



Effective Keyword Searching Using the RSA Archer eGRC Platform

Patrick Boos

Designated Support Engineer

October 2012

Objective

This Free Friday Tech Huddle will provide effective strategies for keyword searching. In addition, we will cover common search issues and their solutions.

Agenda

- Quick Search description
- Advanced Search description
- Keyword Search Operators
- Common Search Issues
- How to Perform an Index Rebuild
- Q&A

What is Quick Search?

- Located in the top of the user interface
- Performs a search across all applications of a solution
- Narrow search results by using a variety of keyword search operators



What is Advanced Search?

- Search records across a single application or across a chain of applications
- The primary application is the application from which you originate your search, and secondary applications are any number of subsequent applications linked to the primary application
- When searching related content, the criteria must match on all levels of a leveled application to return results
- Combination of Keywords and Filters can be used to narrow the search

Advanced Search (continued)

Multiple-Application Search

- Each secondary application has a direct relationship to the primary application. The system ignores any relationships between the secondary applications.

The screenshot displays the 'Advanced Search: PrimaryApplication' interface. It features a 'Fields To Display' section with an information icon and the instruction 'Select fields to display on the search results page.' Below this, there are two columns: 'Available' and 'Selected'. The 'Available' column contains a search box, a 'Name' dropdown, and a tree view of fields. The 'Selected' column shows the chosen fields with 'x' icons for removal. Blue arrows point from the text 'Primary Application' to the 'PrimaryApplication' field in the tree, and from 'Secondary Applications' to the 'SecondaryApplication1' and 'SecondaryApplication2' fields. At the bottom, there is a 'Statistics Mode' checkbox and a 'Configure Relationship' link.

Available	Selected
Find: <input type="text"/> Name <input type="text"/>	PrimaryApplication
<input type="checkbox"/> PrimaryApplication	Tracking ID <input type="checkbox"/>
First Published	SecondaryApplication1
Last Updated	No Fields Selected.
SecApp1	SecondaryApplication2
SecApp2	No Fields Selected.
Tracking ID <input type="checkbox"/>	
<input type="checkbox"/> SecondaryApplication1	
<input type="checkbox"/> SecondaryApplication2	

Statistics Mode Return search results in the form of a statistics report by grouping and aggregating field values. [Configure Relationship](#)

Advanced Search (continued)

N-Tier Search

- The primary application has a direct relationship to a secondary application; the secondary application in turn has a direct relationship to another secondary application, and so on.

Fields To Display

Select fields to display on the search results page.

Available

Find: Name

- [-] PrimaryApplication **Primary Application**
 - First Published
 - Last Updated
 - SecApp1
 - SecApp2
 - Tracking ID
- [-] SecondaryApplication1 **Second Level Application**
 - First Published
 - Last Updated
 - PrimaryApplication (SecApp1)
 - SecondaryApplication2 (SecApp1xref) **Third/N-Tier Level Application**
 - Tracking ID
- [+] SecondaryApplication2

What types of items can be returned in a search?

- Application Records
- Items in Files from the following file types:
 - Microsoft Word
 - Microsoft Excel
 - HTML
 - PDF
 - Text
 - CSV
- File Names from the following file types:
 - HTM
 - JPG
 - JPEG
 - GIF
 - PNG
 - BMP

Keyword Search Types

- Single Term
- Phrase
- Wildcard
- Fuzzy
- Proximity
- Operators
- Grouping
- Escaping Special Characters

Single Term

Returns all records that contain the term specified in the search.

Example:





A search input field with an orange border containing the text "authentication". To the right of the input field are two icons: a magnifying glass and a downward-pointing arrow.

Quick Search Results	
New Modify Save 1 to 50 (of 1,262)	
Search Results	
Results: All (1262) , Authoritative Sources (215) , Control Procedures (548) , Control Standards (70) , Policies (22) , Question Library (407)	
09.1.04 Authentication Establishes requirements for user authentication to external connections.	100%
NIST800.53.09-T007 Identification and Authentication	92%
CP-124539 Technical ♦ Use only secure authentication for VPN connections. ♦ In Scope ♦ Compliant ♦ ATCP-25792	74%
CP-124581 Technical ♦ Use only secure authentication for VPN connections. ♦ In Scope ♦ Compliant ♦ ATCP-25834	74%
CP-129097 Technical ♦ Windows Authentication should be enabled when online responder role service is installed ♦ In Scope ♦ Compliant ♦ ATCP-29391	72%

Phrase

- Returns all items within quotes.
- If words are not enclosed in quotes, results can be returned without all words in the phrase.

Example:

Search Results	
Results: All (3) , Authoritative Sources (2) , Control Standards (1)	
08.05.07 User Identification - Authentication Policies PCIDSS2_0-SS069	100%
08.05 Authentication and Password Management PCIDSS2_0-S031	50%
ATCS-018 Communicating Existing, New and Changed Security Policies ♦ The Company's Information Security Policy should be available to all Company personnel via an Intranet-based application, or other appropriate medium. Company personnel should be informed when policies or control standards are created or changed. ...	31%

Wildcards

- Wildcards are used to substitute for any other character or characters in a string
- Types:
 - ? = Single character wildcard.
a?ert will return – alert, avert, etc.
 - * = Multi-character wildcard.
document* will return – document, documentation, documenting, etc.

Searching using the “*” character only will return an invalid search.

Note: Wildcards cannot be placed at the beginning of a search.

Fuzzy and Proximity Search

Fuzzy – returns words which have a similar spelling or misspelled words

receive~ returns both receive and recieve.

Proximity – returns words which are within a specified amount of words

“important document”~4 returns phrases which include important and document that are within four words of each other.

Operators

AND – Returns records that have all of the words joined with the operator

Example: *important AND document*

Will only return records which include both the words important and document.

OR – Returns records that have either of the words joined with the operator

Example: *important OR document*

Will return records that contain important, document, or important and document.

NOT – Excludes words specified by the operator

Examples:

important NOT document

Will return records that contain important but not document.

Operators continued

“+” - Returns records with the first word in the statement, all words in the statement, but not records with only the last word in the statement.

Example:

+important document

Returns records which contain important, important and document, but not records with only the word document.

“-” - Returns records without words referenced after the operator.

Example:

-important document

Returns records which contain document, but not records with the word important.

Grouping

Allows keywords to be grouped within parenthesis to alter search results

Example:

(important OR urgent) AND document

Search will return all records with the term document and either or both the words important and urgent.

Escaping Special Characters

Specific characters need to be escaped with quotes to return accurate results. These characters include:

+ - && || ! () { } [] ^ " ~ * ? : \

Example:

“12:01” – Returns all records that contain 12:01

12:01 – Returns no results due to the special character

Keyword Search Demo

Common Issues

Issue: Search does not produce results or inconsistent results.

Resolutions:

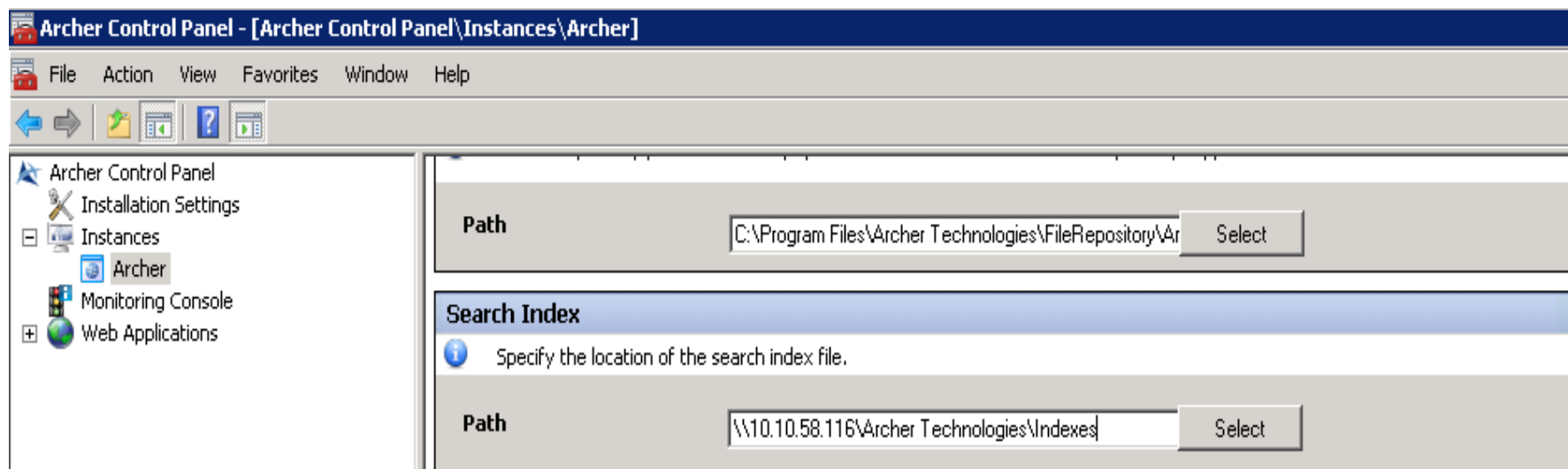
1. Ensure the Queuing service on the services server is set to automatic. If it is set to manual, the service would need to be manually started
2. The Archer Queuing Service creates the indexNumber (i.e. 50000), quicksearch and filerepository sub-directories within the index\indexNumber location. It and then creates the index files within these directories.
The Archer Queuing Service creates, deletes, and updates files in these folders. The Archer application (IIS app pool) reads from these files. Virus scanning systems (and backup systems) may temporarily lock the index files and prevent the Archer Queuing Service from updating or deleting the files.
3. Rebuild the Search Index. Performing an index rebuild drops and re-creates the index. This removes fragmentation and reorders the index rows in adjacent pages.

Common Issues

Issue: Search does not return results in a multi-server environment

Resolution: The index location must be placed in a folder in which the service account and application pool account have modify access. The search index file location is in the Archer Control Panel > Instance > InstanceName > Search Index. In a multi-server environment, the location must be specified using the UNC path. We recommend to place this folder on the same machine which hosts the queuing service.

Example: \\ServerName or IP\PathToDirectory



Common Issues

Issue: Keyword Search returns results in quick search, but does not return results in Advanced Search.

Resolution: In a quick search, results are returned from all levels of the application. In advanced search, the criteria must match on all levels of the application.

Issue: Record counts are different for some users using the same search

Resolution: Permissions apply regardless of the structure of the search. Record Permission fields restrict access to records. You cannot view records that you do not have access to.

How to perform a Search Index Rebuild

1. Stop the Archer Datafeed Service
2. Stop the Archer Job Engine Service
3. Stop the Archer Queuing Service
4. Delete list.bin file if it exists (By default it is located in ...\\Archer Technologies\\Services folder)

How to perform a Search Index Rebuild (continued)

5. Run the following script on the instance database

```
TRUNCATE TABLE dbo.tblSearchMessageContent

SET ROWCOUNT 100000

WHILE EXISTS ( SELECT    1

                FROM      dbo.tblSearchMessageQueue smq

                LEFT OUTER JOIN  dbo.tblSearchMessageContent smc ON smq.message_id = smc.message_id

                WHERE  smc.message_id IS NULL )

BEGIN

    DELETE    smq

    FROM      dbo.tblSearchMessageQueue smq

    LEFT OUTER JOIN  dbo.tblSearchMessageContent smc ON smq.message_id = smc.message_id

    WHERE  smc.message_id IS NULL

END

SET ROWCOUNT 0
```

How to perform a Search Index Rebuild (continued)

6. Delete the old Index files (you can obtain the index location from the Archer Control Panel, Search Indexes icon)
7. Start the Archer Queuing Service
8. Start the Archer Data Feed Service
9. Start the Archer Job Engine Service
10. Open the Archer Control Panel, select the instance name, initiate the full index rebuild from the right most menu.

How to ensure the index is being built

Run the following query in the instance database and monitor the count that it returns. This is the amount of records that are queued for indexing. You should see the number decreasing:

```
SELECT COUNT(*) FROM tblSearchMessageContent
```

In addition, the time stamps on the files in the index directory will also allow you to monitor the change in the index.

NOTE: Do not assume the index needs to be rebuilt just because the index is not updating. It is important to investigate and find the root cause of the issue.

Questions?

Contacting Support

- Email:

archersupport@rsa.com

- Phone:

USA: 1-800-995-5095 (option 5 for Archer)

Global numbers:

<http://www.emc.com/support/rsa/contact/phone-numbers.htm>

Resources for You



- Archer Community – private community for your use: discussion forums, blog, events, Archer downloads, on-demand videos and more
- Archer Exchange – search and download on-demand bus application for your GRC platform, download content, get tools for systems integrations
- Monthly Customer Newsletter – emailed to you
- SCOL - locate and search a support knowledgebase, download current patches and bug fixes, sign up for advisory notifications, manage cases and more

Resources (continued)

- GRC Roadshows – Coming to a city near you!
- Weekly Webcasts on the core Solutions, use cases, best practices: every Thursday 2:00EDT
- Weekly Friday's Free Customer Training with Customer Support: every Friday at 12:00EDT

ANNOUNCEMENT: TOP EXECUTIVES SAY GRC PROGRAMS MUST BETTER ALIGN TO STRATEGIC PRIORITIES [Show Details](#) 1 2 3 4

COMMUNITIES

- GRC Ecosystem
- RSA Archer Community
- RSA Archer Exchange
- RSA Product Communities

Search RSA Archer

RECENT BLOG POSTS

- [Cloud Security and Compliance – Where the heck can you start? in RSA Archer](#)
- [Gray Areas in RSA Archer](#)
- [Q2-2012 Additions to the RSA Archer eGRC Content Library in RSA Archer](#)
- [Knowing the Past, Teaching the Future: GRC Process Maturity in RSA Archer](#)

[More >](#)

DOUBLE AD TAGS

RSA Archer Community NEWSLETTER

Read the latest edition

[Click Here](#)



The RSA Archer eGRC Community enables collaboration among RSA Archer GRC clients, partners and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer product roadmap.

Downloads



Access an array of Archer training materials, help and reference guides, product overviews and solution content.

Discussions



Share opinions, ask questions, and exchange best practices about Archer product use and configuration.

Ideas



Submit and discuss enhancement requests. Members may cast votes for ideas that would fuel their organization's success.

Blog



Get news on industry issues and a variety of topics, ranging from product enhancements to upcoming events.



- [RSA Breaking News](#)
- [SecurCare Online](#)
- [Summit Videos](#)
- [Summit Presentations](#)
- [Customer Testimonials](#)
- [RSA Webcasts](#)
- [Solution Demo Videos](#)
- [Customer Support](#)
- [Training](#)
- [Have Questions?](#)

ACTIONS

- [Start a discussion](#)
- [Create a document](#)
- [Write a blog post](#)

NEW Solution Packages Available On RSA ARCHER EXCHANGE

Audit Management 4

Policy Management 3

Issue Management 3

Vendor Management 3

Risk Management 4

Compliance Management 4

Incident Management 3

The New Packages allow users to bundle, move & deploy solutions much faster, significantly shortening the migration & upgrade process. All solutions and packages require instance of the RSA Archer eGRC Platform 5.2. On each Exchange solution posting you will find:

- Installation Files
- Release Notes
- Installation Guide

Note: '4' was formerly 5.2; '3' was formerly 5.0



GRC Roadshows are coming to city near you

- Join your colleagues for the 'free, full-day' GRC Roadshows within various city locations within the US and Europe. The events provide a unique networking forum that foster engagement with fellow risk and compliance professionals to discuss GRC trends, challenges and opportunities. **As of 10/3 10:18 am**

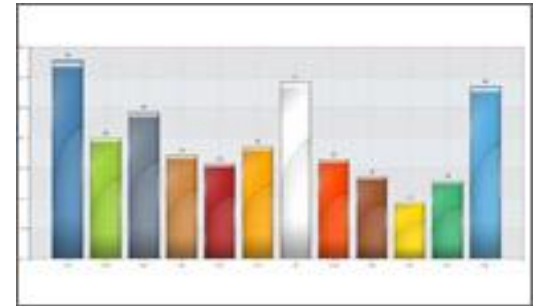
CITY	DATE	LOCATION
Chicago	Oct. 29	Aon
Minneapolis	Oct. 30	US Bank
Toronto	TBD	The Herjavec Group
Vancouver	TBD	Bell
Kansas City	Nov. 1	Fishnet
Seattle	Nov. 7	KPMG
Atlanta	Nov. 8	Equifax
Los Angeles	Nov. 8	KPMG
Charlotte	Nov. 15	Deloitte
Washington, D.C.	Nov. 28	CSC
Boston	Nov. 29	Genzyme
Dallas	Dec. 3	American Airlines
Houston	Dec. 4	KPMG
Denver	Dec. 11	Accuvant
New York City	Dec. 12	Time Inc.
Philadelphia	Dec. 13	Deloitte
San Francisco	Dec. 14	eBay



Special 5.3 Webcast: Thursday October 25 at 12 ET

Please attend and review...

- 5.3 Data Visualization changes
- Potential changes to the look and feel of existing charts and graphs
- 5.3 charting changes and ways to identify potential charts that may change
- Strategies to adjust these to work with the new charting engine
- Go to the RSA Archer Community for the web link and dial-in number



*5.3 Release WEBCAST
Thursday, Oct 25
12:00 ET*

RSA Archer Administrative training: Basic and Advanced. Instructor-led, at your office or ours, online virtual, video learning and more.

RSA Archer Certification: exam, testing centers, cost, study and preparation

<http://www.emc.com/training/rsa-education-services/certification.htm>

« SUPPORT & TRAINING

☑ CONTACT SALES ☑ SHARE

RSA SECURITY TRAINING AND CERTIFICATION



OVERVIEW



COURSES AND REGISTRATION

ONSITE TRAINING

TRAINING CREDITS



CERTIFICATION

PAYMENT AND CANCELLATION

CONTACT INFORMATION

FAQ

Courses and Registration

RSA Education Services provides training for core RSA products as well as RSA Archer and RSA NetWitness offerings. Various media are available to meet customer schedules and budgets as well as to accommodate individual learning styles.

Training Options

- **Instructor-led** — Classroom-based training delivered globally by experienced training professionals.
[View courses and register.*](#)
- **Online Virtual** — A live instructor with students logging into their training session remotely. Lecture, demos, student materials, and lab exercises are included just like a traditional classroom experience.
[View courses and register.*](#)
- **Video ILT** — Provides the student with instructor-led video learning that is packaged in a convenient self-paced CD format with an intuitive navigation menu. Lecture content, lab exercises, and student materials are identical to classroom training.
[View courses and register.*](#)
- **eLearning** — Offers students the ability to start and stop their learning at will and participate at a pace that suits their schedules. RSA's eLearning offerings are interspersed with lecture segments as well as practical simulations.
[View courses and register.*](#)



THANK YOU