

## Advanced Searching

The search box can be used to search for simple terms as well as for more structured queries. This section describes the syntax for advanced queries.

An advanced query consists of terms and operators. Terms can be single words (such as "test" or "hello"), or a phrase enclosed in double quotes (such as "hello dolly"). Single terms (but not phrases) can include wildcards, \* and ?, anywhere except the start of a term.

In addition to terms and operators, queries can refer to specific fields, such as "assetType:computer."

There are more esoteric search facilities. For example, a term that ends with a tilde (~) is a proximity search. Fielded range searches, such as likelihood:[1 TO 4], are supported. When searching for more than one term, a query can "boost" the relevance of a particular term.

Terms are combined with Boolean operators to form more complex queries.

Search Type	Example
Basic	server
Phrase	"cvss score"
Wildcard	serv* (matches server, serving, serves) te?t (matches test, text)
Fielded	assetType:computer
Boolean Operators	The following Boolean operators are supported: <ul style="list-style-type: none"><li>▪ <i>term1 AND term2</i></li><li>▪ <i>+term1 term2</i> (+ indicates that term1 must exist to match)</li><li>▪ <i>term1 NOT term2</i></li><li>▪ <i>term1 -term2</i></li></ul>
Fuzzy	server~ (matches server, swerver, fever, fervor, etc.)
Fielded range	impact:[1 TO 4] (inclusive--matches impact 1, 2, 3, or 4) impact:{1 TO 4} (exclusive--matches impact 2 or 3)

### Additional Information

For more information about the advanced searching features built in to RiskVision, see [http://lucene.apache.org/core/2\\_9\\_4/queryparsersyntax.html](http://lucene.apache.org/core/2_9_4/queryparsersyntax.html).

**Using special characters to search objects might not return correct results. Instead, you can use the Advance Filter in the Filter by drop-down list if you have to perform a multi-criteria search.**

### Supported Fields

The following fields can be used to narrow the scope of a search to a particular field for certain objects. In the context of a grid of Policy objects, for example, you can search for specific policy types:

**policyType:**

## Asset/Entity

- assetType
- assetSubtype
- name
- organization
- division
- subDivision
- assetNumber
- address.name
- address.address
- address.physicalPosition
- address.floor
- address.building
- address.city
- address.state
- address.region
- address.postalCode
- address.country
- assetTags.name
- assetTags.category
- assetTags.description
- assetTags.createdBy
- assetTags.createdTime
- assetTags.displayName
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1

## Computer System

Kind of Asset/Entity; adds:

- applicationLinks.cpe.description
- applicationLinks.cpe.title
- applicationLinks.cpe.part
- applicationLinks.cpe.vendor

- applicationLinks.cpe.version
- operatingSystems.cpe.description
- operatingSystems.cpe.title
- operatingSystems.cpe.part
- operatingSystems.cpe.vendor
- operatingSystems.cpe.version

### Exception Request

- name
- justification
- startDate
- nextReviewDate
- requestedBy
- approvedBy
- status
- restart
- reEnd
- risk
- gap.createdBy
- gap.creationTime
- gap.name
- gap.status
- gap.priority
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3
- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3
- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

### Incident

- title
- description
- timeStarted
- timeDetected
- timeReceived
- uiIncidentId
- incidentNumber
- currentWorkflowStageName
- incidentType.typeName
- incidentType.typeDescription
- incidentSubtype.subtypeName
- incidentSubtype.subtypeDescription
- incidentDetail.severity
- incidentDetail.priority
- incidentDetail.status
- incidentDetail.preventiveMeasures
- incidentDetail.causeAnalysis
- incidentDetail.confidentialityAffected
- incidentDetail.integrityAffected
- incidentDetail.availabilityAffected
- incidentDetail.businessCriticality
- incidentSubmitter.caption
- attachments.name [Note misspelling]
- attachments.pathId [Note misspelling]
- attachments.url [Note misspelling]
- attachments.version [Note misspelling]
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3
- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3

- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

### Policy Set

- title
- description
- descriptor
- definitions
- scope
- purpose
- audience
- supportingInformation
- keyPoints
- policysetType
- policysetSubtype
- parentPolicySetIds
- policySetCategoryIds
- currentWorkflowStageName
- workflowUserDefinedStatus
- tags.name
- tags.category
- tags.description
- tags.createdBy
- tags.createdTime
- tags.displayName
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1

### Policy

- title
- description
- descriptor
- policyType
- checkFunction

- parameters
- checkType
- checkDescription
- organization
- parentPolicySetIds
- policySetCategoryIds
- tags.name
- tags.category
- tags.description
- tags.createdBy
- tags.createdTime
- tags.displayName
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1

## Report

- name
- displayName
- description
- reportOn
- reportFocus
- reportType
- reportChartType
- reportCreationType

## Ticket

- name
- description
- plannedStartDate
- startDate
- owner
- priority
- createdBy
- updatedBy

- exceptionExpireTime
- incident.title
- submitter.userid
- attachments.name [Note misspelling]
- attachments.pathId [Note misspelling]
- attachments.url [Note misspelling]
- attachments.version [Note misspelling]
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3
- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3
- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

### **Vulnerability ID**

- captionDB (vulnerability title)
- identifier (use title if available)
- description
- abstractText
- analysis
- recovery
- defaultSeverity
- cvssVector (matches value to first '!')
- likelihood
- source
- sourceFlags (string from int; for example, 3 is 'nvdbidefense')
- assessmentCheckSystem
- assessmentCheckName
- assessmentCheckHref
- recordType

- vulnerableProducts.description
- vulnerableProducts.title
- vulnerableProducts.vendor
- vulnerableProducts.version
- data.data
- tags.name
- tags.description
- tags.type
- tags.referenceType

### **Vendor ID**

Kind of Asset/Entity; adds:

- vendor.vendorType
- vendor.vendorTier
- vendor.vendorStatus
- vendor.vendorPreviousName