving or backing up data, see "Backing up RapidResponse program files" on page 314.

Argument	Description	Value
filename	Optional argument that specifies the folder and file name of the backup files package.	Text that specifies the folder, file name, or both. For example, **C:\backup** specifies a folder and **C:\backup\rr.pkg** specifies a folder and file name. If a folder name is not specified then the package is stored in the **C:\RapidResponse\Packages** folder. If a file name is not specified then the package is named **backup_*ServerName*_*timestamp*.pkg**.
type	Optional argument that specifies whether to only include log files in the package file. You might want to create an package that contains only log files if you need to send information to Kinaxis Customer Support and do not want to send data.	**Logs**—only include log files in the package file. If any other value is used then the package file includes data and log files. This is the default if not present.

Note: This command is not available in On-Demand RapidResponse systems.

DataExpiry command

RapidResponse logs information about various activities such as user sign-in attempts and data changes. This information is stored in the RapidResponse database. Over time, these system records can grow in size and potentially consume significant amounts of system memory. To prevent excessive growth of these system records, use the RapidResponse DataExpiry command to delete old system records.

This command determines whether system records have exceeded the age deletion threshold and, if they have, deletes them from the RapidResponse database. This command is not available to data administrators.

This command is available for use in RapidResponse scripts. For more information, see the executeDataExpiry method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

This command does not take arguments. However, you specify the age deletion thresholds for different types of system records in the **Auto-delete Configuration** worksheet of the **Scheduled System Tasks** workbook.

▸To change the age deletion threshold for system records

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. Click the **Auto-delete Configuration** tab.
3. Locate the specific record type you want to change and in the **Maximum Record Age** column type in the number of days to preserve the system records.

For more information about specifying thresholds, see " Automatic deletion of system records" on page 277.

Note: This command is not available in On-Demand RapidResponse systems.

DataImport command

This command performs a data import, and stops and restarts RapidResponse. Normally a data import is performed only once as part of the RapidResponse configuration process. It is assumed that your company will import data only once. However, there are cases where you might want to re-import data.

For example, if RapidResponse Server encounters a problem that causes it to stop running you might need to perform a data import to ensure the RapidResponse data is valid. You might also want to re-import to reset the RapidResponse database.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423. This command also persists specified data provided you set up data persistence. For more information, see "Data persistence" on page 329.

For more information about the data import processes, see the *RapidResponse Data Integration Guide*.

Caution: Performing a data import overwrites the Enterprise Data and Approved Actions scenarios with new data. Any child scenarios of these scenarios, unless set as permanent, are deleted and users must create new scenarios.

For more information about data imports, see "Reviewing system status and operation logs" on page 421.

Argument	Description	Value
EnableLastKnownGoodPackage	Optional argument that specifies whether to create a set of data files in the package that could be used to restore RapidResponse to its state before the data import occurred. This can be used in cases where the data import is not acceptable or turned off while testing an import to save time. The package is stored in the **C:\RapidResponse\Packages** folder and is named **PreDataImport.pkg** or **PreDataImport.zip**. The file set in the package is the same as that created by the CreateDataPackage command and uses the same file naming convention. For more information, see "CreateDataPackage command" on page 388.	**False**—disables the creation of the data file set. **True**—enables the creation of the data file set (default if not present). Any value other than True is treated as False.
EnableQuality Checks	Optional argument that specifies whether to test extract files during a data import against the extract files used in the most recent successful data import or update to determine if they meet data change tolerance settings. Not testing the extract can save significant time in the data import process. For more information about data testing, see the *RapidResponse Data Integration Guide*.	**False**—disables the testing (default if not present). **True**—enables the testing. Any value other than True is treated as False.

Argument	Description	Value
EnableSaveHistory	Optional argument that specifies whether after the completion of the data import, to copy the contents of the **\Working** folder to the **\History*timestamp*.DataImport**folder. Not copying the contents can save significant time in the data import process and it might not be required in a test environment. For more information, see the *RapidResponse Data Integration Guide*.	**False**—disables copying the contents. **True**—enables copying the contents (default if not present). Any value other than True is treated as False.

Note: This command is not available in On-Demand RapidResponse systems.

DataIntegrityCheck command

This command performs a test on the RapidResponse database for invalid references and inconsistent counts in scenarios. This procedure is called a data integrity check and can alert you in advance of potential operational problems with RapidResponse. Taking a proactive approach, rather than waiting for a system problem or failure, can potentially and significantly reduce system downtime. For more information, see " RapidResponse database integrity" on page 327.

This command is available for use in RapidResponse scripts. For more information, see the executeDataIntegrityCheck method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423. In addition, issues are written to the **Server.log** log file and a message is sent to all system administrators.

You should contact Kinaxis Customer Support for assistance if any warnings or errors occur after running the DataIntegrityCheck system command.

Argument	Description	Value
MaxPlans	Optional argument that specifies the number of scenarios that are verified by the DataIntegrityCheck command. The order in which the scenarios are verified is determined by their level in the scenario tree. The Enterprise Data (root) scenario is considered the top level of the tree and is checked first. The Enterprise Data scenario's direct children are verified next and so on.	A positive integer specifying the number of scenarios. If a value is not present then the default is 8,192 which is the maximum number of scenarios that can exist in the RapidResponse database.
MaxPlanDepth	Optional argument that specifies the depth of scenarios in the scenario tree that are verified. For example, the depth of the Enterprise Data (root) scenario is 0 and any direct children of this scenario are considered to be at a depth of 1 in the scenario tree.	A positive integer specifying the scenario depth. If a value is not present then the default is 1.

Argument	Description	Value

Plans	Optional argument that specifies the scenarios to test.	A comma separated list of scenarios to test. Private and shared scenario names must be specified using the ?Shared and ?Private notation. For example:
		`?Shared:ABC, ?Private:XYZ`
		You can only test the private scenarios you own.
		If your RapidResponse system is using unique scenario names, do not use the shared and private notation. For example:
		`ABC,XYZ`
		For more information, see "Non-unique scenario names" on page 170.

Notes:

- You can control whether the database integrity check stops after detecting one problematic scenario by changing the **IntegrityCheckMaxProblemPlans** values in the Windows Registry. For more information, see "IntegrityCheckMaxProblemPlans" on page 353.

Blocking specific tests

The Data Integrity Check command can be configured to block four types of tests on a scenario-by-scenario basis.

By blocking some tests you can improve the Data Integrity Check command performance. You might consider blocking some tests because there might not be a way to resolve the underlying issue. For example, the introduction of vector data (RapidResponse 2014.4) might have resulted in instances where two (or more) records in a vector set have the same key value (a key-uniqueness issue). This can be a difficult and time consuming problem to overcome, especially in historical scenarios.

The following tests can be blocked from running:

- **DuplicateKeys**—Tests whether two (or more) records in a set have the same key value (key uniqueness). For example, two or more records in the HistoricalDemandHeader table have the same primary key.
- **InconsistentSet**—Tests whether the number of records in a set on one table matches the number of records in the same set on a different table. For example, the OnHands set on the Location table reports 100 records but the OnHands set on the Part table reports 101.
- **IncorrectReference**—Tests whether a record refers to a record in another table but that record does not contain the referencing record in its set. For example, a record in the OnHand table refers to a Part record that does not contain that OnHand record in its OnHands set.
- **IncorrectSort**—Tests that the vector data is correctly sorted. For example, records might be sorted by a means other than date.

Use the Database Integrity Check Configuration worksheet in the Scheduled System Tasks workbook to specify tests to block from running.

Task Arguments | Extract Definitions | Extract Filters | Auto-delete Configuration | Database Integrity Check Configuration

	Scenario	Edit Scenario	Table (Namespace::Table)	Omit Test for Error Type	Scenario Owner
1	Baseline	Baseline	Mfg::PlanningCalendars	DuplicateKeys	Admin
2	Rajiv Test	?sequenceNumber:273290354	Mfg::PartType	InconsistentSet	Admin

The following settings are required to block Data Integrity Check tests:

- **Scenario**—Specifies the name of the scenario where the test is blocked.

  You can type a shared scenario's name, and you can use wildcard characters (* and ?) to specify a range of scenario names. You can also use * to include all shared scenarios. Private scenarios are not recognized, even if their names match.

  You can also refer to scenarios by their unique sequence numbers, which can be found in the Scenarios workbook. Use the following syntax:

  ?sequenceNumber:*sequence number*

  Example: `?sequenceNumber:2006172072`

  The only way to specify a private scenario is to use its sequence number.

- **Table**—Specifies the namespace and table name where the test is blocked. You can use wildcard characters (* and ?) to specify table names. You can also use * to specify all tables.
- **Omit Test for Error Type**—Specifies the test to block.

Notes:

- This command is not available in On-Demand RapidResponse systems.
- To change the scenario used in an existing Database Integrity Check Configuration record, type a new scenario name in the Edit Scenario field. When you save your changes, the Scenario field is updated.
- The Data Integrity Check command logs warning information about failed tests in the Administration Log workbook. This includes tests for records that have the same key value (key uniqueness) and vector data is incorrectly sorted. For more information, see " System administration logs" on page 423.

DataSynchronize command

This command initiates the data update process on a set of data extract folders. These folders are typically created as named extracts by the ExtractData or ExtractNetChangeData commands, and include a timestamp in the folder name. Because the extract folder names cannot be predicted, this command uses the generated extract folders' parent folder and then processes the data in the order the extracts were created. All folders processed by this command must contain a timestamp, otherwise they are ignored by the update process.

The extract commands create tab-delimited data files with one record per line, so the DataSynchronize command requires all files in the extract folders in this format. If your extracted data contained Notes fields, these values are flattened into a single line, with characters inserted to show where the new lines were. For more information, see "ExtractData command" on page 403 or "ExtractNetChangeData command" on page 404.

Data from each extract folder in the specified location is brought in to RapidResponse in sequence. When an update is complete, if there are additional extracts in the specified folder, the data update continues with the next extract folder. When all extract folders under the specified folder are complete, the folders are moved into history.

You can specify how references are evaluated in the import files. By default, all key fields in the referenced table are used to determine if the reference is a valid record or null. A reference is considered null only if all its key fields are null or blank. However, depending on your data requirements, you can consider a reference to be null if only its base key fields are null. For more information, see "Specifying how references are considered null" on page 401.

Key fields not present in the import file are considered null, unless the field has a default value specified. If all key field values are blank, the reference is considered null, regardless of the default values defined for the fields.

When this command updates data in a scenario, data that is present in RapidResponse but not in the extract folders is deleted. This is different from regular data update processing, which does not delete records from non-root scenarios.

Argument	Description	Value
DetailTransactionLog	Optional argument that specifies whether to log detailed data changes during a data synchronize. This option is typically enabled when integrating data, changing integration settings, or troubleshooting data problems. **Caution:** Enabling this option can significantly slow RapidResponse system performance. You can review detailed data change information in the Data Changes worksheet in the Data Import and Update Log workbook. For more information, see "Data import and data update logs" on page 442. You can also log detailed data change information on an ad hoc basis by enabling the "Log all data changes" option from the **Data Mapping Test** dialog box. For more information, see the *RapidResponse Data Integration Guide*.	**FALSE**—disables the logging of detailed changes to data during a data synchronize (default if not present). **TRUE**—enables the logging of detailed changes to data during a data synchronize.
NamedExtractSet	Mandatory argument that defines the extract folder that all the extracts to be included in the data update are located in. This folder is defined relative to the **C:\RapidResponse\NamedExtractSets** folder.	String that specifies the name of the subfolder in the **NamedExtractSets** folder the extracts are stored in. For example, **Demands**.
Scenario	Optional argument that defines the scenario the data update targets. This must be a shared scenario.	The name of a shared scenario.

For more information and prerequisites for the data update command, see "DataUpdate command" on page 395. For more information about extracting data, see "ExtractData command" on page 403 and "ExtractNetChangeData command" on page 404.

Notes:

- A DataSynchronize command cannot run on a folder that is being used by another DataSynchronize command.

- Each DataUpdate command that is run by a DataSynchronize command records its history in the Data Import and Update Log workbook. The DataSynchronize command itself does not record history. For more information, see "Data import and data update logs" on page 442.
- If the DataSynchronize command runs and there is no new data in the specified folder, the command fails, however, you are not notified, and information about the failure is not recorded in the Data Import and Update Log workbook.
- If any records in the extract data have blank values for all of the table's key fields, that record is rejected if there is no existing record with blank key field values. This typically occurs when a record with null reference values is extracted.
- In some RapidResponse systems that have been upgraded from Version 2014.4 (or earlier), the system administrator might not have turned on the non-unique scenario names feature. If the non-unique scenario names feature is not turned on, the DataSynchronize command can also work with a private scenario. For more information, see "Non-unique scenario names" on page 170.

DataUpdate command

This command initiates the data update process. It relies on the data update processes being configured as explained in the *RapidResponse Data Integration Guide*.

This command is available in On-Demand environments.

You can specify how references are evaluated in the import files. By default, all key fields in the referenced table are used to determine if the reference is a valid record or null. A reference is considered null only if all its key fields are null or blank. However, depending on your data requirements, you can consider a reference to be null if only its base key fields are null. For more information, see "Specifying how references are considered null" on page 401.

Key fields not present in the import file are considered null, unless the field has a default value specified. If all key field values are blank, the reference is considered null, regardless of the default values defined for the fields.

Data administrators receive a message after the DataUpdate command is executed. The message indicates Success or Failed. A Failed message might be generated if no new data was available when it last attempted (or not all the required data sources were available). In some cases, data administrators can also receive a Pending or Expired message. For more information, see "Pending Period setting" on page 395 below.

In addition to arguments, the DataUpdate command also supports two settings in the Scheduled System Tasks worksheet not available to other RapidResponse commands.

Pending Period setting

Optional setting that specifies, in minutes, when to rerun the scheduled DataUpdate command if no new data was available when it last attempted to run (or not all the required data sources were available). RapidResponse only attempts to rerun within the scheduled command's run-time window. For more information, see "Run-time windows for scheduled system tasks" on page 417.

If Pending Period set to a positive number and the scheduled task could not run because no new data was available then DataUpdate command's Status setting returns **Pending** (instead of **Success** or **Failed**). In addition, if the scheduled task's time window expired and the command could not run

because no new data was available then data administrators receive an Expired message and the status is set to **Expired**.

If set to 0 or a value is not present, then RapidResponse does not attempt to rerun the scheduled task. If you have specified a repeat frequency for the task that runs this command, this setting is ignored and should be set to a blank value.

Maximum Retries setting

Specifies how many times to try to rerun a scheduled DataUpdate command if no new data was available when it last attempted to run (or not all the required data sources were available). If set to 0 or a value is not present, then RapidResponse does not attempt to rerun the command. If you have specified a repeat frequency for the task that runs this command, this setting is ignored and should be set to a blank value.

For more information, see "To run a RapidResponse command/scheduled task on demand" on page 416 and "Run-time windows for scheduled system tasks" on page 417.

Notes:

- If you try again to run a scheduled DataUpdate command on demand, the maximum retry counter is reset to 0.
- The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

The following table lists the arguments for use with the DataUpdate command.

Argument	Description	Value
AllowDeletes	Optional argument that specifies whether RapidResponse deletes records during a data update. By not deleting existing records, you can indirectly store historical data in RapidResponse. If this setting and the AllowModifications setting are set to FALSE, the DataUpdate command only inserts records.	**FALSE**—does not allow records to be deleted during a data update. **TRUE**—deletes records during a data update (default if not present).
AllowModifications	Optional argument that specifies whether RapidResponse modifies records during a data update. If this setting and the AllowDeletes setting are set to FALSE, the DataUpdate command only inserts records.	**FALSE**—does not allow records to be modified during a data update. **TRUE**—modifies records during a data update (default if not present).

Argument	Description	Value
CreatePrevious DataUpdate	Optional argument that specifies whether a scenario named **PreviousDataUpdate** is created before the DataUpdate command is run. This scenario is a copy of the root scenario and is available to data administrators. This scenario is especially useful in cases where there are changes to the data extraction process. For more information about the PreviousDataUpdateScenario scenario, see the *RapidResponse Data Integration Guide*.	**FALSE**—The PreviousDataUpdate scenario is not created. This setting is not effective unless the PreviousDataUpdate scenario is deleted. **TRUE**—The PreviousDataUpdate scenario is created (default if not present).
DetailTransactionLog	Optional argument that specifies whether to log detailed data changes during a data update. This option is typically enabled when integrating data, changing integration settings, or troubleshooting data problems. **Caution:** Enabling this option can significantly slow RapidResponse system performance. You can review detailed data change information in the Data Changes worksheet in the Data Import and Update Log workbook. For more information, see "Data import and data update logs" on page 442. You can also log detailed data change information on an ad hoc basis by enabling the "Log all data changes" option from the **Data Mapping Test** dialog box. For more information, see the *RapidResponse Data Integration Guide*.	**FALSE**—disables the logging of detailed changes to data during a data update (default if not present). **TRUE**—enables the logging of detailed changes to data during a data update.
EnableLastKnownGoodPackage	Optional argument that specifies whether to create a set of data files in the package that could be used to restore RapidResponse to its state before the data update occurred. This can be used in cases where the data update is not acceptable or turned off while testing an import to save time. The package is stored in the **C:\RapidResponse\Packages** folder and is named **PreDataImport.pkg**. The file set in the package is the same as that created by the CreateDataPackage command and uses the same file naming convention. For more information, see "CreateDataPackage command" on page 388.	**False**—disables the creation of the data file set. This is the default if not present. **True**—enables the creation of the data file set. Any value other than True is treated as False.
EnableQuality Checks	Optional argument that specifies whether to test extract files during data updates against the extract files used in the most recent successful data import or update to determine if they meet data change tolerance settings. This argument is ignored if you use the Scenario argument to update data in a scenario other than the root scenario. For more information, see "Scenario" on page 399. Not testing the extract can save significant time in the data import process. For more information about data testing, see the *RapidResponse Data Integration Guide*.	**False**—disables the testing. **True**—enables the testing (default if not present). Any value other than True is treated as False.

Argument	Description	Value
EnableSaveHistory	Optional argument that specifies whether after the completion of the data update, to copy the contents of the **\Working** folder to the **\History*timestamp*.DataImport** folder. Not copying the contents can save significant time in the data update process and it might not be required in a test environment. For more information, see the *RapidResponse Data Integration Guide*.	**False**—disables copying the contents. **True**—enables copying the contents (default if not present). Any value other than True is treated as False.
ExpectedData Sources	Optional argument that specifies the list of data sources that are expected to be included in the new data extract files. If any data sources are missing, the data update proceeds and a warning message is sent to all data administrators.	Specifies the expected data sources in a comma-delimited list. For example: `China, Italy, Texas`
ExpectedRegions	This argument was renamed ExpectedDataSources in RapidResponse 9.2. It continues to function. However, it is recommended that you use its new name.	Specifies the expected data sources in a comma-delimited list. For example: `China, Italy, Texas`
ForceHistory	Optional argument that specifies whether data update history is recorded in the Data Import and Update Log workbook if there is no extract data presented when the scheduled DataUpdate task runs. If a data update runs with no extract data and it records history, the Data Import and Update Log workbook contains a history record with a **No new extract data** status. For more information, see "Data import and data update logs" on page 442.	**FALSE**—the data update does not record history if there is no extract data. **TRUE**—the data update records history if there is no extract data.
IntegrationScenario	Optional argument that specifies the scenario that data sources and mapping information are defined in, if they are not defined in the Enterprise Data scenario.	The name of a shared scenario.
KeepExtract	Optional argument that specifies whether to move the data source folders from **\Extract** to **\Working**. This argument is most useful when you are testing RapidResponse data integration settings and data files.	**FALSE**—data source folders are moved (default if not present). **TRUE**—data source folders are not moved.

Argument	Description	Value
MaxRecords	Optional argument that specifies the maximum number records from each data file to import. This argument is most useful when you are testing RapidResponse data integration settings and data files.	An integer specifying the record limit for each data file. If set to 0 or a value is not present, then RapidResponse does not limit the number of records.
NamedExtractSet	Optional argument that can be used when RapidResponse Web Services are used in the Net Change Data Update process. Instead of using the **\Extract** folder in the data update process, use a subfolder in the **C:\RapidResponse\NamedExtractSets** folder. The subfolder you specify is treated as the **\Extract** folder, and the data files must be placed in a folder under this subfolder, which is treated as the data source. For example, **NamedExtractSets\Data_Extract\Data_Source**. Your extract process must place data files in the **\Data_Source** folder. This argument might be created by a Kinaxis integration consultant when setting up your data import processes.	String that specifies the name of the subfolder in the **\NamedExtractSets** folder.
RequiredData Sources	Optional argument that specifies the list of data sources that must be included in the new data extract files in order for the data update to proceed. If any data sources are missing a warning message is sent to all data administrators. As well, the DataUpdate command can return a **Failed** or **Pending** status. For more information, see "Pending Period setting" on page 395.	Specifies the required data sources as a comma-delimited list. For example: `China, Italy, Texas`
RequiredRegions	This argument was renamed RequiredDataSources in RapidResponse 9.2. It continues to function. However, it is recommended that you use its new name.	Specifies the required data sources as a comma-delimited list. For example: `China, Italy, Texas`
Scenario	Optional argument that specifies the scenario the data update targets. If this argument is used to target a scenario other than the root scenario, no quality checks are performed on the data, including tolerance tests and error limit checks. This must be a shared scenario.	The name of a shared scenario.

Argument	Description	Value
SetRapidResponseOrigin	Optional argument that specifies whether the data origin of records is set to User, indicating the data originates in RapidResponse and cannot be modified by subsequent data updates. This applies to data updates that bring data into a scenario other than the root scenario. If this argument is set to False, the data file is set as the origin of the data, which allows subsequent data updates to modify and delete the records. For more information about data origins, see "Origin of database records" in the *RapidResponse Data Integration Guide*.	**FALSE**—the data origin is set to the originating file name. This is the default if not present for data updates that target the root scenario. **TRUE**—the data origin is set to User. This is the default if not present for data updates that target a scenario other than the root scenario.
StopErrorLimits	Optional argument that specifies the maximum number of error types per error for each table. The DataUpdate stops updating a table if the error maximum is reached for any error type. This argument is most useful when you are testing RapidResponse data integration settings and data files.	An integer specifying the error limit. If set to 0 or a value is not present, then RapidResponse does use the maximum error limit per table setting.
Transaction Logging	Optional argument that specifies whether to disable transactional logging during a data update. Every RapidResponse transaction (changes to data and resources) is stored in-memory and in a transactional database file the transactions are written to the RapidResponse database. You should only use this option when bringing in a very large amount of data such as a bulk import of historical data. **Caution:** Disabling this option can significantly increase the speed of a data update operation, especially when bringing in a significant amount of historical data. However, disabling transaction logging also prevents RapidResponse user changes from being logged, which can result in data losses if the RapidResponse Server stops unexpectedly.	**0**—disables transaction logging during data updates. **1**—enables transaction logging during data updates (default if not present).

Note: In some RapidResponse systems that have been upgraded from Version 2014.4 (or earlier), the system administrator might not have turned on the non-unique scenario names feature. If the non-unique scenario names feature is not turned on, the DataUpdate command can also work with a private scenario. For more information, see "Non-unique scenario names" on page 170.

DataUpdate command error codes

The following error return codes can help with diagnostic reviews.

Return code	Description
41	Failed to create map file
40	Missing expected region
39	Missing required region
38	Cannot prepare overlay data
37	Configuration cannot be prepared for update
36	Cannot load map file
35	Persist failed
34	Cannot load XML file
32	Cannot find site/region definition
31	Cannot find map file
30	Cannot execute RapidResponse
29	COM error
28	Cannot prepare regional data
27	Data source folder or Schema.web file missing
24	Cannot rename folder
23	Another instance of the command is running
2	Waiting for user to commit
1	Pending
-7	Nothing to process

Specifying how references are considered null

You can specify how you want to handle null and blank values in references when data is brought in by the DataUpdate or DataSynchronize command. You can use all key fields in the reference, including both base fields and reference fields. In this case every key field in the reference must be blank or null to be considered a null reference. This is the default behavior as of RapidResponse 2016.2 Service Update 27.

If you choose to not use all key values in the reference, only blank or null values in the referenced table's base key fields produce a null reference, regardless of the values in the reference key fields. This is the behavior prior to RapidResponse 2016.2 Service Update 27, and is the behavior used by default if you have upgraded to this version.

▸To specify null reference behavior

1. On the **Administration** pane, under **System Settings**, click **Configuration**.
2. In the **RapidResponse Administration** workbook, click the **Processing Rules** worksheet.

3. Insert the following record:
   - **ID**—DataUpdate.ExtractNullRef.UseAllKeys
   - **Value**—Y to require all reference fields to be blank or null, N otherwise.
4. Click **Save and Close**.

DeleteData command

This command deletes data from shared scenarios. Using this command can help reduce the size of the RapidResponse database by deleting data that is no longer relevant or required. It is good practice to create a scheduled task for this command to delete data once it reaches a historical threshold.

This command is available in On-Demand environments.

By using this command, you can reduce the system memory consumed by the RapidResponse database. Consider using this command to reduce or thin stored historical data. For example, you could store the historical data of the last three months on a daily basis, data older than three months and less than a year on a weekly basis, and data older than a year on a monthly basis.

Data deleted with this command is not reported in the Scenario Properties tab (Pending Commits, Pending Updates, Pending Update Conflicting Changes, and Inherited Data Changes worksheets).

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

For more information about historical tables in RapidResponse, see the *RapidResponse Analytic and Data Model Guide*. For more information about managing historical data in RapidResponse, see the *RapidResponse Data Integration Guide*.

Argument	Description	Value
scenario	Mandatory argument that specifies which scenario to use. You must have modify permissions for the scenario.	The name of a shared scenario. If you want to delete data from the Enterprise Data scenario, use the DeleteEnterpriseData command.
table	Mandatory argument that specifies the table to delete data from.	Specifies the table name. For example: `HistoricalDemandActual`
filter	Mandatory argument that specifies the data to delete through a filter. The filter is typically date-based.	A valid filter expression. For example, the following filter could be used to delete data that is older than 180 days (six months): `Date < d'today' - 180` The Date field in the HistoricalDemandActual table is used in this example.

Note: In some RapidResponse systems that have been upgraded from Version 2014.4 (or earlier), the system administrator might not have turned on the non-unique scenario names feature. If the non-unique scenario names feature is not turned on, the DeleteData command can also work with a private scenario. For more information, see "Non-unique scenario names" on page 170.

DeleteEnterpriseData command

This command deletes data from the Enterprise Data scenario and is typically used with data in historical tables such as HistoricalDemandActual or HistoricalSupplyActual. The command is similar to the DeleteData command but can only be used with the Enterprise Data scenario.

This command is available in On-Demand environments.

Argument	Description	Value
table	Mandatory argument that specifies the table to delete data from. You must have modify permissions for the scenario.	Specifies the table name. For example: `HistoricalDemandActual`
filter	Mandatory argument that specifies a filter expression, typically date-based, that specifies the data to delete.	A valid filter expression. For example, the following filter could be used to delete data that is older than 180 days (six months): `Date < d'today' - 180` The Date field in the HistoricalDemandActual table is used in this example.

DeleteFiles command

This command deletes files and folders from a disk location that has been defined as a RapidResponse file location.

Argument	Description	Value

path	The file location and optional folder to delete files and folders from. This must begin with a RapidResponse file location in square brackets ([]).
	You can specify a file to delete or use a wildcard search to delete a set of specific files.
	The path cannot contain '..', which is interpreted as a higher folder level. You can access only folders in or below the file location.
		The file location, folder, and files to delete.
		`[FileLocation]`
		`[FileLocation]\folder`
		`[FileLocation]\folder\filename`
		`[FileLocation]\folder\*.type`

Note: This command is not available in On-Demand RapidResponse systems.

ExtractData command

This command generates a set of extract data that contains all records from a set of tables and fields. An extract definition specifies the tables and records provided in the generated extract. The definition consists of a list of tables and filters to be applied to those tables. For more information, see the *RapidResponse Data Integration Guide*.

The extracted data is represented as a single file for each table that contains tab-delimited values for each field, with one record per line. To ensure the data in this file is mapped to the correct RapidResponse tables and fields, another file that defines the mappings for each field is also created for the extracted data. During a data update, the mappings are used to bring data into fields as required.

This command is typically used to move data between RapidResponse instances, such as from a data integration server to a planning server. For more information, see the *RapidResponse Data Integration Guide*.

The **ExtractNetChangeData** command is similar to the **ExtractData** command but it writes only records from a set of tables and fields that have been modified since the last time an extract was generated. For more information, see "ExtractNetChangeData command" on page 404.

Argument	Description	Value
Folder	Mandatory argument that defines the folder to create the generated extract files in. The folder is specified using the following syntax: `[FileLocation]\Subfolder` • **FileLocation** is a file location that represents a folder that has already been predefined in the RapidResponse system. For more information about specifying the predefined folders and reviewing a list of existing folders, see "Specifying file location folders" on page 676. The file location must be enclosed in square brackets ([ ]). • **Subfolder** is the name of the subfolder in the folder specified in FileLocation. For example, you could use the value **[extract]\Demands**. In this case the generated extract files will be added to the **Demands** subfolder of the **extract** file location. If **extract** represents **Y:\RapidResponsefiles** then the files will be written to **Y:\RapidResponsefiles\Demands**.	The file location and folder name. For example, **[extract]\Demands**
Scenario	Mandatory argument that defines the scenario that data is generated from.	The name of a shared scenario.
ExtractDefinition	Mandatory argument that defines the tables that are included in the generated extract. This can be defined in the Extract Definitions worksheet in the Scheduled System Tasks workbook. For more information about creating extract definitions, see the *RapidResponse Data Integration Guide*.	A text string that identifies the definition to use. For example, **All Demand Tables**.

Notes:

- If you extract data for a Notes table or a multi-line String field, new lines and carriage returns are flattened into a single line, to ensure the data can be brought in by the DataSynchronize command. New line characters are inserted into the text where lines were removed. For more information, see "DataSynchronize command" on page 393.
- If you extract a table that contains null values in reference fields, the key values for the reference are all extracted as blank values. This might not match a record in the table and, in this case, is rejected by the DataSynchronize command. To ensure records can be brought in, you should correct any null values in non-nullable reference fields.

ExtractNetChangeData command

This command generates a set of extract data that contains only records from a set of tables and fields that have been modified since the last time an extract was generated. An extract definition specifies the tables and records provided in the generated extract. The definition consists of a list of tables and filters to be applied to those tables. For more information, see the *RapidResponse Data Integration Guide*.

As part of its execution, the ExtractNetChangeData command compares records in each scenario, and therefore only tables that have key fields are processed. Keyless tables cannot be compared and are ignored during the command's execution.

The extracted data is represented as a single file for each table that contains tab-delimited values for each field, with one record per line. To ensure the data in this file is mapped to the correct RapidResponse tables and fields, another file that defines the mappings for each field is also created for the extracted data. During a data update, the mappings are used to bring data into fields as required.

If there are no changes, the extract folder is not created and no files are extracted.

This command is typically used to move data between RapidResponse instances, such as from a data integration server to a planning server. For more information, see the *RapidResponse Data Integration Guide*.

The **ExtractData** command is similar to the **ExtractNetChangeData** command but it writes all records from a set of tables and fields. For more information, see "ExtractData command" on page 403.

Argument	Description	Value
Folder	Mandatory argument that defines the folder to create the generated extract files in. The folder is specified using the following syntax: `[FileLocation]\Subfolder` • **FileLocation** is a file location that represents a folder that has already been predefined in the RapidResponse system. For more information about specifying the predefined folders and reviewing a list of existing folders, see "Specifying file location folders" on page 676. The file location must be enclosed in square brackets ([ ]). • **Subfolder** is the name of the subfolder in the folder specified in FileLocation. For example, you could use the value **[extract]\Demands**. In this case the generated extract files will be added to the **Demands** subfolder of the **extract** file location. If **extract** represents **Y:\RapidResponsefiles** then the files will be written to **Y:\RapidResponsefiles\Demands**.	The file location and folder name. For example, **[extract]\Demands**
Scenario	Mandatory argument that defines the scenario that data is generated from.	The name of a shared scenario.
BaselineScenario	Mandatory argument that defines the scenario used to determine which records have been changed since the previous extract. This scenario must be a child of the scenario specified for the `scenario` argument, and should be updated with changes following the extract process.	The name of a shared scenario.
ExtractDefinition	Mandatory argument that defines the tables that are included in the generated extract. This can be defined in the Extract Definitions worksheet in the Scheduled System Tasks workbook. For more information about creating extract definitions, see the *RapidResponse Data Integration Guide*.	A text string that identifies the definition to use. For example, **All Demand Tables**.

Notes:

- If you extract data for a Notes table or a multi-line String field, new lines and carriage returns are flattened into a single line, to ensure the data can be brought in by the DataSynchronize command. New line characters are inserted into the text where lines were removed. For more information, see "DataSynchronize command" on page 393.

- If you extract a table that contains null values in reference fields, the key values for the reference are all extracted as blank values. This might not match a record in the table and, in this case, is rejected by the DataSynchronize command. To ensure records can be brought in, you should correct any null values in non-nullable reference fields.

FilterTT command

As of RapidResponse 9.4, this command is no longer supported. It was used to filter the RapidResponse Transaction table. As of RapidResponse 8.1, Kinaxis recommended using the Show Data Changes feature in RapidResponse and the new DataChanges table. For information about using this feature, see the RapidResponse Help and for information about administrating this feature, see "Data change tracking and record identification" on page 829.

Note: This command is not available in On-Demand RapidResponse systems.

PruneFiles command

This command is used to delete files, most typically saved backup data packages, from the computer where RapidResponse Server is installed.

The CreateBackup schedule task that creates data packages is scheduled, by default, to run every day. Creating a backup package daily could use a significant portion of hard disk space on the RapidResponse Server computer. Without enough free disk space, RapidResponse Server commands such as Condense might not properly execute. As such, it is important to manage the number of data packages saved to ensure they do not consume all the free disk space.

For more information about data packages, see "Backing up and restoring the RapidResponse database" on page 315.

Argument	Description	Value
NumberTo Retain	Mandatory argument that specifies the number of files to retain. The most newly created files are retained when the PruneFiles command is run.	A whole number.
Pattern	Mandatory argument that specifies the names of the files to delete using the DOS file name standards. The * and ? wildcards are acceptable. This argument can specify an absolute path or a relative path. Relative paths are to the RapidResponse Server folder (C:\RapidResponse).	Text string that specifies the folder and files to be deleted. For example, **Packages\backup*.pkg** specifies to delete all **.pkg** files that begin with the string **backup** in the C:\RapidResponse\Packages folder, or **Packages*.zip** specifies to delete all **.zip** files in the C:\RapidResponse\Packages folder.

Notes:

- This command is not available in On-Demand RapidResponse systems.

- You might also want to use the PruneFiles command with the compressed files created when problems were detected during a data integrity check (DIC). These files are called **DIC_*servername_timestamp*.pkg** or **DIC_*servername_timestamp*.zip**. For more information, see " RapidResponse database integrity" on page 327.
- You might also want to use the PruneFiles command with the backup data packages created when customizing the RapidResponse data model. These files are called **PreTransform_ServerName-DateTimeStamp.pkg** or **PreTransform_ServerName-DateTimeStamp.zip**, and are stored in the **RapidResponse\Packages** folder. For more information, see the *RapidResponse Data Integration Guide*.

Restart command

This command runs the Capture command, and then stops and restarts RapidResponse Server.

Restarting releases resources that are no longer being used from the system memory. RapidResponse sometimes needs to be restarted to apply configuration changes.

This command is available for use in RapidResponse scripts. For more information, see the executeRestart method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Notes:

- This command is not available in On-Demand RapidResponse systems.
- Restarting RapidResponse from this command does not apply data model changes. For more information, see "To restart the RapidResponse Server service and apply data model changes" on page 232.

RunAddin command

This command runs a registered add-in. Add-ins are custom applications that extend RapidResponse functionality.

If the add-in application was developed to run in the foreground, you will be unable to perform any other tasks in RapidResponse while the application is running. When an application runs in the foreground, an hourglass is displayed, and you are notified when the process is complete.

If the add-in application was developed to run in the background, you can continue working in RapidResponse. You are not notified when the application finishes running.

This command is not available to data administrators.

For more information, see "Configuring add-ins" on page 638.

Argument	Description	Value
AddIn	Mandatory argument that specifies the add-in to run.	The name of add-in that has already been configured in RapidResponse. For more information, see "Configuring add-ins" on page 638.
User	Mandatory argument that specifies the user ID of RapidResponse user running the add-in.	A valid internal user ID.
Env	Optional argument that specifies the environment variables to pass to the add-in.	Valid environment variables and values in a semi-colon delimited list. They should be listed in the following format: `NAME1=VALUE;NAME2=VALUE`

Note: This command is not available in On-Demand RapidResponse systems.

ScenarioCommit command

This command commits a shared scenario to its parent. The scenario that is being committed and its child scenarios are not kept after the changes are committed to the parent scenario. Any alerts or scheduled tasks that use the scenario are kept.

You might want to use this command in an automated process where RapidResponse users are not required to manually review and approve changes in the data.

This command is available in On-Demand environments.

For more information about scenarios, see "Scenario management" on page 703.

Argument	Description	Value
ForceUpdate	Optional argument that specifies whether to update the scenario before committing it.	**FALSE**—does not update the scenario before committing it (default if not present). If the scenario is out of date, the command fails. **TRUE**—updates the scenario before committing it.
Scenario	Mandatory argument that specifies the scenario to commit to its parent.	The name of a shared scenario.

Note: In some RapidResponse systems that have been upgraded from Version 2014.4 (or earlier), the system administrator might not have turned on the non-unique scenario names feature. If the non-unique scenario names feature is not turned on, the ScenarioCommit command can also work with a private scenario. For more information, see "Non-unique scenario names" on page 170.

ScenarioReset command

This command discards all data changes in a shared scenario. After running this command, the data in the specified scenario is identical to the data in its parent scenario. Discarding changes in a scenario results in the deletion of all data changes and all data changes made to the specified scenario's parent are brought into the specified scenario. For more information, see "Scenario management" on page 703.

This command is available in On-Demand environments.

Argument	Description	Value
Scenario	Mandatory argument that specifies the scenario to discard all changes in.	The name of a shared scenario.
MessageSubject	Optional argument that specifies the subject of the message that is displayed in the scenario's Activity Log.	Text string. For example: `Discard all changes after review`
Message	Optional argument that specifies the message that is displayed in the scenario's Activity Log.	Text string. For example: `Data changes were discarded in this scenario after ...`

Caution: After discarding all changes the data will be identical to the data in the parent scenario. Changes in any child scenarios will also need to be discarded if those scenarios are to be synchronized with their parent scenario.

Note: In some RapidResponse systems that have been upgraded from Version 2014.4 (or earlier), the system administrator might not have turned on the non-unique scenario names feature. If the non-unique scenario names feature is not turned on, the ScenarioReset command can also work with a private scenario. For more information, see "Non-unique scenario names" on page 170.

ScenarioUpdate command

This command updates a shared scenario with data changes from its parent. This command is typically used to update a scenario that contains data that is not modifiable, such as historical data. Because this type of data is not modifiable, the scenario cannot be updated by user actions. For more information, see "Scenario management" on page 703.

This command is available in On-Demand environments.

Argument	Description	Value
Scenario	Mandatory argument that specifies the scenario to update.	The name of a shared scenario.

Note: In some RapidResponse systems that have been upgraded from Version 2014.4 (or earlier), the system administrator might not have turned on the non-unique scenario names feature. If the non-unique scenario names feature is not turned on, the ScenarioUpdate command can also work with a private scenario. For more information, see "Non-unique scenario names" on page 170.

Snapshot command

As users or automated processes (for example, scheduled tasks) modify data or resources, the changes are stored in-memory. The changes are also written to transactional database files named XACT. This

helps to maintain system performance and makes the changes available for recovery in case of system failure.

The XACT files are stored in the **C:\RapidResponse\Data** folder (default location). The data changes are subsequently written to the RapidResponse database by a RapidResponse Server command named **Capture**.

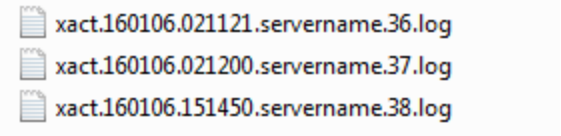
Transactional data can be broken into multiple files so multiple XACT files can exist and each file is named **xact.*timestamp.servername*.sequence.log**. For example:

```
xact.160114.021121.server1792.36.log
```

The timestamp indicates when the file was created.

Running the **Snapshot** command closes the active transaction data file. A new active file is then created. Once the transaction data files are written to the RapidResponse database, the files are deleted and a new active transaction data file is created.

The following is an example of three transaction files created over three days.



The XACT file with the latest timestamp is considered the active transaction file. Each transaction data file contains the full set of transactions that have been executed between the time it was created and the time it was closed. The transaction data files that are not active cannot accept changes.

For more information about transaction data files and snapshots, see "XACT files" on page 311.

Disaster recovery process

By default, the Snapshot command is not scheduled to run at a specified time. A scheduled task is not recommended unless your company has implemented a disaster recovery process. In that case, you can set up a process where each transaction data file is copied to another local disk or an off site disk. The frequency of the snapshots would correspond to your company's data loss disaster policy.

In case of disaster, you could recover the saved transaction data files to a fixed point in time. For more information, see "Rolling back the RapidResponse database" on page 318.

Snapshot command notes

This command is not available to data administrators. This command is available for use in RapidResponse scripts. For more information, see the **executeSnapshot** method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Note: This command is not available in On-Demand RapidResponse systems.

VersionReclaim command

Note: As of RapidResponse 2014.1, the VersionReclaim command is no longer supported. The following information has been maintained in this guide for reference purposes. RapidResponse 2016.2 introduced the VersionReclaimSweep command. This command is similar to the VersionReclaim command. For more information, see "VersionReclaimSweep command" on page 411.

This command was used to clean up the internal version structure used to support scenarios. The version reclaim process reduced the size the RapidResponse database and freed system memory.

RapidResponse automatically deletes versions when 300 (of the 8,192) remain. This can occur during high-user activity periods and can be very disruptive to your user community. You can schedule the VersionReclaim command to run during low-user activity periods. This could prevent RapidResponse from reaching the 300 threshold and automatically running a scenario version reclaim.

You should consider scheduling the VersionReclaim command to run after significant operations which create many versions such as automatic data modifications.

Argument	Description	Value
Threshold	Optional argument that specifies the threshold of available scenarios before a scenario version reclaim executes. For example, assume the threshold is set to 75%. The VersionReclaim command will only execute if more than 6,144 scenarios are used (75% of 8,192 available scenarios and versions). By using this optional argument, you can avoid needless execution of this command.	A number from 0 through 1 that specifies the percentage. For example, 0.75 specifies to 75%

This command is not available to data administrators.

This command is available for use in RapidResponse scripts. For more information, see the executeVersionReclaim method in the *RapidResponse Scripting Guide*.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Note: This command is not available in On-Demand RapidResponse systems.

VersionReclaimSweep command

This command is used to clean up the internal version structure used to support scenarios. The version reclaim process reduces the size the RapidResponse database and frees system memory.

RapidResponse automatically runs version reclaim operations in the background when it is able to reclaim versions. These reclaim operations lock the RapidResponse database but have been optimized to be very brief and should not be noticed by users.

The VersionReclaimSweep command is more aggressive than the standard background version reclaim operation. It forces RapidResponse Server to review all records on the reclaim pass. The first time it runs it can take a considerable amount of time to re-claim older data.

When the VersionReclaimSweep command runs, it write-locks the RapidResponse database. As such, it should only be run during low user activity periods.

After running this command, run the Condense command. For more information, see "Condense command" on page 387.

This command is not available to data administrators.

The execution of this command is logged in the Administration Log workbook. For more information, see " System administration logs" on page 423.

Notes:

- RapidResponse 2016.2 introduced the VersionReclaimSweep command. This command is similar to the VersionReclaim command that was no longer supported as of RapidResponse 2014.1. For more information, see "VersionReclaim command" on page 411.
- It is recommended that this command be run after upgrading RapidResponse to a newer version.
- This command is not available in On-Demand RapidResponse systems.

Scheduling RapidResponse commands

RapidResponse commands are scheduled (and run on demand) from the RapidResponse Scheduled System Tasks workbook. Access to this system workbook is available from the System Settings section of the Administration pane. This workbook includes worksheets you can use to schedule system tasks, define task arguments, configure data to be extracted for a planning server, configure data that should be automatically deleted, and specify data integrity settings.

The worksheets used for scheduling tasks and defining arguments are described in this section. For more information about the other worksheets, see "DataExpiry command" on page 389, "DataIntegrityCheck command" on page 391, or the *RapidResponse Data Integration Guide*.

Scheduled System Tasks worksheet

The Scheduled System Tasks worksheet is used to run a RapidResponse command on demand or to schedule a command. The settings for each command are also stored in this worksheet.

Start | Scheduled System Tasks

	System Task	Enabled?	Schedule	Repeat Frequency (min)	Start Time Window Earliest	Start Time Window Latest	Start Time Window Time Zone	Description	Command	Arguments	Pending Period	Maximum Retries	Group
1	Restart	N	Everyday		2:10 AM	4:00 AM	UTC	System Task ** do not delete **	Restart				
2	Data Update	N	Everyday		2:15 AM	6:00 AM	UTC	System Task ** do not delete **	DataUpdate		5	30	
3	Data Import (delete non-permanent scenarios)	N	Sunday		3:00 AM	6:00 AM	UTC	System Task ** do not delete **	DataImport				
4	Snapshot	N	Everyday		12:00 PM	1:00 PM	UTC	System Task ** do not delete **	Snapshot				
5	Condense	Y	Sunday		12:00 AM	1:00 AM	UTC	System Task ** do not delete **	Condense				
6	Database Integrity Check	Y	Everyday		2:00 AM	4:00 AM	UTC	System Task ** do not delete **	DataIntegrityCheck				DIC
7	Auto-delete	Y	Everyday		2:01 AM	6:00 AM	UTC	System Task ** do not delete **	DataExpiry				
8	Capture	Y	Everyday		2:05 AM	4:00 AM	UTC	System Task ** do not delete **	Capture				
9	Create Backup	Y	Everyday		2:12 AM	4:00 AM	UTC	System Task ** do not delete **	CreateDataPackage				
10	Prune Backup Packages	Y	Everyday		2:30 AM	4:00 AM	UTC	System Task ** do not delete **	PruneFiles	2			

Task Arguments | Extract Definitions | Extract Filters | Auto-delete Configuration | Database Integrity Check Configuration

	System Task	Command	Argument	Value
1	Prune Backup Packages	PruneFiles	NumberToRetain	5
2	Prune Backup Packages	PruneFiles	Pattern	.\Packages\backup*.pkg

By default, RapidResponse includes a scheduled system task for almost all RapidResponse commands (Command column). These tasks should not be deleted and each scheduled task specifies when the command is run (Schedule column), the parameters, and whether it is enabled (all default scheduled system tasks are initially disabled).

On-Demand: System and data administrators might not have access to all scheduled system tasks available with RapidResponse. However, when using a RapidResponse test environment, RapidResponse administrators have the same tools, functionality, and permissions as the Master Administrator at Kinaxis.

On-Premises: System administrators can view, run, and edit all predefined scheduled system tasks. Data administrators can only view, run, or edit some scheduled system tasks.

The following table describes the columns in the Scheduled System Tasks worksheet.

Column	Description
System Task	Specifies the name of the scheduled task. This name must be unique.
Enabled?	Specifies whether the scheduled task is enabled. Valid values are Y (yes) and N (no). You can run a scheduled task that is not enabled by clicking the **Run Task Now** button ▷.
Schedule	Specifies when to run the scheduled task. Valid values are any calendars in your system that have more than one date or any day of the week (Monday through Sunday in English only). After saving changes, items in red text with a yellow highlight are not valid and need to be corrected.
Repeat Frequency (min)	Specifies, in minutes, how often to repeat the running of a scheduled task within its time window (Start Time Window-Earliest to Start Time Window-Latest). RapidResponse only attempts to re-run the scheduled task after the amount of time specified in this setting has elapsed since it last completed running (Start Time Window-Latest). For more information, see "Repeating scheduled system tasks" on page 417. **Note:** If you specify a repeat frequency for a scheduled task that runs the DataUpdate command, the command reruns on the specified frequency if no new data is provided. If no data is provided before the scheduled task's start time window ends, the scheduled task reports a **Failed** status.
Start Time Window-Earliest	Specifies the earliest time that RapidResponse can run the scheduled task (the Start Time Window-Time Zone column specifies the time zone). A time window is required in case RapidResponse is not ready or busy, and cannot run a task at a specified time. For more information, see "Run-time windows for scheduled system tasks" on page 417.
Start Time Window-Latest	Specifies the latest time that RapidResponse can run the scheduled task (the Start Time Window-Time Zone column specifies the time zone). This must be at least five minutes greater than the earliest start time.
Start Time Window-Time Zone	Specifies the time zone to use for the Start Time Window.
Description	Specifies a description of the scheduled task. This is optional.
Command	Specifies the RapidResponse command to run. Valid values are described in "RapidResponse system commands" on page 384. After saving changes, items in red text with a yellow highlight are not valid and need to be corrected.

Column	Description
Arguments?	Display setting that indicates the number of defined arguments for the command. This column cannot be edited. Arguments are defined in the Task Arguments worksheet. For more information about this setting, see "Task Arguments worksheet" on page 415. You can click on any number in this column to filter the results in the Task Arguments worksheet for a selected scheduled task.
Pending Period	Optional setting that specifies, in minutes, when to rerun the scheduled DataUpdate command if no new data was available when it last attempted to run (or not all the required data sources were available). RapidResponse only attempts to rerun within the scheduled command's run-time window. For more information, see "Run-time windows for scheduled system tasks" on page 417. If Pending Period set to a positive number and the scheduled task could not run because no new data was available then DataUpdate command's Status setting returns **Pending** (instead of **Success** or **Failed**). In addition, if the scheduled task's time window expired and the command could not run because no new data was available then data administrators receive an Expired message and the status is set to **Expired**. If set to 0 or a value is not present, then RapidResponse does not attempt to rerun the DataUpdate scheduled task. **Notes:** • This value is ignored for all commands except DataUpdate. • If you specify a repeat frequency for the DataUpdate scheduled task, the task reruns on the frequency you specified, and this setting is ignored. If you have specified a repeat frequency, you should leave this field blank.
Maximum Retries	Specifies how many times to try to rerun a scheduled DataUpdate command if no new data was available when it last attempted to run (or not all the required data sources were available). If set to 0 or a value is not present, then RapidResponse does not attempt to rerun the command. For more information, see "To run a RapidResponse command/scheduled task on demand" on page 416 and "Run-time windows for scheduled system tasks" on page 417. **Notes:** • If you try again to run a scheduled DataUpdate command on demand, the maximum retry counter is reset to 0. • If you specify a repeat frequency for the DataUpdate scheduled task, the task reruns on the frequency you specified, and this setting is ignored. If you have specified a repeat frequency, you should leave this field blank. • This value is ignored for all commands except DataUpdate.
Group	RapidResponse administrators have the option to run scheduled system tasks concurrently by grouping them. By grouping scheduled system tasks, RapidResponse can serialize running scheduled system tasks within the same group but tasks from a different group can run concurrently. All tasks with the same Group setting are considered grouped. If the a scheduled task's Group field is blank, it belongs to the " " (blank group). For more information, see "Running scheduled tasks concurrently" on page 417.
Last Run-Status	Displays the status of the scheduled task's last run. Valid values are Running, OK, Pending, Failed, and Expired (for the DataUpdate command only). If Pending Period is set to a positive number and a DataUpdate command scheduled task could not run because no new data was available then DataUpdate command's Status setting returns Pending. In addition, if the scheduled task's time window expired and the command could not run because no new data was available then the status is set to Expired. This column cannot be edited.

Column	Description
Last Run-Started	Displays when the scheduled task started running (date and time). The time is displayed as the administrator's local time. This column cannot be edited.
Last Run-Finished	Displays when the scheduled task finished running (date and time). The time is displayed as the administrator's local time. This column cannot be edited.

Notes:

- Due to the way RapidResponse performs date calculations, you cannot use a calendar with only one date to schedule a system task. If you select a calendar with only one date, that date becomes sticky and will return a value of either Past or Future. As a result, the system task cannot run as scheduled. To ensure calendars are valid for scheduled system tasks, add another date in the **CalendarDate** table. For more information about calendar and date arithmetic, see the *RapidResponse Analytic and Data Model Guide*.
- If your region participates in Daylight Saving Time (DST), your scheduled system tasks might not run as you expect if they are scheduled between 1:00 AM and 3:00 AM on the dates DST begins and ends. When DST begins, tasks scheduled between 2:00 AM and 3:00 AM run at the equivalent time an hour later, for example, at 3:15 instead of 2:15. When DST ends, tasks scheduled between 1:00 AM and 2:00 AM run only once, despite the hour repeating.

Task Arguments worksheet

The Task Arguments worksheet is used to specify arguments for RapidResponse commands. To specify arguments for a command, enter the following information in the Task Arguments worksheet:

- **System Task**—Specifies the name of the scheduled task; not the name of the actual RapidResponse command the scheduled task is running.
- **Command**—Specifies the name of the command the specified scheduled task runs. It does not need to be entered into the worksheet.
- **Argument**—Specifies the argument associated with the RapidResponse command. The arguments available for each command are described in "RapidResponse system commands" on page 384.
- **Value**—Specifies a value for the argument. This value must not be contained in quotes.

Notes:

- If a system task has multiple versions of the same argument, the first argument listed in the Task Arguments worksheet is used and the others are ignored.
- You cannot manually run a scheduled system task on demand if the Task Arguments worksheet includes unsaved changes. For more information, see "Running scheduled tasks on demand" on page 416.

Using commands and scheduled system tasks

You must be a system or data administrator to perform the procedures described in this section.

▶To create or modify a RapidResponse scheduled task

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. Do one of the following:
   - Insert a record and create column settings based on the information in " Scheduling RapidResponse commands" on page 412.
   - Locate the scheduled task, and modify the schedule task's settings based on the information in " Scheduling RapidResponse commands" on page 412.
3. Save the changes.

▶To enable a RapidResponse scheduled task

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. Locate the scheduled task, and in the **Enabled?** column set the value to **Y**.
3. Save the changes.

Running scheduled tasks on demand

As an administrator, you can run scheduled tasks on demand from the Scheduled System Tasks worksheet. You cannot manually run a scheduled system task on demand if the Task Arguments worksheet includes unsaved changes.

You can confirm whether a scheduled task ran successfully by reviewing the Last Run-Status, Last Run-Started, and Last Run-Finished columns.

▶To run a RapidResponse command/scheduled task on demand

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. Click anywhere in the row of the scheduled task you want to run.
3. Click **Run Task Now** ▶.
4. Click **Yes** to confirm you want to run the task.

Notes:

- If a scheduled task fails to run (scheduled or on demand), a Message Center message is sent indicating the failure. The message includes a log file summarizing the failure. If the scheduled task was run on demand, the message is sent to the user who initiated it. If the task was run on schedule and failed, the message is sent to all system administrators.
- **On-Premises:** You can review the progress of command execution from the RapidResponse Console. For more information, see "Reviewing RapidResponse Server activity" on page 239.
- **On-Premises:** You can run the Capture, Condense, CreateDataPackage, Restart, and Snapshot commands from the RapidResponse Console. To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.
- You can also run RapidResponse commands in a Microsoft Windows command window or batch file by using the **ServerCommand** command. For more information, see "Automatic server operations with ServerCommand" on page 339.
- If multiple scheduled tasks are run in the same second, the tasks are scheduled by the millisecond, which ensures the tasks run in the correct order.

Run-time windows for scheduled system tasks

As noted in " Scheduling RapidResponse commands" on page 412, you cannot set a specific time to run scheduled system tasks; rather a scheduled task has a time window when it can run provided the RapidResponse Server is available.

For example, you cannot schedule a Condense command to start running at the same time as Restart command. Instead the commands are serialized to run in a time window (provided RapidResponse is available). To run a Restart command after a Condense command, offset the start times by a minute.

Time windows help to ensure that the scheduled task will eventually run even if RapidResponse was unavailable at the scheduled start time. Scheduled tasks cannot start outside of their time window unless run manually.

Notes:

- RapidResponse Server reviews the scheduled task list every two minutes to determine whether a task is ready to start.
- If RapidResponse Server stops while running a scheduled task, the task is not rescheduled when RapidResponse Server restarts.

Running scheduled tasks concurrently

By default, only a single scheduled task can run at one time. When the first scheduled task finishes, RapidResponse identifies all other tasks that are still within their run window and runs the task with the earliest start time. For example, you can order two scheduled system tasks by having one start at 2:00 A.M., and another start at 2:01 A.M. The second one will start immediately after the first provided it is still inside its time window.

RapidResponse administrators have the option to run scheduled system tasks concurrently by grouping them. By grouping scheduled system tasks, RapidResponse can serialize running scheduled system tasks within the same group. Tasks from a different group can run concurrently.

Tasks are grouped using the Group column in the Scheduled System Tasks worksheet. All tasks with the same Group setting are considered grouped. If the a scheduled task's Group field is blank, it belongs to the " " (blank group).

By default, the Database Integrity Check scheduled task belongs to the **DIC** group. This task runs the DataIntegrityCheck command which can often take hours to complete. By having Database Integrity Check scheduled task part of a different group than the other default scheduled system tasks, it can run concurrently with other commands including Restart and CreateDataPackage.

Repeating scheduled system tasks

You might require more than one scheduled task for a single command. For example, if you want to restart RapidResponse twice a day, you require two scheduled system tasks that run each day during two time periods.

Instead of creating more scheduled system tasks, you can instead specify a frequency to repeat a scheduled task. For example, you can check whether new data is available for the DataUpdate command

on an hourly basis. To do so, specify 60 (number of minutes) in the **Repeat Frequency (min)** column in the Scheduled System Tasks worksheet for the Data Update scheduled task. As well, the Time Window needs to be set to start at 00:00 (12:00 a.m.) and end at 23:59 (11:59 p.m.) to run the scheduled task every hour.

Using this example, the Data Update schedule task will try to run 60 minutes after the last time it previously completed running. The frequency repeat setting does not guarantee when a schedule task will be run. It only controls when the scheduled task should be attempted to run again and RapidResponse Server continues to only run a single task at a time.

Turning off all scheduled system tasks

When testing or upgrading your RapidResponse system, you might want to turn off all scheduled system tasks. You can do so by creating or modifying a Windows registry setting on the computer where the RapidResponse Server is installed.

Setting **RunScheduledTasks** to 0 prevents scheduled system tasks from running on a schedule. However, it does not prevent scheduled system tasks from being run on demand.

If **RunScheduledTasks** is set to 0, a message is written to the **Server.log** file that indicates scheduled system tasks will not run. For more information about the log file, see " Server.log file" on page 464.

Deleting the **RunScheduledTasks** registry setting or setting it to a value other than 0 turns the scheduled system tasks back on. For more information, "RunScheduledTasks" on page 356.

Notes:

- If a scheduled system task is manually triggered to run while scheduled tasks are turned off, a message will be logged in the Server.log file. To enable tasks to run as scheduled, delete the registry setting or set it to a value other than 0.
- If you are using the On-Demand service, you cannot modify Windows registry settings. Registry settings can be configured by Kinaxis Customer Support.

Logged messages for scheduled tasks

The execution of scheduled system tasks (and most commands) is logged in the Administration Log workbook.

- **Server Operations** worksheet displays log information regarding the execution of RapidResponse commands (usually scheduled system tasks) and some data integration setting changes.
- **Command Messages** worksheet displays detailed RapidResponse command (usually through scheduled system tasks) logging. Information in this worksheet might be requested by Kinaxis Customer Support to help diagnose issues.
- **Changes to Root scenario** worksheet displays data changes that have been committed to the root scenario.

For more information, see " System administration logs" on page 423.

Scheduled system tasks might also generate their own logging information. For example, running the DataUpdate command adds information to the data update logs. For more information about logging, see "Reviewing system status and operation logs" on page 421.

Some messages can include return codes that help with diagnostic reviews.

Return code	Description
999	Generic error
41	Failed to create map file (DataUpdate command only)
40	Missing expected region (DataUpdate command only)
39	Missing required region (DataUpdate command only)
38	Cannot prepare overlay data (DataUpdate command only)
37	Configuration cannot be prepared for update (DataUpdate command only)
36	Cannot load map file (DataUpdate command only)
35	Persist failed (DataUpdate command only)
34	Cannot load XML file (DataUpdate command only)
32	Cannot find site/data source definition (DataUpdate command only)
31	Cannot find map file (DataUpdate command only)
30	Cannot execute RapidResponse (DataUpdate command only)
29	COM error (DataUpdate command only)
28	Cannot prepare regional data (DataUpdate command only)
27	Data source folder or Schema.web file missing (DataUpdate command only)
24	Cannot rename folder (DataUpdate command only)
23	Another instance of the command is running (DataUpdate command only)
2	Waiting for user to commit (DataUpdate command only)
1	Pending (DataUpdate command only)
0	Command executed OK
-1	No such command
-2	Wrong run level for command (RapidResponse Server not fully started)
-3	Unauthorized
-4	Cannot initialize
-5	License expired
-6	Missing argument
-7	Nothing to process (DataUpdate command only)
-8	Invalid argument
-9	Window expired
-10	Canceled
-11	Already running

Return code	Description
-99	Bad password
-100	Bad file
-101	Disk error
-102	Bad scenario
-103	Pending disabled

Note: Return codes greater than 0 to indicate a command specific error condition.

CHAPTER 33: Reviewing system status and operation logs

Message notifications 421
System administration logs 423
Bulletin board information for users 441
Data import and data update logs 442
Automation logging 448
Text logging for alerts 461
RapidResponse text-based log files 462
Viewing log data in the Central Log Collector 479

Almost every RapidResponse operation, including data import, data update, and capturing transaction changes, generates a message or a comment in a log. A RapidResponse administrator needs to be assigned the task of reviewing these feedback tools on a daily basis. By proactively reviewing the logs on a daily basis, you can optimize performance and troubleshoot issues before they arise.

RapidResponse logs system information in the Administration Log workbook, which is accessed from the RapidResponse client. Information related to the data import and data update processes is logged in the Data Import and Update Log workbook.

On-Premises: Much of the information logged in the Administration Log and the Data Import and Update Log workbooks is also available in text-based log files. If, for some reason, you cannot start the RapidResponse client or the RapidResponse Server, you might need to review the text-based log files to troubleshoot an issue.

This chapter also outlines error conditions that users and administrators might encounter in RapidResponse. For more information about resolving RapidResponse issues, see "User account maintenance and troubleshooting " on page 593.

Message notifications

Data administrators receive messages regarding data updates and failures in RapidResponse Message Center. These messages can be forwarded to their email accounts.

System administrators can choose whether to receive these messages. For more information about data update notifications and logging, see "Data import and data update logs" on page 442.

▸To change the data update message setting (only system administrators)

1. On the **Tools** menu, click **Options**.
2. In the **Options** dialog box, click the **Settings** tab.
3. Check or clear the **Send me data update messages** check box.

Note: If profile pictures are enabled on your RapidResponse system, you can access **Options** by clicking on your profile picture in the RapidResponse toolbar.

Master Administrator message notifications

This topic only applies to the On-Premises version of RapidResponse.

The Master Administrator user account (Admin) has a RapidResponse Message Center account and an associated email address. Both Message Center and the email account receive status, warning, and exception messages from RapidResponse. The email account associated with the Master Administrator user account should be reviewed on a daily basis.

▸To change the Master Administrator user email address

- In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
- Click the **Users** tab, select the Master Administrator, and then click **Properties**.
- In the **Email address** box, type an email address.

Caution: Ensure the Master Administrator user account has a valid email address and that this email account is monitored.

Notes:

- If the Master Administrator user account does not have an email address or a default email address has not been specified, users will be unable to forward messages from RapidResponse Message Center to their email addresses.
- By default, the Master Administrator and system administrators have messages in RapidResponse Message Center automatically forwarded to their email accounts.

Tip: If you want two or more people to receive Master Administrator email messages, type the address of an email distribution list.

Problematic queries

Problematic queries generate messages for RapidResponse administrators and users. These types of queries could come from poorly constructed worksheet expressions or control table settings that might not produce valid calculations.

RapidResponse handles problematic queries by doing the following:

- Maintaining the RapidResponse service and ensuring it does not stop unexpectedly or crash. This ensures data changes are not lost and RapidResponse uptime remains high.
- **On-Demand:** Sending a message to the RapidResponse Master Administrator at Kinaxis who can then troubleshoot the issue.
- **On-Premises:** Sending a message to the Master Administrator (Admin user) that summarizes the issue. The message can be used to troubleshoot the issue or to provide information to the Kinaxis Customer Support team. The message will also include an attachment that can help the Support team in the troubleshooting exercise.
- Generating a diagnostic package that can be used by Kinaxis Customer Support to help diagnose the problem. For more information about packages, see "Internal errors and system crashes" on page 244. If during the same RapidResponse process the same or another problematic query is encountered then another diagnostic package is generated. On-Premises administrators can disable the creation of subsequent diagnostic files by modifying a configuration record.

The rest of this topic only applies to the On-Premises version of RapidResponse.

If this type of problem is encountered, a RapidResponse administrator should stop and restart the RapidResponse Server to ensure data integrity.

▸To disable the automatic creation of subsequent diagnostic packages

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Database** category.
3. In the **Diagnostic package on problem query** box, select **Yes**.
4. Click **OK**.
5. Restart the RapidResponse Server. It can be restarted using the Scheduled System Tasks workbook or the RapidResponse Console. For more information see, "Commands and scheduling system tasks" on page 381 or "To stop and restart the RapidResponse Server service in one step" on page 231.

Notes:

- To re-enable this setting, select **No**.
- RapidResponse Server must be restarted to make a change to this setting effective. For information, see "Starting and stopping RapidResponse services" on page 228.

System administration logs

RapidResponse logs information about system operations, including:

- Executions of RapidResponse commands (usually scheduled system tasks) and some data integration setting changes. See the "Server Operations worksheet" on page 424.
- Detailed log messages associated with the execution of RapidResponse commands. See the"Command Messages worksheet" on page 424.
- Data changes in the root scenario. See the "Changes to Root Scenario worksheet" on page 425.
- The number of input records in the root scenario and the number of scenarios on your system. See "Input Records and Scenarios worksheet" on page 425.
- System maintenance activities. See the "System Maintenance worksheet" on page 428.

- Changes related to system configuration, users and groups, permissions, resource dependencies, profile variables, and macros. See the "Security Audit worksheet" on page 430.
- Resources that users cannot access because of errors that occurred during resource import. See "Limited Access Resources worksheet" on page 439.

This information can be very valuable in troubleshooting situations. For example, you might want to review the administration information logs if RapidResponse is not operating normally after a data integration settings change, such as customizing the data model. Or you can determine who executed a RapidResponse command.

The logged information is available in the Administration Log workbook. This workbook is available to system and data administrators only.

▸To review the system administration logs

- In the **Administration** pane, under **System Monitoring**, click **Administration Log**.

Note: RapidResponse logs information displayed in the Administration Log workbook in the RapidResponse database as system records. Over time, these records can grow in size and potentially consume significant amounts of memory. By default, RapidResponse automatically deletes these records after a specified number of days.
On-Demand: The frequency in which these records are deleted can be configured by Kinaxis Customer Support.
On-Premises: The frequency in which these records are deleted can be configured as discussed in " Automatic deletion of system records" on page 277.

Server Operations worksheet

This worksheet displays summary information about RapidResponse command execution. For more information about these commands, see "RapidResponse system commands" on page 384.

In addition, this worksheet also displays information about:

- Executions of scheduled tasks.
- Applications of RapidResponse data model customizations and changes.
- Deletions of data by automated processes.
- Resets of counts and statistics.
- Restarts of the RapidResponse system.
- Additional diagnostic functions.

Command Messages worksheet

This worksheet displays the detailed log messages associated with the execution of the following RapidResponse commands:

- Capture
- Condense

- CreateDataPackage
- DataExpiry
- DataIntegrityCheck
- DataSynchronize
- ExtractData
- ExtractNetChangeData
- Snapshot

The commands are usually run as scheduled system tasks. This worksheet is most useful in cases of investigation or troubleshooting. For example, if a command could not run, you should review this worksheet. For basic command logging information, use the Server Operations worksheet.

Information in this worksheet might be requested by Kinaxis Customer Support to help diagnose issues.

Use the Command control to specify a RapidResponse command to review. Only commands that have run are available.

Debug information can make this log difficult to read. You can hide this information by typing NOT DEBUG in the Search row.

This worksheet does not log information about the DataImport or DataUpdate commands. For this information, see "Data import and data update logs" on page 442. However, any DataUpdate commands that run because of a DataSynchronize command are listed in this worksheet, but displayed only when the DataSynchronize command is selected in the Command list.

For more information about this worksheet, see the Administration Log's workbook help.

Note: The data in this worksheet is not automatically updated. Click **Refresh this worksheet** to update the data.

Changes to Root Scenario worksheet

This worksheet displays the data changes that have been committed to the root scenario (typically named Enterprise Data). It also identifies the user who made each change, and shows the table and field values affected by the change.

The Record and Data Changes columns typically contain multiple data items for each individual change record. Therefore, searches on these columns can only support Is Exactly, Contains, Starts With, and Ends With search criteria.

For more information about this worksheet, see the Administration Log's workbook help or "Committing data to the root scenario" on page 717.

Input Records and Scenarios worksheet

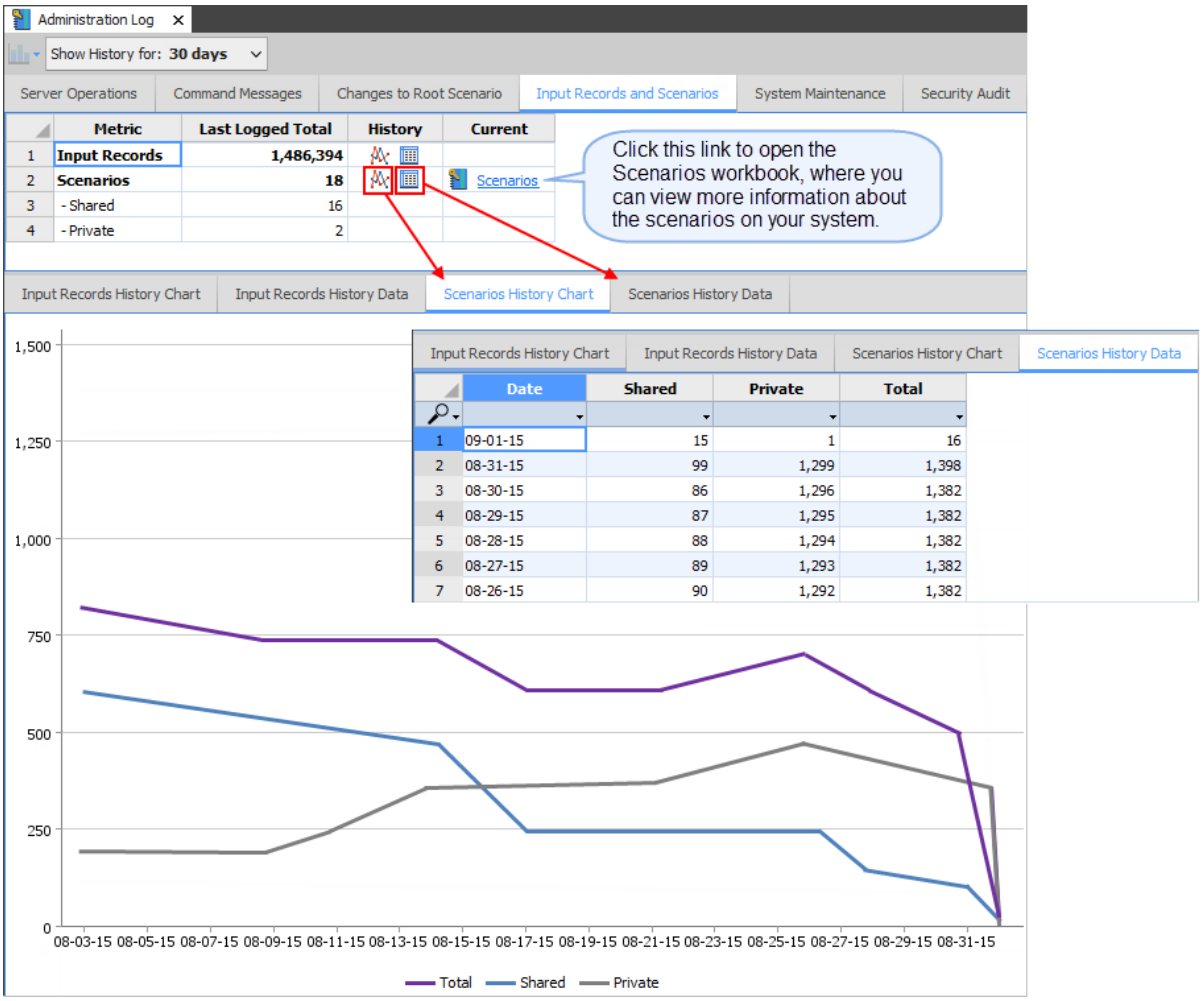
Monitoring the growth of input data and scenario usage are key responsibilities of RapidResponse system administrators. As input data grows, it consumes more system memory. An excessively large amount of input data can negatively impact system performance. Similarly, scenarios can contribute to excessive system memory usage. The two most obvious contributors are scenarios that are no longer being used and historical scenarios that are not being updated.

The Input Records and Scenarios worksheet logs the following metrics:

- The number of input records in data tables in the root scenario.
- The number of scenarios on your RapidResponse system. This includes shared and private scenarios.

You can use the Input Records and Scenarios worksheet to monitor input records and scenario totals and observe trends over time.

The metric totals are logged daily by the Write Administration Metrics scheduled task. The scheduled task must be configured before data is logged in this worksheet. For more information, see "Generating metric data" on page 427.



The Input Records and Scenarios worksheet displays only the values that were logged the most recently. To view the most up-to-date information about the private and shared scenarios on your RapidResponse system, you can click the Scenarios link in the Current column. Clicking this link opens the Scenarios workbook, where you can view information about the shared and private scenarios on your system or delete scenarios that are no longer required. For more information, see "Administrator tools for scenario management" on page 708.

The Scenarios workbook includes the Scenario Metrics worksheet, which provides the same scenario data as the Input Records and Scenarios worksheet. However, the Scenario Metrics worksheet displays scenario data only.

Metric history worksheets

The Input Records and Scenarios worksheet displays only the metric totals that were logged the most recently. To view historical metric data as a line chart, click **Show Chart** in the History column to open the Input Records History Chart worksheet or the Scenarios History Chart worksheet.

To view records of all historical logged values for a metric, click **Details** in the History column to open the Input Records History Data worksheet or Scenarios History Data worksheet.

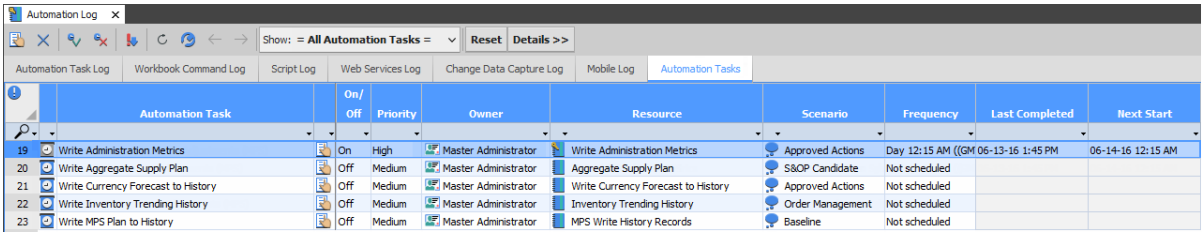
By default, the history worksheets display 30 days of logged data. You can use the worksheet's Show History for data control at the top of the worksheet to change the amount of historical data displayed in these worksheets, You can view history for 30 days, 90 days, one year, two years, or three years. Metric records older than three years are automatically deleted by the Auto-Delete scheduled system task. For more information about this scheduled task, see " Automatic deletion of system records" on page 277.

Notes:

- On-Premises administrators can retain less than three years of data by modifying the Maximum Record Age (Days) setting for data metric log records in the Auto-Delete Configuration worksheet.
- The year settings are not exact, as the metric worksheets are based on an Everyday calendar. For example, the 3 years setting is equivalent to approximately three years and one month, or 1,130 days (the default length of time that metric history records are maintained before being deleted).

Generating metric data

Metric data is logged daily by the Write Administration Metrics scheduled task, which is private and owned by the Master Administrator. This scheduled task runs the Update Usage Metrics workbook command in the Write Administration Metrics system workbook. This workbook is visible to the Master Administrator account only and is not intended to be used interactively.



The scheduled task must be configured manually before it will log metric data. The following table lists each tab of the Scheduled Task Properties dialog box and the settings that should be modified on each tab so that the Write Administration Metrics task successfully logs metric data. It is recommended that you do not modify the default settings.

Tab	Actions
General	• Ensure that the task is enabled. • Optionally, change the priority of the task.
Data	• Optionally, change the selected shared scenario. No scenario is modified when this scheduled task runs. However, any shared scenario must be selected for the task to run.
Data Actions	• No settings should be modified.
Frequency	• Schedule the task to run every day. • Optionally, modify the time that the task runs and the time zone.
Notify	• If the scheduled task fails, the owner should be notified. Other notifications are optional.

Note: The Write Administration Metrics scheduled task and the Write Administration Metrics workbook are not visible in the Resources workbook.

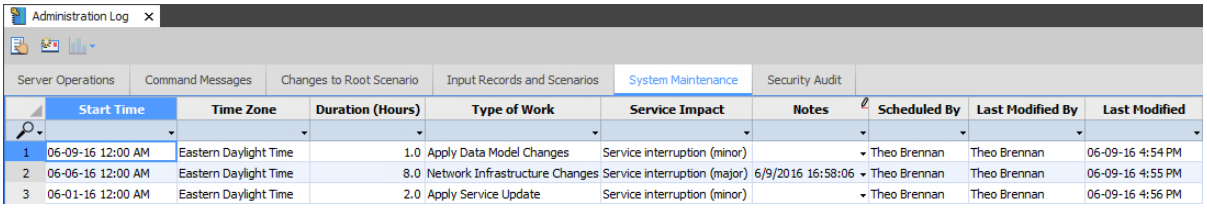
System Maintenance worksheet

RapidResponse data and system administrators carry out regular maintenance activities. These activities can be related to the RapidResponse system, or to the operating system and computer where RapidResponse resides. Here are some examples:

- Applying service updates to RapidResponse;
- Upgrading RapidResponse
- Applying data model changes
- Adding data from a new site
- Network infrastructure maintenance (such as updating the operating system or hardware)

The System Maintenance worksheet provides a summary of the historical maintenance activities. This information can be useful in troubleshooting situations or to better understand changes in system behavior. Additionally, this worksheet also notes the impact on the RapidResponse service.

The information in this workbook is added by RapidResponse system and data administrators, and by the Master Administrator at Kinaxis (for On-Demand systems). It should be reviewed on a regular basis to better understand potential RapidResponse service interruptions. An example of the System Maintenance worksheet is shown in the following image.



	Start Time	Time Zone	Duration (Hours)	Type of Work	Service Impact	Notes	Scheduled By	Last Modified By	Last Modified
1	06-09-16 12:00 AM	Eastern Daylight Time	1.0	Apply Data Model Changes	Service interruption (minor)		Theo Brennan	Theo Brennan	06-09-16 4:54 PM
2	06-06-16 12:00 AM	Eastern Daylight Time	8.0	Network Infrastructure Changes	Service interruption (major)	6/9/2016 16:58:06	Theo Brennan	Theo Brennan	06-09-16 4:55 PM
3	06-01-16 12:00 AM	Eastern Daylight Time	2.0	Apply Service Update	Service interruption (minor)		Theo Brennan	Theo Brennan	06-09-16 4:56 PM

▸To insert a new system maintenance record

1. To specify a setting, on the **Edit** menu click **Insert Record**.
2. In the **Insert Record** dialog box, do the following:
   - In the **Start Time** box, click the down button and select a date and time.

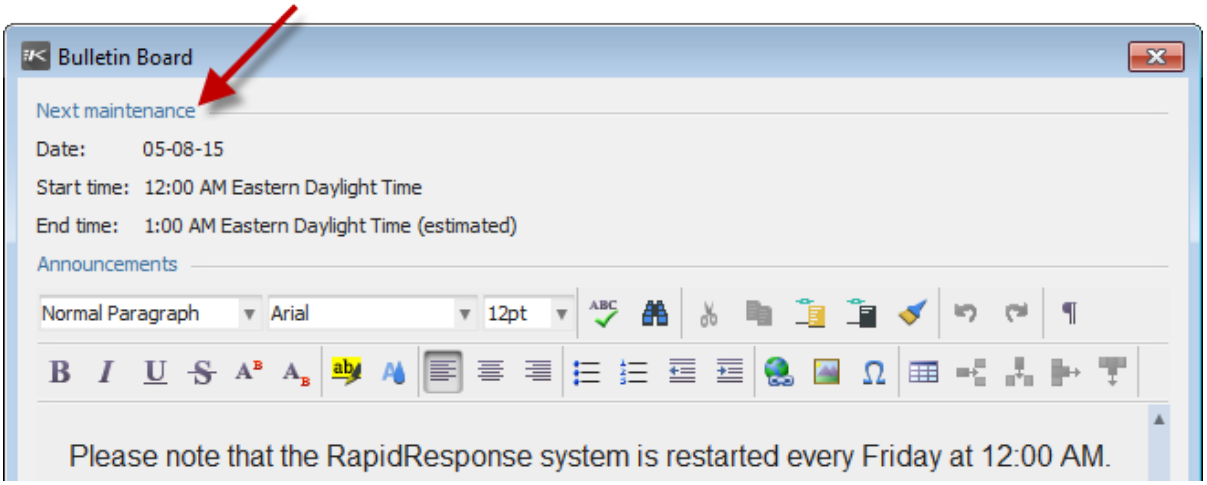
     As the time zone field cannot be modified, the date and time is based on your computer's time zone.
   - In the **Duration (hours)** box, type the estimated number of hours associated with the maintenance task.
   - In the **Type of Work** box, select a maintenance activity.

     If you want to add an activity to the list, click **Add**.
   - In the **Service Impact** box, select an impact description.

     If you want to add an impact description to the list, click **Add**.
3. Click **Save and Close**.
4. Optionally, add a note for the new record by clicking in the **Notes** column.

Bulletin Board and system maintenance

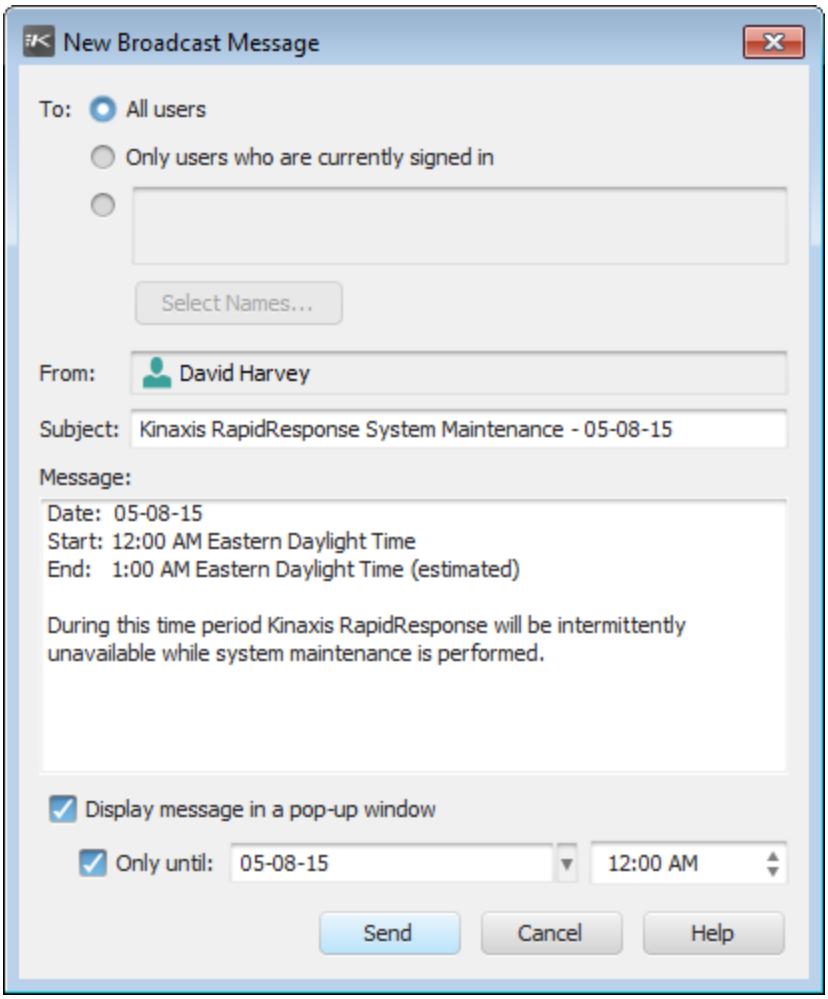
RapidResponse users have access to the Bulletin Board dialog box. From this dialog box, users can review messages from administrators. It also includes a section that displays the next scheduled maintenance record. This information is automatically updated from the records in the System Maintenance worksheet. In the following image, the Bulletin Board dialog box shows the date and time of the next scheduled system maintenance.



For more information about the Bulletin Board, see "Bulletin board information for users" on page 441.

Sending a broadcast message from the System Maintenance worksheet

From the System Maintenance worksheet you can broadcast a message to all or selected RapidResponse users. The message is automatically filled with information from the selected record in the worksheet.



To send a message, select a row and then click **New Broadcast Message** in the System Maintenance worksheet toolbar.

For more information about broadcasting messages, see "Communicating with users" on page 593.

Security Audit worksheet

Changes made in RapidResponse that can impact system security are logged in the Security Audit worksheet. You can use the information reported in this worksheet to monitor the key security controls of your RapidResponse system and to perform security audits.

This worksheet logs the following types of changes:

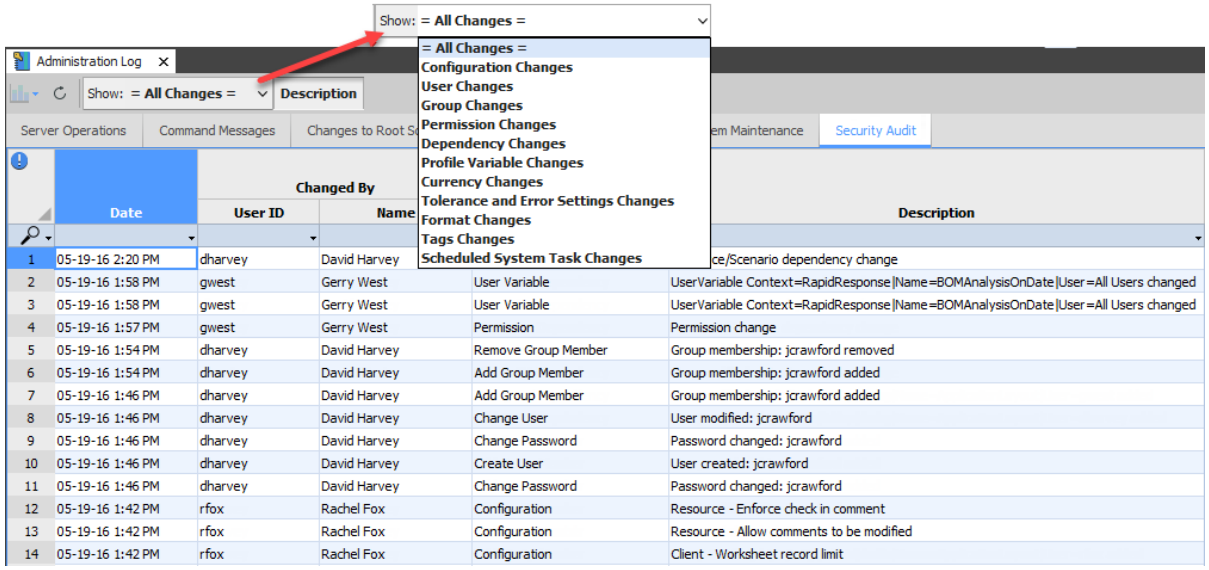
- System configuration changes
- User changes
- Group changes
- Permission changes
- Resource dependency changes

- Profile variable changes
- Macro changes
- Data tolerance and error setting changes
- Resource tag changes
- Data format changes
- Currency changes
- Scheduled system task changes
- Server authentication changes

The date and time the change was made, the user ID and name of the user who made the change, the type of change, and a description of the change are provided for each record in the worksheet. The time is displayed as the local time of the administrator looking at the worksheet.

Other details about each change are provided in columns to the right of the description, and the details vary depending on the type of change. For a better view of these details, you can hide the Description column by clicking the Description button in the worksheet toolbar. You can also filter the worksheet so that only one type of change is displayed by selecting a type of change from the Show list.

Note that, to view macro changes, All Changes must be selected from the Show list. Additionally, the Security Audit worksheet does not display details about macro changes.



	Date	User ID	Name		Description
1	05-19-16 2:20 PM	dharvey	David Harvey		ce/Scenario dependency change
2	05-19-16 1:58 PM	gwest	Gerry West	User Variable	UserVariable Context=RapidResponse|Name=BOMAnalysisOnDate|User=All Users changed
3	05-19-16 1:58 PM	gwest	Gerry West	User Variable	UserVariable Context=RapidResponse|Name=BOMAnalysisOnDate|User=All Users changed
4	05-19-16 1:57 PM	gwest	Gerry West	Permission	Permission change
5	05-19-16 1:54 PM	dharvey	David Harvey	Remove Group Member	Group membership: jcrawford removed
6	05-19-16 1:54 PM	dharvey	David Harvey	Add Group Member	Group membership: jcrawford added
7	05-19-16 1:46 PM	dharvey	David Harvey	Add Group Member	Group membership: jcrawford added
8	05-19-16 1:46 PM	dharvey	David Harvey	Change User	User modified: jcrawford
9	05-19-16 1:46 PM	dharvey	David Harvey	Change Password	Password changed: jcrawford
10	05-19-16 1:46 PM	dharvey	David Harvey	Create User	User created: jcrawford
11	05-19-16 1:46 PM	dharvey	David Harvey	Change Password	Password changed: jcrawford
12	05-19-16 1:42 PM	rfox	Rachel Fox	Configuration	Resource - Enforce check in comment
13	05-19-16 1:42 PM	rfox	Rachel Fox	Configuration	Resource - Allow comments to be modified
14	05-19-16 1:42 PM	rfox	Rachel Fox	Configuration	Client - Worksheet record limit

If you are using an On-Premises RapidResponse system, these changes are also recorded in a text-based log file. For more information, see "SecurityAudit.log file" on page 477.

Note: You can create an alert that monitors the data in this worksheet and notifies you when certain changes have occurred. For example, you can create an alert that notifies you each time a new user is created. For more information, see the *RapidResponse User Guide*.

Configuration changes

Configuration changes are actions that modify the configuration of your RapidResponse system settings.

Changes made in the following worksheets in the RapidResponse Administration workbook are logged as configuration changes:

- File Locations
- Processing Rules
- Other Settings

Changes made in the following dialog boxes are logged as configuration changes:

- Global Settings
- Password Security Policies
- Help Settings
- Message Center and Email
- Print Settings
- Sign-in Notice
- Licenses (importing license keys)

The following actions resulted in the configuration changes shown in the image below:

- In the Global Settings dialog box, the **Worksheet record limit - Tabular** setting was changed to 9000 and the **User session time out** setting was changed to 260.
- In the Print Settings dialog box, the **Maximum number of pages in printed reports** was changed to 300.
- In the **File Locations** worksheet in the RapidResponse Administration workbook, a new file location with ID "FileLoc" was added.

System Maintenance | Security Audit

Type of Change	Description	System Configuration		
		Type of Setting	ID	New Value
Configuration	C:\RapidResponse\Data Publish	FileSystem	FileLoc	C:\RapidResponse\Data Publish
Configuration	Maximum number of pages in printed reports	ProcessingRule	Client_MaximumPDFPageCount	300
Configuration	Client - User session time out	ProcessingRule	Client_SessionTimeout	260
Configuration	Client - Worksheet record limit	ProcessingRule	WorksheetRecordLimit	9000

User changes

User changes are actions that modify a user account. The following actions are logged as user changes:

- Creating a user
- Deleting a user
- Changing a user's name, password, email address, or account type
- Unlocking a user account

Changes to a user's profile picture and contact information, such as title, phone number, location, and so on, are not logged in this worksheet.

The following image shows the records that are logged when a new user account is created. The new user was given an ID, name, email address, and password and was added to the Master Schedulers group.

System Maintenance | Security Audit

Type of Change	Description	User Account			
		User ID	Name	Old Value	New Value
Change User	User modified: jrice	jrice	Jon Rice	PasswordChangeRequired=N	PasswordChangeRequired=Y
Change Password	Password changed: jrice	jrice	Jon Rice		
Create User	User created: jrice	jrice	Jon Rice		
Change Password	Password changed: jrice	jrice	Jon Rice		

The user will be prompted to change his password the next time he signs in to RapidResponse.

When a user account is modified, pipe-delimited values reporting the user's email address, whether the account is locked out, the user's name, and the account type are logged as a user change record. This information is logged even if these values were not changed. For example, a user administrator gave user "jrice" the job title "Master Scheduler". The Security Audit worksheet logs these values but not the job title, as shown in the following image. The old and new values are the same.

System Maintenance | Security Audit

Type of Change	Description	User Account			
		User ID	Name	Old Value	New Value
Change User	User modified: jrice	jrice	Jon Rice	EMail=jrice@kinaxis.com|IsLockedOut=N|LongName=Jon Rice|Type=Internal	EMail=jrice@kinaxis.com|IsLockedOut=N|LongName=Jon Rice|Type=Internal

Group changes

Group changes are actions that modify a group. The following actions are logged as group changes:

- Creating a group
- Deleting a group
- Adding a new member to a group or removing an existing member
- Changing a group's description
- Changing a group from non-system to system (or the opposite)

The following actions resulted in the group changes shown in the image below:

- User "jrice" was added to the Master Schedulers group
- A group named "Buyers North America" was created.
- The Buyers North America group was added to the Buyers group.
- A description of the Buyers North America group was added.

System Maintenance | Security Audit

Type of Change	Description	Group Settings					
		Group	Group Member			Old Value	New Value
			Type	Group Name / User ID	User Name		
Change User Group	Group modified: Buyers North America	Buyers North America				Description=|IsSystem=N	Description=This group applies to buyers at North American sites.
Add Group Member	Group membership: Buyers North Americ	Buyers	Group	Buyers North America			
Create User Group	Group created: Buyers North America	Buyers North America					
Add Group Member	Group membership: jrice added	Master Schedulers	User	jrice	Jon Rice		

When a group is modified, pipe-delimited values reporting the group's description and whether the group is a system group are logged as a group change record. This information is logged even if these values were not changed. For example, the owner of the Sales group was changed. The Security Audit worksheet logs these values but not the changed owner, as shown in the following image. The old and new values are the same.

Security Audit

Description	Group Settings					
	Group	Group Member			Old Value	New Value
		Type	Group Name / User ID	User Name		
Group modified: Sales	Sales				Description=Responsible for reviewing the sales forecast. |IsSystem=N	Description=Responsible for reviewing the sales forecast. |IsSystem=N

Permission changes

Permission changes are actions that modify a level of permission, such as changing settings on the Permissions tab of the User or Group Properties dialog box or granting or denying a user or group access to a resource.

The following actions resulted in the permission changes shown in the image below:

- The user "jrice" was granted permission to author and share workbooks
- The Master Data workbook was shared with the user.
- The user was denied permission to author scorecards.
- The Master Schedulers group was denied the permission to author scorecards.
- The user was granted permission to author scorecards.

System Maintenance | Security Audit

Type of Change	Description	Permission						
		User/ Group	Group Name / User ID	User Name	Resource / Permission		Old	New
					Type	Name		
Permission	Permission change	User	jrice	Jon Rice	Permission	authorScorecards	None	Full
Permission	Permission change	User	jrice	Jon Rice	Permission	authorScorecards	Deny	None
Permission	Permission change	Group	Master Schedulers		Permission	authorScorecards	Full	None
Permission	Permission change	User	jrice	Jon Rice	Permission	authorScorecards	None	Deny
Permission	Permission change	User	jrice	Jon Rice	Workbook	Master Data	None	View
Permission	Permission change	User	jrice	Jon Rice	Permission	shareWorkbooks	None	Full
Permission	Permission change	User	jrice	Jon Rice	Permission	authorWorkbooks	None	Full

The user is granted the permission directly. The permission changes from "Deny" to "None" due to the group change, then from "None" to "Full" because the user now has direct permission.

The direct permission is removed from the group.

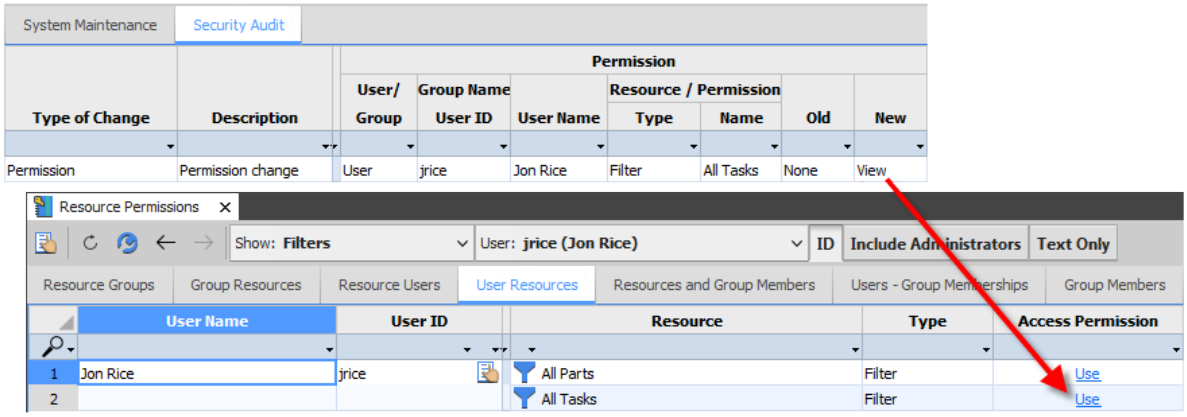
The user's indirect permission is denied.

A user's level of permission is reported as "None" if they are granted a permission indirectly through group membership. It is therefore possible for a user's permission level to appear as "None" in this worksheet when they do have the permission.

An example of this is shown in the above image. Initially, the Master Schedulers group had direct access to author scorecards. When the user was added to this group, he was indirectly granted the permission to author scorecards. This is why, when the permission to author scorecards was removed directly in user properties, the permission changes from "None" to Deny". When the permission was denied for the Master Schedulers group and then granted to the user, he finally has "Full" permission because it was granted directly.

When a resource is shared with a user, the permission level is usually reported as "View". This broad term might not reflect how the user can access the resource, as indicated in user or group properties or the Resource Permissions workbook. A permission level of "View" in the Security Audit worksheet might appear as "View", "Open", "Run" or "Use" in the Resource Permissions workbook, depending on the resource. For example, when a filter is shared with a user, the Security Audit worksheet reports the

resource permission level as "View". In the Resource Permissions workbook, the access permission is reported as "Use", meaning that the filter can be used with an openable resource.



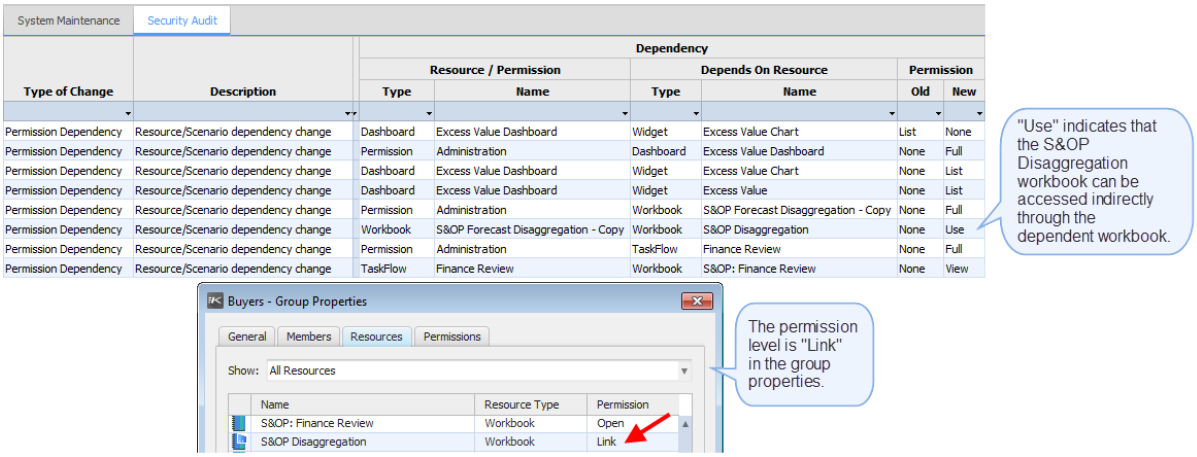
For more information about access permission levels, see "About the Resource Permissions workbook" on page 575.

Dependency changes

Dependency changes are actions that modify a dependency of a permission or resource, such as creating a new public resource that depends on other resources.

The following actions resulted in the dependency changes shown in the image below:

- A task flow named "Finance Review" was created with a step that opens the S&OP: Finance Review workbook.
- The S&OP Forecast Disaggregation workbook was copied and renamed "S&OP Forecast Disaggregation - Copy".
- A dashboard named "Excess Value Dashboard" was created. It uses the Excess Value and Excess Value Chart widgets.
- The Excess Value Chart widget was deleted from the Excess Value Dashboard.



Each dependency change record indicates how the access permission of a resource changes because another resource now depends on it. These resource permission levels might differ from those that appear in user or group properties or the Resource Permissions workbook. The following table shows how the permission levels reported in the Security Audit worksheet relate to the more common permission levels used in RapidResponse. For example, "Use" in the Security Audit worksheet appears as "Link" in group properties.

Security Audit worksheet	User and group properties Resource Permissions workbook
Use	Link
List	List
View	View Open Use Run
Modify	Modify
Full	Manage

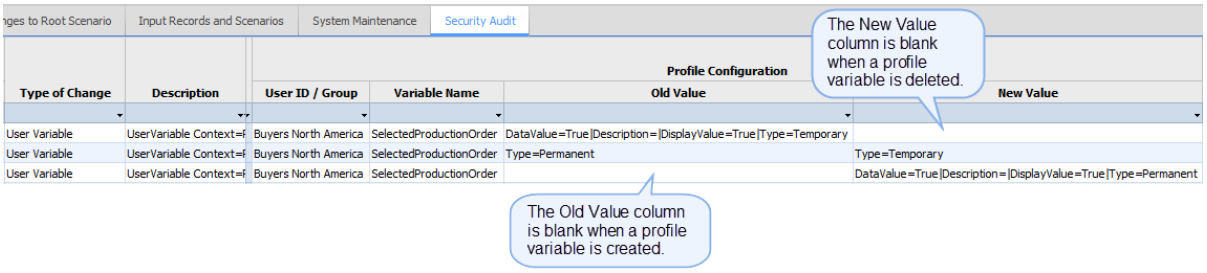
For more information about access permission levels, see "About the Resource Permissions workbook" on page 575.

Profile variable changes

Profile variable changes are actions that modify a profile variable, such as creating or deleting a profile variable or modifying the properties of an existing profile variable.

The following actions resulted in the profile variable changes shown in the image below:

- A profile variable named "SelectedProductionOrder" was defined for the Buyers North America group.
- The SelectedProductionOrder profile variable's type was changed from permanent to temporary.
- The SelectedProductionOrder profile variable was deleted.



Macro changes

Macro changes are changes that modify a macro, such as creating or deleting a macro or modifying the properties of an existing macro. Macro changes are visible only when all types of changes are displayed in the worksheet.

The following actions resulted in the macro changes shown in the image below:

- A macro named "PlannedOrderAction3" was created.
- The parameters of the "PlannedOrderAction3" macro were modified.
- The "PlannedOrderAction3" macro was deleted.
- The expression of the "MarketingFcst_EvaluationHorizonStart" macro was modified.

Server Operations | Command Messages | Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit

	Date	Changed By		Type of Change	Description
		User ID	Name		
1	08-15-16 1:20 PM	rfox	Rachel Fox	Macro	Macro Name=MarketingFcst_EvaluationHorizonStart changed
2	08-15-16 1:19 PM	rfox	Rachel Fox	Macro	Macro Name=PlannedOrderAction3 deleted
3	08-15-16 1:18 PM	rfox	Rachel Fox	Macro	Macro Name=PlannedOrderAction3 changed
4	08-15-16 1:16 PM	rfox	Rachel Fox	Macro	Macro Name=PlannedOrderAction3 added

The Security Audit worksheet does not display details about macro changes. However, if you are using an On-Premises RapidResponse system, you can view details about macro changes in the SecurityAudit.log file. For more information, see "SecurityAudit.log file" on page 477.

Data tolerance and error setting changes

Data tolerance and error setting changes are changes that modify a data tolerance test or an error tolerance test for data updates.

The following actions resulted in the changes shown in the image below:

- A tolerance test for the Part table was created.
- An error limit setting for the PartSource table was created.
- The Part tolerance test value was changed from 10 to 15.
- The PartSource error limit setting was deleted.

Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit | Limited Access Resources

New Value column is blank for deleted tolerance tests and error settings

Changed By			Data Tolerance and Error Settings		
Name	Type of Change	Description	Type	Old Value	New Value
Leigh Mendez	Delete		Error Limits by Table	|ErrorType=DuplicateRecord|Limit=10|Table=Mfg::PArtSource|	
Leigh Mendez	Change		Tolerance Settings by Table	|Check=InsertionCount|MaxPercentRecords=10|Table=Mfg::Part|	|Check=InsertionCount|MaxPercentRecords=15|Table=Mfg::Part|
Leigh Mendez	Insert		Error Limits by Table		|ErrorType=DuplicateRecord|Limit=10|Table=Mfg::PArtSource|
Leigh Mendez	Insert		Tolerance Settings by Table		|Check=InsertionCount|MaxPercentRecords=10|Table=Mfg::Part|

Reports whether the change is made to a tolerance test or an error setting

Old Value is blank for new tolerance tests and error settings

Resource tag changes

Resource tag changes include creating and deleting tags that are used for classifying and grouping resources.

The following action resulted in the tag change shown in the image below:

- A tag named Operation Changes was created

Server Operations | Command Messages | Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit | Limited Access Resources

	Date	Changed By		Type of Change	Description	Tags
		User ID	Name			Name
1	11-23-18 5:28 PM	lmendez	Leigh Mendez	Insert		Operational Changes

Data format changes

Data format changes are changes made to the date and currency formats, including decimal separators, thousands separators, displaying month names or numbers, displaying day names or numbers, or the number of digits to display for years. Adding or removing predefined formats are reported as changes.

The following actions resulted in the data format changes shown in the image below:

- A currency format was removed.
- A date format was added
- The d.m.yyyy date format was changed to dd.mm.yyyy

hanges to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit | Limited Access Resources

Changed By			Format		
Name	Type of Change	Description	Type	Old Value	New Value
Leigh Mendez	Change		Date	|AvailableToUser=Y|Default=N|Format=d.m.yyyy|	|AvailableToUser=Y|Default=N|Format=dd.mm.yyyy|
Leigh Mendez	Change		Date	|AvailableToUser=N|Default=N|Format=d.m.yyyy|	|AvailableToUser=Y|Default=N|Format=d.m.yyyy|
Leigh Mendez	Change		Currency	|AvailableToUser=Y|DecimalPlaces=2|DecimalSymbol	|AvailableToUser=N|DecimalPlaces=2|DecimalSymbol=. |Default=N|DigitGroupingSymbol=

Currency changes

Currency changes are changes to the names, symbols, and descriptions of currencies, or changes to the base currency.

The following actions resulted in the currency changes shown in the image below:

- Three currencies were added
- The description of the Colombian Peso currency was modified.

Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit | Limited Access Resources

Old and new values for all properties are listed for changes

Changed By			Currency	
Name	Type of Change	Description	Old Value	New Value
Leigh Mendez	Change		|Description=Colombia|IsBase=N|Name=Colombian Peso|Symbol=$|Value=COP|	|Description=Colombian Peso|IsBase=N|Name=Colombian Peso|Symbol=$|Value=COP
Leigh Mendez	Insert			|Description=Costa Rica|IsBase=N|Name=Costa Rican Colon|Symbol=₡|Value=CRC|
Leigh Mendez	Insert			|Description=Colombia|IsBase=N|Name=Colombian Peso|Symbol=$|Value=COP|
Leigh Mendez	Insert			|Description=Brazil|IsBase=N|Name=Brazilian Real|Symbol=R$|Value=BRL|

Old Value column is blank for new currencies

Scheduled system task changes

Scheduled system task changes are changes to the scheduled system tasks or their arguments. This includes inserting, modifying, or deleting scheduled system tasks and arguments in the Scheduled System Tasks workbook. Scheduled system tasks are also included in this worksheet when they run, because the start and end times for each run are updated automatically.

The following actions resulted in the scheduled system task changes shown in the image below.

- Arguments for the Data Update task were added
- The schedule for the Create Backup task was modified
- The Prune Backup Packages task was enabled
- The NumberToRetain argument for the Prune Backup Packages task was changed to 5.

Horizon: Today's activity | Show: Scheduled System Task Changes | Description

Server Operations | Command Messages | Changes to Root Scenario | Input Records and Scenarios | System Maintenance | Security Audit | Limited Access Resources

	Changed By				Scheduled System Tasks		
	User ID	Name	Type of Change	Description	Type	Old Value	New Value
1	dharvey	David Harvey	Change		Scheduled Task Argument	|Name=NumberToRetain|Task.Name=Prune Backup Packages|Value=2|	|Name=NumberToRetain|Task.Name=Prune Backup Packages|Value=5|
2	dharvey	David Harvey	Change		Scheduled Task	|Attempts=0|Command=PruneFiles|Description=System Task ** do not del	|Attempts=0|Command=PruneFiles|Description=System Task ** do not de
3	dharvey	David Harvey	Change		Scheduled Task	|Attempts=0|Command=CreateDataPackage|Description=System Task ** (	|Attempts=0|Command=CreateDataPackage|Description=System Task **
4	rfox	Rachel Fox	Insert		Scheduled Task Argument		|Name=KeepExtract|Task.Name=Data Update|Value=True|
5	rfox	Rachel Fox	Insert		Scheduled Task Argument		|Name=AllowDeletes|Task.Name=Data Update|Value=False|

Changes to the scheduled system task properties are listed with all properties of the scheduled system task, so you might need to hover over the value to display the values in a tooltip. For example, the change to the Create Backup task's schedule is shown in the following illustration.

Scheduled System Tasks		
Type	Old Value	New Value
Scheduled Task	|Attempts=0|Command=CreateDataPackage|Description=System Task ** do not delete **|Enabled=Y|Group=|LastEndTime=|LastReturnCode=0|LastStartTime=|MaxRetry=0|Name=Create Backup|PendingPeriod=0|RepeatFrequency=0|RunCalendar=Everyday|RunNow=N|RunNowMS=0|RunNowTime=|RunNow User=|RunTimezone.Value=(GMT-05:00) Eastern Time|RunWindowClose=04:00:00|RunWindowOpen=02:12:00|SelfDestruct=N|Successes=0|	iption=System Task

	Scheduled System Tasks		
Description	Type	Old Value	New Value
|Attempts=0|Command=CreateDataPackage|Description=System Task ** do not delete **|Enabled=Y|Group=|LastEndTime=|LastReturnCode=0|LastStartTime=|MaxRetry=0|Name=Create Backup|PendingPeriod=0|RepeatFrequency=0|RunCalendar=Everyday|RunNow=N|RunNowMS=0|RunNowTime=|RunNow User=|RunTimezone.Value=(GMT-05:00) Eastern Time|RunWindowClose=05:00:00|RunWindowOpen=03:00:00|SelfDestruct=N|Successes=0|			|Attempts=0|Command=CreateDataPackage|

Server authentication changes

This section applies only to On-Premises RapidResponse. Server authentication changes are changes to the encryption keys used to ensure communication between RapidResponse components are authenticated, such as registering a new Application Server client.

Limited Access Resources worksheet

Resources listed in the Limited Access Resources worksheet are only available to their owners. This is most likely the result of an error that occurred when the resources were being imported.

This worksheet should not contain any records. If it does contain records, this is a problem that needs to be fixed by the owner of each resource listed. If possible, use the resource package method that follows to fix the resource while retaining its public tags, sharing information, and version history.

▶Fix errors that limit access to resources—resource package method

1. Create a resource package containing the resources listed in this worksheet that belong to you. For more information, see "Exporting a resource package" on page 752.
2. Delete the affected resources from the RapidResponse system. For more information, see "To delete resources" on page 748.
3. Import the resource package that you just created, containing the affected resources. For more information, see "Importing a resource package" on page 757.
4. Check the **Limited Access Resources** worksheet to ensure that it does contain any resources that you own.

If the resource package method does not resolve the problem and you still see resources that you own in the worksheet, you can fix the problem by re-importing them individually as private resources and then sharing them.

▶Fix errors that limit access to resources—individual resource method

1. Export each resource that you own that is listed in this worksheet.
2. Delete your affected resources from the RapidResponse system.
3. Import each of your affected resources as a private resource.
4. Add each imported resource to the versioned repository, share it, and add tags as needed.

For more information about exporting, importing, and sharing individual resources, see the *RapidResponse Resource Authoring Guide*. For information about adding resource tags, see "Managing global resource tags" on page 772.

Caution: Version history is lost if you use the individual resource method to fix your resources.

Monitoring the system for errors that limit access to resources

It is recommended that an administrators who will be importing resource packages monitor the RapidResponse system for import errors that limit access to resources. To ensure that administrators are notified of any such errors, create an alert to monitor the Limited Access Resources worksheet.

▶Monitor the system for errors that limit access to resources

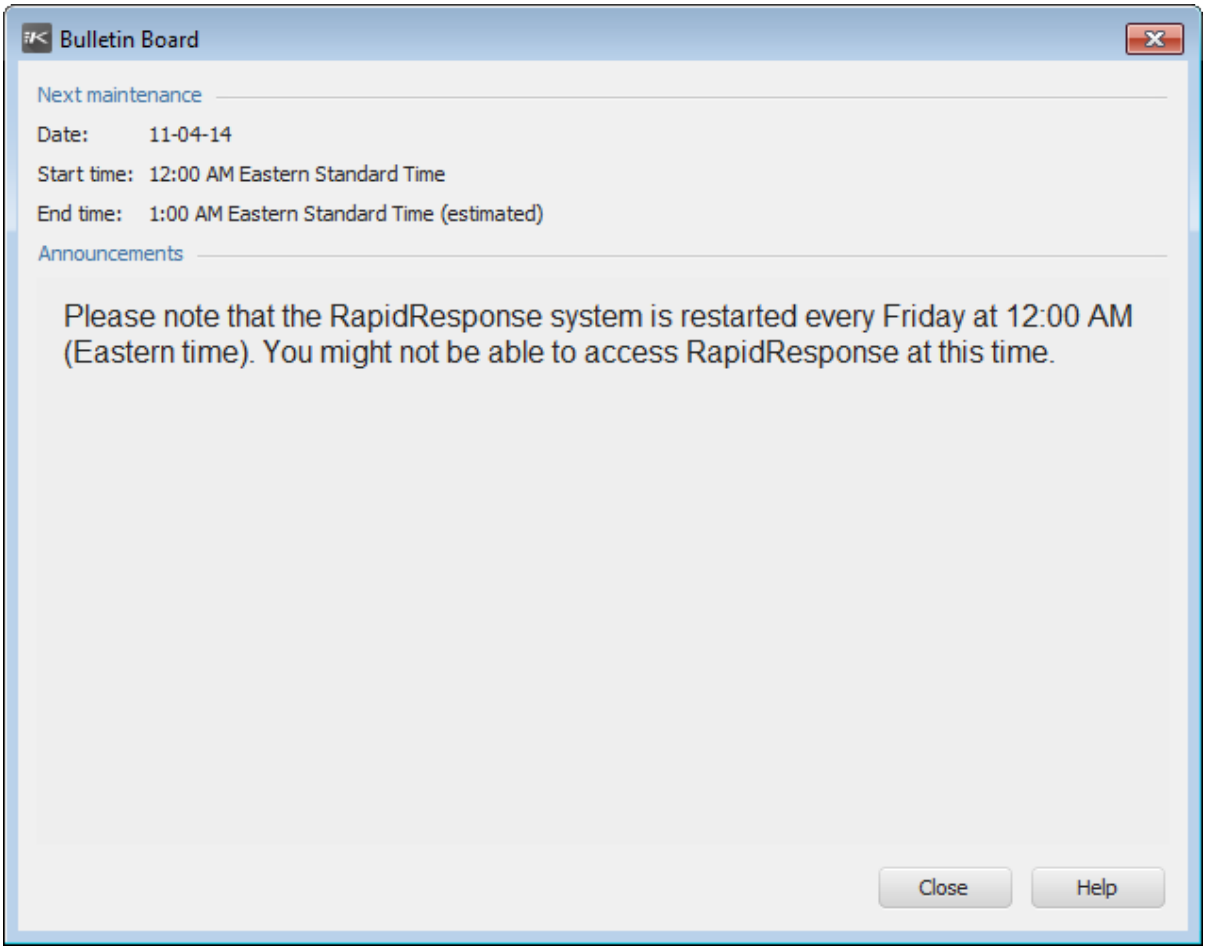
- Create a new alert based on the **Limited Access Resources** worksheet in the **Administration Log** workbook. For more information about creating alerts, see the *RapidResponse User Guide*. Ensure that the following key settings are selected.
  - On the **General** tab, select **Alert is: On**.
  - On the **Condition** tab, in the **Alert** drop-down menu, select **If the worksheet contains any data**.
  - On the **Frequency** tab, under **Check for the condition**, select **Every** or **Use schedule**, and specify a frequency.
  - On the **Notify** tab, ensure that the correct administrators are included in the notification list.

Bulletin board information for users

RapidResponse users have access to the Bulletin Board dialog box which provides information about the RapidResponse system. This dialog box provides:

- Information about the next scheduled maintenance activity. For more details, see "Bulletin Board and system maintenance" on page 429.
- Announcements from RapidResponse system and data administrators and the Master Administrator at Kinaxis (for On-Demand systems).

The following image shows the Bulletin Board dialog box as viewed by RapidResponse users.



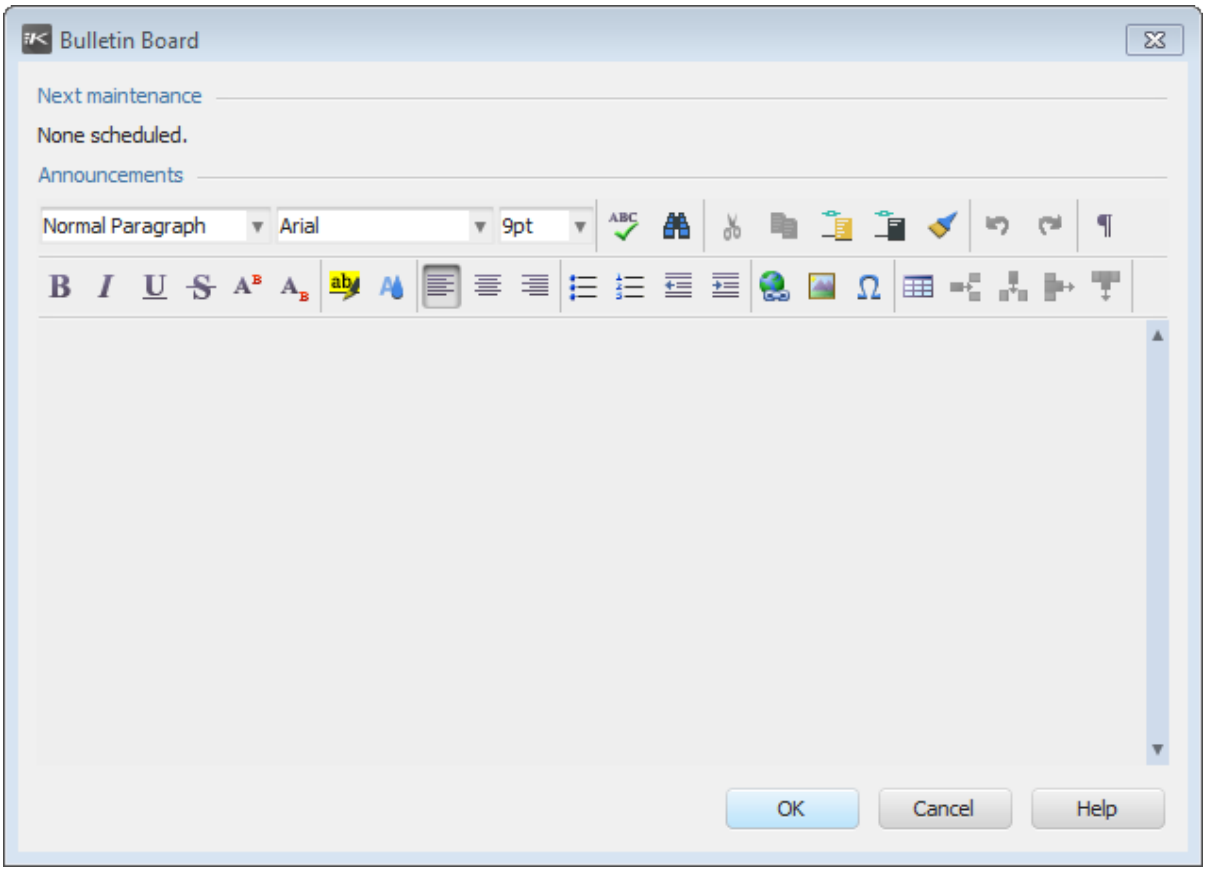
The Announcements section should include information about system activities such as when data updates and system restarts will occur. This could help RapidResponse users pick optimal times to schedule their own automatic activities such as alerts or scheduled reports.

▸To create or modify Bulletin Board announcements

1. From the **Help** menu, click **Bulletin Board**.
2. Type the announcement text.

Use the rich text editor to format the text, or insert images and hyperlinks.

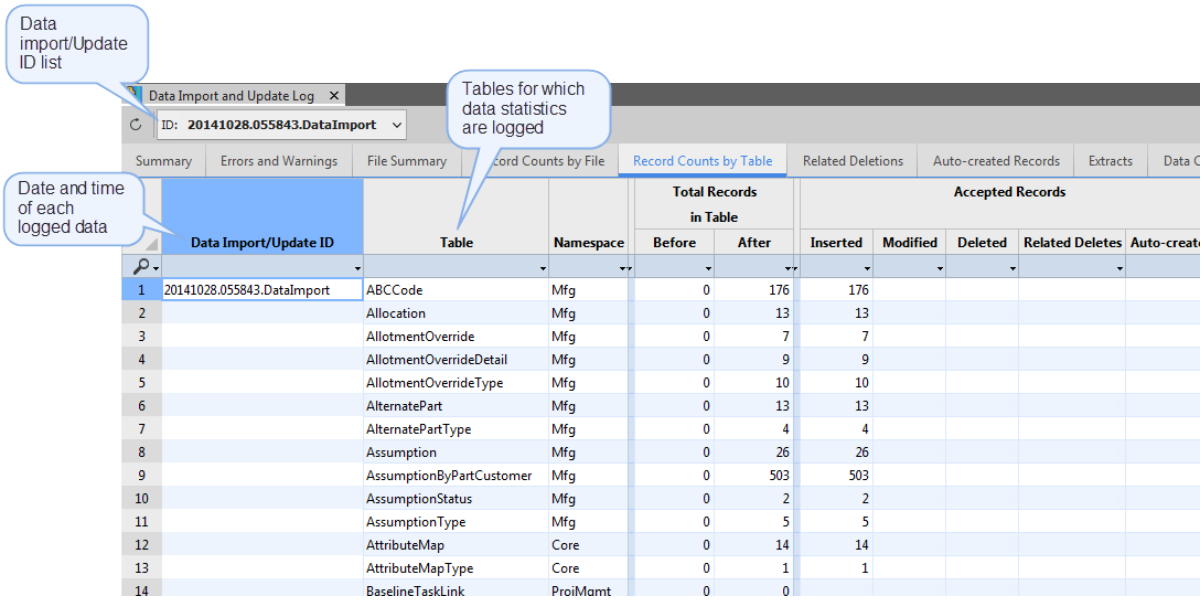
The following image shows the Bulletin Board dialog box as viewed by RapidResponse administrators.



Data import and data update logs

RapidResponse data and system administrators use the Data Import and Update Log workbook in the RapidResponse client to view detailed information about data imports and data updates, including all data updates that are performed by a data synchronize operation, which does not save history. This workbook presents the information across several worksheets in an easy to read and sort format.

The Data Import and Update Log workbook lets you view status information about RapidResponse data imports and data updates (for example, did a data update complete successfully or did it fail), and also shows warning and error messages generated by RapidResponse during a data import or update. Additionally, this workbook shows summaries about the data extract files and RapidResponse input tables used in a data import process (for example, how many successful insertions were made to a given table during a data update). In the following example, the Record Counts by Table worksheet is selected.



	Data Import/Update ID	Table	Namespace	Before	After	Inserted	Modified	Deleted	Related Deletes	Auto-creat
1	20141028.055843.DataImport	ABCCode	Mfg	0	176	176				
2		Allocation	Mfg	0	13	13				
3		AllotmentOverride	Mfg	0	7	7				
4		AllotmentOverrideDetail	Mfg	0	9	9				
5		AllotmentOverrideType	Mfg	0	10	10				
6		AlternatePart	Mfg	0	13	13				
7		AlternatePartType	Mfg	0	4	4				
8		Assumption	Mfg	0	26	26				
9		AssumptionByPartCustomer	Mfg	0	503	503				
10		AssumptionStatus	Mfg	0	2	2				
11		AssumptionType	Mfg	0	5	5				
12		AttributeMap	Core	0	14	14				
13		AttributeMapType	Core	0	1	1				
14		BaselineTaskLink	ProjMgmt	0	0					

Notes:

- RapidResponse logs data import and data update information in the RapidResponse database. Over time, these system records can grow in size and potentially consume significant amounts of memory. By default, RapidResponse automatically deletes these records after 14 days.
  - **On-Demand:** The frequency in which these records are deleted can be configured Kinaxis Customer Support.
  - **On-Premises:** The frequency in which these records are deleted can be configured as discussed in " Automatic deletion of system records" on page 277.
- Click **Refresh this worksheet** to update the worksheet data you are reviewing. The data in this workbook is not automatically updated.
- The Data Import and Update Log workbook only includes information regarding data imports and data updates. It does not include information about data imported by RapidResponse users through an import to scenario or ad hoc import, or data updated by an automation task.
- The Data Import and Update Log workbook logs information about data persistence operations. For more information, see "Logging of persistence operations" on page 333.
- Data updates performed by a DataSynchronize command are logged in this workbook, however, the DataSynchronize operation itself is not. If you require information about a DataSynchronize operation, see " System administration logs" on page 423.
- If no new data is present for a DataUpdate operation, a failed data update is recorded in this workbook. However, if no new data is present for a DataSynchronize operation, no information is recorded in this workbook.
- Data updates performed by grouped messages in the Real-time Integration Platform are not reported in this workbook. Instead, those data updates are reported in the Real-time Message Log workbook. For more information, see the *RapidResponse Data Integration Guide*.

Data Import and Update Log worksheets

This section provides a summary of the worksheets in the Data Import and Update Log workbook that display logged information. Detailed reference information about the data stored in these worksheets is available from the workbook help included with the **Data Import and Update Log** workbook.

- **Summary**—during data imports and data update, data from the latest extract files is compared to data in the root scenario, and the changes are committed into the root scenario. For each data import or data update, this worksheet contains a single row showing the times, status of the operation, number of records in the table before and after the operation, and records inserted, modified, deleted, or rejected by the operation.

  In cases where the data update was unable to complete due to a data issue (that is, it has a status of "Completion pending"), the pending data update is created as a child scenario of the root scenario. Intervention is then required by a system or data administrator. One of the following buttons needs to be clicked:

  - **Cancel Data Update**—used to cancel the data update and leave the root scenario as is.
  - **Commit Data Update to Enterprise Data**—used to commit the pending update into the root scenario.

  > **Note:** Record counts are not recorded for historical tables. However, the number of records inserted in these tables are recorded.

- **Errors and Warnings**—reports detailed messages, of varying levels of severity, associated with data imports and data updates. Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting. Use the Show control on the workbook toolbar to specify whether all messages are shown, or only error and warning messages. For information about controlling the errors and warnings reported, see "Limiting errors and warnings" on page 445.
- **File Summary**—provides a summary of data extract files (text or Microsoft Excel) used in a data import or data update. It reports details such as file size and number of records. Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting.
- **Record Counts by File**—contains details of each data extract file (text or Microsoft Excel) used in a data import or data update. It reports details on these files such as the number of successful and failed operations (insertions, modifications, and deletions) that occurred in each input table. Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting.
- **Record Counts by Table**—reports the number of successful and failed data import and data update operations (insertions, modifications, and deletions) that occurred in each input table. It also provides a count of the number of records that existed in each table before and after the data update. Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting.
- **Related Deletions**—reports summary information for cases where a deletion in one table causes the deletion of records in a dependent table. When a record is deleted, all the information related to that record is also deleted. For example, if a part record is deleted, any records associated with that part are also deleted, such as bill of material, order, and receipt information (even though

these records might still be present in the data files being imported). Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting.

- **Auto-created Records**—reports details of records that were automatically created in a table based on values found in a referencing table. For example, new DemandOrder records might be automatically created based on new values found in an IndependentDemand record being imported. Two tables are described in this worksheet: the table into which the record was automatically created, and the referencing table into which a record was imported that triggered the automatic creation. Use the Data Import/Update ID list control to specify a specific data update when you are troubleshooting.
- **Extracts**—reports the Extract folders associated with each data source for each data update. This information might be useful when troubleshooting the data update process, especially when running net change data updates. Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting.
- **Data Changes**—reports detailed information about data changes after a data update. Use the Data Import/Update ID list control to specify a data import or data update when you are troubleshooting. This worksheet provides detailed information about data that was changed after a data import or data update. Storing detailed logging information can significantly slow RapidResponse system performance and should only be used when integrating data or troubleshooting.

  Use the Table and File list controls to specify the data to review.

  This worksheet is only populated if the DataUpdate command has the DetailTransactionLog argument set to TRUE or if you have enabled the "Log all data changes" option from the **Data Mapping Test** dialog box. For more information, see "DataUpdate command" on page 395.
- **Historical Records**—Use this worksheet to monitor the growth of records in the historical tables in the root scenario.

▸To view logged data import and update information

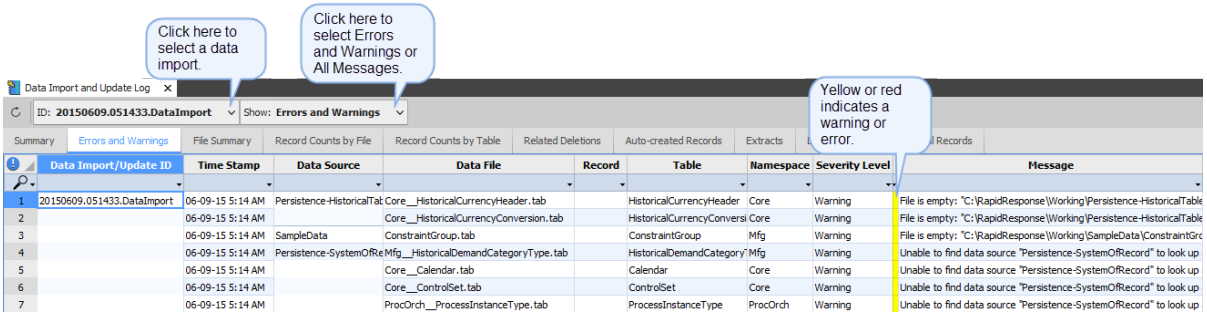
1. In the **Administration** pane, under **System Monitoring**, click **Data Import and Update Log**.
2. Click the tab of the worksheet you want to review.
3. Optionally, select a data import or data update from the **Data Import/Update ID** list. Data imports and updates are identified using time stamps.

   The time stamps are based on folder names used in the data importing process. See the *RapidResponse Data Integration Guide* for more information about the data import folders.

Limiting errors and warnings

If you change your data integration settings, you might generate many errors and warnings which can make the log files very large and difficult to read. You can set limits to the number of errors and warnings recorded and displayed in the **Errors and Warnings** worksheet in the **Data Import and Update Log** workbook.

Errors are highlighted with red and warnings are highlighted with yellow in the **Errors and Warnings** worksheet.



By specifying a limit, you limit the number of each error and warning type for a table on a per data file basis. For example, if you set maximum number of errors to 20 for a specific table, then RapidResponse reports up to 20 errors for each of the error types for each data file that is used to populate the specified table. Additionally, you can specify a limit based on the error type.

If not specified, the default limit per table is 200 error or warning messages of each type.

During a data import or data update process, RapidResponse can log the following types of errors and warnings:

Name	Type	Description
All	Errors and Warnings	All errors and warnings included in this table.
AutoCreateConflict	Error	RapidResponse rejects multiple changes to automatically created records with the same key values but different non-key fields. For example, two parts might specify the same PlannerCode, but different values for PlannerCode.Description. In this case, the subsequent changes (all but the first) to the PlannerCode.Description are rejected. The error limit is applied against the table to which the conflicted changes are targeted. **Note:** RapidResponse also reports the number of conflicts on a per-table basis in the Record Counts by Table worksheet.
AutoCreateFailed	Error	Records that are dependent on the automatic creation of records in another table which does not allow for the automatic creation of records.
BadDataType	Warning	Field values are not appropriate for the field type. Examples of inappropriate values include invalid ASCII characters such as Line Feeds and Carriage Returns. Reviewing and eliminating these invalid characters in the source data will correct these errors. **Note:** RapidResponse also reports the number of invalid values on a per-table basis in the Record Counts by Table worksheet and on a per-file basis in the Record Counts by File worksheet.
BadReference	Error	A referenced record does not exist. **Note:** RapidResponse also reports the number of missing references on a per-table basis in the Record Counts by Table worksheet and on a per-file basis in the Record Counts by File worksheet.

Name	Type	Description
DuplicateRecord	Error	Identical record rejected because the key field values are not unique. **Note:** RapidResponse also reports the number of duplicate keys on a per-table basis in the Record Counts by Table worksheet and on a per-file basis in the Record Counts by File worksheet.
ExtraDelimiter	Warning	Records that include extra delimiter characters.
NoDefaultRecord	Error	Failed to find and automatically create a referenced record.
NotFound	Error	The update map did not specify a enum reference for an enum table without a default record.
UnexpectedNewExtractRecord	Error	The data update operation is set to not expect new extract record. In this case new extract records are included in the data update.
VectorOriginViolation	Error	Records rejected because of vector header data originating from more than one data file or more than one data source. **Note:** RapidResponse also reports the number of records with multiple vector header files on a per-table basis in the Record Counts by Table worksheet and on a per-file basis in the Record Counts by File worksheet.

Errors or warnings can also apply to an entire table or data file. In this case, only one warning is displayed for the table or data file.

Message	Description
File is empty	The specified data file contains no records.
The CurrencyConversionActual table will not be updated because the root scenario is not targeted by this data update.	Data can be updated in the CurrencyConversionActual table only if the data update brings data in to the root scenario. This ensures actual conversion rates are not accidentally added or deleted.

▸To specify error limits per table

1. In the **Administration** pane, under **Data Integration**, click **Tolerance and Error Settings**.
2. Click the **Error Limits by Table** worksheet.
3. To specify a setting, on the **Edit** menu click **Insert Record**.
4. In the **Table** box, type the table name for which the limit is applicable. You can use a wildcard character (*) to specify all tables. However, this does not explicitly override a table that has a specified setting.
5. In the **Error Type** list click **All** to select all error types or click a specific error as described in the above tables.
6. In the **Maximum Number of Errors** box type the maximum number of errors to log for the corresponding table. This number applies to each of the error types.
7. Do one of the following:
   - Click **Save and Close** to add the limit and return to the worksheet.
   - Click **Save** to add the limit and to add another limit.

Note: Error limits specified in the **Error Limits by Table** worksheet also apply to **Messages.xml** file. For more information, see "RapidResponse text-based log files" on page 462.

List of non-printable characters

The following characters are not supported in RapidResponse. If used, they can cause unexpected errors.

Character	ASCII Character	Unicode Value	Description
0, Nul, \0, ^@	U+0000	U+2400	Null
SOH, ^A	U+0001	U+2401	Start of Header
STX, ^B	U+0002	U+2402	Start of text
ETX, ^C	U+0003	U+2403	End of text
EOT, ^D	U+0004	U+2404	End of transmission
ENQ, ^E	U+0005	U+2405	Enquiry
ACK, ^F	U+0006	U+2406	Acknowledge
BEL, \a, ^G	U+0007	U+2407	Bell
BS, \b, ^H	U+0008	U+2408	Backspace
FF, \f, ^L	U+000C	U+240C	Form feed
SO, ^N	U+000E	U+240E	Shift out
SI, ^O	U+000F	U+2401	Shift in
SUB, EOF, ^Z	U+001A	U+241A	Control-Z
ESC, \e, GCC only, ^[	U+001B	U+241B	ESC/Escape
SP, SUB	U+0020	U+2420	Space
ƀ	U+180B	U+2422	Blank
NL, \n	U+0085	U+2424	Next line

Automation logging

RapidResponse administrators use the Automation Log workbook in the RapidResponse client to view detailed information about automated processes, such as alerts, scheduled tasks, automation chains, and scripts. You can also view information about processes that have been run interactively by users, such as workbook commands. This workbook logs many details including run status, successes, and failures.

If you notice any issues after viewing these details, you can use the Automation Log workbook to delete automation tasks or modify their scheduling and properties.

The information in the Automation Log workbook is presented in worksheets, which you can sort and search to view only the information relevant to you. In addition, you can specify how much history to display in the worksheets. For example, you can view only alerts that have run on the current date, automation chains that have run in the past three days, or scheduled tasks that have run in the past month.

The Automation Log workbook includes the following worksheets:

- **Automation Task Log**. For more information, see "Automation Task Log worksheet" on page 449.
- **Workbook Command Log**. For more information, see "Workbook Command Log worksheet" on page 454.
- **Script Log**. For more information, see "Script Log worksheet" on page 458.
- **Web Services Log**. For more information, see the *RapidResponse Web Services Guide*.
- **Change Data Capture Log**. For more information, see "Change Data Capture Log" on page 458.
- **Mobile Log**. For more information, see "Mobile Log" on page 459.
- **Automation Tasks**. For more information, see "Automation Tasks" on page 459.

▸To view the automation log

- In the **Administration** pane, under **System Monitoring**, click **Automation Log**.

▸To specify how many days of log entries are displayed

- In the **Automation Log** workbook, in the **Horizon** list, click the number of days to display entries for.

Note: The data in the Automation Log worksheets is not automatically updated. Click **Refresh worksheet** to update the data.

Tip: You can also view information about your personal alerts, scheduled tasks, and automation chains in the **Automation Details and Log** workbook. This workbook includes information about all automation tasks that have been shared with you and scripts and workbook commands that you have run. For more information, see the *RapidResponse User Guide*.

Automation Task Log worksheet

All automation tasks (alerts, scheduled tasks, and automation chains) run by all users are logged in the Automation task Log worksheet of the Automation Log workbook, including alerts that monitor worksheets or scorecards, scheduled tasks that publish data to subscribers, automatically modify data, or run scripts, and automation chains that perform sequences of modifications and reports.

This worksheet includes automation tasks that ran manually, as well as ones that were scheduled, ran based on data changes in scenarios, or that ran as part of an automation chain.

You can choose to view only alerts, only scheduled tasks, only automation chains, or all automation tasks in this worksheet.

If you want to create a report of the automation tasks in your system, you can print or export the data in these worksheets. For more information, see the *RapidResponse User Guide*.

For each automation task, the log includes its start and end time, how long it took to run, who ran it, whether it completed successfully, the resource monitored or edited, and for scheduled tasks that modify data, the number of records modified, inserted, or deleted and the number of errors that occurred.

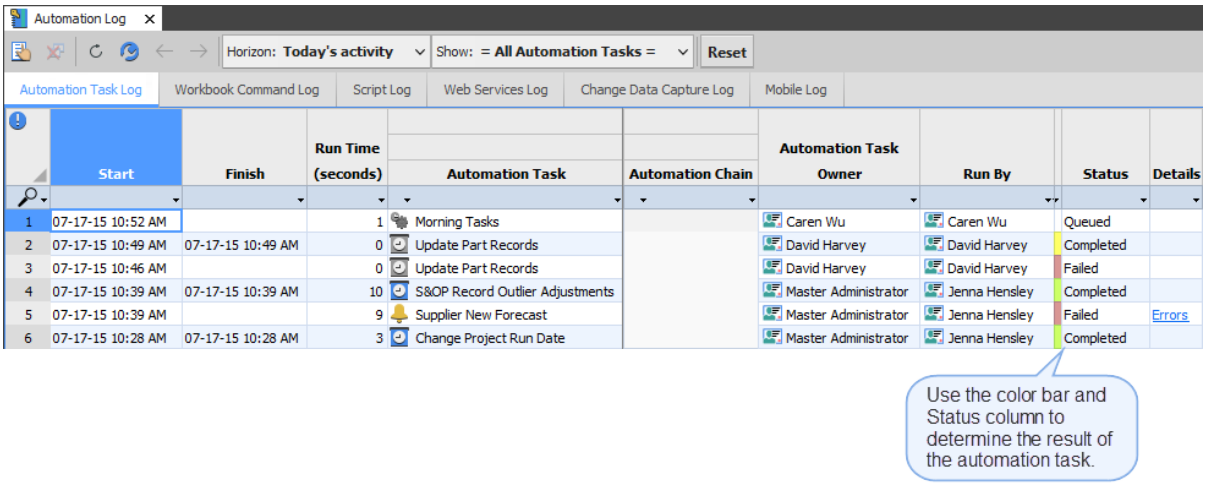
The Automation Task Log worksheet includes links to the Data Modification Details worksheet, where you can view details about the records modified by command actions, and the Error Details worksheet, where you can investigate data modification errors. When you open the Data Modification Details worksheet or the Error Details worksheet by clicking a link, the row is highlighted with yellow. Click Reset on the workbook toolbar to close the detail worksheets. For more information, see "Data Modification Details worksheet" on page 456 and "Error Details worksheet" on page 457.

Automation task status

You can use the Automation Task Log worksheet to see the current state of an automation task or to determine whether it has successfully completed or if it failed.

When a data modification command is run as a scheduled task, there are a few possible outcomes. If there are no errors or if the number of errors does not exceed the acceptable limit, a command is successfully completed. If the acceptable number of errors is exceeded, the command fails.

During worksheet configuration, an author can specify if errors are allowed to occur when a command runs. For example, they can configure whether a data modification command fails when the first error occurs or completes successfully even if a certain number of errors have occurred. If the author allows some errors to occur, they need to set an error limit for the worksheet. As long as the limit is not exceeded, the command can complete successfully even though not all record insertions, modifications, or deletions have occurred. Using the status information in this worksheet, you can differentiate between the commands that were run successfully without and with errors (applies only to data modification commands).



The following are the task states that can display in the Status column along with the color bar that corresponds with each state (if applicable):

Completed—The automation task is successfully completed. If a data modification command was run, there were no errors.

Completed—The data modification command was successfully completed, but with some errors.

Started—The automation task is currently running.

Queued—The automation task is waiting to be executed.

Canceled—The automation task was canceled. If a data modification command was run, details about the command are not available. In addition, the number of records inserted, modified, and deleted are displayed in gray text, and the changes are not applied.

Failed—The automation task could not be completed. If a data modification command failed, it's because the acceptable number of errors was exceeded. As a result, no data changes were made. A command might also fail due to a non-data error, such as an invalid scenario or a missing resource that prevents the command from successfully completing. To determine the cause of the failure, you can review the information about these errors in the Details column.

For automation tasks that fail, the Finish column does not report a value. When an automation task fails, a message is sent to its owner and anyone else the owner has specified. However, if that user is away and has not included notifications for anybody else, the only indication that an automation task has failed is its entry in the Automation Task Log worksheet. If you want to be notified when any automation task fails, you can create an alert on this worksheet.

The Automation Task Owner column displays the user name of the user who owns the Automation task. When automation tasks fail, consider contacting this user for assistance. Click the button beside the user's name to view contact information.

Data Modification columns

The Data Modification columns contain information about data changes made by scheduled tasks that run data modification commands. The number of records that are inserted, modified, and deleted are displayed with the number of errors, if any, that occurred. These record counts apply only to the data in tables that the worksheets updated by the command are based on. They do not include inserted reference records or related deleted records.

The Inserted, Modified, and Deleted columns contain a number if the worksheet is configured to perform that operation (this number can be zero). If there is no number in the column, the worksheet is not configured to perform that operation. If the data modification cannot complete successfully, these numbers are displayed in gray text to indicate that the changes were not made.

Data Modification				
	Records			
Command	Inserted	Modified	Deleted	Errors
Delete Expired Allotments			504	
Add New Part Records	1			51
Add New Part Records	1			51

The Data Modification columns display the total number of records that are inserted, modified, and deleted by a command. You can click the name of a command to open the Data Modification Details worksheet, which displays the number of records modified by each command action. You can also access this worksheet from the Workbook Command Log worksheet. For more information about this worksheet, see "Data Modification Details worksheet" on page 456.

You can click the number of errors in the Errors column to open the Error Details worksheet, which provides information about any errors that occurred. You can also access this worksheet from the Workbook Command Log worksheet. For more information about this worksheet, see "Error Details worksheet" on page 457.

▸To view details about scheduled tasks that modify data

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. For the scheduled task you want to view details about, in the **Command** column, click the command's name link to open the **Data Modification Details** worksheet.
3. Click **Reset** to close the details worksheet.

▸To view details about data modification command errors

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. For the scheduled task with errors that you want to view details about, in the **Errors** column, click the link to open the **Error Details** worksheet.
3. Click **Reset** to close the details worksheet.

Note: On-Premises: In addition to the **Automation Log** workbook, RapidResponse writes automation task processing information to the **ServiceHost.log**, which by default is located in the **C:\RapidResponse\Logs** folder. For more information, see "Text logging for alerts" on page 461.

Tip: The Errors column in the Data Modification Details worksheet also includes a link to the Error Details worksheet. To view error information for one specific command action only, open Error Details from this worksheet instead.

▸To specify which automation tasks are displayed

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. In the **Show** list, click one of the following:
   - **All Automation Tasks**—All alerts, scheduled tasks, and automation chains are displayed in the worksheet.
   - **Alerts**—Only alerts are displayed in the worksheet.
   - **Scheduled Tasks**—Only scheduled tasks are displayed in the worksheet.
   - **Automation Chains**—Only automation chains are displayed in the worksheet.
3. To view all automation tasks that are part of an automation chain, do the following:
   - In the **Show** list, click **All Automation Tasks**.
   - Search the **Automation Chain** column for the name of the automation chain you want to view, or for non-blank values to view all steps of all automation chains.

Note: If an automation task has been deleted, an icon is not displayed beside its name.

▸To view the properties of an automation task

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. Do one of the following:
   - Select the automation task you want to view, and then on the workbook toolbar, click **Properties** .
   - Click the automation task name.

> **Note:** If you own the automation task or it has been shared, you can also modify its properties. For more information, see the *RapidResponse User Guide*.

▸To change the priority of an automation task

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. Open the properties of the automation task you want to modify.
3. In the **Priority** list, click one of the following:
   - **Critical**—These automation tasks always run first. This priority is typically reserved for system tasks and critical business processes.
   - **Urgent**—These automation tasks run when there are no more Critical priorities in the queue. These are typically very important but not business-critical.
   - **High**—These automation tasks run when there are no more Urgent priorities in the queue. These are typically more important than general users' automation tasks.
   - **Medium**—These automation tasks run when there are no more High priorities in the queue. This is the default priority for automation tasks and is typically the priority a general user's automation tasks run at.
   - **Low**—These automation tasks run only when there are no higher priorities in the queue. These are typically automation tasks that can run at any time.
4. Click **OK**.

▸To view details about a failed automation task

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. Do one of the following:
   - In the **Details** column, click the **Errors** link for the failed alert, scheduled task, or automation chain you want to view details about.

     The error message for the automation task is displayed in the **Error message** dialog box.
   - For a failed scheduled task that runs a data modification command, click the link in the **Errors** column to open the **Error Details** worksheet. When you are finished reviewing details, click **Reset** on the toolbar to close the details worksheet.

▸To monitor for failed automation tasks

1. In the **Automation Log** workbook, click the **Automation Task Log** worksheet.
2. In the **Status** column, search for **'Failed'**.
3. On the RapidResponse toolbar, click **New Resource** , point to **Alert**, and then click **Monitor Worksheet**.
4. Click **Monitor all records matching the worksheet data settings**, and then click **OK**.

5. Customize the alert settings. For more information, see “Monitoring data” in the *RapidResponse User Guide*.

Note: By default, 14 days of alert logging information is stored.
On-Demand: The number of days can be changed by Kinaxis Customer Support.
On-Premises: For information about changing the default setting, see " Automatic deletion of system records" on page 277.

Workbook Command Log worksheet

Each time a user interactively runs a workbook command, this activity is logged in the Workbook Command Log worksheet. You can use this worksheet to review information about the commands that have been run, including when the command was run, the workbook that contains the command, the scenario that was modified by the command, and the status of the command (for example, whether it completed successfully or failed). This worksheet also provides counts of the number of records that were inserted, modified, or deleted by the command and of the number of records in error.

When a workbook author tests a worksheet’s automated data modification operations, this activity is also logged in this worksheet.

The Workbook Command Log worksheet includes links to the following worksheets:

- "Data Modification Details worksheet" on page 456
- "Error Details worksheet" on page 457

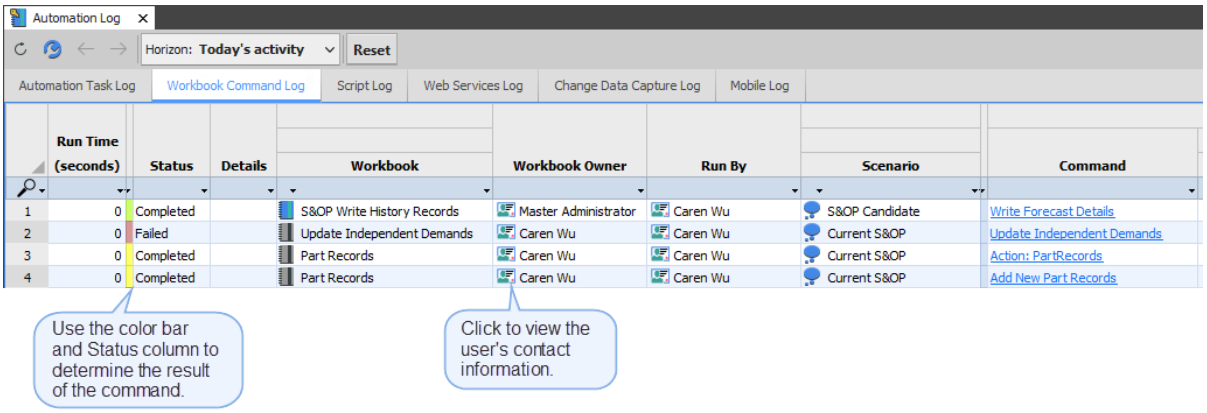
The Data Modification Details worksheet can be used to more closely examine the data modifications made by each command action. The Error Details worksheet can be used to investigate errors. When you open the Data Modification Details worksheet or the Error Details worksheet by clicking a link, the row is highlighted with yellow. Click Reset on the workbook toolbar to close the detail worksheets.

You can display log entries that have run in a specific time frame by selecting from the Horizon list.

Command status

When a user runs a workbook command, the command can complete successfully if there are no errors or if the number of errors does not exceed an acceptable number. If the acceptable number of errors is exceeded, the command fails. The user can also cancel the command before the data changes are saved. This worksheet provides a status column and a color bar to help you quickly recognize whether a command has completed successfully, failed, or was canceled.

The acceptable number of errors that can occur when a command runs is set by the worksheet author. Authors can configure whether a data modification command fails when the first error occurs or completes successfully even though some errors have occurred. When the author allows some errors to occur, they set an error limit for the worksheet. If this limit is not exceeded, the command can complete successfully. Therefore, a user might be able to confirm a command's data changes even though not all record insertions, modifications, or deletions have occurred successfully. The Status column and the color bar can help you to differentiate between the commands that were successful and the commands that were successful yet had errors.



The status of a command can be one of the following:

Completed—The command completed successfully with no errors.

Completed—The command completed successfully with some errors.

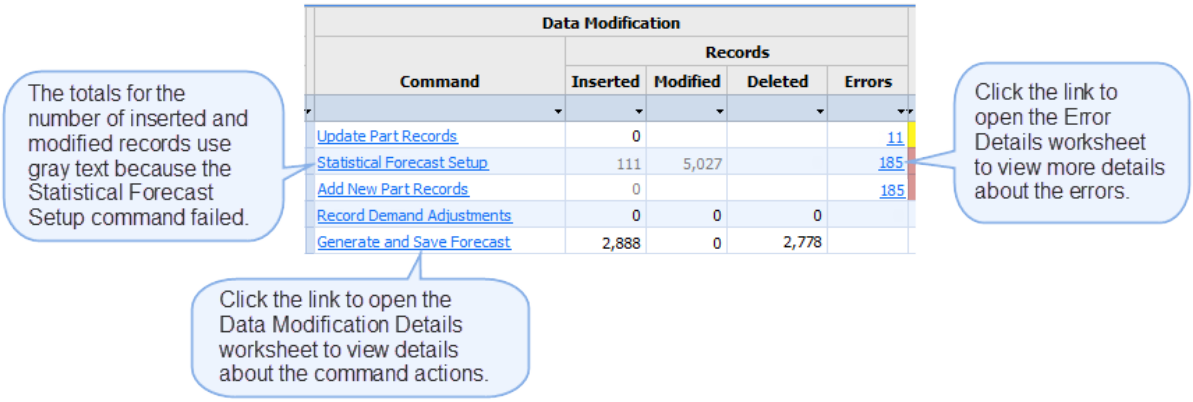
Canceled—The command was canceled by the user. No data changes were made.

Failed—The command failed because the acceptable number of errors was exceeded. No data changes were made. A command might also fail due to a non-data error, such as an invalid scenario or a missing resource that prevents the command from completing successfully. Information about these errors is provided in the Details column.

Data Modification columns

The Data Modification columns contain information about data changes made by commands. The number of records that are inserted, modified, and deleted are displayed with the number of errors, if any, that occurred. These record counts apply only to the data in tables that the worksheets updated by the command are based on. They do not include inserted reference records or related deleted records.

The Inserted, Modified, and Deleted columns contain a number if the worksheet is configured to perform that operation (this number can be zero). If there is no number in the column, the worksheet is not configured to perform that operation. These numbers are displayed even if a command fails or is canceled. However, the text is gray to indicate that the changes were not made.



The Data Modification columns display the total number of records that are inserted, modified, and deleted by a command. You can click the name of a command to open the Data Modification Details worksheet, which displays the number of records modified by each command action. You can click the number of errors in the Errors column to open the Error Details worksheet, which provides information about any errors that occurred.

When a worksheet test is logged in the Workbook Command Log worksheet, the Command column displays the word Action followed by the name of the worksheet (for example, Action: Updated Independent Demands).

Note: The records in this worksheet are automatically deleted after 14 days.
On-Demand: The number of days can be changed by Kinaxis Customer Support.
On-Premises: For information about changing the default setting, see " Automatic deletion of system records" on page 277.

Data Modification Details worksheet

This worksheet shows details about the results of each action of a data modification command. The number of records that were inserted, modified, or deleted by each action of the command and the errors that occurred, if any, are reported. This worksheet also provides other information, including the statuses of the actions (such as whether they completed successfully or failed) and the worksheet that is updated by each action.

You can access this worksheet by clicking a link in the Command column of the Automation Task Log worksheet or the Workbook Command Log worksheet.

Action status

An action can complete successfully if there are no errors or if the number of errors does not exceed an acceptable number. If the acceptable number of errors is exceeded, the action fails, causing the command to fail. This worksheet provides a status column and a color bar to help you recognize whether a command action has completed successfully or failed.

The acceptable number of errors that can occur when an action is performed is set by the worksheet author. Authors can configure whether a data modification action fails when the first error occurs or completes successfully even though some errors have occurred. When the author allows some errors to occur, they set an error limit for the worksheet. If this limit is not exceeded, the action can complete successfully. Therefore, you might be able to confirm a command's data changes even though not all record insertions, modifications, or deletions have occurred successfully. The Status column and the color bar can help you to quickly differentiate between the actions that were successful and the actions that were successful yet had errors.

A user can also cancel a command ran interactively before the data changes are saved. However, when a command is canceled, command actions still report a "Completed" status. You should use the information provided in the details worksheet in conjunction with the Workbook Command Log worksheet to understand the overall result of the command. Additionally, you can check for gray text in the Inserted, Modified, and Deleted columns. Gray text means that the data changes were not made.

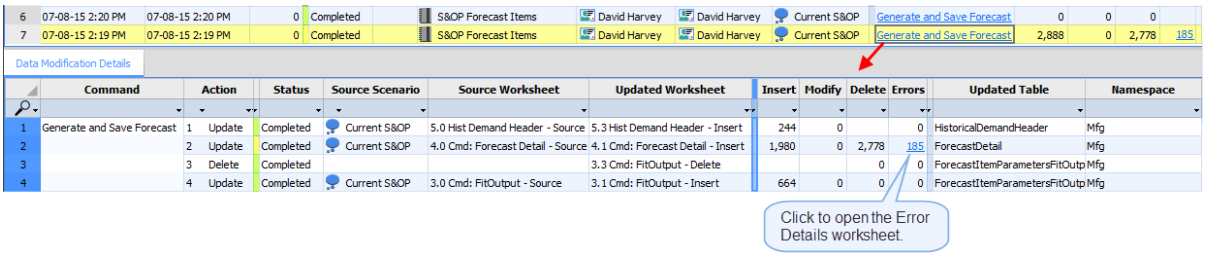
The status of an action can be one of the following:

Completed—The action completed successfully with no errors.

Completed—The action completed successfully with some errors.

Failed—The action failed because the acceptable number of errors was exceeded. No data changes were made because a failed action results in a failed command. If an action fails, any subsequent actions are not displayed in this worksheet. A command might also fail due to a non-data error, such as an invalid scenario or a missing resource that prevents the command from completing successfully.

When you click a command name in the Automation Task Log worksheet or the Workbook Command Log worksheet, the row is highlighted to identify the command you are viewing information about. To close the Data Modification Details worksheet and remove any highlighting, click Reset on the workbook toolbar. This will also close the Error Details worksheet if it is open.



If errors occurred when an action was being performed, you can click the link in the Errors column to open the Error Details worksheet, which displays information about only those errors.

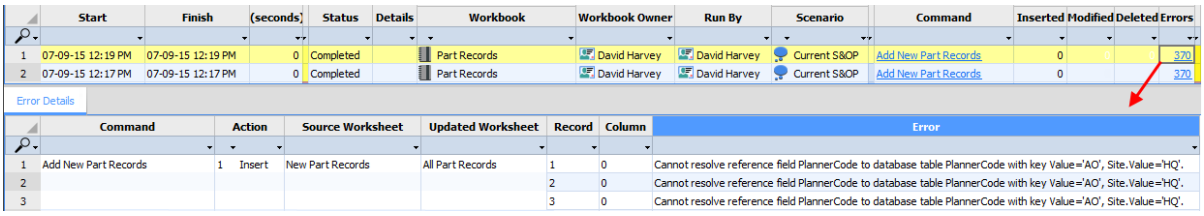
> **Note:** By default, 14 days of workbook command logging information is stored.
> **On-Demand:** The number of days can be changed by Kinaxis Customer Support.
> **On-Premises:** For information about changing the default setting, see " Automatic deletion of system records" on page 277.

Error Details worksheet

If errors occur when a data modification command runs, you might need to fix the errors so that the command can run successfully. You can use the information logged in this worksheet to investigate and then fix data modification errors. Any errors that are identified when an action is performed are logged in this worksheet. You can view information about the errors, including the location of the records in error and why the errors occurred.

You can access this worksheet by clicking on the number of errors that appears in the Errors column of the Automation Task Log worksheet, the Workbook Command Log worksheet, or the Data Modification Details worksheet.

When you click an error link in the Automation Task Log worksheet or the Workbook Command Log worksheet, the row is highlighted to identify the command you are viewing information about. To close the Error Details worksheet and remove any highlighting, click Reset on the workbook toolbar.



The maximum number of error records displayed in the Error Details worksheet is set by an administrator. This maximum number applies to the number of errors that occur for each action in the command. For more information, see "Setting the maximum number of command errors logged" on page 623.

> **Note:** By default, 14 days of workbook command logging information is stored.
> **On-Demand:** The number of days can be changed by Kinaxis Customer Support.
> **On-Premises:** For information about changing the default setting, see " Automatic deletion of system records" on page 277.

Script Log worksheet

This worksheet provides information about RapidResponse scripts that have been run by all users, including scripts that are run:

- manually from the Run Automation Task dialog box or Explorer.
- by scheduled tasks.
- by automation chains.
- by forms.
- by other scripts.
- through workbook commands.
- by a Web service client program.

For each script, the log includes its start and end time, how long it took to run, the user that ran it, the output, and any parameter values passed to the script. You can use this information to determine if scripts are running properly. If the script failed, you can also view the values passed to the script to determine if the script failed due to an invalid input.

You can also view scripts that are running, including which user is running the script and how long the script has been running, and cancel a running script. For more information, see "Monitoring and canceling scripts" on page 750.

▸To view the properties of a script

1. In the **Automation Log** workbook, click the **Script Log** worksheet.
2. Do one of the following:
   - Select the script you want to view, and then on the workbook toolbar, click **Properties** .
   - Click the script name.

> **Note:** For more information about RapidResponse scripts, see the *RapidResponse Scripting Guide*.

Change Data Capture Log

This worksheet provides information about all Change Data Capture (CDC) activities performed in RapidResponse and through Web services. This includes the following operations:

- Creating CDC instances.
- Capturing changes in an instance.
- Clearing changes in an instance.
- Deleting instances.

The Instance control contains all CDC instances currently active in your system. If you want to view data for an instance that is not in the list, such as a deleted instance, you can select **= All =** in the list. This displays data for every instance in the worksheet, and you can then search for the instance you want.

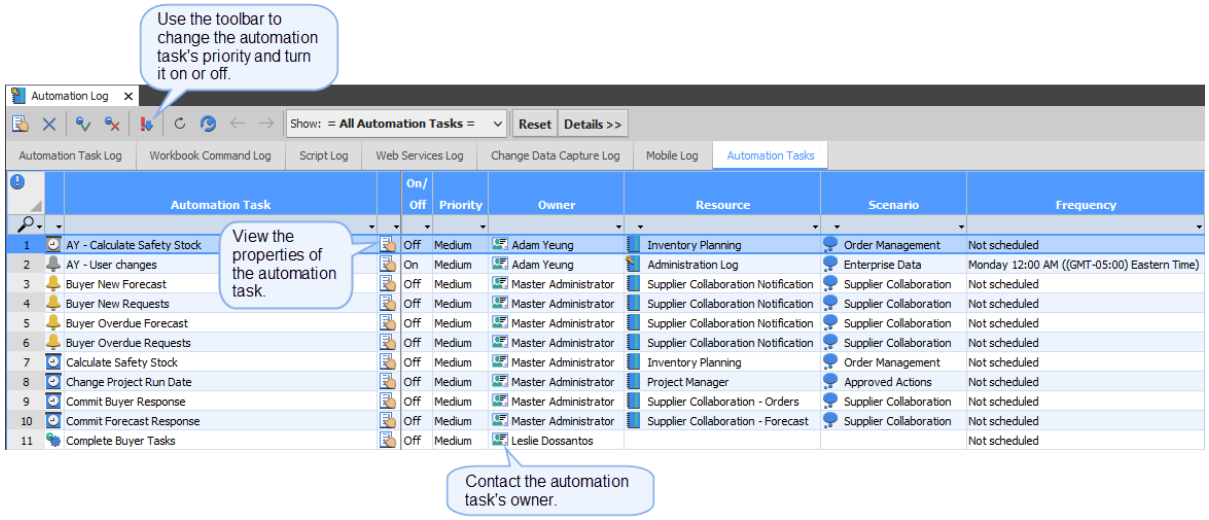
Mobile Log

The web client communicates with the RapidResponse system by running internal RapidResponse scripts. The Mobile Log tracks the execution of these scripts. This log resource can be useful when troubleshooting web client issues. Information in this log might be requested by Kinaxis Customer Support.

Automation Tasks

The Automation Tasks worksheet lists all of the automation tasks used on your RapidResponse system and shows details about each task, including whether the automation task is scheduled to run, when the automation task is scheduled to run, and the automation task's priority. You can choose to view all automation tasks (alerts, automation chains, and scheduled tasks) or a single type.

Depending on the type of automation task you are viewing information about, you might want to show or hide the Worksheet/Metric, Sequence, and Report columns. You can do this by clicking **Details** on the workbook toolbar.



Both private and public automation tasks are displayed in this worksheet. You can view the properties of any automation task by selecting its row and clicking Properties in the workbook toolbar or by clicking the Properties button beside the automation task's name. You can modify the properties of any

automation task that you can also modify from the Explorer. You cannot modify the properties of a private automation task owned by another user. To contact the user who owns the automation task, click the User contact information button beside the name displayed in the Owner column of the worksheet. You can send the user a Message Center message from their contact card.

You can perform similar actions and view additional details about automation tasks, and other resources, in the Resources workbook. For more information, see "Monitoring resource usage" on page 746.

Note: If your RapidResponse system has version control turned on, you must check out a public automation task before you can edit its properties in the Automation Tasks worksheet.

Note: You must have permission to author alerts, automation chains, and scheduled tasks to view and modify the properties of these automation tasks.

Turning automation tasks on and off

Occasionally, you might need to turn off automation tasks so that they do not run as scheduled. For example, when upgrading to the latest version of RapidResponse you might need to turn off all automation tasks to ensure modifications or reports are not generated on data that is still being modified to support new database tables or analytics. You can turn on and off any automation task in the Automation Tasks worksheet.

▸To turn an automation task on and off

1. In the **Automation Tasks** worksheet, select the row for the automation task that you want to turn on or off, and then click one of the following:
   - **Turn On**.
   - **Turn Off**.

Tip: You can also turn automation tasks on or off using the Resources workbook. For more information about using this workbook, see "Monitoring resource usage" on page 746.

Changing automation task priority

Each automation task runs with a specific priority, which determines the order that automation tasks are queued in. Higher priority automation tasks are always queued to run before lower priority ones, which ensures important system tasks and business-critical reports are placed in the queue before any other automation tasks in the queue. The automation tasks that run as part of an automation chain are all queued with the priority of the automation chain, regardless of the priority set for each automation task within the chain.

In some cases, a new business process might take precedence over others, and require the priority of older automation tasks to be reduced, which ensures the new process is queued first. You can change the priority of automation tasks in the Resources workbook. You should assign the highest priority to the most important automation tasks, which ensures they run before any others.

The priority you assign to an automation task is the priority used by any user who runs the alert. However, if you give an automation task to a general user or user administrator, the automation task's

priority is changed to Medium, and you must modify the priority if it should be higher. If you want multiple users to run the automation task with the priority you specify, you should share the automation task with those users. For information about sharing and giving automation tasks, see the *RapidResponse User Guide*.

▸To change the priority of an automation task

1. In the **Automation Tasks** worksheet, select the row for the automation task you want to change.
2. On the workbook toolbar, click **Change Priority**.
3. In the **Change Priority** dialog box, select one of the following priorities.
   - **Critical**—These tasks always run first. This priority is typically reserved for system tasks and critical business processes.
   - **Urgent**—These tasks run when there are no more Critical priorities in the queue. These are typically very important but not business-critical.
   - **High**—These tasks run when there are no more Urgent priorities in the queue. These are typically more important than general users' tasks.
   - **Medium**—These tasks run when there are no more High priorities in the queue. This is the default priority, and is typically the priority a general user's tasks run at.
   - **Low**—These tasks run only when there are no higher priorities in the queue. These are typically alerts that can run at any time.

Tip: You can also change the priority of an automation task using the Resources workbook. For more information about using this workbook, see "Monitoring resource usage" on page 746.

Deleting automation tasks

You can use the Automation Tasks worksheet to delete automation tasks that are no longer in use. For example, you might notice that a significant amount of time has passed since the last time an automation task completed. Or, you might need to delete private automation tasks owned by users who are no longer with your company. Deleting unneeded resources can reduce system memory requirements and improve system performance.

Deleting an automation task removes it from all users who had access to it, and it no longer runs. The workbooks, scorecards, scripts, alerts, scheduled tasks, or automation chains used in the automation task are not deleted.

▸To delete an automation task

1. In the **Automation Tasks** worksheet, select the row for the automation task you want to delete.
2. Click **Delete**.
3. Click **OK**.

Text logging for alerts

This topic only applies to the On-Premises version of RapidResponse.

In addition to the Automation Log workbook, RapidResponse writes alert processing information to the **ServiceHost.log**, which by default is located in the **C:\RapidResponse\Logs** folder. Alerts that fail are

noted in the **ServiceHost.log** file along with the processing details of each failed alert. This file is always opened in append mode. The alert creator is notified through RapidResponse Message Center (and possibly by email) if an error occurs during alert processing. Mail system errors will be reported in the **ServiceHost.log**. This log file is found in the folder specified in the registry key:

HKEY_LOCAL_MACHINE\Software\Webplan Inc.\Webplan\Directories\Logs

When an alert fails, an error message is written to the **ServiceHost.log**, and an identical message is sent to the alert creator. The first line of each error message states:

```
<Date> <Time> Failed alert: <alertName>. Creator: <Creator name>
```

The error messages will identify the reason(s) for the alert failure. For example:

```
<02/28/05> <3:15pm> Failed alert: <Action List>. Creator: <Bob>
Scenario <My Scenario> does not exist.
```

▸To view the ServiceHost.log file

1. Open **Microsoft Windows Explorer**.
2. Navigate to the file **ServiceHost.log** in the following location:

   C:\RapidResponse\Logs

   This is the default location for log files.

> **Note:** Your log files might be located in a different folder structure, depending on how you customized your RapidResponse installation. To check the location of your log files, open the Microsoft Windows Registry Editor and navigate to the following folder: **HKEY_LOCAL_MACHINE\Software\Webplan Inc.\Webplan\Directories**

The file path name beside the Logs entry tells you where all your log files are located. The location of log files cannot be changed by editing this registry value.

RapidResponse text-based log files

This topic applies only to the On-Premises version of RapidResponse.

Much of the information logged in the **Administration Log** and the **Data Import and Update Log** workbooks is also available in text-based log files. If, for some reason, you cannot start the RapidResponse client or the RapidResponse Server, you might need to review the text-based log files to troubleshoot an issue.

All log files are stored in the **C:\RapidResponse\Logs** folder on the same computer as the RapidResponse Server executables. The **Logs** folder location cannot be customized; that is, the Logs folder can only be a sub-folder to the main RapidResponse folder.

The log files can be used for debugging purposes or analysis by Kinaxis Customer Support to help diagnose problems or improve system performance.

The following table summarizes the operational RapidResponse log files.

Log file	Description
Heartbeat.log	The system status messages (also known as heartbeats) are written to this log. These are the same messages written to the **Server.log** file. However, the status messages in **Server.log** are written over four lines. The messages in this file are written over one line in a tab-delimited format that can be easily imported into Microsoft Excel for analysis. For more information about the fields in this file, see "Heartbeat.log file" on page 470.
Performance.log	This log file can be used to diagnose RapidResponse Server performance issues. It logs the amount of time server operations and commands take to complete and the amount of time spent waiting before operations can execute. For more information about the fields in this file, see "Performance.log file" on page 473.
Query.log	Logs every query executed by RapidResponse. However, writing to this file is not enabled without instructions from Kinaxis Customer Support. Writing to this file can consume a significant amount of system resources which can impact system and user performance.
QueryHistory.log	This file can be configured to log details on all RapidResponse queries that have moved to a status of Closed. This allows you to look at more historical query information than is available in Query Manager which provides details on all queries run in the past five hours, including active queries. For more information about this log file, see " QueryHistory.log file" on page 474. For more information about Query Manager, see "Monitoring and canceling problematic queries " on page 603.
RRMonitor.log	Logs the activities of the RapidResponse Server Monitor service. This service monitors the status of the RapidResponse Server service. If the RapidResponse Server service stops unexpectedly or crashes, this service saves debugging information for analysis by Kinaxis Customer Support to help diagnose the problem. For more information, see "Internal errors and system crashes" on page 244.
SecurityAudit.log	Logs changes related to key security controls, including changes to system configuration, users and groups, permissions, resource dependencies, and profile variables. The information in this file is available in the Security Audit worksheet in the Administration Log workbook. For more information, see "SecurityAudit.log file" on page 477.
Server.log	Much of the information in this file is available in the Administration Log workbook. Amongst the items noted in this log file are system and data import status. This log file also includes system status messages (also know as heartbeats) and performance statistics. For more information, see " Server.log file" on page 464.
ServerAudit.log	Logs internal RapidResponse information. This file is sometimes requested by Kinaxis Customer Support to help diagnose problems or improve system performance.
ServiceHost.log	Records all alert and collaboration processing information. Alerts that fail are noted along with the processing details of each failed alert. This file is always opened in append mode. The alert creator is notified through RapidResponse (and possibly by email) if an error occurs during alert processing. For more information, see "Automation logging" on page 448. This file is stored in the **ServiceHost** subfolder in the **Logs** folder.
UtilityServer.log	Records messages generated by internal RapidResponse utility programs.

Note: Most of the files noted in the previous table are never empty; new messages are appended. You might need to periodically review the size of the log files and remove older information, if necessary.

Management of log files

An accumulation of log files can potentially consume a significant amount of disk space which can impact RapidResponse Server system performance. This section describes how the files are automatically managed for you.

The following log files include a timestamp in their file names:

- Heartbeat
- Performance
- Query
- QueryHistory
- SecurityAudit
- Server
- ServerAudit

For example, the **Server.log** files are named **Server.*timestamp*.log** where the timestamp is in the **yymmdd-hhmmss** format. Here's an example:

Server.141222-155832.log.

New files are created for each of these logs when RapidResponse Server is started. Data is written to these active files until RapidResponse Server is restarted and new versions of the log files are created. The timestamp represents the date and time the files were created.

Log files are limited to 10 MB in size. If a log file reaches this limit, it is closed and a new active file is created.

Log files older than 180 days are automatically deleted when RapidResponse Server is restarted. However, this only applies to log files that include a timestamp in their name. Consider reviewing the Logs folder periodically to remove some of the older log files that do not use timestamps and you no longer need. You can also use the **PruneFiles** command to manage logs files that do not use a timestamp. For more information, see "PruneFiles command" on page 406.

Server.log file

Much of the information in the **Server.log** file is available in the Administration Log workbook. Amongst the items noted in this log file are system and data import status.

The following is an example of a **Server.log** file.

```
2014-12-22 16:18:07 INFO - Startup: RapidResponse Server version
12.0.0.1366:x64
2014-12-22 16:18:07 INFO - Code compiled: Nov 29 2014 00:47:30 Release build
2014-12-22 16:18:07 WARN - DeleteDirectory(directory =
'C:\RapidResponse\Program\Vault\vault_141222_155900_1', noRecycleBin = TRUE,
mustExist = TRUE) entered
2014-12-22 16:18:07 WARN - DeleteDirectory() exited returning TRUE
2014-12-22 16:18:07 INFO - Server role is assuming active because it's own
heartbeat is still valid ... self_expiry=22.443000
2014-12-22 16:18:07 INFO - Server is running in Active mode.
2014-12-22 16:18:07 INFO - File cache size: 0 GB ... 1024 GB
```

Heartbeat messages

Every 15 minutes, RapidResponse Server writes a *heartbeat*, or status, message to **Server.log**. These heartbeat messages provide a status of the RapidResponse Server, and can provide valuable information and usage statistics when trying to diagnose system issues.

Heartbeat messages are also written before RapidResponse Server is stopped or stops unexpectedly (if possible).

Each heartbeat is comprised of several lines. For example:

```
2019-05-24 14:37:33 INFO - Heartbeat: Query: 1129 (+9111 System) in 238s;
Memory 77%: input 26%, query 9%, calculated 15% (recycled 3104MB),
cachedQuery 0%; free versions: 8188; Users: 2; RecordId usage: 0%, MemMapped:
0.00GB
2019-05-24 14:37:33 INFO - QE3 Execution Statistics: exec=1120 fallback=28
fail=0 Overhead=0s
2019-05-24 14:37:33 INFO - Total Client Response Time (Parse, Exec, Validate,
Submit): 5.268, 180.660, 0.000, 0.000 System Queries: 9.505, 18.098, 0.009,
0.033
2019-05-24 14:37:33 INFO - System idle: 76%, % time by num active queries: 24
0 ^ 0 0
2019-05-24 14:37:33 INFO - Pool Usage: NewPool=0.0KB (FreeList: 0.0KB,
LargeAlloc: 0.0KB); MemPool=960.8MB; Largest are: Mfg::CTPInternal(301.8MB),
LoadedRecordBlock(152.3MB), Query Results(137.3MB), Query Parse(116.9MB),
Mfg::NetInternal(113.7MB)
2019-05-24 14:37:33 INFO - Page Usage: PageMem: 1.4GB; Largest are: Memory
pool(863.7MB), LoadedRecordBlockBodies(460.7MB), Page fragment pool(76.7MB),
RootContainer(14.0MB), RecordSet(8.8MB)
2019-05-24 14:37:33 INFO - SIMPLIFIED HEARTBEAT STATS:
2019-05-24 14:37:33 INFO - Memory Limits: Physical Memory(4.00GB), RR Process
Limit (2.80GB)
2019-05-24 14:37:33 INFO - Memory Coordinator: Hard Limit(2.52GB), Soft Limit
(2.27GB)
2019-05-24 14:37:33 INFO - OS Report: Working Set (2.97GB), Page File Usage
(4.89GB)
2019-05-24 14:37:33 INFO - Memory Consumer (InUse, Quota, Urgency):
2019-05-24 14:37:33 INFO - RecordBlock (613.1MB, 613.1MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - JEMalloc (507.2MB, 507.2MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - Calculated (439.1MB, 711.4MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - Query (270.1MB, 269.9MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - Other (87.5MB, 87.5MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - Input (52.1MB, 52.1MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - ReferenceIndex (50.3MB, 50.3MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - HashIndex (20.8MB, 20.8MB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - BigBlockAllocator (512.0KB, 512.0KB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - RecordBlockCache (0.0KB, 0.0KB, UNDER_LIMIT)
2019-05-24 14:37:33 INFO - JEMalloc Memory Stats
2019-05-24 14:37:33 INFO - In Use (0.50GB)
2019-05-24 14:37:33 INFO - Resident (0.52GB)
2019-05-24 14:37:33 INFO - Retained (0.0GB)
2019-05-24 14:37:33 INFO - Allocated (0.45GB)
2019-05-24 14:37:33 INFO - Active (0.47GB)
2019-05-24 14:37:33 INFO - Metadata (0.02GB)
2019-05-24 14:37:33 INFO - Page Pool: Committed Pages (3.00GB), Free
Committed Pages (1.32GB)
2019-05-24 14:37:33 INFO - Large Pages (0.0GB)
2019-05-24 14:37:33 INFO - Memory High Water Mark(%): input 26%, query 9%,
calculated 15%, cachedQuery 0%
2019-05-24 14:37:33 INFO - Memory High Water Mark(#): input 742.3MB, query
270.1MB, calculated 444.0MB, cachedQuery 1.0KB
2019-05-24 14:37:33 INFO - Recalculations since last heartbeat -- Total:
190485 recalculations (3.0GB)
Core::CalcDateTables: 68 recalculations (1.0MB)
```

```
Mfg::CalcConsensusForecast: 30512 recalculations (18.5MB)
Mfg::CalcDirectComponent: 10702 recalculations (11.0MB)
Mfg::CalcEventDisaggregationTotals: 50 recalculations (1009.6KB)
Mfg::CalcSeries: 1651 recalculations (1.8MB)
Mfg::CalcSupplySeries: 30 recalculations (29.8KB)
Mfg::CTPForecastCostInfoInternal: 8849 recalculations (10.4MB)
Mfg::CTPInternal: 36159 recalculations (1.5GB)
Mfg::FLPWCInternal: 19147 recalculations (888.4MB)
Mfg::IndDmdCOGSInternal: 28061 recalculations (29.3MB)
Mfg::InvalidateCachedCostOfGoodsSold: 8849 recalculations (8.6MB)
Mfg::NetForecast: 9863 recalculations (29.7MB)
Mfg::NetInternal: 36454 recalculations (583.3MB)
Mfg::RoutingInternal: 20 recalculations (19.8KB)
Mfg::WorkCenterCapacityInternal: 70 recalculations (2.0MB)
```

The heartbeat messages in the **Server.log** file are also written to the **Heartbeat.log** file. Each heartbeat message in this file is written over one line in a tab-delimited format that can be easily imported into Microsoft Excel for analysis. For more information about the fields in this file, see "Heartbeat.log file" on page 470. Here are some of the details about the fields in the heartbeat message.

▸Heartbeat message - Line 1

The following table describes the first line of the heartbeat message.

Heartbeat item	Description
Query	The number of queries run in seconds. In the above example, 249 queries were run in 4 seconds. The value in parentheses represents the number of queries run against system tables. For more information about system tables, see "System tables" on page 481.
Memory	The percentage of system memory RapidResponse is consuming.
Input	The percentage of system memory RapidResponse input data is consuming.
Query	The percentage of system memory RapidResponse queries are consuming.
Cache (recycled nnMB)	Amount of calculated memory that is reused.
Free versions	RapidResponse can maintain 8,192 scenarios (and versions). This number indicates the number of scenarios available. For more information about scenarios and versions available, see "Scenario memory consumption" on page 270.
Users	Number of users signed into RapidResponse.

Heartbeat item	Description
RecordId usage	Each record contained in an input table has a unique identifier, known as a RecordId. They are not recycled as records are deleted. The **RecordId usage** reports, as a percentage of the 4 billion records, the highest RecordId value amongst all the input tables (with less than 4 billion records). For example, 10 percent indicates 400,000,000 RecordIds have been used by a single input table. Once an input table uses about 3 billion RecordIds, it is no longer tracked for RecordId usage as RapidResponse Server manages and the stores the RecordIds in a different internal format (64-bit addressing instead of 32-bit). This change is applied during a RapidResponse Server restart and is noted in the **Server.log** file. Administrators should also be aware that after this change is applied more system memory will be consumed by the RapidResponse database. Values of less than one percent are displayed as 0. This measure does not report the name of the table. However, the **Server.log** file notes any input tables that are using more than 3 billion RecordIds. For more information about RecordId, see the the *RapidResponse Resource Authoring Guide*.
MemMapped	Amount of memory consumed by files loaded into memory.

▸Heartbeat message - Line 2

The second line of the heartbeat message provides information about query execution. In RapidResponse 2016.2 (and later), the internal query execution against the RapidResponse database improved. However, some queries continue to use the query execution methods from RapidResponse 2015.3 (and earlier). This line in the heartbeat message can help you better understand if you have queries that are using the old query execution methods.

Using the previous example again:

```
2019-05-24 14:37:33 INFO - QE3 Execution Statistics: exec=1120 fallback=28
fail=0 Overhead=0s
```

The information in the example consists of the following:

- **exec**—Represents the number of queries executed in a 15-minute period using query execution methods introduced in RapidResponse 2016.2. In this example, 1120 queries were executed.
- **fallback**—Represents the number of queries executed in a 15-minute period using query execution methods from RapidResponse 2015.3 (and earlier). In this example, 28 queries were executed.
- **fail**—Used for internal purposes and Kinaxis Support. Typically displays 0.
- **Overhead**—The number of CPU seconds (in a 15-minute period) used as overhead when executing queries.

▸Heartbeat message - Line 3

The third line of the heartbeat message provides timing information, which includes the CPU time spent parsing, executing, validating, and submitting queries to the database. Separate timings are presented for queries on input data and on data in system tables.

Using the previous example again:

```
2019-05-24 14:37:33 INFO - Total Client Response Time (Parse, Exec, Validate,
Submit): 5.268, 180.660, 0.000, 0.000 System Queries: 9.505, 18.098, 0.009,
0.033
```

In this example, a total of 5.268 seconds have been spent parsing user queries, and 180.66 seconds were used to execute those queries. Over the same period, a total of 9.505 seconds of CPU time have been spent parsing queries on system data, and executing those queries took 18.098 seconds.

▸Heartbeat message - Line 4

The fourth line of the heartbeat message provides query load statistics.

The System Idle represents the amount of time within the heartbeat that queries were not being run.

The other numbers in this heartbeat line represent the percentage of time queries were running. This is a series of numbers and delimiters. For example,

```
2019-05-24 14:37:33 INFO - System idle: 76%, % time by num active queries: 24
0 ^ 0 0
```

Three delimiters are used in this series:

- : (colon)—inserted after every fifth number in the series
- | (pipe)—inserted after every tenth number in the series
- ^ (carat)—inserted to mark the number of cores. In the previous example, six numbers are displayed before the carat. This means the computer where RapidResponse Server is installed has six cores. Cores can include physical cores and logical cores (if hyper-threading is enabled).

  The carat is only displayed if there are more queries than cores in the heartbeat interval.

The numbers in the series represent the percentage of time the cores were loaded with active queries.

The following example shows a heartbeat for a system running with six cores.

```
% time by num active queries: 7 10 20 6 4 : 2 ^ 30 5 0 0 | 0 0 0 0 0 : 0
```

Here's how to interpret the example:

- First number—a single query was running for 7 percent of the heartbeat time.
- Second number—two queries were running simultaneously for 10 percent of the heartbeat time. The queries were running on two cores.
- Third number—three queries were running simultaneously for 20 percent of the heartbeat time. The queries were running on three cores.
- Fourth number—four queries were running simultaneously for 6 percent of the heartbeat time. The queries were running on four cores.
- Fifth number—five queries were running simultaneously for 4 percent of the heartbeat time. The queries were running on five cores.
- Sixth number—six queries were running simultaneously for 2 percent of the heartbeat time. The queries were running on six cores.

Values beyond the six cores indicate that queries were queueing.

- Seventh number—seven queries were trying to run simultaneously for 30 percent of the heartbeat time.
- Eighth number—eight queries were trying to run simultaneously for 5 percent of the heartbeat time.
- Ninth number—nine queries were trying to run simultaneously for less than 1 percent of the heartbeat time.

  The following zeros in the sequence are all less than one percent.

▸Heartbeat message - Line 5

The fifth line of the heartbeat message provides information about memory consumption. This includes the sizes of the newest memory pool created in your system, and the amount of memory consumed from the total memory pool. The five largest memory consumers are listed, along with the amount of memory each is consuming.

Using the previous example again:

```
2019-05-24 14:37:33 INFO - Pool Usage: NewPool=0.0KB (FreeList: 0.0KB,
LargeAlloc: 0.0KB); MemPool=960.8MB; Largest are: Mfg::CTPInternal(301.8MB),
LoadedRecordBlock(152.3MB), Query Results(137.3MB), Query Parse(116.9MB),
Mfg::NetInternal(113.7MB)
```

In this example, the newest memory pool is empty, and of the total memory pool, 960.8 MB have been consumed. For these pools, CTP results are consuming the most memory.

▸Heartbeat message - Line 6

The sixth line of the heartbeat message provides information about memory page consumption. This includes the sizes of the amount of memory consumed from the total memory page. The five largest memory consumers are listed, along with the amount of memory each is consuming.

```
14:37:33 INFO - Page Usage: PageMem: 1.4GB; Largest are: Memory pool
(863.7MB), LoadedRecordBlockBodies(460.7MB), Page fragment pool(76.7MB),
RootContainer(14.0MB), RecordSet(8.8MB)
```

In this example, a total of 1.4 GB of paged memory is used, with the memory pool consuming the largest portion of it.

▸Heartbeat message - Recalculated tables section

The final section of the heartbeat identifies calculated tables that have been recalculated since the last heartbeat. This identifies a table that has been unloaded from memory because it was not used or invalidated by a query operation, but then needed to be reloaded. Each recalculated table reports the number of records and the size of the data that was reloaded. For more information about unloading data, see "RapidResponse system memory usage" on page 260.

If many tables are being recalculated in every heartbeat, it might indicate a lack of available memory. Data is unloaded from memory to allow other data to load, so if many tables are being unloaded and reloaded in every heartbeat period, you can improve system performance by adding more memory to the computer that RapidResponse Server is installed on.

```
14:37:33 INFO - Recalculations since last heartbeat -- Total: 190485
recalculations (3.0GB)
      Core::CalcDateTables: 68 recalculations (1.0MB)

      Mfg::CalcConsensusForecast: 30512 recalculations (18.5MB)

      Mfg::CalcDirectComponent: 10702 recalculations (11.0MB)

      Mfg::CalcEventDisaggregationTotals: 50 recalculations (1009.6KB)

      Mfg::CalcSeries: 1651 recalculations (1.8MB)

      Mfg::CalcSupplySeries: 30 recalculations (29.8KB)

      Mfg::CTPForecastCostInfoInternal: 8849 recalculations (10.4MB)

      Mfg::CTPInternal: 36159 recalculations (1.5GB)

      Mfg::FLPWCInternal: 19147 recalculations (888.4MB)

      Mfg::IndDmdCOGSInternal: 28061 recalculations (29.3MB)
```

```
Mfg::InvalidateCachedCostOfGoodsSold: 8849 recalculations (8.6MB)
Mfg::NetForecast: 9863 recalculations (29.7MB)
Mfg::NetInternal: 36454 recalculations (583.3MB)
Mfg::RoutingInternal: 20 recalculations (19.8KB)
Mfg::WorkCenterCapacityInternal: 70 recalculations (2.0MB)
```

Performance messages

The **Server.log** file logs the amount of time server operations and commands take to complete and the amount of time spent waiting before operations can execute. This type of information can be used to diagnose RapidResponse Server performance issues.

Here is an example of the performance information in the **Server.log** file:

```
2014-04-03 13:25:11.078 INFO [Server.Operation.Performance ] RapidResponse -
'Query' operation on 'Update System::TableInfo{System::Name,
System::Namespace.System::Name, System::A' took 1.1 seconds. Locked during
execution: this context (1.039749 s) nested contexts (0.000000 s) -- Top 5
critical sections (by wait time): WriteLock (1.039746)
```

The performance messages in the **Server.log** file are also written to the **Performance.log** file. The messages in this file are written over one line in a tab-delimited format that can be easily imported into Microsoft Excel for analysis. For more information about the fields in this file, see "Performance.log file" on page 473.

RapidResponse Server error codes and messages

The following error codes display if RapidResponse Server fails to restart after being instructed to do so.

- **Error Code 1—**There was an error in initializing communication with the Windows Service Manager.
- **Error Code 2—**There was an error in initializing for reception of RPC calls from the RapidResponse Server.
- **Error Code 3—**There was an error in initializing RapidResponse's data structures. This occurs if RapidResponse's registry keys cannot be opened, nor created.
- **Error Code 4—**There was an error in loading data. See **Server.log** for further information. Possible causes include errors in the data mapping, or a data integrity problem (such as an incorrect reference key).

Heartbeat.log file

The system status messages (also known as heartbeats) are written to the **Server.log** file. Each heartbeat message is four lines. The same heartbeat messages are written to the **Heartbeat.log** file but over one line in a tab-delimited format that can be imported into Microsoft Excel for analysis. The fields in **Server.log** are not in the same order in **Heartbeat.log**.

The following table describes the fields in the **Heartbeat.log** file.

Field	Description
TimeStamp	The date and time of the heartbeat. Heartbeats are recorded every 15 seconds.
NumQuery	The number of queries run in the heartbeat.
NumSysQuery	The number of queries run in the heartbeat against system tables. For more information about system tables, see "System tables" on page 481.
TotalQueryTime	Amount of CPU time used (expressed as number of seconds).
Users	Number of users signed into RapidResponse.
ParseTime	The number of seconds within the heartbeat (15 seconds) spent parsing queries against non-system tables (versioned data).
ExecTime	The number of seconds within the heartbeat (15 seconds) spent executing queries against non-system tables (versioned data).
ValidateTime	The number of seconds within the heartbeat (15 seconds) spent validating queries against non-system tables (versioned data).
SubmitTime	The number of seconds within the heartbeat (15 seconds) spent submitting queries against non-system tables (versioned data).
SysParseTime	The number of seconds within the heartbeat (15 seconds) spent parsing queries against system tables.
SysExecTime	The number of seconds within the heartbeat (15 seconds) spent executing queries against system tables.
SysValidateTime	The number of seconds within the heartbeat (15 seconds) spent validating queries against system tables.
SysSubmitTime	The number of seconds within the heartbeat (15 seconds) spent submitting queries against system tables.
Idle(%)	The amount of time within the heartbeat that queries were not being run (expressed as a percentage).
ActiveQueriesPercent	A series of numbers that represents the percentage of time queries were running. The numbers in the series represent the percentage of time the cores were loaded with active queries. For a detailed explanation, see "ActiveQueriesPercent field" on page 472.
TotalMemory(%)	The percentage of system memory RapidResponse is consuming.
InputMemory(%)	The percentage of system memory input data is consuming.
QueryMemory(%)	The percentage of system memory queries are consuming.
AnalyticMemory(%)	The percentage of system memory analytic calculations are consuming.
FreeVersions	RapidResponse can maintain 8,192 scenarios (and versions). This number indicates the number of scenarios available. For more information about scenarios and versions available, see "Scenario memory consumption" on page 270.

Field	Description
NewPool(GB)	This field shows the size of the newest memory pool in GB, including memory to be freed and large allocations. Memory pools for storing input data and results, and holding intermediate results. Stored results are maintained as long as possible to prevent recalculation in the event they are required again. Intermediate results are maintained in a memory pool while they are being recalculated. For more information about memory pools, see "Memory settings for calculations" on page 266.
MemPool(GB)	The size of the entire memory pool in GB.
Pool1(GB)	The name of the largest memory pool and size (GB) using the `name:size` format.
Pool2(GB)	The name of the second largest memory pool and size (GB) using the `name:size` format.
Pool3(GB)	The name of the third largest memory pool and size (GB) using the `name:size` format.
Pool4(GB)	The name of the fourth largest memory pool and size (GB) using the `name:size` format.
Pool5(GB)	The name of the fifth largest memory pool and size (GB) using the `name:size` format.
SlowLock1	The type of lock that is causing threads to have to wait. This field only displays information if you have consulted Kinaxis Customer Support and they have assisted you in turning it on.
Wait|Slp|MxWt1 (s)	The total time threads had to wait to process, total time waiting threads were in a sleep state, and the maximum wait time for a single thread, in seconds. This field only displays information if you have consulted Kinaxis Customer Support and they have assisted you in turning it on.
Collision1	The number of threads that had to wait because of the lock. This field only displays information if you have consulted Kinaxis Customer Support and they have assisted you in turning it on.
Cache (recycled MB)	Number of calculated memory that is reused.
MemMappedFiles	The amount of memory consumed by files loaded into memory. This memory is not reported in the memory consumption fields.

ActiveQueriesPercent field

The ActiveQueriesPercent field represents the percentage of time queries were running and is expressed as a series of numbers. Here is an example:

```
7 10 20 6 4 : 2 ^ 30 5 0 0 | 0 0 0 0 0 : 0
```

Three delimiters are used in this series:

- : (colon)—inserted after every fifth number in the series
- | (pipe)—inserted after every tenth number in the series
- ^ (carat)—inserted to mark the number of cores. In the previous example, six numbers are displayed before the carat. This means the computer where RapidResponse Server is installed has six cores. Cores can include physical cores and logical cores (if hyper-threading is enabled).

  The carat is only displayed if there are more queries than cores in the heartbeat interval.

The numbers in the series represent the percentage of time the cores were loaded with active queries.

Here's how to interpret the example:

- First number—a single query was running for 7 percent of the heartbeat time.
- Second number—two queries were running simultaneously for 10 percent of the heartbeat time. The queries were running on two cores.
- Third number—three queries were running simultaneously for 20 percent of the heartbeat time. The queries were running on three cores.
- Fourth number—four queries were running simultaneously for 6 percent of the heartbeat time. The queries were running on four cores.
- Fifth number—five queries were running simultaneously for 4 percent of the heartbeat time. The queries were running on five cores.
- Sixth number—six queries were running simultaneously for 2 percent of the heartbeat time. The queries were running on six cores.

Values beyond the six cores indicate that queries were queuing.

- Seventh number—seven queries were trying to run simultaneously for 30 percent of the heartbeat time.
- Eighth number—eight queries were trying to run simultaneously for 5 percent of the heartbeat time.
- Ninth number—nine queries were trying to run simultaneously for less than 1 percent of the heartbeat time.

  The following zeros in the sequence are all less than one percent.

Performance.log file

The **Server.log** file logs the amount of time server operations and commands take to complete and the amount of time spent waiting before operations can execute. This type of information can be used to diagnose RapidResponse Server performance issues. This information is also written to the **Performance.log** file but over one line in a tab-delimited format that can be imported into Microsoft Excel for analysis.

Here is an example of the performance information in the **Server.log** file:

```
2014-04-03 13:25:11.078 INFO [Server.Operation.Performance ] RapidResponse -
'Query' operation on 'Update System::TableInfo{System::Name,
System::Namespace.System::Name, System::A' took 1.1 seconds. Locked during
execution: this context (1.039749 s) nested contexts (0.000000 s) -- Top 5
critical sections (by wait time): WriteLock (1.039746)
```

The performance logging includes the information about the system commands and tasks such Capture, Condense, and system start up. For more information about the commands, see "RapidResponse system commands" on page 384. Internal system operations are also included in performance logging.

RapidResponse logs performance information about server operations and commands for the two following cases:

- The RapidResponse Server operation or command execution time is greater than five seconds.
- The three following cases occur:
  - The total wait time to run the operation or command is greater than 0.01 seconds.
  - The total wait time is greater than 10 percent of the total operation or command execution time.
  - The RapidResponse Server operation or command execution time is greater than one second.

The following table describes the fields in the **Performance.log** file.

Field	Description
TimeStamp	The date and time of the performance logging.
HttpId	If the operation or command executed is initiated by the RapidResponse Application Server then this field is populated with query information.
Operation	The name of the operation or command that is executed.
Details	Information about the operation or command that is executed. This field might not be populated.
Time	The amount of time (in seconds) to execute the operation or command. This includes wait time.
WaitForLockThis	The amount of time (in seconds) to that the system waited before executing the operation or command.
WaitForLockNested	The amount of time (in seconds) to that the system waited before executing the nested operations or command.
WaitForLock1	The most critical operation ranked by total wait time (in seconds) that is causing a wait lock and expressed in the following format: `(WriteLock: 1.039746)` If this field is empty, it displays `(,)`.
WaitForLock2	The second most critical operation ranked by total wait time (in seconds) that is causing a wait lock.
WaitForLock3	The third most critical operation ranked by total wait time (in seconds) that is causing a wait lock.
WaitForLock4	The fourth most critical operation ranked by total wait time (in seconds) that is causing a wait lock.
WaitForLock5	The fifth most critical operation ranked by total wait time (in seconds) that is causing a wait lock.

QueryHistory.log file

The Query Manager workbook in the RapidResponse client provides information on currently running queries (in the Active Queries worksheet), as well as all queries that have run in the past five hours (in the Recent Query History worksheet). This information can be used when investigating system performance issues, such as alerts not completing on time or workbooks taking longer than expected to open. For more information, see "Monitoring and canceling problematic queries " on page 603.

If you want to save a longer period of historical query information, you can review the **QueryHistory.log** file. This file logs every query that has its status changed to closed. Each record is made up of a number

of fields, including all those reported in the Recent Query History worksheet, that provide details on a particular query. Data in **QueryHistory.log** can be saved for a longer definable time than data in Query Manager.

By default, the **QueryHistory.log** file includes the following fields for each record (or line).

Field	Description
Id	Internal RapidResponse query identifier.
CreateTime	Date and time when RapidResponse received the query request.
PreparationDuration	Number of seconds taken to prepare (parse) the query.
ExecutionDuration	Number of seconds taken to run the query.
CachedAnalyticTime	The total time, in seconds, to process the cached analytic calculations generated by a query. For more information about caching results, see the *RapidResponse Resource Authoring Guide* and "Caching worksheet results" on page 763.
UncachedAnalyticTime	The total time, in seconds, to process the non-cached analytic calculations generated by a query.
ExecutionCPUTime	Number of seconds of CPU time to run the query.
ValidateDuration	For queries that modify data, the number of seconds to validate that changes are acceptable.
SubmitDuration	For queries that modify data, the number of seconds to write the data changes to the database. While changes are written to the database, a write-lock is held by the query. However, if data changes are being written to a temporary scenario, the query can only hold the write-lock for one second.
ResultRowCount	Number of rows of data returned by this query.
TrackingDataChanges	Whether data changes are tracked for this query. For more information about data change tracking, see "Data change tracking and record identification" on page 829.
Insert	The number of inserted records
AutoCreate	The number of auto created records.
Update	The number of modified records.
Delete	The number of deleted records.
Unchanged	The number of unchanged records.
Source	The resource that initiated the query. Common examples included workbooks (WBK), scorecards (SCD), scheduled tasks, alerts, and actions that modify data.
Table	The namespace and table in the RapidResponse data model this query was run against. If the query was run against more than one table, `<Multiple>` is returned.
User ID	The ID of the RapidResponse user whose action generated the query request. An ID of RapidResponse indicates the query was run under an internal account used by RapidResponse. For example, this is the account used to run alerts.
MemoryUsage	Total memory usage in MB for the query result.

Field	Description
MaxMemoryUsage	Peak memory usage in MB for the query result.
Priority	Priority level of the query, either `Low` or `Normal`. Low priority is used for queries generated from alerts, and normal priority is used for all other queries.
Status	Current status of the query. All records in this log file will have a status of `Closed`.
Scenario	The scenario in which the user generated this query request. Temporary scenarios use the question mark character (?) as the initial character in their name. For example, **?6fc0e16d-1d9a-46a4-ae6d-294c4e27c025**. Temporary scenarios are automatically created while data is being modified (transactions). The changes are stored internally in temporary scenarios in the RapidResponse database. RapidResponse continuously manages these scenarios. For more information about scenarios used in the query, see the "ScenarioPath" on page 476 field in this table.
CloseTime	Date and time when the query was closed (removed from RapidResponse Server memory). In some cases, Microsoft Excel might convert this and date and time value into an unexpected format.
LifeTime	Total time, in seconds, from when the query request was received until the query was subsequently closed.
ExecutionCount	Number of times the query was run between the time it was created and when it was closed.
CancelIssuedTime	Date and time of a query cancel operation. Empty is not canceled.
ErrorMsg	An error code associated with this query.
HTTPRequest	A value corresponding to entries in the Application Server logs.
ErrorOffset	Error offset for this record. This is internal information and might be requested by Kinaxis Customer Support.
User Name	The name of the RapidResponse user whose action generated the query request. The user name of the RapidResponse user whose action generated the query request. A user name of RapidResponse indicates the query was run under an internal account used by RapidResponse. For example, this is the account used to run alerts.
Parameters	This is internal information and might be requested by Kinaxis Customer Support.
IdGuid	Internal RapidResponse query identifier expressed a GUID (Globally Unique Identifier).
ScenarioPath	The scenario in which the user generated this query request. The scenario's child-parent relationship path is represented. For example: `Approved Actions\Baseline\DeleteRecords` In this case the scenario is **DeleteRecords** which is child of **Baseline** which is child of **Approved Actions** which is child of the root scenario. Temporary scenarios use the question mark character (?) as the initial character in their name. For example, **?6fc0e16d-1d9a-46a4-ae6d-294c4e27c025**. Temporary scenarios are automatically created while data is being modified (transactions). The changes are stored internally in temporary scenarios in the RapidResponse database. RapidResponse continuously manages these scenarios.

Field	Description
QE3Status	In RapidResponse 2016.2, the internal query execution against the RapidResponse database improved. However, some queries continue to use the query execution methods from RapidResponse 2015.3. This field can hold one of 3 values: • **QE3**—Query was executed using methods introduced in RapidResponse 2016.2. • **QE3::ToDo::*queryName***—Query was executed using RapidResponse 2015.3 methods. The queryName represents internal query identifiers might be requested by Kinaxis Customer Support. • **[*blank*]**—Query was executed against RapidResponse system tables.
QE3PerformanceGainQuotient	For queries executed using the RapidResponse 2016.2 query methods, determines how much of the total execution time was spent calculating results, which indicates the performance benefit of executing the query using the RapidResponse 2016.2 methods. This is calculated by dividing the query's **ExecutionCPUTime** value by its **ExecutionDuration** value.

Notes:

- For information on using Query Manager to view details of current and recently run queries, see "Monitoring and canceling problematic queries " on page 603.
- You can also choose to import **QueryHistory.log** into Microsoft Excel for analysis. If doing so, you should import the file as delimited text, and select **Tab** as the **Delimiter** and **"** as the **Text qualifier**. In some cases, Microsoft Excel might convert date and time data into an unexpected format.

SecurityAudit.log file

The **SecurityAudit.log** file provides information about changes made in RapidResponse that can impact system security. You can use the information reported in this file to monitor the key security controls of your RapidResponse system and to perform security audits. This information is also available in the Security Audit worksheet in the Administration Log workbook. For more information, see "Security Audit worksheet" on page 430.

The **SecurityAudit.log** file provides information about the following types of changes:

- Configuration changes—actions that modify the configuration of your RapidResponse system settings, such as changing a setting in the Global Settings dialog box or in the RapidResponse Administration workbook.
- User changes—actions that modify a user account, such as creating or deleting a user.
- Group changes—actions that modify a group, such as adding a new member to a group.
- Permission changes—actions that modify a level of permission, such as changing settings on the Permissions tab of a User or Group Properties dialog box or granting or denying a user or group access to a resource.
- Dependency changes—actions that modify a dependency of a permission or resource, such as creating a new public resource that depends on other resources.
- Profile variable changes—actions that modify a profile variable, such as creating or deleting a profile variable, or modifying the properties of an existing profile variable.
- Macro changes—actions that modify a macro, such as creating or deleting a macro, or modifying the properties of an existing macro.

The following table describes the fields in the **SecurityAudit.log** file.

Field	Description
DateTime	The date and time the change occurred.
UserName	The name of the user who made the change.
UserIdentity	The GUID (Globally Unique Identifier) of the user who made the change.
Type	The type of change.
Description	A simple description of the change.
Details	A pipe-delimited description that provides more details about the change. For example, this field might include the before and after values of a permission change or the name and identifier of a newly-created user. The details vary depending on the type of change.

The following is an example of a configuration change logged in the **SecurityAudit.log** file. The Alarm - Critical for input data load setting was changed to 40.

```
2016-05-12 09:44:59.3740509 JRAdmin 91d46787-f7a5-11e4-b6d3-005056004e3b
Configuration Database - Alarm - Critical for input data load
AfterValue=40|ConfigurationId=InputMemoryLoadCritical|ConfigurationLocalized
Text=Database - Alarm - Critical for input data
load|ConfigurationType=ProcessingRule
```

The following is an example of a user change. The Administrator with ID "JRAdmin" created a user with ID "jrice".

```
2016-05-12 09:49:31.7242839 JRAdmin 91d46787-f7a5-11e4-b6d3-005056004e3b
CreateUser User created: jrice PrincipleIdentifier=36f2ddb0-f8ad-11e4-9bca-
005056c00008|PrincipleName=jrice|PrincipleType=User
```

The following is an example of a group change. The description of the Buyers group was modified.

```
2016-05-12 10:22:03.441436 JRAdmin 91d46787-f7a5-11e4-b6d3-005056004e3b
ChangeUserGroup Group modified: Buyers AfterValues=Description=This group is
used in the supplier collaboration process. All required predefined resources
have been shared with this group.|IsSystem=N|BeforeValues=Description=This
group is used in the supplier collaboration process.
|IsSystem=N|PrincipleIdentifier=eaa3963f-f8b2-11e4-9bca-
005056c00008|PrincipleName=Buyers|PrincipleType=Group
```

The following is an example of a permission change. The Demand Planners group was given permission to access the Demand Planner dashboard.

```
2016-05-12 10:23:20.0010915 JRAdmin 91d46787-f7a5-11e4-b6d3-005056004e3b
Permission Permission change
AfterValue=View|BeforeValue=None|PrincipleIdentifier=6ea5963f-f8b2-11e4-9bca-
005056c00008|PrincipleName=Demand
Planners|PrincipleType=Group|ResourceIsShared=Y|ResourceName=Demand
Planner|ResourceOwner=Admin|ResourceSecuredObjectId=6bac85a4-7896-4f33-a27a-
774f4278dac8|ResourceSecuredObjectType=Dashboard|ResourceType=Dashboard
```

The following is an example of a dependency change. The Committed Forecast widget is dependent upon the dashboard named Supplier Dashboard.

```
2016-05-12 10:22:46.4327342 JRAdmin 91d46787-f7a5-11e4-b6d3-005056004e3b
PermissionDependency Resource/Scenario dependency change
AfterValue=List|BeforeValue=None|DependentResourceIsShared=Y|DependentResour
ceName=Committed
Forecast|DependentResourceOwner=JRAdmin|DependentResourceSecuredObjectId=321
f986c-de88-42e3-8ebc-
```

```
8f10b857e746|DependentResourceSecuredObjectType=Widget|DependentResourceType
=Widget|ResourceIsShared=Y|ResourceName=Supplier
Dashboard|ResourceOwner=JRAdmin|ResourceSecuredObjectId=bf7e5a7d-47ca-4dd9-
babe-2954f986c982|ResourceSecuredObjectType=Dashboard|ResourceType=Dashboard
```

The following is an example of a profile variable change. The type of the FulfillmentOrderLink profile variable was changed from permanent to temporary.

```
2016-06-09 15:33:37.0036774 tbrennan 6c308517-2e75-11e6-80cf-005056197233
UserVariable UserVariable
Context=RapidResponse|Name=FulfillmentOrderLink|User=Order Fulfillment
changed
AfterValue=Type=Temporary|BeforeValue=Type=Permanent|Context=RapidResponse|N
ame=FulfillmentOrderLink|User=Order Fulfillment
```

The following is an example of a macro change. A macro named IntegrationCheckAnswer was created with the specified expression and parameters.

```
2016-06-09 02:20:34.2370386 Admin 7e137ddc-2dfb-11e6-89a9-0050563f8f45 Macro
Macro Name=IntegrationCheckAnswer added AfterValue=Expression=?
IntegrationCheckAnswerBool( QuestionId, AnswerValue) 1
0|Parameters=QuestionId, AnswerValue|Name=IntegrationCheckAnswer
```

Viewing log data in the Central Log Collector

If you are using the RapidResponse On-Demand service or an On-Premises implementation of RapidResponse with the Performance Monitor Service running, data about your RapidResponse system are collected. For information about what is collected, see "Data collected by the Performance Monitor Service" on page 370.

These data are sent to Kinaxis and archived. Kinaxis retains the archived records for one year.

Selected data from the archived records are extracted and imported into an instance of RapidResponse known as the Central Log Collector (CLC).

Access to the Central Log Collector

Data in the Central Log Collector are available to some Kinaxis employees and administrators of customers' RapidResponse systems.

Kinaxis employee access to the CLC

All data in the Central Log Collector are available to the support team at Kinaxis. They use it to help customers solve technical challenges that arise.

The information is also available to some employees in product development roles. They use it to identify usage trends and identify customers who might be affected by changes to specific RapidResponse features.

RapidResponse administrator access to the CLC

If you are a RapidResponse administrator who is authorized to contact support, you can receive sign in credentials and view information in the Central Log Collector. For security reasons, you are only given

access to information about your company. Authoring and administration permissions on this system are restricted.

Information available from the Central Log Collector

The following reports are available to RapidResponse administrators who can access the Central Log Collector:

- The Health Check dashboard displays metrics related to system performance, including
  - Average duration of netting calculations.
  - Sign-ins.
  - User activity.
  - Data changes.
  - Report usage.
  - Scenarios.
- The Health Check workbook, which supports the Health Check dashboard and includes additional details.

CHAPTER 34: RapidResponse system workbooks reference

Standard system workbooks 482
RapidResponse System Data workbook 486

In addition to the predefined workbooks included with RapidResponse to view data and solve business problems, RapidResponse includes system workbooks. Generally, system workbooks support administration functionality and are not directly opened or accessed from the Explorer pane. Instead system workbooks are opened by clicking a link in the Administration pane.

System workbooks use a yellow key icon to differentiate them from standard workbooks.

For more information about the system workbooks included with RapidResponse, see "Standard system workbooks" on page 482.

Note: System workbooks cannot be exported. In addition, they cannot be included resource packages.

System tables

Most system workbooks are based on system tables. System tables hold information used internally by RapidResponse, such as user information, system settings, or any other information that is not directly used in calculations or imported from an enterprise system. Some of the system tables are described in the *RapidResponse Analytic and Data Model Guide*.

You cannot create or modify system workbooks or worksheets based on system tables, except for presentation attributes such as column widths, sorting, or freezing columns. These settings are not maintained the next time you open the system workbook.

However, you can create and modify resources based on the RapidResponse System Data library workbook. For more information about the RapidResponse System Data workbook, see "RapidResponse System Data workbook" on page 486.

For more information about creating resources based on library workbooks, see the *RapidResponse Resource Authoring Guide*.

Standard system workbooks

The following table lists the system workbooks included with RapidResponse. Also noted are the administrator types that can open the system workbooks from their Explorer pane. For more information about these workbooks, see the workbook help included with the workbooks.

Workbook	Description
Administration Log	RapidResponse logs the execution of RapidResponse commands (usually scheduled system tasks) and some data integration setting changes in this workbook. This information can be very valuable in troubleshooting situations. For example, you might want to review the administration information logs if RapidResponse is not operating normally after a data integration settings change such a customizing the data model. It can be accessed in the **Administration** pane by clicking **Administration Log** under **System Monitoring**. For more information, see" System administration logs" on page 423. **Administrator**: All administrators except user administrators.
Application Settings	Use this workbook to configure RapidResponse application-specific settings to better meet the need of RapidResponse users. Each worksheet provides different configuration points such as Application Variables, Historical KPI Data, Supplier Collaboration, and Supplier ID Reference. This workbook can be accessed in the **Administration** pane by clicking **Application Settings** under **System Settings**. For more information, see "Application configuration and settings" on page 777 and the "Restricting data for suppliers" section of "Adding a new supplier and users" on page 825. **Administrator**: All administrators.
Automation Details and Log	This workbook provides RapidResponse users a view to detailed information about their automated processes such as alerts, tasks, and scripts. This workbook displays many details including run status, successes, and failures. This workbook can be accessed by clicking **Alert Details and Log** on the **View** menu. For more information, see the *RapidResponse User Guide*. **Administrator**: All administrators.
Automation Log	RapidResponse administrators use this workbook to view detailed information about automated processes such as alerts, tasks, and scripts. This workbook logs many details including run status, successes, and failures. This information is presented in worksheets, which you can sort and search to view only the information relevant to you. In addition, you can specify how much history to display in the worksheets. For example, you can view only alerts and tasks that have run on the current date, the past three days, or the past month. This workbook can be accessed in the **Administration** pane by clicking **Automation Log** under **System Monitoring**. For more information, see "Automation logging" on page 448. **Administrator**: All administrators.
Business Message Definition	Reports all business message definitions, as well as all sources, targets, message types, and data formats required to send and receive business messages using the Real-time Integration Service. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: System and data administrators.
Business Message Log	Reports all business messages that have been received by or sent from the Real-time Integration Service. You can use this information to locate messages that have expired or failed, and to trace a transaction's audit trail. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: System and data administrators.

Workbook	Description
Collaborations	Used to track all open and archived collaborations in the system. The only location where collaborations can be permanently deleted from the system is from this workbook. The scenarios and resources used in the collaboration are not deleted when the collaboration is deleted. To keep the list of collaborations in your system manageable, it is recommended that you regularly delete empty collaborations or unneeded archived collaborations from the Collaborations workbook. **Administrator**: System and user administrators.
Control Sets	Used to define control sets and the control table values contained within each. Each control set, and its control table values, define how analytic calculations are performed for all sites that use that control set. This workbook can be accessed in the **Administration** pane by clicking **Control Sets** under **Data**. **Administrator**: System and data administrators.
Data Extract Log	Provides status information about data extracted from RapidResponse. You can use this information to view when extracts were performed, whether full or net change data was extracted, which tables data was extracted from, and how many records were extracted. This information is most relevant for a data integration server that extracts data to send to a planning server. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: System and data administrators.
Data Import and Update Log	Provides status information on RapidResponse data imports and updates (for example, did a data update complete successfully or did it fail?), and also shows informational and error messages generated by RapidResponse Server during a data update. Additionally, this workbook shows statistics about the data extract files and RapidResponse Input tables used in a data update (for example, how many successful insertions were made to a given table during the Update). When a data update fails a tolerance test, this workbook provides functionality to either manually commit or cancel the pending data update. It can be accessed in the **Administration** pane by clicking **Data Import and Update Log** under **System Monitoring**. For more information, see "Data import and data update logs" on page 442. **Administrator**: All administrators except user administrators.
Data Model Overview	This workbook provides RapidResponse administrators a table view of the Namespaces, Tables, ad Fields in RapidResponse. The workbook and worksheets will show Kinaxis and custom Namespaces, Tables, and Fields. Administrators can filter the different worksheets to show only certain Namespaces and Tables.
Data Origin	Used to determine the origin of records in the RapidResponse database. It can be accessed in the **Administration** pane by clicking **Data Origin** under **Data**. **Administrator**: System and data administrators.
Data Persistence Rules	Used to define persistence rules that indicate the data to be persisted in a specific scenario during a data import. It can be accessed in the **Administration** pane by clicking **Data Persistence Rules** under **Data**. **Administrator**: System and data administrators.
Data Tolerance and Error Settings	Used to set the tolerance settings used to determine the conditions under which a data update should fail. When this happens, this workbook also provides functionality to either manually commit or cancel the pending data update. It can be accessed in the **Administration** pane by clicking **Tolerance and Error Settings** under **Data Integration**. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: All administrators except user administrators.

Workbook	Description
Duplicate Actual Conversion Rates	Used to delete duplicate currency conversion rates, and to ensure only one rate is available for performing conversions. For more information, see "Deleting duplicate actual conversion rates" on page 693. **Administrator**: All administrators.
Macros and Profile Variables	Used by workbook authors to create macros and profile variables used in workbook definitions. It can also be used by administrators to define profile variables for users. It can be accessed in the **Administration** pane by clicking **User Profile Variables** under **User Accounts**. Authors can access it from the **View** menu. **Administrator**: All administrators.
Perspectives	Administrators use this workbook to apply a preconfigured set of control table settings to a scenario without having to change them manually. It can be accessed in the **Administration** pane by clicking **Perspectives** under **Data**. **Administrator**: All administrators except user administrators.
Process Instances	This system workbook can be accessed from the **Process Activities** workbook. Used to view information about existing processes. Also allows you to delete a process instance. **Administrator**: All administrators.
Query Manager	Administrators use this workbook to cancel queries that are taking an unusually long time. It can be accessed in the **Administration** pane by clicking **Query Manager** under **System Monitoring**. **Administrator**: All administrators except data administrators.
RapidResponse Administration	Administrators use this workbook to configure and review RapidResponse settings and functions. **Administrator**: System administrators.
RapidResponse Scenario Changes	Shows the details of user-initiated changes (inserted, modified, or deleted records) in scenarios. It does not include details of changes or differences in scenarios resulting from data update operations or made by custom applications. The worksheets in this workbook are used as tabs in the Scenario properties windows. Typically this workbook is not opened directly. This workbook track the differences between the selected scenario and its parent scenario. For example, if you are trying to commit changes into the parent and the current scenario is now out of date with it, it shows the details of the changes made in the parent. **Administrator**: System administrators.
RapidResponse System Data	This workbook is a library system workbook. It contains worksheets that display data from various system tables. For example, worksheets in this workbook show system data such as scenario information, query history, data import and update logs, server operations and logs, user and group membership details, user resource and permission details, group resource and permission details, user sign-in information, and resource usage details. The raw worksheets in this workbook can be used by system administrators to build their own workbooks reporting details of system data as they best see fit. For example, formatting can be applied, columns can be moved or removed, and worksheet views can be joined in composites. The workbooks that system administrators create based on the data views provided in this workbook can then be shared to other users, both administrators or non-administrators. Note that the data presented in this workbook is not editable, and is provided only to allow creating custom views into your organization's system data. For more information, see the "RapidResponse System Data workbook" on page 486 **Administrator**: System administrators.

Workbook	Description
RapidResponse User Administration	Contains the groups and users information. Do not modify or delete this workbook. For more information, see " Managing users" on page 569. **Administrator**: System administrators.
Real-time Message Log	Reports all messages that have been received by or sent from the Real-time Integration Platform. You can use this information to locate messages that have failed, and to trace a transaction's audit trail. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: System and data administrators.
Real-time Integration Service Endpoints	Used to specify endpoints for Real-time Integration Service application hosts. Application hosts can be servers within your company or external host systems, and must have a Real-time Integration Service adapter instance installed on it. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: System and data administrators.
Real-time Integration Service Status	Used view the status of application hosts and the applications that run on them. Applications are included here if the host's endpoint has been specified and that host's status reporting flow can connect to the Real-time Integration Service. For more information, see the *RapidResponse Data Integration Guide*. **Administrator**: System and data administrators.
Resources	Administrators can use this workbook to monitor how often resources such as workbooks and filters are used. This workbook can be accessed in the **Administration** pane by clicking **Resources** under **System Monitoring**. For more information, see "Monitoring resource usage" on page 746. **Administrator**: All administrators.
Resource Permissions	Administrators use this workbook to review resources assigned to users, and to review all users who have access to a particular resource. You can review resource assignments to audit the resources and access permissions for groups. This workbook can be accessed in the **Administration** pane by clicking **Resource Permissions** under **User Accounts**. For more information, see "Reviewing resource assignments" on page 575. **Administrator**: All administrators.
Scenarios	Administrators can use this workbook to monitor scenarios and view the scenario structure. You can find information including when scenarios were last used or updated. Administrators with the Manage all scenarios permission can delete scenarios or toggle the permanent status of scenarios. This workbook can be accessed in the **Administration** pane by clicking **Scenarios** under **System Monitoring**. For more information, see "Administrator tools for scenario management" on page 708.
Scheduled System Tasks	Administrators use this workbook to run a RapidResponse scheduled task on demand or modify the settings of a scheduled task. This workbook can be accessed in the **Administration** pane by clicking **Scheduled System Tasks** under **System Settings**. For more information, see "Commands and scheduling system tasks" on page 381. **Administrator**: All administrators except user administrators.
Server Resource Monitoring	Administrators use this workbook to understand the input data memory load and CPU usage on the RapidResponse Server computer. For more information, see "Monitoring input data growth" on page 263 and "Monitoring CPU usage" on page 271. **Administrator**: System administrators.

Workbook	Description
Sign-in Log	Lists failed and successful RapidResponse sign-in attempts. The records displayed in this workbook are deleted after a specified period of time. To determine how long records remain visible in this workbook, click the Settings button on the workbook toolbar. You can also review the sign-in attempts that failed due to a user ID error by clicking the Invalid User ID Count button on the workbook toolbar. This workbook can be accessed in the **Administration** pane by clicking **Sign-in Log** under **System Monitoring**. **Administrator**: All administrators except data administrators.
Sites	Administrators can use this workbook to add and manage sites. This workbook can be accessed in the **Administration** pane by clicking **Sites** under **Data**. **Administrator**: System and data administrators.
Tags	Use this workbook to create or delete global resource tags. You can also see how many resources each tag is applied to. This workbook can be accessed in the Administration pane by clicking **Tags** under **System Settings**. **Administrator**: All administrators.
Update Conversion Rates	Contains commands that copy currency conversion rates from one scenario to another. This workbook is intended only to be used by the **Update Conversion Rates** script. For more information, see "Updating conversion rates in scenarios" on page 691. **Administrator**: All administrators.

For information about the different administrator types, see "RapidResponse administration roles" on page 33.

RapidResponse System Data workbook

RapidResponse includes a number of system workbooks, which are accessed by clicking a link in the Administration pane. These workbooks are not accessible to non-administrator users and are not modifiable. To work with the data that is shown in system workbooks, a new resource can be created using the RapidResponse System Data workbook.

The RapidResponse System Data workbook is a system library workbook that displays raw data from various system tables. The system data presented in this workbook is not editable, and is provided only to allow system administrators to create new workbooks that report details of system data as required. For example, formatting can be applied, columns can be moved or removed, and filters can be added. The workbooks that system administrators create based on the system data provided in this workbook can then be shared to other users, both administrators or non-administrators.

For example, the Data Import and Update Log is not accessible to non-administrator users. However, a system administrator can create a new workbook with a composite worksheet based on the Data Import and Update worksheets provided in the RapidResponse System Data workbook. The system administrator can then share this new workbook with a non-administrator user who has authoring permissions. The non-administrator user who has authoring permissions can then create more resources based on the new workbook.

For more information about using worksheets from a library workbook, see the *RapidResponse Resource Authoring Guide*.

Note: Because the worksheets in library workbooks are often used in composite worksheets, you should be familiar with the different methods of merging records in composite worksheets. For more information, see "Understand how component worksheets are combined" in the *RapidResponse Resource Authoring Guide*.

System tables

The following table describes the worksheets in the RapidResponse System Data workbook and identifies the system table that the worksheet is based on.

Worksheet name	System table	Description
• Scenarios • Scenarios - Hierarchical	Plan	Shows information about the scenarios being used on the RapidResponse system.
Users	User	Shows information about all of the user accounts in your system.
Groups	GroupProfile	Shows information about all of the user groups in your system.
• Users - Group Memberships • Group Members	GroupMember	Shows group membership details for users and groups. **Note**: Added in Version 2016.2 Service Update 14.
• User Resources • User Permissions • Group Resources • Group Permissions	Note that these worksheets are composites and therefore are based on more than one system table. • User Resources worksheet and Group Resources worksheet: User table + system tables for each resource type • User Permissions worksheet and Group Permissions worksheet: User table + Capability table	Shows resources and permissions for users and groups. **Note**: Added in Version 2016.2 Service Update 14.
Automation Task Log	AlertActivity	Provides information about automated operations that have run in the RapidResponse system, including alerts, scheduled tasks, and automation chains.
Workbook Command Log	DataChangeCommandSummary	Provides summary information about data change actions made by workbook commands and scheduled tasks.

Worksheet name	System table	Description
Data Modification Details	DataChangeActionSummary	Provides detailed information about the results of each data change action made by workbook commands and scheduled tasks.
Data Modification Error Details	DataChangeErrorDetail	Provides detailed information about errors that occurred during each data change action made by workbook commands and scheduled tasks.
• Script Log • Web Services Log • Change Data Capture Log • Mobile Log	ApplicationLog	Provides information about automated operations that have run in the RapidResponse system, including scripts, web service calls, Change Data Capture (CDC) activities, and mobile scripts.
Data Extract Log Summary	GenExHistory	Provides information about each ExtractData and ExtractNetChangeData command that has run in the RapidResponse system. This includes how long the command ran, the extract definition that was used, the number of tables that were extracted, and the arguments that were passed to the command.
Data Extract Log Details	GenExTableHistory	Provides information about the data files created by running an ExtractData or ExtractNetChangeData command. This includes the file names, the tables that were extracted, the types of records included in the data files, and the number of records included in each file.
Data Import and Update Errors and Warnings	DataUpdateMessage	Reports detailed messages, of varying levels of severity, associated with data imports and data updates.
• Data Import and Update File Summary • Data Import and Update Record Counts By File	DataUpdateFileHistory	Provides details of data extract files (text or Microsoft Excel) used in a data import or data update.
Data Import and Update Record Counts By Table	DataUpdateTableHistory	Reports the number of successful and failed data import and data update operations (insertions, modifications, and deletions) that occurred in each input table.
Data Import and Update Related Deletions	DataUpdateCascadeDeletions	Reports summary information for cases where a deletion in one table causes the deletion of records in a dependent table.
Data Import and Update Summary	DataUpdateHistory	Reports a summary of each data import or data update, including the times, status of the operation, number of records in the table before and after the operation, and records inserted, modified, deleted, or rejected by the operation.

Worksheet name	System table	Description
Data Import and Update Extracts	DataUpdateExtractHistory	Reports the Extract folders associated with each data source for each data update.
Recent Query History	QueryHistory	Provides information about the last 5,000 queries in the RapidResponse system.
• Server Input Data Memory Load • Server CPU Usage	PerformanceHistory	Provides information about the RapidResponse server such as its input data memory load and CPU usage.
Server Operations Log	AdministrationLog	Provides detailed information about the execution of RapidResponse system commands. For more information about these commands, see "RapidResponse system commands" on page 384.
Server Command Messages	CommandHistoryMessage	Provides details about the log messages associated with the execution of RapidResponse system commands. For more information about these commands, see "RapidResponse system commands" on page 384.
• History Log - Input Records • History Log - Scenarios	UsageMetrics	Shows metrics about RapidResponse system memory usage such as the number of input records in data tables in the root scenario, and the number of scenarios in your RapidResponse system.
• Sign-in Log - Successes • Sign-in Log - Failures	Logon	Shows information about sign-in activity in RapidResponse such as successful sign-ins, unsuccessful sign-ins, and the reason why the sign-in failed.
• Alerts • Automation Chains • Scheduled Tasks	AutomationTask	Shows details about all automated resources (alerts, automation chains, and scheduled tasks) that are defined in your system. **Note**: Added in Version 2016.2 Service Update 14.
Dashboards	Dashboard	Shows details about all of the dashboards in your system, including a count of how many times, from a specified date, a dashboard has been used. **Note**: Added in Version 2016.2 Service Update 14.

Worksheet name	System table	Description
Filters	Filter	Shows details about all of the standard filters in your system, including a count of how many times, from a specified date, a standard filter has been used. You cannot view site filter details in this worksheet. **Note**: Added in Version 2016.2 Service Update 14.
• Forms • Hierarchies • Processes • Scorecards • Scripts • Task Flows	Resource (System)	Shows details about all of the forms, hierarchies, processes, scorecards, scripts, and task flows in your system, including a count of how many times, from a specified date, the resource has been used. **Note**: Added in Version 2016.2 Service Update 14.
Responsibilities	ResponsibilityRole	Shows details about all of the responsibilities in your system, including a count of how many times, from a specified date, a responsibility has been used. **Note**: Added in Version 2016.2 Service Update 14.
Site Filters	SiteGroup	Shows details about all of the site filters in your system, including whether a site is public or private, who the site owner is, and date specific information. **Note**: Added in Version 2016.2 Service Update 14.
Widgets	Widget	Shows details about all of the widgets in your system, including a count of how many times, from a specified date, a widget has been used. **Note**: Added in Version 2016.2 Service Update 14.
Workbooks	Workbook	Shows details about all of the workbooks in your system, including a count of how many times, from a specified date, a workbook has been used, which table the workbook filter is compatible with, and whether the workbook allows for data import or data update operations. **Note**: Added in Version 2016.2 Service Update 14.

For more information about a worksheet, see the RapidResponse System Data workbook help.

Part 6: User administration

- "Best practices for setting up user accounts" on page 493
- "Guidelines for group setup and user experiences" on page 503
- "Creating groups" on page 513
- "Creating user accounts" on page 539
- "Managing groups and users" on page 565
- "Reviewing resource assignments" on page 575
- "User account maintenance and troubleshooting " on page 593

CHAPTER 35: Best practices for setting up user accounts

About predefined groups 493
Predefined user groups 494

RapidResponse user administrators are responsible for creating user accounts for every RapidResponse user. Administrators also control the permissions and resource access RapidResponse users are granted. By controlling the resources users are assigned, you can control the data users have access to.

Permissions control the tasks that RapidResponse users can perform. The tasks users can perform within RapidResponse vary from viewing data to creating scenarios that simulate a business situation, to administering various aspects of RapidResponse.

Providing access to only the resources the user requires helps to ensure data security. For example, a customer service representative does not have access to workbooks that show financial information.

A company that deploys RapidResponse can typically have a large number of users performing a variety of roles within the company, and each role likely requires access to specific types of information and permissions. For example, customer service representatives solving supply chain management (SCM) problems need access to order information and the ability to simulate the effect of an order change on existing orders. However, a demand planner working on the S&OP process requires access to different resources and, possibly, a different set of user permissions.

The recommended method of providing users with the permissions and resource access to perform specific tasks is by organizing the users into groups that represent the roles in your company. Each group has a set of permissions and resource access associated with it, which determine what group members are allowed to see and use.

About predefined groups

By using groups, you can grant the same RapidResponse permissions and resource access to multiple users simultaneously. It is recommended that you grant permissions to users by placing them in groups that have the desired permissions and access to required resources.

RapidResponse includes groups designed to help you organize users according to their roles in a typical organization. You can use this group structure as-is, modify it to meet your requirements, or create custom groups. Each group has an administrator designated as its owner. This administrator is responsible for adding and removing users to and from the group.

The predefined RapidResponse groups support supply chain manufacturing (SCM), sales and operations planning users (S&OP), and project management.

The SCM groups are based on the typical functions and tasks performed within manufacturing companies. These predefined groups can be used as is. However, they are most often used as a template to create custom groups to support a company's specific SCM process.

The S&OP groups support a specific RapidResponse process to solve business problems. Users working with the S&OP process should be added to predefined S&OP groups.

The project manager groups are based on the typical functions and tasks performed by project managers. These predefined groups can be used as is. However, they are most often used as a template to create custom groups to support a company's specific project management process.

Predefined user groups

This section provides a summary of the resources and permissions provided to the predefined RapidResponse user groups.

The predefined groups can be divided into the following types:

- "Supply Change Management (SCM) groups" on page 494
- "Sales and Operations Planning (S&OP) groups" on page 498
- "Project manager groups" on page 499
- "Supplier collaboration groups" on page 500
- "Administrator groups" on page 501

Supply Change Management (SCM) groups

This section describes the SCM groups available with RapidResponse.

- "Auto-Publish Running Plan group" on page 495
- "Business Analysts group" on page 495
- "Capacity Manager group" on page 495
- "Constraint Manager group" on page 495
- "Customer Order Managers group" on page 495
- "Customers group" on page 496
- "Demand Managers group" on page 496
- "Engineering Change Manager group" on page 496
- "Global Supply Planners" on page 496
- "Inventory Managers group" on page 496
- "Kanban Manager Analysts group" on page 496
- "Kanban Manager Viewers group" on page 497
- "Manufacturing Engineers group" on page 497
- "Master Schedulers group" on page 497
- "Material Planners group" on page 497
- "Multi-Enterprise Managers group" on page 497
- "Operations Managers group" on page 497
- "Order Fulfillment group" on page 497

- "Production Planners group" on page 497
- "Risk/Opportunity Analysts group" on page 498

To give users access to resources, you can add them into these groups, or you can use these groups as templates when creating groups. This section outlines the groups included with RapidResponse, and the resources assigned to each group.

Auto-Publish Running Plan group

This group, and the Running Plan scenario, are available only to users who have upgraded from RapidResponse 9.1 and earlier.

The Running Plan scenario is automatically shared with this group. During every data update, the Running Plan scenario is updated with the latest version of your enterprise data. You should add anyone who requires access to the Running Plan scenario to this group.

Users in this group, who have simulation permissions, can commit changes in child scenarios into the Running Plan scenario. For more information, see "Assigning scenarios" on page 533.

Business Analysts group

Users in this group are typically responsible for monitoring and analyzing business performance against defined targets. They also analyze product standard costs and gross margins. The following table outlines the resources available to this group.

Capacity Manager group

Available only if your company has enabled the Capacity Manager. Users added to this group get all of the Capacity Manager resources.

Constraint Manager group

Users added to this group get all of the Constraint Manager application resources.

Note: Installations of RapidResponse 2014.2 (and later) do not include this user group. This predefined user group is included if your company has ever upgraded from RapidResponse 2014.1 (or earlier).

Customer Order Managers group

Users in this group are responsible for entering and maintaining order information and providing updates on order status to customers. They need to know when customers can expect to receive the products they order so they can manage customer expectations. The following table outlines the resources available to this group.

Note: Installations of RapidResponse 2014.2 (and later) do not include this user group. This predefined user group is included if your company has ever upgraded from RapidResponse 2014.1 (or earlier).

Customers group

Users in this group typically want up-to-the-minute information on order status. The following table outlines the resources available to this group.

Caution: Do not provide additional permissions to this group. Doing so might result in inadvertent data exposure.

Note: Installations of RapidResponse 2014.2 (and later) do not include this user group. This predefined user group is included if your company has ever upgraded from RapidResponse 2014.1 (or earlier).

Demand Managers group

Users in this group are responsible for creating, maintaining, allocating supplies to, and managing supply consumption by forecasts. In addition, Demand Managers might be expected to work with order fulfillment, management, or financial departments to determine the best orders to fill.

Engineering Change Manager group

Available only if your company has enabled the Engineering Change Manager. Users added to this group get all of the Engineering Change Manager resources.

Global Supply Planners

Users in this group are responsible for developing and evaluating the supply plan for a product family over an extended planning horizon, for example, 12 to 24 months.

Inventory Managers group

Users in this group are responsible for defining inventory policies that minimize inventory levels while achieving desired levels of customer service. They often lead inventory reduction initiatives and monitor inventory policy compliance.

Kanban Manager Analysts group

Users in this group have full access to the Kanban Manager workbook for use with a kanban material replenishment system. They can view data pertaining to shop and source kanbans, and can also create kanban scenarios and run kanban analysis to calculate new recommended bin sizes and quantities. You should ensure that members of this group are also given permission to share scenarios to allow sharing with other members of this group or with members of the Kanban Manager Viewers group.

Note: Installations of RapidResponse 2014.2 (and later) do not include this user group. This predefined user group is included if your company has ever upgraded from RapidResponse 2014.1 (or earlier).

Kanban Manager Viewers group

Users in this group have access to the Kanban Manager workbook for use with a Kanban Manager material replenishment system. They can view data pertaining to shop and source kanbans, but cannot create kanban scenarios or run kanban analysis.

Note: Installations of RapidResponse 2014.2 (and later) do not include this user group. This predefined user group is included if your company has ever upgraded from RapidResponse 2014.1 (or earlier).

Manufacturing Engineers group

Users in this group are responsible for the production bill of materials (BOM). A key challenge for them is to keep all product information current and accurate. They work with Product Engineering around the timing of product changes such as new product introductions, engineering change orders, and product phase-outs.

Master Schedulers group

The users in this group manage the master production schedule (MPS) for end items to meet expected demand. They strive to maximize customer service and minimize inventory while respecting material and capacity limitations.

Material Planners group

Users in this group strive to ensure that the material supplies required to support the master production schedule are available at the right time. They work with Master Schedulers, Production Planners and Buyers to align supply with demand by actioning expedite, cancel, and delay messages.

Multi-Enterprise Managers group

The users in this group manage supply from subsidiary manufacturing facilities, particularly outsourced manufacturing.

Operations Managers group

The users in this group focus on supply chain management, production, and procurement. These users are responsible for meeting business objectives through effective and efficient operations.

Order Fulfillment group

Users in this group are responsible for entering customer orders into RapidResponse, ensuring the orders are satisfied on time, and communicating with the customer if an order cannot be fulfilled on time.

Production Planners group

The users in this group utilize available material and capacity to create an achievable, level-loaded production schedule that maximizes on time delivery. They also work with Material Planners, Buyers, and Master Schedulers to clear production orders that do not have needed materials for release.

Risk/Opportunity Analysts group

Users in this group review financial impact in key areas of risk and opportunity, and gain access to enough detailed information to take action.

Sales and Operations Planning (S&OP) groups

This section describes the S&OP groups available with RapidResponse. The groups are integrated with the RapidResponse processes and the permissions should not be modified.

- "Demand Planners group" on page 498
- "Engineering group" on page 498
- "Executives group" on page 498
- "Finance group" on page 498
- "Marketing group" on page 498
- "Operations group" on page 498
- "S&OP Process Owners group" on page 499
- "S&OP Team" on page 499
- "Sales group" on page 499

Demand Planners group

Users in this group review the consensus forecast and the demand plan.

Engineering group

Users in this group work with the Operations group to provide information about new product introduction, product end of life, and engineering changes required to support the S&OP plan. This group also ensures that production is available to meet the supply plan.

Executives group

Users in this group provide executive sign-off on the S&OP plan.

Finance group

Users in this group provide compare each group's supply or demand plan to the S&OP plan to ensure the plan is feasible.

Marketing group

Users in this group provide data used in calculating statistical forecasts, and provide marketing forecasts for the S&OP plan.

Operations group

Users in this group provide product planning and scheduling information, including production planning, scheduling, and distribution.

S&OP Process Owners group

Users in this group start the S&OP process or an S&OP sub-process and publish the updated plan at the end of a cycle.

S&OP Team

This group contains all the other S&OP groups. It is recommended that this group not be modified in any way or that users be added directly to this group. Users should be added to a specific S&OP user group.

Sales group

Users in this group provide actual sales data and sales forecasts for the S&OP plan.

Project manager groups

- This section describes the project manager groups available with RapidResponse.
- "Field Managers group" on page 499
- "Project Managers group" on page 499
- "Resource Managers group" on page 499

Field Managers group

Users in this group generally work on location of a major project, for example, construction of a new building or aircraft. The field manager updates the project plan information on a daily basis as work on the project activities is completed.

Note: Installations of RapidResponse 2014.2 (and later) do not include this user group. This predefined user group is included if your company has ever upgraded from RapidResponse 2014.1 (or earlier).

Project Managers group

Users in this group to create and manage projects and monitor project statuses.

Resource Managers group

Users in this group often works in conjunction with the project manager and are responsible for managing the information about the resources that are available to work on the projects. They might also update information about the number of hours resources actually work on certain tasks in a project.

Supplier collaboration groups

This section describes the supplier collaboration groups available with RapidResponse. The groups are integrated with the RapidResponse process and should not be modified. This section also highlights the resources and permissions available to each group.

- "Buyers group" on page 500
- "Suppliers group " on page 500
- "Suppliers - [Template] group " on page 500

Buyers group

This group is used in the supplier collaboration process. Predefined resources have been shared with this group and it has been assigned permissions related to the process.

This group requires access to the Supplier Collaboration scenario with the Modify permission.

For more information about the process, see the *RapidResponse Applications Guide*. For more information about the buyer role, see the *RapidResponse Resource Authoring Guide*.

Suppliers group

This group is used in the supplier collaboration process, and provides the required resources and permissions to supplier users. Do not directly add supplier users to this group.

To ensure that each supplier sees only their own order and forecast data, it is recommended that you create a subgroup for each supplier company by duplicating the **Suppliers - [Template]** group, and include the supplier's users in that subgroup.

Consider the following naming convention for the supplier subgroups to aid in sorting:

- Suppliers - Company Name 1
- Suppliers - Company Name 2
- Suppliers - Company Name 3

A supplier collaboration profile variable is required for each supplier subgroup to ensure that each supplier is provided with only their own order and forecast data. This group requires access to the Supplier Collaboration scenario with the Modify permission.

For more information about the process, see the *RapidResponse Applications Guide*. For more information about the supplier role, see the *RapidResponse Resource Authoring Guide*.

Caution: Do not provide additional permissions to this group. Doing so might result in inadvertent data exposure.

Suppliers - [Template] group

Duplicate this group to create a group for each supplier participating in the supplier collaboration process, to ensure that each supplier is provided with only their own order and forecast data. These individual supplier groups are all members of the Suppliers group from which resources and permissions are inherited. Recommendations when duplicating this group:

- **Group Name**—Suppliers - Company Name
- **Members**—The supplier users for a single supplier company.
- Do not adjust the resources or permissions except to perhaps add site access.

After creating a supplier subgroup for a company, create a supplier collaboration profile variable.

For more information about the process, see the *RapidResponse Applications Guide*. For more information about the supplier role, see the *RapidResponse Resource Authoring Guide*.

Administrator groups

RapidResponse includes three predefined administration groups.

- System Administrators
- User Administrators
- Data Administrators

To give users administrator permissions and capabilities, you can add them into these groups, or you can use these groups as templates to create your own administrative groups with different permissions. All administrators have access to every RapidResponse resource.

For more information about administrators and assigning administration permissions, see "RapidResponse administration roles" on page 33.

CHAPTER 36: Guidelines for group setup and user experiences

Guidelines for initial custom group setup **503**
User experiences **504**
Planning the group structure **510**

As discussed in "Best practices for setting up user accounts" on page 493, RapidResponse includes predefined user groups designed to help you organize users according to their roles in a typical organization. You can use this group structure as-is, modify it to meet your requirements, or create custom groups.

This chapter explains the concept of groups in RapidResponse and takes you through the best practices of setting up custom groups and a user structure. Ensure to review this information before creating user accounts and groups for employees in your company.

As discussed in the previous chapter, S&OP users should be added to predefined S&OP groups. The S&OP groups support a specific RapidResponse process to solve business problems.

The SCM groups are based on the typical functions and tasks performed within manufacturing companies. These predefined groups can be used as is. However, they are most often used as a template to create custom groups to support a company's specific SCM process.

Before creating custom groups or modifying the groups included with RapidResponse, you must plan your group structure. You also must decide how groups represent the roles within your company, and decide the resources and permissions each group requires. For more information, see "Best practices for setting up user accounts" on page 493.

Guidelines for initial custom group setup

It is recommended that you implement the following guidelines in the order they are presented:

1. Evaluate the requirements of potential users. Consider the role they play in your company and the tasks they might have to perform. For more information, see "User experiences" on page 504.
2. Plan the group hierarchy. Groups can inherit resources and permissions from other groups. You can create groups with common permissions, such as viewing information or having access to the Approved Actions scenario, and then create groups with more specific requirements, such as viewing workbook properties or authoring task flows. The groups with specific requirements can be added to the groups with common requirements to create a hierarchy. For more information, see "Planning the group structure" on page 510.

RapidResponse includes groups based on typical functional groups within companies. You can add users to these groups or use them as a basis for creating groups of users with the same job function in different locations. For example, you could use the included Buyers group to create Buyers-NA and Buyers-Asia groups for all buyers based in North America and Asia respectively. For information about the permissions and resources available to these groups, see "Predefined user groups" on page 494.

3. If required, create the groups you planned in your hierarchy and grant them appropriate RapidResponse permissions and access to resources such as workbooks, scorecards, or filters. For more information, see "Creating a group" on page 513.

   Each group must have access either to the Approved Actions scenario or one other permanent scenario that is configured to be updated with the latest enterprise data during a data update. For more information, see "Assigning scenarios" on page 533.
4. Although you can add groups to other groups so that permissions can be inherited, it is recommended that you keep the group hierarchy shallow to avoid complex inherited permissions that might become difficult to track.
5. Create user accounts. Add each user to the appropriate group or groups. For more information, see "Creating user accounts" on page 539.
6. Be consistent in how you specify user names—all user names should be defined using the first name first and the last name last or vice versa. This helps users search for user names when they are sharing resources.
7. Avoid placing a user into too many groups. It can be difficult to track the permissions granted to such users.

Note: Although these guidelines recommend creating groups, then users, and assigning group memberships to users as you create them, you can create the users first, and then add the users to groups as you create them if this approach is preferred.

User experiences

Depending on the resources and permissions you provide, different users can experience RapidResponse in different ways. For example, when a user has access to only one report and does not have permission to create other resources, that report opens automatically after sign in, and some menu options, such as New Resource, are not available. A user with access to many resources and permission to create new resources, on the other hand, sees many resources listed in the Explorer and has more options available on the toolbar, and therefore has a more complex user experience.

The experiences shown below are examples only. Typically, you should give more capabilities to more experienced users, and provide a simplified experience for new users or external users who sign in to your RapidResponse system, such as customers or suppliers.

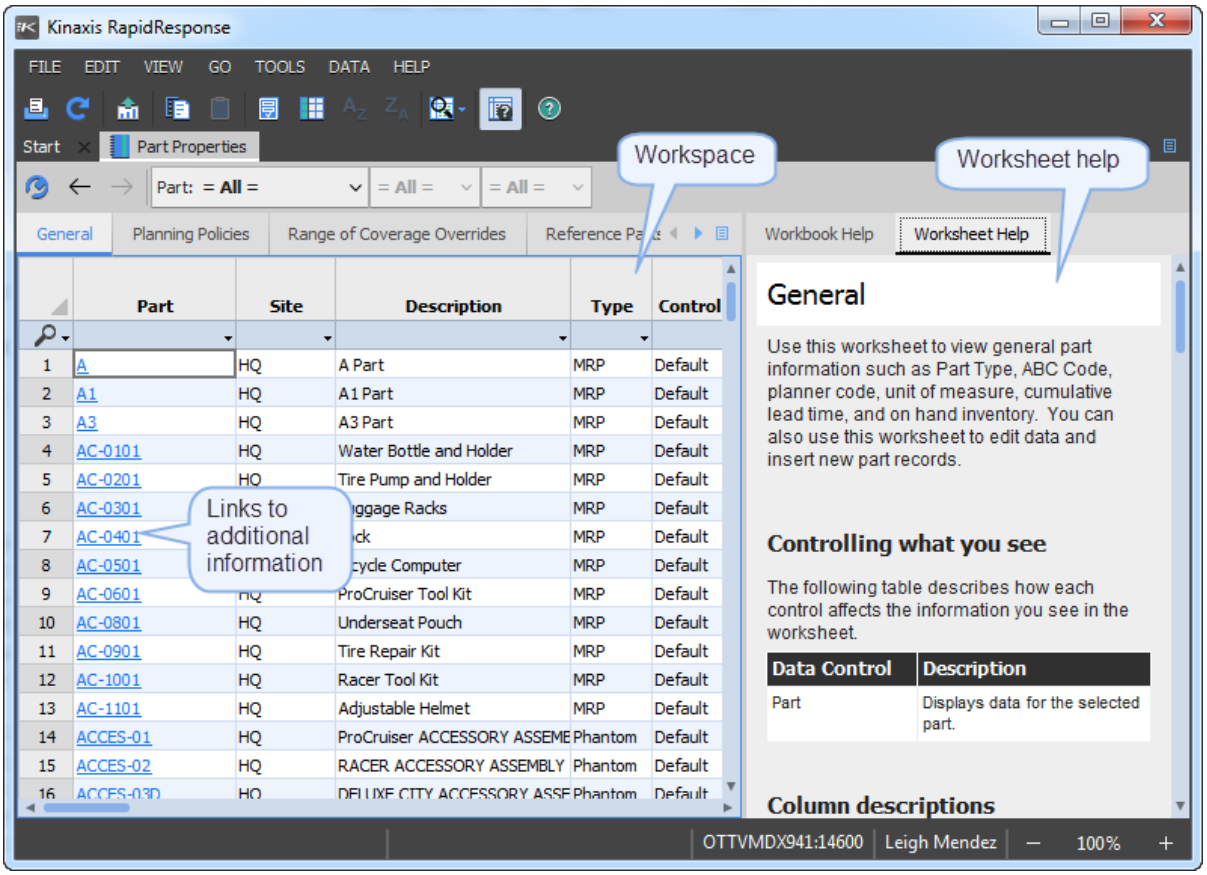
User experiences can belong to one of the following broad categories.

- **Consumer**—users can view some data from their company's enterprise data systems and might be able to monitor data by creating personal alerts.
- **Contributor**—users can view and modify data in one or more scenarios that have been shared with them.
- **Simulation/Collaboration**—users can create what-if scenarios to simulate business problems. They might also be able to collaborate on solutions with other RapidResponse users.
- **Resource Author**—users can create a variety of RapidResponse resources.

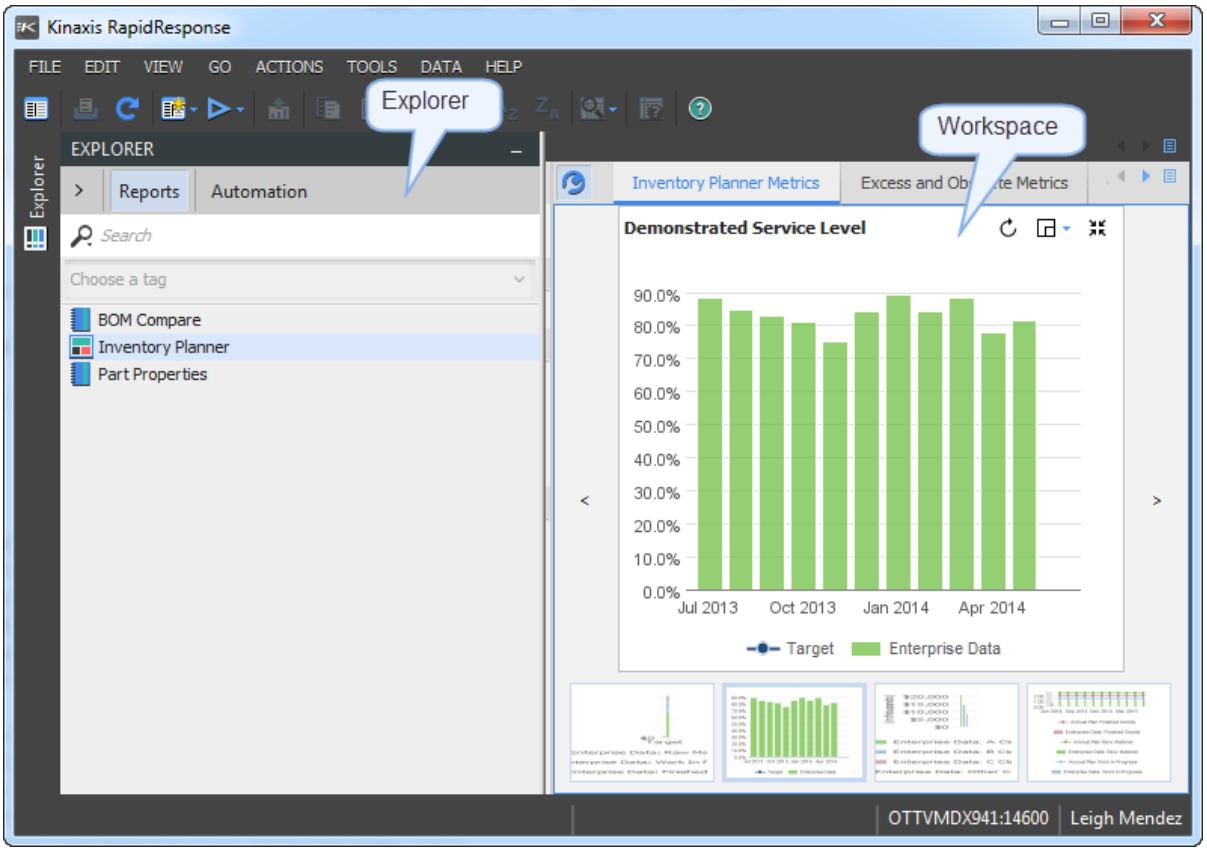
For more information about the permissions and resources you can assign to a user or group, see "Creating groups" on page 513.

Consumers

Consumers could include managers and financial analysts. They typically view data in reports created for them. Upon signing in to RapidResponse, consumers might be presented with reports that display data related to their job functions, and includes links to detailed information, as in the following illustration.



Consumers might also have access to multiple reports, which they can open from the Explorer. They might also be able to create personal alerts that monitor data and send notifications when the monitored data changes.



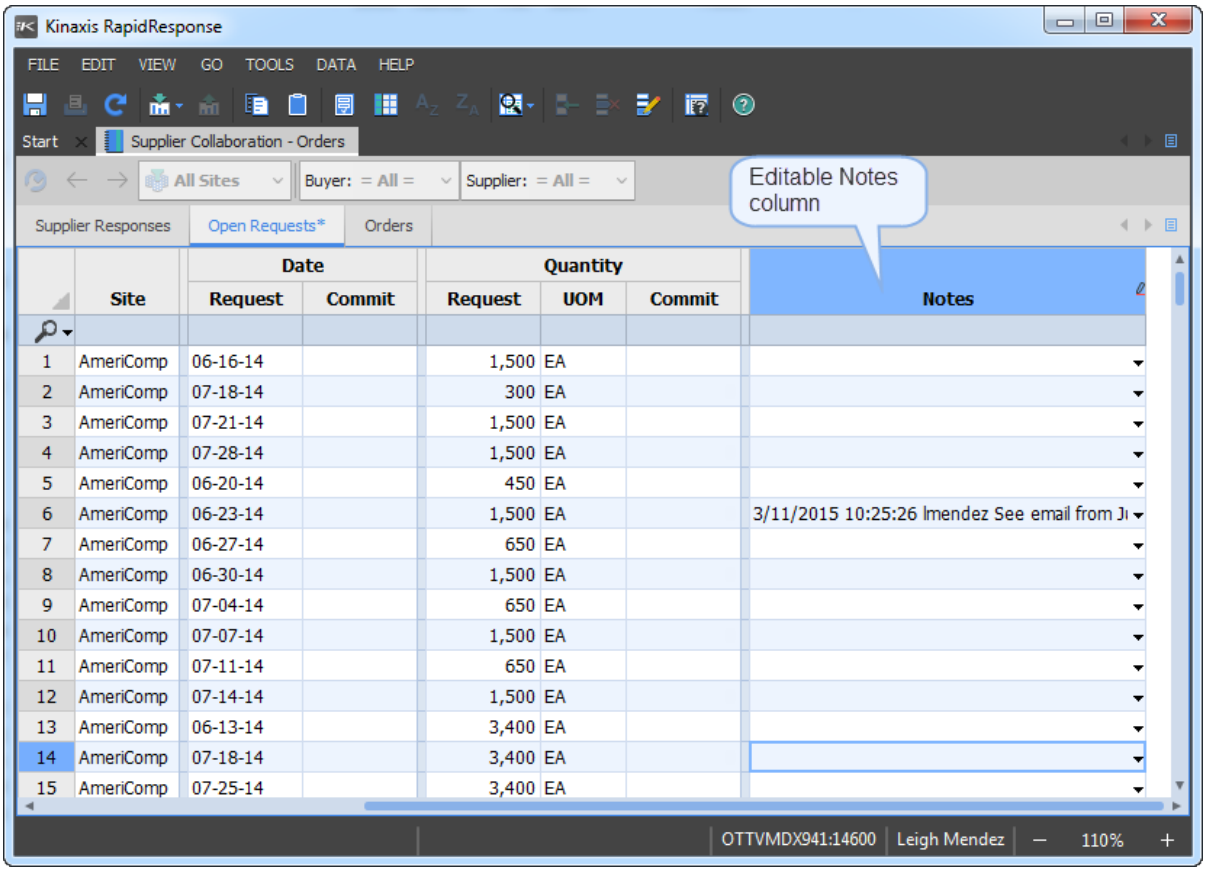
In some cases, a user might be able to access more than one report or form, but still not have access to the Explorer. This can happen when a single report has been shared with the user, and it contains links that can be used to open other resources. As an example, the SCM Dashboard links to several workbooks, which can be opened through the dashboard. For more information about linked resources, see "About the Resource Permissions workbook" on page 575, the *RapidResponse User Guide*, and the *RapidResponse Resource Authoring Guide*.

For consumer users who require more than one workbook, dashboard, or scorecard, you should provide them with resources that relate to their job functions, such as demand-oriented workbooks for customer service representatives.

Contributors

Contributors not only view data in RapidResponse, but contribute by editing or adding information. For example, a warehouse manager might use a form to update inventory data. Contributors might also be external users, such as suppliers and customers, who need to modify order information. A supplier, for example, might open a workbook to view new part orders, and then commit to delivering the parts, decline the orders, or propose changes.

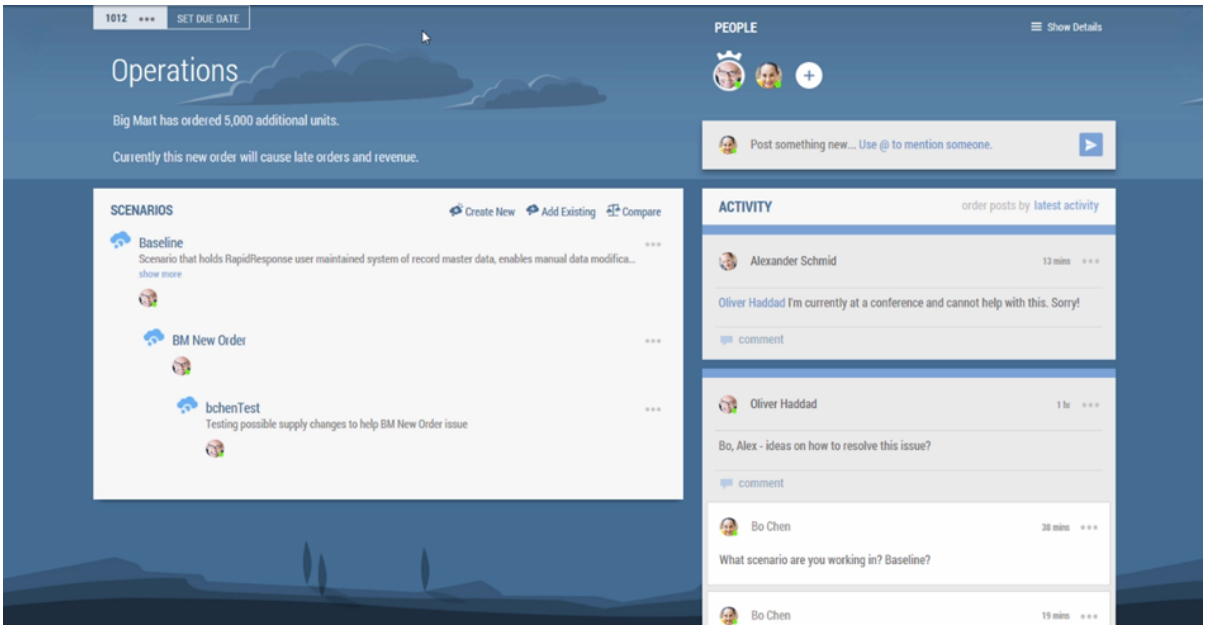
Contributor users with access to multiple reports can decide which reports to open to view data, or you can provide them with task flows that describe a process they can follow.



Simulation/Collaboration users

Users such as master schedulers, production planners, or material planners can view and modify data to perform what-if simulations to resolve issues. These users require access to multiple dashboards, workbooks, scorecards, filters, sites, and scenarios. These users can create scenarios, and have access to the Scenarios pane.

These users might also be able to share scenarios and use collaborations to communicate and share data and resource views. The following image shows an open collaboration in process.

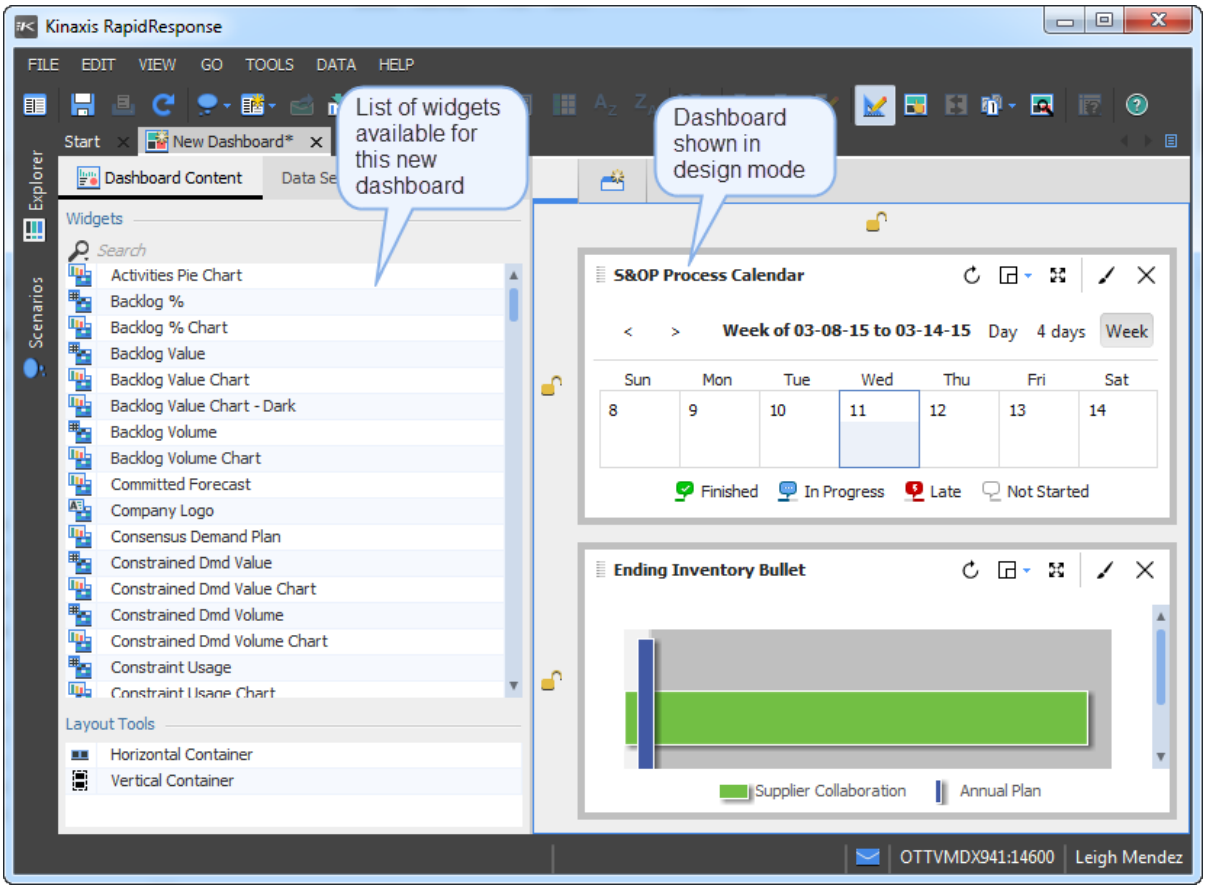


Resource authors

Users with permission to create resources such as dashboards, workbooks, scorecards, filters, forms, task flows, or hierarchies. Sometimes they create these resources for their own purposes, and they might also have permission to share resources with other users.

These users have more menu options than simulation/collaboration users. For example, a workbook author sees options to import and export workbooks on the File menu.

The following illustration shows an author user experience.



The resources and permissions granted to an author depend on the types of resources the author is expected to create. For example, workbook authors require filters, sites, scenarios, and hierarchies to test the workbooks they create, and might also require additional workbooks, which can be used as examples or to provide worksheets for new workbooks.

Users who can create resources might require access to the following resources, depending on the resources they can create:

- Resources to be used as examples when creating new resources
- Metric workbooks for creating scorecards
- Scenarios for testing resources
- Filters for testing resources and to be used as examples for new filters
- Hierarchies for testing resources and to be used as examples for new hierarchies
- Sites for testing resources
- Widgets to add to dashboards
- Scripts to use as a basis for forms

Workbook authors might also require the following permissions:

- Configure insert definitions
- Modify macros and profile variables
- Retrieve predefined workbooks

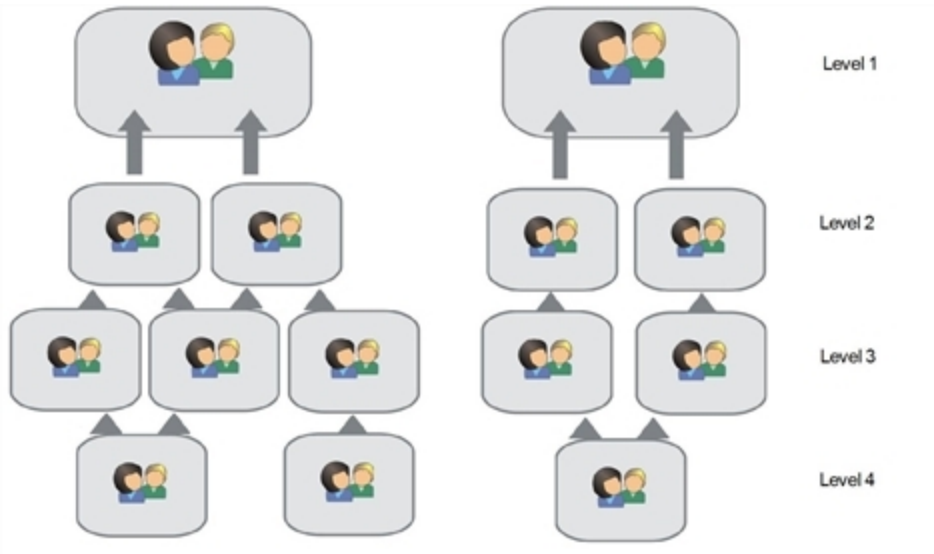
For information about permissions, see "Assigning and removing permissions" on page 517.

A filter author can be granted permission to create either static value filters, which compare a set of values to the data in a worksheet, or expression-based filters, which use an expression to determine the data that should display in a worksheet. For more information about filter expressions, see the *RapidResponse User Guide*.

Planning the group structure

Before creating custom groups, you should decide how many groups are required, how they relate to each other, and which resources and permissions each group requires. Groups with similar resource and permission requirements can be arranged so one is a member of the other, or so both are members of another group with similar resources and permissions.

Groups can represent roles within your company or roles within RapidResponse, and can define a user experience. For example, you can have one group that represents demand managers, with access to the resources they require to manage demands and the permissions they require to perform their jobs, and another group that represents workbook authors, with access to all workbooks and permission to create and share workbooks. These groups can exist in the same group structure, and one user can be a member of both.



Your group structure should begin with groups that are granted the basic permissions required by every RapidResponse user, indicated as "Level 1" in the preceding illustration. For example, it is recommended you have a group with permission to view the Approved Actions scenario and a group with permission to modify the Approved Actions scenario, and you can create additional groups for other common scenarios your company uses. These groups form the base of your group structure, and every other group is a member of them.

If your system contains workbooks that you want only certain users to modify data in, you can specify the worksheets in that workbook be editable only if a profile variable evaluates to "True". You can then control the editability by creating profile variables for the groups at this level that evaluate to "False", and then for the group you want to edit data, define a profile variable with the same name that evaluates to "True". For more information about conditional editability and creating profile variables, see the *RapidResponse Resource Authoring Guide*.

The next level in your group structure, "Level 2" in the illustration above, can contain groups that grant permission to the most common resources and permissions, such as the ability to author alerts. If you do not want to create this level of the structure, you could grant these common permissions to the groups in the first level, or to each group in the next level.

The next level in your group structure, "Level 3" in the illustration above, can be given more specific permissions. For example, you can have a group with access to some workbooks and filters, and permission to simulate data changes. Groups in this level will have the majority of users in them.

The next, and possibly final, level in your structure, "Level 4" in the illustration above, can be given the most specific permissions, such as the ability to author workbooks or modify data in shared scenarios. Users in these groups will likely be power users, or users who also fit into other groups but require more permissions to perform their jobs.

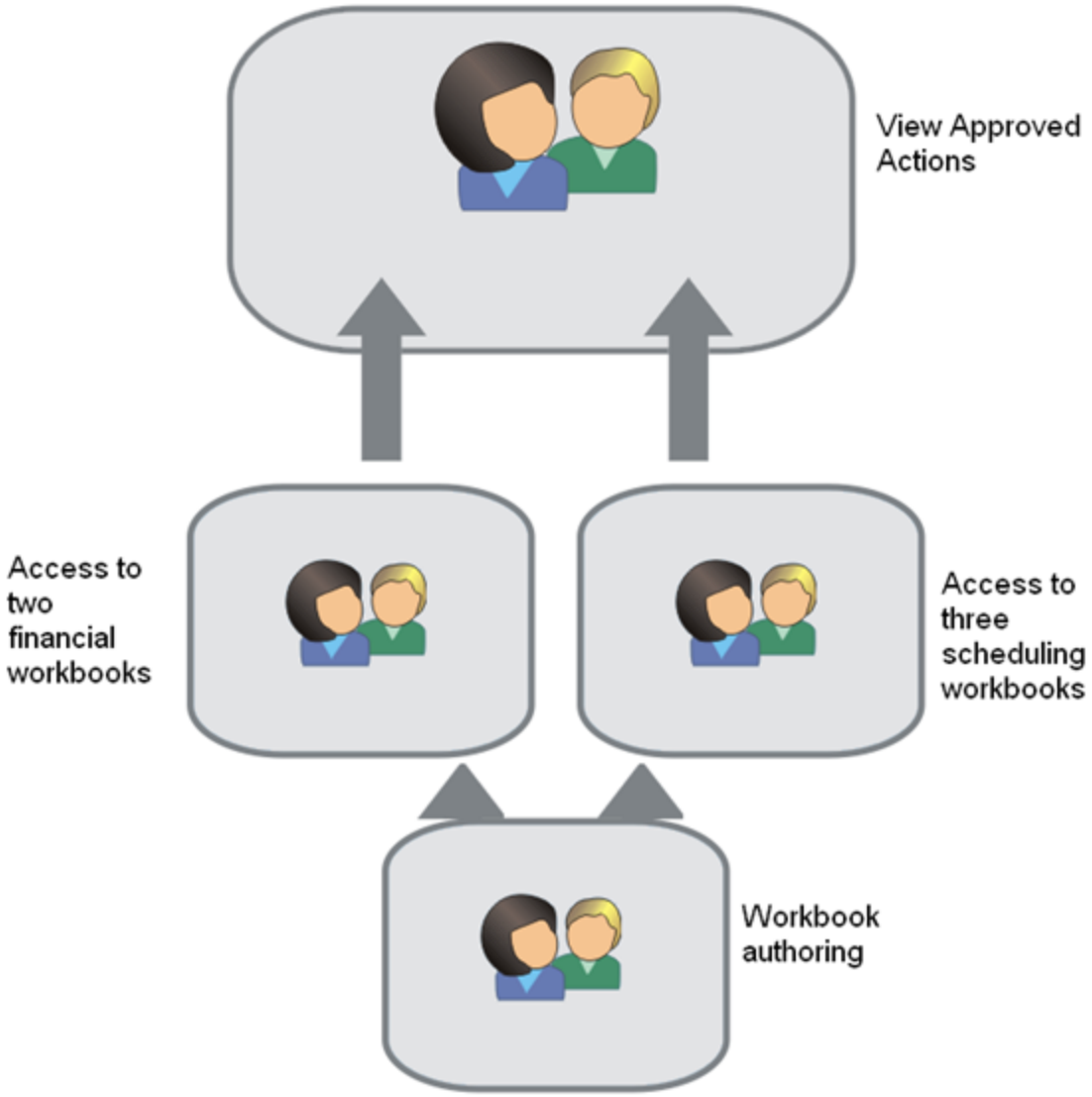
When deciding which groups a group should be a member of, you should review the resources and permissions each group has. This enables you to decide which groups have access to the resources you want each group to have. For more information, see "To review the resources and permissions assigned to a group" on page 567.

Example of a group structure

Assume you have users with the following requirements:

- All users must be able to view, but not modify the Approved Actions scenario.
- Some users require access to two financial workbooks, others require access to three scheduling workbooks.
- One power user must be able to modify those workbooks.

You can create the group structure in the following illustration to meet these requirements.



When you add users to these groups, you only need to add them to the groups with access to the workbooks. The ability to view Approved Actions is inherited from the group with that permission. The power user who modifies the workbooks is added only to the group with permission to author workbooks, which inherits access to the workbooks and the ability to view Approved Actions from the other groups.

CHAPTER 37: Creating groups

Creating a group 513
Assigning and removing permissions 517
Assigning resources 529
Assigning scenarios 533
Scenario permissions in collaboration 535
System groups 537

As a RapidResponse user administrator, you are responsible for creating and managing groups to provide users with permissions to access tools and resources they require to perform a particular task. Different users in your organization require different permissions and levels of functionality in RapidResponse. Some users might only view data, while others might perform simulations and create workbooks or filters.

It is recommended that you provide users with access to RapidResponse resources by adding them to groups that have the required permissions and resources. This allows you to grant permissions to one group rather than many times to multiple users. This chapter describes how to provide RapidResponse permissions and resources to groups.

If a group does not provide all of the permissions or resources a user requires, you can add that user to multiple groups. Although it is recommended you assign resources and permissions through group memberships, if required, you can provide the user with access to RapidResponse resources and permissions on an individual basis. For more information, see "Assigning and removing permissions for a user" on page 554.

Group membership might also be used to determine who can be assigned responsibility for data using a responsibility definition. For more information, see the *RapidResponse Resource Authoring Guide*.

Note: As discussed in "Best practices for setting up user accounts" on page 493, S&OP users should be added to predefined S&OP groups. The S&OP groups support a specific RapidResponse process to solve business problems.

Creating a group

You can define groups from “scratch” and add all new members, or you can duplicate an existing group to quickly create a group with similar permissions and members. When creating a group, you can define a message that will be sent to each user that is added to the group. It is recommended you use this

message to provide group members with information about the group's purpose and the resources it provides access to.

▸To create a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Groups** tab.
3. Click **New Group**.
4. Type a unique name for the group in the **Name** box. This name cannot contain the apostrophe (') or backslash (\) characters.
5. If you are creating the group for somebody else, in the **Owner** list, click the administrator you want to be responsible for the group.
6. In the **Description** box, type a description of the group's purpose and resources.
7. If you have already created user accounts or groups that you want to be members of the new group, click the **Members** tab, and then click **Add Members**. Continue to the next step.

   Otherwise, go to step 9.
8. In the **Add Members** dialog box, do the following:
   - On the **Users** tab, select a user from the list, and then click **Add**. Repeat for each user you want to add.
   - On the **Groups** tab, select a group from the list, and then click **Add**. Repeat for each group you want to add. You cannot add any groups that the new group is a member of.
   - Click **OK**.
9. If you want to send a message to notify the group members of their addition to the group, select the **Send message to new members** check box, and then do the following:
   - In the **Subject** box, change the subject for the message, if desired.
   - In the **Message** box, type the message the new members receive. For example, you might want to provide information about the resources provided to group members, or give contact information for someone that group members can contact if they have questions or difficulties.

     If you have a long message, you can compose it in a word processor and then copy and paste it here.
10. Make the group a member of other groups to inherit permissions and resources, and then assign any additional resources or permissions that are required. For more information, see "Resource and permission inheritance" on page 515.
11. Optionally, do any of the following:
    - Add users to the group that provides the required resources and permissions. For more information, see "Adding users to groups" on page 554.
    - Assign permissions to the group. For more information, see "Assigning and removing permissions" on page 517.
    - Assign resources to the group. For more information, see " Assigning resources" on page 529.

Note: When adding members to a group, you can select multiple groups or users. To select nonadjacent items, hold down **CTRL**, and then click each item. To select adjacent items, hold down **SHIFT**, and then click the first and last item in the sequence.

Tips:

- You can also create a new group by duplicating an existing group. To duplicate a group, click a group in the grid, and then click **Duplicate Group** .
- To find out more about the users you can add to the group, move the pointer over their names.

Resource and permission inheritance

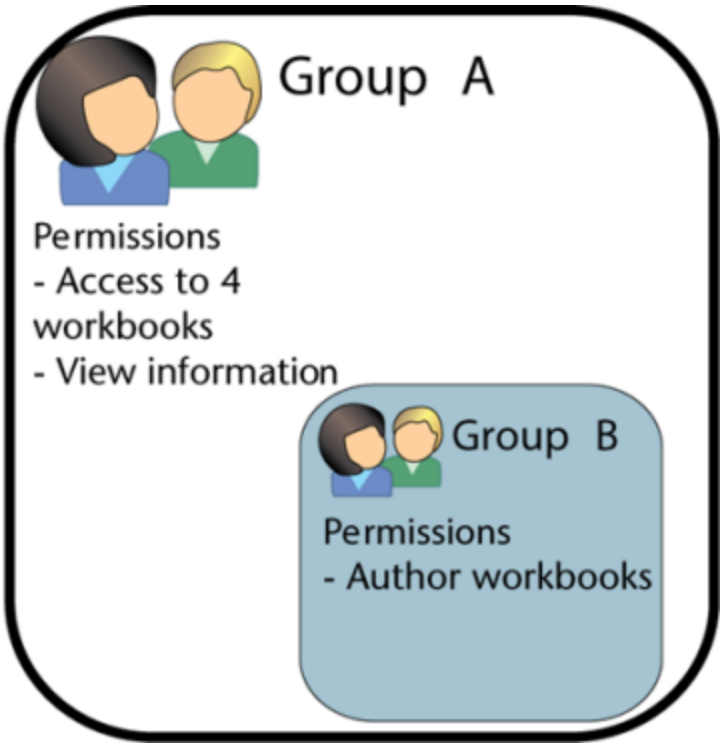
Although permissions and resources are inherited from groups, each group you create likely requires more resources and permissions than the parent groups provide. In this case, you must determine which additional resources and permissions you must give to the group.

You should only assign the resources that group members need to perform their jobs. For example, a group of master schedulers would not need access to financial workbooks, or a group based in North America would not need access to data for sites in Europe. Assigning only the resources the group requires also helps ensure data security. For example, the Customers group does not have access to workbooks that show financial information.

When granting additional permissions to a group, take care to not grant more permissions than required. For example, you might not want a group of general users to be able to modify data in shared scenarios.

A group that is a member of another group inherits the parent group's resources and permissions. Before making a group a member of another group, you must know which groups have access to resources and permissions that members of the new group require. For more information, see "Planning the group structure" on page 510.

For example, certain users might need extra permissions, such as the ability to author workbooks instead of only viewing information. In these situations, you should create two groups, grant one of them permissions, and make one a member of the other group as shown in the following illustration.



Members of Group A have permissions to access four workbooks and to view information in RapidResponse. Because Group B is a member of Group A, members of Group B have the same permissions as Group A, plus workbook authoring permissions. For more information about permission to view information, see " Assigning resources" on page 529.

▸To make a group a member of another group

1. In the **New Group** or **Group Properties** dialog box, click the **General** tab.
2. Click **Select Groups**.
3. In the **Select Groups** dialog box, select the group you want to make the new group a member of, and then click **Select**.
4. Repeat step 3 for each group you want to make the new group a member of.
5. Click **OK**.
6. Add any additional resources and permissions the group requires. For more information, see "Creating groups" on page 513.

Notes:

- If you add the group to groups that have permission to view and to modify a scenario, the modify permission overrides the view permission.
- Group memberships cannot contain circular dependency. For example, if Group A is a member of Group B, Group B cannot be a member of group A.

Assigning and removing permissions

You can assign permissions to a user or group. By default, permissions assigned to groups are inherited by the group's members, including users and other groups. For more information about inheriting permissions, see "Resource and permission inheritance" on page 515.

▸To assign permissions

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** or **Groups** tab.
3. Click a **User ID** or **Group** name.
4. In the **User Properties** or **Group Properties** dialog box, click the **Permissions** or **Authoring** tab.
5. Select permissions as required.

   If you are creating the group and have not made it a member of any other groups, the group has no permissions granted. If you have made it a member of other groups, the inherited permissions are shown as selected check boxes.

The permissions you can assign to users and groups are outlined in the following tables.

Permissions tab

Permission	Description
Sign In group	**Permissions affecting users' sign-in experience** **Both of the password options in this group must be selected if you are using a single sign-in environment, and are not available for users that sign in only using SSI.**
Start page	Provides access to the Start page in the Java client. Consider denying access for users outside of your company, such as suppliers; you could also deny access for customers who might not be interested in RapidResponse resources that appear on the Start page, such as learning videos and new feature descriptions, and who only have access to one or two reports.
Password never expires	Specifies if users have passwords that do not expire. If the passwords do not expire, they never need to be changed.
Cannot change password	Specifies if users are allowed to change their passwords.
Collaboration Tools group	**Permissions that affect how users can interact with each other.**
Message Center	Receive and view messages in Message Center. This permission also provides access to messages on the Start page in the Java client. Users without this permission will not be able to see Message Center widgets in dashboards.

Permission	Description
Send links	Send a link to a predefined view of resources to other users. Users who do not have this permission can include links in messages sent from the Send Message dialog box. Users access this dialog box by clicking the Compose button on a contact card. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Add users to collaborations	Users with this permission have access to the entire RapidResponse user list and can add other users to collaborations. Users with External license types do not have access to this permission. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. However, users who do not have this permission can still participate in collaborations.
Manage S&OP	• Process—Specifies that the user can start new S&OP cycles. • Sub-process—Specifies that the user can start an S&OP sub-cycle. **Note:** If users have either process or sub-process permission, they will automatically have the permission to publish the S&OP plan.
User Visibility	Controls the visibility of other users' names and contact information to this user. Options include: • **All**: Users can see information about all other users. • **Limited**: Users can see information about themselves and users with the All visibility level. • **None**: Users can only see information about themselves. This option is only shown in User Properties. User visibility cannot be controlled at the group level. For more information, see "Limiting visibility of user information" on page 556.
Administration group	**Assigns administrative permissions. It is recommended you assign administrative permissions by adding users to an administration group. For more information, see "Assigning administrator permissions" on page 41.**
System	**On-Premises:** System administrators can perform any administrative task except those that can only be performed by the Master Administrator (Admin user). **On-Demand:** System administrators can perform any administrative task except those that can only be performed by the Master Administrator at Kinaxis. Granting this permission also grants sharing permission for every resource type and access to Message Center. Only system administrators can grant this permission. For more information, see "System administrator responsibilities" on page 34.

Permission	Description
User	User administrators can perform administrative tasks related to creating and managing user accounts and groups. Granting this permission also grants sharing permission for every resource type and access to Message Center. Only system administrators can grant this permission. For more information, see "User administrator responsibilities" on page 35.
Data	Grants users in the group data administrator permissions. Data administrators can perform administrative tasks related to importing and mapping data from enterprise data sources. Granting this permission also grants sharing permission for every resource type and access to Message Center. Only system administrators can grant this permission. For more information, see "Data administrator responsibilities" on page 36.
Modify data integration	Specifies if a user with System or Data administration permissions can modify any of the following data integration settings: • Sites • Data Sources and Mapping • Data Model • Data Persistence Rules If this option is not enabled, then the administrative user has read-only access to the dialog boxes that control data integration settings. For more information about this option, see "Permission to modify data integration settings" on page 36.
Manage all scenarios	Specifies if an administrator can modify shared scenarios (including those not shared to the administrator), delete any shared or private scenario, and give any shared scenario to another user. All administrator types have access to the Scenarios workbook. With this workbook, administrators can view (in a tree view) all private and shared scenarios in RapidResponse. It includes information such as the last time that a scenario was used or updated and the permanent status. If an administrator also has the **Manage all Scenarios** permission, they can also use this workbook to can delete any shared or private scenarios.
Application Server Event Log	Access to the Application Server Event Log. By default, system administrators have this permission. For more information, see "RapidResponse Application Server Event Log" on page 606. This permission is only available in an On-Premises environment.
Working with Data group	**These permissions determine what scenario management options users have, and what types of actions they can take when working with data.**
Create scenarios	Create new scenarios and edit scenario properties. This permission also provides access to the Scenarios pane. Users with this permission get access to the Scenarios pane in the Navigation pane.

Permission	Description
Share	Share scenarios with other users. Granting this permission also grants the permission to create new scenarios. Select one of the following options: • **Scenarios owned by user**—share only the scenarios the user owns. • **Any accessible scenario**—share any scenario the user has access to. Users with this permission can access to the Scenarios pane in the Navigation pane. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Edit data in shared scenarios	Specifies if a user can modify data directly in a shared scenario. Users without this permission can only indirectly modify data in a shared scenario by making changes in a child scenario of the shared scenario and then committing the changes to the shared scenario. This permission is commonly not granted to enforce scenario commit best practices. For example, users who have not been granted this permission cannot directly modify permanent or automatically updated scenarios. **Note:** To modify a shared scenario, directly or indirectly, a user must have it shared to them with the **Modify** permission (not **View only**).
Warn before editing	Specifies if a user who can edit data in a shared scenario is given a warning before making any data changes.
Import data to scenarios	Specifies if a user can import data from a Microsoft Excel file into a scenario. With this permission, general users can also customize the Microsoft Excel files for importing data into RapidResponse scenarios. Prior to RapidResponse 10.1, only system and data administrators could customize the Microsoft Excel files for importing data into RapidResponse scenarios. For more information, see the *RapidResponse User Guide*.
Override the worksheet record limit	Specifies if a user can view every record in a worksheet that exceeds the worksheet record limit. The limit by default is 5,000 records for vertical worksheets and 500,000 for crosstab worksheets. These settings can be modified. This permission does not apply to crosstab worksheets. For more information, see "Setting the worksheet record limit" on page 657. Allowing users to override the record limit can place heavy demands on the RapidResponse system. Large amounts of data being processed might result in slowed RapidResponse performance for all users. It is recommended you grant this permission only to a few users, and only if they require access to every record in a table as part of their job. For example, a user who exports data to Microsoft Excel to send to customers or suppliers might require this permission to ensure that every record in the worksheet is exported.

Permission	Description
View workbook properties	View properties of workbooks the user has access to. This permission is automatically granted to workbook authors. This permission also provides access to the *RapidResponse Resource Authoring Guide*. **Caution:** With this permission users can view data from any table and from any site they can access. For example, if the user has access to the New York site, they can view any records with Site = 'New York'. This might bypass your data security policies.
System Tools group	**These permissions are intended for administrators and expert users.**
View data model	View the properties of the RapidResponse data model using the Data Model dialog box. General users open this dialog box from the **View** menu. Access to the dialog box might help general users troubleshoot issues. It can also provide authors with a better understanding of the data model to improve the resource authoring process. This permission also provides access to the *RapidResponse Analytic and Data Model Guide*. This setting is automatically enabled for system and data administrators. For more information about the Data Model dialog box, see the *RapidResponse Data Integration Guide*.
Use web services	RapidResponse Web services perform a variety of tasks including retrieving data, changing data, running scripts, updating data, and importing and exporting data. For information about RapidResponse Web services, see the *RapidResponse Web Services Guide*.
External query access	For a user or group with web service access, allows that user or group to run web service clients that execute queries to retrieve and update records with data from an external application. For information, see the *RapidResponse Web Services Guide*.

Permission	Description
Manage insert definitions	Create and edit definitions available to users for inserting records into the RapidResponse database. Users with this permission can edit the insert definition for any table, or set the default insert definition. These insert definitions can be used by workbook authors to define how records in their worksheets are inserted. For more information, see "Customizing data insertion" in the *RapidResponse Resource Authoring Guide*. Users with permission to author workbooks can create custom insert definitions specific to the worksheets they create, regardless of whether they have this permission.
Modify macros and profile variables	Edit the macros and profile variables used to customize worksheets and perform calculations.
Retrieve predefined workbooks	Obtain private copies of predefined workbooks included with RapidResponse. For more information, see "Retrieving predefined workbooks" on page 751.
Business Message Log	Access to the Business Message Log. By default, system and data administrators have this permission. This permission is available only if your company uses the Real-time Integration Service. For more information, see the *RapidResponse Data Integration Guide*.

Authoring tab

Permissions for authoring and sharing resources are grouped on this tab.

Permission	Description
Add-ins	• **Share**—share add-ins with other users. **On-Premises:** For more information, see "Configuring add-ins" on page 638.
Alerts	• **Author**—create and edit alerts. • **Share**—share alerts with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Automation Chains	• **Author**—create and edit automation chains. Automation chains allow users to create a series of alerts, scheduled tasks, and automation chains that run sequentially. • **Share**—share automation chains with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Dashboards	• **Author**—create and edit dashboards. Users with this permission can view dashboard properties. **Note:** Users with authoring permissions can create dashboards using any widget that has been shared with them through other dashboards. For more information, see the *RapidResponse Resource Authoring Guide*. • **Share**—share dashboards they own with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Filters	• **Author**—create and edit filters. Depending on the selection made in the **Filter type** list, users can either create filters using static values or expressions. • **Share**—share filters with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Filter type	Specifies the types of filters users with the filter authoring permission are allowed to create. • **Static only**—create only static value filters, which compare worksheet values to a list of values. This permission also allows users to create BOM filters, which can be used to find common or unique parts in bills of materials. • **All**—create all types of filters, including static value, BOM, and expression-based filters, which determine worksheet content by an expression. This permission also allows users to create site filters, which allow users to view data from multiple sites instead of a single site.

Permission	Description
Forms	• **Author**—create and edit forms. Authors must also have script authoring permission to generate scripts from new forms. • **Share**—share forms with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Hierarchies	• **Author**—create and edit hierarchies. • **Share**—share hierarchies with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Processes	• **Author**—create and edit processes and create process instances. • **Share**—share processes with other users. Users who have access to a process can run instances of that process. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list. If a user or group is assigned the Processes sharing permission, ensure you also share the Process Activities workbook with them. This workbook is required for a process owner to work with process instances.
Responsibility	• **Author**—create and edit responsibility definitions. • **Share**—share responsibility definitions with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Scheduled Tasks	• **Author**—create and edit scheduled tasks. Scheduled tasks support scripts and automatically modifying data and publishing data. • **Share**—share scheduled tasks with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Scorecards	• **Author**—create and edit scorecards. Users with this permission can view scorecard properties. • **Share**—share scorecards with other users. When a scorecard is shared, the metric workbooks it requires are also shared automatically. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.

Permission	Description
Scripts	• **Author**—create and edit scripts. **Note:** Users can be given a script without being an author. However, they can only run the script and not modify it. • **Share**—share scripts with other users. When a script is shared, any resources (for example, workbooks) it requires are also shared automatically. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Task Flows	• **Author**—create and edit task flows. • **Share**—share task flows with other users. When a task flow is shared, any workbooks or scorecards it requires are also shared automatically. Granting this permission also grants permission to author task flows. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Widgets	• **Author**—create and edit widgets. Users with this permission can view widget properties. **Note:** Users with authoring permissions can create a worksheet widget on any workbook they have access to, including linked workbooks. All worksheet widgets that have been shared through a dashboard are based on linked workbooks. • **Share**—share widgets they own with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.
Workbooks	• **Author**—create and edit workbooks. Workbook authors can create standard workbooks and metric workbooks. Granting this permission also grants permission to view workbook properties. **Caution:** Workbook authors can view data from any table and from any site they can access. For example, if the workbook author has access to the New York site, they can view any records with Site = 'New York'. This might bypass your data security policies. **Note:** Administrators can also create Change Data Capture workbooks. If your company started tracking responsibility in RapidResponse in version 2014.2 (or earlier), administrators might also be able to create Responsibility workbooks. For more information about Responsibility workbooks, see the *RapidResponse Administration Guide* for version 2014.2. • **Share**—share workbooks they own with other users. Providing this permission to users outside of your company (for example, customers and suppliers) can result in inadvertent data exposure. Users with this permission have access to the entire RapidResponse user list.

Permission	Description
Data modification commands	Specifies whether users with the workbook authoring permission are allowed to create workbooks with automation capabilities (or view automation settings in workbooks). Automation includes defining workbook commands and designating worksheets for automatic data modifications. For more information, see the *RapidResponse Resource Authoring Guide*. If a user with the workbook author permission does not have this permission is given a workbook that included automation tools, then the user cannot modify the workbook definition. This applies to all users including administrators.
Author library workbooks	Specifies whether users are allowed to create library workbooks, which contain worksheets that encapsulate business logic that can be reused in many workbooks, in the form of composite or spreader worksheets. For more information, see the *RapidResponse Resource Authoring Guide*.

Notes:

- The permissions that you assign will take effect the next time the user signs in to RapidResponse.
- Web service permissions should be granted to individual users, not to groups.

Permissions for administrators

By default, the predefined groups for RapidResponse administrators (system, user, and data) are granted all the permissions on the Authoring tab. The following permissions on the Permissions tab are also granted to these groups by default.

Permission	User	Data	System
Sign In group			
Start page	•	•	•
Collaboration Tools group			
Message Center	•	•	•
Send Links	•	•	•
Add users to collaborations	•	•	•

Permission	User	Data	System
Administration group			
Application Server Event log			•
Working with Data group			
Create Scenarios	•	•	•
Share Scenarios (Any accessible scenario)	•	•	•
Edit data in shared scenarios	•	•	•
Warn before editing	•	•	•
Override the worksheet record limit	•	•	•
View workbook properties	•	•	•
System Tools group			
View data model		•	•
Manage insert definitions	•	•	•
Modify macros and profile variables	•	•	•
Retrieve predefined resources	•	•	•

All administrators have access to all panes available in the RapidResponse client and can view all the shared workbooks, filters, scorecards, alerts, and task flows available to users in RapidResponse.

For more information about the permissions granted to the different administrator types, see "RapidResponse administration roles" on page 33.

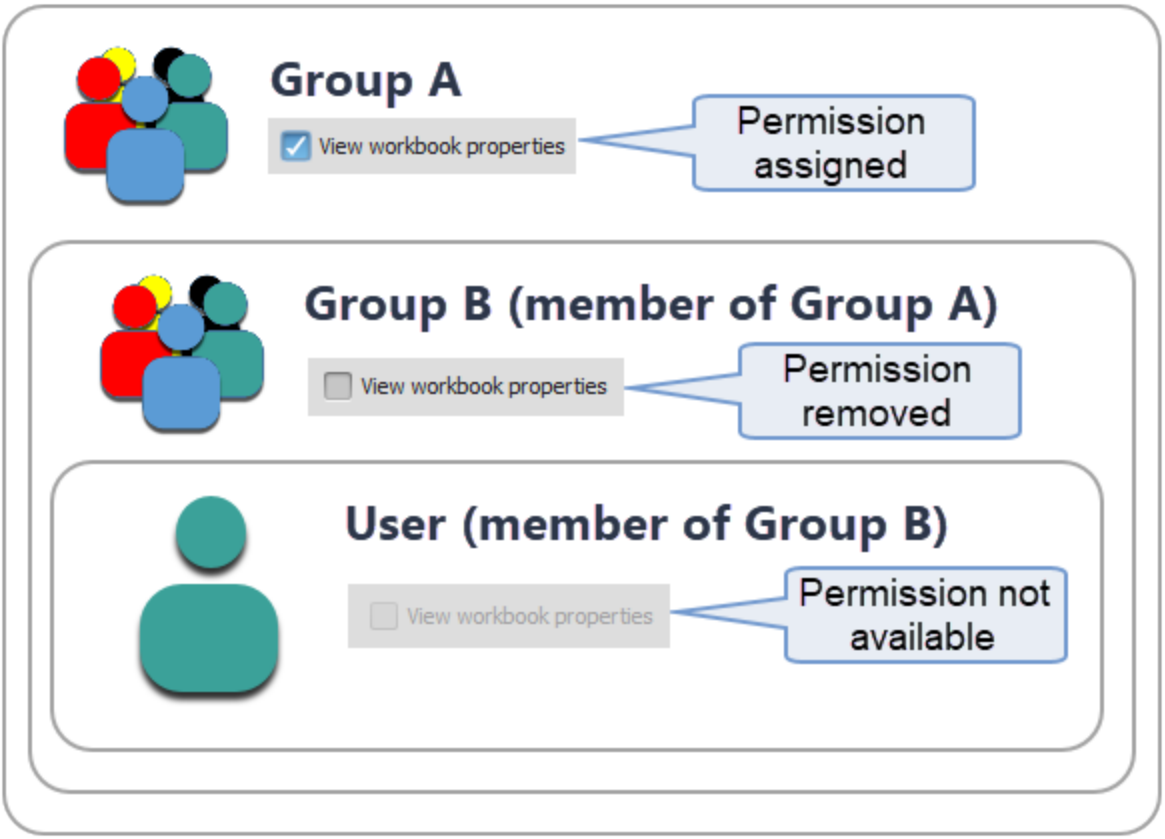
Removing permissions from groups

You can remove a permission that a user or group has inherited as a result of belonging to a group. Permissions that are removed from a group always override permissions that are assigned to its members.

You might do this if you have a group with access to resources that you want another group to have, but that has some permissions you do not want the new group to have. In this case, you could make the

new group a member of the group with the desired resources, and then remove the permissions you do not want the group to have. This is done by editing the properties of the new group and clearing the checkboxes for those permissions.

In the following diagram, the user cannot have the permission to view workbook properties because it was removed from Group B.



Because removing permissions can make it hard to determine how another group or user inherited permissions, removing permissions is not recommended. Instead, only assign required permissions. If some members of a group require a permission and some do not, you can create a smaller group that is a member of the larger group and only assign the permission to the smaller group. For an example, see "Resource and permission inheritance" on page 515

> **Note:** A permission is removed from child groups only if it was initially assigned to the parent group. If the permissions of the parent group are changed after the permission is removed from the child group and the permission is no longer assigned to the parent group, it is still removed from the child group.

▸To remove an inherited permission

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** or **Groups** tab.

3. Click a **User ID** or **Group** name.
4. In the **User Properties** or **Group Properties** dialog box, click the **Permissions** or **Authoring** tab.
5. Clear the checkbox beside the inherited permission.

Assigning resources

You can assign any resource to the predefined groups or to custom groups. Depending on the resources you assign to the group, you can customize the group members' user experience, such as allowing users to edit data.

When a new user is created in your RapidResponse system, you must ensure the user has access to, at a minimum, the following resources (directly or through their group membership):

- An openable resource (dashboard, workbook, scorecard, or task flow)
- A filter. For more information, see "Filters" on page 529.
- A site. For more information, see "Sites" on page 530
- A scenario. For more information, see "Assigning scenarios" on page 533.

You can provide users with access to resources included with RapidResponse or resources that are created by RapidResponse users within your organization and shared with at least one user or group.

If you assign access to only one openable resource then that resource is always used by the user or group. For example, if you assign only the Risk/Opportunity Assessment workbook to a group, users in that group always have that workbook open when they sign in to RapidResponse. However, if you assign one workbook and one dashboard, the user can choose which resource to open.

If you assign access to only one filter, scenario, and site, those resources are used in every dashboard, workbook or scorecard the user opens. If you assign more than one, the user can choose which is used in resources from the control bar.

Resource notes

This section provides information that administrators need to be aware of when assigning access to resources.

Filters

RapidResponse users need access to at least one filter before they can view and analyze data. For example, when users apply a filter to a workbook, they see the data that corresponds to the conditions built into the filter. When users apply a filter to a scorecard, the scorecard metrics provide results only for the records that correspond to the conditions built into the filter.

A filter is always associated with a RapidResponse database table, and can be applied to any workbook or scorecard that has a connection to the same table. The filters you provide must adequately filter data so that the number of records that display is a manageable size for the user to work with, and does not exceed the worksheet record limit. If the worksheet record limit is exceeded, the user receives a warning message, and is prompted to refine the search.

Processes

When you share a process with a user or group, you must also ensure to share the Process Activities workbook with the same user or group. The Process Activities workbook is required for a process owner to work with process instances.

Sites

In RapidResponse, users can examine and compare data across multiple sites. You can control users' access to data by granting permissions to various sites. Users can select sites and site filters to which they have access on the toolbar in workbooks and scorecards. Users can see site filters that contain at least one site to which they have access.

Users with the appropriate filter authoring and sharing permissions can group the sites to which they have access into site filters. They might also be able to share them with other users if they have the required permissions. For more information about creating and sharing site filters, see the *RapidResponse Resource Authoring Guide*.

Resource permissions

For each resource the user has access to, you can determine how that resource is shared with the user. Each resource has a permission associated with it, which determines how users in the group can access it. The resource permissions are:

Full—The user owns the resource. Users that own the resource can modify, share, or delete it. Applies to sites. Administrators with the appropriate permission also have a Full permission associated with the site and can give or remove access to it.

Manage—The user has author permission for the resource, in addition to the ability to share, give, or delete the resource. Administrators with the appropriate permission also have a Manage permission associated with the resource. This permission applies to all resource types except for sites.

Author—The user can check the resource in and out of the versioned repository, edit the resource, and export it.

Use—The user can use these resources with reports such as dashboards and workbooks. Applies to filters and hierarchies.

Modify—This permission applies only to scenarios. A user with this permission can view and modify data in the scenario.

Run—The user can perform the actions defined in the resource. Applies to alerts, scheduled tasks, automation chains, and scripts.

Open—The user can open the resource from the Explorer. This permission applies to reports (dashboards, workbooks, and scorecards), tasks (forms, processes, responsibilities, and task flows), and linked resources that have been shared with a task flow or process.

View—This permission applies to scenarios, sites, widgets, and add-ins. For scenarios and sites, the user can view data using the resource. In the case of widgets, it means the widget has been shared with the user.

List—This permission only applies to widgets. When a dashboard is shared with a user, the dashboard's widgets are also shared using the List permission. Users with dashboard authoring permissions can use

widgets shared in this manner in their own dashboards. These widgets are not listed in the Explorer, but they are listed in the Widgets list when the user is authoring a dashboard.

Link—The user can open the resource by clicking a link in another resource. Applies to dashboards, workbooks, scorecards, forms, alerts, scheduled tasks, automation chains, and scripts. A linked resource can be opened only from another resource and is not displayed in the user's Explorer. Some linked resources, such as library workbooks, cannot be accessed by the user and are only linked to provide data for another resource.

The following table summarizes the RapidResponse resources that can be linked.

Main resource	Can link to
Alerts	• Workbooks • Scorecards
Automation chain	• Alerts • Automation chains • Scheduled tasks
Form	• Scripts
Process	• Dashboards • Workbooks • Scorecards • Forms
Script	• Scripts • Workbooks • Forms
Scorecard	• Workbooks
Scheduled task	• Scripts • Workbooks
Task flow	• Dashboards • Scorecards • Workbooks • Forms • Task flows
Widget	• Dashboards • Scorecards • Workbooks • Forms • Task flows
Workbook	• Scripts • Workbooks • Forms

Note: Most of these resource types are dependent resources and are required by the shared resource to function.

You can review the resources assigned to a group. This is useful when you are creating new groups and want to see which resources the group has inherited from its group memberships. You can view all resources, or filter the list to show each type of resource individually.

You can also view a report of all users or groups who have access to a resource, and how those users and groups received access to the resource. For more information, see "Reviewing resource assignments" on page 575.

Reviewing assigned resources

▸To review the resources assigned to a group or a user

1. Do one of the following:
   - In the **New Group** or **Group Properties** dialog box, click the **Resources** tab.
   - In the **New User** or **User Properties** dialog box, click the **Resources** tab.
2. If this is the first time you have clicked this tab or if you have made changes in the **Member of groups** area of the **General** tab, you are prompted to save the group before assigning resources. Click **Yes**.
3. In the **Show** list, click the resource type you want to see.
4. To sort the list of resources, click the **Name** or **Resource Type** column headers.
5. To determine how users and group can access a resource, look at the value in the **Permission** column.
6. Select the **Show component resources** check box to include linked automation chains, alerts, scheduled tasks, and library workbooks. Selecting this check box also includes widgets with the List permission. For more information about resource sharing permissions, see "Resource permissions" on page 530.
7. To see how the user or group received access to a resource (such as which parent group the group inherited the resource from), move the pointer over the resource.

▸To assign resources

1. Do one of the following:
   - In the **New Group** or **Group Properties** dialog box, click the **Resources** tab.
   - In the **New User** or **User Properties** dialog box, click the **Resources** tab.
2. If this is the first time you have clicked this tab or if you have made changes in the **Member of groups** area of the **General** tab, you are prompted to save the group before assigning resources. Click **Yes**.
3. Click **Select Resources**.
4. In the **Select Resources** dialog box, in the **Show** list, click the resource type you want to assign.
5. In the list of resources, select the resources you want to assign, and then click **Add**.

   You can select multiple resources by holding **CTRL** and clicking each item, or select a group of resources by holding **SHIFT** and clicking the first and last resources in the group.
6. Repeat steps 4 and 5 for each type of resource you want to add.

7. Click **OK**.

   You can see how each resource you assign is shared with the user in the **Permission** column on the Resources tab. For example, resources that the user can open from the Explorer are identified with the 'Open' permission. For more information, see "Resource permissions" on page 530.

> **Note:** When you select a different resource type, the resources you have already added are still shown in the **Add** box.

▸To remove access to a resource

1. In the **Resources** pane of the **Group Properties** or the **User Properties** dialog box, select a resource.
2. Click **Remove**.

> **Note:** You cannot remove access to a resource that was inherited from a parent group.

Assigning scenarios

To view data, users must have access to at least one scenario. The Enterprise Data scenario represents the most recent enterprise data imported into the RapidResponse database. Only a data administrator or system administrator can modify data in the Enterprise Data scenario; therefore, after the RapidResponse installation and the import of your enterprise data, a copy of the Enterprise Data scenario called Approved Actions is created. This scenario can be modified by users with appropriate permissions.

Depending on your permissions, you might be able to share:

- Only scenarios you own.
- Any scenario you have access to.
- Any scenario.

When you share a scenario with a group or user, you must specify if the group has permission to modify the data in the scenario, or if the scenario is view-only. If you can share any scenario you have access to, you can share scenarios you do not own with the view-only permission.

If you can share only the scenarios you own and want to assign a scenario that belongs to another user or administrator, you require the owner's assistance to assign it to groups. For more information about permissions to share scenarios, see "Assigning and removing permissions" on page 517.

When you share a scenario with a group, only that scenario is available to the group members. The scenario's parent is also shared, but is not available to any users unless you share it directly with them. If you share only one scenario with a group, the members of that group do not see the scenario control in workbooks, allowing you to control what data the group members can see.

For each additional scenario you share, the scenarios will display in a tree only if they have a parent-child relationship. If you want users to be able to commit changes from one scenario to its parent, ensure that the users have permission to modify the parent.

Notes:

- System administrators and data administrators are automatically given access to the Enterprise Data scenario, with permission to modify data.
- All users who will be using responsibility definitions to assign responsibility for data require View access to the responsibility scenario. For more information about the responsibility scenario, see "Configuring responsibility" on page 635.
- Users attempting to modify data in a shared scenario will see a confirmation dialog box verifying their intent to modify data in a shared scenario. This option can be disabled by administrators in the properties of the scenario. If you select to turn off notifications about editing data in a shared scenario, it might result in performance issues. For more information, see " Scenario data changes and memory consumption" on page 704

▸To share a scenario

1. Do one of the following:
   - In the **New Group** or **Group Properties** dialog box, click the **Resources** tab.
   - In the **New User** or **User Properties** dialog box, click the **Resources** tab.
2. If this is the first time you have clicked this tab or if you have made changes in the **Member of groups** area of the **General** tab, you are prompted to save the group before assigning resources. Click **Yes**.
3. Click **Select Resources**.
4. In the **Select Resources** dialog box, in the **Show** list, click **Scenarios**.
5. Click the scenario you want to share with the group, and then click one of the following:
   - **View**—Users in the group can only view the data in the scenario.
   - **Modify**—Users in the group can modify the data in the scenario.
6. If you want the users to see the full scenario tree, share the scenario's parents. If you do not share the parents, the users will see only the scenario you shared in step 5.

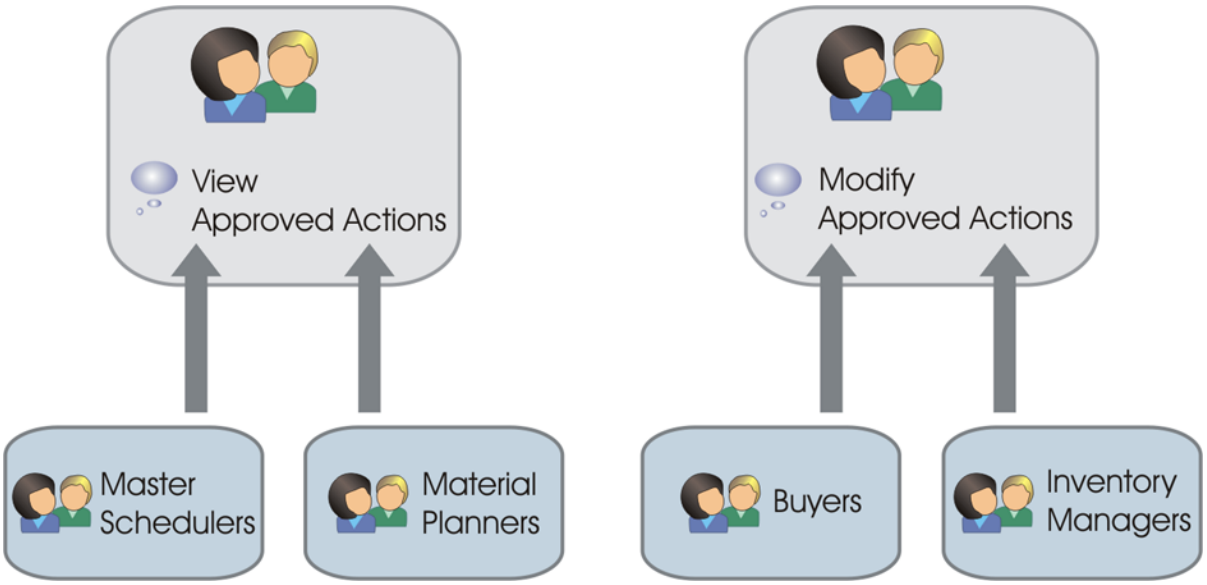
Note: If you share a scenario with a group with one permission (for example, Modify), and then share the same scenario with a user in the group with the other permission (View), the permission granted to the user overrides the permission granted to the group.

Sharing the Approved Actions scenario

If you need to share the Approved Actions scenario with users in your company, do the following:

1. Create two groups—one for users that can only view the data in the Approved Actions scenario and one for users who can modify the data. For example, you can create a View Approved Actions group and a Modify Approved Actions group.
2. All users should be granted permissions through groups designed to meet the needs of employees in your company. Add the groups that contain users that can view the data in the Approved Actions scenario to the View Approved Actions group. Add the groups that contain users that can modify the data in the Approved Actions scenario to the Modify Approved Actions group.
3. Share the Approved Actions scenario with the View Approved Actions group with View Only permission, and with the Modify Approved Actions group with Modify permission. If you do not have permission to share all scenarios and you are not the owner of the Approved Actions

scenario, it is likely owned by a system administrator. The scenario's owner will have to share the Approved Actions scenario with the groups you created.



Once you have set up the groups and shared the scenarios, you can use these groups in the future when you need to provide access to the Approved Actions scenario to new users.

You can also use these recommendations to share any other permanent scenarios that users in your company might need access to.

Scenario permissions in collaboration

Users can be granted two different share permissions for scenarios:

- **Scenarios owned by user**—share only the scenarios the user owns.
- **Any accessible scenario**—share any scenario the user has access to.

Depending on what share permissions for scenarios a user is granted, they can perform different actions to scenarios shared in a collaboration.

Creating new scenarios

Users who have permission to create scenarios can add a new scenario to a collaboration, however the scenario remains private. Users who have permission to create and share scenarios can add new scenarios to collaboration and they must select whether data in the scenario can be modified or only viewed by all the other participants in the collaboration.

Adding existing scenarios

Users who have no scenario permissions or who can only create scenarios can add any existing scenarios to a collaboration that they have access to. Users who have scenario creation and sharing permissions can add existing scenarios they have access to and set the data editing permission for the

scenario: modify or view only. When users add an existing scenario that has children, the user can select whether or not to add the child scenarios to the collaboration along with the parent scenario.

Sharing scenarios

Only users who have scenario creation and sharing permissions can select whether or not to share a new, existing, or child scenario with all other collaboration participants. When users without scenario sharing permission add a scenario to a collaboration, only participants who already have access to the scenario will see it display in the Scenarios area of the collaboration.

Creating child scenarios

Only users who have scenario creation permission can create child scenarios from any other scenario added to a collaboration.

Committing scenarios

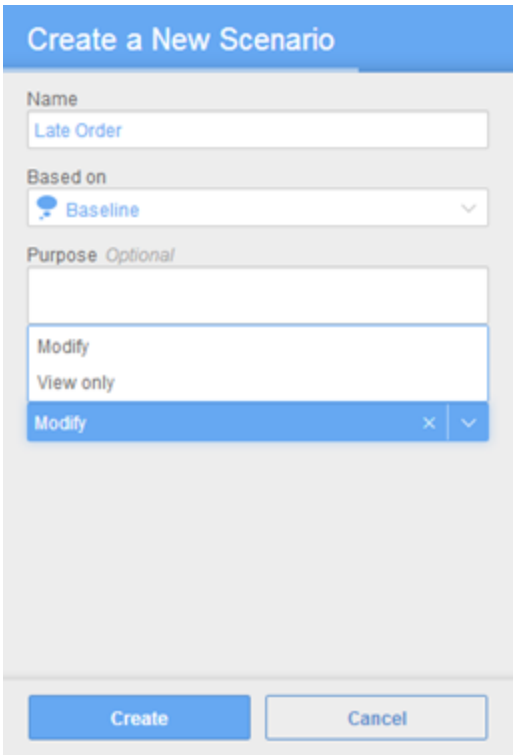
Users can only commit scenarios that they own.

Removing scenarios

Users with all types of scenario permissions can remove any scenario, including any child scenarios, from a collaboration. A scenario can only be removed and deleted by the collaboration participant who owns the scenario.

Editing data in collaboration scenarios

When users add an existing or new scenario to a collaboration, they determine what level of data editing is available to other collaboration participants: Modify or View only.



System groups

In addition to standard user groups included in RapidResponse (for example, Buyers) and custom user groups developed by your company, RapidResponse also includes system groups.

System groups are used internally by the RapidResponse system for a variety of tasks including controlling user permissions, access to resources, and making specific functionality available to users.

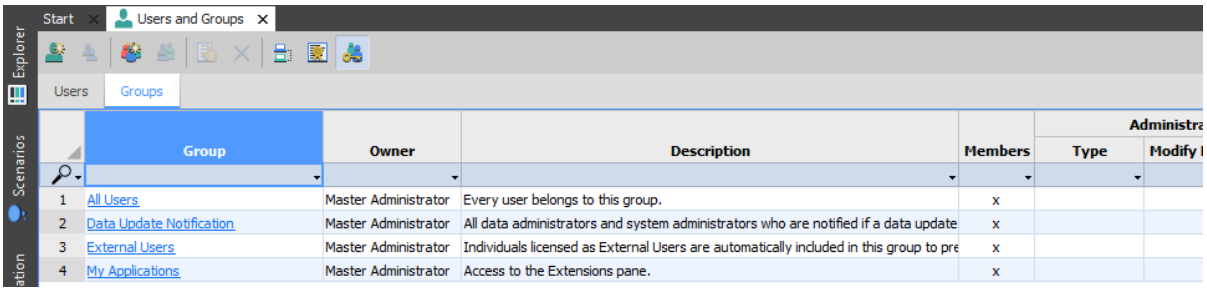
The All Users system group is used to define every RapidResponse user, and every user is added to this group when they are created.

You can review the system groups included in your system from Groups worksheet in the User and Groups workbook.

Caution: Do not edit or delete system groups. Doing so can result in unexpected changes to user permissions and functionality.

▸To view system groups

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, click .



On-Demand: Only system administrators can review system groups and only the RapidResponse Master Administrator at Kinaxis can create system groups.

On-Premises: Only system administrators can review system groups and only the Master Administrator (Admin user) can create system groups.

CHAPTER 38: Creating user accounts

Understanding user accounts and license types 539
Types of RapidResponse users 541
System requirements for users 541
Creating users 548
Adding users to groups 554
Assigning and removing permissions for a user 554
Limiting visibility of user information 556
Specifying default data formats for users 559
Setting profile pictures 560
Automatically opening resources upon sign in 562

To access RapidResponse, a user requires a RapidResponse user account, which is created by a user or system administrator.

By default, all users can perform the most basic RapidResponse tasks. Administrators place users in groups to grant permissions (such as creating simulation scenarios and creating alerts) and to provide access to resources (dashboards, workbooks, scorecards, and so on).

Although it is recommended that you give users access to RapidResponse resources and grant permissions by adding them into appropriate groups, you can give access to resources and grant or deny permissions on an individual basis. Any permissions granted or denied to the user override the permissions granted to any group or groups to which the user might belong.

As a user administrator, you need to understand RapidResponse user licensing and the types of user licenses that RapidResponse supports.

Understanding user accounts and license types

Each RapidResponse user account consumes a user license. RapidResponse supports the following types of user licenses, which are distinguished by the permissions that administrators can assign to them:

- **Alert**—this type of user can only receive emailed reports generated from RapidResponse alerts. By creating an Alert access user, there is no need to manually enter a user's email address in the alert reporting or notification properties. RapidResponse provides an unlimited number of Alert licenses.

  Alert users cannot sign in to RapidResponse and cannot be granted permissions.

  For more information about automated reporting, see the *RapidResponse User Guide*.

- **Report**—this type of user can sign in to RapidResponse and take any action that does not require a permission, such as viewing data in a report that has been shared with them or contributing to a collaboration. They can also be given permission to:
  - override the worksheet record limit
  - use Message Center and the Start page.
  - have passwords that never expire or cannot be changed.

  Other permissions, such as resource authoring or administration permissions, cannot be assigned to this type of account.

  This user type might be assigned to externally-based users, such as your suppliers and customers. Providing external users such as customers and suppliers with resource sharing permissions can result in inadvertent data exposure.
- **Light**—this type of user can sign in to RapidResponse and take any action that does not require a permission. They can also be given all of the permissions you can give to Report access users, plus:
  - create private filters (static and expression-based).
  - add users to collaborations.
  - send resource links.
  - edit data in shared scenarios.
  - import data into scenarios.

  Other permissions, such as resource sharing or administration permissions, cannot be assigned to this type of account.

  Managers who need to view data and collaborate with others in RapidResponse, but are not expected to edit data, could be light access users.

  This option is displayed only if your company has licensed Light access users.
- **Full**—this type of user can sign in to RapidResponse and take any action that does not require a permission. They can also have every available RapidResponse permission assigned to them including administration, authoring, and resource sharing permissions.

Note: Upon upgrade from RapidResponse 2016.2 Service Update 25 or earlier, Light use who were previously External users remain in the External Users system group. If you want these Light users to be able to create filters, send resource links, or add users to collaborations, remove them from the External Users group.

System accounts

Another type of account, System, does not consume user licenses. It is used for special accounts required for successful RapidResponse operation, such as the Master Administrator. System accounts are visible only in the Users and Groups workbook.

If your company uses the Real-time Integration Service, two system user accounts are created. These user accounts, **bmWsUser** and **dataWsUser**, are used to securely connect RapidResponse with the Real-time Integration Service, and must not be deleted or modified. These are system user accounts and do not consume user licenses. For more information, see the *RapidResponse Data Integration Guide*.

Reviewing user license information

Occasionally, you might want to review your user license status to verify how many user licenses are remaining, or to determine the date when the licenses must be renewed.

▸To determine how many licenses are available

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the Users and Groups toolbar, click **User Licenses** .
3. In the **User Licenses** dialog box, review the information in the **Available** and **Expiry Date** columns.

Types of RapidResponse users

You can create RapidResponse user accounts that fall into two general types:

- **General Users**—users who require access to RapidResponse resources such as workbooks and filters. This user type can also be granted resource authoring permissions (for example, workbooks and dashboards). General users can be members of any group.
- **Administrators**—users who are responsible for managing the RapidResponse system. Administrators are members of groups that have administrative permissions.

The user's type is determined by the groups the user is a member of. Any group with administrative permissions, such as the System Administrators, User Administrators, or Data Administrators groups, designates its members as administrators. Other groups can also identify their members as administrators, if they have been granted administrative permissions. For more information, see "Assigning and removing permissions" on page 517.

For more information about administrators, see "RapidResponse administration roles" on page 33.

Note: Administrators require only one user account (that is, they do not require a general user account in addition to their administrator account).

System requirements for users

As an administrator, you should ensure that every RapidResponse user's computer or mobile device meets the minimum system requirements as outlined in this section. Users should also have a working knowledge of their computer or mobile device, and its operating system.

Java client requirements

The Java client runs as a standalone Java Web Start application but is started from a Web browser. The following table describes the system requirements for RapidResponse users.

Requirement	Supported and Verified
System memory	Minimum 4 GB of RAM Recommended 8 GB of RAM
Operating system	**Microsoft Windows:** • Microsoft Windows Vista Business SP2 (32-bit and 64-bit) • Microsoft Windows Vista Enterprise SP2 (32-bit and 64-bit) • Microsoft Windows 7 SP1 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) **Mac OS:** • Mac OS X 10.10 (Yosemite) • Mac OS X 10.11 (El Capitan) **Notes:** • It is advisable that the operating system also include the latest updates, service packs, and patches. • For more information about using the Mac OS operating system with RapidResponse, see "Java client on the Mac OS operating system" on page 544.
Java Runtime Environment (JRE)	Oracle Java Runtime Environment (JRE), version 8 (any update) or 10. **Notes:** • To protect your system from potential security threats, it is recommended that users use an up-to-date version of JRE 8. As of 2019, updates to Java 8 require a maintenance contract with Oracle. • You can test the version of the JRE you are using by visiting https://www.java.com/en/download/installed8.jsp. You can also download a supported version of the JRE by visiting http://www.java.com/en/. • By default, the RapidResponse user's JRE controls how much system memory RapidResponse can consume. This can be changed by RapidResponse administrators. For more information, see "Memory settings for the Java client" on page 544.

Requirement	Supported and Verified
Web browser	Browsers are used to initially start RapidResponse as a Java Web Start application. Kinaxis has verified that the following browsers can be used to start the Java client. However, you might also be able to use other browsers. **Microsoft Windows:** • Microsoft Internet Explorer 11 • Microsoft Edge 25 (and later) • Mozilla Firefox 31 (and later) • Google Chrome 40 (and later) **Mac OS:** • Apple Safari 8 and 9 • Mozilla Firefox 31 (and later) • Google Chrome 40 (and later) **Notes:** • RapidResponse can be used with 32-bit and 64-bit versions of the supported browsers. However, the JRE configuration determines whether Java Web Start runs as 32-bit or 64-bit application. • Depending on how your browser is configured, you might need to change some browser security settings to ensure that RapidResponse can start and properly communicate with the Microsoft Windows operating system.
Monitor	**Microsoft Windows:** 1024 x 768 (minimum resolution) **Mac OS:** 1440 x 900 (minimum resolution)
System peripherals	Keyboard and mouse
PDF viewer application	A PDF viewer such as Adobe Reader or Preview for Mac OS is required to open RapidResponse guides and documents.
Adobe Flash Player	Adobe Flash Player 11.8 or later (browser plug-in) is required to view videos included in the RapidResponse help systems and documentation. A sound card, and speakers or headphones to listen to the audio portion of the video recording is also required. You can verify that Adobe Flash Player is properly set up by visiting http://www.adobe.com/software/flash/about/.

Notes:

- Kinaxis has verified that RapidResponse runs effectively with the operating systems and browsers noted in the previous table. In certain cases, you might experience unexpected results or performance issues using newer browsers and JREs or other operating systems. Kinaxis endeavors to verify new platforms as they are released.
- It is strongly recommended that user systems have the latest service updates and patches applied to operating systems, browsers, and JREs to maintain system performance and security.

Java client on the Mac OS operating system

The Java client can be used on Microsoft Windows and Mac OS operating systems. However, not all RapidResponse features supported on Microsoft Windows are supported on Mac OS. This includes:

- The Start page
- Forms
- Collaboration Center

In addition, some RapidResponse applications such as Order Fulfillment make use of forms in process and workflows. These applications should only be used with the Java client on the Microsoft Windows operating system.

Users whose computers are running Mac OS can use the web client to take advantage of forms or Collaboration Center. For more information about signing in to the web client, see "Providing the RapidResponse URL and credentials" on page 553.

Alternatively, users might be able to run Microsoft Windows in a Mac OS virtual environment to run the Java client and access these features.

Google Chrome browser settings

This topic only applies to the **On-Premises** version of RapidResponse.

Users that try to start RapidResponse from the Google Chrome browser with the Java plug-in disabled will see an error. As an administrator, you can have your users bypass this error by modifying the RapidResponse Application Server's **web.config** file.

▸To start RapidResponse from Chrome with Java plug-in disabled

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. On the computer where RapidResponse Application Server is installed, open the **Web.config** file located in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder with an XML or text editor.
2. Add the following line to the file:
   ```
   <supportedJavaRuntimes ignoreWebStartInstalledCheck = "true" />
   ```
3. Save the **Web.config** file.

> **Note:** If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of RapidResponse Application Server is installed.

Memory settings for the Java client

RapidResponse requires an installed and enabled Java Runtime Environment (JRE) on the user's computer. By default, the RapidResponse user's JRE controls how much system memory RapidResponse (a Java Web Start application) can consume. For example the 32-bit version of the JRE 8 sets the Java Web Start memory to 256 MB. The 64-bit version sets the Java Web start memory to one quarter of the

available system memory. For example, on a system with 32 GB of memory, the Java Web Start memory is set to 8 GB.

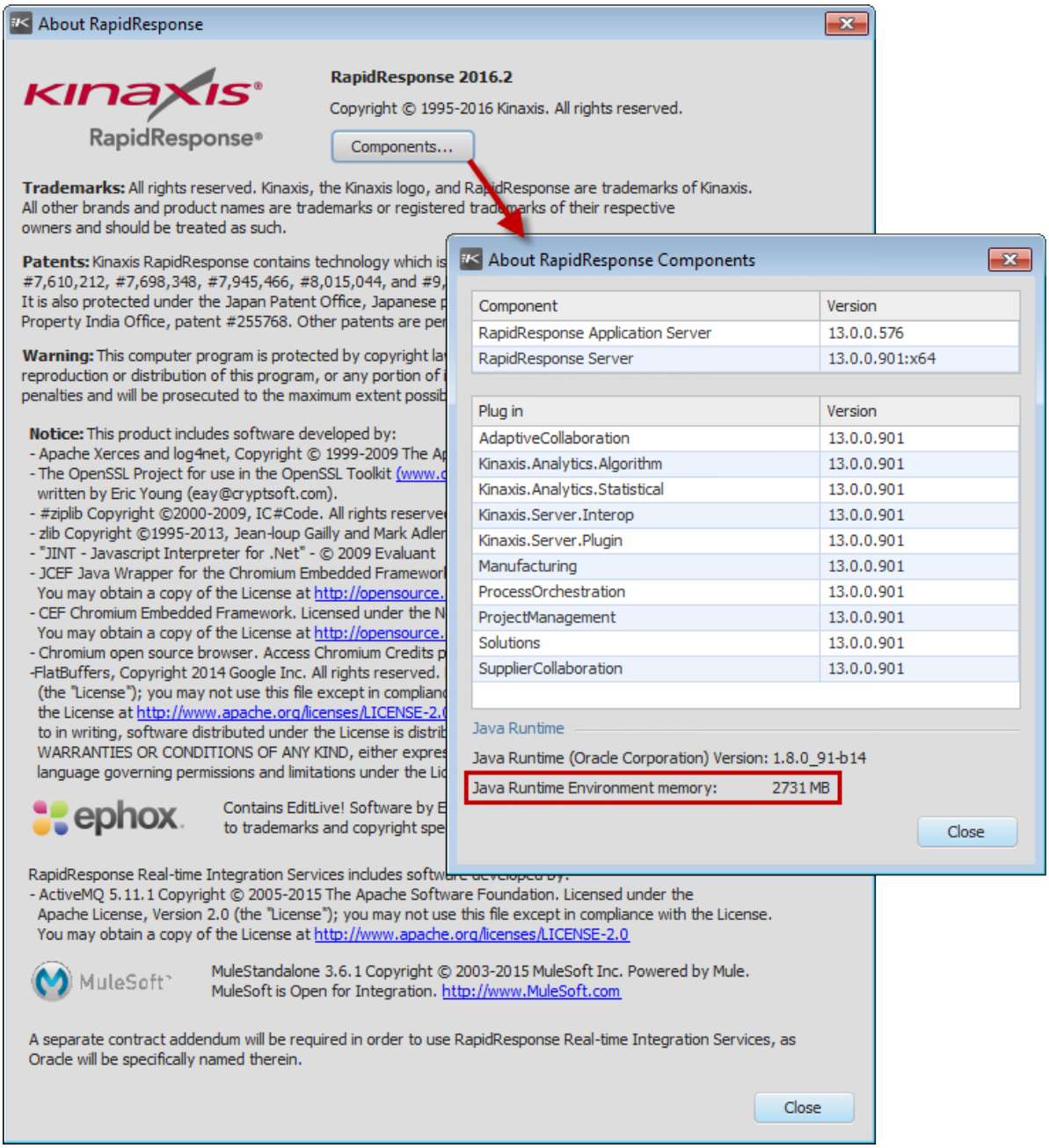
If RapidResponse users with a 32-bit browser are using a 64-bit version of a JRE, they will not be able to sign into RapidResponse if a 32-bit JRE is not also installed on their system. Upon trying to sign into RapidResponse, they will be warned that a JRE is not enabled. To work around this, install a 32-bit JRE.

As a Java Web Start application, RapidResponse is launched by a JNLP file from a browser. The JNLP file is associated with the enabled JRE. If more than one JRE is enabled, for example, a 32-bit and a 64-bit version, the JNLP file and the RapidResponse client use the most recent JRE that was installed on the user's system. The most recent JRE installed takes into account updates.

Note: Mac OS systems support only the 64-bit JRE.

RapidResponse users can determine their JRE memory setting from the About RapidResponse dialog box (from the **Help** menu, click **About RapidResponse** and then click **Components**).

The following illustration shows the About RapidResponse and About RapidResponse Components dialog boxes.



If users keep many reports (dashboards, workbooks and scorecards) open, they might receive low memory warning messages from RapidResponse. If users often receive these messages, administrators should consider changing the JRE memory limit setting.

Overriding all user's JRE memory setting.

This topic only applies to the **On-Premises** version of RapidResponse.

Administrators with access to the computer where RapidResponse Application Server is installed can override the JRE memory setting for all users.

If you are using the **On-Demand** version of RapidResponse, Kinaxis Customer Support can override the JRE memory setting for all users with a value that you specify.

If you override the JRE memory setting, the **About RapidResponse Components** dialog box continues to display the user's JRE memory setting. However, the **Web.config** setting is used by the user's RapidResponse client.

▸To override all users' JRE memory setting

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. On the computer where RapidResponse Application Server is installed, open the **Web.config** file located in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder with an XML or text editor.
2. Locate the **`supportedJavaRuntimes`** element.
3. Edit the element to set the memory setting. The following example shows how to set it to 256 MB.
   ```
   <supportedJavaRuntimes minimumMemory="256"/>
   ```
4. Save the **Web.config** file.

Caution: If the memory setting is too high, the user's JRE will fail to load if memory cannot be fully allocated. If the JRE fails to load, RapidResponse does not start.

Note: If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of RapidResponse Application Server is installed.

Web client requirements

The web client can be used with devices that support a HTML5 browser. Users of the web client on a desktop system use a mouse and keyboard to interact. Equivalent touch screen interactions allow mobile device users to access most features of this client.

Desktop browsers

The web client can be used with desktop browsers that support HTML5 such as:

- Google Chrome 48
- Mozilla Firefox 32
- Microsoft Internet Explorer 11
- Microsoft Edge 25

Mobile devices

Kinaxis has verified that the following devices (and operating systems) can be used.

- Apple iPhone 6 and later (iOS 9) with the Safari browser
- Samsung Galaxy S6 and later (Android 5.0) with the Google Chrome browser
- Apple iPad Air 2 and later (iOS 9) with the Safari browser
- Samsung Galaxy Tab Pro 8.4 and later (Android 5.0) with the Google Chrome browser

Users of other mobile devices that support an HTML5 browser might be able to run RapidResponse. However, it is recommended you verify whether RapidResponse runs as expected on other devices.

Notes:

- Kinaxis endeavors to verify new devices and browsers as they are released.
- RapidResponse displays in both portrait view and landscape view on mobile devices, but has been optimized for landscape view on tablets and portrait view on phones.

Creating users

At a minimum, creating a user account involves giving the user a unique ID and a password and specifying their license type. Permissions and access to resources could then be provided on an individual basis or by adding the new user to a group.

A user requires access to at least one scenario and filter to be able to sign in, and at least one of the following resources:

- Dashboard
- Workbook
- Scorecard
- Task flow
- Form

You should place new users into the groups that have access to the resources and permissions they require. By becoming a member of a group, users inherit the group's permissions and resources. Alternatively, you can create all your user accounts without placing them in groups, and then edit your groups to include the users. This method might be more efficient if you are adding users to a small number of groups, especially during the initial setup of groups and users. For more information, see "Adding users to groups" on page 554.

You can also specify a user's contact information, including their job title, phone number, and location. If you do not provide this information, the user can add their own information. This information allows users to contact each other, and can be used for collaborative work efforts.

You can set profile pictures for the user accounts you create, or users might set their own profile pictures. For more information, see "Setting profile pictures" on page 560.

If you are implementing a Single Sign-In (SSI) system, you can specify whether users are able to sign in to RapidResponse using their user name and password, or whether they can use only SSI . By enforcing SSI only, you can ensure the credentials for each user are managed in your authentication system. This can improve security because no user knows their password, and a user cannot sign in as other users if the passwords become known. For more information, see " Configuring single sign-in for On-Premises" on page 835 or "Configuring single sign-in for On-Demand" on page 863. If you specify a user as SSI only, you cannot specify a password for that user, and the password cannot be changed.

When a user account is created, a message welcoming the user to RapidResponse is sent to their email account, and to their Message Center if they have access to it. If you are creating the user accounts in advance of allowing the users access to RapidResponse, you can choose to not specify the users' email addresses until you are ready to provide access.

Notes:

- If you want to create a user with similar permissions to an existing user, you can duplicate the existing user's account. For more information, see "Duplicating a user account" on page 551.
- You should ensure your users have computers that meet the minimum system requirements. For more information, see "System requirements for users" on page 541.

Bulk creation of user accounts

As you a user administrator, you might need to create many users account at once. For example, a new site is added to your RapidResponse system and you need to create 100 new RapidResponse user accounts.

Using RapidResponse Scripting, you can avoid the slow and labor intensive process of creating numerous accounts manually. RapidResponse Scripting supports the creation, deletion and the modification of user accounts. A file script argument type enables you to use information contained in a file as input to the script being executed. For example, you can use a file argument to easily create multiple RapidResponse user accounts based on an existing employee directory. After running this type of script, you can then add the new users to user groups so that each RapidResponse user receives the appropriate access to resources and scenarios.

For more information about this capability, see the **User collection** information in the the *RapidResponse Scripting Guide*.

▸To create a Full, Light, or Report user account

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, click **New User** .
3. On the **General** tab, type information in the following boxes:
   - **User ID**—the name or string users type at the sign in prompt when they start RapidResponse.

     This user ID must be unique, and, if applicable, should be the same as the user's ID in your enterprise system. The apostrophe ('), backslash (\), semicolon (;) and straight quotation mark (") characters cannot be used in a user ID. A user ID cannot contain more than 250 characters.

     Using the at (@) sign in a User ID or Name is not recommended because it can interfere with the functionality of social markup in collaborations.

     Caution: Because user IDs are shown in some places instead of names when a user's personal information is blocked, ensure that user IDs do not contain information that should not be available to all users. For more information, see "Limiting visibility of user information" on page 556.

   - **Name**—the user's name or an identifier. A user's name cannot contain more than 256 characters.

- **Email address**—the user's email address, which is required for users that use any email functionality in RapidResponse.

4. Select **Forward a copy of each message to the user's email address** to have RapidResponse messages automatically forwarded from Message Center to the user's specified email address. This setting can only be applied at the user level (not to a group). A user does not need access to Message Center to have messages forwarded.
5. From the **License** type list, select one of the following:
   - **Full**
   - **Light**
   - **Report**

   For more information about license types, see "Understanding user accounts and license types" on page 539.
6. If this user's credentials will be stored in and managed by your SSI infrastructure, select the **SSO only** check box. When this is selected, you cannot specify a password for the user. Go to step 9.
7. In the **Password** box, type the string the user must type to sign in to RapidResponse. You cannot use the straight quotation mark (") character or the semicolon (;) character in the password. A password cannot contain more than 256 characters.
8. In the **Confirm password** box, type the same string you typed in the **Password** box.
9. In the **Contact** area, specify any of the following information:
   - **Title**—the user's job title.
   - **Phone**—the user's telephone number and extension.
   - **Fax**—the user's fax number.
   - **Mobile**—the user's mobile telephone number.
   - **Pager**—the user's pager number.
   - **Location**—the user's job site.

     If the user is outside of your company or at a site not represented in RapidResponse, then you can type their site.
   - **Country/Region**—where the user's site is located.
   - **Notes**—any additional information about the user.

   Note: Users can modify their personal contact information using the Options dialog box. From the Tools menu, click Options and select the Contact tab. If profile pictures are enabled on your RapidResponse system, the Options dialog box can also be accessed by clicking on your profile picture in the RapidResponse toolbar.

10. Optionally, do any of the following:
    - Set the user's profile picture. For more information, see "Setting profile pictures" on page 560.
    - Make the user a member of the groups that provide the required resources and permissions. For more information, see "Adding users to groups" on page 554.
    - Grant the new user RapidResponse permissions. For more information, see "Assigning and removing permissions" on page 517.
    - Provide the new user access to resources. For more information, see "Resource permissions" on page 530.
    - Set default data formats for the user. For more information, see "Specifying default data formats for users" on page 559.

▸To create a user account for a report recipient (alerts)

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, click **New User** .
3. On the **General** tab, type information in the following boxes:
   - **User ID**—the unique name or word to identify this user account.
   - **User name**—the user's real name.
   - **Email address**—the email address the user uses to receive reports generated by the RapidResponse Service Host.
4. In the **License type** list, click **Alert (email recipient)**.
5. In the **Contact** area, specify any of the following information:
   - **Title**—the user's job title.
   - **Phone**—the user's telephone number and extension.
   - **Fax**—the user's fax number.
   - **Mobile**—the user's mobile telephone number.
   - **Pager**—the user's pager number.
   - **Location**—the user's job site.
   - **Country/Region**—where the user's site is located.
   - **Notes**—any additional information about the user.

Note: You do not have to create a user account for users who only receive reports. Instead, users can manually type the email address each time they create an alert for this type of user. By creating an Alert user, the user can be chosen from a list of RapidResponse users and their email address does not need to be manually entered for each alert. You can create an unlimited number of Alert users.

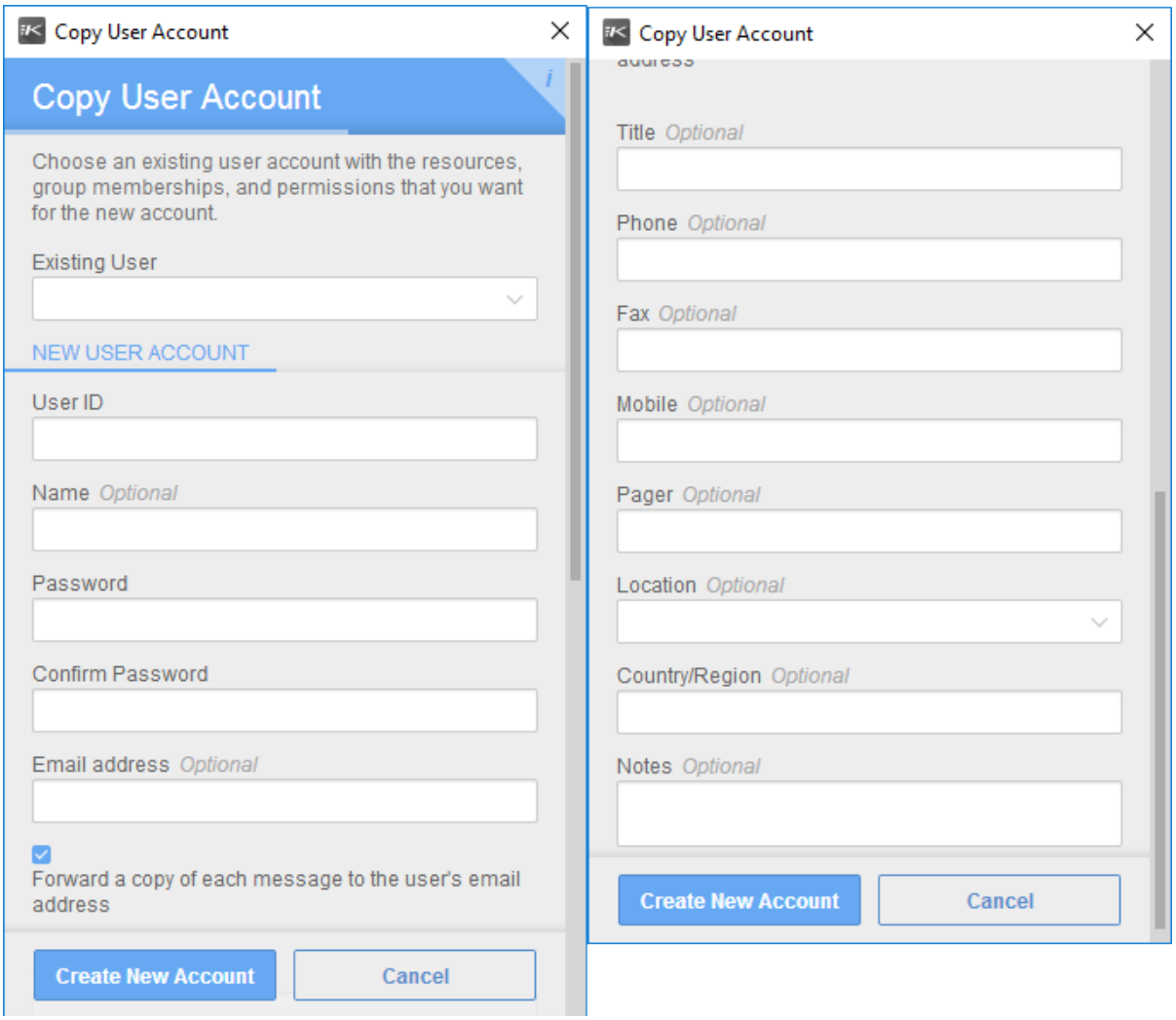
Duplicating a user account

To save time, you can create a new user by duplicating an existing user account. When you duplicate an account, the new user inherits the following from the existing user:

- Permissions the existing user has.
- Memberships to groups the existing user belongs to.
- Access to resources accessible to the existing user.

The user ID, name, email address, profile picture, and contact information for the existing user are not copied. To create the new user, you must at minimum specify a unique ID and password.

You can duplicate a user by using either the Users and Groups workbook from the Administration pane or the Copy User Account form, shown in the illustration below.



Unlike the Users and Groups workbook, the Copy User Account form cannot be used to do the following:

- Copy currency and format settings to the new user account.
- Duplicate an administrator account.
- Copy system administrator settings.
- Share task flows, scorecards, processes, responsibilities, or add-ins directly with the new user.
- Share resources that have been shared directly with the existing user if you do not have the appropriate sharing permissions. For example, if you do not have the Share Workbook permission, no workbooks are shared with the new user even if workbooks have been shared directly with the existing user.

The Copy User Account form can be accessed using the web client, so you can duplicate user accounts when you are away from your desktop.

Note: If your company has established password security requirements, those requirements are displayed in the **Password** text box's tooltip. For more information, see "Setting password security options" on page 648

▸To duplicate a user account from the Administration pane

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** tab, click the user account that you want to duplicate, and then click **Duplicate User** .
3. Specify the user account properties.

▸To duplicate a user account using the Copy User Account form

1. Do one of the following:
   - **Java client**—From the **Explorer**, under **Forms**, double-click **Copy User Account**.
   - **Web client**—Sign in, then open the **Copy User Account** form.
2. From the **Existing User** list, select a user.
   You can also use search if you know the name of the user you want to copy.
3. Specify the user account properties.
4. Click **Create New Account**.

Note: When duplicating a user, RapidResponse processes the request by copying all of the permissions of the user being duplicated to the new user account. Depending on the number of permissions granted to the existing user, the user duplication process might take up to 20 seconds.

Providing the RapidResponse URL and credentials

Once you have created users in your company to access RapidResponse, you will need to provide them with the URL to the sign in page.

On-Demand: The URL for signing in to the Java client is https://rapidresponse.kinaxis.com. The URL for signing in to the web client is https://rapidresponse.kinaxis.com/mobile.

On-Premises: The RapidResponse URL is dependent on where RapidResponse Application Server was installed on your network. For the Java client, it typically it looks like **http://*computername*/rapidresponse/**. For the web client, it typically it looks like **http://*computername*/rapidresponse/mobile**.

You should also ensure that the RapidResponse users you create meet the minimum system requirements outlined in "System requirements for users" on page 541.

In addition, user administrators need to provide the following sign-in credentials to their RapidResponse users:

- company ID (used in On-Demand only)
- user ID
- password

The company ID and user ID are not case sensitive; the password is case sensitive (for example, KINAXIS is not the same as Kinaxis or kinaxis). If users are having trouble signing into RapidResponse, they might have CAPS LOCK enabled on their keyboard.

Adding users to groups

Groups are the primary method through which users are granted permissions and access to resources. When determining which groups a user should be a member of, you must consider the resources and permissions the group has, and compare them to the resources and permissions the user requires.

A new user account will not be a member of any groups. You can add a user to a group by modifying the user's properties. You can review the groups the user already belongs to, and then add the user to other groups.

For a summary of the predefined groups included with RapidResponse, see "Predefined user groups" on page 494.

If you are a system administrator, you can make a user a member of the Data Administrators, User Administrators, System Administrators group, or any other group that has been granted administrative permissions.

If you have a group that has the majority of permissions and resources the user requires, you can add the user to that group, then assign additional resources and permissions to the user. For more information, see "Assigning and removing permissions for a user" on page 554.

▸To add a user to a group

1. In the **New User** or **User Properties** dialog box, click the **Group Memberships** tab.
2. Click **Select Groups**.
3. In the **Select Groups** dialog box, select the groups you want to add the user to, and then click **Select**.

   You can select multiple groups. To select nonadjacent groups, hold down **CTRL**, and then click each group. To select adjacent groups, hold down **SHIFT**, and then click the first and last group in the sequence.
4. Click **OK**.

Note: For security purposes, administrators cannot add themselves to groups.

Assigning and removing permissions for a user

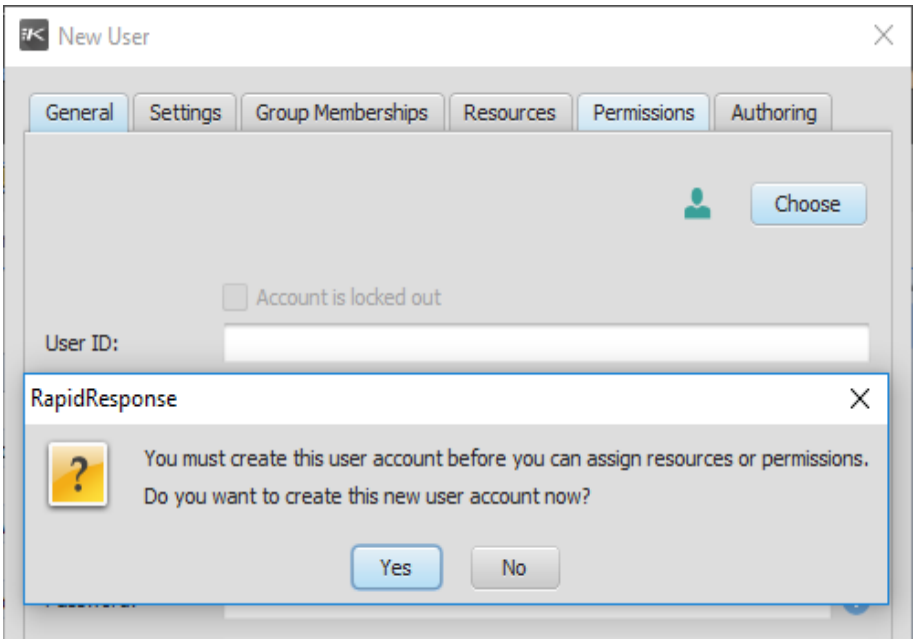
Although it is recommended that you give users access to RapidResponse resources and assign permissions by adding them into appropriate groups, you can give access to resources and assign or remove permissions on an individual basis. Any permissions assigned to or removed from a group always override the permissions previously assigned to or removed from an individual user.

▸Example of overriding permissions

If you assign a group the permission to create scenarios, the users that you add to that group will automatically inherit the permission to create scenarios. If an individual user from that group requires permission to share scenarios, you can assign that permission that will allow the user to be able to share scenarios, in addition to being able to create scenarios. However, if the permission to create scenarios is removed from the group, (since the user is a member of that group) then the user will also lose both the permissions to create scenarios and share scenarios.

Note: You cannot remove resources that were assigned to the user through group membership. To remove resources that were assigned through group membership, you must remove the user from that group.

You can only assign resources or permissions to a user account that has already been created and does not have any unsaved changes made to it. As shown in the image below, if you are creating a new user or have modified options on the Group Memberships tab, when you click the Resources, Permissions, or Authoring tab you will be prompted to create or save the user account first, and then you can continue to edit the Resources, Permissions, or Authoring tab.



If you change permissions for a user who is signed in, the user receives the permission the next time they sign in to RapidResponse.

For more information about the permissions you can assign to a user, see "Assigning and removing permissions" on page 517.

▸To assign a user access to resources

1. In the **New User** or **User Properties** dialog box, click the **Resources** tab.
2. Click **Select Resources**, and then do the following for each resource you want to assign to the user:
   - In the **Show** list, click the resource type you want to assign.
   - Select a resource in the list, and then click **Add**.

     If you are assigning a scenario, click either **View** or **Modify** to determine whether the user can only view data in the scenario or if they can modify it.
3. Click **OK**.

▸To assign or remove permissions for a user

1. In the **New User** or **User Properties** dialog box, click the **Permissions** or **Authoring** tab.
2. Select the check boxes for the permissions you want to assign.

3. Clear the check boxes for permissions you want to remove.
4. Click **OK**.

Limiting visibility of user information

You can limit the visibility of users' names and contact information to selected users. This makes it possible for you to give someone access to a RapidResponse system without automatically providing them access to the other users' personal information. For example, you can provide your suppliers with access to your RapidResponse system to collaborate and plan, without showing information that enables them to identify each other.

There are three visibility levels to choose from:

Visibility level	Can see information about
All (default)	All users
Limited	Self and users with the All visibility level
None	Self only

▸Change the visibility level for a user

1. From the **Administration** pane, under **User Accounts**, select **Users and Groups**.
2. In the **Users** worksheet, click the **User ID** of the user whose visibility level you want to change.
3. In the **User Properties** box, click the **Permissions** tab.
4. Under **Collaboration Tools**, select a different **User Visibility** level.

Caution: Because user IDs are shown in some places instead of names when a user's personal information is blocked, ensure that user IDs do not contain information that should not be available to all users. For more information about how blocked users are handled, see "Places where visibility is limited" on page 556.

Tip: The Visibility setting is available for individual users, but not for groups. If you need to change the visibility level of many users, you can use a script for this task. For more information about scripts, see the *RapidResponse Scripting Guide*.

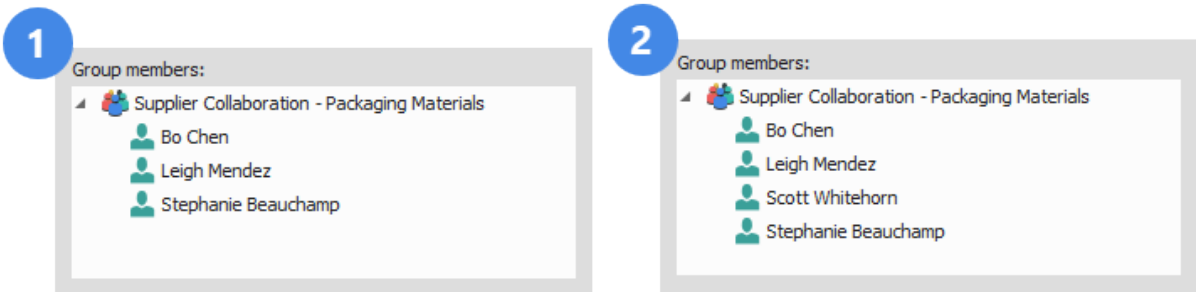
Places where visibility is limited

This section describes what happens when a user with a visibility setting of Limited or None and their ability to view information about another user is blocked as a result. Blocked users are handled differently in different places.

Names omitted from lists

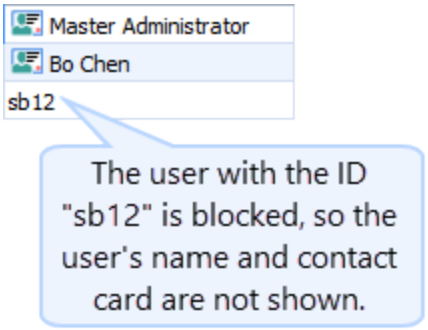
In places where a list of user names is displayed, blocked user names are omitted from the list.

The following image shows what two different users see when they view the list of Supplier Collaboration - Packaging Materials group members. The first user has Limited visibility and cannot see Scott Whitehorn, who also has Limited visibility. The second user has a visibility level of All and can see all of the members of the group.

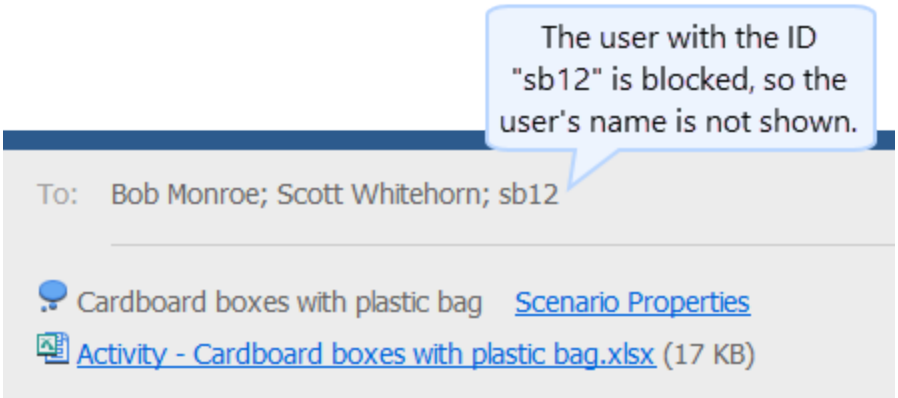


Names replaced with user IDs

When a column is formatted to display user names and contact cards, user IDs without contact cards are shown for blocked users. (This is the same treatment that any text string that is not a valid, current user ID receives.)



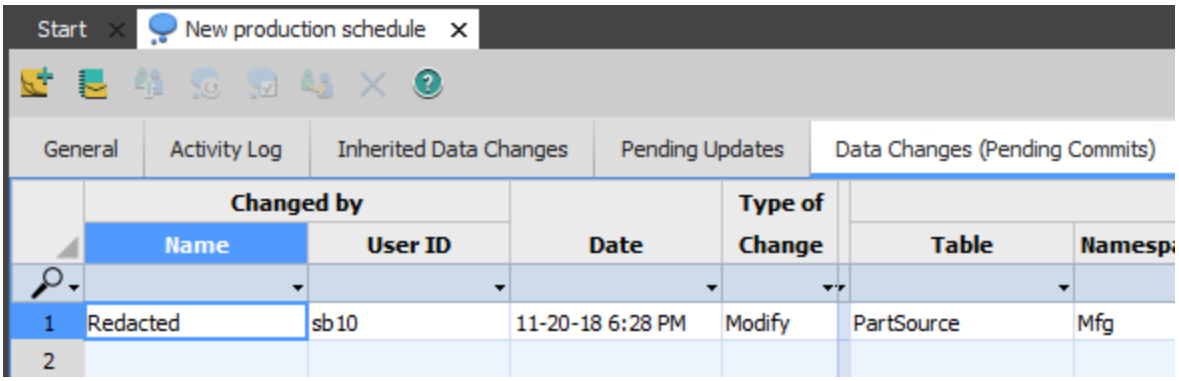
User IDs are also shown for blocked users in some places where user names are normally displayed without contact cards. The following image shows this occurring in Message Center.



User information replaced with "Redacted"

When information about a blocked user, such as an email address, would otherwise be displayed in a column, the text is replaced with "Redacted." This sometimes occurs with user names, depending on how the column is configured.

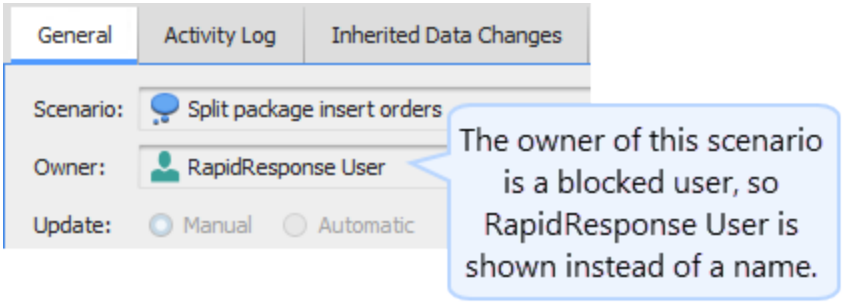
The following image shows an example of this on the Data Changes (Pending Commits) tab of a scenario's properties.



Names replaced with "RapidResponse User"

Where the name of a single user is normally displayed in a dialog box, a blocked user is replaced with the text, "RapidResponse User." Users might see this in the properties of a resource or a scenario.

The following image shows an example of this in a scenario's properties.



Users ignored by scripts

If a script is run using the credentials of a user who has a visibility level of Limited or None, blocked users are omitted from the users collection. The script cannot get information about these users.

Exceptions to limitations on user visibility

Exceptions to limits on user visibility can occur when using automation resources and collaboration.

Automation resources

Depending on how they are configured, alerts and scheduled tasks might make it possible for a user to obtain information about other users that they would not normally have access to. For more information about authoring and running alerts and scheduled tasks, see the *RapidResponse User Guide*.

Alerts

Sometimes, an alert might send a report based on a worksheet that contains user information, such as the names of users in a responsibility column. Visibility of user information in the report depends the permissions of the person whose credentials are used to run the alert, rather than the report recipient. The following are examples of situations where someone can receive a report generated using another user's credentials.

- The alert owner adds other users to the notification list and then runs the alert.
- A shared alert is configured to run using the owner's credentials and sends a report to the person who runs the alert.

Scheduled tasks

Shared scheduled tasks can be configured to run using the credentials of the scheduled task owner when they are run by other users. In these cases, the visibility level of the scheduled task's owner, rather than the visibility level of the person running the task, determines which users can be included in the users collection.

Collaborations

When users are in a collaboration together, they can see the text of other users' comments, which could include names of blocked users (for example, if those users are tagged by another user with social markup) or any other identifying information that is mentioned. For this reason, including users who should not be aware of each other in the same collaboration is not recommended.

Users are warned when they add users who have visibility restrictions to a collaboration.

Specifying default data formats for users

Date, time, number, and currency information displayed in RapidResponse resources (dashboards, workbooks, and scorecards) has formatting applied. For example, number information can be displayed using commas or spaces as thousands separators, or date information can be displayed with a two-digit or four-digit year.

The formats applied to data can be defined by the resource’s author. In resources where the author has not specified a format, the user’s specified format is used.

If your RapidResponse system supports multiple currencies, users can also specify the currency to use when the resource author has not specified the currency to use.

As a RapidResponse user administrator, you can specify the default data formats to use when a resource author has not explicitly specified data formats in a resource. This can only be specified at the user level (not the group level). Additionally, you can specify the user’s currency setting. Users have the option of changing the default data formats and currency assigned to them.

The data formats and currencies available in RapidResponse are controlled by administrators. They also control the default formats for all users. For more information, see "Making data formats available to users and resource authors" on page 663 and "Overview of adding or creating a currency" on page 684.

▸Specify default formats for number, date, time, and currency data

1. In the **New User** or **User Properties** dialog box, click the **Settings** tab.
2. In the **Formats** area, click a format in any of the following lists:
   - Currency
   - Number
   - Date
   - Time

▸Specify the preferred currency for a user

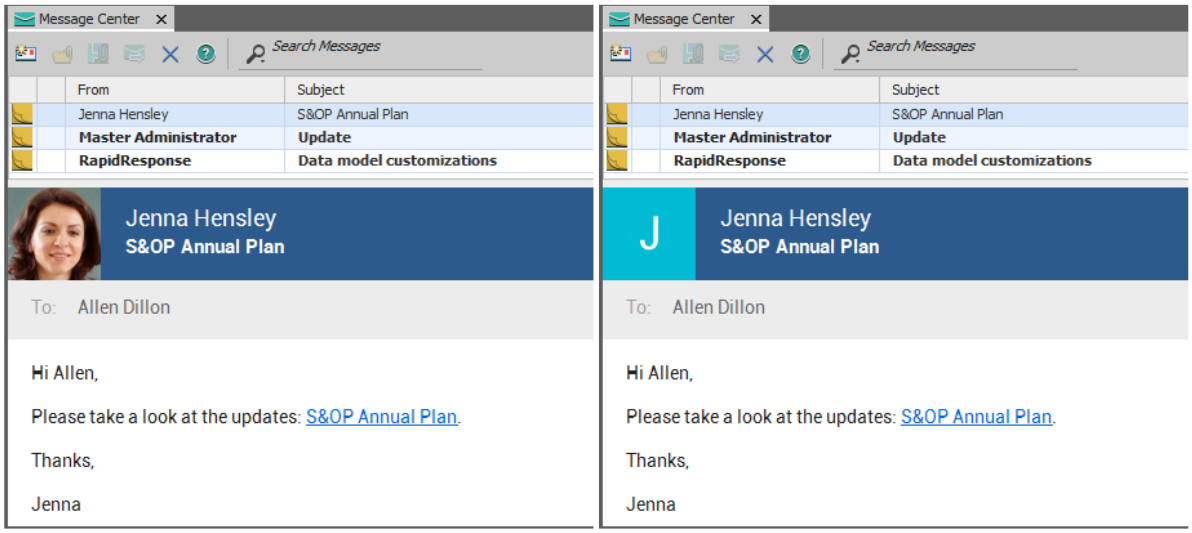
1. In the **New User** or **User Properties** dialog box, click the **Settings** tab.
2. In the **Currency** list, select the user's preferred currency.

> **Tip:** To view information about the currency, currency format, or number format you have selected, click the ··· button beside the currency or format.

Setting profile pictures

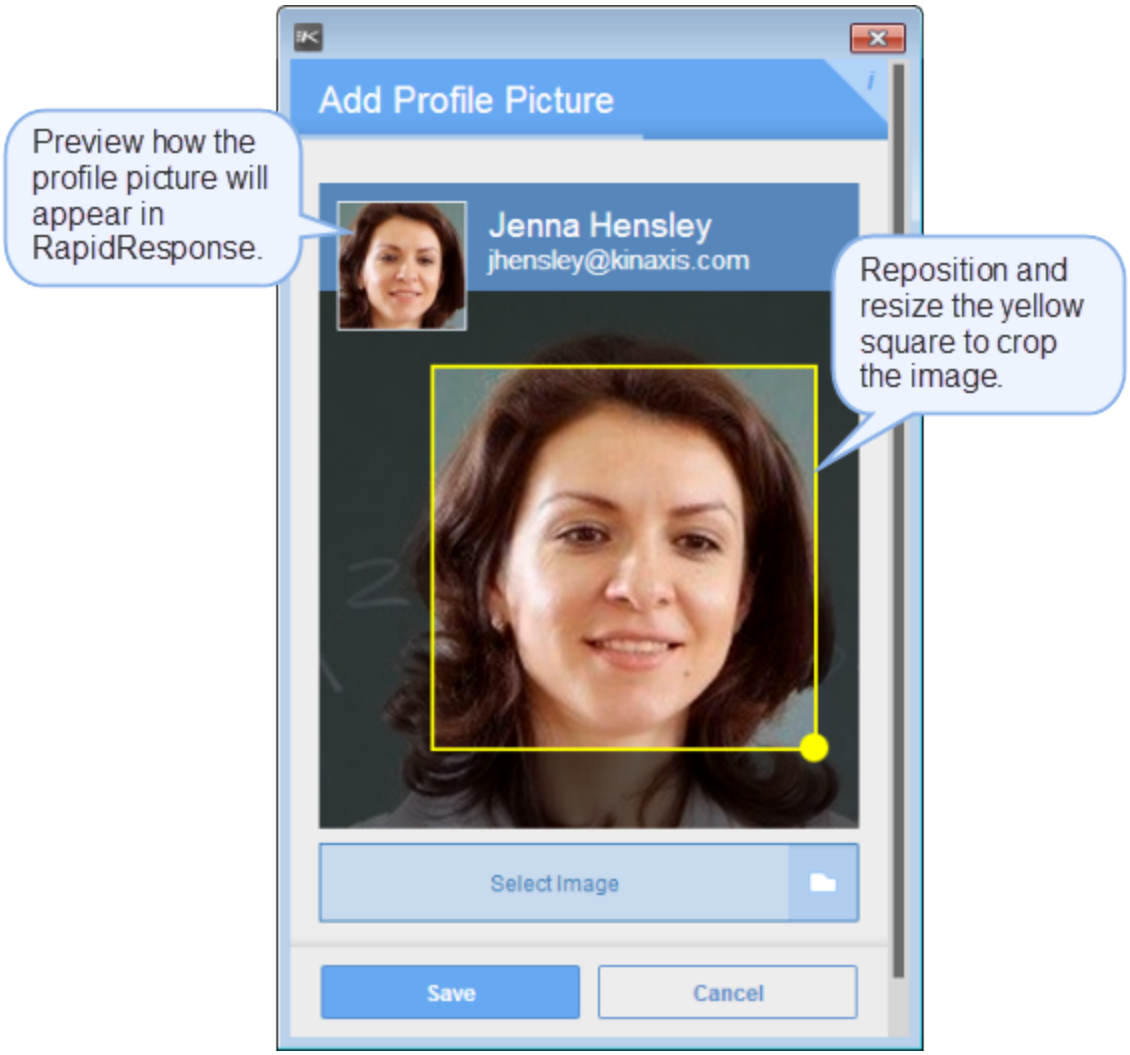
Each RapidResponse user account can display a profile picture, which can help users to more easily recognize the individuals responsible for certain data or key players in collaboration activities.

Profile pictures are displayed in the Java client and the web client. In the web client, they are displayed in the toolbar, contact cards, and collaborations. In the Java client, they are displayed in the toolbar, contact cards, broadcast messages, collaborations, and messages in Message Center. If a profile picture is not set for a user, the first initial of the user's name or user ID is displayed instead. The following image shows how the appearance of a message changes depending on whether the sender's profile picture has been set.



Each user can set their own profile picture, or profile pictures can be set by an administrator from user account properties. To set a profile picture, you upload an image from your computer or network. When

uploaded, you can crop the image using the Add Profile Picture dialog box, shown below. A preview image shows you how the profile picture will appear in RapidResponse.

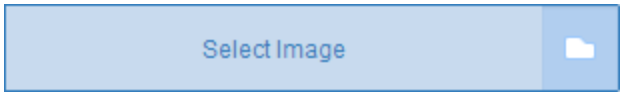


Profile pictures are displayed by default, but they can be turned off. For more information, see " Displaying profile pictures" on page 617.

▸Set or change a user's profile picture

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Select the user whose profile picture you want to change and click **Properties**.
3. In the **User Properties** dialog box, click **Choose**.
4. In the **Add Profile Picture** dialog box, do one of the following:
   - click the Camera button.

- Click the placeholder image in the dialog box.
- Click the **Select Image** button.



5. Locate and select the image file you want to upload and click **Open**.
6. If necessary, resize the dialog box to show the whole image.
7. To change the image you have uploaded, click the **Select Image** button.
8. If necessary, crop the image by doing any of the following:
   - Click within the yellow square and drag it to a different area of the image.
   - Drag the yellow circle inward or outward.
9. Click **Save**.
10. Click **OK**.

Notes:

- You can use the following file types to set a profile picture: BMP, GIF, JPG, JPEG, PICT, PNG, TIFF, WEBP, ICO, JFIF, PJPEG, PJP, SVGZ, TIF, XBM, and SVG.
- The image file size must be 20 MB or smaller.
- You cannot re-crop an image after you have exited the **Add Profile Picture** dialog box. To crop the image differently, you must upload the image again.

▸Remove an uploaded profile picture

1. In the **Administration pane**, under **User Accounts**, click **Users and Groups**.
2. Select the user whose profile picture you want to remove and click **Properties**.
3. In the **User Properties** dialog box, click **Remove**.
4. Click **OK**.

Automatically opening resources upon sign in

If a user uses a dashboard, workbook, scorecard, or task flow frequently, or usually starts with it when they start to work in RapidResponse, you set that it automatically opens each time they sign in.

▸To automatically open a resource upon sign in

1. In the **New User** or **User Properties** dialog box, click the **Resources** tab.
2. In the **On sign in** area, select the **Open** check box, and then click the resource or shortcut.

   The resource lists includes the user's private resources and any resources that have been shared with the user.

Notes:

- This setting is not available to groups.
- If the user has access to only one resource, it will open automatically when they sign in to

RapidResponse.

Users have the option of changing the default resource that opens upon sign in.

Tip: If you want to open a resource with specific data display settings applied, create a shortcut before performing this procedure and select it from the list.

CHAPTER 39: Managing groups and users

Managing groups 565
Managing users 569

After the initial creation of groups and users, you might find it necessary to modify or delete your groups or users. New employees require access to groups, people changing jobs require different resources and permissions, and people leaving the company can be removed from the system.

Depending on the change required, you can change either the user account or the group. For example, if you are adding a user to a group, you can modify the group properties or the user properties.

Managing groups

Many properties of a group can be modified, including its description, owner, members, resources, and permissions. If a group is no longer required, you can delete it.

Editing groups

You can change a group's description, add new members to, or remove members from groups, change the group owner, change the groups that belong to the group, and add, change, or remove the message sent to new group members.

Members removed from a group can no longer access the resources available to the group.

Adding a group to a parent group gives that group inherited access to all the permissions granted to the parent group. Conversely, removing a group from a parent group removes all of the permissions that the child group inherited from the parent group.

You can also modify the resources and permissions assigned to a group. Before modifying the group, you can review which resources and permissions it has. For more information about resources and permissions, see "Creating groups" on page 513.

If you know the name of the group that you want to edit, you can search for the group name instead of scrolling through the group records. For information about searching, see the *RapidResponse User Guide*.

The group's owner will typically be responsible for managing the group. However, any administrator can modify a group.

Note: The group name cannot be changed.

▸To edit the description of a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.

   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Edit or type a new description in the **Description** box.

▸To change the members of a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.

   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Members** tab.
4. To add a member, click **Add Members**, and then in the **Add Members** dialog box, do the following:
   - On the **Users** tab, select a user from the list, and then click **Add**.
   - On the **Groups** tab, select a group from the list, and then click **Add**.
   - Click **OK**.
5. To remove a member, select a group or user in the **Members of this group** list, and then click **Remove**.

Notes:

- You can select multiple groups or users. To select nonadjacent items, hold down **CTRL**, and then click each item. To select adjacent items, hold down **SHIFT**, and then click the first and last item in the sequence.
- If you add a group, that group inherits the parent group's permissions and access to resources. You cannot add a group that the modified group is a member of.
- You can also add a user to a group by modifying the user's properties. For more information, see "Adding users to groups" on page 554.

Tip: To find out more about the users you can add to or remove from the group, move the pointer over their names.

▸To change the owner of a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.

   You can also open the group's properties by clicking the group's name in the **Group** column.
3. In the **Owner** list, click the administrator you want to own the group.

▸To add a message for new group members

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.
   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Members** tab.
4. In the **New member notification** area, select the **Send message to new members** check box.
5. In the **Subject** box, type a subject for the message.
6. In the **Message** box, type the message the new members receive.

▸To change the message sent to new members

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.
   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Members** tab.
4. In the **Subject** box, type a new subject for the message.
5. In the **Message** box, type the new message the new members receive.

▸To remove the message sent to new members

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.
   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Members** tab.
4. In the **New member notification** area, clear the **Send message to new members** check box.

▸To review the resources and permissions assigned to a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.
   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Resources** tab.
4. To change the type of resource listed, in the **Show** list, click the resource type you want to see.
5. To sort the list of resources, click the **Name** or **Resource Type** column headers.
6. To determine how users in the group can access a resource, look at the value in the **Permission** column.
7. Select the **Show component resources** check box to include Linked automation chains, alerts, scheduled tasks, and library workbooks. Selecting this check box also includes widgets with the List permission. For more information about resource sharing permissions, see "Resource permissions" on page 530.
8. To see how the group got access to a resource (such as which parent group the group inherited the resource from), move the mouse over the resource.
9. Review the **Permissions** and **Authoring** tabs.

Any check box that is selected indicates a permission that has been granted to the group. For more information about the permissions, see "Assigning and removing permissions" on page 517.

▸To modify the resources assigned to a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.

   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Resources** tab.
4. To assign a resource, click **Select Resources**, and then do the following for each resource you want to assign to the group:
   - In the **Show** list, click the resource type you want to assign.
   - Select a resource in the list, and then click **Open**, **Author**, or **Manage**.

     If the resource is a scenario, click either **View** or **Modify** to determine whether the users in the group can only view data in the scenario or if they can modify it.
5. If a resource has been directly assigned to the group and you want to remove it, select the resource and then click **Remove**.
6. Click **OK**.

Note: You cannot remove resources that were inherited from a group membership.

▸To grant access to a site

In addition to using the **Resources** tab in the **User Properties** or **Group Properties** dialog boxes, you can also use the **Site Permissions** dialog box to control access to sites.

1. From the **Administration** pane, under **User Accounts**, click **Site Permissions**.
2. In the **Site Permissions** dialog box, select the site you want to assign access to.
3. Click **Select Names**.
4. In the **Select Names** dialog box, select the users and groups you want to assign access to, and then click **Share With**.
5. Click **OK**.

Note: Only system administrators and user administrators can grant access to a site. If you are a data administrator, you must contact a system administrator or user administrator and request that they grant access to the site.

▸To modify the sharing permission of a scenario

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.

   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Resources** tab.
4. In the **Show** list, click **Scenarios**.

5. In the **Permission** column, click one of the following:
   - **View only**—Allows users in the group to only view data in the scenario.
   - **Modify**—Allows users in the group to modify data in the scenario.

▸To modify the permissions granted to a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group, and then click **Properties** on the Users and Groups toolbar.

   You can also open the group's properties by clicking the group's name in the **Group** column.
3. Click the **Permissions** or **Authoring** tab.
4. Select the check boxes for the permissions you want to grant.
5. Clear the check boxes for permissions you want to deny.
6. Click **OK**.

Caution: Denying a permission also denies it for all groups that are members of this group. If the permission is denied, it cannot be granted to the members.

Note: For complete information about the permissions that can be granted to a group, see "Assigning and removing permissions" on page 517.

Deleting groups

When you delete a group, the members of the group no longer have the permissions or access to resources provided to the group. Deleting a group does not delete the members within the group. For information about deleting users, see "Deleting user accounts" on page 573. For information about permissions, see "Creating groups" on page 513.

Deleting a group does not delete any of the group's resources. If these resources are not used by other groups, you can delete them. For more information about deleting resources, see the *RapidResponse User Guide* and the *Rapidresponse Author Guide*.

▸To delete a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, select a group.
3. Click **Delete** ✕.

Managing users

You can modify any property of a user, except their user ID. If the user account is no longer required, you can delete it and free up a RapidResponse user license.

Editing user accounts

You can edit the details about a user, such as the user's password, email address, user type, license type, profile picture, or contact information.

You can add a user to or remove a user from a group.

If you know the name of the user whose account you want to edit, you can search for the user name or ID instead of scrolling through the user accounts. For information about searching, see the *RapidResponse User Guide*.

If you change the user's license type from Internal to Alert, any private resources the user owns will not be accessible. If any of the user's private resources are required, you can give them to another user before changing the user's license type (you can change the user's password, sign in as the user, and then give the resources). For more information about license types, see "Understanding user accounts and license types" on page 539.

However, any shared resources the user owns will remain available to the users that the resource has been shared with, and the resources can be shared or modified by any administrator.

If you need to change a user's password only, you can do so quickly by using the Reset User Account form. This form is also available on your mobile device. For more information about the Reset User Account form, see "Unlocking a user account" on page 599.

▸To edit user details

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. On the **General** tab, change the settings or contact information.
4. Click **OK**.

Note: The user ID cannot be modified.

▸To add a user to a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. Click the **Group Memberships** tab.
4. Click **Select Groups**.
5. In the list, select the group to which you want to add the user, and then click **Select**.

   You can select multiple groups. To select nonadjacent groups, hold down **CTRL**, and then click each group. To select adjacent groups, hold down **SHIFT**, and then click the first and last group in the sequence.
6. Click **OK**.

▸To remove a user from a group

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. Click the **Group Memberships** tab.
4. In the **Member of groups** list, click the group from which you want to remove the user, and then click **Remove**.

   You can select multiple groups. To select nonadjacent groups, hold down **CTRL**, and then click each group. To select adjacent group, hold down **SHIFT**, and then click the first and last group in the sequence.

▸To review the resources and permissions assigned to a user

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. Click the **Resources** tab.
4. To change the type of resource listed, in the **Show** list, click the resource type you want to see.
5. To sort the list of resources, click the **Name** or **Resource Type** column headers.
6. To determine how the user can access a resource, look at the value in the **Permission** column.
7. To see the linked resources the user has access to, select the **Show component resources** check box.
8. To see how the user got access to a resource (such as which group the user inherited the resource from), move the mouse over the resource.
9. Review the **Permissions** and **Authoring** tabs.

   Any check box that is selected indicates a permission that has been granted to the user. For more information about the permissions, see "Assigning and removing permissions" on page 517.

▸To modify the resources assigned to a user

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. Click the **Resources** tab.
4. To assign a resource, click **Select Resources**, and then do the following for each resource you want to assign to the user:
   - In the **Show** list, click the resource type you want to assign.
   - Select a resource in the list, and then click **Open**, **Author**, or **Manage**.

     If the resource is a scenario, click either **View** or **Modify** to determine whether the user can only view data in the scenario or if they can modify it.
5. If a resource has been directly assigned to the user and you want to remove it, select the resource and then click **Remove**.
6. Click **OK**.

Note: You cannot remove resources that were assigned to the user by a group membership.

▸To grant access to a site

In addition to using the **Resources** tab in the **User Properties** or **Group Properties** dialog boxes, you can also use the **Site Permissions** dialog box to control access to sites.

1. From the **Administration** pane, under **User Accounts**, click **Site Permissions**.
2. In the **Site Permissions** dialog box, select the site you want to assign access to.
3. Click **Select Names**.
4. In the **Select Names** dialog box, select the users and groups you want to assign access to, and then click **Share With**.
5. Click **OK**.

Note: Only system administrators and user administrators can grant access to a site. If you are a data administrator, you must contact a system administrator or user administrator and request that they grant access to the site.

▸To modify the sharing permission of a scenario

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. Click the **Resources** tab.
4. In the **Show** list, click **Scenarios**.
5. In the **Permission** column, click one of the following:
   - **View only**—Allows the user to only view data in the scenario.
   - **Modify**—Allows the user to modify data in the scenario.

▸To modify the permissions granted to a user

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, select a user, and then click **Properties** on the Users and Groups toolbar.

   You can also open the user properties by clicking the user's identifier in the **User ID** column.
3. Click the **Permissions** or **Authoring** tab.
4. Select the check boxes for the permissions you want to grant.
5. Clear the check boxes for permissions you want to deny.
6. Click **OK**.

Note: For complete information about the permissions that can be granted to or denied from a user, see "Assigning and removing permissions" on page 517.

▸To set a new password using the Reset User Account form

1. Do one of the following:
   - **Java client**—From the **Explorer**, under **Forms**, double-click **Reset User Account**.
   - **Web client**—Sign in, then open the **Reset User Account** form.

For more information about signing in to the web client, see "Providing the RapidResponse URL and credentials" on page 553.

2. From the **User Account** list, select a user.

   If you are changing the password of a user that is not locked out of their account, make sure the **List only locked out users** check box is not selected.

3. Click **Reset User Account**.

Note: If your company has established password security requirements, those requirements are displayed in the **New Password** field's tooltip. For more information, see "Setting password security options" on page 648

Deleting user accounts

If the user account is no longer required, you can delete it and free up a RapidResponse user license. You can monitor when users last signed in to RapidResponse. This helps you determine if any user accounts are obsolete and should be deleted.

Before you attempt to delete any user accounts, you should be aware of the following results:

- All private resources and private scenarios are deleted along with a user. If any of the user's private resources are required, you can give them to another user before deleting the user (you can change the user's password, sign in as the user, and then give the resources).
- Shared or public resources owned by the deleted user are transferred to the administrator who deleted the user. The resources can be subsequently shared, modified or deleted by any administrator.
- Ownership of shared scenarios owned by the deleted user are transferred to the RapidResponse Master Administrator.
- If you delete a user that has been assigned responsibility for data, that data becomes the responsibility of whoever is designated in the responsibility definition as the user responsible for unassigned items, unless those items belong to a category in which a different user is designated as responsible for all unassigned items. For more information about making users responsible for unassigned items, see the *RapidResponse Resource Authoring Guide*.
- If you delete a user account that is defined for a subscriber, the subscriber is also deleted. Prior to deleting a user that's defined for a subscriber, define a different user for the subscriber. For more information, see "Defining subscribers" on page 892.
- You cannot delete your own user account, or that of any user with an active connection to RapidResponse. For information about disconnecting users, see "Disconnecting users from RapidResponse" on page 601.
- You cannot delete any administrator who owns a group, and only system administrators can delete other administrator accounts. You cannot delete the Master Administrator (Admin) user (On-Premises only).

▸To determine when a user signed in last

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, review the information in the **Last Sign In** column.

Note: Occasionally, the **Last Sign In** column might be blank for some users. This indicates that the user has not signed in to RapidResponse.

▸To delete a user account

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** tab.
3. Select a user, and then click **Delete** ✕. Ensure that the entire row is selected by clicking the row number.

CHAPTER 40: Reviewing resource assignments

About the Resource Permissions workbook 575
Understanding access permissions 579
Reviewing resource assignments by group 582
Reviewing resource assignments by user 585
Reviewing resource assignments by resource 587
Example: Investigating a resource assignment 590

As a user administrator, you might need to review or audit the resources that users and groups on your RapidResponse system have access to and the access permissions of those resources. You can accomplish this with the Resource Permissions workbook, which is available from the Administration pane.

For example, you can use the Resource Permissions workbook to review assignments to determine whether users or groups have received access to a resource they should not have or if a resource has been shared with users outside of their group memberships. You can also find all of the users or groups that have access to a particular resource. You can correct any assignment errors by modifying user or group properties directly from a worksheet.

Additionally, you have the option of exporting text-only versions of the reports provided by the Resource Permissions workbook, which are more suitable for use outside of RapidResponse.

About the Resource Permissions workbook

You can use the Resource Permissions workbook to review resource assignments and ensure that the correct resources are available to each user and group. You can configure the settings for each worksheet to suit your needs and, if you require this information for auditing purposes, you can export the reports. This workbook is available from the Administration pane.

The Resource Permissions workbook includes eight worksheets. Depending on the worksheet, you can find the information you need by using the reference point (group, user, or resource) that is most useful to you. For example, you can select the name of a group to display the group's members or the group's resources. You can select a user to display the resources they can access or the groups they are a member of. Or, you can select a type of resource to display the groups or users that can access resources of that type. To figure out which worksheet is best suited to the task you want to accomplish, see "Determining the worksheet to use" on page 578.

Resources are typically shared with users through group memberships. If you notice that a resource has been shared with a user outside of their group memberships, you can investigate how the user received this permission in the Sharing Details worksheet. Several worksheets included in the Resource

Permissions workbook link to this worksheet. For more information about the Sharing Details worksheet, see "Understanding access permissions" on page 579.

If you find a resource assignment error, such as a user or group that received permission to access a resource they should not have, you can open the user or group properties directly from a worksheet to correct the error. For more information, see "Editing user accounts" on page 570 and "Editing groups" on page 565.

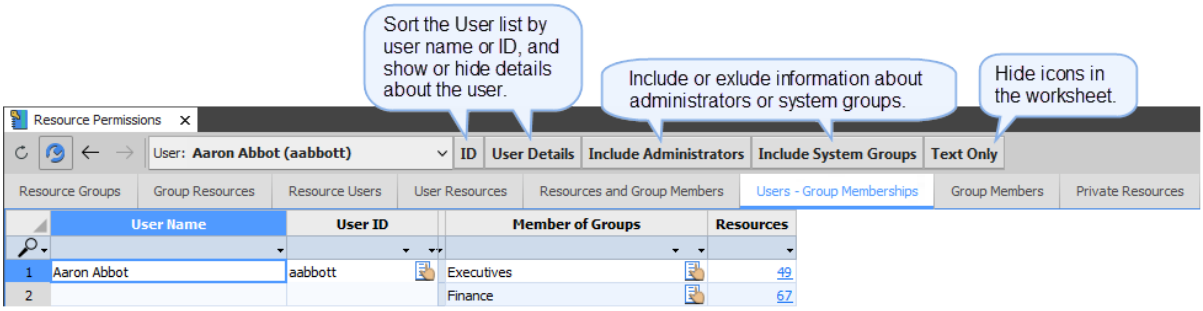
Resources must be added to the versioned repository for them to appear in most of the worksheets in this workbook. The Private Resources worksheet displays all private resources on your RapidResponse system.

Configuring worksheet data settings

Because administrators have permission to access all resources, you have the option to include or exclude administrator users in any worksheet that provides information about users. Similarly, you can include or exclude information about system groups in all worksheets that provide information about groups except for the Resources and Group Members worksheet.

You might also be able to view a text-only version of a worksheet by clicking Text Only in the toolbar. This hides any image columns in the worksheet, improving the legibility of the report and rendering it more suitable for export and use outside of RapidResponse.

In worksheets where you can select which user you want to view information about, you can control whether the User list is sorted by user name or ID by clicking ID on the toolbar. Also, by clicking User Details, you can view extra details about the selected user. You can show or hide the user's email address, license type, title, location, and whether the user is an administrator.



In addition to using workbook toolbar buttons to control the information displayed in each worksheet, you can modify settings using the Data Settings dialog box. The table below describes the data settings you can change in the dialog box, which you open by clicking Data Settings on the workbook toolbar.

Data setting	Description
Worksheet	The worksheet you want to view.
Show	The type or category of resources you want to view information about. This includes scenarios.
Group	The group you want to view information about. Groups with no members are not displayed.
User	The user you want to view information about.
ID	Whether the User list is sorted by user names or IDs. If you change this setting after you have already selected a user, a red x appears beside the name or ID of the selected user and information might not appear in the worksheet. Select the user again to display information.
Include Administrators	Whether administrator users are included in or excluded from worksheets that provide information about users.
Include System Groups	Whether system groups are included in or excluded from worksheets that provide information about groups.
Text Only	Whether the worksheet displays icons. Use the Text Only view when printing or exporting worksheet data. The image columns are hidden so the report is suitable for use outside of RapidResponse.
Resources and Group Members	
Group	In the Resources and Group Members worksheet, the group you want to view information about. Resource access permissions will be shown for the users in this group. Groups with no members are not displayed.
Include unassigned resources	In the Resources and Group Members worksheet, whether resources that are not assigned to members of the selected group are displayed.
Users - Group Memberships	
User Details	In the Users - Group Memberships worksheet, whether some details about users are shown or hidden. You can show or hide the user's email address, license type, title, location, and whether the user is an administrator.

Configuring worksheet data settings for auditing

You can audit the resource assignments of users and groups on your RapidResponse system by regularly exporting the reports generated by the Resource Permissions workbook. Consider creating an alert that automatically generates these reports. For more information, see the *RapidResponse User Guide*.

When you export information from the Resource Permissions workbook for auditing purposes, it is recommended that you use the following data settings:

- **Show**—All users, all groups, or all resources (depending on the worksheet). This provides a complete picture of the resource assignments on your system.

  It is possible that using this setting will result in the worksheet record limit being exceeded. In this case, you will need to generate multiple reports. For example, show only one type of resource or only one group in each report. You might also be able to use column search to achieve the results you want.
- **Include Administrators**—Yes. The report should include all users on your RapidResponse system.
- **Text Only**—Yes. The icons that appear in image columns in the worksheets are not useful in exported reports.

Determining the worksheet to use

Each worksheet in the Resource Permissions workbook is designed to provide particular information about resource permissions, thereby helping you to perform a certain task. Use the following table to determine which worksheet is best suited to the task you want to accomplish.

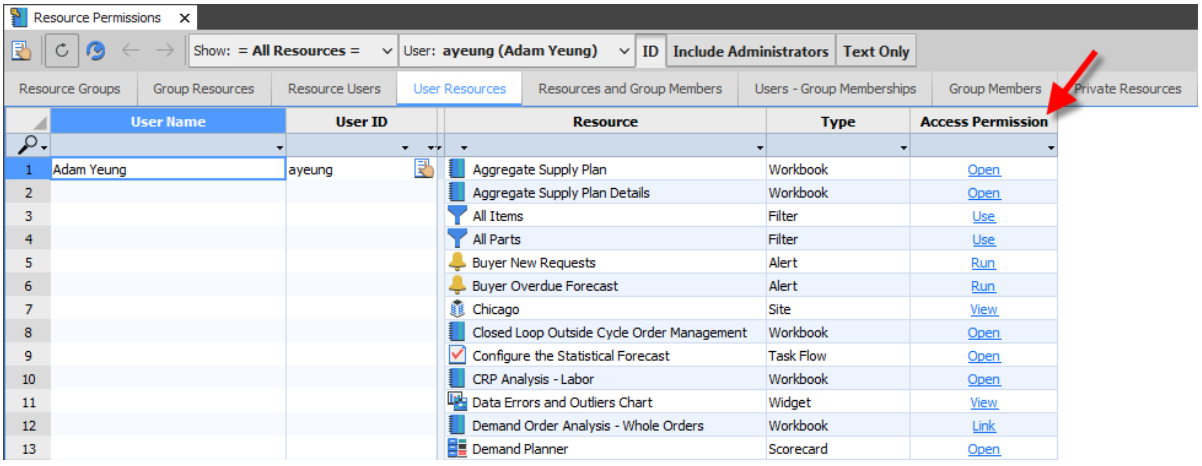
Task	Worksheet
For a group:	
View the resources that the group has access to.	"Group Resources worksheet" on page 583
View how each group member can access their resources.	"Resources and Group Members worksheet" on page 583
View the members of the group.	"Group Members worksheet" on page 584
For a user:	
View the resources that the user has access to.	"User Resources worksheet" on page 586
View the groups they are a member of.	"Users - Group Memberships worksheet" on page 586

Task	Worksheet
For a type of resource:	
View the groups that have access to resources of that type.	"Resource Groups worksheet" on page 588
View the users that have access to resources of that type.	"Resource Users worksheet" on page 588
View the private resources of that type on your system.	"Private Resources worksheet" on page 589

You can also use the Resources and Group Members worksheet to view resources that have not been assigned to any users. For more information, see "Reviewing unassigned resources" on page 584.

Understanding access permissions

The Resource Users and User Resources worksheets in the Resource Permissions workbook include an Access Permission column, which tells you how a user is allowed to use a resource. Access permissions can vary depending on the type of resource. For example, if you share a workbook with a user, the access permission the user has for the workbook is Open (the user can open the workbook from the Explorer). If you share an alert with a user, the access permission the user has for the alert is Run (the user can run the alert from the Explorer).



The Resources and Group Members worksheet also displays access permissions for each member of a group.

Show: = All Resources = | Group: Buyers - North America

Resource Groups | Group Resources | Resource Users | User Resources | Resources and Group Members | Users - Group Memberships | Group Members | Private Resources

	Resource	Type	Access Permission by User						
			awashington	ayeung	bball	gduncan	ldossantos	mgray	pmann
1	Aggregate Supply Plan	Workbook	Open	Open	Open	Open	Open	Open	Open
2	Aggregate Supply Plan Details	Workbook	Link	Link	Link	Link	Link	Link	Link
3	All Items	Filter	Use	Use	Use	Use	Use	Use	Use
4	All Parts	Filter	Use	Use	Use	Use	Use	Use	Use
5	Attribute Rules	Workbook	Open	Open	Open	Open	Open	Open	Open
6	Buyer New Requests	Alert	Run	Run	Run	Run	Run	Run	Run

When you click an access permission link in any of these worksheets, you open the Sharing Details worksheet. This worksheet provides details about how the user received the permission to access the resource. For more information, see "Determining how a resource was shared" on page 581.

Users can access resources in the following ways:

- **Open**—The user can open the resource from the Explorer. This permission applies to reports (dashboards, workbooks, and scorecards), tasks (forms, processes, responsibilities, and task flows), and linked resources that have been shared with a task flow or process.
- **Use**—The user can use these resources with openable resources such as dashboards and workbooks. Applies to filters and hierarchies.
- **Manage**—The user owns the resource. Users that own the resource can modify, share, or delete it. Administrators with the appropriate permission also have a Manage permission associated with the resource. This permission applies to all resource types except for sites. System and user administrators can grant users this access.
- **View**—This permission applies to scenarios, sites, widgets, and add-ins. For scenarios and sites, the user can view data using the resource. In the case of widgets, it means the widget has been shared with the user.
- **Modify**—This permission applies only to scenarios. A user with this permission can view and modify data in the scenario. System and user administrators can grant users this access.
- **Run**—The user can perform the actions defined in the resource. Applies to alerts, scheduled tasks, automation chains, and scripts.
- **List**—This permission only applies to widgets. When a dashboard is shared with a user, the dashboard's widgets are also shared using the List permission. Users with dashboard authoring permissions can use widgets shared in this manner in their own dashboards. These widgets are not listed in the Explorer, but they are listed in the Widgets list when the user is authoring a dashboard.
- **Link**—The user can open the resource by clicking a link in another resource. Applies to dashboards, workbooks, scorecards, forms, alerts, scheduled tasks, automation chains, and scripts. A linked resource can be opened only from another resource and is not displayed in the user's Explorer. Some linked resources, such as library workbooks, cannot be accessed by the user and are only linked to provide data for another resource.
- **Full**—The user owns the resource. Users that own the resource can modify, share, or delete it. Applies to sites. Administrators with the appropriate permission also have a Full permission associated with the site and can give or remove access to it.

The following table summarizes the RapidResponse resources that can be linked.

Main resource	Can link to
Alerts	• Workbooks • Scorecards
Automation chain	• Alerts • Automation chains • Scheduled tasks
Form	• Scripts
Process	• Dashboards • Workbooks • Scorecards • Forms
Script	• Scripts • Workbooks • Forms
Scorecard	• Workbooks
Scheduled task	• Scripts • Workbooks
Task flow	• Dashboards • Scorecards • Workbooks • Forms • Task flows
Widget	• Dashboards • Scorecards • Workbooks • Forms • Task flows
Workbook	• Scripts • Workbooks • Forms

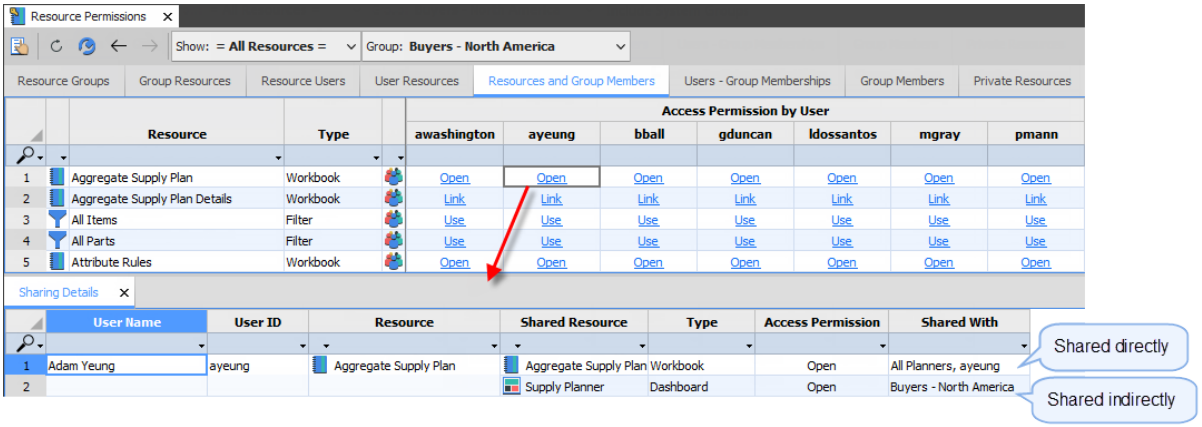
Note: Most of these resource types are dependent resources and are required by the shared resource to function.

Determining how a resource was shared

Details about how a user was given access to a resource are displayed in the Sharing Details worksheet. You might examine this worksheet if, for example, you notice that a user has access to a resource

outside of their group memberships and you want to verify that this is not an error.

You open this worksheet by clicking a link in the Resource Users, User Resources, or Resources and Group Members worksheet in the Resource Permissions workbook. You can view details about any user and resource.



For a resource, any resources that it is linked from are listed in the Shared Resource column of the worksheet. If the resource was shared directly with the user or any group the user is a member of, only that resource is displayed in the worksheet.

The Shared With column lists all of the groups the user is a member of that the resource has been shared with. If the resource was shared directly with the user, the user's name or ID is also listed as a way the user gained access to the resource.

In the above image, the worksheet indicates that the Aggregate Supply Plan workbook was shared directly with the user. The workbook was also shared directly with the All Planners group, which the user is a member of. Additionally, the user has indirect access to the workbook through the Supply Planner dashboard, which was shared with the Buyers - North America Group.

If you notice that the Shared With column contains a group name that the user should not be a member of, modify the group properties to remove that user. Or, if the column contains the user's name but the resource should not be shared with that user, either modify the user's properties or the resource's sharing properties.

Note: A Manage or Full access permission level indicates that the user owns the resource or that the user is an administrator. Manage and Full permissions do not display as links in the worksheets.

Reviewing resource assignments by group

The following worksheets allow you to select a group to view information about the group's resources, the group's members, and how the group's members can access each resource.

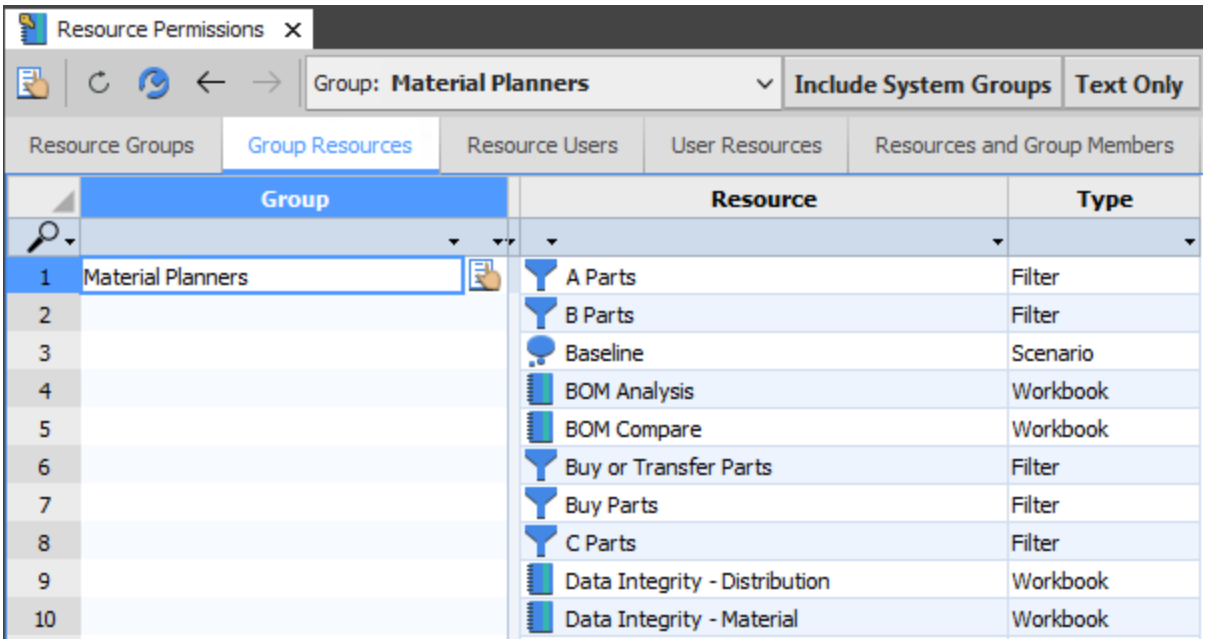
- "Group Resources worksheet" on page 583
- "Resources and Group Members worksheet" on page 583
- "Group Members worksheet" on page 584

You can review resource assignments for all groups or a particular group by selecting from the Group list on the workbook toolbar. You can include or exclude system groups in a worksheet by clicking Include System Groups. You can also make these changes from the workbook's data settings. For more information, see "Configuring worksheet data settings" on page 576.

Groups with no members are not included in any worksheets in the Resource Permissions workbook.

Group Resources worksheet

The Group Resources worksheet lists the resources that a group has access to. These include resources that have been shared with the group directly and indirectly.



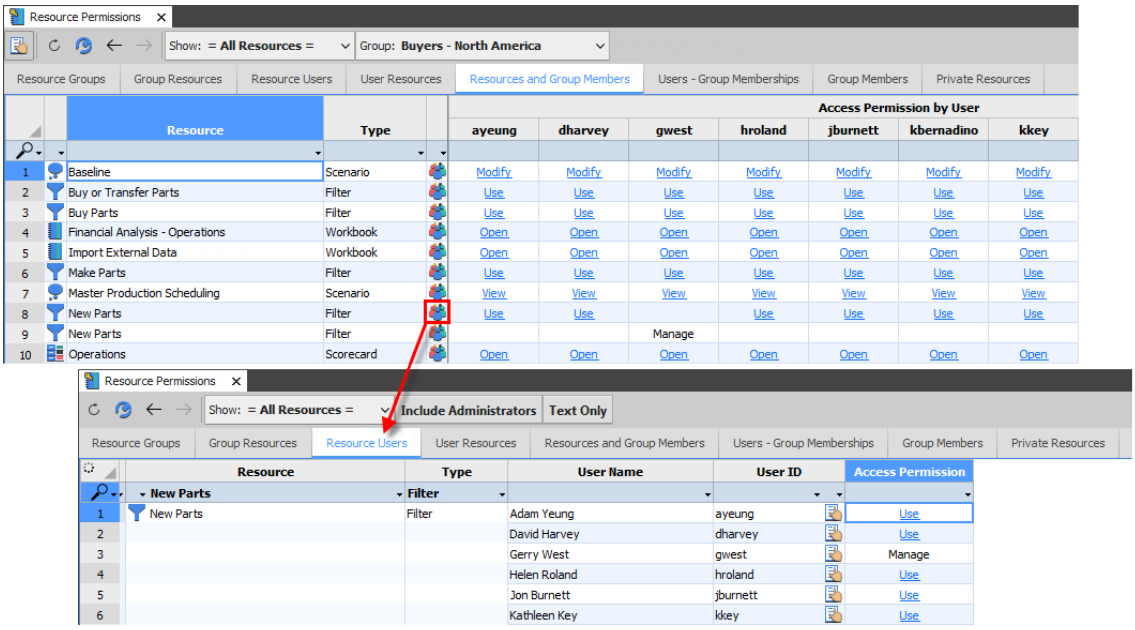
You can open the properties of any group listed in the worksheet by selecting the row and clicking Group Properties on the workbook toolbar or by clicking the Group Properties button beside the group's name.

If you are exporting this worksheet, click Text Only on the toolbar. This hides any image columns in the worksheet.

Resources and Group Members worksheet

The Resources and Group Members worksheet lists the members of a group and the access permission levels for the resources that group members have access to. By clicking an access permission link, you open the Sharing Details worksheet. This worksheet provides more information about how the resource became available to the user. For more information, see "Understanding access permissions" on page 579.

For any resource listed in the worksheet, you can click the Show list of resource users button to open the Resource Users worksheet. This worksheet opens to display all of the users who have access to that resource. For more information, see "Resource Users worksheet" on page 588.



You can open the properties of any group listed in the worksheet by selecting the row and clicking Group Properties on the workbook toolbar.

> **Note:** Users with administration permission are not included in this worksheet. Groups with administration permission are omitted from the Group list.

Reviewing unassigned resources

In addition to viewing which users have access to resources, you can use the Resources and Group Members worksheet to view all resources that have not been assigned to users. Unassigned resources are represented as rows that have blank values in the user columns.

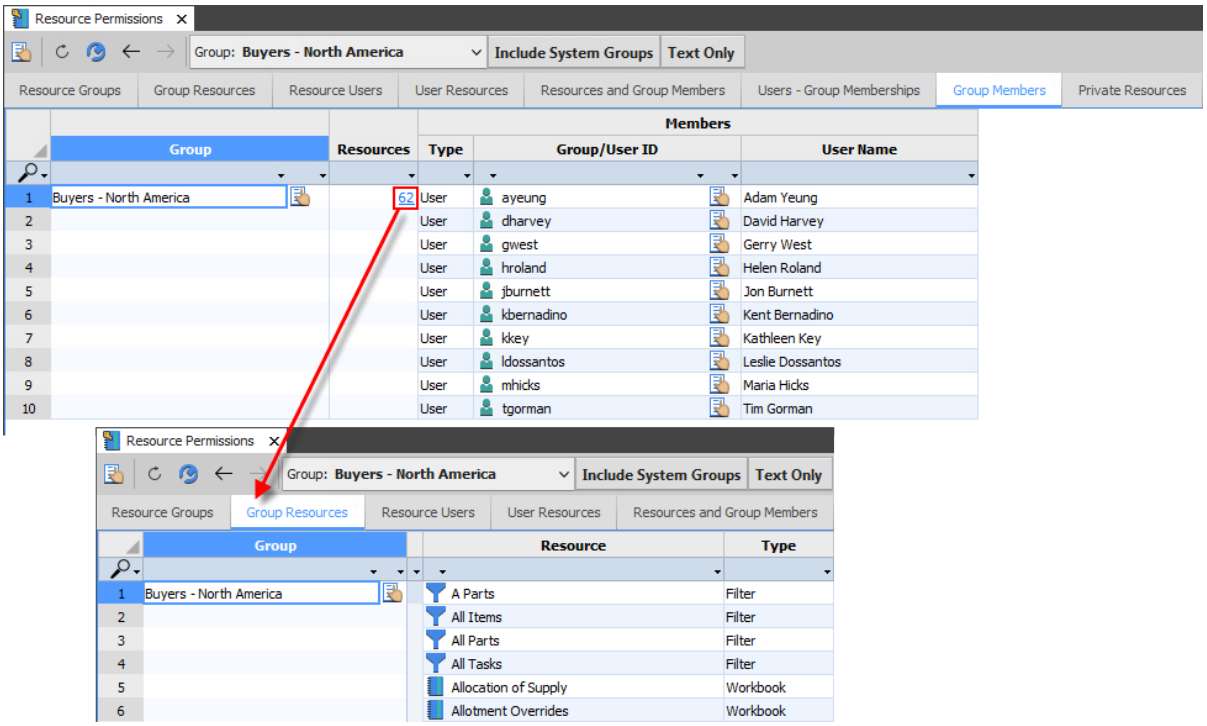
You can view the unassigned resources to determine which resources are needed by a group or user and then modify the group or user properties to assign that resource. If you are intending to delete resources, you can view the unassigned resources to determine which ones are not needed.

You view unassigned resources by clicking Data Settings in the workbook toolbar and selecting Yes in the Include unassigned resources list. For more information about data settings, see "Configuring worksheet data settings" on page 576.

Group Members worksheet

The Group Members worksheet lists the users and groups that are direct members of a group. The Resources column provides counts of the number of resources that have been shared with the group.

By clicking a link in this column, you open the Group Resources worksheet, which displays more information about the shared resources.



You can open the properties of any user or group listed in the Group Members worksheet by clicking the User or Group Properties button beside the user's ID or group name. You can also open a group's properties by selecting a record and clicking Group Properties on the workbook toolbar.

If you are exporting this worksheet, click Text Only on the toolbar. This hides any image columns in the worksheet.

Reviewing resource assignments by user

The following worksheets allow you to select a user to view information about the user's resources and group memberships.

- "User Resources worksheet" on page 586
- "Users - Group Memberships worksheet" on page 586

You can review resource assignments for all users or a particular user by selecting from the User list on the workbook toolbar. You can control whether the User list is sorted by user names or IDs by clicking ID. You can include or exclude administrator users in a worksheet by clicking Include Administrators.

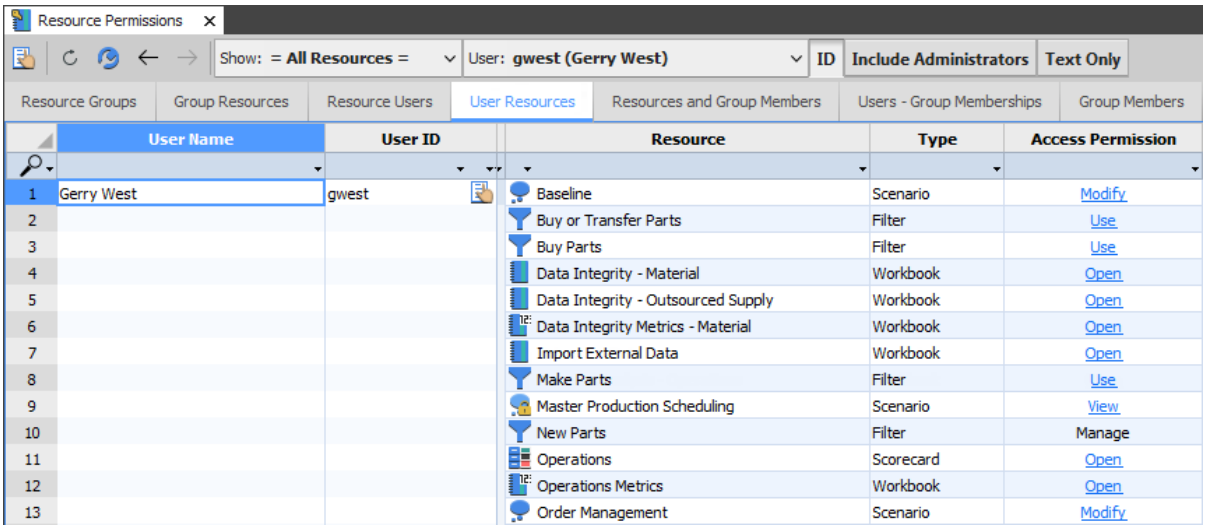
If you are exporting the worksheet, click Text Only on the toolbar. This hides any image columns in the worksheet.

You can also make these changes from the workbook's data settings. For more information, see "Configuring worksheet data settings" on page 576.

User Resources worksheet

The User Resources worksheet lists the resources that a user has access to. These include resources from all groups the user is a member of, that have been shared directly with the user, and that the user owns.

The Access Permission column tells you how a user is allowed to use each resource. Clicking a link in this column opens the Sharing Details worksheet, which provides details about how the resource became available to the user. For more information, see "Understanding access permissions" on page 579.

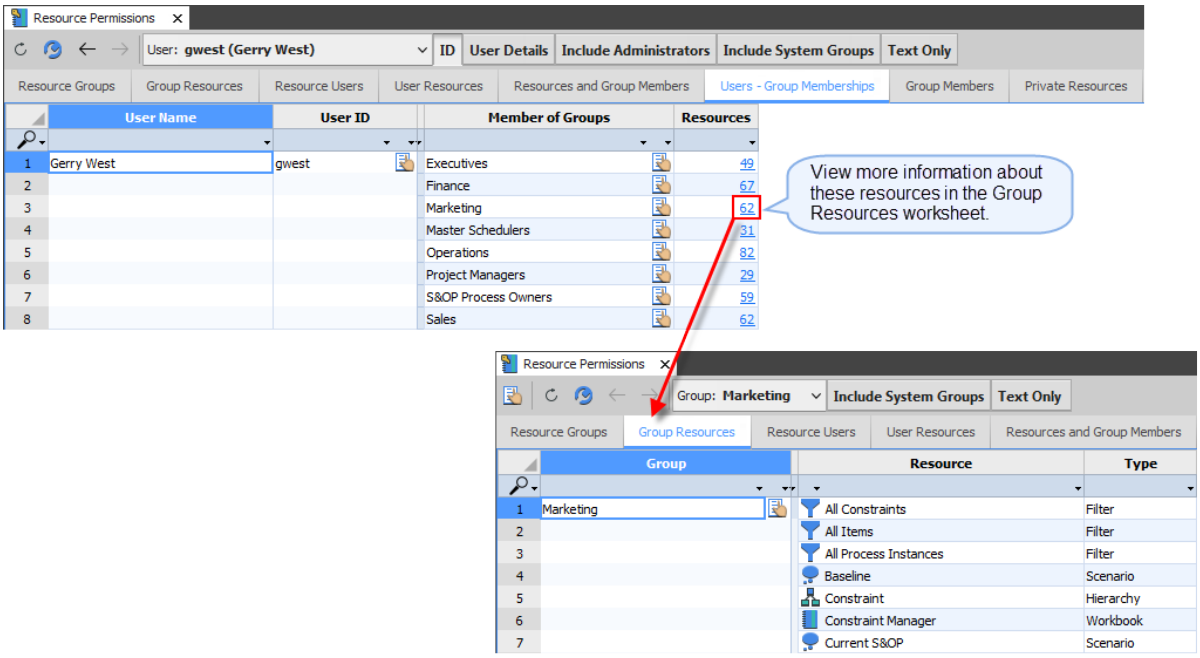


	User Name	User ID	Resource	Type	Access Permission
1	Gerry West	gwest	Baseline	Scenario	Modify
2			Buy or Transfer Parts	Filter	Use
3			Buy Parts	Filter	Use
4			Data Integrity - Material	Workbook	Open
5			Data Integrity - Outsourced Supply	Workbook	Open
6			Data Integrity Metrics - Material	Workbook	Open
7			Import External Data	Workbook	Open
8			Make Parts	Filter	Use
9			Master Production Scheduling	Scenario	View
10			New Parts	Filter	Manage
11			Operations	Scorecard	Open
12			Operations Metrics	Workbook	Open
13			Order Management	Scenario	Modify

You can open the properties of any user listed in the worksheet by selecting the row and clicking User Properties in the workbook toolbar or by clicking the User Properties button beside the user's ID.

Users - Group Memberships worksheet

The Users - Group Memberships worksheet lists the groups that a user is a direct member of. The Resources column provides counts of the number of resources that each group has access to. When you click a link in this column, the Group Resources worksheet opens to display more information about these shared resources.



Click User details to view extra details about the user, including the user's email address, license type, title, location, and whether the user is an administrator.

You can open the properties of any user or group listed in the Users - Group Memberships worksheet by clicking the User or Group Properties button beside the user's ID or group name.

You can include or exclude system groups in the worksheet by clicking Include System Groups.

Reviewing resource assignments by resource

The following worksheets allow you to select a type of resource to view details about the users and groups that have access to it.

- "Resource Groups worksheet" on page 588
- "Resource Users worksheet" on page 588
- "Private Resources worksheet" on page 589

You can review resource assignments for all resource types. By selecting from the Show list in the workbook toolbar, you can view details about individual resources, including scenarios, or any of the following resource categories:

- **= Reports =**—Resources that display data, including dashboards, workbooks, and scorecards.
- **= Automation =**—Resources that are used to schedule and automate activities, including alerts, scheduled tasks, automation chains, and scripts.
- **= Filtering =**—Resources that are used to control the data displayed in a report, including sites, filters, site filters, and hierarchies.
- **= Tasks =**—Resources that are used to manage actions, including forms, processes, responsibilities, and task flows.

If you are exporting a worksheet, click Text Only on the toolbar. This hides any image columns in the worksheet.

You can also make these changes from the workbook's data settings. For more information, see "Configuring worksheet data settings" on page 576.

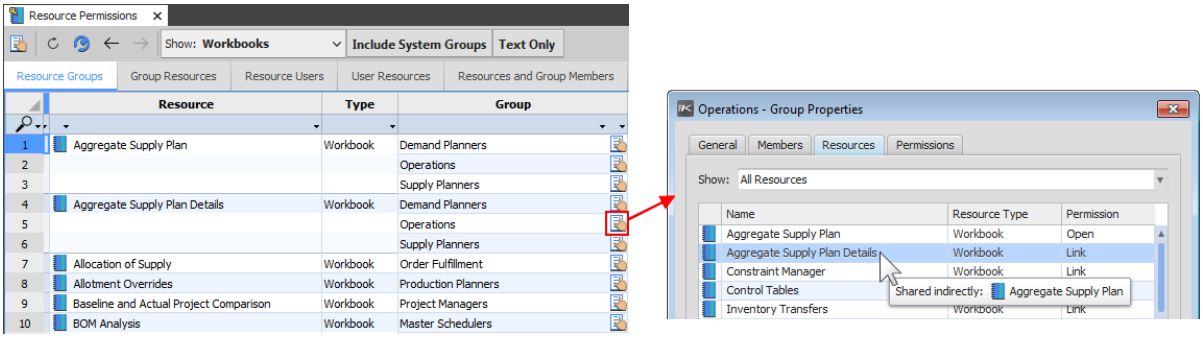
> **Note:** You can also view information about a specific type of resource in the Resources and Group Members worksheet. For more information, see "Resources and Group Members worksheet" on page 583.

Resource Groups worksheet

The Resource Groups worksheet lists the groups that have access to a resource. A group is listed in the worksheet if:

- The resource was shared directly with the group.
- The group can access the resource indirectly through linking.
- The group can access the resource through administrator permission.

These resource-group relationships reflect those displayed on the Resources tab of the Group Properties dialog box.



You can open the properties of any group listed in the worksheet by selecting the row and clicking Group Properties in the workbook toolbar. You can also click the Group Properties button beside the group's name in the Group column.

You can include or exclude system groups in the worksheet by clicking Include System Groups in the toolbar.

Resource Users worksheet

The Resource Users worksheet lists the users that have access to a resource.

The Access Permission column tells you how a user is allowed to use each resource. Clicking a link in this column opens the Sharing Details worksheet, which provides details about how the resource became available to the user. For more information, see "Understanding access permissions" on page 579.

Resource Permissions

Show: **Alerts** | **Include Administrators** | **Text Only**

Resource Groups | Group Resources | Resource Users | User Resources | Resources and Group Members | Users - Group Memberships | Group Members

	Resource	Type	User Name	User ID	Access Permission
1	Buyer New Forecast	Alert	David Harvey	dharvey	Run
2			Gerry West	gwest	Run
3	CPU Usage	Alert	Adam Yeung	ayeung	Run
4			David Harvey	dharvey	Run
5			Gerry West	gwest	Run
6			Helen Roland	hroland	Run
7			Jon Burnett	jburnett	Run
8			Kathleen Key	kkey	Run
9			Kent Bernadino	kbernadino	Run
10			Leslie Dossantos	ldossantos	Run
11			Maria Hicks	mhicks	Run
12			Tim Gorman	tgorman	Run
13	Input Data Memory Load	Alert	Adam Yeung	ayeung	Run
14			David Harvey	dharvey	Run

You can open the properties of any user listed in the worksheet by clicking the User Properties button beside the user's ID.

You can include or exclude administrator users in the worksheet by clicking Include Administrators in the toolbar.

Private Resources worksheet

The Private Resources worksheet lists all the private resources on your RapidResponse system.

Resource Permissions

Show: **= All Resources =** | **Include Administrators** | **Text Only**

Resource Groups | Group Resources | Resource Users | User Resources | Resources and Group Members | Users - Group Memberships | Group Members | Private Resources

	Resource	Type	Owner	
			Name	User ID
1	C Parts	Filter	Leslie Dossantos	ldossantos
2	KK - End of day tasks	Task Flow	Kathleen Key	kkey
3	Part Properties - GW	Workbook	Gerry West	gwest
4	Planning Sheet - GW	Workbook	Gerry West	gwest
5	Project Baseline	Scenario	Master Administrator	Admin
6	Supply updates	Alert	David Harvey	dharvey
7	Write Administration Metrics	Scheduled Task	Master Administrator	Admin

You can open the properties of any user listed in the worksheet by selecting the row and clicking User Properties in the workbook toolbar.

You can include or exclude administrator users in the worksheet by clicking Include Administrators in the toolbar.

Example: Investigating a resource assignment

You are auditing the resource assignments for the Buyers - North America group. In the Resources and Group Members worksheet, you notice that RapidResponse user with ID 'asim' has access to the Supply Chain Risk Management workbook and the rest of the group does not.

Resource Permissions

Show: = **Reports** = | Group: **Buyers - North America**

Resource Groups | Group Resources | Resource Users | User Resources | Resources and Group Members | Users - Group Memberships | Group Members | Private Resources

	Resource	Type	Access Permission by User					
			asim	gchen	jcrawford	mcoleman	pkovak	rmendez
5	Inventory Transfers	Workbook	Link	Link	Link	Link	Link	Link
6	Master Data	Workbook	Open	Open	Open	Open	Open	Open
7	Orders at Risk	Workbook	Open	Open	Open	Open	Open	Open
8	Part Properties	Workbook	Open	Open	Open	Open	Open	Open
9	Possible Data Integrity Issues	Workbook	Open	Open	Open	Open	Open	Open
10	Potential Excess and Obsolete	Workbook	Link	Link	Link	Link	Link	Link
11	Prioritized ERP Actions	Workbook	Open	Open	Open	Open	Open	Open
12	Purchase Avoidance Opportunities	Workbook	Open	Open	Open	Open	Open	Open
13	Revenue Opportunities	Workbook	Open	Open	Open	Open	Open	Open
14	Risk/Opportunity Assessment	Workbook	Open	Open	Open	Open	Open	Open
15	Supply Analysis	Workbook	Open	Open	Open	Open	Open	Open
16	Supply Chain Risk Management	Workbook	Open					
17	Supply Order Analysis	Workbook	Open	Open	Open	Open	Open	Open
18	Supply Plan Exceptions Details	Workbook	Link	Link	Link	Link	Link	Link
19	Supply Plan Exceptions Widgets	Workbook	Open	Open	Open	Open	Open	Open

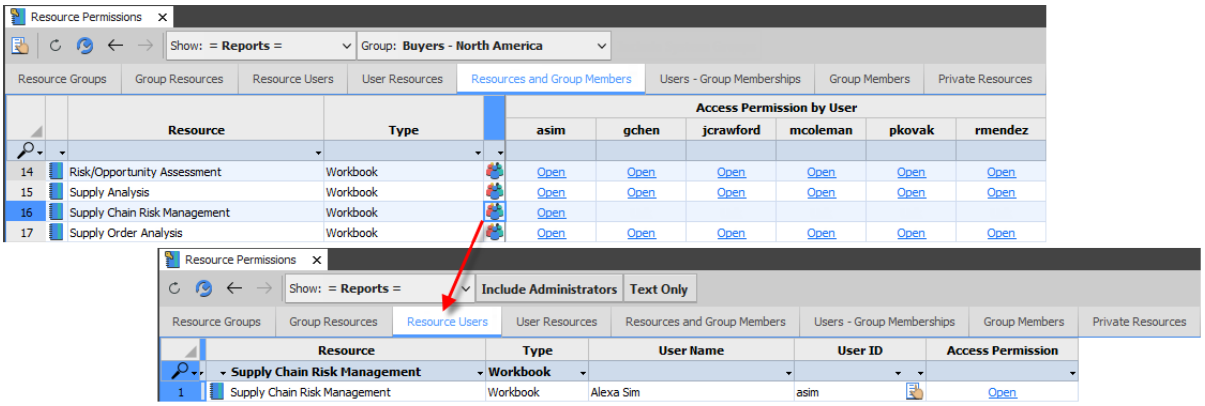
You want to determine if the user should have access to this workbook or if it might have been shared with the user by mistake. Clicking on the Open link for this user and resource, you see that the user ID is displayed in the Shared With column, indicating the workbook has been shared directly with the user.

15	Supply Analysis	Workbook	Open	Open	Open	Open	Open	Open
16	Supply Chain Risk Management	Workbook	Open					
17	Supply Order Analysis	Workbook	Open	Open	Open	Open	Open	Open

Sharing Details

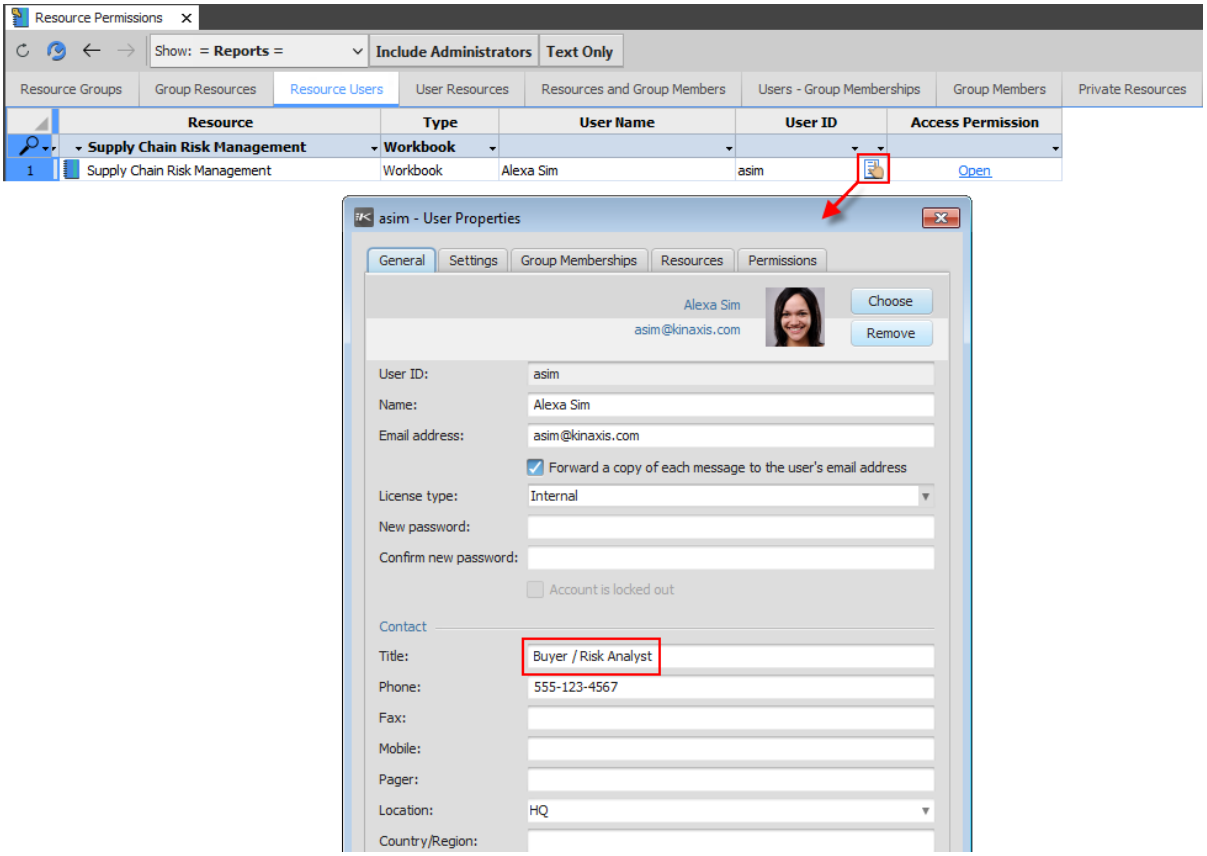
	User Name	User ID	Resource	Shared Resource	Type	Access Permission	Shared With
1	Alexa Sim	asim	Supply Chain Risk Management	Supply Chain Risk Management	Workbook	Open	asim

To determine whether the user should have access to the workbook, you decide to check if other users have access to it. You can use this information to determine if the user should be added to another group.



In this case, this user is the only general user with access to the workbook.

Next, you can check the user's properties to determine whether the resource assignment was a mistake. You can access the properties by clicking the User Properties icon beside the user's ID. Select the General tab to view the user's contact information.



The user performs risk analysis as part of her job, so the Supply Chain Risk Management workbook is required. The user should therefore retain access to the workbook.

CHAPTER 41: User account maintenance and troubleshooting

Communicating with users 593
Monitoring sign-in activities 595
Monitoring user and group changes 596
Monitoring user adoption 598
Unlocking a user account 599
Disconnecting users from RapidResponse 601
Resolving RapidResponse error messages 602
Monitoring and canceling problematic queries 603
RapidResponse Application Server Event Log 606
Monitoring RapidResponse connection speed 607

As a user administrator, you are responsible for maintaining RapidResponse user accounts. This involves several activities, such as communicating any RapidResponse maintenance that impacts users and alerting users if RapidResponse might be unexpectedly unavailable. You can also monitor which users are signed in, unlock user accounts that have been locked due to exceeding a specified number of unsuccessful sign-in attempts, and disconnect users.

You might also be called on to troubleshoot errors users are receiving when signing into RapidResponse or opening workbooks. This chapter outlines error conditions that users might encounter and how to resolve them.

Also included are instructions on how to stop queries that consume too many RapidResponse resources and possibly negatively impact RapidResponse performance.

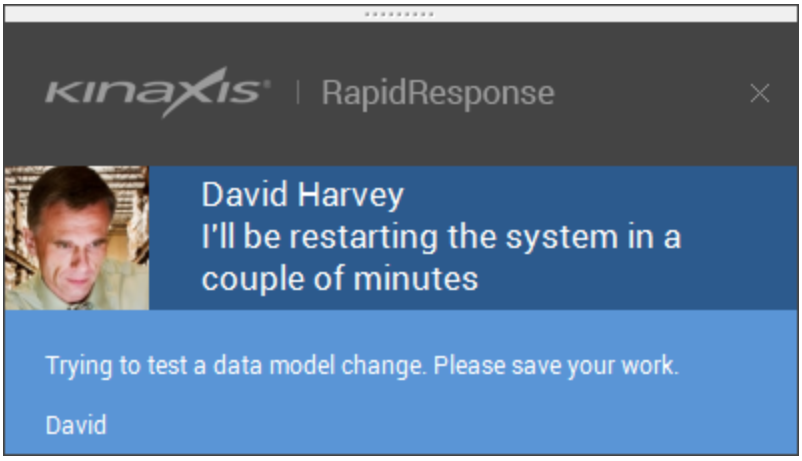
Communicating with users

As a RapidResponse administrator, you might need to communicate information to users. For example, you can notify RapidResponse users of upcoming RapidResponse maintenance that will make RapidResponse temporarily unavailable. Or, if emergency service that shuts down RapidResponse is required, you can ensure that users who are currently signed in are alerted and have the opportunity to save their work. You can also inform users of scheduled training sessions or share tips about using RapidResponse.

All users with permission to access Message Center will receive the message in Message Center. For all users without access to Message Center, they will receive the message in their email client provided their RapidResponse account has an associated email address. For more information, see "Assigning and removing permissions" on page 517.

Optionally, the message can also be displayed in a pop-up broadcast message. This ensures signed in users are alerted immediately after the message is sent. Consider using this option to communicate urgent information, for example, if the RapidResponse system will be shutting down.

The following image shows a pop-up broadcast message from an administrator.



Users who are not signed in when the message was sent can receive the broadcast message when they sign in.

▸To send a message to users

1. In the **Administration** pane, under **Communication**, click **Send Broadcast Message**.
2. In the **New Broadcast Message** dialog box, click one of the following options:
   - **All users**—the message is sent to all RapidResponse users. The message is sent to the user's Message Center, email account, or both.
   - **Only users who are currently signed in**—the message is sent to users currently signed in to the Java client. The message is sent to the user's email or Message Center, and is also displayed in a pop-up window.
   - **Select Names**—selected groups and users. Use this option to target specific types of users. For example, administrators, customers, or suppliers.

     If this option is selected, the same names are pre-populated the next time the dialog box is opened.
3. In the **Subject** box, type the subject for the message.
4. In the **Message** box, type the message content.
5. Optionally, select the **Display message in a pop-up window**.

   If this option is selected, you can choose an expiry date for the pop-up window by selecting the **Only until** check box. If a user does not sign in before the expiry date, they never see the message in the pop-up window.

   The expiry date and time is based on the RapidResponse client's computer.
6. Click **Send**.

Note: Users on the web client do not receive the pop-up broadcast messages. Additionally, the web client does not support Message Center.

Tips:

- You can also create a message by clicking **New Broadcast Message** in Message Center.
- Broadcast messages can also be created from the System Maintenance worksheet in the Administration Log workbook. The message is automatically filled with information from the selected record in the worksheet. For more information, see "System Maintenance worksheet" on page 428.

Monitoring sign-in activities

You can track and review information about sign-in activity in RapidResponse, which can be especially important if externally-based users, such as customers and suppliers, can access your RapidResponse system. The sign-in activities of users can potentially alert you to possible sign-in attempts by unauthorized users. For example, you can look for multiple failed sign-in attempts or sign-ins by users who you know are away from the office and not able to access the system.

You can review:

- Unsuccessful sign-in attempts
- Unsuccessful sign-in attempts due to the use of invalid User IDs
- Successful sign-ins
- Users locked out of their accounts (for more information, see "Unlocking a user account" on page 599)

The sign-in logging records are automatically deleted after a preconfigured number of days.

▸To review sign-in failures

1. In the **Administration** pane, under **System Monitoring**, click **Sign-in Log**.
2. On the **Failures** tab, review the information.

▸To review sign-in failures due to invalid user IDs

1. In the **Administration** pane, under **System Monitoring**, click **Sign-in Log**.
2. On the **Failures** tab, click **Invalid User ID Count**.
3. In the **Invalid User IDs** dialog box, review the number of failed sign-ins since the date and time specified.

Tip: To reset the specified date to the current date and time and the failure count to zero, click **Reset**.

▸To review successful sign-in information

1. In the **Administration** pane, under **System Monitoring**, click **Sign-in Log**.
2. On the **Successes** tab, review the information.

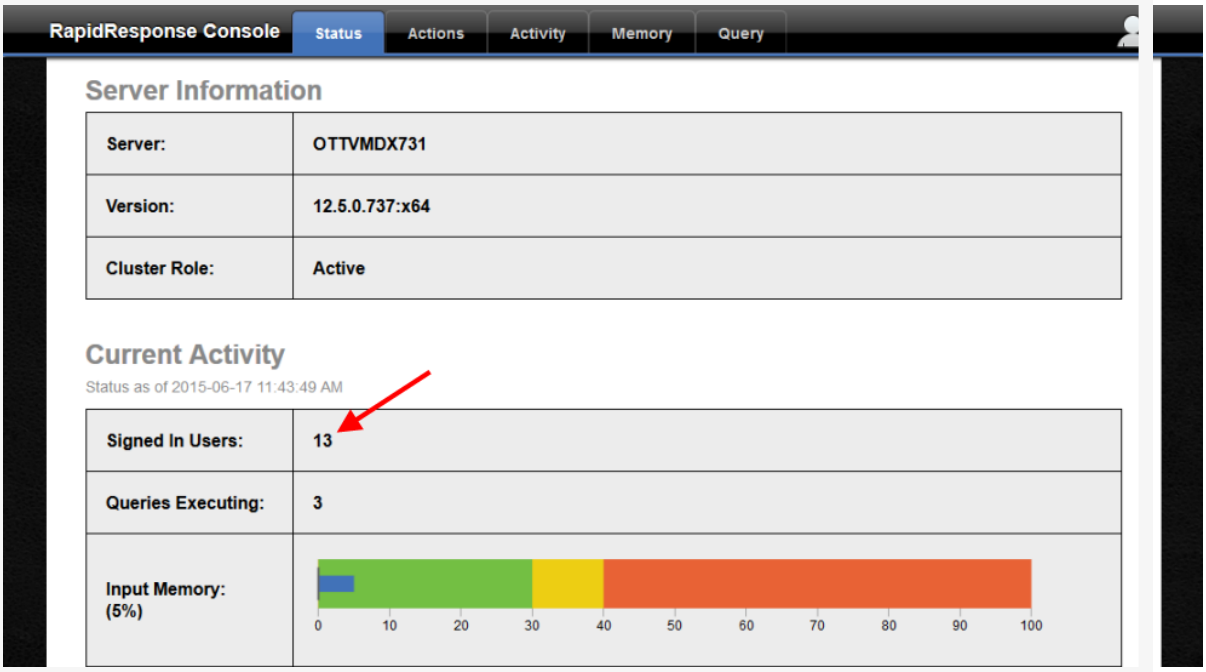
Notes:

- By default, 45 days of sign-in information (successes and failures) is stored.
  On-Demand: You can request the number of days be changed by Kinaxis Customer Support.
  On-Premises: For information about changing the default setting, see " Automatic deletion of system records" on page 277.
- You might notice duplicate entries for successful sign-ins in the Successes worksheet. This is likely due to network configuration settings. The second sign-in log entry can be ignored.

▸To review the users currently signed into RapidResponse

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** worksheet tab.
3. In the **Signed In Now** column, search for **x**.
   The Users worksheet now lists only signed-in users.

Tip: On-Premises only: The Status page on the RapidResponse Console provides a quick view of the number of users signed in. To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

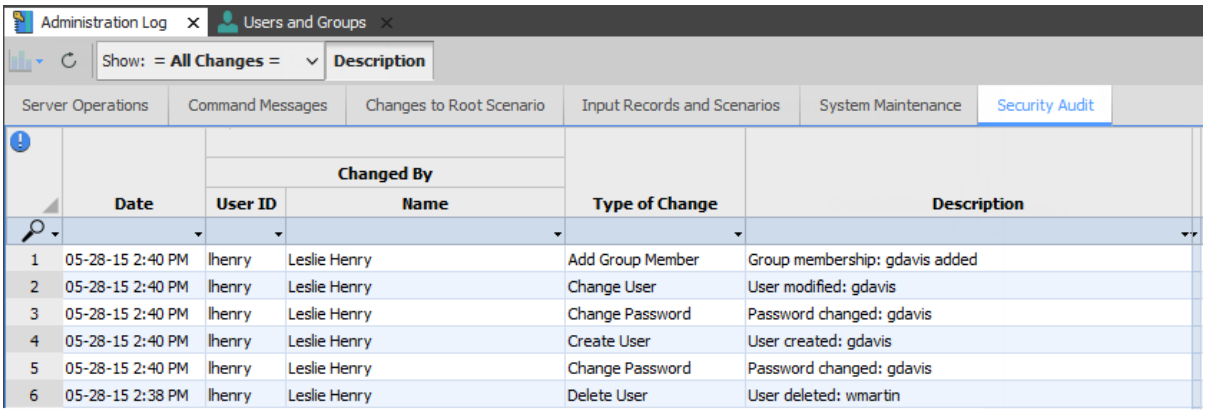


Monitoring user and group changes

User and group changes are logged in the Security Audit worksheet in the Administration Log workbook. When a user or group is created, deleted, or modified in certain ways, you can review records of these actions. You can use the information reported in this worksheet to monitor the key security controls of your RapidResponse system and to perform security audits.

In addition to user and group changes, the Security Audit worksheet logs system configuration changes, permission changes, resource dependency changes, and profile variable changes. For more information, see "Security Audit worksheet" on page 430.

Consider creating an alert that you can use to monitor when user and group changes are logged in this worksheet. For more information, see the *RapidResponse User Guide*.



	Date	Changed By		Type of Change	Description
		User ID	Name		
1	05-28-15 2:40 PM	lhenry	Leslie Henry	Add Group Member	Group membership: gdavis added
2	05-28-15 2:40 PM	lhenry	Leslie Henry	Change User	User modified: gdavis
3	05-28-15 2:40 PM	lhenry	Leslie Henry	Change Password	Password changed: gdavis
4	05-28-15 2:40 PM	lhenry	Leslie Henry	Create User	User created: gdavis
5	05-28-15 2:40 PM	lhenry	Leslie Henry	Change Password	Password changed: gdavis
6	05-28-15 2:38 PM	lhenry	Leslie Henry	Delete User	User deleted: wmartin

The date and time the change was made, the user ID and name of the user who made the change, the type of change, and a description of the change are provided for each record in the worksheet. Other details about each change are provided in columns to the right of the description, and the details vary depending on the type of change. For a better view of these details, you can hide the Description column by clicking the Description button on the worksheet toolbar. You can also filter the worksheet so that only one type of change is displayed by selecting a type of change from the Show list.

If you are using an On-Premises RapidResponse system, the changes logged in the Security Audit Worksheet are also recorded in a text-based log file. For more information, see "SecurityAudit.log file" on page 477.

User changes

User changes are actions that modify a user account. The following actions are logged as user changes:

- Creating a user
- Deleting a user
- Changing a user's name, password, email address, or account type
- Unlocking a user account

Changes to a user's profile picture and contact information, such as title, phone number, location, and so on, are not logged in this worksheet.

System Maintenance | Security Audit

Type of Change	Description	User Account			
		User ID	Name	Old Value	New Value
Delete User	User deleted: gdavis	gdavis	gdavis		
Change User	User modified: gdavis	gdavis	gdavis	EMail=gdavis@email.com|IsLockedOut=N	EMail=gdavis@kinaxis.com|IsLockedOut=N|LongN
Change User	User modified: gdavis	gdavis	gdavis	PasswordChangeRequired=N	PasswordChangeRequired=Y
Change Password	Password changed: gdavis	gdavis	gdavis		
Change User	User modified: gdavis	gdavis	gdavis	EMail=gdavis@email.com|IsLockedOut=N	EMail=gdavis@email.com|IsLockedOut=N|LongNa

When a user account is modified, pipe-delimited values reporting the user's email address, whether the account is locked out, the user's name, and the account type are logged as a user change record. This information is logged even if these values were not changed.

Group changes

Group changes are actions that modify a group. The following actions are logged as group changes:

- Creating a group
- Deleting a group
- Adding a new member to a group or removing an existing member
- Changing a group's description
- Changing a group from non-system to system (or the opposite)

System Maintenance | Security Audit

Type of Change	Description	Group Settings					
		Group	Group Member			Old Value	New Value
			Type	Group Name / User ID	User Name		
Delete User Group	Group deleted: Sales - North America	Sales - North America					
Remove Group Member	Group membership: abarrett removed	Sales	User	abarrett	Allan Barrett		
Change User Group	Group modified: Sales	Sales				Description=Responsible for reviewin	Description=Responsible for reviewin
Add Group Member	Group membership: abarrett added	Sales - North America	User	abarrett	Allan Barrett		
Create User Group	Group created: Sales - North America	Sales - North America					

When a group is modified, pipe-delimited values reporting the group's description and whether the group is a system group are logged as a group change record. This information is logged even if these values were not changed.

Monitoring user adoption

You can track information on user sign in activity, communications, and responsibility assignments in the Adoption Dashboard.

All of the widgets on this dashboard display data using the RapidResponse Workday and Week calendars.

On the Monitoring tab you can review:

Users—Tracks users sign ins. Use this widget to view:

- The total number of users signed in on each workday.
- The total number of users who have not signed in for 30 days from each workday.

Messages—Tracks the number of messages sent and received in Message Center using. Use this widget to view:

- The total number of read and unread messages sent each workday.
- The total number of unread messages for each workday.

Collaborations—Tracks the number of collaborations. Use this widget to view:

- The total number of open collaborations for each week.
- The total number of archived collaborations for each week.

Unassigned Responsibilities—Tracks the percentage of responsibilities for Parts and for Constraints that have not been assigned. Use this widget to view:

- The percentage of parts where no planner or buyer code has been assigned to a part for each week.
- The percentage of constraints where no planner code has been assigned to a constraint for each week.

On the Data Quality tab you can review:

Sites with Questionable Data—Tracks the total number of sites in your manufacturing system that have data with possible integrity issues. The issues are organized by type of data. Click a value to see more details about that issue.

Sites with Questionable Data—Tracks the total for data with possible integrity issues organized by site. Click a data point to see more details about the issue.

▸To review user adoption metrics

- In the Explorer pane, click **Adoption Dashboard**.

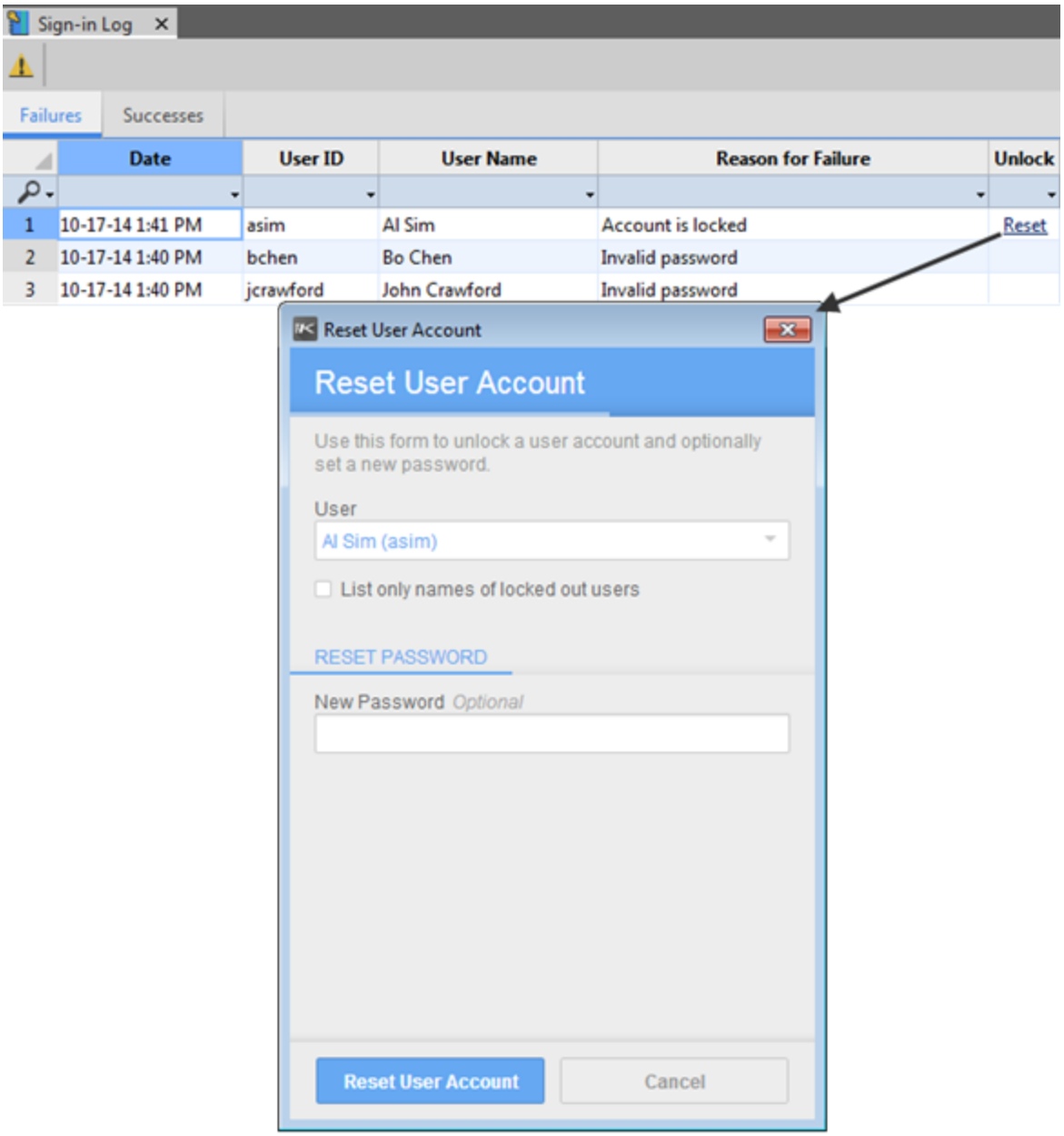
Note: The Executives group is provided with default access to the Adoption Dashboard.

Unlocking a user account

If a RapidResponse system administrator has configured RapidResponse to lock out users after a specified number of unsuccessful sign-in attempts, you might have to unlock user accounts. A user whose account has been locked out will likely contact you for assistance, though you can use the Sign-in Log workbook to review all users who have been locked out of their accounts.

For information about lock out settings and other password security settings, see "Setting password security options" on page 648.

In the Sign-in Log workbook, the Unlock column contains a **Reset** link if a user is locked out of RapidResponse due to consecutive sign-in failures. To unlock the user account, you can click the link to open the Reset User Account form, shown in the following illustration.



If the locked out user requires a new password, you can also use the Reset User Account form to set a new password when you unlock the user's account. You can also use this form to set a new password for a user who is not locked out. For more information, see "Editing user accounts" on page 570.

The Reset User Account form can be accessed from the Explorer pane in RapidResponse. Additionally, you can use the form on your mobile device so you can unlock user accounts when you are away from your desktop.

You can also review locked user accounts and unlock user accounts using the Users and Groups workbook from the Administration pane.

Note: If your company has established password security requirements, those requirements are displayed in the **New Password** field's tooltip.

▸To unlock a user account from the Sign-in Log workbook

1. Beside the name of the locked out user, click **Reset**.
2. On the **Reset User Account** form, click **Reset User Account**.

▸To unlock a user account from the web client

1. Sign in to the web client.
   For more information about signing in to this client, see "Providing the RapidResponse URL and credentials" on page 553.
2. Open the **Reset User Account** form.
3. Select the **List only locked out users** check box, then select a user from the **User Account** list.
   You can also use search if you know the name of the locked out user.
4. Click **Reset User Account**.

▸To unlock a user account from the Explorer pane

1. From the **Explorer**, under **Forms**, double-click **Reset User Account**.
2. Select the **List only locked out users** check box, then select a user from the **User Account** list.
   You can also use search if you know the name of the locked out user.
3. Click **Reset User Account**.

▸To review locked out users from the Administration pane

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, type **x** in the Search row for the **Locked Out** column.
   This step filters the worksheet to list only locked out users.

▸To unlock a user account from the Administration pane

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, locate and select the user whose account is locked.
3. Click **Properties** on the Users and Groups toolbar.
   Click to clear the **Account is locked out** check box.

Disconnecting users from RapidResponse

A user's session might occasionally remain active due to network problems or a user's computer failure. This can prevent the user from signing in to RapidResponse. In this case you must disconnect the user from RapidResponse so that the user can sign in again. To avoid the possibility of any errors, it is recommended that you use this feature only when necessary.

▸To disconnect a user from RapidResponse

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Users** tab, click **Connections**.
3. In the **Connected users** list, click the user that you want to disconnect, and then click **Disconnect**.

Note: You can select multiple users. To select nonadjacent users, hold down **CTRL**, and then click each user. To select adjacent users, hold down **SHIFT**, and then click the first and last user in the sequence.

Resolving RapidResponse error messages

This section outlines errors that users might experience, and how you can resolve them.

Errors when signing in to RapidResponse

Users might experience the following error condition when signing in to RapidResponse.

You can't sign in to RapidResponse because you haven't been granted access to scenarios. Notify your administrator.

You have not given access to a scenario to this user. Make the user a member of a group to which you have given access to a scenario.

You can't sign in to RapidResponse because you haven't been granted access to any sites. Notify your administrator.

You have not given permissions to this user. Make the user a member of a group to which you have given access to at least one site.

Errors when opening workbooks in RapidResponse

Users who access workbooks in RapidResponse might encounter one of the following error conditions. These errors can occur when the user attempts to access a particular workbook or worksheet.

You cannot open this worksheet because it uses the 'X' profile variable which is not defined for you. Please contact your RapidResponse Administrator.

The user cannot view a worksheet because a profile variable is not defined for that user. Define the profile variable specified.

A variable named 'X' is not defined.

The user cannot view a worksheet because a variable has not been defined. The variable could be used in the worksheet filter expression, a column expression, the user's selected filter, or a macro used in any of the previous.

Ensure the variable is either defined in the workbook or defined for the user, depending on whether it is a workbook variable or a profile variable.

You can search resources to determine which workbooks or filters use the variable in expressions. For more information, see "Searching resources" in the *RapidResponse Resource Authoring Guide*.

"Open with Filter" Not There

This error occurs when a user tries to display a worksheet under the following conditions:

- The user does not have access to the filter specified in the Always Open with Selected Filter parameter. This parameter is visible in the Workbook Properties dialog box.
- The selected filter is automatically set to the filter that is specified in the Always Open with Selected Filter parameter

"Open with Filter" Expression Variable not Defined

The user cannot open a workbook with a filter because a profile variable is not defined for that user. Define the profile variable specified.

Expression Variable not Defined

This error occurs when a user tries to display a worksheet under the following conditions:

- The worksheet filter expression or a column expression contains a profile variable not defined for the user (with the RapidResponse context).
- The filter expression for the filter the user has chosen contains a profile variable that has not been defined for that user.

Monitoring and canceling problematic queries

Various data retrieval actions, such as opening a dashboard, workbook or scorecard, or opening a worksheet in a workbook, generate queries on the RapidResponse database. Occasionally, a resource can generate queries that take significant time to complete and consume many RapidResponse resources. This might be due to an overly intensive or poorly configured workbook or filter.

Queries are also generated from alerts. The queries associated with alerts are always assigned a lower priority in RapidResponse than queries associated with user actions such as opening a workbook. Occasionally, an alert might not complete in a timely manner. This might be because the alert is based on a poorly configured workbook, or because RapidResponse is too busy processing queries from higher priority user actions to allow it to handle the alert.

If users contact you with resource problems that you think are related to slow running queries, you can use the Query Manager workbook to investigate the issue.

User administrators who are monitoring queries should consider signing in to RapidResponse at the beginning of the day and remaining signed in all day. If the administrator waits until someone contacts her with a long-running query performance problem, she might experience extreme delays in getting signed in because of that query.

This workbook includes two worksheets and is available to all user and system administrators. For more information about Query Manager, including descriptions of its worksheets and columns, see the Query Manager workbook help.

Active Queries worksheet

The Active Queries worksheet displays a record for each RapidResponse query that is currently running, and has been running for more than thirty seconds. It is useful for locating overly intensive queries. As necessary, problematic queries can be canceled using the Cancel Query button .

If you identify queries that negatively impact RapidResponse performance because they are too lengthy or are using too many resources, you can cancel them. Before canceling a query, however, it is recommended that you determine if any problems reported by a user are actually caused by this user and not by another user. You might need to inquire about the specific task the user was performing prior to contacting you. This also helps with identifying the resource that is causing the problem.

After canceling any problematic queries, you should ensure that the resources that were generating such queries are modified. For example, a worksheet might require a more refined worksheet expression. If the problem occurs when a user opens a scorecard, a metric might need to be modified or removed from a scorecard. Or, the scorecard definition might need to specify that it always open with a filter that minimizes the amount of data calculated by the metrics.

Recent Query History worksheet

This worksheet identifies the last 5,000 queries. As appropriate, you can use worksheet searches to find records of particular interest in Query Manager. For example, you might want to review only queries generated by a particular user or within a given time frame.

The **Processing Time - Elapsed** column shows the total number of seconds taken to prepare (parse) and run the query. This column is pre-configured with a worksheet search setting to only show queries that have taken more than two seconds to run. The search settings can be removed from the column. If the search settings are removed, the worksheet shows the last 5,000 significant queries. Queries that take less than a second to run are considered insignificant and are removed from the query history when the 5,000 record limit is reached. The query history is not intended to be a complete list of all queries that have run as this could consume a significant amount of system memory.

> **Note:** On-Premises system administrators also have access to other query monitoring and management tools. For more information, see "Query monitoring and management tools" on page 267.

Query Manager

Active Queries (> 30 seconds) | Recent Query History

			Processing Time (seconds)														
				Analytics Calculations													
	Submitted	Status	Elapsed	Cached	Not Cached	CPU	Memory Usage Open Queries (KB)	User ID	Priority	Source	Table	Namespace	Scenario	Other Scenarios	Result Rows	Query
			>2													
1	05-20-16 9:48 AM	Open	2	0	1	4	90,732	Admin	Normal	WBK Manage Inventory / Stock-out Details	SupplyDemand	Mfg	S&OP Candidate		725	$IDrillFrom='Commit';$IExpediteType='None';$IScheduledReceipt
2	05-20-16 9:48 AM	Open	2	0	2	4	14,189	Admin	Normal	WBK Manage Inventory / Projected Late Revenue by Driver	<Multiple>	<Multiple>	S&OP Candidate		5,000	$IDrillFrom='Commit';$IExpediteType='None';$IScheduledReceipt
3	05-20-16 9:48 AM	Open	2	0	2	5	22,741	Admin	Normal	WBK Manage Inventory / On-time Delivery Details	<Multiple>	<Multiple>	S&OP Candidate		4,367	$IDrillFrom='Commit';$IExpediteType='None';$IScheduledReceipt
4	05-20-16 9:48 AM	Open	3	0	5	5	6,872	Admin	Normal	WBK Manage Inventory / Late Demand Orders Impacting Re	<Multiple>	<Multiple>	S&OP Candidate		3,502	$IDrillFrom='Commit';$IExpediteType='None';$IScheduledReceipt
5	05-20-16 9:45 AM	Open	16	1	7	29	314,673	Admin	Normal	WBK Manage Inventory / Period Ending Inventory Details	<Multiple>	<Multiple>	S&OP Candidate		5,000	$IDrillFrom='Commit';$IExpediteType='None';$IScheduledReceipt
6	05-20-16 9:39 AM	Closed	40	0	38	72	648,911	Admin	Normal	WBK Line of Balance - Unit / Supply Details	WhereConsumedFc	Mfg	S&OP Candidate		5,000	$ILOBComponentFilter='PUBLIC s('All Items');$ILOBStartDate=Pa
7	05-20-16 9:36 AM	Closed	55	0	53	100	528,488	Admin	Normal	WBK Line of Balance - Unit / Summary by Date	<Multiple>	<Multiple>	S&OP Candidate		5,000	$ILOBComponentFilter='PUBLIC s('All Items');$ILOBStartDate=Pa
8	05-20-16 9:35 AM	Closed	77	0	0	0	1,467,506	Admin	Normal	WBK Line of Balance - Unit / Summary by Order	<Multiple>	<Multiple>	S&OP Candidate		0	$ILOBComponentFilter='PUBLIC s('All Items');$ILOBStartDate=Pa

Queries in this worksheet are typically too long to display in the worksheet columns, however, the full query can be displayed in a tooltip. The following illustration shows a query, which also includes encapsulation notation.

Source	Table	Namespace	Scenario	Other Scenarios	Result Rows	Query
WBK Supply Plan Exceptions Widgets / Revenue Miss	$!BaseDate='PlanDate';$!LatenessBase='PlanDate';$!Consensus='False';$!RawMaterial='Raw Material';$!FinishedGoods='Finished Goods';$!WorkInProgress='Work In Progress';_SelectedFilterSet=Mfg::Part[PUBLIC s'All Items' And Mfg::Site[PUBLIC Site 'All Sites']]{Self:By};LateRevenue!!Buckets={d'Past',-1}+{d'20170601',0}+{d'20170703',1}+{d'20170801',2}+{d'20170901',3}+{d'20171002',4}+{d'20171101',5}+{d'20171201',6}+{d'20180101',7}+{d'20180201',8}+{0180301',9}+{d'20180402',10}+{d'20180501',11}+{d'20180601',12}+{d'Undefined',-1};SOPConfiguration=g::SOPAnalyticsConfiguration{CycleCalendar=«CycleCalendar»«:Ref :Max»};LateRevenueID=Mfg::IndependentDemand[«Mfg::Part[In _SelectedFilterSet!]»][«Part.Type.ProcessingRule LIKE 'MPS*' AND Quantity >0 AND AvailableDate > DueDate AND EffectiveDemand > 0 AND EffectiveUnitPrice > 0»]{Date=«IF($LatenessBase='PlanDate', DueDate, AvailableDate)», RevenueLate=«IF((DueDate + 1 SOPConfiguration!CycleCalendar) <= AvailableDate, EffectiveDemand - OnTimeQuantity , 0)* EffectiveUnitPrice», OrderTypeProcessingRule=«Order.Type.ProcessingRule»};LateRevenueCTPF=Mfg::CTPForecast[«Mfg::Par _SelectedFilterSet!]»][«IF(NOT $consensus, false, (Forecast.ForecastSource = 'ConsensusForecast')	$!BaseDate='PlanDate';$!LatenessBase='PlanDate';$!C
Scheduled Task: Create Backup						{cmd=CreateDataPackage('debug', '', '')}.cmd{ReturnC
Scheduled Task: Database Integrity Check						{cmd=DataIntegrityCheck(0, 8192, '', false, 0)}.cmd{R

▸To view currently running queries

1. In the **Administration** pane, under **System Monitoring**, click **Query Manager**.
2. Click the **Active Queries (> 30 seconds)** worksheet.

   All queries that have been running for more than 30 seconds are listed, and you can see the processing time and memory usage associated with each. The queries with the longest processing times are displayed at the top of the list.
3. Click **Refresh this worksheet** ↻ to update the data. The data in this worksheet is not automatically updated.

▸To view recent query history

1. In the **Administration** pane, under **System Monitoring**, click **Query Manager**.
2. Click the **Recent Query History** worksheet.

   The last 5,000 queries are listed. You can view details of each query such as its current status, memory usage, source, and full query string. The most recently submitted queries are displayed at the top of the list.
3. If insufficient memory is available for calculated results, review the **Memory Usage Open Queries (KB)** column to identify any queries that are consuming a large amount of memory. Ask the user to close the corresponding resource identified in the Source column, or disconnect that user's session. For more information, see "To disconnect a user from RapidResponse" on page 601.
4. Click **Refresh this worksheet** ↻ to update the data. The data in this worksheet is not automatically updated.

> **Note:** On-Premises administrators can also log information on all completed queries to the **QueryHistory.log** file. For more information, see " QueryHistory.log file" on page 474.

▸To cancel an active query

1. In the **Administration** pane, under **System Monitoring**, click **Query Manager**
2. Click the **Active Queries (> 30 seconds)** worksheet.
3. Select the row corresponding to the query you want to cancel, and then click **Cancel Query**.

4. After clicking Cancel Query, the Status column displays **Canceled**. This indicates that RapidResponse is attempting to cancel the query. Once the query cancellation process is complete, it is removed from the list.
5. After canceling a query, you might need to cancel another query. This might occur if the query you cancelled was generated by an alert that generates customized reports for different users. Click **Refresh this worksheet** and review the information again to ensure that no other queries need to be canceled.

Note: When you cancel a query, the user who generated the query is notified; a message is displayed in the resource that was causing the query.

RapidResponse users canceling queries

If a RapidResponse user initiated query runs for more than 20 seconds, they are presented with a Retrieving Data dialog box that includes a Cancel button. By clicking the Cancel button, users can cancel the long-running query.

On-Demand: You can request this default be changed if necessary. For more information, contact Kinaxis Customer Support.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

RapidResponse system administrators can change the 20-second default setting.

▸To modify the query cancel setting

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Query cancel dialog delay** box, type a number (seconds).

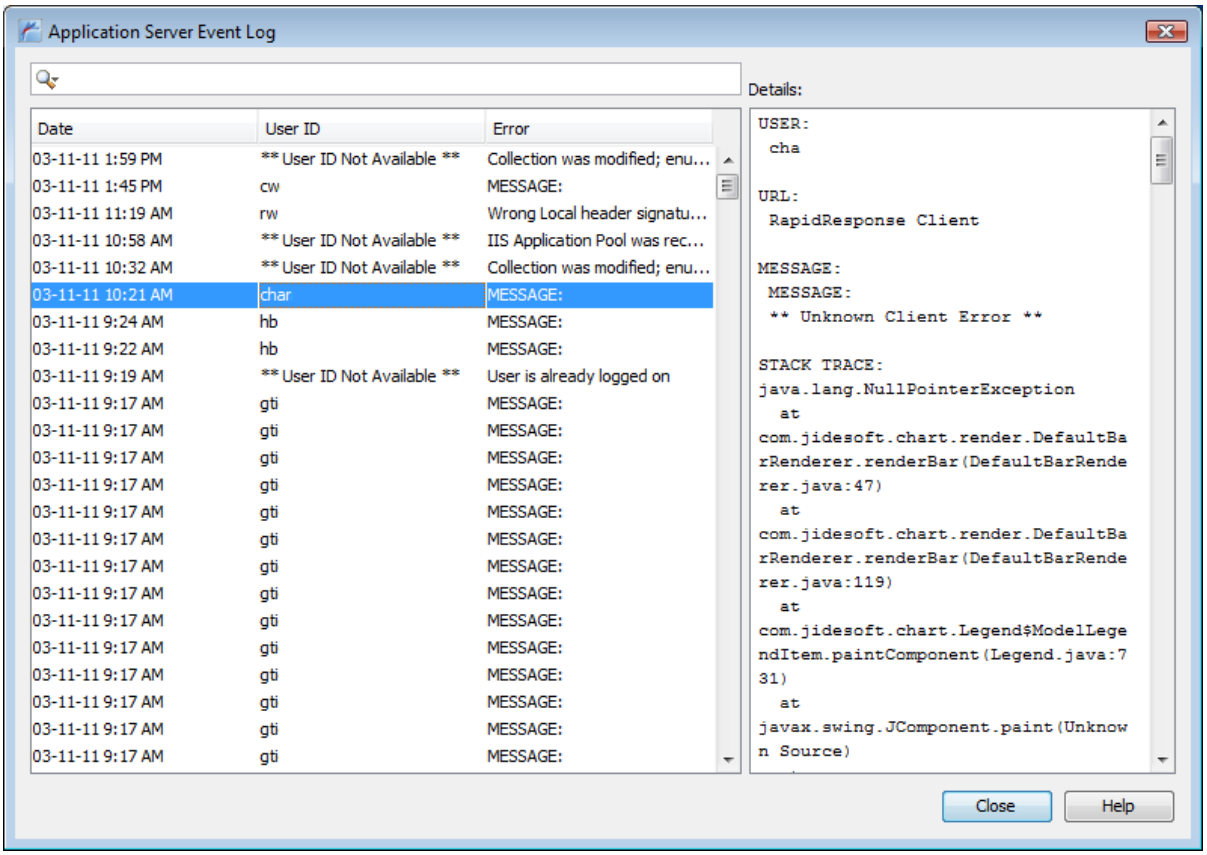
RapidResponse Application Server Event Log

This topic only applies to the On-Premises version of RapidResponse.

System administrators can review the event log available with RapidResponse Application Server. A detailed error report is written to the event log if a user receives an error message while using RapidResponse. The event log can help you or Kinaxis Customer Support diagnose RapidResponse application issues and problems.

Each error report includes:

- The date and time the error occurred. The time value comes from the local time on the RapidResponse Application Server.
- The User ID of the user that triggered the error.
- An error title.
- A detailed description of the error. Descriptions can include query error information that might be useful in better understanding issues related to dashboards, workbooks, and scorecards.



User administrators, data administrators, and general users who have been granted the Application Server Event Log permission can also access this tool. For more information, see "Assigning and removing permissions" on page 517.

▸To access the Application Server Event Log from RapidResponse

1. In the **Administration** pane, under **System Monitoring**, click **Application Server Event Log**.
2. On the **Event Log** page, locate the error for which you want details.
3. In the **Cause of error** column, click the error you want to view detail about.

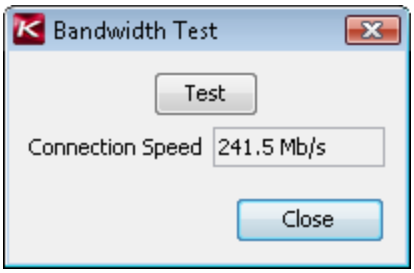
Note: General users open the Application Server Event Log from the **View** menu.

Tip: The event log can also be accessed directly from the IIS Web server hosting RapidResponse Application Server using the Windows Event Viewer.

Monitoring RapidResponse connection speed

RapidResponse performance issues might be caused by high CPU usage or memory consumption. However, the user's connection speed to the RapidResponse web server can also contribute to perceived performance problems. For example, with a very slow connection, a process might appear to be running more slowly than it actually is. You can view your current connection speed using the

bandwidth monitor, which you can use to help determine whether the problem might be the result of a poor connection.



▸To test your connection speed

1. To open the bandwidth monitor, press `CTRL` + `ALT` + `SHIFT` + `B`.
2. In the **Bandwidth Test** dialog box, click **Test**.

   Your current connection speed is displayed in the **Connection Speed** box, and is displayed in kilobits per second (Kb/s) or megabits per second (Mb/s), depending on your connection speed.
3. To update the connection speed, click **Test**.

Notes:

- Consider clicking the **Test** button several times and take an average of the connection speed in cases of variable speeds.
- For information about data transfer and bandwidth considerations, see "Web client to RapidResponse Application Server communication" on page 53.

Part 7: RapidResponse client administration

- "Customizing the RapidResponse client " on page 611
- "Customizing RapidResponse user settings" on page 643
- "Creating and managing currencies" on page 683
- "Scenario management" on page 703
- "Managing RapidResponse resources" on page 739
- "Application configuration and settings" on page 777
- "Predefined resource and tool settings" on page 807
- "Configuring RapidResponse maps" on page 811
- "Supplier collaboration setup" on page 815
- "Data change tracking and record identification" on page 829
- " Configuring single sign-in for On-Premises" on page 835
- "Configuring single sign-in for On-Demand" on page 863

CHAPTER 42: Customizing the RapidResponse client

Changing the session expiry setting 611
Extending web client sign in durations 612
Customizing help and documentation settings 613
Setting the sign-in notice 614
Displaying profile pictures 617
Customizing the workbook link menu 618
Setting the maximum number of command errors logged 623
Adding custom links 624
Enabling the Reference Part toggle 628
Specifying display names for calendars 629
Adjusting calendars for bucketing 630
Specifying the separator for split orders 631
Configuring column headers 631
Configuring status bar identification text 632
Specifying the AND operator for feature lists 632
Defining integrated project management settings 633
Defining process orchestration settings 634
Configuring responsibility 635
Specifying the annual plan target scenario 636
Specifying whether historical data is editable 637
Configuring add-ins 638
Configuring data origin for record modifications 641

The RapidResponse client user interface is flexible and can be customized to suit the needs of your RapidResponse users. For example, you add custom links or integrate your own custom-built help into the RapidResponse client. As well, custom applications that extend base RapidResponse functionality can be configured to launch from the Add-ins Pane.

Changing the session expiry setting

A user's RapidResponse session automatically expires if it is inactive for a specified amount of time. If this occurs, the user will need to re-sign into RapidResponse. This is also known as a time out setting.

On-Demand: The default setting is four hours (240 minutes) and can be changed by Kinaxis Customer Support.

On-Premises: The default setting is four hours (240 minutes) and can be changed by a system administrator.

It is recommended you maintain an automatic session expiry setting. Automatically expiring sessions helps to contribute to greater security of your system and releases resources and data results of inactive RapidResponse sessions.

If a user's session expires, their data and resource changes are lost.

▸To change the session expiry setting (On-Premises)

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **User session time out** box, type a value (in minutes).

Extending web client sign in durations

In the web client, a user's session automatically expires if it is inactive for one hour (60 minutes). When their session expires, users need to re-sign into RapidResponse. They also need to re-sign in if they close the browser displaying the web client.

You can extend sign in durations for the web client and provide users with a more streamlined experience, reducing the number of times they need to sign in over a specified time period. Extending the sign in also persists past opening and closing a browsers. Users will be able to close the browser displaying web client and then open a new browser and open RapidResponse without having to type their sign in credentials. The default extended sign in period is seven days and is applied to all web client on your system.

An authentication token is created for each user the extended sign in applies to. You can view and delete authentication tokens in RapidResponse User Administration workbook.

Caution: If you have extended the sign in period for web client users, anyone who has access to their computer can open their instance of the web client. Depending on your company policies, you have the flexibility to set the extended sign on duration to any number of days you specify.

▸To enable extended sign in periods for web client users

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Keep mobile users signed in** box, select **Yes**.
4. Click **OK**.

▸To set or change the sign in duration for web client users

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Sign in duration** box, type a value (in days).
4. Click **OK**.

▸To view or delete authentication tokens

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. In the **RapidResponse User Administration workbook**, click the **Authentication Tokens** worksheet tab.
3. To delete a token, select the user row the token has been applied to and click **Delete** ✕ on the workbook toolbar.

Note: Authentication tokens are only generated after extended sign on has been enabled and users have signed in to the web client on their devices.

Customizing help and documentation settings

System administrators can customize help and documentation settings.

Custom help

Your company might have created additional help topics, processes, or other information about using RapidResponse to solve your company's business problems. If the information resides on your company intranet or the Internet you can create a link to it from the Help menu in RapidResponse.

▸To add custom help to RapidResponse

1. In the **Administration** pane, under **System Settings**, click **Help Settings**.
2. In the **Custom Help** area, select the **Access custom help from the Help menu** check box.
3. In the **Help menu command** box, type the command name that will be displayed on the Help menu, for example, **Our company's processes**.
4. In the **Custom help address** box, type the Web address (Internet only) of the custom link.
5. In the **Custom help address** box, type the Web address of the custom link. For example, you can include a link to your intranet or to the Internet.

Tip: You can also add help, documentation, and links to the RapidResponse client with task flows or custom links in the **Extensions** pane. For more information, see "Adding custom links" on page 624.

Modifying the location of help resources

This topic only applies to the On-Premises version of RapidResponse.

By default, the RapidResponse client accesses the help and documentation resources from the Internet on a Web server hosted by Kinaxis.

The help and documentation resources hosted by Kinaxis are continually updated to reflect functionality introduced in service updates, as well for corrective content and general improvements. Also, in the help

system hosted by Kinaxis, RapidResponse users can provide comments in help topics, see comments other users have made, and rate individual topics.

Instead, you can choose to have RapidResponse access these Help resources from a location on the system in your network where RapidResponse Application Server is installed. You might choose this option if your users do not have Internet access.

Additionally, if RapidResponse is set to access help and documentation resources from the Internet, and a user loses Internet access, they automatically receive their resources from the local RapidResponse system until their Internet access is resourced.

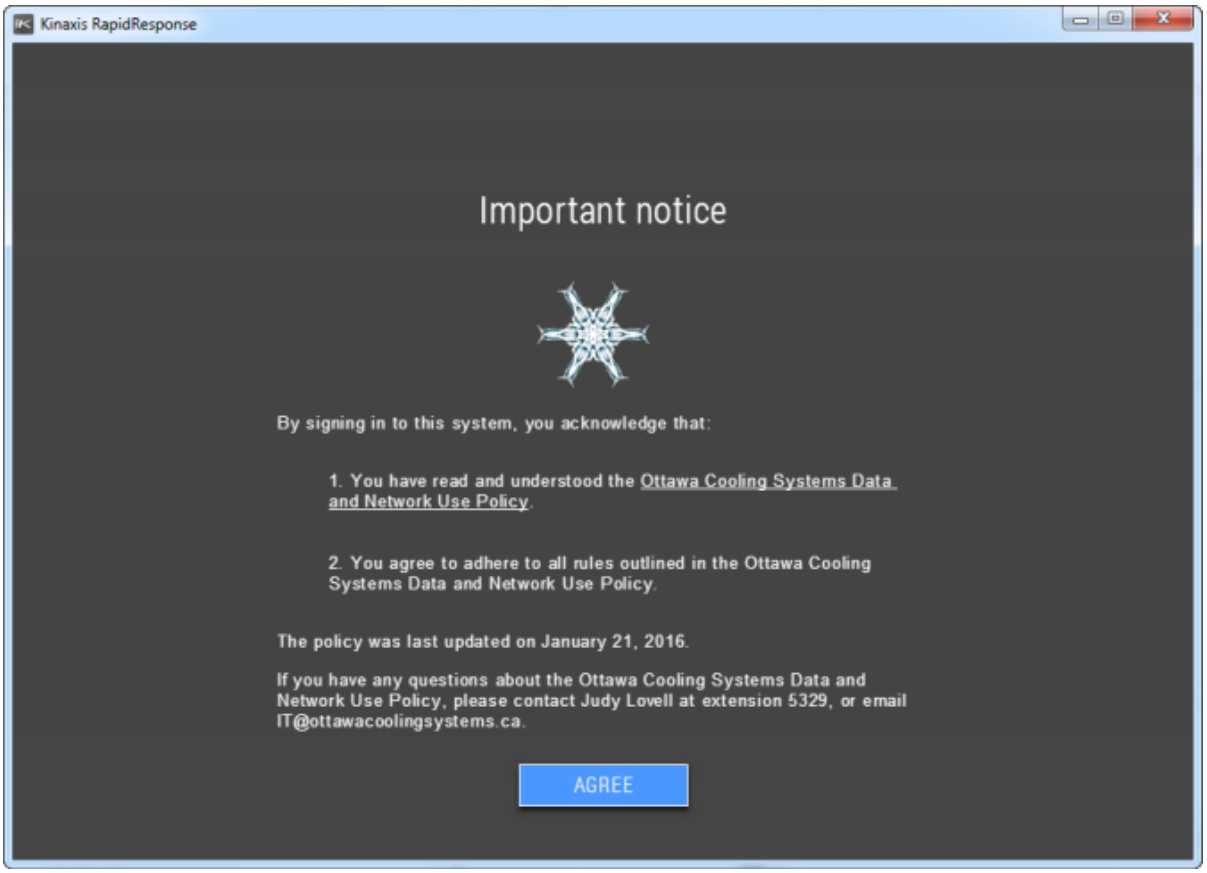
▸To change how help and documentation resources are accessed

1. In the **Administration** pane, under **System Settings**, click **Help Settings**.
2. In the **Internet-based help and documentation** area, click one of the following:
   - Hosted by Kinaxis (this is the default setting)
   - Hosted on the server that also hosts RapidResponse Application Server

Note: When RapidResponse Application Server is installed, **Docs** and **Help** folders are created for storing the RapidResponse Help resources. By default, however, these folders are empty (with the exception of the *Administration Guide*). If there is an expectation that users will need access to Help located on the RapidResponse Application Server system, Help resources should be downloaded and extracted into these folders as discussed in "Installing RapidResponse documentation resources" on page 121.

Setting the sign-in notice

System administrators can set RapidResponse to display a notice to all users as soon as they sign in to RapidResponse. In single sign-in environments, signed-in users see the notice when they start RapidResponse. Users must click a button to acknowledge this notice before they can perform any other actions in RapidResponse. Their only other option is to close the RapidResponse window. The following image shows a sign-in notice screen.



You can determine the title of the notice, the text of the notice, and the label on the button that users must click to acknowledge the notice. For example, you could set RapidResponse to display your company's data use policy, and require users to click an Agree button before they can continue.

If the notice is long, a scroll bar appears so that users can scroll through the notice text.

You can preview a sign-in notice before it is shown to users. You can also turn off an existing sign-in notice so that it is saved, but not shown to users unless you turn it on it again.

Adding a title to the notice

The title is optional. You can type up to 60 characters in the title box, but depending on the size and number of characters you type, they might not fit in the space allowed for the title in the notice. For example, 60 Chinese characters are unlikely to fit. Characters that do not fit in the space are not displayed in the notice. Preview the notice to see what the title will look like to users.

The font for the title is fixed, and formatting options are not available for the title. If you want to add formatting, such as superscript, or display a graphic above or beside the title, consider typing the title in the notice text area instead of the title box.

Formatting the content of the notice

You can type the notice in the text box in the Sign-in Notice dialog box, or you can paste rich text from other applications, such as Microsoft Word or HTML browsers. When you copy text from other applications, some of the original formatting might not be copied. When you copy text from an HTML

browser, the HTML tags used to format the text are copied along with the text, although you do not see the tags. A limited set of HTML tags is allowed in the sign-in notice: <a>, <p>, <ul>, <ol>, <li>, <table>, <tr>, <th>, <td>, <tbody>, <img>, <h1>, <h2>, <h3>, <h4>, , , , <sup>, <sub>, <br>, and <pre>. Any text copied from a browser that is inside a tag that is not included in this list is not shown in the preview or the sign-in notice, although this text is shown in the editor.

> **Tip:** If text that you copied from a browser is not included in the sign-in notice when you preview it, try pasting the text into a word processing program, such as Microsoft Word, and then copy it from there. Since Word does not use HTML tags, the tags are automatically removed.

The text editing tools available for editing and formatting the notice text are similar to those in other text editing dialog boxes in RapidResponse. You can include features such as tables, hyperlinks, lists, and graphics in the notice text. Fonts, however, are limited to three standard styles. For more information about using the text editing tools in RapidResponse, see the *RapidResponse Resource Authoring Guide*.

The notice text can be up to 30,000 characters long, including HTML formatting, such as paragraph tags, which is not displayed in the text editing window.

Adding images

The notice is displayed against a dark background at runtime, so images, such as logos, with white backgrounds might not look good in the notice. Consider using images with transparent backgrounds instead.

Images that are too big might not fit in the notice area. You can fix this problem by choosing a smaller image or re-sizing the image in the editor.

You can preview the notice to see what it will look like to users.

Specifying the text on the button below the notice

You can type a text string of up to 20 characters for the button label, but depending on the number and size of the characters you type, they might not all fit on the button. Preview the notice to see what the button will look like to users.

Regardless of the label on the button, the function of the button is always the same. The font of the button label is fixed, and formatting options are not available for this text.

▸Set RapidResponse to display a sign-in notice

1. On the **Administration** pane, click **Sign-in Notice**.
2. Check the **Show this notice to users on sign-in** box.
3. If desired, type a title in the **Title** box.
4. Type the label for the button in the **Button label** box.
5. Type or paste in the notice text, including any pictures, tables, or hyperlinks. For information about using the text editing tools in this box, see the *RapidResponse Resource Authoring Guide*.
6. Click **OK**.

▸Preview the sign-in notice

1. In the **Sign-in Notice** dialog box, click **Preview**.
2. When you finish previewing the notice, click **Edit** to continue editing the text or click **OK** to save the sign-in notice settings.

▸Re-size an image

1. In the **Sign-in Notice** dialog box, click the image to select it.
2. Move your mouse cursor over one of the squares at the edge of the image, so that it turns into an arrow.
3. Click and drag the edge of the image until it is the right size.

▸Turn the sign-in notice on or off

- In the **Sign-in Notice** dialog box, check or uncheck the **Show this notice to users on sign-in** check box.

Displaying profile pictures

By default, profile pictures are turned on in the RapidResponse clients (Java client and web client). This means that users and administrators can add profile pictures to RapidResponse user accounts. Profile pictures can be useful as part of the collaboration process, allowing users to more quickly and easily identify key team members.

In the web client, profile pictures are displayed in the toolbar and in collaborations. In the Java client, they are displayed in the toolbar, messages in Message Center, broadcast messages, and contact cards. If no image has been uploaded to display as a user's profile picture, a default image displays the first initial of the user's name or user ID. For more information, see "Setting profile pictures" on page 560.

System administrators can turn off profile pictures for all users. When turned off, profile pictures and any options to set a profile picture are not available.

▸To turn off profile pictures

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. If necessary, expand the **Client** category.
3. In the **Display user profile pictures** box, select **No**.
4. Click **OK**.

Note: Turning profile pictures off does not delete uploaded images from the database. If you turn profile pictures back on, uploaded profile pictures are displayed again.

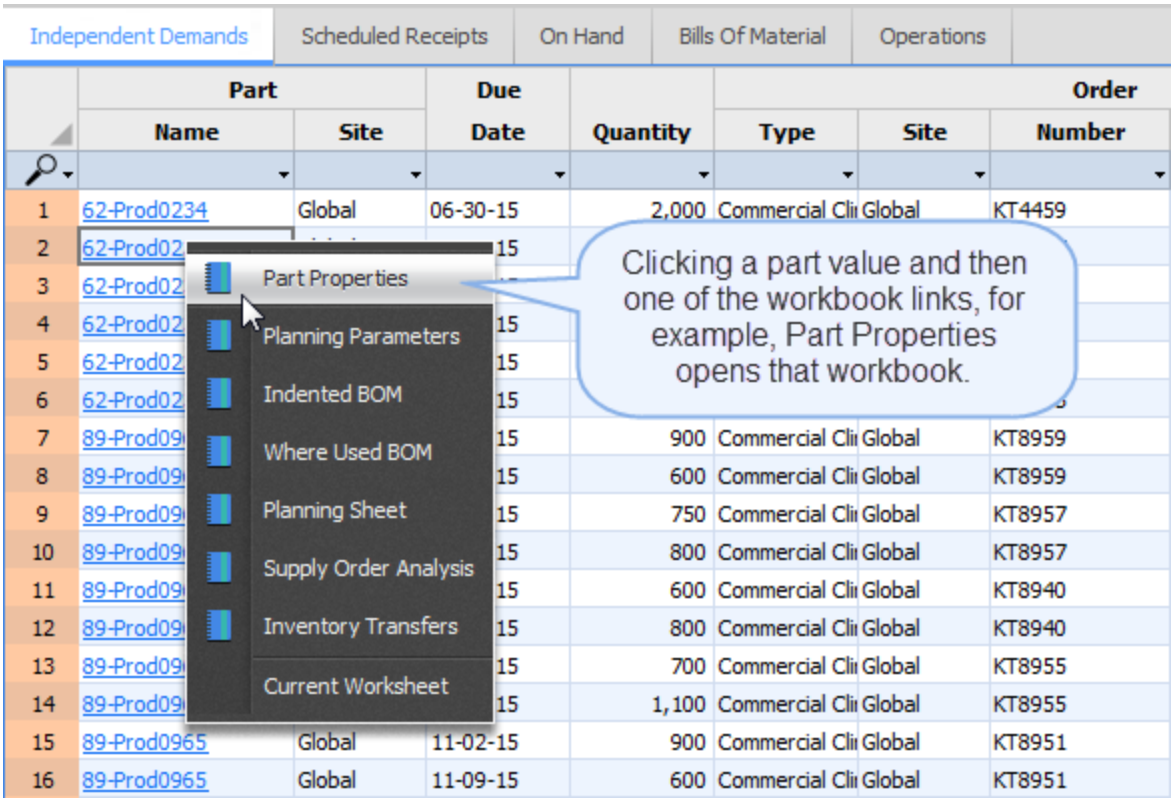
Tip: If you want to turn on profile pictures, change the setting to **Yes**.

Customizing the workbook link menu

RapidResponse worksheets that include part, reference part, constraint, project, or work center columns usually provide a contextual link menu to other workbooks and worksheets. For example, users can click on a part name in a worksheet column to open the Part Properties workbook with the selected part active.

Note: Other workbook drilling and linking capabilities are available in RapidResponse. For more information, see the *RapidResponse Resource Authoring Guide*.

The following illustration shows how the Part Properties workbook is accessed from the link menu on part column.



The links on the workbook link menu vary depending on the type of data value from which the link menu is accessed. For example, if the worksheet is based on the Part table, the link menu displays links to workbooks that contain part information and allows users to view additional data related to a selected part. For example, links might provide access to worksheets displaying a part's bill of material structure or all supply orders for a part.

Each user can only see links to workbooks they have access to. For example, users who do not have access to the Part Properties workbook will not see the Part Properties link on the link menu.

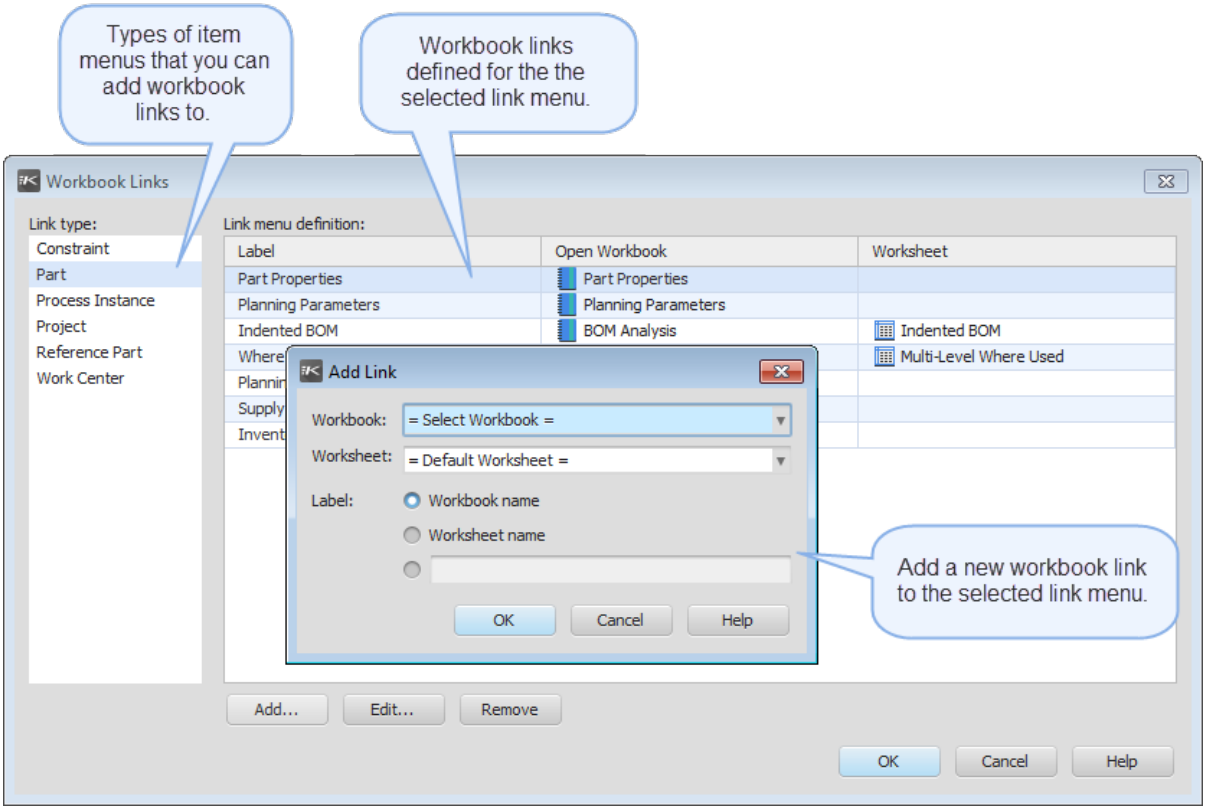
The workbook links you define for a given item are added to the standard link menu used in all worksheets displaying either part, constraint, project, or work center names. By default, these link menus contain links to some of the standard workbooks included with RapidResponse, and you should consider removing links to any of these standard workbooks which your company does not use.

Adding workbook links to the standard link menu

You can add links to the contextual link menus for part, reference part, constraint, project, or work center columns. These link menus appear for every column that displays the base key field from either the Constraint, Part, ProcessInstance, Project, ReferencePart, and WorkCenter table. This includes columns in worksheets based on other tables that contain references to the base key field in any of those tables.

You can also edit or delete existing workbook link definitions. For example, a red X next to any workbook name in the Workbook Links dialog box indicates that the workbook has been deleted from RapidResponse. This might indicate a pre-defined RapidResponse workbook, included on the default workbook link menu, which your company is not using and has previously deleted. You should delete any workbook links definitions marked with a red X.

The standard link menus are customized using the Workbook Links dialog box as shown in the following illustration. Only system administrators have access to this dialog box.



▸To add a workbook link to the link menu

1. In the **Administration** pane, under **System Settings**, click **Workbook Links**.
2. In the **Link type** area, select one of the following:
   - **Constraint**—add items to the link menu for constraint columns.
   - **Part**—add items to the link menu for part columns.
   - **Process Instance**—add items to the link menu for process instance columns.
   - **Project**—add items to the link menu for project columns.
   - **Reference Part**—add items to the link menu for reference part columns.
   - **Work Center**—add items to the link menu for work center columns.
3. Click **Add**.
4. In the **Add Link** dialog box, do the following:
   - From the **Workbook** list, select the workbook that opens when this link is clicked.
   - Optionally, from the **Worksheet** list, select the specific worksheet that opens when this link is clicked. If you do not select a worksheet, the link will open with the workbooks' default worksheet selected.
   - In the **Label** area, select the text that appears on the link menu for this link. You can select **Workbook name**, **Worksheet name** or type in your own text.
5. Click **OK**.

   The new link definition is added to the **Link menu definition** area.
6. Optionally, drag the link definition up or down to set its position on the link menu.

   Changes made in the Workbook Links dialog box will not be visible in workbook link menus until the next time you sign in to RapidResponse.

Note: You can also add workbook links to the link menu for a specific worksheet. This requires defining XML code in the Worksheet Properties dialog as discussed in "Adding workbook links to a specific worksheet" on page 621.

▸To remove a workbook link from the link menu

1. In the **Administration** pane, click **Workbook Links**.
2. In the **Link type** area, select a type.
3. In the **Link menu definition** area, select the item to remove.
4. Click **Remove**.

▸To edit a workbook link on the link menu

1. In the **Administration** pane, click **Workbook Links**.
2. In the **Link type** area, select a type.
3. In the **Link menu definition** area, select the item to edit.
4. Click **Edit**.
5. In the **Edit Link** dialog box, make any of the following changes:
   - From the **Workbook** list, select the workbook to open when this link is clicked.
   - Optionally, from the **Worksheet** list, select the specific worksheet to open when this link is clicked.

- In the **Label** area, select the text that appears on the link menu for this link. You can select **Workbook name**, **Worksheet name** or type in your own text.

6. Click **Ok**.

Adding workbook links to a specific worksheet

In some cases, you might want to add a link to the workbook link menu in a specific worksheet only. This can be done by defining the link through XML code in the worksheet's Worksheet Properties dialog box.

▸To add a workbook link to the link menu in a specific worksheet

1. In the **Explorer**, click a workbook.
2. On the **Actions** menu, click **Properties**.
3. Click the **Worksheets** tab.
4. In the **Worksheets in this workbook** box, click a worksheet, and then click **Properties**.
5. Click **Advanced**.
6. Click the **Options** tab.
7. In the text box, type or copy and paste the following XML code to reference the schema files:

```
<clientConfig xmlns="http://schemas.webplan.com/Web/ClientConfig/1.0"
xmlns:app="http://schemas.webplan.com/Web/ClientConfig/App/1.0"
xmlns:session="http://schemas.webplan.com/Web/ClientConfig/Session/1.0"
xmlns:module="http://schemas.webplan.com/Web/ClientConfig/Module/1.0"
xmlns:workbookModule="http://schemas.webplan.com/Web/ClientConfig/Modul
e/Workbook/1.0"
xmlns:workbook="http://schemas.webplan.com/Web/ClientConfig/Workbook/1.
0"
xmlns:worksheet="http://schemas.webplan.com/Web/ClientConfig/Worksheet/
1.0">
```

   After pasting, the code above may contain spaces that should not be present in the XML code. If you copy and paste this code from the PDF document, for any line that ends with a slash (/), place the insertion point at the end of that line and then press the **Delete** key.
8. Under the code inserted in the previous step, type the code defining the workbook link as discussed in "XML syntax for defining a workbook link in a specific worksheet" on page 621.
9. After inserting the appropriate code, type `</clientConfig>` as the last line of the code.
10. Click **OK**.

▸XML syntax for defining a workbook link in a specific worksheet

The following is an example of the syntax used in defining a workbook link within an individual worksheet. This example shows adding a link labelled "Where Used BOM" to the Part link menu that opens the BOM Analysis workbook with the Multi-Level Where Used worksheet selected. For a detailed explanation of the syntax, see the table following the example.

```
A → <definitions>
B → <worksheet:link id="WhereUsedBOM" extends="PartLink">
C → <label>Where Used BOM</label>
D → <workbookName>BOM Analysis</workbookName>
E → <initialWorksheetName>Multi-Level Where Used</initialWorksheetName>
      </worksheet:link>
    </definitions>
F → <layouts>
G → <worksheet:linkMenu>
H → <worksheet:linkRef ref="WhereUsedBOM" />
      </worksheet:linkMenu>
    </layouts>
```

The following table describes each element and attribute used in the syntax for adding a workbook link as shown in the example above.

Section	Description
A	The **<definitions>** element contains the properties of all links defined for the worksheet.
B	A **<worksheet:link>** element is added within the **<definitions>** element for each link you want add to the link menu in the worksheet. This element contains two attributes. The **id** attribute identifies each **<worksheet:link>** element as unique. The **extends** attribute specifies the link menu on which the link is added. There are four possible values for this attribute: • **PartLink**—the workbook link is added to the link menu for any worksheet columns that return the base key field from the Part table. • **ReferencePartLink**—the workbook link is added to the link menu for any worksheet columns that return the base key field from the ReferencePart table. • **ConstraintLink**—the workbook link is added to the link menu for any worksheet columns that return the base key field from the Constraint table. • **WorkCenterLink**—the workbook link is added to the link menu for any worksheet columns that return the base key field from the WorkCenter table.
C	The **<label>** element is optional and specifies the text for this link on the link menu. If you don't specify a label, the workbook name displays on the link menu.
D	The **<workbookName>** element specifies the workbook to be opened by this link.
E	The **<initialWorksheetName>** element is optional and specifies the worksheet that is displayed when the workbook is first opened using the link menu. If no worksheet is specified, the workbook link opens to the workbook's default worksheet.
F	The **<layouts>** element contains all workbook link definitions for a worksheet.
G	The **<worksheet:linkMenu>** element defines all links to be added to the worksheet link menu (this is in addition to any standard workbook links).
H	A **<worksheet:linkRef>** element is used to reference each workbook link definition from the worksheet's **<definitions>** element.

Setting the maximum number of command errors logged

When a user runs a data modification command, either interactively or as a scheduled task, errors can occur. The command can complete successfully if the command's error limit has not been exceeded. However, if the command fails due to errors, you can investigate the cause of the errors using the Error Details worksheet. For more information, see "Error Details worksheet" on page 457.

> **Note:** The error limit applies only to errors in the data being modified by the workbook command. It does not apply to errors that prevent the command from running, such as an invalid scenario or missing resource. The Error Details worksheet provides information about data errors only.

Data Modification Details | Error Details

	Command	Action	Source Worksheet	Updated Worksheet	Record	Column	Error
1	Write Forecast Details	2 Insert	Forecast Detail Records	Historical Demand Table for Insert Forecast Details	1	1	Key from column 'HistoricalDemandTableForInsertForecastDetails!BeginDate' already exist
2					2	1	Key from column 'HistoricalDemandTableForInsertForecastDetails!BeginDate' already exist
3					3	1	Key from column 'HistoricalDemandTableForInsertForecastDetails!BeginDate' already exist
4					4	1	Key from column 'HistoricalDemandTableForInsertForecastDetails!BeginDate' already exist
5					5	1	Key from column 'HistoricalDemandTableForInsertForecastDetails!BeginDate' already exist
6					6	1	Key from column 'HistoricalDemandTableForInsertForecastDetails!BeginDate' already exist

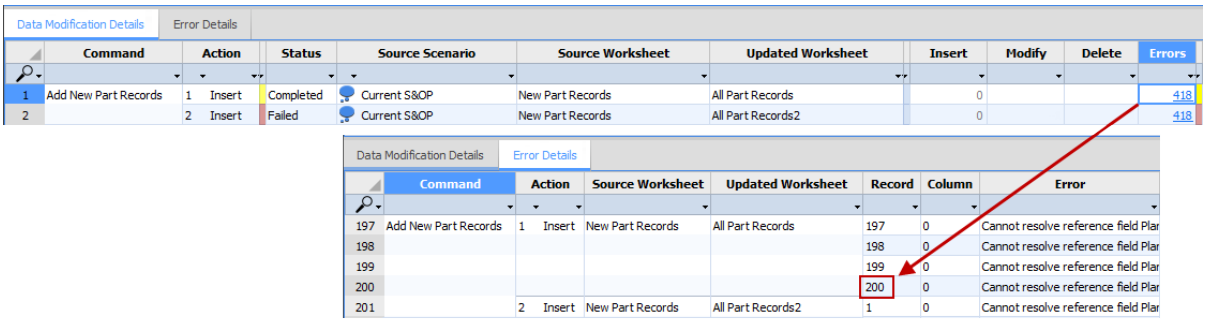
This worksheet can be opened by clicking a link in the Errors column of the following worksheets in the Automation Log workbook:

- "Automation Task Log worksheet" on page 449
- "Workbook Command Log worksheet" on page 454
- "Data Modification Details worksheet" on page 456

Users can view their personal workbook command and automation task activity in the Automation Details and Log workbook, which includes the same worksheets.

RapidResponse might return a large number of errors when a data modification command runs. You can configure the number of errors that are logged in the Error Details worksheet by changing the **Maximum errors logged for commands** setting in the Global Settings dialog box. The default value is 200, the minimum value is 100, and the maximum value is 500.

The maximum number of logged errors applies to the number of errors that should be logged for each command action. For example, in the following image, the Data Modification Details worksheet shows that the first command action returned 418 errors. However, the Error Details worksheet displays 200 errors for the action because, by default, the **Maximum errors logged for commands** setting is set to 200.

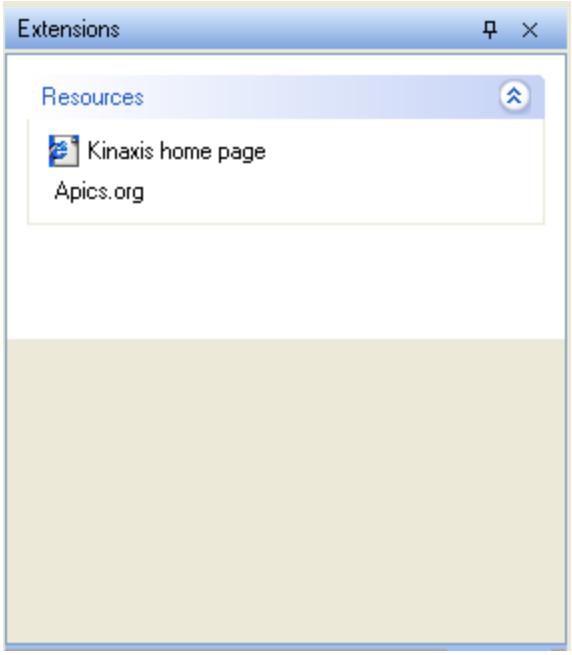


▸To set the maximum number of errors logged

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. If necessary, expand the **Automation** category.
3. In the **Maximum errors logged for commands** box, type the maximum number of errors that will be logged in the Error Details worksheet.
4. Click **OK**.

Adding custom links

The RapidResponse Extensions pane can contain links to Web sites, your intranet, Web-based applications, documents, and applications on a user's local computer. For example, you can add custom links to Web sites that your RapidResponse users might require. When a user clicks a custom link in the Extensions pane, the targeted information is opened in a new browser window. The following image shows two custom links.



On-Demand: Contact Kinaxis Customer Support for request custom links in the Extensions pane.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

System administrators can create custom links in the Extensions pane however they will require the assistance of the Master Administrator (Admin) user.

The links in the Extensions pane can be grouped into sections. Administrators control user access to specific sections or links in the Extensions pane. By default, all users have access to all custom links. To limit access, you must create an access group.

There are three steps to creating custom links:

1. Specifying the custom links in the configuration file.
2. Creating groups to control access.
3. Providing users access to custom links.

This section also includes an example of code you can use as template. For more information, see "Example code for copy and paste purposes" on page 628.

Specifying the custom links in the configuration file

The first step to creating custom links in the Extensions pane requires that you modify the **config.xml** file. This file is stored in the **C:\Program Files\Kinaxis\RapidResponse\launchpad\config** folder.

> **Caution:** Files containing invalid XML syntax can prevent RapidResponse from functioning. Before replacing the original **config.xml** file, save the modified file to another folder, and open it in browser. Files that contain invalid XML syntax open with an error message that indicates the incorrect syntax.

The following table lists the mandatory and most frequently used optional attributes that you can use to create custom links. It also provides syntax examples.

Attribute	Status	Purpose	Syntax examples
id	Mandatory	Specifies a unique identification string for the section title.	`id="myresources"`
label	Optional	Specifies the custom link text.	`label="Resources"`
allow	Optional	Specifies the user group that controls access to this section of the Extensions pane.	`allow="Extensions Resources"`
icon	Optional	Specifies an icon to display beside the link. See note below this table for more information about specifying icons.	`icon="graphic.gif"`
href	Optional for the section title. Mandatory for each link.	Specifies a relative or absolute URL to open in a new browser window.	`href="http://www.kinaxis.com"`

Notes:

- Icons can be in any graphic file format the browser supports and anything more than 16 pixels in height is cut off from display.
- By default, RapidResponse searches for graphic files in the **C:\Program Files\Kinaxis\RapidResponse\Web\en** folder. You can also specify the graphic file location as a relative path.
- If using icons, you will require access to the RapidResponse Application Server computer to store the graphic files.
- If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of RapidResponse Application Server is installed.

Example: Adding a custom section and links to the Extensions pane

The following example guides you through the process of adding a custom section titled Resources to the Extensions pane. This custom section provides users with a link to the Kinaxis home page and a link to the APICS Web site. The example is shown in the figure at the beginning of "Adding custom links" on page 624.

The following XML code has to be inserted into the **config.xml** file between **serviceDirectory** syntax to create the custom section displayed in the example illustration. Each labeled item in the illustration has corresponding XML code, which is provided below. The sections and links in the Extensions pane are referred to as "services" in the XML syntax. The bold black text is customizable, and the rest of the text is mandatory XML.

```
<services>
  A  <services id="myresources" label="Resources">
       <authorization allow="Extensions Resources" />
     <service id="myresources:source" label="Kinaxis home
       page" icon="msie.GIF" href="http://www.kinaxis.com">
  B    <authorization allow="Extensions Kinaxis Web Page" />
     </service>
     <service id="myresources:source" label="Apics.org"
       href="http:// www.apics.org">
  C    <authorization allow="Extensions Apics Web Page" />
     </service>
   </services>
</services>
```

The following table explains the XML syntax for each section.

Section	Function
A	The <services> element defines parameters for the **Resources** section of the Extensions pane, including the service ID and the section label. The optional <authorization> element specifies that a group membership will be used to control access to this custom section. If the <authorization> element is not present, all users have access to this section, regardless of group memberships.
B	This <service> element defines parameters for the **Kinaxis home page** link, including the service ID, the custom link label, icon, and the Web site URL. The optional <authorization> element specifies that a group membership will be used to control access to this custom section. If the <authorization> element is not present, all users have access to this section, regardless of group memberships.
C	This <service> element defines parameters for the **Apics.org** link, including the service ID, the custom link label, and the Web site URL. The optional <authorization> element specifies that a group membership will be used to control access to this custom section. If the <authorization> element is not present, all users have access to this section, regardless of group memberships.

You can further customize the new links on the RapidResponse menu by defining other parameters. For example, you can specify that a tooltip display when a user hovers the cursor over a link. For more information about other parameters, see "The following table lists the mandatory and most frequently used optional attributes that you can use to create custom links. It also provides syntax examples." on page 625.

After you modify the **config.xml** file, you might have to restart Microsoft IIS for the changes to be reflected in RapidResponse. If you are not authorized to do this, contact your network administrator.

Note: Because XML is case sensitive, ensure to type the XML code exactly as provided.

Creating groups to control access

The second step to creating custom links in the Extensions pane requires that you create groups to control which users are given access to the links. These groups are referred to in the **config.xml** file when you use the <authorization> element. If you want to control which users are given access to the custom links, you must create a group for each section and custom link. Only users in the group are given access to the custom links.

If you did not specify a value for the <authorization> element, or if you do not create a group with the same name as specified in the <authorization> element, the links will be available to all users.

A user administrator or system administrator can create the groups to provide access to the custom links. It is recommended you give the groups names that indicate they are used to control access to items on the Extensions pane. For more information about creating groups, see "Best practices for setting up user accounts" on page 493.

The group that controls access to the custom link must be a member of the My Applications system group. Otherwise the group is not identified as a group that controls access to a link, and the links continue to be available to all users. Only a system administrator can add members to a system group. For more information, see "To make a group a member of another group" on page 516.

For the purpose of the example discussed in this section, the following groups were created:

- Extensions Resources
- Extensions Kinaxis Web Page
- Extensions Apics Web Page

After creating the groups, you can add users or groups to them to provide access to the links.

Example code for copy and paste purposes

The following code is based on the example discussed previously in this section. You can use this code as a template for your own custom links by copying and pasting it.

```
<serviceDirectory>
<services>
<services id="myresources" label="Resources">
<authorization allow="Extensions Resources" />
<service id="myresources:source" label="Kinaxis home page" icon="msie.GIF"
href="http://www.kinaxis.com">
<authorization allow="Extensions Kinaxis Web Page" />
</service>
<service id="myresources:source" label="Apics.org"
href="http://www.apics.org">
<authorization allow="Extensions Apics Web Page" />
</service>
</services>
</services>
</serviceDirectory>
```

Providing users access to custom links

After you create the groups, only members of those groups can access the custom links. For a user to have access to a custom link, they require a user administrator place them in the group that controls access to the links.

Users with administrative permissions always have access to all custom links. The following procedures explain how to provide access to custom links.

▸To provide access to the custom links in the Extensions pane

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. On the **Groups** tab, click a group, and then click **Properties** .
3. On the **General** tab, click **Select Groups**.
4. Select the group you created to provide access to the custom link, and then click **Select**.
5. Click **OK**.

Enabling the Reference Part toggle

Some predefined RapidResponse workbooks include a part control where users can select a specific part for which to display data. System administrators can configure RapidResponse to display the **List Reference Parts** button in these workbooks. This button toggles the contents of the part list

between alternative part names that your company might be using, such as names from an old part naming system, and actual part names. For more information, see the *RapidResponse User Guide*.

You can only perform this task if you are a system administrator.

▸To enable the reference part toggle

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Allow toggling to the reference part list** box, select **Yes**.

Tip: If you want to disable the reference part toggle, change the setting to **No**.

Specifying display names for calendars

You can specify display names for calendar dates in the CalendarDate table. This allows you to provide labels for the calendars used for bucketing in crosstab worksheets, so that worksheet users see a date such as 'Aug 2008' instead of '08-01-08' for a monthly bucket for August. The following image shows an example of a crosstab worksheet with calendar display names.

Forecast Totals

		Quantity by Due Date							
		Month							
	Part	Apr 2008	May 2008	Jun 2008	Jul 2008	Aug 2008	Sep 2008	Oct 2008	Nov 2008
1	ACKIT-01	0	350	2,815	3,565	2,857	3,025	1,300	1,000
2	ACKIT-02	0	450	3,775	4,175	4,470	3,200	1,650	1,200
3	ACKIT-03D	0	300	2,250	2,700	2,438	2,138	1,100	800
4	ACKIT-03S	0	300	2,300	2,290	2,323	1,950	1,100	800
5	ACKIT-04	0	375	2,840	3,515	2,669	2,826	1,300	1,000
6	CRUISER	0	0	14,281	17,456	9,939	8,488	4,700	3,300
7	LTKIT-01	0	650	3,875	3,435	2,690	2,820	1,300	1,000
8	LTKIT-02	0	2,250	12,216	15,424	15,555	13,599	8,250	6,000
9	MOUNTAIN	0	750	7,021	7,021	4,313	3,889	3,000	3,000
10	PROCRUISER	0	0	5,252	6,085	6,361	5,613	3,150	3,000
11	PRORACER	0	750	5,700	5,700	5,875	3,250	3,000	3,000
12	RACER	0	0	3,730	6,200	6,592	3,625	3,000	3,000

The display names you specify are used in every crosstab worksheet, as long as the worksheet author selects to use the display names. If the author uses the display names but the calendar does not have display names specified, the date values are shown in the worksheet.

To specify display names for calendar units, you must create a worksheet based on the CalendarDate table and then modify the data in it.

▸To specify display values for a calendar

1. On the **File** menu, point to **New**, and then click **Workbook**.
2. In the **New Workbook** dialog box, in the **Name** box, type a name for the workbook.

3. Click the **Worksheets** tab.
4. Click **New**, and then click **Worksheet (Table-based)**.
5. In the **New Worksheet** dialog box, in the **Name** box, type a name for the worksheet.
6. In the **Table** list, click **CalendarDate**.
7. Click the **Columns** tab.
8. Click **Add Fields**.
9. In the **Add Fields** dialog box, add the following fields:
   - **Calendar**
   - **DisplayValue**
   - **Value**
10. Click **OK**, and then click **OK** again.
11. Click **Yes** to open the workbook and then click **OK** to accept the Data Settings.
12. In your worksheet, in the **Calendar** column, type the name of the calendar you want to add display values for.
13. In the **Display Value** column, type the value you want displayed for each calendar unit.
14. Click **Save Data**.
15. Repeat steps 12 - 14 for each calendar you want to specify display values for and save.
16. Commit the data changes to a scenario that you can use to update other scenarios. For example, the root scenario.

Adjusting calendars for bucketing

Worksheets can be bucketed by date, using any calendar that includes the planning date. Depending on how your calendars are defined, authors and users might not be able to use them if the planning date passes beyond the last date of the calendar.

To ensure your calendars are always available for bucketing, you can add a date in the future as the last date. For example, you can use December 31, 2037, which is the latest date recognized by RapidResponse.

Typically you only need to do this if you are using a specialized calendar that contains a specific set of dates, such as a set of historical periods.

▸To add a date to a calendar

1. Open or, if necessary, create a worksheet based on the **CalendarDate** table.
2. Select a cell containing a date in the calendar you want to add to.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Date** field, type **12-31-37**.
5. Optionally, in the **Bucket Label** field, type a label for this date.

Note: Depending on the date format your company uses, you might enter the date differently.

Tip: You can also select a date by clicking the down arrow in the **Date** field.

Specifying the separator for split orders

A character is automatically added to a line number when a user splits an order. By default a decimal point is used. However, if this character is not suitable, a system administrator can specify a different character. For example, if your company's line numbers use decimals, you can change the separator to a different character.

You can use any character as a separator. However, it is recommended you use a symbol character, such as an underscore (_) or hyphen (-).

▸To specify the separator character

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Split line separator character** box, type a character. Ensure the character chosen is not one used in your RapidResponse data set.

Note: The separator can contain multiple characters.

Configuring column headers

RapidResponse system administrators can control whether column headers and subtotal row headers are displayed with a bold font in all workbooks and scorecards. Bold headers can differentiate the headers from the worksheet data and improve the appearance of worksheets. By default, the column headers are bold.

On-Demand: Contact Kinaxis Customer Support to request bold column headers.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

You can perform this task only if you are a system administrator.

▸To specify whether column headers are bold

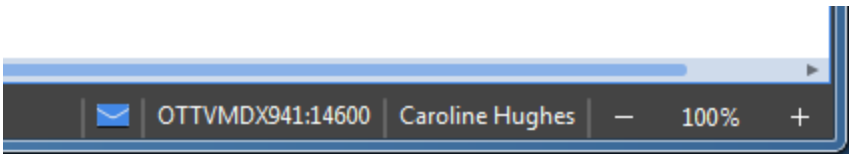
1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. In the **Configuration** worksheet, locate or insert the following record:
   - **ID—**Client_BoldHeaders
4. In the **Value** column for this record, specify one of the following:
   - **Y**—Column headers are bold.
   - **N**—Column headers are not bold.
5. Click **Save and Close**.

Notes:
- If this configuration record is not present, the column headers are bold.
- If you enable bold column headers, you should ensure the columns in your company's worksheets are wide enough to fit the wider bold header.

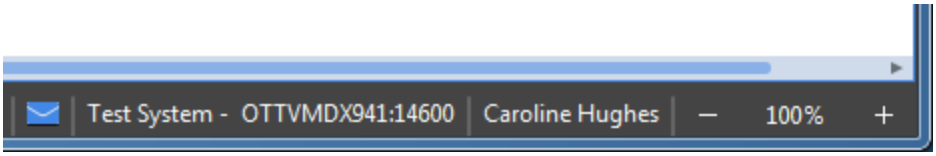
Configuring status bar identification text

This section applies to the **On-Premises** version of RapidResponse.

The status bar in the RapidResponse client shows the name of the signed in user and the RapidResponse Server the client is accessing. This information could be of use if your company has deployed RapidResponse Server in a failover configuration. For more information, see "RapidResponse Server failover clustering" on page 289. In the following image, the status bar shows the RapidResponse Server name and signed in user.



If you are deploying more than one RapidResponse Server, a test server for example, you can add an identification prefix to the server name. This can help to make it more obvious which server the RapidResponse client is accessing. In the following image, the status bar shows the RapidResponse Server name with a prefix (Test System -).



You can perform this task only if you are a system administrator.

▸To specify a RapidResponse Server prefix in the status bar

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Other Settings** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **Type** box, select Servers.
   - In the **ID** box, type **ServerType**.
   - In the **Value** box, type the text prefix for the RapidResponse Server name. For example, **Test System**.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.
6. Sign out and then sign back into RapidResponse to make the change effective.

Specifying the AND operator for feature lists

If your company is using Feature BOM capabilities in RapidResponse to model configurable end items, you might leverage the **Orders by Feature** workbook to report orders that are associated with a specific

feature or features. For reporting orders that use combinations of features, this workbook lets users specify lists of features that either "and" features together, "or" features together, or both. The comma character (,) is always used to represent "or", and by default the ampersand character (&) is used to represent "and". However, a different character can be setup to represent "and" if required. For example, if the ampersand character is expected to be used in some of your company's feature codes, then a different character should be chosen.

▸To specify the AND operator for use in feature lists

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **AND operator for features** box, type any single character. Ensure this is a character that is not expected to appear in any actual feature codes.

Notes:

- You cannot specify the comma character (,) as the AND operator for feature lists.
- The chosen character is also used as the operator to "and" features together in the **BillOfMaterial.FeatureRule** field used to define the rules that determine component usage in configurable end-items.

Defining integrated project management settings

If your company is leveraging integrated project management in RapidResponse, you must specify how RapidResponse reports a task's finish date and select the scenario used for saving project baselines. You can also activate a scheduled task included with RapidResponse if you want the project run date to be automatically updated.

Specifying how a task's finish date is reported

A task's calculated finish date is affected by several factors, such as task duration, dependencies, and assigned resources. You can specify whether RapidResponse reports the finish date as the end of the last day of the task or as the beginning of the day following the last day of the task. The end of the last day reporting method is widely used in project management programs and is the default setting.

▸To specify how a task's finish date is reported

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Analytics** category.
3. In the **Project management finish dates** list, click one of the following:
   - End of day
   - Beginning of next day

Specify the scenario for saving project baselines

A project baseline is a complete snapshot of a project plan at a specific point in time. Users can create project baselines only if a project management baseline scenario has been designated.

Integrated project management in RapidResponse is configured by Kinaxis consultants, who create scenarios specifically for project management. Typically, the scenario for saving project baselines is named Project Baseline, and is a permanent scenario, however, a different name might have been used. If you choose a scenario other than Project Baseline, ensure that it is a permanent scenario.

▸To specify the scenario where project baselines are saved

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Scenarios** category.
3. In the **Project management baseline scenario** list, click **Project Baseline**.

Note: The **Project management baseline scenario** list only includes shared scenarios that are available to you.

Automatically update the project run date

The project run date is used in RapidResponse projects to determine the status of the tasks in a project and can be used to schedule tasks. In some cases, project managers might want to manually update their projects' run dates, especially in run date driven projects. In other cases, it might be useful to have the project run date automatically, for example, if your company only uses projects that are not run date driven.

RapidResponse includes a scheduled task, Change Project Run Date that can update the run date of all your projects. You can schedule the task to update the run date at desired intervals. For more information about scheduled tasks, see the *RapidResponse User Help*.

Defining process orchestration settings

If your company is leveraging process orchestration in RapidResponse, you must specify how RapidResponse reports an activity's finish date.

An activity's calculated finish date is affected by several factors, such as activity duration, activity start date, and the instance calendar. You can specify whether RapidResponse reports the finish date as the end of the last day of the activity or as the beginning of the day following the last day of the activity.

▸To specify how an activity's finish date is reported

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Analytics** category.

3. In the **Process orchestration finish dates** list, click one of the following:
   - End of day
   - Beginning of next day

Configuring responsibility

Before users begin to track responsibility for data in RapidResponse, select a responsibility scenario. Ensure that users who need to use responsibility definitions have access to this scenario.

If resource authors have created custom responsibility definitions, and you want responsibility columns in predefined workbooks to refer to these custom responsibility definitions instead of predefined responsibility definitions, consider making changes to the responsibility role configuration.

Specifying the responsibility scenario

The responsibility scenario is used to populate the list of values for each field when users open responsibility definitions to assign responsibility for data. To open a responsibility definition, users must have View access to the responsibility scenario. For more information about assigning data using a responsibility definition, see the *RapidResponse User Guide*.

The Enterprise Data (root) scenario is the default responsibility scenario, because different RapidResponse implementations have different scenario structures but there is always a root scenario. However, Enterprise Data is not a suitable responsibility scenario. Always specify a different scenario be used in determining responsibility. The following criteria are important when selecting a responsibility scenario:

- It must be a scenario that everyone who needs to use responsibility definitions can be given View access to.
- It must be a scenario that is kept reasonably current, so that when a new record is added, responsibility for that data can be assigned.
- Choose a permanent scenario to reduce the risk of the responsibility scenario being accidentally deleted.

If you change the responsibility scenario, remember to share the new responsibility scenario with users and groups who require access to it.

▸To specify the scenario used to determine responsibility

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Scenarios** category if necessary.
3. In the **Responsibility scenario** list, click a scenario.

Caution: If the responsibility scenario is deleted, responsibility assignments are not deleted, but nobody can create new responsibility assignments or view responsibility information in worksheets until a new responsibility scenario is selected or another scenario with the same name is created and shared.

Note: The **Responsibility scenario** list only includes shared scenarios that are available to you.

Configuring responsibility roles

Some predefined workbooks included with RapidResponse use responsibility role variables in column expressions to show who is responsible for data. Because these variables are used, instead of direct references to specific responsibility definitions, you can change the responsibility definition used to populate any worksheet column that uses one of these variables by changing the responsibility definition associated with the variable.

By default, each of these variables is mapped to one of the standard responsibility definitions that comes with RapidResponse, but you can select a custom responsibility definition instead. For example if your company has a custom responsibility definition called Procurement that is used to determine who is responsible for buying parts, you can select it for the Buyers role. Now all predefined RapidResponse workbooks that display information about who is responsible for buying parts will get that information from your Procurement responsibility definition.

RapidResponse workbook authors can also use responsibility roles in column expressions.

You can change the responsibility definitions associated with responsibility roles in the Responsibility Roles worksheet in the RapidResponse Administration workbook, available to system administrators. You can also create new responsibility roles by adding records.

▸Change the responsibility definition associated with a responsibility role

1. In the **Administration pane**, under **System Settings**, click **Configuration**.
2. Select the **Responsibility Roles** worksheet tab.
3. In the **Responsibility Definition** column, type the name of the responsibility definition you want to use for that role.
4. Click **Save Data**.

Specifying the annual plan target scenario

If your company maintains an annual plan in RapidResponse, values from the annual plan can be used as scorecard targets. To ensure that scorecards use annual plan data from correct scenario, change the annual plan target scenario any time there is a change to the scenario specified in resources that your company uses to maintain its annual plan.

For information about predefined resources that can be used to maintain the annual plan, see the *RapidResponse Applications Guide*. For information about editing resources, see the *RapidResponse Resource Authoring Guide*.

In order to create scorecards that use annual plan targets, or view annual plan targets in a scorecard, users must have access to the annual plan target scenario. Therefore, ensure that all users who are expected to create or use scorecards with annual plan targets have access to the scenario that you specify.

▸To specify the annual plan target scenario

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Scenarios** category.

3. In the **Annual plan target scenario** list, click a scenario. Only shared scenarios can be selected, and it is recommended that you select a permanent scenario.

> **Note:** The default annual plan target scenario is Baseline, which is commonly used to store annual plan data.

Specifying whether historical data is editable

Historical data is typically intended for reference and reporting. However, some processes require adjustments to historical data, such as forecast adjustments or copying orders into history to create waterfall reports. Typically, only administrators are permitted to modify the data in historical tables, however, if these operations are performed regularly, you might want to allow some users to edit this data.

The following tables can be made editable for general users:

- HistoricalDemandActual
- HistoricalDemandHeader
- HistoricalDemandSeries
- HistoricalDemandSeriesDetail
- HistoricalPartKPI
- HistoricalReceipt
- HistoricalReceiptHeader
- HistoricalSupplyActual
- HistoricalSupplyHeader
- HistoricalSupplySeries
- HistoricalSupplySeriesDetail

By default, only administrators are able to edit the data in these tables. However, you can optionally allow general users to also edit data in these tables. After making this change, users who have access to a worksheet based on any of these historical tables can edit, insert, or delete values in the table, depending on how the worksheet has been configured.

If you allow users to edit historical data, you should consider creating a group to control access to the historical tables, and revise workbooks to only allow users in this group to edit data in the historical columns. For more information about configuring editability in worksheets, see the *RapidResponse Resource Authoring Guide*.

▸To allow editable historical data

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. In the **Global Settings** dialog box, under **Client**, click **Allow general users to edit historical data**.
3. Select **Yes**, and then click **OK**.

> **Note:** If you change the value of this setting, users can edit data in any of the tables listed above. If you want only some of the tables to be editable, you can restrict access to the others by overriding editing in worksheets.

Configuring add-ins

Custom applications, known as “add-ins,” can be added to RapidResponse to extend base functionality.

On-Demand: Kinaxis Customer Support is responsible for registering and configuring RapidResponse add-ins. Once registered and configured, a RapidResponse administrator needs to provide users access to add-ins. For more information about providing access, see "Providing access to add-ins" on page 640.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

As a RapidResponse administrator you are responsible for registering and configuring add-ins, and providing users with access to them.

For information about creating custom add-in applications, contact Kinaxis Customer Support.

The add-in developer needs to provide the system administrator information to register and configure the add-in. There are three steps to registering and configuring add-ins.

1. "Storing the add-in in a network location" on page 638.
2. "Registering the add-in’s network location" on page 638
3. "Configuring the add-in’s properties" on page 639

After completing these steps, administrators need to provide users access to add-ins. You can only configure add-ins if you are a system administrator.

Storing the add-in in a network location

The first step to registering and configuring an add-in is store it in an accessible network location. It is recommended that add-ins be stored as follows:

- On the same computer as RapidResponse Server and within the folder structure that contains RapidResponse Server. This provides easier maintenance for both security backup and security permissions, as well as a central location for all add-ins.
- Each add-in, and its accompanying files, should be stored in a separate folder. For example:
  - C:\RapidResponse\Add-Ins\add-in1
  - C:\RapidResponse\Add-Ins\add-in2
  - C:\RapidResponse\Add-Ins\add-in3

  Creating a separate folder for add-ins adds more security to your system because only the folder containing the add-in needs to be made available to the client computers.

Note: Add-in files can be stored on any computer on the network. However, the network account for any user running the add-in must be configured to access the relevant network file locations.

Registering the add-in’s network location

The second step to implement an add-in is to register the network location where it is stored.

▸To register the network location for an add-in

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Add-In Locations** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **Location ID** box, type an identifying name for the add-in; for example, **MyAddIn**.
   - In the **Path** box, type the network path of the add-in's location, like this: **\\<server name>\<folder name>.** For example: **\\RapidResponseServer\addins**
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.

Note: If users attempt to access an add-in registered with a server name and are unable to connect, use the IP address instead.

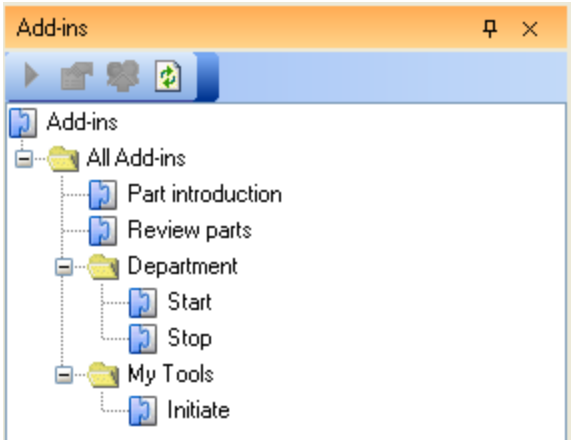
Configuring the add-in's properties

The third step to implement an add-in is to configure its properties. Many of the properties are based on how the add-in was developed. You might require information from the add-in's developer to complete this step.

▸To configure an add-in's properties

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Add-ins** worksheet tab.
3. On the **Edit** menu, click **Insert Record**.
4. Type the add-in properties in each field. Detailed information about the properties is available in the table that follows this procedure.
5. Click **Save** to insert the record or click **Save and Close** to insert the record and close the **Insert** dialog box.
6. Sign out and then sign back into RapidResponse to make the add-in's properties effective.

Field name	Description
Name	Specifies a unique name for the add-in. This name is only visible to administrators and can also be used by other add-ins to call this add-in.
Location	Specifies the network location of the add-in. This must be the same value that you typed in the **ID** box when you completed the procedure "To register the network location for an add-in" on page 639. Valid values are all records with a Type of **FileSystemAddIn** on the Configuration worksheet.
File Name	Specifies the add-in's filename including extension. For example, **MyAddin.vbs**.
Parameters	Specifies any parameters that are included in the command string each time the add-in is run. These parameters might constrain what the add-in does, how it will run, or the resources that are available to it while it runs. Separate multiple parameters by a comma.

Field name	Description
Mode	Specifies whether users can perform other RapidResponse tasks while the add-in runs. Set to one of the following: • **Foreground—**add-ins will run in the foreground. The user is prevented from performing any other tasks within RapidResponse until the application has finished • **Background—**add-ins will run in the background. The user can continue with RapidResponse activity while the add-in runs.
Message	Specifies whether a notification message is displayed when an add-in is executed. The run-time message tells the user that the add-in is running (for foreground applications), or has been launched (for background applications.)
Command	Specifies the add-in name users see in the Add-in pane. To have the add-in display in a subfolder, precede the add-in name with the folder name and a forward slash (/) character. For example, **Department/Start** would display as follows in the Add-in pane:  Leave this field blank if the add-in will not be available to users; that is, if the add-in will only be called by another **add-in**. If blank, only administrators can see the add-in in the pane and it will use the name specified in the Name field.
Notes	Descriptive text that displays in the Add-In Properties dialog box. The notes could include special instructions for running an add-in.

Note: If an add-in displays a dialog box that requires a response from the user, the client freezes. To remedy this situation, you must stop and restart the RapidResponse Server to give the user access to RapidResponse again.

Providing access to add-ins

To run an add-in, a user requires a user administrator share the add-in with them or add them to a group that has had the add-in shared with it.

Although users with administrative permissions can always view a listing of add-ins in the Add-ins pane, they still require an administrator (even themselves) to share the add-in to them to run it.

▸**To share an add-in**

1. In the **Add-ins** pane, select an add-in.
2. Click **Share** .
3. Click **Select Names**.
4. In the **Select Names** dialog, do the following:
   - On the **Users** tab, select each user you want to share the add-in with, and then click **Share with**.
   - On the **Groups** tab, select each group you want to share the add-in with, and then click **Share with**.
5. Click **OK**.

Notes:

- Custom help can be created for add-ins. for more information, see "Customizing help and documentation settings" on page 613.
- To take away a user's or group's access to an add-in, select them from the **Name** list and then click **Remove**.
- After being provided access, users cannot access the add-in until they sign out and sign back in to the RapidResponse.

Tips:

- You can also share an add-in with a group using the Group Properties dialog box. For more information, see " Assigning resources" on page 529.
- To find out more about the people you can share add-ins with, move the pointer over their names.

RunAddin command

Add-in applications can be scheduled to run at specific times using the RapidResponse RunAddin command. For more information about this command, see "RunAddin command" on page 407.

Configuring data origin for record modifications

This information applies to On-Premises RapidResponse.

By default, changes made to data are assigned a User data origin, which identifies the record as originating in RapidResponse. These records, if committed to the Enterprise Data scenario, are automatically persisted and are not managed by data updates. For more information about data origins, see the *RapidResponse Data Integration Guide*.

If this behavior is not desirable, system administrators can specify a value for the SetRapidResponseOriginOnModify processing rule to control whether the User data origin is set when the record is modified. If this processing rule is not present or is set to True, the records that have been

modified have the User origin applied and are not managed by data updates. If this processing rule is set to False, all records included in a data update are updated, which might overwrite your modifications.

If you modify the SetRapidResponseOriginOnModify processing rule to be False, any existing records with the User data origin are not modified. These records continue to be persisted and ignored by data updates.

▸To disable the User data origin when modifying data

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the toolbar, click **Insert Record**.
4. In the **Insert Record** dialog box, specify the following:
   - **ID**—SetRapidResponseOriginOnModify
   - **Value**—False
5. Click **Save and Close**.
6. Restart RapidResponse Server.

CHAPTER 43: Customizing RapidResponse user settings

Configuring printed report settings 643
Setting password security options 648
Setting Message Center options 650
Setting file size limits for importing data 653
Specifying email settings 655
Setting the worksheet record limit 657
Setting the record deletion warning threshold 659
Changing image upload size limits 660
Setting hierarchy limits 660
Options for importing Excel data to scenarios 662
Making data formats available to users and resource authors 663
Turning unsaved workbook changes warning on or off 668
Defining time zones 669
Overriding the Everyday calendar name 671
Configuring settings for automation tasks 671
Specifying file location folders 676
Migrating user groups 677

As a system administrator you can control the RapidResponse user experience by setting default settings for many options to meet the specific needs of your company. For example, you can specify the look for printed reports throughout your organization including standardizing standard headers and footers.

The RapidResponse system administrator is also responsible for setting password security options for the RapidResponse system.

Several other customization points are discussed in this chapter including setting file location for reports generated by alerts or specifying the RapidResponse worksheet record limit to ensure that users don't experience poor performance due to working with a large amount of records. As well, you can set default data formats for new user accounts and control which data formats are available to users and define time zones used by RapidResponse.

Configuring printed report settings

RapidResponse uses Portable Document Format (PDF) functionality as part of the printing process. When a report is printed, a PDF document is created and the RapidResponse user can then send the document to their printer.

Users require a PDF viewer application such as Adobe Reader or Preview for Mac OS to print reports.

System administrators can customize the appearance of printed reports for RapidResponse users by specifying the font be used for all printed reports. As well, system administrators can set page limits for printed reports and impose standard headers and footers.

You can only perform these tasks if you are a system administrator.

Setting font options

Across an entire RapidResponse system, only one font can be used for all printed reports (generated in PDF format). The initial default font used in all printed reports is Arial. To change the font, you can choose a PDF reader font, an Asian font for Asian data, or any other font available on the server where RapidResponse is installed. If you are using the On-Premises version of RapidResponse, you can use any other font available on the Web server where RapidResponse Application Server is installed.

▸To use a specific font in all printed reports

1. In the **Administration** pane, under **System Settings**, click **Print Settings**.
2. In the **Font in printed reports** section, do one of the following:
   - To use a PDF reader font, click **PDF**, and then click a font from the list. This setting is recommended for optimal performance because it generates the smallest PDF document file.
   - If you have users who work with Asian data, click **CJK**, and then click a font from the list. If you select a CJK font, Microsoft Windows users who do not have an Asian version will need to download an Asian font pack for Adobe Reader from the Adobe Web site.
   - To use another font, click **Other,** and then click a font from the list. The fonts in this list are the ones available on the server where RapidResponse is installed.
3. Click **Save**.

Notes:

- System fonts, Type 1 fonts, and OpenType fonts that do not allow for document embedding are not supported in RapidResponse.
- If your users might be printing reports that use characters from more than one Asian or Eastern European language, it is recommended that you set the default font to a Unicode font that supports the different language characters. For example, the Arial Unicode MS font that is included with Microsoft Office supports characters from many language sets.

Setting the page limit for PDF reports

When RapidResponse users print reports (worksheets and scorecards), printable PDF documents are generated. PDF reports can also be generated by RapidResponse alerts. By default, the maximum number of pages that can be contained in printable reports is 200. The page limit can be changed by system administrators.

▸To set the PDF report page limit

1. In the **Administration** pane, under **System Settings**, click **Print Settings**.
2. Type a value in the **Maximum number of pages in printed reports box**.

Caution: Increasing the PDF page limit might result in slower or unpredictable RapidResponse performance.

Setting standard headers and footers

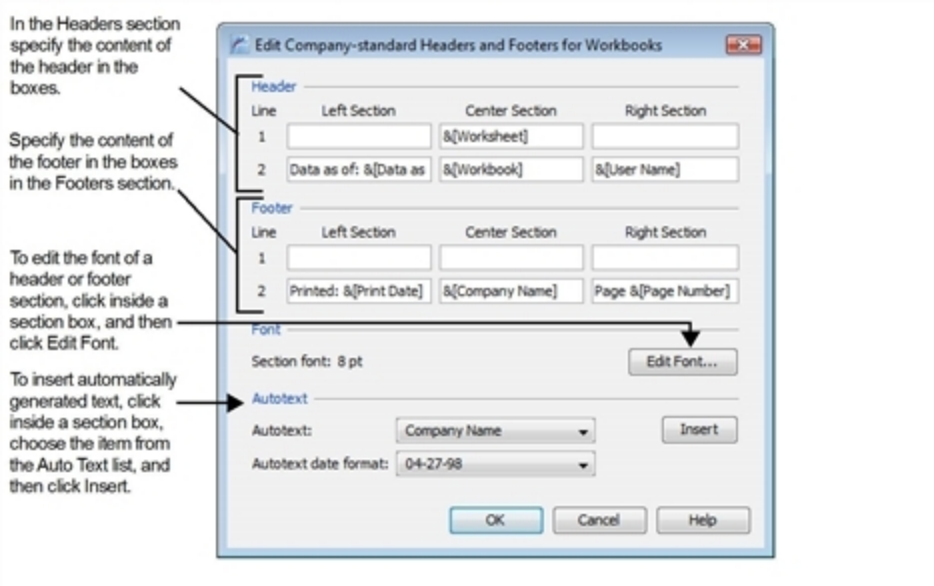
System administrators can impose company-standard headers and footers in all shared workbooks and shared scorecards that are printed by RapidResponse users, thereby ensuring a consistent look throughout your organization. Private worksheets and scorecards created by users are not affected. Different standard headers and footers can be set for worksheets and scorecards.

When you standardize headers and footers, users cannot edit headers and footers when printing shared worksheets and scorecards. If you subsequently turn off the standardized headers and footers, each user's personal header and footer settings are restored. Every user can edit headers and footers in their private workbooks and scorecards, but when they share their workbooks and scorecards, the standard headers and footers override the custom ones.

Changes to header and footer settings take effect the next time the user signs in to RapidResponse. For example, if the administrator turns on standard header and footer formats while a user is signed in, the user does not see the effects of the changes until the next time she signs in.

If more than one RapidResponse system administrator is updating the company-standard headers and footers at the same time (their sessions overlap), they will not see the effect of each other's changes. The settings of the administrator who saves her changes last are saved. It is recommended that one user with system administrator privileges be given the responsibility of managing company-standard header and footer formatting.

The following illustration displays the dialog box for editing standard headers and footers for workbooks. The dialog box for editing standard headers and footers for scorecards is almost identical. You can refer to this illustration when setting standard headers and footers for scorecards.



When setting the header or footer, you can specify that certain information in the header or footer be automatically generated during printing. For example, you can ensure that the currently selected filter name displays in the header or footer. The following table lists the items that can be automatically generated by inserting AutoText code. When you insert an AutoText item, the AutoText code displays in the box. It consists of the text from the AutoText items list in square brackets, preceded by an ampersand (&), for example, `&[Filter]`. The items available in the Auto Text list depend on whether you're printing a workbook or a scorecard summary.

AutoText item	Description of inserted information
Company Name	Your company name as specified in the software license keys.
Constraint	Name of the selected constraint. The output is blank if a Constraint control is not applicable to the resource being printed. Not available when setting headers or footers for scorecards.
Filter	The name of the currently selected filter.
Filter: Private/Shared	Displays whether the filter is shared or private. Insert this item in the same section of the header or footer as the filter item.
Model	The name of the selected model. The output is blank if a Model control is not applicable to the resource being printed.
Data as of Date	The date when data from an enterprise data source was last imported into RapidResponse. If your company has multiple sites, the date that users see in a printed report might not be accurate for the site that they have selected. For example, assume a user is viewing data from the Chicago site, for which data was last updated on May 4, 2008. The data for site Atlanta, however, was updated on May 6, 2008; therefore, the date printed in the report is May 6, 2008.
Page Number	The number of the page being printed.
Part	The name of the selected Part. The output is blank if a Part control does not apply to the resource being printed. Not available when setting headers or footers for scorecards.
Pool	The name of the selected pool. Blank if not applicable to the printed resource, or if the Inventory Pooling functionality is not enabled by your organization.
Print Date	The date the report was printed. The date on the computer where RapidResponse is hosted. The date format is determined by the item selected in the AutoText date list.
Project	The name of the selected project. The output is blank if a Project control does not apply to the resource being printed. Not available when setting headers or footers for scorecards.
Scenario	The name of the currently selected scenario. Not available when setting headers or footers for scorecards.
Scenario: Private/Shared	Displays whether the scenario is shared or private. Insert this item in the same section of the header or footer as the scenario item. Not available when setting headers or footers for scorecards.
Scorecard	The scorecard name. Not available when setting headers or footers for worksheets.
Site(s)	The name of the currently selected site or site filter.

AutoText item	Description of inserted information
Time Zone	The time zone of the computer where RapidResponse is hosted. This is useful if the worksheet contains a column of date values, which are always displayed in the time zone of the Web server computer, and you want to print that time zone.
User ID	The user ID of the user printing the report.
User Name	The user name of the user printing the report.
Work Center	The name of the selected work center. The output is blank if a Work Center control does not apply to the resource being printed. Not available when setting headers or footers for scorecards.
Workbook	The workbook name. Not available when setting headers or footers for scorecards.
Workbook: Private/Shared	Displays whether the workbook is shared or private. Insert this item in the same section of the header or footer as the workbook item. Not available when setting headers or footers for scorecards.
Worksheet	The worksheet name. Not available when setting headers or footers for scorecards.

After you set the company-standard headers and footers, you can preview your settings by printing a sample report. For more information about printing, see the *RapidResponse User Guide*.

▸To set company-standard headers and footers for printed reports

1. In the **Administration** pane, under **System Settings**, click **Print Settings**.
2. In the **Company-standard headers and footers** area, do one of the following:
   - Select the **Workbooks** check box, and then click **Edit**.
   - Select the **Scorecards** check box, and then click **Edit**.
3. In the **Header** or **Footer** section, click in the box where you want to insert text, and do any of the following:
   - To insert text that is automatically generated during printing, in the **AutoText** list, click the item you want to insert, and then click **Insert**. For information about the items you can choose, see the previous table.
   - To insert fixed text, type the constant text you want.
4. In the **AutoText date format** list, click a date format. This date format applies to all **AutoText** dates.
5. Click **Save**.

▸To edit the font of headers and footers

1. In the worksheet or scorecard **Edit Company-standard Headers and Footers** dialog box, click inside one of the boxes where you specify header or footer content, and then click **Edit Font**.
2. Set the font options, and then click **OK**.

Notes:

- The font is changed only for the text in the individual box. To change the font for each

header or footer element, you must change the font in each box.

- If you click **Cancel** in the main **Edit Company-standard Headers and Footers** dialog box, any changes made to the fonts are not saved.

Setting page breaks

In worksheets that contain a subtotal row, you can specify that a page break be inserted after each subtotal row. For more information, see the *RapidResponse User Guide*.

Setting password security options

To ensure the security of your RapidResponse implementation, system administrators can set security options for user passwords to minimize the risk of unauthorized access to your company's data. For example, you can set the maximum number of days for which a password is valid and specify the minimum password length.

If you have implemented single sign-in in your environment, users do not need their passwords to sign in. In this case, you should not modify these options because users cannot change their passwords. For more information about single-sign in, see " Configuring single sign-in for On-Premises" on page 835.

▸To set password security options

1. In the **Administration** pane, under **System Settings**, click **Password Security Policies**.
2. In the **Password Security Policies** dialog box, select the check box for each security option you want to enable and type a value in the appropriate boxes.

Security option	Description
Lock out user account after...consecutive sign-in failures	Prevents users from signing in to RapidResponse after the specified number of consecutive sign-in failures. For more information, see "Unlocking a user account" on page 599.
Maximum password age	Specifies the maximum number of days for which a password is valid. When their password expires, users are prompted to change it. From the **Users** worksheet in the **User and Groups** workbook, you can review the last time a password was changed for a user. For more information, see "To review the password age for individual users" on page 649.
Minimum password length	Specifies the minimum number of characters for a password. The default value for this option is 8. Specifying a number of characters lower than 8 is not recommended.

Security option	Description

Password complexity requirements:	Select the level of complexity users' passwords must meet to be considered valid. The available values are:
	• **None**—The password can contain any character.
	• **Moderate**—The password must meet at least two of the following requirements:
	  • Includes at least one letter (a-z, A-Z)
	  • Includes at least one number (0-9)
	  • Includes at least one special character (!, @, #, &, ...)
	• **Strict**—The password must meet all of the following requirements:
	  • Includes at least one upper-case letter (A-Z)
	  • Includes at least one lower-case letter (a-z)
	  • Includes at least one number (0-9)
	  • Includes at least one special character (!, @, #, &, ...)

Enforce password history	Prevents users from using a previous password when they change their password. You can specify the number of previous passwords that are stored for each user.

If you are using On-Premises RapidResponse, no password security policies are set by default. However, if you are using the On-Demand RapidResponse service, passwords are preconfigured with the following settings:

- User accounts are locked out after four failed attempts
- Passwords must be changed every 90 days
- Passwords must be eight characters or longer
- Passwords use Moderate complexity requirements
- Password history is enforced, and the previous 10 passwords are remembered

If you change the password complexity requirements, the new requirement is enforced the next time a user changes their password.

Note: The password length and complexity requirements are displayed to users wherever they specify their password.

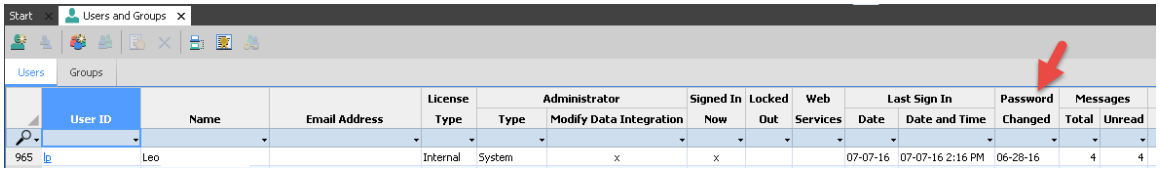
▸To review the password age for individual users

From the **Users** worksheet in the **User and Groups** workbook, you can review the last time a password was changed for a user. This information can be useful in better understanding password usage and policies. It could also be used in conjunction with the **Maximum password age** security policy.

You can create an alerts based on the **Users** worksheet. Consider creating an alert that reports passwords that exceed a date age threshold.

1. In the **Administration** pane, under **User Accounts**, click **Users and Groups**.
2. Click the **Users** tab and review the **Password Changed** column. This column can be sorted by

ascending or descending date.



Notes:

- For more information about RapidResponse security features, see "Security and infrastructure" on page 45.
- Changes made to password policies are not retroactively applied to user accounts. For example, assume the minimum password length is changed from six characters to eight characters. Users will passwords of less than eight characters are not forced to immediately change their password. However, once the user does attempt to change their password, they will be forced to comply with the current password policies.

Setting Message Center options

System administrators can control Message Center settings to limit memory usage and improve system performance.

Message limits

System administrators can limit the number of messages each user can have in their Message Center. When a user is at the limit and receives a new message, the oldest message is deleted. The limit can be decreased to save storage space, or can be increased to prevent lost messages. The default message limit is 1,000. The minimum is 100. If you change the limit, you should inform users of the change.

The message limit also defines the maximum number of entries that can appear in a **Scenario Properties** tab's Activity Log tab. For more information about the **Scenario Properties** tab, see the *RapidResponse User Guide*.

▸To set the message limit

1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. In the **Maximum number of messages per user** text box, type a number greater than 100.

Notes:

- The text box should contain only numbers, no decimals or thousands separators.
- If any invalid characters are included in the subject or body of a message, RapidResponse automatically removes the invalid character. For a list of unsupported characters recognized as invalid in RapidResponse, see "List of non-printable characters" on page 448.

Message age deletion thresholds

Messages and links to resources, reports, and web addresses in messages (and email messages) are stored in the RapidResponse database. By default, they are automatically deleted after 45 days. This setting can be modified by both On-Demand and On-Premises system administrators.

▸To change the age deletion threshold for messages

1. In the **Administration** pane, under **System Settings**, click **Schedule System Tasks**.
2. Click the **Auto-delete Configuration** tab.
3. Locate the **Messages** entry, and in the **Maximum Record Age (Days)** column type in the number of days to preserve messages.

Note: For more information about auto-delete, see " Automatic deletion of system records" on page 277.

Message Center file attachment limit for opening

RapidResponse can also control the maximum file attachment size that can be opened from a message. Any attachment larger than the limit cannot be directly opened in RapidResponse. Instead, users who attempt to open a file that exceed the limit are prompted to save the file to their system and then open the file with an associated application.

By default, the maximum file attachment that can be opened from Message Center is 2 MB and it can be modified by system administrators.

▸To set the maximum attachment size that can be opened

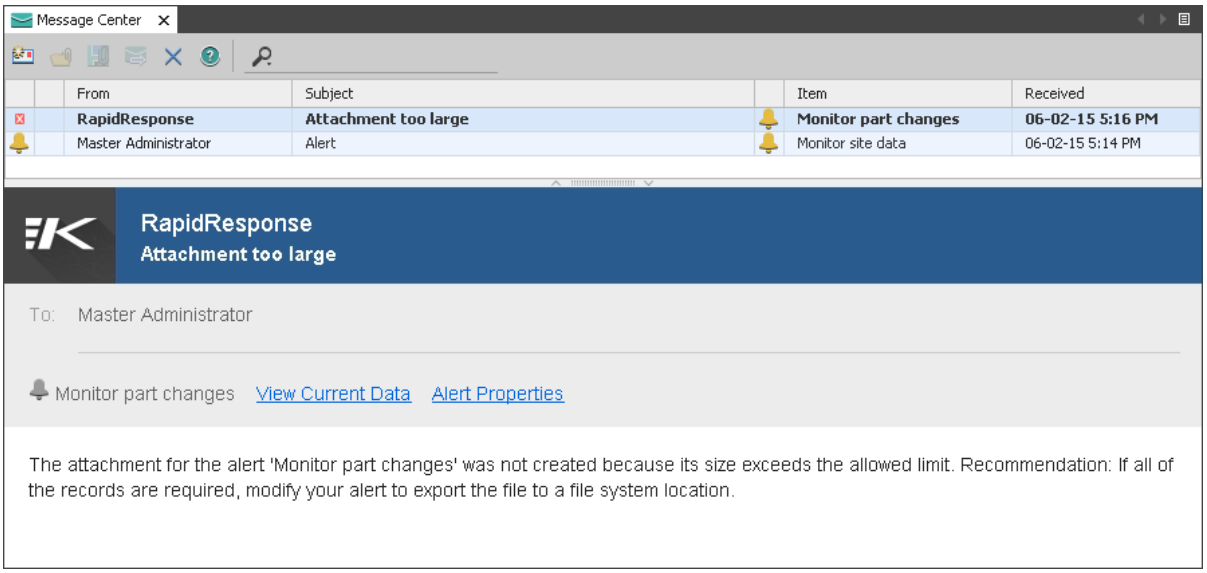
1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. In the **Maximum size of attached files to open** box, type or select the size in MB.

Caution: Increasing the maximum attachment size increases the amount of system memory used, which could have negative impacts on system performance.

Message Center file attachment size limit

RapidResponse also controls the maximum file size of Message Center file attachments. The default setting is 10 MB and it can be modified.

If RapidResponse generates an attachment that exceeds the maximum file size then the Message Center message that includes an error description and the process that generates error fails. The following image shows an example of an alert that generates a file that exceeds the maximum size.



On-Demand: You can request to have the maximum file size of Message Center file attachments modified if necessary. For more information, contact Kinaxis Customer Support.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

The default setting of 10 MB can be modified by an administrator who has administrative rights to the computer where RapidResponse Server is installed.

Changing the maximum file size requires you to stop the RapidResponse Service Host, modify its configuration file, and then restart the Service Host.

Changing the maximum attachment size requires an XML editor. The maximum attachment size is specified in the `<eMailAttachment>` element, and is expressed in bytes.

Caution: Increasing the maximum attachment size increases the amount of system memory used, which could have negative impacts on system performance.

▸To stop the RapidResponse Service Host

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.

2. In the **Services** window, click the **RapidResponse Service Host** service.
3. On the **General** menu, click **Stop**.

▸To set the maximum attachment size shown in Message Center

1. In Windows Explorer, navigate to the **C:\RapidResponse\Program\ServiceHost** folder.
2. Open the **ServiceHost.exe.config** file in an XML or text editor.
3. In the `<eMailAttachment>` element, change the value of the `maximumSize` attribute.
4. On the **File** menu, click **Save**.

▸To restart the RapidResponse Service Host

1. In the **Services** window, click the **RapidResponse Service Host** service.
2. On the **General** menu, click **Start**.

Setting file size limits for importing data

RapidResponse limits the file size that can be imported into a scenario or uploaded for previewing before the data file is included in the data import process. By default, the limit is 50 MB but this can be changed.

> **Caution:** Increasing the file size limit can allow you to import very large files but this can degrade system performance. It can also make your system more vulnerable to denial of service attacks that are carried out by uploading very large files. For these reasons, increasing the limit above the default is not recommended in most cases.

On-Demand: You can request this limit be changed if necessary. For more information, contact Kinaxis Customer Support.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

You can modify this setting if you have access to the computer where RapidResponse Application Server is installed. Changing the maximum file size requires you to modify three settings in a RapidResponse Application Server configuration file with an XML (or text) editor. The maximum file size is specified in the elements listed in the following table.

The settings are expressed in kilobytes or bytes, as indicated in the procedure. To convert MB to KB, multiply by 1024. To convert MB to bytes, multiply by 1048576.

File	XML element to modify
C:\Program Files\Kinaxis\RapidResponse\web\web.config	• `<configuration> <RapidResponse> <appletParameters> <param name="MAXIMUM_FILE_TRANSFER_SIZE">` • `<configuration> <system.web> <httpRuntime maxRequestLength>` • `<configuration> <system.webserver> <security> <requestFiltering maxAllowedContentLength>`

If you modify the file size limit, you should notify any users who perform these imports to clear their Java cache. This ensures the updated setting is applied to their environment, and prevents issues with files being incorrectly rejected due to their size.

▸To modify the file size limit

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. On the computer where RapidResponse Application Server is installed, open the **Web.config** file located in the **C:\Program Files\Kinaxis\RapidResponse\Web** folder with an XML or text editor.
2. In the `<appletParameters>` section, locate the `<param name="MAXIMUM_FILE_TRANSFER_SIZE">` element.
3. Modify the number in the **value** attribute to the file size you want, expressed in kilobytes.

   For example, **value="16384"** to change the file size limit to 16 MB.
4. In the `<system.web>` section, locate the `<httpRuntime>` element.
5. Modify the number in the **maxRequestLength**attribute to the file size you want, expressed in kilobytes.

   For example, **maxRequestLength="16384"** to change the file size limit to 16 MB.
6. In the `<requestFiltering>` section, locate the `<requestLimits>` element.
7. Modify the number in the **maxAllowedContentLength** attribute to the file size you want, expressed in bytes.

   For example, **maxAllowedContentLength="16777216"** to change the file size limit to 16 MB.
8. Save the changes.

Notes:

- If your implementation of RapidResponse includes more than one RapidResponse Application Server, ensure to repeat this procedure on every computer where an instance of RapidResponse Application Server is installed.

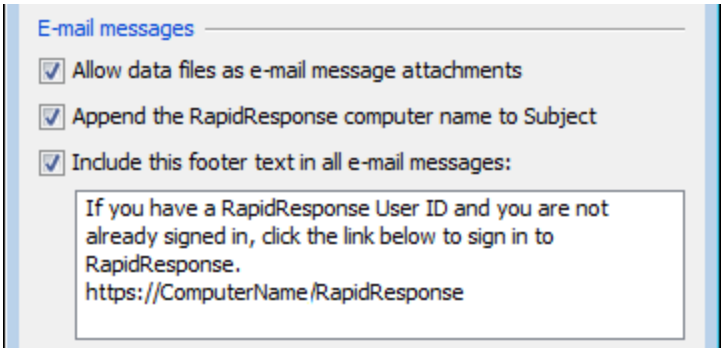
- Users can import a maximum of 500,000 records into a crosstab worksheet, regardless of whether this volume of data is smaller than the file size limit you specify.

Specifying email settings

System administrators can specify that standard footer text be included with every email message RapidResponse sends. This footer can be used to add your company's legal or confidentiality disclaimer, information about your company for externally-based users, or links to RapidResponse for internal-type users or to your company's Web site for external-type users.

The footer is plain text. However, many email systems automatically interpret properly formatted URLs as links. For example, the text **https://rapidresponse.kinaxis.com** is interpreted as a link in Microsoft Outlook, and anyone receiving email from RapidResponse in Microsoft Outlook is able to click it to sign in to RapidResponse (this example only applies if you are using the On-Demand RapidResponse service).

The footer cannot contain any HTML formatting. Links must be entered with the complete URL, and no link text can be specified, as shown in the following illustration.



To increase security, you can disable file attachments in email messages sent from RapidResponse. This can prevent your company's data from being sent to people outside the company, but also prevents externally-based users from receiving reports by email.

RapidResponse administrators can also specify whether to include the name of the computer where RapidResponse is installed in email messages generated by RapidResponse. The computer name is appended to the subject of the message. This might be useful in troubleshooting situations if you have more than one RapidResponse system, for example, a test system.

▸To add a standard email footer

1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. Select the **Include this footer text in all email messages** check box.
3. Edit or add to the text in the text box.

   If you want to keep the sign-in URL in the email footer, you must replace the default URL with the one users sign in to RapidResponse with. If you have both internally-based and externally-based users, you should include the URLs both types of users use to sign in.

▸To disable attachments in email messages

1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. In the **Message Center and Email** dialog box, under **Security**, clear the **Allow data files as email message attachments** check box.

Notes:

- For more information about email settings, see "Configuring email support" on page 276.
- If you do not allow attachments in email messages, ensure you inform users of that fact. All reports generated by alerts are sent as attachments, and users who receive alert notifications by email will not receive the reports if attachments are disabled.

▸To add the RapidResponse computer name to email messages

1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. Select the **Append the RapidResponse computer name to Subject** check box.

Note: On-Premises only: If your company has implemented the RapidResponse Server failover configuration, message subject lines might also indicate which RapidResponse generated the message: active server or standby server. For more information, see "RapidResponse Server failover clustering" on page 289.

Specifying a default email address

When a user-generated email message is sent from RapidResponse, it is sent using the name and email address of the user who generated it. For example, an alert notification is sent using the alert owner's name and email address. If that user does not have an email address defined in RapidResponse, the email messages are sent using the RapidResponse default email address. However, it is still recommended that every user with alert authoring permission have an email address.

The default email address is also used in email messages origination from the RapidResponse system such as alarm, warning, or status messages (as opposed to user generated messages).

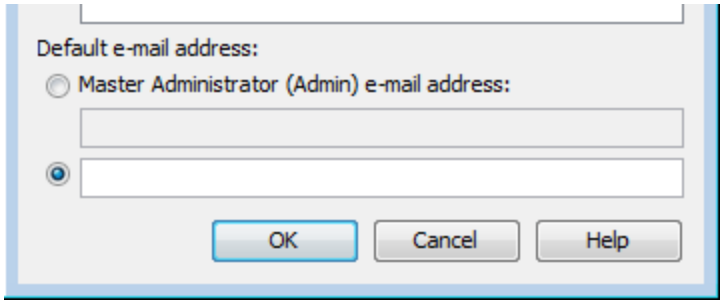
On-Demand: If the RapidResponse default email address is not specified, then messages are sent using the Master Administrator at Kinaxis' email address.

On-Premises: If the RapidResponse default email address is not specified, then messages are sent using the Master Administrator's (Admin user) email address.

▸To specify a default email address

1. In the **Administration** pane, under **Communication**, click **Message Center and Email**.
2. In the **Default email address** section, click the second option and type the email address in the

box.



Phishing attacks and other malicious actions

Some messages that are sent from RapidResponse contain links to sign into the user's RapidResponse account. These links can help users quickly sign in, see the most up to date information, and take necessary actions. It is possible, however, that unauthorized third parties could attempt to steal RapidResponse account information using a phishing attack—an email message that is intended to look like it comes from your company's RapidResponse server, but directs the user to a fake instance of the RapidResponse sign-in page or another website that exists for the purpose of collecting account information.

If users have concerns about the authenticity of a RapidResponse message, they should not click any of its links. Instead, users should open their web browser and sign in to RapidResponse directly from there, or contact their RapidResponse administrator.

As an administrator, ensure your RapidResponse users are educated about phishing attacks and other malicious actions.

Setting the worksheet record limit

A filter or search applied to data can generate a very large number of records. This can cause poor performance, especially where large data sets are being used.

RapidResponse includes default worksheet record limits for vertical, also called tabular, worksheets (5,000) and crosstab worksheets (500,000).

On-Demand: These settings can be changed by Kinaxis Customer Support.

On-Premises: These settings can be changed by a system administrator.

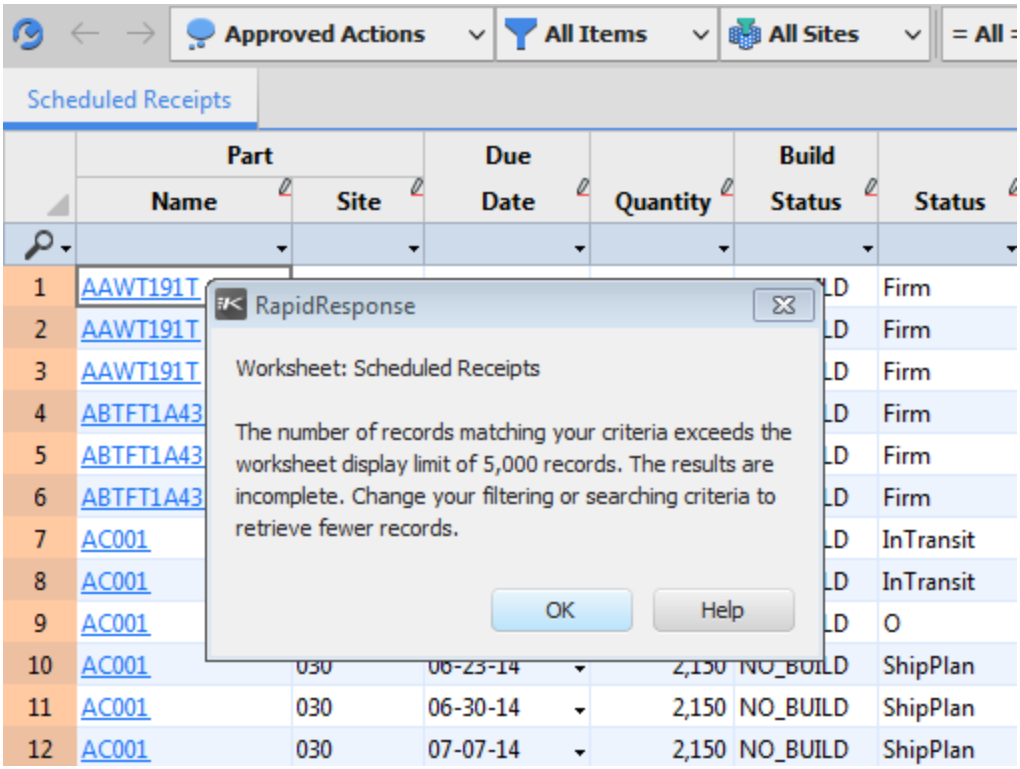
Note: The minimum number of records that you can specify is 100, and there is no maximum.

Vertical worksheet limits

The worksheet record limit applies only to the final output of the worksheet. Any records that are required to generate the final output, such as records in multi-scenario columns or grouped records,

are not limited by the worksheet record limit. In the case of a composite worksheet, only the final output of the composite is affected by the worksheet record limit.

If the results of applying a filter or a search exceed the worksheet record limit, a message is displayed notifying the user that the number of records matching their filtering and searching criteria exceeds the worksheet limit. The results that could be retrieved are displayed; however, these results are partial, generated randomly, and should not be used for decision making purposes. In particular, worksheets with grouped and summarized columns might display incomplete data, especially in columns that display quantity or price. Additionally, the worksheet row labels are formatted with an orange background to remind the user that the data displayed is incomplete, as shown in the following illustration.



The returned records are displayed to give a hint of how a different filter or an enhanced search could be used to produce fewer records.

You can grant select groups and users the permission to override the vertical worksheet record limit. Allowing users to override the record limit can place heavy demands on the RapidResponse system. Large amounts of data being processed might result in slowed RapidResponse performance for all users. For more information, see "Assigning and removing permissions" on page 517.

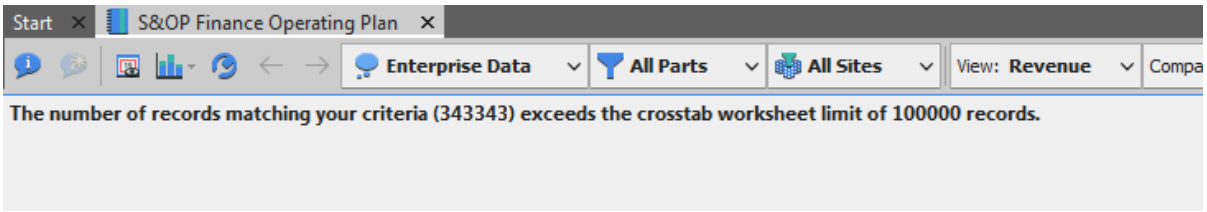
This procedure applies to the On-Premises version of RapidResponse.

▸To set the vertical worksheet record limit

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. In the **Client** category, beside the **Worksheet record limit - Tabular** box, type a value.

Crosstab worksheet limits

When the record limit is exceeded in a crosstab worksheet, no records are displayed. A message appears, indicating that the user's criteria exceeds the limit, as shown in the following illustration.



A crosstab worksheet's record limit applies to the number of source records; that is, the number of records that would be returned if the crosstab worksheet was formatted as a vertical worksheet, or the number of rows in the worksheet multiplied by the number of buckets.

There is no option to override the record limit of a crosstab worksheet. You may be able to adjust data and bucket settings to display records in the worksheet; or, you can change the limit using the following procedure.

This procedure applies to the On-Premises version of RapidResponse.

▸To set the crosstab worksheet record limit

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. In the **Client** category, beside the **Worksheet record limit - Crosstab** box, type a value.

Note: If you modify the worksheet record limit for a crosstab worksheet, the import record limit is not modified, and users can only import a maximum of 500,000 records into a crosstab worksheet.

Setting the record deletion warning threshold

When a user selects thousands of records in a worksheet and deletes them, this action might take longer than the user expects. It might also affect system performance for all signed-in users.

To ensure that the user is aware of the potential performance impact, a warning message is displayed whenever large numbers of records are marked for deletion in a worksheet. The user can choose whether to delete the records anyway or cancel the action.

By default, the warning is displayed when a user marks more than 25,000 records for deletion in a worksheet. You can change the threshold that determines when users are warned about the number of records that they are deleting.

▸To change the record deletion warning limit

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Worksheet delete record warning limit** box, type a new number.
4. Click **OK**.

Note: If users are expected to use a workbook to routinely delete very large numbers of records, it is a good practice to provide a workbook command for this operation, if possible. Deleting records using a workbook command is more efficient.

Changing image upload size limits

Users with resource authoring permissions can upload images to the image library, making them available for use in resources. For example, a user might upload an icon to display in a worksheet column or an illustration to clarify a task flow step. In most cases, very large images are not needed.

To help optimize system performance, RapidResponse limits the size of image that users can upload to the image library. The default limits are:

- Maximum file size: 1MB (1048576 bytes)
- Maximum width: 2048 pixels
- Maximum height: 2048 pixels

System administrators can change these limits if necessary.

▸Change image upload size limits

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. In the **Client** category, change any of the following values:
   - **Maximum file size of user-uploaded images** (bytes)
   - **Maximum width of user-uploaded images** (pixels)
   - **Maximum height of user-uploaded images** (pixels)

Setting hierarchy limits

RapidResponse can limit the number of records that are retrieved when a user selects a hierarchy in a workbook's hierarchy panel. Hierarchies consist of levels of related data, and are shown in RapidResponse in the hierarchy panel. When a user clicks a value in a level, the worksheet is filtered and summarized by each value in the levels below the selected value.

RapidResponse automatically loads the hierarchy data into memory so the user can move through the hierarchy without waiting for data to load. When a user selects a hierarchy, RapidResponse controls the hierarchy display according to the following criteria:

- When the hierarchy is first added to the workbook, the top levels of the hierarchy are loaded. The number of levels loaded when the hierarchy is added to the workbook is controlled by the Hierarchy_MaximumLevelsRetrieved configuration setting. The default for this setting is three

levels.

- If the top levels contain more than the maximum allowed total entries, one less level is loaded. If the top levels still have too many entries, one less level is loaded again, until a single level is loaded. The number of entries allowed in these levels is controlled by the Hierarchy_MultipleLevelRecordLimit configuration setting. The default for this setting is 100 entries.
- For each level of the hierarchy, a specific number of entries are loaded. If a user expands a level that contains more than this number of entries, the user is prompted to wait for the rest of the entries to load. This limit is controlled by the Hierarchy_ConfirmationRecordLimit configuration setting. The default for this setting is 1,000 entries.
- If the level contains more than the maximum number of entries, the entries are not loaded and the user is prompted to redefine the hierarchy. This limit is controlled by the Hierarchy_MaximumRecordLimit configuration setting. The default for this setting is 10,000 entries.

On-Demand: You can request Kinaxis Customer Support customize all of the above rules, if necessary.

On-Premises: RapidResponse system administrators can customize all of the above rules by editing configuration settings.

▸To specify the hierarchy settings (On-Premises only)

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. Locate or insert the following records:

Name	Description
Hierarchy_MaximumLevelsRetrieved	Controls how many levels are loaded when the hierarchy is first selected.
Hierarchy_MultipleLevelRecordLimit	Controls how many hierarchy values are allowed in the first levels loaded.
Hierarchy_ConfirmationRecordLimit	Controls how many hierarchy values are loaded for a single level.
Hierarchy_MaximumRecordLimit	Controls the maximum number of hierarchy values that can be loaded for a level.

4. In the **Value** column for each configuration setting, change the value to the new limit.
5. Click **Save and Close**.

Note: Increasing the hierarchy limits can result in decreased system performance.

Delimiter for hierarchy standard variables

RapidResponse includes several standard variables to support hierarchy authoring. The $SelectedHierarchyTreePath variable provides the full path of the selected hierarchy value, separated by a delimiter character. By default, the delimiter is the pipe (|) character but it can be modified by a RapidResponse system administrator in cases where the data includes this character.

You can use any character as a delimiter. However, it is recommended you use a symbol character, such as a pipe character (|), underscore (_) or hyphen (-).

▸To change the delimiter used in $SelectedHierarchyTreePath

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Hierarchies** category.
3. In the **Path delimiter character** box, type a character. Ensure the character chosen is not one used in your RapidResponse data set.

Options for importing Excel data to scenarios

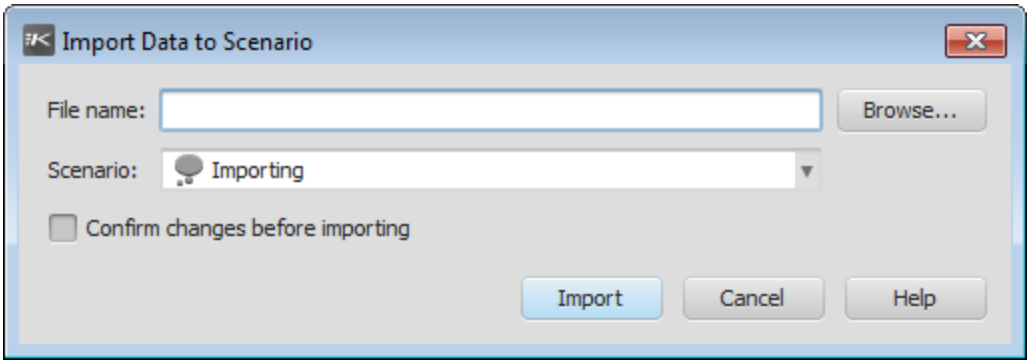
Users can import data from Microsoft Excel into their private scenarios. By default, new records are imported and any duplicate records replace existing records in the user's RapidResponse scenario.

If this is not the desired behavior, you can provide RapidResponse users two additional options:

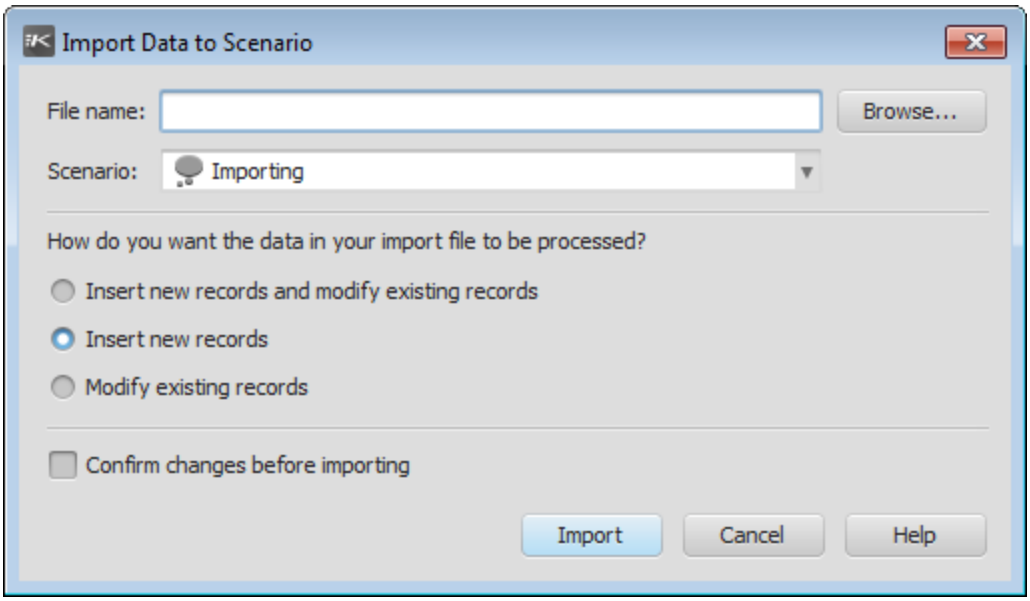
- Insert new records and ignore duplicate records on import.
- Modify records and reject any records that do not exist in RapidResponse

By doing so, the Import Data to Scenario dialog box includes three options for users.

The following illustration shows the default Import Data to Scenario dialog box.



The following illustration shows the Import Data to Scenario dialog box with additional options.



You can only perform this task if you are a system administrator.

▸To provide options in the Import Data to Scenario dialog box

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Excel import to scenario options** box, select **Yes**.

Note: Data administrators and system administrators always have access to all three options.

Making data formats available to users and resource authors

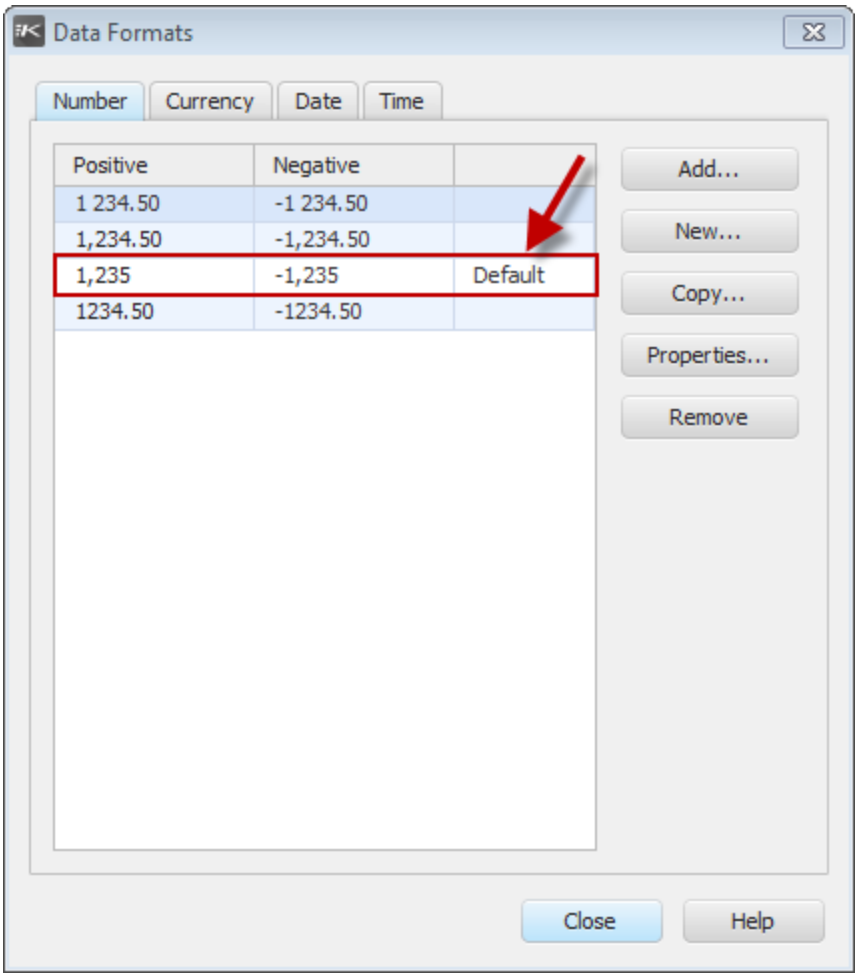
Number, currency, date, and time information displayed in RapidResponse resources has formatting applied. For example, number information can be displayed using commas or spaces as thousands separators, or date information can be displayed with a two-digit or four-digit year.

The formats applied to data can be defined by the resource's author. In resources where the author has not specified a format, the user's specified format is used.

As a system administrator or data administrator, you must determine the formats that are available to users and resource authors. Users and resource authors cannot create data formats.

RapidResponse includes many number, currency, date, and time formats, several of which are available to users and authors by default. You can make the additional formats included with RapidResponse available or create new data formats. For example, you might need to create new formats for multiple currencies, or for users in different international locales, such as North America, Europe, or Asia.

One data format per category (number, currency, date, and time) is specified as the system default format for all users. For more information, see "Specifying default data formats for users" on page 559.



▸To make a data format available

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. On any of the tabs, click **Add**.
3. In the list, click the format you want to add, and then click **Add**.

Caution: Do not make conflicting formats available. For example, do not make both the **mm-dd-yy** and **dd-mm-yy** date formats available because they could potentially be misunderstood, especially when used together in a worksheet.

Note: You can select multiple formats. To select nonadjacent formats, hold down **CTRL**, and then click each format. To select adjacent formats, hold down **SHIFT**, and then click the first and last format in the sequence.

▸To make a data format unavailable

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. On any of the format tabs, click a format in the list, and then click **Remove**.

Note: You cannot remove a format that is designated as the default format.

Editing and creating formats

You can edit existing formats and create new formats.

▸To edit a format

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. On any of the format tabs, click a format in the list, and then click **Properties**.
3. Make any changes you want.

▸To create a new number format

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. On the **Number** tab, click **New**.
3. In the **Decimal symbol** list, click a symbol to use for the decimal symbol.
4. In the **Decimal places** box, type the number of decimal places you want to display in the new format.
5. In the **Digit grouping symbol** list, click a symbol that separates the hundreds, thousands, and millions columns in the number format.
6. From the **Negative number format** list, choose a format to be applied to negative numbers.

Note: The **Decimal places** setting does not specify the number of decimal places to use in reports. This is used in other user input or user interaction areas of RapidResponse.

▸To create a new currency format

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. Click the **Currency** tab, and then click **New**.
3. In the **Currency symbol** area, click one of the following:
   - **Symbol**—The currency symbol is displayed on all values, for example, $300.
   - **ID**—The currency code is displayed on all values, for example, USD 300.
4. In the **Positive currency format** list, click a style for positive currency numbers.
5. In the **Negative currency format** list, click a format for negative currency numbers.
6. In the **Decimal symbol** list, select the symbol used to represent the decimal point.
7. In the **Decimal places** box, type the number of decimal places. The **Decimal places** setting does not specify the number of decimal places to use in reports. This is used in other user input or user interaction areas of RapidResponse.
8. In the **Digit grouping symbol** list, select the symbol used to separate groups of digits.

Notes:

- Currency formats can be applied to any money data or quantity data formatted as currency,

and do not specify a symbol to denote the currency. Some currencies do not use a symbol, in which case formats that display the symbol before or after the value look identical when applied to that currency.

- The symbol displayed on currency formats in the **Data Formats** and **New Currency Format** dialog boxes is the symbol for your preferred currency.

Tips:

- You can also duplicate an existing format by selecting the format and clicking **Copy**. For example, you might copy a format if you want the positive, negative, and digit grouping symbol for the new format to be identical to an existing format, but want to display more decimal places.
- You can also access the **Currency** tab by clicking **Formats** on the **Currencies** dialog box. For more information, see "Adding standard currencies" on page 684.

▸To create a new date format

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. Click the **Date** tab, and then click **New**.
3. In the **Format** box, type the new date format.

▸To create a new time format

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. Click the **Time** tab, and then click **New**.
3. In the **Format** box, type the new time format.
4. In the **AM symbol** and **PM symbol** lists, do one of the following:
5. Click AM for times between 00:00 and 11:59, and click PM for times between 12:00 and 23:59.
   - Click the blank item if you do not want a symbol.
   - Click the blank item and type a custom text string if you want a custom symbol.

Note: Any changes made to formatting are available the next time the user signs in to RapidResponse.

Date and time codes

The following table shows the date codes that are used in RapidResponse:

Date Code	Display
m	Months as 1-12 with no leading zeros.
mm	Months as 01-12.
mmm	Month name as a 3-character abbreviation of the name.
mmmm	Full month name.

Date Code	Display
d	Days as 1-31 with no leading zeros.
dd	Days as 01-31.
ddd	Day of the week as a 3-character abbreviation of the name.
dddd	Full name of the day of the week.
yy	Years as 00-99.
yyyy	Four-digit year value, for example, 1999. RapidResponse supports years 1970 to 2037.

Note: RapidResponse supports date values from January 2, 1970 to December 31, 2037.

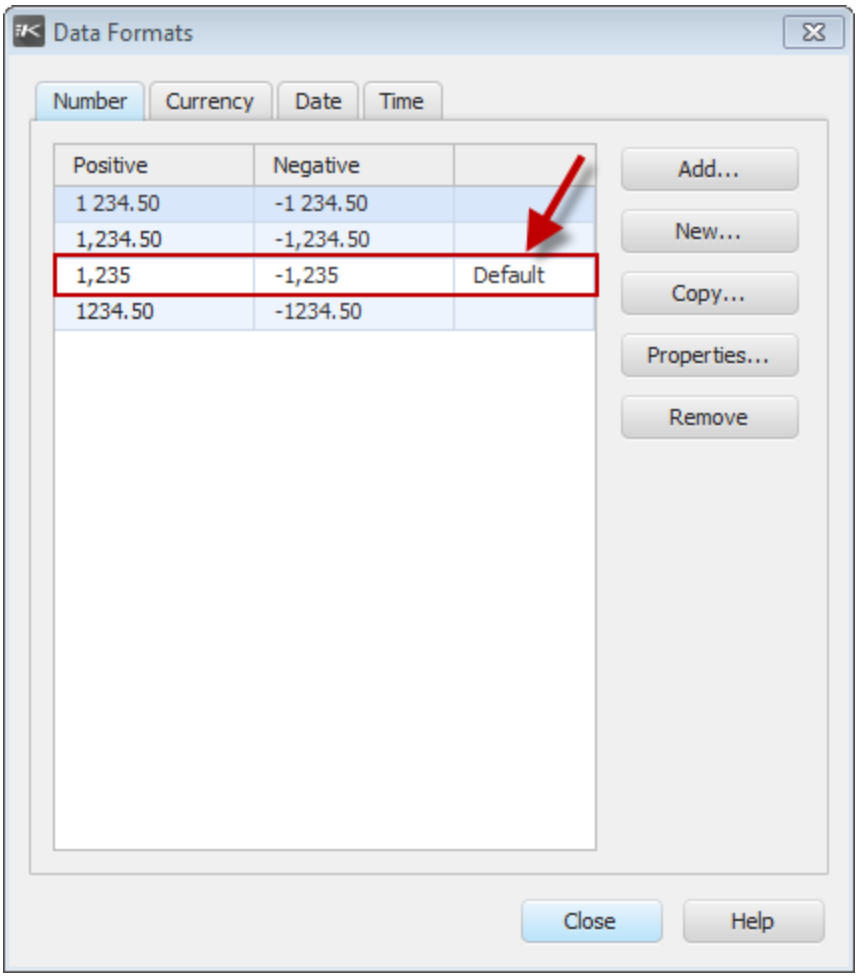
The following table shows the time codes that are used by RapidResponse:

Time Code	Display
h	Hours as 0-23.
hh	Hours as 00-23.
min	Minutes as 00-59.
ss	Seconds as 00-59.
tt	Time will be displayed using the 12-hour clock, that is, hours are between zero and 12.

For more information about time zones, see "Defining time zones" on page 669.

Default formats for new users

The default number, date, currency, and time formats that users see data in are determined by RapidResponse administrators.



▸To set a format as the system default

1. In the **Administration** pane, under **System Settings**, click **Data Formats**.
2. On any of the format tabs, click a format in the list, and then click **Properties**.
3. In the **Format Properties** dialog box, select the **Default format** check box.

User administrators can override the default for individual users. Users can set their own data format settings, too. For more information, see "Specifying default data formats for users" on page 559.

Turning unsaved workbook changes warning on or off

By default, workbook authors are asked for confirmation when they take actions that would result in their changes to a workbook or worksheet being discarded. This is intended to prevent accidental losses that could occur if authors make mistakes, such as clicking Cancel instead of OK after making changes to a workbook's properties.

Administrators can turn these warnings off (or back on).

▸To turn the unsaved workbook changes warning on or off

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Dialogs** category if necessary.
3. In the **Unsaved changes warning for authors** box, select the desired setting.

> **Note:** Individual authors can select a check box on the warning if they do not ever want to see it again. This permanently suppresses the warning and takes precedence over the global setting.

Defining time zones

Most dates and times displayed in RapidResponse are displayed according to the settings on the user's computer; a few dates are displayed in the time zone of the computer where RapidResponse is hosted.

For example, assume your main manufacturing site is in New Jersey ((UTC-5:00) Eastern Time), and you have a distribution site in California ((UTC-8:00) Pacific Time). If a user at the distribution site adds a note to an order at 8:00 A.M., the planner at the main site will see the note as having been added at 11:00 A.M because Pacific Time is 3 hours behind Eastern Time.

Similarly, if a supplier from Hong Kong ((UTC+8:00) Hong Kong) signs into RapidResponse to make changes at 9:00 A.M. on 02-02-06, the User Administrator in New Jersey would see the supplier as having signed in at 8:00 P.M. on 02-01-06.

Dates of scheduled receipts and independent demands are displayed in the time zone of the computer on which RapidResponse is hosted. For On-Premises, the computer where RapidResponse Server is installed is considered the host computer.

For example, if the supplier in Hong Kong views a requirement for 200 on 03-04-06, the demand is needed 03-04-06 Eastern Time.

RapidResponse takes Daylight Savings Time for each time zone into account when calculating time.

Many time zones are predefined in RapidResponse; however, you can add time zones if required. For example, you might want to use a different name for an already defined time zone. You must be a data or system administrator to perform this task.

▸To check the time zone used on a computer

1. In the Microsoft Windows Control Panel, double-click **Date and Time**.
2. Click the **Time Zone** tab.

   The time zone is displayed in the list at the top.

▸To add time zones

1. In the **Administration** pane, under **System Settings**, click **Time Zones**.
2. Click a time zone in the **Select a time zone** list.

   The time zone names listed come from the Windows Registry on the computer where RapidResponse is hosted; therefore, local strings for the names are listed.
3. In the **Enter the display name** box, type a name that you want to be displayed for this time zone. It is recommended you specify a name in the following format because the value is displayed in different dialog boxes in RapidResponse:

(UTC-5:00) Eastern Time

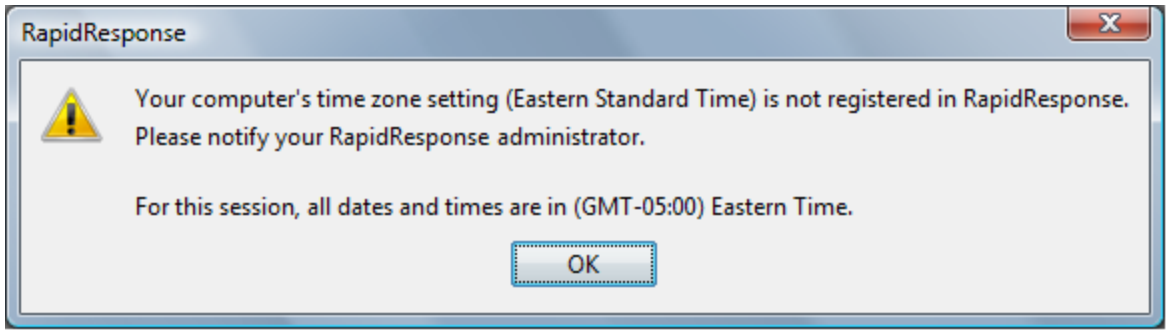
4. Click **Add**.

Caution: You cannot remove a time zone from RapidResponse once you click **OK**.

Note: If you add a time zone with the same parameters as a time zone that's already been defined, the most recently added time zone is used by RapidResponse.

Time zone warning

When a user signs in to RapidResponse, their computer's time zone is automatically detected. If that time zone is not defined in RapidResponse, they are notified and instructed to request that their time zone be added. A sample warning message is shown in the following image.



If you are contacted by a user who encounters the message about their time zone not being defined, have the user verify the time zone setting on his or her computer before adding the time zone.

Time zone changes

National, state, and provincial governments set standard and daylight savings laws and these laws sometimes change. For example, the U.S. Energy Policy Act of 2005 changed the start and end dates for daylight time (effective March 2007). With this change, Microsoft issued new time zone definitions for computers running the Windows operating system (see http://support.microsoft.com/kb/931836 for more information).

RapidResponse uses time zone information for reporting local date values and to schedule tasks such as alerts. If new standard and daylight time laws are introduced and the RapidResponse system does not have the time zone definitions added then two problems can occur:

1. RapidResponse users, upon sign in, will receive a warning that their current time zone has not been defined in RapidResponse (provided that the user has updated their operating system).
2. Scheduled tasks such as alerts will not run at the expected time. For example, an alert might run an hour earlier or later than expected.

RapidResponse users will also receive a warning if RapidResponse has updated time zone definitions and they have not updated their operating system to support the changes in standard and daylight time.

If you have users in a time zone that has changed standard and daylight times, you need to change the time zone's definition in RapidResponse. However, the Time Zones dialog box available from the Administration pane in RapidResponse does not allow you to modify existing RapidResponse definitions. As such, you will need a worksheet based on the RapidResponse TimeZone table to modify existing time zone definitions. Kinaxis Customer Support can provide you this type of worksheet through the Kinaxis Knowledge Base. For example, KB #2096697 provides a workbook and instructions on how to update RapidResponse for U.S. daylight savings changes introduced in March 2007.

Overriding the Everyday calendar name

The Everyday calendar has no entries defined for it, and thus ensures that every calendar day is included. If necessary, you can override the name of the Everyday calendar (for example, if you want to define a calendar named "Everyday" for some other use).

On-Demand: Contact Kinaxis Customer Support to request the name of the Everyday calendar to be overridden.

The rest of this topic only applies to the **On-Premises** version of RapidResponse.

To perform this task, you must be a system administrator.

▸To override the name of the Everyday calendar

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **ID** box, type **EverydayCalendar**.
   - In the **Value** box, type a new name to the refer to the "Everyday" calendar by.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.

Configuring settings for automation tasks

This topic only applies to the On-Premises version of RapidResponse.

Setting up alert functionality

Before users can create alerts, used to monitor data or automatically create reports, a system administrator must perform the following tasks.

- Ensure that an email server has been defined in association with RapidResponse Server. For more information, see "Configuring email support" on page 276.

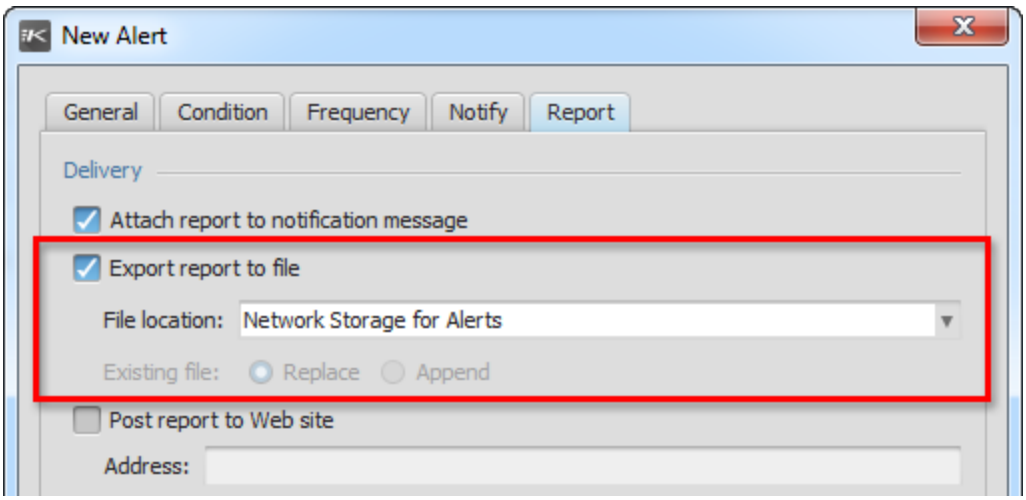
- Provide users who will create alerts with alert authoring permissions. For more information, see "Creating groups" on page 513.
- Specify folders where reports generated by alerts are saved. For more information, see "Specify storage folders for alert-generated reports" on page 672.
- Specify a down time interval to run automation tasks that should have been run if alerting functionality was deactivated. For more information, see "Specifying a down-time interval to run automation tasks" on page 674.
- Test the setup by creating and running an alert. For more information, see the *RapidResponse User Guide*.
- Review logs created by alerts. For example, if an alert fails, the failure is recorded in a log file, which can be used to find and resolve problems. For more information, see "Automation logging" on page 448.

Some alert settings can be overridden, such as sending messages to a different email address or exporting reports to a different file location than is defined in the alert. These overrides can be used to temporarily change an alert's settings if you are developing or testing them on a test system computer, or if you need to perform maintenance on a resource used by alerts, such as the network file location that alerts export files to. For more information, see "Alert overrides in a development environment" on page 675.

Administrators can view all alerts in RapidResponse, and can delete or edit any alert's settings except the condition and data being monitored. This allows you to delete or modify any alerts that are too memory intensive. In addition, you can delete alerts owned by users who are no longer with your company, or give those alerts to another user. For more information, see "Managing alerts" in the *RapidResponse User Guide*.

Specify storage folders for alert-generated reports

RapidResponse users can create alerts that generate reports which can be saved on your local network. This report option is only available if a system administrator has specified a folder for storing the alert-generated reports using the File Locations worksheet in the RapidResponse Administration workbook.



It is recommended system administrators create storage folders on the computer where RapidResponse Server is installed. However, they can also create storage folders on their local network.

The folder location is also used to run alert post-processing commands.

For information about setting up the predefined folder locations, see "Specifying file location folders" on page 676.

Report storage folder and RapidResponseService user permissions

The RapidResponse Service Host service, by default, runs all alerts using the Microsoft Windows user account named RapidResponseService. The RapidResponseService user account requires read-write-modify permissions to all folders that alerts export reports to. For more information about modifying Windows user account permissions, see the *Microsoft Windows Help*. Depending on the Microsoft Windows version and configuration, the following procedure describes how to provide permissions to the RapidResponseService user account.

If you have configured the Service Host to use a different user account, you must assign the same permissions required by the RapidResponseService account, and follow the same procedure to configure it. This procedure assumes the RapidResponseService user is being used.

The RapidResponseService user account requires read-write permissions to all folders that alerts use for post-processing commands.

▶To grant permissions to the RapidResponseService user

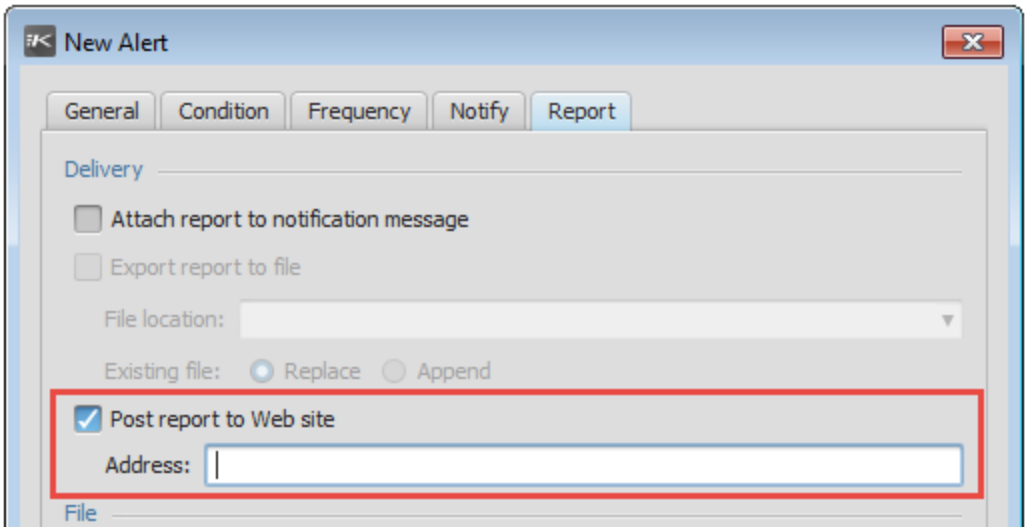
1. In Windows Explorer, navigate to the folder referenced by a network location.
2. On the **File** menu, click **Properties**.
3. Click the **Security** tab.
4. Click **Add**.
5. Ensure the location in the **From this location** box is the name of the computer where RapidResponse Server is installed.
   - If it is not, click **Locations**, click the computer name, and then click **OK**.
6. In the **Enter object names to select** box, type **RapidResponseService**.
7. Click **OK**.
8. In the **Permissions** list, select the **Read**, **Write** and **Modify** check boxes.

For more information about the RapidResponse Service Host service, see "Configuring RapidResponse Service Host" on page 234.

Caution: If the properties of the RapidResponse Service Host service or the RapidResponseService user account are modified then alerts might not function. If alerts stop functioning, the likely cause is a change to either the RapidResponse Service Host settings or the RapidResponseService user account. This problem can be corrected by resetting the RapidResponse Service Host settings. For more information about resetting the RapidResponse Service Host, see "Resetting the RapidResponse Service Host" on page 234.

Posting reports to web sites

RapidResponse users can create alerts that generate reports which can be posted the report to a Web site using either the HTTP or the secure HTTPS protocols.



When a report is posted to a web site, the RapidResponse Service Host service executes an HTTP POST to the URL specified in the **Report** tab of the **Alert** properties dialog box.

To support the RapidResponse posting functionality, the computer hosting the web server where the report is being posted must be properly configured. This includes the following:

- The web server must be configured to support the Posting command.
- The computer hosting the web server must be accessible from the computer hosting the RapidResponse Service Host.

For more information about the RapidResponse Service Host service, see "RapidResponse Windows Services" on page 227.

Specifying a down-time interval to run automation tasks

When automation functionality is disabled, alerts, scheduled tasks, and automation chains cannot run. Automation functionality, for example, might be disabled if the RapidResponse Server service or the RapidResponse Service Host service is stopped.

You can configure RapidResponse to run scheduled automation tasks that did not execute by setting a down time interval (in hours). RapidResponse runs any scheduled automation tasks that fall into the down time interval.

For example, assume the RapidResponse Server service was stopped for five hours and the down time interval was set to two hours. Once the server is restarted and automation functionality is reactivated, all automation tasks that were supposed to be run in the last two hours will be run. Automation tasks scheduled to be run prior to the last two hours are ignored.

Any tasks that users tried to run manually are always checked when the RapidResponse Service Host is restarted, no matter how much time has passed. For example, if a user clicks the Run Alert Now button for an alert at noon and the RapidResponse Service Host is restarted at midnight, the user's alert checks for conditions at midnight. Any automation tasks that were scheduled or that should have been run due to data changes are only checked if they were supposed to run within the specified time interval.

▸To specify a down time interval

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Automation** category.
3. In the **Restart window after down time** box, type a value (in hours).

Note: The default is 0. If this value is not changed, RapidResponse does not run any automation tasks that were scheduled to run while the automation functionality was disabled.

Alert overrides in a development environment

If your RapidResponse authors are testing or developing alerts, or other automation resources that run alerts, in a RapidResponse test environment, you can take advantage of alert override settings to help them more quickly develop alerts and predefined schedules, or deactivate all alerting functionality to prevent any alerts from checking for conditions while they develop. Alert overrides can also be used in a production environment.

By using the alert override settings, you can do the following:

- Use an alternate or test email address.
- Overriding the file export location.

To apply any the override settings, alerting functionality must be deactivated and reactivated. Alerting functionality is included in a Windows service (RapidResponse Service Host) which can be stopped using Windows Administrative Tools.

Activating and deactivating automation functionality

If you are developing automation resources and do not want any of the scheduled automation tasks to run until you are finished, you can deactivate all automation functionality. Automation is handled by a Windows service, which can be stopped by using Windows Administrative Tools.

In addition, automation functionality must be deactivated and reactivated to apply alert override settings.

▸To activate and deactivate automation functionality

1. In the Microsoft Windows Control Panel, double-click **Administrative Tools**, and then double-click **Services**.
2. Click **RapidResponse Service Host**.
3. Do one of the following:
   - On the **Actions** menu, click **Stop** to deactivate.
   - On the **Actions** menu, click **Start** to reactivate.

Automation tasks scheduled during the deactivation time do not check for conditions until you reactivate the automation functionality.

Use an alternate or test email address

If your users are developing alerts and the alert recipients receive notifications through email addresses (instead of RapidResponse Message Center), consider temporarily overriding the email address. By doing so, alert authors can more easily test the alerts they are developing without test (or nuisance) email messages being sent to their internal RapidResponse users, and external customers and suppliers.

This override applies only to alert recipients specified by email addresses ("To", "CC", and "BCC"). If RapidResponse users are specified, a notification message is still sent to each recipient's Message Center. To prevent recipients from receiving messages, consider removing all users and groups from the recipients list before testing the alert.

▸To override email addresses used by alerts

1. On the computer where RapidResponse Server is installed and from the Windows **Start** Menu, choose **Run**.
2. In the **Open** box, type **regedit** and click **OK**.
3. Create or modify the Windows Registry setting for **Webplan\Overrides\EmailOverride**.

For more information about the RapidResponse Windows Registry settings, see "Registry Settings for RapidResponse Server" on page 351. For more information about the EmailOverride setting, see "EmailOverride" on page 362.

Overriding the file export location

If your users are developing alerts, or other automation resources that run alerts, and the alerts export reports to a network file location, consider temporarily overriding this location. By doing so, the exported files could be directed to a location on a RapidResponse test system. You might also want to override the location if the test system cannot connect to the file location on your network. By using a file location override you do not need to modify alerts to send reports to a different location.

▸To override the export file location

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Automation** category.
3. In the **File export location override for alerts** box, type the complete path to the alternate file location.
4. Click **OK**.
5. Deactivate and reactivate the RapidResponse alert functionality. For more information, see "Activating and deactivating automation functionality" on page 675.

Note: To remove the override, delete the file location from the Global Settings dialog box and deactivate and reactivate the RapidResponse alert functionality.

Specifying file location folders

This topic only applies to the On-Premises version of RapidResponse.

Several RapidResponse operations and tasks can write files to predefined folders including:

- Alerts that generate reports. For more information, see "Configuring settings for automation tasks" on page 671.
- Post-processing commands for alerts.
- The **ExtractData** and **ExtractNetChangeData** commands. For more information, see "ExtractData command" on page 403 and "ExtractNetChangeData command" on page 404.
- Script arguments.
- Automation tasks.

RapidResponse administrators are responsible for specifying the predefined folders where files can be written.

It is recommended system administrators create predefined folders on the computer where RapidResponse Server is installed. However, they can also create predefined folders on their local network. The network location of the folders must be fully resolvable by RapidResponse Server.

▸To specify a file location folder

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **File Locations** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** dialog box, do the following:
   - In the **ID** box, type the name that will be visible to users in the RapidResponse client.
   - In the **Value** box, type the path to the folder where files can be written to. Provide a complete path, including the drive or the network computer name. The path should be fully resolvable by RapidResponse Server. The folder must already exist.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.

Note: If you are defining a file location to send reports back to your environment using the Data Transfer Client (DTC), you cannot name the file location "Outbound". This folder name is used by the DTC to define the data to send to RapidResponse.

Migrating user groups

Rapidresponse user groups, such as Network Planners and S&OP Team, are often developed on a test or development system and then moved to a production system. As a system or user administrator, you can migrate user groups in bulk between RapidResponse systems. When you create a user group package, you select the groups to export and RapidResponse automatically adds any permissions required to the package. New user groups that you do not have in your system are automatically imported.

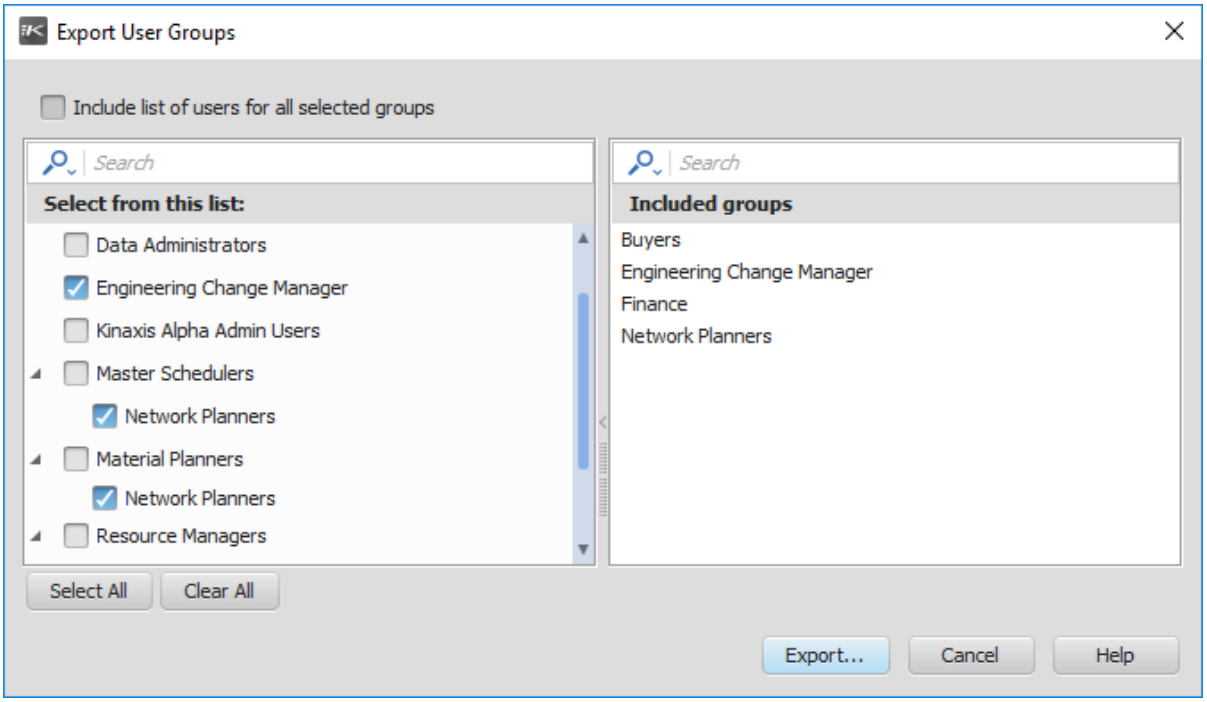
User group packages can be used to migrate small or large groups of users and their dependent permissions. The details of users that are in each group is not automatically exported with a user group, however you are able to turn this feature on.

Note: Both system and user administrators can migrate user groups, however it is recommended that system administrators manage the process.

Exporting a User Group

When you export a user group package, a package containing user groups and permissions for the groups is created. By default, the package does not contain the users of the groups. You can choose to include the user names for the groups.

You can customize the user groups included in the package and search for specific groups.



The user groups you have selected display in the Included groups pane. They will display in alphabetical order.

▸To export a user group package

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Under **User group package**, click **Export**.
3. In the **Select from this list:** pane of the **Export User Groups** dialog box, select the user groups to include in the package.
   - To add all user groups to the export package, click **Select All**.
   - To include a list of users for all selected groups, check the **Include list of users for all selected groups** box.
4. Click **Export**.
5. In the **Save User Groups** dialog box, select a location to save the package.

- The resource package is saved with the .spk extension.

6. Click **Save**.
   - To open and view the saved package, click **Open Folder**.
   - To continue without opening and viewing the saved package, click **Close** twice.

Importing a user group package

When you import a user group package into RapidResponse, it contains new user groups and updated versions of user groups currently in your system. You are only able to import the full package, and cannot select specific groups or users to import.

Importing a user group package only allows you to add or change groups.

The Import User Groups dialog box displays all of the user groups included in the package and highlights the groups that are new or changed.

After the import is complete, a message is sent to Message Center with an attached log. The log describes all the resources in the package and what action was performed on the user groups.

▸To import a user group package

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Under **User group package**, click **Import**.
3. In the **Open User Groups** dialog box locate the resource package file with the .spk file extension, and then click **Open**.
4. Optionally, in the **Import User Groups** dialog, click **See Difference** next to a user group to see the changes between current and new user groups. Click **Close**.
5. Click **Import** .
6. To confirm the import, click **Yes**.
7. Click **OK**.
8. Click **Close**.

Caution: When you confirm the import, for existing groups that are being replaced with a changed group from the package, all the group settings, permissions, and resources are overwritten.

Note: For more information on comparing user groups, see "Comparing user group packages" on page 681

Restoring a user group package

You can restore your user group package to an earlier version of a resource if any of the changes made to it were unsatisfactory or caused conflict.

There are two ways that user group packages can be restored:

Implicit restore—Restore that was triggered by a failure that occurred during an import.

Explicit restore—Restore that was triggered by the administrator.

The Backup History dialog box lists all of the saved backups that you can restore your system to. By default, five backups will be saved, however system administrators can change this default number in Global Settings.

The Restore User Groups dialog box displays all of the user groups included in the package and highlights the groups that are new or changed.

After the import is complete, a message is sent to Message Center with an attached log. The log describes all the resources in the package and what action was performed on the user groups.

▸To restore a user group package

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Under **User group package**, click **Restore**.
3. In the **Backup History** dialog, select the user group backup you want to restore to and click **OK**.
4. Optionally, in the **Restore User Groups** dialog, click **See Difference** next to a user group to see the changes between current and new user groups. Click **Close**.
5. Click **Restore**.
6. To confirm the restore, click **Yes**.
7. Click **OK**.
8. Click **Close**.

Cautions:

- When you confirm the restore, for existing groups that are being replaced with a changed group from the package, all the group settings, permissions, and resources are overwritten.
- Restoring the user group package will remove any user groups that were not there at the time the restore was saved.

Note: For more information on comparing user groups, see "Comparing user group packages" on page 681

Setting the limit on backups

Any time you import a user group package, a backup of the current user groups and their permissions is created. This backup can then be used to restore the user groups to a previous version. By default, the RapidResponse system will only save five backups.

On-Premise system administrators can change the default.

To request changes to the default backup setting for On-Demand installations, contact Kinaxis Customer Support.

The rest of this topic only applies to the On-Premises version of RapidResponse.

▸To modify the saved user groups backup

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Saved user group backups** text box, type a number.
4. Click **OK**.

Comparing user group packages

You can compare differences in the user group package with their current versions in RapidResponse after you import or restore a user group package.

▸To compare an import user group package to the current user groups

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Under **User group package**, click **Import**.
3. In the **Open User Groups** dialog box locate the resource package file with the .spk file extension, and then click **Open**.
4. In the **Import User Groups** dialog, click **See Difference** next to a user group.

▸To compare a restore user group package to the current user groups

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Under **User group package**, click **Restore**.
3. In the **Backup History** dialog, select the user group package you want to restore to and click **OK**.
4. In the **Restore User Groups** dialog, click **See Difference** next to a user group.

CHAPTER 44: Creating and managing currencies

About currencies 683
Overview of adding or creating a currency 684
Adding standard currencies 684
Currency codes 685
Creating currencies 686
Managing currencies 686
Currency conversions 687
Managing conversion rates 689

RapidResponse can display Money data using multiple currencies, which allows users to view data in their preferred currency, and resource authors to create dashboards, workbooks, and scorecards that display and convert values to different currencies.

As a system or data administrator, you can make currencies available to users, create currency formats, and define how values can be converted between different currencies.

About currencies

If your company does business in multiple countries, you can configure RapidResponse to report money data using each country's local currency. You can add currencies as required, and configure formats for displaying money data in worksheets. Each user can specify a currency they want to view money values in.

One currency must be defined as the base currency, which is the currency used as the base for all conversions. Currencies have associated conversion rates, which are multiplied or divided by the monetary values to convert between the base currency and the target currency. You can specify how conversions are performed, and the operation you choose is used for all currencies you define. For more information, see "Currency conversions" on page 687.

Workbook authors can specify the currency that money values are displayed in, which might require values to be converted before they are displayed. For example, money values in a specific table might be stored in different currencies, and are converted when viewed in a worksheet that specifies the currency. Authors can also specify the conversion dates for worksheet columns, which allows them to convert currencies using rates from past periods and compare values to current rates.

If a worksheet column does not specify the currency to use, money values are converted to the workbook's currency setting, which could be the user's preferred currency or a currency specified by the workbook author.

Overview of adding or creating a currency

Users can view monetary information in any available currency in RapidResponse, unless a resource author specifies a currency. If a currency is required but not available, you can add the currency to make it available. You can add any ISO standard currency, or create a custom currency.

To add or create a currency, perform the following steps:

1. Determine whether a standard currency or new custom currency is required.
2. If a standard currency is needed, add the currency. For more information, see "Adding standard currencies" on page 684.
3. If a new currency is needed, create the currency. For more information, see "Creating currencies" on page 686.
4. Integrate the new currency and import conversion rates. For more information, see "Managing conversion rates" on page 689.

Adding standard currencies

RapidResponse includes over 100 ISO standard currencies, which you can add to your system. For more information about the currencies included with RapidResponse, see "Currency codes" on page 685.

When you add a standard currency, you can search for the currency you want or to find currencies that have a specific symbol or name. The following image shows a search for currencies named "Dollar".

Caution: After you add a currency, it becomes available to all users. If you do not import conversion rates for the currency, any values users view in that currency are identical to the values in the base currency. The values will be displayed using the new currency's symbol, and might result in incorrect data. Decisions should not be made using currencies that do not have conversion rates. For more information, see "Managing conversion rates" on page 689.

▸To add a currency

1. On the **Administration** pane, under **Data**, click **Currencies**.
2. In the **Currencies** dialog box, click **Add**.
3. In the **Add Currency** dialog box, select the currency you want to add.

4. Click **Add**.
5. In the confirmation dialog box, click **Yes** to add the currency.

▸To search for a currency

1. In the **Add Currency** dialog box, click in the search box.
2. To specify search options, click , and then click any of the following:
   - **All**—Searches for the specified text in all columns in the currency list.
   - **ID**—Searches for the specified text in the **ID** column. You can use this option to find specific currency codes.
   - **Symbol**—Searches for the specified text in the **Symbol** column. You can use this option to find currencies that use a specific symbol.
   - **Currency Name**—Searches for the specified text in the **Currency Name** column. You can use this option to find specific currencies or currencies that have common names.
   - **Description**—Searches for the specified text in the **Description** column. You can use this option to find currencies used in a specific country.
   - **Match from start**—The search text you specify is matched against the beginning of each word.
   - **Match anywhere**—The search text you specify can match any part of a word.
3. In the search box, type the text you want to search for. For example, a currency code, a symbol, or a country name.

Currency codes

RapidResponse provides more than 100 ISO standard currency codes, including the following.

ID	Name	Symbol	Description
AUD	Australian Dollar	$	Australia
CAD	Canadian Dollar	$	Canada
CHW	WIR Franc	Fr.	Switzerland
CNY	Yuan Renminbi	¥	China
EUR	Euro	€	European Union
GBP	Pound Sterling	£	United Kingdom
HKD	Hong Kong Dollar	HK$	Hong Kong
JPY	Yen	¥	Japan
KRW	Won	₩	Korea, Republic of
MXN	Mexican Peso	$	Mexico
RUB	Russian Ruble	₽	Russian Federation
TWD	New Taiwan Dollar	NT$	Taiwan, Province of China
USD	US Dollar	$	United States

For a complete list of ISO currency codes, go to http://www.currency-iso.org/en/home/tables/table-a1.html.

Creating currencies

If a standard currency does not meet your needs, you can create a new currency. You might need to create a currency if, for example, you do business in a region that does not have an ISO standard currency code.

> **Caution:** After you create a currency, it becomes available to all users. If you do not import conversion rates for the currency, any values users view in that currency are identical to the values in the base currency. The values will be displayed using the new currency's symbol, and might result in incorrect data. Decisions should not be made using currencies that do not have conversion rates. For more information, see "Managing conversion rates" on page 689.

▸To create a new currency

1. On the **Administration** pane, under **Data**, click **Currencies**.
2. In the **Currencies** dialog box, click **New**.
3. In the **New Currency** dialog box, in the **ID** box, type a code to identify the currency.
4. In the **Name** box, type a name for the currency.
5. In the **Symbol** box, select or type a symbol used to denote the currency.
6. In the **Description** box, type information about the currency, such as when it should be used.
7. Click **OK**.

Managing currencies

Any currencies you add or create are available to all users, and must have conversion rates. If you no longer need a currency, you can stop updating its conversion rates and modify its description to indicate it should not be used. If a currency is incorrect, you can remove it. Any resources that use the currency must be modified to use a different currency. Removing a currency does not delete its conversion rates.

It is recommended you remove currencies only if they have not been used or conversion rates have not been added. Removing a currency does not remove the conversion rates, however, the currency is no longer associated with the rate, and any values stored in that currency are not accurate. If you remove a currency, you must also modify all values, resources, and sites that use that currency to ensure values are correct.

Money data can be displayed in worksheets using any currency you add or create. Depending on the currency or the worksheet user's preference, different currency formatting might be required. Several currency formats are included with RapidResponse, or you can specify your own. For more information, see "Editing and creating formats" on page 665.

Caution: If you change the base currency, you must also update the conversion rates in the **CurrencyConversionActual** and **CurrencyConversionForecast** tables to convert to the new base currency. You must also make changes to your integration and data extract programs to ensure the conversion rates for the old base currency are brought in to RapidResponse and to remove the conversion rates for the new base currency. For more information, see and "Currency conversions" on page 687. For more information about these tables, see the *RapidResponse Analytic and Data Model Guide*.

▸To modify a currency

1. On the **Administration** pane, under **Data**, click **Currencies**.
2. In the **Currencies** dialog box, select the currency you want to modify, and then click **Properties**.
3. In the **Currency Properties** dialog box, modify any of the following:
   - Name
   - Symbol
   - Description

▸To specify the base currency

1. On the **Administration** pane, under **Data**, click **Currencies**.
2. In the **Currencies** dialog box, select the currency you want to make the base, and then click **Set as Base**.
3. Update your integration settings and data extracts to bring in the conversion rates for the currencies that require rates and to update the rates to convert to the new base currency.

▸To remove a currency

1. On the **Administration** pane, under **Data**, click **Currencies**.
2. In the **Currencies** dialog box, select the currency you want to remove, and then click **Remove**.
3. In the confirmation dialog box, click **Yes**.
4. Update your integration settings and data extracts to no longer bring in conversion rates for this currency.

Note: You cannot remove the base currency.

Currency conversions

Any money value can be converted from one currency to any other currency. All conversions are performed by either multiplying or dividing the value by the conversion rate to the base currency. You can choose the operation performed to convert the currencies.

Conversion rates can be brought in to RapidResponse as part of the data update process, or you can insert or edit rates using the Currency Conversion Rates workbook. For more information, see "Managing conversion rates" on page 689.

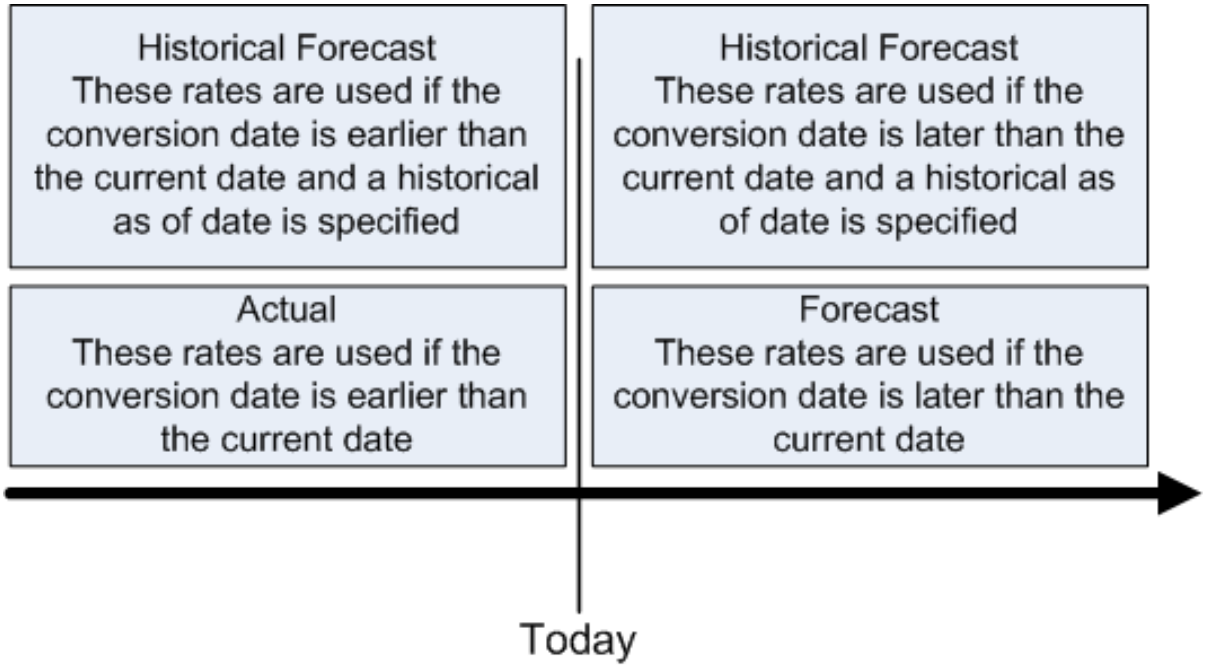
Currencies are converted in worksheets that display column values in a specific currency, or when a user's preferred currency is different than the currency a monetary value is stored in.

The data in the **CurrencyConversionActual**, **CurrencyConversionForecast**, and **HistoricalCurrencyConversion** tables is combined, and are considered to be a single table when determining the date to use to convert a money value. The date specified for the conversion determines which table the conversion rate is taken from. By default, the actual conversion rate for the current date is used for converting currencies.

Expressions that perform currency conversions can specify the date to use for converting the value, using the CONVERTONDATE function, which takes a currency and a conversion date as parameters. The conversion date relative to the current date determines whether the conversion rate is taken from the actual or forecast conversion table. For example, if you specify a conversion date earlier than the current date, a rate from the **CurrencyConversionActual** table is used. If you specify a conversion date later than the current date, a rate from the **CurrencyConversionForecast** table is used.

The CONVERTONDATE function can also take a historical as of date parameter, which is optional. If the historical date is specified, a historical forecast rate from the **HistoricalCurrencyConversion** table is used. For more information about managing historical currency conversions, see the *RapidResponse Data Integration Guide*.

The following diagram shows currency conversion dates and tables.



For all currency conversions, the conversion rate on or before the specified date is used. For example, if conversion rates are updated monthly and you specify 06-21-12 as the conversion date, the rate from 06-01-12 is used. For the **HistoricalCurrencyConversion** table, this also applies to the as of date. For example, if historical data is generated monthly and you specify a conversion date of 07-10-09 and an as of date of 02-20-10, the rate for 07-01-09 for the historical series generated as of 02-01-10 is used.

You can specify whether the current date or each scenario's planning date is used as the default conversion date. If you use historical scenarios, the planning date in those scenarios is not updated, which ensures the converted Money values do not change as new conversion rates are brought in by data updates.

If you use the planning date as the default conversion date, the planning date is also used to determine whether an actual or forecast rate is selected for converting Money values in that scenario.

For more information about these tables, see the *RapidResponse Analytic and Data Model Guide*. For more information about the CONVERTONDATE function, see the *RapidResponse Resource Authoring Guide*.

▸To configure how conversions are performed

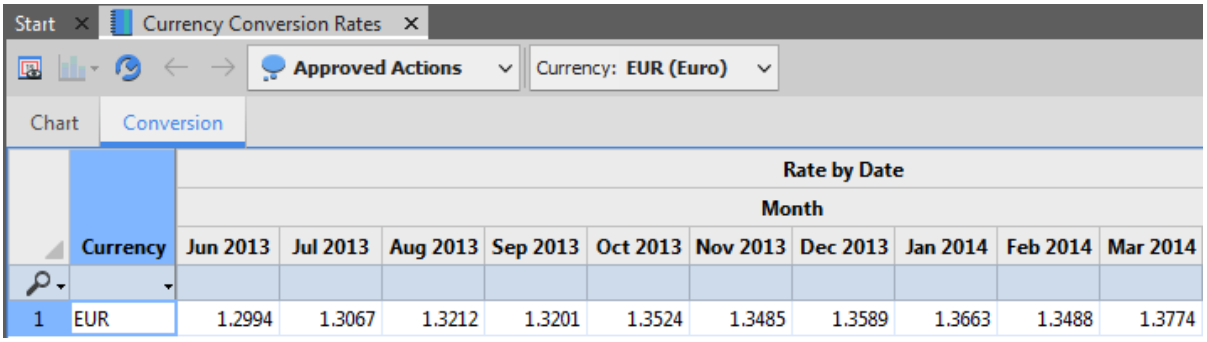
1. On the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Under **Database**, change the value for the **Currency conversion** setting to one of the following:
   - **Multiply**—The monetary values are multiplied by the conversion rate to convert to the base currency.
   - **Divide**—The monetary values are divided by the conversion rate to convert to the base currency.

▸To configure the default conversion date

1. On the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Under **Scenarios**, change the value for the **Default currency conversion date** setting to one of the following:
   - **Current date**—The current date is used as the default conversion date.
   - **MRPDate (planning date)**—Each scenario's planning date is used as the default conversion date.

Managing conversion rates

You can manage and modify conversion rates in the Currency Conversion Rates workbook. This workbook displays all forecast and historical conversion rates for each currency. This workbook is available to all administrators, however, you can share it with users if they require the ability to view and simulate forecast conversion rate changes. All rates in this workbook convert to the base currency. If you share the workbook with users, you should tell them what the base currency is, so they have context for the rates.



	Currency	Rate by Date									
		Month									
		Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014
1	EUR	1.2994	1.3067	1.3212	1.3201	1.3524	1.3485	1.3589	1.3663	1.3488	1.3774

In this example, rates are calculated for the beginning of each month. When currencies are converted, the date used for the conversion determines which monthly rate is used to perform the conversion. The rate from the date before the specified date is used for the conversion. For example, if a conversion date is specified as May 20, 2011, the rate for May 1, 2011 is used.

For conversions that do not specify a conversion date, if the conversion is performed on an input Money field, the conversion rate for the current date is used. For more information, see the *RapidResponse Resource Authoring Guide*.

New and updated conversion rates can be brought in from your enterprise data sources as part of a data update. You can also add and modify rates using the Currency Conversion Rates workbook. You can modify the current rates, or forecast rates. For information about managing historical conversion rates, see the *RapidResponse Data Integration Guide*.

If you add or create a currency, you must update your data extract programs to bring in conversion rates for the new currency, and then perform a data update to bring in the conversion rates and allow the currency to be used in resources. For more information, see .

Caution: If you import or add current conversion rates with the same date as an existing current rate, the rate used for conversions is not predictable. In this case, you should not use the converted money values to make decisions. For information about resolving issues with multiple rates on the same date, see "Deleting duplicate actual conversion rates" on page 693

▸To modify current conversion rates

1. In the **Explorer**, double-click the **Currency Conversion Rates** workbook.
2. In the **Horizon** control, click **Current**.
3. In the **Conversion Detail** worksheet, select the value in the **Rate** column, then type a new value.
4. On the **File** menu, click **Save Data**.

Note: Rates specified using the **Current** horizon are visible in all scenarios.

▸To add a current rate

1. In the **Explorer**, double-click the **Currency Conversion Rates** workbook.
2. In the **Horizon** control, click **Current**.
3. Click the **Conversion Detail** worksheet tab.
4. On the **Edit** menu, click **Insert Record**.
5. In the **Insert Record** dialog box, specify the following:
   - **Currency**—The currency you are inserting a rate for.
   - **Date**—The date the new rate is effective on. If you specify a future date, the rate becomes effective on the date specified, however, this rate is not displayed in the **Currency Conversion** worksheets.
   - **Rate**—The conversion rate.
6. Click **Save and Close**.

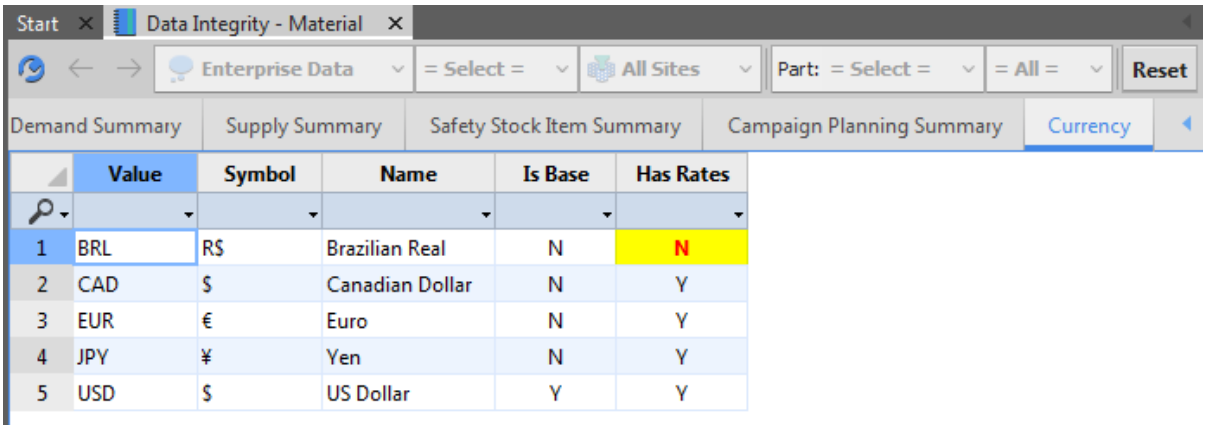
Note: Rates specified using the **Current** horizon are visible in all scenarios.

Tip: You can also insert forecast rates by selecting **Future** in the **Horizon** control. You should insert forecast rates in a private scenario.

Verifying conversion rates

After adding currencies, you can use the data integrity workbooks to verify the currencies have conversion rates. Any currency that does not have conversion rates defined is identical to the base currency, and might result in incorrect data. Decisions should not be made using currencies that do not have conversion rates.

The Data Integrity - Material workbook contains the Currency worksheet, which displays all currencies defined in your system and indicates whether the currency has rates defined.



	Value	Symbol	Name	Is Base	Has Rates
1	BRL	R$	Brazilian Real	N	N
2	CAD	$	Canadian Dollar	N	Y
3	EUR	€	Euro	N	Y
4	JPY	¥	Yen	N	Y
5	USD	$	US Dollar	Y	Y

In this example, the BRL currency does not have rates. You can define a rate using the Currency Conversion Rates workbook, or bring the rates for that currency in using a data update.

Note: The base currency is shown as having rates defined in the **Data Integrity - Material** workbook, however, this currency does not have or require conversion rates.

▸To verify currencies have conversion rates

1. In the **Explorer**, double-click the **Data Integrity - Material** workbook.
2. Click the **Currency** tab.
3. Optionally, search or sort the **Has Rates** column to find any currencies that have an **'N'** value.

Updating conversion rates in scenarios

When you update conversion rates, the new actual rates are updated in all scenarios. New forecast and historical rates, however, are updated in only those scenarios that are configured to automatically update. All scenarios that automatically update from the root scenario receive the updated rates. Any children of an automatically updated scenario can receive the rates when a user updates the scenario. For other scenarios, you can update these rates using the Update Conversion Rates script, which is available to system administrators.

This script is intended to update rates for scenarios that are kept isolated from other data, such as the children of a scenario that is not automatically updated, and that does not have the rates available in its parent. For example, you might have a branch of your scenario tree that is used to simulate changes for a specific set of customer orders, and is not updated with order changes. You could use the script to update the conversion rates in these scenarios, without updating the rest of the data.

You might have access to scenarios for the following purposes

Scenario purpose	Description
Historical	Contains information showing the state of the system at a previous point in time. These scenarios should not have their rates updated.
S&OP cycle	Scenarios created as part of the S&OP process. These scenarios typically are not modified by data updates. If you update the rates in these scenarios, you should update only the forecast rates.
Upgrade	Scenarios created in RapidResponse Version 10.1 or earlier, which did not support money data. Data in these scenarios is represented in a single currency. Updating rates in these scenarios would bring in conversion rates that are not used. These scenarios should not have their rates updated.
Planning	Planning scenarios that represent a frozen snapshot of data. These scenarios are not updated by data updates. If you update the rates in these scenarios, you should update only the forecast rates.
Private	Scenarios owned by users for performing simulations. These scenarios should have their rates updated if the user needs the most recent data. You can also share the script with these users so they can run it and update their own scenarios.

If a user commits a scenario that has had its conversion rates updated by the script, duplicate conversion rate records might be created in the parent scenario. You can delete the duplicate records if desired, but they should not affect conversion calculations. However, if a user has simulated a change in the forecast rates, the forecast rates for that date will have different values, and you cannot predict which rate will be used in calculations.

The Update Conversion Rates script copies the rates from one scenario you specify into other scenarios. You can copy rates into other users' private scenarios if you have permission to manage all scenarios, or you can provide the script to users who have access to at least one scenario that is automatically updated with conversion rates, such as Enterprise Data or Approved Actions.

When you run the script, you can choose to update the forecast or historical rates, or both.

▸To update rates in scenarios

1. In the **Explorer**, double-click the **Update Conversion Rates** script.
2. In the **Source Scenario** list, select the scenario to take the rates from.
3. In the **Destination Scenarios** box, type the name of each scenario to update, separated by commas.

   If a scenario name contains a comma or backslash, you must precede the comma or backslash with the escape character (\). For example, for a scenario named 'Make, Build', you can specify the name by typing `'Make\, Build'`. For a scenario named 'Build\Transfer Sources', you could type `'Build\\Transfer Sources'`.

4. To update historical conversion rates, in the **Include Historical Tables?** list, select **'Yes'**.
5. To update forecast conversion rates, in the **Include Currency Rates?** list, select **'Yes'**.

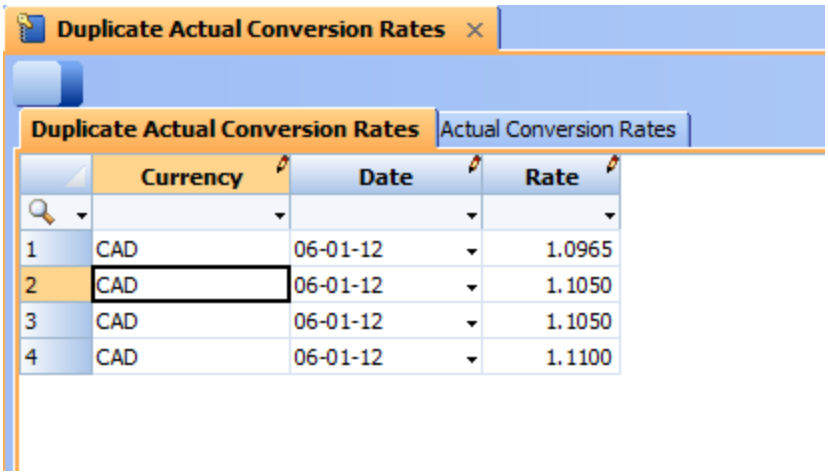
Notes:

- If required, you can share the script with users who own the scenarios that need to be updated. If you share the script, you must ensure those users also have access to a scenario that is automatically updated with conversion rates. For more information, see " Assigning resources" on page 529.
- This script runs commands from the **Update Conversion Rates** workbook, which is available in the **Explorer**. This workbook is intended only for the script and should not be used for other purposes. If you share the script with general users, they do not see the workbook in their **Explorer**.

Deleting duplicate actual conversion rates

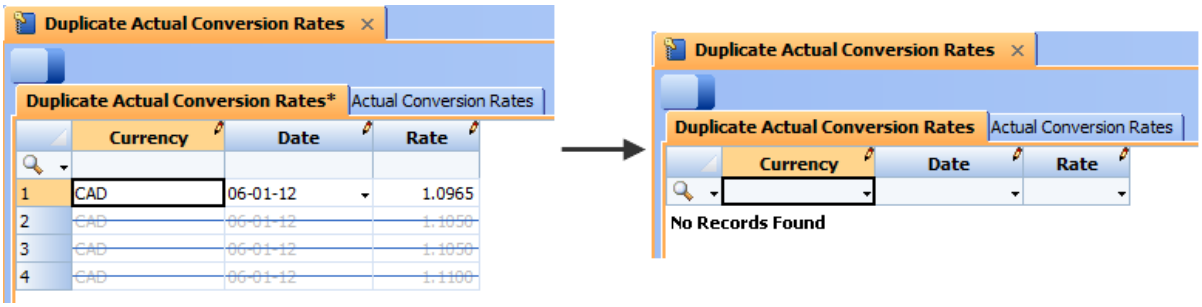
If multiple actual conversion rates have been inserted or imported for the same date, the rate that is used to perform conversions cannot be predicted, and the results might be incorrect. You can delete the duplicate rates, and ensure only one rate is available.

The Duplicate Actual Conversion Rates workbook shows all currencies that have more than one actual conversion rate defined for a date in the Duplicate Actual Conversion Rates worksheet, as shown in the following illustration.



Only currencies that have more than one rate defined on a date are displayed in this worksheet.

You can delete the rates you do not want to use, and ensure that only one rate is specified. When deleting actual conversion rates, you must know which rate is correct. Rates you delete using this workbook are removed from every scenario. When you delete the last duplicate rate, the remaining rate is not displayed in the worksheet, as shown in the following illustration.



You can also view all actual conversion rates in the Actual Conversion Rates worksheet.

▸To delete duplicate actual conversion rates

1. In the **Explorer**, double-click the **Duplicate Actual Conversion Rates** workbook.
2. In the **Duplicate Actual Conversion Rates** worksheet, for each currency and date, determine which rate is the correct rate.
3. For each duplicate rate, do the following:
   - Select the row.
   - On the **Edit** menu, click **Delete Record**.
   - Save your changes.

▸To view actual conversion rates

1. In the **Explorer**, double-click the **Duplicate Actual Conversion Rates** workbook.
2. Click the **Actual Conversion Rates** worksheet tab.

Configuring conversions on calculated fields

You can configure the conversion rate used to convert calculated Money fields in a scenario. Typically, these fields use the most current conversion rate, however, you can configure control tables and perspectives to specify a historical currency conversion date to use for the conversion.

If you want to use a historical date for conversions, you must ensure the currency has rates in the CurrencyConversionActual, CurrencyConversionForecast, and HistoricalCurrencyConversion tables.

If you specify a historical date for conversions in a scenario, that date is also used to determine whether actual or forecast conversion rates are used in conversions. This overrides the current date or planning date, as specified in the Global Settings dialog box. For more information, see "Currency conversions" on page 687.

The currency conversion date is set by the ScenarioSetting control table, which contains a single field, CurrencyAsOfDate, and a single record. The CurrencyAsOfDate field can be used by a perspective to specify a historical currency conversion date to use for converting calculated fields in a scenario. For more information, see "Scenario perspectives" on page 725.

CHAPTER 45: Configuring unit conversions

Quantity values can be expressed in units, which defines how the quantity is measured. The unit of measure a numeric value is expressed in allows you to display values at different levels of detail. For example, you can measure an order quantity in terms of the number of units, the number of cases those units occupy, or the number of pallets those cases occupy.

Each part in your database has an associated unit of measure, which determines the quantities that part is stored, shipped, and recorded in. When you view data in workbooks, you can choose to display the values in different units, which are then converted from the part's standard unit to the selected unit. You can define units and their conversion rates. The values saved in the RapidResponse database are not affected by the units you view the data in, the conversions are performed only in worksheets.

Defining units of measure

Units of measure can be converted, which allows you to create reports that can display those quantities in different units, and users can choose which units they view the values in. Each part has an associated unit, which is the base unit for that part. All conversions are performed relative to this base unit, by multiplying the quantity value by the ratio of the base unit and target unit. Units of measure can be brought in to RapidResponse from your enterprise data sources, or you can define them. If you bring units in from your data sources, you must define the conversion rates for the units.

Units can be converted as long as they are defined in the same control set. You can also use categories to group similar units, and use the category to define sets of units that are meant to be converted. For example, a mass category can include ounces, kilograms, pounds, and tonnes, and then conversion rates for each units can be specified.

Any units in any category can be converted, depending on the units available to be used in a workbook. However, these conversions might not always produce meaningful results. For example, if you have defined length measures and volume measures, a conversion from miles to gallons might be possible, but would not be meaningful. In this case, workbooks would need to define the categories to allow users to select. For more information, see the *RapidResponse Resource Authoring Guide*.

If you attempt to convert units that do not exist in the same control set, the conversion returns NaN (Not a Number), but does not display an error.

By default, RapidResponse does not include predefined units of measure. You must define the units you want to use in reports and calculations, and the conversion rates between them.

Units of measure and conversions are defined in the Control Tables or Control Sets workbooks. Each control set can contain different measures, and you can perform conversions only within the same control set.

Start | Control Tables

Add Category | Enterprise Data

Unit of Measure | Work Center Type | DRP Configuration | IM Configuration | IPO Configuration | MPS Configuration | OF Configuration | SOP Analytics Configuration

	Value	Control Set	Number of Parts	Number of Part Sources	Number of Unit Of Measures	Unit of Measure Description	Category ID	Base Conversion	Rounding Precision
1	DZ	Default			12	Dozen	Count	12.000	9
2		SOPDefault			12	Dozen	Count	12.000	9
3		SOPDemandMgmt			12	Dozen	Count	12.000	9
4	EA	BOMSubstn	23	23	12	Each	Count	1.000	9
5		Default	7,927	4,919	12	Each	Count	1.000	9
6		DemandMgmt	120	135	12	Each	Count	1.000	9
7		Pharma	20	33	12	Each	Count	1.000	9
8		SOPDefault	426	418	12	Each	Count	1.000	9
9		SOPDemandMgmt	130	142	12	Each	Count	1.000	9
10		Training	31	26	12	Each	Count	1.000	9
11	FT	Default	1	1	4	Feet	Length	0.305	9
12		SOPDefault			4	Feet	Length	0.305	9

Units of measure can be organized into categories, which define units that represent similar types of measures at different scales. Units in a category are intended to be converted from one to another, and the base conversions specified for each measure determine the calculation performed within the category.

For example, if you have defined a category for masses, that category can contain kilograms and pounds, so you can convert to or from metric weights for shipments to different regions. An example of measures in this category is shown in the following illustration.

Value	Control Set	Number of Parts	Number of Part Sources	Number of Unit Of Measures	Unit of Measure Description	Category ID	Base Conversion
KG	Default			8	Kilogram	Mass	1.000
	SOPDefault			8	Kilogram	Mass	1.000
	SOPDemandMgmt			8	Kilogram	Mass	1.000
LB	Default			8	Pound	Mass	0.450
	SOPDefault			8	Pound	Mass	0.450

In this example, kilograms are defined as units in three control sets and pounds in two. If you need to convert kilograms to pounds for items that use the SOPDemandMgmt control set, you must first define the pound measure for that control set.

For other metric conversions, you should decide which unit to be the basis of the conversion, and define the other with the value to multiply by to complete the conversion. In the above example, kilogram was chosen as the basis for the conversion, and to convert to pounds, the standard measure's base conversion is divided by the target measure's base conversion, and that value multiplied by the quantity, using the following formula:

```
Quantity * Part base conversion / target base conversion
```

For example, a weight of 1 kilogram converts to 2.22 (repeating) pounds, using the following formula.

Mass in pounds = Quantity * kilogram base conversion / pound base conversion

= 1 * 1 / 0.45

= 1 * 2.22

= 2.22

However, for Money fields, the formula for converting units is

```
Money * target base conversion / Part base conversion
```

Money fields apply to Quantity values on a per-unit basis, and are typically used to display values for the total quantity. When Quantity values are converted into larger or smaller units, the corresponding Money values scale to smaller or larger units respectively, to maintain the total values. For example, assume you have a quantity of 2000 kilograms of parts with a selling price of $1 USD each. If you choose to view the quantity in tonnes (1000 kilograms), the resulting 2 tonnes of parts has a selling price of $1000 USD each. These conversions are represented using the following calculations:

Quantity in tonnes = Quantity * kilogram base conversion / tonne base conversion

= 2000 * 1 / 1000

= 2000 / 1000

= 2

Money in tonnes = Money * tonne base conversion / kilogram base conversion

= 1 * 1000 / 1

= 1000 / 1

= 1000

The total price for this quantity of parts is $2000 USD regardless of the units the values are displayed in.

When you create measures, you must define the unit's base conversion so it calculates the correct values when converted from other units in the category.

▸To define a unit of measure conversion

1. In the **Explorer**, double-click the **Control Tables** workbook.
2. Click the **Unit of Measure** worksheet.
3. Create or select a private scenario to define the measure in.
4. Insert a record, specifying the following:
   - **Control Set**—The control set to add the unit to.
   - **Name**—The unit name.
   - **Base Conversion**—The value used to convert the unit.
   - **Category Id**—The category of measures the unit belongs to. For more information, see "Creating unit categories" on page 700.
   - **Description**—What the unit represents. This value is displayed in unit of measure controls in workbooks.
   - **Rounding Precision**—The number of decimal places to include when performing conversions.
5. Click **Save and Close**.

▸To assign a conversion rate to a unit of measure

1. In the **Control Tables** or **Control Sets** workbook, ensure the **Unit of Measure** worksheet is selected.
2. Ensure a private scenario is active.
3. For the measure you want to define conversion rates for, select the cell in the **Base Conversion** column.
4. Type the value to be used for converting to that unit, and then save your changes.

Defining part-specific unit conversions

In some cases, you might have a part that requires a specific unit of measure conversion. You might do this, for example, you have defined a unit for the number of items in a shipping crate, and either have shipping requirements for certain parts that reduce the number of items that can be shipped together or the part sizes allow for more units per crate.

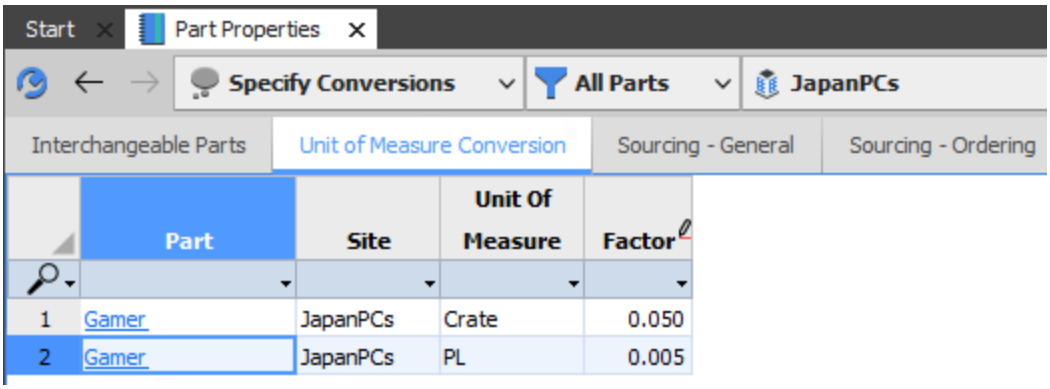
Part-specific unit conversions are calculated by multiplying the quantity by the conversion factor, using the following formula:

```
Quantity * Part conversion factor
```

This conversion does not use the part's standard conversion rate in the calculation. Therefore, you must specify the conversion rate as a fractional value if the target unit is less than the initial unit, which is the opposite of defining the base conversion factors for units. For example, assume you have defined units for units, crates, and pallets, where by default a crate contains 10 units and a pallet contains 10 crates. You might then require a different conversion rate for one part, where a crate contains 20 units. For this example, you would define the part-specific conversion rate as 0.05, which would then divide the unit counts by 20 when conversions are performed.

Similarly, for conversion rates to smaller units, the value you specify must be a value greater than 1, which is multiplied by the quantity.

Part-specific conversion rates are defined in the Part Properties workbook. An example of part-specific rates is shown in the following illustration.



In this example, the Gamer part ships 20 units to a crate and retains the standard conversion of 10 crates to a pallet, which means this part ships 200 units to a pallet.

Start | Part Properties | Shipments

Specify Conversions | All Parts | JapanPCs | EA (Each)

Demand Orders

	Order Id	Line	Part Name	Order Site	Order Type	Due Date	Quantity
12	CS-002	7	Server	JapanPCs	Forecast	07-13-17	150.00
13	CS-002	8	Server	JapanPCs	Forecast	07-20-17	150.00
14	CS-003	3	Gamer	JapanPCs	Forecast	06-15-17	100.00
15	CS-003	4	Gamer	JapanPCs	Forecast	06-22-17	100.00
16	CS-003	5	Gamer	JapanPCs	Forecast	06-29-17	100.00
17	CS-003	6	Gamer	JapanPCs	Forecast	07-06-17	100.00
18	CS-003	7	Gamer	JapanPCs	Forecast	07-13-17	100.00
19	CS-003	8	Gamer	JapanPCs	Forecast	07-20-17	100.00
20	CS-ACT100	1	Workstation	JapanPCs	Actual	06-01-17	200.00
21	CS-ACT100	2	Workstation	JapanPCs	Actual	06-08-17	210.00

Start | Part Properties | Shipments

Specify Conversions | All Parts | JapanPCs | Crate (Crate)

Demand Orders

	Order Id	Line	Part Name	Order Site	Order Type	Due Date	Quantity
12	CS-002	7	Server	JapanPCs	Forecast	07-13-17	15.00
13	CS-002	8	Server	JapanPCs	Forecast	07-20-17	15.00
14	CS-003	3	Gamer	JapanPCs	Forecast	06-15-17	5.00
15	CS-003	4	Gamer	JapanPCs	Forecast	06-22-17	5.00
16	CS-003	5	Gamer	JapanPCs	Forecast	06-29-17	5.00
17	CS-003	6	Gamer	JapanPCs	Forecast	07-06-17	5.00
18	CS-003	7	Gamer	JapanPCs	Forecast	07-13-17	5.00
19	CS-003	8	Gamer	JapanPCs	Forecast	07-20-17	5.00
20	CS-ACT100	1	Workstation	JapanPCs	Actual	06-01-17	20.00
21	CS-ACT100	2	Workstation	JapanPCs	Actual	06-08-17	21.00

Start | Part Properties | Shipments

Specify Conversions | All Parts | JapanPCs | PL (Pallet)

Demand Orders

	Order Id	Line	Part Name	Order Site	Order Type	Due Date	Quantity
12	CS-002	7	Server	JapanPCs	Forecast	07-13-17	1.50
13	CS-002	8	Server	JapanPCs	Forecast	07-20-17	1.50
14	CS-003	3	Gamer	JapanPCs	Forecast	06-15-17	0.50
15	CS-003	4	Gamer	JapanPCs	Forecast	06-22-17	0.50
16	CS-003	5	Gamer	JapanPCs	Forecast	06-29-17	0.50
17	CS-003	6	Gamer	JapanPCs	Forecast	07-06-17	0.50
18	CS-003	7	Gamer	JapanPCs	Forecast	07-13-17	0.50
19	CS-003	8	Gamer	JapanPCs	Forecast	07-20-17	0.50
20	CS-ACT100	1	Workstation	JapanPCs	Actual	06-01-17	2.00
21	CS-ACT100	2	Workstation	JapanPCs	Actual	06-08-17	2.10

In a workbook that uses unit conversions, the standard conversion rate is used for the Server and Workstation parts, while the Gamer part uses its custom rates.

Similarly to base conversions, part-specific conversions on Money fields divide the value by the conversion factor, using the following formula:

```
Money / Part conversion factor
```

▸To specify a part-specific rate

1. In the **Explorer**, double-click the **Part Properties** workbook.
2. Click the **Unit of Measure Conversion** worksheet.
3. Insert a record, specifying the following:
   - **Site**—The site you are defining the part-specific conversion for.
   - **Part**—The part you are defining the rate for.
   - **Unit of Measure**—The unit you are defining the part-specific rate for.
   - **Factor**—The conversion factor to use for converting this part to the specified unit of measure.
4. Click **Save and Close**.

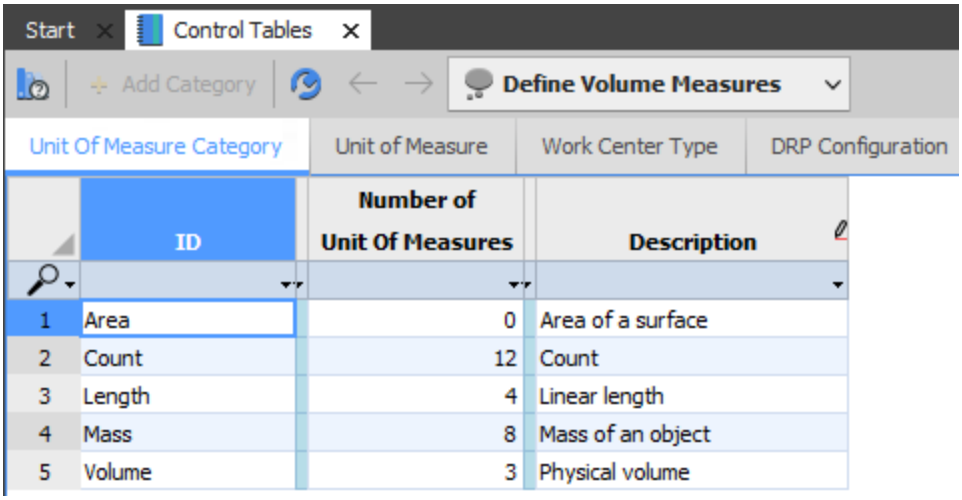
Creating unit categories

Units can be organized into groups, which define units of similar types but at different scales. For example, you might define a volume group, which can contain units such as gallons, tanks, and barrels, where there might be 50 gallons in a barrel and 12 barrels in a tank (600 gallons per tank). You might then take orders in gallons, record inventory levels in barrels, and plan shipments in tanks.

You can create categories to organize your units of measure and define the units that represent similar types of measures at different scales. Each unit can be assigned to a single category, and workbook authors can specify which categories of measures are available in workbooks. For more information, see the *RapidResponse Resource Authoring Guide*.

In the example of the volume units given above, the Volume category could be displayed in a workbook, which would then allow users to display the values in any of the volume units.

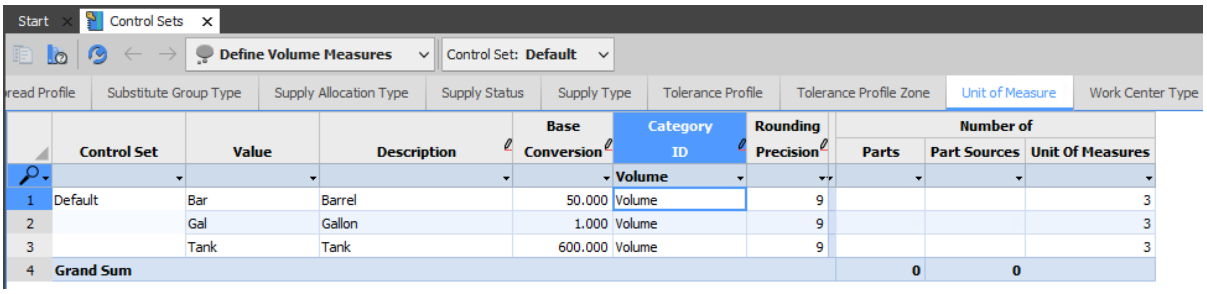
Unit of measure categories are created in the Control Tables workbook.



	ID	Number of Unit Of Measures	Description
1	Area	0	Area of a surface
2	Count	12	Count
3	Length	4	Linear length
4	Mass	8	Mass of an object
5	Volume	3	Physical volume

Each category includes a count of measures assigned to that category. This can help you identify categories that might not be needed, such as the Area category in the above example.

you can assign the measures to categories in either the Control Sets or Control Tables workbook. An example of the volume measures in the group is shown in the following illustration.



	Control Set	Value	Description	Base Conversion	Category ID	Rounding Precision	Number of Parts	Number of Part Sources	Number of Unit Of Measures
					Volume				
1	Default	Bar	Barrel	50.000	Volume	9			3
2		Gal	Gallon	1.000	Volume	9			3
3		Tank	Tank	600.000	Volume	9			3
4	Grand Sum						0	0	

A category can contain measures in multiple control sets. For example, the Count category shown in the following illustration contains twelve measures across seven control sets.

Start | Control Sets

Approved Actions | Control Set: = All =

read Profile | Substitute Group Type | Supply Allocation Type | Supply Status | Supply Type | Tolerance Profile | Tolerance Profile Zone | Unit of Measure | Work Center Type

	Control Set	Value	Description	Base Conversion	Category ID	Rounding Precision	Number of Parts	Number of Part Sources	Number of Unit Of Measures
					Count				
1	BOMSubstn	EA	Each	1.000	Count	9	23	23	12
2	Default	DZ	Dozen	12.000	Count	9			12
3		EA	Each	1.000	Count	9	7,927	4,919	12
4		PL	Pallet	100.000	Count	9			12
5	DemandMgmt	EA	Each	1.000	Count	9	120	135	12
6	Pharma	EA	Each	1.000	Count	9	20	39	12
7		PAC		1.000	Count	9	6		12
8	SOPDefault	DZ	Dozen	12.000	Count	9			12
9		EA	Each	1.000	Count	9	426	418	12
10	SOPDemandMgmt	DZ	Dozen	12.000	Count	9			12
11		EA	Each	1.000	Count	9	130	142	12
12	Training	EA	Each	1.000	Count	9	31	26	12
13	**Grand Sum**						**8,683**	**5,702**	

▸To create a category

1. In the **Explorer**, double-click the **Control Tables** workbook.
2. Click the **Unit of Measure Category** worksheet.
3. Create or select a private scenario to define the measure in.
4. Insert a record, specifying the following:
   - **Id**—The category name.
   - **Description**—What the category represents.
5. Click **Save and Close**.

CHAPTER 46: Scenario management

RapidResponse database and scenarios 703
Scenario data changes and memory consumption 704
Updating scenarios 707
Administrator tools for scenario management 708
Committing data to the root scenario 717
Renaming the root scenario 719
Creating scenario hierarchies 719
Scheduling scenario updates 724
Scenario perspectives 725

RapidResponse system administrators, data administrators, and user administrators can perform various tasks with scenarios. System administrators can perform all scenario tasks, but user administrators and data administrators can perform only tasks they have permission to perform.

User administrators can locate unused scenarios and share scenarios with users and groups.

Data administrators can make scenarios permanent, commit data changes to the root scenario, create hierarchies of scenarios to support business processes, schedule scenario updates, and define perspectives for simulating data changes with different control settings.

Administrators with the “Manage all scenarios” permission can modify shared scenarios (including those not shared to the administrator), delete any shared or private scenario, and give any shared scenario to another user. For more information about permissions, see "Assigning and removing permissions" on page 517.

On-Premises system administrators should also review "Scenario memory consumption" on page 270.

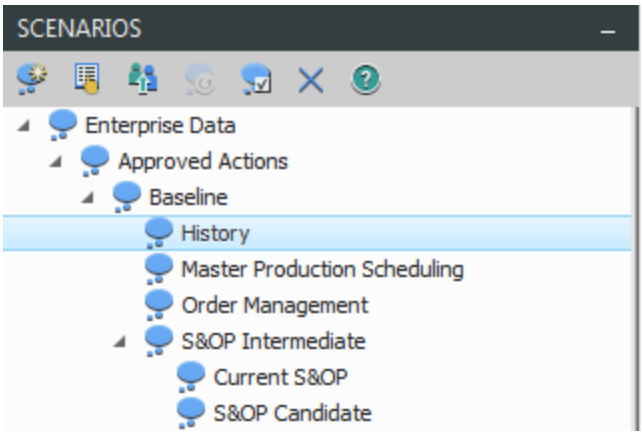
RapidResponse database and scenarios

RapidResponse users access the RapidResponse database through a selected scenario in an open report. The most recent enterprise data imported into RapidResponse is available in the root scenario (typically named Enterprise Data). This scenario can be renamed.

Data in the root scenario is modified by one of the following:

- The data import/update process.
- A data administrator or system administrator committing changes to it.
- An automation process

By default, the root scenario is the only scenario that cannot be deleted. Most implementations of RapidResponse include permanent child scenarios of the root scenario which are used in predefined RapidResponse business processes. Permanent scenarios cannot be deleted. For more information, see "Making scenarios permanent" on page 714.



Your scenario tree will vary depending on which RapidResponse applications your company has licensed, and what scenarios have been created to support your company's business processes.

Scenarios and the data import process

Normally a data import is performed once as part of the RapidResponse data integration process. After the initial RapidResponse data import, regularly scheduled data updates are used to modify the data in the root (Enterprise Data) and other selected scenarios. A data update only modifies the data that has changed since the last data update (or data import).

Performing a data import overwrites the root and permanent scenarios with new data. Any child scenarios of these scenarios, except those that are set as permanent, are deleted and users will need to create new scenarios. For more information about permanent scenarios, see " Creating scenario hierarchies" on page 719.

Scenario data changes and memory consumption

Input data from enterprise data sources is represented in RapidResponse as the Enterprise Data scenario (sometimes called the root scenario). All other scenarios in RapidResponse are based on this scenario and together they can consume a significant portion of system memory. If too much system memory is used, RapidResponse system performance can be adversely affected. As such, it is important to understand how scenarios contribute to memory consumption.

RapidResponse uses a versioned database and every scenario can be considered a copy of its parent. Creating a child scenario does not copy all the data from its parent. Instead, the scenarios are linked; the parent and child scenarios share the same database records except for the records unique to the child due to modifications, deletions, and insertions. Changing data in a child scenario creates a new and unique record relative to its parent and adds another record to the RapidResponse database.

Unless the data in a child scenario changes significantly, child scenarios usually use much less memory than their parent. However, as child scenarios become more out-of-date with the data in their parent, their memory usage can considerably increase.

Consider a RapidResponse system that has 50,000 records changing on a daily basis. This system also keeps a daily snapshot of a historical scenario for 30 days. This RapidResponse system will need to store 1.5 million additional records to accommodate the 30 historical scenarios.

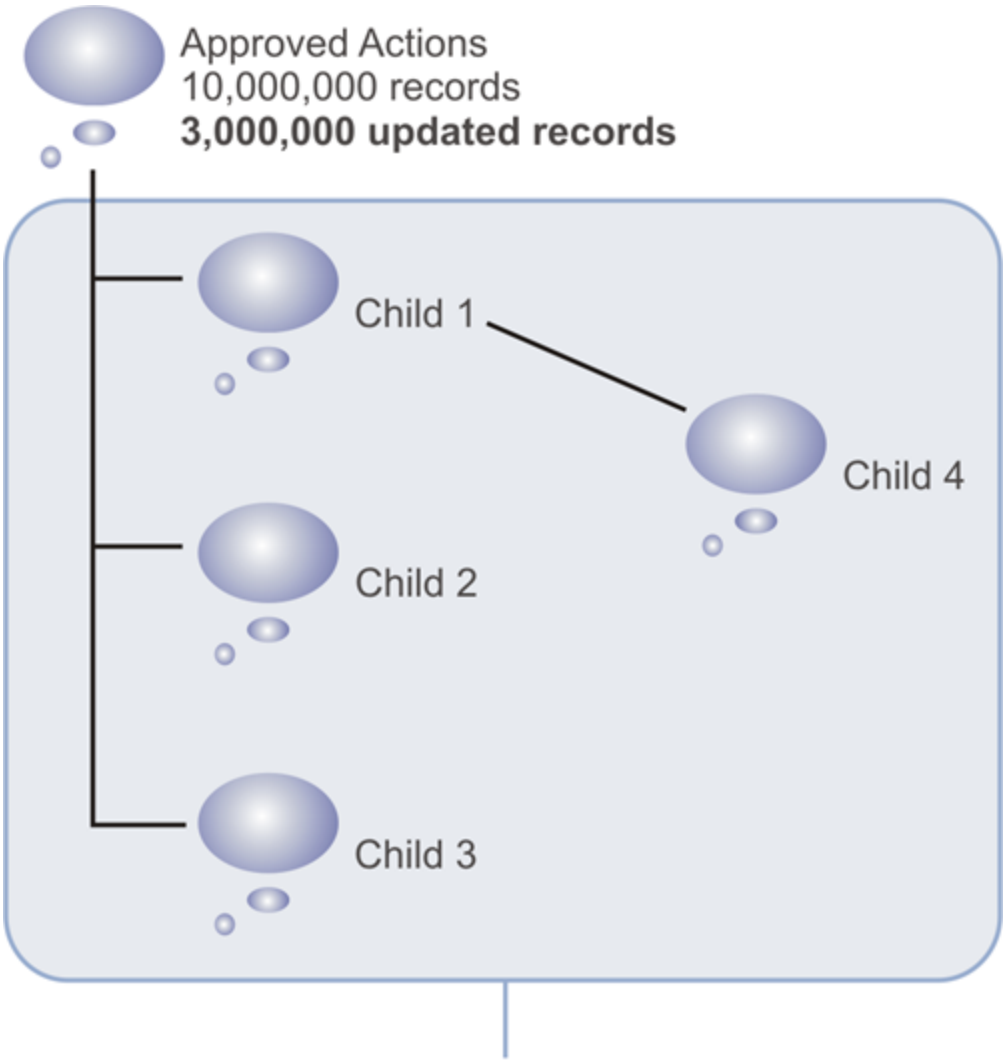
Let's consider another example where scenarios are not synchronized or updated with changes in the root scenario.

When a data update is run, data in the Enterprise Data scenario is updated. By default, the data changes cascade to the Approved Actions scenario and to any other child scenarios that are set to automatically update. Some scenarios can be set to automatically update when a data update is run. All other child scenarios remain out of date with their parents unless manually updated. These out-of-date child scenarios can potentially consume a significant amount of system memory.

Assume the Approved Actions scenario has four child scenarios and none are automatically updated. Over several weeks, 3,000,000 records out of the 10,000,000 input records in the Approved Actions scenario have changed as a result of data updates.

As a result, the four child scenarios have 3,000,000 records out of date with their parent, Approved Actions. If you assume the four child scenarios are almost identical to each other, then the RapidResponse database includes 13,000,000 input records:

- 7,000,000 (original records in the Approved Actions scenario)
- 3,000,000 (records changed as a result of data updates in the Approved Actions scenario)
- 3,000,000 (records out of date in the child scenarios)



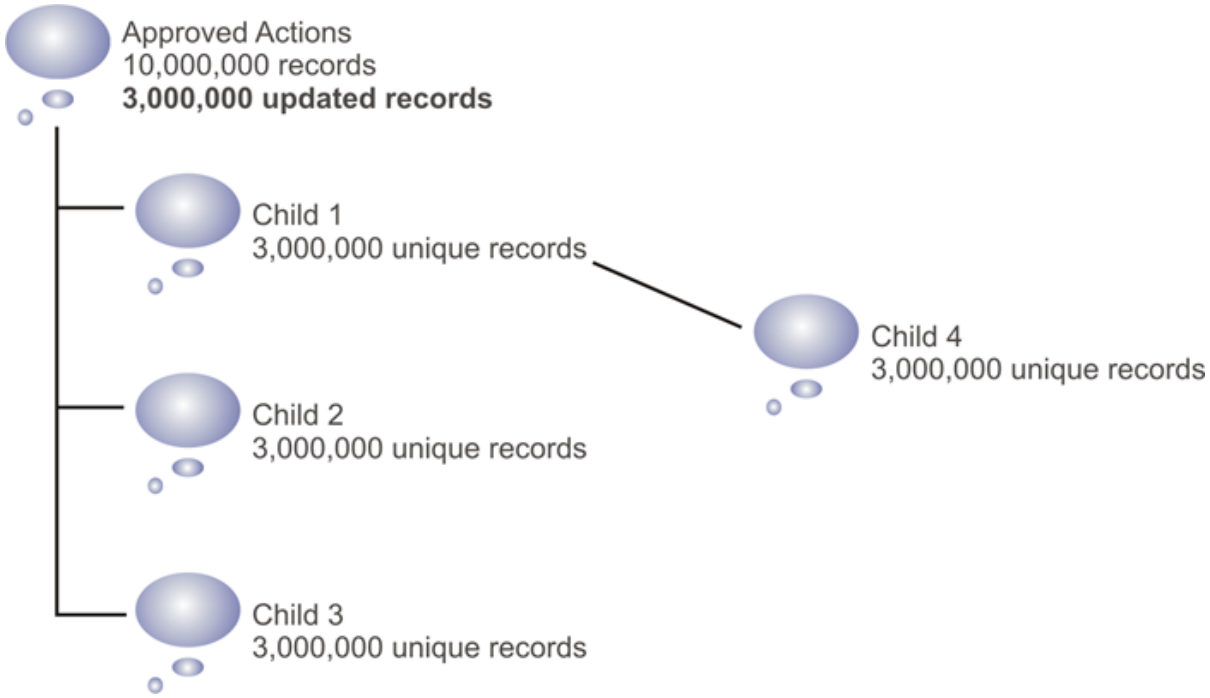
The four out-of-date child scenarios share 3,000,000 records that are out of date with the parent.

The 3,000,000 out-of-date records in the four child scenarios are only counted once (not four times) because RapidResponse automatically shares database records (and memory allocation for the records) when multiple child scenarios become out of date with their parent scenario.

However, if the child scenarios were very different from each other, then the system memory consumption could dramatically increase. Assume the records that changed in the parent scenario (Approved Actions) were unique in each of the child scenarios; that is, each child scenario has different records for the 3,000,000 updated records. This results in 22,000,000 records in the RapidResponse database:

- 7,000,000 (original records in the Approved Actions scenario)
- 3,000,000 (records changed as a result of data updates in the Approved Actions scenario)
- 3,000,000 (records out of date in Child1 scenario)
- 3,000,000 (records out of date in Child2 scenario)

- 3,000,000 (records out of date in Child3 scenario)
- 3,000,000 (records out of date in Child4 scenario)



To help reduce system memory consumption due to scenarios being out of date with their parents, administrators need to consider automatically deleting scenarios that are no longer used or automatically updating child scenarios when their parent changes.

Modifying shared scenarios

When modifying data in shared scenarios, each change causes a data refresh for all users who have worksheets using the scenario. Instead of a single refresh when multiple changes from a private scenario are committed to the shared parent, each update to the shared scenario causes a refresh in worksheets that use the scenario.

By default, users attempting to change data in a shared scenario receive a warning message confirming their intent to change data in a shared scenario. Changing a shared scenario that is accessed by a large number of users, or that is used for worksheets that involve analytics can result in performance issues with RapidResponse. Administrators can disable this warning on a scenario-by-scenario basis in the scenario properties, particularly if there will not be frequent changes to the scenario data.

Updating scenarios

Updating a scenario copies data changes from the parent scenario to a child scenario.

Users should update a scenario when they require the most recent data from its parent. For example, if a change has been made to a group of parts, a user might want to update their scenario to determine how that change has impacted their simulation, or to ensure any data they modify is up to date.

If a user updates a scenario that has conflicting changes in its parent, they are warned about the conflicts, and have the choice to overwrite their changes with the changes in the parent, or to cancel the update. If they cancel the update, they can view the conflicts in the scenario's properties.

Each scenario update operation analyzes the data changes that are to be copied from the parent to child scenario. Internally, data that has been deleted in the child scenario is temporarily re-applied (includes any related deletes). This consolidation process requires the RapidResponse database to be placed in a temporary locked state to ensure consistency of the results. During this time, RapidResponse users might experience longer than normal runtimes when saving data changes.

If data has been modified in a table that contains vector data, updating the scenario might overwrite records in the vector data that you do not expect to be modified. Vector records are defined in terms of their vector key fields, so if you delete and then insert a vector record with the same keys, that record is considered to be the same as the record you deleted. If you then update the scenario with changes from its parent, if the same vector record is in the parent scenario, its value overwrites the value in the child scenario, which might lead to unexpected results. For more information about vector data, see the *RapidResponse Data Integration Guide*.

Some RapidResponse systems deploy a scenario structure that might hold a significant number of deleted records.

It is recommended that scenarios with large volumes of deleted records not be automatically updated when out of date with their parent. Instead schedule the scenario update operation to run at a specified time. This helps to ensure a more predictable experience for RapidResponse users.

For more information about scheduling commands, see "Commands and scheduling system tasks" on page 381.

Administrator tools for scenario management

All RapidResponse administrators can use the Scenarios workbook to review information about the scenarios being used on their RapidResponse systems. For example, the workbook reports whether a scenario is shared, its owner, when it was last used, whether it is permanent, and other information.

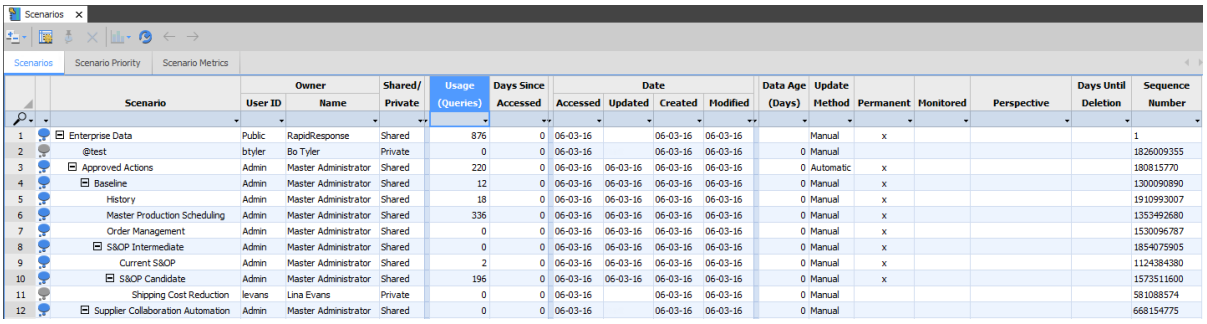
The Scenarios workbook includes three worksheets:

- The Scenarios worksheet, which lists (in a tree view) all private and shared scenarios available in RapidResponse.
- The Scenario Priority worksheet, which lets you prioritize scenarios and determine which ones will have their cached results discarded first when system memory usage is too high.
- The Scenario Metrics worksheet, which provides current and historical information about the total number of private and public scenarios on your RapidResponse system. This worksheet provides the same scenario data as the Input Records and Scenarios worksheet in the Administration Log workbook. The Input Records and Scenarios worksheet also logs the number of input records in the root scenario. For more information, see "Input Records and Scenarios worksheet" on page 425.

Note: The Scenarios workbook is available to all administrator types. However, only administrators with the Manage all scenarios permission can use this workbook to delete scenarios. For more information, see "Deleting scenarios" on page 711.

Reviewing scenario usage

The Scenarios worksheet includes information such as the last time a scenario was used or updated and the permanent status. It also includes several key pieces of information that can help reduce the number of scenarios in use and subsequently reduce the amount of memory being consumed.



Scenarios | Scenario Priority | Scenario Metrics

	Scenario	Owner		Shared/	Usage	Days Since	Date				Data Age	Update	Permanent	Monitored	Perspective	Days Until	Sequence
		User ID	Name	Private	(Queries)	Accessed	Accessed	Updated	Created	Modified	(Days)	Method				Deletion	Number
1	Enterprise Data	Public	RapidResponse	Shared	876	0	06-03-16		06-03-16	06-03-16		Manual	x				1
2	@test	btyler	Bo Tyler	Private	0	0	06-03-16		06-03-16	06-03-16	0	Manual					1826009355
3	Approved Actions	Admin	Master Administrator	Shared	220	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Automatic	x				180815770
4	Baseline	Admin	Master Administrator	Shared	12	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1300090890
5	History	Admin	Master Administrator	Shared	18	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1910993007
6	Master Production Scheduling	Admin	Master Administrator	Shared	336	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1353492680
7	Order Management	Admin	Master Administrator	Shared	0	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1530096787
8	S&OP Intermediate	Admin	Master Administrator	Shared	0	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1854075905
9	Current S&OP	Admin	Master Administrator	Shared	2	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1124384380
10	S&OP Candidate	Admin	Master Administrator	Shared	196	0	06-03-16	06-03-16	06-03-16	06-03-16	0	Manual	x				1573511600
11	Shipping Cost Reduction	levans	Lina Evans	Private	0	0	06-03-16		06-03-16	06-03-16	0	Manual					581088574
12	Supplier Collaboration Automation	Admin	Master Administrator	Shared	0	0	06-03-16		06-03-16	06-03-16	0	Manual					668154775

Administrators with the Manage All Scenarios permission can delete shared and private scenarios from this worksheet. For more information about permission to delete other users' scenarios, see "Assigning and removing permissions" on page 517.

Column	Description
Scenario	The name of the scenario.
Owner-User ID	The user ID of the scenario's owner. Together with Owner - Name, this information helps to distinguish private scenarios that have the same name.
Owner - Name	The user ID of the scenario's owner. Together with Owner - User ID, this information helps to distinguish private scenarios that have the same name.
Shared/ Private	Indicates whether the scenario is shared or private.
Usage (Queries)	Number of queries that have been run against this scenario. For example, opening a workbook and selecting the scenario counts as a query. Note that this value might be approximate. This value is reset when the usage count is reset.
Days Since Accessed	The number of days since the scenario was last used by a user or a process (for example, alerts). If a scenario has not been accessed for a significant amount of time, consider deleting it or contacting the owner and requesting the scenario be deleted.
Date - Accessed	The date the scenario was last used by a user or a process (for example, alerts). If a scenario has not been accessed for a significant amount of time, consider deleting it or contacting the owner and requesting the scenario be deleted.

Column	Description
Date - Updated	The date the scenario was last synchronized with its parent. Synchronization includes updating the scenario or discarding all changes in the scenario. If the scenario has never been synchronized the column is blank. If a scenario has not been synchronized for a significant amount of time (or never synchronized), consider deleting it or contacting the owner and requesting the scenario be deleted.
Date - Created	The date the scenario was created. Consider deleting significantly old scenarios not in use or contacting the owner and requesting the scenario be deleted.
Date - Modified	The date the scenario was last modified. If a scenario has not been modified for a significant amount of time, consider deleting it or contacting the owner and requesting the scenario be deleted.
Data Age (Days)	The number of days since the scenario was last synchronized with its parent. Synchronization includes updating the scenario or discarding all changes in the scenario. If the scenario has never been synchronized then the number of days since the scenario was created. Scenarios that have not been synchronized for 90 days or more are highlighted with a yellow background. This column is blank for the root scenario. If a scenario has not been synchronized for a significant amount of time (or never synchronized), consider deleting it or contacting the owner and requesting the scenario be deleted.
Update method	The method that is used to update the scenario, which can be either manual or automatic.
Permanent	An X is displayed if the scenario is permanent. Permanent scenarios are always kept when they are committed, and they cannot be deleted.
Monitored	An X is displayed if the scenario is monitored by a Change Data Capture instance to capture changes in records.
Perspective	If a perspective is applied to the scenario, the perspective name.
Days Until Deletion	If you have defined an unused scenario deletion limit, the number of days before the scenario is automatically deleted. Permanent scenarios report a blank value in this column. If you do not use a scenario deletion limit, this column is blank and can be hidden.
Sequence Number	This number uniquely identifies a scenario in RapidResponse. If a scenario is deleted and then recreated, the sequence number will not be the same. This number is sometimes used to identify a private scenario in system workbooks and administration processes.

▸To sort dates in the Scenarios workbook

1. In the **Administration** pane, under **System Monitoring**, click **Scenarios**.
2. Select a column based on dates, and then on the **Data** menu, click **Sort Ascending**.

▸To reset the resources and scenarios counter

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click **Usage Counts** on the workbook toolbar.
3. Click **Reset**.

   This resets the value in the **Usage** column to zero for all scenarios, and changes the date in the **Usage Counts** dialog box to today's date. Usage counts in the **Resources** workbook are also reset. For information about the **Resources** workbook, see "Monitoring resource usage" on page 746.

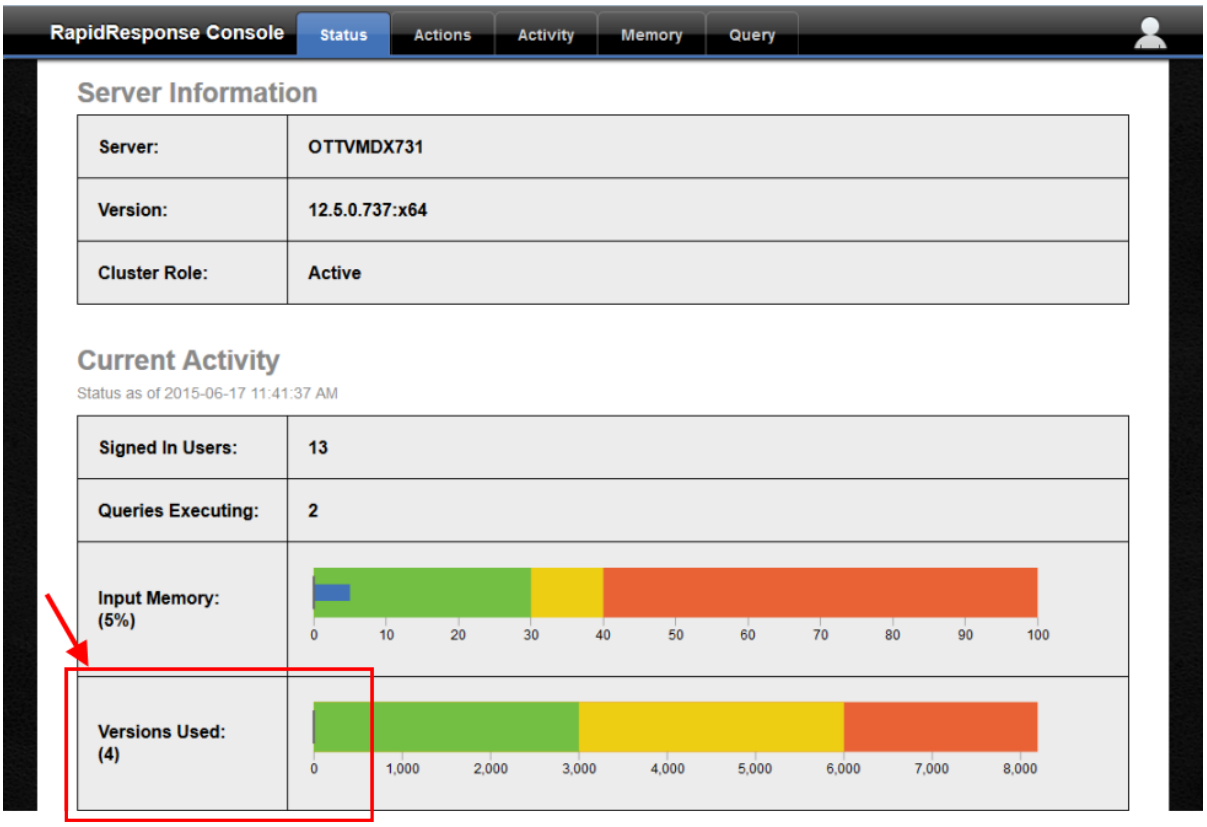
Scenario usage statistics from RapidResponse Console

This topic only applies to the **On-Premises** version of RapidResponse.

From the RapidResponse Console's **Status** page, you can quickly review the number of scenarios in use.

Scenarios internally are built out of *versions*. The number of versions a scenario requires depends on its relationship with other scenarios in the system. RapidResponse can support up to 8,192 versions. While data is being modified (transactions), the changes are stored internally in temporary scenarios in the RapidResponse database. As data and scenarios change, RapidResponse continuously manages the versions by collapsing and deleting versions that are no longer required.

In the following example, 4 scenarios (and versions) are being consumed. To start RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.



Deleting scenarios

An excess number of scenarios, particularly out-of-date scenarios, can degrade RapidResponse system performance. Deleting unused or stale scenarios frees up system memory.

Scenarios can only be deleted by their owners or by administrators who have been assigned the "Manage all scenarios" permission. With this permission, you can use the Scenarios workbook to delete any scenario, including private scenarios owned by other users. You can also delete shared scenarios or your own private scenarios through the Scenarios pane. For more information about permissions to manage scenarios, see "Assigning and removing permissions" on page 517.

If a scenario is permanent, you cannot delete it until you remove its permanent status. For information about permanent scenarios, see "Making scenarios permanent" on page 714.

Sometimes deleting a scenario affects other scenarios, users, or resources. For example, when you delete a scenario, all of its child scenarios are also deleted.

Before you confirm the deletion of a scenario, you are warned if:

- The scenario has child scenarios.
- The scenario or its child scenarios are currently being used by someone else.
- You own alerts or scheduled tasks that use the scenario. If you own alerts and scheduled tasks that use the scenario you are deleting, you are prompted to delete or keep these resources.

Note: If someone else owns alerts, scheduled tasks, or automation chains that are based on the scenario that you are deleting, you are not warned. These resources are kept.

▸To delete scenarios using the Scenarios workbook

1. In the Administration pane, under System Monitoring, click **Scenarios**.
2. Select the scenario you want to delete. Be sure to select the entire row by clicking the row number.
3. In the worksheet toolbar, click **Delete** ✕.
4. Click **Yes** to confirm the deletion.
   The selected scenario and all of its child scenarios are deleted.

▸To delete shared scenarios using the Scenarios pane

1. In the **Scenarios** pane, select a scenario.
2. On the **Actions** menu, click **Properties**.
3. On the scenario properties toolbar, click **Delete** ✕.
4. Click **Yes** to confirm the deletion.
   The selected scenario and all of its child scenarios are deleted.

Note: Some resources close automatically after a scenario they were using is deleted, including scorecards that will have their only scenarios deleted, workbooks with scenario comparison columns, and scenario properties windows.

Tip: You can also click **Delete** on the **Actions** menu, or click ✕ on the Scenarios pane toolbar.

Automatically deleting unused scenarios

An excess number of scenarios and obsolete scenarios can degrade RapidResponse system performance. Deleting unused or stale scenarios frees up system memory.

RapidResponse can be configured to automatically delete all scenarios that have not been used after a specified number of days and that have no child scenarios that were used during that time period. The

scenario is deleted 24 hours after the specified number of days or when the RapidResponse service is restarted. The default period for deleting unused scenarios is one of the following:

- **On-Demand**: 30 days.
- **On-Premises**: No default value.

If the scenario deletion is based on the specified data age (in days) of the scenario, a scenario that has not been used for the specified period is marked for deletion. After the scenarios are deleted, a message listing the deleted scenarios is sent to the Master Administrator.

Scenario usage includes the following categories:

- Accessed (for example, used in a query)
- Updated (or synchronized) with its parent
- Created date
- Modified (for example, data was changed)

The Scenarios workbook (shown in the following image) includes columns that show these dates.

Date			
Accessed	Updated	Created	Modified
06-19-15		03-20-15	03-20-15
05-14-15		05-14-15	05-14-15
05-29-15	05-28-15	05-28-15	05-29-15
05-29-15	05-28-15	05-28-15	05-29-15

For more information, see "Reviewing scenario usage" on page 709.

As scenarios approach deletion, administrators and the scenario owner can be notified of the upcoming deletion. You can configure how many days before deletion this notification is sent, and the notification is sent every day until either the scenario is used or it is deleted. This notification includes a list of scenarios and how many days remain before they are deleted. Notifications sent to scenario owners include only that user's scenarios, and notifications sent to administrators include every scenario that is due to be deleted.

You can only perform this task if you are using On-Premises RapidResponse, and you are a system administrator.

▸To specify the number of days after which a scenario is deleted

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Scenarios** category.
3. In the **Unused scenario deletion limit** box, type the number of days after which an unused scenario is to be deleted.
4. In the **Unused scenario deletion notification** box, type the number of days before deletion to send a notification about deleting the scenario.
5. Click **OK**.
6. Sign out and back into RapidResponse so that the changes take effect.

Note: You can specify a number of days for the deletion notification, but if you have not specified a value for the deletion limit, these notifications are not sent.

Setting scenario priority

Administrators can use the Scenario Priority worksheet in the Scenarios workbook to prioritize the order in which cached results from permanent scenarios are discarded when system memory is reclaimed on a RapidResponse server. If system memory needs to be reclaimed, cached results from scenarios are discarded to reclaim available memory. By prioritizing the scenarios, you can specify which scenarios have cached results that are more important and should be discarded as a last resort, after lower priorities.

Scenarios with a higher number in the priority column are considered a higher priority and have their cached results discarded last when memory is reclaimed.

Notes:

- The unused scenarios are deleted upon restart of the RapidResponse service.
- Permanent scenarios cannot be automatically deleted.
- Scenarios with child scenarios are not deleted. However, if the child scenarios are deleted due to exceeding the non-use threshold, then the parent scenario could also be deleted if it also exceeds the threshold.

Making scenarios permanent

If your company has scenarios that are required for your business processes, a data administrator or system administrator can make them permanent. A permanent scenario cannot be deleted, and is always present after a scenario commit or a data import. Only shared scenarios can be made permanent. To make a scenario permanent, you must have access to its parent, and the parent must be permanent. For more information about supporting business processes with permanent scenarios, see " Creating scenario hierarchies" on page 719.

You can make a scenario permanent (or remove its permanent status) if all of the following conditions are met:

- It is a shared scenario. (You can tell a scenario is shared when the icon beside it is blue.)
- Its parent scenario is permanent.
- You are a system or data administrator who owns the scenario, you have permission to manage all scenarios, or both.

▸To make a scenario permanent or remove its permanent status

1. In the **Administration** pane, under **System Monitoring**, click **Scenarios**.
2. Select the scenario you want to make permanent or non-permanent, and then click **Change the Permanent Setting** 🔒 on the workbook toolbar.

Notes:

- You cannot change the permanent setting of the root scenario.
- You cannot change the permanent setting of a scenario that is being monitored for data changes. For information about RapidResponse Web Services, see the *RapidResponse Web Services Guide*.

Tip: If you meet the requirements for toggling a scenario's permanent status in the **Scenarios** workbook, you can also toggle its permanent status in the **Scenario Properties** dialog box by selecting or deselecting the **Permanent** check box on the **General** tab.

Committing permanent scenarios

When a scenario that is not permanent is committed, its data changes and Activity Log are moved into its parent, and the user has the option to delete or keep the scenario. The default option is to delete the scenario. If the user deletes the scenario, all child scenarios of the committed scenario are also deleted. While it is good practice to delete scenarios when they are no longer needed, deleting the committed scenario and its child scenarios could be disruptive to business processes in some situations.

You can eliminate the risk of this type of error by making a scenario permanent. When a permanent scenario is committed, users do not have the option to delete the scenario so the scenario and any child scenarios it might have are maintained.

When the scenario being committed is kept, it is updated with the most recent changes from its parent, then its data changes and Activity Log are moved into its parent. After the scenario is committed, the scenario and its parent contain the same data. Child scenarios of the committed scenario are unaffected.

Making a scenario permanent also allows users who do not own the scenario, but have permission to modify both the scenario and its parent, to commit the scenario.

Data import and permanent scenarios

If you perform a data import, all scenarios that are not permanent are deleted. Permanent scenarios retain their sharing permissions, but lose their data and all entries in their Activity Logs.

Automatically updating scenarios

You can make a shared scenario that you own update automatically when its parent is updated. For a scenario to update automatically, its parent scenario must also be a shared scenario.

You might do this for a scenario that you always want to keep up to date, such as one with automatic data modifications or one used as part of a scenario hierarchy, as discussed in " Creating scenario hierarchies" on page 719. For more information about automatic data modifications, see “Schedule an automatic data modification” in the *RapidResponse User Guide*.

Some scenarios such as Approved Actions are set to update automatically by default.

For complete information about making a scenario update automatically, see “Automatically update a scenario” in the *RapidResponse User Guide*.

Giving scenarios to other users

Administrators with the “Manage all scenarios” permission can give any shared scenario to another user. The user must have permission to create scenarios.

You might give a scenario if the user is no longer responsible for maintaining it, or is changing job functions. The user to whom you give the scenario becomes the owner of the scenario, though if the scenario is shared, you can choose to have the original owner maintain access to the scenario. Shared scenarios can only be given to recipients who also have permission to share scenarios.

▸To give a scenario as an administrator

1. In the **Scenarios** pane, select the scenario you want to give.
2. On the **Actions** menu, click **Give**.

3. In the **Give Scenario** dialog box, do the following as applicable:
   - In the **Owner** list, click the user you are giving the scenario to.
   - Optionally, in the **Notify new owner** area, type a message to notify the new owner that the scenario has been given to them.
   - Select **Give current owner's child scenarios** to give child scenarios based on the scenario that is being given.
   - Select **Allow current owner to access this scenario with permission** to provide the current owner access to the scenario that is being given. Choose **View** only or **Modify** from the drop down list.
   - Select the **Close all resources that are using this scenario** check box if you are not retaining access to the scenario and want to close the resources using it.

Committing data to the root scenario

A data administrator or system administrator can commit data changes to the root scenario. Typically, you would commit or modify data in the root scenario only to do any of the following:

- Commit data integration configuration settings.
- Add or remove sites.
- Add or remove control sets.
- Persist data that does not exist in your enterprise data sources.
- Modify records that have been automatically created.

Caution: Performing any other operations with data in the root scenario can cause damage to your data. Committing data changes to the root scenario can change the modified records' data sources. Records that are brought in to RapidResponse by a full data update should never be modified in the root scenario.

Committing data to the root scenario can result in records being incorrectly labelled as duplicates. For example, if you modify records in a child scenario and commit the changes to the root scenario, the modified records are considered to belong to RapidResponse. If a data update contains records with the same key values, the records are modified to match the data in the update, and the records' data source is modified to match the source of the data update. However, if the data source of that update is not the records' original source, any data updates from the original source will consider the record to be a duplicate.

Committing data to the root scenario can also result in records not being deleted when they should be. For example, if a record in the root scenario does not exist in a data source, it is not deleted during a data update. If a record is modified in the root scenario and then deleted from its data sources, the record is never deleted from the root scenario following a data update.

If you delete records in the root scenario (through committing a scenario), those records are removed from the RapidResponse database. Record deletion cannot be undone. However, if the records exist in a data source, they are brought in to RapidResponse the next time a data update is performed. If you want to delete a record from RapidResponse, you should delete it only from the data source, because records that do not exist in the data source but do exist in RapidResponse are deleted as part of the data update.

Importing data from Microsoft Excel into a child of the root scenario and committing the changes is not recommended. By committing imported data into the root scenario, the data is considered to exist only

in RapidResponse instead of being associated with a data source. Data without a data source can be modified by any matching record during a data update, which could result in data that does not match your expectations. To ensure the data being imported is associated with the correct data source, you should always use the data update functionality to bring data in to the root scenario.

Before you commit data changes to the root scenario, you should always review the changes to ensure they are correct. A commit cannot be undone, and any changes made to the root scenario are immediately visible in child scenarios that are configured to automatically update. You can also review the data changes that have been committed to the root scenario.

▸To determine changes are correct

1. In the **Scenarios** pane, click the child scenario that contains the data changes.
2. On the **Actions** menu, click **Properties**.
3. Click the **Data Changes (Pending Commits)** tab.
4. Examine each change to ensure the correct fields are being modified with the correct data.

Notes:

- The Data Changes (Pending Commits) worksheet only displays data changes if the data change tracking option is enabled. For more information, see "Data change tracking and record identification" on page 829.
- Changes from Automatic data modification workbooks are not logged in the Data Changes (Pending Commits) worksheet unless the command has enabled logging. For more information, see the *RapidResponse Resource Authoring Guide*.

▸To commit changes to the root scenario

1. In the **Scenarios** pane, click the child scenario you want to commit.
2. On the **Scenarios** pane toolbar, click **Commit**.
3. In the confirmation dialog, click **Yes**.
4. In the **Commit Scenario** dialog box, optionally type a message to be displayed in the root scenario's Activity Log.
5. Click **OK**.

Note: When you are committing changes to the root scenario, the option to add a response does not appear on the **Commit Scenario** dialog box.

▸Reviewing data changes in the root scenario

1. In the **Administration** pane, under **System Monitoring**, click **Administration Log**.
2. Click the **Changes to Root Scenario** worksheet.

Notes:

- For more information about the **Changes to Root scenario** worksheet, see Administration Log's workbook help.
- RapidResponse logs information about root scenario data changes in the RapidResponse database. Over time, these system records can grow in size and potentially consume

significant amounts of memory. By default, RapidResponse automatically deletes these records after 45 days.
On-Demand: The frequency in which these records are deleted can be configured Kinaxis Customer Support.
On-Premises: The frequency in which these records are deleted can be configured as discussed in " Automatic deletion of system records" on page 277.

Renaming the root scenario

The root scenario contains the most recent data extracted from your enterprise data sources, and is the basis for all simulation scenarios users create. By default, the root scenario is named Enterprise Data.

System administrators can change the name of the root scenario.

If you rename the root scenario, you must also change the name in any workbooks, alerts, or filters that reference it. All users must be signed off of RapidResponse before the root scenario can be renamed.

▸To rename the root scenario

1. In the **Administration pane**, under **System Settings**, click **Global Settings**.
2. Expand the **Scenarios** category.
3. In the **Root scenario name** box, type the new scenario name.
4. Click **OK**.
5. Do one of the following:
   - **On-Premises:** Restart the RapidResponse Server. It can be restarted using the Scheduled System Tasks workbook or the RapidResponse Console. For more information see, "Commands and scheduling system tasks" on page 381 or "To stop and restart the RapidResponse Server service in one step" on page 231.
   - **On-Demand:** Contact Kinaxis Customer Support to request your RapidResponse instance be restarted.

Note: The root scenario's name cannot begin with a question mark (?) character.

Creating scenario hierarchies

If you are a data administrator or system administrator, you can create a hierarchy of permanent scenarios to support a required business process. The hierarchy you can create depends on the structure of your company, data requirements, and whether historical scenarios are required.

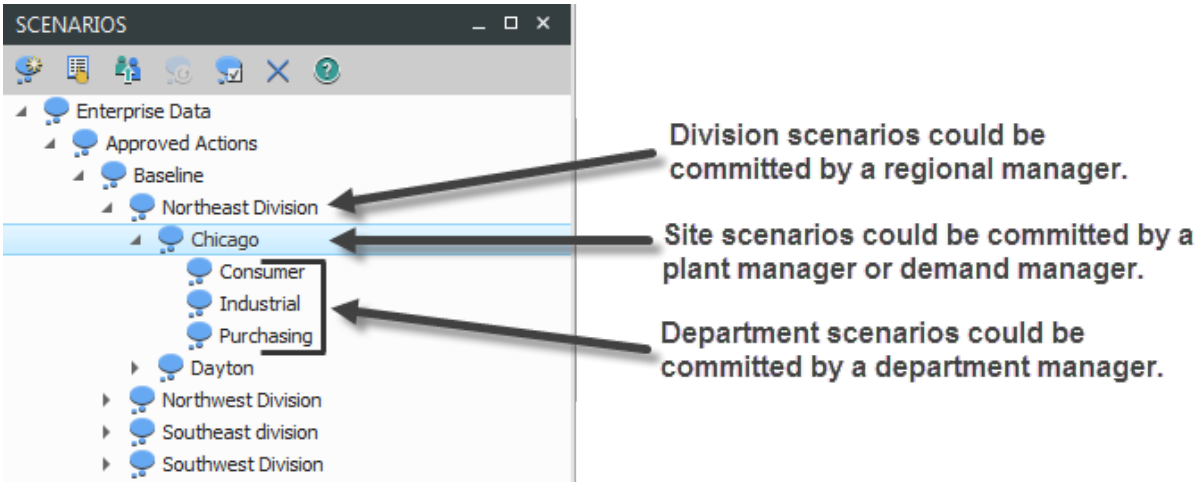
Before creating a scenario hierarchy, you should decide what scenarios you require. If you create a hierarchy of company divisions, you must decide how many levels of scenarios you need. If historical scenarios are required, you must decide which scenarios need history saved, and whether any divisional scenarios require separate historical scenarios. If scenarios with data modifications are required, you must decide which scenarios are modified, which scenarios are provided for users to modify, where separate branches with modified data are required, and whether any divisional or historical scenarios require modifications.

Scenarios with automatic data modifications typically are not intended to be modified, and update a child scenario with the changes resulting from the modification. Therefore, a scenario with data modifications might add another level to the hierarchy. For more information, see "Schedule an automatic data modification" in the *RapidResponse User Guide*.

A scenario hierarchy was created for you during the RapidResponse data integration.

Creating a hierarchy of company divisions

You can create a scenario hierarchy to reflect the structure of your company. For example, you might have a process in which all changes made by the company in a day are collected in a "pending actions" scenario, which is then committed into the Approved Actions scenario at the end of the day. The pending actions scenario receives data commits from each division of the company. Each division collects changes in a scenario that receives data from the sites in that division, and each site collects changes in a scenario that receives information from the departments within that site. At the end of the day, the departments validate and commit their changes to the site scenario, the sites validate and commit their changes to the division scenario, and so on.



In this example, the Consumer, Industrial, and Purchasing departments of the Chicago site would commit their daily changes into the Chicago scenario. The Chicago scenario would then be committed into the Northeast Division scenario, and so on. If a scenario owner accidentally deleted the scenario when committing it, that scenario and all of its child scenarios would have to be re-created the next day.

To avoid accidental deletions, you can create the scenarios in the hierarchy, make them permanent, and then give them to the people responsible for committing the changes. Those scenarios will never get deleted during the commit, and each day users can create new private scenarios or re-use existing private scenarios to perform the day's simulations.

▸To create a scenario hierarchy of divisions

1. Create a scenario based on the **Approved Actions** scenario, and then do the following:
   - Create scenarios for each division in your company, each based on the scenario you created in the previous step.

- Create scenarios for each site in your company, based on the scenario you created for its division in the previous step.
- Create scenarios for each department, based on the scenario you created for its site in the previous step.
- If you require more levels in the hierarchy, create them as described above.

2. Share each scenario you created in step 1 with the user who is responsible for committing the changes, by doing the following:
   - In the **Scenarios** pane, click the scenario you want to share.
   - On the **Scenarios** pane toolbar, click **Share** .
   - Click **Select Names**.
   - In the **Select Names** dialog box, click the person responsible for committing the scenario, and then click **Modify**. Ensure you also share the scenario's parent, otherwise the user will not be able to commit changes,

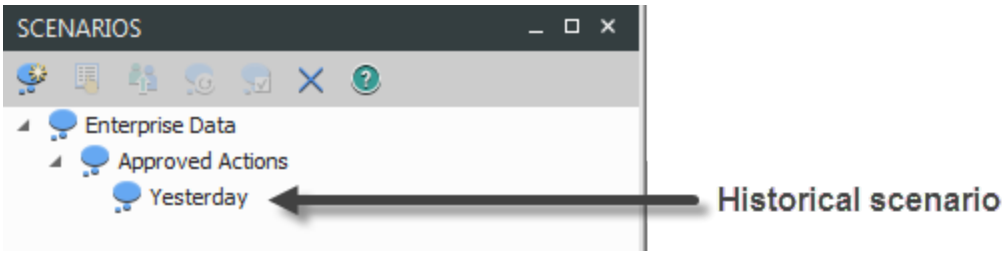
   Optionally, you can share each scenario with every user who requires access to it. Typically this would be only that user's department scenario.

   If you do not want users to see the scenarios before the hierarchy is finished, you can share the scenario with yourself.
3. Make each scenario you created in step 1 permanent, by doing the following:
   - In the **Administration** pane, under **System Monitoring**, click **Resources**.
   - Click the **Scenarios** tab.
   - Select the scenario you want to make permanent, and then click **Change the Permanent Setting** .
4. Give each scenario you created in step 1 to the user responsible for committing the changes, by doing the following:
   - In the **Scenarios** pane, click the scenario you want to give.
   - On the **Scenarios** pane toolbar, click **Give** .
   - In the **Give Scenario** dialog box, in the **New Owner** list, click the person responsible for committing the changes.
   - Optionally, type a message informing the new owner about the purpose of the scenario.
   - Click **OK**.

Tip: If you want to see the hierarchy after you give the scenarios to their owners, you can share the scenarios with yourself.

Creating a hierarchy with historical scenarios

You can create a scenario hierarchy to maintain historical data. The historical scenarios can contain data from any amount of time, and can be set up to reflect the historical state of their parent scenario. For example, if you perform daily data updates, you can create a scenario to show the previous day's Approved Actions scenario to see the data as it was after the previous day's changes were approved.



In this example, the Approved Actions scenario has a historical child scenario. This scenario is set to update every day, and is intended to not be modifiable. Users can view data in this scenario to see the previous day's data, and can use it in scenario comparisons to see how the current data has changed from the previous day's.

Maintaining historical scenarios can be resource-intensive, and if many historical scenarios are created, system performance can be affected.

Creating a historical hierarchy requires a scheduled task to update each historical scenario. For more information, see "Scheduling scenario updates" on page 724.

▸To create a historical scenario hierarchy

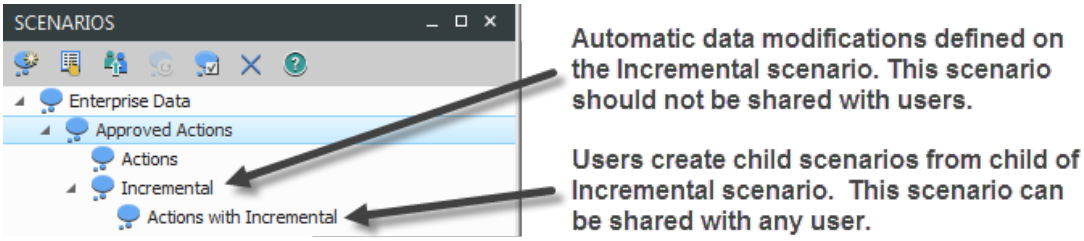
1. Create a scenario based on each scenario you want to save history for.
2. Create a scheduled task to update each scenario you created in step 1. For more information, see "Scheduling scenario updates" on page 724.
3. Share each scenario you created in step 1 with the users who require it, by doing the following:
   - In the **Scenarios** pane, select a scenario.
   - On the **Scenarios** pane toolbar, click **Share**.
   - Click **Select Names**.
   - In the **Select names** dialog box, click each user who requires the historical scenario, and then click **View-Only**.
   - Click **OK**.
4. Make each scenario you created in step 1 permanent, by doing the following:
   - In the **Administration** pane, under **System Monitoring**, click **Resources**.
   - Click the **Scenarios** tab.
   - Select the scenario you want to make permanent, and then click **Change the Permanent Setting**.

Note: You can create historical scenarios that update on intervals longer than one day. Any calendar your company has defined can be specified in the scheduled system tasks's **Schedule** field. For more information, see "Commands and scheduling system tasks" on page 381.

Creating a hierarchy with automatic data modifications

You can create a hierarchy that contains scenarios that use data modified specifically for performing simulations with special conditions. For example, you might have some parts that require incremental availability for specific orders. You do not want incremental availability calculated for all parts and all

orders, so you can create a scenario hierarchy that contains one scenario that applies incremental availability to the parts and orders that need it. The scenario that applies incremental availability automatically modifies the required data, and then updates its child with the modified data. Users can create simulations based on the child with incremental availability for the orders that require it, and create simulations on a scenario without incremental availability for the other orders. For more information, see "Schedule an automatic data modification" in the *RapidResponse User Guide*.



In this example, the Incremental scenario modifies a set of data to apply incremental availability, using an automatic data modification. Users create simulations based on the Actions or Actions with Incremental scenarios, depending on whether they need incremental availability.

The Incremental scenario should be set to update automatically, so that any updated records that require incremental availability are always available to users working in the Actions with Incremental scenario. The Actions with Incremental scenario is updated by the data modification, and should be set to update manually. The Incremental scenario must not be used for simulation, because any data changes or commits made to it will be processed by the automatic data modification, and might produce incorrect results. To ensure users do not modify the data in this scenario, you can share only the Actions with Incremental scenario. Users will not see the Incremental scenario in their Scenarios pane, and will not be able to commit changes to it.

You can also create automatic data modifications that modify data in other scenarios, such as an operation that copies data from one scenario to another. In these cases, your scenario hierarchy can be flatter. For example, you can create an automatic data modification that takes records from the Approved Actions scenario and applies incremental availability directly in the Actions with Incremental scenario. This means you do not have to include the Incremental scenario in the scenario hierarchy. The changes are made only in the Actions with Incremental scenario, and the automatic data modification runs only when the Approved Actions scenario is updated. For more information, see "Create a workbook command" in the *RapidResponse Resource Authoring Guide*.

If users schedule their own data modifications, ensure they have permission to create scenarios. They can then use the scenario they create to modify the data, and then provide access to other users for simulations.

▸To create a hierarchy with automatic data modifications

1. For each special condition you want to include in the hierarchy, create a scenario based on the **Approved Actions** scenario, and another scenario based on the one you created.

   The first scenario you create performs the automatic data modifications. The second is used to create simulations using the modified data.
2. For each scenario that requires it, schedule an automatic data modification to be performed when the scenario is updated. For more information, see the *RapidResponse User Guide*.
3. Share the scenarios used to create simulations with the modified data with the users who require access to them by doing the following:

- In the **Scenarios** pane, select a scenario.
- On the **Scenarios** pane toolbar, click **Share** .
- Click **Select Names**.
- In the **Select Names** dialog box, click each user who requires access to the scenario, and then click **Modify** or **View-Only**.

  The scenario's parent is automatically shared, but will only be visible to yourself and other administrators.

4. Make each scenario with an automatic data modification update automatically by doing the following:
   - In the **Scenarios** pane, select a scenario.
   - On the **Scenarios** pane toolbar, click **Properties** .
   - On the **General tab** of the scenario properties dialog box, beside **Update**, select **Automatic**.
5. Make each scenario you created in step 1 permanent by doing the following:
   - In the **Administration** pane, under **System Monitoring**, click **Resources**.
   - Click the **Scenarios** tab.
   - Select the scenario you want to make permanent, and then click **Change the Permanent Setting** .

Scheduling scenario updates

Data administrators and system administrators can schedule any scenario to be updated with data changes from its parent. For example, assume you have a scenario named Yesterday, which contains all of the previous day's data changes. If you perform full data updates at midnight every day, you can schedule the Yesterday scenario to be updated before the full data update occurs. When the full data update finishes, the Enterprise Data and Approved Actions scenarios contain the newest data from your enterprise data sources, and the Yesterday scenario contains yesterday's data.

Scheduling a scenario update requires a scheduled task. The task has one required argument, `scenario`, which specifies the scenario to update.

These scheduled updates occur regardless of who owns the scenario, whether the scenario is shared or private, or whether the owner of the scenario has access to its parent.

▸To schedule a scenario update

1. In the **Administration** pane, under **System Settings**, click **Scheduled System Tasks**.
2. On the **Edit** menu, click **Insert Record**.
3. In the **Name** box, type a name for the task.
4. In the **Command** box, type **ScenarioUpdate**.
5. In the **Schedule** box, type the day or calendar interval you want the task to run on.
6. In the **Earliest Start Time** and **Latest Start Time** boxes, type the times that the task can run between.
7. In the **Time Zone** list, click the time zone that the task should run in.
8. In the **Enabled** list, click **Y**.
9. Click **Save and Close**.
10. Click the **Task Arguments** worksheet.

11. On the **Edit** menu, click **Insert Record**.
12. In the **Task** box, type the name of the task you created in step 3.
13. In the **Argument** box, type **Scenario**.
14. In the **Value** box, type the name of the scenario you want to update.

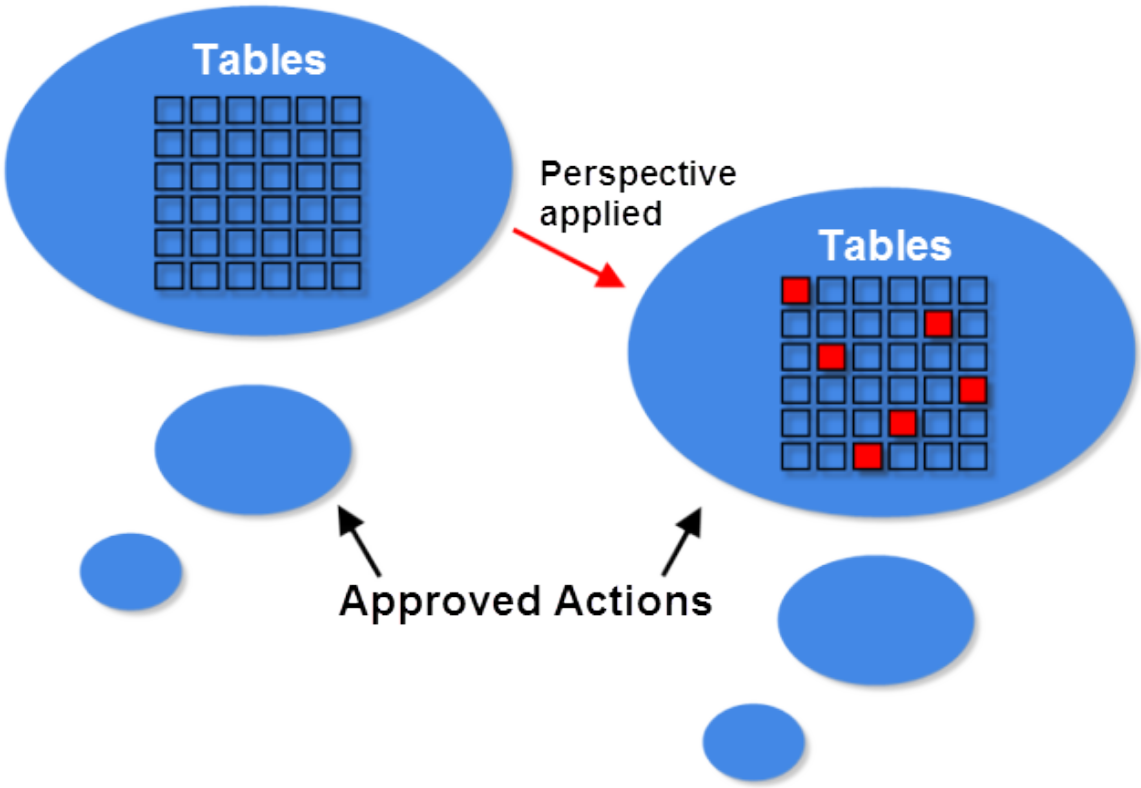
Note: For more information about scheduled system tasks, see "Commands and scheduling system tasks" on page 381.

Scenario perspectives

The configuration of control tables and input tables determine which, and how, calculations are performed against your data and thereby affects the data generated in the tables. Tables are configured during the integration and setup of RapidResponse. They ensure that RapidResponse calculations closely emulate the behavior of your enterprise system.

Perspectives allow you to modify field values of control tables and input tables and then apply this configuration to a scenario. By using perspectives, you can avoid having to change these values manually. You generate a different set, or view, of calculated data by modifying table values.

For example, in the following illustration, a scenario with a perspective applied is the same as its parent except that some field values are different, resulting in different calculated values. The filled-in squares in the child scenario represent field values that differ from the parent scenario, in this case the Approved Actions scenario.



Brand owners that have integrated data from their contract manufacturers are typical users of perspectives. By applying perspectives, brand owners can control how the integrated data is calculated into their overall data set.

Using a perspective, a brand owner user can model their outsourced supply chain in different ways to answer questions such as:

- What is the available date for orders considering only supplier commitments and on-hand inventory?
- What is the available date if supply chain capability is considered?

You can also use perspectives to control currency conversion dates for calculated fields. For example, you can create a perspective that uses a conversion rate from the beginning of the year to view calculations that match the currency conversion rates your budget was calculated using, or a conversion rate for the previous year to compare conversion rates. For information about inserting the required table record, see "Configuring conversions on calculated fields" on page 694.

RapidResponse data or system administrators are responsible for defining perspectives and only RapidResponse users who are authorized to create scenarios can apply perspectives to their scenarios.

Cautions:

- Modifying table values can cause significant changes in the data generated by RapidResponse calculations. Use caution when modifying table configurations. For more information, see the *RapidResponse Analytic and Data Model Guide*.
- Modifying input table values, rather than control table values, can seriously impact the performance of your RapidResponse system. The performance impact of a perspective is proportional to the number of records in the table. For example, the BillOfMaterial table (input) might contain 30 million records while the BOMType table (control) might contain less than 50 records. Exercise caution when modifying input table values in perspective definitions.

Note: Perspectives cannot be applied to data in a table that contains vector series data. For more information about vector data, see the *RapidResponse Analytic and Data Model Guide* and the *RapidResponse Data Integration Guide*.

Perspective impacts on scenario data

When a perspective is applied to a scenario, fields in records returned by the perspective definition expression are replaced with values defined in the perspective definition. In other words, some fields in control table or input table records have their values replaced. The field values are replaced by having the perspective value overlaid on top of the value in the scenario. The original field value that has been overlaid by the perspective value is maintained in the scenario but it is considered hidden.

The field values overlaid by the perspective are used in analytic calculations and query results. For example, records returned in a worksheet display the perspective value and not the hidden value.

The following illustration shows a record with six fields and the values associated with the fields.

Field 1	Field 2	Field 3	Field 4	Field 5	Field 6
abc	def	123	456	abc123	def456

After the perspective is applied to the scenario, two fields (#2 and #4) have their values overlaid by the perspective. The original values are maintained in the database.

Field 1	Field 2	Field 3	Field 4	Field 5	Field 6
abc	xyz ~~def~~	123	999 ~~456~~	abc123	def456

Scenarios that have perspectives applied can be modified. In fact, users can also modify data that has a perspective applied to it. However, after the data has been modified, it is immediately overlaid (or hidden) with the values defined in the perspective definition. The user-modified data will not affect analytic calculations or query results as it is considered hidden.

For example, assume a user modifies a field in a worksheet that has a perspective value applied to it. When the user saves the data changes in the worksheet, the perspective value is overlaid. To the user it will seem as if the data edit was discarded. In reality, the perspective value is overlaid on the user's data edit. However, the data change is visible from the Pending Commits tab in the Scenario Properties pane.

Let's continue the previous example. The user modifies Field 2 and changes the value to **ddd**. The perspective continues to overlay the Field 2 value in this record with **xyz**. However, the **ddd** value is maintained and is hidden in the database.

Field 1	Field 2	Field 3	Field 4	Field 5	Field 6
abc	xyz ~~ddd~~ (modified value) ~~def~~ (original value)	123	999 ~~456~~	abc123	def456

A scenario with a perspective applied against it can be committed to its parent. During the commit operation, the data overlaid by the perspective in the child scenario is ignored and not committed to the parent. However, all pending data commits, including the user-modified data that was overlaid by a perspective, is committed to the parent. In the previous example, the Field 2 value (**ddd**) modified by a user is committed to the parent scenario.

The Perspectives workbook includes the Hidden Data Changes worksheet. This worksheet identifies user-modified data changes that are hidden in any scenario because a perspective value is overlaid.

Perspectives

Scenario Details

Perspectives | Hidden Data Changes

	Scenario	Perspective	Record				Perspective-Hidden Data Changes		
			Table	Namespace	Field	Value	Field	Value in Scenario (Hidden)	Value in Parent Scenario
1	BOMType Perspective	BOMType	BOMType	Mfg	Value	Normal	DateRule	CalcDockDate	CalcStartDate
2					Control Set	BOMSubstn			
3	BOMType Perspective	BOMType	DemandType	Mfg	Value	Actual	AllotmentOrder	2	1
4					Control Set	Default			
5	Supplier Commitments	Supplier Commitments	SupplyStatus	Mfg	Value	Ignore	AvailableDateLimit	Due	CalcStart
6					Control Set	Default			
7	Supplier Commitments	Supplier Commitments	SupplyType	Mfg	Value	Consensus	ProcessingRule	RecommendOnly	NonReschedulable
8					Control Set	Training			

Committing these data values could provide unwanted or unexpected changes to the data in the parent scenario.

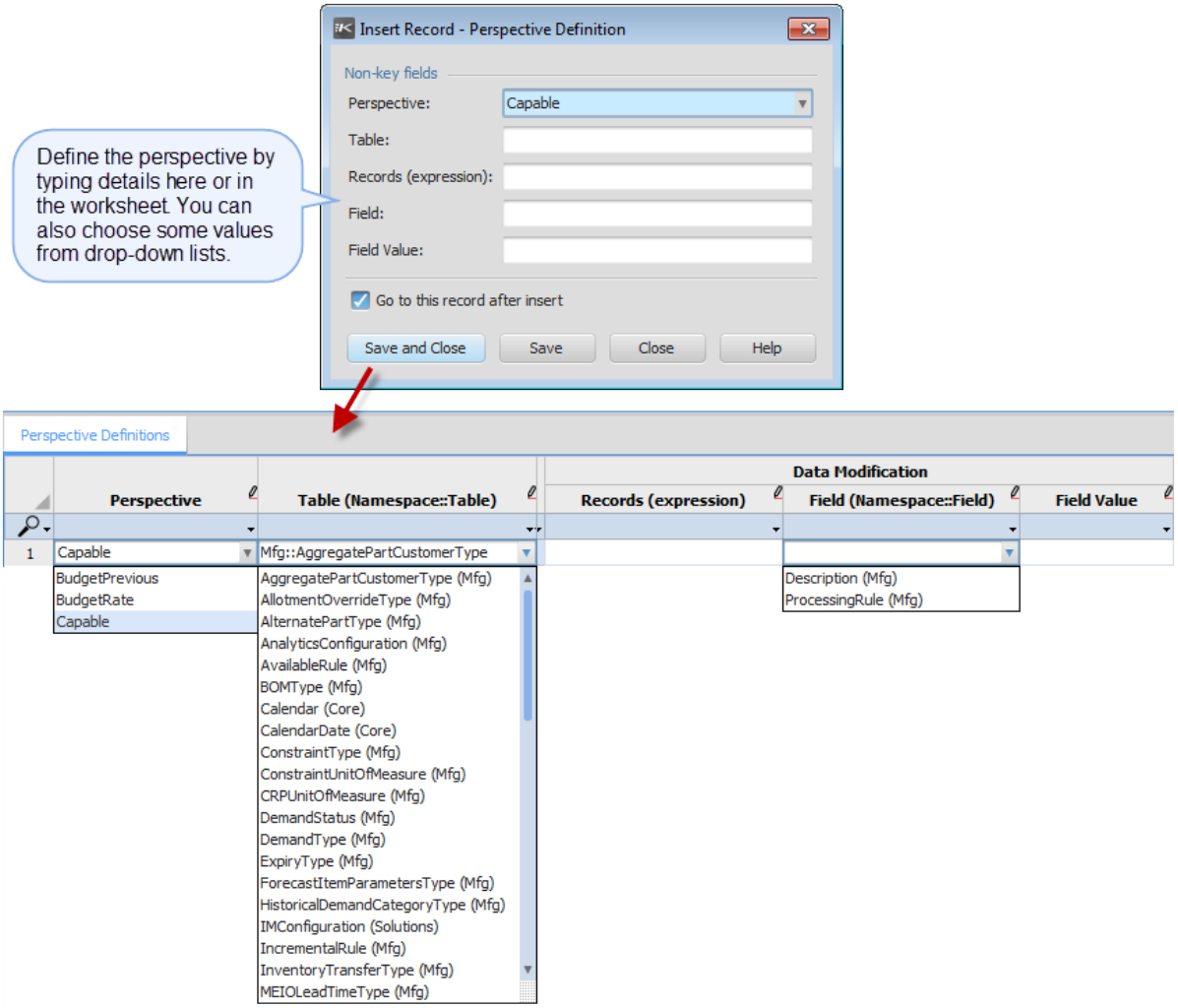
RapidResponse also includes the **Perspective - Hidden Data Changes** alert, which is available to all system administrators. This alert is based on the Hidden Data Changes worksheet and can be used to notify administrators and users about user-modified data that has been overlaid by a perspective. By default, the alert is unscheduled but administrators should consider scheduling it to run on a weekly or monthly basis.

Creating perspectives

Creating a perspective is a two-step process. The first is to name the perspective by inserting a record into the Perspectives worksheet. The second is to define the perspective by specifying the control table or input table field values you want to modify by inserting a record into the Perspective Definitions worksheet.

You can define a perspective in three ways:

- By typing information into the Insert Record dialog box when you insert a record into the Perspective Definitions worksheet.
- By typing information into cells of the Perspective Definitions worksheet once a record has been inserted. You cannot type into the Perspective and Field columns of the worksheet.
- By selecting values from drop-down lists in the Perspective Definitions worksheet. A record must be inserted into the worksheet for the drop-down lists to become available. You can select the perspective, the table, and the field from drop-down lists, as shown in the following image. Only control tables are available in the Table column's drop-down list, but you can type the name of an input table if required. The Field column's drop-down list is available only when a control table has been specified for the record.

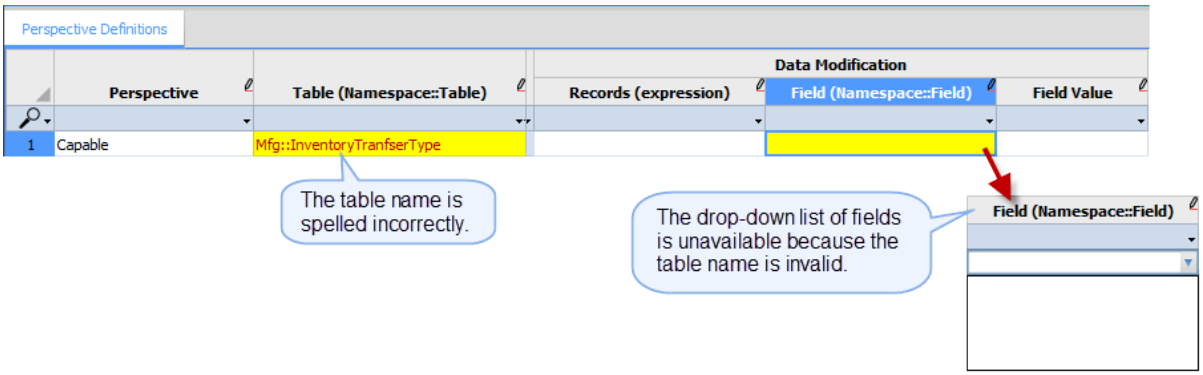


If you specify a table or field by typing into the Insert Record dialog box or the worksheet, it is suggested that you include the namespace with the table or field name, separated by two colons. For example:

- **Namespace::TableName**—specifies the table.
- **Namespace::FieldName**—specifies the field.

If you do not include the namespace with table and field names, the values are still valid. However, including the namespace can reduce errors caused by the record referring to the wrong table or field.

If the name of the perspective, the table, or the field is an invalid value, these errors are identified in the Perspective Definitions worksheet. Cells that include errors are highlighted with a yellow background and any text within the cell becomes red, as shown in the following image. This allows you to easily locate errors so you can correct them as you define the perspective.



If there are errors in the Records (expression) or Field Value columns, they are not identified in the Perspective Definitions worksheet. However, you can validate the perspective to check for errors in all parts of the definition. Validating a perspective can also provide you with more information about why an error has occurred in any column. For more information, see "Validating perspectives" on page 732.

If you specify a reference field in the perspective definition, the values specified in the perspective definition must match a record in the referenced table, otherwise the record is not affected by the perspective. If that reference is nullable, a null value is replaced with a key value composed of the default values for each of the table's key fields. If the reference is to a table that has a contextual default value, such as the Site or ControlSet tables, the contextual default is used.

Notes:

- Using a one-colon format when specifying table and field names (**Namespace:Table** or **Namespace:Field**) results in valid perspective definitions. However, values in this format are identified as invalid in the Perspective Definitions worksheet to encourage you to use two colons.
- Variables are not valid in the perspective definition expressions.

Perspective definition errors

The following table lists possible causes of the errors that can occur in the Perspective, Table, and Field columns. This list is not exhaustive, but provides you with an idea of how you can edit the perspective to correct an error.

Column with error	Possible causes of the error
Perspective	• The name of the perspective is invalid
Table	• The cell is blank • The table is a vector, system, or versioned table • No table of that name exists • Multiple tables with the same name exist • No table of that name exists in the specified namespace (if the namespace is included with the table name)

Column with error	Possible causes of the error
Field	• The cell is blank • The field is a read only, key, or system field in the table • The field is not an input field in the table • No field of that name exists in the table • Multiple fields with the same name exist in the table • The table does not contain a field with that name in the specified namespace (if the namespace is included with the field name) **Note:** If the field name uses red text with no yellow background, this means that the table name is invalid. The red text returns to black text if a valid table is specified for the record.

▸To name a perspective

1. In the **Administration** pane, under **Data**, click **Perspectives**.
2. Click the **Perspectives** worksheet.
3. On the **Edit** menu, click **Insert Record**.
4. In the **Insert Record** box, type information in the following boxes:
   - **Name**—the name of the perspective. This is the name RapidResponse users see when applying a perspective to a scenario.
   - **Description**—the purpose of the perspective.
5. Do one of the following:
   - Click **Save and Close** to add the perspective and return to the worksheet.
   - Click **Save** to add the perspective and then add another perspective.

▸To define a perspective

1. In the **Administration** pane, under **Data**, click **Perspectives**.
2. Click the **Perspective Definitions** worksheet.
3. On the **Edit** menu, click **Insert Record**.
4. Select the name of the perspective you are defining.
5. Optionally, define the perspective by typing information in the following boxes:
   - **Table**—the name of the control table or input table containing the record that the perspective modifies.
   - **Records (expression)**—the records to modify. The records are specified using a filter. The filter uses the RapidResponse query language, cannot be enclosed in parentheses, and cannot contain variables. For example, `Value = 'Buy'`. For more information, see "Example of a perspective definition " on page 732.
   - **Field**—the field in the control table or input table that the perspective definition modifies.
   - **Field Value**—the field value to use in the perspective.
6. Optionally, click **Save** to add the perspective definition record and specify another.

   Typically, several field values are modified by a perspective. Each field needs to be defined as a separate record or line.

7. Click **Save and Close** to add the perspective definition record and return to the worksheet.
8. Optionally, define the perspective by typing in the worksheet cells or selecting values from drop-down lists.

   If you specified the records to modify by typing in the worksheet, click outside the text field or **OK** to close the text field and leave your changes in the cell. Click **Cancel** to close the text field and cancel your changes.
9. Click **Save**.

Notes:

- When a scenario perspective definition is modified, it immediately affects any scenarios that have the perspective applied to it.
- Upon a restart of the RapidResponse system, system administrators are alerted in Message Center about any perspectives that have errors.

Example of a perspective definition

Perspective Definitions

	Perspective	Table (Namespace::Table)	Data Modification		
			Records (expression)	Field (Namespace::Field)	Field Value
1	Capable	Mfg::BOMType	Value='Normal'	Mfg::BlowThrough	N
2			Value='Phantom'	Mfg::BlowThrough	Y

In this example, the Capable perspective defines two control table settings. The settings modify the BlowThrough field value in the BOMType control table.

The first setting, `Value='Normal'`, specifies that if the BillOfMaterial.Type value is set to Normal, then set BlowThrough to No.

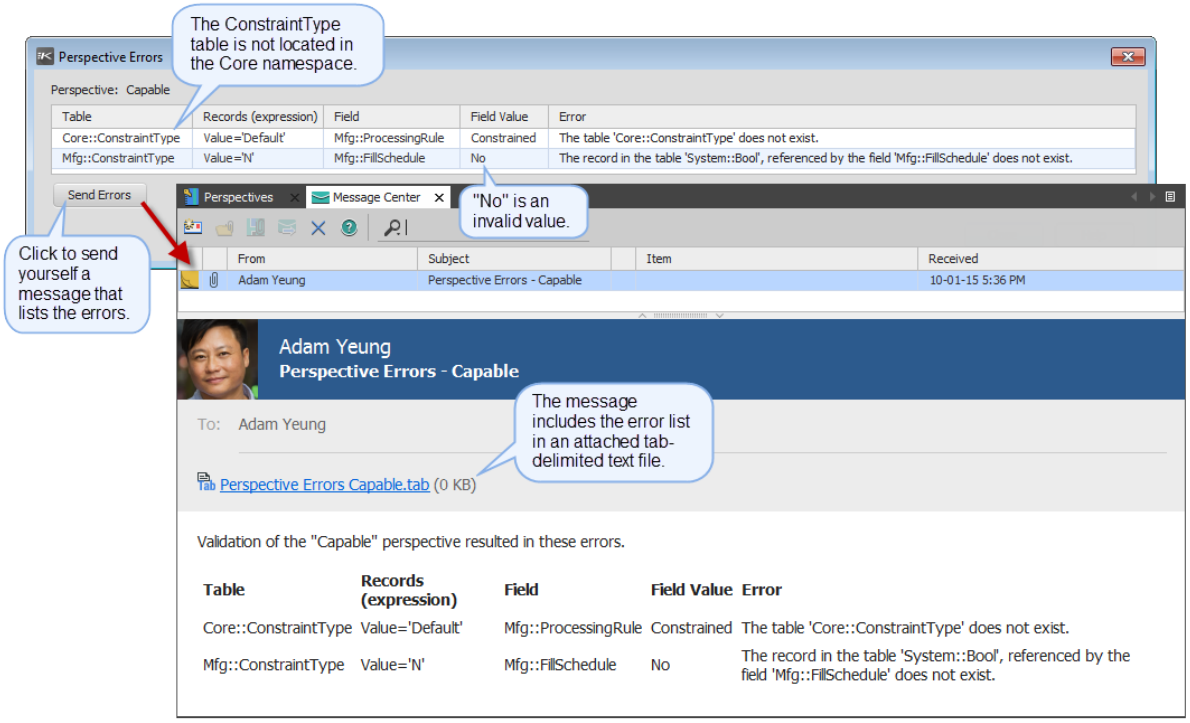
The second, `Value='Phantom'`, specifies that if the BillOfMaterial.Type value is set to Phantom, then set BlowThrough to Yes.

Validating perspectives

Once you have named and defined a perspective, you can validate it to verify that it does not contain any errors. You validate a perspective by selecting either the perspective in the Perspectives worksheet or one of the perspective's definition records in the Perspective Definitions worksheet and then clicking the Validate Perspective Definition button on the workbook toolbar.

If the perspective definition contains invalid values, the Perspective Errors dialog box opens and provides you with a list of the values in error and why the error occurred. Only one error is displayed for each definition record. For example, if both the Table and Records columns contain invalid values in one record, the Perspective Errors dialog box reports only one error for that record (that the table does not exist). If you make corrections to the definition, you should save then validate the perspective again to check if there are other errors in the definition.

By clicking Send Errors, you can send yourself the list of errors in a Message Center message, which can be used as a reference while you correct the definition. The message also includes the error list in an attached tab-delimited text file, which can be opened in Microsoft Excel and printed.



▸To validate a perspective

1. In the **Administration** pane, under **Data**, click **Perspectives**.
2. Select the perspective you want to validate (in the **Perspectives** worksheet) or one of the perspective's definition records (in the **Perspective Definitions** worksheet) and click **Validate Perspective Definition** .
3. If the perspective does not contain any errors, click **OK**.
4. If the perspective contains one or more errors, in the **Perspective Errors** dialog box do the following:
   - Optionally, click **Send Errors** to send yourself a message containing a list of the perspective's errors and then click **OK**.
   - Optionally, take a screen shot of the **Perspective Errors** dialog box.
   - Click **Close**.

Filtering perspectives

Once you have created several perspectives, it can be useful to filter the Perspective Definitions worksheet so that you view only the records that apply to one perspective. You can do this by clicking the number beside the perspective's name in the Definitions column of the Perspectives worksheet, as shown in the following image. The number represents the number of field values that are modified by the perspective.

Perspectives

Perspectives | Hidden Data Changes

	Perspective	Definitions	Description
1	BudgetPrevious	1	CurrencyAsOfDate - beginning of previous year.
2	BudgetRate	1	CurrencyAsOfDate - beginning of current year.
3	Capable	8	Available date - taking supply chain capability into account.
4	Supplier	5	Available date - taking only supplier commitments into account.

Five fields are modified by the Supplier perspective. Click to filter the Perspective Definitions worksheet to show only these five records.

To view all definition records for all perspectives, you must close then reopen the Perspectives workbook.

Perspective definitions for currency conversion

Perspective Definitions

	Perspective	Table (Namespace::Table)	Data Modification		
			Records (expression)	Field (Namespace::Field)	Field Value
1	BudgetPrevious	Core::ScenarioSetting		Core::CurrencyAsOfDate	20140101
2	BudgetRate	Core::ScenarioSetting		Core::CurrencyAsOfDate	20150101

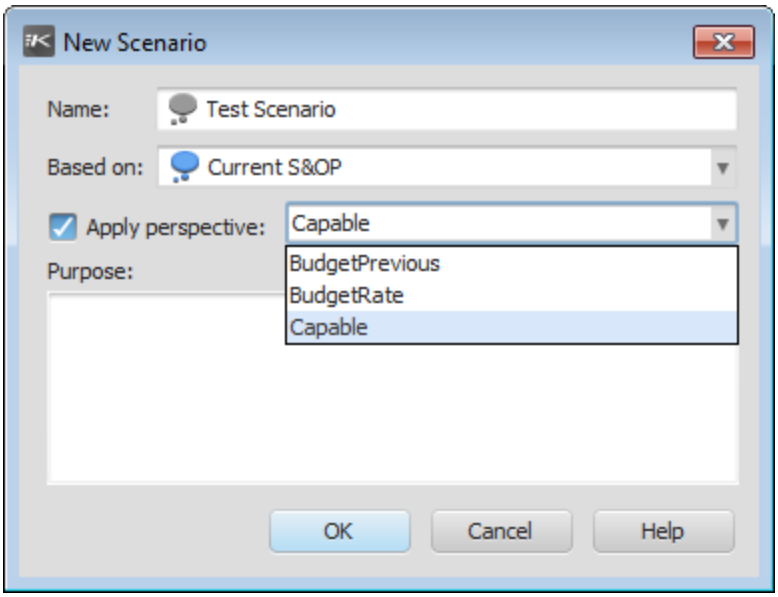
In this example, one control table setting is defined for each perspective. The CurrencyAsOfDate field for each perspective is set to the beginning of the current year for the BudgetRate perspective and to the beginning of the previous year for the BudgetPrevious perspective.

The Core::ScenarioSetting table contains only one record, so an expression is not required.

In scenarios that use these perspectives, calculated fields are converted using the conversion rates as specified on the CurrencyAsOfDate. For more information, see "Currency conversions" on page 687.

Applying perspectives

Only RapidResponse users who are authorized to create scenarios can apply perspectives to their scenarios. To determine whether users can create a scenario with a perspective applied to it, open the New Scenario dialog box. If perspectives have been defined, the New Scenario dialog box includes the Apply perspective check box and list.



Using the New Scenario dialog box, you can only apply a perspective to a scenario when the scenario is created. Administrators can change the perspective applied to a scenario. For more information, see "Changing the perspective applied to a scenario" on page 736.

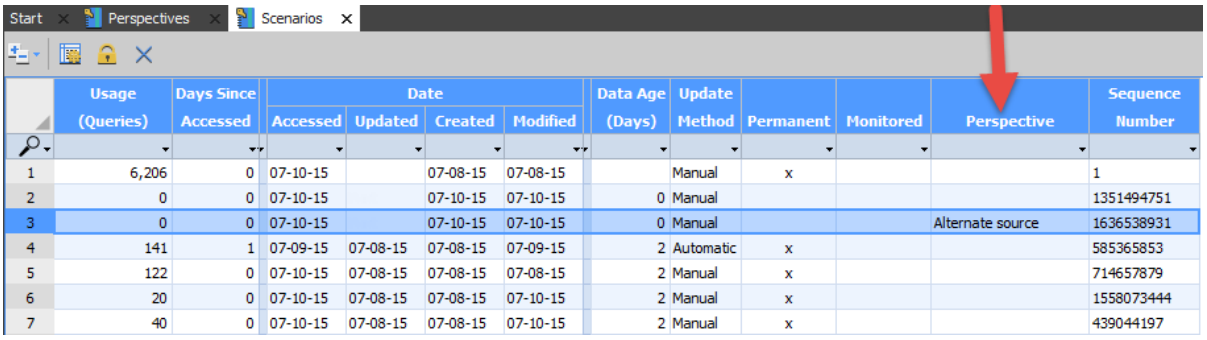
When you create a child scenario of a scenario that has a perspective applied to it, you have three options:

- Apply the same perspective as the parent scenario.
- Apply a different perspective than the parent scenario.
- Do not apply a perspective.

Only one perspective can be applied to a scenario.

Determining where perspectives are used

As an administrator, you might be interested in understanding which scenarios have a perspective applied and which perspectives are being used. The Scenarios workbook includes a Perspective column. If a scenario in your RapidResponse system uses a perspective, the perspective name will be noted in the column.



	Usage (Queries)	Days Since Accessed	Date				Data Age (Days)	Update Method	Permanent	Monitored	Perspective	Sequence Number
			Accessed	Updated	Created	Modified						
1	6,206	0	07-10-15		07-08-15	07-08-15		Manual	x			1
2	0	0	07-10-15		07-10-15	07-10-15	0	Manual				1351494751
3	0	0	07-10-15		07-10-15	07-10-15	0	Manual			Alternate source	1636538931
4	141	1	07-09-15	07-08-15	07-08-15	07-09-15	2	Automatic	x			585365853
5	122	0	07-10-15	07-08-15	07-08-15	07-08-15	2	Manual	x			714657879
6	20	0	07-10-15	07-08-15	07-08-15	07-10-15	2	Manual	x			1558073444
7	40	0	07-10-15	07-08-15	07-08-15	07-10-15	2	Manual	x			439044197

To only show scenarios with a perspective applied, in the Search row use the **!''** search criteria in the Perspective column. For more information about this worksheet, see "Reviewing scenario usage" on page 709.

Changing the perspective applied to a scenario

If you are using On-Premises RapidResponse, you can change which perspective is applied to a scenario. If you are using the On-Demand RapidResponse service, Kinaxis Customer Support can perform this procedure for you.

For most scenarios, you can delete and re-create the scenario with the new perspective. However, you cannot delete permanent scenarios, so if you need to change the perspective, you must use the RapidResponse Console to execute a query that modifies the scenario. You can also perform this process for scenarios that you do not want to delete, such as ones that contain many modifications that you do not want to commit to the scenario's parent.

In the RapidResponse Console, you can execute queries on the Query tab. You must be a system administrator to perform this process. For more information, see "RapidResponse Console" on page 235.

After applying the new perspective, you should restart RapidResponse Server to ensure all calculated results use the new perspective.

Caution: Running queries that modify data can potentially corrupt your RapidResponse database. Only do so with the assistance of Kinaxis Customer Support.

You can change the perspective applied to a scenario using the following syntax.

```
ScenarioApplyPerspective(Name, Perspective, PermitOnPublicPlan)
```

where

- `Name` is the name of the scenario you are applying the new perspective to.
- `Perspective` is the new perspective to apply.
- `PermitOnPublicPlan` is an optional argument that specifies whether the perspective can be applied to a public or shared scenario. If the scenario you have specified is shared, this value should be set to "true". If you do not specify this parameter, "false" is used, and the perspective can be applied to only private scenarios.

For example, to apply the EnableDRPForecast perspective to the shared Regions scenario, specify the following.

```
ScenarioApplyPerspective("Regions", "EnableDRPForecast", "true")
```

To apply the BudgetPrevious perspective to the private Cost Analysis scenario, specify the following.

```
ScenarioApplyPerspective("Cost Analysis", "BudgetPrevious")
```

▸To specify a perspective for a scenario

1. Sign in to the RapidResponse Console. For more information, see "RapidResponse Console" on page 235.
2. Click the **Query** tab.

3. In the **Query** box, specify the **ScenarioApplyPerspective** expression that defines the scenario to modify and the perspective to apply.
4. Click **Submit**.
5. On the **Results** tab, ensure the **ReturnCode** column contains '**Ok**'.
6. Restart RapidResponse Server.

CHAPTER 47: Managing RapidResponse resources

Administrator access to resources 739
Managing version control 741
Allowing web service and server calls from workbooks 744
Reviewing the Check In Log 745
Monitoring resource usage 746
Managing process instances 750
Monitoring and canceling scripts 750
Retrieving predefined workbooks 751
Migrating RapidResponse resources 752
Caching worksheet results 763
Forms included in RapidResponse 765
Running automation tasks 767
Unlocking automation resources 769
Responding to a scenario 771
Managing global resource tags 772

Users within your organization likely have created resources, such as reports and filters, to meet your company's specific business needs. You can modify these resources if they have been added to the versioned repository, modify any predefined resources, and retrieve new copies of any predefined workbooks. You can also monitor how often resources are accessed and delete any that are infrequently used.

This guide describes how to oversee and manage resources in a system with version control turned on. Where applicable, this guide will also provide information for a system with version control turned off.

Administrator access to resources

The predefined RapidResponse administrator groups (system, data, and user) are, by default, granted resource authoring permissions. Administrators can create, modify, and share public resources including dashboards, workbooks, scorecards, alerts, scheduled tasks, and so on.

Version control and resource states

Depending on whether version control is turned on in a system, resources might exist in different states.

States when version control is turned off

In a system with version control turned off, resources can be private or shared. Private resources are only visible in the Explorer to the resource's owner. Shared resources are visible in the Explorer for the owner, administrators, and users with whom the resource has been shared. Any resources visible in the Explorer can be opened.

States when version control is turned on

In a system with version control turned on, resources can be private or public. Public resources are visible in the Explorer to the resource's owner and to administrators. Private resources are made public when they are added to the versioned repository.

For other users to have access to the resource, the public resource must be shared with those users. For more information about version control, see "Managing version control" on page 741.

Accessing resources as an administrator

In the Explorer, administrators see their own private resources and public resources that have been shared with them. In addition, administrators see a listing of all public (or shared) resources that have not been shared with them.

Viewing and modifying public resources

From the Explorer, administrators can view and modify the properties of any public resource in the system. They can also open, modify, give, or share any public resource or delete it. Resource check outs can also be discarded by administrators, if for example, an emergency fix of a resource is required. For more information, see "Discarding a resource check out" on page 743.

An administrator's view of a report might not be the same as another user's view of the report. For example:

- You might belong to different groups or have different profile variables set on your account. This can affect the data that is displayed in a report or the actions you can take, including preventing you from taking actions that users belonging to other groups can take.
- You might have access to data settings, such as filters and sites, that another user does not have access to.
- You can create new responsibility assignments in a responsibility definition where non-administrators can only edit existing responsibility assignments.

Therefore, it is recommended that, when testing or troubleshooting a resource, you sign in with an account that has similar charactersistics to the users who are normally expected to use that resource.

Deleting private resources

As an administrator, you might also need to delete private resources. For example, you might need to delete private alerts owned by users who are no longer with your company. This can be accomplished from the Resources workbook. For more information about deleting private resources, see "Monitoring resource usage" on page 746. You can also delete automation tasks from the Automation Tasks worksheet in the Automation Log workbook. For more information about this worksheet, see "Automation Tasks" on page 459.

For information about modifying alerts and scheduled tasks, see the *RapidResponse User Guide*. For more information about modifying other resources, see the *RapidResponse Resource Authoring Guide*. For information about Scenario management, see "Scenario management" on page 703.

Accessing system forms and workbooks

Some forms and workbooks are system resources, which means that they are used for administrative functions in RapidResponse, such as maintaining user account information and tracking resources. In the Explorer, system resources are marked with a small key at the top left corner of the resource icon.

- System workbooks:
- System forms:

Administrators with access to system resources can open them, however some functions are not possible with system resources:

- Resource management activities, including copying, deleting, sharing, and giving cannot be performed on system resources.
- System resources cannot be edited.
- You cannot view the properties of a system resource.
- The Compare function does not allow system workbooks to be compared with other resources.
- Resource Usage information is not available for system resources.
- System resources are not listed in the Resources workbook or the Resource Permissions workbook.

For more information about system workbooks, see "RapidResponse system workbooks reference" on page 481.

Managing version control

Version control is a resource management system that tracks changes to resources, such as reports, and regulates how those resources are developed in multi-authoring environments. Only one author at a time can modify a resource, thereby preventing conflicts. By checking it out from a centralized, versioned repository, you can prevent other authors from making changes to the resource while you are working with it. Each copy of a resource that is saved back into the versioned repository is assigned a version number. Changes are tracked, saved, and time-stamped, with details about the changes recorded in the form of comments. Authors can use version control to manage how private resources and public resources they own are modified. Authors with administrator permissions can create and modify all resource types in your system. For more information, see the *RapidResponse Resource Authoring Guide*.

As a system administrator, you can review version control details for resources, turn version control system on or off in your system, specify how check in comments are treated, and specify if comments can be edited. In addition, you can view a specific resource's version history and discard other users' resource check outs. Author can check in one or more resources at a time in to the versioned repository. From the Check In Log pane, you can view details for all check ins into your company's RapidResponse system.

Turning version control on or off

Version control for resources, or resource versioning, is turned on or off from the Global Settings dialog box by system administrators.

- For new installations of RapidResponse, resource versioning is turned on by default.
- If you have upgraded from RapidResponse 2013.4 (or earlier), resource versioning is turned off by default.

When version control is turned on, all resources in that system have a 1.0 version number applied to them.

In a RapidResponse system with version control turned on for resources, if you select to turn resource versioning off, all version histories will be permanently deleted. It is recommended that you create a backup of the RapidResponse database before you turn version control off.

On-Demand: To request your RapidResponse database be backed up, contact Kinaxis Customer Support.

On-Premises: For more information, see "Backing up and restoring the RapidResponse database" on page 315.

▸To turn version control on or off

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Resources** category.
3. For **Resource versioning**, select **Yes** or **No** from the drop-down menu.

Specifying how check in comments are enforced

You can make comments mandatory, suggested, or optional. You must have Resource Versioning turned on to modify how comments are enforced.

▸To specify how check in comments are enforced

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Resources** category.
3. Do one of the following for **Enforce check in comment**:
   - Select **Yes** to make comments mandatory.

     Users will not be able to add or check in resources in to the versioned repository without a check in comment.
   - Select **Warn** to suggest comments be made.

     Users will receive a warning when they add or check in resources without a check in comment. They can proceed without typing a comment.
   - Select **No** to make comments optional.

     Users can add or check in resources without adding a check in comment.

Specifying if check in comments are editable

Users can modify comments on private resources. However, you can specify the editing permission for public resources. When check in comments are set to be editable, authors can modify their own comments on public resources they own and administrators can modify any resource's comments.

▸To specify if check in comments are editable

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Resources** category.
3. For **Allow comments to be modified**, select **Yes** or **No** from the drop-down menu.

Viewing a resource's version history

You can view the version history for a selected resource. In the Version History dialog box, view the list of modifications made to the resource over time, save a resource version as a private resource under another name, or restore to an earlier resource version. For more information on the actions available in the Version History dialog box, see the *RapidResponse Resource Authoring Guide*.

▸To view a resource's version history

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click the resource tab for the resource you want to view.
3. Select the resource.
4. Click **Version History** on the workbook toolbar.

Discarding a resource check out

You can discard a resource's check out to make the resource available for others to modify. For example, a workbook currently checked out to one user might require an emergency fix by another user.

If you discard a user's check out from the Explorer, that user still retains the private copy of the resource. A message informs the user that the resource check out has been discarded.

When you discard a user's check out from the Resources workbook, you can delete any private resources, including private copied of checked out resources. Optionally, you can also send a message to the user whose check out was discarded.

▸To discard a resource check out

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click the **resource tab for the resource you want to discard.**
3. Select the checked out public resource.

4. Click **Discard Check Out** on the workbook toolbar.
5. Click **Yes**.

Note: You must select the checked out public copy of the resource to discard the check out. Discarding a check out is not available if you select the private copy of the checked out resource.

Allowing web service and server calls from workbooks

Workbooks can include web service and server calls in the custom XML on the Options tab in their Advanced configuration. These calls are only allowed if they use URLs that are on the lists of accepted URLs in your RapidResponse system's Global Settings.

- If a URL that is not included in the applicable list is used, the workbook cannot be opened and an error message is displayed.
- If a workbook author includes a web service or server call using a URL that is not on the list, a warning is displayed when opening or saving the workbook configuration.

By default, the list of accepted URLs for web services includes all of the ones that are required by RapidResponse predefined resources. If additional URLs are required to support your company's workbooks, you can add them.

▸Change the lists of accepted URLs

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. In the **Resources** category, edit the list of URLs for one of the following settings:
   - **Accepted URLs for CallWebservice client configuration**
   - **Accepted URLs for CallServer client configuration**

   URLs must be separated by commas.

   Tip: You might find it easier to paste the list of URLs if there are many.
3. Click **OK**.

Caution: Removing URLs that are included by default might interfere with the functioning of predefined resources.

Note: Changing either of these lists of accepted URLs results in an entry being added to the Security Audit worksheet in the Administration Log workbook.

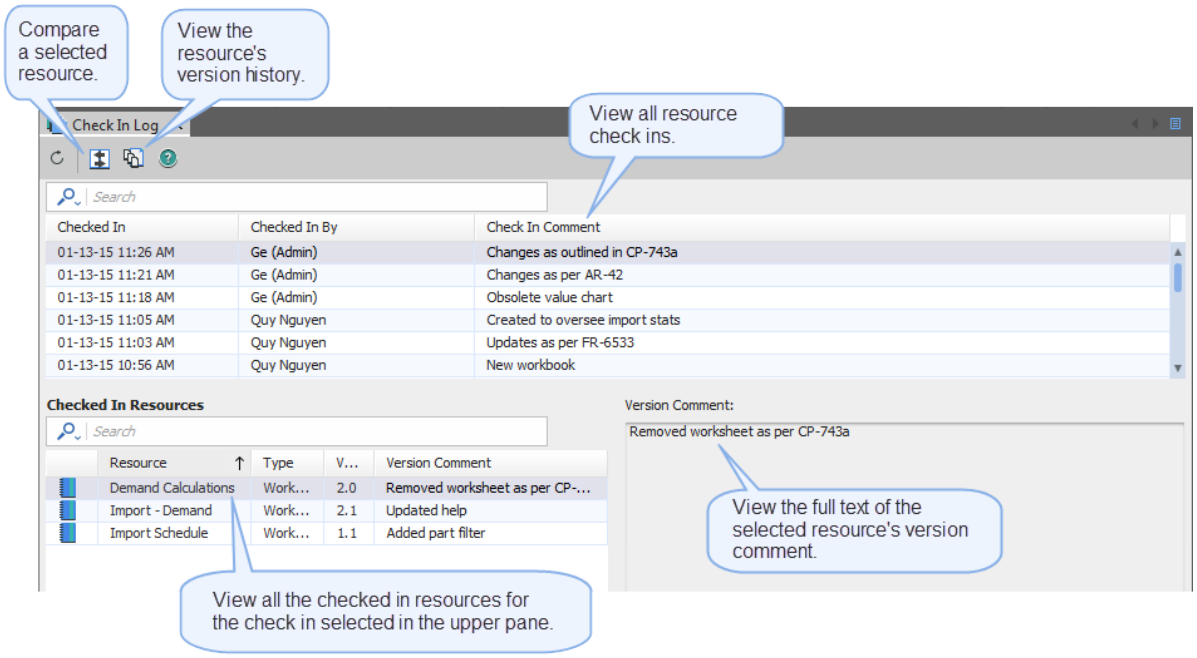
Upgrade behavior

Occasionally, when you upgrade RapidResponse, new URLs might be added to the default settings to support predefined resources.

- If you have not changed these system settings from the defaults, the new URLs are added automatically.
- If you have changed these settings from their defaults, the new URLs are not added to your lists of accepted URLs automatically. Users will see error messages if they attempt to open workbooks that require URLs that are not included in your current settings. You can resolve any such errors by restoring the default settings and then adding any custom URLs again.

Reviewing the Check In Log

You can use the Check In Log to review and understand all the resource check ins in your system. For each check in, you can view when it was checked in, who checked it in, all of the resources included in the check in, and all comments for the resources. For individual resources included in a check in, you can compare a resource to an earlier version of that resource or view the version history for the resource. You can search through the list of check ins or checked in resources. At any time, you can refresh the data displayed in the Check In Log to ensure you are viewing the most current check ins.



▸To view details for a check in

1. In the **Administration** pane, under **System Monitoring**, click **Resource Check In Log**.
2. In the top pane, select a check in record.

   The resources included in the check in, along with type, version number, and comment display in **Checked In Resources** area.

▸To compare a resource to an earlier version

1. In the **Administration** pane, under **System Monitoring**, click **Resource Check In Log**.
2. In the top pane, select a check in record.

3. In the **Checked In Resources** pane, select the resource to compare.
4. On the toolbar, click **Compare** .

▸To view a checked in resource's version history

1. In the **Administration** pane, under **System Monitoring**, click **Resource Check In Log**.
2. In the top pane, select a check in record.
3. In the **Checked In Resources** pane, select the resource to compare.
4. On the toolbar, click **Version History** .

▸To refresh data displayed in the Check In Log

- On the toolbar, click **Refresh Check Ins** .

Monitoring resource usage

RapidResponse provides administrators with the Resources workbook to manage and understand how users are using resources. The Resources workbook can be used for a variety of purposes, including:

- Viewing a resource's state: public, private, and whether it is shared.
- Reviewing which resources are checked out, were last used, or have been recently modified.
- Monitoring how many times resources have been used since a specific date and time.
- Deleting unneeded resources or resources no longer in use. Deleting resources can reduce system memory requirements and improve system performance.

You can monitor all RapidResponse resources from the Resources workbook. Each type of resource has a dedicated worksheet that includes key information tracked by RapidResponse and tools to manage resources. The following resources are tracked in the Resources workbook:

- **Alerts**—For more information, see "Turning automation tasks on and off" on page 748.
- **Automation Chains**
- **Dashboards**
- **Filters**—The usage of site filters is not tracked. As such, site filters are not displayed in this worksheet.
- **Forms**—System forms are not displayed in this worksheet. For more information, see "Accessing system forms and workbooks" on page 741.
- **Hierarchies**
- **Processes**
- **Responsibilities**
- **Scheduled Tasks**
- **Scorecards**
- **Scripts**
- **Task flows**
- **Widgets**
- **Workbooks**—System workbooks are not displayed in this worksheet. For more information, see "Accessing system forms and workbooks" on page 741.

The following image shows the Workbooks tab in the Resources workbook, with version control turned on.

Alerts | Automation Chains | Dashboards | Filters | Forms | Hierarchies | Processes | Responsibilities | Scheduled Tasks | Scorecards | Scripts | Task Flows | Widgets | Workbooks

	Workbook	Owner		Type	Public/		Usage	Days Since	Date			Modified By	Version	Checked Out	
		User ID	Name		Private	Shared?		Accessed	Accessed	Created	Modified			Date	By
102	Periods of Supply Details	Admin	Master Administrator	Standard	Public	No	0	0	10-22-14	10-22-14	10-22-14	Master Administrator	(Revision		
103	Periods of Supply Treemaps	Admin	Master Administrator	Standard	Public	No	0	0	10-22-14	10-22-14	10-22-14	Master Administrator	(Revision		
104	Planning - Constraints	js	Joseph Stashin	Standard	Public	No	0	0	10-22-14	10-22-14	10-22-14	Joseph Stashin	0.1	10-22-14	Joseph Stashin
105	Planning - Constraints	js	Joseph Stashin	Standard	Private		0	0	10-22-14	10-22-14	10-22-14	Joseph Stashin			
106	Planning Sheet	Admin	Master Administrator	Standard	Public	Yes	0	0	10-22-14	10-22-14	10-22-14	Master Administrator	0.2		

▸To review resource usage

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click a tab to review usage information and review any of the following columns:
   - **Owner-UserID**—The User ID of the resource's owner.
   - **Owner-Name**—The name of the resource's owner.
   - **Public/Private**—Specifies whether the resource is private or added to the versioned repository.
   - **Shared?**—Specifies if the resource is shared with users. Only public resources can be shared.
   - **Usage**—The number of times the resource has been used since the last time the usage counter was reset.
   - **Days Since Accessed**—The number of days since the resource was last used.
   - **Date-Accessed**—The date the resource was last used.
   - **Date-Modified**—The date the resource was last modified.
   - **Date-Created**—The date the resource was created.
   - **Days Since Run** (Alerts and Scheduled Tasks only)—The number of days since the alert or scheduled task last ran.
   - **Last completed** (Alerts and Scheduled Tasks only)—The time and date the alert or scheduled task last ran.
   - **Modified By**—The name of the author or administrator who created or last modified the resource.
   - **Version**—The version number of the resource.
   - **Checked Out-Date**—The date the resource was checked out of the versioned repository. This applies only to resources checked out at the time you are viewing the Resources workbook.
   - **Checked Out-By**—The name of the author or administrator who checked the resource out of the versioned repository.

Tip: To better understand how often resources are used, you should review the date on which the usage count began. This can be done by clicking the **Settings** button .

Note: The usage statistics in the Resources workbook also includes indirect usage. For example, when a workbook is used by an alert or dashboard it counts towards usage and access.

▸To reset the resources and scenarios counter

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click **Usage Counts** on the workbook toolbar.
3. Click **Reset**.

   This resets the value in the **Usage** column to zero for all the resources, and changes the date in the **Usage Counts** dialog box to today's date. Usage counts in the **Scenarios** workbook are also reset. For information about the **Scenarios** workbook, see "Administrator tools for scenario management" on page 708.

Note: The date and time is displayed according to the time zone on your computer.

▸To delete resources

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click any worksheet tab.
3. Select the resource you want to delete. Ensure to select the entire row by clicking the row number.
4. Click **Delete** ✕.
5. Click **Yes**.

Note: You cannot delete users' private copies of checked out resources when you discard the check out for a resource. For more information, see "Discarding a resource check out" on page 743.

Tip: If you want to delete multiple items, you can sort the **Usage** column and then select infrequently used items.

Turning automation tasks on and off

Occasionally, you might need to turn off automation tasks (alerts, scheduled tasks, and automation chains) so that they do not run as scheduled. For example, when upgrading to the latest version of RapidResponse you might need to turn off all automation tasks to ensure modifications or reports are not generated on data that is still being modified to support new database tables or analytics. You can turn automation tasks on and off in the Resources workbook.

▸To turn an automation task on and off

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click a tab corresponding to the type of resource that you want to turn on or off (**Alerts**, **Scheduled tasks**, or **Automation Chains**).
3. Select the row for the automation task or tasks that you want to turn on or off, and then click one of the following:

- **Turn On** .
- **Turn Off** .

> **Tip:** You can also turn automation tasks on or off using the Automation Tasks worksheet in the Automation Log workbook. For more information about using the Automation Log workbook, see "Automation logging" on page 448.

Changing automation task priority

Automation tasks (alerts, scheduled tasks, and automation chains) each run with a specific priority, which determines the order that automation tasks are queued in. Higher priority automation tasks are always queued to run before lower priority ones, which ensures important system tasks and business-critical reports are placed in the queue before any other automation tasks in the queue. The automation tasks that run as part of an automation chain are all queued with the priority of the automation chain, regardless of the priority set for each automation task within the chain.

In some cases, a new business process might take precedence over others, and require the priority of older automation tasks to be reduced, which ensures the new process is queued first. You can change the priority of automation tasks in the Resources workbook. You should assign the highest priority to the most important automation tasks, which ensures they run before any others.

The priority you assign to an automation task is the priority used by any user who runs the alert. However, if you give an automation task to a general user or user administrator, the automation task's priority is changed to Medium, and you must modify the priority if it should be higher. If you want multiple users to run the automation task with the priority you specify, you should share the automation task with those users. For information about sharing and giving automation tasks, see the *RapidResponse User Guide*.

▸To change the priority of an automation task

1. In the **Administration** pane, under **System Monitoring**, click **Resources**.
2. Click a tab corresponding to the type of automation task (**Alerts**, **Scheduled tasks**, or **Automation Chains**) you want to change.
3. Select the row for the task or tasks you want to change.
4. On the workbook toolbar, click **Change Priority** .
5. In the **Change Priority** dialog box, select one of the following priorities.
   - **Critical**—These tasks always run first. This priority is typically reserved for system tasks and critical business processes.
   - **Urgent**—These tasks run when there are no more Critical priorities in the queue. These are typically very important but not business-critical.
   - **High**—These tasks run when there are no more Urgent priorities in the queue. These are typically more important than general users' tasks.
   - **Medium**—These tasks run when there are no more High priorities in the queue. This is the default priority, and is typically the priority a general user's tasks run at.
   - **Low**—These tasks run only when there are no higher priorities in the queue. These are typically alerts that can run at any time.

Tip: You can also change the priority of automation tasks using the Automation Tasks worksheet in the Automation Log workbook. For more information about using the Automation Log workbook, see "Automation logging" on page 448.

Managing process instances

As a system administrator you can change the status of process instances and activities. You can also delete process instances. You might have to change the status of a process instance or delete it if its process owner is unavailable to do so.

▸Change the status of a process instance

1. In the **Explorer**, click the process you want, and then on the **Actions** menu click **View Instances**.
2. In the **Process Instances** workbook, in the **Status** column, change the status of the process instance you want.

▸Change the status of a performer on an activity

1. In the **Explorer**, double-click the **Process Activities** workbook.
2. On the workbook toolbar, click **Calendar** to display the process instance tree view.
3. In the **Performers** column, click the performer whose status you want to change.
4. In the **Assignments** worksheet, in the **Status** column, change the status.

▸Delete a process instance

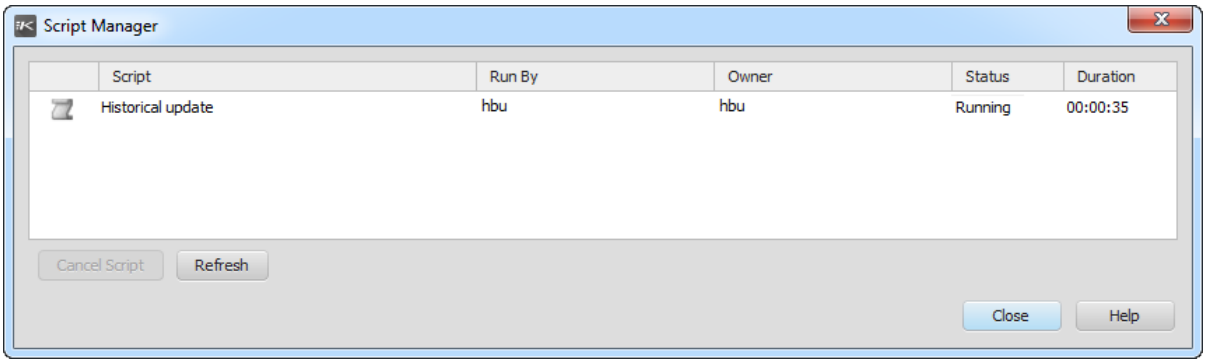
1. In the **Explorer**, click the process you want, and then on the **Actions** menu click **View Instances**.
2. In the **Process Instances** workbook, select the entire row of a process instance, and then on the workbook toolbar, click **Delete** ✕.

Monitoring and canceling scripts

As a system administrator, you can cancel any script that is running. You might be required to cancel a script for another user, because users who are not script authors cannot cancel the scripts they run. For example, you might want to cancel a script if a user has contacted you to find out if their script is still running, or if it has been running for over an hour.

In addition to canceling scripts, you can monitor the running scripts, which shows you who is running the script and how long the script has been running. You might want to monitor running scripts to determine if a long-running script is impacting system performance.

You can view the scripts that are running in the Script Manager dialog box, which you can access from the Script Log worksheet of the Automation Log workbook. For information about script logging, see "Script Log worksheet" on page 458.



In the above example, the Historical update script has been running for 35 seconds.

When you cancel a script, any changes to data the script has already made are retained, which might include changes that are part of a process. If you cancel a script before its changes are complete, the in-progress changes are not reverted, and might result in system instability. Before you cancel a script, you should verify the operations the script performs and whether canceling them could be problematic with the script's author.

▸To view and cancel running scripts

1. In the **Automation Log** workbook, click the **Script Log** worksheet.
2. On the workbook toolbar, click **Show Running Scripts** .
3. To cancel a script, in the **Script Manager** dialog box, select the script you want to cancel, and then click **Cancel Script**.

Note: Canceling scripts is similar to canceling queries. For more information, see "Monitoring and canceling problematic queries " on page 603.

Retrieving predefined workbooks

RapidResponse includes predefined workbooks that are used to solve supply chain management (SCM) and sales & operations planning (S&OP) business problems. These workbooks can be modified to fit your company's requirements or used as the basis for the workbooks and worksheets you create.

It is recommended you not edit the predefined workbooks as it might impact the upgrade process. Rather, make a copy of the workbook and edit it.

If you do make changes to a predefined workbook and want to revert your changes, or if a predefined workbook is accidentally deleted, you can retrieve an original version of the workbook from a special repository in the RapidResponse database.

▸Retrieve a predefined workbook

1. In the **Explorer**, select any workbook.
2. On the **Actions** menu, click **Retrieve Predefined Workbook**.
3. In the **Predefined Workbooks** box, select the workbook(s) to import.
4. Click **OK**.

5. A private copy of the predefined workbook is added to your **All Workbooks** folder.
6. Optionally, add the retrieved workbook to the versioned repository and share it with other users or groups.

Notes:

- Administrators and users who have been granted the retrieving permission can retrieve the predefined workbooks.
- For a listing of all predefined workbooks, see the *RapidResponse Predefined Resources Reference*.

Tip: You can select multiple workbooks by holding CTRL and then clicking each workbook you want to select, or by clicking the first workbook, then holding SHIFT and clicking the last workbook you want to select.

Migrating RapidResponse resources

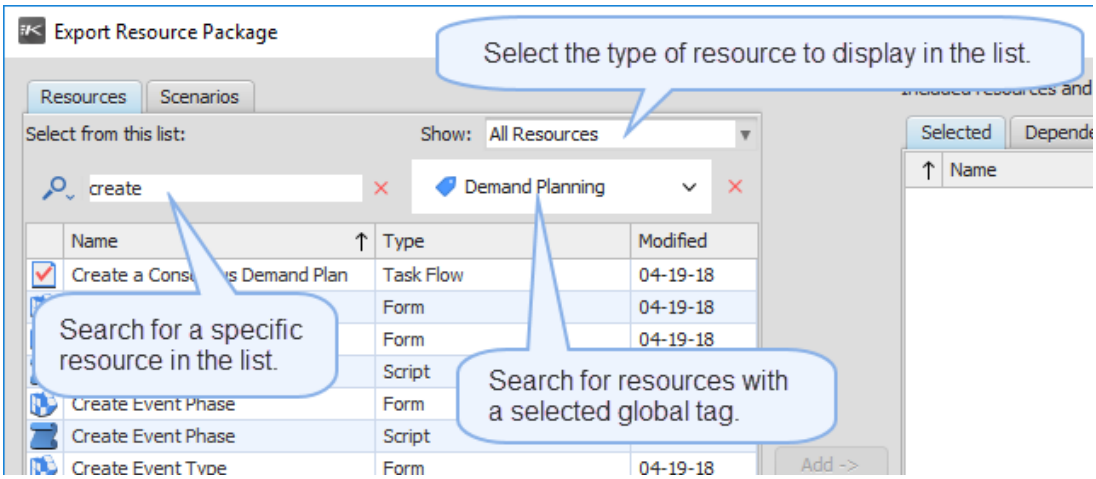
RapidResponse resources, such as dashboards or workbooks, are often developed on a test or development system and then moved to a production system. As a system or data administrator, you can migrate resources in bulk between RapidResponse systems. When you create a resource package, you select the public or shared resources and scenarios to export and RapidResponse automatically adds any dependent resources required to the package.

When you import a resource package, you control which of the resources and scenarios are imported. New resources you do not have in your system are set to automatically import. For resources and scenarios with older or existing copies already in your system, you can select whether or not to import them.

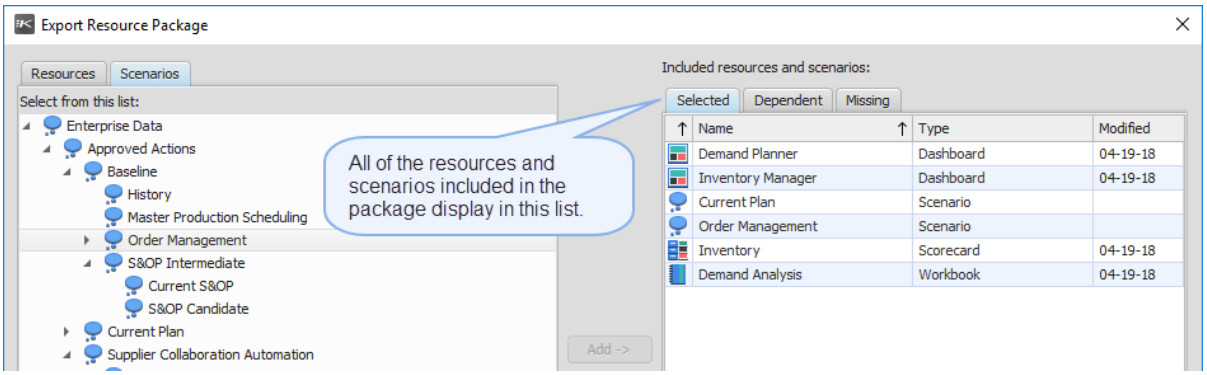
Resource packages can be used to migrate small or large groups of resources, their dependent resources, and scenarios. Individual resources, including any dependent resources, can be exported or imported by users with authoring and sharing permissions and by administrators. For more information, see the *RapidResponse Resource Authoring Guide*.

Exporting a resource package

When you create a resource package to export, all of the public or shared resources and scenarios available to you display. On the Resources tab, the most recent version of each resource along with its comments are available for export. You can filter the resource list to show only a specific type of resource or only resources with a selected global tag, and you can sort by name, type, or date modified by clicking the column headers. For example, you might sort the resource list by “modified” to display the most recently modified resources at the top of the list.



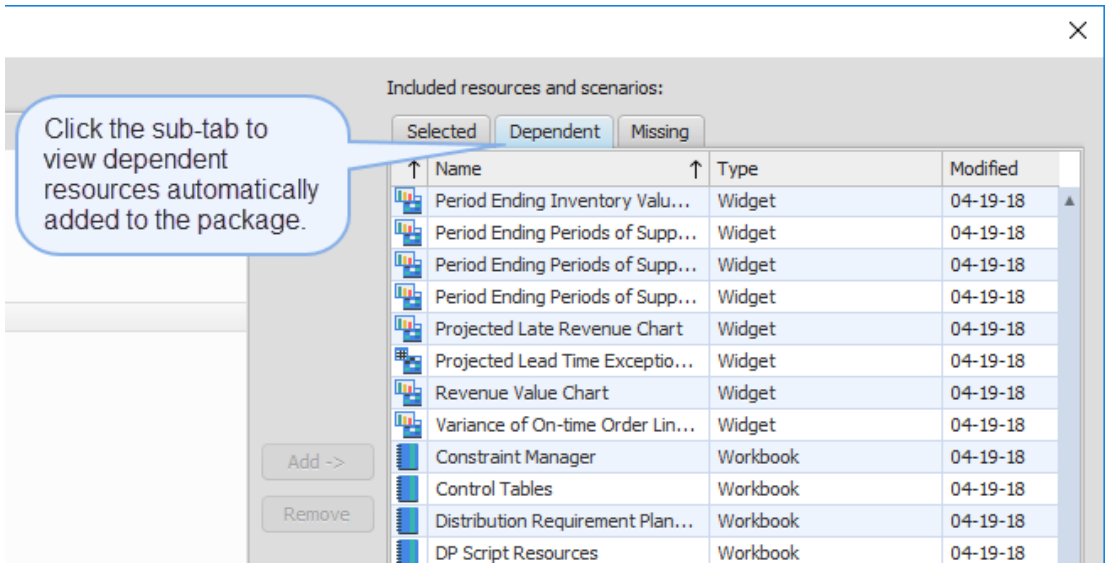
Resources and scenarios you have selected display on the Selected sub-tab.



After selecting resources to include in the package, any dependent resources are automatically added to the Dependent sub-tab.

Dependent resources might include items such as:

- Resources listed as dependencies of a workbook
- Metric workbooks required by a scorecard
- Images used by a resource



Some resources, such as images, can only be added as dependent resources. Scenarios are added by themselves, their parent and child scenarios are not added as dependencies.

Resources that might be missing or broken, or that a user does not have both authoring and sharing permission for, display on the Missing tab. Resources might be broken when they are missing a key element. For example, a component worksheet might have been deleted and the composite worksheet that depends on it is now broken. You must fix the broken or missing dependency to include the resource in the package.

However, if the dependency has been specified as optional, you are able to include resources with missing or broken dependencies in the package. For more information, see the *RapidResponse Resource Authoring Guide*.

You can also view version histories for resources before selecting to include them in a package. For more information, see "Viewing a resource's version history" on page 743.

Notes:

- A dependent resource cannot be removed from the **Included resources** list unless the selected resource or resources that depend on it are removed from the package.
- Private resources and scenarios cannot be added to a resource package. You must add the resource to the versioned repository before you can add it to the resource package or share it with another user.
- If you include a scenario that has a perspective applied, the perspective and its associated data changes are not included with the scenario.
- System workbooks and site filters cannot be exported or imported as part of a resource package.
- The resource package can include resources used by the Real-time Integration Service, which are not displayed in the Resources workbook. These include business message definitions and transformations. For more information, see the *RapidResponse Data Integration Guide*.

▸To export a resource package

You can filter the resource list to show only a specific type of resource or only resources with a selected global tag, and you can sort by name, type, or date modified by clicking the column headers.

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities.**
2. Click **Export**.
3. On the **Resources** tab, select a resource to include in the package.
4. Click **Add**.
5. Optionally, you can filter the list of resources. For more information, see "Filter the resource list" on page 755.
6. Repeat step 3 - 4 for each resource that will be part of the package.

   You can select multiple resources by holding CTRL and clicking each item, or select a group of resources by holding SHIFT and clicking the first and last resources in the group.
7. On the **Scenarios** tab, select a scenario to include in the package.

   Expand or collapse the scenario hierarchies by clicking the arrows.
8. Click **Add**.
9. Repeat step 7 - 8 for each resource that will be part of the package.
10. To remove an added resource or scenario, select it in the **Selected** sub-tab and click **Remove**.
11. Click **OK** once all resources and scenarios have been added to the package.
12. Select where to save the package.
13. Optionally, type a new file name for the package.
14. Click **Save**.

    The resource package is saved with the .RPK extension.
15. To open and view the saved package, click **Open Folder**.
16. To continue without opening and viewing the saved package, click **Close** twice.

Filter the resource list

You can filter the list of resources in multiple ways to focus on only the resources you want to select.

▸Sort by column

- Click any of the column headers to sort the list by name, type, or modified date.

▸Sort by type

1. In the Show drop-down list, select a resource type.
2. To clear the type filtering, select All Resources.

▸Search for a resource name using a text string

- In the **Search** box, start typing the string you want to search for.

  The list automatically starts filtering the list as you type.

▸Search using a tag

- Click in the **Choose a tag** box and select a global tag in the list.

Tips:

- To filter the resource types displayed, select the resource type from the **Show** drop-down menu.
- To search for a resource, type the name of the resource in the search box.
- To sort the list of resources, click the **Name**, **Type**, or **Modified** column headers.

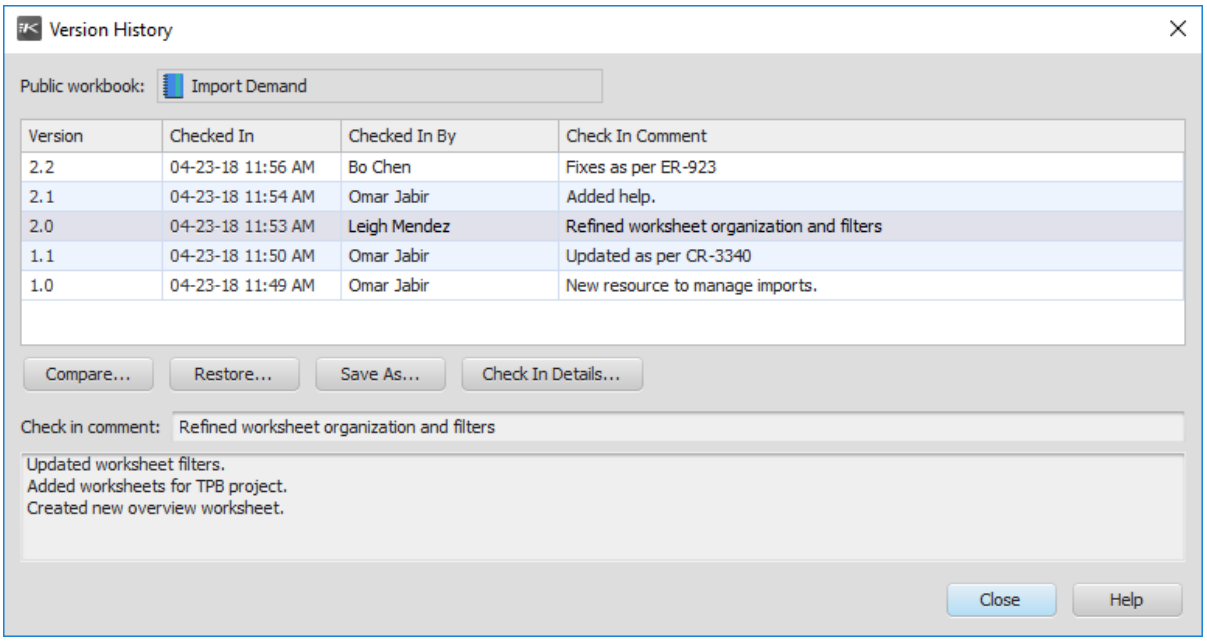
Viewing a resource's version history for export

The version history for a resource displays comments that have been added about modifications made to the resource, such as enhancement details or information on what new dependencies have been added to the resource and why.

You can only view the version history for a resource in a RapidResponse system that has version control enabled. The version history button does not display for systems with version control turned off. For more information, see "Turning version control on or off" on page 742.

▸To view a resource's version history

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Click **Export**.
3. Click the **Resources** tab.
4. Select the resource to view a version history and then click **Version History**.



Note: You can select to view the version history for any resource in the **Select from this list** pane or the **Included Resources** pane. In the **Included Resources** pane, you can view the version history for a resource on any of the three tabs: **Selected**, **Dependent**, or **Missing**.

Importing a resource package

To import a resource package, you must have the following permissions:

- Create and share permissions for all resources in the package.
- Create, share, and manage permissions for all scenarios in the package.

When you import a resource package into RapidResponse, it can contain both new and updated versions of resources and scenarios. The new resources and scenarios are set to be automatically imported into your system. For updated or modified versions of resources and scenarios, you can select whether to import them or keep the current versions in your system.

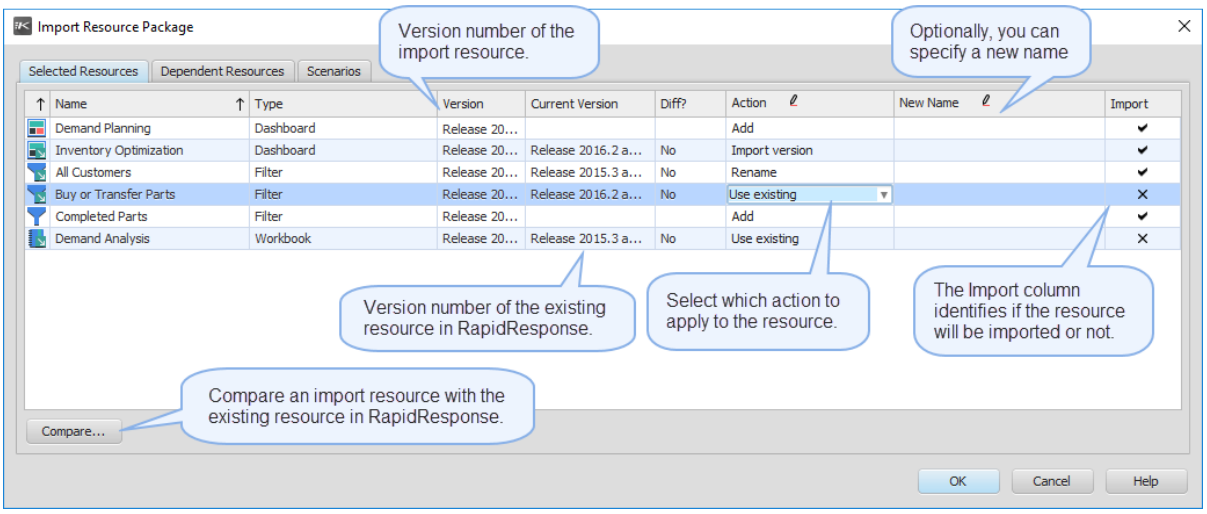
For a resource, the import action includes a default comment identifying it as an imported version and any migrated comments attached to the resource. Any global tags applied to the resource when it was exported are also migrated.

Even though scenarios are not imported with their parents or children, the parent scenario for each imported scenario is identified. If the parent exists in your system, the imported scenario is made a child of that scenario. If the parent scenario does not exist in your system, the imported scenario is made a child of your root scenario.

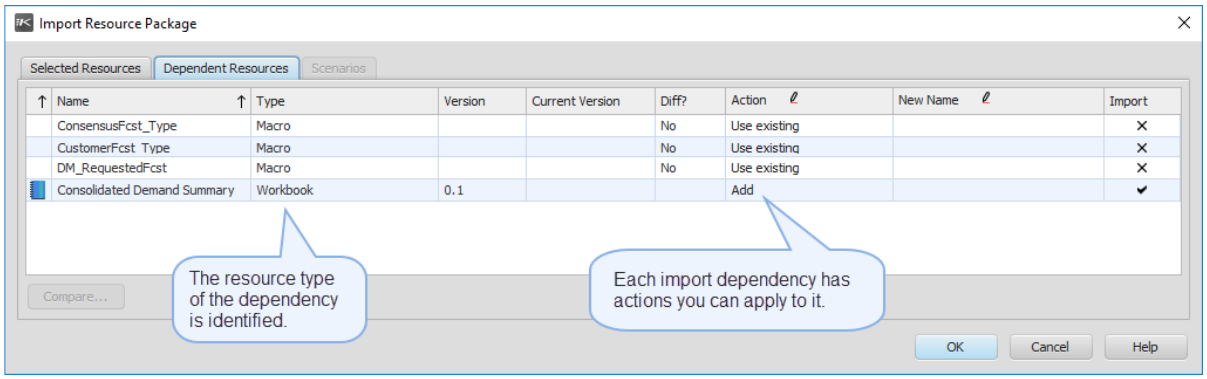
The ownership of resources and scenarios do not change when they has been migrated from one system to another. However, if the owner of a resource or scenario is not in your system, the ownership transfers to the administrator who imported that resource or scenario.

The Import Resource package dialog box includes three tabs:

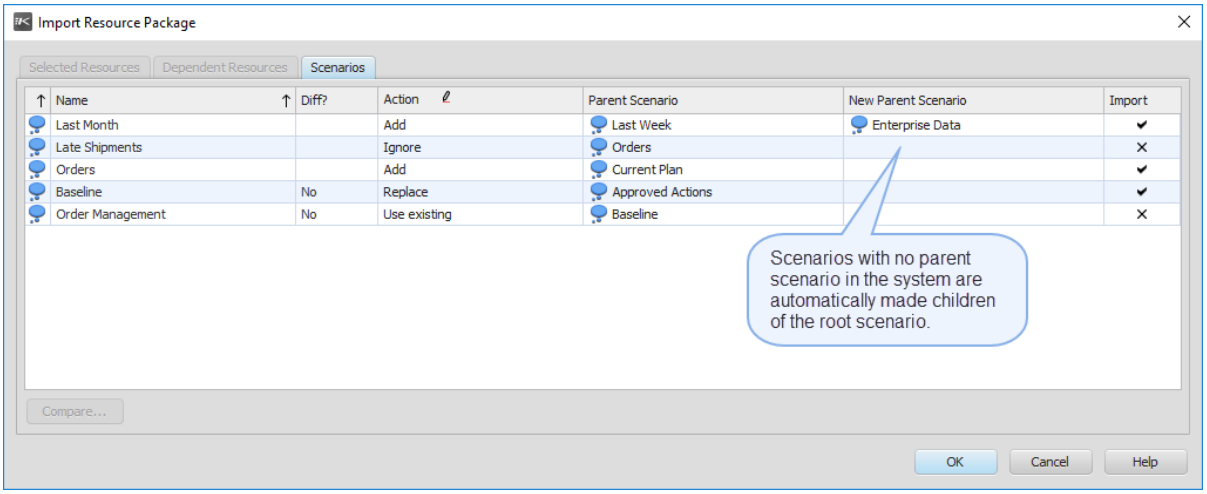
Selected Resources—All of the public and shared resources included in the resource package display on this tab.



Dependent Resources—All of the public dependent resources included in the resource package display on this tab. The relationship of the dependent resources to the selected resources is not shown, however, after import you can view the resource dependencies to explore how the resources are related. For more information, see the *RapidResponse Resource Authoring Guide*.



Scenarios—All of the shared scenarios included in the resource package display on this tab, identifying their original parent scenario and if required, their new parent scenario in your system.



Import actions

When you import a resource package, the default action for new resources and scenario is Add. New resources must be imported. New scenarios can be added or ignored. If you do not need those new resources or scenarios, you can delete them after the import or create a new resource package that does not contain them.

For resources and scenarios in the package that are updated or different versions of those already existing in the system, you can select one of the following actions:

- **Use existing**—The resource or scenario in the package is not imported. Instead, the current version in RapidResponse is maintained.
- **Import version**—This action only applies to resources. The current resource in RapidResponse is replaced with the import version from the package. The imported resource carries the same sharing permissions as the replaced version with the same users and groups retaining access to the resource.

  The most recent version of the resource along with its comments are migrated as the import version.

- **Rename**—The resource in the package is imported with a new name. When you are renaming resources, be aware of any dependencies that might change.

  For example, you might have the selected resource, A and its dependent resource, B, in a resource package you are importing. If you rename B to C and then import resource A, it will be linked to the renamed dependent resource C. If you do not import resource A, it will still be linked to dependent resource B.

- **Replace**—This action only applies to scenarios. The current scenario is replaced and the sharing permissions are transferred.
- **Ignore**—This action only applies to scenarios. The new scenario in the package is not imported.

During the import process, resources and scenarios being replaced cannot be deleted or modified. For resources that are checked out and will be replaced during the import, you must discard the check outs to continue importing the resource package. The authors who originally checked out the resources is informed of the discard in an automatic message.

For new resources and scenarios in the package, you must share each new resource or scenario with users after they are imported. The new resources and scenarios are still owned by their original authors and can only be shared by that author or an administrator.

You can compare differences between a resource in the package and the current resource in RapidResponse to determine what action to take. You can only compare resources in a resource package that have differences between the resource you importing and the existing resource in the system. For more information, see "Comparing resources" on page 761.

After the import is complete, users will receive a message in Message Center with an attached log, describing all of the resources and scenarios in the resource package and what action was taken for each one. For example, the message identifies what was imported or renamed.

Notes:

- If resources for a circular dependency, all those resources are added to the resource package as selected resource and no dependencies display on the Dependent Resources tab.
- If you are importing a resource package from a system without version control into a system with version control turned on, a default version number and comment are applied to each resource in the package.
- If you do not have permission to create, share, or manage any of the resources in the package or for scenarios then you will not be able to import the resource package.
- In systems with version control turned off, the **Import Version** action displays as **Replace** for resources. The current resource is replaced and the sharing permissions are transferred.
- You can only import resource packages that were created in the same version of RapidResponse or earlier. Attempting to import a resource package that was created in a version of RapidResponse later than the one it is being imported to will result in en error.

▸To import a resource package

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Click **Import**.
3. Locate the resource package file with the .rpk file extension, and then click **Open**.

4. On the **Selected Resources** tab, for each resource, select the **Action:**
   - **Use existing**
   - **Import version** or **Replace**
   - **Rename**

     If you select **Rename**, type a new name for the resource.
5. To compare a resource you are importing with the current resource in your system, select the resource and click **Compare**.
6. Optionally, on the Dependent Resources tab, for each resource, select the Action:
   - **Use existing**
   - **Import version** or **Replace**
   - **Rename**
7. On the **Scenarios** tab, for each scenario, select the **Action:**
   - **Use existing**
   - **Replace**
   - **Ignore**
8. Click **OK** once all the resources to be imported have been selected.

   You will see a message stating that the package has been successfully imported.
9. Click **OK**.

Caution: If you choose to rename a dependent resource, it might affect the imported resource that depends on it.

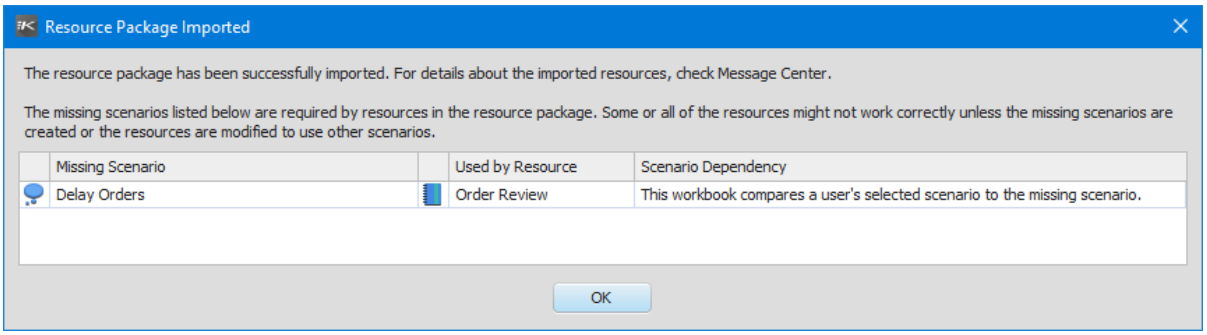
Notes:
- You cannot include scorecards to import in a resource package unless their metric workbooks are first added to the package. Therefore, to import a resource package with scorecards, you must first import the scorecard's metric workbooks, and then you can add the scorecard.
- You cannot import a resource package that contains resources you do not have permission to create.
- You cannot import unlicensed resources, or resources you do not have permission for. The resource package import will fail.
- If you rename a resource in the package, the new name cannot be blank and must begin with a letter.

Tip: Compare resources to better understand the changes in a resource before you import a resource or deploy the resource to another environment, such as from a development environment to a production environment.

Identifying missing scenarios

If a resource requires a specific scenario to function and that scenario is not included in the package or does not exist in the RapidResponse system you are importing into, that resource might not work as expected.

When a resource package is imported, any required scenarios are identified as missing. Each missing scenario is listed with the resource that depends on it and the details of that dependency.

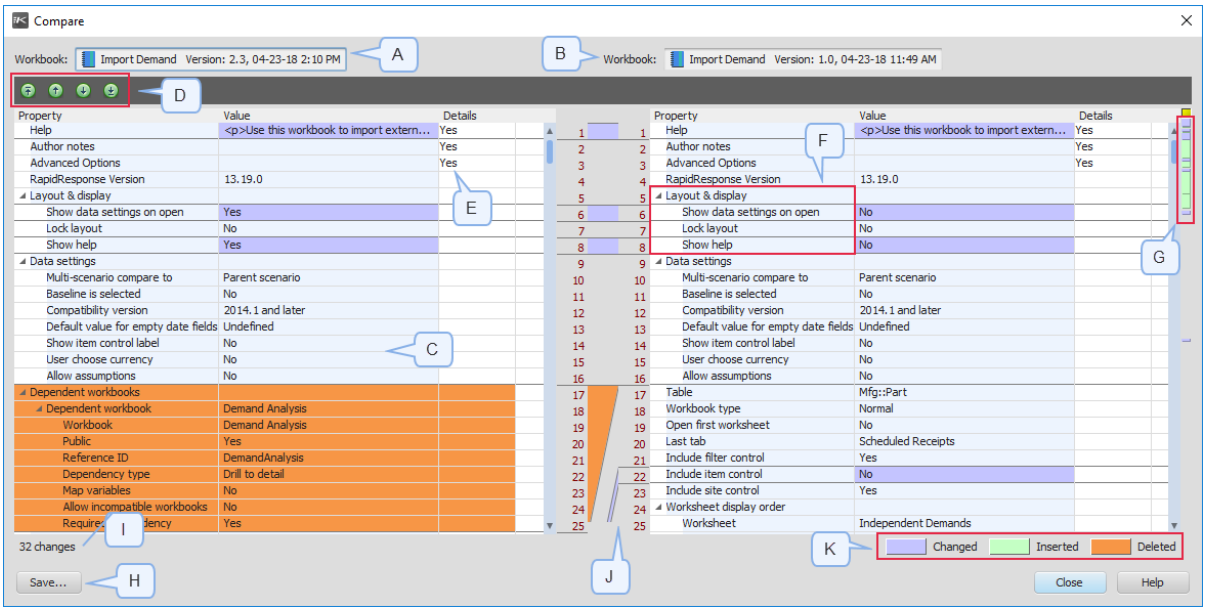


You can create a new data package and include the missing scenario in it along with the resource that requires the scenario. If you want to resolve the missing scenarios in the RapidResponse system you are importing the package into, you can do any of the following:

- Re-create the missing scenarios.
- Modify the imported resources to use scenarios that are already available in the system.

Comparing resources

You can compare resources in the resource package with their current versions in RapidResponse to determine what action to take, such as whether to import the resource or save it under a new name. You can also compare resources to view the differences and then manually merge those differences. For example, the current resource might be customized for your company. The resource package contains a version of the resource with changes you want to incorporate into your customized version. You can compare the two resources to record which changes to make, or you can import the resource with a new name and compare the two resources at a later date. For more information about comparing resources, see the *RapidResponse Resource Authoring Guide*.



Letter	Description
A	Baseline resource—the current resource in the system that you compare to the resource in the package.
B	Compare resource—the resource you are importing that you compare against the current resource in the system.
C	Resource properties list—these properties are selected and modified in the resource's properties dialog box.
D	Move from difference to difference using the navigation arrows.
E	Click "Yes" to view a more detailed comparison.
F	Some properties expand to display the fields that make up the property.
G	Visual indicators map the type, number, and location of a difference. Click on an indicator to jump to that location in the property list.
H	Save the comparison details as a text file to keep a record of resource differences.
I	The estimated number of differences between the two resources.
J	Row numbers allow you to track the number of properties and to cite specifically where the differences exist.
K	The types of differences are conditionally highlighted in the property list. • Purple identifies properties that have changed. • Green identifies properties that have been inserted. • Orange identifies properties that have been deleted.

▸To compare an import resource with a current resource

1. In the **Administration** pane, under **System Monitoring**, click **System Utilities**.
2. Click **Import**.
3. Locate the resource package file with the .rpk file extension, and click **Open**.

4. Select the import resource to compare.
5. Click **Compare**.

Caching worksheet results

For frequently used worksheets that perform intensive calculations and take longer to load, you can cache the worksheet results to speed up workbook opening times. The cached results are stored in the same memory as RapidResponse analytics: system memory dedicated to calculations. For more information, see "Calculations and system memory" on page 265.

You can use cached worksheet results to speed up dashboard opening times. For example, a widget based on a source worksheet with time-consuming calculations might slow the opening of any dashboards the widget is placed on. Caching results for the source worksheet cache can display data faster in the widget and thereby, display data faster on a dashboard.

Cached worksheet results are specific to a scenario. Cached results are only shared between parent and child scenarios that have the same data. Each time data is changed in a scenario, the current cached results are deleted and the worksheet is recalculated and the results cached again.

Notes:

- The server might delete cached results if system memory is required.
- Cached results are only as current as the scenario the results were cached in.

Using resources with cached worksheet results

The first time a worksheet that caches results is opened, the data takes longer to display because it is being calculated and then cached. Each time the worksheet is subsequently opened, it displays results at the faster, cached rate. It is recommended that after you turn on results caching for a worksheet, you open it for the first time at the slower rate to ensure a faster experience for users who open the worksheet after you.

For some workbooks that have worksheets that display cached results, you can create a script to automatically run the worksheet queries at a specified time. The workbook is then prepared for users who open the workbook after the script has been run. For example, your company might have a workbook that only a few users have permission to modify data in and your company process is to submit all resource changes by the end of day. You can create a script to run the worksheet queries in the workbook at the beginning of the next day so all users start the day with data that displays at a faster rate. For more information, see the *RapidResponse Scripting Guide*.

For dashboards, you can use a RapidResponse script to run the queries for all the widgets on the dashboards before a user opens the dashboard. When the queries are executed for widgets based on source worksheets that cache results, the results are calculated and cached. Users that then open the dashboard experience a faster data viewing experience. For more information, see "Prepare a dashboard with cached results for users" on page 764.

Authors have permission to create worksheets compatible with displaying cached results. However, because caching worksheet results impacts system memory, only RapidResponse administrators have permission to turn caching on or off for a worksheet. for more information, see "RapidResponse system memory usage" on page 260.

Note: While only data changes made in a scenario trigger a worksheet to recalculate results, it is possible that a user might need to manually refresh a worksheet after data settings are changed in a worksheet.

Monitoring worksheets with cached results

System administrators can view a list of all the cached worksheets in your RapidResponse system using the RapidResponse Console. Only cached worksheets display in the list. The Console is only available to the On-Premises installation of RapidResponse.

The **Worksheet ID** column shows the actual worksheet ID and not the worksheet label. The **Exec Counter** column represents the number of records that have been calculated and cached. The **Memory %** column represents the percentage of cached memory the worksheet is consuming.

Workbook	Worksheet ID	Owner	Shared?	Exec Counter	Memory (MB)	Memory %
SCM Widgets Workbook	AllIndependentDemandCached	lpao	N	5039	2.91	82.00
SCM Widgets Workbook	ExpiryCached	lpao	N	5039	0.63	18.00
S&OP Constraint Widgets	TotalKeyConstraintUsageCached	Admin	Y	0	0.00	0.00
S&OP Demand Metrics	LateDemandComponentforCached	Admin	Y	0	0.00	0.00
S&OP Inventory Metrics	ProjectedInventoryDetailsBaseCACHED	Admin	Y	0	0.00	0.00
S&OP Inventory Metrics	ProjectedInventorySummaryBaseCACHED	Admin	Y	0	0.00	0.00
S&OP Widgets Workbook	AllIndependentDemandCached	Admin	Y	0	0.00	0.00

For information about opening the RapidResponse Console, see "To sign in to RapidResponse Console" on page 230.

For information about system memory, see "RapidResponse system memory usage" on page 260.

Caution: A large number of worksheets with cached results can negatively impact system performance if they take up too much system memory. For more information about monitoring system memory levels, see "System memory details in RapidResponse Console" on page 261.

▸Turn caching on or off for a worksheet

1. In **Worksheet Properties**, on the **General** tab, click **Advanced**.
2. On the **Extended Configuration** tab, select the **Cache worksheet results** check box

   Ensure worksheet is compatible with caching results should already be selected. For more information on creating worksheets that can display cached results, see the *RapidResponse Resource Authoring Guide*.

Prepare a dashboard with cached results for users

For dashboards with widgets based on worksheets that display cached results, you can prepare the dashboard to ensure faster viewing experiences for users. You can use a script to run the worksheet queries for all the widgets on the dashboard. The worksheet results are calculated, and when applicable, cached. Users who open the dashboard after the script is run view the data at the faster, cached rate. For more information, see "Using resources with cached worksheet results" on page 763.

You can run the script as a scheduled task. For more information, see the *RapidResponse Scripting Guide*.

System administrators can use the **Prepare Dashboard** script to prepare the dashboard for users. It is recommended that two specialized scenarios be used for the dashboard:

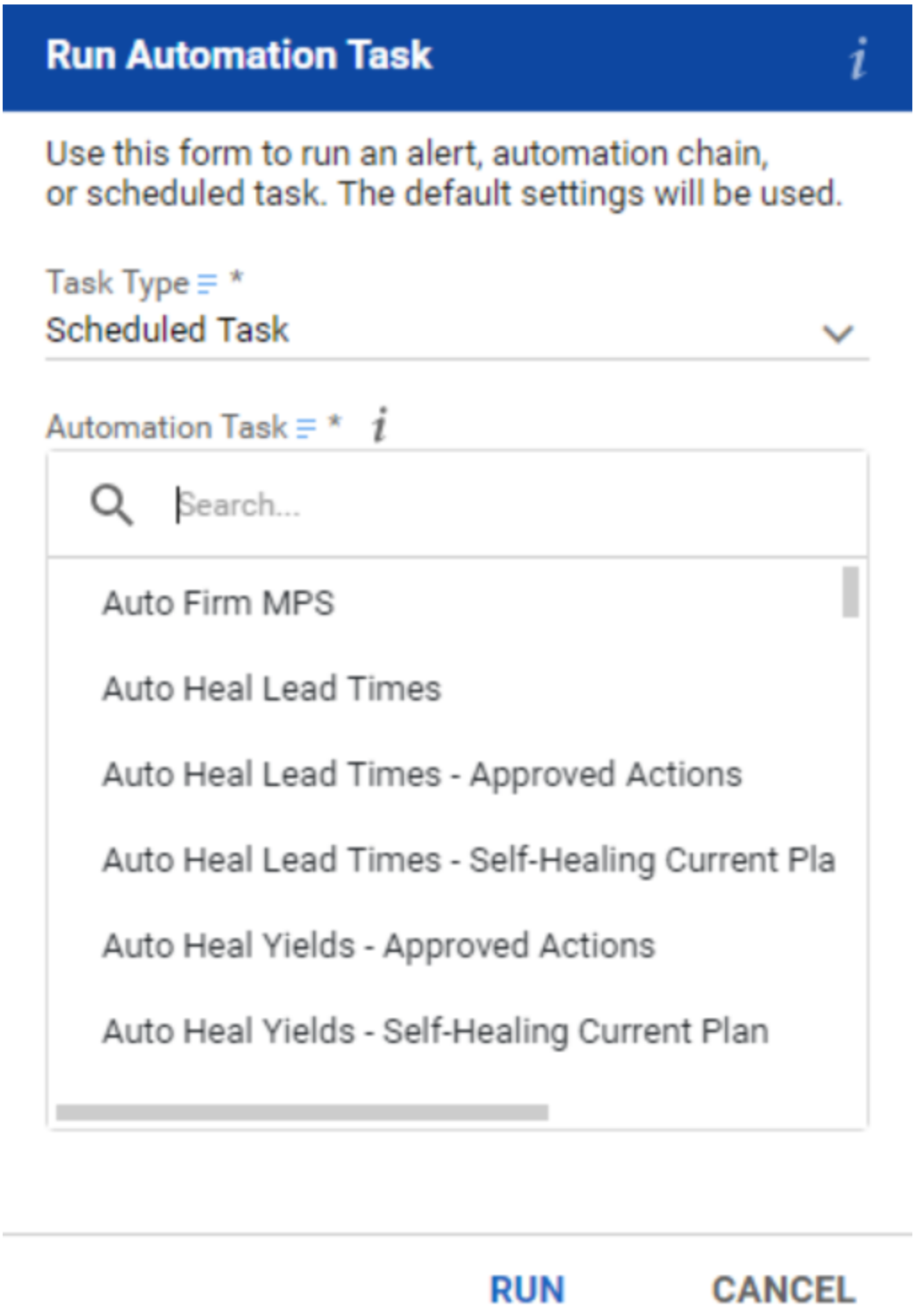
- Scenario with data to cache
  - A staging scenario that is private and owned by the administrator. Specify the staging scenario as the Override Scenario when you run the script.
    - A reporting scenario that is public and read-only for users. The dashboard should be configured to use the reporting scenario.

▸Prepare a dashboard with cached results for users

1. Reset the staging scenario, to account for any changes made in the parent scenario.
2. Run the **Prepare Dashboard** script to run the queries for all widgets on the dashboard.
3. Reset the reporting scenario to make the cached worksheet results available.

Forms included in RapidResponse

Forms are a resource type that are customizable interfaces to RapidResponse scripts. By default, RapidResponse includes several forms that can help improve administrator efficiency. You complete tasks by specifying values in the form that are then passed to the underlying script when it is executed. For example, if you need to run the Commit Buyer Response Scheduled Task, you can specify the required values in the Run Automation Task form, shown in the illustration below.



Forms can be run from the Java client or the web client. Running forms from the web client allows you to continue to complete important tasks when you are away from your desktop. All users can sign in to the web client. For more information, see "Providing the RapidResponse URL and credentials" on page 553.

System forms are automatically shared with all administrators and cannot be shared with general users or authors. Non-system forms can be shared with all users.

The following table lists tasks that you can complete using forms.

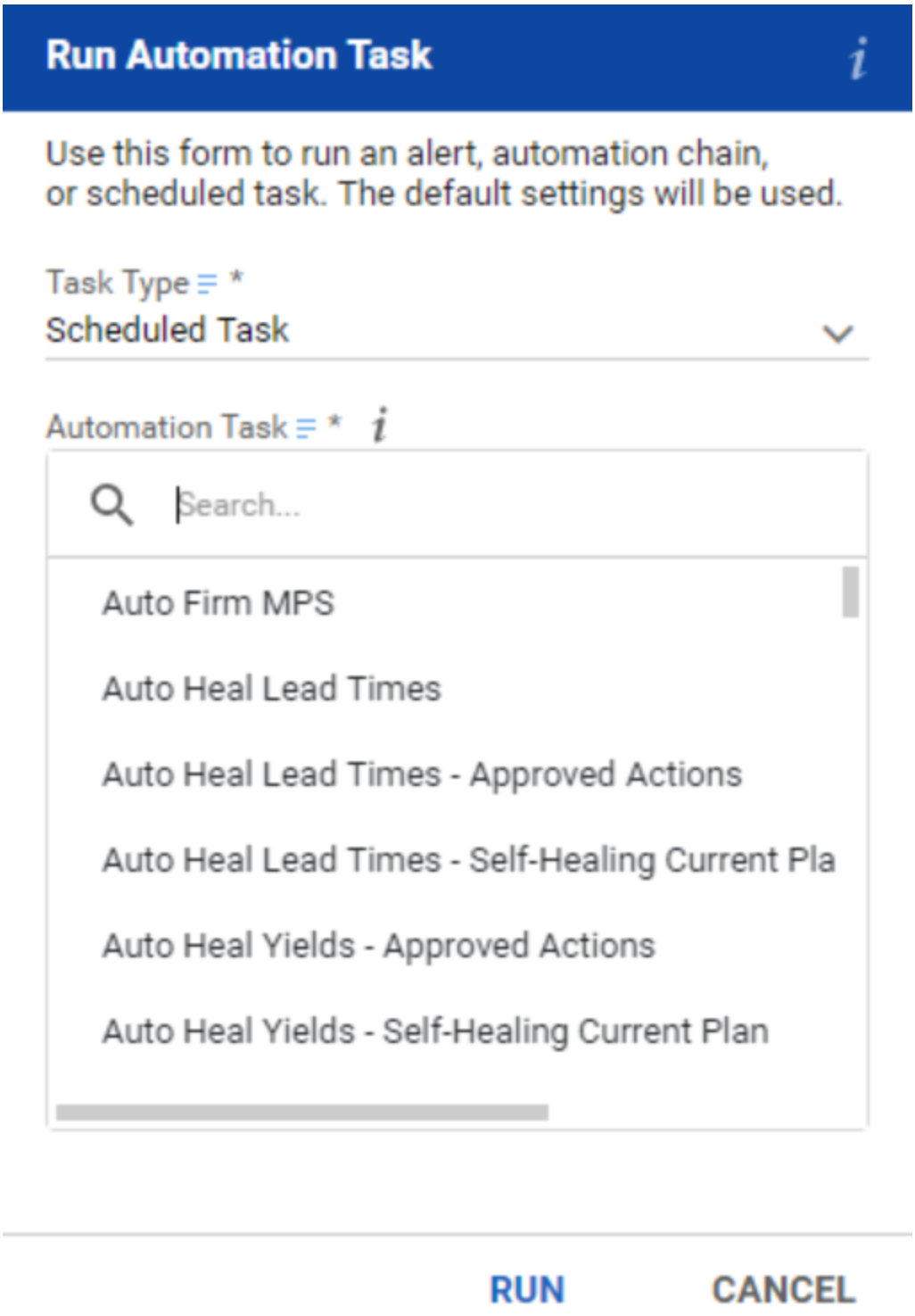
Task	Form	Type
Create a new user account by duplicating an existing account. For more information, see "Duplicating a user account" on page 551.	Copy User Account	System form
Unlock a user account. For more information, see "Unlocking a user account" on page 599. Set a new password for a user. For more information, see "Editing user accounts" on page 570.	Reset User Account	System form
Run an alert, automation chain, or scheduled task. For more information, see "Running automation tasks" on page 767.	Run Automation Task	System form
Respond to a scenario. For more information, see "Responding to a scenario" on page 771.	Scenario Response	Non-system form (can be shared with all users)

Your RapidResponse system might include other forms related to specific applications. For more information, see the *RapidResponse Applications Guide*.

Running automation tasks

RapidResponse automation tasks are resources that support automated processes. Automation tasks can be used to modify data, run other automated processes, and notify you of changes made by the process. Automation tasks include alerts, scheduled tasks, automation chains, and scripts.

You can run automation tasks that you have access to from the Explorer, the RapidResponse toolbar, or by using the Run Automation Task form, shown in the illustration below.



This form can be used on your mobile device using the web client, so you can run an automation task when you are away from your desktop. For more information about signing in to this client, see "Providing the RapidResponse URL and credentials" on page 553.

Note: You cannot use the Run Automation Task form to run a script.

▸Run an automation task from the Java client toolbar

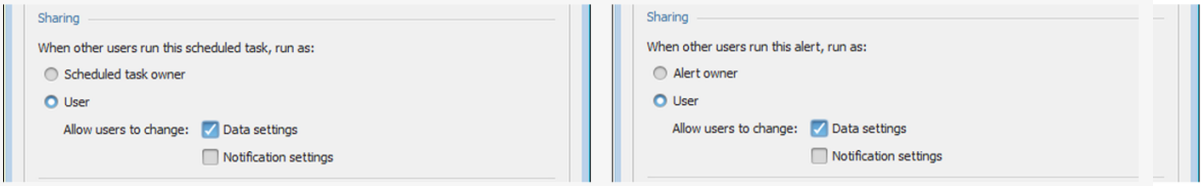
1. On the toolbar, click **Run Automation Task**.
2. In the **Run Automation Task** dialog box, select the automation task you want to run.
3. Optionally, do the following to sort the automation task list.
   - Click **Name** to sort the list alphabetically by name, which allows you to select from the beginning or end of the list.
   - Click **Type** to sort the list by type, which allows you to select from only the type of automation tasks you want to run.
4. Click **OK**.
5. Depending on the automation task type you selected and the settings of that automation task, specify settings for the automation task.

Note: You can also run automation tasks from the Explorer. To do so, select a resource, right-click, and select **Run Now**.

▸Run an automation task using the Run Automation Task form

1. Do one of the following:
   - **Java client**—From the **Explorer**, under **Forms**, double-click **Run Automation Task**.
   - **Web client**—Sign in, then open the **Run Automation Task** form.
2. From the **Task Type** list, select the type of automation task.
3. From the **Automation Task** list, select the automation task.
4. Click **Run**.

Note: When you run an automation task using the Run Automation Task form, the default authored settings are used. Properties of alerts and scheduled tasks that allow the user to change data settings, such as those shown in the following illustrations, are ignored.



Unlocking automation resources

When an alert, scheduled task, or automation chain is given to a new owner, it is locked and cannot run until its owner or an administrator unlocks it. This helps to prevent automation resources from running using inappropriate permissions, producing unexpected results.

As an administrator, you might be asked to unlock an automation resource if its new owner is not available to unlock it. For example, if an alert is given to someone while they are on vacation, an administrator can unlock it before the owner returns so the alert can continue to run on schedule.

Before you unlock an automation resource, it is good practice to review the owner's permissions, the properties of the resource, and any other automation resources that the locked resource will run. Ensure that the resources are appropriately configured, considering the new owner's permissions.

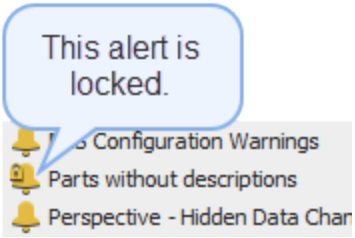
▸Unlock an automation resource

1. In the **Explorer**, right-click a locked automation resource.
2. Select **Edit** or **Check Out and Edit**.
3. Review the automation task's properties and make any necessary changes.
4. On the **General** tab of the automation task's properties, clear the **Locked** box.

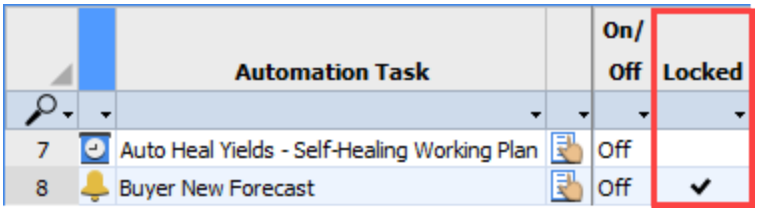
5. Click **OK** to save your changes.
6. If you selected **Check Out and Edit** in the first step, check the changes in to the versioned repository. For more information, see the *RapidResponse Resource Authoring Guide*.

Identifying locked automation resources

An automation resource that is locked is shown in the Explorer with a lock on its icon.



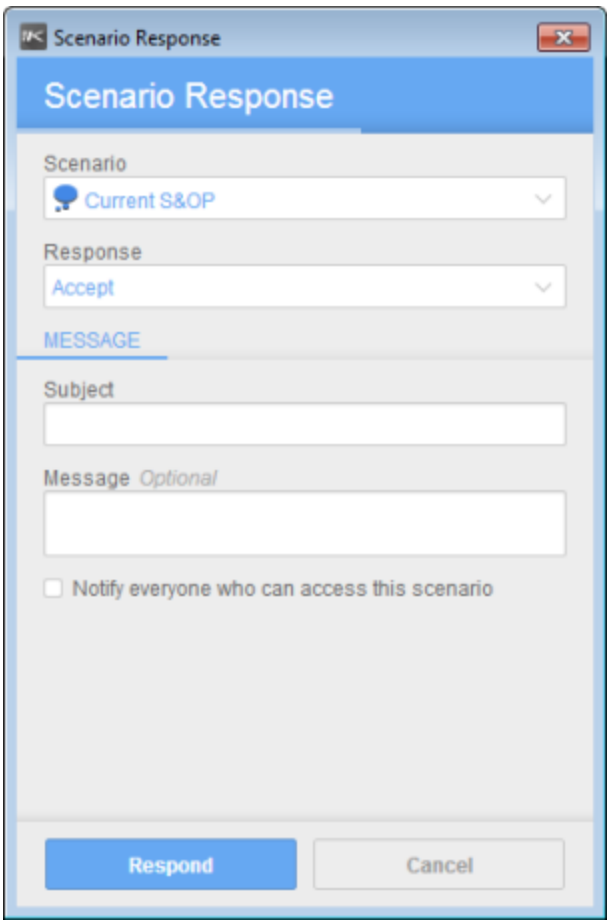
In the Automation Task worksheet in the Automation Log workbook, the Locked column shows which automation resources are locked.



Responding to a scenario

After viewing a scenario's properties, you can add a response to the scenario. You can accept, reject, or add a note to a scenario. You can also send a message to the scenario owner and other users with your response.

In addition to using the Scenario Properties pane, you can respond to a scenario by using the Scenario Response form, shown in the illustration below.



The Scenario Response form can be shared with all users. Users can run this form from the Java client and from the web client using a desktop computer or mobile device, so they can respond to a scenario when they are away from their desktops.

If you share this form with other users, you should also provide them with instructions on how to sign in to the web client. For more information about signing in to this client, see "Providing the RapidResponse URL and credentials" on page 553.

▸To respond to a scenario from the Scenario Properties pane

1. On the **Scenario Properties** tab, click **Respond** .
2. In the **Respond** dialog box, in the **Response** area click one of the following:
   - **Note**—Information about what you are doing with the scenario.
   - **Accept**—You have solved your part of the problem.
   - **Reject**—You cannot solve your part of the problem.
3. Optionally, in the **Subject** and **Message** text boxes, specify a subject and message explaining your response that will be sent to the scenario's owner.
4. If you are the scenario owner, select the **Notify everyone who can access this scenario** check box if you want to send the message to each member of the action team.

Note: The message specified in this dialog box is shown on the **General** and **Activity Log** tabs of the **Scenario Properties** tab.

Tip: You can also click **Respond** on the **Actions** menu.

▸To respond to a scenario using the Scenario Response form

1. Do one of the following:
   - **Java client**—From the **Explorer**, under **Forms**, double-click **Scenario Response**.
   - **Web client**—Sign in, then open the **Scenario Response** form.
2. From the **Scenario** list, select the scenario.

   You can also search if you know the name of the scenario.
3. From the **Response** list, select one of the following:
   - **Accept**—You have solved your part of the problem.
   - **Reject**—You cannot solve your part of the problem.
   - **Note**—Adds information about what you are doing with the scenario.
4. In the **Subject** field specify the subject of the response and optionally add a message explaining your response.
5. If you are the scenario owner, select the **Notify everyone who can access this scenario** check box if you want to send the message to each member of the action team.

Note: You cannot include a link in your message when responding to a scenario using the Scenario Response form. To include a link, respond to the scenario from the Scenario Properties pane.

Managing global resource tags

RapidResponse administrators can create global tags to group resources related to different business functions. For example, you could use a global tag to group all resources related to a particular business process, to help ensure that the full set of resources is shared with the people who need it, and to help users to locate resources. Global tags can also be used to help administrators locate resources to

include in resource packages. For more information, see "Migrating RapidResponse resources" on page 752.

When you export a single resource by selecting it in the Explorer and then selecting Export from the File menu, tags are not exported with it. However, if you create a resource package or a data package, global tags are exported along with the resources. When the package is imported, the workbooks remain tagged, and if the Tags workbook does not already list all of the tags that are applied to the resources, records are created for the new tags. Some RapidResponse resources are also installed with tags applied.

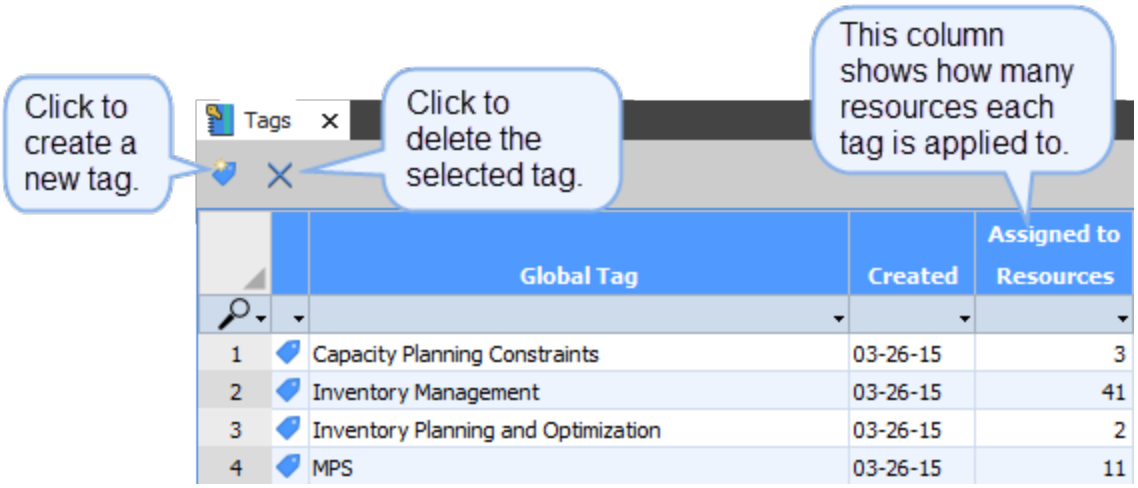
Personal tags versus global tags

The following table outlines key differences between personal tags and global tags.

Personal tags	Global tags
Are only visible to the user who created them.	Are visible to all users who can see resources that they are applied to in the Explorer.
Can be created and applied to resources by any user with access to the Explorer.	Can only be created and applied to resources by administrators.
Can be applied to both private resources, shared resources, and shortcuts.	Can only be applied to shared resources.
Are created in the Add Tags dialog box, which is opened from the Explorer.	Are created using the Tags workbook, which can be accessed from the Administration pane or the Explorer.
Are automatically deleted when they are no longer applied to any resources	Can only be deleted using the Tags workbook.

Creating and deleting global tags

Global tags are created and deleted using the Tags system workbook, shown in the following illustration.



▸Create a global tag

1. In the **Administration** pane, click **Tags** under the **System Settings** heading.
   The **Tags** workbook opens.
2. Click **New Global Tag** on the workbook toolbar.
3. Type a name for the new tag.

▸Delete a global tag

1. In the **Administration** pane, click **Tags** under the **System Settings** heading.
   The **Tags** workbook opens.
2. Select the row containing the tag that you want to delete. You can also select multiple consecutive rows to delete more than one tag at a time.
3. Click **Delete** on the workbook toolbar.

Applying and removing global tags

Global resource tags can only be applied or removed by administrators. They cannot be applied to private resources or shortcuts. When the option to apply or remove global tags is available, though, it works the same way as applying or removing personal tags.

▸Assign a tag to a resource

1. In the **Explorer**, select the resource you want to assign the tag to and click **Add and remove tags** .
2. In the **Add Tags** dialog box do one of the following:
   - Type the tag name and press **Enter**. This adds a personal resource tag.
   - Select an existing tag name by clicking the name of the tag in the list.
3. Repeat the previous step if you want to add additional tags.
4. When you are done adding tags to the resource, click **Close** .

Note: If you type a new tag name in the Add Tags dialog box and press enter, a personal tag with that name is created and applied to the resource. You cannot create a new global tag using the Add Tags dialog box.

CHAPTER 48: Tracking and managing adaptive collaborations

Administrator tools for collaboration management 775

Collaborations provide a single interface for users to communicate securely, share simulated data in scenarios, and compare solutions as a team. RapidResponse system and user administrators track and manage all open and archived collaborations in a system. Administrators can open collaborations from the Collaborations workbook and add posts, users, scenarios, and perform any of the other collaboration actions available to participants in the collaboration. For more information about the actions that can be performed in a collaboration, see the *RapidResponse User Guide*.

To keep the list of collaborations in your system manageable, it is recommended that you regularly delete empty collaborations or unneeded archived collaborations from the Collaborations workbook. For more information, see "Administrator tools for collaboration management" on page 775.

Administrator tools for collaboration management

System and user administrators can use the Collaborations workbook to review information about collaborations being conducted on their RapidResponse systems. For example, the workbook reports the collaboration creation, access, and modification dates, its status, and other information. You can open or delete collaborations in the system from the Collaborations workbook.

Reviewing collaborations in your system

The Collaborations workbook also includes information such as the user ID for the collaboration owner or the number of days since the collaboration was last accessed.

Start | Collaborations

		Owner			Days Since	Date				Modified By	
	Collaboration ID	User ID	Name	Status	Accessed	Created	Accessed	Modified	Due	User ID	Name
1	1001	bchen	Bo Chen	Open	2	06-21-16	06-21-16	06-21-16		lmendez	Leigh Mendez
2	1003	ohaddad	Oliver Haddad	Archived	2	06-21-16	06-21-16	06-21-16	05-25-16	ohaddad	Oliver Haddad
3	1004	bchen	Bo Chen	Open	2	06-21-16	06-21-16	06-21-16	10-03-16	lmendez	Leigh Mendez
4	1014	bchen	Bo Chen	Open	1	06-21-16	06-22-16	06-22-16		ylee	Yingying Lee
5	1015	ylee	Yingying Lee	Open	0	06-21-16	06-23-16	06-23-16	01-09-17	bchen	Bo Chen
6	1016	ylee	Yingying Lee	Open	2	06-21-16	06-21-16	06-21-16	08-26-16	ohaddad	Oliver Haddad

Column	Description
Collaboration ID	The unique ID used to identify the collaboration. Users see this ID displayed in the upper left of the collaboration.
Owner - User ID	The user ID of the person who owns the collaboration. This role can be reassigned.
Owner - Name	The user name of the person who owns the collaboration.
Status	The status of the collaboration: **Open**—the collaboration is active. **Archived**—the collaboration has been completed and shifted to the Archived Collaborations list.
Days Since Accessed	The number of days since the collaboration was last accessed.
Date - Created	The date the collaboration was created.
Date - Accessed	The date the collaboration was last accessed.
Date - Modified	The date the collaboration was last modified.
Date - Due	The due date set by the collaboration team. This date can be edited.
Modified By - User ID	The user ID of the person who last modified the collaboration.
Modified By - Name	The user name of the person who last modified the collaboration.

▸To open a collaboration from the Collaborations workbook

1. In the **Administration** pane, under **System Monitoring**, click **Collaborations**.
2. For the collaboration you want to open, click Collaboration ID value in that row.

▸To delete a collaboration in your RapidResponse system

1. In the **Administration** pane, under **System Monitoring**, click **Collaborations**.
2. Select the row for the collaboration you want to delete.
3. Click **Delete Record(s)** .

Tip: A scripting method is also available for deleting collaborations. This method can be used by system and user administrators. For more information, see the *RapidResponse Scripting Guide*.

CHAPTER 49: Application configuration and settings

Configuring S&OP application resources 777
Configuring other application settings 783
Configuring supporting resources 785
Configuring Self-Healing Supply Chain resources 792
Self-Healing Supply Chain scenario structure 793
Self-Healing Supply Chain control fields 796
Self-Healing Supply Chain automation tasks 798
Self-Healing Supply Chain users and groups 801

RapidResponse includes applications that are designed to help your company respond to a variety of business challenges. You can change application settings to better meet the needs of RapidResponse users.

Note: Many of the settings that are described in this section are typically configured during the RapidResponse deployment by Kinaxis consultants.

Configuring S&OP application resources

As a RapidResponse administrator, you can specify and modify S&OP profile variables (Category, Target, and Misc.) for S&OP resources by using the Application Variables worksheet in the Application Settings workbook.

S&OP data modification scheduled tasks can also insert, delete, and modify S&OP data. For example, the scheduled task called "Delete Scheduled Receipts from Supply Plan" deletes the Scheduled Receipts records and modifies the S&OP Candidate scenario.

S&OP resources and calculations

You can use the Application Variables worksheet in the Application Settings workbook to specify profile variables for the Sales and Operations Planning (S&OP) resources. The profile variables control S&OP settings.

The profile variables are prefixed with DP_ (for Demand Planning) and are divided into three types:

- Category—settings for target categories and demand categories. Most include the suffix Target or Category.
- Target—settings for disaggregation.
- Miscellaneous—settings for analytic and worksheet calculations.

Category type variable	Default value	Description
DP_ActualsCategory	Shipment	Displays the historical demand for the category selected.
DP_AdjustmentsCategory	ForecastAdjustments	
DP_BaselineForecastCategory	Statistical	
DP_BudgetForecastCategory	FinanceOperatingPlan	
DP_BudgetForecastEventCategory	FinanceOperatingPlanEvent	
DP_BudgetForecastOptimistic	FinanceOperatingPlanOptimistic	
DP_BudgetForecastOptimisticEvent	FinanceOperatingPlanOptimisticEvent	
DP_BudgetForecastPessimistic	FinanceOperatingPlanPessimistic	
DP_BudgetForecastPessimisticEvent	FinanceOperatingPlanPessimisticEvent	
DP_ConsensusEventAdjustment	EventAdjustment	
DP_DemandPlanCategory	Statistical	
DP_MarginPercentCategory	ActualDemand	
DP_MarketingForecastCategory	MarketingForecast	
DP_ MarketingForecastEventCategory	MarketingForecastEvent	
DP_MarketingForecastOptimistic	MarketingForecastOptimistic	
DP_ MarketingForecastOptimisticEvent	MarketingForecastOptimisticEvent	
DP_MarketingForecastPessimistic	MarketingForecastPessimistic	
DP_ MarketingForecastPessimisticEvent	MarketingForecastPessimisticEvent	
DP_ OnTimeDeliveryToCommitCategory	ActualDemand	
DP_ OnTimeDeliveryToRequestCategory	ActualDemand	
DP_PastDueBacklogCategory	PastDue	
DP_ PromotionalAdjustmentsCategory	PromotionalAdjustments	
DP_SalesForecastCategory	SalesForecast	
DP_SalesForecastEventCategory	SalesForecastEvent	
DP_SalesForecastOptimistic	SalesForecastOptimistic	

Category type variable	Default value	Description
DP_SalesForecastOptimisticEvent	SalesForecastOptimisticEvent	
DP_SalesForecastPessimistic	SalesForecastPessimistic	
DP_SalesForecastPessimisticEvent	SalesForecastPessimisticEvent	
DP_StatisticalForecastCategory	Statistical	
DP_SupplyPlanCategory	SupplyPlan	

Target type variable	Default value	Description
DP_BacklogPercentTarget	BacklogPercentTarget	
DP_BacklogValueTarget	BacklogValueTarget	
DP_BacklogVolumeTarget	BacklogVolumeTarget	
DP_BudgetValueTarget	BudgetVolumeTarget	
DP_BudgetVolumeTarget	BudgetVolumeTarget	
DP_ConstrainedDemandUnitTarget	ConstrainedDemandUnitTarget	
DP_ConstrainedDemandValueTarget	ConstrainedDemandValueTarget	
DP_ConstraintUsageTarget	ConstraintUsageTarget	
DP_DemandPlanAPIVolumeTarget	DemandPlanAPIVolumeTarget	
DP_DemandPlanValueTarget	DemandPlanValueTarget	
DP_DemandPlanVolumeTarget	DemandPlanVolumeTarget	
DP_ExcessUnitTarget	ExcessUnitTarget	
DP_ExcessValueTarget	ExcessValueTarget	
DP_ExpiryValueTarget	ExpiryValueTarget	
DP_ExpiryVolumeTarget	ExpiryVolumeTarget	
DP_FGInventoryTarget	FGInventoryTarget	
DP_FGPeriodsofCoverageTarget	FGPeriodsofCoverageTarget	
DP_FulfillmentRateTarget	FulfillmentRateTarget	
DP_GrossMarginPercentTarget	GrossMarginPercentTarget	
DP_GrossMarginTarget	GrossMarginTarget	
DP_InventoryTurnsTarget	InventoryTurnsTarget	
DP_KeyConstraintUsageTarget	KeyConstraintUsageTarget	
DP_MarginPercentTarget	MarginPercentTarget	
DP_MarketingValueTarget	MarketingValueTarget	
DP_MarketingVolumeTarget	MarketingVolumeTarget	

Target type variable	Default value	Description
DP_ObsoleteUnitTarget	ObsoleteUnitTarget	
DP_ObsoleteValueTarget	ObsoleteValueTarget	
DP_OnTimeCommitTarget	OnTimeCommitTarget	
DP_OnTimeRequestTarget	OnTimeRequestTarget	
DP_OverloadedConstraintsTarget	OverloadedConstraintsTarget	
DP_PastDueBacklogValueTarget	PastDueBacklogValueTarget	
DP_PastDueBacklogVolumeTarget	PastDueBacklogVolumeTarget	
DP_ PeriodEndingInventoryAPIUnitTarget	PeriodEndingInventoryAPIUnitTarget	
DP_PeriodEndingInventoryUnitTarget	PeriodEndingInventoryUnitTarget	
DP_ PeriodEndingInventoryValueTarget	PeriodEndingInventoryValueTarget	
DP_PeriodsOfCoverageTarget	PeriodsOfCoverageTarget	
DP_RevenueAtRiskTarget	RevenueAtRiskTarget	
DP_RMInventoryTarget	RawMaterialInventoryTarget	
DP_RMPeriodsofCoverageTarget	RMPeriodsofCoverageTarget	
DP_SalesValueTarget	SalesValueTarget	
DP_SalesVolumeTarget	SalesVolumeTarget	
DP_SpendTarget	SpendTarget	
DP_StatisticalValueTarget	StatisticalValueTarget	
DP_StatisticalVolumeTarget	StatisticalVolumeTarget	
DP_SupplyPlanUnitTarget	SupplyPlanUnitTarget	
DP_SupplyPlanValueTarget	SupplyPlanValueTarget	
DP_UnconstrainedDemandUnitTarget	UnconstrainedDemandUnitTarget	
DP_ UnconstrainedDemandValueTarget	UnconstrainedDemandValueTarget	
DP_UnderloadedConstraintsTarget	UnderloadedConstraintsTarget	
DP_WIPInventoryTarget	WIPInventoryTarget	
DP_WIPPeriodsofCoverageTarget	WIPPeriodsofCoverageTarget	

Miscellaneous type variable	Default value	Description
DP_ AssumptionComponentsLimit	100	Variable that is used with the S&OP Assumptions workbook to limit calculations that can degrade overall system performance. If the number of part records on the FlatBillDown table that are returned exceeds this variable's setting, then an error is returned to a user.
DP_ ConsensusDemandOrderNumber	Demand Plan	Text string title that is displayed in S&OP dashboard widgets when displaying forecast details. The text can be customized.
DP_CustomerForecast	CustomerForecast	
DP_DemandTypeforConsensus	DemandPlan	Variable that must be set to a valid HistoricalDemandCategory.Value. The S&OP Write History Records workbook includes the Write Forecast Details command that will create a HistoricalDemandCategory record if it does not exist already. It is also used to define the HistoricalDemandCategory that writes the current Consensus Forecast in the HistoricalDemandSeriesDetail table. This command actually copies records from the calculated ConsensusForecast table into the HistoricalDemandSeriesDetail table using this HistoricalDemandCategory. Other resources that report the historical Demand Plan use the variable to filter out those HistoricalDemandSeriesDetail records based on their Series.Header.Category (HistoricalDemandCategory). These reporting workbooks include S&OP Backlog Reports, S&OP Consensus Demand Planning, S&OP Demand Review, S&OP Finance Review, S&OP Forecast Accuracy, and S&OP Supply Review.
DP_ExcessIntervalCalendar	Month	
DP_ExcessIntervalCount	12	
DP_GatingSuppliesLimit	150	Variable that is used with the S&OP Gating Supplies workbook to limit calculations that can degrade overall system performance. If the number of IndependentDemand and ConsensusForecast records with gating supplies that are returned exceeds this variable's setting, then an error is returned to a user.
DP_HideEventPlanning	Yes	Hides or displays the "Apply an existing event" button in the S&OP Forecast related workbooks. If this variable is set to Yes, the button is hidden. If this variable is set to No, the button is displayed.
DP_HideRangeForecasting	Yes	Hides or displays the pessimistic and optimistic forecast rows in the S&OP Forecast related workbooks. If this variable is set to No, the rows are hidden. If this variable is set to Yes, the rows are displayed.

Miscellaneous type variable	Default value	Description
DP_InventoryActuals	InventoryActuals	
DP_RevenueAtRiskIntervalCount	1	

▸Modify S&OP profile variables

1. In the **Administration** pane, under **System Settings**, click **Application Settings**.
2. Click the **Application Variables** worksheet.
3. Edit the variable that you want to modify.
4. Click **Save Data** .

S&OP data modification scheduled tasks

This section describes pre-configured data modification scheduled tasks that insert, delete, and modify S&OP data.

In On-Demand environments, these scheduled tasks are owned by the Master Administrator at Kinaxis. In On-Premises environments, these scheduled tasks are owned by the Master Administrator (Admin user).

S&OP Delete Scheduled Receipts from Supply Plan

This task uses the S&OP Delete Supply Plan workbook. It deletes the Scheduled Receipts records that were created by running the command in the Aggregate Supply Plan workbook and then resets the OrderGenerationRule on the specified PartTypes. This task modifies the S&OP Candidate scenario. It must run after the S&OP process owner starts a new S&OP cycle and before S&OP team members start modifying data.

S&OP Insert Backlog into History

This task uses the S&OP Write History Records workbook. It inserts current backlog IndependentDemand records to the HistoricalDemandActuals table.

Backlog demands satisfy the following filter:

```
(DueDate < MRPDate + 0 $DP_CycleForecastCalendar) and EffectiveDemand > 0 and
Order.Type.ProcessingRule = 'SalesActual'
```

This task modifies the S&OP Candidate scenario. It must run after the S&OP cycle ends and before the S&OP process owner publishes the S&OP plan.

S&OP Insert Demand Planning History

This task uses the S&OP Write History Records workbook. It inserts ForecastDetail records into the HistoricalDemandSeriesDetail table. This task modifies the S&OP Candidate scenario. It must run after the S&OP cycle ends but before the S&OP process owner publishes the S&OP plan.

S&OP Insert Statistical Forecast

This task uses the S&OP Statistical Forecasting (Automated) workbook. It inserts statistical forecasts into the ForecastDetail table and writes information about the statistical forecast (such as model parameters and error measures) to the ForecastItemFitOutput table. It also deletes obsolete entries from the ForecastItemFitOutput table. This task modifies the S&OP Candidate scenario. It must run after the S&OP process owner starts a new S&OP cycle and before S&OP team members start modifying data.

S&OP Insert SupplyPlan into History

This task uses the S&OP Write History Records workbook. It inserts SupplyPlan records into the ForecastDetail and HistoricalDemandSeriesDetail tables. Supply plan is reported in the S&OP Consensus Demand Planning and S&OP Supply Review workbooks. This task modifies the S&OP Candidate scenario. It must run after the S&OP cycle ends but before the S&OP process owner publishes the S&OP plan.

Configuring other application settings

You can also use the Application Variables worksheet in the Application Settings workbook to specify and modify profile variables and settings (Category, Target, and Misc.) for resources specific to other RapidResponse applications. The profile variables control settings for the following applications:

- Supply Chain Management
- Master Production Scheduling
- Inventory Management
- Distribution Requirements Planning (DRP)
- General

Supply Chain Management settings

The SCM variables are prefixed with SCM_ (for Supply Chain Management) and are Target type variables.

Target type variable	Default value	Description
SCM_ConstraintUsageTarget	SCMConstraintUsageTarget	
SCM_EndingInventoryValueTarget	SCMEndingInventoryValueTarget	
SCM_EndingInventoryVolumeTarget	SCMEndingInventoryVolumeTarget	
SCM_ObsoleteValueTarget	SCMObsoleteValueTarget	
SCM_ObsoleteVolumeTarget	SCMObsoleteVolumeTarget	
SCM_OverloadsTarget	SCMOverloadsTarget	
SCM_SpendValueTarget	SCMSpendValueTarget	

Master Production Scheduling settings

The Master Production Scheduling variables are prefixed by MPS_ (for Master Production Scheduling) and are divided into Category, Target, and Miscellaneous type variables.

Type	Variable	Default value	Description
Category	MPS_Orders	MPSOrders	
Target	MPS_ AttainmentPercentTarget	MPSAttainmentPercentTarget	
Miscellaneous	MPS_Plan	MPSSupplyPlan	

Inventory Management settings

The Inventory Management variables are prefixed by IM_ (for Inventory Management) and are divided into Category and Target type variables.

Type	Variable	Default value	Description
Category	IM_SupplyActuals	Receipt	
Target	IM_IQRTarget	InventoryQualityRatioTarget	
Target	IM_ PeriodsOfSupplyMaximumTarget	PeriodsOfSupplyMaximumTarget	
Target	IM_PeriodsOfSupplyMinimumTarget	PeriodsOfSupplyMinimumTarget	

Distribution Requirements Planning settings

The Distribution Requirements Planning variables are prefixed by DRP_ (for Distribution Requirements Planning) and are divided into Category and Target type variables.

Type	Variable	Default value	Description
Category	DRP_TransferCategory	DRPTransfer	
Target	DRP_DistributionCostValueTarget	DistributionCostValueTarget	

General settings

The General variables are prefixed by Default and are Miscellaneous type variables.

Miscellaneous type variable	Default value	Description
DefaultCriticalLimit	5	
DefaultWarningLimit	0	

▸Modify the other application settings

1. In the **Administration** pane, under **System Settings**, click **Application Settings**.
2. Click the **Application Variables** worksheet.
3. Edit the variable that you want to modify.
4. Click **Save Data** .

Configuring supporting resources

RapidResponse has workbooks that you can configure to allow you to improve your supply chain performance. Depending on the workbook, the workbook can allow you to view and analyze the capability of your supply chain, for example, or allow you to make manual adjustments (among other capabilities).

The workbooks that this section focuses on are the following:

- Data Integrity-Material workbook and metrics
- Line of Balance workbook
- Clear to Build workbook
- Attribute Rules workbook
- Kanban Manager workbook
- Allotment Overrides workbook
- Risk Opportunity Assessment workbook
- Multi-enterprise workbooks

Data Integrity - Material workbook and metrics

With the Data Integrity - Material workbook and metrics, users can verify the integrity of the enterprise source data. These resources use RapidResponse macros to define and report likely data errors. As an

administrator, you can modify certain macros so that they return results that are consistent with your operations.

Line of Balance workbooks

RapidResponse includes two versions of the Line of Balance workbook: Line of Balance - Date and Line of Balance - Unit. Both of these workbooks are shared with several predefined groups in RapidResponse. However, your company should use only one of these workbooks.

If your company uses the Model-Unit Effectivity functionality, then delete the Line of Balance - Date workbook. If not, then delete the Line of Balance - Unit workbook.

Clear to Build workbook

RapidResponse includes the Clear to Build workbook for analyzing production orders that are blocked (cannot be completed) due to supply being unavailable.

Blocked order calculations are controlled through macros and profile variables. You can view and edit these macros and profile variables within RapidResponse as discussed in "Clear to Build resources" in the *RapidResponse Analytic and Data Model Guide*.

Attribute Rules workbook

The Attribute Rules workbook supports the use of attributes in planning. This workbook is used to define the attribute rules that can get applied during supply allotment, forecast consumption, or forecast consumption calculations.

To use the Attribute Rules workbook, the following tasks should be performed (some or all of these tasks might have been performed during the RapidResponse deployment). For more information, see Attribute Rules workbook.

Kanban Manager workbook

You can use the Kanban Manager workbook with a kanban material replenishment system. You can use this workbook to view kanban data and run a kanban analysis to calculate new recommended bin quantities and sizes.

Kanban Manager calculations are controlled through profile variables and macros. You can view and edit these profile variables and macros within RapidResponse, as discussed in "Kanban Manager calculations" in the *RapidResponse Analytic and Data Model Guide*.

Note: To use the **Kanban Manager Settings** in the **Kanban Manager** workbook, you must share the **Kanban** add-in with any user that needs access to the **Kanban Manager** workbook.

Allotment Overrides workbook

You can use the Allotment Overrides workbook to manually direct quantities of limited or constrained components to specific higher-level demands and supplies. These allotment overrides will override the

default, calculated supply allotments, which are based on some combination of criteria, such as due date, order priority, and fair or equal share logic.

This workbook contains editable crosstab worksheets, so you can type an override quantity in a cell to automatically create or modify the underlying records as necessary to set up the allotment override. For example, entering a value in a crosstab cell can add new records to the AllotmentOverride and AllotmentOverrideDetail tables, and modify records in driver tables (such as IndependentDemand or ScheduledReceipt) to reference the new records.

To support this process, the Allotment Overrides workbook relies on resources such as macros, workbook commands, variables, and custom insert definitions. These resources assume that certain record values exist in your environment. These are usually set up during the initial RapidResponse deployment. However, if the required values do not exist, users will encounter difficulties using the Allotment Overrides workbook (such as being unable to view data or create allotment overrides). Therefore, if your company is using the Allotment Overrides workbook, you should complete the following tasks:

- Update the macro with valid calendars

  The RR_AllotmentOverrideDriver macro defines the groupings of end items against which you can direct components (such as customer and site). This macro includes references to Quarter and Year calendars. If your company uses a quarterly calendar that is named anything other than Quarter, or a yearly calendar that is named anything other than Year, you must update the macro expression to refer to the correct calendar names. If the macro references calendar names that do not exist in your system, users will be unable to view data in the Allotment Overrides worksheet. For more information, see "Update the AllotmentOverride macro to use valid calendar names" on page 788.

- Define an AllotmentOverrideType

  Each AllotmentOverride record must reference a valid record value in the AllotmentOverrideType control table. The values in this table define when analytic calculations use an allotment override. Therefore, you must ensure that you define at least one record in the AllotmentOverrideType table. For more information, see "Create an AllotmentOverrideType record" on page 788.

- Update workbook variables

  The Allotment Overrides workbook includes workbook variables that set the default AllotmentOverrideType value for each new AllotmentOverride record that the workbook creates. Initially, these variables reference an AllotmentOverrideType.Value of Default in the Default control set. However, if these values do not exist in your system, or are not the values that you want to associate with new AllotmentOverride records, you can modify the workbook variables. The Allotment Overrides workbook cannot create new AllotmentOverride records if the workbook variables reference a Type that is not defined in your RapidResponse environment. For more information, see "Update the workbook variables to reference a valid AllotmentOverrideType record" on page 789.

- Update the custom worksheet insert definition

  The Allotment Overrides workbook includes a custom worksheet insert definition that automatically adds new records to the AllotmentOverrideDetail table (and if necessary, the AllotmentOverride table). Initially, this insert definition assumes that any associated AllotmentOverride records that are being created reference an AllotmentOverrideType.Value of Default in the Default control set. However, if these values do not exist in your environment, or they are not the values that you want to associate with each new AllotmentOverride record, you can modify the insert definition. The Allotment Overrides workbook cannot create new AllotmentOverride records if the insert definition references a Type that is not defined in your

RapidResponse environment. For more information, see "Update the workbook insert definitions to reference a valid AllotmentOverrideType record" on page 790.

- Define appropriate filters

  The Allotment Overrides workbook has two worksheets to which you can apply filters. The Allotment Overrides worksheet includes a filter control that limits the components whose supply you can reserve against higher level groupings of demands and supplies. The Assembly Allotment Overrides worksheet includes two filter controls: one limits the components whose supply is being reserved, and the second limits the assemblies for which the components are reserved. You can define filters that return the component or assembly parts that you are interested in. These filters will also reduce worksheet processing times. For more information about creating filters, see .

Note: The Master Administrator can use the **Delete Expired Allotments** scheduled task to run or schedule a workbook command that deletes expired allotments that were made through the **Allotment Overrides** workbook. Expired allotments are the allotment override detail records that have an active quantity that is associated with independent demands that have been fulfilled or canceled. If you require access to this scheduled task, contact your Master Administrator.

▸Update the AllotmentOverride macro to use valid calendar names

1. From the **Administration** pane, under **User Accounts**, click **Macros**.

   The **Macros and Profile Variables** workbook appears.
2. Click the **Macros** worksheet.
3. Locate the record where the **Name** is **RR_AllotmentOverrideDriver**.
4. In the **Expression** column, do either of the following:
   - If your company uses a quarterly calendar named anything other than **Quarter**, change each instance of **Quarter** to refer to the applicable calendar name instead.
   - If your company uses a yearly calendar named anything other than **Year**, change each instance of **Year** to refer to the applicable calendar name instead.
5. Click **Save Data**.

Tip: The **RR_AllotmentOverrideDriver** macro is a lengthy and complex macro. To simplify editing and reduce the potential for error, copy and paste the macro **Expression** cell into a text editor for modification, and then copy and paste the modified expression back into the workbook when complete.

▸Create an AllotmentOverrideType record

1. In the **Administration** pane, under **Data**, click **Control Sets**.

   The **Control Sets** workbook appears.
2. Click the **Allotment Override Type** worksheet.
3. Click **Insert Record**.
4. In the **Insert Record** dialog box, specify the following:
   - **Control Set**—the control set to which the new record applies.
   - **Value**—a unique identifier for the new record.

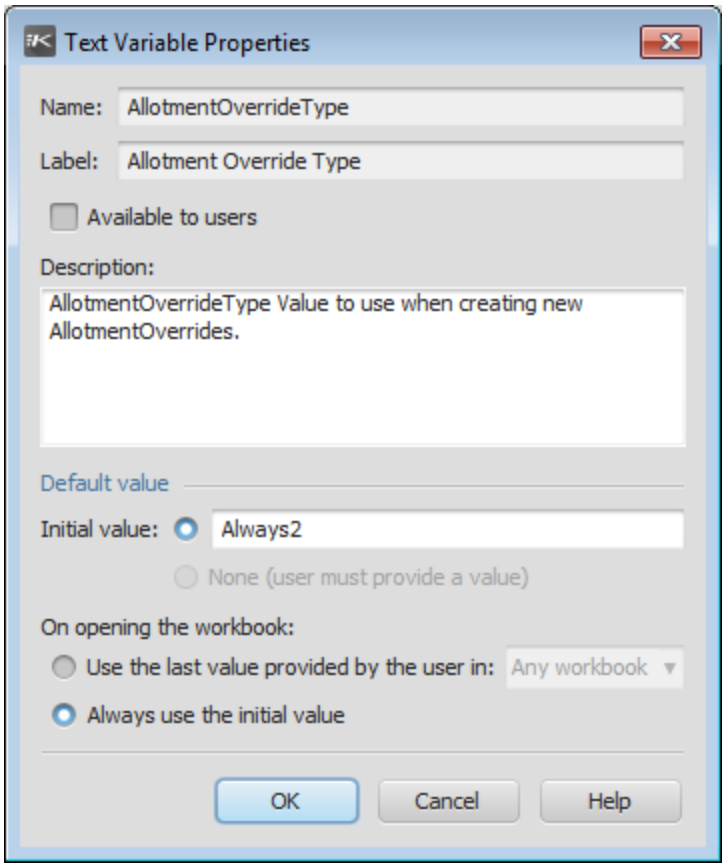
- **Description**—an optional description for the new record.
- **Processing Rule**—a rule that controls processing and effectivity for the allotment overrides that reference this record **Type**. A value of **Always** or **AfterRunDate** is required for any active allotment overrides (a setting of **Ignore** disregards any allotment overrides that reference the record).

5. Click **Save and Close**.

> **Caution:** You should add new **AllotmentOverrideType** records to a new scenario that is derived from the root scenario. When you are satisfied with the change, you can commit it back into the root scenario. You should not commit input planning data into the root scenario.

▸Update the workbook variables to reference a valid AllotmentOverrideType record

1. In the **Explorer**, ensure that workbooks are shown by selecting **Reports**.
2. Right-click the **Allotment Overrides** workbook, and then click **Properties**.
3. Click the **Variables** tab, and then do the following:
   - Select the **AllotmentOverrideType** variable, and then click **Edit**.
   - In the **Initial value** box, type the value that you want from the **AllotmentOverrideType.Value** field, as shown in the following illustration.



   - Click **OK**.
   - Select the **AllotmentOverrideTypeControlSet** variable, and then click **Edit**.

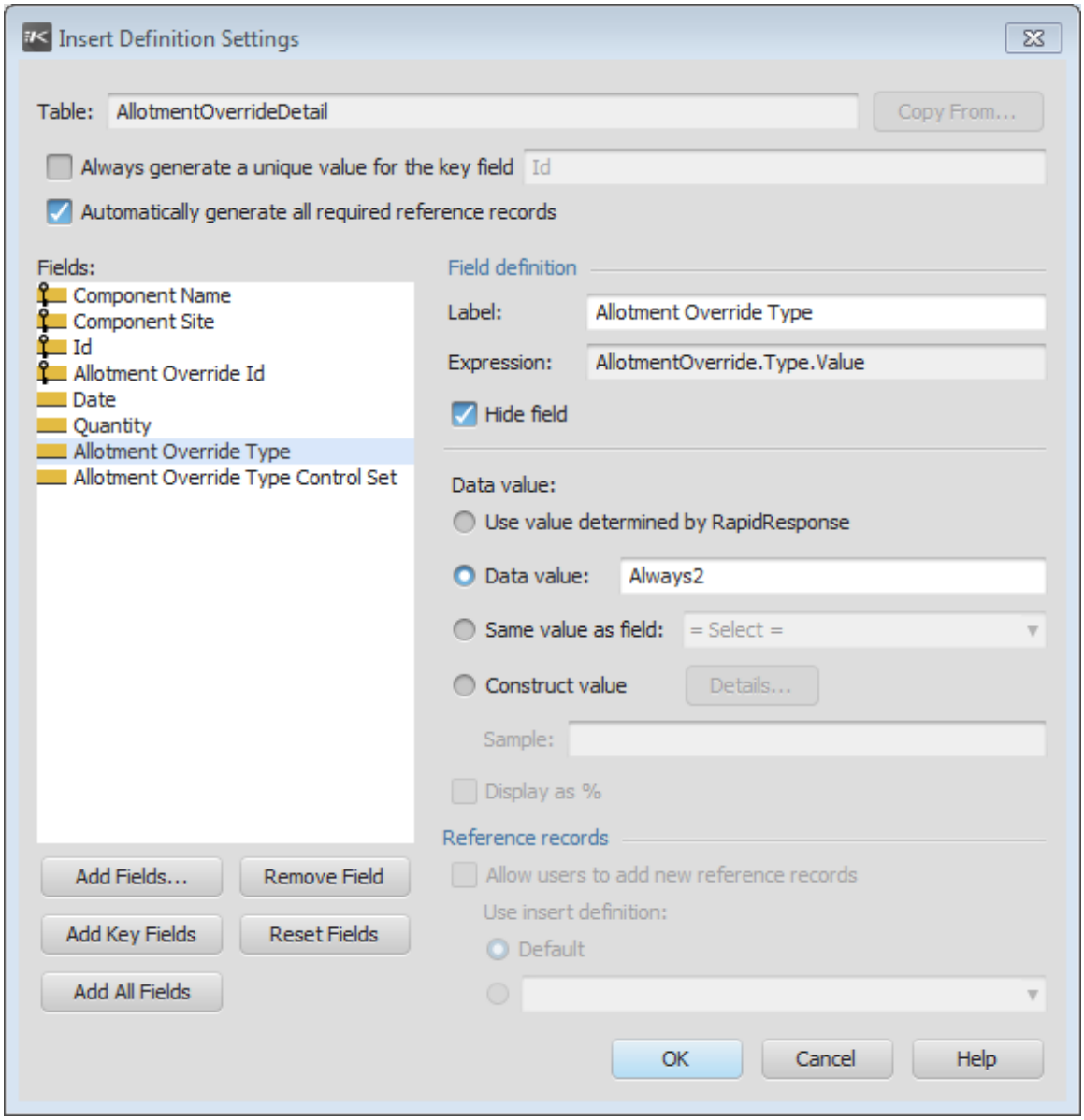
- In the **Initial value** box, type the name of the control set that is associated with the **AllotmentOverrideType** value that you specified.
- Click **OK**.

4. Click **OK** to close the **Workbook Properties** dialog box.

▸Update the workbook insert definitions to reference a valid AllotmentOverrideType record

1. In the **Explorer**, ensure that workbooks are shown by selecting **Reports**.
2. Right-click the **Allotment Overrides** workbook, and then click **Properties**.
3. Click the **Worksheets** tab.
4. Select the **1.1 SRC Editable Allotment Override Detail** worksheet, and then click **Properties**.
5. On the **Group** tab, in the table, click the **Quantity** row.
   The **Data Editing** button becomes available.
6. Click **Data Editing**.
7. Click the **New Records** tab.
8. In the **Field value definitions** section, click **Custom insert definition**, and then click **Settings**.
9. In the **Insert Definition Settings** dialog box, do the following:
   - In the **Fields** list, click **Allotment Override Type**.
   - In the **Data value** box of the **Data Value** area, type the value that you want from the

AllotmentOverrideType.Value field, as shown in the following illustration.



- In the **Fields** list, click **Allotment Override Type Control Set**.
- In the **Data value** box of the **Data value** area, type the name of the control set that is associated with the new **AllotmentOverride.Type.ControlSet.Value** default value.

10. Click **OK** three times.
11. On the **Workbook Properties** dialog box, select the **1.8 Edit PS Allotment Override Detail** worksheet, and then click **Properties**.
12. Repeat steps 5 to 10 for this worksheet.
13. Click **OK** three times.

Risk/Opportunity Assessment workbook

You can use the Risk/Opportunity Assessment workbook to improve supply chain performance, reduce inventory, and increase on-time delivery.

Here you can review a summary of your supply chain performance in the following key categories:

- Orders at Risk—orders and forecasts that are at risk of shipping late.
- Excess and Obsolete—information about excess and obsolete supply.
- Prioritized ERP Actions—actions that are recommended by your enterprise data system in a prioritized order and simple format.

For each category, you can view information for the baseline scenario, or you can click Show Changes and see how the baseline scenario compares to another scenario.

To see detailed data, click the links in the Supply Chain Performance Categories column. This opens worksheets where the detailed data is displayed. You will notice that many of the worksheets you access contain data values that are also links that can take you to additional information.

Multi-enterprise workbooks

Brand owners can use the Multi-Enterprise Inventory and Multi-Enterprise Management workbooks to view and coordinate supply information from their suppliers across multiple sites.

Multi-enterprise inventory and management calculations are controlled through macros. You can view and edit these macros within RapidResponse, as discussed in "Multi-enterprise resources" in the *RapidResponse Analytic and Data Model Guide*.

Inventory Analysis workbook

You can configure buckets for Inventory Analysis tables. For example, you can set the date buckets, specify the number of date buckets generated before and after the MRPDate, and also specify Inventory Analysis buckets that are specific to a workbook. For more information, see the "Configuring buckets for Inventory Analysis tables" section in the *RapidResponse Analytic and Data Model Guide*.

Configuring Self-Healing Supply Chain resources

A machine learning service is deployed for the RapidResponse Self-Healing Supply Chain. The Self-Healing Supply Chain is available only for the RapidResponse On-Demand service and is configured by your deployment team during the initial setup.

The following assumptions are made after the initial deployment of the machine learning service:

- RapidResponse is installed and is running on version 2016.2 Service Update 21 or later.
  (If the Self-Healing Supply Chain will also be used to heal Yield parameters, RapidResponse must be running on version G1903 or later)
- The machine learning service is deployed and running in the RapidResponse Data Center.

- The resource package for the Self-Healing Supply Chain is installed and all predefined resources are available.
- The SelfHealingSupplyChain license key is inserted.

> **Note:** The **SelfHealingSupplyChain** license key is required to enable Self-Healing Supply Chain functionality. To verify whether the **SelfHealingSupplyChain** license key exists in RapidResponse, in the **Administration** pane, under **System Settings**, click **Licenses** and then click **License Keys**. If the **SelfHealingSupplyChain** license key is not present, contact Kinaxis Customer Support.

This section provides information on the resources and settings that need to be configured to use the Self-Healing Supply Chain once the machine learning service is deployed. For example, as a RapidResponse administrator you can specify and modify Self-Healing Supply Chain profile variables. You can also configure the frequency of the Self-Healing Common scheduled task that creates the Self-Healing Upload scenario (if it does not exist) to populate the ItemSource table with Historical Supply Actual and Historical Receipt data, and also triggers the machine learning service to retrieve the Historical Supply Actual and Historical Receipt data to forecast new lead times and yields.

Self-Healing Supply Chain scenario structure

The RapidResponse Self-Healing Supply Chain process requires a specific scenario setup with the following scenarios:

- Self-Healing Current Plan
  - Self-Healing Load
    - Self-Healing Upload
    - As Designed by Self-Healing
    - As Demonstrated by Self-Healing
    - Self-Healing Working Plan

This scenario structure is typically a child of the Approved Actions scenario. The Self-Healing Load and the Self-Healing Upload scenarios are used for receiving data from and sending data to the machine learning server via web services and should not be made visible to users.

The scenarios have the following properties:

Scenario	Properties	Purpose
Self-Healing Current Plan	• Permanent • Typically a child of Approved Actions. **Note:** The parent scenario for Self-Healing Current Plan can be changed to a different scenario than Approved Actions.	Shows updated Time Phased Part Source Lead Time records from the Self-Healing Working Plan scenario for accepted lead time corrections. Also shows updated Time Phased Yield records from the Self-Healing Working Plan scenario for accepted yield corrections.
Self-Healing Load	• Only visible to the MLServiceUser • Permanent	• Sends and receives data to and from the machine learning server. • Loads the projected parameter data from the Self-Healing Upload scenario into the As Designed by Self-Healing, the As Demonstrated by Self-Healing, and the Self-Healing Working Plan scenarios.
Self-Healing Upload	• Child of Self-Healing Load • Private • Not visible • Not permanent	• Receives projected parameter results from the machine learning server and commits them to the Self-Healing Load scenario. • Is created by the Run Self-Healing scheduled task (if it does not already exist).
As Designed by Self-Healing	• Child of Self-Healing Load • Automatically updated • Permanent • Shared with ML Self-Healing Users group	Shows historical parameter actuals and the impact of ignoring all corrections recommended by the machine learning server.
As Demonstrated by Self-Healing	• Child of Self-Healing Load • Automatically updated • Permanent • Shared with ML Self-Healing Users group	Shows projected parameters and the impact of accepting all corrections recommended by the machine learning server.
Self-Healing Working Plan	• Child of Self-Healing Load • Automatically updated • Permanent • Shared with ML Self-Healing Users group • Editable	• Shows data from the Self-Healing Current Plan scenario with any parameters that are automatically corrected, as determined by the Automated Lead Time Type and Automated Yield Type settings. • Used for accepting or rejecting the corrections recommended by the machine learning server. • Accepted lead time corrections for ItemSource records are copied to the Time Phased Part Source Lead Time table and then committed to the Self-Healing Current Plan scenario, and optionally, also to its parent scenario. • Accepted yield corrections for ItemSource records are copied to the Time Phased Yield table and then committed to the Self-Healing Current Plan scenario, and optionally, also to its parent scenario.

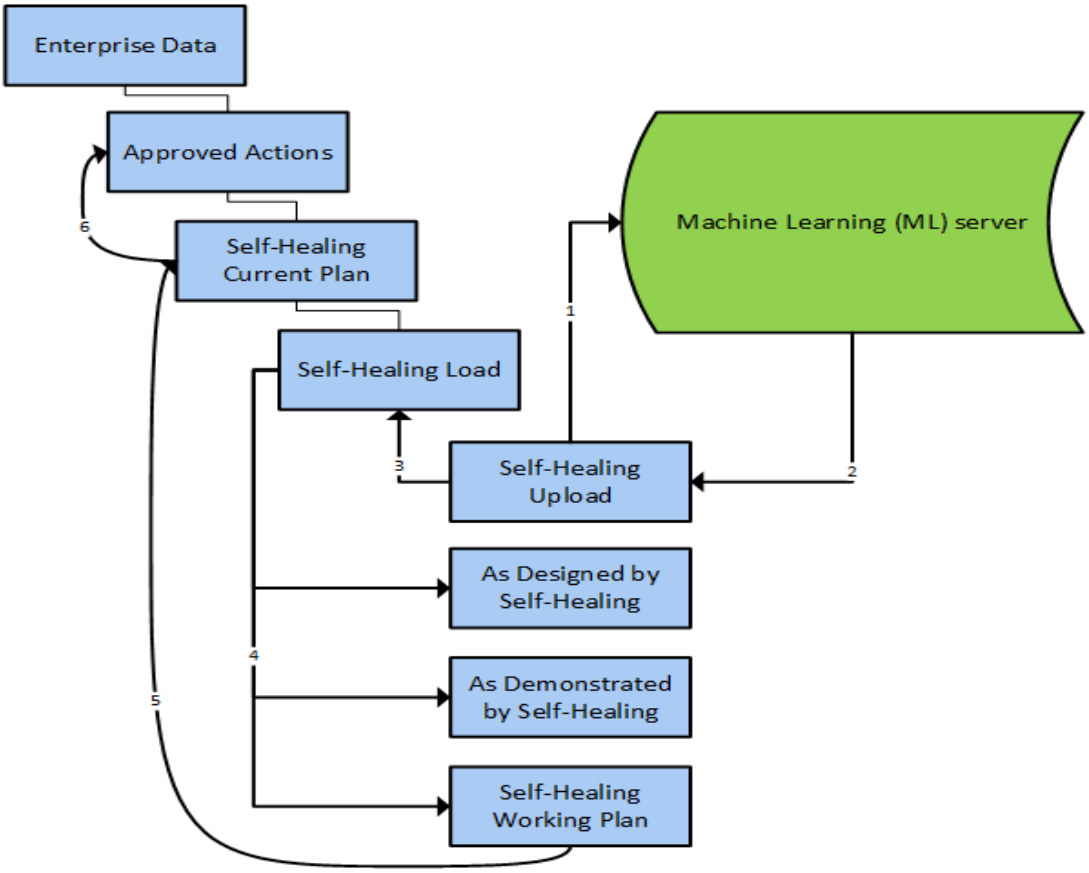
If the scenarios listed in the table above are not permanent, do the following:

1. In the **Scenarios** pane, right-click on the scenario name and select **Properties**.
2. On the **General** tab, select the **Permanent** check box.
3. Click **Save Data**.

Notes:

- These scenarios are typically configured by your deployment team during the initial setup of the Self-Healing Supply Chain.
- The ML Service User script creates the Self-Healing Current Plan, the Self-Healing Load, the As Designed by Self-Healing, the As Demonstrated by Self-Healing, and the Self-Healing Working Plan scenarios (if they do not already exist) and shares them with both the MLServiceUser and the ML Self-Healing Users group. If the scenarios already exist, the ML Service User script verifies that the correct parent scenarios are set-up. For more information, see "Self-Healing Supply Chain users and groups" on page 801.

The Self-Healing Supply Chain process is described in more detail with the scenario structure below.



1. The Run Self-Healing scheduled task runs the Trigger ML Service script that creates the Self-Healing Upload scenario based on the Self-Healing Load scenario (if it doesn't already exist), and populates the ItemSource table with Historical Supply Actual (HSA) and Historical Receipt (HR) data. If there is at least one valid record in the ItemSource table that is not set to Ignore, the

script then triggers the machine learning service to retrieve the parameter data (HSA and/or HR) from the Self-Healing Upload scenario in RapidResponse.

2. Once the machine learning server calculates the results for the projected parameters, the cluster, and the cluster properties, the parameter data is uploaded into the Self-Healing Upload scenario.
3. The parameter data in the Self-Healing Upload scenario is then committed to the Self-Healing Load scenario.
4. Based on the parameter data in the Self-Healing Load scenario and on the AutomatedLeadTimeType abd AutomatedYieldType settings, scheduled processes in the Self-Healing Common, Self-Healing Lead Time, and Self-Healing Yield automation chains automatically update parameter data in the As Designed by Self-Healing, As Demonstrated by Self-Healing, and Self-Healing Working Plan scenarios for planners to analyze in the Self-Healing Lead Time and Self-Healing Yield Impact Analysis dashboards.
   - Once planners have reviewed the parameter data in the Lead Time Healing or Yield Correction workbooks, the Correct Accepted Lead Times or Correct Accepted Yields command copies the accepted parameter values to the current scenario that is either the Self-Healing Working Plan scenario or a private child scenario of Self-Healing Working Plan.
5. Accepted parameter values are then committed from the current scenario that is either the Self-Healing Working Plan scenario or a private child scenario of Self-Healing Working Plan, to the Self-Healing Current Plan scenario.
6. Optionally, based on the setting for Commit To Parent Scenario in the SHSCConfiguration control table, accepted parameter values are also committed to the parent of the Self-Healing Current Plan scenario (whether it is the Approved Actions scenario or a different scenario).

For more information about the automated processes mentioned above, see "Self-Healing Supply Chain automation tasks" on page 798.

Self-Healing Supply Chain control fields

You can use the SHSCConfiguration Table worksheet in the Control Tables workbook to specify control settings for the Self-Healing Supply Chain resources.

Field name	Data type	Default value	Description
CommitToParentScenario	Boolean	Yes	Determines whether changes in the SH Working Plan scenario are committed to the parent scenario of Self-Healing Current Plan or not. **Notes:** • The Self-Healing Current Plan and the Approved Actions scenarios are hard-coded into the Commit Lead Time Corrections form. If the parent scenario for Self-Healing Current Plan is set to a different scenario than Approved Actions, then the Approved Actions scenario should be changed to the parent scenario that is used instead. • Similarly, if the parent scenario for Self-Healing Current Plan is set to a different scenario than Approved Actions, then the scenario in the Auto Heal Lead Times – Approved Actions scheduled task that is part of the Self-Healing Lead Time automation chain should also be changed to point to the parent scenario that is used instead.
Lead Time - HistoricalHorizon	Integer	24	Determines how many historical periods to include in analysis for Lead Time. For example, how many months of historical data will be included.
Lead Time - Calendar	Reference	Months	Determines what calendar periods to use to define the history. For example, measure the HistoricalHorizon by months.
Yield - Future Horizon	Integer	26	Determines how many future periods to predict for Yield. For example, how many weeks of yield will be predicted.
Yield - HistoricalHorizon	Integer	156	Determines how many historical periods to include in analysis for Yield. For example, how many weeks of historical data will be included.
Yield - Calendar	Reference	Weeks	Determines what calendar periods to use to define the history. For example, measure the HistoricalHorizon by months.
LeadTimeType	Reference	Auto	When running the machine learning service for the first time, the lead time type value set here will be used for all Item Source records as the default value for **AutomatedLeadTimeType**. **Note:** After the first run of the machine learning service, you can assign different **AutomatedLeadTimeType**records to **ItemSource** records. To change the AutomatedLeadTimeType for an ItemSource, use the **Item Source** worksheet in the **Self-Healing Data**workbook. **Tip:** The AutomatedLeadTimeType record should be created first in the **Automated Lead Time Type** worksheet of the **Control Tables**workbook. For more information, see the *RapidResponse Analytic and Data Model Guide*.

Field name	Data type	Default value	Description
YieldType	Reference	Auto	When running the machine learning service for the first time, the yield type value set here will be used for all Item Source records as the default value for **AutomatedYieldType**. **Note:** After the first run of the machine learning service, you can assign different **AutomatedYieldType**records to **ItemSource** records. To change the AutomatedYieldType for an ItemSource, use the **Item Source** worksheet in the **Self-Healing Data**workbook. **Tip:** The AutomatedYieldType record should be created first in the **Automated Yield Type** worksheet of the **Control Tables**workbook. For more information, see the *RapidResponse Analytic and Data Model Guide*.
NewSupplyStatus - ControlSet	Reference	Default	
NewSupplyStatus - Value	Reference	Ignore	Displays the default Order Status to use for disabling Scheduled Receipt records for the Self-Healing Supply Chain. **Tip:** This field should point to a record where **SupplyStatus.IgnoreSupply** = 'Y'.
OrderPolicy - ControlSet	Reference	Default	
OrderPolicy - Value	Reference		Displays the default Order Policy to use for disabling Part Source records for the Self-Healing Supply Chain. **Tip:** This field should point to a record where **OrderPolicy.OrderGenerationRule** = 'NoOrders', **UseFixedLeadTime** = 'Y', **OrderPolicy.YieldUsage** ≠ 'Ignore', and **OrderPolicy.YieldUsage** ≠ 'ScrapPiece'.

Self-Healing Supply Chain automation tasks

This section describes pre-configured automation tasks that insert, delete, and modify self-healing supply chain data in the Self-Healing Load, SH Current Performance, SH Suggested Plan, and Self-Healing Working Plan scenarios.

The following automation tasks are described in this section:

- "Run Self-Healing scheduled task" on page 799
- "Self-Healing Common automation chain" on page 799
- "Self-Healing Lead Time automation chain" on page 800
- "Self-Healing Yield automation chain" on page 800

Run Self-Healing scheduled task

This task uses the Self-Healing Script workbook. It builds the Self-Healing Upload scenario (if it does not exist), which populates the ItemSource table with Historical Supply Actual (HSA) and Historical Receipt (HR) data and triggers the machine learning service to retrieve the HSA and HR data from RapidResponse. The machine learning service will run based on the frequency that is configured for this scheduled task.

To configure the frequency of the Run Self-Healing scheduled task, do the following:

1. In the **Explorer**, select the **Run Self-Healing** scheduled task.
2. Right-click on the scheduled task name and select **Properties**.
3. On the General tab of the **Scheduled Task Properties – Run Script** dialog box, make sure the scheduled task is **Enabled**.
4. Click the **Frequency** tab.
5. Select **Every**, and then select one of the following values from the list:
   - **Weekly**—The Machine Learning service runs every week. This is the recommended maximum frequency.
   - **Monthly**—The Machine Learning service runs every month. This is the recommended default setting.
   - **Quarterly**—The Machine Learning service runs every quarter.
6. Select a **Time**.
7. Select the check box to ensure that the task must finish before it can be run again.
8. Click **OK**.

Self-Healing Common automation chain

When the Cluster and Forecast results of a machine learning run are returned to RapidResponse, the Trigger Self-Healing script runs the Self-Healing Common automation chain, which in turn runs the Self-Healing Lead Time and Self-Healing Yield automation chain. At a high level, the Self-Healing Common automation chain does the following:

- Updates the Self-Healing Load scenario (so that the scenario has the latest planning data).
- Commits the Self-Healing Load scenario (so that the ML results are in Self-Healing Current Plan).
- Resets the three Self-Healing Supply Chain scenarios (As Designed by Self-Healing, As Demonstrated by Self-Healing, and Self-Healing Working Plan) with the latest results from the Machine Learning server.
- Runs the Self-Healing Lead Time automation chain
- Runs the Self-Healing Yield automation chain
- Disables Planning for lead time and yields in As Designed by Self-Healing and Self-Healing Working Plan scenarios
- Sends the alerts for both lead time and yields

Note: The Self-Healing Common automation chain is owned by the Master Administrator and is run by the MLServiceUser.

For more information about the MLServiceUser and ML Self-Healing Users group, see "Self-Healing Supply Chain users and groups" on page 801.

Self-Healing Lead Time automation chain

This automation chain runs scheduled tasks that build the data in the Self-Healing Lead Time scenarios used to analyze the projected impact of the lead time deviations (As Designed by Self-Healing, As Demonstrated by Self-Healing, and Self-Healing Working Plan), corrects the lead times in the Self-Healing Working Plan scenario for parts that are configured to be automatically healed, and notifies the ML Self-Healing Users that the Machine Learning jobs for the Self-Healing Lead Time are completed.

The following lists the high-level steps that are part of the Self-Healing Lead Time automation chain:

- Copies all projected lead times to the TimePhasedPartSourceLeadTime table in the As Demonstrated by Self-Healing scenario.
- Creates new Scheduled Receipts, reschedules existing Scheduled Receipts and disables all planning in the As Designed by Self-Healing scenario
- Creates new Scheduled Receipts and disables planning for non-corrected item sources in the Self-Healing Working Plan scenarios.
- Accepts and commits projected lead times for ItemSource records set to "AutoAccept" in the Self-Healing Working Plan scenario.

Note: The Self-Healing Lead Time automation chain is owned by the Master Administrator and is run by the MLServiceUser.

For more information about the MLServiceUser and ML Self-Healing Users group, see "Self-Healing Supply Chain users and groups" on page 801.

Self-Healing Yield automation chain

The Self-Healing Yield automation chain runs the following tasks for evaluating Self-Healing Yield results:

- Auto Heal Yields in the Self-Healing Working Plan scenario
- Auto Heal Yields in the Self-Healing Current Plan scenario
- Auto Heal Yields in the Approved Actions scenario
- Copies all ProjectedYield records to the TimePhasedYield table in the As Demonstrated by Self-Healing scenario
- Converts existing planned orders in the As Designed by Self-Healing scenario to scheduled receipts, applying the new forecasted yields
- Converts existing planned orders in the Self-Healing Working Plan scenario to scheduled receipts, applying the new forecasted yields

- Modifies existing scheduled receipts in the As Designed by Self-Healing scenario, applying the new forecasted yields.
- Modifies existing scheduled receipts in the Self-Healing Working Plan scenario, applying the new forecasted yields.

Note: The Self-Healing Yield automation chain is owned by the Master Administrator and is run by the MLServiceUser.

For more information about the MLServiceUser and ML Self-Healing Users group, see "Self-Healing Supply Chain users and groups" on page 801.

Self-Healing Supply Chain users and groups

To use the Self-Healing Supply Chain, the following users and groups are required:

- "MLServiceUser " on page 801
- "ML Self-Healing Users group" on page 803

The Self-Healing Supply Chain users and groups are typically configured by your deployment team during the initial setup.

MLServiceUser

The MLServiceUser is a web service user account that has permissions to access web services such as the machine learning service, and has external query access. Thus, the MLServiceUser is the owner of the scheduled tasks and the alert that are listed in the Resources table below.

For the Self-Healing Supply Chain, when the Run Self-Healing scheduled task runs it generates a request for an authentication token from the RapidResponse data server to allow the machine learning service to retrieve and update data in RapidResponse via the Web Service API. For more information about users with web service permissions or token based authentication, see the *RapidResponse Web Services Guide*.

Resources

The MLServiceUser should have the following resources:

Resource name	Resource type	Permission
Self-Healing Common	Automation Chain	Author
Self-Healing Lead Time	Automation Chain	Author
Self-Healing Yield	Automation Chain	Author
Self-Healing Data	Workbook	Author
Self-Healing Script	Workbook	Author
Commit Lead Time Corrections	Form	Link

Resource name	Resource type	Permission
Commit Yield Corrections	Form	Link
Insert Lead Time Override	Form	Link
Insert Yield Override	Form	Link
Lead Time Healing	Workbook	Link
Yield Correction	Workbook	Link
Self-Healing Lead Time Alert	Alert	Manage
Self-Healing Yield Alert	Alert	Manage
Auto Heal Lead Times	Scheduled Task	Manage
Auto Heal Lead Times - Approved Actions	Scheduled Task	Manage
Auto Heal Lead Times - Self-Healing Current Plan	Scheduled Task	Manage
Auto Heal Yields - Approved Actions	Scheduled Task	Manage
Auto Heal Yields - Self-Healing Current Plan	Scheduled Task	Manage
Auto Heal Yields - Self-Healing Working Plan	Scheduled Task	Manage
Copy All Lead Times	Scheduled Task	Manage
Copy All Yields	Scheduled Task	Manage
Create New Scheduled Receipts (Lead Time) - As Designed by Self-Healing	Scheduled Task	Manage
Create New Scheduled Receipts (Lead Time) - Self-Healing Working Plan	Scheduled Task	Manage
Create New Scheduled Receipts (Yields) - As Designed by Self-Healing	Scheduled Task	Manage
Create New Scheduled Receipts (Yields) - Self-Healing Working Plan	Scheduled Task	Manage
Disable Planning - All	Scheduled Task	Manage
Disable Planning - Not Accepted	Scheduled Task	Manage
Disable Planning for Yields - As Designed by Self-Healing	Scheduled Task	Manage
Disable Planning for Yields - Self-Healing Working Plan	Scheduled Task	Manage
Modify Existing Scheduled Receipts for Yields - As Designed by Self-Healing	Scheduled Task	Manage
Modify Existing Scheduled Receipts for Yields - Self-Healing Working PLan	Scheduled Task	Manage
Reschedule Existing Scheduled Receipts - As Designed by Self-Healing	Scheduled Task	Manage
Run Self-Healing	Scheduled Task	Manage
Trigger ML Service	Script	Manage
Trigger Self-Healing	Script	Manage
Approved Actions	Scenario	Modify
Self-Healing Load	Scenario	Modify

Resource name	Resource type	Permission
As Designed by Self-Healing	Scenario	Modify
Self-Healing Current Plan	Scenario	Modify
As Demonstrated by Self-Healing	Scenario	Modify
Self-Healing Working Plan	Scenario	Modify
All Parts	Filter	Use
Enterprise Data	Scenario	View
All sites	Site	View

Permissions

In addition, the MLServiceUser should have the following permissions:

- Create scenarios and share scenarios owned by user.
- Author alerts and scheduled tasks.
- Edit data in shared scenarios.
- Use web services and external query access.
- Access to Start page.

Note: The ML Service User script is used to create the MLServiceUser with the resources and permissions listed above, and also shares the Self-Healing Current Plan, the Self-Healing Load, the As Designed by Self-Healing, the As Demonstrated by Self-Healing, and the Self-Healing Working Plan scenarios with the ML Self-Healing Users group.

To create the MLServiceUser

If the MLServiceUser is not already created, do the following:

1. In the **Explorer**, select the **ML Service User** script.
2. Right-click on the script name and select **Run Now**.
3. Click **OK**.

The MLServiceUser user account is created with the required resources and permissions. To verify that the user has been created, you can use the **Users and Groups** workbook in the **Administration** pane.

For more information, see" Managing users" on page 569.

ML Self-Healing Users group

The ML Self-Healing Users group is for planners who receive the Self-Healing Lead Time Alert once the Cluster and Forecast results are returned from the machine learning service, and are responsible to analyze and heal the lead time deviations that are detected as part of the Self-Healing Supply Chain process.

The ML Self-Healing Users group is typically created by your deployment team during the initial setup. However, as a RapidResponse administrator, you must add the required planners to the group and assign the required resources and permissions.

Note: The Self-Healing Current Plan, the Self-Healing Load, the As Designed by Self-Healing, the As Demonstrated by Self-Healing, and the Self-Healing Working Plan scenarios are automatically created and shared with the ML Self-Healing Users group via the ML Service User script.

For more information, see "Managing groups" on page 565.

Resources

The ML Self-Healing Users group should have the following resources:

Resource name	Resource type	Permission
Commit Lead Time Corrections	Form	Link
Commit Yield Corrections	Form	Link
Create Automated Lead Time Type	Form	Link
Create Automated Yield Type	Form	Link
Create Forecast Horizon	Form	Link
Create Historical Demand Category Rolling Weight	Form	Link
Delete Forecast Horizon	Form	Link
Delete Historical Demand Category Rolling Weight	Form	Link
Insert Lead Time Override	Form	Link
Insert Yield Override	Form	Link
Control Tables	Workbook	Link
DP Script Resources	Workbook	Link
Part Properties	Workbook	Link
As Designed by Self-Healing	Scenario	Modify
Self-Healing Current Plan	Scenario	Modify
As Demonstrated by Self-Healing	Scenario	Modify
Self-Healing Working Plan	Scenario	Modify
Self-Healing Lead Time	Dashboard	Open
Self-Healing Yield Impact Analysis	Dashboard	Open
Analyze lead time deviations	Task Flow	Open
Heal lead time deviations	Task Flow	Open
Data Integrity - Self-Healing Supply Chain	Workbook	Open
Lead Time Deviation Treemap	Workbook	Open

Resource name	Resource type	Permission
Lead Time Healing	Workbook	Open
Yield Correction	Workbook	Open
Manual Closed Loop Self-Healing Lead Time	Workbook	Open
Manual Closed Loop Self-Healing Yield	Workbook	Open
Self-Healing Data	Workbook	Open
Self-Healing Job Status	Workbook	Open
Self-Healing Widgets	Workbook	Open
Self-Healing Widgets - Single Scenario	Workbook	Open
Self-Healing Script	Workbook	Open
Baseline	Scenario	View
Enterprise Data	Scenario	View
Self-Healing Lead Time - Late Revenue by Tolerance Category	Widget	View
Self-Healing Lead Time - Part Count by Tolerance Category	Widget	View
Self-Healing Lead Time - Projected Inventory by Tolerance Category	Widget	View
Self-Healing Lead Time - Projected Inventory Cost	Widget	View
Self-Healing Lead Time - Projected Late Revenue	Widget	View

Permissions

In addition, the ML Self-Healing Users group should have the following permissions:

- Create scenarios and share scenarios owned by user.
- Edit data in shared scenarios, and warn before editing.
- Access to Message Center and Start page.

CHAPTER 50: Predefined resource and tool settings

Model, unit, and pool information 807
Attribute Rules workbook 807

RapidResponse includes predefined resources and tools designed to help your organization respond to a variety of business challenges. You can change resource settings to better meet the needs of RapidResponse users.

Note: For information about retrieving copies of predefined workbooks, see "Retrieving predefined workbooks" on page 751.

Model, unit, and pool information

Each worksheet that can show model, unit, and pool information contains hidden Model, Unit, and Pool columns. If you have enabled the Model-Unit Effectivity or Pool functionality, you must modify the workbooks included with RapidResponse to show the Model, Unit, and Pool columns in worksheets. For more information about modifying worksheets, see "Worksheet authoring" in the *RapidResponse Resource Authoring Guide*.

Attribute Rules workbook

The Attribute Rules workbook is included with RapidResponse to support the use of attributes in planning. This workbook is used to define the attribute-rules that can get applied during supply allotment, forecast consumption, and/or forecast consumption calculations.

In order to enable use of the Attribute Rules workbook, the following tasks should typically be performed (some or all of these tasks may have already been performed by a Kinaxis consultant during a RapidResponse deployment).

Share the Attribute Rules workbook

By default, this workbook is only shared to members of the Data Administrators group. However, members of this group can share it with other groups or users as required.

▸**Share the Attribute Rules workbook**

1. In the **Explorer**, ensure that workbooks are shown by selecting **Reports**.
2. Right-click the **Attribute Rules** workbook, and then click **Share**.
3. Click **Select Names**, and in the **Select Names** dialog box, do the following:
   - On the **Groups** tab, select any groups that you want to share the workbook to, and then click **Share with**.
   - On the **Users** tab, select any individual users that you want to share the workbook to, and then click **Share with**.
4. Click **OK**, and then **OK** again.

Define the required control table settings

Each new record added through the Attribute Rules workbook has a reference to the **AttributeMapType** table. Values in this control table determine where the attribute rules that reference it are applicable. Based on three separate control settings in this table, each **AttributeMapType** record can be used to enable attribute rules in any combination of the supply allotment, forecast consumption, and forecast adjustment calculations. For more information, see Create an AttributeMapType record.

Additionally, the **AttributeRule** setting in the **MUEPoolNettingType** table controls whether a given part is eligible for use in attribute calculations (regardless of any attribute rules defined for its demands and/or supplies). Therefore, you should ensure that all parts expected to use attribute-based planning reference a **MUEPoolNettingType.AttributeRule** field value of "Net". For more information, see Allow attribute-based planning at the part level.

Note: For complete reference information about the **AttributeMapType** and **MUEPoolNettingType** tables, see the *RapidResponse Analytic and Data Model Guide*

▸ **Create an AttributeMapType record**

Caution: You should add new **AttributeMapType** records to a new scenario that is derived from the root scenario. When you are satisfied with the change, you should commit it back into the root scenario. You should not commit input planning data into the root scenario

1. In the **Explorer**, ensure that workbooks are shown by selecting **Reports**.
2. Double-click the **Control Tables** workbook.
3. Click the **Attribute Map Type** worksheet.
4. Click **Insert Record**, and then do the following:
   - In the **Value** box, type a unique identifier for the new record.
   - In the **Description** box, type an optional description for the new record.
   - From the **Forecast Adjustment** list, select **Y** (yes) if this type should use attribute rules to apply adjustments to forecast details, and **N** (no) if it should not.
   - From the **Forecast Consumption** list, select **Y** (yes) if this type should use attribute rules when actual demands consume forecasts, and **N** (no) if it should not.
   - From the **Supply Selection** list, select **Y** (yes) if this type should use attribute rules to allot supply to demand, and **N** (no) if it should not.

5. Click **Save and Close**.

▸Allow attribute-based planning at the part level

> **Caution:** You should add or modify **MUEPoolNettingType** records in a new scenario that is derived from the root scenario. When you are satisfied with the change, commit it back into the root scenario. You should not commit input planning data into the root scenario.

1. In the **Explorer**, ensure that workbooks are shown by selecting **Reports**.
2. Double-click the **Control Tables** workbook.
3. Click the **MUE Pool Netting Type** worksheet.
4. If you want existing **MUEPoolNEttingType** records to be able to use attribute-based planning on the parts that reference them, ensure that their **Attribute Rule** column value is set to **Net**.
5. To define a new **MUEPoolNettingType** record, click **Insert Record**, and then specify the following:
   - From the **Control Set** list, select the control set to which the new record applies.
   - In the **Value** box, type a unique identifier for the new record.
   - From the **Attribute Flow To Common** list, select one of the following rules:
     - **Forecast**—when selected for attribute-based forecast consumption, actual demands for parts of this type will first consume from forecasts with matching attribute rules, and then the remaining demand will consume from the common (blank) pool.
     - **Ignore**—when selected for attribute-based forecast consumption, actual demands for parts of this type will only consume from forecasts with matching attribute rules.
   - From the **Attribute Rule** list, select one of the following rules:
     - **Ignore**—attribute-based planning cannot be used for any parts that use this type and any parts below them in a product structure. Use this value for parts that are not expected to use attribute-based planning or that are not required to pass attribute values to lower-level components.
     - **Net**—attribute-based planning can be used for parts that use this type. Use this value for parts that are expected to require attribute-based planning or to propagate attribute-based planning logic to lower-level parts in a product structure (for example, to dependent components where attributes are relevant in the supply allotment process).
   - In the **Description** box, type an optional description for the new record.
   - From the other lists, select rules to set standard usage. For more information about the settings in the **MUEPoolNettingType** table, see the *RapidResponse Data Model and Analytic Guide*.
6. To define a new **MUEPoolNettingType** record, click **Insert Record**, and then specify the following:
   - From the **Control Set** list, select the control set to which the new record applies.
   - In the **Value** box, type a unique identifier for the new record.
   - From the **Attribute Flow To Common** list, select one of the following rules:
     - **Forecast**—when selected for attribute-based forecast consumption, actual demands for parts of this type will first consume from forecasts with matching attribute rules, and then the remaining demand will consume from the common (blank) pool.
     - **Ignore**—when selected for attribute-based forecast consumption, actual demands for parts of this type will only consume from forecasts with matching attribute rules.

- From the **Attribute Rule** list, select one of the following rules:
  - **Ignore**—attribute-based planning cannot be used for any parts that use this type and any parts below them in a product structure. Use this value for parts that are not expected to use attribute-based planning or that are not required to pass attribute values to lower-level components.
  - **Net**—attribute-based planning can be used for parts that use this type. Use this value for parts that are expected to require attribute-based planning or to propagate attribute-based planning logic to lower-level parts in a product structure (for example, to dependent components where attributes are relevant in the supply allotment process).
- In the **Description** box, type an optional description for the new record.
- From the other lists, select rules to set standard usage. For more information about the settings in the **MUEPoolNettingType** table, see the *RapidResponse Analytic and Data Model Guide*.

7. Click **Save and Close**.

Configure hidden resources

Several workbooks included with RapidResponse include columns showing details of supply and/or demand attributes. These columns are all hidden by default, but can be unhidden by users as required. In addition, the Planning Sheet workbook includes a hidden worksheet, Supply & Demand - with Attributes, which is similar to the standard Supply & Demand worksheet but includes details of applicable supply and demand attributes. This worksheet can be made available to users if necessary.

▸Unhide columns that display attributes

1. From the **Tools** menu, click **Search Resources**.
2. Click the **Text** option.
3. In the **Text** box, type **Attribute<*>**.
4. In the **Resources** section, select the **Workbooks** check box.
5. In the **Search** section, select **Expressions**.
6. In the **Include** list of options, click **All resources**.
7. Click **Search**.

   A list of search results appears.
8. Double-click each result where the text is found in a column expression.

   The worksheet properties open to the column with the text showing in the column expression.
9. For results where the column is hidden, as indicated in the **Hide** section of the dialog box, clear the **Hide column** check box, and click **OK** twice to save the change.

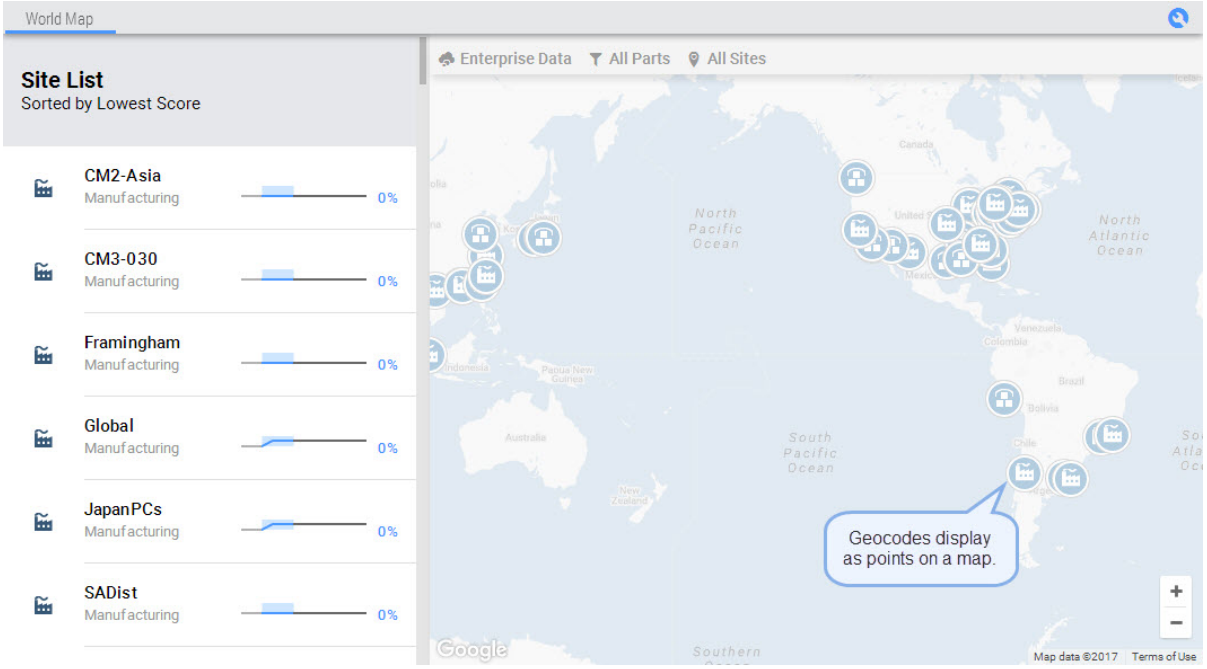
▸Unhide the Supply & Demand - with Attributes worksheet

1. From the **Go** menu, click **Workbooks**.
2. In the **Explorer**, right-click the **Planning Sheet** workbook and then click **Properties**.
3. On the **Worksheets** tab, right-click **Supply & Demand - with Attributes [Hidden]** and then click **Properties**.
4. On the **General** tab, click to clear the **Hide worksheet** check box.
5. Click **Ok**, and then **Ok** again.

CHAPTER 50: Configuring RapidResponse maps

Setting up access to maps 812
Mapping requirements 812
Set up access to the mapping service 812
Configuring geocode data for maps 813

RapidResponse maps are geographic visualizations available to users in some dashboards. The maps provide users with the ability to view, track, or edit data for their manufacturing and distribution sites.



The site locations are determined using precise latitude and longitude coordinates called geocodes. For more information, see "Configuring geocode data for maps" on page 813.

System administrators are responsible for setting up access to maps in RapidResponse. This includes importing the required resources if they are not already available in your system, setting up the map visualization configuration, and reviewing or adding coordinate values to the Sites workbook. For more information, see "Setting up access to maps" on page 812.

Note: Maps were introduced in RapidResponse 2016.2, Service Update 10.

Setting up access to maps

The following steps are required to set up and run RapidResponse maps:

- Install the required version of RapidResponse. For more information, see "Mapping requirements" on page 812.
- If required, import resource packages with the required resources. For more information, see "Mapping requirements" on page 812 and "Migrating RapidResponse resources" on page 752.
- Configure the map visualization set up. For more information, see "Set up access to the mapping service" on page 812.
- Review or add site addresses in the Sites system workbook. For more information, see "Configuring geocode data for maps" on page 813.

Mapping requirements

To provide users with access to the map visualizations available in the Supply Chain Health and Order Fulfillment dashboards, the following versions of RapidResponse must be installed:

- Supply Chain Health dashboard—RapidResponse 2016.2 Service Update 10
- Order Fulfillment dashboard—RapidResponse 2016.2, Service Update 13

The Supply Chain Health and Order Fulfillment dashboards are available as components in the RapidResponse Sales and Operations Planning and Order Fulfillment applications. If you do not have either of these applications licensed and are interested in purchasing one or both of the applications, contact Kinaxis Customer Support.

For more information, see "RapidResponse upgrade process overview" on page 141.

Set up access to the mapping service

In On-Premises environments, system administrators are responsible for setting up access to the mapping service. This includes configuring the map visualization setup and verifying and adding any required site addresses to convert to geocode values. For more information, see "Configuring geocode data for maps" on page 813.

▸Set up access to the mapping service

1. Contact Kinaxis Customer Support to obtain the following information for your RapidResponse installation:

    - An assigned company ID.
    - A Kinaxis data center address.
2. Ensure that your internal network or firewall allows external access to the following:
    - The assigned Kinaxis data center address.
    - https://maps.googlapis.com from all user machines.
3. In the **Administration** pane, under **System Settings**, click **Map Visualization Setup**.
4. Type the **Kinaxis Data URL** and **Company ID** provided by Kinaxis Customer Support.
5. Click **Validate** to confirm access to the mapping service and maps API.
6. Click **Save**.

Configuring geocode data for maps

Geocode columns are a column formatting property applied to a string value. If the string is a valid address, the value is converted into coordinates on a map. Address data is typically imported from your enterprise system as an integration step. For addresses you not automatically imported, you can manually input the address data in the Sites workbook.

Guidelines for valid address data

Maps can only display sites when the addresses converted to geocode values are accurate and complete. Invalid addresses display with a value of 0,0. To ensure that address data will display on a map, use the following guidelines to correct invalid address data:

- Use the address format defined by the national postal service of a country.
- If they are not included in the address format defined by a country's postal service, do not include additional details such as:
    - Business names
    - Unit numbers
    - Floor numbers
    - Suite numbers
- Avoid using the building name at an address. Use the street number instead.
- Avoid specify cross streets or intersections for an address. Use the street number instead.
- Do not include non-address details such as nearby landmarks.

Issues with maps or geocodes are logged. If your maps are not displaying data as expected, contact Kinaxis Customer Service.

CHAPTER 51: Supplier collaboration setup

Supplier collaboration overview 815
Automated data flows 817
Scenario setup for supplier collaboration 820
Supplier collaboration predefined resources 822
Adding a new supplier and users 825
Adding a new buyer user 828

Using supplier collaboration, buyers can collaborate and share part requirements with suppliers, increasing the flexibility of the supply chain. Using the RapidResponse supplier collaboration process, you can:

- Make faster, more cost effective decisions.
- Improve communication with your suppliers.
- Resolve supply management issues in a manner that minimizes impact to both buyers and suppliers.
- Improve cycle time and inventory turns.
- Effectively manage unexpected changes in a volatile demand environment.

Supplier collaboration relies on the RapidResponse Real-time Data Integration Service infrastructure to support all buyer and supplier transactions.

Caution: Do not turn on supplier collaboration if RapidResponse is using responsibility. Doing so can result in your suppliers viewing a list of users on your system.

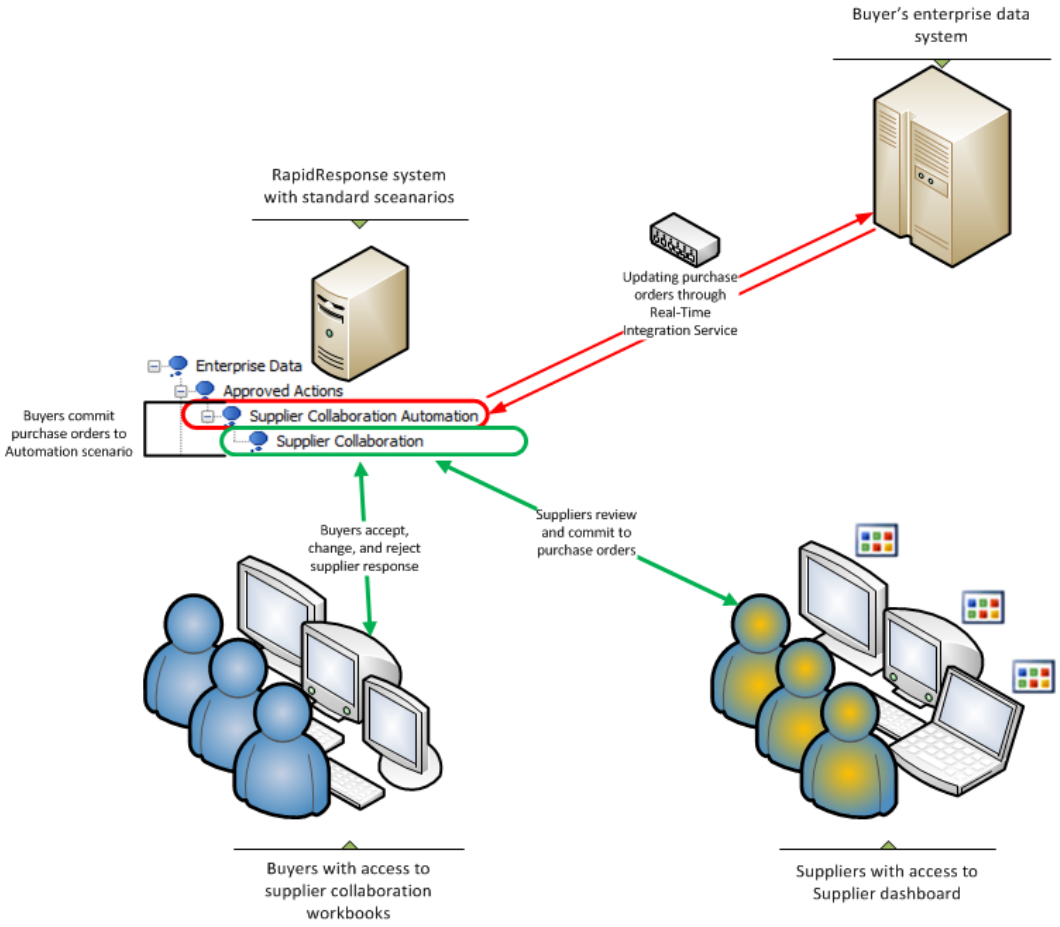
Supplier collaboration overview

Supplier collaboration contributes to increased confidence in the state of your supply chain by connecting your buyers with their suppliers in RapidResponse.

Data is exchanged and edited by both suppliers and buyers, and committed purchase orders return, updated, to your enterprise management system. Forecast data can only be viewed by buyers, as suppliers respond and commit to proposed forecast quantities.

Purchase order data flow

The following illustration provides an overview of the data flow within the supplier collaboration process for purchase orders.



Purchase orders are sent from your enterprise data system into RapidResponse through the Real-time Integration Service. Suppliers and buyers view the same purchase order data in resources that are designed specifically for them.

Suppliers respond to purchase order requests, which buyers then review and answer. For some purchase orders, both supplier and buyer will accept and commit to the order details right away. For other orders, suppliers and buyers might negotiate different dates or quantities by sending the order back and forth with explanatory notes. When an agreement is reached, the order is accepted and committed. Committed orders are also updated through the Real-time Integration Service to your enterprise data system.

Forecast data flow

Buyers can view tentative and committed forecast quantities from suppliers, as well as any differences between the two quantities, in a predefined workbook. Forecast requests for suppliers to review and commit to are sent from your enterprise data system through the Real-time Integration Service into RapidResponse.

Automated data flows

The RapidResponse Real-time Integration Service includes business message definitions that support the supplier collaboration process. It is used to:

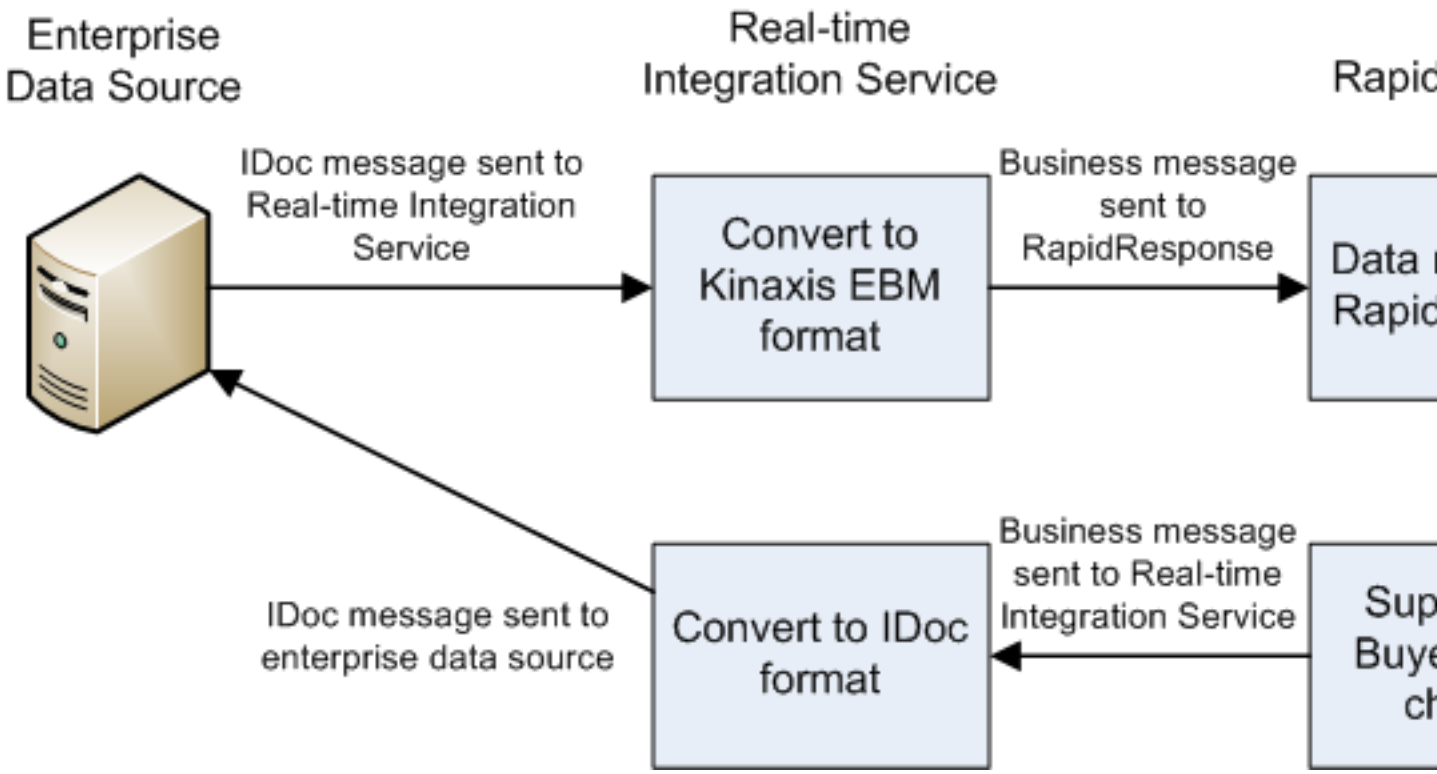
- Send purchase order requests and forecast data from your enterprise data system to your RapidResponse system so that suppliers can review and commit.
- Send purchase orders your suppliers have committed to from RapidResponse to your enterprise data system.

Purchase order requests and forecasts are sent through the Real-time Integration Service as business messages which define the order. Business messages use either the Kinaxis-EBM format, which determines the RapidResponse tables and fields the order provides data for, or the IDoc-XML format, which represents an IDoc message.

The rest of this section discusses how the Real-time Integration Service supports the RapidResponse supplier collaboration capability. The implementation for this service is typically completed by Kinaxis integration consultants. For more detailed information about this service, see the *the RapidResponse Data Integration Guide*.

Data flow overview

The following illustration shows a supplier collaboration data and process flow. This example uses an enterprise data source that sends business messages using the IDoc format. These messages are converted to the Kinaxis-EBM format, and the data is mapped to RapidResponse tables and fields by the Real-time Integration Service, and then sent to RapidResponse.



The transactions that are created in the enterprise data source are sent to RapidResponse using an enterprise business message, which creates the required purchase orders in RapidResponse. After the buyers and suppliers perform their tasks, the accepted orders are sent to the enterprise data source by an outbound message. If the orders were modified by the buyer or supplier, the changes are made in the enterprise data source, and the orders are moved into production.

Data from the IDoc message is moved into RapidResponse fields. If you require more information from the IDoc messages, you can add fields to the RapidResponse data model and have Kinaxis Customer Support modify the Real-time Integration Service adapters to accept the additional IDoc data. However, if you require time data from the IDoc message, you should create a DateTime field for this data.

If the messages are created using the IDoc-XML format, the Real-time Integration Service can send and receive IDoc messages, and convert to the Kinaxis EBM format only for mapping the data to and from RapidResponse. If the message uses the Kinaxis EBM format, the Real-time Integration Service must be configured to convert the message to the format that is required by your enterprise data sources. For more information, see the *the RapidResponse Data Integration Guide*.

Predefined business message definitions

RapidResponse includes predefined business domains and business message definitions, which provide the infrastructure for supplier collaboration processes. These domains and business message definitions can be used for sending and receiving messages. Business message definition templates are also available, and you can use these templates to create or customize business message definitions.

Business domains

The following business domain is included to support supplier collaboration:

Business domain	Description
Supplier Collaboration	Includes business message definitions to support receiving order requests and sending confirmations and expected delivery dates.

Business message definitions

The following business message definitions are included:

Business message definition	Description
CreatePurchaseOrder	An inbound message that inserts a purchase order, using the Kinaxis-EBM format.
CreatePurchaseOrderIDOC	An inbound message that inserts a purchase order, using the IDoc-XML format.
ChangePurchaseOrder	An inbound message that modifies a purchase order, using the Kinaxis-EBM format.
ChangePurchaseOrderIDOC	An inbound message that modifies a purchase order, using the IDoc-XML format.
CreateForecast	An inbound message that inserts a forecast., using the Kinaxis-EBM format.
CreateForecastIDOC	An inbound message that inserts a forecast, using the IDoc-XML format.
PurchaseOrderResponse	An outbound message that confirms, changes, or rejects a purchase order, using the Kinaxis-EBM format.
PurchaseOrderResponseIDOC	An outbound message that confirms, changes, or rejects a purchase order, using the IDoc-XML format.

The following business message definition templates are included:

Business message definition template	Description
CreatePurchaseOrderTemplate	An inbound message template that inserts a purchase order, using the Kinaxis-EBM format.
CreatePurchaseOrderIDOC Template	An inbound message template that inserts a purchase order, using the IDoc-XML format.
ChangePurchaseOrderTemplate	An inbound message template that modifies a purchase order, using the Kinaxis-EBM format.
ChangePurchaseOrderIDOC Template	An inbound message template that modifies a purchase order, using the IDoc-XML format.
CreateForecastTemplate	An inbound message template that inserts a forecast, using the Kinaxis-EBM format.
CreateForecastIDOCTemplate	An inbound message template that inserts a forecast, using the IDoc-XML format.

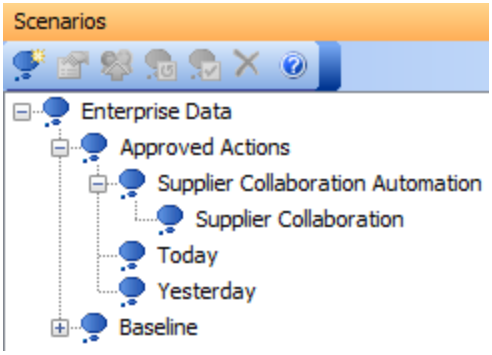
Business message definition template	Description
PurchaseOrderResponseTemplate	An outbound message template that confirms, changes, or rejects a purchase order, using the Kinaxis-EBM format.
PurchaseOrderResponseIDOC Template	An outbound message template that confirms, changes, or rejects a purchase order, using the IDoc-XML format.

Scenario setup for supplier collaboration

The RapidResponse supplier collaboration process requires a specific scenario setup and two scenarios:

- Supplier Collaboration Automation
- Supplier Collaboration

An example of this scenario structure is shown in the following illustration.



This scenario structure is typically a child of the Approved Actions scenario. The Supplier Collaboration Automation scenario should not be made available to users, and is used only for receiving data from and sending data to the Real-time Integration Service.

When data is brought in to the Supplier Collaboration Automation scenario by the Real-time Integration Service, the changes are automatically updated in a child of that scenario named Supplier Collaboration.

Scheduled processes send approved supplier commitments from the Supplier Collaboration scenario to the Supplier Collaboration Automation scenario. Automation scripts then send the data from the Supplier Collaboration Automation scenario to the enterprise data source through the Real-time Integration Service.

The scenarios have the following properties.

Scenario	Properties
Supplier Collaboration Automation	• Permanent
Supplier Collaboration	• Permanent • Child of Supplier Collaboration Automation • Automatically updated • Shared with Buyers and Suppliers groups

These scenarios must be created if they were not created by your data integration consultant.

▸Create the supplier collaboration scenarios

1. On the toolbar, click **Scenario**, and then click **New Scenario**.
2. In the **New Scenario** dialog box, specify the following information, and then click **OK**:
   - **Name**—Supplier Collaboration Automation
   - **Based on**—Approved Actions
   - **Purpose**—Inbound data
3. In the **Scenarios** pane, click the **Supplier Collaboration Automation** scenario, and then on the toolbar, click **New Scenario**.
4. In the **New Scenario** dialog box, specify the following information, and then click **OK**:
   - **Name**—Supplier Collaboration
   - **Based on**—Supplier Collaboration Automation
   - **Purpose**—Collaboration between buyers and suppliers
5. In the **Scenarios** pane, click **Supplier Collaboration**, and then on the toolbar, click **Share**.
6. In the **Share Scenario** dialog box, click **Select Names**.
7. In the **Select Names** dialog box, on the **Groups** tab, select your buyer and supplier groups, and then click **Modify** or **View only**, depending on the permissions that you want each group to have.
8. Click **OK** twice.
9. In the **Scenarios** pane, click **Supplier Collaboration Automation**, and then on the **Scenarios** pane toolbar, click **Properties**.

   The scenario's properties appear on a tab.
10. Select the **Permanent** check box.
11. Click **Save Data**, and then close the **Supplier Collaboration Automation** scenario properties.
12. In the **Scenarios** pane, click **Supplier Collaboration**, and then on the **Scenarios** pane toolbar, click **Properties**.

    The scenario's properties appear on a tab.
13. In the **Update** area, click **Automatic**.
14. Select the **Permanent** check box.
15. Click **Save Data**, and then close the **Supplier Collaboration** scenario properties.

Supplier collaboration predefined resources

The supplier collaboration process in RapidResponse relies on predefined resources and two predefined groups (Buyers and Suppliers). The resources are used by buyers in your company and the RapidResponse users at your supplier.

Administrators are responsible for modifying or customizing some of these predefined resources. Upon installation, the resources are owned by the Master Administrator. If the resources must be modified, they should be shared with system and data administrators.

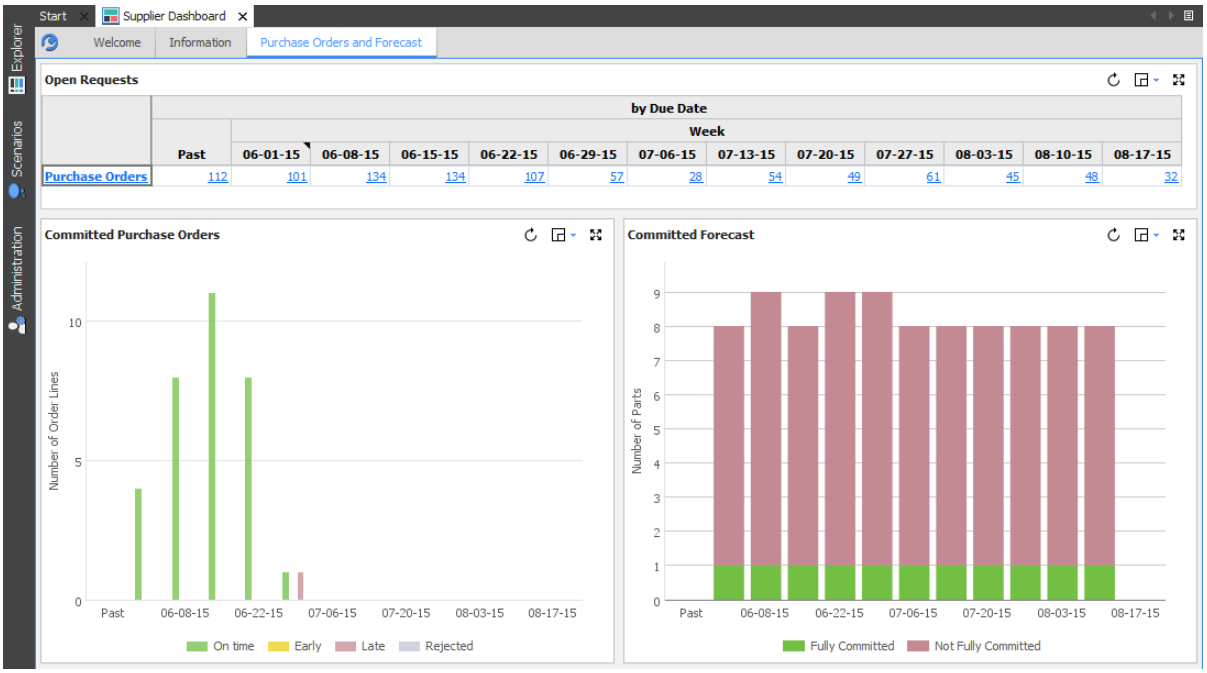
Buyer resources

Buyers within your company have access to two workbooks for supplier collaboration:

- Supplier Collaboration - Orders—view open purchase order requests, respond to supplier commitments on purchase orders, and review orders.
- Supplier Collaboration - Forecast—view previous, latest, and committed forecast quantities from suppliers.

Supplier resources

Supplier users have access to the Supplier dashboard. This is the only resource that they have direct access to.



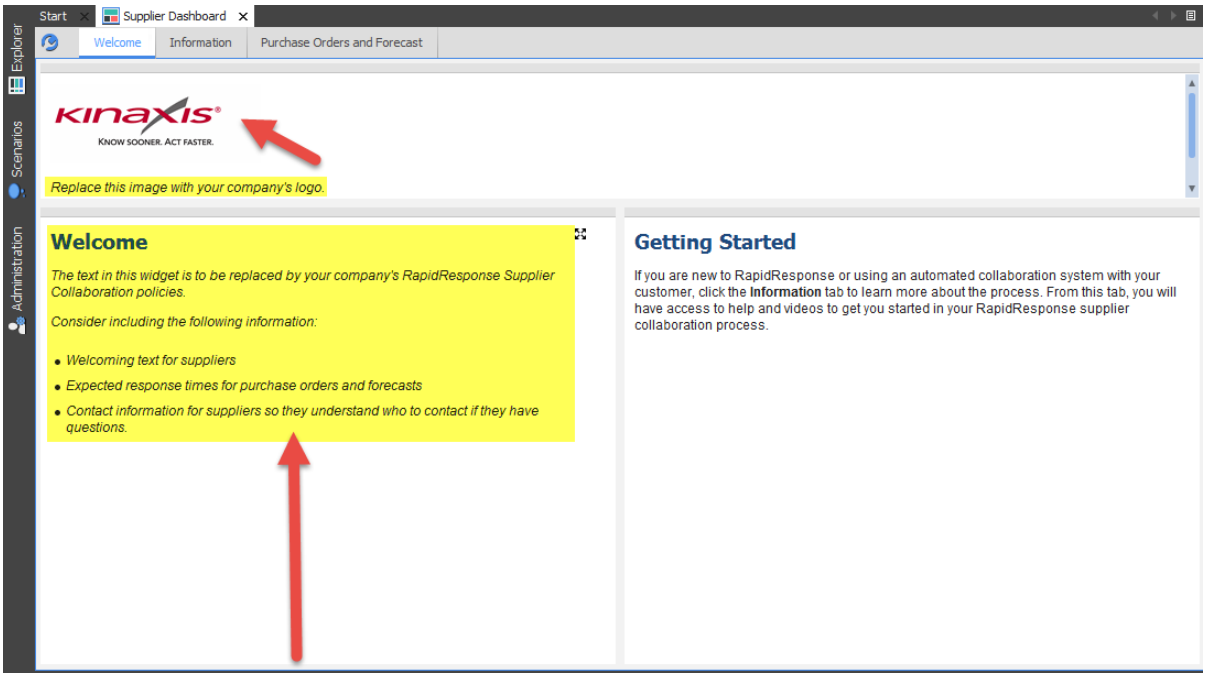
From the dashboard, supplier users can drill down into two workbooks:

- Purchase Order Response—respond to new purchase orders or purchase order changes from the customer and view commitments.
- Forecast Response—respond to forecast requests from the customer and view commitments.

These workbooks might require the following customizations:

- If supplier part numbers are available in the database, unhide the Supplier Part column in all of the worksheets.
- If the part descriptions are meaningful to suppliers, unhide the Part Descriptions column in all of the worksheets.
- If the buyer contact information is in the system, such as in the BuyerCode table Description field or in a custom field, add that field to the Line Details worksheet in the Purchase Order Response workbook. This helps suppliers determine who they might need to contact.

The Welcome tab in the Supplier dashboard is the first view that supplier users have when they sign into RapidResponse.



Consider replacing the Kinaxis logo in the top widget with your company logo. The logo file is stored in the Company Logo widget.

The Welcome widget provides the information your suppliers must know. The widget should include information about your company's supplier collaboration policies. You might also want to include the following information:

- Welcoming text for suppliers
- Expected response times for purchase orders and forecasts
- Contact information for suppliers so they know who to contact if they have questions

The widget is named Supplier Welcome. For information about modifying dashboard widgets, see the *RapidResponse Resource Authoring Guide*.

Administrator resources

The RapidResponse supplier collaboration process relies on resources that are owned by administrators. Upon installation, the resources are owned by the Master Administrator. If the resources must be modified, they should be shared with system and data administrators.

Alerts

As part of the RapidResponse Supplier Collaboration process, alert messages are sent to buyers and suppliers. The following alerts are included in the list:

- Buyer New Forecast—notifies buyers when suppliers have responded to new forecast requests.
- Buyer New Requests—notifies buyers when suppliers have responded to new purchase order requests.
- Buyer Overdue Forecast—notifies buyers when suppliers are late in responding to new forecast requests.
- Buyer Overdue Requests—notifies buyers when suppliers are late in responding to new purchase order requests.
- Supplier New Forecast—notifies suppliers when new forecast requests from customers are waiting commitment.
- Supplier New Requests—notifies suppliers when new purchase order requests from customers are waiting commitment.
- Supplier Overdue Forecast—notifies suppliers when overdue forecast requests from customers are waiting for commitment.
- Supplier Overdue Requests—notifies suppliers when overdue purchase order requests from customers are waiting for commitment.

During the RapidResponse data integration process, it is likely that the execution schedule for the alerts was configured. If the alerts have been shared, you can modify the existing schedule to meet your business needs. For more information about modifying alerts, see the *RapidResponse User Guide*.

Workbooks

The supplier collaboration process makes use of the following two workbooks:

- Buyer Commit to ERP—used by the Buyer Commit to ERP script. This script sends finalized purchase orders from the Supplier Collaboration Automation scenario to the enterprise data system using the Real-time Integration service. A purchase order is finalized when a supplier commits to the dates and quantities and a buyer accepts and commits the purchase order.
- Supplier Collaboration Order Cleanup—used in a process to modify purchase order lines in the RapidResponse database. Enterprise data systems such as SAP can delete lines from purchase orders. If the deleted purchase order line already exists in the Supplier Collaboration Automation scenario, a scheduled workbook command modifies the deleted line from the enterprise system in RapidResponse by setting the quantity to 0. To maintain history, such as notes, the line is not removed from the Supplier Collaboration Automation scenario. This scheduled command also sets the ScheduledReceipt.LastModifiedDate field to the latest date.

Scheduled tasks

The following scheduled tasks are part of the RapidResponse Supplier Collaboration process:

- Commit Buyer Response—commits purchase orders that buyers accepted and committed from the Supplier Collaboration scenario to the Supplier Collaboration Automation scenario.
- Commit Forecast Response—commits forecast responses that buyers accepted and committed from the Supplier Collaboration scenario to the Supplier Collaboration Automation scenario.
- Run Buyer Commitment Script—runs the Buyer Commit to ERP script.
- Supplier Collaboration Order Cleanup—runs the Address Deleted Lines command in the Supplier Collaboration Order Cleanup workbook.

During the RapidResponse data integration, it is likely that the execution schedule for the tasks were configured. If the scheduled tasks have been shared, you can modify the existing schedule to meet your business needs. For more information about modifying scheduled tasks, see the *RapidResponse User Guide*.

Scripts

The Buyer Commit to ERP script sends finalized purchase orders from the Supplier Collaboration Automation scenario to the enterprise data system using the RapidResponse Real-time Integration service. A purchase order is finalized when a supplier commits to the dates and quantities and a buyer accepts and commits the purchase order. This script also sets the ScheduledReceipt.Processed field to Y.

This script is scheduled to run with the Run Buyer Commitment Script scheduled task.

Adding a new supplier and users

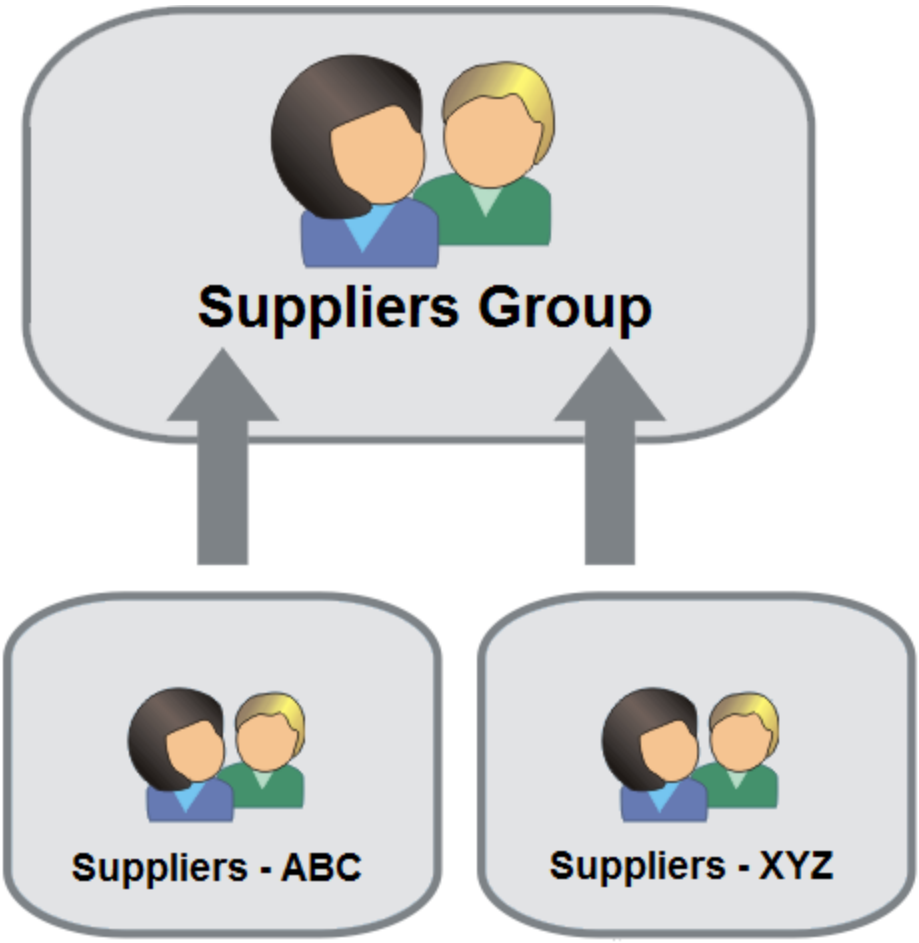
To support supplier collaboration, RapidResponse includes the following two predefined groups for suppliers:

- Suppliers group—predefined resources are shared with this group, and it is assigned permissions that are related to the supplier collaboration process. You should not assign additional permissions to members of this group, as doing so can result in inadvertent data exposure. Members of this group have permission to edit data in shared scenarios and to the Message Center. Members do not have the Send Link permission or access to the Welcome page. You should not directly add supplier users to this group.
- Suppliers - [Template] group—this group is a template to create a supplier group for a company. This group is a subgroup to the Suppliers group and has the same permissions.

Supplier setup through groups

You should not directly add supplier users to the Suppliers group. Instead, create a subgroup for each supplier and add supplier users to the subgroup. You can use the following naming convention for the supplier subgroups to aid in sorting:

- Suppliers - Company Name 1
- Suppliers - Company Name 2
- Suppliers - Company Name 3



If a supplier company requires only a single user, you should still create a group.

When creating a new supplier company, duplicate the Suppliers - [Template] group to copy the group's permissions and shared resources.

▸Add new supplier companies and users

1. In the **Administration** pane, in the **User Accounts** section, click **Users and Groups**.
   The **Users and Groups** workbook appears.
2. Select the **Suppliers - [Template]** group, and click **Duplicate Group** .
3. In the **New Groups** dialog box, enter a name for the group, such as **Suppliers - CompanyName**.
4. Click the **Resources** tab.
   A message appears asking if you want to create the new group now.
5. Click **Yes** to save the new group and display the **Resources** tab.
6. Select **Sites** from the **Show** list, and assign sites to the group that you created.
   Only assign the order sites that the supplier needs to see. At least one site must be assigned.
7. Click **OK** to save the group.
8. To create a user account for a supplier, click **New User** .
   The **New User** dialog box appears.

9. Enter the details about the supplier.

   Consider a user ID naming convention that makes it easy to find supplier users in a list. For example, **CompanyName - UserName**. Also consider adding contact information.
10. On the **Group Memberships** tab, assign the supplier user account to the supplier subgroup.

    The user accounts inherit the required resources and permissions through the group structure.
11. Assign the new supplier subgroup to the **SupplierCollab** profile variable. For more information, see the following section, "Restricting data for suppliers" on page 827.

Restricting data for suppliers

As a RapidResponse administrator, you need to restrict the data that suppliers have access to. Suppliers should only be able to see their own data.

Profile variables allow users to see only their own data in the Supplier dashboard and workbooks. For example, a profile variable could be used as part of a worksheet filter to ensure each supplier sees records only pertaining to their parts.

To create the SupplierCollab profile variable, you need the name of the supplier subgroup and the corresponding supplier ID. Use the Supplier ID Reference worksheet to view the Supplier IDs that are available in the RapidResponse system. The supplier IDs are stored in the Supplier table.

You can view and edit the Supplier Collaboration profile variables in the Supplier Collaboration worksheet in the Application Settings workbook. You can access this workbook from the Administration pane by clicking Application Settings under System Settings.

▸Add a profile variable for a new supplier

1. In the **Administration** pane, click **Application Settings** under **System Settings**.

   The **Application Settings** workbook appears.
2. Click the **Supplier Collaboration** worksheet.
3. Click **Insert Record** .
4. In the **Insert Record – Supplier Collaboration Profile Variable** dialog box, specify the following:
   - **Group ID**—select the name of the supplier subgroup that you created.
   - **Supplier ID**—enter the Supplier ID that you want to associate with the supplier subgroup. You must enclose the Supplier ID in single quotation marks. For example, 'Supplier ABC'. Consider copying the supplier ID from the **Supplier ID Reference** worksheet and then pasting it in the Insert Record dialog box to ensure that the proper name is entered.
   - **Description**—enter a description for the new supplier. This is optional.
5. Click **Save and Close**.

   The new SupplierCollab profile variable is added to the worksheet.

Caution: We strongly recommend that you do not delete any profile variables from the **Supplier Collaboration** worksheet. If you delete a profile variable, it could cause errors and prevent some resources, such as workbooks, from functioning correctly. If you determine that a profile variable is obsolete, instead of deleting it, add a note to the **Description** field to indicate that it should no longer be used. Alternatively, if you want to proceed with deleting a profile variable, search for the profile variable to make sure it's not referenced by any resources before you delete it. You can search for a variable by clicking **Tools** > **Search Resources** and typing the profile variable name in the **Text** box. Make sure to click **Select All** to search for all instances.

Notes:

- The SupplierCollab profile variables are validated when saved. The fourth column displays error and warning icons. The icon indicates that the Supplier ID value is not valid. This might occur when the supplier ID has not been entered correctly. Validation is performed in the root scenario, so an error will always be returned if the supplier is not committed to the root scenario. These types of errors do not need to be corrected for the resources to work correctly. The icon indicates that the Supplier ID has been assigned to multiple groups.
- The Supplier ID field can include more than one supplier. For example, supplier1, supplier2. You can use this syntax if your supplier companies have merged. Do not use this syntax in other cases, as it will expose the data from each supplier to the other supplier.

Adding a new buyer user

To add a new buyer to the supplier collaboration process, add the user to the Buyers group. After you add the user to the group, the user will have access to the two buyer workbooks (Supplier Collaboration - Orders and Supplier Collaboration - Forecast).

Note: This group requires access to the **Supplier Collaboration** scenario with the **Modify** permission. Ensure that you share the scenario with this group.

CHAPTER 52: Data change tracking and record identification

Configuring data change tracking 829
Deleting data change records 833

RapidResponse users who have simulation permissions can create new scenarios and change data in them. They can also potentially change data in a parent of their scenario by committing their changes back into it. RapidResponse automatically tracks the history and status of these data changes in the DataChange table (calculated), and presents them to users through the Scenarios properties pane.

The changes can also be transferred to your original enterprise data source if your company has implemented a system that feeds RapidResponse data back into your enterprise data source. This type of setup is typically called "closing the loop". Data change tracking also supports the Change Data Capture functionality in RapidResponse.

This chapter explains how to configure data change tracking, as well as how to control the frequency in which records are deleted from the DataChange table (for reference information about the DataChange table, see the *RapidResponse Analytic and Data Model Guide*).

Notes:

- Certain tasks described in this chapter can only be performed by system or data administrators who have been assigned permission to modify a data integration.
- For information about viewing data change records, see "Tracking scenario data changes" in the *RapidResponse User Guide*.

Configuring data change tracking

RapidResponse tracks user-initiated data changes between a selected scenario and its parent scenario using the DataChange table. This table holds changes made to data in a given scenario as well as changes made in its parent that the scenario has not yet been updated with.

The following types of changes are recorded in this table:

- **Insert**—for each record insertion in a scenario, a single record is added to this table. If an inserted record is subsequently modified, the insert record is updated with the new values and no modification record is created (as long as there have been no intervening scenario operations involving that scenario).

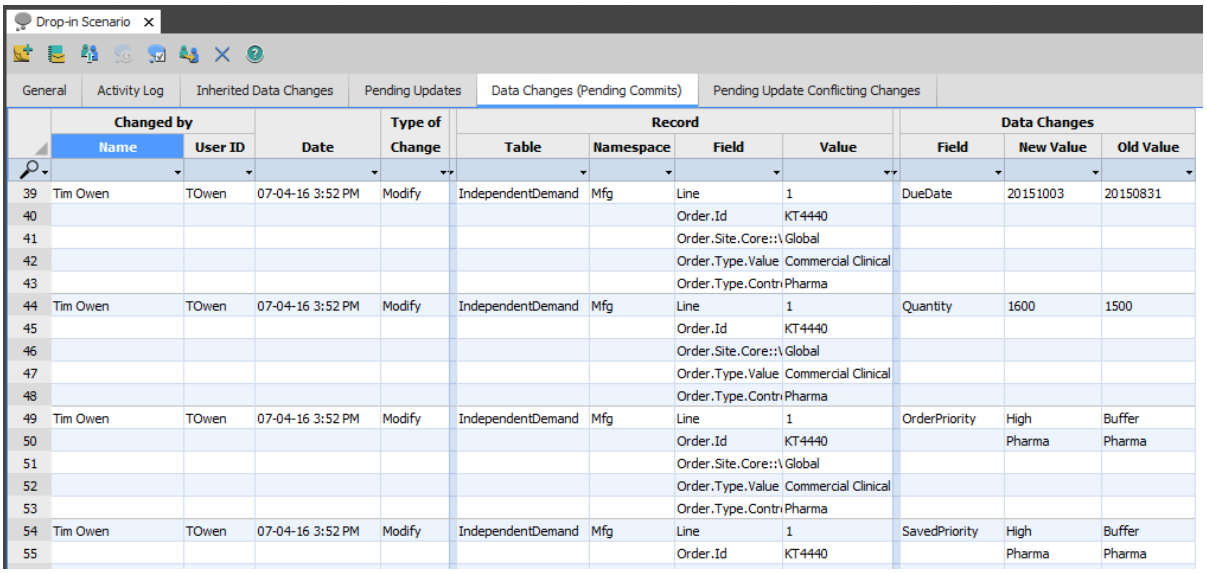
- **Modify**—for each individual field value modified on a given record in a scenario, a single record is added to this table. If a single user makes multiple modifications to a given field value in a scenario, only one modification record is created (as long as there have been no intervening scenario operations involving that scenario).
- **Delete**—for each record deletion in a scenario, a single record is added to this table. When a record is deleted, any existing data change records pertaining to it (inserts or modifications) are also deleted. As well, any deletions that happen as a result of another deletion are not recorded.

> **Note:** User-initiated changes do not included adhoc data imports, data updates to a specific scenario, and automatic data modifications.

The DataChange table is used in the Changes to Root Scenario worksheet in the Administration Log workbook.

RapidResponse 2016.2 introduced three tables that are almost identical to the DataChange table. Each of these tables run faster than the original DataChange table and are less memory intensive. The three tables each support a worksheet tab in the Scenario properties window.

- Inherited Data Changes tab (DataChange_Historical table)
- Pending Updates tab (DataChange_PendingUpdate table)
- Data Changes (Pending Commits) tab (DataChange_Local table)



	Changed by			Type of	Record				Data Changes		
	Name	User ID	Date	Change	Table	Namespace	Field	Value	Field	New Value	Old Value
39	Tim Owen	TOwen	07-04-16 3:52 PM	Modify	IndependentDemand	Mfg	Line	1	DueDate	20151003	20150831
40							Order.Id	KT4440			
41							Order.Site.Core::\	Global			
42							Order.Type.Value	Commercial Clinical			
43							Order.Type.Contr	Pharma			
44	Tim Owen	TOwen	07-04-16 3:52 PM	Modify	IndependentDemand	Mfg	Line	1	Quantity	1600	1500
45							Order.Id	KT4440			
46							Order.Site.Core::\	Global			
47							Order.Type.Value	Commercial Clinical			
48							Order.Type.Contr	Pharma			
49	Tim Owen	TOwen	07-04-16 3:52 PM	Modify	IndependentDemand	Mfg	Line	1	OrderPriority	High	Buffer
50							Order.Id	KT4440		Pharma	Pharma
51							Order.Site.Core::\	Global			
52							Order.Type.Value	Commercial Clinical			
53							Order.Type.Contr	Pharma			
54	Tim Owen	TOwen	07-04-16 3:52 PM	Modify	IndependentDemand	Mfg	Line	1	SavedPriority	High	Buffer
55							Order.Id	KT4440		Pharma	Pharma

Using the DataChange tables and worksheets can help users better understand differences between a parent scenario and a child scenario. For example, suppose you are ready to commit data changes to a parent scenario. For each scenario in your Scenarios pane, the changes in the scenario can be viewed along with details of each change, such as the user who made the change, the type of action that resulted in the change, and the field values affected by the change. These changes are viewed through the **Data Changes (Pending Commits)** worksheet in the Scenario Properties tab.

▸View the data changes between a scenario and its parent

1. In the **Scenarios** pane, select a scenario.
2. On the **Actions** menu, click **Properties**.
3. To see changes made in the scenario, click the **Data Changes (Pending Commits)** tab.

   Data changes in input and control tables are reported. Any changes made in Notes tables (for example, IndependentDemand_Notes) are not shown.

Data tracked by RapidResponse

Scenario data changes are saved to the DataChange table. The changes, or transactions, that can be recorded include addition of new records, as well as modification and deletion of existing records.

One transaction record is created and stored in the RapidResponse database for each change and some of the information stored includes the following:

- The scenario in which the changes were made.
- When the change occurred.
- The user who made the change.
- The type of change.
- Information identifying the specific record that was changed.
- Details of the change.

To send data changes back to your enterprise system, you might want to consider creating a custom worksheet based on the DataChange table. The data in worksheet could then be exported from RapidResponse and programmatically added to your enterprise data source. This type of setup is typically called "closing the loop". For more information about the DataChange table, see the *RapidResponse Analytic and Data Model Guide*.

Record identification fields

Data change tracking relies on certain fields in each input table to uniquely identify records for the purpose of tracking and reporting data changes. These fields are known as record identification fields.

For tables that contain key fields, the keys are always used as record identification fields. However, other fields can be added as required. For example, you might want to report additional field values when identifying changed records. For tables without key fields, there are no restrictions on the fields that can be used as record identification fields. However, you should typically choose a combination of fields whose values you do not expect to be common across large numbers of records in a table or, if possible, a combination of fields that will be unique for each record in a table. For tables that do not have keys defined, this can greatly speed up the time taken to process records during a data update.

▸To define record identification fields for a table

1. In the **Administration** pane, under **Data**, click **Data Model**.
2. From the **Show** list, select **Input tables**.

3. In the **Table** box, select the table for which you want to set the fields used to identify changed records. You might need to change the selection in the **Namespace** list if the table whose properties you want to modify is not shown.
4. Click **Table**, and then **Properties**.
5. Click the **Record Identification** tab.
6. Click **Add Fields**.
7. Select a field you want to use as a record identification field, and then click **Add**.
8. Repeat the previous step for any other fields you want to add, and then click **OK**.

   You remove any field you have added to a tables' record identification set by selecting it on the **Record Identification** tab, and then clicking **Remove**. You can also click **Reset** to restore each table's default set of record identification fields (typically, this is the set of key fields that identify records in the table).

Note: This procedure can only be performed by data or system administrators who have been assigned permission to modify a data integration.

Specifying a delimiter for multiple values in a field

Four fields in the DataChange table can include multiple separate values:

- ChangedFieldNames
- ChangedFieldValues
- IdentificationFieldNames
- IdentificationFieldValues

A delimiter is used to separate the values in a field. By default, the delimiter is a vertical bar (|), sometimes called the pipe character. If your data set uses the delimiter character a system administrator can change it.

For more information about these DataChange fields, see the *RapidResponse Analytic and Data Model Guide*.

▸To change the delimiter used in multiple value fields

1. In the **Administration** pane, under **System Settings**, click **Global Settings**.
2. Expand the **Client** category.
3. In the **Data field delimiter character** box, type in the new delimiter character. You should ensure the character chosen is not one used in your data set (typically, a symbol character should be chosen). It is recommended that you use a symbol character that is not in your data, such as underscore (_) or hyphen (-)

Notes:

- This procedure can only be performed by system administrators.
- This delimiter is also used to separate the key field values in a column that is being explicitly used as a reference. For more information, see "Add and remove columns" in the *RapidResponse Resource Authoring Guide*.

Deleting data change records

RapidResponse automatically logs information about data changes in the RapidResponse database. Over time, these system records can grow in size and potentially consume significant amounts of memory. By default, RapidResponse automatically deletes data change records after 45 days.

If your company does not require any of the features that utilize data change tracking (such as Change Data Capture, or the ability to identify changes made in a scenario), you might want to set the frequency to a low value.

On-Demand: The frequency in which these records are deleted can be configured by Kinaxis Customer Support.

On-Premises: The frequency in which these records are deleted can be configured as discussed in " Automatic deletion of system records" on page 277.

Note: A data import deletes all existing data change records.

CHAPTER 53: Configuring single sign-in for On-Premises

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, see "Configuring single sign-in for On-Demand" on page 863.

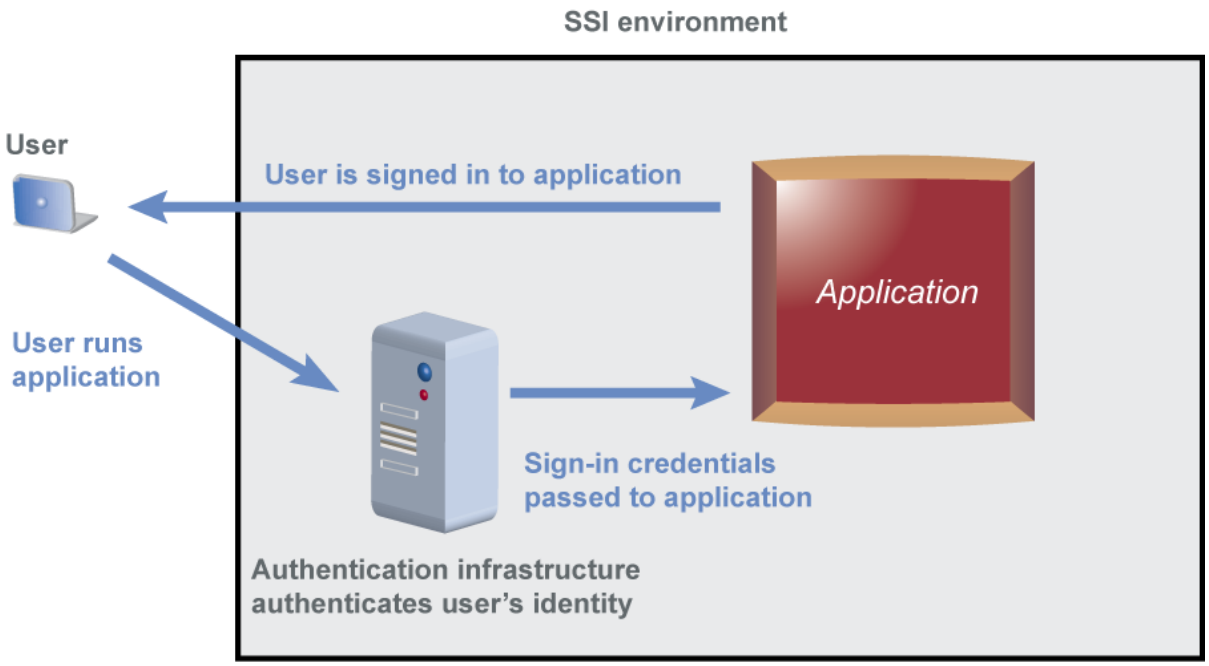
About single sign-in 835
Implementing single sign-in for RapidResponse 843
Integrating RapidResponse with an existing single sign-in environment 847
Implementing single sign-in using SAML2 855
Allowing users to use prompted sign in 860

Single sign-in (SSI) allows users to sign in to RapidResponse without needing to type in their user ID and password, provided their credentials have been authenticated. This can prevent unnecessary administrative work changing passwords for users who have forgotten them, and unlocking accounts for users who have entered their password incorrectly.

Enabling SSI also provides increased security by allowing only trusted users to sign in.

About single sign-in

A single sign-in environment consists of an application that requires users to sign in, a set of credentials, and an authentication infrastructure, such as a Windows Active Directory domain. An example of an SSI environment is shown in the following illustration.



When a user tries to run the application, their identity is authenticated by the authentication infrastructure, and their credentials are passed to the application. Credentials coming from the infrastructure are trusted by the application, and the user is signed in.

Single sign-in for RapidResponse

A single sign-in environment for RapidResponse obtains a user's sign-in credentials from an authentication infrastructure. The users in the infrastructure are authenticated, and when a user tries to sign in to RapidResponse, their credentials are passed from the infrastructure to RapidResponse. Because the credentials are trusted, the user is signed in without being prompted for their user ID and password.

If the user's identity is not authenticated by the authentication infrastructure, they are not signed in automatically. Depending on how the SSI environment is implemented, unauthenticated users might be prompted for their credentials, or might be unable to sign in to RapidResponse.

An SSI environment implementation can replace the RapidResponse prompted sign in screen, or can be embedded into a corporate portal so users are signed in when they start the RapidResponse client. An included software development kit (SDK) can be used to integrate RapidResponse into an existing SSI environment.

If your company uses an identity provider that conforms to the Security Assertion Markup Language V2 (SAML2) standard, you can also integrate RapidResponse with that provider to create a trust relationship. You can also encrypt the SAML2 requests and assertions.

This section discusses the skills and knowledge required to use RapidResponse SSI, describes the interfaces and authentication modes that can be used, provides an example of the code that specifies the SSI environment, and discusses the limitations of SSI.

Required skills and knowledge

Depending on the authentication mode chosen, SSI has different knowledge and skill requirements, which are shown in the following table. For more information about the authentication modes, see "Single sign-in authentication modes" on page 837.

Authentication mode	Required knowledge and skills
Pass-through	• Familiarity with your company's portal. • Using the HTTP GET command or creating cookies to pass credentials through an HTML hyperlink. • Editing XML and HTML.
Trusted	• Familiarity with your authentication infrastructure, including knowledge of how to add an application to it. • Programming experience in C# to implement methods provided with the RapidResponse SSI SDK. • Editing XML or HTML.
SAML2	• Familiarity with your identity provider, including how to obtain and work with federation metadata • Integrating applications with the identity provider. • Familiarity with the SAML 2.0 Web SSO profile standard.

Note: The Kinaxis Customer Support team cannot help you implement the integration of RapidResponse SSI with your enterprise authentication infrastructure or corporate portal.

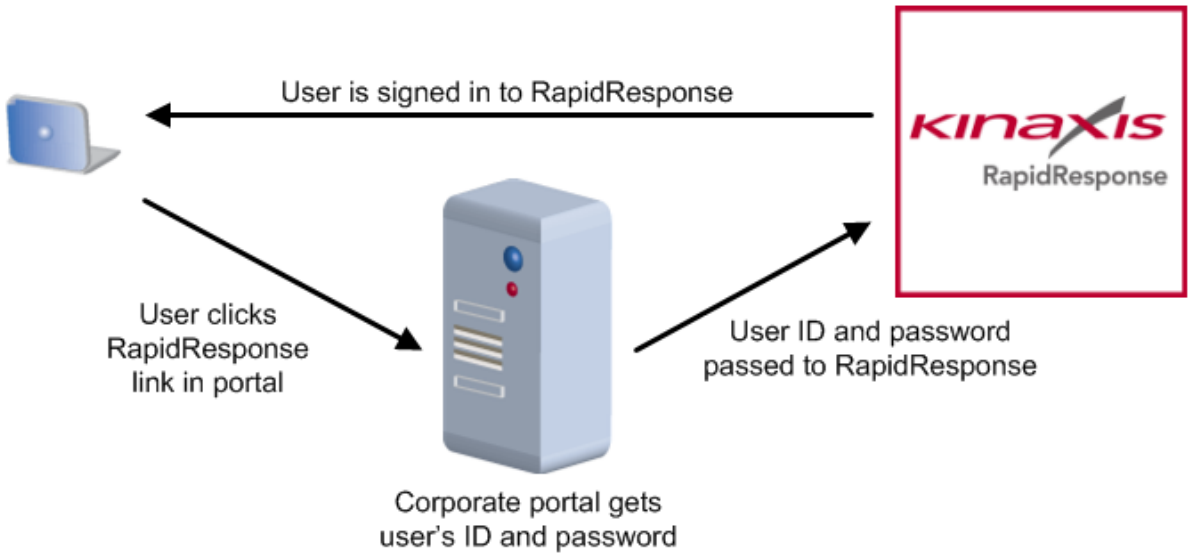
Note: For more information about the SAML2 specification, go to http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

Single sign-in authentication modes

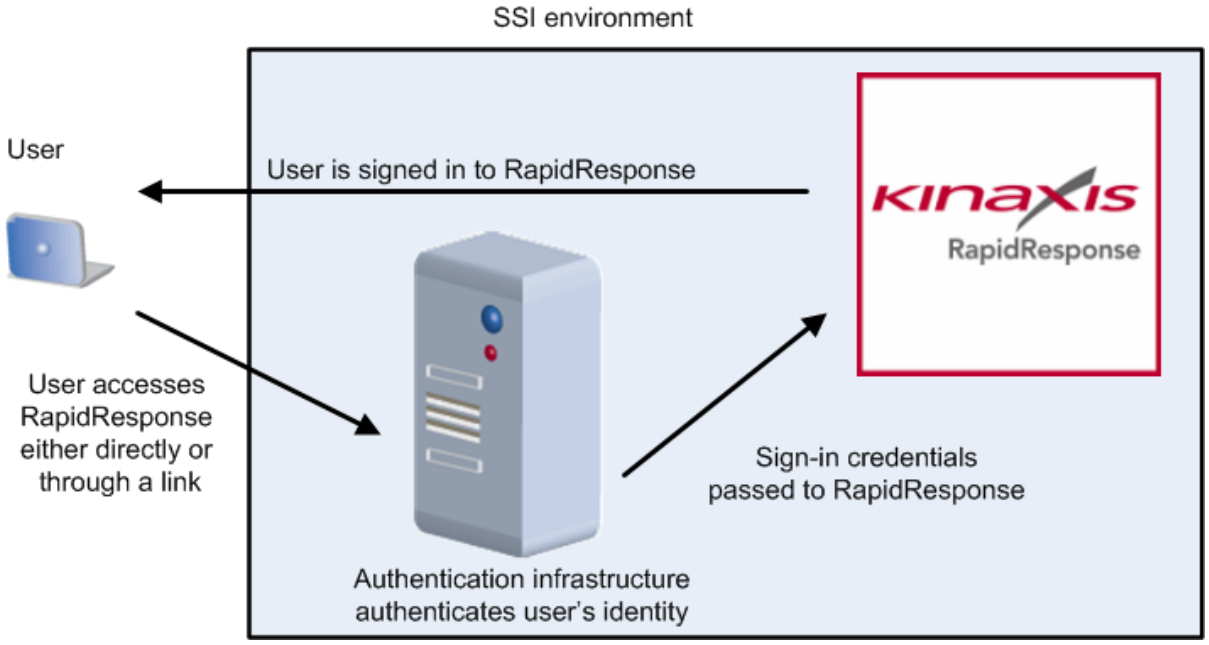
Before implementing SSI, you must choose an authentication mode and the user interfaces you want to use. The authentication mode defines how each user's authentication credentials get passed to RapidResponse. The interfaces define how users sign in and how the sign in screens look. For more information about interfaces, see "Single sign-in interfaces" on page 839.

The authentication mode used for your SSI environment should be decided based on if your company already uses SSI. Pass-through authentication should be used if your company does not already use an SSI environment. Trusted authentication integrates RapidResponse with an existing SSI environment. SAML2 authentication uses an existing identity provider and SAML2 Web profile to authenticate RapidResponse users.

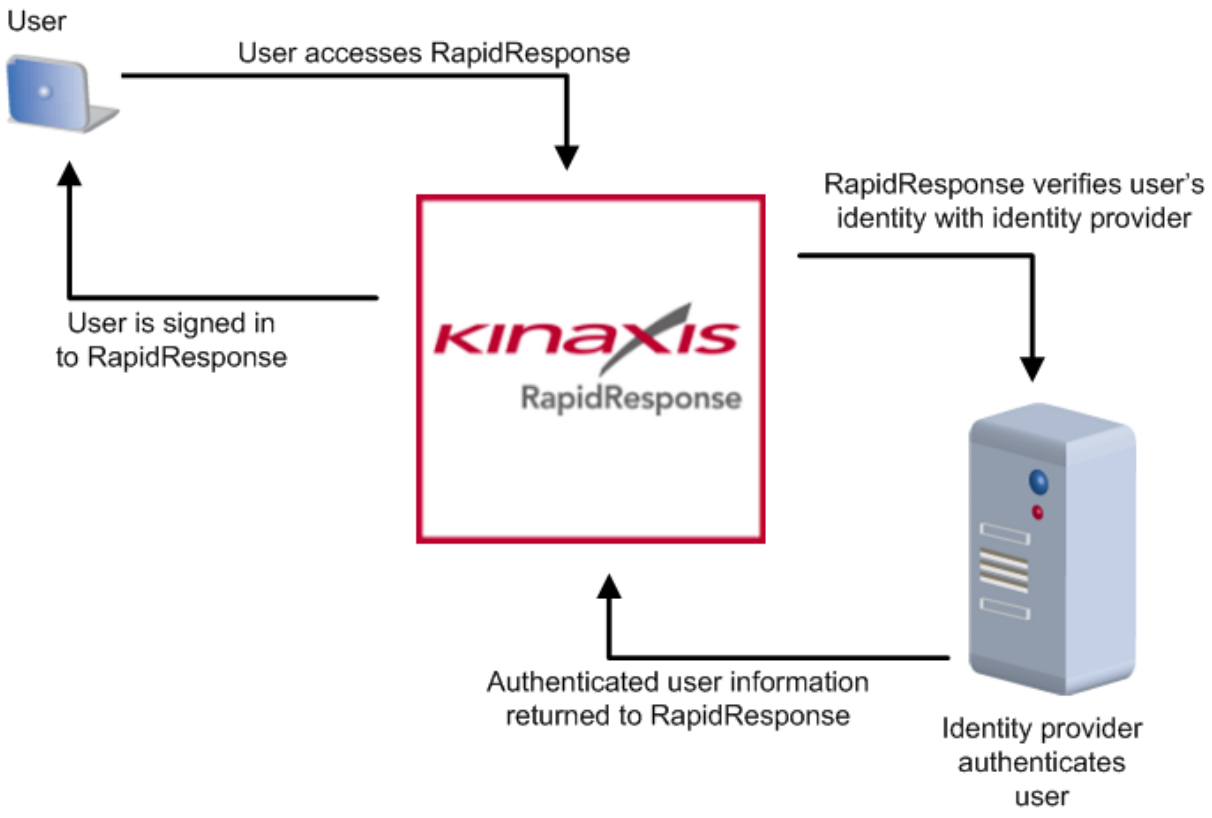
Pass-through authentication passes RapidResponse user IDs and passwords through a link to sign users in to RapidResponse, as shown in the following illustration. For more information, see "Implementing single sign-in for RapidResponse" on page 843.



Trusted authentication uses credentials from an existing SSI environment to sign authenticated users in to RapidResponse, as shown in the following illustration. For more information, see "Integrating RapidResponse with an existing single sign-in environment" on page 847.

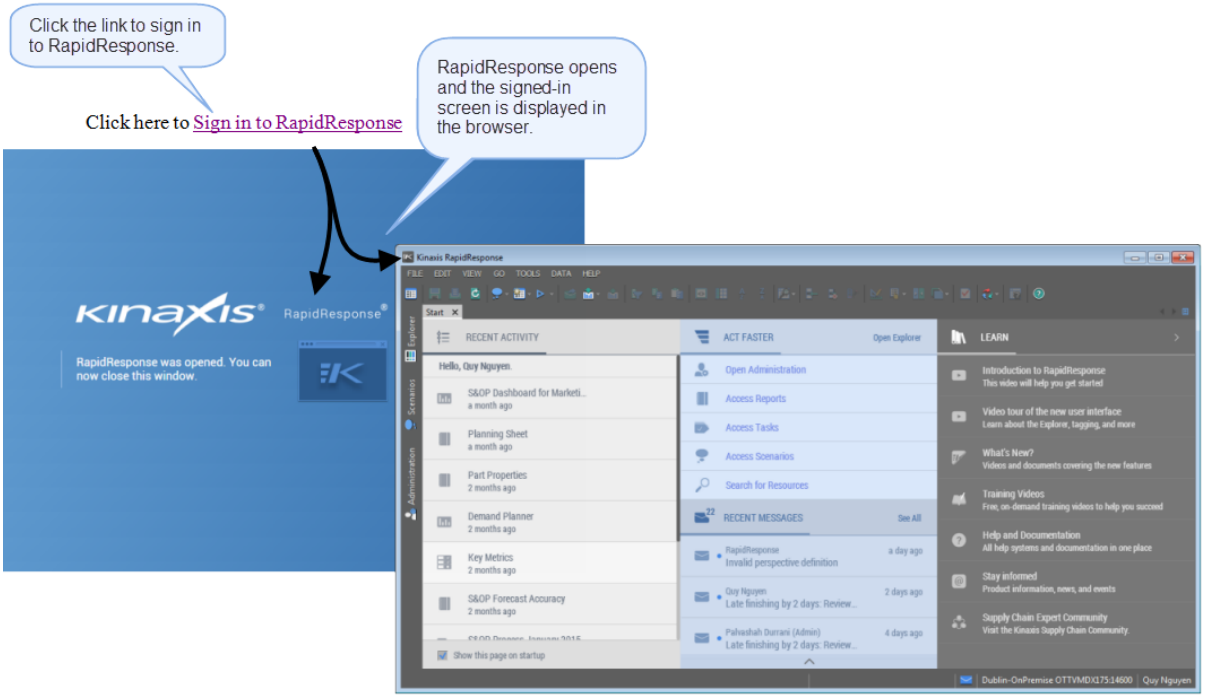


SAML2 authentication uses a SAML 2.0 Web SSO profile to federate credentials from an identity provider, which are used to authenticate users signing into RapidResponse. When a user accesses RapidResponse, RapidResponse sends a request to the identity provider for that user's authenticated identity. The identity provider verifies the user's identity, and then responds to RapidResponse with an assertion that the user is authentic. The user can then sign in to RapidResponse using the authenticated identity, as shown in the following illustration. For more information, see "Implementing single sign-in using SAML2" on page 855.



Single sign-in interfaces

An SSI environment can use an integrated or embedded interface, or both. The integrated interface replaces the RapidResponse sign in screen and allows the user to sign in by clicking a link, as shown in the following illustration.



The embedded interface passes the credentials to RapidResponse through a link from a company portal or Web site. If the sign in is successful, RapidResponse opens in a new window. An example of an embedded interface is shown in the following illustration.

The integrated and embedded interfaces can be used together or separately, depending on your company's needs. However, only the integrated interface is available if you are using SAML2 authentication.

Single sign-in configuration

RapidResponse SSI is configured by running the SSIConfig utility included with RapidResponse. This utility performs the following configuration steps:

- Configures the RapidResponse Application Server Web.config file with the appropriate settings for your chosen authentication method.

- Creates the security certificates to use for signing and decrypting requests and assertions.
- Reads the metadata from your identity provider.

Depending on the authentication type you use, some configuration steps might not be required, or additional configuration might be required. For example, if you specify pass-through authentication, you do not need to define a trusted user account. If you specify trusted authentication, you must create a trusted assembly using the RapidResponse SSI SDK, as described in "Integrating RapidResponse with an existing single sign-in environment" on page 847.

The SSIConfig utility can take the following options.

Option	Description
disable	Disables single sign-in.
mode	Specifies which authentication mode is used. You must specify one of the following. • **passthrough**—Configures RapidResponse to use pass-through authentication for SSI. • **trusted**—Configures RapidResponse to use trusted authentication for SSI. • **saml2**—Configures RapidResponse to use SAML2 authentication for SSI.
importmetadata	For SAML2 authentication, specifies the location of the identity provider's metadata. You can specify either a file location or network address. The identity provider's metadata is typically provided in an XML file.
sign	Specifies whether outgoing SAML requests are signed. Specifying this option requires a certificate and a public key, which are automatically created for you.
decrypt	Specifies the decryption key for encrypted SAML2 assertions. Specifying this option requires a certificate and a public key, which are automatically created for you.

The SSI environment is defined by the RapidResponse Application Server. The definition is contained in the **Web.config** file, which is found by default in **C:\Program Files\Kinaxis\RapidResponse\Web**. When a user accesses the RapidResponse Application Server, the definition is read and the specified configuration applied. You can modify some aspects of the SSI setup in this file.

The following code shows the default values for SSI in the **Web.config** file.

```
A → <singleSignIn enabled="false" xmlns="http://www.kinaxis.com/ns/2010/06/singleSignIn">
B →   <authentication mode="saml2">
C →     <trustedAuthenticationMode type="type,assembly"/>
        <saml2AuthenticationMode>
D →       <signing enabled="false"/>
          <encryption enabled="false"/>
E →       <idpConfiguration>
            <signatureVerification enabled="false"/>
            <assertion>
F →           <conditions clockSkew="00:10:00"/>
            </assertion>
            <saml2WebSSOProfile>
              <authNRequest signRequests="false">
G →             <endpoint>https://IdP/auth</endpoint>
              </authNRequest>
            </saml2WebSSOProfile>
          </idpConfiguration>
        </saml2AuthenticationMode>
      </authentication>
H →   <userInterface>
I →     <embeddedUserInterface enabled="false">
J →       <styleSheet href=""/>
K →       <launchLabel></launchLabel>
        </embeddedUserInterface>
L →     <integratedUserInterface enabled="true">
M →       <definition mode="explicit" explicitUserDefaultSSI="true"/>
        </integratedUserInterface>
      </userInterface>
    </singleSignIn>
```

The following table provides an explanation of the syntax.

Section	Function
A	Indicates if SSI is enabled. Valid values for the `enabled` attribute are: • **true**—SSI is enabled and the environment described by the other sections of code. • **false**—SSI is disabled and the rest of the code is ignored.
B	Defines the authentication mode used for SSI. Valid values for the `mode` attribute are: • **passthrough**—RapidResponse user ID and password are required, and are passed to RapidResponse from an external source by using a cookie or link properties. • **trusted**—only a RapidResponse user ID is required, and authentication is performed by an authentication infrastructure. This mode requires an implementation of a trusted authentication assembly. • **saml2**—the user's identity is provided and authenticated by an external identity provider. This mode requires RapidResponse to be integrated with an identity provider.
C	Specifies a trusted authentication assembly. Valid values for the type attribute are a combination of a class name and the assembly that contains the class, which are compiled by an SDK included with RapidResponse. For more information, see "Integrating RapidResponse with an existing single sign-in environment" on page 847.
D	Specifies signing and encryption certificates for SAML2 authentication. For more information, see "Configuring certificates" on page 858.
E	Configuration options for the identity provider.
F	Timing tolerance for assertions. If RapidResponse and the identity provider are not using synchronized time, assertions might be interpreted as being received outside of their expiration period. Increasing the clockSkew value provides more tolerance for time differences and ensures assertions are valid.
G	The endpoint URL that authentication requests are sent to.

Section	Function
H	Defines which SSI user interfaces are used.
I	Indicates if the embedded user interface for SSI is used. Valid values for the `enabled` attribute are: • **true**—the embedded interface is available. • **false**—the embedded interface is unavailable.
J	Specifies a cascading style sheet to be applied to the RapidResponse sign in page. The `href` attribute should be set to the location of your company's standard style sheet. This setting is optional.
K	Specifies the link text to start RapidResponse. Formatting must be valid HTML and encoded for containment in an XML element.
L	Indicates if the integrated user interface for SSI is used. Valid values for the `enabled` attribute are: • **true**—the integrated interface is available. • **false**—the integrated interface is unavailable.
M	Defines the availability of the integrated or prompted sign-in screen. Valid values for the `mode` attribute are: • **automatic**—if credentials are passed, the user is signed in using SSI; otherwise, user must provide a user ID and password using the prompted sign in screen. • **exclusive**—only SSI is available. If no credentials are passed, the prompted sign in screen is not displayed and the user cannot sign in. • **explicit**—the user is signed in using SSI only if RapidResponse is accessed from the SSI URL. Otherwise, user must provide a user ID and password using the prompted sign-in screen. If the `mode` attribute is set to `explicit`, the valid values for the `explicitUserDefaultSSI` attribute are: • **false**—if RapidResponse is accessed from a resource link, the user must sign in with their credentials. • **true**—if RapidResponse is accessed from a resource link, the user is signed in using SSI.

Limitations of single sign-in

SSI applies only to users created in RapidResponse. You cannot access RapidResponse using your portal, identity provider, or trusted credentials if you do not have a corresponding account in RapidResponse.

Implementing single sign-in for RapidResponse

If your company does not already use SSI, you can implement an SSI environment for RapidResponse by using pass-through authentication. In this case, a corporate portal acts as the authentication infrastructure. Users are authenticated by the portal, and when a user tries to sign in to RapidResponse, their credentials are passed from the portal to RapidResponse.

Implementing an SSI environment using pass-through authentication has the following steps:

1. Create user accounts that match accounts in the portal. For more information, see "User accounts for pass-through authentication" on page 844.
2. Configure SSI. For more information, see "Configuring single sign-in" on page 844.

3. Specify the SSI interfaces. For more information, see "Specifying single sign-in interfaces" on page 845.
4. Create links to sign in to RapidResponse, including link parameters to obtain the user ID and password to pass to RapidResponse. For more information, see "Creating links to sign in to RapidResponse" on page 846.

User accounts for pass-through authentication

When pass-through authentication is used, each user's RapidResponse user ID and password must match their user ID and password in the system that passes the credentials. If a user in a pass-through authentication environment changes their password, the RapidResponse password must change to match. The password can be edited in the user's properties.

Users should not be allowed to change their RapidResponse passwords. If a user's password changes, that user will not be able to sign in because the SSI environment uses the password from the authentication infrastructure. If the passwords do not match, the user cannot sign in, and might become locked out of RapidResponse. In addition, passwords should be set to never expire.

If your company is installing RapidResponse for the first time, you should ensure that for each user you create, the user ID and password match the user ID and password in your portal.

If your company is upgrading RapidResponse, your existing user accounts might not match. In this case, you can copy each user and give the copy a userID and password that match the portal account, or you can map the account names within the portal so that each user's RapidResponse user ID is passed to RapidResponse, and not their portal user ID. For more information about copying users, see "To duplicate a user account from the Administration pane" on page 553.

If you delete a user account from the portal, you should also delete the user in RapidResponse. Deleted users will be unable to use SSI, but can still sign in using their RapidResponse user ID and password if the password is known.

Configuring single sign-in

Once the user accounts have been created, SSI can be configured. The configuration utility is used to enable and configure SSI. However, if you want to modify the settings or define the interfaces that will be used, you must modify the **Web.config** file on the computer where RapidResponse Application Server is installed. For more information, see "Specifying single sign-in interfaces" on page 845.

▸To configure RapidResponse for pass-through authentication

1. On the computer where RapidResponse Application Server is installed, open a **Command Prompt** window.
2. Navigate to the **C:\Program Files\Kinaxis\RapidResponse\SSIConfig** folder.
3. Run the **SSIConfig.exe** file with the following option:
   - `-mode=passthrough`
4. Specify the embedded and integrated interface settings. For more information, see "Specifying single sign-in interfaces" on page 845.

Specifying single sign-in interfaces

When pass-through authentication is used, the embedded interface is the recommended interface for providing access to RapidResponse. The embedded SSI interface uses a link from your company's internal Web site or portal to pass sign in credentials to RapidResponse. If the sign in is successful, RapidResponse opens in a new browser window.

The integrated interface can be used with the embedded interface, but should not be used alone. Because the credentials cannot be passed to RapidResponse except through a link or browser Favorite entry, the credentials must be specified in the URL. Text in a URL cannot be hidden or encrypted, so each user's credentials will be displayed whenever they access the link. Because of the security risk this situation presents, use of the integrated interface is not recommended for pass-through authentication.

▸To enable the embedded interface

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder on the computer where RapidResponse Application Server is installed.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Ensure the value of the **enabled** attribute is **"true".**
5. In the <**embeddedUserInterface>** element, change the value of the **enabled** attribute to **"true"**.
6. In the <**styleSheet>** element, type the URL of the style sheet used for the Web site the link is embedded in. This step is optional.
7. In the <**launchLabel>** element, type the link text you want to appear on the Web page. This step is optional.
8. On the **File** menu, click **Save**.

▸To enable the integrated interface

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder on the computer where RapidResponse Application Server is installed.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Ensure the value of the **enabled** attribute is **"true".**

5. In the **<integratedUserInterface>** element, change the value of the **enabled** attribute to **"true"**.
6. In the <**definition>** element, change the value of the **mode** attribute to match the interface you want to use. For more information see "The following table provides an explanation of the syntax." on page 842.
7. On the **File** menu, click **Save**.

Creating links to sign in to RapidResponse

The embedded interface defines a link that signs in to RapidResponse. This link must be added to a Web page within your company's portal in order to be used. The link should be embedded in an HTML <iframe> element, which must be at least 500 pixels wide and 20 pixels tall to accommodate any messages that RapidResponse might display.

The link to pass credentials through an embedded interface must include a method to obtain the required credentials. This can be done by including the user ID and password as parameters on the <iframe> element's src attribute, or by creating cookies to hold the same information.

A link to the integrated interface can be created on a Web page within your company's portal, and is not embedded in an <iframe> element. The link to the integrated interface contains the user ID and password in the URL, which displays the credentials in the Web browser **Address** bar. This is not a secure method of passing credentials, and its use is not recommended.

If you do not have permission to edit the Web page, either request permission or get help from the person in your organization who maintains the internal Web pages.

▸To embed a link to RapidResponse

1. Determine where on your internal Web page or portal the link to RapidResponse should appear.
2. Using an HTML editor, add the following line to the source code of your Web site for the Java client.

   ```
   <iframe marginheight="0" marginwidth="0" frameborder="0"
   src="http://server/RapidResponse/ssi.ashx?embed&uid=userID&pwd=password"
   height="20" width="500">
   </iframe>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on, `userID` is the user's RapidResponse sign in name, and `password` is the user's password.
3. Using an HTML editor, add the following line to the source code of your Web site for the web client.

   ```
   <iframe marginheight="0" marginwidth="0" frameborder="0"
   src="http://server/RapidResponse/ssi.ashx/mobile?embed&uid=userID&pwd=p
   assword" height="20" width="500">
   </iframe>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on, `userID` is the user's RapidResponse sign in name, and `password` is the user's password.
4. Save the file, and then open the Web page in a Web browser to test the link.

Note: If HTTPS is enabled on the RapidResponse IIS Web site, the link can be embedded using the secure `https` protocol.

▸To create a link to RapidResponse

1. Determine where the link to RapidResponse should appear.
2. Using an HTML editor, add the following line to the source code of your Web site for the Java client.

   ```
   <A
   href="http://server/RapidResponse/ssi.ashx?uid=UserID&pwd=password">Sta
   rt RapidResponse</A>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on, `userID` is the user's RapidResponse sign in name, and `password` is the user's password.
3. Using an HTML editor, add the following line to the source code of your Web site for the web client.

   ```
   <A
   href="http://server/RapidResponse/ssi.ashx/mobile?uid=UserID&pwd=passwo
   rd">Start RapidResponse</A>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on, `userID` is the user's RapidResponse sign in name, and `password` is the user's password.
4. Save the file, and then open the Web page in a Web browser to test the link.

Integrating RapidResponse with an existing single sign-in environment

If your company already uses an SSI environment, you might be able to integrate RapidResponse with it. A software development kit included with RapidResponse can be used to create a trusted authentication assembly customized for your company's environment.

A project template for creating a trusted authentication assembly is included with the RapidResponse SSI SDK, and can be opened in Microsoft Visual Studio or Microsoft Visual C# Express. A sample implementation using Windows Integrated Authentication is included.

The test application provided with the SDK requires Microsoft Internet Information Services. For information about installing IIS, contact your system administrator.

Adding RapidResponse to an SSI environment has the following steps:

1. Create RapidResponse user accounts that match the accounts in the authentication infrastructure. For more information, see "User accounts for trusted authentication" on page 848.
2. Install the SSI SDK. For more information, see "Installing the software development kit" on page 848.
3. Create the trusted authentication assembly. For more information, see "Creating a trusted authentication assembly" on page 849.
4. Test the trusted authentication assembly. For more information, see "Testing a trusted authentication assembly" on page 850.
5. Configure SSI in RapidResponse. For more information, see "Configuring single sign-in" on page 851.
6. Specify SSI interfaces. For more information, see "Specifying single sign-in interfaces" on page 853.
7. Create links to sign in to RapidResponse. For more information, see "Creating links to sign in to RapidResponse" on page 854.

User accounts for trusted authentication

Even though a password is required when creating a user account, trusted authentication does not require a user's RapidResponse password to sign in. Because the password is not used to sign in, you can choose to not tell users what their RapidResponse passwords are.

Because users do not know their passwords, the passwords should be set to never expire and the users should not be allowed to change their passwords. If a password expires, the user will be unable to change it or sign in, and might be locked out of RapidResponse. If the password can be changed, the user is prompted to change the password the first time they sign in to RapidResponse.

If your company is installing RapidResponse for the first time, you should ensure that for each user you create, the RapidResponse user ID matches the user ID in your authentication infrastructure.

If your company is upgrading RapidResponse, your existing user accounts might not match. In this case, you can copy each user and give the copy a userID that matches the account in the authentication infrastructure, or you can map the account names within the trusted authentication assembly. For more information about copying users, see "To duplicate a user account from the Administration pane" on page 553.

If you delete a user account from the authentication infrastructure, you should also delete the user in RapidResponse. Deleted users will be unable to use SSI, but can still sign in using their RapidResponse user ID and password if the password is known.

Installing the software development kit

The SDK for SSI consists of the following:

- A Microsoft Visual Studio solution containing:
  - a blank solution template
  - a sample implementation for Windows authentication.
- a Web site definition for testing SSI.
- a program that configures RapidResponse to use the trusted Windows account.

The SDK is available from the RapidResponse DVD, and can be installed on any computer with Microsoft Windows XP or Microsoft Windows 2003 Server, and must be able to connect to RapidResponse Server. The RapidResponse Application Server is not required to install the SDK or to test an implementation of SSI.

▸To install the software development kit

1. Log on as a Windows Server administrator on the computer where the RapidResponse Single Sign In SDK will be installed and insert the RapidResponse DVD.

   If a menu does not display, use Windows Explorer to navigate to your DVD drive, and double-click the DVD drive icon to run the RapidResponse DVD.
2. On the **Welcome** screen that displays, click **Browse this DVD**.
3. In Windows Explorer, double-click the **Application Server** folder, and then double-click the **Single Sign In SDK** folder.
4. Double-click the **setup.exe** file.

5. On the **Welcome** screen, click **Next**.
6. On the **License Agreement** screen, click **I agree to the terms in the license agreement**, and then click **Next**.
7. On the **Customer Information** screen, do the following:
   - In the **User Name** text box, type the name of the computer where you are installing the SDK if it is not automatically entered.
   - In the **Organization** text box, type your company's name.
   - In the Install this application for area, click **Anyone who uses this computer (all users)**.
   - Click **Next**.
8. On the **Destination Folder** screen, do the following:
   - If you want to install the SDK in a different location, click **Change**, and the navigate to a folder.
   - Click **Next**.
9. Click **Install**.
10. When the installation is complete, click **Finish**.

Software development kit folder structure

The SDK installs by default to the **C:\Program Files\Kinaxis\Single Sign In SDK** folder, and creates the folder structure shown in the following illustration:

The following describes the folders created when the SDK is installed:

- **Samples**—contains a C# solution for implementing SSI, including a sample implementation for Windows authentication and a blank template for other authentication infrastructures.
- **Web**—contains the test Web site definition for IIS, plus a Web page for testing the embedded interface. The test Web site simulates signing in to RapidResponse.

Creating a trusted authentication assembly

To integrate RapidResponse into an SSI environment using trusted authentication you must create a trusted authentication assembly, which implements an authentication method and allows the user accounts in the authentication infrastructure to be used in RapidResponse. The implementation varies depending on the authentication infrastructure and SSI environment your company uses.

A blank template for implementing trusted authentication and a sample implementation for Windows authentication are provided with the SDK, and can be opened with Microsoft Visual Studio or Microsoft Visual C# Express. The blank template contains no code, but provides the methods that must be implemented. Comments in the code tell you what each method should do and return.

The blank template and sample implementation are both contained in the Microsoft Visual Studio solution **Samples.sln** in the **Single Sign In SDK\Samples** folder.

▸To create a trusted authentication assembly

1. In Microsoft Visual Studio or Microsoft Visual C# Express, open the **Samples.sln** file.
2. Using the **Solution Explorer**, locate and open the **BlankTemplate** project.
3. In the **Authenticate** class, add the code to implement trusted authentication with your authentication infrastructure.
4. On the **Build** menu, click **Build Solution**.

Testing a trusted authentication assembly

Before integrating RapidResponse into the SSI environment, you should use the included test Web site and Web page to ensure the trusted authentication assembly is configured properly. The test Web site is located in the **Single Sign In SDK\Web** folder, and simulates signing in to RapidResponse with the credentials provided by the trusted authentication assembly.

The test Web site must be configured to use the trusted authentication assembly. Settings must be changed in the **Web.config** file located in the **Single Sign In SDK\Web** folder. In addition, the test Web site definition must be configured with the RRSingleSignInUser account's password, which allows the Web site definition to sign in to RapidResponse. You must be logged in as a Windows administrator to run the configuration program.

The test Web site is defined in Microsoft IIS, and is located at **http://server/SSITest**, where **server** is the name of computer the SDK is installed on. The test Web page contains an embedded link to the test Web site.

▸To configure Web.config for trusted authentication

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **Single Sign In SDK\Web** folder.
2. Right-click **Web.config**, and then click **Edit**.
3. In the **<authentication>** element, change the value of the **mode** attribute to **"trusted"**.
4. In the <**trustedAuthenticationMode>** element, change the value of the **type** attribute to **"assemblyName.Authenticate, assemblyName"**, where `assemblyName` is the trusted authentication assembly compiled by the SDK.

   The assembly is a .dll file, and should be included in the type attribute without the .dll extension.
5. Specify the embedded and integrated interface settings. For more information, see "Specifying single sign-in interfaces" on page 853.
6. If your company's RapidResponse Server is installed on a different computer, in the **<ServerAPI>** element, change the value of the following attribute:
   - **server**—the name of the computer with RapidResponse Server installed on it.

▸To configure the test Web site to use the trusted assembly

1. In Windows Explorer, navigate to the folder that contains the trusted authentication assembly.
2. Copy **assemblyName.dll** and **assemblyName.pdb** to the Windows clipboard.
3. Navigate to the **Single Sign In SDK\Web\bin** folder.
4. Paste **assemblyName.dll** and **assemblyName.pdb**.

▸To test the trusted assembly using the embedded interface

1. Use Windows Explorer to navigate to the **Single Sign In SDK\Web** folder, right-click the **portaltest.htm** file, and then click **Edit**.
2. In the **<iframe>** element, ensure the **src** attribute is set to **http://server/SSITest/ssi.ashx?embed**, where `server` is the name of the computer the SDK is installed on.
3. Open **portaltest.htm** in your Web browser.
4. Click the link to sign in to RapidResponse.

   If the trusted assembly is correctly implemented and the environment properly configured, a success message is displayed in a new window.

▸To test the trusted assembly using the integrated interface

1. Start your Web browser.
2. If the explicit integrated interface is being used, in the Address bar, type **http://server/SSITest/ssi.ashx**, and then press **Enter**.

   If the automatic or exclusive integrated interfaces are being used, in the Address bar, type **http://server/SSITest/Default.aspx**, and then press **Enter**.

   Where `server` is the computer the SDK is installed on.

   If the trusted assembly is correctly implemented and the environment properly configured, a success message is displayed in a new window.

Configuring single sign-in

Once the trusted assembly has been tested, it can be used to configure SSI on the RapidResponse Application Server. The configuration utility is used to enable and configure SSI. However, if you want to modify the settings or define the interfaces that will be used, you must modify the **Web.config** file on the computer where RapidResponse Application Server is installed. For more information, see "Specifying single sign-in interfaces" on page 853.

In addition, the Application Server must be configured with the trusted password, which allows the RRSingleSignInUser account to sign in to RapidResponse Server. The configuration program can configure this, and create the user account if it does not already exist. You must be logged in as a Windows administrator to run the configuration program.

If you are implementing SSI for the web client, you must also configure Microsoft Internet Information Services (IIS) to prevent authentication issues. In particular, RapidResponse should be configured to allow anonymous authentication, and the ssi.ashx file configured to use Windows authentication. Otherwise, users accessing RapidResponse using the web client must re-authenticate when they access the RapidResponse URL.

▸To configure Web.config for trusted authentication

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Ensure you are logged in to Windows as an administrator.
2. On the computer where RapidResponse Application Server is installed, open a **Command Prompt** window.
3. Navigate to the **C:\Program Files\Kinaxis\RapidResponse\SSIConfig** folder.
4. Run the **SSIConfig.exe** file with the following option:
   - `-mode=trusted`
5. Close the Command Prompt window.
6. In Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse** folder.
7. Right-click **Web.config**, and then click **Edit**.
8. In the <**trustedAuthenticationMode**> element, change the value of the **type** attribute to **"assemblyName.Authenticate, assemblyName"**, where `assemblyName` is the implementation compiled by the SDK.

   The assembly is a .dll file, and should be included in the **type** attribute without the .dll extension.
9. Specify the embedded and integrated interface settings. For more information, see "Specifying single sign-in interfaces" on page 853.

▸To configure RapidResponse to use the trusted assembly

1. In Windows Explorer, navigate to the folder on the computer with the SDK that contains the trusted authentication assembly.
2. Copy **assemblyName.dll** and **assemblyName.pdb** to the Windows clipboard.
3. Navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web\bin** folder.
4. Paste **assemblyName.dll** and **assemblyName.pdb**.

▸To configure IIS authentication for web client

1. In Microsoft Windows, from the **Control Panel**, click **Administrative Tools**, and then double-click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the **Sites** item to reveal the **RapidResponse** virtual site.
3. In the **IIS** section, double-click **Authentication**.
4. In the **Status** column, ensure only **Anonymous Authentication** is set to **Enabled**.
5. Click **Content View**.
6. In the **Name** column, right-click **ssi.ashx**, and then click **Switch to Features View**.
7. In the **IIS** section, double-click **Authentication**.
8. In the **Status** column, ensure only **Windows Authentication** is set to **Enabled**.

Specifying single sign-in interfaces

When trusted authentication is used, the embedded and integrated interfaces both provide access to RapidResponse. The embedded SSI interface uses a link from your company's internal Web site or portal to start RapidResponse, using the trusted assembly to sign in. If the sign in is successful, RapidResponse opens in a new browser window.

The integrated interface replaces the RapidResponse prompted sign in screen, and can be reached by directly accessing RapidResponse in a Web browser. If the trusted assembly is properly set up, the user is presented with a Go button. Pressing this button starts RapidResponse and signs the user in.

The embedded and integrated interfaces can also be used together. In this case, users can access RapidResponse either through an embedded link or directly in a Web browser. Users who click the embedded link are signed in automatically, and users who access directly click a button to sign in.

▸To enable the embedded interface

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder on the computer where RapidResponse Application Server is installed.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Ensure the value of the **enabled** attribute is **"true".**
5. In the <**embeddedUserInterface>** element, change the value of the **enabled** attribute to **"true"**.
6. In the <**styleSheet>** element, type the URL of the style sheet used for the Web site the link is embedded in. This step is optional.
7. In the <**launchLabel>** element, type the link text you want to appear on the Web page. This step is optional.
8. On the **File** menu, click **Save**.

▸To enable the integrated interface

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Ensure the value of the **enabled** attribute is **"true".**

5. In the **<integratedUserInterface>** element, change the value of the **enabled** attribute to **"true"**.
6. In the <**definition>** element, change the value of the **mode** attribute to match the interface you want to use. For more information see "The following table provides an explanation of the syntax." on page 842.
7. On the **File** menu, click **Save**.

Creating links to sign in to RapidResponse

The embedded interface defines a link that signs in to RapidResponse. This link must be added to a Web page in order to be used. The link should be embedded in an iframe element, which must be at least 500 pixels wide and 20 pixels tall to accommodate any messages that RapidResponse might display.

A link to the integrated interface can be created on any Web page, or can be saved as a bookmark. Users who click the link are allowed to sign in if they are authenticated by the trusted assembly.

If you do not have permission to edit the Web page, either request permission or get help from the person in your organization who maintains the internal Web pages.

▸To embed a link to RapidResponse

1. Determine where on your internal Web site or portal the link to RapidResponse should appear.
2. Using an HTML editor, add the following line to the source code of your Web site for the Java client.

   ```
   <iframe marginheight="0" marginwidth="0" frameborder="0"
   src="http://server/RapidResponse/ssi.ashx?embed" height="20"
   width="500">
   </iframe>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on.
3. Using an HTML editor, add the following line to the source code of your Web site for the web client.

   ```
   <iframe marginheight="0" marginwidth="0" frameborder="0"
   src="http://server/RapidResponse/ssi.ashx/mobile?embed" height="20"
   width="500">
   </iframe>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on.
4. Save the file, and then open the Web page in a Web browser to test the link.

Note: If HTTPS is enabled on the RapidResponse IIS Web site, the link can be embedded using the secure `https` protocol.

▸To create a link to RapidResponse

1. Determine where on your internal Web site or portal the link to RapidResponse should appear.
2. For the Java client, edit the source code of your internal Web site or portal to add the following line.

   ```
   <A href="http://server/RapidResponse/ssi.ashx">Start RapidResponse</A>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on.

3. For the web client, edit the source code of your internal Web site or portal to add the following line.

   ```
   <A href="http://server/RapidResponse/ssi.ashx/mobile">Start
   RapidResponse</A>
   ```

   Where `server` is the name of the computer RapidResponse Server is installed on.
4. Save the file, and then open the Web page in a Web browser to test the link.

Implementing single sign-in using SAML2

If your company already has a single sign-in environment that uses an identity provider with SAML2 authentication, you can integrate RapidResponse into this environment. User accounts must be the same in RapidResponse and your identity provider.

To integrate RapidResponse with your identity provider, each program's federation metadata can be provided for the other. This metadata is an XML file that describes how the application and identity provider can interact with each other.

Using the information specified in the metadata, the identity provider can process authentication requests coming from RapidResponse, and RapidResponse can process responses coming from the identity provider. A trust relationship is established between the identity provider and RapidResponse using the metadata, so the user can sign in to RapidResponse using the identity provider's information.

To improve security, the requests and responses between RapidResponse and the identity provider can be encrypted using HTTPS. You can also encrypt SAML assertions using public key encryption with x.509 certificates. These certificates can be configured during the SSI set up process, or you can use an existing certificate.

When users sign in using the identity provider, their sign-in experience is provided by that system. For this reason, only the integrated single sign-in interface is available with SAML2 authentication. Accessing RapidResponse launches the identity provider's authentication, which allows the user to sign in to RapidResponse.

Implementing an SSI environment using SAML2 authentication includes the following steps:

1. Create user accounts that are mapped to the user accounts defined in the identity provider. For more information, see "User accounts for SAML2 authentication (step 1)" on page 855.
2. Obtain the metadata from the identity provider. For more information, see "Obtaining the identity provider metadata (step 2)" on page 856.
3. Configure single sign-in. For more information, see "Configuring single sign-in (step 3)" on page 856.
4. Obtain the metadata from RapidResponse for use in the identity provider. For more information, see "Obtaining RapidResponse metadata (step 4)" on page 860.
5. Provide users with the link to sign in to RapidResponse. For more information, see "Providing the link to sign in to RapidResponse (step 5)" on page 860.

User accounts for SAML2 authentication (step 1)

When SAML2 authentication is used, the identity provider returns a NameID to RapidResponse, which must map to a RapidResponse user ID. Even though a password is required when creating a user account, SAML2 authentication does not require a user's RapidResponse password to sign in. Because

the password is not used to sign in, you can choose to not tell users what their RapidResponse passwords are.

Because users do not know their passwords, the passwords should be set to never expire and the users should not be allowed to change their passwords. If a password expires, the user will be unable to change it or sign in, and might be locked out of RapidResponse. If the password can be changed, the user is prompted to change the password the first time they sign in to RapidResponse.

If your company is installing RapidResponse for the first time, you should ensure that for each user you create, the RapidResponse user ID is available as a NameID from your identity provider.

If your company is upgrading RapidResponse, your existing user accounts might not be appropriate for your identity provider. In this case, you can copy each user and give the copy a user ID that matches the NameID available from your identity provider. For more information about copying users, see "To duplicate a user account from the Administration pane" on page 553.

If you delete a user account from the authentication infrastructure, you should also delete the user in RapidResponse. Deleted users will be unable to use SSI, but can still sign in to RapidResponse using their user ID and password if the password is known.

Obtaining the identity provider metadata (step 2)

Depending on your identity provider, the metadata might be available from a URL, or you might need to export it to a file. For information about how to obtain the metadata, consult your identity provider's documentation.

You require the full path to the file or the URL to include the metadata in the SSI setup.

Configuring single sign-in (step 3)

After you have created user accounts and prepared the identity provider, you can configure single sign-in. The configuration utility provides the functionality required to configure SSI, import the identity provider's metadata, and configure the Windows trusted user account.

In addition, if signing requests or encrypting assertions is required, the configuration utility can set up the security certificates required. If these certificates do not already exist on the computer that RapidResponse Application Server is installed on, the configuration utility can create them. You can also customize the certificates or use external certificates other than the ones automatically created by the utility.

If you are using external certificates, you must specify the following:

- CN—certificate name
- O—organization
- L—location
- S—state
- C—country

Assertions sent from the identity provider to RapidResponse have a built-in expiration time. If RapidResponse and the identity provider are not using synchronized times, the assertion might be interpreted as being received outside of its expiration period and rejected. To prevent this, you can

adjust the time difference tolerance (clock skew) between RapidResponse and the identity provider. This ensures the assertions are recognized as valid if the time difference between computers is too great. You can adjust the tolerance by hours, minutes, and seconds.

▸To configure single sign-in

1. Ensure you are logged in to Windows as an administrator.
2. On the computer where RapidResponse Application Server is installed, open a **Command Prompt** window.
3. Navigate to the **C:\Program Files\Kinaxis\RapidResponse\SSIConfig** folder.
4. Run the **SSIConfig.exe** file with the following options:
   - `-mode=saml2`
   - `-sign`

     This option is required only if requests must be signed. If you are using an external signing certificate, you must specify the name, organization, location, state, and country defined for the certificate. If you do not specify certificate information, an internal certificate is used or created if necessary.
     For example, `"-sign=CN:Your Signing Certificate, O=Your Company, L=Your City, S=Your State, C=Your Country"`
   - `-decrypt`

     This option is required only if the assertions made by the identity provider are encrypted. If you are using an external decrypting certificate, you must specify the name, organization, location, state, and country defined for the certificate. If you do not specify certificate information, an internal certificate is used or created if necessary.
     For example, `"-decrypt=CN:Your Decryption Certificate, O=Your Company, L=Your City, S=Your State, C=Your Country"`
   - `-importmetadata=path to metadata`

     Where `path to metadata` is either the location of the metadata file or the URL that returns the metadata from the identity provider.

▸To adjust the clock skew for assertions

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Locate the **<assertions>** element.
5. In the **<condition>** element, for the **clockSkew** property, type the number of hours, minutes, and seconds to adjust the tolerance by.

   For example, "00:15:00" specifies a 15 minute clock skew.
6. On the **File** menu, click **Save**.

Configuring certificates

When you use the `-sign` and `-decrypt` options with the SSIConfig utility, certificate sections are added to the **Web.config** file, with certificates generated by the utility. You can use different certificates, either from the Windows Certificate Store or from a certificate file. To use different certificates, you can modify the following sections of the **Web.config** file.

```
<saml2AuthenticationMode>
  <signing enabled="true">
    <x509Certificate src="certificateStore">
      <certficateStore>
        <match findType="FindBySubjectDistinguishedName">CN=Kinaxis RapidResponse SAML 2.0 Signing</match>
        <match findType="FindByThumbprint">305FC9180FA69BC4195DF877E16E838CBFF5EE98</match>
      </certficateStore>
    </x509Certificate>
  </signing>
  <encryption enabled="true">
    <x509Certificate src="certificateStore">
      <certficateStore>
        <match findType="FindBySubjectDistinguishedName">CN=Kinaxis RapidResponse SAML 2.0 Encryption</match>
        <match findType="FindByThumbprint">AE09206EF52E22CC191394DF8A4407C6498C5474</match>
      </certficateStore>
    </x509Certificate>
  </encryption>
```

The following table provides an explanation of the syntax.

Section	Description
x509Certificate	Defines where to obtain the certificate. Valid values for the **src** attribute are: • **certificateStore**—Obtains the certificate from the Windows Certificate Store. • **file**—Obtains the certificate from a file in the RapidResponse Application Server's Web folder (**Program Files\Kinaxis\RapidResponse\Web**)
certificateStore	Specifies the certificates are retrieved from the Windows Certificate Store.
match	Identifies the certificate used, defined in the Windows Certificate Store. The following values are required for the **findType** attributes to identify the certificate: • **FindBySubjectDistinguishingName**—The name of the certificate in the certificate store. • **FindByThumbprint**—Identifies the certificate. These values are available from the certificate's properties in the certificate store.
file	Identifies the certificate, defined as a .pfx file. The following attributes are required to identify the file to load the certificate from: • **location**—The file name to load the certificate from. • **password**—The password required to access the certificate. If there is no password, set this attribute to a blank string "".

▸To specify a certificate

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Locate the **<saml2AuthenticationMode>** element.
5. Modify the **<match>** elements to refer to the certificate name and thumbprint specified in the certificate store.

▸To configure the Web.config file to use a certificate from a file

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. Using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. Locate the **<saml2AuthenticationMode>** element.
5. In the **<x509Certificate>** element, modify the value of the **src** attribute to be `"file"`.
6. Remove the **<certificateStore>** and **<match>** elements.
7. Add the following element in the **<x509Certificate>** section:
   `<file location="certificate.pfx" password="pwd">`

   where `certificate.pfx` is the certificate file and `pwd` is the password required to access the certificate.

For information about the certificate store, see the Microsoft Windows documentation.

Updating a SAML2 configuration

If you have upgraded to RapidResponse 2016.2 Service Update 12 (or later) from Service Update 11 (or earlier), the certificate signing algorithm has been updated to provide additional security. If you had configured SAML2 to sign authentication requests prior to upgrading, the previous configuration is not valid and the SAML2 configuration cannot be used to sign in to RapidResponse.

To correct this situation, you can run the `SSIConfig.exe` utility with the `-replace` option to update your configuration with the new signing algorithm.

▸To update the certificate

1. Ensure you are logged in to Windows as an administrator.
2. On the computer where RapidResponse Application Server is installed, open a **Command Prompt** window.
3. Navigate to the **C:\Program Files\Kinaxis\RapidResponse\SSIConfig** folder.
4. Run the **SSIConfig.exe** file with the following options:
   - `-replace`
   - `-sign`

Obtaining RapidResponse metadata (step 4)

The metadata required to integrate RapidResponse with the identity provider can be found in the following location:

`https://host/RapidResponse/saml2metadata.ashx`

Where `host` is the computer RapidResponse Server is installed on.

Depending on your identity provider, you can either include this URL directly in your identity provider, or you can save the metadata as an XML file and then import it. For information about including this information in your identity provider, consult your identity provider's documentation.

Providing the link to sign in to RapidResponse (step 5)

After SSI has been set up and the metadata for each program integrated, you can provide users with a link that allows them to automatically sign in to RapidResponse with their authenticated identities. Users who click the link are allowed to sign in if they are authenticated by the identity provider.

Users can sign in to the Java client using the following link:

`http://host/RapidResponse/ssi.ashx`

Users can sign in to the web client using the following link:

`http://host/RapidResponse/ssi.ashx/mobile`

Where `host` is the name of the computer RapidResponse Server is installed on.

Allowing users to use prompted sign in

The information in this section applies only if you have not configured users to sign in only using SSI.

When the integrated interface is used, you must decide if users will be allowed to sign in with their credentials and not use SSI. This is most applicable for user accounts in RapidResponse that do not have a corresponding account in the authentication infrastructure, such as the Admin account (the master administrator user account).

If users are not allowed to use the prompted sign in screen, the Admin user must have a separate SSI identity, which requires a new Windows account for the Admin user. If users are allowed to use the prompted sign in screen, anyone signing in with the Admin account must enter the credentials.

Users who receive their RapidResponse messages in their email can click resource links, which opens the resource in RapidResponse. If the user does not have RapidResponse open when they click the link, it is launched and they are signed in. By default the user is signed in automatically using SSI, but you can choose to require these users to enter their credentials. This allows you to ensure only valid users can access RapidResponse by clicking these links.

Users can only use prompted sign in if they know their passwords, the automatic or explicit definition is used, and they either click the **Sign in as another user** link, access RapidResponse through a URL that does not include the **ssi.ashx** file, or click a resource link.

▸To allow users to use the prompted sign in screen

This procedure requires that you modify the **Web.config** file on the computer where RapidResponse Application Server is installed. Modifying this file disconnects RapidResponse users from their sessions and they will need to sign back in after the file is saved. Consider sending a broadcast message to users alerting them about being disconnected from the system. For more information, see "Communicating with users" on page 593. For information about manually disconnecting users, see "Disconnecting users from RapidResponse" on page 601.

1. On the computer where the RapidResponse Application server is installed, using Windows Explorer, navigate to the **C:\Program Files\Kinaxis\RapidResponse\Web** folder.
2. Right-click **Web.config**, and then click **Edit**.
3. Locate the **<singleSignIn>** element.
4. In the **<integratedUserInterface>** section, in the **<definition>** element, do the following:
   - Change the value of the **mode** attribute to either **automatic** or **explicit**.
   - If you changed the **mode** value to **explicit** and want users to provide their credentials when clicking resource links, change the value of the **explicitUserDefaultSSI** attribute to **false**.

   If the automatic definition is used, users who do not have SSI credentials are prompted for their RapidResponse user ID and password.

   If the explicit definition is used, only users who access RapidResponse by clicking a link that defines their user ID and password are given the SSI interface. Others are prompted for their user ID and password. If the **explicitUserDefaultSSI** parameter is set to **false**, a user clicking a resource link is always prompted for their user ID and password.

CHAPTER 54: Configuring single sign-in for On-Demand

This section applies to the On-Demand service only. If you are using RapidResponse On-Premises, see " Configuring single sign-in for On-Premises" on page 835.

About single sign-in 863
Implementing single sign-in 865

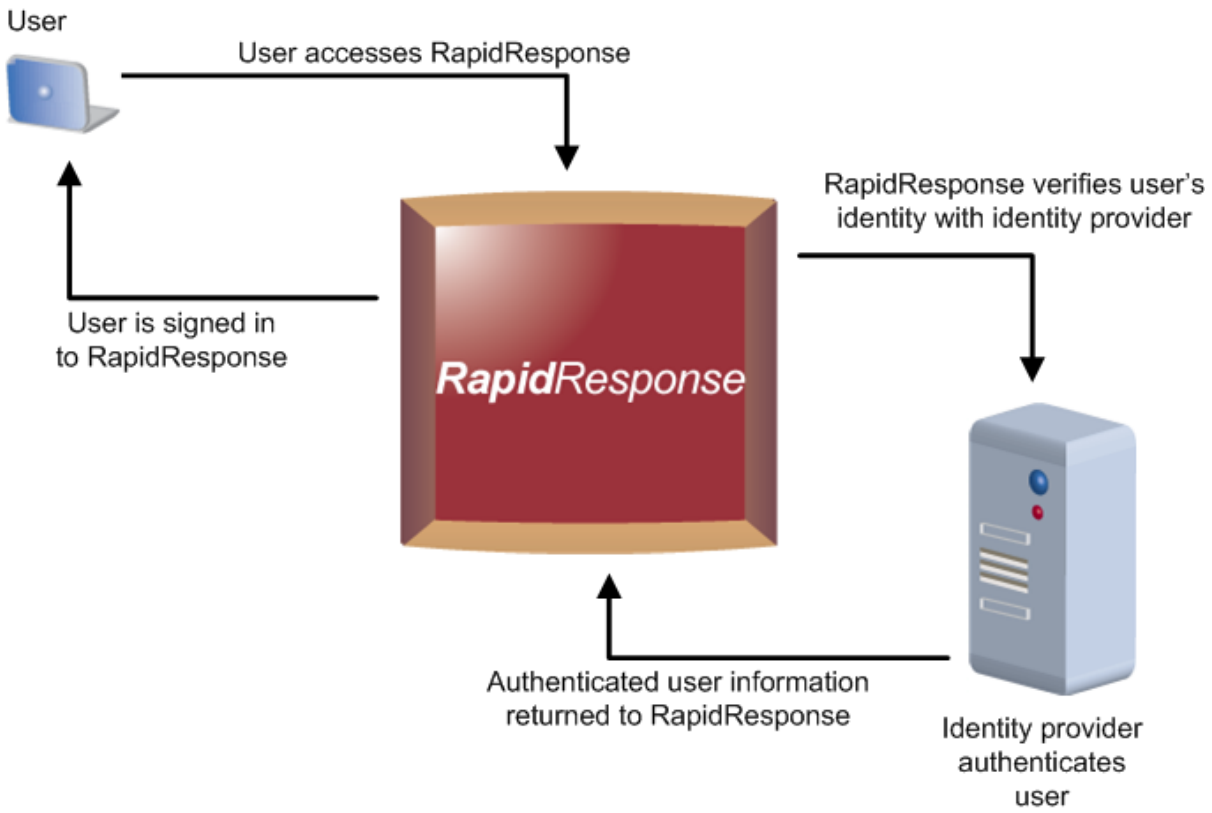
Single sign-in (SSI) allows users to sign in to RapidResponse using credentials authenticated by an identity provider. This can prevent unnecessary administrative work changing passwords for users who have forgotten them, and unlocking accounts for users who have entered their password incorrectly.

Enabling SSI also provides increased security by allowing only trusted users to sign in.

About single sign-in

If your company uses an identity provider that conforms to the Security Assertion Markup Language V2.0 (SAML2) standard, you can integrate RapidResponse with that provider to create a trust relationship, which allows authenticated users to sign in to RapidResponse.

When a user accesses RapidResponse, RapidResponse sends a request to the identity provider for that user's authenticated identity. The identity provider verifies the user's identity, and then responds to RapidResponse with an assertion that the user is authentic. The user can then sign in to RapidResponse using the authenticated identity, as shown in the following illustration. For more information, see "Implementing single sign-in" on page 865.



This section discusses the skills and knowledge required to use RapidResponse SSI, and the limitations of SSI.

Required skills and knowledge

Integrating RapidResponse with your identity provider requires familiarity with the SAML 2.0 Web SSO profile specification and your identity provider. You must be familiar with how to obtain and work with federation metadata, including how to integrate the metadata of other applications to create a trust relationship.

Your identity provider's metadata can be provided for and imported into RapidResponse, and RapidResponse's metadata can be provided for the identity provider. You can work with Kinaxis Customer Support to exchange this metadata and ensure both systems are properly configured.

For more information about the SAML2 specification, go to http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

Limitations of single sign-in

You must create users in RapidResponse to use SSI. You cannot access RapidResponse using your identity provider if you do not have a corresponding account in RapidResponse.

Implementing single sign-in

If your company already has a single sign-in environment that uses an identity provider with SAML2 authentication, you can integrate RapidResponse into this environment. User accounts must be the same in RapidResponse and your identity provider.

To integrate RapidResponse with your identity provider, each program's federation metadata can be provided for the other. This metadata is an XML file that describes how the application and identity provider can interact with each other.

Using the information specified in the metadata, the identity provider can process authentication requests coming from RapidResponse, and RapidResponse can process responses coming from the identity provider. A trust relationship is established between the identity provider and RapidResponse using the metadata, so the user can sign in to RapidResponse using the identity provider's information.

To improve security, the requests and responses between RapidResponse and the identity provider can be encrypted using HTTPS. You can also encrypt SAML assertions using public key encryption with x.509 certificates. These certificates can be configured by Kinaxis Customer Support.

When users sign in using the identity provider, their sign-in experience is provided by that system. Accessing RapidResponse launches the identity provider's authentication, which allows the user to sign in to RapidResponse.

Implementing an SSI environment using SAML2 authentication includes the following steps:

1. Create RapidResponse user accounts that are mapped to the user accounts defined in the identity provider. For more information, see "User accounts for SAML2 authentication (step 1)" on page 865.
2. Obtain the metadata from the identity provider. For more information, see "Obtaining the identity provider metadata (step 2)" on page 866.
3. Obtain the metadata from RapidResponse for use in the identity provider. For more information, see "Obtaining RapidResponse metadata (step 3)" on page 866.
4. Provide users with the link to sign in to RapidResponse. For more information, see "Providing the link to sign in to RapidResponse (step 4)" on page 866.

User accounts for SAML2 authentication (step 1)

When SAML2 authentication is used, the identity provider returns a NameID to RapidResponse, which must map to a RapidResponse user ID. Even though a password is required when creating a user account, SAML2 authentication does not require a user's RapidResponse password to sign in. Because the password is not used to sign in, you can choose to not tell users what their RapidResponse passwords are.

Because users do not know their passwords, the passwords should be set to never expire and the users should not be allowed to change their passwords. If a password expires, the user will be unable to change it or sign in, and might be locked out of RapidResponse. If the password can be changed, the user is prompted to change the password the first time they sign in to RapidResponse.

If your company is installing RapidResponse for the first time, you should ensure that for each user you create, the RapidResponse user ID is available as a NameID from your identity provider.

If your company is upgrading RapidResponse, your existing user accounts might not be appropriate for your identity provider. In this case, you can copy each user and give the copy a user ID that matches the

NameID available from your identity provider. For more information about copying users, see "To duplicate a user account from the Administration pane" on page 553.

If you delete a user account from the identity provider, you should also delete the user in RapidResponse. Deleted users will be unable to use SSI, but can still sign in to RapidResponse using their user ID and password if the password is known.

Obtaining the identity provider metadata (step 2)

Depending on your identity provider, the metadata might be available from a publicly accessible URL, or you might need to export it to a file. For information about how to obtain the metadata, consult your identity provider's documentation.

After you have obtained the metadata URL or file, you must provide it to Kinaxis Customer Support. If the metadata is available as a URL, you must ensure that URL is accessible outside your company's firewall. For more information, contact your network administrator.

Obtaining RapidResponse metadata (step 3)

The metadata required to integrate RapidResponse with the identity provider can be found in the following location:

`https://rapidresponse.kinaxis.com/CompanyID/saml2.metadata`

Where `CompanyID` is your company's identifier as provided by Kinaxis.

Depending on your identity provider, you can either include this URL directly in your identity provider, or you can save the metadata as an XML file and then import it. For information about including this information in your identity provider, consult your identity provider's documentation.

Providing the link to sign in to RapidResponse (step 4)

After SSI has been set up and the metadata for each program integrated, you can provide users with a link that allows them to automatically sign in to RapidResponse with their authenticated identities. Users who click the link are allowed to sign in if they are authenticated by the identity provider.

Users can sign in to the Java client using the following link:

`https://rapidresponse.kinaxis.com/CompanyID/saml2`

Users can sign in to the web client using the following link:

`https://rapidresponse.kinaxis.com/Mobile/CompanyID/saml2`

Where `CompanyID` is your company's identifier as provided by Kinaxis.

Allowing users to use prompted sign in

Users who receive their RapidResponse messages in their email can click resource links, which opens the resource in RapidResponse. If the user does not have RapidResponse open when they click the link, it is launched and they are signed in. By default the user is signed in automatically, but you can choose to require users to enter their credentials. This allows you to ensure only valid users can access RapidResponse by clicking these links.

If you allow users to provide credentials, each user must know their RapidResponse password. However, they will only need to enter their password when they launch RapidResponse from a resource link or if they sign out.

To request users be allowed to provide their credentials, contact Kinaxis Customer Support.

Part 8: Data Publishing

- "Setting up for data publishing for On-Premises" on page 871
- "Setting up for data publishing for On-Demand" on page 889

CHAPTER 55: Setting up for data publishing for On-Premises

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, see "Setting up for data publishing for On-Demand" on page 889.

RapidResponse-to-RapidResponse connection 871
Steps to configure data publishing 873
Creating the publisher ID record 873
Data required for publishing 874
Installing the Data Transfer Client for data publishing 875
Moving data to the Data Transfer Client computer 881
Configuring global data transfer settings 881
Configuring data feeds and file locations 882
Defining and configuring subscribers 885
Providing users with data publishing resources and permissions 887

Companies that publish data (publishers) to brand owners (subscribers) need to set up RapidResponse so that designated users within their company can quickly publish relevant data to customers. Publishing of data is enabled by the RapidResponse-to-RapidResponse connection. You can publish to subscribers who are using either a version of RapidResponse hosted at the RapidResponse Data Center (On-Demand), or a version of RapidResponse installed at their own site (On-Premises).

This chapter describes the RapidResponse-to-RapidResponse connection and outlines the steps you must take to set up RapidResponse for publishing data. This includes configuring publisher and subscriber settings in RapidResponse, as well as installing and configuring the RapidResponse Data Transfer Client to securely transfer data across the Internet to your subscribers.

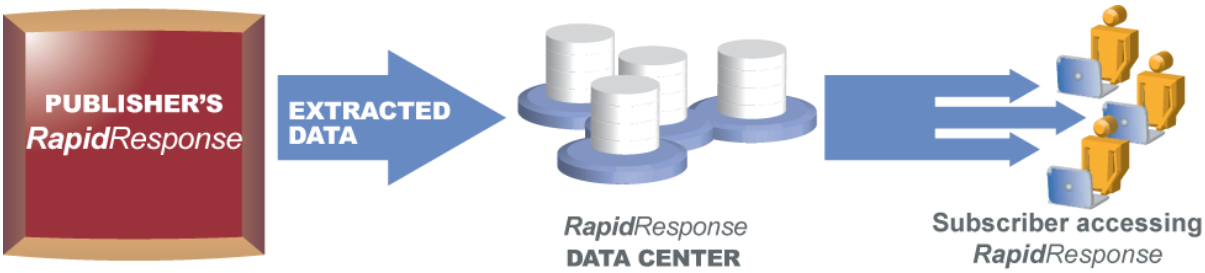
This instance of the Data Transfer Client is configured specifically for the data publishing process. If you are not publishing data and want to use the Data Transfer Client for transferring data from your data sources to the RapidResponse Data Center, see the *RapidResponse Data Integration Guide*.

Note: Configuration of the RapidResponse Data Transfer Client is done through the Data Transfer Settings dialog box. This dialog box is accessed from a command prompt by running a script installed with the Data Transfer Client.

RapidResponse-to-RapidResponse connection

A RapidResponse-to-RapidResponse connection provides the unique ability to publish data from one instance of RapidResponse into another, giving brand owners (subscribers) visibility into their contract

manufacturers' (publisher's) supply chain data. The following illustrates the concept of the RapidResponse-to-RapidResponse connection.



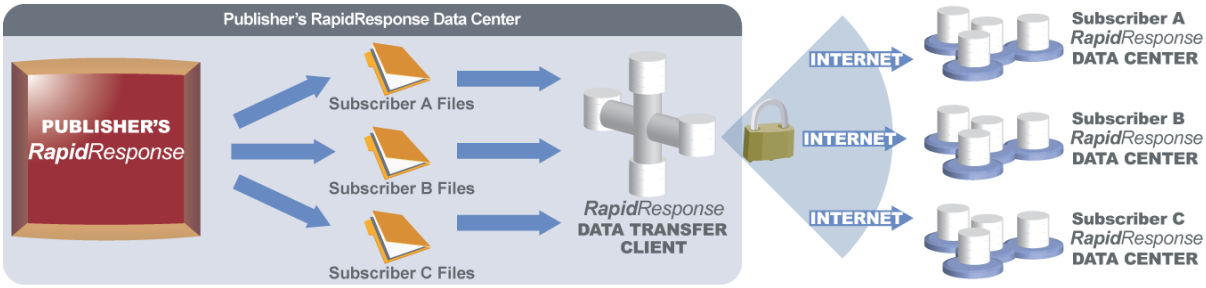
As a contract manufacturer, you can enhance the value your company provides to customers by publishing data to customers. You can participate in a RapidResponse-to-RapidResponse connection at no cost to your company. Depending on your customer's configuration, you either publish data directly to a RapidResponse site they maintain or, as shown in the above image, to a hosted service provided by Kinaxis and paid for by your customer.

Publishing data provides you with the following benefits:

- Enhanced customer service.
- Decreased need for your company's IT organization to satisfy customer requirements for data visibility.
- Your customers are empowered to gain their own visibility and perform analysis using RapidResponse.
- Synchronized view of data for you and your customers.

Publishing subscriber data

After you complete the initial setup of RapidResponse for data publishing, other users in your company can publish data to subscribers. Subscriber data is extracted to a network location and then transferred to either the RapidResponse Data Center (On-Demand) or a site the subscriber maintains (On-Premises). The following illustration outlines how data is moved from your company's RapidResponse system to a location where the subscriber can view it.



The data extracted from your RapidResponse system is defined in a Data Publish workbook. To control the data that each subscriber receives, you create a filter identifying each subscriber's parts. The data is exported into a series of extract files using a RapidResponse scheduled task. The extract files are then

automatically moved to the RapidResponse Data Transfer Client. The RapidResponse Data Transfer Client then sends the extract files through an Internet connection using the SFTP (SSH) protocol to each subscriber.

Steps to configure data publishing

This section outlines the steps for setting up RapidResponse to enable other users in your company to publish data to subscribers, and setting up the RapidResponse Data Transfer Client for secure data transfers to your subscribers.

Step	Description
Ensure RapidResponse holds the appropriate data.	You might need to make some minor additions to your RapidResponse data set in order to ensure subscribers are provided with the necessary and relevant data. For example, you might need to add a subscriber's part names. For more information, see "Data required for publishing" on page 874. Ensure all required data is in the RapidResponse database. You might need to work with your RapidResponse System Administrator at Kinaxis to import data.
Install the Data Transfer Client.	The RapidResponse Data Transfer Client is used to securely transfer extracted data across the Internet to the RapidResponse Data Center or a subscriber's site. This tool must be downloaded from the Kinaxis Knowledge Network and installed on the appropriate computer. For more information, see "Installing the Data Transfer Client for data publishing" on page 875.
Move data to the Data Transfer Client computer.	In order for the RapidResponse Data Transfer Client to send data to a subscriber, the data must first be moved from the RapidResponse computer where it was extracted to the computer where the Data Transfer Client is installed or a folder the Data Transfer Client monitors. Scripts should be written to carry out this process. For more information, see "Moving data to the Data Transfer Client computer" on page 881.
Configure global data transfer settings.	Initial configuration of the Data Transfer Client has several steps. This includes specifying FTP accounts and passwords associated with connections to the RapidResponse Data Center. For more information, see "Configuring global data transfer settings" on page 881.
Define and configure subscribers.	For each new subscriber you want to add, you define them in RapidResponse and identify the user responsible for publishing data to them. The Data Transfer Client also needs to be configured to support connections to the subscriber. For more information, see "Defining and configuring subscribers" on page 885.
Provide users with data publishing resources and permissions.	Users responsible for publishing data to subscribers require scheduled task, filter, and workbook authoring permissions, as well as access to the Data Publish workbook. For more information, see "Providing users with data publishing resources and permissions" on page 887.

Creating the publisher ID record

To enable the adding of subscribers and allow users to publish data to them, you must create a publisher ID configuration record in RapidResponse. The publisher ID value is provided to you by Kinaxis.

▸To create the publisher ID record

1. In the **Administration** pane, under **System Settings**, click **Configuration**.
2. Click the **Processing Rules** tab.
3. On the **Edit** menu, click **Insert Record**.
4. In the Insert Record dialog box, do the following:
   - In the **ID** box, type **DataPublisher**.
   - In the **Value** box, type the publisher ID provided to you by Kinaxis.
   - Optionally, in the **Comments** box, type a description of this record.
5. Click **Save and Close**.

Data required for publishing

To maximize the value that your customers derive from your RapidResponse data, you might need to make a few minor additions to the data.

For the subscriber to get value from resources in RapidResponse (such as workbooks), the subscriber needs data that reflects the in-transit lead time added to your company's due date. The **IndependendDemand.DueDate** field in the RapidResponse data model stores the due date for which a demand is due at your company's site. However, a subscriber will want to know the date when the demand is to be delivered at their site. It is expected that, for data publishing purposes, this date is stored in the **IndependentDemand.PromisedDate** field. If you don't already store the subscriber's due date in this field, then you need to change the column expression of this column in the Data Publish workbook to refer to the field that does store it. For example, you might store this data in a custom field. For information about customizing the Data Publish workbook, see "Customize the Data Publish workbook" in the *RapidResponse User Guide*.

Additionally, the subscriber also requires information about supplies that are currently in transit. To ensure that this information is available, populate the following tables with your company's in-transit data:

- CustomerDelivery
- CustomerOrder
- CustomerPart
- CustomerShipment

The **CustomerDelivery** table refers to an entry in the IndependentDemand table. This reference must be maintained by keeping the IndependentDemand in the RapidResponse database until the shipment is received by the subscriber. To prevent the processing of shipped IndependentDemands by the planning analytics, set **Order.Type.ProcessingRule** to "Ignore".

Reference part data

Most subscribers (brand owners) do not use the same part naming system as their publishers. To help subscribers understand how your part names relate to their company's part names, you need to include the subscriber's part names in the data extracted from your RapidResponse system.

The Data Publish workbook includes a ReferencePart worksheet where the subscriber's part names can be defined. The worksheet contains three columns: Name, Site, and a Reference Part column. If your

company has added a field to the Part table that stores the subscriber part names, then change the column expression of the Reference Part column to use the field that stores the subscriber's part name data.

If the subscriber's part name data is available only in an enterprise data source outside of RapidResponse, then you need to import this data into RapidResponse. If your company is not using the ProductGroup1 or ProductGroup2 fields on the Part table, you can import the subscriber part information into one of these fields and then change the column expression of the Reference Part column to use the field.

If the subscriber's part data is available in a text file, you can provide this file to Kinaxis so that the data in the file can be imported into the subscriber's RapidResponse.

You can also do the following:

- Create a tab-delimited text file, with the same 3 columns of data as in the ReferencePart worksheet. This file can be created, for example, by extracting data from your ERP system. This file must be accessible by the RapidResponse Server.
- Set the filter expression on the ReferencePart worksheet in the Data Publish workbook to "FALSE".
- Modify the scheduled task for the subscriber so that its post-process command calls a script which copies this data file into the appropriate subscriber folder.

Hiding data

The Data Publish workbook is used in the data publishing process and is available to all administrators; however, it is not accessible to other users.

Users who are responsible for extracting subscriber data are likely to customize the Data Publish workbook according to the information required by each subscriber. You might want to customize the Data Publish workbook to ensure that certain types of data are not made available to the subscriber; however, it is recommended that no columns be added to this workbook. Do not remove any column from this workbook. For information about customizing this workbook and the complete list of changes that should not be performed, see "Customize the Data Publish workbook" in the *RapidResponse User Guide*.

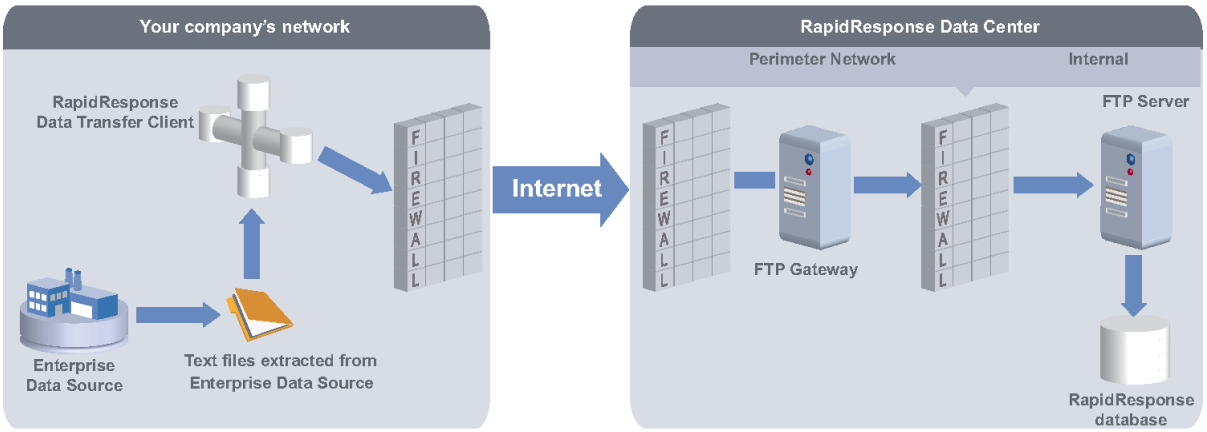
Installing the Data Transfer Client for data publishing

This section applies only to the data publishing process. If you are installing the Data Transfer Client to transfer data from your data sources to the RapidResponse Data Center, see "Installing the Data Transfer Client" in the *RapidResponse Data Integration Guide*.

RapidResponse Data Transfer Client transfers extracts of subscriber data to either the RapidResponse Data Center (On-Demand) or a subscriber maintained site (On-Premises). It can be installed as a Windows service, or on Linux platforms as a crontab process.

RapidResponse Data Transfer Client monitors for extracts of subscriber data received from your RapidResponse Server computer. When a new data extract is received for a given subscriber, the Data Transfer Client securely transfers this data across the Internet to either the RapidResponse Data Center or the subscriber's site. As shown in the following illustration, sent data extracts pass through two

separate servers. The first is the FTP Gateway, located in the Perimeter Network, that serves incoming traffic. Data files are never stored on this server, which delegates processing to the second server, the FTP Server. The FTP Server is located inside the inner firewall, and receives the extract data passed on from the FTP Gateway. It then immediately passes the data on to the computer where RapidResponse is installed so it can subsequently be used in a data import or update and viewed by the subscriber. After the extract data is moved into RapidResponse, it is deleted from the FTP Server.



SFTP data transfers rely on a secure shell (SSH2) communication between the RapidResponse Data Transfer Client and either the RapidResponse Data Center or subscriber site. For authentication, the use of public/private keys is supported. A single port, typically port 22, is used for both communication and file transfers, and this port is required to be open on your company's firewall.

Notes:

- After each file is transferred to the Data Center, its integrity on the FTP Server is verified to ensure the file was transferred accurately, and it is automatically retransmitted if necessary.
- At subscriber hosted sites, the RapidResponse Server is installed on the same computer as the FTP Server.
- Before transferring the files, the Data Transfer Client compresses all the files into a file named **temp.zip**. On arrival at the Data Center, the **temp.zip** file is decompressed. Alternatively, you can set up your extract program to compress the files that are to be transferred into a single ZIP file. This might make it easier and more efficient to transfer the files over your internal network.

Installation for Windows

The RapidResponse Data Transfer Client for Windows is installed as a Windows service named **RapidResponseDataTransferClient**. It is distributed in a .ZIP archive file named **DataTransferClient-Windows.zip** and is available for download from the Kinaxis Knowledge Network. (Just paste the file name into the search bar.)

Before installing the Data Transfer Client, ensure the Windows computer meets the following system requirements.

Requirement	Supported and Verified
Operating System	Microsoft Windows Server 2012 Standard Microsoft Windows Server 2012 Standard R2 Microsoft Windows Server 2012 Datacenter Microsoft Windows Server 2012 Datacenter R2 **Note:** In addition to the using the correct Windows Service Pack (SP), it is advisable that the operating system also include the latest Windows Updates.
Operating system components	The Data Transfer Client requires the **Microsoft Visual C++ 2010 Redistributable Package (x64)**. This might not be installed with your operating system. If not installed, it can be downloaded from the Microsoft Download Center at https://www.microsoft.com/en-ca/download/details.aspx?id=14632.
Java Runtime Environment (JRE)	Oracle Java Runtime Environment (JRE), version 8 (all updates). The Data Transfer Client supports the 64-bit version of the JRE. You can test the version of the JRE you are using by visiting http://www.java.com/en/download/help/testvm.xml. You can also download the latest version of the JRE by visiting http://www.java.com/en/.
Processor	Intel Xeon 64-bit, 2-way, 3.0 GHz (supporting Intel Extended Memory 64 Technology or EM64T)
Physical memory	4 GB of RAM Increasing physical memory might improve performance in cases where data transfers are large (more than 2 GB).
Hard disk space	10 GB

To install the Data Transfer Client, you must be logged onto Windows using an account that has administrative privileges on the computer where it is to be installed. As well, the computer you are installing the Data Transfer Client on must be able to create outgoing FTP command and data connections. If you will be configuring network locations to read data from, you must be logged onto Windows using an account that has privileges to read and modify data on each network location. For more information, see "Configuring data feeds and file locations" on page 882.

Configurations for your RapidResponse environments are provided by Kinaxis Customer Support. These consist of the Kinaxis FTP accounts for each system, and are provided as a folder that you can copy into your Data Transfer Client installation. If you have not been provided this information, contact Kinaxis.

If you are configuring the Data Transfer Client manually, you must configure FTP account settings, such as the user name and password the Data Transfer Client will use when connecting and transferring data. This information is provided by Kinaxis Customer Support.

After installation, you can run a test to ensure the Data Transfer Client has been successfully configured and is able to transfer data to the RapidResponse Data Center.

▸To install the Data Transfer Client on a Windows computer

1. Extract the contents of the **DataTransferClient-Windows.zip** archive to the location where the Data Transfer Client is to be run from. When extracting, ensure that the **Use folder names** and **All files/folders in archive** options are selected. This preserves the **KinaxisDataTransfer** folder structure as shown in "Folder structure and files" on page 879.
2. If this is a new installation, copy the **conf** folder provided to you by Kinaxis into the **KinaxisDataTransfer** folder.

If you are configuring the Data Transfer Client manually, copy the **conf-sample** folder, and name the copy **conf**. The **datatransferclient.properties** file found in this folder is required for initial configuration of the Data Transfer Client, and is installed in a sample folder to avoid overwriting any existing customized files during an upgrade. When you run the Data Transfer Client or open the **Data Transfer Client Settings** dialog box for the first time, the properties file is replaced by **datatransferclient.settings** which is an encrypted file that can only be viewed and edited through the **Data Transfer Client Settings** dialog box.

3. Open a **Command Prompt** window, and ensure you are running it as an administrator.
4. Install and start the Windows service process by running the command script in **InstallAndStart.cmd** from the **KinaxisDataTransfer** folder.

Note: After installation, the Data Transfer Client needs to be configured once with your Publisher ID and other global settings as discussed in "Configuring global data transfer settings" on page 881. Subsequently, it needs to be configured to support each new subscriber you add as discussed in "Configuring subscribers for data transfers" on page 886.

▸To uninstall from a Windows computer

1. Run the command script in **Uninstall.cmd** from the **KinaxisDataTransfer** folder.
2. Delete all files in the **KinaxisDataTransfer** folder.

Installation for Linux

The RapidResponse Data Transfer Client for Linux operating systems is installed as a crontab task. It is distributed in a .ZIP archive file named **DataTransferClient-Unix.zip** which is available from the Kinaxis Knowledge Network. (Just paste the file name into the search bar.)

In order to install the Data Transfer Client, you must be logged on using the account under which the Data Transfer Client will run; this must be an account which is allowed to execute crontab. As well, the computer you are installing the Data Transfer Client on must be able to create outgoing FTP commands and data connections.

Before installing the Data Transfer client, contact Kinaxis Customer Support to ensure the UNIX computer meets the system requirements. For more information, visit www.kinaxis.com.

▸To install the Data Transfer Client on a UNIX computer

1. Extract the contents of the **DataTransferClient-Unix.zip** archive to the location where the Data Transfer Client is to be run from (for example, the home directory of the current user). When the archive is extracted, the **KinaxisDataTransfer** directory structure is created as shown in "Folder structure and files" on page 879.
2. Ensure that execute permissions are set on the scripts in the run directory. Type the following command from a command prompt with the current working directory set to the **KinaxisDataTransfer** directory:

   ```
   chmod +x *.sh
   ```

3. If this is a new installation, copy the **conf** directory provided to you by Kinaxis into the **KinaxisDataTransfer** directory.

If you are configuring the Data Transfer Client manually, copy the **conf-sample** directory, and name the copy **conf**. The **datatransferclient.properties** file found in the **conf-sample** directory is required for initial configuration of the Data Transfer Client, and is installed in a sample folder to avoid overwriting any existing customized files during an upgrade. When you run the Data Transfer Client or open the **Data Transfer Client Settings** dialog box for the first time, the properties file is replaced by **datatransferclient.settings**, which is an encrypted file that can only be viewed and edited through the **Data Transfer Client Settings** dialog box.

4. Install and start the RapidResponse Data Transfer Client background process by running the shell script in **InstallAndStart.sh** (that is, **./InstallAndStart.sh**). This script must be run with the **KinaxisDataTransfer** directory as the current working directory.

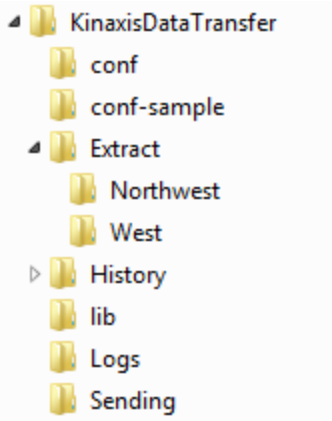
Note: After installation, the Data Transfer Client needs to be configured once with your Publisher ID and other global settings as discussed in "Configuring global data transfer settings" on page 881. Subsequently, it needs to be configured to support each new subscriber you add as discussed in "Configuring subscribers for data transfers" on page 886.

▸To uninstall from a Linux computer

1. Run the shell script in **Uninstall.sh**. This script must be run with the **KinaxisDataTransfer** directory as the current working directory.
2. Delete all files in the **KinaxisDataTransfer** folder.

Folder structure and files

Installing the RapidResponse Data Transfer Client creates the **KinaxisDataTransfer** folder structure shown in the following illustration.



The **KinaxisDataTransfer** root folder contains the scripts used to install, start, configure, and test the RapidResponse Data Transfer Client. It also contains the following sub-folders.

Folder	Description
conf	This folder contains various files used to configure the RapidResponse Data Transfer Client. For example: • **datatransferclient.settings** is created the first time you run the Data Transfer Client or open the Data Transfer Client Settings dialog box, and contains details of connections to the RapidResponse Data Center (username, password, frequency at which the Data Center is checked for new files to download, and so on). This file is encrypted. • **log.properties** is used to configure aspects of the logging functionality associated with the Data Transfer Client (size of the log file, which log entries are persisted, and so on). Changes made to these files while the Data Transfer Client is running are recognized without any need to restart it. Typically, these changes take place within 5 minutes. This folder is manually created during the installation process.
conf-sample	This folder contains various files used as templates for configuring the RapidResponse Data Transfer Client. If you have not been provided a configuration by Kinaxis, you can copy this folder to create the **conf** folder.
Extract	This folder is monitored by the Data Transfer Client for new extract data. This folder contains a subfolder for each data source for which a data extract is provided. The subfolders cannot contain additional subfolders. For example, **\Extract\Northwest\Area1**. In this case, the **Area1** subfolder would be ignored during processing. This folder is created automatically when you test an FTP account, or you can create it. In addition to this folder, you can configure additional folders or network locations to be monitored for new data. For more information, see "Configuring data feeds and file locations" on page 882. Typically, these file locations contain data extracts provided by the RapidResponse Extractor, which are typically stored in folders on the computer the Extractor is installed on.
History	This folder contains historical extracts that have been successfully sent to the RapidResponse Data Center. Each subfolder for a given data feed has a date and time stamp appended to the data feed name. If you have defined multiple file locations for the Data Transfer Client to read data from, a History folder is created in each specified location. These History folders store the transfer history for each extract from each file location.
Inbound	This folder stores files downloaded from the RapidResponse Data Center (typically, reports generated by alerts). If a file is downloaded with the same file name as an existing file in this folder, the existing file is replaced. **Note:** This folder is created when the Data Transfer Client first connects to the FTP Server at the Data Center to download files. It is not created during installation of the Data Transfer Client.
lib	This folder contains Java classes used by the RapidResponse Data Transfer Client.
Logs	This folder contains the log files used to track events from the Data Transfer Client (for example, when monitoring of the Extract folder has started or stopped, when a data transfer has started or completed, and so on).
Sending	This folder contains extracts which are currently being sent to the RapidResponse Data Center. When the Data Transfer Client detects a new extract in the Extract folder, it immediately moves the extract to this folder for sending. If you have defined multiple file locations for the Data Transfer Client to read data from, a Sending subfolder is created for each data feed. These Sending subfolders are used to send the data from each file location to the RapidResponse Data Center.

Moving data to the Data Transfer Client computer

The data extracted for each of your subscribers is placed in a folder named in accordance with their SubscriberId. This folder is located under the "DataPublishRoot" folder which by default is set to **C:\RapidResponse\Data Publish** (as defined by the DataPublishRoot configuration record). You can modify the default location from the **File Locations** worksheet in the **RapidResponse Administration** workbook. To open this workbook, in the **Administration** pane, under **System Settings**, click **Configuration**.

From there, the files must be transferred to the computer where the RapidResponse Data Transfer Client is installed. To move the data extract files, a target folder needs to be created on the computer where the RapidResponse Data Transfer Client is installed. You also need to create a script that performs the following steps:

1. Monitors the sub-folders of the root Data Publisher folder on the RapidResponse Server computer, for a file called **extract.done**. This file is created when a data extract is completed.
2. If no **extract.done** file is found, the script should pause briefly and then continue monitoring the sub-folders. If the file is located, the script should perform the following:
   - Create a folder in the Extract folder on the Data Transfer Client computer named in accordance with the SubscriberId of the subscriber for which an **extract.done** file was located (if such a folder does not already exist).
   - Copy all of the files from the subscriber folder on the RapidResponse Server computer to the subscriber folder on the Data Transfer Client computer.
   - Create an **extract.done** file in the subscriber folder on the Data Transfer Client computer.
   - Delete the content of the subscriber folder on the RapidResponse Server computer.

You can also configure the Data Transfer Client to monitor additional folders and network locations for new data extracts. The same process of moving data to these folders can be used, with the files being copied to a target folder in the folder being monitored. For more information, see "Configuring data feeds and file locations" on page 882.

Configuring global data transfer settings

If you are sending data to On-Demand RapidResponse subscribers (hosted at the RapidResponse Data Center), then you need to configure aspects of your connection to the RapidResponse Data Center.

Configurations for your On-Demand subscribers are provided by Kinaxis Customer Support. These consist of the Kinaxis FTP accounts for each system, and are provided as a folder that you can copy into your Data Transfer Client installation. If you have not been provided this information, contact Kinaxis.

If you are configuring the Data Transfer Client manually, you must configure FTP account settings, such as the user name and password the Data Transfer Client will use when connecting and transferring data. This information is provided by Kinaxis Customer Support. For more information about

If you are sending data to On-Premises RapidResponse subscribers (hosted at their own sites), you must configure the connection to your On-Premises subscribers by configuring the FTP server information the subscriber has provided for you. For more information, see "Defining and configuring subscribers" on page 885.

1. With **KinaxisDataTransfer** as the current folder, do one of the following to open the **Data Transfer Client Settings** dialog box.
   - In a Windows environment, run the command script in **Settings.cmd**.
   - In a Linux environment, run the shell script in **Settings.sh**.
2. If you need to create additional FTP accounts, in the **Data Transfer Client Settings** dialog box, click the **Kinaxis FTP Accounts** tab.

   Otherwise, go to step 6.
3. Click **New**.
4. In the **New Kinaxis FTP Account** dialog box, specify the following information:
   - **Username**—The user account to use to log in to the FTP server.
   - **Password**—The password for the user account.
   - **Confirm new password**—Repeat the password.
   - **Host**—The FTP server to connect to.
   - **Description**—Optional information about the FTP server.
5. If necessary, change the port number in the **Port** box.
6. Test the FTP accounts by doing the following:
   - On the **Kinaxis FTP Accounts** tab, select the FTP account you want to test.
   - Click **Test**.
   - Verify that the sample file has been sent to the RapidResponse Data Center by viewing the outbound log file for the FTP account located in the **Logs** folder. The last entry in this file should indicate a category name of **RapidResponse.DataTransferClient.Complete**.
7. Click the **Data Feeds** tab.
8. Click **New**.
9. In the **New Data Feed** dialog box, specify the following:
   - **File location**—The folder or network location that data extracts are available from.
   - **Kinaxis FTP account**—The FTP account to send data to.
   - **Data feed is**—**Enabled** if you want to begin sending data immediately.
10. Click **Ok**.

Notes:

- For more information about FTP account options, see "Defining and configuring subscribers" on page 885.
- Testing an FTP account also creates the Extract folder, which is typically monitored for new data to send to the RapidResponse Data Center. For more information, see "Folder structure and files" on page 879.
- For more information about data feeds, see "Configuring data feeds and file locations" on page 882.

Configuring data feeds and file locations

You can configure the Data Transfer Client to send data from multiple data sources, or file locations, to the RapidResponse Data Center. This can include multiple subfolders in the Data Transfer Client's Extract folder, as well as locations other processes copy data to. For example, if you are extracting data for multiple subscribers and have extracts that are stored in their own folders, you can configure the Data

Transfer Client to take data from each extract's individual folder and send the relevant data to each subscriber. You can specify up to 100 data sources for the Data Transfer Client.

Each data source you specify can contain multiple folders, each of which is treated as a separate source folder. Each source folder in all data sources that provide data to the same subscriber FTP account must be uniquely named, because these source folders are combined in the RapidResponse Data Center. If any source folders were not unique, the data would be merged, which might lead to unexpected results.

For each file location, including the Data Transfer Client's Extract folder, you can define each subfolder in that folder as a separate data source if you do not want to send all data to all FTP accounts. When you define these data sources, you must ensure the subfolder names match the data sources defined in the RapidResponse instances. Typically, you manually create these subfolders, however, an automated process can also create them. Regardless, the subfolders must exist before you can define data feeds for them.

Data sources are associated with subscriber FTP accounts to create data feeds. Depending on your data requirements, you might require the same data to be sent to multiple RapidResponse systems. In this case, Kinaxis Customer Support will configure a process to copy the data to the systems that require it. If you define multiple data feeds to send the same data to the corresponding FTP accounts, the data will be duplicated at each RapidResponse system.

Extracts from any data feed are sent to the Data Center only if the extract.done file is created in the folder. You can also configure how often the Data Transfer Client scans for new data to send, and when any extract folder with an extract.done file is located, that data is sent to the Data Center.

If you are creating data feeds that take data from locations on your network, you must have permission to read and write to directories on the computers where you are defining the file locations. Data must be able to be removed from the source location when it is sent to the RapidResponse Data Center.

Each data feed you specify creates a Sending and History subfolder in the KinaxisDataTransfer History and Sending folders, if they do not already exist. These folders are used to send the data files to the RapidResponse Data Center and to store data extract history. For more information about the folders used for transferring data, see "Folder structure and files" on page 879.

▸To specify a data feed

1. With **KinaxisDataTransfer** as the current folder, run the command script or shell script in **Settings.cmd**.
2. In the **Data Transfer Client Settings** dialog box, click the **Data Feeds** tab.
3. Click **New**.
4. In the **New Data Feed** dialog box, in the **File location** box, do one of the following:
   - Click **Browse**, navigate to the folder or location you want to take data from, and then click **OK**.
   - Type or paste the folder or network location you want to take data from.
5. In the **Kinaxis FTP account** list, select the subscriber FTP account you want this data feed to provide data for.
6. In the **Data feed is** area, click one of the following:
   - **Enabled**—The data feed is actively monitoring for new data and will send files when detected.
   - **Disabled**—The data feed doe snot send data.
7. Click **OK**.

Notes:

- Each data folder in the file locations you specify must have a unique name.

- If you specify a network location, you must be logged on with a user account that has permission to read and modify data in that location. Otherwise, you cannot add that location.

▸To modify a data feed

1. With **KinaxisDataTransfer** as the current folder, run the command script or shell script in **Settings.cmd**.
2. In the **Data Transfer Client Settings** dialog box, click the **Data Feeds** tab.
3. Select the data feed you want to modify, and then click **Edit**.
4. To change the data source folder, in the **File location** box, do one of the following:
   - Click **Browse**, navigate to the folder or location you want to take data from, and then click **OK**.
   - Type or paste the folder or network location you want to take data from in the **Folder** box.
5. To change the FTP account the data feed provides data for, in the **Kinaxis FTP account** list, select the subscriber FTP account.
6. In the **Data feed is** area, do one of the following:
   - To start sending data from this data feed, click **Enabled**.
   - To stop sending data from this data feed, click **Disabled**.
7. Click **OK**.

Notes:
- Each data folder in the file locations you specify must have a unique name.
- If you specify a network location, you must be logged on with a user account that has permission to read and modify data in that location. Otherwise, you cannot add that location.

▸To specify how often to check for new data

1. In the **Data Transfer Client Settings** dialog box, click the **Data Feeds** tab.
2. Click **Frequency**.
3. In the **Data Transfer Frequency** dialog box, specify the length of the period to check for new data.
4. In the list, select the period length.

Note: The minimum value you can specify is either 10 seconds or one minute. The maximum value you can specify is either 86,400 seconds or 440 minutes, which is 24 hours.

▸To remove a data feed

1. With **KinaxisDataTransfer** as the current folder, run the command script or shell script in **Settings.cmd**.
2. In the **Data Transfer Client Settings** dialog box, click the **Data Feeds** tab.
3. Select a data feed, and then click **Delete**.
4. In the confirmation dialog box, click **Yes**.

Defining and configuring subscribers

For each new subscriber, you must define the subscriber in RapidResponse and configure the RapidResponse Data Transfer Client for data transfers to that subscriber.

Defining subscribers

Before your company can publish data to a subscriber, you must define the subscriber. You must also associate a user with each subscriber. This user is then responsible for publishing data to that subscriber (and is the only user who can publish data to them).

▸To define a subscriber

1. In the **Administration** pane, under **System Settings**, click **Data Publishing Setup**.
2. Click **New Subscriber**.
3. In the **Subscriber** box, type the SubscriberID. This is either provided to your company by Kinaxis (On-Demand) or by the subscriber themselves (On-Premises).

Notes:

- Defining a subscriber adds a folder named in accordance with that subscriber's ID under the DataPublishRoot folder. This is the folder in which RapidResponse places extracts for the subscriber. By default, the DataPublishRoot folder is **RapidResponse\Data Publish** (as defined by the DataPublishRoot configuration record).
- You should define this folder as a data source for the subscriber. For more information, see "Configuring data feeds and file locations" on page 882.

▸To associate a user with a subscriber

1. In the **Administration** pane, under **System Settings**, click **Data Publishing Setup**.
2. Select the subscriber for which you want to assign a user, and then click **Select Name**.
3. In the **Select Name** dialog box, select a name and then click **OK**.

Notes:

- If you delete a user account that is defined for a subscriber, the subscriber is also deleted. Prior to deleting a user that's associated with a subscriber, associate a different user with the subscriber.
- If you assign a subscriber to a signed-in user, the subscriber is visible the next time that user signs in to RapidResponse.

▸To delete a subscriber

1. In the **Administration** pane, under **System Settings**, click **Data Publishing Setup**.
2. Select a subscriber.
3. Click **Delete**.

Note: After you delete a subscriber, any scheduled task for this subscriber will not run and should be deleted. For information about deleting scheduled tasks, see the *RapidResponse User Guide*.

Configuring subscribers for data transfers

For each new subscriber you must configure the Data Transfer Client to send data transfers to that subscriber. All subscribers can be classified as either "On-Demand", or "On-Premises", and can be configured as FTP accounts in the Data Transfer Client.

On-Demand subscribers use a version of RapidResponse hosted at the RapidResponse Data Center. Because you will have already set up the connection to the RapidResponse Data Center, the only configuration required in this case is specifying the FTP account and configuring the data feeds to supply data to it. The FTP account information can be provided by Kinaxis Customer Support. For information about data feeds, see "Configuring data feeds and file locations" on page 882.

On-Premises subscribers use a version of RapidResponse that they maintain at a site of their own. This means that you must specify the FTP server account for the subscriber's site, and configure the data feeds that supply the data for that subscriber. The subscriber must provide you with the DNS or IP address of their site, as well as the user name and password used to access that site. For information about data feeds, see "Configuring data feeds and file locations" on page 882.

▸To add a subscriber

1. With **KinaxisDataTransfer** as the current folder, run the command script or shell script in **Settings.cmd**.
2. Click the **Kinaxis FTP Accounts** tab.
3. Click **New**.
4. In the **New Kinaxis FTP Account** dialog box, specify the following information:
   - **Username**—The user account to use to log in to the FTP server.
   - **Password**—The password for the user account.
   - **Confirm new password**—Repeat the password.
   - **Host**—The FTP server to connect to.
   - **Description**—Optional information about the FTP server. This is used as a label for the FTP account when creating data feeds.
5. If necessary, change the port number in the **Port** box.
6. In the **Outbound** area, type the number of history entries to keep for each data feed.
7. In the **Inbound** area, specify how often to check for reports.

Note: You can subsequently modify the subscriber's properties by clicking **Edit**.

▸To delete a subscriber

1. With **KinaxisDataTransfer** as the current folder, do one of the following to open the **Data Transfer Client Settings** dialog:

- In a Windows environment, run the command script in **Settings.cmd**.
- In a Linux environment, run the shell script in **Settings.sh**.

2. On the **Kinaxis FTP Accounts** tab, select the subscriber to delete.
3. Click **Delete**.

Providing users with data publishing resources and permissions

Users who publish data to a subscriber are responsible for customizing the Data Publish workbook to determine the data that gets published, creating a part-based filter that returns only the subscriber's parts, and creating a scheduled task that determines when data is published. Therefore, users who are expected to set up data extracts for subscribers must have the following permissions:

- Scheduled task authoring
- Filter authoring
- Workbook authoring

Users also require access to the Data Publish workbook. After you've made any global customizations to the workbook, you can share it with users who are responsible for extracting the data for subscribers. Different users might be responsible for publishing data to different subscribers.

The Data Publish workbook uses the **yyyymmdd** date format. You should ensure this format is defined in RapidResponse. As well, the Data Publish workbook contains a worksheet based on the CPO_BaselinePlannedOrder table. This table can potentially contain a very large number of records. Therefore, to avoid problems during data publishing, you should either set the worksheet record limit to a high value or ensure that users who publish data also are granted permissions to override the worksheet record limit. For more information, see "Assigning and removing permissions" on page 517.

Users with scheduled task authoring permission can create data publishing scheduled tasks only if they have a subscriber assigned to them. For more information, see "Defining subscribers" on page 885.

Note: For more information about sharing workbooks, see the *RapidResponse Resource Authoring Guide*.

CHAPTER 56: Setting up for data publishing for On-Demand

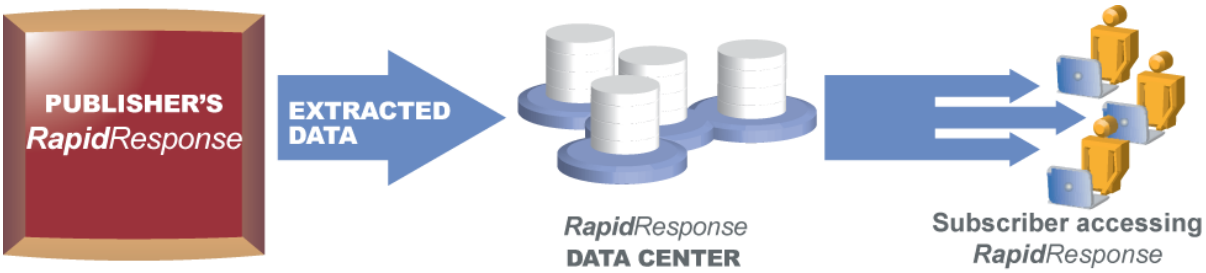
This section applies to the On-Demand service only. If you are using RapidResponse On-Premises, see "Setting up for data publishing for On-Premises" on page 871.

RapidResponse-to-RapidResponse connection 889
Summary of initial setup steps 890
Data required for publishing 891
Defining subscribers 892
Providing users with data publishing resources and permissions 893

Companies that publish data to brand owners must set up RapidResponse so that designated users within their company can quickly publish relevant data to customers. Publishing of data is enabled by the RapidResponse-to-RapidResponse connection. This chapter describes the RapidResponse-to-RapidResponse connection and outlines the steps you must take to set up RapidResponse for publishing data.

RapidResponse-to-RapidResponse connection

A RapidResponse-to-RapidResponse connection provides the unique ability to publish data from one instance of RapidResponse into another, giving brand owners (subscribers) visibility into their contract manufacturers' (publisher's) supply chain data. The following illustrates the concept of the RapidResponse-to-RapidResponse connection.



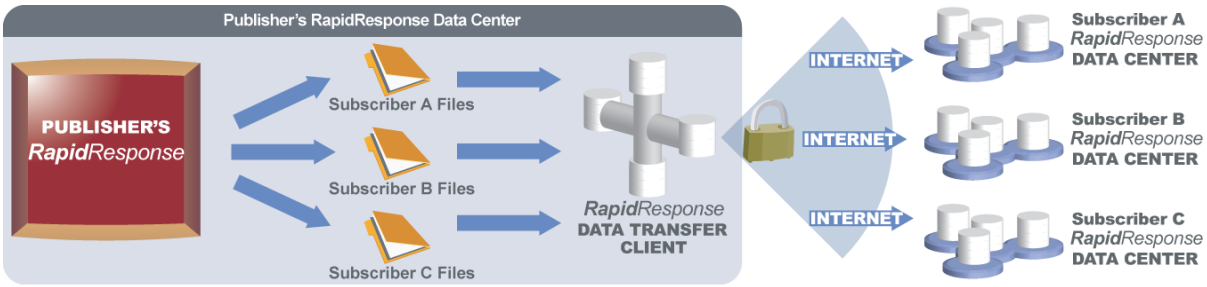
As a contract manufacturer, you can enhance the value your company provides to customers by publishing data to customers. You can participate in a RapidResponse-to-RapidResponse connection at no cost to your company. Kinaxis hosts your customer's data through a service paid for by your customer.

Publishing data provides you with the following benefits:

- Enhanced customer service.
- Decreased need for your company's IT organization to satisfy customer requirements for data visibility.
- Your customers are empowered to gain their own visibility and perform analysis using RapidResponse.
- Synchronized view of data for you and your customers.

Publishing subscriber data

After you complete the initial setup of RapidResponse for data publishing, other users in your company can publish data to subscribers. Subscriber data is extracted to a network location and then transferred to either the subscriber's RapidResponse Data Center or a RapidResponse system they maintain at their own site. The following illustration outlines how data is moved from your company's RapidResponse system to the subscriber.



The data extracted from your RapidResponse system is defined in a Data Publish workbook. To control the data that each subscriber receives, you create a filter identifying each subscriber's parts. The data is exported into a series of extract files using a scheduled task. The extract files are then automatically moved to the RapidResponse Data Transfer Client. The RapidResponse Data Transfer Client sends the extract files through a secure Internet connection to each subscriber's RapidResponse Data Center or a site they maintain.

Summary of initial setup steps

This section outlines the steps for setting up RapidResponse to enable other users in your company to publish subscriber data.

1. Ensure all required data is in the RapidResponse database. You might need to work with Kinaxis Customer Support to import data.

   This entails that you might have to customize the RapidResponse Data Publish workbook. This step is required only if you need to perform a customization that applies to all of the subscribers that will receive the published data. In addition, users responsible for publishing data will make the customizations applicable to a specific subscriber.
2. Define the subscriber and the contact person in your company who is responsible for publishing data to the subscriber.
3. Share the Data Publish workbook with users who are responsible for setting up specific subscriber data extracts.

4. Ensure that the yyyymmdd date format is defined in RapidResponse. This date format is used in the Data Publish workbook. For more information, see "Making data formats available to users and resource authors" on page 663.

Data required for publishing

To maximize the value that your customers derive from your RapidResponse data, you might need to make a few minor additions to the data.

For the subscriber to get value from certain resources in RapidResponse (such as workbooks), the subscriber needs data that reflects the in-transit lead time added to your company's due date. The **IndependendDemand.DueDate** field in the RapidResponse data model stores the due date for which a demand is due at your company's site. However, a subscriber will want to know the date when the demand is to be delivered at their site. It is expected that, for data publishing purposes, this date is stored in the **IndependentDemand.PromisedDate** field. If you don't already store the subscriber's due date in this field, then you need to change the column expression of this column in the Data Publish workbook to refer to the field that does store it. For example, you might store this data in a custom field. For information about customizing the Data Publish workbook, see the *RapidResponse User Guide*.

Additionally, the subscriber also requires information about supplies that are currently in transit. To ensure that this information is available, populate the following tables with your company's in-transit data:

- CustomerDelivery
- CustomerOrder
- CustomerPart
- CustomerShipment

The **CustomerDelivery** table refers to an entry the IndependentDemand table. This reference must be maintained by keeping the IndependentDemand in the RapidResponse database until the shipment is received by the subscriber. To prevent the processing of shipped IndependentDemands by the planning analytics, set **Order.Type.ProcessingRule** to "Ignore".

Reference part data

Most subscribers don't use the same part naming system as their publishers. To help subscribers understand how your part names relate to their company's part names, you need to include the subscriber's part names in the data extracted from your RapidResponse system.

The Data Publish workbook includes a ReferencePart worksheet where the subscriber's part names can be defined. The worksheet contains three columns: Name, Site, and a Reference Part column. If your company has added a field to the Part table that stores the subscriber part names, then change the column expression of the Reference Part column to use the field that stores the subscriber's part name data.

If the subscriber's part name data is available only in an enterprise data source outside of RapidResponse, then you need to import this data into RapidResponse. If your company isn't using the ProductGroup1 or ProductGroup2 fields on the Part table, you can import the subscriber part information into one of these fields and then change the column expression of the Reference Part column to use the field.

If the subscriber's part data is available in a text file, you can provide this file to Kinaxis so that the data in the file can be imported into the subscriber's RapidResponse.

Hiding data

The Data Publish workbook is used in the data publishing process and is available to all administrators in the Explorer; however, it's not accessible to other users.

Users who are responsible for extracting subscriber data are likely to customize the Data Publish workbook according to the information required by each subscriber. You might want to customize the Data Publish workbook to ensure that certain types of data are not made available to the subscriber; however, it is recommended that no columns be added to this workbook. Do not remove any column from this workbook. For information about customizing this workbook and the complete list of changes that should not be performed, see the *RapidResponse User Guide*.

Defining subscribers

Before users can publish data to subscribers, you must define the subscribers. For each subscriber, you must also identify the user who is responsible for publishing data to the subscriber. Only that user will be able to publish data to the subscriber.

▸To define a subscriber

1. In the **Administration** pane, under **System Settings**, click **Data Publishing Setup**.
2. Click **New Subscriber**.
3. In the **Subscriber** box, type the name of the subscriber. The name is typically provided to your company by Kinaxis.

▸To define a user for a subscriber

1. In the **Administration** pane, under **System Settings**, click **Data Publishing Setup**.
2. Select the subscriber for which you want to assign a user, and then click **Select Name**.
3. In the **Select Name** dialog box, select a name and then click **OK**.

Notes:

- If you delete a user account that is defined for a subscriber, the subscriber is also deleted. Prior to deleting a user that's defined for a subscriber, define a different user for the subscriber.
- If you assign a subscriber to a signed-in user, the subscriber is visible the next time that user signs in to RapidResponse.

▸To delete a subscriber

1. In the **Administration** pane, under **System Settings**, click **Data Publishing Setup**.
2. Select a subscriber.
3. Click **Delete**.

Note: After you delete a subscriber, any scheduled tasks for this subscriber do not run and must be deleted. For information about deleting scheduled tasks, see the *RapidResponse User Guide*.

Providing users with data publishing resources and permissions

Users who are expected to set up data extracts for subscribers have the following permissions:

- Scheduled task authoring
- Filter authoring
- Workbook authoring

Users also require access to the Data Publish workbook. After you've made any global customizations to the workbook, you can share it with users who are responsible for extracting the data for subscribers. Different users might be responsible for publishing data to different subscribers.

The Data Publish workbook uses the **yyyymmdd** date format. You should ensure this format is defined in RapidResponse. As well, the Data Publish workbook contains a worksheet based on the CPO_BaselinePlannedOrder table. This table can potentially contain a very large number of records. Therefore, to avoid problems during data publishing, you should either set the worksheet record limit to a high value or ensure that users who publish data also are granted permissions to override the worksheet record limit. For more information, see "Assigning and removing permissions" on page 517.

Users with scheduled task authoring permission can create data publishing scheduled tasks only if they have a subscriber assigned to them. For more information, see "Defining subscribers" on page 892.

Note: For more information about sharing workbooks, see the *RapidResponse Resource Authoring Guide*.

Part 9: Configuring RapidResponse subscribers (On-Premises only)

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

- "RapidResponse-to-RapidResponse connection" on page 897
- "Installing and configuring GlobalSCAPE software" on page 901
- "Installing and configuring Copy Command" on page 907
- "Adding publishers" on page 911

CHAPTER 57: RapidResponse-to-RapidResponse connection

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

The RapidResponse-to-RapidResponse connection 897
Steps in configuring the RapidResponse-to-RapidResponse connection 898

In a RapidResponse-to-RapidResponse connection, contract manufacturers (publishers) publish relevant data from RapidResponse and send it to brand owners (subscribers). Publishers can either have their own installed version of RapidResponse (On-Premises) or might be using a version of RapidResponse hosted at the RapidResponse Data Center (On-Demand).

This chapter describes the RapidResponse-to-RapidResponse connection, and outlines the steps your company should take to ensure reliable and secure connections with the FTP client used by publishers (the RapidResponse Data Transfer Client). This includes installing and configuring the GlobalSCAPE Enhanced File Transfer (EFT) Server and DMZ Gateway, enabling the transfer of received data extracts to the RapidResponse Extract folder for use in data updates and imports, and creating user accounts for each of your publishers on the EFT Server.

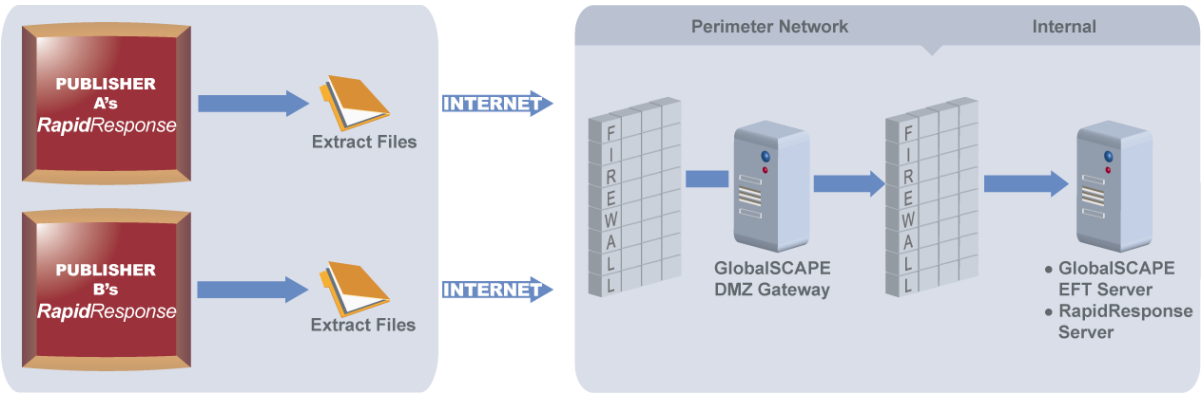
Note: While other FTP Servers might potentially be used, Kinaxis strongly recommends installation and use of the GlobalSCAPE EFT Server. This is the only FTP Server supported by Kinaxis for use in data transfers, and all documentation provided assumes use of this application.

The RapidResponse-to-RapidResponse connection

A RapidResponse-to-RapidResponse connection enables you to receive relevant data from multiple publishers (contract manufacturers), and view it in your installation of RapidResponse. This provides unique visibility into your contract manufacturer's supply chain data as it pertains to your company.

As shown in the following illustration, a secure RapidResponse-to-RapidResponse connection requires you to set up two separate servers. The first server should have the GlobalSCAPE DMZ Gateway installed. This server sits in your perimeter network and handles incoming data extracts from each publisher's RapidResponse Data Transfer Client. Data files are never stored on this server which then delegates all processing to the second server. The second server should have both the GlobalSCAPE Enhanced File

Transfer (EFT) Server and the RapidResponse Server installed, and should be located behind your company's inner firewall.



In order to protect and ensure the integrity of the data being sent to you, all connections made with publishers are done using a secure process. The publisher's Data Transfer Client uses the SSH File Transfer Protocol (SFTP) for transferring files. SFTP data transfers rely on a secure shell (SSH2) communication between the RapidResponse Data Transfer Client and your RapidResponse Server. Once a publisher's Data Transfer Client establishes a secure connection with your site, the publisher's user name and password is then validated. As well, after each extract file is transferred from a publisher, its integrity is validated on your server, and it is automatically retransmitted, if necessary.

Once data is received on the EFT Server, it needs to be moved to the RapidResponse Extract folder where it can be used in a data update or import. This is done using the Copy Command tool which is configured to monitor for new extracts received from publishers and then move them to the appropriate location.

Note: For more information about the data update and import process, see the *RapidResponse Data Integration Guide*

Steps in configuring the RapidResponse-to-RapidResponse connection

The following table outlines the steps, as fully described in other chapters in this section, required to set up your environment to receive data transfers from publishers.

Step	Description
Install the GlobalSCAPE software	Hosting a RapidResponse-to-RapidResponse connection requires installation of the GlobalSCAPE Enhanced File Transfer Server and DMZ Gateway. This step includes creating the FTP site to receive data transfers. For more information, see "Installing the GlobalSCAPE EFT & DMZ Gateway Servers" on page 901
Configure the GlobalSCAPE software	Once installed, the GlobalSCAPE software needs to be configured. This includes setting up your FTP Site to handle connections with the FTP Client used by data publishers, and enabling the connection between the Enhanced File Transfer Server and DMZ Gateway. For more information, see "Configuring the GlobalSCAPE EFT Server" on page 903.

Step	Description
Set up the Copy Command tool.	The Copy Command tool needs to be installed, and the EFT Server configured to run Copy Command each time it receives extract data from a data publisher. For more information, see "Installing and configuring Copy Command" on page 907.
Add publishers	Each publisher you want to receive data from requires a user account created on your FTP site, and the necessary connection information provided to them. The publisher must also be added as a data source in RapidResponse to support the receipt of data from the publisher. For more information, see "Adding publishers" on page 911.

CHAPTER 58: Installing and configuring GlobalSCAPE software

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Installing the GlobalSCAPE EFT & DMZ Gateway Servers 901
Configuring the GlobalSCAPE EFT Server 903

To receive data transfers from publishers, you need to successfully install and configure the GlobalSCAPE Enhanced File Transfer (EFT) Server and the DMZ Gateway. Most configuration is done using the EFT Administrator tool installed with the EFT Server.

Note: The GlobalSCAPE EFT Server is the only FTP Server supported by Kinaxis for use in data transfers. Kinaxis strongly recommends use of this application. If you choose to use another FTP Server, you should first review "Considerations in using other FTP Servers" on page 903.

Installing the GlobalSCAPE EFT & DMZ Gateway Servers

This section discusses installation of the GlobalSCAPE EFT Server and DMZ Gateway Server, as well as network and other considerations to keep in mind when installing these applications.

Network and security considerations

When installing the GlobalSCAPE EFT Server and DMZ Gateway Server, there are a number of network and security considerations to keep in mind as outlined in the following list:

- The DMZ Gateway Server should be installed in your perimeter network, and must have its own DNS name and IP address. This address is used in connections made by the RapidResponse Data Transfer Client used by data publishers.
- The DMZ Gateway Server should allow requests on Port 22.
- The TCP timeout settings for the relevant ports must be set appropriately. In particular, the command channel port (22) must have a timeout setting longer than the amount of time it is

expected any one file will take to transfer. The timeouts for the data port can be set to a very low value (for example, 5 seconds).

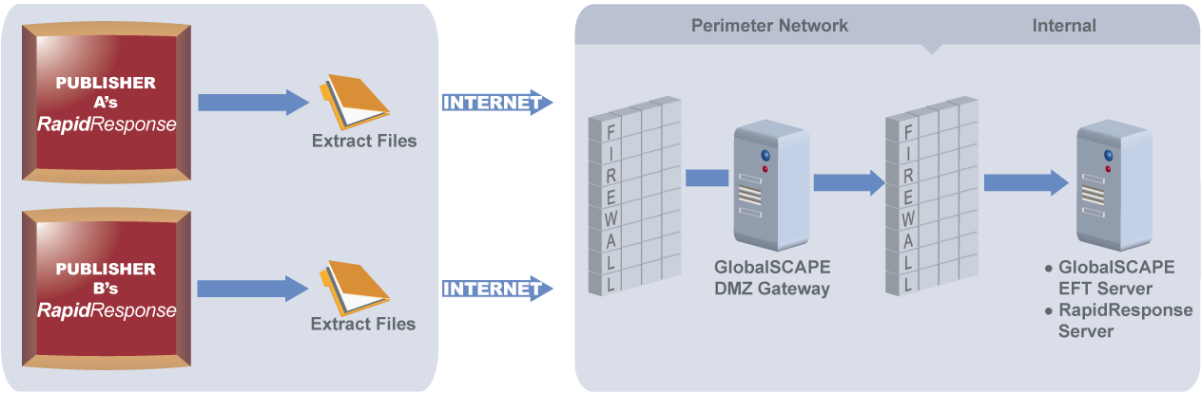
- The EFT Server must be installed behind your inner firewall, and on the same computer as RapidResponse Server.
- The EFT Server must be able to open a connection to the DMZ Gateway Server on port 44500. This port is configurable, but the firewall settings must match the settings in the DMZ Gateway configuration (as discussed in, link to "Gateway settings" on page 905).

Note: For more information on configuring your servers to meet the requirements outlined above, see "Configuring the GlobalSCAPE EFT Server" on page 903.

Installation

The GlobalSCAPE EFT Server must be installed on the same computer where RapidResponse Server is installed. This computer should be located behind your inner firewall as shown in the following illustration. For procedural information on installing and registering the EFT Server, see the *Enhanced File Transfer Server Help*. For information on configuring the EFT Server to support data transfers, see "Configuring the GlobalSCAPE EFT Server" on page 903.

The DMZ Gateway should be installed on a computer in your company's perimeter network as shown in the following illustration. For procedural information on installing and registering the DMZ Gateway Server, see the *DMZ Gateway Help*. For information on enabling a connection between the DMZ Gateway and EFT Server, see "Gateway settings" on page 905.



Creating an account to run the EFT Server

To run the Enhanced File Transfer Server securely as a service, you need to create a user account for it in Windows. The EFT Server should not be run under the local system account. For procedural information about creating a user account for the EFT Server, see the *Enhanced File Transfer Server Help*.

You should also ensure that the account created has full control of the **RapidResponse\Extract** folder.

Creating an FTP Site

After you have successfully installed the EFT Server, you can create an FTP Site. For procedural information about creating an FTP Site, see the *Enhanced File Transfer Server Help*. For information about configuring the FTP Site for data transfers, see "Site settings" on page 904.

Considerations in using other FTP Servers

Kinaxis strongly recommends using the GlobalSCAPE Enhanced File Transfer Server. This is the only FTP Server supported for use with the Data Transfer Client used by RapidResponse publishers to send data. All documentation provided by Kinaxis assumes use of this application.

If you elect to install and use another FTP Server, ensure that it supports the following features:

- Standard FTP commands as defined in RFC 959
- MODE Z
- XCRC
- Ability to restrict a user to their own home directory
- An event mechanism that allows a command to be invoked when a directory is renamed

Configuring the GlobalSCAPE EFT Server

After installation, the GlobalSCAPE EFT Server and DMZ Gateway Server must be properly configured to support the secure receipt of data transfers from your publishers. This section discusses configuring the following four groups of settings:

- **Server settings** (see "Server settings" on page 903).
- **Site settings** (see "Site settings" on page 904).
- **User default settings** (see "User default settings" on page 904).
- **Gateway settings** (see "Gateway settings" on page 905).

Note: For complete information about configuring GlobalSCAPE EFT Server settings, see the *Enhanced File Transfer Server Help*.

Server settings

Server settings include setting the default folder for Server log files, and ensuring that remote administration is disabled. The EFT Server is assumed to be administered locally.

▸To set Server options

1. Start EFT Administrator, and click the **Server** tab.
2. In the left-hand pane, select the local server.

3. On the **Server Options** tab, do the following:
   - In the **Folder to save log files** box, specify the location to save log files, or accept the default folder (**Program Files\GlobalSCAPE\EFT\Logs**).
   - In the **Log file format** list, click **Microsoft IIS Log File Format**.
   - In the **Log type** list, click **Verbose**.
   - In the **Rotate Log File** area, click **Daily**.
4. On the **Remote Administration** tab, do the following:
   - In the **Administrator home IP** list, click **127.0.0.1**
   - In the **Administrator port** box, type **1100**.
   - Ensure the **Allow remote administration** check box is not selected.

Site settings

Site settings let you specify security and account creation options for an FTP Site (the site must be created first as discussed in "Creating an FTP Site" on page 903). This includes specifying the protocols allowed by the site.

▸To set Site options

1. Start EFT Administrator, and select the **Server** tab.
2. In the left-hand pane, expand the Server, and select the FTP Site.
3. On the **Site Options** tab, do the following:
   - In the **Security** area, select the **Block anti-timeout schemes** and **Block site to site transfer** check boxes.
   - In the **Account Creation Options** area, select the **Automatically create home folder for newly added users** and **Grant FULL permissions to users in this folder** check boxes.
   - If you do not want to accept the default root folder for the FTP Site, specify a new one in the **Site root folder** box.
4. On the **Connection Options** tab, do the following:
   - Select the **Enable explicit SSL/TLS access (AUTH commands on default port)** check box.
   - In the **SSL Compatibility** area, click **TSL 1.0**.
   - In the **Certificate file path** box, specify the location of the **.CRT** file.
   - In the **Private key file path** box, specify the location of the **.KEY** file.
   - In the **Private key passphrase** box, type the private key password.

User default settings

The EFT Server includes one user settings level called Default Settings. This lets you to define certain user options once and have them applied to all subsequent users you create. These include options designed to ensure the security of each publisher's data, and options that enable the EFT Server to work correctly with the Data Transfer Client used by publishers.

▸To set User default settings

1. Start EFT Administrator, and select the **Server** tab.
2. In the left-hand pane, expand the Server, and then the FTP Site.
3. Click **User Setting Levels**, and then click **Default Settings**.
4. On the **Main** tab, do the following:
   - Select the **Enable this settings level** check box.
   - Select the **Treat home folder as the user's default root folder** check box. This prevents the possibility of one user seeing another's data.
5. On the **Security** tab, do the following:
   - Select the **Disable account after** check box, and then specify the number of incorrect logins allowed before a given user account is disabled.
   - Select the **XCRC command for data integrity validation** check box.
   - Select the **Allow MODE Z Compression** check box.
   - Select the **Allow access using SSL over FTP/HTTP protocols** check box.
6. On the **Quota** tab, do the following:
   - Select the **Enable time out (sec)** check box.
   - In the box provided, specify the timeout value. Because the EFT Server is an automated program, and never idles in a connected state, it should be set to a low value. For example, 30 seconds.

Note: If a user account is disabled because the number of incorrect logins allowed is exceeded, it can be subsequently be re-enabled on the **Main** tab for that user's account. For more information, see the *Enhanced File Transfer Server Help*.

Gateway settings

Gateway settings let you specify the address used by publishers to access the DMZ Gateway Server, as well as enabling the connection between the DMZ Gateway and EFT Server.

▸To set Gateway settings

1. Start EFT Administrator, and select the **Server** tab.
2. In the left-hand pane, expand the Server, and then click **Gateway**.
3. Click the **General** tab.
4. Select the **Enable gateway** check box.
5. In the **Address** and **Port** boxes, type the address and port the EFT Server uses to access the DMZ Gateway Server. These must match the Server IP and Port values specified for EFT connections when installing the DMZ Gateway Server.
6. In the **Passive (PASV) Mode Options** area, do the following:
   - Select the **Assign PASV mode IP address** check box.
   - In the **IP** box, type the address used by publishers to access the DMZ Gateway Server during a data transfer.

CHAPTER 59: Installing and configuring Copy Command

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Installing Copy Command 907
Configuring the GlobalSCAPE EFT Server to run Copy Command 908
Logging 909

The Copy Command tool is used to move data received from publishers from the folder where the GlobalSCAPE Enhanced File Transfer Server saves it and into the RapidResponse Extract folder where it can be used in a data import or update.

This chapter discusses installing Copy Command, and configuring the GlobalScape EFT Server to run Copy Command each time it receives a transfer of extract data.

Installing Copy Command

This section contains the system requirements for the computer on which Copy Command is being installed, as well as how to install it.

System Requirements

Ensure the following are installed on the computer where you are installing Copy Command:

- RapidResponse Server
- GlobalSCAPE Enhanced File Transfer Server 4.X
- Microsoft Visual C++ 2005 Redistributable Package (x86)

Note: The Microsoft Visual C++ 2005 Redistributable Package is available for download from the Microsoft Web site.

Installation

The Copy Command tool is distributed in the archive **CopyCommand.zip**. During installation of RapidResponse Server, this archive is copied into the **RapidResponse\Program** folder. It contains the following three files:

- **CopyCommand.exe**
- **log4cxx.dll**
- **log4.properties**

To install Copy Command, extract the three files listed above to a single folder. For example, you might extract all three files to a CopyCommand subfolder you created in the GlobalSCAPE EFT Server folder (that is, **Program Files\GlobalSCAPE\EFT\CopyCommand**).

Note: It does not matter which folder the files in **CopyCommand.zip** are extracted to, as long as they remain together.

Configuring the GlobalSCAPE EFT Server to run Copy Command

Once the Copy Command tool has been installed, EFT Administrator is used to configure the EFT Server to run Copy Command each time data is received from a publisher. This involves the following two steps:

- **Creating a custom command**—You first need to create a new custom command that runs the Copy Command executable file (**CopyCommand.exe**). When run, Copy Command moves the data from the folder where the GlobalSCAPE EFT Server saves it to the RapidResponse Extract folder.
- **Creating an event rule to trigger the new command**—Once the new command is created, you need to create an event rule that triggers the command to be run after the final step of the data transfer process completes. That is, it should run after the incoming data directory is renamed to **Received.*subscriber.timestamp*** (where *subscriber* is replaced by your company's Subscriber ID, and *timestamp* is in the form YYYYMMDD.HHMMSS).

▸To create the custom command

1. Start EFT Administrator, and select the **Server** tab.
2. In the left-hand navigation pane, do the following:
   - Expand the local server and log on to the server.
   - Expand the FTP Server.
   - Select the **Commands** icon, and then click **New**.
3. On the **Command** tab, do the following:
   - Select the **Enable this command** check box.
   - In the **Command Name** box, type a name for the new command.
   - In the **Description** box, type an (optional) description for the new command.
   - In the **Executable** box, type the full path to the location where **CopyCommand.exe** is installed.

- In the **Output** area, ensure the **Redirect output to client** and **Redirect output to system log** check boxes are not selected.

4. On the **Advanced** tab, do the following:
   - In the **Pass the following to the command** box, type **%1%**.
   - Select the **Require parameters** check box, and specify **1** in the parameters area.
   - Ensure the **Enable process timeout** check box is not selected.
5. On the **Permissions** tab, ensure that no users are granted permission to execute the command.
6. Click **Apply**.

   The new command is saved.

> **Note:** During initial configuration, it might be useful to select **Redirect output to system log** in order to diagnose configuration problems. The log file created is named **cmdout.log**.

▸To create an event rule to trigger the custom command

1. Right-click the **Event Rules** icon, and then click **New Event Rule**.
2. In the **Create New Rule** dialog box, do the following:
   - Under **File System Events**, click **File Rename**.
   - Click **OK** to create the new event rule (named **On File Rename Rule**).
3. Select the newly created rule, and then do the following in the right-hand pane:
   - Select **Enable this rule**.
   - Under **Specify zero or more conditions**, select the **If Virtual Destination Path does match**.
   - Under **Specify condition parameters**, click the last parameter and then change it to **/Usr/*/Received.*.*.***
   - Under **Specify at least one action**, select **Execute command in folder**.
   - Under **Specify action parameters**, click either of the parameters (this launches the dialog box for specifying command parameters).
4. In the **Custom Command** dialog box, do the following:
   - In the **Select command** list, select the command you created earlier (as discussed in "To create the custom command" on page 908).
   - In the **Specify command parameters** box, type **%FS.DST_PATH%**.
   - In the **Specify command working folder** box, specify the folder where you want Copy Command log files stored (typically, you might want this to be the same folder where it is installed).
   - Click **OK**.
5. Click **Apply**.

   The new event rule is saved.

Logging

When the Copy Command tool moves data, it generates log event messages to track the processing of the copy operation. By default, these events are generated in the **Copy.log** file which is stored in the folder where Copy Command is installed.

These log events are useful after installation to ensure that Copy Command is working correctly, as well as to diagnose problems that might occur. The log events can also be used on an ongoing basis to monitor operations.

If you require some alternative format or destination for the log events, you can edit the **log4.properties** file. For more information on this file, see the Apache log4cxx documentation at http://logging.apache.org/log4cxx.

CHAPTER 60: Adding publishers

This section applies to On-Premises only. If you are using the RapidResponse On-Demand service, ignore this section.

Creating a new user account 911
Adding a publisher as a data source 912

Each new publisher you add requires a user account created on your FTP Site, and you must also provide them the information required to access your site. You should also add the publisher as a data source to ensure the data is imported. Also, if a publisher is upgrading to a later version of RapidResponse, you must update the publisher's configuration details.

Creating a new user account

In order to transfer data to your site, each publisher requires a user account on your FTP Site. Publishers should also be provided with a password to access the site. The following outlines the steps that should be taken to enable a new user account on your FTP site.

▸To add a new user account to your FTP site

1. Using the GlobalSCAPE Administration interface, create a user account and password for the publisher. For complete procedural information about adding a new user to an FTP site, see the *Enhanced File Transfer Server Help*.
2. Using a secure means, provide the following to the publisher:
   - The password associated with their user account.
   - The remote host address (that is, the DNS name or IP address used to access your DMZ Gateway server).
   - Your Subscriber ID. To ensure a unique ID across all RapidResponse installations, it is recommend that you ask Kinaxis to provide you with your Subscriber ID.
3. If necessary, adjust your firewall or DMZ Gateway settings to allow incoming connections from the publisher. For more information, see "Network and security considerations" on page 901, and "Gateway settings" on page 905.

Note: When adding a user account for an On-Demand publisher (that is, a publisher using a RapidResponse hosted at the RapidResponse Data Center), you will co-ordinate the above activities with Kinaxis instead of the publisher themselves.

Adding a publisher as a data source

If your company is importing data into RapidResponse from a new publisher, you must add that publisher as a data source to ensure the data is imported. Data sources are defined in the Data Sources and Mapping window within RapidResponse. When adding a data publisher as a data source, you must create that data source using one of the pre-defined data source templates available from Kinaxis. The template you should use depends on the version of RapidResponse used by the data publisher you are configuring. You can then modify the template as necessary to reflect the data you will be receiving from this publisher.

▸To import a data source template

1. From the **Data** menu, point to **Import Data To**, and then click **Scenario**.
2. In the **Import Data to Scenario** dialog box, do the following:
   - Click the **Browse** button, and navigate to the location where you have saved the data source template corresponding to the version of RapidResponse used by this publisher.
   - Select the required data source template, and then click **Open**.
   - From the **Scenario** list, select the scenario you are importing the data source template into. This should be the scenario you created to make integration changes in as discussed in the *RapidResponse Data Integration Guide*
   - Click **Import**.
3. In the **Administration** pane, under **Data**, click **Data Sources and Mapping**.

   The Data Sources and Mapping window opens.
4. From the **Scenario** list, select the scenario you imported the data source template into.
5. In the **Data Source** area, right-click the template and then click **Duplicate**.
6. In the **Duplicate Data Source** area, type a name for this data source (for example, you can name it after the data publisher).
7. Click **Ok**.
8. In the **Data Source** area, right-click the template and then click **Properties.**
9. In the **Key field prefix** area, type a prefix that can be added to key field values in the publisher's data. This protects against data collisions when the publisher's data is merged with your data in RapidResponse (that is, if the same key value exists in each data set).
10. Click **Ok**.
11. Configure the new data source as appropriate to reflect and map the data you expect to receive from this publisher. For more information on configuring data sources, see the *RapidResponse Data Integration Guide*

Index

$

$Scenario# variable 170
$ScenarioX 171
$SelectedHierarchyTreePath
  modifying delimiter 661

.

.PFX files 858
.pkg files (packages) 251

2

25, port for email 276

4

443 port 126

8

80 port 126

A

about
  Admin user account 34
  Approved Actions scenario 703
  Copy Command 907
  data publishing 872
  data transfers 875
  Enterprise Data scenario 703
  groups 493
  Master Administrator account 34
  On-Demand RapidResponse service 16
  permissions 513
  persisting data 329
  RapidResponse-to-RapidResponse connection 871, 897
  RapidResponse Data Transfer Client 875
  security 45
  ServerCommand 339
  single sign-in 835, 863
  webpInSC 335
accepted URLs 744
access
  controlling 627
access permissions, granting to groups 513
accessing
  help and documentation 21
active server 301
activities
  setting finish date reporting 634
add-in applications
  properties 639
  providing to users 640
  specifying network locations 639
add-ins
  assigning to groups 529
Add-Ins worksheet 639
AddIn command argument 408
adding
  groups 513
  links to Extensions pane 624
  to a single sign-in environment 847
  users 549
  users to groups 566
Admin user account
  about 34
  allowing to bypass single sign-in 860
  email address 34, 421
AdminEMail registry value 352
administration
  remote 59
Administration log records
  system records 278
Administration Log system workbook 418, 482
administration logs 423
administration permissions 41
administration role
  about 33
administration workbooks 481
administrator
  changing password 34
  data 36
  Master Administrator 34
  system 34
  user 35
administrator permissions, assigning 41
administrator roles
  about 33
administrators
  about 33
  On-Demand 58
Adobe Flash Player 543
Adobe Reader 22
age deletion threshold 277
Alert and scheduled task log records
  system records 278
alert user license 539
alerts
  development environment 675
  down time interval 674
  failed 461
  initial setup 671
  settings 675
  Supplier Collaboration 824
  troubleshooting 234
  turn on and off 748

unlocking 769
AlgorithmCacheMemoryLimitMB 267
Allotment Overrides workbook 786
AllowDeletes command argument 396
allowing web service calls 744
AllowModifications command argument 396
AnalyticMemoryLimitMB 267
analytics
memory settings 266
AND operator
in feature lists 632
announcements 441
annual plan target scenario 636
antivirus 56
Apple Safari 4 543
application components 99
Application Server
backing up 314
configuration 162
Application Settings system workbook 482
Application Settings workbook 783
applications
enabling 124, 273
upgrading 184
ApplyEnvSuffixToEmailSubject registry value 365
Approved Actions scenario
about 703
giving access to 533
updating 533
archive file
diagnostics 245
archives
decompressing 251
log files 241
overview 251
archiving
database files 324
arguments
commands 384
scheduled system tasks 414
Arial Unicode MS font 644
ASA file 245
AsaOnlyOnFirstChance registry value 362
Asian characters 644
assigning administrator permissions 41
Attribute Rules workbook 807
authentication 59
authors 504
Auto-delete scheduled task 382
Auto-Publish Running Plan group 495
automated data flows 817
Automated Server-incident Analysis file 245
automatic scenario updates 716
automatic server operations
error messages 338
automatically restarting RapidResponse 233
automating RapidResponse Server operations 335
automation chains
unlocking 769
Automation Details and Log system workbook 482
Automation Log system workbook 482
Automation Log workbook 623, 750
automation resources
locked 769
automation tasks
running 767
Automation Tasks 459
AutoText
date format 647
using in headers and footers 646

B

backing up
database 315
program files 314
RapidResponse Application Server 314
RapidResponse database 315
RapidResponse Server 314
Backup
limit 680
backup files
managing 316
Backup registry value 357
Backup_servername_timestamp.pkg 316
BackUpPackages registry value 352
BackUpRoot registry value 357
backups 56
bandwidth considerations 53
base currency 687
BaselineScenario command argument 405
batch files 335
bold column headers 631
broadcast messages
sending to users 593
buckets
for Inventory Analysis 792
bulk user provisioning 549
Bulletin Board announcements 441
Business Analysts group 495
business domains 819
Business Message Definition system workbook 482
business message definitions 819
Business Message Log system workbook 482
Buyer Commit to ERP workbook 824
Buyers group 500
bypassing single sign-in 860

C

caching
dashboard results 764
worksheet results 763
Calculated Data Model poster 23
calculations
differences after upgrading 142
invalidating 270
modifying 725
MRPDate 286
calendar, Everyday 671
calendars
adding dates 630
display names 629
cancel queries
threshold 606
users 606
canceling
queries 605
canceling queries 269

Capacity Manager
optional module 133
uninstalling 132
Capacity Manager group 495
Capacity Planning (CRP)
installing 131
Capture command 385
Capture scheduled task 382
Central Log Collector 479
certificates
.PFX files 858
customizing 858
generating 126
X.509 858
change management 61
Changes to Root Scenario worksheet 425
changing passwords
Admin 34
character sets, international 65
characters
invalid group names 514
invalid user IDs 549
Checkpoint and Version Reclaim scheduled task 382
Checkpoint command 386
checkpointing
disk space warnings 314
CLC 479
Clear to Build workbook 786
client connections to RapidResponse 123
Client_MaximumPDFPageCount configuration
record 644
closing the loop 829
clustering
failover 289
collaboration
specifying scenario for calculations 635
collaborations
deleting 776
managing 775
Collaborations workbook 775
CollectArchives.exe
command line 243
column headers, bold 631
Command Messages worksheet 424
commands
arguments 384
Capture 385
Checkpoint 386
Condense 387
CreateDataPackage 388
DataExpiry 277, 389
DataImport 390
DataIntegrityCheck 160, 391
DataSynchronize 393
DataUpdate 395
DeleteData 402
DeleteEnterpriseData 403
DeleteFiles 403
FilterTT 406
GenerateExtract 403
GenerateNetChangeExtract 404
in RapidResponse Server[commands
RapidResponse] 384
logs 423
PruneFiles 406
Restart 407
RunAddin 407
ScenarioCommit 408
ScenarioReset 408
ScenarioUpdate 409
scheduling as tasks 384
Snapshot 409
structure for webplnSC 337
VersionReclaim 411
VersionReclaimSweep 411
committing scenarios 408
to root scenario 717
communicating
with RapidResponse users 593
communication protocols 57
comparing
resources 761
Comparing 681
compatibility levels 156
Complete Diagnostics Archive
manually generating 248
complete diagnostics archive file
troubleshooting 245
complete installation 102
compliance (compatibility) levels 156
compressed archives
decompressing 251
overview 251
computer server ID
generate 124, 274
Condense command 387
Condense scheduled task 382
confidentiality
data 59
configuration
bold column headers 631
data publishing 873
RapidResponse-to-RapidResponse connection 873
ResponsibilityPlan 635
ServiceHost_ThreadCount 235
setting locale 282
specifying split order separator 631
subscribers 898
configuration files
deleting users 573
connection to enterprise system 703
connections
troubleshooting 123
Console; HTTPS 237
Constraint Manager group 495
Contents tab 24
Control Sets system workbook 483
control table settings, changing 725
controlling access to custom links 627
conversion rates 689
converting
currencies 687
CONVERTONDATE 688
cookies 50
Copy Command
about 907
GlobalSCAPE EFT Server 908
installing 907

logging 909
CPU usage
monitoring 271
crash
failover 289
crashes
resolving 241
Create Backup scheduled task 382
CreateDataPackage command 388
CreatePreviousDataUpdate command argument 397
creating
alert users 551
data formats 665
global tags 772
groups 513
publisher ID records 873
single sign-in environment 843, 865
trusted assembly for single sign-in 849
users 549
currencies 683
adding 684
converting 687, 689
creating 686
deleting 687
modifying 687
vector data 210
currency
codes 685
creating format 665
Currency Conversion Rates workbook 689
custom applications
specifying network locations 639
custom data mode
restoring 407
custom help, adding to RapidResponse 613
custom links
adding to Extensions pane 624
controlling access to 627
custom XML 744
Customer Order Managers group 495
Customers group 496
customizing
link menu 618
customizing certificates for SSI 858

D

dashboards 161
caching results 764
help 28
Supplier Collaboration 822
data
canceling queries 605
change tracking 829
confidentiality 59
deleting historical 402-403
flow 703
hiding 892
moving to RapidResponse Data Transfer Client 881
persisting during import 329
publishing 893
reference parts 874
required for publishing 874, 891
restoring 315
security 45
viewing with perspectives 725
data administrator
about 36
Data Center subscribers, global settings 881
Data change records
system records 278-279
data change records, deleting 833
data change tracking 51
data configuration 100
Data Extract Log system workbook 483
data feeds 882
data files
recovering in case of upgrade failure 183
data formats
creating 665
default 667
editing 665
making available 663
making unavailable 664
Data import and update log records
system records 280
Data Import and Update Log system workbook 483
data import process
setting the file size limit 653
Data Import scheduled task 383
data imports
after initial import 704
impact on scenarios 703
Data Integrity - Material workbook 785
Data metric log records
system records 280
data model 156
calculation differences after upgrading 142
Data Model for Import poster 23
Data Model Overview 483
data model posters 22
Data Origin workbook 483
data package
database backup 382
decompress 318
managing backup files 316
data persistence 330
rules 330
Data Persistence Rules workbook 330, 483
Data Publish workbook
hiding data in 875
reference parts 874
setting up 874
sharing 887
data publishing
about 872
publisher ID 873
required data 874
steps to configure 873
Data registry value 358
data security 54
data sources
adding publishers 912
Data Tolerance and Error Settings workbook 483
Data Transfer Client 55, 875, 882
data transfers
about 875
subscribers 886

Data update
failure message notifications 421
Data Update Log
file 442
Data Update scheduled task 383
data updates 213
error codes 400
log files 442
MRPDate 286
DATA_UPDATE_KEY (environment variable) 345
DataBackUpWindowMinutes registry value 352
database
backing up 315
create backup package 382
file location 310
integrity 327
restoring back up 317, 319
versioned 270, 704
Database Integrity Check scheduled task 383
Database registry key 356
DataExpiry command 277, 389
DataImport command 390
DataIntegrityCheck command 160, 391
DataLoad registry key 356
DataSource registry value 356
DataSynchronize command 393
DataUpdate command 395
date
codes 666
creating formats 666
formats with AutoText 647
dates
buckets for Inventory Analysis 792
display names 629
daylight savings time changes 670
decompress
data package 318
decompressing
archives 251
default
data formats 667
default email address 656
defining
subscribers 892
defining perspectives 725
delete
process instances 750
DeleteData command 402
DeleteEnterpriseData command 403
DeleteFiles command 403
deleting
collaborations 776
currencies 687
data change records 833
filters 748
global tags 772
groups 569
hierarchies 748
historical data 402-403
private resources 740
public resources 740
scenarios 711
scorecards 748
subscribers 892
system records automatically 277
task flows 748
unused scenarios 712
users 573
workbooks 748
Demand Manager group 496
Demand Planners group 498
denying permissions
for users 554
DetailTransactionLog command argument 394, 397
development environment for alerts 675
diagnostics_servername_timestamp.pkg file 245
DIC_servername_timestamp.pkg 328
Directories registry key 357
disaster recovery
failover clustering 289
Discard All Changes (ScenarioReset) 408
disconnecting users from RapidResponse 601
disk space warnings 314
display names for calendars 629
DMZ
installing Application Server 126
DMZ Gateway 901
DNS 55
documentation
customizing location 613
feedback 25
Internet-based 613
documentation conventions 24
documentation, accessing 21-22, 24
down time interval
alerts 674
drill-through 618
drop down (link menu) 618
dump file
troubleshooting 245
Dump File
manually generating 248
DumpDirectory registry value 363
Duplicate Actual Conversion Rates system workbook 484
duplicating
groups 515
users 553

E

Eastern European characters 644
editing
data formats 665
groups 566
EFT Server (GlobalSCAPE) 901
EM64T (Intel Extended Memory 64) 105
email
administrator 34
default address 656
defining servers 276
notices for administrator 34
notifications 421
notifications and sharing scenarios 276
port 25 276
using Sender Policy Framework 96
EmailAttachment registry value 356
EmailOverride registry value 362
EmailWho registry value 357
embedded interface for single sign-in 839

EnableLastKnownGoodPackage command argument 390, 397
EnableQualityCheck command argument 390, 397
EnableSaveHistory command argument 391, 398
enabling
email functionality 276
RapidResponse modules 124, 273
reference part toggle button 628
encryption
passwords 48
Engineering Change Manager
components 135
installing 133
uninstalling 134
Engineering Change Manager group 496
Engineering group 498
Enterprise Data scenario 533, 703
renaming 719
enterprise system, connecting to 703
Env command argument 408
environment variables 344
DATA_UPDATE_KEY 345
EXIT_NAME 345
RAPIDRESPONSE_ROOT 345
SERVER_ID 345
SESSION_ID 345
SESSION_PASSWORD 345
USER_ID 345
ERP (enterprise systems) 703
error codes
data updates 400
restoration 470
Error codes for plan operations 347
error messages
automatic server operations 338
restoration 470
webpInSC 338
ErrorLimit registry value 357
errors
Event log 606
opening workbooks 602
restoration 470
signing in 602
Event log, RapidResponse Application Server 606
Everyday calendar, overriding name 671
example
customizing the Extensions pane 626
Excel import configuration records
system records 280
Excessive Query Memory
error message 269
Executives group 498
EXIT_NAME (environment variable) 345
ExpectedDataSources command argument 398
ExpectedRegions command argument 398
expiry of sessions 611
expiry, license keys 273
exported reports
file locations 672
exporting
resource package 752
Exporting
User groups 678
EXS Server
virtualization 106
Extended Memory 64 Technology. See Intel Extended Memory 64 Technology[Extended Memory 64 Technology] 105
extensions
assigning to groups 529
Extensions pane
adding links to 624
example of customizing 626
external access to RapidResponse 126
extract.done 881
ExtractDefinition command argument 404-405

F

failover
clustering 289
log files 304
restarting 293
service updates 305
setup 290
system requirements 293
upgrading 305
Failover Configuration program 294
failure recovery 183
failures signing in 595
feature lists
AND operator 632
feedback
email 421
feedback, providing 25
file attachement limit 651
file locations 676, 882
specifying 672
file size limit, setting 653
filename command argument 389
files
.PFX 858
.pkg
pkg] 251
batch 335
DIC_servername_timestamp.pkg 328
extract.done 881
locations for exported reports 672
Logs_servername_timestamp.pkg 242
manifest 388
Web.config 841
filter command argument 402-403
filters
assigning to groups 529
deleting 748
exceeding worksheet record limit 529
providing access 529
tables 529
FilterTT command 406
Finance group 498
Firefox 3.5 543
firewall 126
firewalls 57
Folder command argument 404-405
folder structure
RapidResponse Application Server 124
RapidResponse Data Transfer Client 879
RapidResponse server 249

folders
RapidResponse Data Transfer Client 879
fonts
used in PDF files 644
used in printed reports 644
fonts in headers and footers 647
footers
editing font 647
inserting AutoText 646
inserting fixed text 647
setting standard 645
ForceHistory command argument 398
ForceUpdate command argument 408
forceVersionReclaim command argument 387
Forecast Response workbook 823
formats
currency 665
date 666
editing 665
number 665
time 666
time and date 666
forms
help 29
Forms 765
fraud protection 57
FTP
adding accounts for publishers 911
Gateway and Server 875
Full Data Import scheduled task 383
full user license 539
FullDumpOnFirstChance registry value 363
FullDumpOnSecondChance registry value 363

G

general user type 541
GenerateExtract command 403
GenerateNetChangeExtract command 404
generating certificates 126
generating system information
troubleshooting 244
geocode data 813
getserverid.exe 124, 274
GetSession15 298
Global Settings 659
annual plan target scenario 636
Backups 680
Global Supply Planners group 496
global tags 772
global tools (international characters) 65
GlobalSCAPE DMZ Gateway, installing 902
GlobalSCAPE EFT Server
Copy Command 907
installing 902
network considerations 901
ports 901
running Copy Command 908
server settings 903
site settings 904
user default settings 904
golden workbooks (predefined) 751
granting permissions
to users 554
group names
Auto-Publish Running Plan 495
Business Analysts 495
Buyers 500
Capacity Manager 495
Constraint Manager 495
Customer Order Managers 495
Customers 496
Demand Manager 496
Demand Planners 498
Engineering 498
Engineering Change Manager 496
Executives 498
Finance 498
Global Supply Planners 496
Inventory Managers 496
Kanban Manager Viewers 496-497
Manufacturing Engineers 497
Marketing 498
Master Schedulers 497
Material Planners 497
Operations 498
Operations Managers 497
Order Fulfillment 497
Production Planners 497
Risk/Opportunity Analysts 498
S&OP Process Owners 499
Sales 499
Suppliers 500
Suppliers [Template] 500
groups
about 493
about system groups 537
adding users 554
adding users to 566
assigning resources 529
creating 513
deleting 569
duplicating 515
editing 566
granting permissions 513
guidelines for creating 503
included with RapidResponse 494
invalid characters 514
members 584
naming 514
removing users from 566
resource assignments 582
system 537, 540
guidelines, creating groups and users 503

H

hard disks
effect on performance 310
hardware requirements 104
header records 213
headers
editing font 647
inserting AutoText 646
inserting fixed text 647
setting standard 645
health check reports 62
Heartbeat.log 470

help
accessing 21
custom 613
setting location to use 613
hierarchies
assigning to groups 529
deleting 748
hierarchy limits, setting 660
historical data
deleting 402-403
Historical Demand poster 24
Historical Supply poster 24
HistoricalPartKPI 792
HKEY_LOCAL_MACHINE registry settings 351
hosting 58, 60
HTTPS protocol 46
secure communications 126
security 104
HTTPS; Console 237
HttpsRapidResponseConsole registry value 353
hyperlink menu (link menu) 618

I

ID
generate computer ID 124, 274
IFS files
database files 311
IIS (Microsoft Internet Information Services) 105
IIS Session State Mode 120
Import registry value 361
importing
persisting data during 329
resource packages 757
software license keys 124, 273
Importing
User groups 679
importing data
options for importing to scenario 662
setting the file size limit 653
Index tab 24
initial
data formatting 667
setup for alerts 671
initial RapidResponse sign-in 122
InsertDefInstaller.log 193
installation
starting RapidResponse 122
testing 122
installing
Capacity Planning (CRP) 131
Copy Command 907
Engineering Change Manager 133
GlobalSCAPE DMZ Gateway 902
GlobalSCAPE EFT Server 902
preparing 114, 189
prerequisites 130
RapidResponse 101
RapidResponse Application Server 118, 130
RapidResponse Data Transfer Client (Unix) 878
RapidResponse Data Transfer Client (Windows) 876
RapidResponse Server 111
single sign-in SDK 848
integrated interface for single sign-in 839
integrated project management 633
Integrated Project Management poster 24
integration settings
modifying 36
integration, data 703
IntegrationScenario command argument 398
integrity, database 327
IntegrityCheckMaxPlans registry value 327, 392
IntegrityCheckMaxProblemPlans registry value 327, 353, 392
Intel Extended Memory 64 Technology 105
international character sets 65
international data, setting locale 281
Internet-based help 613
Internet Explorer (Microsoft) 543
Internet Information Services (IIS) 106
intrusion prevention 56
invalid user IDs
invalid characters 549
sign-in attempts 595
InvalidateAll registry value 353
invalidating results 270
invalidation of results
queries 270
Inventory Analysis workbook
setting up 792
Inventory Managers group 496
Inventory Planning and Optimization poster 24
inventory sites 274
ISP 52

J

Java
memory settings 544
Java Runtime Environment 542
Java Web Start application 541
JRE 542
memory settings 544
JRE memory setting
override 547

K

Kanban Manager
setting up 786
Kanban Manager Viewers group 496-497
KeepExtract command argument 398
key fields, replacing 174
key management 58
key reference fields 175
key uniqueness 205
Kinaxis
about 19
contacting 19
providing feedback to 25
Kinaxis Customer Support 19
Kinaxis data center 58
Kinaxis Knowledge Network 20

L

LAN connection 102-103
language settings 65
Last Known Good archive 390, 397
last sign in 573

LastUsed registry value 361
LCID numbers 281
license key expiry 273
licenses
    user types 539
    users 541
licensing
    importing keys 124, 273
    sites 274
light user license 539
limitations of single sign-in 843, 864
LimitedDumpOnFirstChance registry value 363
LimitedDumpOnFirstChanceAnalytics registry value 363
LimitedDumpOnSecondChance registry value 363
limiting
    pages in printed reports 644
    records in worksheets 657
Line of Balance workbooks
    configuring 786
link menu
    customizing 618
Links in messages
    system records 280
links, adding to Extensions pane 624
List Reference Parts button 628
locale
    LCID numbers 281
    setting in RapidResponse Server 281
    setting in the configuration table 282
locked automation resources 769
locked user accounts 599
log file archives
    generating 241
log files 156
    alerts 461
    archiving 367
    error limit 623
    failover 304
    for Copy Command[log files
        Copy Command] 909
    for date updates[log files
        data updates] 442
    Heartbeat.log 470
    OpenAPI applications 223
    Performance.log 473
    Query.log 463
    QueryHistory.log 474
    RapidResponse 462
    RRMonitor.log 246
    scheduled system tasks 418
    SecurityAudit.log 477
    server.log 464
    ServerAudit.log 463
    ServiceHost.log 463
    upgrade 185, 193
    UtilityServer.log 463
Log Service
    architecture 368
    installing 372
LogFlags registry key 361
logging command execution 423
logical sites 274
Logs_servername_timestamp.pkg 242
LogUsesOfUnscopedPrivatePlans processing rule 170

M

Mac OS 24
macros
    importing 168
Macros and Profile Variables workbook 484
mail server, defining 276
MailServer registry value 353
malicious actions 657
malware 56
managing
    process instances 750
managing RapidResponse Server memory 260
manifest file 388
Manufacturing Engineers group 497
maps
    geocode data 813
    set up 812
Marketing group 498
Master Administrator account
    about 34
master administrator user 422
Master Schedulers group 497
Material Planners group 497
MaxBackupFiles registry value 358
Maximum Retries 396
    scheduled task 414
MaxPlanDepth command argument 391
MaxPlans command argument 391
MaxRecord command argument 399
McAfee Virus Scan 256
memory
    limit settings 260
    overriding MemoryLimit 260
    usage alerts 268
memory consumption
    scenario 270, 704
Memory limit
    in server.log 262
memory limit settings 544
memory settings
    system settings 260
MemoryLimit registry value 260, 354
MemoryModel registry value 354
message center
    attachment size limit 652
    deletion threshold 651
    file attachment limit 651
    setting message limits 650
Message command argument 409
messages
    scheduled tasks 413
    sending to users 593
Messages
    system records 280
MessageSubject command argument 409
Microsoft Internet Explorer
    system requirements 543
Microsoft Internet Information Services
    certificates for 126
    enabling single sign-in 852
    security 115
    system requirements 106
Microsoft Registry Editor 351

minimumMemory
override JRE memory setting 547
modifiable reference keys 175
modifying
data formats 665
groups 566
public resources 740
resource and tool settings 807
users 570
ModifyKeyReferences processing rule 175
modules, enabling 124, 273
monitoring
CPU usage 271
sign-in 49
monitoring services 57
monitoring sign-in activities 595
Mozilla Firefox 3.5 543
MRPDate calculation
setting 286

N

NamedExtractSet command argument 394, 399
naming 731
Network registry key 361
non-unique scenario names 170
notifications by email 421
NoTraversal registry value 364
number formats, creating 665
NumberToRetain command argument 406

O

On-Demand RapidResponse service 15
administrators 58-59
antivirus 56
authentication 59
backups 56, 61
change management 61
communication protocols 57
confidentiality 59
data security 54
database server service 53
DNS services 55
escalation 61
firewalls 57
fraud protection 57
health check reports 62
hosting 60
infrastructure 51
intrusion prevention 56
ISP 52
key management 58
monitoring 57
operating system 56
outages 61
patches 62
physical security 58
remote data replication 63
system redundancies 56
On-Premises RapidResponse 15
OpenAPI 219
OpenAPILogging registry value 354
Operations group 498
Operations Managers group 497
optional keys 174
options for importing to scenario 662
Oracle
Java Runtime Environment 542
orange background 657
Order Fulfillment group 497
override JRE memory setting 547
overrides
alerts 675
Everyday calendar name 671
memory limit 260
Overrides registry key 362

P

PackageBackUpWindowMinutes registry value 355
Packages folder 251, 315
Packages registry value 359
page breaks, setting 648
page limit 644
Part menu link 618
part toggle button (reference parts) 629
pass-through authentication 843, 865
password policies 48
passwords 48
changing for users 570
encryption 48
PASV mode 905
path command argument 403
Pattern command argument 406
PDF (Adobe Reader) 22
PDF reports 644
PDF viewer application 543
Pending Period
scheduled task 414
Pending Period setting 395
performance 659
monitoring 479
Performance Monitor Service 368
architecture 368
installing 375
plug-ins 370
viewing data 479
Performance.log 473
permanent scenarios
creating 714
creating hierarchies 719
permissions 21, 504, 539, 825, 828
about 513
administrator 41
assigning to groups 513
denying for users 554
filters 529
for custom links 627
granting to users 554
Modify data integration 36
scenarios 533
Persistence-HistoricalTables folder 334
Persistence-RuleBased folder 334
Persistence-SystemOfRecord folder 334
persisting data
about 329
perspectives 169, 731
defining for scenarios 725
Perspectives workbook 484

phishing 50
phishing attacks 657
physical memory (system memory) 259
physical security 58
physical sites 274
PkgDirectory registry value 364
PkgIncludeDataDirectory registry value 364
PkgIncludeFullDump registry value 364
Plan Operations
    PlanCommit 349
    PlanDelete 349
    PlanGive 349
    PlanPublish 349
    PlanUpdate 349
PlanCommit 349
PlanDelete 349
PlanGive 349
PlanPublish 349
Plans command argument 392
PlanUpdate 349
port 25 276
port 443 126
Port registry value 355
ports
    firewall 126
    for GlobalSCAPE EFT Server[ports
        GlobalSCAPE EFT Server] 901
    TCP/IP 283
predefined resources
    workbooks 751
preparing for upgrade 109
PreTransform_ServerName-DateTimeStamp.pkg 407
PreUpgradeAnalyzer utility 207
preventing spam 96
PreviousDataUpdate scenario 397
printed reports
    setting font options 644
    setting page limit 644
printed reports, settings 648
printing
    help 21, 27
private resources 589
    deleting 740
problematic queries 422
process instances
    managing 750
Process Instances system workbook 484
process orchestration
    activity finish dates 634
processes
    upgrading 143
Processes on enable (McAfee) 256
processing rule
    LogUsesOfUnscopedPrivatePlans 170
    ScenarioNameUnique 170
processing rules
    ModifyKeyReferences 175
Production Planners group 497
profile pictures
    displaying 617
    setting 560
profile variables
    Sales and Operations Planning 777
Program registry value 360
programs
    webplnSC 335
project management baseline scenario 633
project management finish dates 633
properties of add-in applications 639
Protocol registry value 361
Prune Backup Packages scheduled task 383
PruneFiles command 406
publishers
    adding as a data source 912
    creating an FTP account for 911
    creating ID records for 873
publishing data 889, 893
Purchase Order Response workbook 823

Q

QE3 477
QE3Status 477
queries
    canceling 269
    high memory usage alerts 268
    invalidation of results 270
    logging 474
    memory settings 267
    problematic 422
    slow running 603
    viewing and canceling 605
Query cancel dialog delay 606
query history 603
Query Manager workbook 484
Query registry value 361
Query.log 463
QueryHistory.log 474
QueryMemoryAlertThreshold registry value 268, 355
QueryMemoryLimit 269

R

RAM (system memory) 259
RapidResponse
    about On-Demand 16
    adding custom help 613
    administration role 33
    automatically restarting 233
    commands 384
    enabling modules 124, 273
    external access 126
    groups 494
    log files 462
    On-Demand 15
    On-Premises 15
    resource and tool settings 777, 807
    scheduled tasks 384
    security 45
    sign-in URL 122, 553
    system requirements 104
    testing installation 122
    upgrading 141
    Windows Services 227
RapidResponse-to-RapidResponse connection 889
    about 871, 897
    benefits 872
    publisher configuration 873
    subscriber configuration 898

RapidResponse Administration workbook 484
RapidResponse Application Server 105
backing up 314
certificates 126
connection problems 123
Event Log 606
folder structure 124
installing 118, 130
preparing to install 114, 189
system requirements 105
testing upgrade 194
uninstalling 127
upgrade log files 193
upgrading 190
RapidResponse Calculated Data Model poster 23
RapidResponse Console
sign in 230
RapidResponse Console; HTTPS 237
RapidResponse Data Center 875
RapidResponse Data Model for Import poster 23
RapidResponse Data Transfer Client
about 875
folder structure 879
moving data to 881
service 228
system requirements 877
uninstalling (Unix) 879
uninstalling (Windows) 878
Unix installation 878
Windows installation 876
RapidResponse database
backing up 315
RapidResponse Event Manager
service 228
RapidResponse framework
connectivity issues 123
RapidResponse Historical Demand poster 24
RapidResponse Historical Supply poster 24
RapidResponse Integrated Project Management poster 24
RapidResponse Integration Center
persisting data 329
RapidResponse Inventory Planning and Optimization poster 24
RapidResponse Log Service 367
configuration 374
RapidResponse OpenAPI
upgrading 217
RapidResponse Sales and Operations Planning poster 23
RapidResponse Scenario Changes workbook 484
RapidResponse Server
automatically restarting 233
backing up 314
controlling in console 337
folder structure 249
installing 111
managing memory 260
preparing to install 109
preparing to upgrade 177
problems connecting to 123
recovering 328
recovering files 183
registry 351
registry settings 351
restoration errors 470
restoring 228
restoring data 315
service 227
setting locale 281
starting 228
stopping 228
system requirements 104
uninstalling 112
upgrade log files 185
upgrading 181
RapidResponse Server Monitor
service 228
RapidResponse Server service
settings 186, 233
RapidResponse Service Host
resetting 234
service 227
RapidResponse services
stopping 180
RapidResponse System Data workbook 484, 486
RapidResponse Task Manager
service 228
RapidResponse User Administration workbook 485
RapidResponse Utility Server
service 228
RapidResponse Vector-related Origin Analysis workbook 213
RAPIDRESPONSE_ROOT (environment variable) 345
RapidResponseDataTransfer folder 879
Real-time data update history
system records 280
Real-time Integration Service Endpoints system workbook 485
Real-time Integration Service Status system workbook 485
Real-time Message Log system workbook 485
Real-time Message Log workbook
system records 280
recalculating results 270
recommendations (guidelines) 503
recommendations for upgrading 177
record deletion
warning 659
record limit 657
records
data change 833
deleting from system tables 277
limit in worksheets 657
worksheet limit 529
recovering
data files 183
RapidResponse Server 328
system 315
Recovery tab
Windows Services setting 233
redacted
user information 558
reference parts
data 874
toggle button 628
registering server exits 346
registry
overriding MemoryLimit 260

settings for RapidResponse Server 351
values for database integrity 327, 392
Registry Editor (Microsoft) 351
registry keys 352
registry values
Database key 356
DataLoad key 356
Directories key 357
LogFlags key 361
Network key 361
Overrides key 362
Webplan key 352
Wow6432Node key 351
removing
groups 569
user accounts 573
users from groups 566
renaming
RapidResponse server 287
root scenario 719
report user license 539
reports
page limit 644
printed page limit 644
RequiredDataSources command argument 399
RequiredRegions command argument 399
requirements (system) 104
resetting
RapidResponse Service Host settings 234
usage count 281
resetting scenarios 408
resetting usage count 710, 748
resiliency 289
server 289
Resouce Permissions workbook 585
resouces
modifying 740
resource assignments 504
by group 582
by resource 587
by user 585
resource authors 504
Resource Check In Log 745
resource package
exporting 752
resource packages
importing 757
Resource Permissions workbook 485, 575, 582, 587
resources
assigning to groups 529
assigning to users 554
comparing 761
deleting 740
exporting 752
providing access 513
settings 777, 807
usage statistics 746
Resources workbook 485, 746
responsibility
specifying scenario for calculations 635
troubleshooting 234
ResponsibilityPlan configuration 635
Restart command 407
Restart scheduled task 383
restoration error codes 470
restoring
data during import 329
data to RapidResponse Server 315
database backup 317, 319
RapidResponse Server 228
Restoring
User Groups 679
retrieving workbooks 751
reverting to predefined workbooks 751
Risk/Opportunity Analysts group 498
Risk/Opportunity Assessment workbook 792
Root registry value 360
root scenario
committing data to 717
root scenario, renaming 719
RootShared registry value 360
RRMonitor registry value 364
RRMonitor.log 246
Run Automation Task form 767
run time windows for scheduled tasks 417
RunAddin command 407
running
automation tasks 767
scheduled system tasks 412
Running Plan scenario (Approved Actions) 703
RunScheduledTasks registry value 356

S

S&OP Process Owners group 499
SaaS (Software as a Service) 15
Safari 543
Sales and Operations Planning
profile variables 777
scheduled tasks 782
Sales and Operations Planning poster 23
Sales group 499
SavedArchives folder 243
saving
data during import 329
scenario command argument 402
Scenario command argument 394, 399, 404-405, 408-409, 411
scenario hierarchies 719
Scenario Response form 771
ScenarioCommit command 408
ScenarioNameUnique processing rule 170
ScenarioReset command 408
scenarios
Approved Actions 533, 703
committing 408
creating hierarchies 719
creating perspectives 725
deleting 711
deleting unused 712
Enterprise data 703
Enterprise Data 533, 703
giving access to 533
memory consumption 270, 704
names 170
permanent 714
renaming root 719
responding to 771
scope 170

setting up with suppliers 820
size 270, 704
specifying for responsibility calculations 635
updating 707, 724
updating automatically 716
Scenarios workbook 485, 709
ScenarioUpdate command 409
scheduled system tasks 170
arguments 414
logging 418
running 412
ScenarioUpdate 724
Scheduled System Tasks workbook 485
Scheduled System Tasks worksheet 412
scheduled tasks
Auto-delete 382
Capture 382
Checkpoint and Version Reclaim 382
commands 384
Condense 382
Create Backup 382
Data Import 383
Data Update 383
Database Integrity Check 383
enabling schedules 416
frequency 417
included with RapidResponse 384
logging 423
messages 413
Prune Backup Packages 383
repeating 417
Restart 383
run time windows 417
Sales and Operations Planning 782
Snapshot 384
Start Time Window 413
Supplier Collaboration 825
turn on and off 748
unlocking 769
SCM. See Supply Chain Management[SCM] 783
scorecards
annual plan targets 636
assigning to groups 529
deleting 748
setting standard headers and footers 645
Script Manager 750
scripts
canceling 750
monitoring 750
Supplier Collaboration 825
SDK
creating trusted assembly 849
installing 848
testing trusted assembly 850
Secure file transfer
Data Transfer Client 876
Secure Sockets Layer
generating certificates 126
security
about 45
generating certificates 126
HTTPS protocol 104
in RapidResponse 45
Security Audit worksheet 430
SecurityAudit.log 477
Select controls 163
self-healing lead time 792
Self-Healing Lead Time 792
Self-Healing Supply Chain 792
self-healing yield 792
Self-Healing Yield 792
Sender Policy Framework 96
SeparateLogs registry value 361
separator
for split orders 631
server
automating operations 335
example setup 102-103
managing memory 260
recovery 315
server administrator role 34
Server Exit table, registering 346
server exits
environment variables 345
plan operations 349
plans 349
registering 346
running 347
server exit methods 349
server operations 344
WshEnvironment object 345
WshShell object 345
server ID
generate 124, 274
server identification text 632
Server Operation worksheet 424
Server operations
ServerDataUpdate 344
ServerPostImport 344
ServerPostRestore 344
Server Performance History system workbook 485
Server registry value 356
server resiliency 289
server.log 464
SERVER_ID (environment variable) 345
ServerAudit.log 463
ServerComm
failover 300
ServerCommand
about 339
ServerConfiguration registry value 365
ServerDataUpdate 344
ServerExits registry value 361
ServerLoadAlertThreshold 260
ServerLoadAlertThreshold registry value 356
ServerPostImport 344
ServerPostRestore 344
Service Host
configuring 234
service settings for RapidResponse 186, 233
service updates 152, 182, 185, 192
failover 305
ServiceHost.log 461, 463
ServiceHost_ThreadCount configuration setting 235
Services
Windows 227
session expiry 611
SESSION_ID (environment variable) 345

SESSION_PASSWORD (environment variable) 345
SetRapidResponseOrigin command argument 400
SetRapidResponseOriginOnModify processing rule 642
setting
    default email address 656
    memory limit 544
    message limits 650
    MRPDate calculation 286
settings
    age deletion threshold 277
    alerts 671
    GlobalSCAPE EFT Server 903
    hierarchy limits 660
    import to scenario options 662
    language 65
    locale 281
    printed report page limit 644
    printed reports 648
    registry 351
    resources and tools 777, 807
    time out 611
    time zones 669
SFTP
    Data Transfer Client 876
sharing
    add-in applications 641
    Data Publish workbook 887, 893
    scenarios 533
Show Data Changes, transaction logging 406
sign-in 46
    activities 595
    errors 602
    failures 595
    invalid user IDs 595
    monitoring 49
    successful 595
    URL 553
sign-in log
    resetting 281
Sign-in log records
    system records 281
Sign-in Log workbook 486
sign-in notice 614
signing in
    URL for RapidResponse 122
single sign-in (SSI)
    about 835, 863
    allowing trusted access 852
    bypassing 860
    creating environment 843, 865
    creating trusted assembly 849
    interfaces 839
    limitations 843, 864
    pass-through authentication 843, 865
    requirements 837, 864
    SDK 848
    trusted authentication 847
    user accounts 844, 848
sites
    assigning to groups 529
    inventory 274
    licensing 274
    logical 274
    physical 274
Sites workbook 486
slow queries 603
SmartStart link menu 618
Snapshot command 409
Snapshot scheduled task 384
software
    importing license keys 124, 273
    system requirements 104
Software as a Service 15
SOP_OrderPolicy macro 786
SOP_PartType macro 786
specifying
    display names for calendars 629
    split order separator 631
SPF (Sender Policy Framework) 96
split orders, separator 631
SSO (single sign-in) 835, 863
standard
    headers and footers 645
    workbooks 751
standby server 301
Start Time Window for scheduled tasks 413
starting
    RapidResponse 122
    RapidResponse Server 228
status bar
    server identification text 632
StopErrorLimits command argument 400
stopping
    RapidResponse Server service 180
stopping RapidResponse Server 228
subscribers
    data transfers 886
    defining 885, 892
    deleting 885, 892
subtotal row, page break after 648
successful sign-ins 595
Supplier Collaboration 815
    alerts 824
    resources 822
    scheduled tasks 825
    scripts 825
    setting up scenarios 820
Supplier Collaboration - Forecast workbook 822
Supplier Collaboration - Orders workbook 822
Supplier Collaboration Order Cleanup workbook 824
Supplier dashboard 822
Suppliers [Template] group 500
Suppliers group 500
Supply Chain Management
    attributes 783
SupplyAgentExportOverride registry value 362
SupplyAgentStartupOverride registry value 362
system administrator
    about 34
    user type 541
system auditing 51
system crashes
    resolving 241
system forms
    accessing 741
system groups 540
    about 537
    required 537

system instability
resolving 241
system memory
32-bit versus 64-bit 260
overview 260
settings overview 260
system performance 659
system records, automatic deletion of records 277
system recovery 315
system redundancies 56
system requirements
hardware 104
Microsoft Internet Explorer 543
Microsoft Internet Information Services 106
RapidResponse Application Server 105
RapidResponse Data Transfer Client 877
RapidResponse Server 104
software 104
upgrading 144
user 541
Web server 105
system tables 487
system workbooks 482
accessing 741
overview 481
RapidResponse System Data 486
Resource Permissions 585
SystemInfo.txt 242

T

table command argument 402-403
tags
global 772
Tags workbook 486, 772
Task Arguments worksheet 415
task flows
deleting 748
TCP/IP ports 283
testing
RapidResponse Application Server upgrades 194
RapidResponse installation 122
trusted assembly for single sign-in 850
time
codes 666
creating formats 666
time-out setting 50, 611
time and date formats 666
time zones
changing 670
setting 669
warning 670
Time Zones dialog box 671
TimeLimit registry value 365
timestamp_full.mdmp file 245
timestamp_limited.mdmp file 245
timestamp_small.mdmp file 245
TimeZone table 671
tool settings 777, 807
tracking data changes 829
TransactionLogging command argument 400
transferring data 55, 875
troubleshooting
alerts 234
generating system information 244
queries 605
RapidResponse connections 123
responsibility 234
sign-in errors 602
webplnSC 338
workbook error messages 602
TruncateOnOpen registry value 361
trusted authentication 847
type command argument 389
types of users 541

U

Unicode
fonts 644
support 65
uninstalling
Capacity Manager 132
Engineering Change Manager 134
RapidResponse Application Server 127
RapidResponse Data Transfer Client (Unix) 879
RapidResponse Data Transfer Client (Windows) 878
RapidResponse Server 112
units of measure
categories 700
conversion 697
creating 695
part-specific conversions 698
unlocking automation resources 769
unlocking user accounts 599
unused scenarios, deleting 712
Update Conversion Rates workbook 486
updating
scenarios 707
scenarios automatically 716
updgrading
RapidResponse server 178
upgrade failure, RapidResponse Server 183
Upgrade x.y.z.log 194
Upgrade x.y.z.tab 194
upgrade.log file 163
upgrading
changes to resources 196
dashboards 161
failover 305
On-Premises considerations 198
overview 141, 177
preparing 109
process 143
RapidResponse Application Server 190
RapidResponse applications 184
RapidResponse OpenAPI 217
RapidResponse Server 181
resources 198
testing 194
URL
RapidResponse sign-in 122
URLs
for web services calls 744
usage
resetting 710, 748
usage statistics
resources 746
user account permissions 49, 504

user administrator
about 35
user type 541
User command argument 408
User groups
Importing 679
Migrating 677
Restoring 679
user IDs 46
user information
visibility 556
user interface 504
user names 556
user provisioning; bulk 549
user types 504
USER_ID (environment variable) 345
users
adding to groups 566
allowing to bypass single sign-in 860
assigning resources 554
changing password 570
creating 549
creating alerts 551
deleting 573
deleting configuration file 573
denying permissions 554
disconnecting 601
duplicating 553
granting permissions 554
group membership 585
guidelines for creating 503
invalid characters 549
last sign in 573
license information 541
licenses 539
modifying 570
passthrough authentication 844
providing access to add-in applications 640
providing data formats 663
removing from groups 566
sign-in URL 122
system requirements 541
trusted authentication 848
types 541
unlocking accounts 599
users cancel query 606
UtilityServer.log 463

V

vector data 213
converting tables 214
currency issues 210
key uniqueness 205
upgrade issues 207
verifying
user licensing information 541
version contol
discarding a check out 743
version control
check in comments 742
check in log 745
resource visibility 739
turning on or off 742
version history 743, 756
Version Reclaim Sweep scheduled task 384
versioned database 270, 704
VersionReclaim command 411
VersionReclaimSweep command 411
versions
scenarios 711
viewing
license keys 274
queries 605
virtual memory
Java Runtime Environment 544
virtualization 106
virus scanning and performance 256
visibility 556
VMWare, system requirements
virtualization 106
VSE (McAfee Virus Scan) 256

W

warnings
record deletion 659
time zones 670
unsaved workbook changes 668
Web-based
client connections 123
Web server system requirements 105
Web server URL 162
Web Start application 541
web.config file 162
Web.config file 841
Webplan registry key 352
webplnSC
about 335
command structure 337
controlling RapidResponse Server in console 337
error messages 338
what's new
overview 67
whitelisting URLs 744
widgets
text 28
viewing help 28
Windows Computer Management dialog box 242
Windows Event Log Service records 242
Windows Services
RapidResponse 227
Work Center link menu 618
workbook
link menu 618
Workbook command log records
system records 281
workbook help 25
show 25
workbook properties 163
workbooks
Administration workbook 346
Application Settings 783
assigning to groups 529
Attribute Rules 786
Buyer Commit to ERP 824
Clear to Build 786
Data Integrity - Material 785
Data Publish 875
deleting 748

error messages 602
Forecast Response 823
hiding data in Data Publish 892
Multi-Enterprise Inventory 792
Multi-Enterprise Management 792
predefined 751
Purchase Order Response 823
retrieving 751
sharing Data Publish 893
Supplier Collaboration 824
Supplier Collaboration - Forecast 822
Supplier Collaboration - Orders 822
Supplier Collaboration Order Cleanup 824
system 481-482, 741
workbooks, procedures with
accessing help 21
worksheet help
show 25
worksheet record limit
exceeding 529
setting 657
worksheets
Add-Ins 639
caching results 763
customizing the link menu 618
setting record limits 657
setting standard headers and footers 645
Wow6432Node registry key 351
wpzip
decompressing archives 251
Write Debugging Information
diagnostics archive 248-249
dump file 248-249
WshEnvironment object 345
WshShell object 345

X

X.509 certificates 858
x64 system requirements 105
Xeon system requirements 105
XML deprecation 163

World Headquarters

700 Silver Seven Road
Ottawa, Ontario
Canada K2V 1C3

Tel. +1 613.592.5780
Toll free. +1 866.236.3249
Support. +1 866.463.7877

Email. info@kinaxis.com

KNOWLEDGE NETWORK

Want knowledge about RapidResponse from Kinaxis-vetted experts? Join the Kinaxis Knowledge Network!

https://knowledge.kinaxis.com