Table of Contents

About Incident Manager

Incident Manager enables organizations to collect, classify, and manage multiple IT and non-IT incidents. Incident Manager is a single collection point for all manually reported and automatically imported incidents. It imports incidents reported from most monitoring systems and scanners as well as security incident management (SIM) solutions. All incidents, including business, operational, and environmental can be reported on using the incident-reporting portal. Incidents are assessed based on configurable workflow and automatically created and classified based on rules that are tracked throughout the incident's lifecycle. Incidents are tied to controls, policies, and risk to provide closed loop feedback for policy and control assessment and risk monitoring. Incidents are rated based on criticality so organizations can respond based on impact to the business.

Other RiskVision Applications

Other RiskVision applications are listed in the table below:

ICON	APPLICATION	DESCRIPTION
✓	Compliance Manager	RiskVision Application enables an organization to effectively manage and measure compliance programs across multiple regulations, standards, and frameworks. It also automates the compliance process through general computer controls (GCC) and questionnaires. The evidence and control results can be automatically collected through connectors or questionnaire results from business users. RiskVision Application enables data classification, ownership configuration, compliance assessment, mitigation, and reporting. It supports popular frameworks, standards, and regulations such as ISO 27002, CIS, HIPAA and PCI, and others. Compliance Manager improves process efficiency and integrity as well as data quality and reliability.
🌐	Enterprise Risk Manager	RiskVision Application is a comprehensive risk lifecycle management solution. When using RiskVision Application, a company can identify, assess, and mitigate risk with an appropriate risk treatment plan. Its flexible risk model supports both qualitative and quantitative methodologies, supporting the calculation of inherent risk, current risk, and residual risk with the context of mitigating controls. RiskVision Application features rich reports and dashboards, as well as easy to use risk assessment tools and enables a company to understand and monitor its organization's enterprise risk posture. RiskVision Application provides rich out-of-the-box support for popular risk methodologies such as COSO, AZ/NZS 4360 and ISO.
🤝	Vendor Risk Manager	RiskVision Application enables organizations to audit and manage third-party risks, as mandated by regulations and standards such as ISO 27001, PCI, and FISMA. RiskVision Application classifies, assesses, and reports on third-party risk based on the standard control framework from shared assessment programs or an organization's custom control framework. It provides a portal where vendors participate in assessments and the results are retrieved by an organization's risk analysts. Vendors are classified automatically into appropriate tiers and applicable controls are applied based on the vendor tier. Powerful delegated administration and automation features enable RiskVision Application to scale to large vendor populations.
⚠	Threat and Vulnerability Manager	RiskVision Application enables organizations to consolidate their threat and vulnerability programs onto a single platform. RiskVision Application integrates with vulnerability and early warning data feeds from iDefense and National Vulnerability. It correlates these vulnerability data feeds with vulnerability scanner results to eliminate false positives and report incidents. Inferred scans are performed by correlating the vulnerability data feeds to a company's RiskVision asset database mitigating risks for assets not reachable by vulnerability scanners. Once detected, vulnerabilities are assessed and remediated using the system's workflow for true closed-loop vulnerability management.
📄	Policy Manager	RiskVision Application enables the management of enterprise policies on a single centralized platform. Organizations can enforce policy and process standards across different locations, departments, and programs. RiskVision Application supports simultaneous policy editing across multiple stakeholders using a rich WYSIWYG user interface. An organization can automate processes for policy authoring, reviewing and approval. Policy templates help enforce consistent formatting and structure. It has a highly configurable workflow enabling an organization to enforce

		change control and maintain accountability and it supports policy awareness campaigns with policy distribution, attestation, and comprehension testing tools.

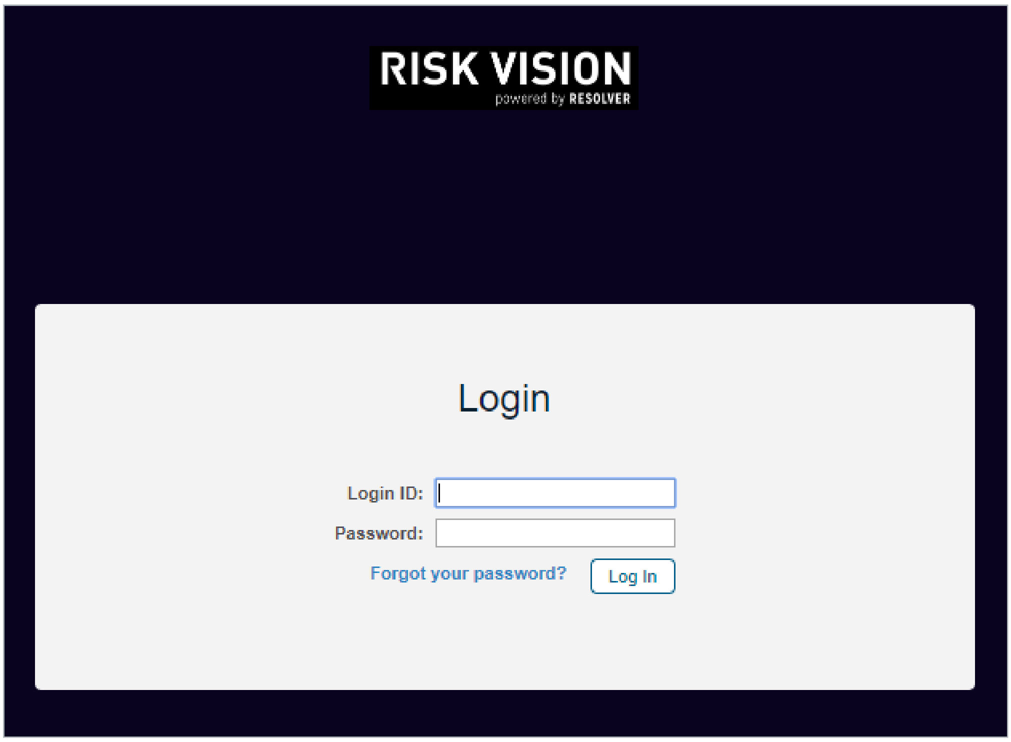
Logging in to RiskVision Application

Your login account may be identical to your Active Directory credentials, or a new ID may have been created for you within the RiskVision Enterprise Risk Manager. Contact your Administrator for your credential information.

For more information on default accounts, please refer to the Installation & Configuration Guide or contact your Resolver Customer Support representative.

To access the application using a web browser:

1. Open a browser and enter the RiskVision URL.



The RiskVision login screen.

2. For example, https://RISKVISION, where RISKVISION is the hostname or IP address for the Resolver RiskVision Server.

   Depending on your browser, you may see a message like "Web site certified by an unknown authority." To avoid seeing these types of messages in future sessions, accept the certificate permanently.

3. Enter the user name or e-mail and password that is specific to your domain, select a domain if the **Domain** drop-down list is available, and then click **Log In**.

   The first time you log in, the *License Agreement* is displayed.

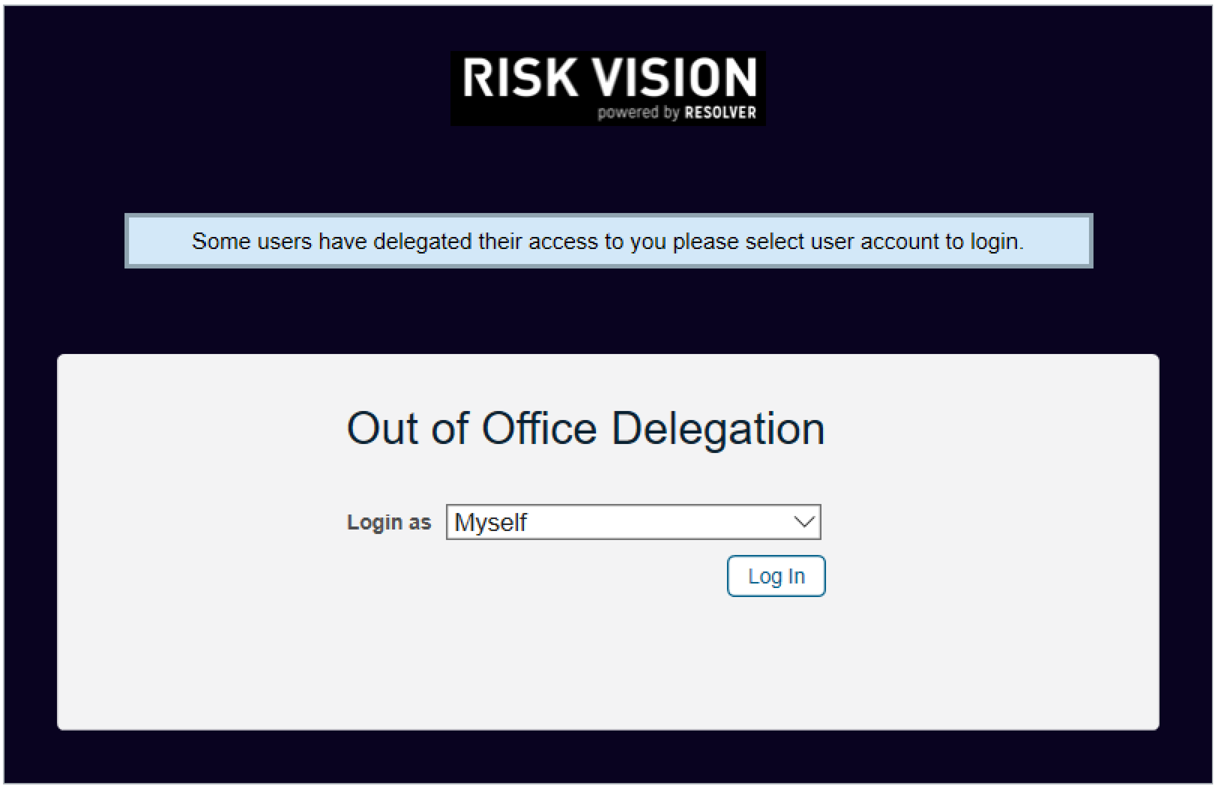
4. Click **Accept** to continue. The **Welcome** page is displayed.

Logging in as a Delegate

You can log into the account of another user if that user or a RiskVision administrator nominates you to access the delegation. To learn how to delegate your RiskVision user account, see Delegating Your RiskVision User Account.

To access a delegated user account:

1. Open a browser and enter the RiskVision server URL.
2. Enter your **Login ID** and **Password**, then click **Log In**.
3. Click **Login as** and select a user account other than **Myself**, then click **Log In**. **Myself** will log you in to your user account.



Some users have delegated their access to you please select user account to login.

Out of Office Delegation

Login as: Myself

The Out of Office Delegation screen.

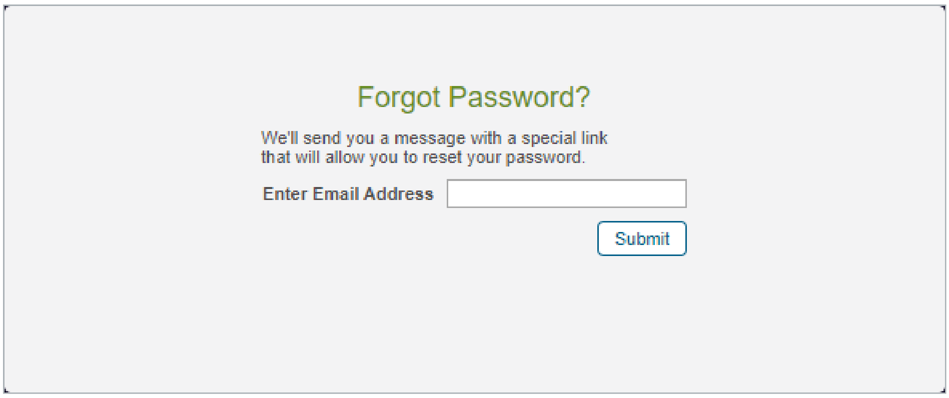
When you are logged into a delegated user account, you can perform any task permitted by that user's account permissions on behalf of that user. When the delegated user logs into RiskVision, the **Current User** will appear as **Logged in as: delegated by [username]**.

Resetting Your Password

If you've forgotten your password, you can set a new one right away with no assistance required from your RiskVision administrator.

To reset your password:

1. Open the login page.
2. Click the **Forgot your Password** link.
3. Enter the email address that has been registered in the RiskVision Server in the **Enter Email Address** field.



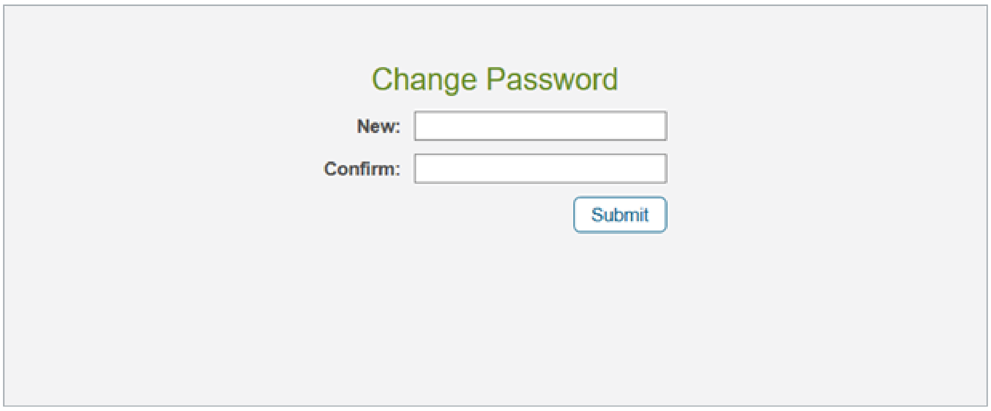
Forgot Password?

We'll send you a message with a special link that will allow you to reset your password.

Enter Email Address

The Forgot Password page.

4. Click **Submit**. An email containing the link to reset your password will be sent to your mail box.
5. Click the link in the email to open the **Change Password** page.



Change Password

New:

Confirm:

The Change Password page.

6. Enter a new password in the **New** and **Confirm** fields.
7. Click **Submit**.

To log on with your new password, see Logging in With Your New Password.

Logging in With Your New Password

After you reset your password using the **Forgot Your Password** link on the login page, you can now log in with your new password. Make sure that you close all your browser windows and then launch the RiskVision application in a new browser window.

Getting Started

All logged in users of any RiskVision application are directed to the **Welcome** page, on the **Home** menu. The **Welcome** page contains active tasks and messages which require your attention. The tasks are divided into categories and displayed as sections with links. If you are not a stakeholder in any task, you will not see any links in the sections. By default, each section will show up to five items you might own more tasks. By clicking the "**Go to...**" link below the section, you will be navigated to the respective page of that section, on the **Home** menu, to view the exhaustive list of items. Besides accessing sections, the **Welcome** page also provides **Quicklinks** to pages so that you can be directed to the desired area instead of having to manually navigate trough the RiskVision applications.

Here's the complete list of pages on the **Home** menu, which appear based on your role and the RiskVision application:

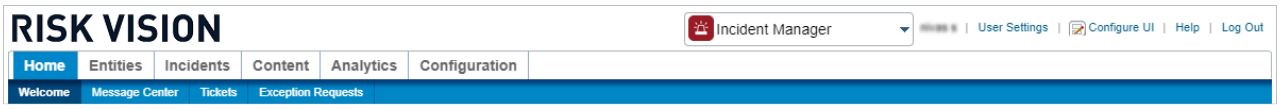
- Welcome
- Message Center
- Tickets
- Exception Requests

The pages as discussed above will help you to view, edit, or update the list of do able items, and these operations can also be accomplished from other points in RiskVision applications. Typically, the stakeholders who will not need their extreme participation in ITGRC projects are provisioned to access the pages on the Home menu. The user interface of each page can be customized to fit the needs of your business goal.

Before you move on to understand the purpose of these pages, RiskVision recommends to familiarizing yourself with the navigation, tree and grid, actions, user settings, and the advance search. For more information, see Navigating in RiskVision.

Navigating the RiskVision System

RiskVision pages use a consistent interface, shown below, to navigate easily wherever you are in the application.



The navigation ribbon in the Incident Manager.

Selecting a different application changes the menus. The specific menus and submenu choices available depends on the current application and the permissions assigned to your user role.

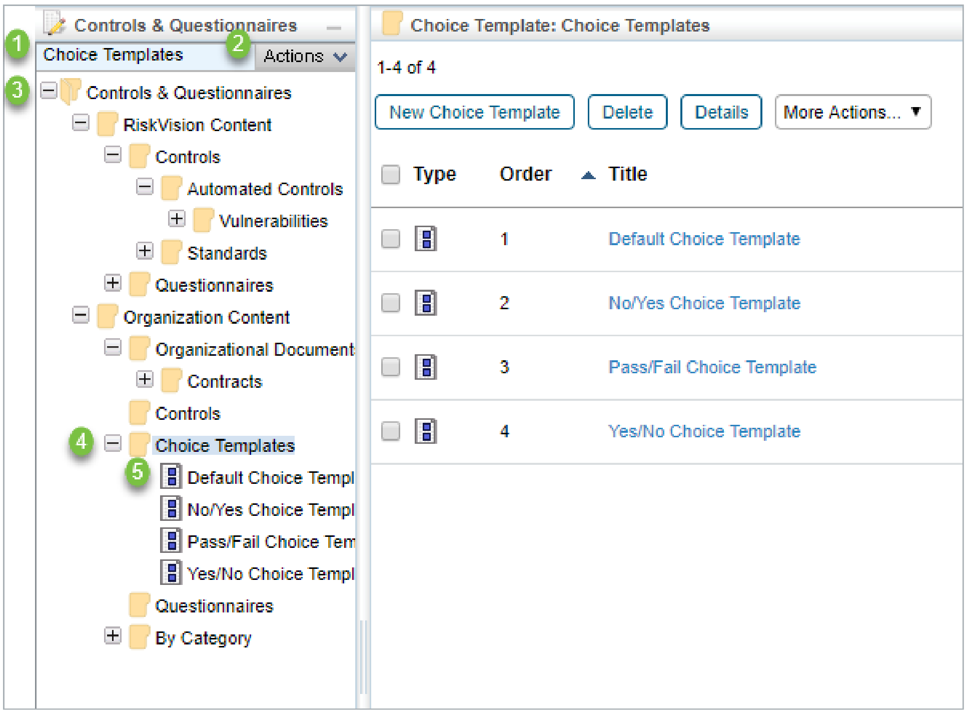
Moving the mouse hover a menu, such as "Home," displays a pull-down submenu of items. You can quickly view a snapshot of the available pages by moving the mouse over each menu.

Clicking the menu selects it and displays as many submenu items as possible under the menus. If your browser window is narrow, there may be more submenu items under the menu than what appears.

Using the Tree and Grid View

Many pages in the RiskVision solution display a hierarchical tree on the left and a tabular grid on the right side of the screen. The tree and grid function in the familiar way that files and folders are shown in Operating Systems like Microsoft Windows.

For more information about the grid side of the tree and grid view, see Using the Grid View.



□	Type	Order	▲ Title
□		1	Default Choice Template
□		2	No/Yes Choice Template
□		3	Pass/Fail Choice Template
□		4	Yes/No Choice Template

The Tree and Grid view.

1. Selected node
2. Actions pulldown
3. Root node
4. Folder
5. Object

To adjust the width of the tree view, click the splitter, the vertical bar between the panes, and drag it to right or left. To hide the entire tree view, move the splitter all the way to the left, or click the minimize button at the top of the tree pane. To view the tree again after it has been minimized, click the splitter—parked on the left edge of the window—and drag it to the right.

Clicking on an item in the tree pane will display its name in the **Selected Node** window. Clicking the **Actions** will bring up a list of actions that can be performed on the selected item, such as refreshing, copying, or deleting it. The contents of the tree pane vary considerably. Some pages use the tree to differentiate read-only content from read-write Organization content, for example. Some trees group the objects you own--My Dashboards, for instance--separately from shared objects and archived objects.

Certain trees include objects. When you click on an object in the tree, the detail pane for that object replaces the grid pane. In other cases, the tree only includes folders. Clicking on a folder or a dynamic group usually displays the objects it contains in the grid pane.

Selecting different nodes of the tree have different effects:

Target	Description
Root / Initial view	May display a grid view showing all objects, or may display a landing page (such as Analytics> Dashboards). The initial view is usually similar to selecting the root of the tree. Selecting the root of the Entities tree is special: it displays a details view for all entities, summarizing the set and providing a convenient place for manually creating an Entity.
Folder	The contents of the folder appear in the grid.

Target	Description
Object	The details view for the selected object replaces the grid view.

Certain root or initial view pages include action buttons, such as the **Import Content (XML)** button on the **Content** > **Controls and Questionnaires** page the **Import Policies (XML)** button on the **Content**> **Policies** page.

Using the Grid View

The grid view is used throughout the RiskVision solution to display a table of objects (users, programs, connectors, and so on) and their attributes. Each row in the table represents an object, and the columns reflect some of the object's attributes. In some cases, you can customize the columns and how they display particular attributes.

Sorting the Table

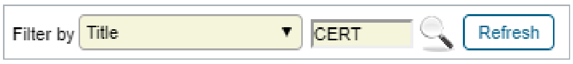
To sort the table by any visible attribute, click that attribute's column heading. To reverse the sort (ascending order instead of descending), click the column heading again. To make a hidden attribute visible, see Customizing the Columns in the following sections.

Refresh

The table represents a snapshot of the underlying data at the time it was first displayed. Some data, such as Charts in Progress, are more dynamic, but all objects can change over time. To update the display with the latest data, click the **Refresh** button.

Limiting the Number of Rows

The grid view may show all objects of a particular kind, such as Ownership Types, or it may show only the contents of the selected dynamic group.



Filtering the grid.

Enable Focus

To focus on objects of interest:

1. Click the **Filter by** dropdown and select an object attribute.
2. Enter a value. Press **Enter**. For text attributes, the value is a case-insensitive, "begins with" query.

To remove the filter and show all rows, select **Show all** from the filter pull down list, or clear the value and hit **Enter**.

Enable Grids

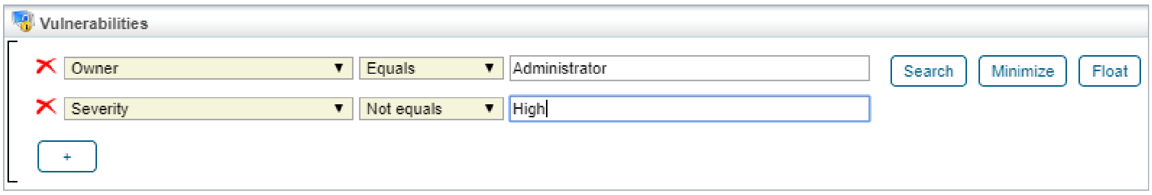
Certain grids, such as Entities, Vendors, and all grids on the Vulnerabilities menu, contain the Advanced Filter to help you locate the objects using one or more advanced search conditions.

To enable the advance search feature in a grid:

1. Select **Advanced Filter** in the **Filter by** dropdown list or click the 🔍 icon next to the **Filter by** drop-down list. You can also click **Float** to perform a search in the **Search** dialog.
2. **Optional**: Click **+** to add more search conditions. You can add a maximum of six conditions. Depending on the field selected, comparison operators and search input varies, and appears in their respective dropdown lists. The search value must be either entered in the text box or selected from the dropdown list.

   Example: To search computer entities owned by a user named Administrator:

   1. Select **Primary Owner** in the first dropdown list.
   2. Select **Equals** in the second drop-down list.
   3. Select **Administrator** in the third drop-down list.
   4. Select '**Type**' '**Equals**' '**Computer**,' and click **Search**.
   5. **Optional**: If you're performing a search in the Search dialog, click **OK** after the selecting the search conditions. The results matching the search conditions are displayed in the grid.

      Owner | Equals | Administrator

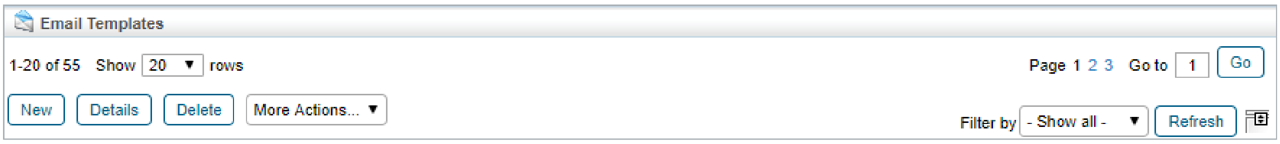
      Severity | Not equals | High

      The Advanced Search filter.

   6. Click **Minimize**.
   7. **Optional**: To re-expand the **Advanced Filter**, click 🔍 .

Pagination

Large numbers of rows are shown in pages at a time. When the grid view is not displaying all rows of a table, the following pagination controls appear.

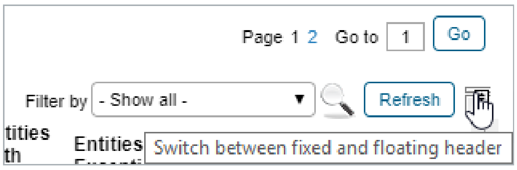


RiskVision's pagination controls.

The controls on the left adjust how many rows are displayed per page (between a minimum of 5 and a maximum of 500). The controls on the right allow for page navigation. The currently selected page is displayed in the text box. To navigate to another page, click the desired page number or the right and left arrow keys (for more than 5 pages). If the desired page number is not visible, type the number into the text box and click **Go** to navigate to that page.

Changing the Grid Header Mode

A RiskVision object grid can have various numbers of rows on any page. When you scroll down to view objects in the grid, the grid header row moves with the other rows, which may make it difficult to interpret the data correctly.



The Grid Header Mode icon.

Click the icon next to the **Refresh** button to prevent the header row from moving.

Actions

Grid views often have buttons such as New, Details, or Delete. The appearance of these buttons depends on the context, the current application, and your user privileges. If you are allowed to create objects here, for example, the **New** button will be shown. To delete one or more objects, check the box to select the rows to remove and click **Delete**.

More Actions... pull down list offers other, context-specific actions, such as import, export, copy to, or move to. Actions such as**Import** are general, but most actions require selecting one or more rows. In the **Home** > **Questionnaires** view, each row has an **Actions** pull-down.

Details

Displaying and updating the attributes of a single object requires showing the object's details which can be accomplished in several ways. From the grid view, check the box to select the desired object and then click **Details**. In some cases, the **Details** action is found in the **More Actions...** pull-down list. In many grid views, the object's name or title is a link that serves as a shortcut to the details.

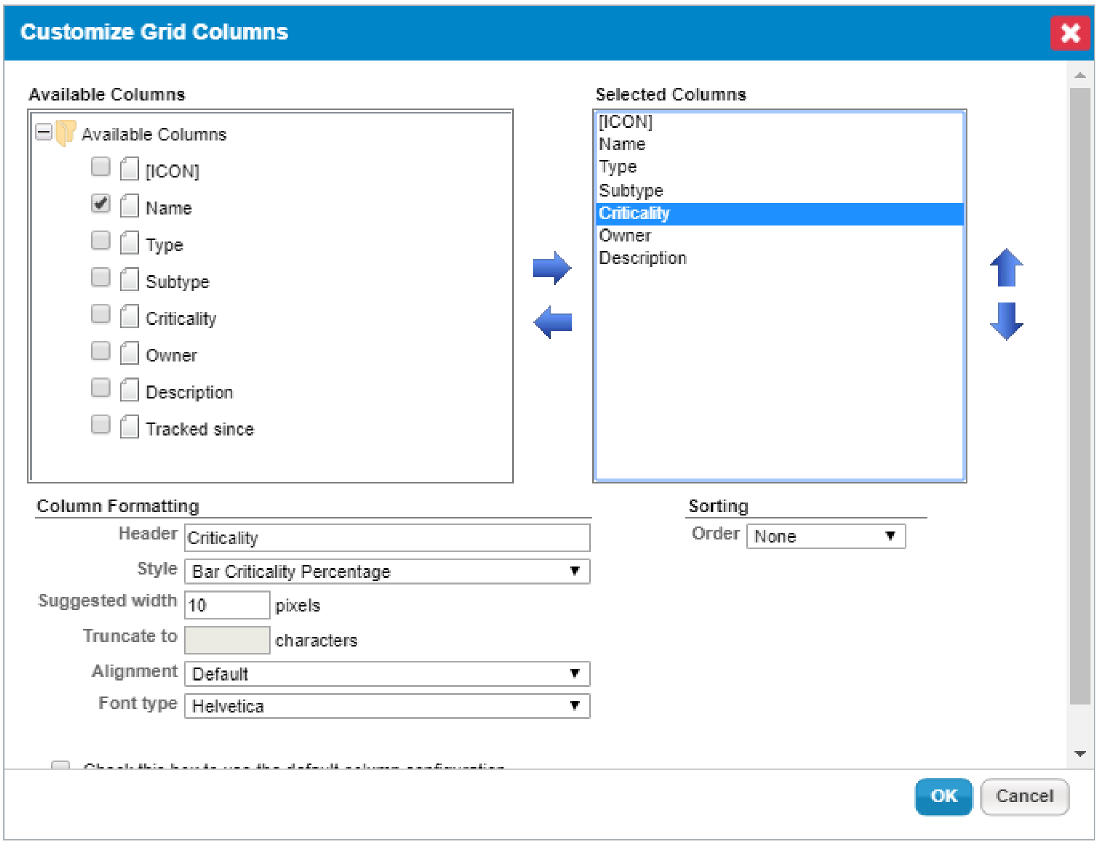
Some kinds of objects do not have details. Some, such as the **Home** > **Questionnaires** view, have links to more than one kind of object (in this case, entities and questionnaires). Details can be displayed in the lower half of the grid view in a popup window, or the details view can replace the entire grid view. Click **Back** to return to the grid view from the details view.

Customize the Columns

In most grid views, you can specify exactly which attributes must be displayed as columns in a given grid view, and you can choose whether attributes must be shown graphically or as text or other options.

To customize the columns:

1. Open the **More Actions...** dropdown list.
2. Click **Customize**.



Customize Grid Columns

Available Columns

- Available Columns
  - □ [ICON]
  - ☑ Name
  - □ Type
  - □ Subtype
  - □ Criticality
  - □ Owner
  - □ Description
  - □ Tracked since

Selected Columns

- [ICON]
- Name
- Type
- Subtype
- Criticality
- Owner
- Description

Column Formatting

Header: Criticality
Style: Bar Criticality Percentage
Suggested width: 10 pixels
Truncate to: characters
Alignment: Default
Font type: Helvetica

Sorting

Order: None

□ Check this box to use the default column configuration

The Customize Grid Columns dialogue.

In the **Customize Grid Columns** dialogue, the object attributes that can be used as grid columns are listed in the **Available Columns** box. The current columns are listed in display order in the **Selected Columns** list.

3. **Optional**:
   a. Add a column to the **Selected Columns** list:
      i. Check the box next to a column in the **Available Columns** list.
      ii. Click the right arrow pointing from the **Available Columns** to the **Selected Columns** list.
   b. Remove a column from the **Selected Columns** list:
      i. Select a column in the **Selected Columns** list by clicking on it.
      ii. Click the left arrow that points from the **Selected Columns** back to the **Available Columns** list.
   c. Specify the format details of a column:
      i. Click a column name to select it in the **Selected Columns** list.
      ii. **Optional**: Edit the **Format > Header** field to change the column name.
      iii. **Optional**: Click the up or down arrow to change the order.

Customizing Grid Columns has no effect on the underlying data.

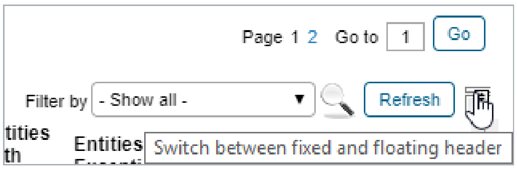
Common Features

A number of common features can be seen in many objects, throughout the RiskVision application. Here is a list of common features you must know before you begin to learn the features in RiskVision application:

- User Settings
- Delegation
- Advanced Searching
- Documents
- Applications
- Rich Text Editor
- Actions
- Visualization

Changing the Grid Header Mode

A RiskVision object grid can have various numbers of rows on any page. When you scroll down to view objects in the grid, the grid header row moves with the other rows, which may make it difficult to interpret the data correctly.



The Grid Header Mode icon.

Click the icon next to the **Refresh** button to prevent the header row from moving.

Advanced Searching

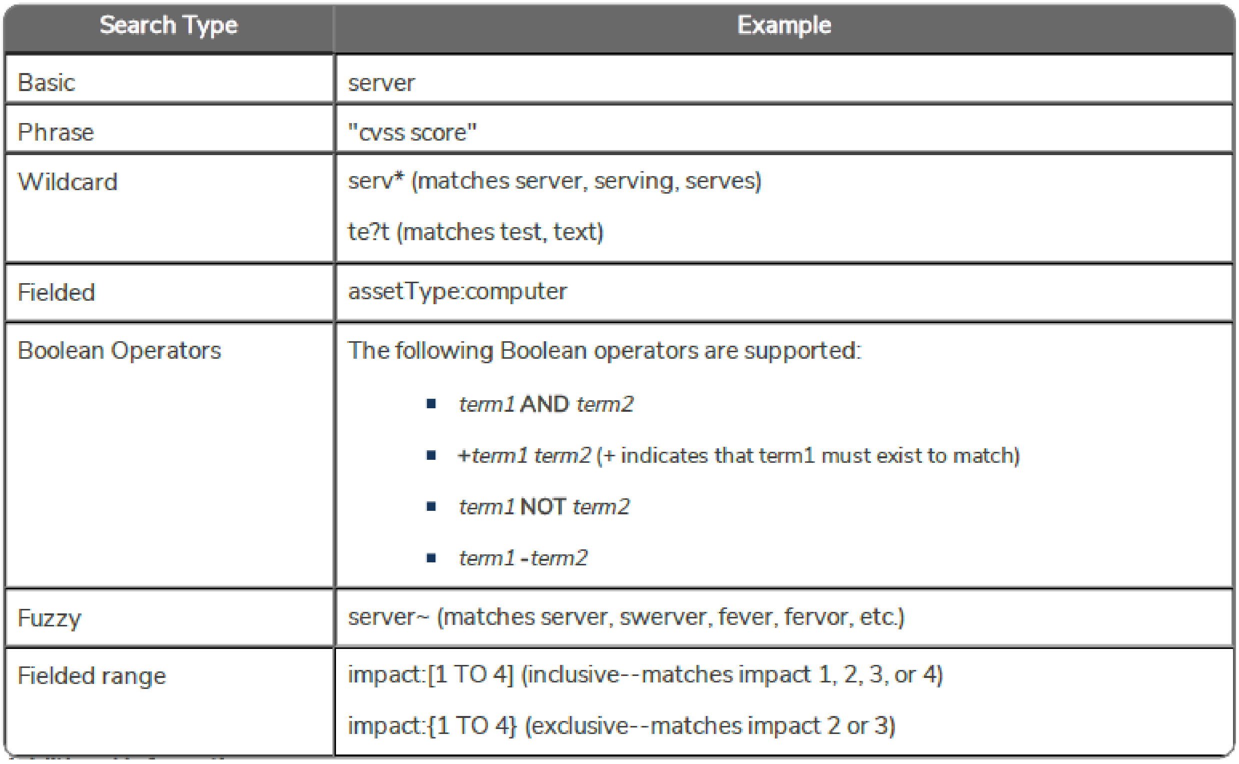
The search box can be used to search for simple terms as well as for more structured queries. This section describes the syntax for advanced queries.

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: ■ *term1* AND *term2* ■ +*term1 term2* (+ indicates that term1 must exist to match) ■ *term1* NOT *term2* ■ *term1* -*term2*
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.

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
- attachements.name [Note misspelling]
- attachements.pathId [Note misspelling]
- attachements.url [Note misspelling]
- attachements.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
- attachements.name [Note misspelling]
- attachements.pathId [Note misspelling]
- attachements.url [Note misspelling]
- attachements.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

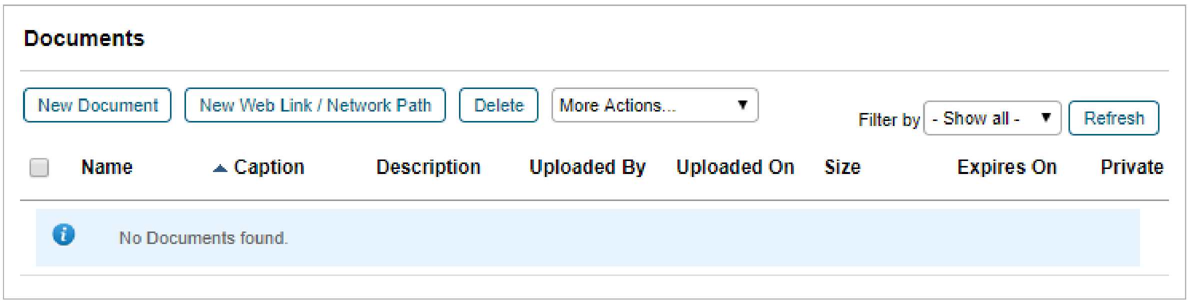
Vendor ID

Kind of Asset/Entity; adds:

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

Documents

The **Documents** tab allows you to attach entity-related documents, such as service contracts. You can attach documents from your local system or document repository, or provide a web link or network link to external information as a reference. The **Documents** tab can be found in the details page of an object, such as an entity, entity collection, program, or control. Note that shared documents cannot be added to all objects.



Documents

☐	Name	▲ Caption	Description	Uploaded By	Uploaded On	Size	Expires On	Private

No Documents found.

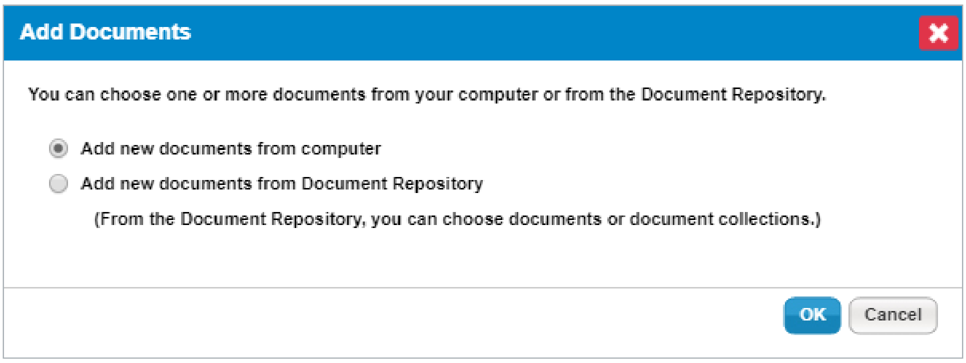
The Documents window.

Other resources allow the attachment of documents in order to document findings, tickets, exception requests, and for other needs. For example, the **Findings** option supports attaching documents in the context of a questionnaire.

To attach a document:

1. Select an object to open its details page, then click the **Documents** tab.

2. Click **New Document**. Select one of the following options:



Add Documents

You can choose one or more documents from your computer or from the Document Repository.

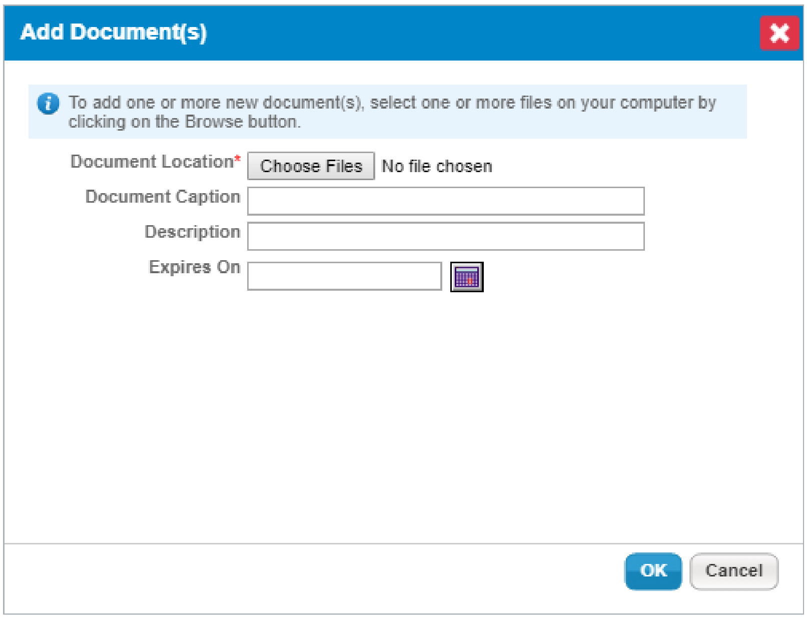
● Add new documents from computer

○ Add new documents from Document Repository

(From the Document Repository, you can choose documents or document collections.)

The Add Documents window.

- **Add new document from Computer**.
  - Click **OK**.
  - Fill out all fields, including **Document Caption**, **Description**, and **Expires On**.



Add Document(s)

To add one or more new document(s), select one or more files on your computer by clicking on the Browse button.

Document Location* Choose Files No file chosen

Document Caption

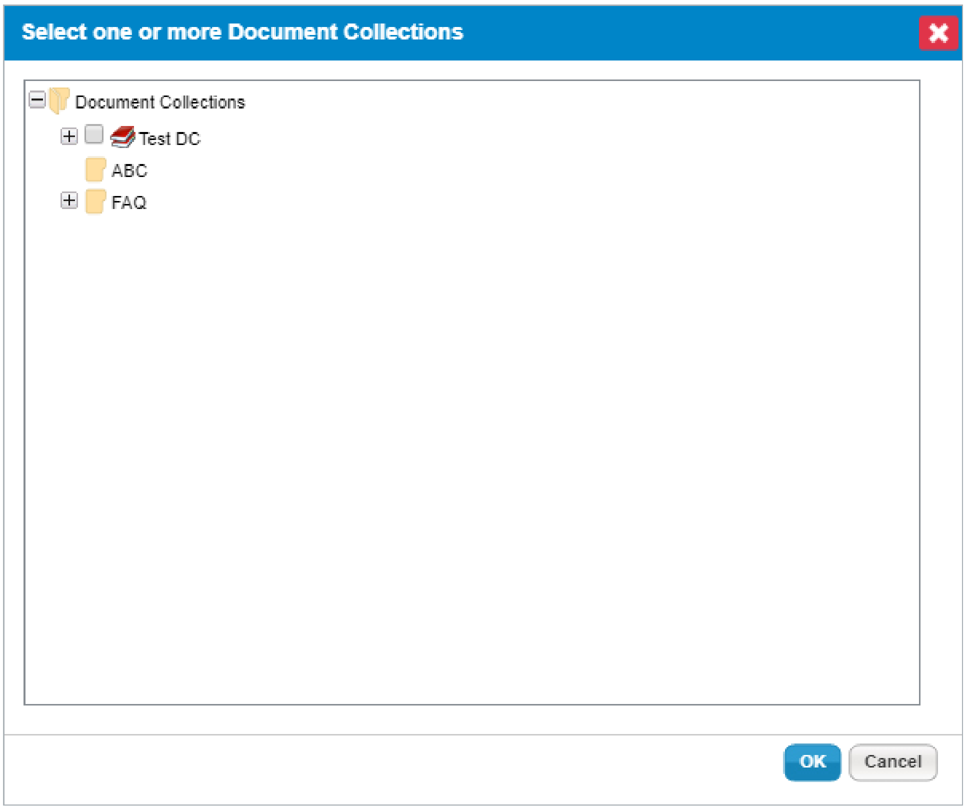
Description

Expires On

The Add new documents from computer window.

- Click **OK**.

- **Add new document from Document Repository**.
  - Click **OK**.
  - Select the required document collection.



Select one or more Document Collections

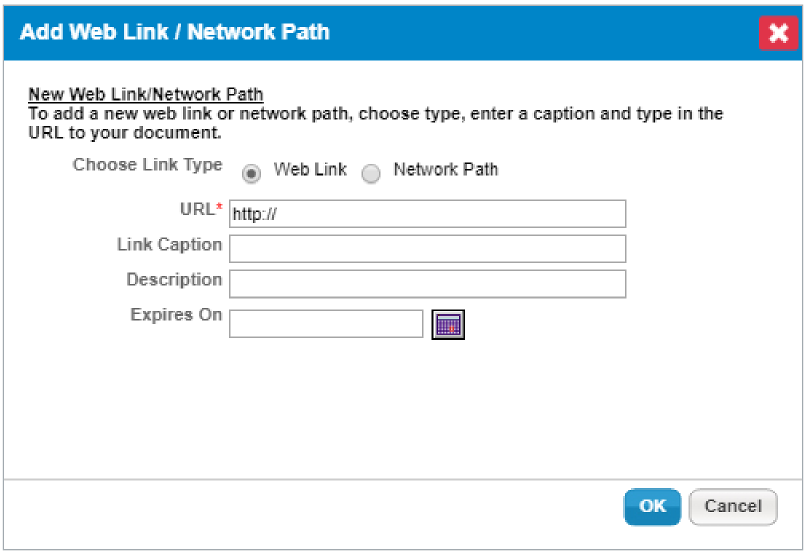
The Add new documents from Document Repository window.

  - Click **OK**.

To attach a web link or network path:

1. Select an object, then click the **Documents** tab.

2. Click **New Web Link/Network Path**.



Add Web Link / Network Path

New Web Link/Network Path

To add a new web link or network path, choose type, enter a caption and type in the URL to your document.

Choose Link Type ● Web Link ○ Network Path

URL* http://

Link Caption

Description

Expires On

The Add Web Link/Network Path window.

3. Click the **URL** field and type the complete URL or Network Path.
4. **Optional**: Enter a **Link Caption** and **Description**, and click the calendar icon to set the **Expires On** field.
5. Click **OK**.

To delete a document, web link or network path:

1. Select an object, then click the **Documents** tab, or go to the user interface area where documents are located.
2. Check the box next to document(s) and web link(s) you want to delete.
3. Click **Delete**.
4. Click **OK**.

The UNC path will display in all browsers but is only be clickable in Internet Explorer because other browsers block direct connection to the UNC path for security reasons. If you're using another browser you will need to manually navigate to the appropriate location on the external file system.

Controlling Object Visibility

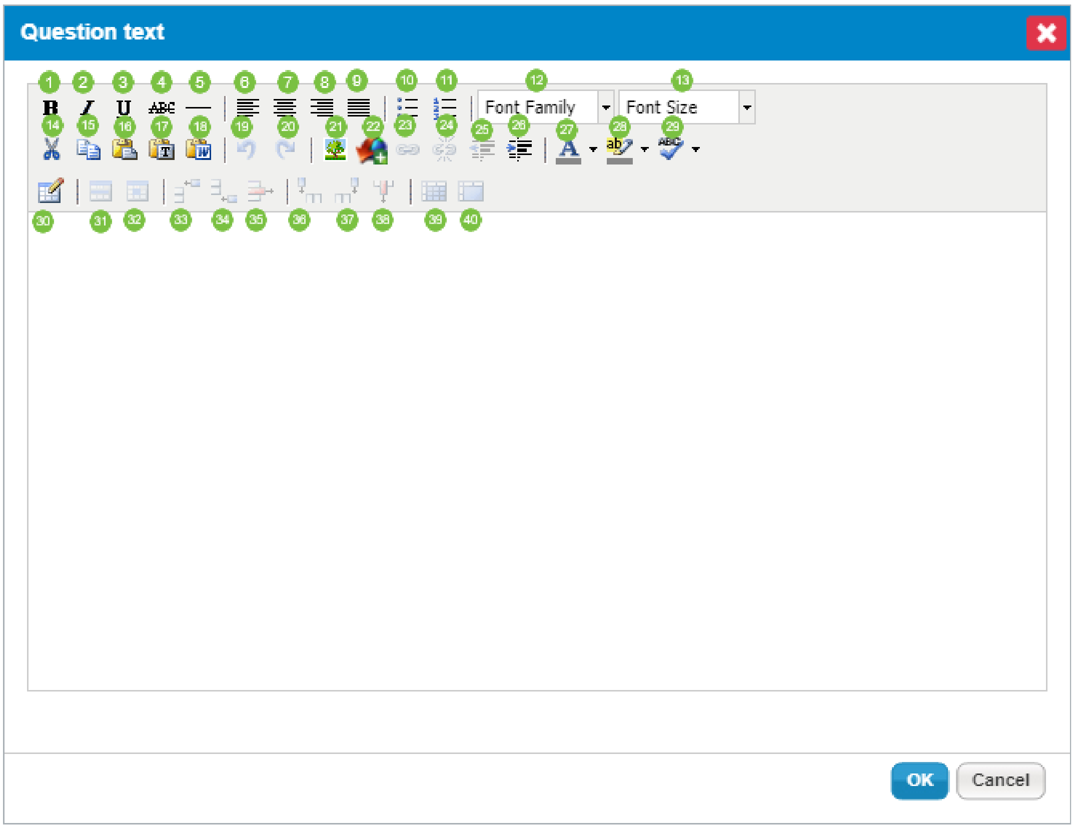
Many default and user-defined objects contain the**Applications** tab in their details page to help you control the visibility of an object in the RiskVision applications. Though you possess sufficient permissions to access the application and the menu item, the object will not be visible to you if the application is not selected in the details page of that object.

To control an object's visibility:

1. In the RiskVision application, select the object containing the **Applications** tab.
2. Click the **Applications** tab.
3. Click **Edit** and select boxes next to application(s).
4. Click **Save**. The object is now visible in the application(s) you have selected in the previous step.

Using Rich Text Editor

The Rich Text editor is similar to word processing applications in that it allows users to enter text, and contains options to format the text with options, such as bold, align, indent, lists, font color, font size, text highlight, and more. The Rich Text editor is found throughout RiskVision in locations where more than simple text entry is required, such as when explaining an answer choice in a questionnaire, and when drafting a questionnaire, content pack or policy. Typically, the Rich Text editor is available for use in the fields of objects that show the **Click to enter text** informational message. When working with the Rich Text editor, you will notice that not all of the options appear for each field. For example, the table options mainly appear only in fields of the questionnaire object.



The Rich Text editor.

The following options are available in the Rich Text editor:

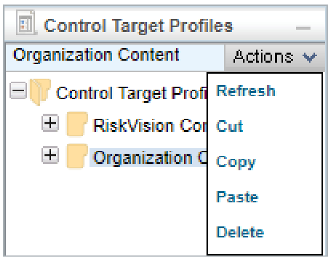
OPTION	DESCRIPTION
1	Makes the selected text bold. Use Ctrl + B as short-cut key.
2	Makes the selected text italic. Use Ctrl + I as short-cut key.
3	Underlines the selected text. Use Ctrl + U as short-cut key.
4	Draws a line through middle of the selected text.
5	Draws a horizontal line at the cursor position.
6	Aligns the text to the left.
7	Aligns the text to the center.
8	Aligns the text to the right.

9	Justifies the left and right alignments.
10	Makes the text a bulleted list.
11	Makes the text a numbered list.
12	Choose the font family for the selected text.
13	Choose the font size for the selected text.
14	Cut the selected text. Use Ctrl + X as short-cut key.
15	Copy the selected text. Use Ctrl + B as short-cut key.
16	Paste the text that is cut or copied. Use Ctrl + V as short-cut key.
17	Paste the text without any formatting.
18	Paste the text which is copied in the Microsoft Word application.
19	Revert the changes. Use Ctrl + Z as short-cut key.
20	Reverse undo changes. Use Ctrl + Y as short-cut key.
21	Insert or edit an image. Allows modification of image properties, such as dimension, space, border, and more.
22	Allows uploading of image from your computer.
23	Allows embedding the link to the selected text.
24	Allows to deactivate working links.
25	Adds space between the margin and the beginning of the text on a line.
26	Removes space in the indented line.
27	Allows choosing the text color.
28	Highlights the selected text.
29	Checks the spelling and grammar of the text.
30	Inserts a table in the editor. Use the General tab to specify the number of rows and columns, alignment, padding, border, and more. Use the Advanced tab to set the advanced properties.
31	Updates the current, odd, even, or all rows in a table.
32	Updates the current cell, all cells of a row, all cells of a column, or all cells in a table.
33	Inserts a row before the cursor position.

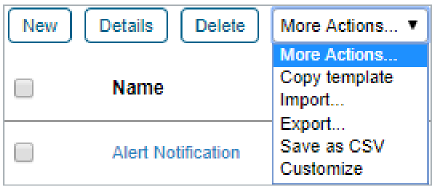
34	Inserts a row after the cursor position.
35	Deletes a row
36	Inserts a column before the cursor position.
37	Inserts a column after the cursor position.
38	Deletes a column.
39	Splits the merged cells.
40	Merges the cells.

Actions

This section covers the most common options available in the **Actions** or **More Actions** drop-down list, seen throughout RiskVision. These drop-down lists are sensitive to the page and the current selection. They can be seen in the tree on the left side of a page, in the center of a page, in the details pane of a page, or at the top-right corner of a page.



The Actions menu.



The More Actions menu.

This article covers how to perform the following actions:

- Refreshing the data;
- Cutting, copying, and pasting;
- Saving the grid as a CSV file; and
- Importing and exporting the data to an XML file.

For information on transitioning bulk findings, tickets, exceptions, or incidents in a workflow, see theBatch Workflow Transitions article.

To refresh the tree view:

1. In the page where a tree view is available, select the folder. The **Actions** menu appears.
2. Click **Actions** and select **Refresh**. The tree is updated.

To cut the selection:

1. In the page where a tree view is available, expand the tree and select the object of interest. The **Actions** menu appears.
2. Click **Actions** and select **Cut**. The object is now ready for paste action.

To copy the selection:

1. In the page where a tree view is available, expand the tree and select the folder of interest. The **Actions** menu appears.
2. Click **Actions** and select **Copy**. The object is copied.

To paste the cut or copied action:

1. In the page where a tree view is available, expand the tree and select the folder of interest. The **Actions** menu appears.
2. Click **Actions** and select **Paste**. The object is pasted.

To delete the selection:

1. In the page where a tree view is available, expand the tree and select the folder of interest. The **Actions** menu appears.
2. Click **Actions** and select **Delete**. The object is deleted.

To save fewer rows in the grid or the complete grid in CSV format:

1. Open the page of interest in which the **More Actions** drop-down list containing the **Save as CSV** option is available.
2. Do one of the following:
   - To save the complete grid, select **Save as CSV** in the More Actions drop-down list.
   - To save the row(s) in grid, select the row(s) of interest and select **Save as CSV** in the More Actions drop-down list.
3. A dialog appears, displaying the options to open or save the file. Follow the instructions displayed by your browser to save the file.

To import a file in XML format:

1. Open the page of interest in which the More Actions drop-down list containing the **Import** option is available.
2. Select **Import** in the More Actions drop-down list. An import dialog sensitive to the object type appears. For example, if you are importing an email template, the **Import Email Templates** dialog will be seen.
3. Click **Browse** to select the file.
4. Click **OK** on the dialog after the file is selected. The dialog is exited and the object(s) is imported.

To export the object(s) or the complete grid in XML format:

1. Open the page of interest in which the More Actions drop-down list containing the **Export** option is available.
2. Do one of the following:
   - Select **Export** in the More Actions drop-down list to export the complete grid.
   - Select the row(s) of interest and select **Export** in the More Actions drop-down list to export the row(s) in grid.
3. A dialog appears, displaying the options to open or save the file. Follow the instructions displayed by your browser to save the file.

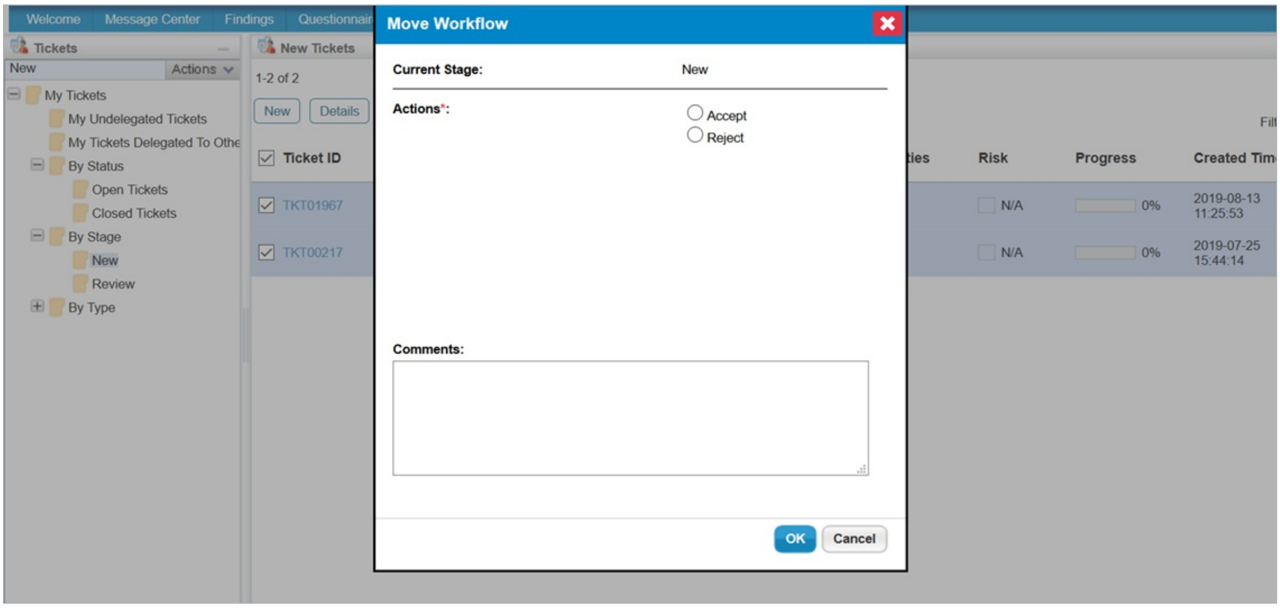
Batch Workflow Transitions

The **Batch Workflow Transition** action makes it possible for users to move multiple objects to another workflow state in bulk. Once objects have successfully transitioned, entries are recorded in each object's **Workflow History**, but a single entry is logged for each bulk-transition on the **Events** page in **Administration**. Depending on the application you're currently working in, these objects include:

- Findings;
- Tickets;
- Exceptions Requests; and
- Incidents.

When using this action, note that:

- Up to 50 objects can be bulk-transitioned at one time.
- Only objects in the same stage from the same workflow can be transitioned in bulk, which are grouped and selected in the **By Stage** folder and its sub-folders. If needed, the workflow settings can be modified in **Configuration > Workflows.**
- If one or more objects cannot be transitioned due to an error, the transition will fail.
- Bulk transitions cannot be performed on closed or terminal objects. Reopening objects in bulk is not supported.
- Only users with **View** and **Update** permissions on the objects can perform this action.



Current Stage: New

Actions*: ○ Accept ○ Reject

Comments:

The Move Workflow window, which allows you to transition multiple objects at once.

Batch workflow transitioning supports the use of the Groovy programming language. If you wish to use Groovy for bulk-transitioning workflows, contact Resolver Support.

In order to support batch workflow transitioning, users upgrading to RiskVision version 9.3 or higher must include the following method signature in the **DetailPane** Groovy file of the desired object: `public boolean isTransitionActionAllowedForBatch(String transitionAction, String toStage, boolean forceTransition, List payloads)`.

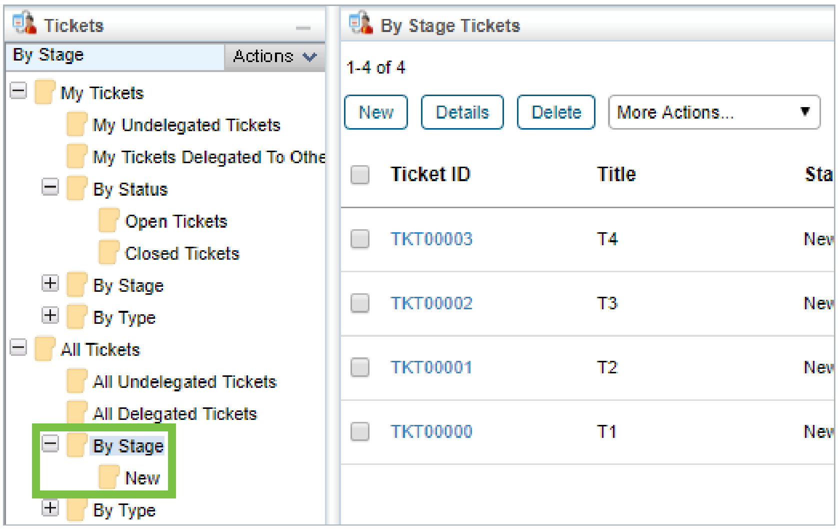
In addition, any Groovy customization files that implement `PayloadScriptAction` must provide implementation for `isTransitionActionAllowedForBatch()` in the **DetailPane** Groovy file.

To bulk-transition objects:

1. Click **Home**, then navigate to the object you wish to perform the action on (i.e., **Findings**, **Tickets**,

Exceptions, or **Incidents**).

2. Click the **+** icon beside the **By Stage** folder in the tree view to display its sub-folders.



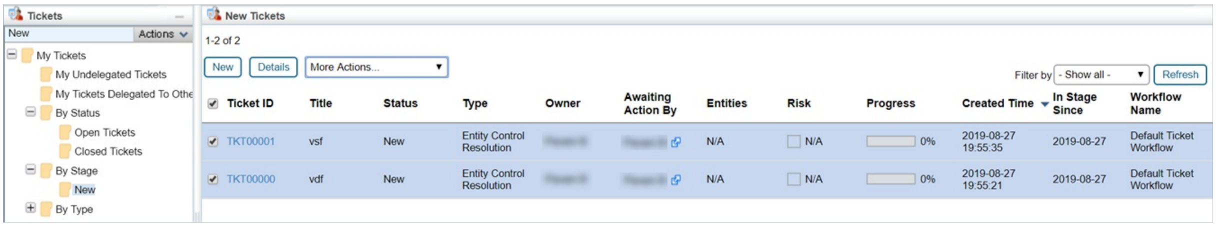
1-4 of 4

□	Ticket ID	Title	Sta
□	TKT00003	T4	New
□	TKT00002	T3	New
□	TKT00001	T2	New
□	TKT00000	T1	New

The By Stage folder in the tree view.

3. Click a sub-folder under **By Stage** to display objects in the grid based on their current stage.

4. Select the checkboxes beside the appropriate objects or select the checkbox in the far-left of the grid's header to select all objects.



1-2 of 2

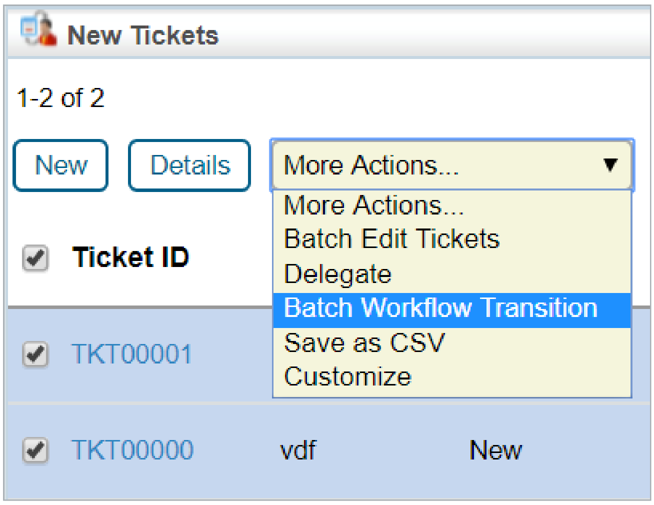
☑	Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since	Workflow Name
☑	TKT00001	vsf	New	Entity Control Resolution	[redacted]	[redacted]	N/A	□ N/A	0%	2019-08-27 19:55:35	2019-08-27	Default Ticket Workflow
☑	TKT00000	vdf	New	Entity Control Resolution	[redacted]	[redacted]	N/A	□ N/A	0%	2019-08-27 19:55:21	2019-08-27	Default Ticket Workflow

Selected objects in the New sub-folder.

> When selecting objects in bulk, review the**Workflow Name** column on the far-right of the grid to ensure all objects belong to the same workflow definition. If a workflow's name was recently modified, the workflow must be synchronized before it will display its current name in the column.

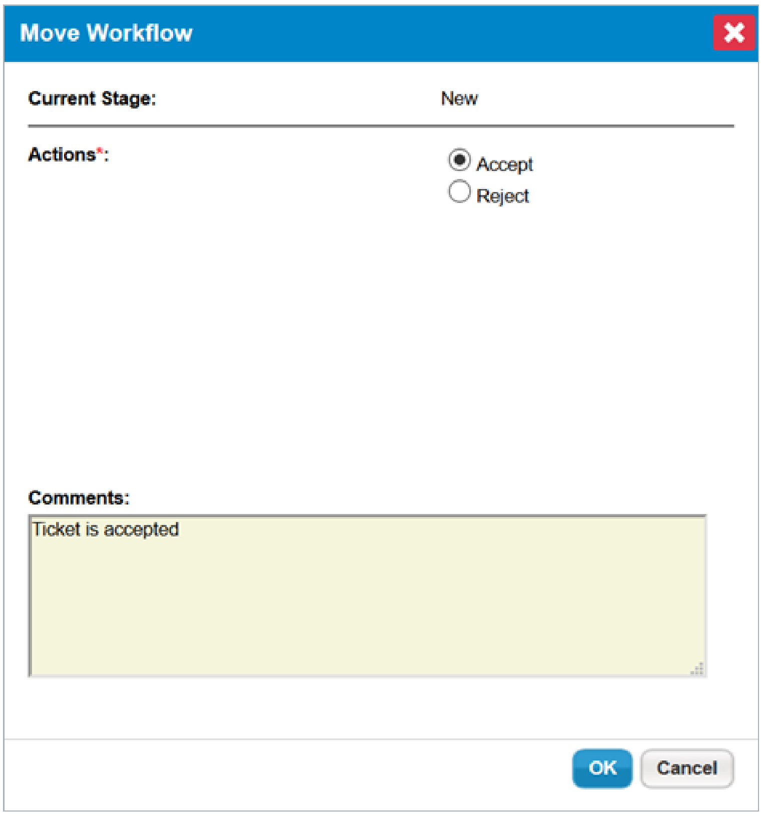
> A maximum of 50 objects can be selected for a single bulk transition. Closed objects cannot be selected.

5. Click the **More Actions...** dropdown menu, then click **Batch Workflow Transition** to display the **Move Workflow** window.



The Batch Workflow Transition option in the More Actions... dropdown menu.

6. Select an option in the **Actions** section to transition the objects to another state.
7. Enter any notes in the **Comments** text box as required.



Current Stage: New

Actions*: ● Accept ○ Reject

Comments: Ticket is accepted

The Move Workflow window.

8. Click **OK** to complete the transition and refresh your browser to see your changes.

Visualizing Objects

The primary goal of this section is to provide an overview of visualization and to discuss the tool options available for navigational purposes. For case-specific information about how the RiskVision visualization tool helps understand the pattern with respect to workflows and relationships, please read the sections, Visualizing Relationships and Visualizing Workflows.

RiskVision has integrated a visualization tool in the objects of entities, entity collections, and workflows to help users visualize relationships between entities, entity collections, and workflow stages. This tool has been incorporated as a separate tab on the details page of the respective objects - the Relationships tab for entities and entity collections and the Stages tab for Workflows. A default graphical layout is displayed by clicking on the Relationships tab and then selecting "Relationship Report" for entities and entity collections, it is also displayed by clicking on Stages tab for workflows.

This tool has different layouts that allow you to choose the representation that is easiest to understand for you. In addition, it contains options to zoom and to move around the graph when there are many nodes in a layout.

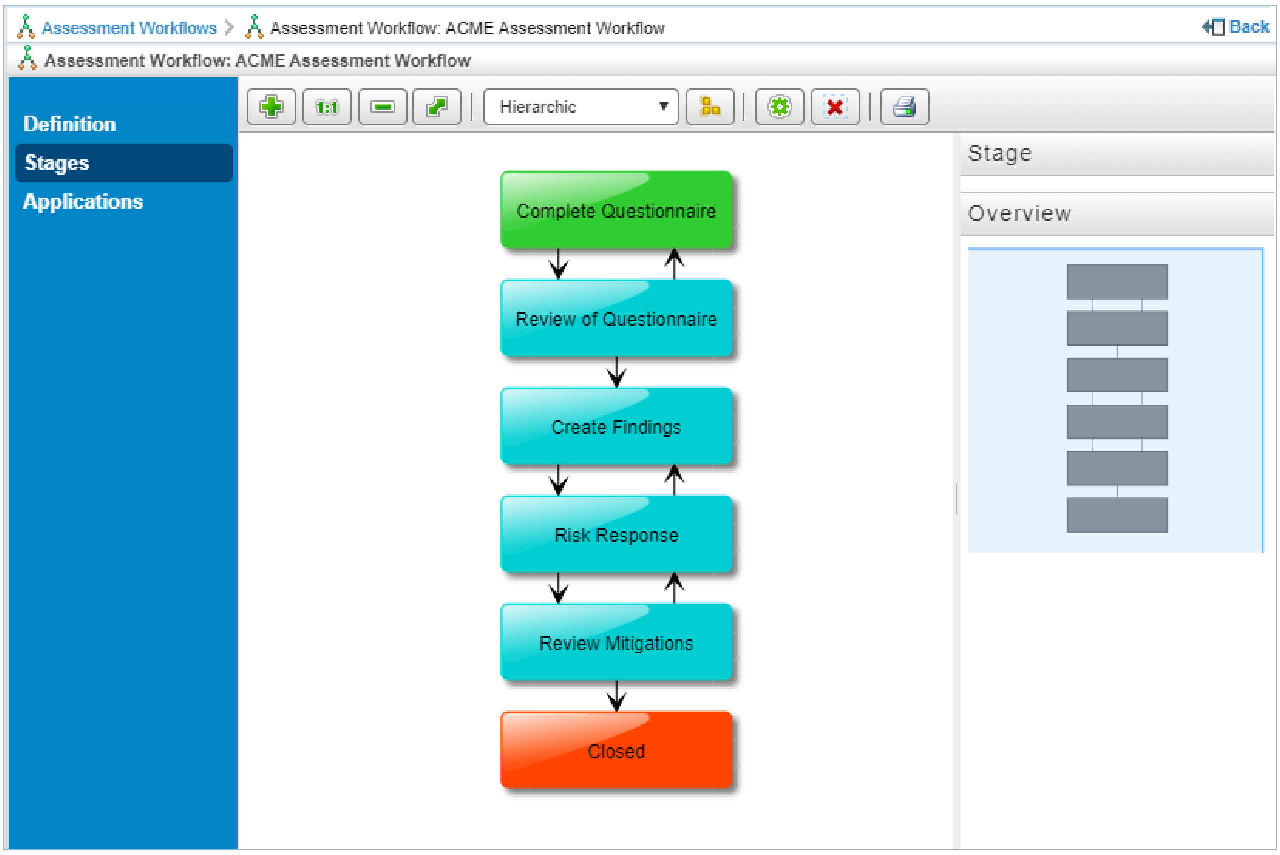
The following tool options are available to enhance your visual experience:

Option	Description
➕	Click to magnify the layout. Continue selecting this icon until you have achieved the desired magnification level.
1:1	Click once to revert the layout to its original size.
➖	Click to reduce the size of the layout. Continue selecting this icon until you have achieved the desired magnification level.
⤢	Click once to make the content fit in the layout.
Selecting layout	Select a desired layout option in the drop-down list at the top of the window.
▦	Click once to revert the layout to its original size and to properly align the layout.
⚙	Click once to show the labels.
✖	Click once to hide the labels.
🖨	Click to open the layout in a new browser tab for printing purposes.
↻	Click to reload the graph with changes you have applied.

For visualizing workflows in RiskVision, you need a web browser with HTML5 support.

Moving the Layout

When a layout contains several nodes, you may want to zoom in on the layout to clearly read the nodes. However, this action limits the number of nodes in views. In order to view the other nodes with same zoom in level, use the **Overview** pane to move the layout.



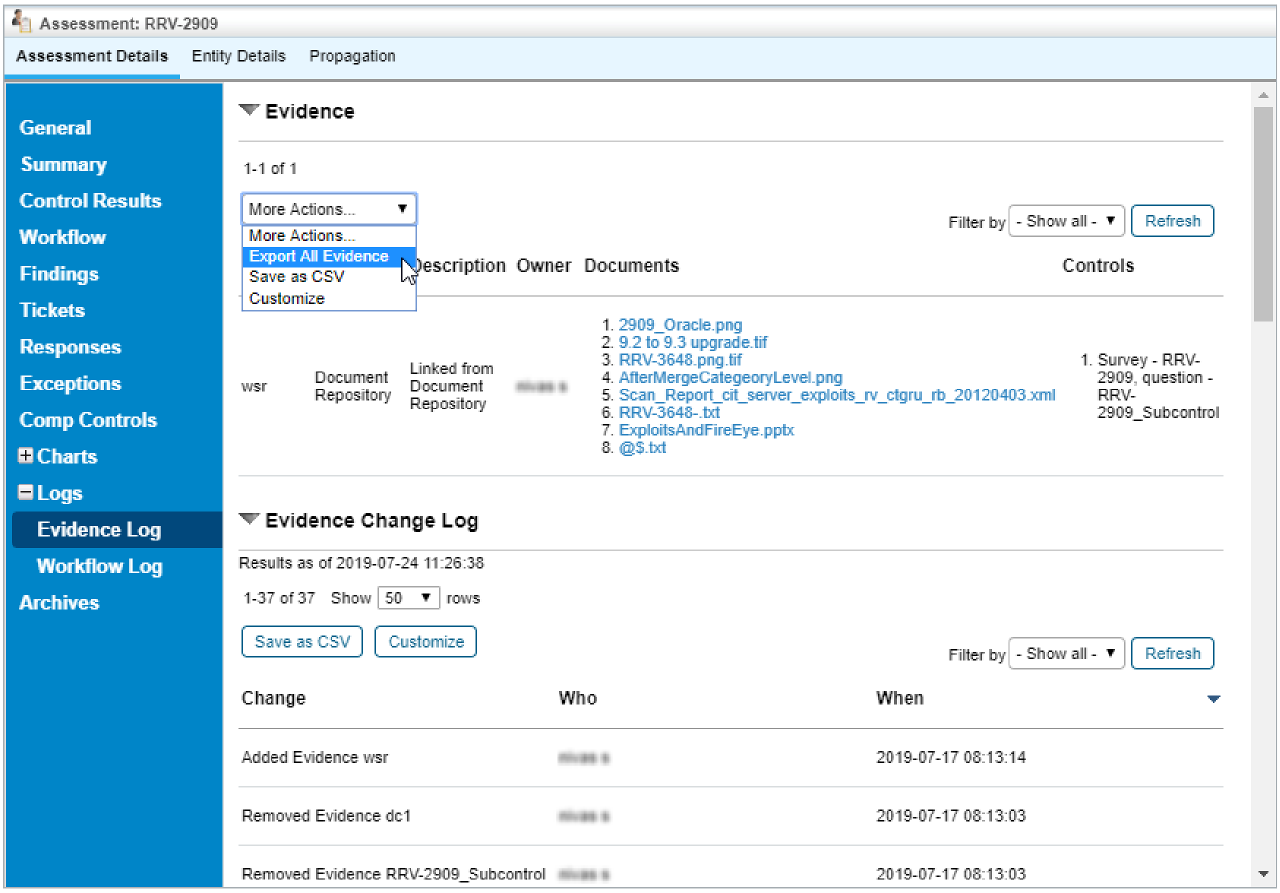
The Workflow Stage layout.

To move the layout:

- In the zoomed layout, move the cursor into the rectangular shaded region of the**Overview** pane at the right-hand side of the window. Hold the left button of the mouse, and move the mouse in the required directions.
- Use the vertical and horizontal scroll-bars around the layout which appears when you expand the layout beyond the best fit.

Bulk Exporting Evidence

RiskVision allows users with the Assessment Manage permission to bulk export evidence from assessments. To perform the bulk export, click**More Actions** > **Export All Evidence**. This option is visible in the **Assessments Details** page > **Evidence Log** tab.



		Description	Owner	Documents	Controls
wsr	Document Repository	Linked from Document Repository	[redacted]	1. 2909_Oracle.png 2. 9.2 to 9.3 upgrade.tif 3. RRV-3648.png.tif 4. AfterMergeCategeoryLevel.png 5. Scan_Report_cit_server_exploits_rv_ctgru_rb_20120403.xml 6. RRV-3648-.txt 7. ExploitsAndFireEye.pptx 8. @$.txt	1. Survey - RRV-2909, question - RRV-2909_Subcontrol

Results as of 2019-07-24 11:26:38

1-37 of 37

Change	Who	When
Added Evidence wsr	[redacted]	2019-07-17 08:13:14
Removed Evidence dc1	[redacted]	2019-07-17 08:13:03
Removed Evidence RRV-2909_Subcontrol	[redacted]	2019-07-17 08:13:03

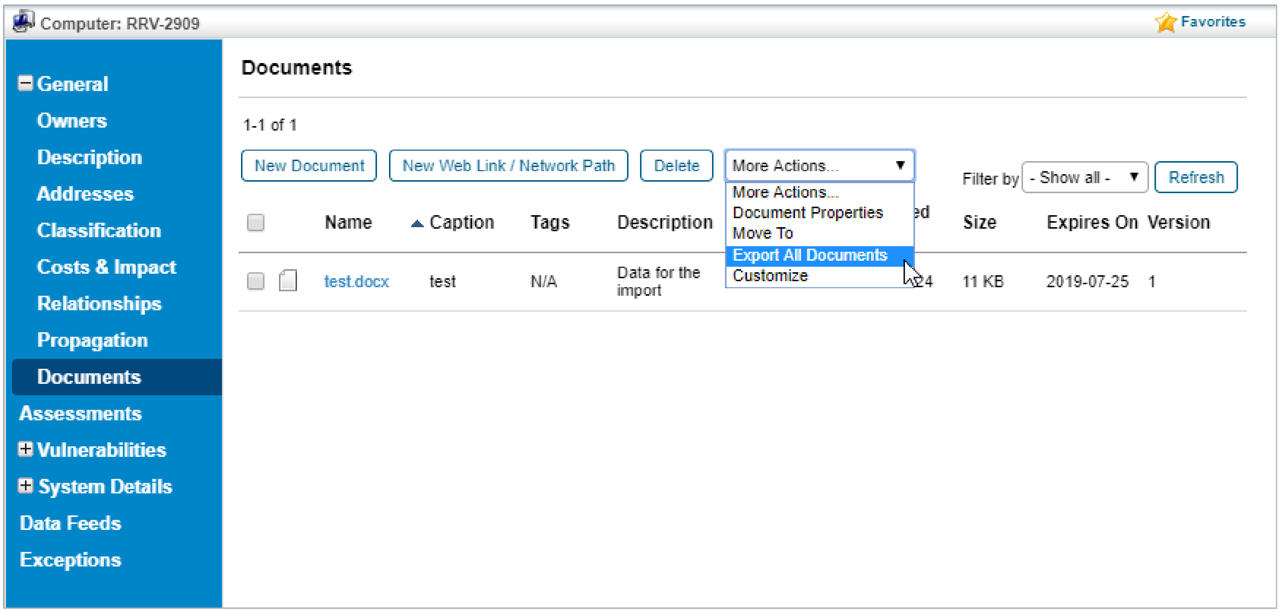
The Evidence Log tab on the Assessment Details page.

When you perform a bulk export of evidence, you will get a single downloaded zip file. For assessments, the zip file name shall be Program - Assessment Name.zip. This zip file will contain multiple folders, one for each question.

If a document is used as evidence for more than one question within that assessment, all the documents are downloaded where user can open and save all the documents.

Bulk Exporting Documents

Users can also export documents attached to entities, findings, and tickets using **More Actions > Export All Documents**. This feature requires object Manage permissions for the object you performing a bulk export from. You can access the bulk export option in the object's **Documents** tab.



Documents

1-1 of 1

□		Name	Caption	Tags	Description	ed	Size	Expires On	Version
□		test.docx	test	N/A	Data for the import	24	11 KB	2019-07-25	1

Accessing the Export All Documents option on an object's Documents tab.

This option is located in a similar position on the Findings and Tickets **Documents** tabs. Bulk exporting of documents results in a single zip file. The name of the zip file depends on the object from which the files have been exported. For entities, the zip file is the entity name, for findings the file name is Finding ID - Finding Name - Entity Name.zip, and for tickets, the file name is Ticket ID - Ticket Name.zip. The Bulk Export Documents feature applies to documents, but not to network paths and web links.

Maximum Zip File Download Size

By default, downloaded zip files for both evidence and documents cannot exceed 200 MB in size.

The maximum file size can be adjusted through the `attachments.export.maxAllowedSize` property. For example, to change the maximum file size to 1 GB, you would set the property as follows: `attachments.export.maxAllowedSize=1024`.

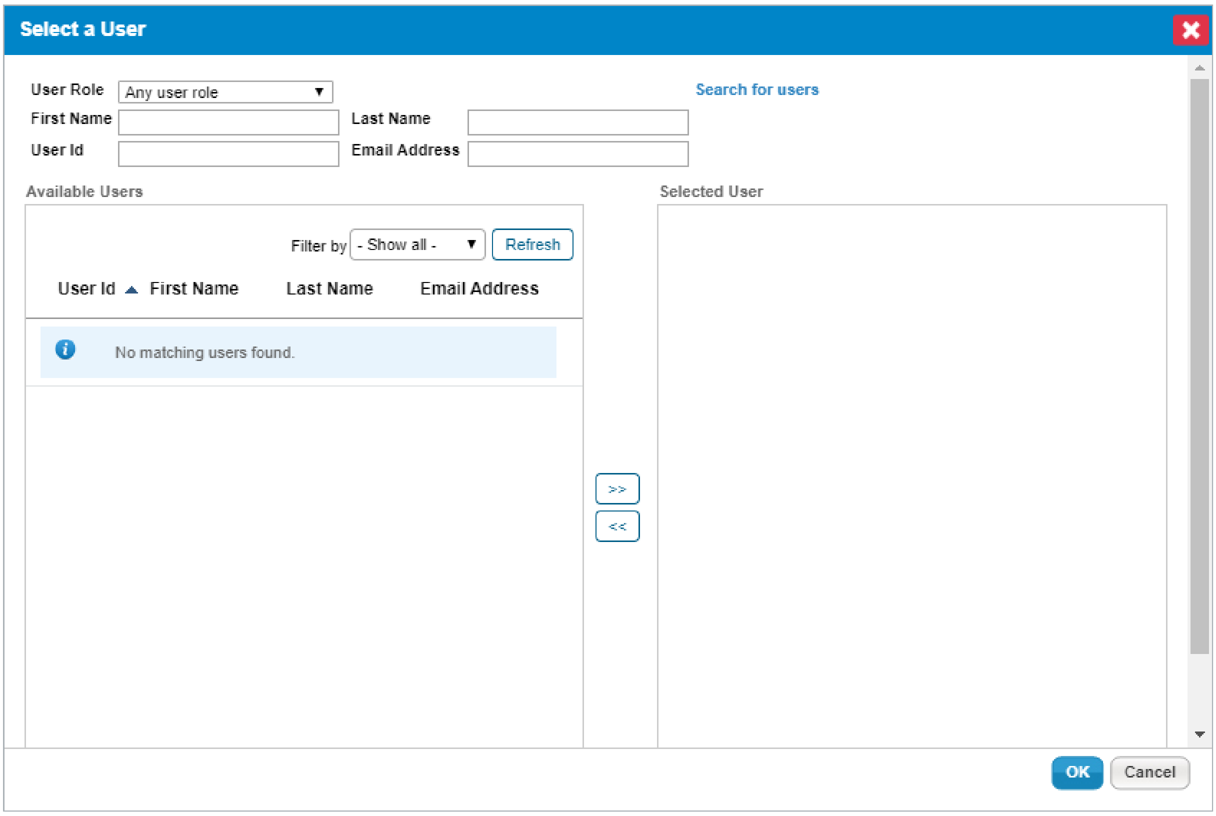
User Picker

You can add users as owners to objects such as entities, tickets, and findings using the **User Picker** window to search for users. This feature allows you to search for users by Source, User Role, First Name, Last Name, User ID, and Email Address. Each search will return a maximum of 200 user records.

The **Source** dropdown menu appears in the **User Picker** window when the `com.agiliance.security.agluserintegration.label=Search External Users` property is enabled, which allows importing users from the Authentication Connector, which connects to your LDAP directories, into RiskVision.

To search for users:

1. Open a page of interest in which the owner or primary owner must be added. Click the + icon to open the**User Picker** window.
2. Pick the appropriate source, if the property is enabled.
3. Enter the search criteria.



No matching users found.

The User Picker window.

4. Click **Search for users**. The result appears in the **Available Users** list.
5. Add a user to the **Selected User** list by selecting the user in the **Available Users** list and clicking the right arrow pointing from the **Available Users** to the **Selected User** list. To remove a user from the **Selected User** list, select it in the **Selected User** list by clicking on it, then click the left arrow that points from the **Selected User** list back to the **Available Users** list.

If the user selected from Authentication Connector does not exist in RiskVision, the new user account is created within the application before assigning them to the object.

Using Search Criteria

1. Search results are filtered using an AND condition between the fields
2. Depending on the Source selected internal users or LDAP users, the use of the wildcard character is different:

   - For Internal Users, the search field supports a single word in which the wildcard of "*" can be used before and/or after the search term. For example: *test* , *test, test * and test

   - For LDAP users search, the search field supports a single word that includes the wildcard of "*" at the beginning and/or end of the search terms as well as anywhere within the search term. For example: *test, test*, tes*t, te*t, and t*est

- Note: If you are not making a wildcard search, your search terms will be exact match terms for each of the terms you are using.

About Welcome Page

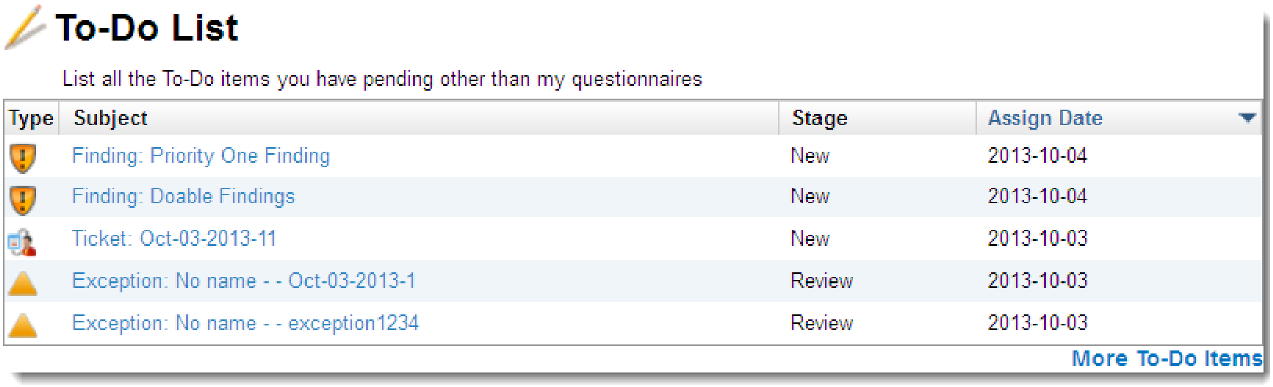
Each RiskVision application has a Welcome page which can be customized for each individual user and their specific roles.

When you first log in, a summary of items assigned to you that you can view and work on or respond to will be displayed. An example of what might be displayed are questionnaires, tickets, exceptions, and notifications. Clicking on any of these items on the Welcome page brings up a navigation pane and detail specific to your selection.

The Welcome page is displayed and the first application is selected when you first log in. The Welcome page contains a number of useful components that change based on the selected application and the privileges assigned to your user account's role.

To-Do List

The **To-Do List** is a component of the Welcome page that displays exception requests, tickets, findings, and other requests for action (except assessments and questionnaires). The items displayed depend on your role, the current status of the system, and the selected application.



To-Do List

List all the To-Do items you have pending other than my questionnaires

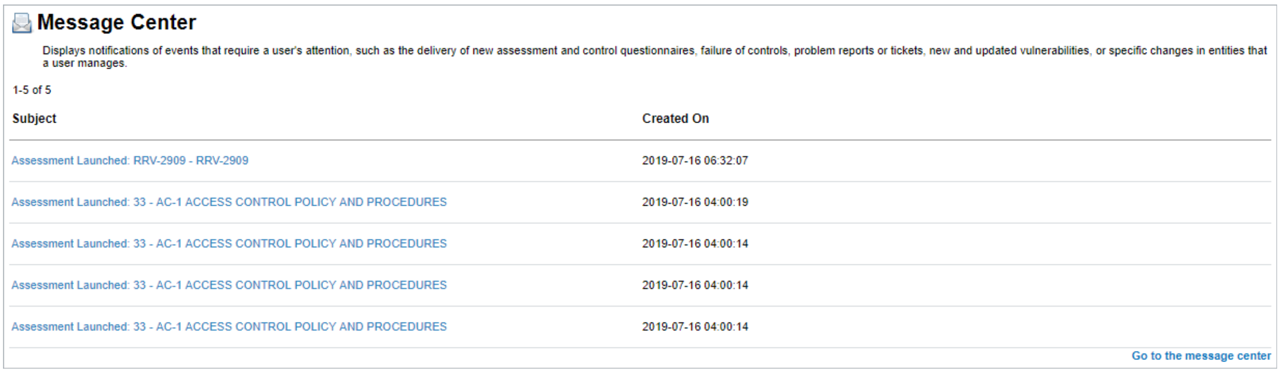
Type	Subject	Stage	Assign Date
🛡	Finding: Priority One Finding	New	2013-10-04
🛡	Finding: Doable Findings	New	2013-10-04
🎫	Ticket: Oct-03-2013-11	New	2013-10-03
▲	Exception: No name - - Oct-03-2013-1	Review	2013-10-03
▲	Exception: No name - - exception1234	Review	2013-10-03

More To-Do Items

Click on an item to see more detail. Click**More To-Do Items** to see all to-do items. As with other grids or tabular displays in RiskVision, click on a column heading to sort by that column.

Message Center

The **Message Center** is a short summary of your most recent notifications, and is displayed on the **Welcome** page.



Message Center

Displays notifications of events that require a user's attention, such as the delivery of new assessment and control questionnaires, failure of controls, problem reports or tickets, new and updated vulnerabilities, or specific changes in entities that a user manages.

1-5 of 5

Subject	Created On
Assessment Launched: RRV-2909 - RRV-2909	2019-07-16 06:32:07
Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	2019-07-16 04:00:19
Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	2019-07-16 04:00:14
Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	2019-07-16 04:00:14
Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	2019-07-16 04:00:14

The Message Center.

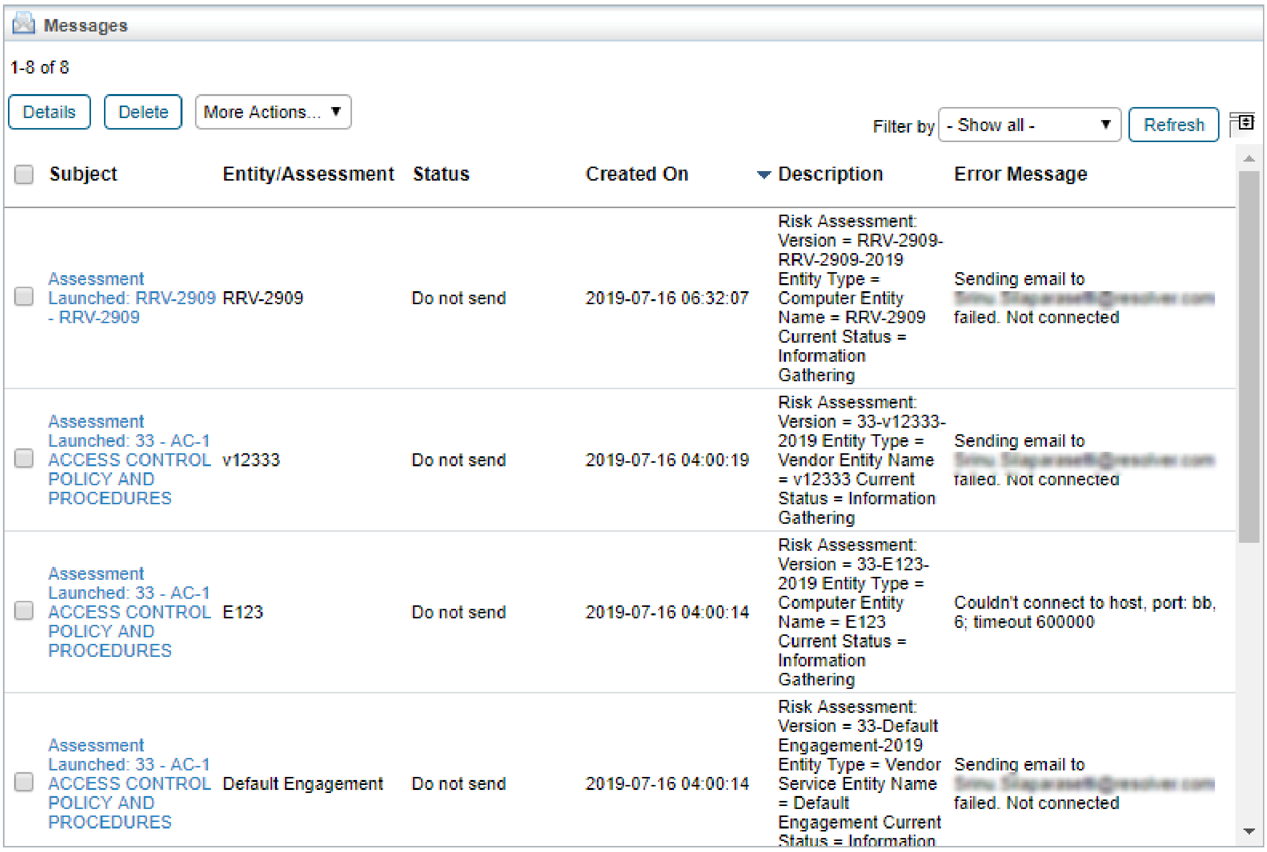
To view a message:

1. Click a message to open the **Alert** window with the message's contents.
2. Click one of the following buttons:
   - **Archive & Close**: Dismiss the window and remove the message from the **Message Center**.
   - **Cancel**: Keep the message in the **Message Center**.
3. **Optional**: To view all messages, click **Go to the message center** or go to **Home** > **Message Center**.

For more information, see Understanding the Message Center.

Understanding the Message Center

The **Message Center** is a page that displays notifications, such as an alert that a workflow has advanced to the next stage. The notifications in the **Message Center** page are always relevant, because of certain criteria. For example, the system only sends alerts to the stakeholders of a particular workflow stage.



□	Subject	Entity/Assessment	Status	Created On	▾ Description	Error Message
□	Assessment Launched: RRV-2909 - RRV-2909	RRV-2909	Do not send	2019-07-16 06:32:07	Risk Assessment: Version = RRV-2909-RRV-2909-2019 Entity Type = Computer Entity Name = RRV-2909 Current Status = Information Gathering	Sending email to [redacted] failed. Not connected
□	Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	v12333	Do not send	2019-07-16 04:00:19	Risk Assessment: Version = 33-v12333-2019 Entity Type = Vendor Entity Name = v12333 Current Status = Information Gathering	Sending email to [redacted] failed. Not connected
□	Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	E123	Do not send	2019-07-16 04:00:14	Risk Assessment: Version = 33-E123-2019 Entity Type = Computer Entity Name = E123 Current Status = Information Gathering	Couldn't connect to host, port: bb, 6; timeout 600000
□	Assessment Launched: 33 - AC-1 ACCESS CONTROL POLICY AND PROCEDURES	Default Engagement	Do not send	2019-07-16 04:00:14	Risk Assessment: Version = 33-Default Engagement-2019 Entity Type = Vendor Service Entity Name = Default Engagement Current Status = Information	Sending email to [redacted] failed. Not connected

The Message Center page.

In the **Message Center** page, you can perform the following tasks:

- Clicking the subject of a message will help you view the details in a pane below the grid.
- Simultaneous deletion or archiving of multiple messages is possible.

About Tickets Page

The **Tickets** page is a grid consisting of tickets in which you are a stakeholder. If you own the responsibility of managing the tickets in your organization, you can view all of the tickets irrespective of the ownership. Depending on the permissions, you can use the **Tickets** page to perform one or more tasks as described below:

- Create a new ticket
- Open a ticket to view the details and to perform the following tasks:
    - Update the general information
    - Transition the workflow
    - Add comments
    - Manage attachments
    - Link or detach entities and vulnerabilities
    - View workflow history and changes
    - Synchronize the changes made to the ticket workflow
    - Delete a ticket

When you access the **Tickets** page, you can view all the tickets that needs your attention as well as the closed ones. For your convenience, the tickets can be segregated using the groups: **By Status, Stage, Type** and **My Tickets Delegated To Others** so that you can view the relevant tickets in one view. For example, you can click the Review group under the Tickets tree to work on the tickets that entered the review stage.

The groups under By Stage appear only when tickets enter a particular stage. For example, if there are tickets in the "New" and "Assigned" stages, only those stage groups appear to the stakeholder.

Tickets

The RiskVision solution provides a ticket management system that lets you create and track tickets for tasks, risk assessment mitigation and remediation, and entity control resolution. Tickets are also used for vulnerability resolution. In addition, sites may deploy and integrate the RiskVision solution with other external ticket management systems, such as Remedy.

In the Tickets page the tree only includes folders. Clicking on a folder usually displays the objects it contains in the grid pane.

Folder	Sub-Folder	
My Tickets	By Status	Open Tickets Closed Tickets
	By Stage	New In Progress Review Closed
	By Type	Entity Control Resolution Incident Response Other Risk Assessment Response Risk Assessment Remediation Threat Mitigation Vulnerability Resolution
	My Tickets Delegated to Others	
	My Undelegated Tickets	
All Tickets	By Stage	New In Progress Review Closed
	By Types	Entity Control Resolution Incident Response Other Risk Assessment Response Risk Assessment Remediation Threat Mitigation Vulnerability Resolution
	All Delegated Tickets	
	All Undelegated Tickets	

1. The folder name under the By Stage depends on the workflow stage names.
2. All Tickets folders are available only if users have the object Mange permission privilege.

Creating a New Ticket

Use tickets to assign tasks to system users and track progress. Create a ticket for each item that you want to track. For each task, the RiskVision solution creates a single ticket and sends the notification to all stakeholders of the initial stage. Each person views, modifies, and transitions the same ticket. Creating a new ticket requires you to have the Ticket View, Create or Manage permissions.

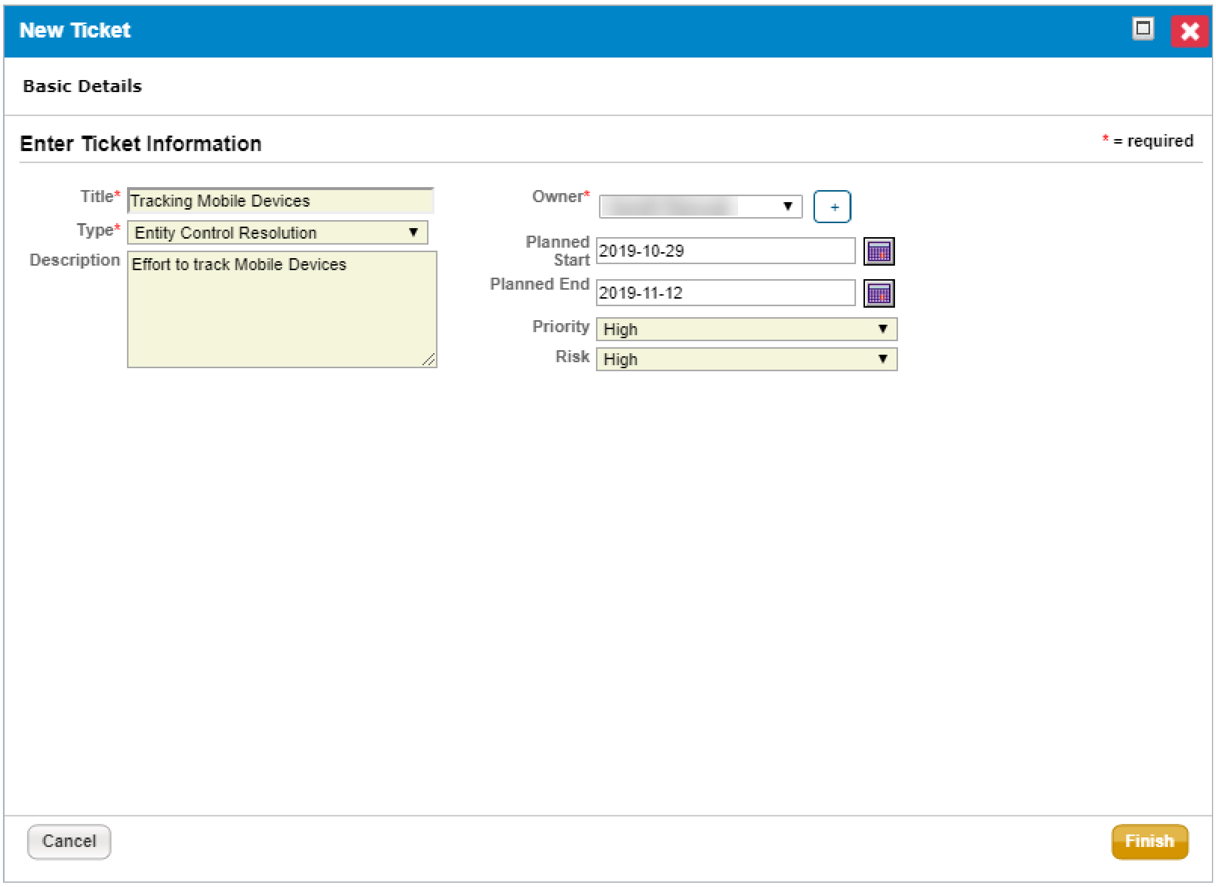
By default, all tickets use the Default Ticket Workflow template.

To create a new ticket:

1. Go to **Home > Tickets**.

2. Select the **My Tickets** folder.

3. Click **New**. The New Ticket window displays.



Title* Tracking Mobile Devices

Type* Entity Control Resolution

Description Effort to track Mobile Devices

Owner* [redacted]

Planned Start 2019-10-29

Planned End 2019-11-12

Priority High

Risk High

The New Ticket window.

4. Enter Title and Description. Select Type, Owner, Priority, and Risk. Also, specify Planned Start and Planned End dates. For information about the description of the fields in the **New Ticket** wizard, see Setting General Ticket Information.

5. Click **OK**.

A new ticket is created and displays in the My Tickets folder. Next, link the ticket to an entity.

You can create a ticket for a finding using the **Tickets** tab on the finding details page, and for a vulnerability using the**Affected Entities** tab on the vulnerabilities details page, and for an incident using the **Actions** and **Tickets** tab on the incidents details page. Creating a ticket manually, automatically marks the vulnerability as acknowledged. If the system (Affected Entities Notification Sender job) creates the ticket automatically, an unacknowledged vulnerability remains unacknowledged.

Batch Edit Tickets

The **Batch Edit Tickets** action makes it possible for users to edit most of the fields in multiple tickets at one time. The fields that **cannot** be edited include:

- Name;
- Status;
- Export Status;
- Submitted By;
- Ticket ID;
- Created Time; and
- Ticket Age.

Once the tickets have been successfully modified, the logged event will include the **Ticket IDs** of the modified tickets, the user who performed the action, records of the modified fields, and the time and date of the action.

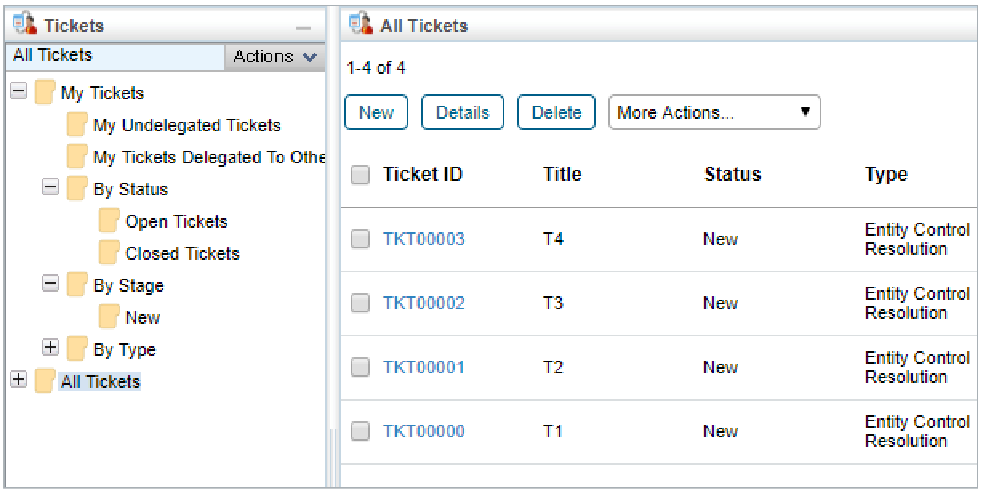
When using this action, note that:

- Up to 50 tickets can be bulk-edited at one time.
- Batch edits cannot be performed on closed or terminal tickets. Reopening tickets in bulk is not supported.
- Only users with **View** and **Update** permissions on tickets can perform this action.

> Batch ticket editing supports the use of the Groovy programming language. If you wish to use Groovy for bulk-editing tickets, contact Resolver Support.

To bulk-edit tickets:

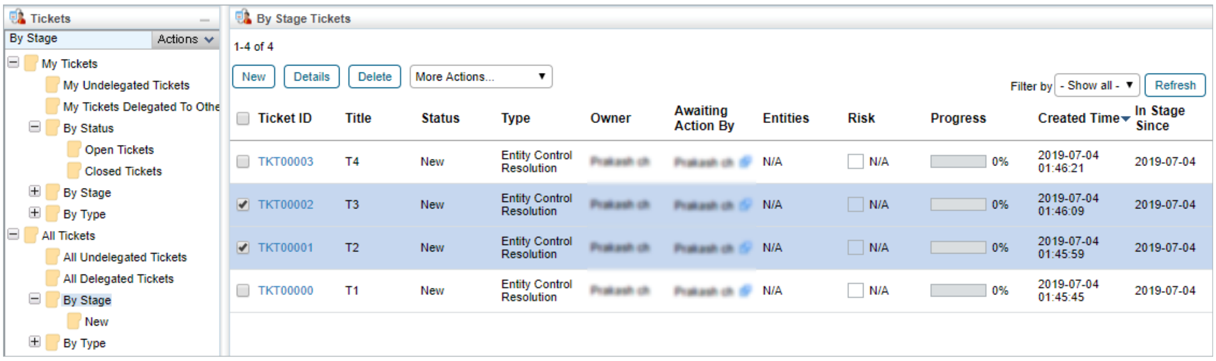
1. Click **Home** > **Tickets**.
2. Click a folder in the tree view to view the tickets in the grid.



☐	Ticket ID	Title	Status	Type
☐	TKT00003	T4	New	Entity Control Resolution
☐	TKT00002	T3	New	Entity Control Resolution
☐	TKT00001	T2	New	Entity Control Resolution
☐	TKT00000	T1	New	Entity Control Resolution

Existing tickets.

3. Select the checkboxes beside the appropriate objects or select the checkbox in the far-left of the grid's header to select all objects.

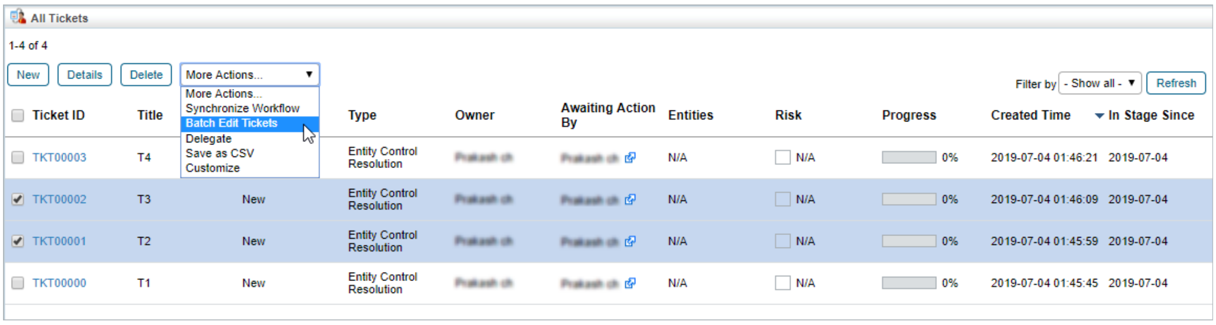


☐	Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
☐	TKT00003	T4	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:46:21	2019-07-04
☑	TKT00002	T3	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:46:09	2019-07-04
☑	TKT00001	T2	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:45:59	2019-07-04
☐	TKT00000	T1	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:45:45	2019-07-04

Selected tickets.

> A maximum of 50 tickets can be selected for a batch edit.

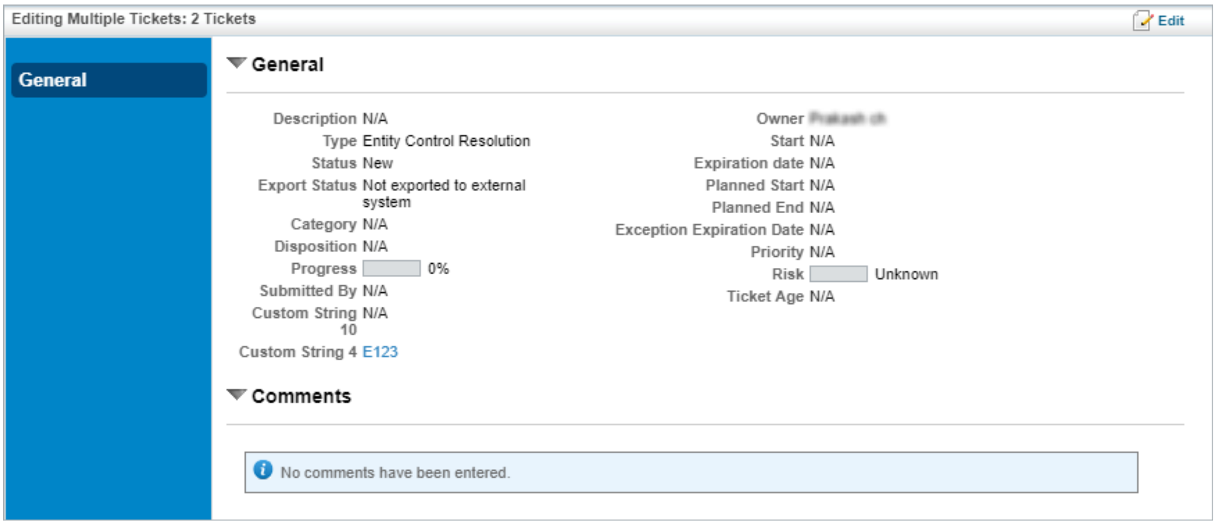
4. Click the **More Actions...** dropdown menu, then click **Batch Edit Tickets** to open the **Editing Multiple Tickets** window.



☐	Ticket ID	Title		Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
☐	TKT00003	T4		Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:46:21	2019-07-04
☑	TKT00002	T3	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:46:09	2019-07-04
☑	TKT00001	T2	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:45:59	2019-07-04
☐	TKT00000	T1	New	Entity Control Resolution	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-07-04 01:45:45	2019-07-04

The Batch Edit Tickets option in the More Actions... dropdown menu.

5. Click **Edit** in the top-right corner of the window.



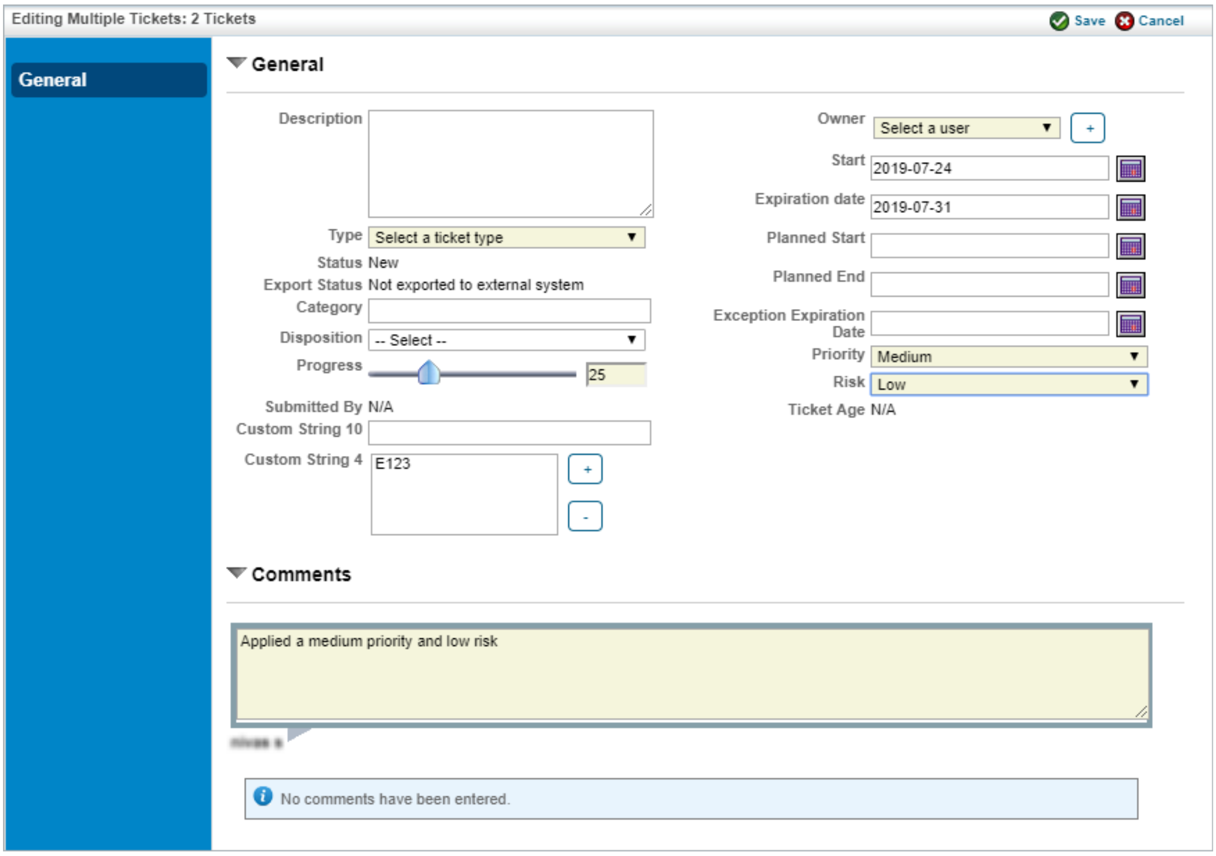
Description N/A
Type Entity Control Resolution
Status New
Export Status Not exported to external system
Category N/A
Disposition N/A
Progress 0%
Submitted By N/A
Custom String 10 N/A
Custom String 4 E123

Owner [redacted]
Start N/A
Expiration date N/A
Planned Start N/A
Planned End N/A
Exception Expiration Date N/A
Priority N/A
Risk Unknown
Ticket Age N/A

No comments have been entered.

The Editing Multiple Tickets window.

6. Make changes to the fields and add comments as required.
7. Click **Save** when finished and refresh your browser to see your changes.



Editing Multiple Tickets: 2 Tickets

General

General

Description

Type: Select a ticket type

Status: New

Export Status: Not exported to external system

Category

Disposition: -- Select --

Progress: 25

Submitted By: N/A

Custom String 10

Custom String 4: E123

Owner: Select a user

Start: 2019-07-24

Expiration date: 2019-07-31

Planned Start

Planned End

Exception Expiration Date

Priority: Medium

Risk: Low

Ticket Age: N/A

Comments

Applied a medium priority and low risk

No comments have been entered.

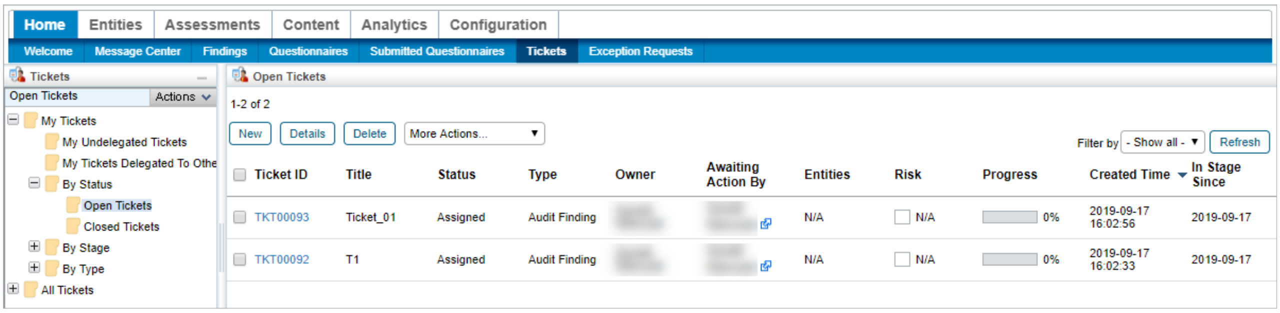
Editing the fields of multiple tickets.

Understanding Ticket Flow

Tickets are used to track efforts to review, analyze, and deploy remediation and prevention steps associated with specific vulnerability instances. The **Tickets** section of a vulnerability lists the tickets associated with the instance.

Tickets have an associated workflow. Vulnerability resolution tickets are related to their vulnerability instance. The status of the ticket corresponds to the current stage of the workflow. The workflow and its stages can be customized to suit specific requirements, but typical ticket workflow stages include:

- New
- In Progress
- Review
- Closed
- Closed via Exception



1-2 of 2

□	Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
□	TKT00093	Ticket_01	Assigned	Audit Finding	[redacted]	[redacted]	N/A	□ N/A	0%	2019-09-17 16:02:56	2019-09-17
□	TKT00092	T1	Assigned	Audit Finding	[redacted]	[redacted]	N/A	□ N/A	0%	2019-09-17 16:02:33	2019-09-17

The Tickets page.

The disposition field affects the workflow while editing a ticket. Set the disposition to **Escalate** or **Exception** or customize the set of disposition choices.

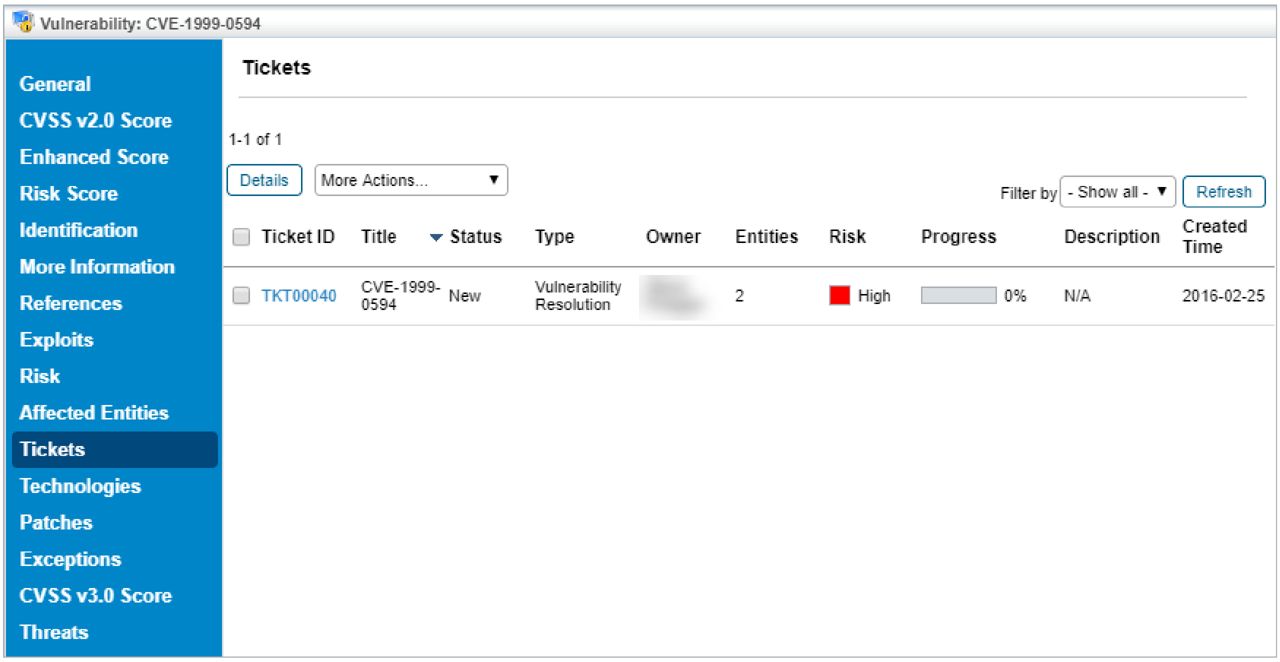
Ticket updates can change the ticket disposition. You can also select a disposition that will not generate escalations. However, changing the ticket disposition does not automatically close the ticket or prevent a closed ticket from being reopened.

Tickets also have an **Exception Expiration** field. If you specify a date in this field, the system will send an email to ticket stakeholders when the ticket is overdue. The email template used for this notification is specified in the property **ticket.exception.expired.notification.template.**

Ticket escalation templates can be specified by priority using the system property: com.agiliance.ticket.escalation.template with a value such as "high, Default Ticket Escalation Template; medium, Default Ticket Escalation Template".

Relevant system properties include:

- vulnerability.status.exception: Names the exception status for all vulnerabilities; and
- vulnerability.status.cannot.overwrite: Names the exception status that cannot be further modified by a scanner or other source reporting the same vulnerability instance again.



□	Ticket ID	Title	Status	Type	Owner	Entities	Risk	Progress	Description	Created Time
□	TKT00040	CVE-1999-0594	New	Vulnerability Resolution	[redacted]	2	🟥 High	0%	N/A	2016-02-25

The Tickets tab of a vulnerability.

Tickets are associated with a vulnerability instance. Ticket email templates can contain the vulnerability title and description. To append vulnerability information in the notification that you send to stakeholders, use the object `getAttachmentVulnerabilities()` to specify the following html code in the email template.

```
#set($vulnerabilities= $ticket.getAttachedVulnerabilities())
#foreach($v in $vulnerabilities)
Vulnerabilities: $v.getCaption()
#end
$ticket.getAttachedVulnerabilities()
```

Linking a Ticket to an Entity

Links between entities and tickets are permanent. Links map workflow stage stakeholders to entity ownership types and allow you to run reports on entities and their corresponding tickets.

The Default Ticket Workflow assigns stage stakeholders based on their entity ownership type. To automatically assign ownership of the tasks related to the ticket process, you must link the entity or entities to which the ticket applies.

Links to incidents display on the Ticket > Link page. You can link tickets to incidents from the Home > Incidents page.

To link a ticket to an entity:

1. Go to **Home > Tickets.**
2. Locate the ticket, select the ticket, and click **Details**.
3. Open the **Linked To** section.
4. Click **Add Entities**. The **Select Entities** window displays.
5. Select a type of entity and click **Search**. A list of entities displays.
6. Select an entity and click the down arrow to move it to the **Selected Entities** field.
7. Click **OK**.

The ticket is now linked to the entity. If you are creating a new ticket, move it to the first stage of the workflow process as described in Transitioning a ticket to the next stage.

Starting and Transitioning the Ticket Process

When you submit a ticket, the ticket process begins in the first stage of the workflow. Only the current stage owner transitions the ticket to another stage. Ticket Administrators can assign the ticket to themselves and then move it to another stage.

The ticket type is mapped to a ticket workflow template. By default, all types are mapped to the Default Ticket Workflow. Each ticket has its own instance of the workflow. Workflow changes don't affect tickets after they start the workflow process. The user can apply workflow changes to tickets manually with the link "Click here to attempt a synchronization."

To transition a ticket:

1. Go to **Home** > **Tickets**.
2. Locate the ticket, select the ticket, and click **Details**.
3. Click **Workflow**.

   The Workflow page displays.
4. Click an action button, such as **Accept**, to transition to the next stage or **Reject** to send it back to the previous stage. The Comment window displays.
5. Enter your transition message and click **OK**.

The ticket moves to another stage and the comment is added to the ticket history.

Changing the Default Ticket Workflow

When a ticket is created, which can be an automatic or manual process, the new ticket will use the default ticket workflow if there is no appropriate custom workflow. The default ticket workflow is "Default Ticket Workflow." Users with sufficient privileges can modify certain aspects of the default workflow, but it is generally better to create a new ticket workflow and make it the default.

To change the default ticket workflow:

1. Create a new ticket workflow as described in Creating a New Ticket.
2. Open the file `%AGILIANCE_HOME%\config\agiliance.properties` by using a text editor. If the file does not exist, create it.
3. Add the following line:

   ```
   default ticket workflow=NewTicketWorkflowName
   ```

4. Reload the configuration, as described in the *Administrator's Guide*, or restart the RiskVision Tomcat service to affect the latest changes.

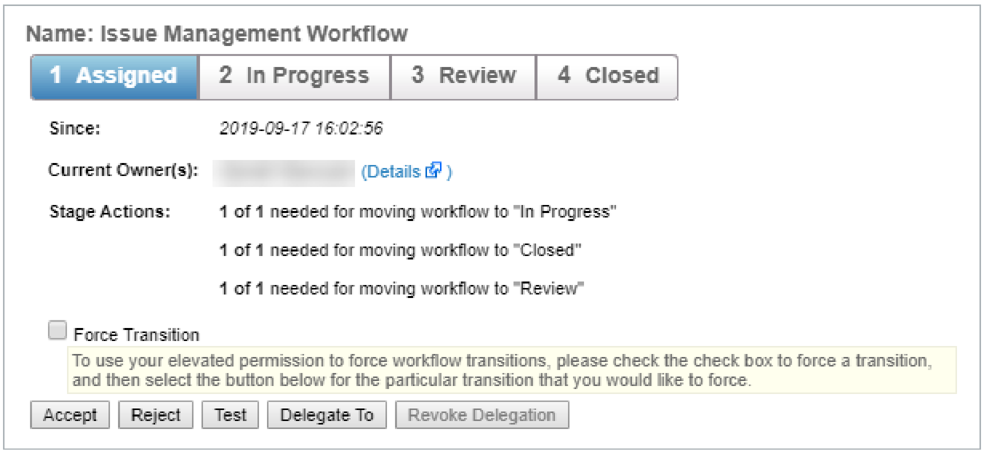
Alternatively, you can use the Selection tab of any custom ticket details page to change the default workflow.

Assigning a Ticket to Another User

Assigning a ticket to another user changes the ownership of current and subsequent workflow stages. You must have Ticket View and Ticket Manage permissions to view the **Delegate To** button to assign a ticket to another user.

To assign a ticket to another user:

1. Go to **Home** > **Tickets**.
2. Click the ticket you want to assign to another user, then click **Details**.
3. Click **Workflow**.



Name: Issue Management Workflow

Since: 2019-09-17 16:02:56

Current Owner(s): [redacted] (Details)

Stage Actions: 1 of 1 needed for moving workflow to "In Progress"

1 of 1 needed for moving workflow to "Closed"

1 of 1 needed for moving workflow to "Review"

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

A ticket's workflow stages.

4. Click **Delegate To** to open the **Select User** window.
5. Locate the user or team that you want to assign, then click **OK**. You can select multiple users, if desired.

The ticket ownership will transfer from the old list of owners to the new list.

Delegating an Object to Another User

Assigning a ticket to another user changes the ownership of current and subsequent workflow stages. Unless you have the Ticket View and Ticket Manage permissions, the **Delegate To** button is not visible for you to assign a ticket to another user.

To assign a ticket to another user

1. Go to **Home** > **Tickets**.

2. Locate the ticket, select it, perform the below steps:

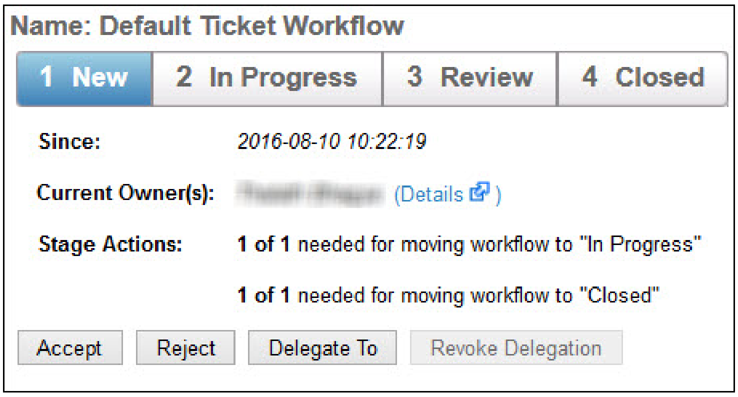
    1. From the **More Action** drop-down list, select the **Delegate** option.

    2. The **Delegate To** dialog box appears, locate the user or team that you want to assign, in the **Select User** or **Select Team** field.

        Here you can also select multiple users

    3. Enter the comment in the **Comment** field and then click **OK** button.

OR

> Locate the user or team that you want to assign. Here you can also select multiple users.
>
> 
>
> Name: Default Ticket Workflow
>
> Since: 2016-08-10 10:22:19
>
> Current Owner(s): [redacted] (Details)
>
> Stage Actions: 1 of 1 needed for moving workflow to "In Progress"
>
> 1 of 1 needed for moving workflow to "Closed"
>
>
>
> - Click **Details** option. The **Ticket** details page appears.
> - Go to **Workflow** section, in the **General** tab. The ticket workflow stage is displayed.
> - Click **Delegate To.** The **Delegate To** dialog box appears.
> - Enter the comment in the **Comment** field.
> - Click **OK** button.

The ticket ownership transfers from the old list of owners to the new list and the Revoke Delegation button is enabled.

Revoking A Delegated Object

Tickets that are delegated can only be revoked delegation. The revoke delegation will change the ownership of current and subsequent workflow stages. Unless you have the Ticket View and Ticket Manage permissions, the **Revoke Delegation** option is enabled for the tickets that are delegated.

To revoke an Assigned Ticket:

1. ## Go to Home > Tickets.

2. Locate the ticket, select it and perform the below steps:
    1. From the **More Action** dropdown list, select the **Revoke Delegation** option.

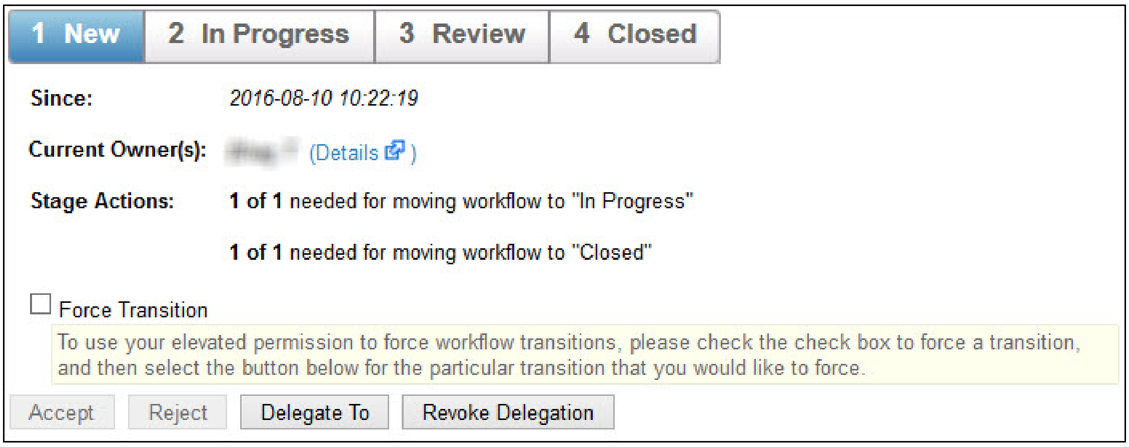
    2. The **Comments** dialog box appears.

    3. In the **Comment** dialog box, enter the reason or comment for revoking delegation access.

4. Click the **OK** button.

OR

- Click **Details** option. The **Ticket** details page appears
- Go to **Workflow** section, in the **General** tab. The ticket workflow stage is displayed. If the ticket is delegated already then the **Revoke Delegation** button is enabled.



Since: 2016-08-10 10:22:19

Current Owner(s): [redacted] (Details)

Stage Actions: **1 of 1** needed for moving workflow to "In Progress"

1 of 1 needed for moving workflow to "Closed"

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

- Click **Revoke Delegation** button. The **Comments** dialog box appears.
- In the **Comment** dialog box, enter the reason or comment for revoking delegation access.
- Click **OK** button.

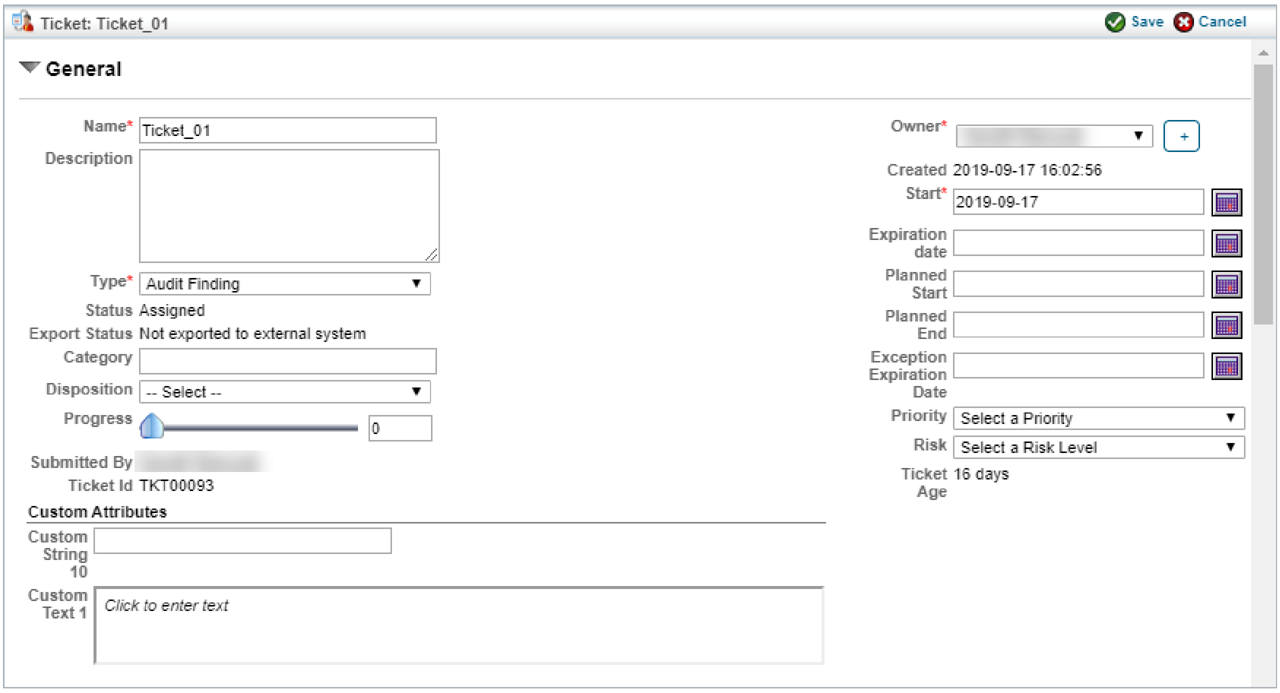
The ticket ownership transfers from the delegated user to the delegated by the user.

Setting General Ticket Information

Once a ticket is created, only the workflow stage owner can change the general ticket information, depending on their permissions. Workflow stage owners can have the following combinations of permissions:

- **Ticket View** permissions: Can view the ticket.
- **Ticket View** and **Update** permissions: Can view the ticket and change the general ticket information.
- **Ticket View** and **Classify** permissions: Can view the ticket and change the general ticket information, ticket priority, risk, and delete attachments.

Ticket administrators only need **Ticket View** and **Manage** permissions to modify the ticket settings, regardless of their participation in the ticket workflow.



Ticket: Ticket_01

General

Name* Ticket_01
Description
Type* Audit Finding
Status Assigned
Export Status Not exported to external system
Category
Disposition -- Select --
Progress 0
Submitted By [redacted]
Ticket Id TKT00093

Custom Attributes

Custom String 10
Custom Text 1 Click to enter text

Owner* [redacted]
Created 2019-09-17 16:02:56
Start* 2019-09-17
Expiration date
Planned Start
Planned End
Exception Expiration Date
Priority Select a Priority
Risk Select a Risk Level
Ticket Age 16 days

The General tab on the Edit Ticket screen.

Updating any of the settings sends an email notification to the owner of a ticket. To avoid sending email notifications to the owner each time settings are updated, use the following property: `com.agiliance.ticket.update.email.enabled=false`

Parameter	Description
Title	Identifies the ticket
Description	Text description for the ticket
Type	Ticket types include: • Entity Control Resolution • Incident Response • Risk Assessment Mitigation • Risk Assessment Remediation • Vulnerability Resolution
Status	Current workflow stage
Export Status	Indicates whether the ticket is linked to a remote ticket system, such as Remedy

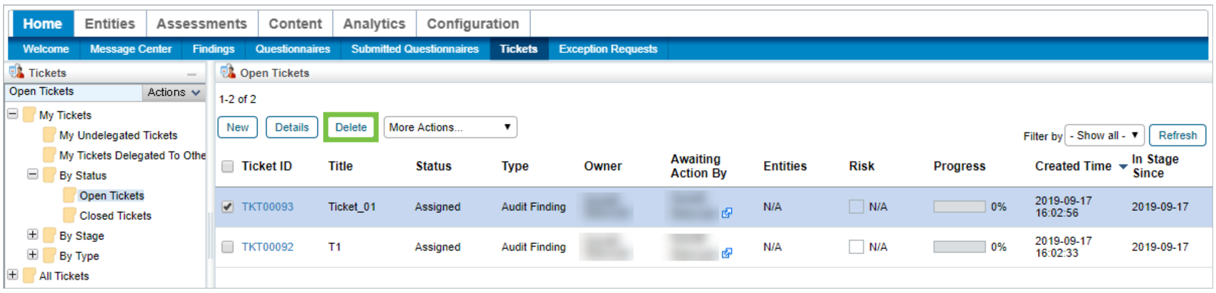
Parameter	Description
Category	Label that you can run reports on
Disposition	Ticket disposition, as specified in Ticket Management Preferences
Progress	Allows workflow stage owner to set the progress of the stage
Owner	The user who owns the ticket
Created Time	The time when a ticket was created
Start	By default, the date the ticket is created
End	By default, the date the ticket is closed
Planned Start	Date when the ticket must begin. You can also select a date in the past
Planned End	Date within which the ticket must be completed
Exception Expiration Date	Expiration date for exception
Priority	Indicates the importance of the ticket
Risk	Indicates the risk exposure of the ticket

Deleting a Ticket

You can delete a ticket if you are the owner and if you have Ticket View and Delete permissions. Users with Ticket View and Manage permissions can delete any ticket, regardless of ownership.

To delete a ticket:

1. Go to **Home > Tickets** and check the box next to the ticket you want to delete.
2. Click **Delete**, then **OK**.



☐	Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
☑	TKT00093	Ticket_01	Assigned	Audit Finding	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-09-17 16:02:56	2019-09-17
☐	TKT00092	T1	Assigned	Audit Finding	[redacted]	[redacted]	N/A	☐ N/A	0%	2019-09-17 16:02:33	2019-09-17

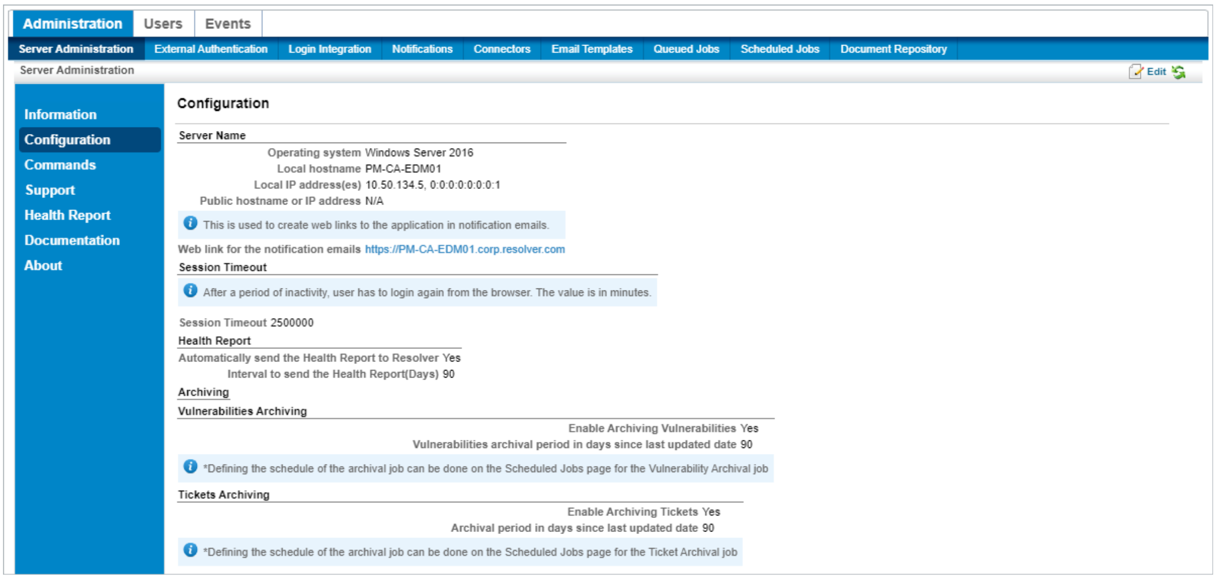
The Delete button on the Tickets page.

Automatic Ticket Archiving

To Enable Automatic Ticket Archiving:

1. In the Administration application, go to **Administration** > **Server Administration**.

2. Open the **Configuration** tab.



Configuration

Server Name

Operating system Windows Server 2016
Local hostname PM-CA-EDM01
Local IP address(es) 10.50.134.5, 0:0:0:0:0:0:0:1
Public hostname or IP address N/A

This is used to create web links to the application in notification emails.

Web link for the notification emails https://PM-CA-EDM01.corp.resolver.com

Session Timeout

After a period of inactivity, user has to login again from the browser. The value is in minutes.

Session Timeout 2500000

Health Report

Automatically send the Health Report to Resolver Yes
Interval to send the Health Report(Days) 90

Archiving

Vulnerabilities Archiving

Enable Archiving Vulnerabilities Yes
Vulnerabilities archival period in days since last updated date 90

*Defining the schedule of the archival job can be done on the Scheduled Jobs page for the Vulnerability Archival job

Tickets Archiving

Enable Archiving Tickets Yes
Archival period in days since last updated date 90

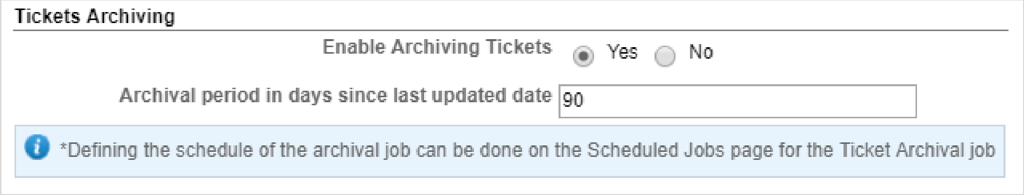
*Defining the schedule of the archival job can be done on the Scheduled Jobs page for the Ticket Archival job

The Configuration tab of the Server Administration page.

3. Click **Edit**.

4. Click the **Yes** radio button to enable archiving in the **Vulnerabilities Archiving and Tickets Archiving** sections.

5. Enter the number of days you want the archival period to last.



Tickets Archiving

Enable Archiving Tickets ● Yes ○ No

Archival period in days since last updated date 90

*Defining the schedule of the archival job can be done on the Scheduled Jobs page for the Ticket Archival job

The Tickets Archiving section of the Edit Configuration screen.

Ticket records will be archived after the specified amount of time has passed since their last update.

About Exception Requests Page

The **Exception Requests** page is a grid consisting of both local and global exceptions in which you are a stakeholder. The operations that you perform in this grid depends on the permissions assigned to your role. You can use the **Exception Requests** page to perform one or more tasks as described below:

- Create a global exception
- Update the general information
- Transition the workflow
- View workflow history
- Enter additional comments in addition to the comments that you enter while transitioning the workflow
- Manage attachments
- Synchronize the changes made to the workflow of an exception
- Delete an exception

Local exceptions can be created in the Questionnaire window or Control Results tab of Assessment Details page. For more information, refer to *Questionnaire Responder's Guide*.

Request Global Exceptions

This section explains how to request global exceptions for entities that are out-of-compliance with a control or subcontrol and you want to override the questionnaire and check results in the compliance and risk scores. The RiskVision solution applies the exception to all assessments with the entity-subcontrol pair. Setting an exception at the control level propagates the override to the subcontrols. If the questionnaire contained a subcontrol only, the global exception applies. You can also create an exception for a finding to override the finding's risk score. In order to request an exception, you must have Exception View and Exception Request permissions.

To request Local exceptions, that is, exceptions for a particular assessment, use the questionnaire. Stakeholders can access the questionnaire from

Folder	Sub-Folder	
My Exceptions	By Stage	Review Sign-Off Closed
	By Type	Control Vulnerability
	My Exceptions Delegated To Others	
	My Undelegated Exceptions	
All Exception	By Stage	Review Sign Off Closed
	By Type	Control Vulnerability
	All Delegated Exceptions	
	All Undelegated Exceptions	

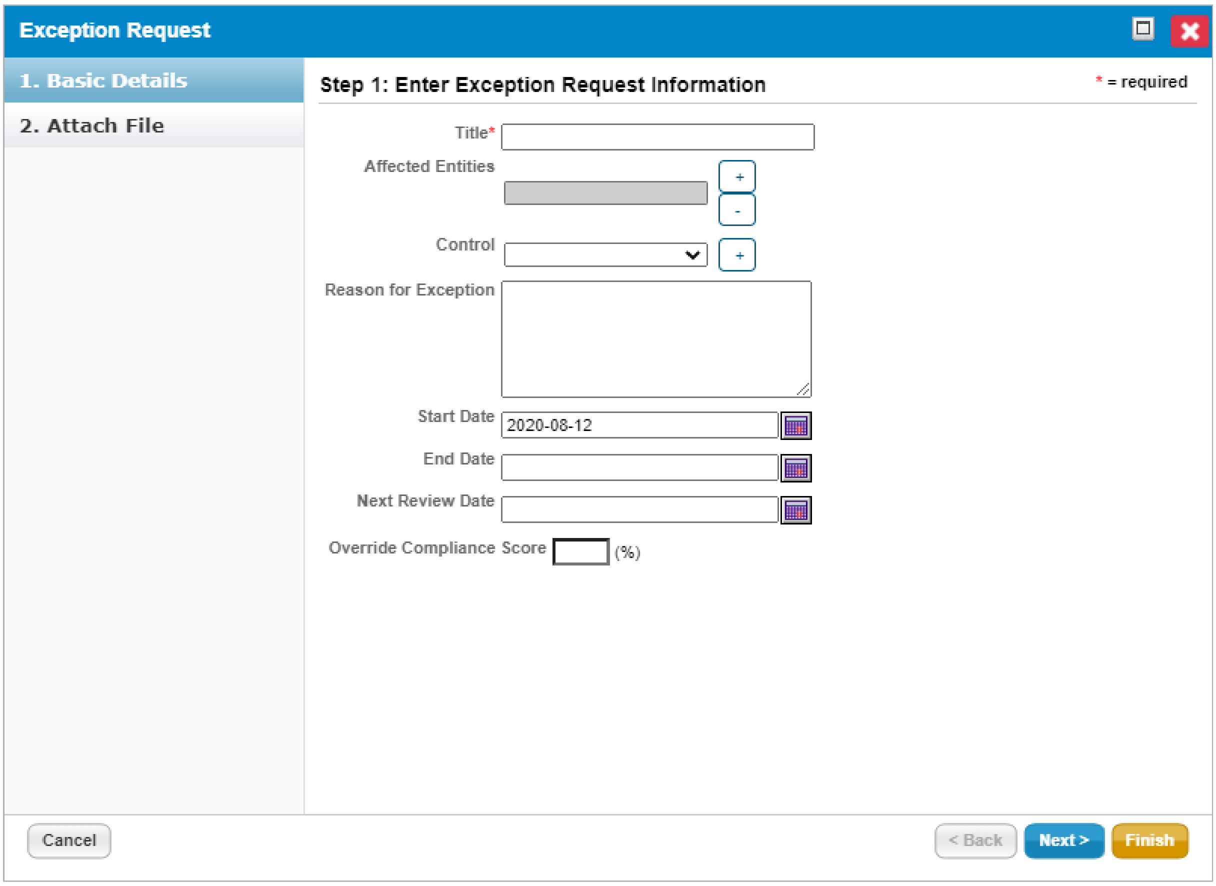
Note:

1. The folder name under the **By Stage** depends on the workflow stage names

2. All Exception folders are available only if users have the object Mange permission privilege.

To request an exception:

1. Go to **Home** > **Exception Requests.**
2. Click **New**. The **Exception Request** wizard appears.



Step 1: Enter Exception Request Information

* = required

Title*

Affected Entities

Control

Reason for Exception

Start Date 2020-08-12

End Date

Next Review Date

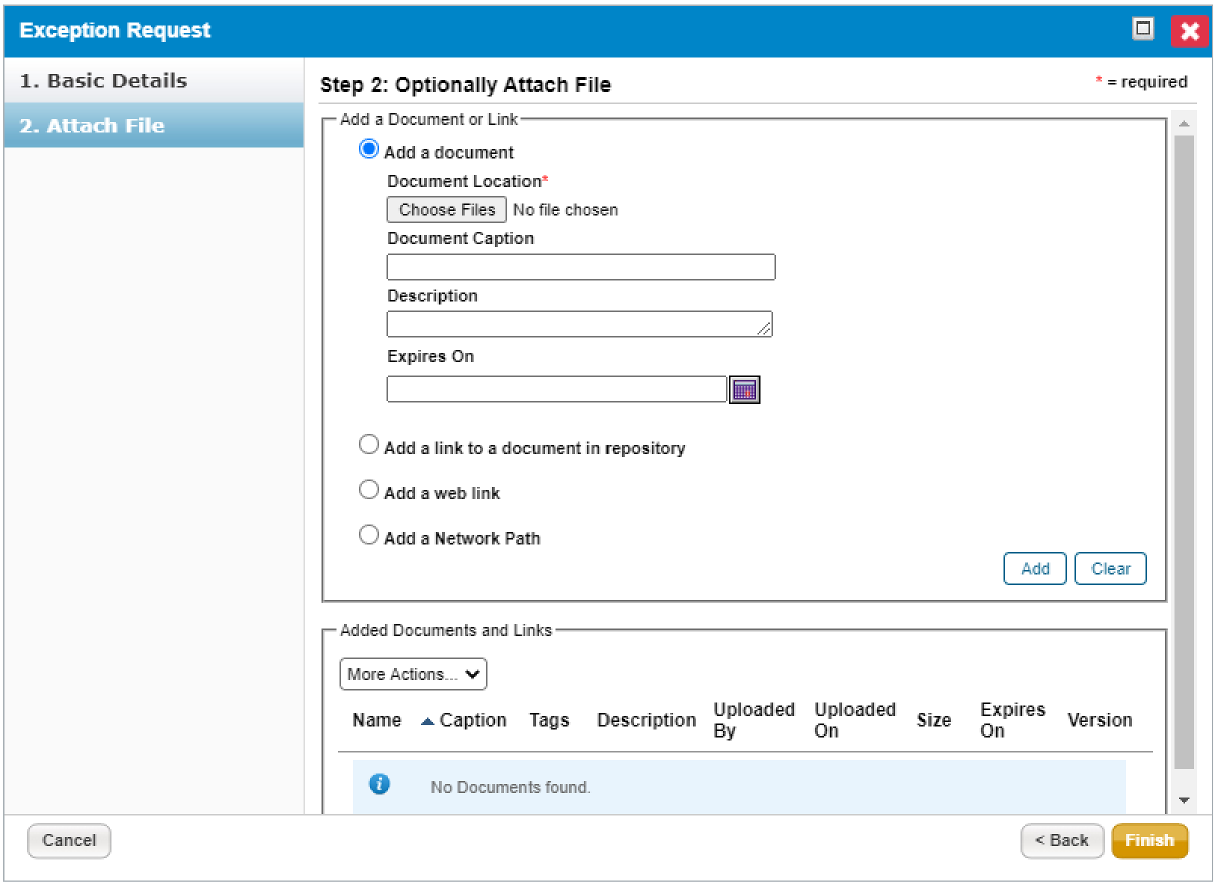
Override Compliance Score (%)

The Exception Request wizard.

3. In the **Basic Details** wizard page, enter the exception information. For more information, see Exception Request Basic Details.

4. Click **Next** to continue.

5. **Optional:** Add a document from your desktop, link to a document in the repository, or URL. For more information, see Exception Request Attachments.



Exception Request

1. Basic Details

2. Attach File

Step 2: Optionally Attach File

* = required

Add a Document or Link

● Add a document

Document Location*

Choose Files No file chosen

Document Caption

Description

Expires On

○ Add a link to a document in repository

○ Add a web link

○ Add a Network Path

Add Clear

Added Documents and Links

More Actions...

Name	▲ Caption	Tags	Description	Uploaded By	Uploaded On	Size	Expires On	Version
	No Documents found.							

Cancel < Back Finish

The Attach File section of the Exception Request wizard.

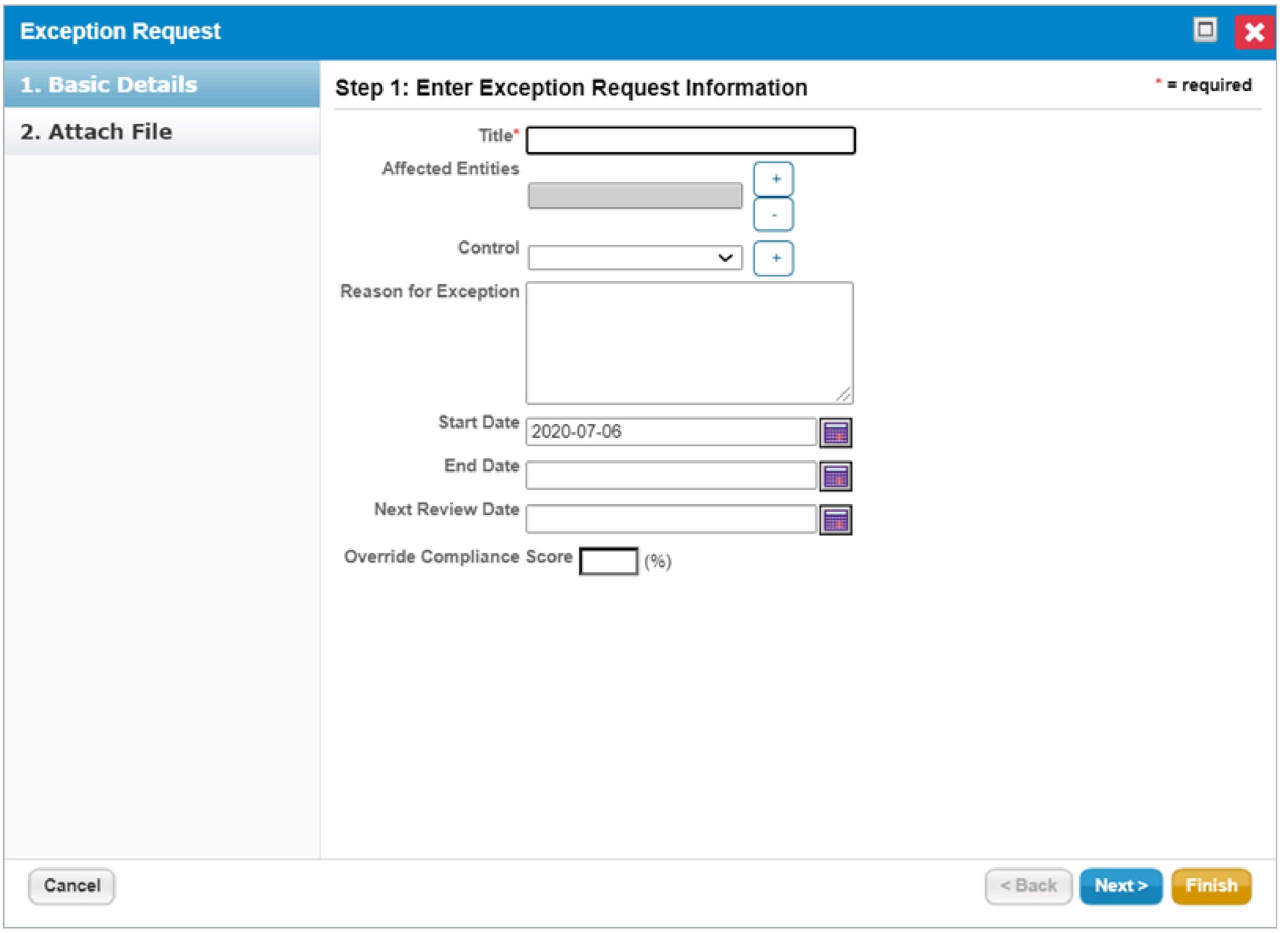
> If you cancel the attachment, it will appear to cancel the entire exception request. Wait a few moments and the exception request will appear without the attachment.

6. Click **Finish** to exit the wizard and to add an exception on**Home** > **Exceptions** page.

The exception has been created, but not requested. Go to the workflow page and submit the exception request. SeeManaging Your Exception Requests

Exception Request Basic Details

The following fields in the **Basic Details** wizard page of **Exception Request** must be specified when creating an exception.



Start Date 2020-07-06

The Basic Details section of the Exception Request wizard.

- **Title.** Enter the text to name the exception request.
- **Affected Entities.** Select entities for which you want to create an exception.
- **Applicable Controls.** Select controls that are applicable to the exception.
- **Reason for Exception.** Enter comments that explain why the exception is required.
- **Compensatory Controls.** Select subcontrols to compensate the non-performing subcontrol.
- **Start Date.** Select a date from when you want to start applying the exception.
- **End Date**. If the exception is for a specific period, select an end date. Otherwise, leave the End Date field empty if the exception is on-going.
- **Next Review.** Select the date and time that you want to automatically send a reminder to review the exception.
- **Override Compliance Score**. Enter a value to override the compliance score.

Exception Request Attachments

The **Attach File** wizard page of an exception request allows you to add documents to an exception. Stakeholders requesting an exception, or exception workflow stage stakeholders, can attach documents or web links.

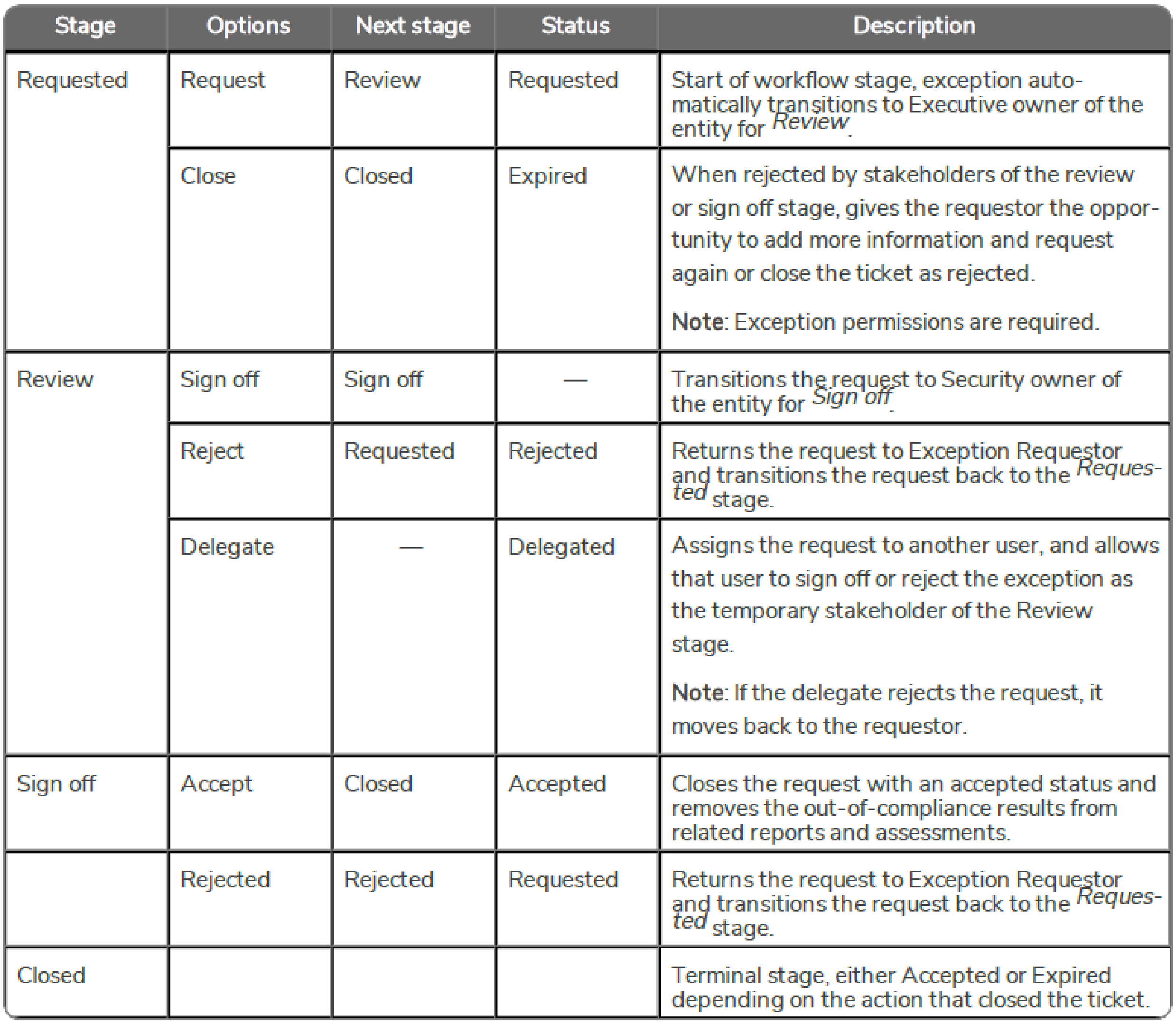
To attach documents to an exception:

Select one of the following options:

1. **Add a document** Specify the following fields:
    - **Document Location**: Click **Browse** to select the document.
    - **Document Caption**: Enter the text to name the document.
    - **Description**: Enter the text that describes the document.
    - **Expires On**: Select the date when the document will expire.
2. **Add a link to a document in repository** Click **Browse** to select a document collection.
3. **Add a web link**, specify the following fields:
    - **URL**: Enter a complete URL including the protocol HTTP or HTTPS.
    - **Link Caption**: Enter the text to name the URL.
    - **Description**: Enter the text that describes the URL.
    - **Expires On**: Select the date when the document will expire.
4. **Add a Network Path**, specify the following fields:
    - **URL**: Enter a complete Network Path.
    - **Link Caption**: Enter the text to name the Network Path.
    - **Description**: Enter the text that describes the Network Path.
    - **Expires On**: Select the date when the document will expire.
5. Click **Add** to display the documents in the **Added Documents and Links** grid. Click **Clear** to clear the selection.

Default Exception Workflow

The following table describes the default exception workflow:



Stage	Options	Next stage	Status	Description
Requested	Request	Review	Requested	Start of workflow stage, exception automatically transitions to Executive owner of the entity for *Review*.
	Close	Closed	Expired	When rejected by stakeholders of the review or sign off stage, gives the requestor the opportunity to add more information and request again or close the ticket as rejected. **Note**: Exception permissions are required.
Review	Sign off	Sign off	—	Transitions the request to Security owner of the entity for *Sign off*.
	Reject	Requested	Rejected	Returns the request to Exception Requestor and transitions the request back to the *Requested* stage.
	Delegate	—	Delegated	Assigns the request to another user, and allows that user to sign off or reject the exception as the temporary stakeholder of the Review stage. **Note**: If the delegate rejects the request, it moves back to the requestor.
Sign off	Accept	Closed	Accepted	Closes the request with an accepted status and removes the out-of-compliance results from related reports and assessments.
	Rejected	Rejected	Requested	Returns the request to Exception Requestor and transitions the request back to the *Requested* stage.
Closed				Terminal stage, either Accepted or Expired depending on the action that closed the ticket.

Edit an Exception

Exception workflow stage stakeholders can edit exceptions to these fields:

- **Information** tab > **General** details;
- Comments in the **Comments** tab; and
- Documents on the **Exception Request Details** page > **Attachments** tab.

Not all fields can be updated under the **General** details. The fields in the **Information** tab use a box to help you understand which fields can be updated when you click the **Edit** link. For information about the description of each field, see Exception Request Basic Details.

Transition Exception Requests

Only workflow stage stakeholders can modify settings and transition an exception to another stage. The user who submits a global request must manually move the exception into the next stage of the workflow.

To transition an exception to the next stage:

1. Go to **Home > Exception Requests**.
2. Click the **My Exceptions** folder.
3. Click the name of the exception.
4. Click the **Workflow** tab.
5. Click an action button to transition the exception to another workflow stage.
6. Enter a comment.
7. Click **OK**.

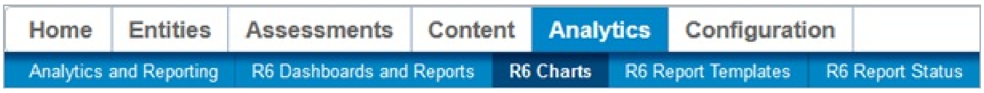
Your comment is added to the log and the exception is transitioned to the next stage.

R6 Report License

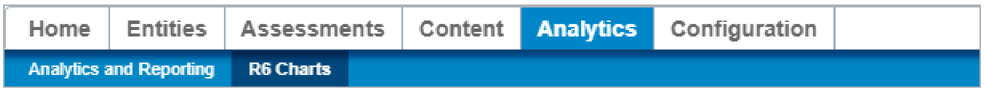
Resolver is preserving R6 Reporting for long-time RiskVision customers who have legacy reports in R6 Reporting that they have not been able to transition to RiskVision's JasperReports Server. As of Version 9.0, customers will need to request a license key with R6 Reporting enabled from Resolver Support.

The following table shows the differences in RiskVision's behavior when the R6 license is enabled:

FEATURE	WITH R6 LICENSE	WITHOUT R6 LICENSE
Menus Available in the Analytics Tab	• Analytics and Reporting • R6 Dashboards and Reports • R6 Charts • R6 Report Templates • R6 Report Status	• Analytics and Reporting
Configure UI Permission	Required for creating an R6 Custom Query chart.	Required to view and create R6 charts. Only table-type charts with custom queries can be created.
Enabled Properties	• To create R6 Charts, enable allowNewReport=true • To create R6 Dashboards and Reports, enable allowNewDashboard=true	• To create R6 table-type charts with custom queries, enable allowNewReport=true
Viewing R6 Charts, Dashboards, and Reports	Users can access R6 Dashboards and Reports, R6 Report Templates, and R6 Report Status.	• To view archived R6 Charts, enable showArchivedReports=true • To view archived R6 Dashboards and Reports, enable showDashboardPage=true
New Group and **Export Group** Actions	Users can select **New Group** and **Export Group** under **My Charts** and **My Dashboards**.	Users cannot execute **New Group** or **Export Group**.



The Analytics tab with an R6 License.



The Analytics tab without an R6 License.

Understanding Configurations

Any assessments you run in the RiskVision application involve various objects available on the **Configuration** menu. You must carefully examine each object to decide up to what extent you will need it and then configure only the required options to meet the essence of your assessment because you may want to choose a different strategy for each assessment. The below list describes the objects that you will want to configure them before the assessments are launched:

- Workflows
- Escalation
- Email Templates
- Filters
- Ownership Types
- Entity Configuration
- Incident Configuration
- Ticket Management Preferences
- **Workflows** - Choosing an appropriate workflow other than the default workflows is possible through the user interface of assessment and policy creation wizards. If you want an exception or ticket to follow a different workflow pattern, other than the default workflows, you must configure the selection criteria within those workflows. For more information on workflows, see the following topics:
    - About Workflows
    - Modifying Stage Settings
    - Specifying Multiple Workflows
- **Escalation** - Escalations are meant for tickets that are left unattended past thier due date so that the requestor, owner manager, or both can be made aware of the situation. For more information, see Creating an Escalation Configuration and Managing Escalation Configurations.
- **Email Templates** - The objects that notify stakeholders of a particular event typically use an email template. Several default email templates are available for selection or are already in-place to handle the notifications. If your organization prefers to follow the standard procedure for all its internal communications, you must design an email template. For more information, see Configuring E-mail Templates.
- **Filters** - A filter contains a set of conditions used by reports to match records, and dynamic groups to limit membership, and to limit user access, among other things. Filter types include Assessment, Dynamic Group, Entity, Exception Request, Incident, Program, Response, Risk, and more. For more information, see About Filters.
- **Ownership Types** - Ownership types link workflow stage stakeholders to the system users who are assigned to an entity or policy. This allows processes such as programs, tickets, and policy pack approval to run automatically. You can restrict which user can be assigned as a type of owner based on the user's role assignment. For more information, see About Ownership Types.
- **Entity Configuration and Incident Configuration** - Depending on the RiskVision application, a common threshold range criteria can be established for assessment, finding, vulnerability, risk or incident objects. When assessments are run, the risk, vulnerability and incident scores are derived according to the default range. Before you run any assessment, ensure that the threshold range is configured according to the assessment objective and meets auditing guidelines and policies. For more information, see Configuring a Threshold Range for Risk, Vulnerability and Incident Scores.
- **Ticket Management Preferences** - Usually, tickets are escalated when they pass the due date. You can add a disposition to avoid sending the escalation. For more information on setting the ticket preferences, see About Ticket Management Preferences.

Workflows

A workflow divides compliance, risk and other related business processes into stages and allows you to pre-assign participants (stakeholders), define requirements for transitioning between stages, and automate run-time process controls and activities, such as sending e-mail notifications and updating status.

The workflow initiator, such as a program owner, manages their own workflow and performs actions like reassigning, adding stakeholders, and forcing a transition to another stage. To view workflows on the **Configuration** menu, you must have the Workflow View permission to create, update or modify a workflow stage, you must have the Workflow Update permission.

The following table lists the RiskVision default workflows. The type of workflow that you see on the **Configuration** > **Workflows** menu depends on the RiskVision application.

Type	Object	Description
Exception	Entities and/or Controls	Specifies the stages of approving or rejecting an exception to a control that is requested by a user taking a questionnaire or from the **Exceptions** page.
Ticket	Entities	Specifies the stages for reporting and tracking various types of required actions. Initiate the ticket workflow from an incident using the Remedy connector, and by manually creating one on the Ticket page.
Finding	Controls or Entities	Specifies the stages to perform the risk assessment to respond to a finding. Creating a finding on the **Home > Findings** page or on the **Control Results** tab or **Findings** tab of **Assessment Detail** page will launch the workflow.

Modifying Stage Settings

This section explains workflow stage options. When you start a new process, such as an assessment or policy pack development, RiskVision copies the selected workflow and creates a separate workflow instance that belongs to the process. Instances and workflow templates are related but require a synchronization in order to have instances that are related to templates reflect the latest template modifications.

Users can modify templates if they have Workflow View and Workflow Update permissions.

Configure Stage Transitions & Actions

This article provides instructions on configuring the workflow transition and action options for the following objects:

- Tickets;
- Incidents;
- Exceptions;
- Findings; and
- Policies.

A stage transition moves the process from the current stage to another stage. The transition is typically associated with a user action, such as approve or reject. For Assessment workflows, the transition can also have questionnaire taking conditions. The stage transition options display as buttons on the workflow page.

By default, a workflow uses at least two actions in each stage. Since you may not need two actions on all occasions for each workflow stage, you may want to use the following properties so that actions can be selected depending on the context of need.

PROPERTY	DESCRIPTION
workflow.min.transitions=	Enter a number which specifies the actions in the workflow stage. If this property value is not set, the default value is 2, meaning there must be at least two transitions for every non-terminal stage.
workflow.max.transitions=	Enter a number so that you will have the choice to select more transitions when needed. By default the value is 4, meaning there can be no more than four transitions for every non-terminal stage.

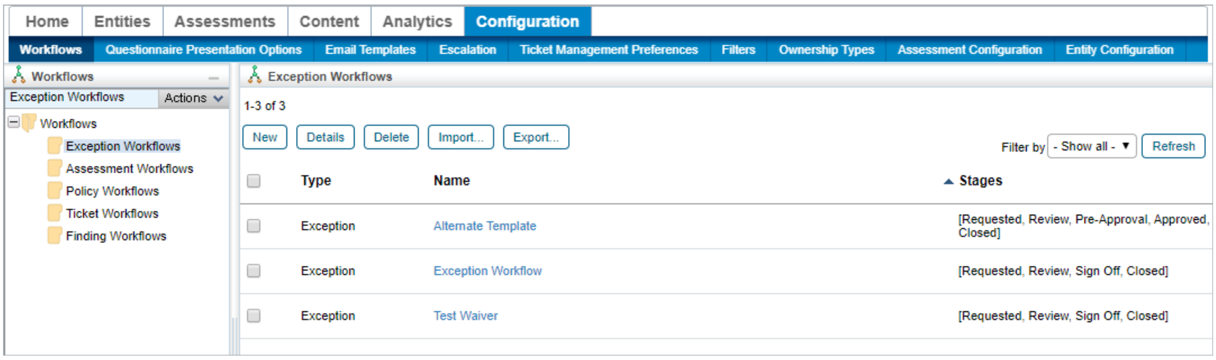
For example, if you need just one action in a workflow stage, you must set the `workflow.min.transition` property to 1 and `workflow.max.transitions` property to an appropriate value so that you can continue to select more actions in stages depending on the context of need.

Only users with**Workflow View** and **Workflow Update** permissions can modify workflows.

As of version 9.5, the `workflow.max.transitions` value for exception workflows will be the entered value plus 1. This extra transition will allow the workflow to expire.

To configure a workflow's transitions and actions:

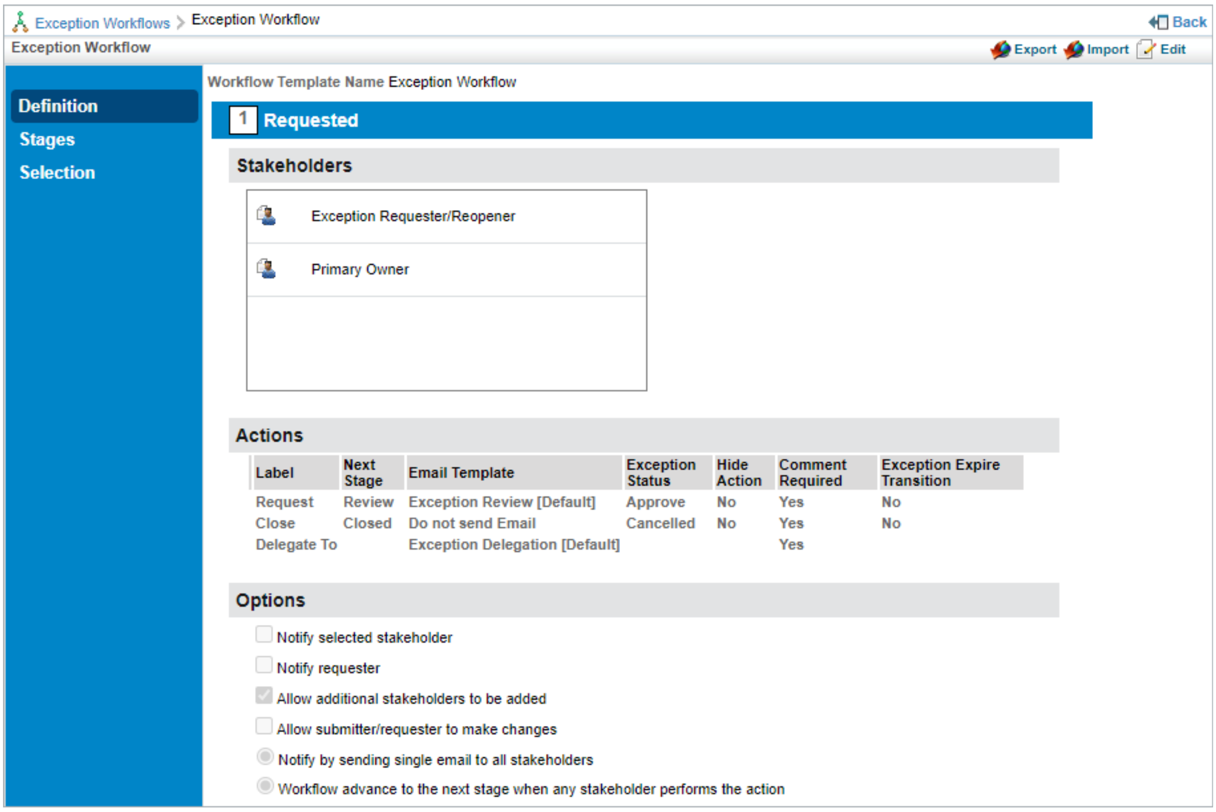
1. Click **Configuration > Workflows**.
2. Click a workflow on the grid to open the workflow settings. If needed, use the tree to the left or the filter dropdown menu on the far right to filter the results on the grid.



□	Type	Name	Stages
□	Exception	Alternate Template	[Requested, Review, Pre-Approval, Approved, Closed]
□	Exception	Exception Workflow	[Requested, Review, Sign Off, Closed]
□	Exception	Test Waiver	[Requested, Review, Sign Off, Closed]

The Workflow settings in Configuration.

3. Click **Definition** in the pane to the left if it's not already selected.



Workflow Template Name Exception Workflow

1 Requested

Stakeholders

- Exception Requester/Reopener
- Primary Owner

Actions

Label	Next Stage	Email Template	Exception Status	Hide Action	Comment Required	Exception Expire Transition
Request	Review	Exception Review [Default]	Approve	No	Yes	No
Close	Closed	Do not send Email	Cancelled	No	Yes	No
Delegate To		Exception Delegation [Default]			Yes	

Options

□ Notify selected stakeholder

□ Notify requester

☑ Allow additional stakeholders to be added

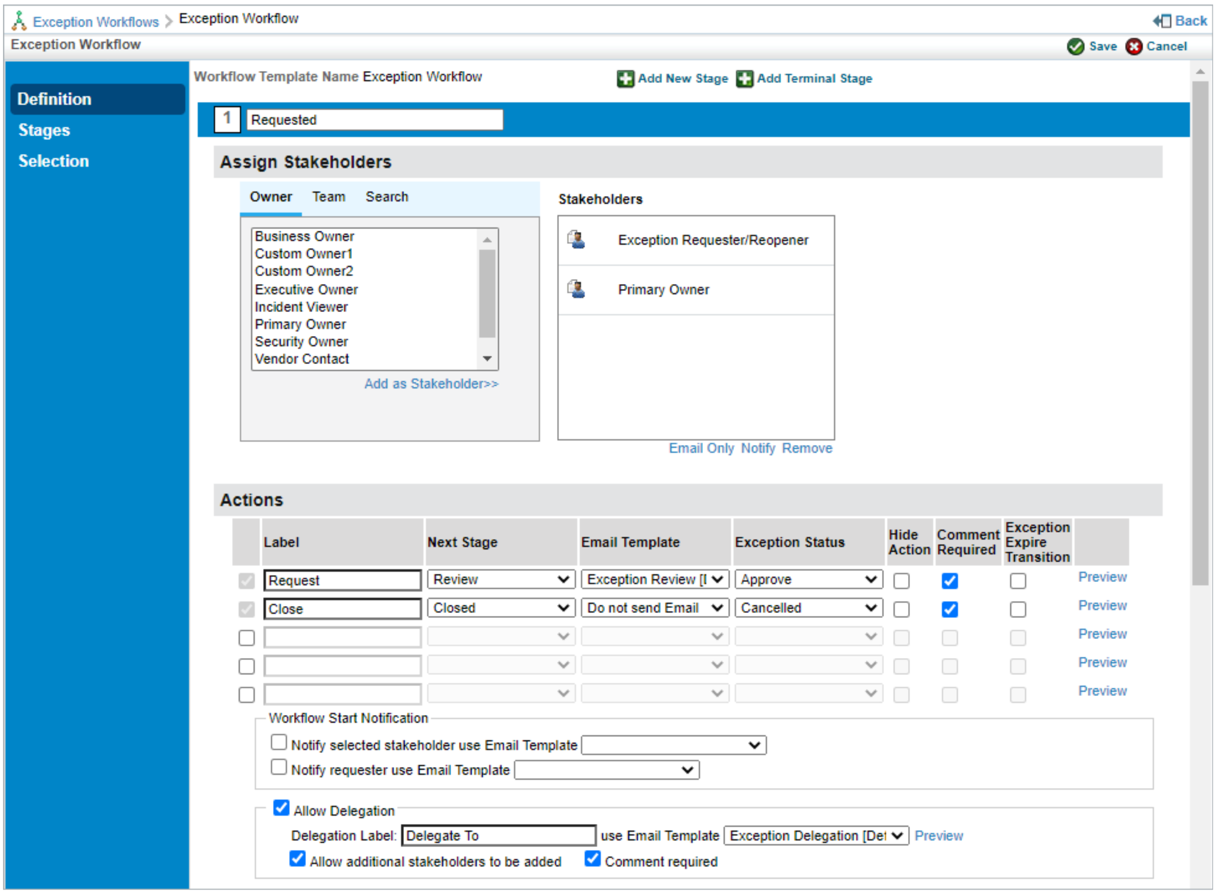
□ Allow submitter/requester to make changes

○ Notify by sending single email to all stakeholders

○ Workflow advance to the next stage when any stakeholder performs the action

Workflow details.

4. Click **Edit** in the top-right of the workflow screen.



Exception Workflows > Exception Workflow

Back

Exception Workflow

Save Cancel

Workflow Template Name Exception Workflow

Add New Stage Add Terminal Stage

1 Requested

Assign Stakeholders

Owner Team Search

Business Owner
Custom Owner1
Custom Owner2
Executive Owner
Incident Viewer
Primary Owner
Security Owner
Vendor Contact

Add as Stakeholder>>

Stakeholders

- Exception Requester/Reopener
- Primary Owner

Email Only Notify Remove

Actions

	Label	Next Stage	Email Template	Exception Status	Hide Action	Comment Required	Exception Expire Transition	
☑	Request	Review	Exception Review [I	Approve	□	☑	□	Preview
☑	Close	Closed	Do not send Email	Cancelled	□	☑	□	Preview
□					□	□	□	Preview
□					□	□	□	Preview
□					□	□	□	Preview

Workflow Start Notification

□ Notify selected stakeholder use Email Template

□ Notify requester use Email Template

☑ Allow Delegation

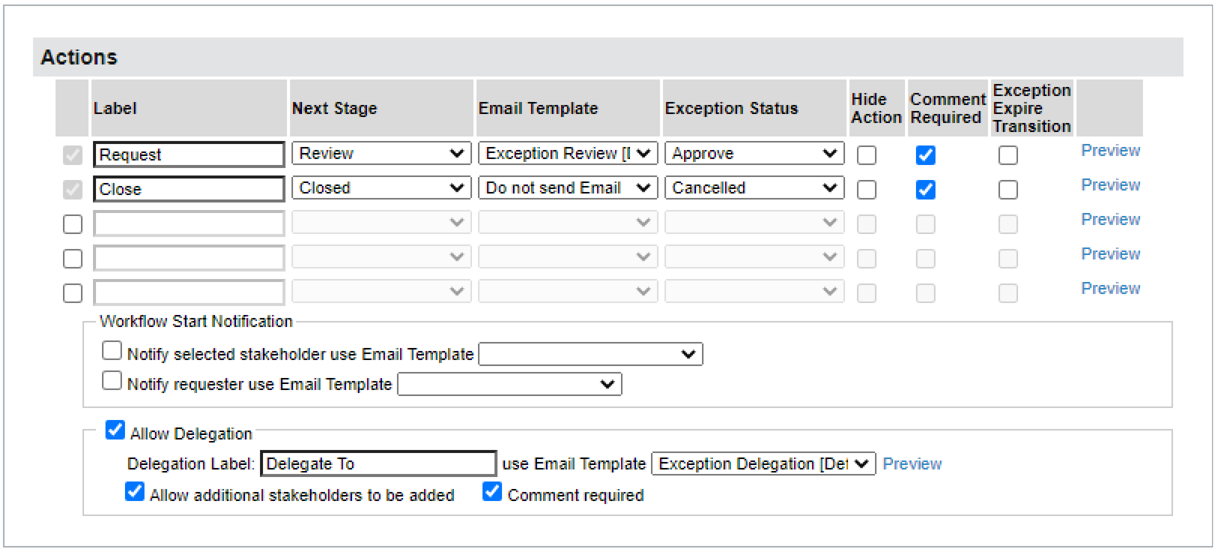
Delegation Label: Delegate To use Email Template Exception Delegation [Det Preview

☑ Allow additional stakeholders to be added ☑ Comment required

The Workflow edit screen.

5. Click a stage to display its **Actions** settings.

6. Enter a name for the stage in the **Label** text box. This is the label that will appear on the button that users click to move the object to another stage.



Actions

	Label	Next Stage	Email Template	Exception Status	Hide Action	Comment Required	Exception Expire Transition	
☑	Request	Review	Exception Review [I	Approve	□	☑	□	Preview
☑	Close	Closed	Do not send Email	Cancelled	□	☑	□	Preview
□					□	□	□	Preview
□					□	□	□	Preview
□					□	□	□	Preview

Workflow Start Notification

□ Notify selected stakeholder use Email Template

□ Notify requester use Email Template

☑ Allow Delegation

Delegation Label: Delegate To use Email Template Exception Delegation [Det Preview

☑ Allow additional stakeholders to be added ☑ Comment required

The Actions settings.

7. Select the stage the object will transition to from the **Next Stage** dropdown menu.

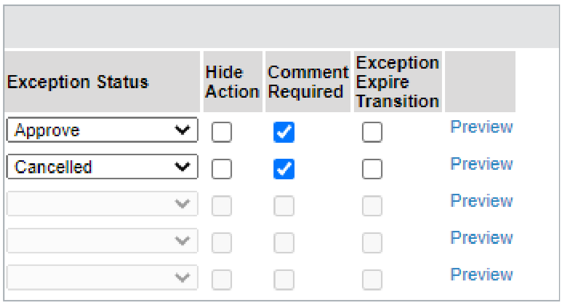
8. **Optional:** Select a template to define which email is sent to stakeholders when the notify settings are enabled. If you do not want an email sent, select **Do not send Email**

9. Enter a status for the object once it transitions in the **Status** field.

For exceptions, this field is a select list called the **Exception Status** field. Users will choose the appropriate status from a predefined list created on the Exception Management Preferences page. All other workflow types will have users enter in their own status values.

10. Select the **Hide Action** checkbox if the transition button should be hidden from end-users in the **Workflow** section of the object. This option is useful when the transition is automated and does not require any action from the user.

11. Deselect the **Comment Required** checkbox if the transition **does not** require end-users to enter comments in the **Workflow** tab before the object transitions. This checkbox is selected by default.



Exception Status	Hide Action	Comment Required	Exception Expire Transition	
Approve	□	☑	□	Preview
Cancelled	□	☑	□	Preview
	□	□	□	Preview
	□	□	□	Preview
	□	□	□	Preview

The Hide Action and Comment Required checkboxes.

12. **Optional:** Click **Preview** if you selected an email template in step 8 above and you wish to preview it.

13. Repeat steps 5 to 12 to modify the settings of additional stages as needed.

14. Click **Save** to save your changes.

Existing objects must be synchronized to reflect changes to the workflow settings. To synchronize, navigate to the objects (e.g. Home > Tickets) and select Synchronize Workflow from the More Actions... dropdown menu or open an individual object to synchronize it from the Workflow section.

Renaming The Stage

The stage name is displayed on the workflow pages of an assessment, policy, exception, ticket, incident, and so on. To change a stage name, select the stage and click Edit. Enter the new name and click Save.

- For assessment type workflows, you can only modify the stage name if there are no programs already in progress that use the workflow.
- For policies, exceptions, tickets, and incidents, the new workflow stage name appears if the process began after you completed the change.

Configuring Stakeholder Settings

A stakeholder is responsible for performing the actions defined in the workflow stage and can transition the process to another stage.

Assigning Stakeholders

You can include roles, specific users, and teams as stakeholders in every workflow stage.

Stakeholders assigned to workflow stages are classified into the following two categories:

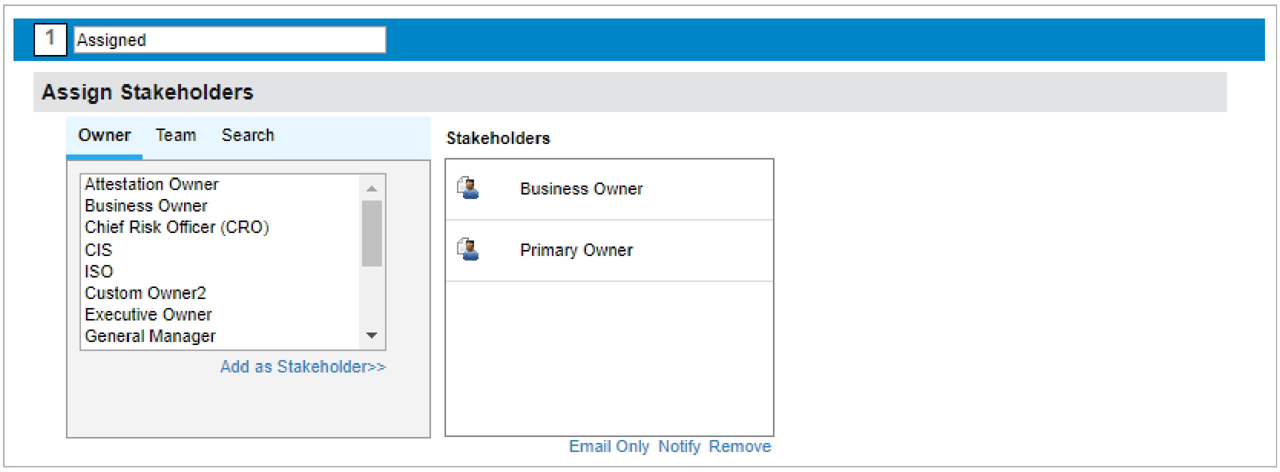
1. Task-performing stakeholders
2. Task-aware stakeholders

Task-performing stakeholders: This type of stakeholder performs different actions based on the workflow stage. By default, the stakeholders assigned to the workflow stage are task-performing stakeholders and have the 👤 icon next to their name.

Task-aware stakeholders: This type of stakeholder cannot perform any action when the workflow enters a stage. Notifications are sent to this type of stakeholder so that they're aware of the workflow's progress. To assign a user, team, or owner as task-aware stakeholder, add the user as stakeholder first, then select the stakeholder, and click **Email Only**. Task-aware stakeholders have the ✉ icon next to their name.

You must assign at least one task-performing stakeholder to every workflow stage. However, you can assign more than one stakeholder depending on your use case. The following table describes the selection options for the purpose of assigning the stakeholders in workflow stages:

OPTION	DESCRIPTION
Owner	Provides a list of ownership types. When selected, the user assigned to the Entity or Policy with the selected ownership type is automatically assigned as a stakeholder for the workflow stage.
Team	Provides a list of available teams. At least one team member must be assigned as an owner to the entity or policy.
Search	Allows you to search the User directory to select users.



The Assign Stakeholders section.

To assign stakeholders:

1. Select a workflow.
2. Click **Edit** in the top-right corner of the workflow **Details** page.
3. Select a stage.

4. Follow the steps below to select stakeholders:

    - To add an ownership type as a stakeholder, select an owner type on the**Owner** tab.
    - To add a team as a stakeholder, select a team on the**Team** tab.
    - To add a user as stakeholder, click the **Search** tab, enter the search criteria, and click **Search**. Under **Search Results**, select the user.

5. Click **Add as Stakeholder**. The assigned stakeholders are indicated with a user icon next to their name.

If you have to assign a team in each workflow stage, ensure that the number of stakeholders in a team is less than 200. Otherwise, it may not be possible to advance a workflow stage when the workflow is assigned to an object such as policy, program, and so on.

To remove a stakeholder:

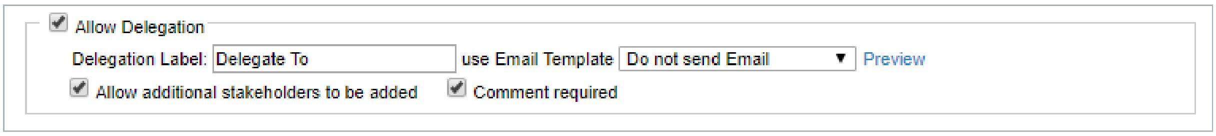
1. Select a workflow.
2. Click **Edit** at the top-right corner of the workflow **Details** page.
3. Select a stage.
4. Under **Assign Stakeholders**, select the stakeholder, and click **Remove**. To remove multiple stakeholders within a stage, press and hold **CTRL** button on your keyboard, click the stakeholders to select them, and click **Remove**. The stakeholder(s) is removed.
5. Click **Save**.

Allowing Stakeholders To Delegate

For each stage, except the terminal stage (closed), you can allow stakeholders to delegate their responsibility to another user or team. The delegate action adds the delegatee as a stakeholder and notifies them of their new task. The delegatee then acts as the original stakeholder.

To allow delegation:

1. Open a workflow for editing.
2. Open the stage.
3. Select **Allow Delegation**.
4. To change the label, enter the new button name.



☑ Allow Delegation

Delegation Label: Delegate To use Email Template Do not send Email ▼ Preview

☑ Allow additional stakeholders to be added ☑ Comment required

The Allow Delegation section.

5. Click **Save**. New workflow instances will be created from the revised template.

The **Delegate** label displays in dropdown lists, questionnaire windows, and other process related locations.

Workflow instances that are already in progress are not changed.

Allowing Stakeholders to Add Other Stakeholders

You can allow users to add stakeholders. New stakeholders must perform the requirements defined by the workflow stage. For example, if a stakeholder is added to the information gathering stage of an assessment, a questionnaire will be sent to them.

Stakeholders can add other stakeholders to workflow definitions, depending on permissions, but not to workflow templates. Synchronizing a workflow definition with its original workflow template will remove any additional ad hoc stakeholders.

If stakeholders are added to an assessment workflow definition, they will be automatically included the next time the assessment runs.

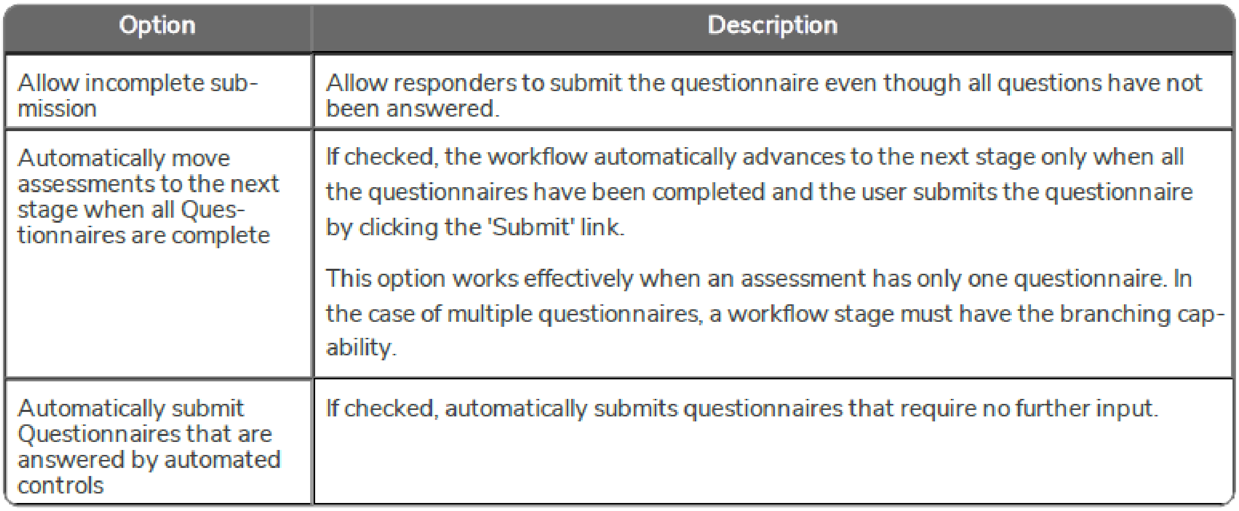
To allow stakeholders to add stakeholders:

1. Open RiskVision Policy Manager.
2. Go to **Configuration** > **Workflows**.
3. Click a workflow name to open. Click Edit.
4. Click a workflow stage to open.
5. Click **Allow Additional Stakeholders to be added**
6. Optional: To send an email when a stakeholder is added, click the name of an email template from the Notification dropdown.
7. Click **Save**. New workflow definitions will be created from the revised template.

Workflow instances that are already in progress will not be changed unless they are synced.

Send to Next Stage

Assessment workflows have a 'Send to Next Stage' section with the following options:

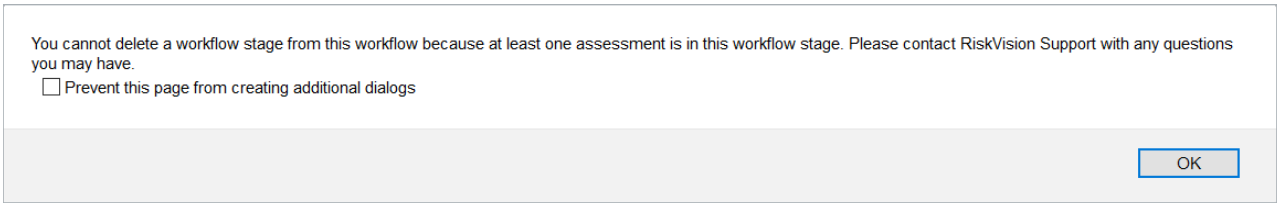


Option	Description
Allow incomplete submission	Allow responders to submit the questionnaire even though all questions have not been answered.
Automatically move assessments to the next stage when all Questionnaires are complete	If checked, the workflow automatically advances to the next stage only when all the questionnaires have been completed and the user submits the questionnaire by clicking the 'Submit' link. This option works effectively when an assessment has only one questionnaire. In the case of multiple questionnaires, a workflow stage must have the branching capability.
Automatically submit Questionnaires that are answered by automated controls	If checked, automatically submits questionnaires that require no further input.

Deleting Workflow Stages

It is possible to delete a workflow's stage in the event it was created in error, or it is no longer needed. Once the stage has been deleted, it will no longer be possible to assign anything to that stage.

As of RiskVision version 9.3.5, assessment workflow stages can also be deleted. An assessment workflow stage can only be deleted if no assessments are currently assigned to it. Attempting to delete an occupied workflow will result in the following message being displayed: **"You cannot delete a workflow stage from this workflow because at least one assessment is in this workflow stage. Please contact RiskVision Support with any questions you may have."**



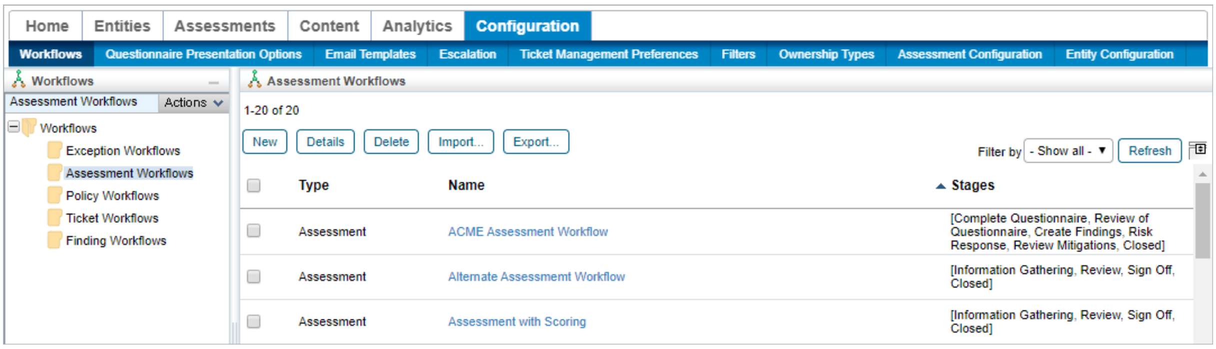
You cannot delete a workflow stage from this workflow because at least one assessment is in this workflow stage. Please contact RiskVision Support with any questions you may have.

□ Prevent this page from creating additional dialogs

The error message displayed when a user attempts to delete a workflow stage with an assessment assigned to it.

To delete a workflow stage:

1. Navigate to **Configuration > Workflows**.

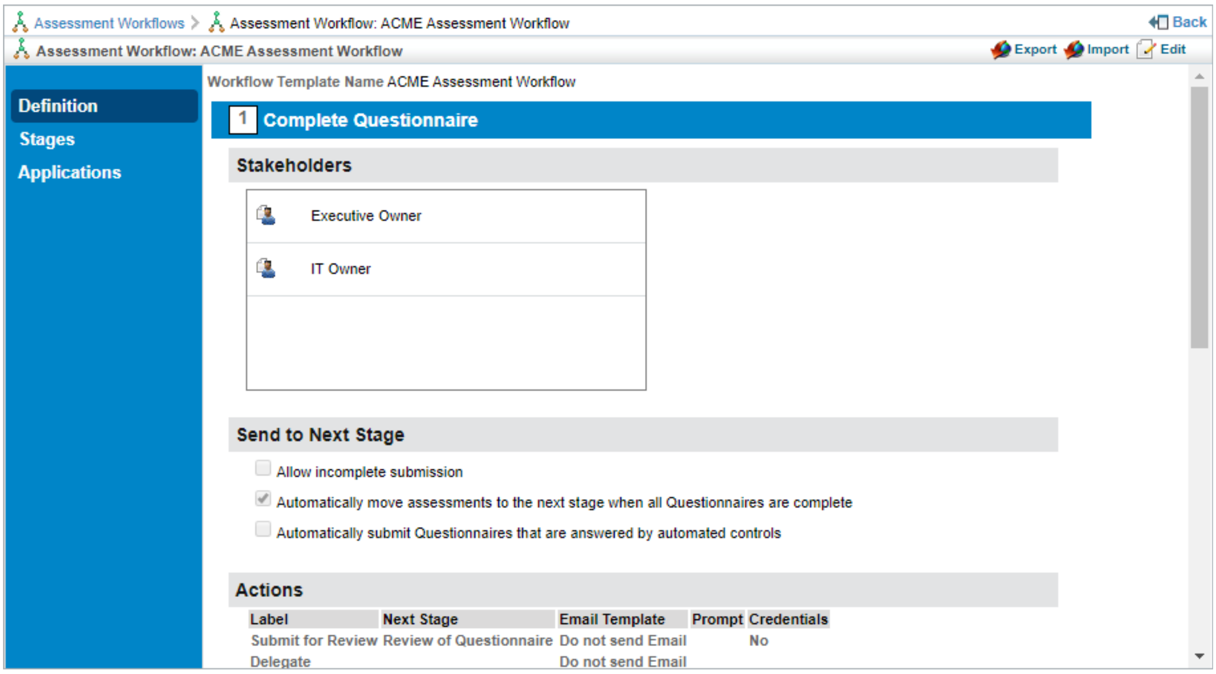


	Type	Name	Stages
□	Assessment	ACME Assessment Workflow	[Complete Questionnaire, Review of Questionnaire, Create Findings, Risk Response, Review Mitigations, Closed]
□	Assessment	Alternate Assessmemt Workflow	[Information Gathering, Review, Sign Off, Closed]
□	Assessment	Assessment with Scoring	[Information Gathering, Review, Sign Off, Closed]

The Workflow settings in Configuration.

2. Click a workflow on the grid to open the workflow settings. If needed, use the tree to the left or the filter dropdown menu on the far right to filter the results on the grid.

3. Click **Definition** in the pane to the left if it's not already selected.



Assessment Workflows > Assessment Workflow: ACME Assessment Workflow

Back

Assessment Workflow: ACME Assessment Workflow

Export Import Edit

Definition
Stages
Applications

Workflow Template Name ACME Assessment Workflow

1 Complete Questionnaire

Stakeholders

Executive Owner

IT Owner

Send to Next Stage

☐ Allow incomplete submission

☑ Automatically move assessments to the next stage when all Questionnaires are complete

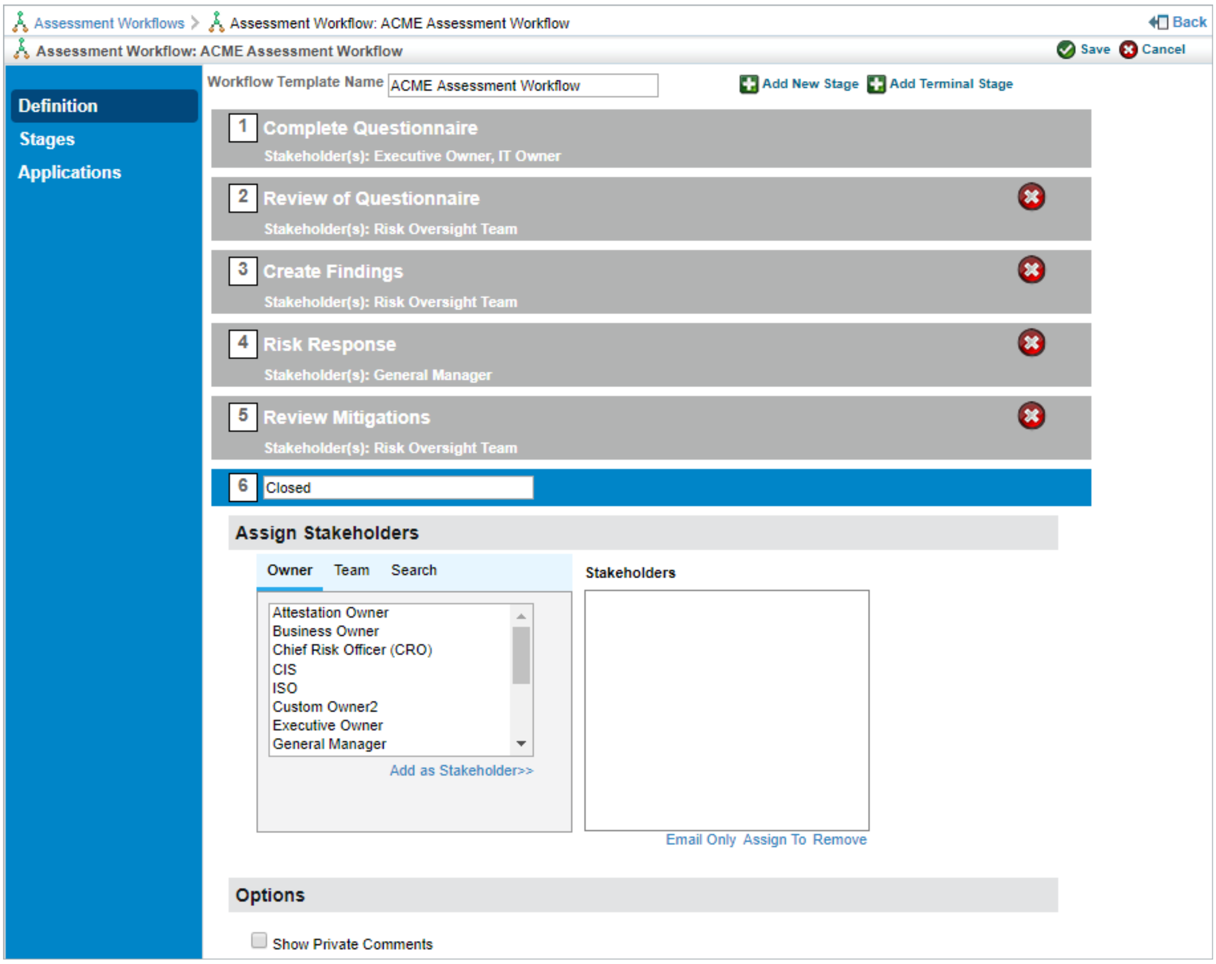
☐ Automatically submit Questionnaires that are answered by automated controls

Actions

Label	Next Stage	Email Template	Prompt	Credentials
Submit for Review	Review of Questionnaire	Do not send Email		No
Delegate		Do not send Email		

The Workflow Details page.

4. Click **Edit** in the top-right of the workflow screen.



Assessment Workflows > Assessment Workflow: ACME Assessment Workflow

Back

Assessment Workflow: ACME Assessment Workflow

Save Cancel

Definition
Stages
Applications

Workflow Template Name ACME Assessment Workflow

Add New Stage Add Terminal Stage

1 Complete Questionnaire
Stakeholder(s): Executive Owner, IT Owner

2 Review of Questionnaire
Stakeholder(s): Risk Oversight Team

3 Create Findings
Stakeholder(s): Risk Oversight Team

4 Risk Response
Stakeholder(s): General Manager

5 Review Mitigations
Stakeholder(s): Risk Oversight Team

6 Closed

Assign Stakeholders

Owner Team Search

Attestation Owner
Business Owner
Chief Risk Officer (CRO)
CIS
ISO
Custom Owner2
Executive Owner
General Manager

Add as Stakeholder>>

Stakeholders

Email Only Assign To Remove

Options

☐ Show Private Comments

The workflow edit screen.

5. Click the ✖ icon next to any stage to delete it.

6. Click **Save** to finalize your changes.

Other Stage Options

Ticket, Incident, and Exception workflow stages (except as noted) present the following additional options for advanced settings.

Option	Workflow Type	Description
Notify selected stakeholder	Ticket, Incident, and Exception	Notify the stakeholder selected in this stage.
Notify owner	Ticket, Incident, and Exception	Notify object owners regarding the object creation.
Allow submitter/requester to make changes	Ticket, Incident, and Exception	If checked, the original submitter or requester can change the ticketor exception request. **Note**: • The workflow option has no bearing on the ticket's owner, who can always make changes to the ticket. • If a user has the object **Manage** permission or is a stakeholder, then they will be able to make changes to the object regardless of whether the option is checked.
Allow additional stakeholders to be added	Ticket	If checked, allow additional stakeholders to add to the stage.
Add Option	All	Click to add reminder and escalation options. For more information, see Sending Reminders and Escalations to Stakeholders.
Notify by sending...	All	Notify by sending an e-mail to each stakeholder individually, or by sending a single e-mail to all stakeholders. For example, if a workflow stage has 2 normal stakeholders and 3 email, only stakeholders and the user selects the below option, • **Notify by sending email individually to each stakeholder**: 2 emails are sent to normal stakeholders in TO list with no one on the CC list and 1 email is sent to email only stakeholders on the CC list with no one on the TO list. • **Notify by sending single email to all stakeholders**: 1 email is sent which includes 2 normal stakeholders in TO list and 3 email only stakeholders in CC list.
Advance to the next stage when...	Ticket and Exception	Automatically advance to the next stage when any, all, or a specified percentage of stakeholders have performed the specified action.

Sending Escalations and Reminders to Stakeholders

RiskVision Server allows you to send of escalations and/or reminders to stakeholders from any stage within a workflow of any type when a workflow does not move forward within a specified time. In each workflow stage, you can add a combination of up to ten reminder and escalation options. The escalations and reminders are sent based on different date fields for different objects. For example, a ticket workflow allows you to remind a ticket stage stakeholder n days before a ticket will expire. The available escalation and reminder options and the date types for different workflows are given in the table below:

Workflow	Escalate/Remind Options	Date Types
Exception	Remind Stakeholder and Escalate to stakeholder's manager	Expiration, Start, and Stage start date, and custom dates
Incident	Remind Stakeholder and Escalate to stakeholder's manager	Due Date, Time Detected, Time Received, Stage start date, and custom dates
Ticket	Remind Stakeholder, Escalate to owner, and Escalate to stakeholder's manager	Created, Exception Expiration Date, End, Start, Planned Start, Planned End, Stage start date, and custom dates

Adding Escalations and Reminders

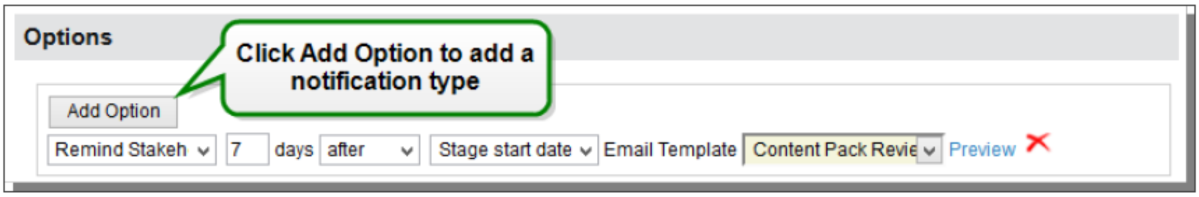
Most of the workflows in RiskVision Policy Manager have default settings for escalation and reminder notifications within each workflow stage. The default settings are provided based on the real and practical use cases. The default reminder and escalation settings for each stage in different workflows are given in the table below:

Workflow	Stages	Default Option Settings
Exception	Stage 1	No reminder and escalation options
	Stage 2 and Stage 3	Remind stakeholder 7 days after the workflow stage start date using the Exception Reminder email template
Incident	Stage 1, Stage 2, and Stage 3	Remind stakeholder 7 days after the workflow stage start date using the Incident Reminder email template
Ticket	Stage 1, Stage 2, and Stage 3	Remind stakeholders 7 days after the start date with the Ticket Reminder email template

You can add more escalation and/or reminder options if the default settings mentioned above do not fulfill your criteria.

To add an escalation or reminder option:

1. In the RiskVision, go to **Configuration** > **Workflows**. The **Workflows** page is displayed.
2. Select the workflow to open its details page.
3. Click **Edit** at the top-right corner of the details page.
4. Click the workflow stage in which you will want to add an escalation or reminder. The details are displayed.
5. Under **Options**, click **Add Option**. A new option is added.



6. In the first drop-down list, select the reminder or escalation option.
7. Enter a number in the days field.
8. In the second drop-down list, select one of the following: **on**, **before**, and **after**.
9. In the third drop-down list, select a date type.
10. In the fourth drop-down list, select an email template to notify users for reminder or escalation purposes.

Editing Escalation and Reminder Settings

You can edit escalation and reminder options one at a time by changing the previously set values.

To edit an escalation or reminder:

1. In the RiskVision application, go to **Configuration** > **Workflows**. The **Workflows** page is displayed.
2. Select the workflow to open its details page.
3. Click **Edit** at the top-right corner of the details page.
4. Click the workflow stage in which you will want to edit escalations and/or reminders. The details are displayed.
5. Change the value or select the value in the row corresponding to the reminder or escalation option.
6. Click **Save** after editing the escalation and/or escalation options.

Deleting Escalation and Reminders

You can choose to delete an escalation or reminder notification in as many stages as you want when you no longer need to notify your stakeholders. Navigate to each stage within a workflow and delete the escalation and reminder options.

To delete escalations and reminders:

1. In the RiskVision Policy Manager, go to **Configuration > Workflows**. The **Workflows** page is displayed.

2. Select the workflow to open its details page.

3. Click **Edit** at the top-right corner of the details page.

4. Click the workflow stage in which you will want to delete escalations and/or reminders. The details are displayed.

5. In the reminder or escalation option row, click ❌ . The option is deleted.

6. Repeat step 4 and step 5 to delete escalation and/or escalation options in other stages.

7. Click **Save** after deleting the escalation and/or escalation options.

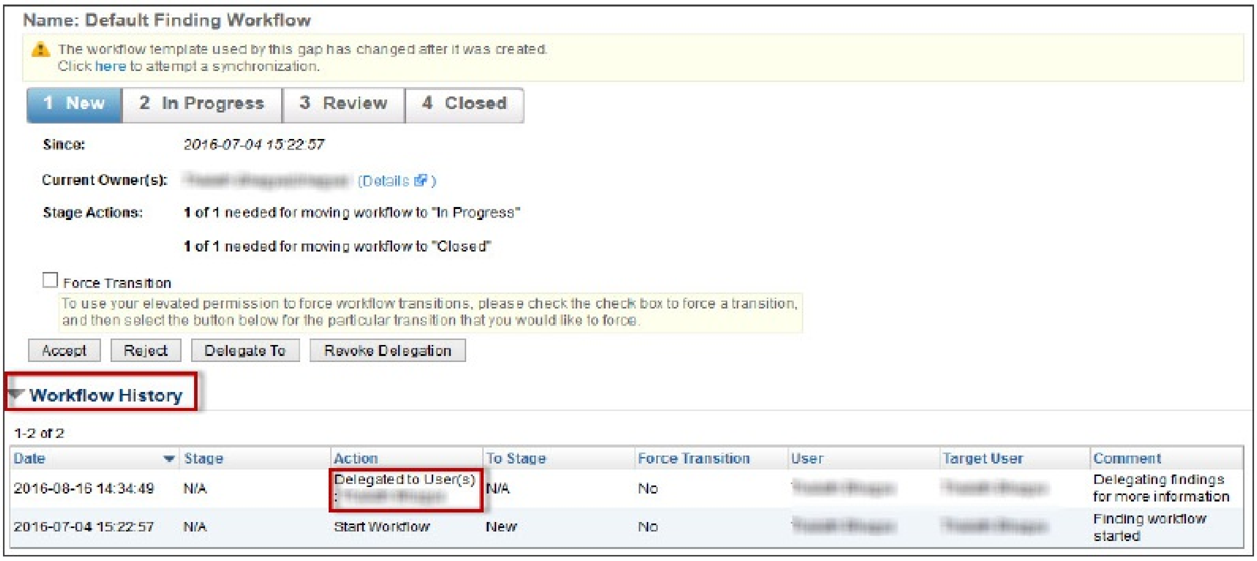
Sending Reminders and Escalations to Task-Aware Stakeholders

By default, the configured reminder and escalation options are sent only to the task-performing stakeholders and not the stakeholders who receive emails only and cannot transition workflows. However, if you want to copy task-aware stakeholders on all of the reminder and escalation notifications, then you can add the **com.agiliance.reminderOrEscaltions.notifyEmailOnlyUsers** property to the **agiliance.properties** file and set it to true. When this property is added, the reminder and escalation notifications are sent out to task-aware stakeholders for all stages and workflow types. For information about task-aware and task-performing stakeholders, see Assigning Stakeholders.

Delegation and Delegation Revocation

Users with Manage permissions on an object can read, create, modify, and update instances of the object they have Manage permissions for. These users can also delegate, revoke delegation, and force workflow transitions. Workflow stages can be delegated to any RiskVision user or team. . In order to delegate a stage in the workflow, delegation must be enabled. Delegation and delegation revocation is controlled on a per-stage basis by the option “Allow Delegation”.

It is a good practice to add a comment/reason for delegation or revoking delegation in the **Comment** section for tracking the purpose of the delegation. The comments added are visible to all users who have read access to the Workflow tab of the object and can view the comments in the **Workflow History** section as show below.



Name: Default Finding Workflow

The workflow template used by this gap has changed after it was created. Click here to attempt a synchronization.

Since: 2016-07-04 15:22:57

Current Owner(s): [redacted] (Details)

Stage Actions: 1 of 1 needed for moving workflow to "In Progress"

1 of 1 needed for moving workflow to "Closed"

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

1-2 of 2

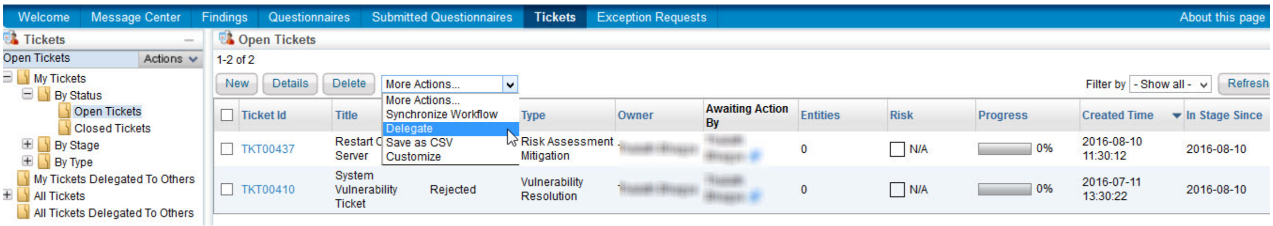
Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2016-08-16 14:34:49	N/A	Delegated to User(s) : [redacted]	N/A	No	[redacted]	[redacted]	Delegating findings for more information
2016-07-04 15:22:57	N/A	Start Workflow	New	No	[redacted]	[redacted]	Finding workflow started

The delegation option that is discussed in this section is available for the below objects:

- Tickets
- Incidents
- Exception Requests

For **Tickets**, **Incidents** and **Exception Requests**, stakeholder for the workflow can view the delegated objects in the **My Tickets Delegated To Others**, **My Findings Delegated to Others**, **My Incidents Delegated to Others,** and **My Exceptions Delegated to Others** column of their respective grids.

For **Tickets**, **Incidents**, and **Exception Requests,** stakeholders can perform bulk delegation and delegation revocation from the **More Actions** drop-down list .

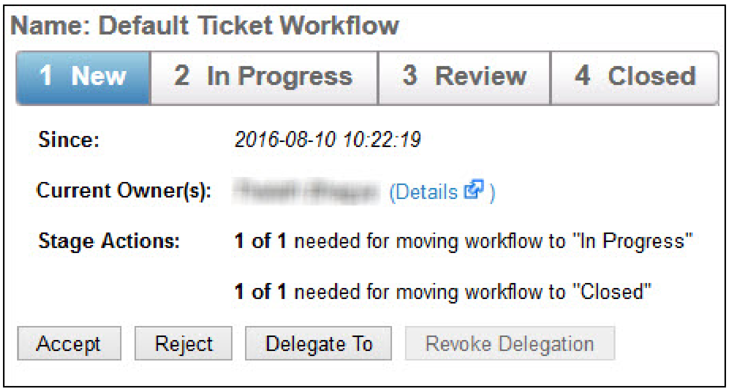


1-2 of 2

□	Ticket Id	Title		Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
□	TKT00437	Restart C Server		Risk Assessment Mitigation	[redacted]	[redacted]	0	□ N/A	0%	2016-08-10 11:30:12	2016-08-10
□	TKT00410	System Vulnerability Ticket	Rejected	Vulnerability Resolution	[redacted]	[redacted]	0	□ N/A	0%	2016-07-11 13:30:22	2016-08-10

Delegation

Any stakeholder of a stage that permits delegation can delegate to another user, the workflow designer can allow team Delegation at each stage. For example, the **In Progress** and **Review** stages may allow for delegation whereas the **Approval** stage might be designed not to allow delegation. The workflow designer can choose another label to describe delegation, such as "**Delegated To**" or "**Transfer Authority**" and can select an e-mail template used to notify the delegate.


Name: Default Ticket Workflow

Since: 2016-08-10 10:22:19

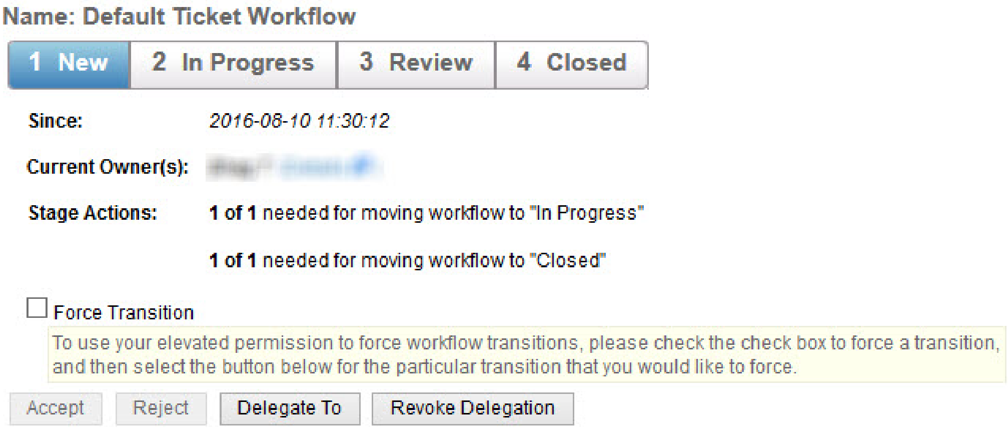
Current Owner(s): [redacted] (Details)

Stage Actions: **1 of 1** needed for moving workflow to "In Progress"

1 of 1 needed for moving workflow to "Closed"

Delegation Revocation

The original stakeholders shall be able to revoke a delegation at any time while an object is in a particular stage regardless of how many times delegation has occurred. This is true regardless of whether the current delegate is the same as the one the original stakeholders delegated to.


Name: Default Ticket Workflow

Since: 2016-08-10 11:30:12

Current Owner(s): [redacted]

Stage Actions: **1 of 1** needed for moving workflow to "In Progress"

1 of 1 needed for moving workflow to "Closed"

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

Forcing Stage Transition

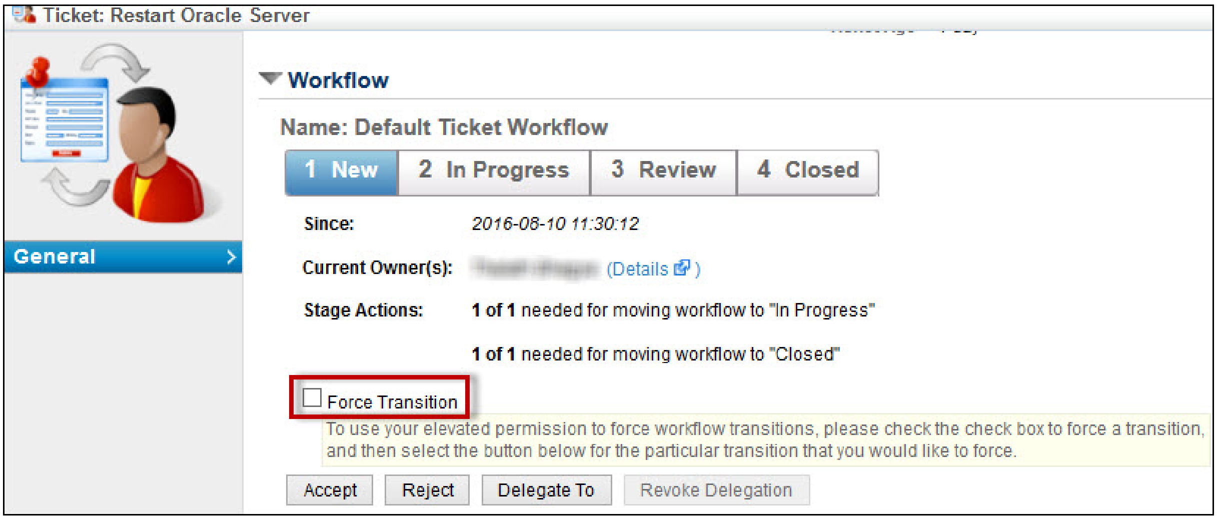
Any user with appropriate permissions can force the stage transition of a workflow, for objects such as tickets, exceptions, findings, or incidents, when the stage stakeholder do not transition the workflow to the next stage in time. Forcing the stage transition in a policy workflow requires that the user own the policy. That is, only a primary owner can force the transition. When a workflow stage is set to advance automatically to the next stage at a specified percentage or any or all of the stakeholders have performed a certain action, force transition will facilitate moving the stage even though the specified trigger may not have been achieved. The following table lists the objects and the permission or ownership criteria required to force a stage transition.

Object	Criteria
Ticket	Manage permission
Exception	Approve permission
Incident	Manage permission

To force a stage transition:

1. Select the object to open its details page.

2. In the **Workflow** section, check the box next to Force Transition, and click the desired action to complete the transition.



Ticket: Restart Oracle Server

Workflow

Name: Default Ticket Workflow

Since: 2016-08-10 11:30:12

Current Owner(s): [redacted] (Details)

Stage Actions: **1 of 1** needed for moving workflow to "In Progress"

1 of 1 needed for moving workflow to "Closed"

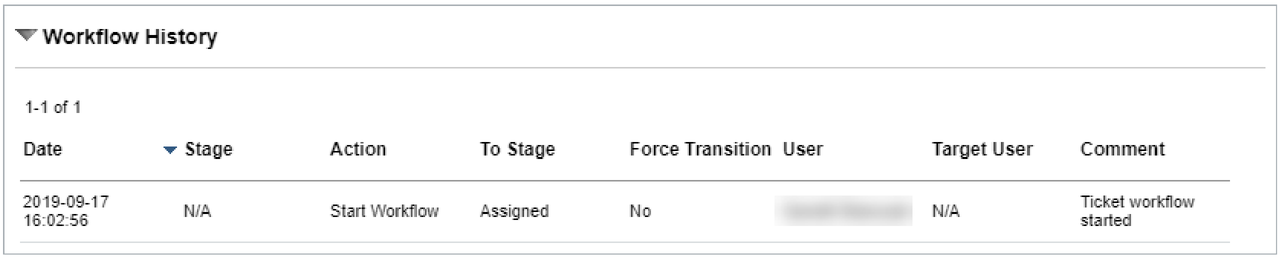
□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

Determining Stage Transition Mode

Users can transition the workflow stage if they are the stage stakeholder, or if they possess the ownership or appropriate permissions. The **Workflow History** section shows how ticket, exception, incident, and policy workflow stages were transitioned and by whom.

The **Force Transition** column indicates whether the transition was forced and the **User** column displays the stakeholder who completed the transition or action.



Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2019-09-17 16:02:56	N/A	Start Workflow	Assigned	No	[redacted]	N/A	Ticket workflow started

The Workflow History section.

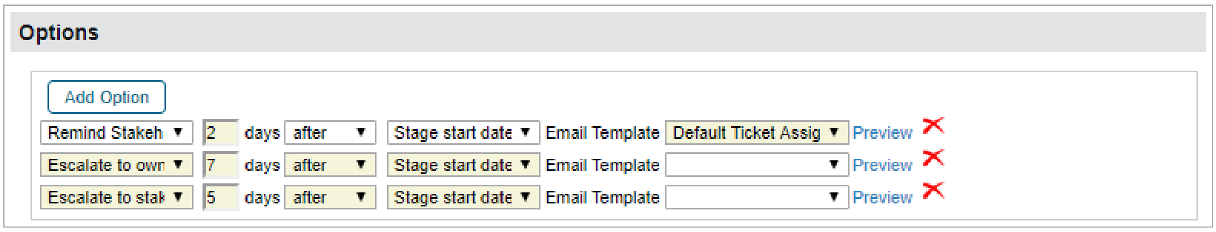
Manage Workflow Escalations

Workflow stages can be configured to send escalations to the program owner, the stakeholder’s manager, or both, for further action if the workflow does not advance to the next stage within a specified time. Each workflow stage can be configured separately with a number of days before automatic escalation. For example, you might configure a compliance assessment workflow to notify the program owner seven days after a questionnaire enters the Review stage. The notification email will use the Questionnaire Escalation template, and will only be sent if the questionnaire stays in the Review stage for more than seven days.

To configure escalations in a workflow:

1. Go to **Configuration** > **Workflows**, select a workflow, and then click **Details**.

2. Click a workflow stage, then click **Edit**.



Options

Add Option

Remind Stakeh ▼	2	days	after ▼	Stage start date ▼	Email Template	Default Ticket Assig ▼	Preview	✕
Escalate to own ▼	7	days	after ▼	Stage start date ▼	Email Template	▼	Preview	✕
Escalate to stak ▼	5	days	after ▼	Stage start date ▼	Email Template	▼	Preview	✕

The Options section.

3. Check the **Escalate to owner** or **Escalate to stakeholder's manager** to send notifications.
4. Enter the number of days, the date, and whether it should be sent before, after, or on the date.
5. Select the email template from the dropdown list to use for the notification. You have the option to send notifications to both the program owner and the stakeholder's manager.
6. Click **Save**.

If the ticket does not have an owner, configuring a ticket workflow for the escalate to owner option will not send notifications to a recipient. In a Policy workflow, selecting the **Escalate to Owner** option sends a notification to the policy's primary owner. If a stakeholder does not have a a manager, **Escalate to stakeholder's manager** will not send a notification.

To assign a manager to a stakeholder:

1. Open the RiskVision Administration application.

2. Click the **Users** tab.
3. Click the stakeholder's username to open their account.
4. Click **Edit**.
5. Click the **Manager** dropdown and select the appropriate user.
6. Click **Save**.

Notifying Assessment Owner

To notify the assessment owner, the stakeholders must access the assessment at the first stage of the workflow. If you are a program owner and want your assessment owners to receive notifications, you must perform the following steps before you create a program:

1. Go to the `%AGILIANCE_HOME%\config` directory, open the `agiliance.properties` file by using a text editor, and add the following properties:
    - `notify.assessment.owner.enabled=true` - set this property as 'true' to enable the effect of **Notify primary owner when assessment is accessed** option.
    - `com.agiliance.assessment.surveystart.notifyowner.emailTemplate=` - specify the email template's name with which you will want to notify stakeholders when a questionnaire is accessed first.
2. Restart the Tomcat application server to update to the latest changes.
3. Once the Tomcat application has restarted, open the assessment workflow details. Click**Edit** to bring the workflow into edit mode, scroll down to the details of the first stage, and select the box next to the **Notify primary owner when assessment is accessed** option.

When assessments are accessed for the first time, a notification is automatically sent to the primary owners of the respective assessments.

Specify Multiple Workflows

RiskVision allows you to switch between workflows. Different workflows can be selected based on the actual value of the runtime property. This is particularly useful for tickets, exceptions, and incident workflows. Multiple workflows allow you to create a fast track ticket workflow. For example, with a single workflow, a ticket would always use the default ticket workflow.

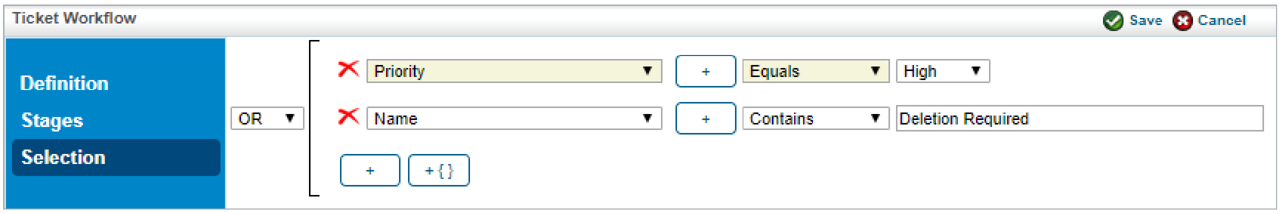
You can specify conditions under which the new workflow will be used in the **Selection** tab.

To define a selection condition:

1. Open a workflow that will be selected under certain conditions. Workflows without selection criteria will be selected by default, as before.

2. Click the **Selection** tab, then click **Edit**.

3. Select an attribute, operation, and value. For example, Priority Equals High.



Ticket Workflow

OR: Priority + Equals High

Name + Contains Deletion Required

The Selection tab in Edit mode.

4. Click **Save**.

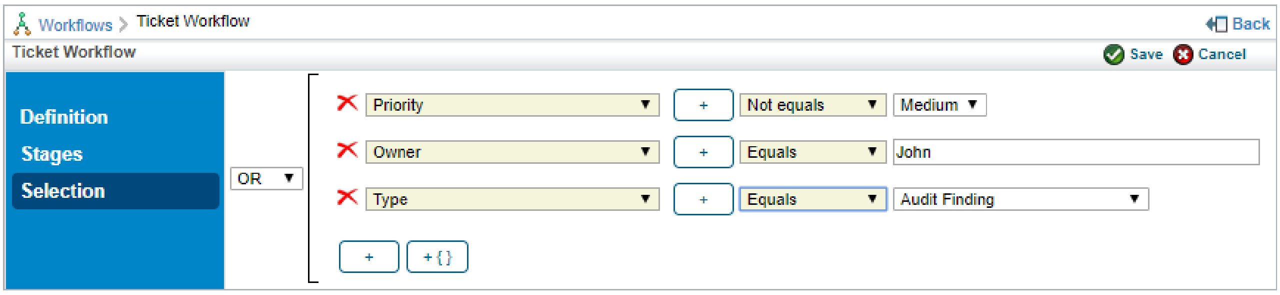
You can import the selection criteria of workflow templates created in RiskVision version 6.0 SP2 or higher.

Defining More Complex Selection Conditions

The Selection Criterion editor can be used to specify complex AND and OR conditions. In addition, parentheses can be used to specify sub-conditions.

For example, if you create three conditions, such as **Priority** =/= **Medium**, **Owner** = **John**, and **Type** = **Audit Finding**, you can choose:

CONJUNCTION	DESCRIPTION
AND	All conditions must be true to select this workflow.
OR	This workflow will be selected if any of the conditions are true.
XOR	Exclusive OR. Select the workflow if one of the conditions is true, but not if more than one is true.



OR

Priority + Not equals Medium

Owner + Equals John

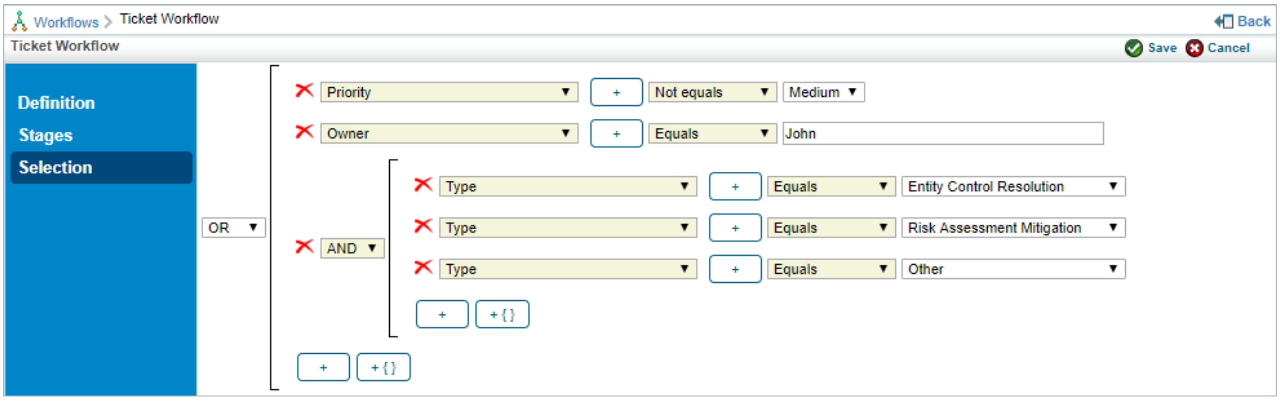
Type + Equals Audit Finding

The Selection Criterion editor.

Specifying Sub-conditions

EXAMPLE

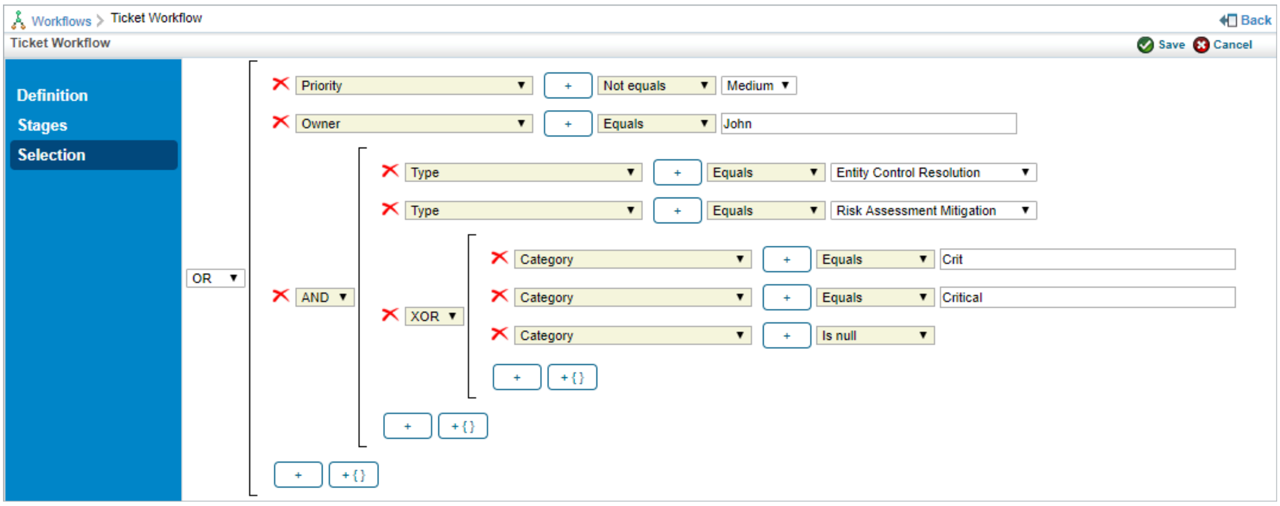
You want to select this workflow when**Priority > Medium**, when **Owner** is **John**, or when **Type** is **Entity Control Resolution**, **Risk Assessment Mitigation**, or **Other**. To specify the last three sub-conditions, you use the **+ { }** button.



OR
- Priority | Not equals | Medium
- Owner | Equals | John
- AND
  - Type | Equals | Entity Control Resolution
  - Type | Equals | Risk Assessment Mitigation
  - Type | Equals | Other

The Selection Criterion editor with sub-conditions.

Sub-conditions can be nested as deeply as necessary. The **OR** and **AND** of the first example might be inverted. You might want to select the workflow when **Priority > Medium** AND when one of a set of sub-conditions is true.



OR
- Priority | Not equals | Medium
- Owner | Equals | John
- AND
  - Type | Equals | Entity Control Resolution
  - Type | Equals | Risk Assessment Mitigation
  - XOR
    - Category | Equals | Crit
    - Category | Equals | Critical
    - Category | Is null

The Selection Criterion editor with two layers of sub-conditions.

In the previous example, the workflow will be selected only when**Priority** does not equal **Medium**, the **Owner** is **John**, and one of the following conditions is true. Either the **Category** is **Null**, it starts with **Crit**, or it ends with **Critical**. If the **Category** starts with **Crit** and ends with **Critical**, the workflow will not be selected because you used the Exclusive OR (**XOR**) operator.

Allowing Independent Stage Transitions

Questionnaires associated with an assessment can advance through workflow stages independently (although entities under assessment can be in different workflow stages, questionnaires had to transition workflow stages in unison in RiskVision solution before 4.1.version.)

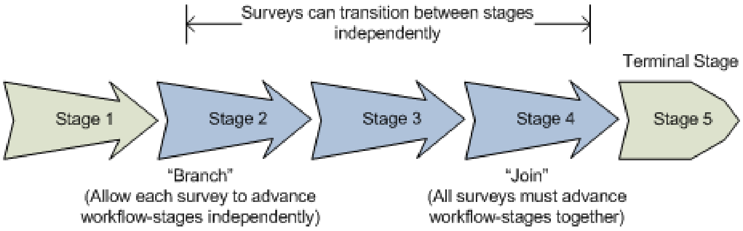
By default, questionnaires advance through workflow stages together. Questionnaires all start in the first stage of a workflow ("Information Gathering," for example) and must reach the Terminal stage together.

Relationships with a set of standard workflow templates, including " Assessments with Branching," which supports independent stage transitions. In addition, you can create custom templates that allow independent stage transitions, also known as branching.

Creating Workflows With Branching

Workflow stages have actions that transition questionnaires to different workflow stages. Typically, questionnaires advance through stages 1, 2, 3, and so on, but returning to previous stages is common. Review or Approval stages, for example, might include a ‘Reject’ action that reverts to an earlier workflow stage.

When you create a custom workflow template, specify the number of stages you would like and end with a Terminal stage. Each stage includes notification and other options. While planning your workflow template, decide which stages will allow questionnaires to advance independently and which will not. In a five-stage workflow, for example, you might allow independent movement in stages 2 through 4. To specify this, set stage 2 to “branch” and stage “4’ to “join” by selecting the “Allow each questionnaire to advance workflow-stages independently” option in stage 2 and selecting the “All questionnaires must advance workflow-stages together” option in stage 4.


Surveys can transition between stages independently
Terminal Stage
Stage 1
Stage 2
Stage 3
Stage 4
Stage 5
“Branch”
(Allow each survey to advance workflow-stages independently)
“Join”
(All surveys must advance workflow-stages together)

There are a few rules:

1. Every "branch" stage ("Allow each questionnaire to advance workflow-stages independently") must have a matching "join" stage ("All questionnaires must advance workflow stages together") later in the workflow.

2. A workflow can have more than one branch-join pair, but they cannot overlap.

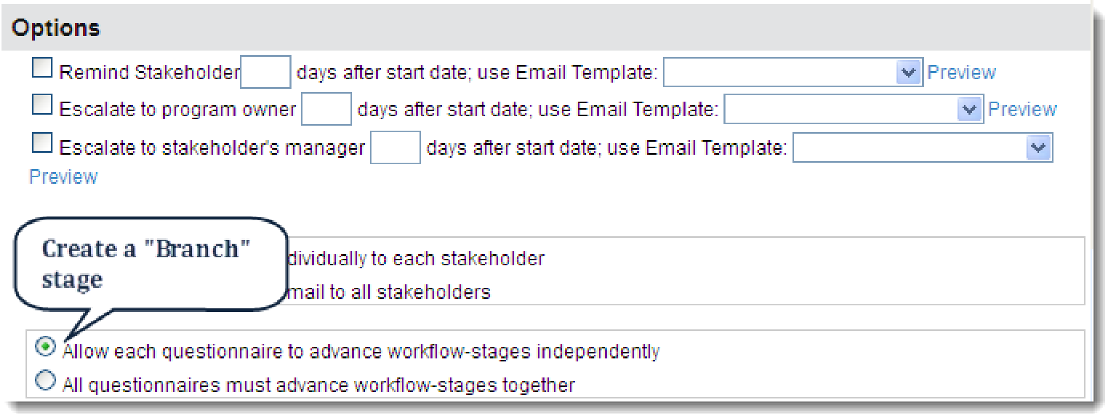
1 - 2 (branch) - 3 - 4 (join) - 5 - 6 (branch) - 7 - 8 (join) - 9 (terminal) <<OK

1 - 2 (branch) - 3 - 4 (branch) <<No, need to join the first branch before starting second branch

1 - 2 (branch) - 3 - 4 (terminal) <<No, need to join the branch before the terminal stage

3. A "branch" stage ("Allow each questionnaire to advance workflow-stages independently") can have actions that transition to stages before the branch stage, but no questionnaire will be able to advance past the "join" stage until all questionnaires have reached the "join" stage.

4. Stages after a "join" stage ("All questionnaires must advance workflow-stages together") cannot have actions that transition to stages before the "join" stage.



Options

□ Remind Stakeholder [ ] days after start date; use Email Template: [ ] Preview

□ Escalate to program owner [ ] days after start date; use Email Template: [ ] Preview

□ Escalate to stakeholder's manager [ ] days after start date; use Email Template: [ ] Preview

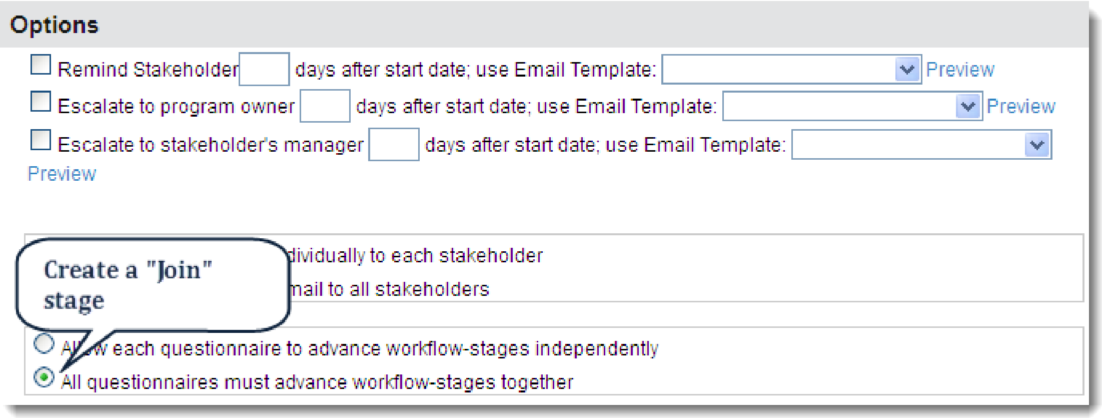
Create a "Branch" stage

dividually to each stakeholder

mail to all stakeholders

● Allow each questionnaire to advance workflow-stages independently

○ All questionnaires must advance workflow-stages together



Options

□ Remind Stakeholder ____ days after start date; use Email Template: ____ Preview

□ Escalate to program owner ____ days after start date; use Email Template: ____ Preview

□ Escalate to stakeholder's manager ____ days after start date; use Email Template: ____ Preview

dividually to each stakeholder

mail to all stakeholders

○ Allow each questionnaire to advance workflow-stages independently

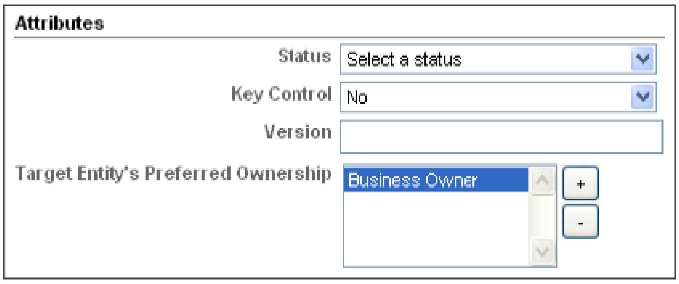
● All questionnaires must advance workflow-stages together

Preferred Ownership

Objects such as entities and controls have at least one owner. Object owners can be nominated as the primary stakeholders of any workflow stage so that the stakeholders can manage the objects in an assessment. Alternatively, you may also assess entities based on the controls, groups or control objectives with preferred ownerships that match the workflow stage owners and entity owners. Preferred ownership allows stakeholders to answer a questionnaire that is different from other stakeholder's questionnaires of the same program assessment. That is,\ preferred ownership allows the first stage of an assessment workflow to send a unique questionnaire to each stakeholder.

To implement preferred ownership efficiently, configure the following:

1. The control, control objective, content pack, or group must list the ownership type in the Target Entity’s Preferred Ownership field.



Attributes

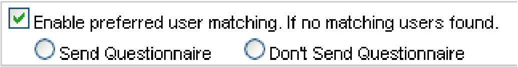
Status: Select a status

Key Control: No

Version:

Target Entity's Preferred Ownership: Business Owner

2. In the assessment workflow options, select **Enable preferred user matching** and indicate whether a questionnaire must be sent if the preferred user is not found for a particular entity.



☑ Enable preferred user matching. If no matching users found.

○ Send Questionnaire ○ Don't Send Questionnaire

If **Enable preferred user matching** is selected and no matching users are found, the default behavior is that the questionnaire will not be sent.

About Preferred Ownership Options

If your assessment is only valid when key object owners participate, you may want to skip sending a questionnaire when no preferred owners match. If any owner can answer when a preferred owner does not exist, send questionnaires even if no preferred owners match. Below are the preferred ownership options that explain whether to send a questionnaire if no matching users are found:

- Assess entities when control preferred owners and workflow stakeholders do not match.
    - Do not send questionnaires if no matching users are found. When you launch an assessment workflow, the RiskVision application will compare the preferred ownership of a control (group or control objective) with the stakeholders of a workflow stage, and if no match is found, controls are not created;meaning the controls are not listed in the assessment details tab of a program.
    - Send questionnaires if no matching users are found. When you launch an assessment workflow, the RiskVision application will compare the preferred ownership of a control (group or control objective) with the stakeholders of a workflow stage and if no match is found, it compares the workflow stage stakeholders with the entity owners. If a match is found, questionnaire is sent to the matched stakeholders to log the answer choice. Otherwise stakeholders can only view the questionnaire.
- Assess entities when control preferred owners and workflow stakeholders match.
    - When you launch assessment workflow, the RiskVision application will compare the ownership of an entity with the matched owners of a workflow stage and control (group or control objective), and if a match is found, a questionnaire is sent to the matched stakeholders to log the answer choice. Otherwise stakeholders can only view the questionnaire.

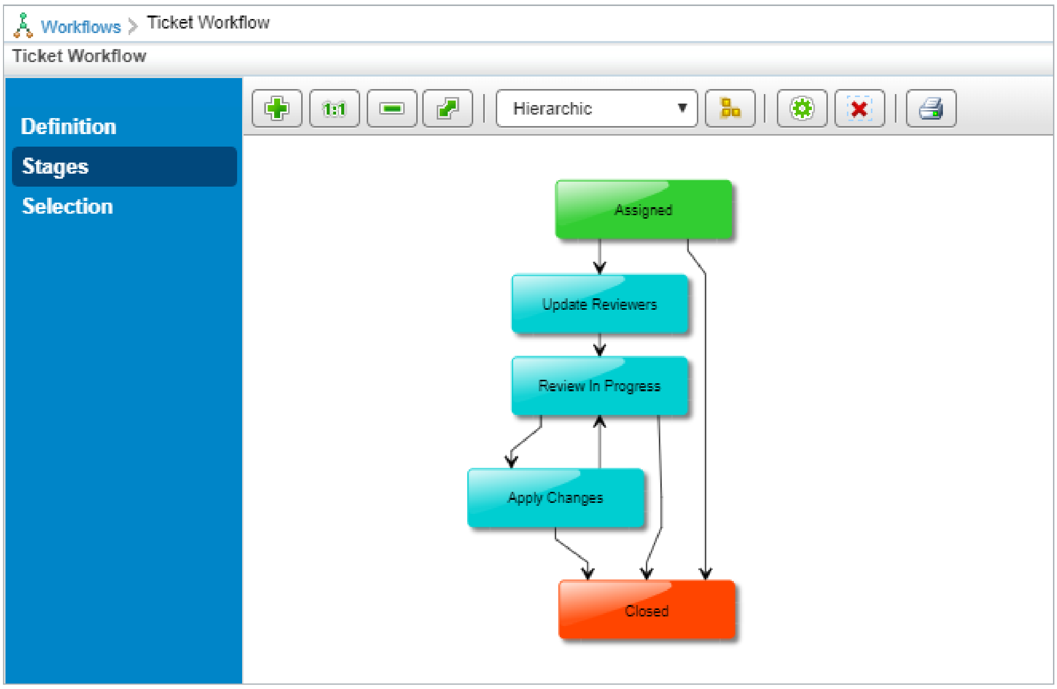
The preferred ownership feature works only in the first stage of assessment workflow that allows each questionnaire to advance the workflow-stages independently**.**

Assign the preferred ownership at the same level as the content added in a program. For example, if the preferred ownership is assigned to the content at the group level, assign the content to the program at the group level. If the preferred ownership is assigned to the content at the control level, assign the content to the program at the control level**.**

Visualizing Workflows

Workflows can be simple or complex, ranging from a few stages with sequential transitions to 20 or more stages with transitions that skip stages and go back to previous stages. For simple workflows, the **Definition** tab allows you to add and configure stages and helps you quickly grasp the stage transitions and the overall behavior.

For workflows with multiple stages, you must be precise in setting up each stage and test the workflow to ensure the behavior is as expected. The **Stages** tab can be used to gain a quick understanding of complex workflows. It shows all stage transitions, both forward and backward, and not just the sequential transitions, and allows workflows to be visualized in graphical layout.

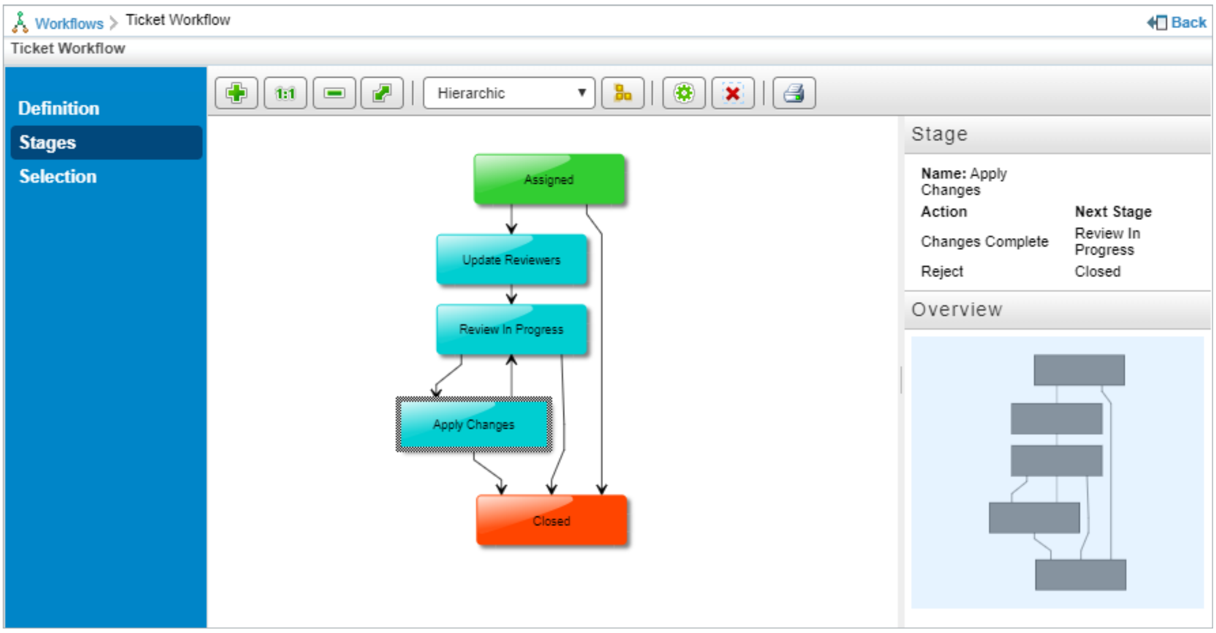


The Stages tab.

For information about the tool options, see Visualizing Objects.

The following is an explanation of the various elements of the **Stages** tab:

- The rounded rectangle in the graph represents the stages in a workflow.
- The incoming and outgoing arrows represent the transitions and indicate that transitions happen only between those stages. The direction of the arrow shows whether the transition is forward or backward.
- The **Stage** pane displays the stage information. Click a stage to view the action and the stage that a workflow will enter when that action is performed by the stakeholder.



Name: Apply Changes	
Action	**Next Stage**
Changes Complete	Review In Progress
Reject	Closed

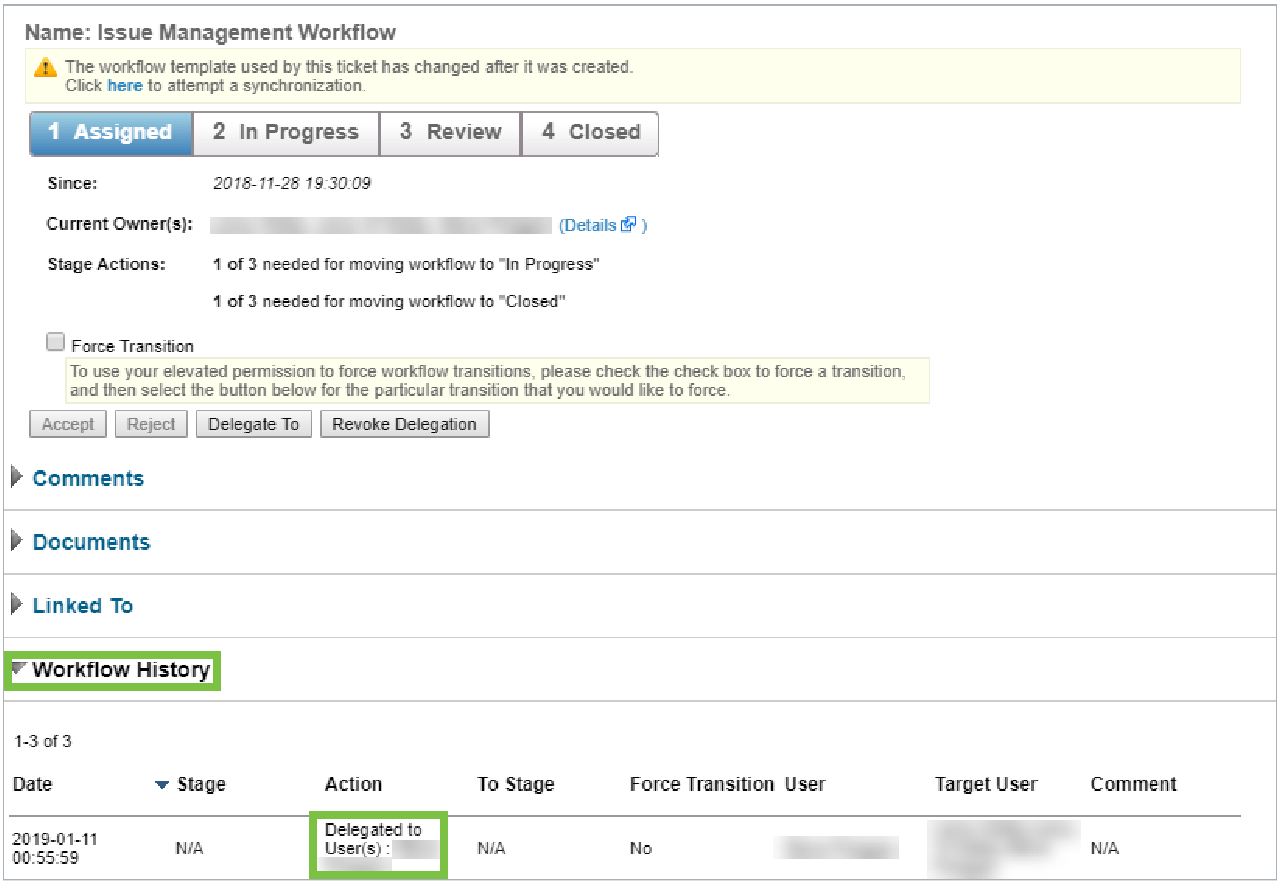
The Stage pane when the Apply Changes stage has been selected.

- The **Overview** pane allows you to move the workflow layout in different directions. For more information, seeMoving the Layout.

Delegation & Delegation Revocation

Users with Manage permissions on an object can read, create, modify, and update instances of that object. These users can also delegate, revoke delegation, and force workflow transitions. Workflow stages can be delegated to any RiskVision user or team. In order to delegate a stage in the workflow, delegation must be enabled. Delegation and delegation revocation is controlled on a per-stage basis by the **Allow Delegation** option.

It's good practice to add a comment/reason for delegation or revoking delegation in the **Comment** section. The comments added are visible to all users who have read access to the Workflow tab of the object and can view the comments in the **Workflow History** section as show below.



Name: Issue Management Workflow

⚠ The workflow template used by this ticket has changed after it was created.
Click here to attempt a synchronization.

Since: 2018-11-28 19:30:09

Current Owner(s): [redacted] (Details)

Stage Actions: 1 of 3 needed for moving workflow to "In Progress"

1 of 3 needed for moving workflow to "Closed"

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

1-3 of 3

Date	Stage	Action	To Stage	Force Transition	User	Target User	Comment
2019-01-11 00:55:59	N/A	Delegated to User(s) : [redacted]	N/A	No	[redacted]	[redacted]	N/A

The Workflow History section of a delegated workflow.

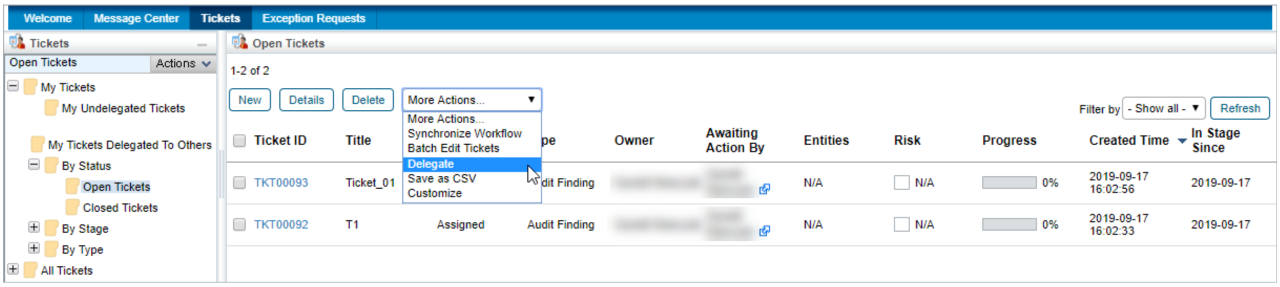
The delegation option that is discussed in this section is available for the below objects:

> Not all of the below objects will be available in each application.

- Tickets
- Findings
- Incidents
- Exception Requests
- Controls
- Policies

For **Tickets**, **Findings**, **Incidents** and **Exception Requests**, workflow stakeholders can view delegated objects in the **My Tickets Delegated To Others**, **My Findings Delegated to Others**, **My Incidents Delegated to Others** and **My Exceptions Delegated to Others** column of their respective grids.

For **Tickets**, **Findings**, **Incidents**, and **Exception Requests,** stakeholders can perform bulk delegation and delegation revocation from the **More Actions** dropdown list.

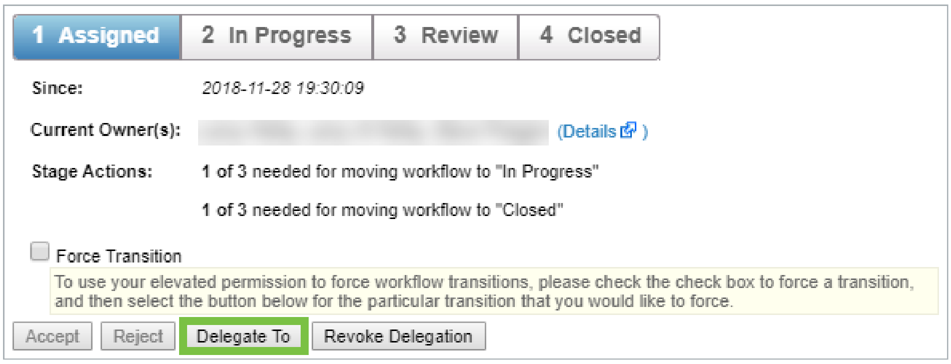


□	Ticket ID	Title		pe	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
□	TKT00093	Ticket_01		dit Finding	[redacted]	[redacted]	N/A	□ N/A	0%	2019-09-17 16:02:56	2019-09-17
□	TKT00092	T1	Assigned	Audit Finding	[redacted]	[redacted]	N/A	□ N/A	0%	2019-09-17 16:02:33	2019-09-17

The Delegate option in the More Actions dropdown.

Delegation

Any stakeholder of a stage that permits delegation can delegate to another user. The workflow designer can allow team Delegation at each stage. For example, the **In Progress** and **Review** stages may allow for delegation, whereas the **Approval** stage might be designed not to allow delegation. The workflow designer can choose another label to describe delegation, such as "Delegated To" or "Transfer Authority" and can select an email template used to notify the delegate.



Since: 2018-11-28 19:30:09

Current Owner(s): [redacted] (Details)

Stage Actions: 1 of 3 needed for moving workflow to "In Progress"

1 of 3 needed for moving workflow to "Closed"

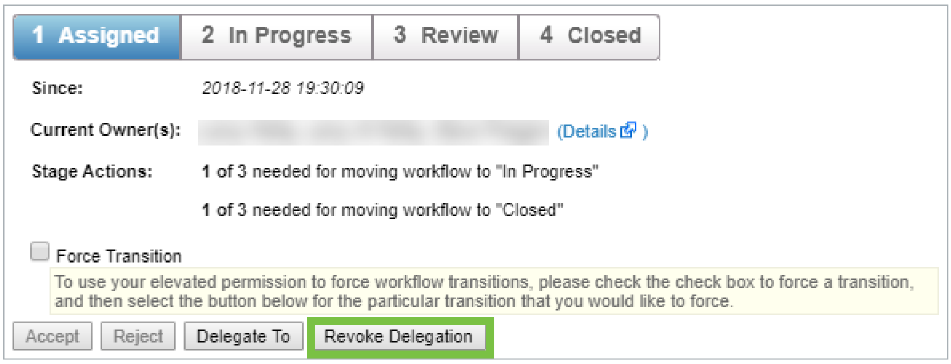
□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

The Delegate To button.

Delegation Revocation

The original stakeholders can revoke a delegation at any time, regardless of how many times delegation has occurred. This is true regardless of whether the current delegate is the original delegate.



Since: 2018-11-28 19:30:09

Current Owner(s): [redacted] (Details)

Stage Actions: 1 of 3 needed for moving workflow to "In Progress"

1 of 3 needed for moving workflow to "Closed"

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

The Revoke Delegation button.

Escalation

Escalation configurations allow you to control e-mail messages sent when a Tickets due date has passed. Three levels of escalation are supported, each with distinct evaluation criteria, recipients, and e-mail templates.

By default, RiskVision provides a single level escalation that sends an e-mail to the ticket's Owner Manager one day after the ticket is due. This escalation uses the Default Escalation E-mail Template by default. You can define additional levels, additional escalations, and individual and team recipients.

For more information about the e-mail template associated with each level of an escalation, seeAbout E-mail Templates.

To manage escalation configurations, go to **Configuration**> **Escalation**.

Creating an Escalation Configuration

Escalation configurations define what happens when a ticket is overdue. Selected recipients are notified using an e-mail template.

If your escalation requires a custom e-mail template, create the e-mail template.

You can create, update, or delete an escalation if your user role has Email Template View and Email Template Manage permissions.

To create a new escalation configuration:

1. Go to **Configuration** > **Escalation**.
2. Click **New**.
3. Enter the **General** settings as follows:
   - Name. Enter the display name that users will use to identify this escalation configuration.
   - Description. Enter a summary that will be visible only on the escalation page.
4. Create an escalation for Level 1 by clicking **New** in the **Escalations** section. You can repeat these steps to create escalations for Level 2 and 3 later, if desired.
5. Enter the **Escalation** settings as follows:
   - Escalation Level. Choose 1 for the first response to an overdue ticket. To create a different response if the ticket remains overdue, create a second Escalation with Level 2.
   - E-mail Template. Select from the list of available e-mail templates. Click Previewto see how the e-mail will look.
   - Escalation Date. The number of days after the ticket is due that triggers this message. Level 1 might be triggered 1 day after a ticket's due date while Level 2 is triggered a few days later. Level 3, if required, would be triggered later.
   - Recipients. Check Requester, Owner Manager, or select individuals or teams to receive this message.
6. Click **OK**.
7. Click **Save** to save the new escalation configuration.

About Email Templates

Use customized e-mail templates to include organization-specific details in messages sent to stakeholders during assessments, ticket resolution, and other processes.

Resolver uses the Velocity template engine to generate workflow and system messages. You can use some basic Velocity syntax and parameters to insert context data, such as the user's name, program name, program owner name, entity name, and dates and deadlines. For example, "Hi $Username" inserts the actual stakeholder's first and last name into the message.

Default Email Templates

The default template types are available for your use depending on the RiskVision solution. Resolver provides the following default templates:

Name	Type	Description
Alert Notification (HTML)	Alert	Used to notify users that a compliance, control or risk score has crossed a specified threshold.
Alert Notification	Alert	Used to notify users that a compliance, control or risk score has crossed a specified threshold.
Default Escalation	Escalation	This template is used for sending an escalation notification.
Default Ticket Escalation Template	Ticket	The default template used when tickets themselves are escalated.
Default Ticket Assignment	Ticket	This template is used when a new ticket has been launched.
Exception Delegation	Exception	This template is used when an exception is delegated from one user to another user.
Exception Escalation	Exception	This template is used to remind user that the exception assigned to them is past the due date.
Exception Expire	Exception	This template informs a user that an exception has expired.
Exception Reminder	Exception	This template is used to remind user about upcoming exception due dates.
Exception Review	Exception	This template is used when an exception is ready for review.
Exception Review Rejection	Exception	This template is used when an exception is rejected during review.
Exception Signoff	Exception	This template is used when an exception is ready for sign-off.
Exception Signoff Rejection	Exception	This template is used when an exception sign-off was rejected.
Incident Closed	Incident	Notifies users that an incident is closed.
Incident Delegation	Incident	This template is used when an incident is delegated from one user to another .
Incident Detected	Incident	Notifies that an incident is detected.
Incident Escalation	Incident	This template is used to remind users that the incident assigned to them is past the due date.
Incident Reminder	Incident	This template is used to remind user about upcoming due dates on incidents.
Incident Review	Incident	This template is used when an incident is ready for review.
Incident Review Rejection	Incident	This template is used when an incident is rejected during review.

Name	Type	Description
Incident Signoff	Incident	This template is used when an incident is ready for sign-off.
Incident Signoff Rejection	Incident	This template is used when an incident sign-off is rejected.
Out of Office Delegation	Access Delegation	This template is used to notify users of assigned access delegations.
Report or Dashboard Delivery	Analytics	This template is used when a report or dashboard is sent to the user.
Threats Advisory Alerts	Alert	Used to notify users when new threats or vulnerabilities are reported by security research organizations.
Ticket Assignment Notification	Ticket	Notifies a user they have been assigned a ticket.
Ticket Update Notification	Ticket	Notifies the ticket owner when the ticket is updated.
Ticket Closed	Ticket	Sends notification that a ticket was closed.
Ticket Delegation	Ticket	Sends notification that a ticket was delegated from one user to another user.
Ticket Escalation	Ticket	Used to alert users that the tickets are assigned to them after the due date is passed.
Ticket Reminder	Ticket	Reminds a user about upcoming due dates on tickets.
Ticket Review	Ticket	Sends notification that a ticket is ready for review.
Ticket Review Rejection	Ticket	Sends notification that a ticket was rejected during review.
Vulnerability Assignment Notification	Alert	Used to notify a user that they have become the owner of a vulnerability.

Configuring Email Templates

This section explains how to create, delete, and modify an e-mail template. On the **Configuration** menu, click **Email Templates** to view default and custom created template types. To view email templates, you must have the Email Template View permission, and in order to create, delete, or modify them, you must have the Email Template View and Email Template Manage permissions.

The following describes the available email template types:

- **Access Delegation**. Used when notifying users of assigned access delegations.
- **Analytics.** Available for selection in the Administration application when a report or dashboard is sent to the user.
- **Ticket.** Available for selection in the ticket workflow.
- **Incident.** Available for selection in the incident workflow.
- **Exceptions.** Available for selection in the exception workflow.
- **Alerts.** Sent for events, such as an entity scoring higher for risk or compliance than the threshold.
- **Escalation.** Used when ticket deadlines are reached.
- **Reports.** Sent for report notifications.

Updating Email Template

Modifications to email templates take effect immediately.

To update an e-mail template:

1. Go to **Configuration**> **Email Templates**.
2. Select a template and then click **Details**.

   The template opens in a pane below the grid.
3. Click **Edit**.
4. In the **General** section, edit the following settings:
   - **Display Name**. Enter the short name for the template.
   - **Template Type.** Select the workflow type.
   - **Content Type**. Select either HTML or Plain text content type of a template.
   - **Description**. Enter information that will help others understand the use of the template.
   - **Send Immediately. Select to send the notifications without sequencing.**
   - **High Priority**. Select to send the notifications with high importance.
   - **Sender Email Account**. Select the email account of the sender to send the notifications. By default, the RiskVision administrator's email account is used for sending email notifications.
   - **Template text**. Author information that suits the template type.
5. When you finish modifying the template, click **Save**.

The new template is now available.

Adding A New Customized E-mail Template

Users with sufficient privileges can create new e-mail templates for later use.

To create an e-mail template:

1. In RiskVision Incident Manager, go to **Configuration** > **Email Templates**. In the Administration application, go to **Administration** > **Email Templates**.

2. Click **New**.

3. In the **General** section, enter the following fields:

   - **Name.** Enter the display name that users select when setting up a workflow.
   - **Template Type.** Select the workflow type.
   - **Content Type.** Select either HTML or Plain text content type of a template.
   - **Description.** Enter information that will help others understand the use of the template.
   - **Send Immediately**. Select to send the notifications without sequencing and/or merging. See also Sequencing and Merging of Email Notifications.
   - **High Priority**. Select to send the notifications with high importance. By default, all of the escalation email templates are sent with high priority.
   - **Sender Email Account**. Select the email account of the sender to send the notifications. By default, the administrator email account is used for sending email notifications.

4. Enter the message content.

   Resolver recommends basing new templates on one of the defaults.

5. Click **Save**.

The email template is now available for selection in workflow templates.

To understand how an email template can be used to notify the stakeholders, see Setting up Email Notifications.

Updating Email Templates

Modifications to email templates take effect immediately.

To update an email template:

1. Go to **Configuration**> **Email Templates**.
2. Select a template and then click **Details**. The template opens in a pane below the grid.
3. Click **Edit**.
4. In the **General** section, edit the following settings:
   - **Display Name**: Enter the short name for the template.
   - **Template Type**: Select the workflow type.
   - **Content Type**: Select either HTML or Plain text content type of a template.
   - **Description**: Enter information that will help others understand the use of template.
   - **Send Immediately**: Send notifications without sequencing.
   - **High Priority**: Send notifications with high importance.
   - **Sender Email Account**: Select the email account that will send the notifications. The RiskVision administrator's email account is used by default.
   - **Template text**: Author information that suits the template type. Text can be formatted using HTML.
5. When you finish modifying the template, click **Save**.

Adding a New Customized Email Template

Users with sufficient privileges can create new e-mail templates for later use.

To create an e-mail template:

1. In the RiskVision application, go to Configuration > Email Templates. In the Administration application, go to Administration > Email Templates.

2. Click New.

3. In the General section, enter the following fields:

    - Name. Enter the display name that users select when setting up a workflow.

    - Template Type. Select the workflow type.

    - Content Type. Select either HTML or Plain text content type of a template.

    - Description. Enter information that will help others understand the use of the template.

    - **Send Immediately**. Select to send the notifications without sequencing and/or merging. See also Sequencing and Merging of Email Notifications.

    - **High Priority**. Select to send the notifications with high importance. By default, all of the escalation email templates are sent with high priority.

    - **Sender Email Account**. Select the email account of the sender to send the notifications. By default, the administrator email account is used for sending email notifications.

4. Enter the message content.

    Resolver recommends basing new templates on one of the defaults.

5. Click Save.

The email template is now available for selection in workflow templates.

To understand how an email template can be used to notify the stakeholders, see Setting up Email Notifications.

Email Template Variables

The system automatically replaces the variables in the following sections with the corresponding value when the notification or email is sent.

In designing your own email template or modifying those provided, use the default templates as a guide to what variables are available for different types of email template and for how they are used.

- Alert Email Templates
- Assessment Email Templates
- Analytics Email Templates
- Exception Email Templates
- Finding Email Templates
- Incident Email Templates
- Risk Email Templates
- Ticket Email Templates
- Vendor Email Templates
- More Variables

Alert Email Templates

The following variables are available to designers of this type of email template:

VARIABLE	DESCRIPTION
details	Includes properties and methods that describe the details of the alert of which the user is being notified. For example, `details.alertRule` is one property. Alert rule is itself an object, comprised of the properties name and description. So, to cause an Alert email template to display the name of the alert rule that triggered the notification, the designer would specify $details.alertRule.name.
details.alertRule.description	The description of the alert rule that triggered an email notification.
details.alertRule.name	The name of the alert rule that triggered an email notification.

Analytics Email Templates

The following variables are available for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
objectValue	The name of dashboard or chart.
passwordProtectedStatement	The password to open the report.
appurl	The URL of the RiskVision application.

Exception Email Templates

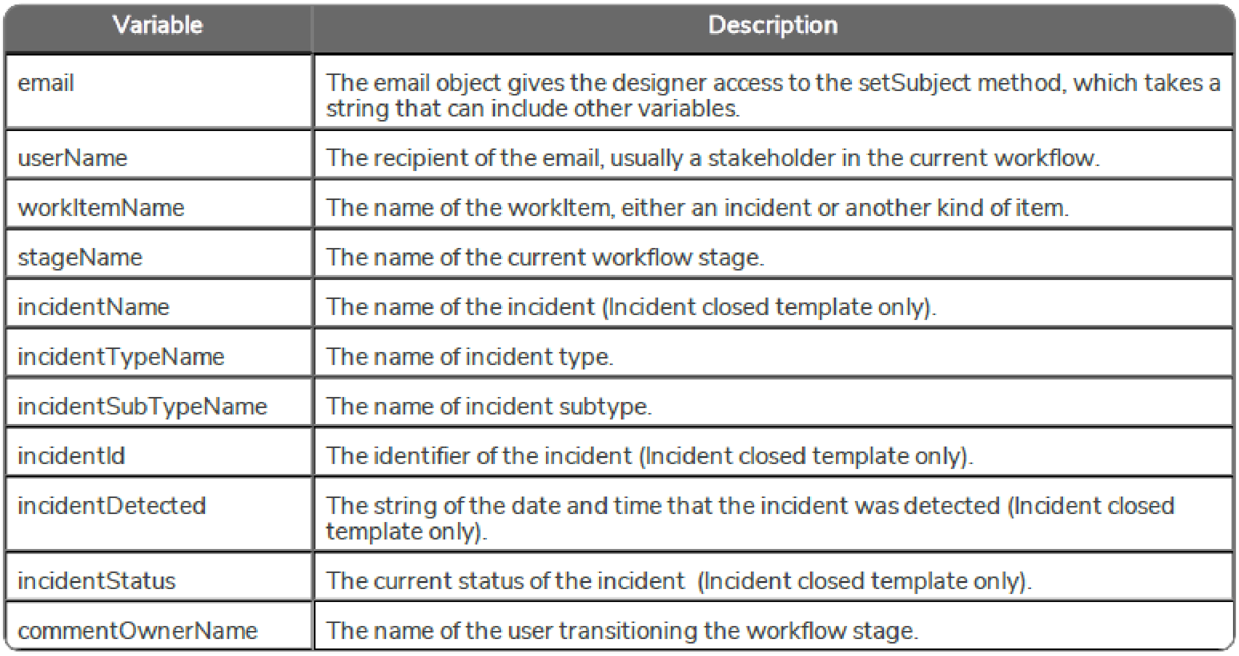
The following variables for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either a Control, a Subcontrol, or another kind of item.
stageName	The name of the current workflow stage.
xceptionName	The name of the exception (Exception expire template only).
exceptionEndDate	The expiration date of the exception (Exception expire template only). SeeModifying a Variable Displaying Date.
ownerName	The owner of the exception (Exception expire template only).
commentOwnerName	The name of the user transitioning the workflow stage.

You can add the $exceptionId variable in any exception email template type to display the exception ID.

Incident Email Templates

The following variables are available to designers of this type of email template:



Variable	Description
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either an incident or another kind of item.
stageName	The name of the current workflow stage.
incidentName	The name of the incident (Incident closed template only).
incidentTypeName	The name of incident type.
incidentSubTypeName	The name of incident subtype.
incidentId	The identifier of the incident (Incident closed template only).
incidentDetected	The string of the date and time that the incident was detected (Incident closed template only).
incidentStatus	The current status of the incident (Incident closed template only).
commentOwnerName	The name of the user transitioning the workflow stage.

Ticket Email Templates

The following variables are available for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
userName	The recipient of the email, usually a stakeholder in the current workflow.
workItemName	The name of the workItem, either a ticket, or another kind of item.
ticketID	The ID of the ticket.
ticketName	The name of the ticket.
ticketPriority	The priority of the ticket (low, medium, high, and so on).
ticketDue	The string of the date that the ticket is due. SeeModifying a Variable Display Date.
ticketStatus	The current status (workflow stage) of the ticket.
ticketDescription	The description of the ticket.
notificationDescription	The description of this ticket notification (Ticket Update Notification templates only).
ticketAttributeChangeDetails	The old and new values of changed attributes (Ticket Update Notification templates only).
commentOwnerName	The name of the user transitioning the workflow stage.

More Variables

The following variables are available for email templates to help point stakeholders to the user interface in which the action is required.

VARIABLE	DESCRIPTION
$NT.getObjectUrl("objectName")	Use this variable in an email template to direct users to the default tab of an object. For example, $NT.getObjectUrl("RAProject").
$NT.getObjectUrlWithTab("objectName", "tabName")	Use this variable in an email template to direct users to a tab available on an object details page. For example, $NT.getObjectUrlWithTab("Assessment", "Control Results").
$NT.getQuestionnaireUrl()	Use this variable in an email template to direct users to the Questionnaire window. This variable must be specified in the email templates defined in the first stage of the assessment workflow.

Modifying a Variable Display Date

Although, variables, such as $ticketDue and $exceptionEndDate will display the date in the 'MM/dd/yyyy hh:mm:ss' format when the notification is sent to the workflow stage stakeholders, you can also use the $dateTool velocity template variable to display an alternative format to the default date format. To change the date format in the email template, use the following code corresponding to the format and replace the code with the email template variable:

For $ticketDue variable

- Date and time - `$dateTool.format('MM/dd/yyyy hh:mm:ss',$ticketDue)`
- Date - `$dateTool.format('MM/dd/yyyy',$ticketDue)`

For $exceptionEndDate variable

- Date and time - `$dateTool.format('MM/dd/yyyy hh:mm:ss',$exceptionEndDate)`
- Date - `$dateTool.format('MM/dd/yyyy',$exceptionEndDate)`

Adding Object Fields in the E-mail Templates

You can add fields from an object's details page as workflow-type variables in stakeholder notifications. You can even include custom attributes that you have added to the objects. The following field types can be added to any email template:

FIELD TYPE	VARIABLE
String	$NT.getValue(".customAttributes.")
Number	$NT.getValue(".customAttributes.")
Boolean	$NT.getValue(".customAttributes.")
Date	$NT.getValue(".customAttributes.")

Add Custom Attributes to Email Templates

Any custom attribute supported by RiskVision can be added as a variable to an email template. The following attribute types can be added:

ATTRIBUTE	VARIABLE	DESCRIPTION
Date	$NT.getValue(".customAttributes.")	The date and time in the YYYY-MM-DD HH:MM:SS format by default.
Encrypted string	$NT.getValue(".customAttributes.")	A string value in encrypted format.
Flag	$NT.getValue(".customAttributes.")	Boolean values.
Image	$NT.getValue(".customAttributes.")	An image that can be displayed in the email.
Number	$NT.getValue(".customAttributes.")	Positive and negative numbers, including zero.
Rational number	$NT.getValue(".customAttributes.")	Positive and negative integers displayed as fractions.
String	$NT.getValue(".customAttributes.")	Multiple characters.
Text	$NT.getValue(".customAttributes.")	Character strings and HTML formatting.

Getting Familiar with Email Notifications

RiskVision notifies system users by email under a variety of circumstances. The user who receives the email notification is almost always determined by the entity or other object ownership.

NOTIFICATION	EMAIL TEMPLATE	RECIPIENTS
Assessment Workflow Started	Assessment Launch, Classification Assessment Launch, ERM Assessment Launch, and Risk Assessment Launch	Stakeholders are always notified. Stakeholders includes 'Primary Owner' by default.
Assessment Restart An assessment is automatically restarted based on recurrence rules	Assessment Recurrence	All stakeholders in the initial stage that are tagged with the notify icon.
Exception Workflow Started	Optional **Do Not Send Email** is the default.	Exception requester is the only stakeholder if **Notify selected stakeholder** is checked.
Ticket Workflow Started	Optional No pre-defined templates.	If **Notify selected stakeholder** is checked.
Workflow Action An action changes a workflow to a new stage.	User-selected. Note: Pull down list for Policy workflow is 'Content Pack' choice. Assessment Review, Assessment Review Rejection, Assessment Signoff, Assessment Signoff Rejection, Ticket Review, and Ticket Review Rejection.	All stakeholders of the stage before the change.
Escalate (optional) The escalations for different objects can be sent based on the available different date types.	User-Selected Email Template	Escalates to the stakeholders in the current workflow stage. See the note at the end of this section.
Reminder The reminders for different objects can be sent based on available different date types.	User-Selected Email Template	Reminds all stakeholders in the current workflow stage. See the note at the end of this section.
Ticket Created	Default Ticket Assignment	The user assigned to the ticket.

Exception or Ticket Delegated	Exception Delegation and Ticket Delegation	The new assignee.
Ticket Exception Expiration Date in a ticket's 'Exception Expiration' field has passed.	Specified in the `ticket.exception.expired.notification.template` Property	All stakeholders of the current stage.
Vendor Account Created	New Vendor Contact Notification	New vendor user.
Assessment is Accessed (Optional in all except terminal stages) Assessment is accessed when questionnaire is opened.	N/A	Primary owner. If the primary owner is removed from list of stakeholders, no email is sent.
Score Crosses a Threshold A control, compliance, or risk score crosses a specified threshold.	Alert Notification	Selected in the alert rule.
A Scheduled Job Completes Successfully	Scheduled Job Completed Successfully	Specified email user.
A Scheduled Job Fails	Scheduled Job Failed	Specified email address.
A Dashboard or Report is Sent to the User	Report or Dashboard Delivery	The original requestor.
Risk Created	Risk Identified	Owner.
New Threats or Vulnerabilities are Reported New threats or vulnerabilities are reported from a security research organization.	Threats Advisory Alerts	Control/entity owner.
User Account Delegation Notify users of assigned	Out of Office Delegation	The user who has been designated as a delegate.

access delegations.		
Content has Been Changed	Questionnaire Changed Notification	Stakeholders in the current workflow stage.

Workflow escalation and reminders can be sent as one email to all (single email to all stakeholders) or one email to each (email individually to each stakeholder).

Filters

A filter contains a set of conditions used by reports to match records and dynamic groups to limit membership, and to limit user access, amongst other things. Filter types include Assessment, Dynamic Group, Entity, Exception Request, Incident, Program, Response, Risk, and others.

The following describes the options on the filter page:

- Filter conditions. Options for creating operands:
    - Field. Displays a list of available fields for the type of filter that you selected.
    - Comparison Op. Displays a list of logical operators that you can select to build a filter condition.
    - Value. The string, number, or other value types that you want to match. To match a user, see User Variables.
    - Perform a case sensitive comparison. Consider the case of strings.
    - Use this condition as a parameter to a chart. Allows users to drill down to the record level of this field.
- Conjunctions. Joins operands in truth tables.

About Filter Data Types

The properties of a field describe the characteristics and behavior of data added to that field. A field's data type is the most important property because it determines what kind of data the field can store. This article describes the data types and other field properties.

Fields contain the following types of data:

Data types	Description
string	Field contains characters, symbols, or numbers.
float, integer, short, long	Field contains a numeric value.
timestamp	Field contains a date. Select the day and time using the calendar widget.
boolean	Field contains true or false.

About Comparison Operators

Comparison operators, as their name implies, allow you to compare two values. Comparison operators are used in logical statements to determine equality or difference between variables or values.

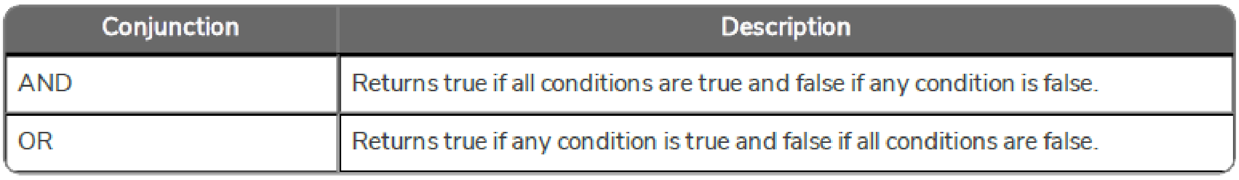
To use a comparison operator, you need to specify the values that you want to compare together with an operator that separates these values. When the input is a collection of values, the comparison operators return any matching values. If there are no matches in a collection, comparison operators do not return anything.

The following table describes the comparison operators:

Operators	Data type	Description
Equals	all	Exactly matches the value. For Tags and Organizational Nodes, use Contains, not ==.
Not equals	all	Any that do not exactly match.
Greater than	float, integer, short, long, timestamp	Definition is higher than the number that you entered.
Greater than or equal	float, integer, short, long, timestamp	Definition is similar or higher than the number that you entered.
Less than	float, integer, short, long, timestamp	Definition is lower than the number that you entered.
Less than or equal	float, integer, short, long, timestamp	Definition is similar or lower than the number that you entered.
Between	string	Value is between two values. (Selecting this Comparison op displays a second value field).
Contains	string	Definition contains the exact phrase that you entered. For example: 'al' matches alright and minimal but not.
Starts with	string	Definition begins with the exact phrase that you entered. For example: 'al' matches alright, but not minimal and.
Ends with	string	Definition ends with the exact phrase that you entered. For example: 'al' matches minimal, but not alright.
Matches filter	string	Allows one filter condition to reference another filter.
Is Null/Is Not Null	all, except boolean	The field, is defined or not defined.

About Conjunctions

Join operands to create a truth table as follows. A single filter can mix AND and OR conjunctions, but the results may not match the author's intent, due to precedence rules. The expression X AND Y OR Z can be interpreted as true only when X and either Y or Z are true, or it can be interpreted as true when either Z or both X and Y are true. Avoid mixing both conjunctions in the same filter. Instead, create two filters and use the 'Matches filter' operator to combine them.



Conjunction	Description
AND	Returns true if all conditions are true and false if any condition is false.
OR	Returns true if any condition is true and false if all conditions are false.

For users, other than the RiskVision administrator, filters can be viewed on the Configuration > Filters menu with the Filter View permission. Creating, modifying, or deleting a filter requires you to have the Filter View and Filter Update permissions.

Adding a Filter

This article explains how to add a filter without conditions. Typically, a filter without any conditions matches all records.

To create a new filter:

1. In the RiskVision application, go to **Configuration** > **Filters**. In the Administration application, go to **Users** > **Filters**.
2. Expand the **Filter** groups to select a specific group to which you want to add the filter.
3. Click **New**. The **New Filter** dialog appears.
4. Enter the general information:
    1. Enter **Name** and Description.
    2. Select the filter type and then click **OK**.

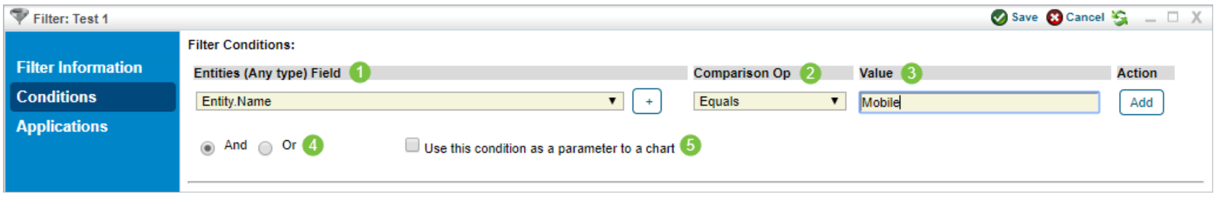
The filter is available for assignment.

Modifying Filter Conditions

This article explains how to add or remove a condition. Changes are applied the next time a report is run or a dashboard is updated. The new settings are used and user access filters are applied the next time the user logs in.

To add a condition:

1. Go to **Configuration** > **Filters**.
2. Expand the **Filters** tree.
3. Select a filter to open.
4. Click the **Conditions** tab.
5. Click **Edit**, then click **Add.**
6. Enter the Filter conditions as follows:



Filter Conditions:

Entities (Any type) Field	Comparison Op	Value	Action
Entity.Name	Equals	Mobile	Add

● And ○ Or

□ Use this condition as a parameter to a chart

The Filter Conditions section.

   1. **Attribute**: Select the field where you want to filter the records.
   2. **Operator**: Select the type of operation you want to use to compare the attribute definition and value.
   3. **Value**: Enter a string or number, or select from the dropdown list.
   4. **Conjunctions**: Joins conditions to build an expression that is matched when returned true. Select the same type for all conditions in a filter. Matches filter to combine AND and OR expressions.
   5. **Use this condition as a parameter to a chart** Allow all users to create reports that can drill down to the record level of this field.

7. Click **Save**.

The Matches Filter operator will not produce correct results if the filter it references is not found. If you must use the Matches Filter operator in the condition of a filter, create the filter to be set in the Matches Filter value first**.**

To remove a condition:

1. Go to **Configuration**> **Filters**. In the **Administration** application, go to **Users** > **Filters**
2. Expand the **Filters** tree.
3. Select a filter to open.
4. Click the **Conditions** tab.
5. Click **Edit**, then click the **Delete X** icon next to the condition.
6. Click **Save**.

Removing a Filter

You can only remove unassigned filters. If you try to remove a filter that is in use, an error lists the location where it is used.

To delete a filter:

1. In the RiskVision application, go to **Configuration** > **Filters**. In the **Administration** application, go to **Users** > **Filters**.

2. Expand the **Filters** tree and locate to select the filter.

3. Click **Delete**.

The filter is no longer available.

Grouping Filters

To make it easier to get an overview of the filters in the filters panel, you can create filter groups within a data table and place certain filters in these. You can only group filters that belong to the same data table. You can then expand or collapse various groups to only work with the filters you want for the moment.

The navigation pane contains the following predefined groups:

GROUP NAME	DESCRIPTION
Filters	Root folder contains RiskVision Content and Organization Content; displays a recursive list of all filters.
My Filters	Contains filters visible to the current user only.
Shared Filters/System	Contains default system filters.
Shared Filters/Public	Contains filters configured by your organization.

Create a New Group

You can only add groups to the **Organization Filters** group.

To add a group:

1. Go to **Configuration > Filters**.
2. Select the organization group.
3. Click **More Actions** > **New Group**.
4. Enter a name and description.
5. Click **OK**.

Deleting a Group

Deleting a group removes all filters in the group. You can only remove groups that contain unassigned filters.

To remove a group:

1. In the RiskVision application, go to **Configuration > Filters**. In the Administration application, go to **Users** > **Filters**.
2. Select the group that contains the one you want to delete. For example, if the group you are removing is in an organization, then select an organization.

   The group displays in the Filter list.

3. Select the group and click **Delete**.

The group and any subgroups and filters are removed.

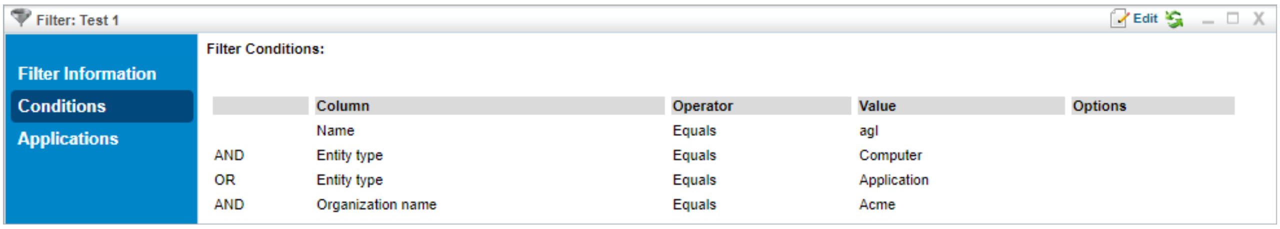
Understanding Complex Filters

A filter can be as simple as **Setting Equals 1**, but more complex filters can be used in reports or for access control.

The built-in filter editor can be used to add conditions one at a time to a filter. These filter conditions are added using the**AND** or **OR** logical operators. By default, the **AND** operator has higher precedence than the **OR** operator. The filter editor does not allow the user to override the precedence (typically done by adding parenthesis).

Example

You have the following filter set up:



Filter Conditions:

	Column	Operator	Value	Options
	Name	Equals	agl	
AND	Entity type	Equals	Computer	
OR	Entity type	Equals	Application	
AND	Organization name	Equals	Acme	

The Conditions tab of a filter.

The filter in this example translates to:

`Entity Name starts with agl AND Entity Type = Computer OR Entity Type = Application AND Organization name = Acme`

Since the **AND** operator has higher precedence than the **OR** operator, the above filter means:

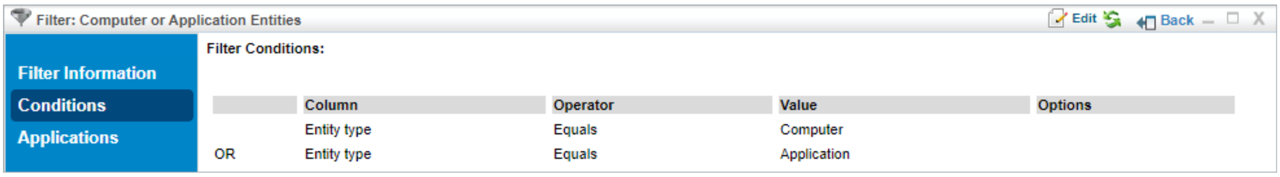
`(Entity Name starts with agl AND Entity Type = Computer) OR (Entity Type = Application AND Organization name = Acme)`

That is, the **AND** operations are performed first.

If you want this filter to evaluate as:

`(Entity Name starts with agl) AND (Entity Type = Computer OR Entity Type = Application) AND (Organization name = Acme)`

There is no way to do this directly by using the filter editor. You must do this using the **Matches Filter** operator. To implement the above filter, you must build a Computer or Application Entities filter for the condition `(Entity Type = Computer OR Entity Type = Application).`



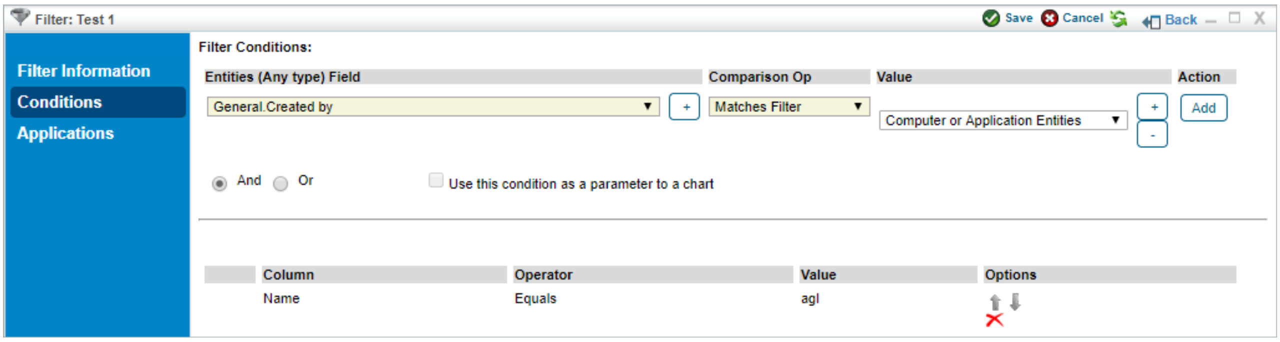
Filter Conditions:

	Column	Operator	Value	Options
	Entity type	Equals	Computer	
OR	Entity type	Equals	Application	

A Computer or Application Entities filter.

The original filter will use the Computer or Application Entities filter using the**Matches Filter** operator.

First, add the **Name Equals agl** condition. Use the **Matches Filter** operator to add the Computer or Application Entities filter. Note that a dummy entry must be selected in the first dropdown of the filter editor. In this case, **Created By** is selected, which is ignored by the server.



Filter Conditions:

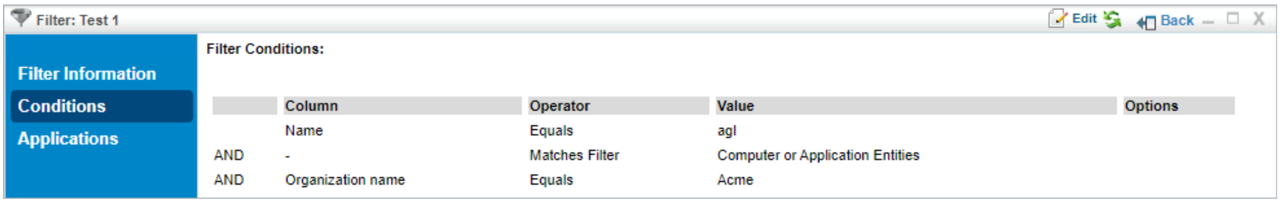
Entities (Any type) Field	Comparison Op	Value	Action
General.Created by	Matches Filter	Computer or Application Entities	Add

● And ○ Or □ Use this condition as a parameter to a chart

	Column	Operator	Value	Options
	Name	Equals	agl	

Adding the Matches Filter operator.

Add **Organization name Equals Acme**. The filter will now look like this:



Filter Conditions:

	Column	Operator	Value	Options
	Name	Equals	agl	
AND	-	Matches Filter	Computer or Application Entities	
AND	Organization name	Equals	Acme	

The filter with the Matches Filter operator added.

Internally, the server surrounds the filter condition of the **Matches Filter** operator with parenthesis. So, this will translate to:

```
(Entity Name starts with agl)AND(Computer or Application Entities) AND (Organization name = Acme)
```

Which is effectively similar to the filter that you set out to construct:

```
(Entity Name starts with agl) AND (Entity Type = Computer OR Entity Type = Application) AND (Organization name = Acme)
```

This can be taken further by using **Matches Filter** operator within the filters used by another **Matches Filter** operator.

User Variables

Users can refer to the following variables when creating filters or custom SQL queries for reports.

USER VARIABLE	DESCRIPTION
%USER_ID%	Login user ID of the current user.
%SYSTEM_USER_ID%	Internal ID of the current user.
%USER_FIRSTNAME%	First name of the current user.
%USER_LASTNAME%	Last name of the current user.
%USER_NAME%	Concatenation of the first name, a single space, and last name of the current user.

Configuring a Threshold Range for Calculating Incident Scores

A common threshold range criteria must be established for assessment, finding, and risk objects. When assessments are run, the risk vulnerability incident scores are derived according to the scale that has been defined for a range. Before running an assessment, ensure that the threshold range is configured to meet the auditing guidelines and policies of the assessment objectives.

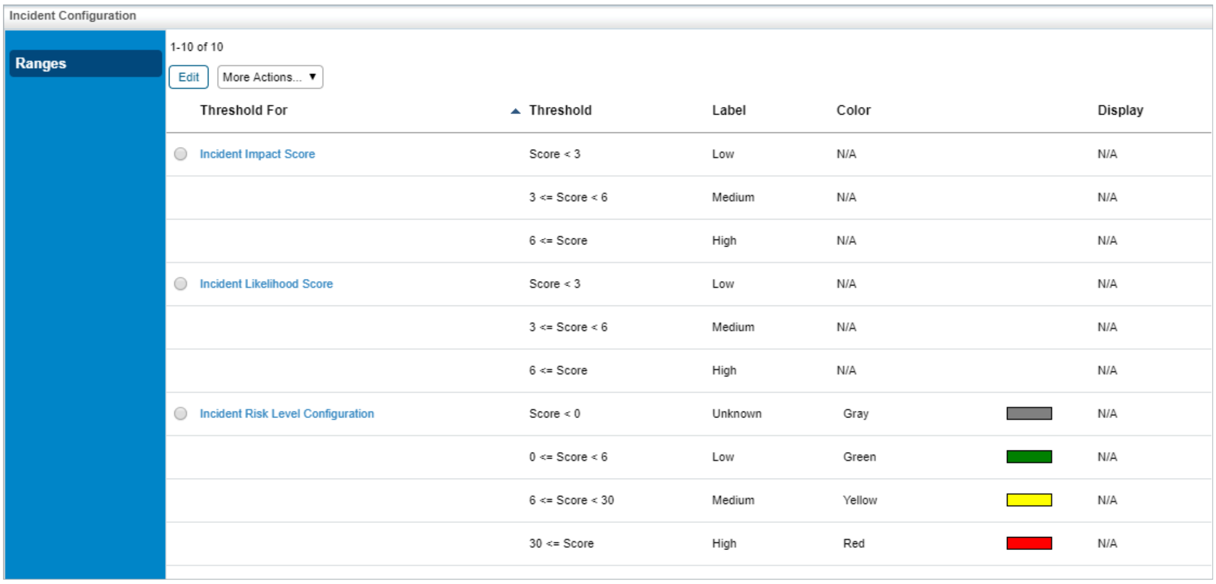
Each configuration range allows the user to adjust the threshold range by specifying the numeric value, unique name, color, and the option to display text or a score.

In order to adjust the configurations, you must have the Tenant Configure permission.

To set up Incident Configuration:

1. Open the Incident Manager.

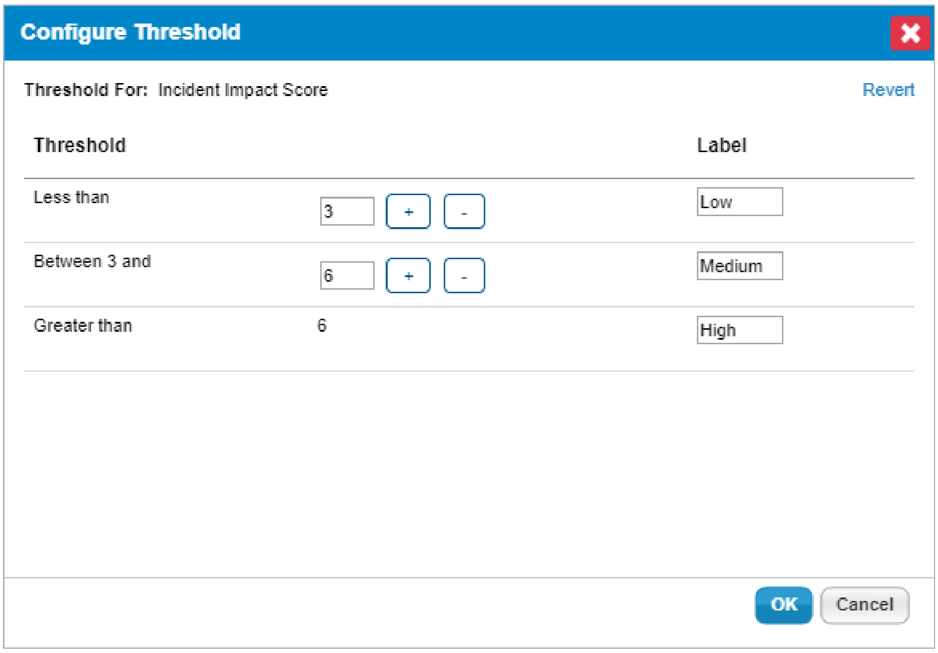
2. Go to **Configuration** > **Incident Configuration**.



Threshold For	▲ Threshold	Label	Color		Display
○ Incident Impact Score	Score < 3	Low	N/A		N/A
	3 <= Score < 6	Medium	N/A		N/A
	6 <= Score	High	N/A		N/A
○ Incident Likelihood Score	Score < 3	Low	N/A		N/A
	3 <= Score < 6	Medium	N/A		N/A
	6 <= Score	High	N/A		N/A
○ Incident Risk Level Configuration	Score < 0	Unknown	Gray	▬	N/A
	0 <= Score < 6	Low	Green	🟩	N/A
	6 <= Score < 30	Medium	Yellow	🟨	N/A
	30 <= Score	High	Red	🟥	N/A

The Incident Configuration tab.

3. Select **Incident Impact Score** and click **Edit**.



Threshold For: Incident Impact Score

Threshold		Label
Less than	3 + -	Low
Between 3 and	6 + -	Medium
Greater than	6	High

The Configure Theshold dialog.

4. Click **+** or **-** to add or remove a threshold range. For any assessment configuration, you can add a maximum of five threshold ranges. At a minimum, any configuration range contains two threshold ranges.

5. **Optional:**

   - To modify a range, enter a numerical value in the threshold range field.
   - To change the threshold display name, enter a name in the **Label** field.
   - To assign a color for a threshold, click the **Color** icon, choose the desired color, and click **Close**. This option may not be available for all thresholds.
   - Choose the **Text** or **Score** option to display the threshold label or the value for the risk after the assessment is run. This option may not be available for all thresholds.

6. Click **Revert** to ignore all the changes or click **OK** to save the configuration.

Similarly, set up **Incident Likelihood Score** and **Incident Risk Level Configuration**.

About Ticket Management Preferences

The **Ticket Management Preferences** page manages the list of ticket dispositions. A ticket disposition is a text string such as "Pending customer confirmation" or "Under investigation." You can use a ticket disposition to label a ticket's status. You can access the **Ticket Management Preferences** page only if you have the Ticket Manage permission.

When a ticket reaches it's due date, it follows the escalation configuration by automatically escalating to additional stakeholders who are notified about the ticket's overdue status.

Ticket Management Preferences allow the user to disable escalations for tickets with a specified disposition. For example, the user may not want to escalate overdue tickets if the disposition is "Pending customer confirmation."

To add to the list of ticket dispositions:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Click **Add**, enter a new disposition in the **Ticket Dispositions** text box, and then click **OK**.
3. Click **Refresh** to update the **Do not escalate when disposition is set to** drop-down list.
4. Click **Save** after you finish modifying a ticket disposition .

To change a ticket disposition:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Click the disposition name to change, update the name, and click **OK**.
3. Click **Refresh** to update the **Do not escalate when disposition is set to** drop-down list.
4. Click **Save** after you finish modifying a ticket disposition.

To delete a ticket disposition:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Select the disposition, click **Delete**, and confirm the action.
3. Click **Refresh** to update the Do not escalate when disposition is set to drop-down list.
4. Click **Save** after you finish modifying a ticket disposition .

To disable escalation for a specific disposition:

1. Go to **Configuration** > **Ticket Management Preferences** and then click **Edit**.
2. Select a disposition from the **Do not escalate when disposition is set to** drop-down list and click **Save.**

Entity Types

For customers using the RiskVision solution to build and deploy a risk and compliance management solution, there are two main components to be concerned with:

Entity Types

The following list describes the predefined entity types:

Icon	Entity	Description
	Account	Account or login information pertaining to privileged access of financial accounts, computer applications, etc.
	Application	Software applications that are critical to a company's operation, for example, financial reporting, CRM, procurement, change management, incident management, and database applications.
	Computer	Computers, servers of different types (file, database, authentication), notebooks, laptops, etc. Predefined subtypes such as Desktop and Notebook.
	Data	Specific data that may be critical to operations and are important enough to be classified and tracked on their own, for example, account numbers, customer lists, documents containing product formulas, market-sensitive information, intellectual property, etc.
	Device	Other network devices such as routers, switches, printers, VPN, etc.
	Domain	An Active Directory domain.
	Financial	Entities related to financial resources such as stocks, bonds, cash, etc.
	Group	An Active Directory security group.
	Intangible	Entities such as intellectual property, product secrets and proprietary information, etc.
	Location	Physical or geographical locations, real estate, offices, etc.
	Mobile Device	Mobile devices are entities, such as mobile phone, personal digital assistant (PDA), and much more that are allowed by organizations under the Bring your own device (BYOD) policy. Employees bring their mobile devices to access email, file servers, and critical applications. Track and assess all employee-owned devices by creating or importing a Mobile Device entity type.
	Network	Computer network infrastructure like subnets and wireless networks.

Icon	Entity	Description
	Network Device	Network devices such as firewall, routers, modems, etc.
	Organizational Unit	An Active Directory organizational unit.
	Person	Individuals within an organization where compliance and risk are managed by the RiskVision system. Also linked as users of applications, processes, documents, and storage.
	Physical	Non-computer entities such as mechanical, manufacturing, and production equipment, vehicles and capital goods.
	Process	Business operations such as order entry, payment transaction, accounts payable and receivable, shipping and receiving, RMA, etc.
	Project	Shows individual entity assessments defined as part of a larger program.
	Vendor	Organizations or entities outside your own enterprise for which you want to apply and monitor control compliance and calculate risk.

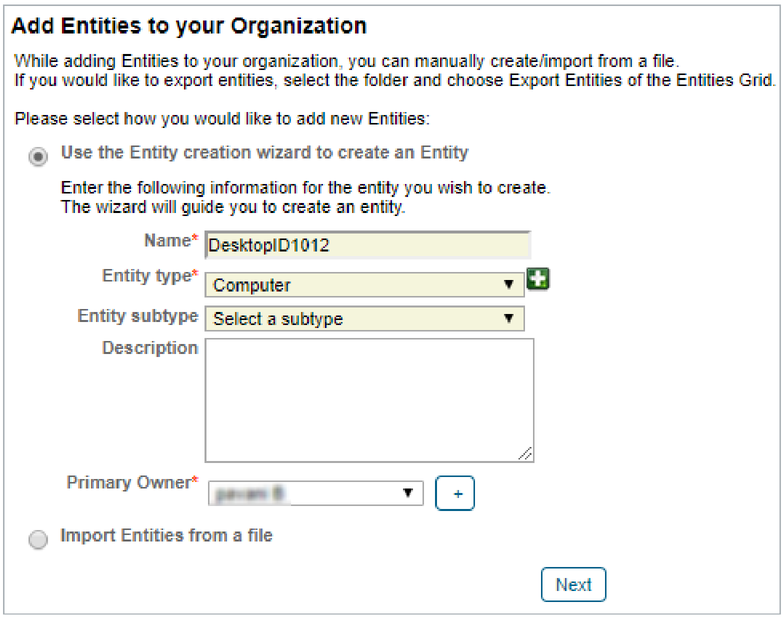
Creating a New Entity

To create a new entity, you must have the Entity View and Entity Create permissions. The entity wizard takes you through the configuration of basic entity settings. For computer type entities, see Creating a New Computer Type Entity.

To create a new entity:

1. Go to **Entities** > **Entities** and select an entity group.

2. Click **New**. The **Add Entities to your Organization** page is displayed.



Add Entities to your Organization

While adding Entities to your organization, you can manually create/import from a file.
If you would like to export entities, select the folder and choose Export Entities of the Entities Grid.

Please select how you would like to add new Entities:

● Use the Entity creation wizard to create an Entity

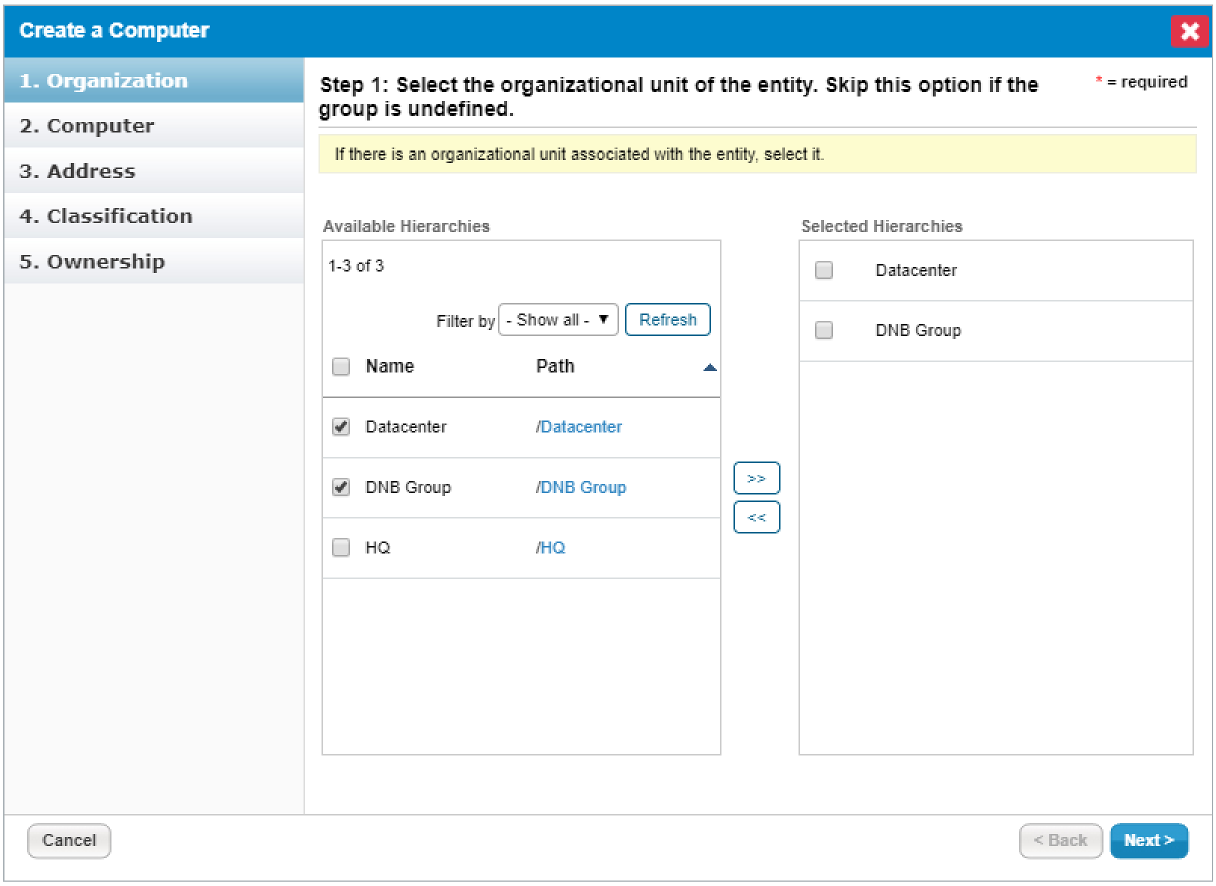
Enter the following information for the entity you wish to create.
The wizard will guide you to create an entity.

Name*	DesktopID1012
Entity type*	Computer ▾
Entity subtype	Select a subtype ▾
Description	
Primary Owner*	[redacted] ▾

○ Import Entities from a file

The Add Entities to your Organization page.

3. Set the name, type, and owner and then click **Next**. The **Create a Computer** wizard appears, showing the **Organization** wizard page.


Create a Computer

1. Organization
2. Computer
3. Address
4. Classification
5. Ownership

Step 1: Select the organizational unit of the entity. Skip this option if the group is undefined.

* = required

If there is an organizational unit associated with the entity, select it.

Available Hierarchies

1-3 of 3

Filter by - Show all - ▼ Refresh

□ Name	Path
☑ Datacenter	/Datacenter
☑ DNB Group	/DNB Group
□ HQ	/HQ

Selected Hierarchies

□ Datacenter

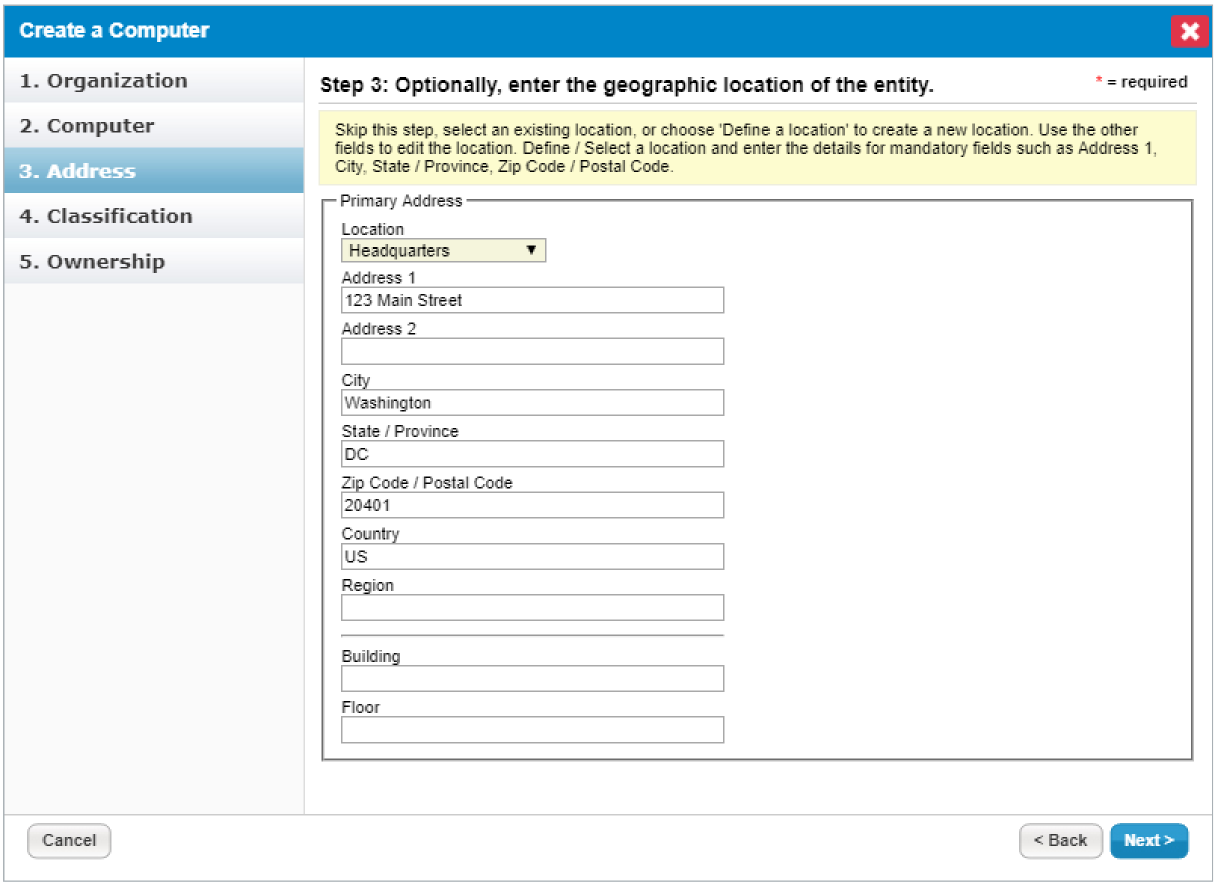
□ DNB Group

The Organization wizard page.

4. Select the organizational group to automatically set the organization fields. Skip this step if the organization has not been configured.

   For more information on organizational groups, see Defining a New Organization.

5. Click **Next**. Click **Next** again. The **Address** wizard page appears.



Step 3: Optionally, enter the geographic location of the entity.

* = required

Skip this step, select an existing location, or choose 'Define a location' to create a new location. Use the other fields to edit the location. Define / Select a location and enter the details for mandatory fields such as Address 1, City, State / Province, Zip Code / Postal Code.

Primary Address

Location: Headquarters

Address 1: 123 Main Street

Address 2:

City: Washington

State / Province: DC

Zip Code / Postal Code: 20401

Country: US

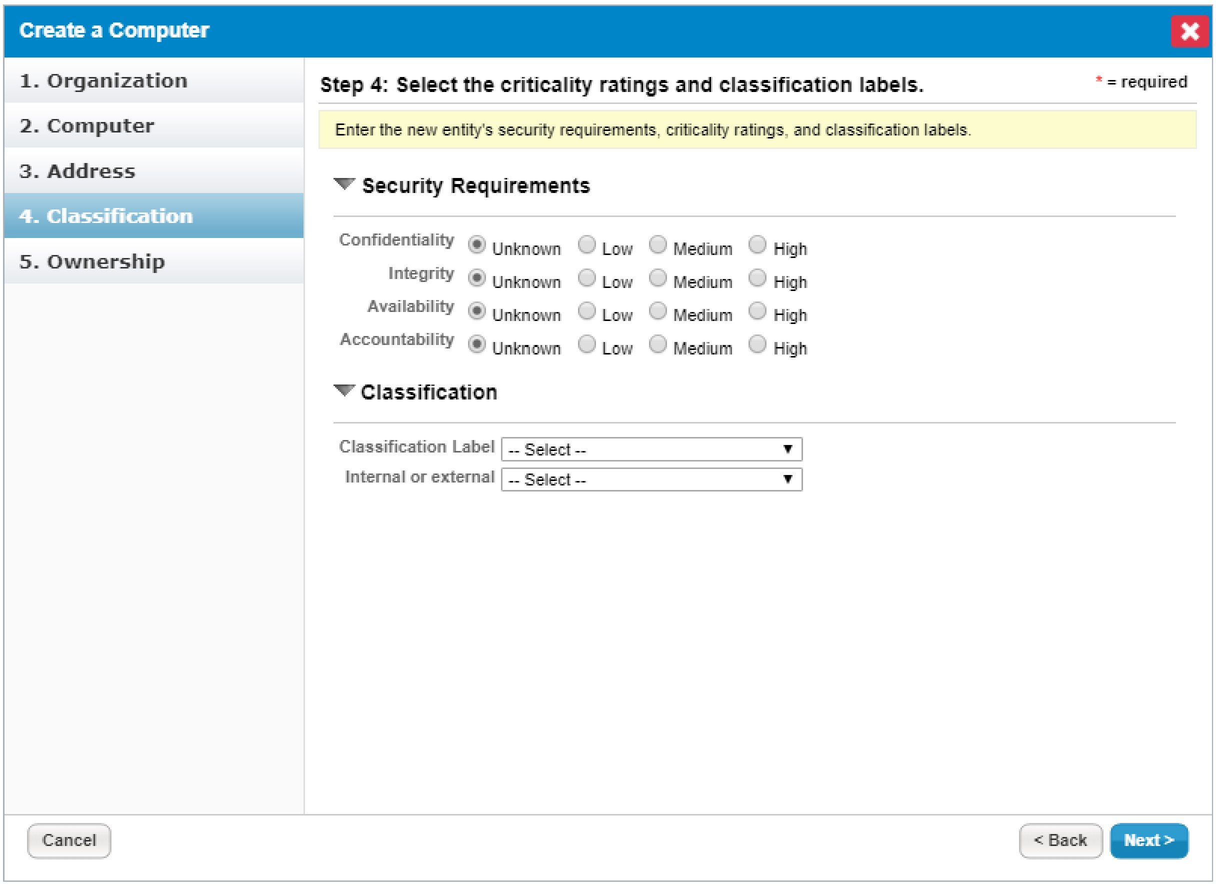
Region:

Building:

Floor:

The Address wizard page.

6. Enter the address and click Next. The **Classification** page is displayed.



Step 4: Select the criticality ratings and classification labels.

* = required

Enter the new entity's security requirements, criticality ratings, and classification labels.

Security Requirements

Confidentiality	● Unknown	○ Low	○ Medium	○ High
Integrity	● Unknown	○ Low	○ Medium	○ High
Availability	● Unknown	○ Low	○ Medium	○ High
Accountability	● Unknown	○ Low	○ Medium	○ High

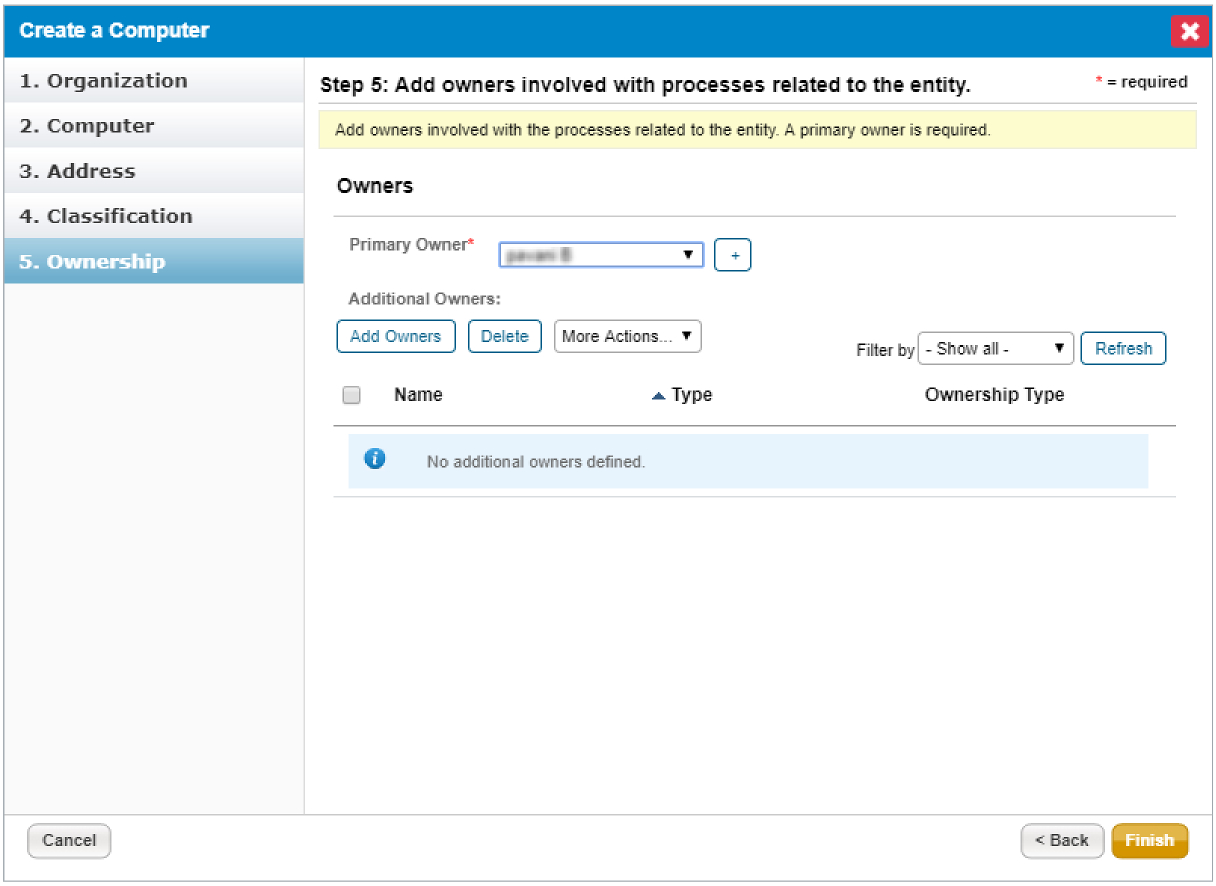
Classification

Classification Label: -- Select --

Internal or external: -- Select --

The Classification wizard page.

7. Select the criticality setting. The **Ownership** page is displayed.



Step 5: Add owners involved with processes related to the entity.

* = required

Add owners involved with the processes related to the entity. A primary owner is required.

Owners

Primary Owner*: [redacted]

Additional Owners:

Filter by: - Show all -

□	Name	▲ Type	Ownership Type

No additional owners defined.

The Ownership wizard page.

8. Change the primary owner and assign other users as owners. See Configuring Owners. While it is possible to import an entity without a primary owner, or to delete an entity's primary owner, many operations require that each entity has a primary owner. Creating a program that references an entity without a primary owner, for example, will cause an error.

9. Click **Finish**.

The entity is added to the system. If the entity is part of a dynamic group, an assessment automatically launches the entity depending on the program settings.

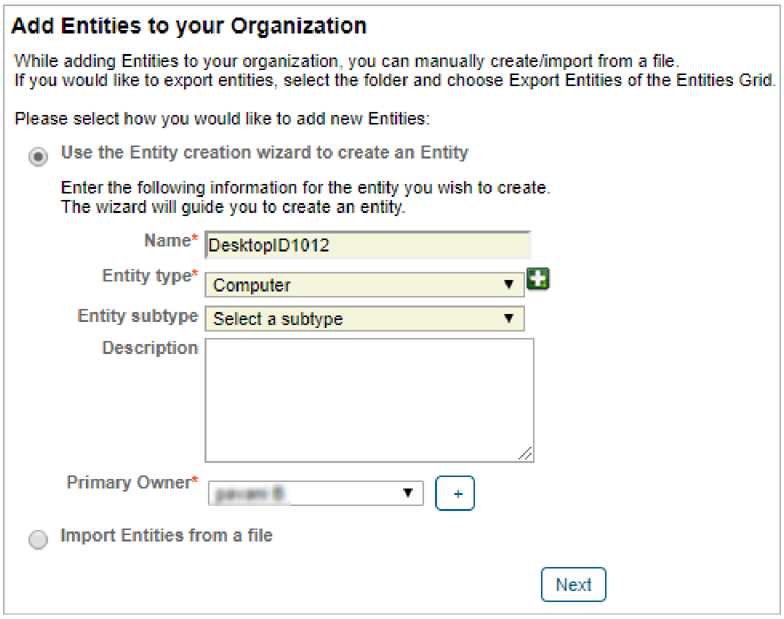
Creating a New Computer Type Entity

The entity wizard takes you through the configuration of basic entity settings.

To create a new entity:

1. Go to **Entities**> **Entities** and select an entity group. The Entities page is displayed.

2. Click **New**.



Add Entities to your Organization

While adding Entities to your organization, you can manually create/import from a file.
If you would like to export entities, select the folder and choose Export Entities of the Entities Grid.

Please select how you would like to add new Entities:

● Use the Entity creation wizard to create an Entity

Enter the following information for the entity you wish to create.
The wizard will guide you to create an entity.

Name* DesktopID1012

Entity type* Computer ▼

Entity subtype Select a subtype ▼

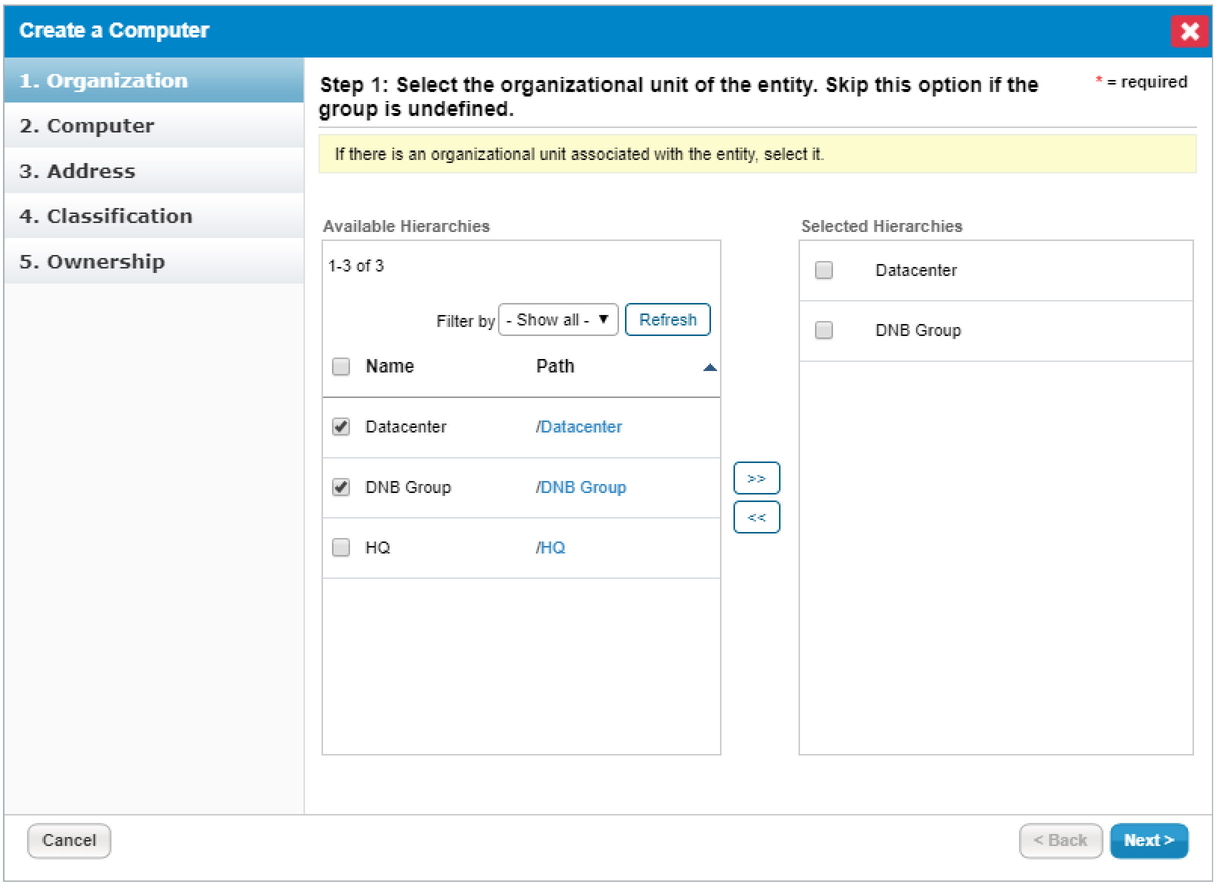
Description

Primary Owner* [redacted] ▼

○ Import Entities from a file

The Add Entities to your Organization page.

3. Select the **Entity type**. Enter the name, select the owner, and then click **Next**.



Create a Computer

Step 1: Select the organizational unit of the entity. Skip this option if the group is undefined.

* = required

If there is an organizational unit associated with the entity, select it.

Available Hierarchies

1-3 of 3

Filter by - Show all - ▼ Refresh

□	Name	Path
☑	Datacenter	/Datacenter
☑	DNB Group	/DNB Group
□	HQ	/HQ

Selected Hierarchies

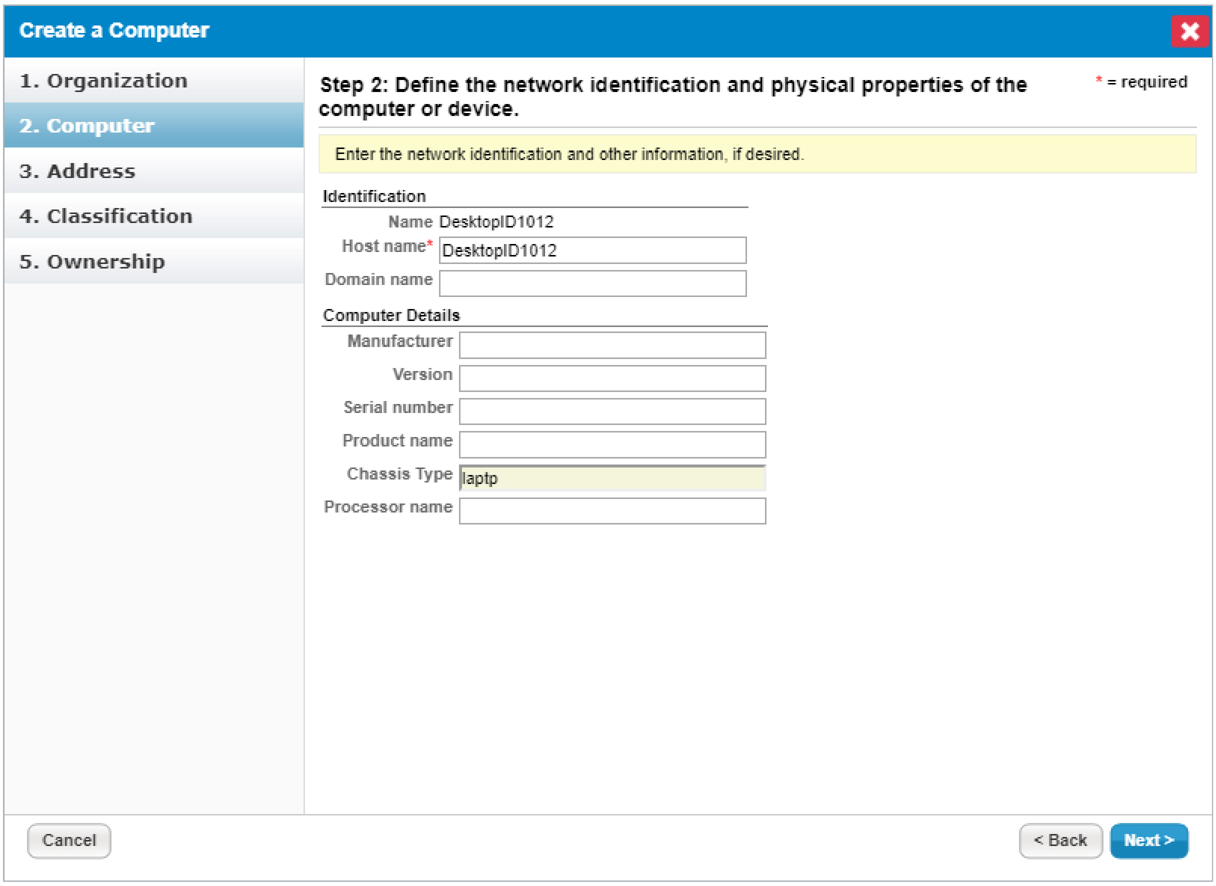
□ Datacenter

□ DNB Group

The Organization wizard page.

4. Select the Organizational group to automatically set the organization fields. Skip this step if the organization has not been configured. For more information on organizational groups see Defining a New Organization.

5. Click **Next**. The **Computer** wizard page appears.



Step 2: Define the network identification and physical properties of the computer or device.

* = required

Enter the network identification and other information, if desired.

Identification

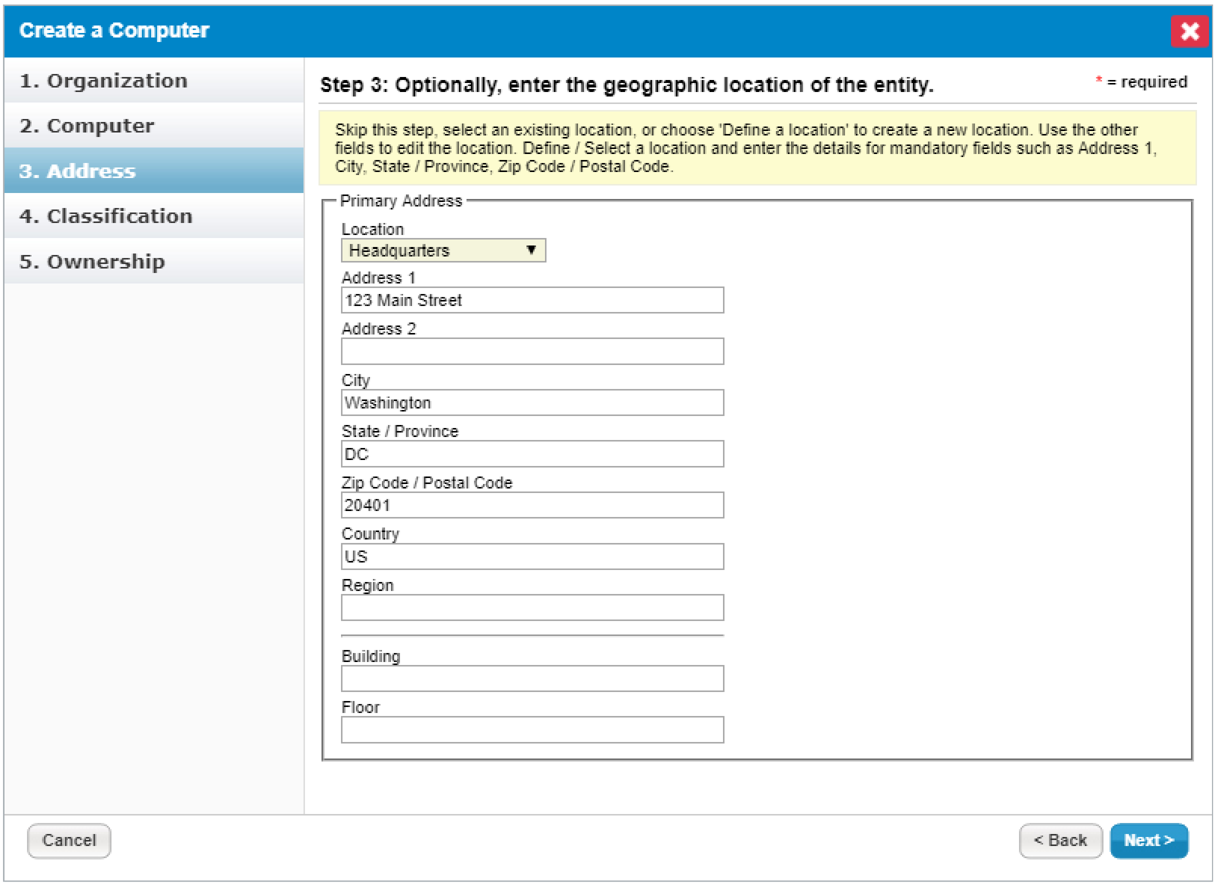
Name	DesktopID1012
Host name*	DesktopID1012
Domain name	

Computer Details

Manufacturer	
Version	
Serial number	
Product name	
Chassis Type	laptp
Processor name	

The Computer wizard page.

6. Enter the **Identification** and **Computer Details**, then click **Next**.



Create a Computer

Step 3: Optionally, enter the geographic location of the entity.

* = required

Skip this step, select an existing location, or choose 'Define a location' to create a new location. Use the other fields to edit the location. Define / Select a location and enter the details for mandatory fields such as Address 1, City, State / Province, Zip Code / Postal Code.

Primary Address

Location: Headquarters

Address 1: 123 Main Street

Address 2:

City: Washington

State / Province: DC

Zip Code / Postal Code: 20401

Country: US

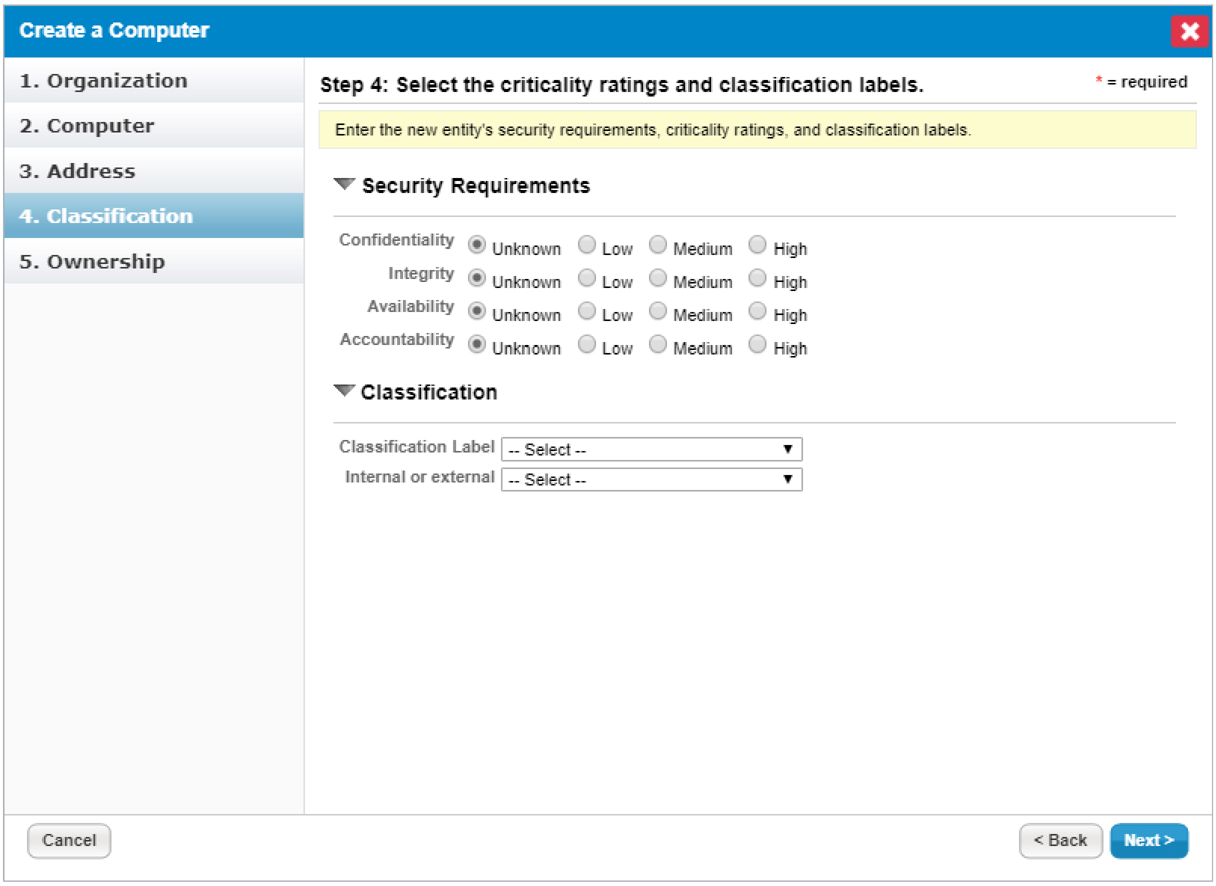
Region:

Building:

Floor:

The Address wizard page.

7. Enter the address, then click **Next**.



Create a Computer

1. Organization
2. Computer
3. Address
4. Classification
5. Ownership

Step 4: Select the criticality ratings and classification labels.

* = required

Enter the new entity's security requirements, criticality ratings, and classification labels.

Security Requirements

Confidentiality	● Unknown	○ Low	○ Medium	○ High
Integrity	● Unknown	○ Low	○ Medium	○ High
Availability	● Unknown	○ Low	○ Medium	○ High
Accountability	● Unknown	○ Low	○ Medium	○ High

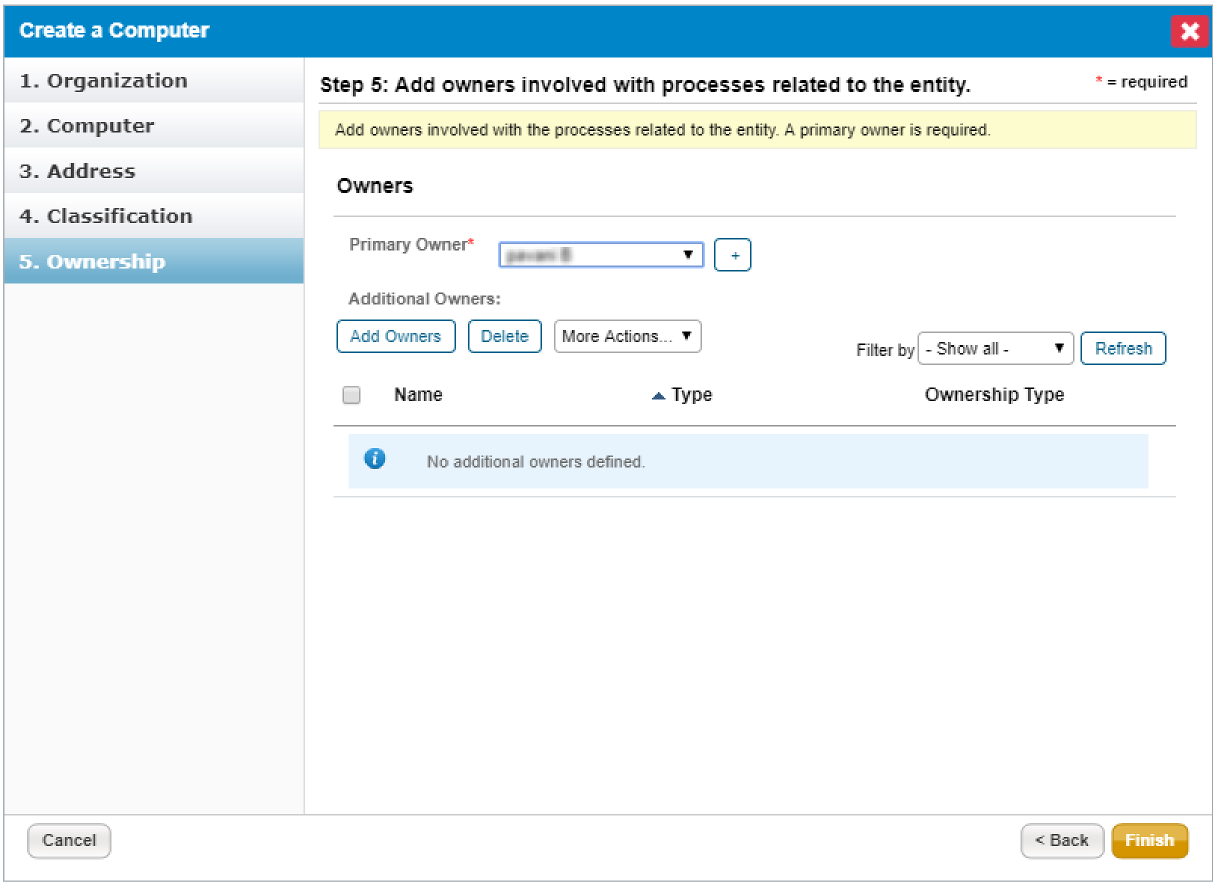
Classification

Classification Label: -- Select --

Internal or external: -- Select --

The Classification wizard page.

8. Select the criticality setting. The **Ownership** wizard page appears.



Create a Computer

Step 5: Add owners involved with processes related to the entity.

* = required

Add owners involved with the processes related to the entity. A primary owner is required.

Owners

Primary Owner*: [redacted]

Additional Owners:

No additional owners defined.

The Ownership wizard page.

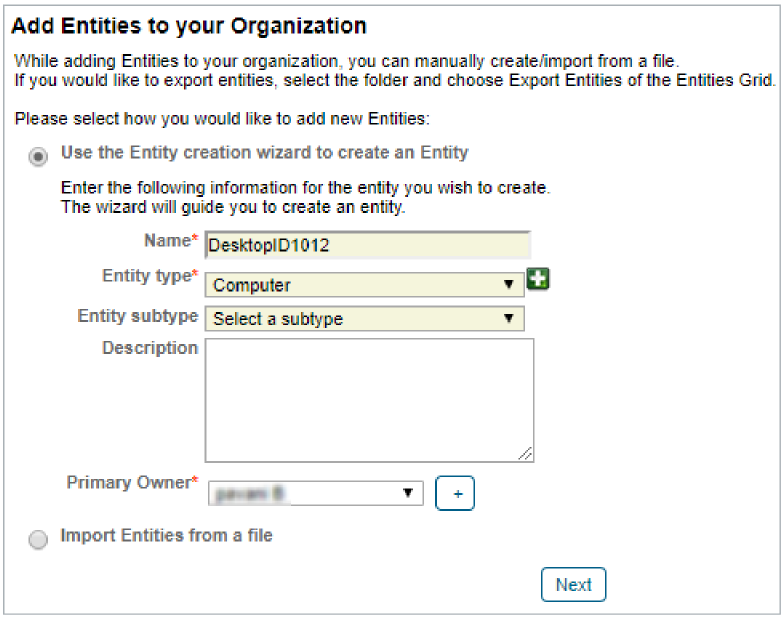
9. Change the primary owner and assign other users as owners. See Configuring owners for more information.

10. Click **Finish**.

The computer type entity is added to your system. If the entity is in a dynamic group that is included in a program, an assessment may automatically launch for the entity, depending on the program settings.

Setting the Name, Type, and Owner for an Entity

Set the following information on the **Entity Wizard Name and Owners** page:



Add Entities to your Organization

While adding Entities to your organization, you can manually create/import from a file.
If you would like to export entities, select the folder and choose Export Entities of the Entities Grid.

Please select how you would like to add new Entities:

● Use the Entity creation wizard to create an Entity

Enter the following information for the entity you wish to create.
The wizard will guide you to create an entity.

Name* DesktopID1012

Entity type* Computer

Entity subtype Select a subtype

Description

Primary Owner* [redacted]

○ Import Entities from a file

The Entity Wizard Name and Owners page.

Setting	Type	Description
Name	string	Enter a name that Identifies the entity in programs, assessments, questionnaires, tickets, exceptions, incidents, and reports.
Entity type	Default entity types	Displays a list of predefined entity types.
	Define new type	Displays a text box where you can enter up to 255 characters. The new type is added to the list of entity types when you save the entity.
Entity subtype	Define new type	(Optional) Displays a text box where you can enter up to 255 characters. The new subtype is added to the selected type and displays as an option the next time you select the type.
Description	string	Enter up to 1024 characters that summarize the entity. Displays in the entity in list and detail pane.
Primary owner	System user	Select a user.

About Discovered Entities

The Discovered, Managed and Unmanaged dynamic groups provide dynamic subgroups that categorize entities by entity type, for example, application, computer, and so on. Entities first show up in the Discovered dynamic group when they are discovered, for example, using a connector, or created from imported entities. Discovered or Unmanaged entities can be moved to the Managed group by selecting the Manage in the Status pull down list in the General detail display for a particular entity. You can also click on the Manage node or any Manage node subgroup and choose the "Start Managing These Entities" option from the right-click context menu. Also, from the list pane display for a selected group, you can choose Manage Entities from the More Actions menu.

Entities require a minimum of a hostname or IP and a domain to be included in displays of Discovered or Managed entities.

Display Entity Details

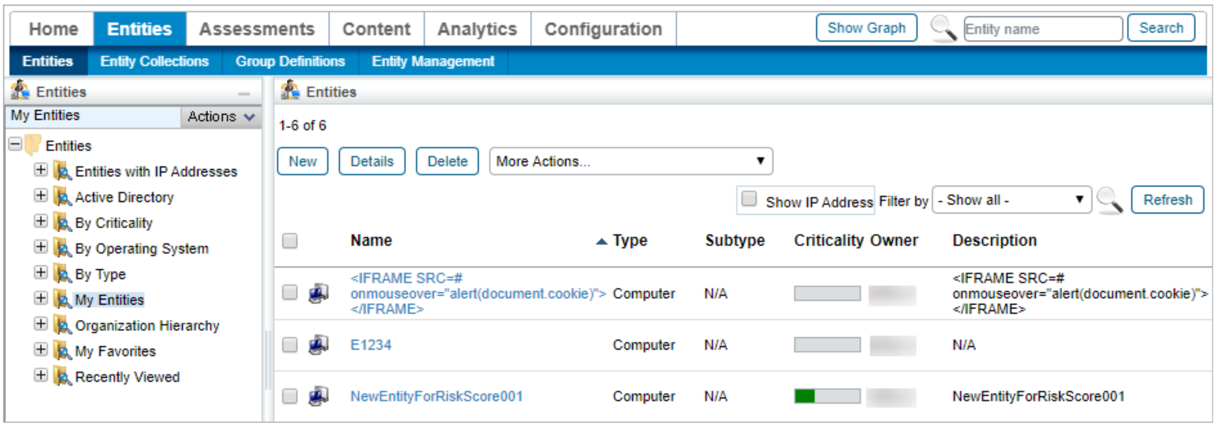
There are a few ways to open the entity details pane from other menus, such as opening the**Assessment Details** page. This section explains how to open the details pane from the **Entities** menu. To view and search an entity, you must have the Entity View permission. In general, entities are visible only to their primary owners. However, if a primary owner nominates another user as a business owner for an entity, then the business owner will be able to view that entity. Find an entity by entering part or all of the name in the search field, then click **Search**.

The search field.

To display the entity details pane:

1. Go to **Entities** > **Entities**.

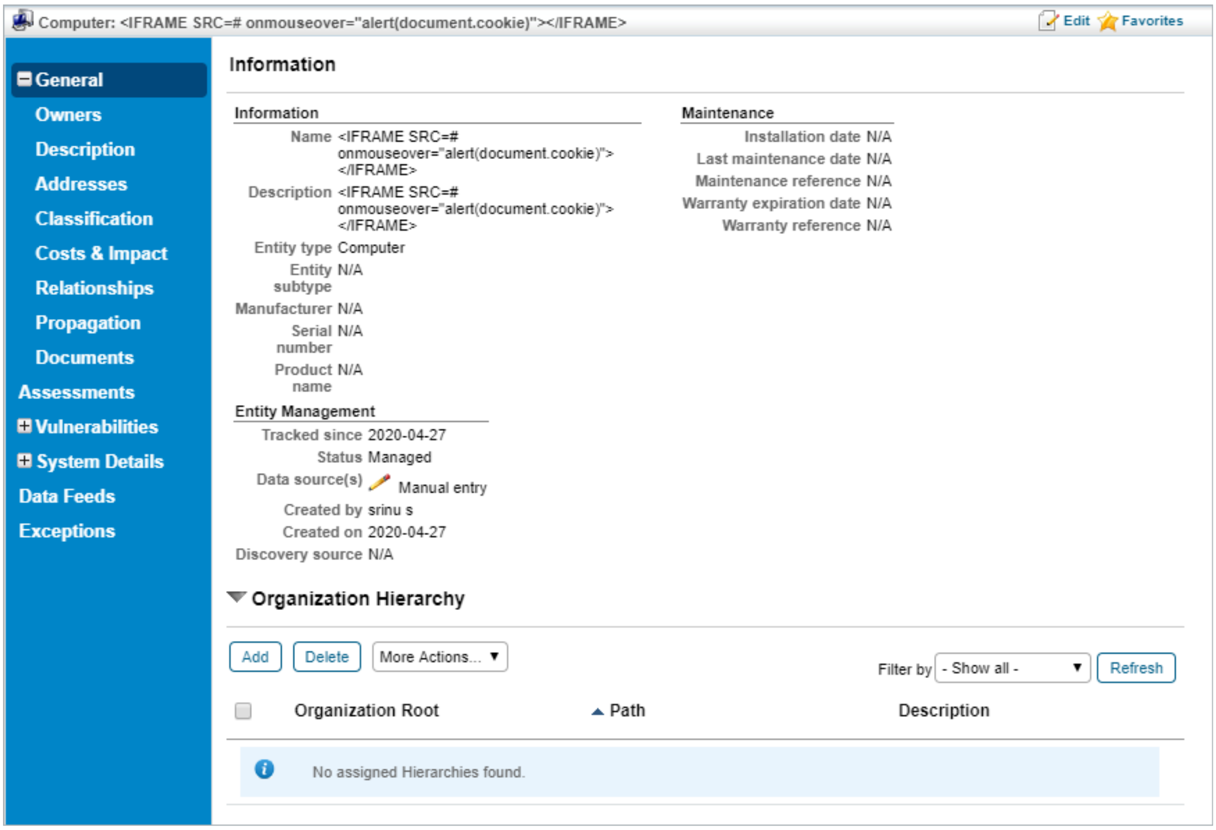
2. Click a group, such as **My Entities**, to display the Entity list.



□	Name	▲ Type	Subtype	Criticality	Owner	Description
□	<IFRAME SRC=# onmouseover="alert(document.cookie)"> </IFRAME>	Computer	N/A		[redacted]	<IFRAME SRC=# onmouseover="alert(document.cookie)"> </IFRAME>
□	E1234	Computer	N/A		[redacted]	N/A
□	NewEntityForRiskScore001	Computer	N/A	🟩	[redacted]	NewEntityForRiskScore001

The My Entities list of entities.

3. Select an entity, then click **Details** to open the **Entities Details** pane.



Computer: <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>

Information

Information

Name <IFRAME SRC=# onmouseover="alert(document.cookie)"> </IFRAME>
Description <IFRAME SRC=# onmouseover="alert(document.cookie)"> </IFRAME>
Entity type Computer
Entity subtype N/A
Manufacturer N/A
Serial number N/A
Product name N/A

Maintenance

Installation date N/A
Last maintenance date N/A
Maintenance reference N/A
Warranty expiration date N/A
Warranty reference N/A

Entity Management

Tracked since 2020-04-27
Status Managed
Data source(s) Manual entry
Created by srinu s
Created on 2020-04-27
Discovery source N/A

Organization Hierarchy

□	Organization Root	Path	Description
	No assigned Hierarchies found.		

The Entities Details pane.

Entity Details Tabs

Entity details are categorized into a set of tabs. The available tabs will depend on the entity type. You can edit these tabs if you have the Entity View and Entity Update permissions. To edit entities created by other users for which you have not been named an additional owner, you must have Entity View and Entity Update all permissions. You can update the **Classification** tab if you have Entity View and Entity Manage permissions.

These are the available entity details tabs:

Tab	Attributes
General	All entity types have a General tab. Attributes include name, type and subtype, and other identifying fields. Status can be Managed or Discovered. The entity's Organization Hierarchy is described here.
Owners	Entities have a primary owner and a grid of additional owners. Click Add Owners to associate more users with this entity.
Description	The Description provides additional type-specific fields, such as Publisher and Version, for applications. The profile information is listed on this tab, if a matching profile is found.
Addresses	A grid of physical addresses, if any, associated with this entity. Click New to define a new physical address. Use the following property to delete an entity's address: com.agiliance.asset.deleteAddress=true.
Classification	Entities can be classified in many different ways, such as Business Criticality, CIAA (Confidentiality, Integrity, Availability, and Accountability), or tags. There is a Change History associated with entity classification.
Cost & Impact	This tab associates specific costs and importance metrics with a particular entity. Costs include attributes such as "business value per hour ($)," and "average remediation time (days)." Important attributes include "number of users."
Relationships	A grid listing the other entities with which this entity has a relationship. Click Add relationship to specify how an entity must relate to another entity. Also, see Relationship Explorer. For a Person-type entity, a relationship is listed in the Teams tab.
Propagation	This tab displays the programs in which the entity is inheriting and propagating the controls. Because the entity is related to another entity, the control results are propagated after answering the assessments.
Documents	The Documents tab is a grid listing documents, web links and network path associated with this entity. Click New Document to upload a document related to the entity, such as a contract for a Vendor type entity, or click New Web Link / Network Path to record an external link. Note: By default, users with the Entity view+create+update permission and without any Document Repository-related permissions can attach or delete documents on Entities, but when users are using the new Global Document Repository feature to attach a document from the Document Repository to an entity, then Document Repository-related permissions and ownerships are required.
Assessments	A grid of the assessments associated with this entity. Click New to create a new assessment.
Automation	Entity types, such as Computer or Application, have an automation tab that displays target type parameters based on the entity type, subtype, and product name.
Vulnerabilities	For some entity types, the Vulnerabilities tab provides a summary of vulnerabilities found by scanners or users. Computer and Vendor types, for example, list vulnerabilities on different tabs.
Vulnerabilities List	The Vulnerabilities List tab is a grid of all vulnerabilities found by scanners or entered manually by users. To create a new vulnerability and associate it with the entity, click either New or Import. To assign an existing vulnerability to this entity, click Assign. For more information, see Assigning Vulnerabilities. Some entity types, such as Vendors, do not have associated vulnerabilities.
Inferred	The Inferred tab lists the vulnerabilities that are associated indirectly with an entity type, such as Computer and Network Device.
Comp Controls	The Comp Controls tab lists each of the vulnerability compensation controls attached to the entity. Users can add new compensating controls, delete them, add notes, and view the recent changes made. Note: Only users with the Entity View, Threats and Vulnerabilities View, and Vulnerability

	Compensating Control Update permissions can view, add, update, and remove vulnerability compensating controls from the entity or add comments. All updates and changes to a vulnerability compensating control will be logged in the Change History section.
System Details	Certain types and subtypes of entity, such as Computers, have a number of tabs organized under the heading 'System Details.' These tabs include: • Network • Ports • Services • Applications • Patches • Network Shares • User Accounts • Membership
Data Feeds	A grid listing the data feeds associated with the entity, if any.
Exceptions	The Exception tab is a grid of all exceptions, including the controls, findings, and vulnerabilities related to the entity that the tab is associated with.

About Ownership Types

Ownership types link workflow stage stakeholders to the system users who are assigned to an entity or policy. This allows processes such as programs, tickets, and policy pack approval to run automatically. You can restrict user access based on the role of the user and the type of ownership.

Different workflow stages are assigned automatically to different object owners:

- Ticket, Assessment program, incident, and exceptions are processes for entities. Therefore the workflow stage stakeholder is linked to an entity ownership type.
- Content packs and control objectives contain content objects such as Controls and Questionnaires that also have owners.

You can also assign users and teams as stakeholders in a workflow. For more information, see About workflows. Adding, modifying, or deleting an ownership type requires you to have the Tenant Configure permission

Adding A New Ownership Type

Add ownership types to create a new mapping between workflow stages and system users you want to automatically assign to workflow related actions.

To create a new ownership type

1. Go to **Configuration** > **Ownership Types**.
2. Click **New**.

   The **Configure Ownership Type** dialog appears.
3. Enter the ownership configuration:
   - In the **Name** field, type name that uniquely identifies the ownership type.
   - In the **Display Name** field, enter the name that you want to display in ownership assignment dialog.

     For example, the display of an Entity type appears in the list on the workflow stage stakeholder owner roles tab.
   - Select the type. Entity: Assign to Entities and the Assessment, Ticket, Exception, and Incident workflows. Policy: Assign to policy packs and policy workflows.
   - Select a role to limit which users can be assigned as the ownership type. The user must have at least one of the roles.

     When no roles are selected, any user can be assigned.
4. Click **OK**.

The new ownership type displays in the list.

Deleting an Ownership Type

You can delete unused ownership types only. Change the ownership type entity and policy owners or remove the ownership type from the workflow stage.

To delete an ownership type:

1. Go to **Configuration** > **Ownership Types**.
2. Select the ownership types.
3. Click **Delete**.

The ownership type is removed from the list and is no longer available on corresponding policy, entity, and workflow pages.

Changing the Setting of an Ownership Type

You can change the display name and role restrictions. Modifying role restriction only affects new ownership assignments.

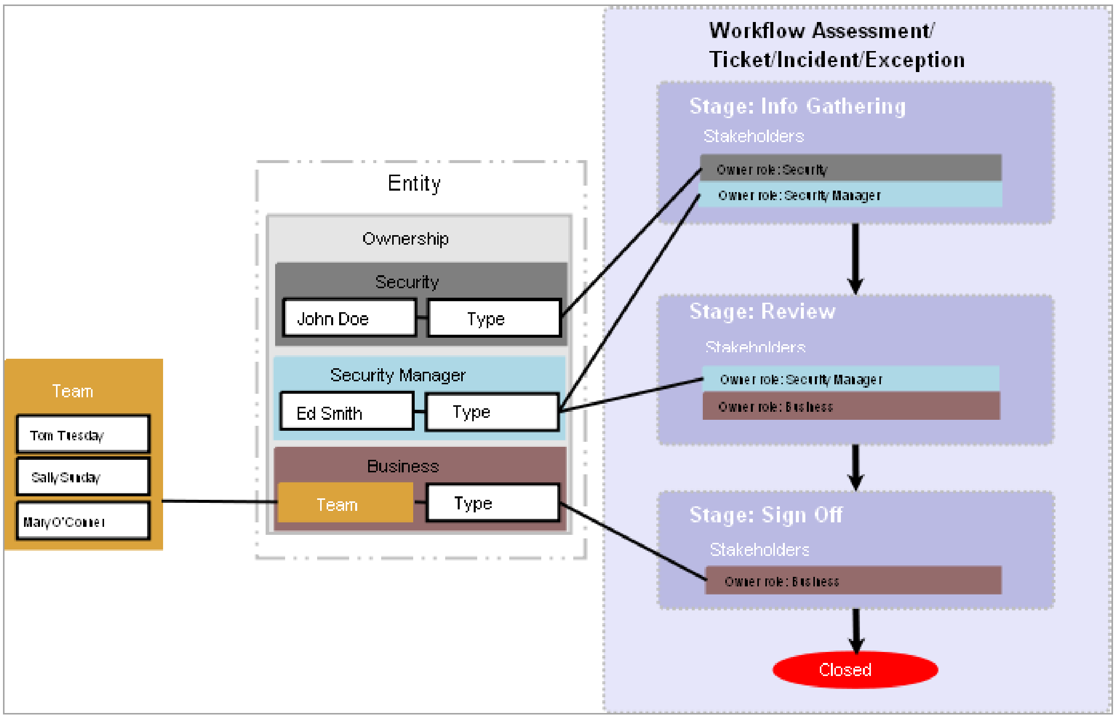
To modify an ownership type settings

1. Go to **Configuration** > **Ownership Types**.
2. Select the ownership type.
3. Click **Edit**. The **Configure Ownership Type** dialog appears.
4. Modify the configuration and click **OK**.

The display name is updated immediately. Role restrictions apply to the next owner assignment.

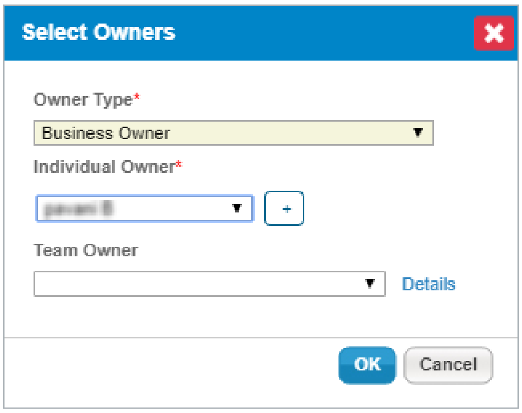
Configure Owners

Entity ownership allows RiskVision to automatically assign stakeholders for workflow stages, such as assessments, when the entity is selected for the process.



To modify owners:

1. Click an entity to open.
2. Go to **Ownership**, then click **Edit**.
3. Perform one of the following actions:
   - To change the primary owner, select a different user from the primary owner dropdown.
   - To remove an owner, click **X** in the top-right corner of the window.
   - To add another user, click **Add Owners**.



Select Owners

Owner Type*: Business Owner

Individual Owner*: [redacted]

Team Owner:

The Add Addinal Owners dialogue.

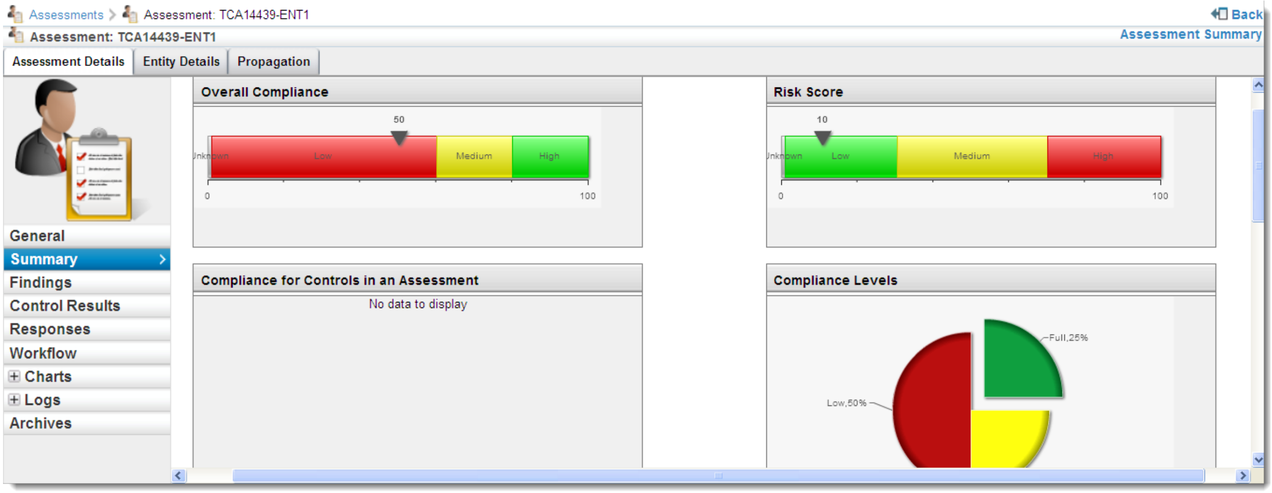
4. Select the ownership type. For more information, see About Ownership Types.
5. Select a user from the individual user dropdown. Skip this option to assign a team only.

6. Select a team from the Team drop-down. Skip this option to assign a user only.
7. Click **OK**.
8. Click **Save**.

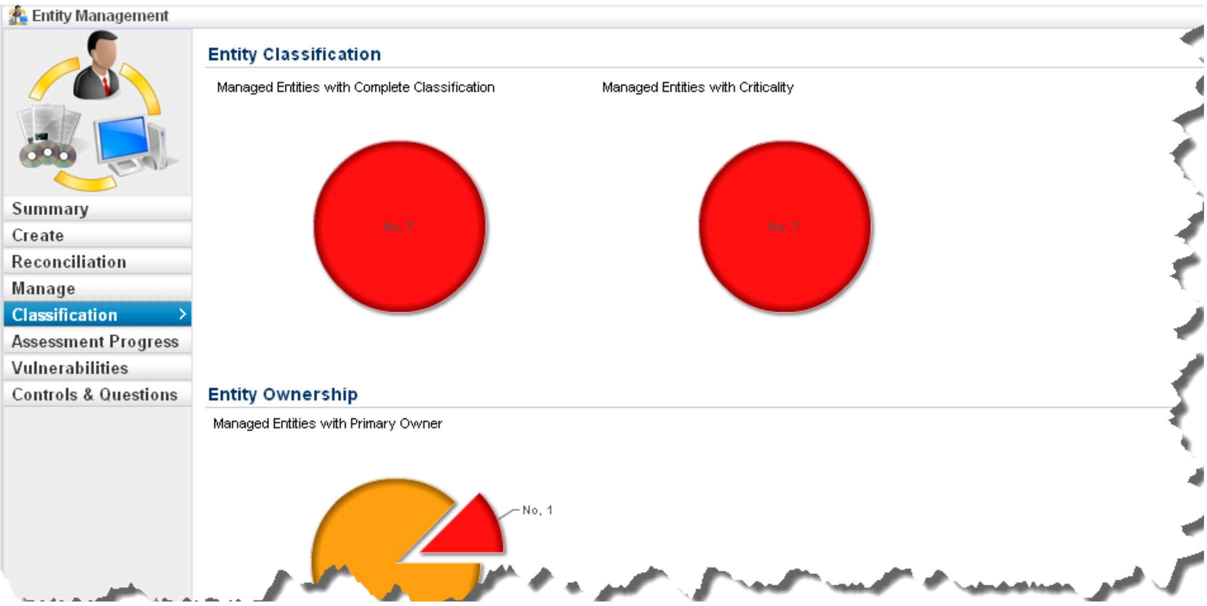
Configuring Entity Compliance and Criticality Ranges

The Range option controls the numeric score for the low, medium, and high or VL (very low), L (low), M (medium), H (high), and VH (very high) selections a user can make on various RiskVision pages as well as the color and ranges that display in graphs and charts on dashboard pages and reports:

- **Compliance range**: Controls the numeric values for displaying overall compliance levels, such as on the Assessment Details > Control Results > Compliance Summary pane.

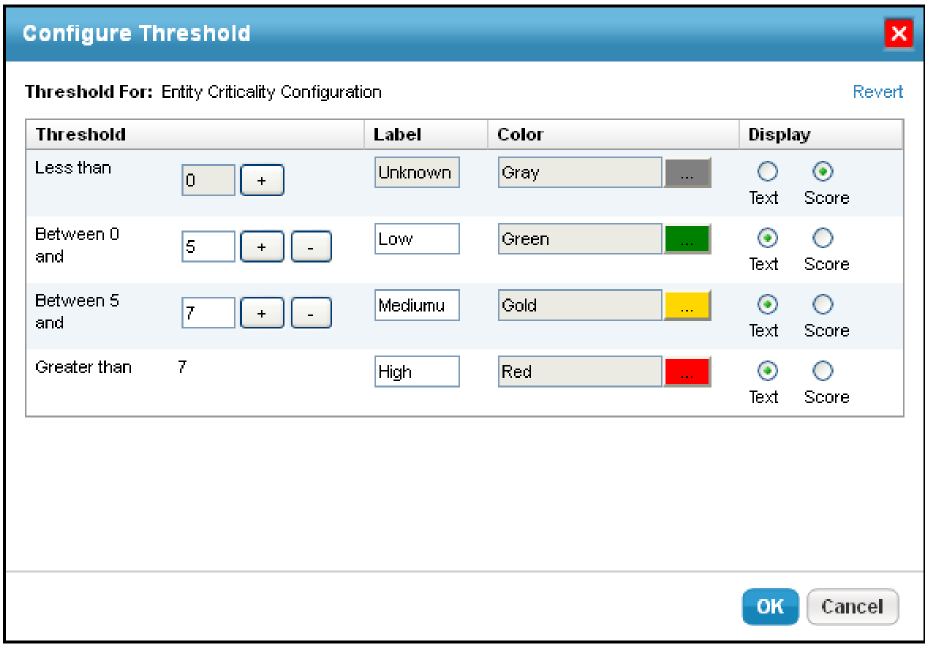


- **Criticality values:** Controls numeric values for the choices on Entity Details > Classification > Security Requirement. The Business criticality is an average of the confidentiality, integrity, and availability security requirement settings.It displays on the Assessment Details page and in reports.



To modify a range:

1. Go to **Configuration**> **Entity Configuration**.
2. Click **Ranges**.



Threshold For: Entity Criticality Configuration

Threshold		Label	Color	Display
Less than	0 +	Unknown	Gray ...	○ Text ● Score
Between 0 and	5 + -	Low	Green ...	● Text ○ Score
Between 5 and	7 + -	Mediumu	Gold ...	● Text ○ Score
Greater than	7	High	Red ...	● Text ○ Score

3. Choose **Entity Criticality Configuration** and click **Edit**.

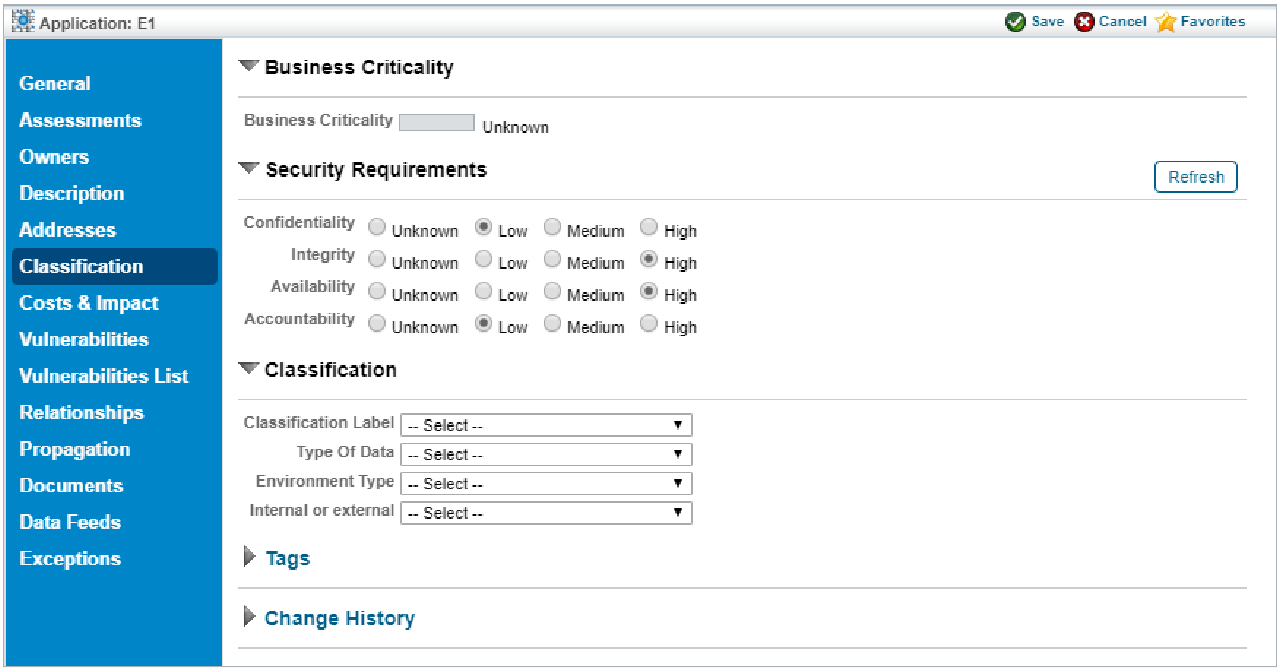
4. If you want to increase the Threshold range, click **+** (plus symbol).

5. Click **-**(minus symbol) to decrease the Threshold range. The color will change based on the selected Threshold range.

6. Click **OK**.

Setting the Criticality

The **Security Requirements** section allows you to manually set the entity criticality.



Business Criticality

Business Criticality Unknown

Security Requirements

Confidentiality	○ Unknown	● Low	○ Medium	○ High
Integrity	○ Unknown	○ Low	○ Medium	● High
Availability	○ Unknown	○ Low	○ Medium	● High
Accountability	○ Unknown	● Low	○ Medium	○ High

Classification

Classification Label: -- Select --

Type Of Data: -- Select --

Environment Type: -- Select --

Internal or external: -- Select --

The Security Requirements section of the Classification tab.

For discovered entities, you can configure a Control Target Profile to automatically set this value.

Criticality is not set when importing vulnerabilities from a saved XML file, even if the vulnerabilities were exported with criticality information. Vulnerabilities can be imported into other entities, and the criticality cannot be assumed.

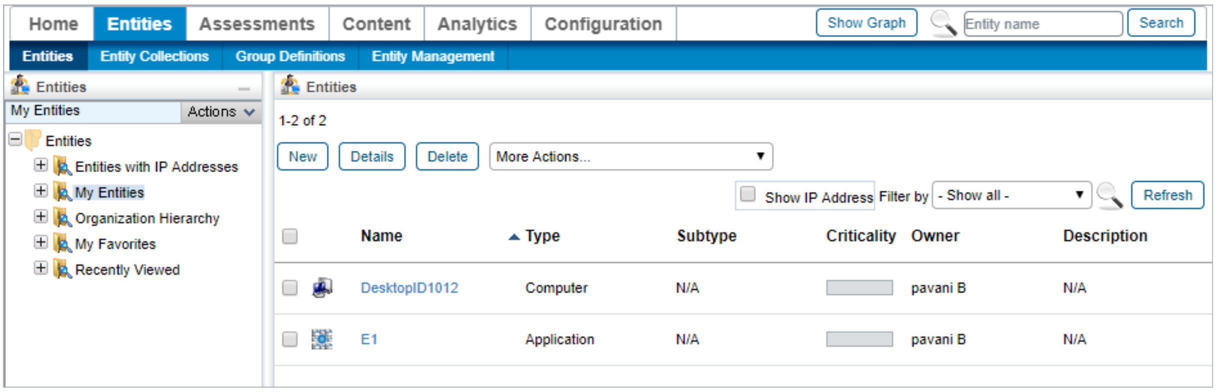
Clicking on the **Refresh** button will manually update the confidentiality, integrity, availability and accountability values of the entity.

These settings are used for:

- Automatically reassessing entities;
- Calculating the simple risk and compliance scores; and
- Calculating the Business Criticality score.

To set the criticality rating:

1. Go to **Entities** > **Entities**.
2. Select a group.



1-2 of 2

Filter by: - Show all -

	Name	▲ Type	Subtype	Criticality	Owner	Description
□	DesktopID1012	Computer	N/A		pavani B	N/A
□	E1	Application	N/A		pavani B	N/A

The Entities list.

3. Select an entity, then click **Details**.

4. Click the **Classification** tab, then click **Edit**.

5. Select the desired radio button in the **Security Requirements** section,

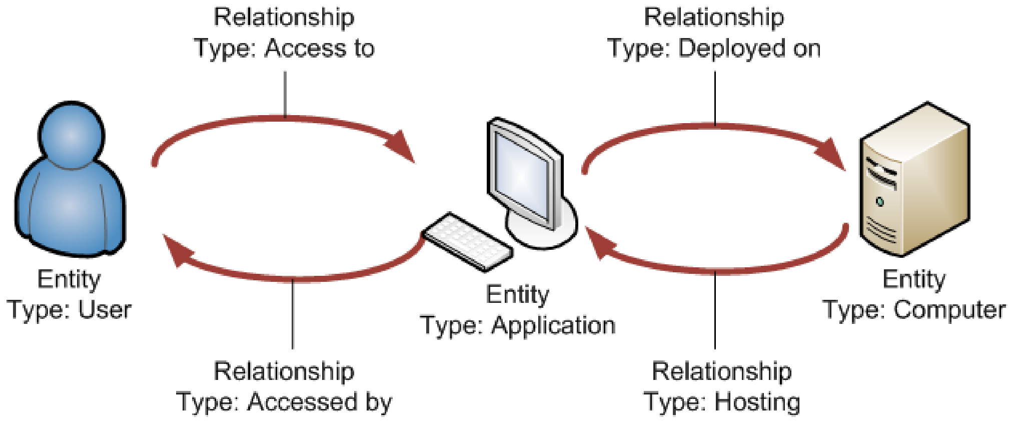
6. Click **Save**.

Related scores and settings are immediately updated.

About Entity Relationships

Entities are related to one another, usually in understood ways. An application is hosted on a particular computer; a user has access to a certain application, and so on. In RiskVision, entity relationships model these associations. Once the relationships between entities are understood by the system, you can propagate controls, risk scores, and other aspects of entities within a given program, for use in dashboards and reports.

Relationships between entities have types, and each are s bidirectional. If an application is deployed on a computer, the computer hosts the application.



Entity relationships allow risks to propagate from entity to entity. For example, Mark Smeeth (User) has access to a critical business application. He leaves his user name and password on a sticky note on his computer monitor at his desk. Despite the security measures (authorization and authentication controls) in place on the server, Mark's negligence increases the risk that an unauthorized person will access the server and application data.

When a parent entity is deleted, the child entities are not automatically included in assessments in which their parents had participated.

By default, entity relationship propagation settings are disabled.

Understanding Relationship Types

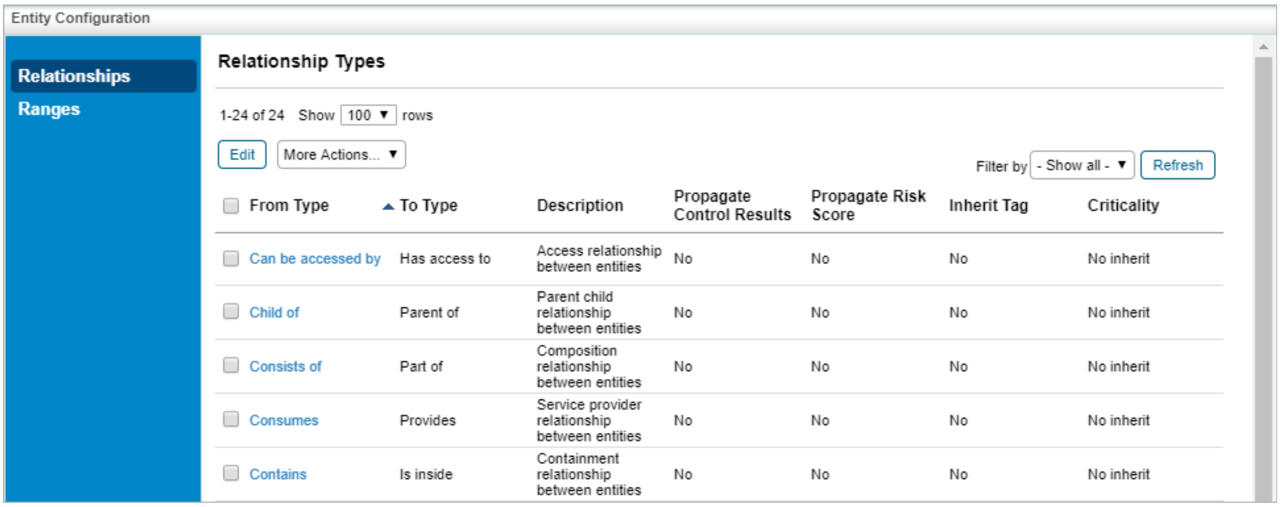
RiskVision defines several entity relationship types. Each relationship type includes propagation and inheritance settings that allow the entities to share controls and show aggregate scores. Propagation and inheritance settings can be specified separately for each direction of a bi-directional relationship.

- **Propagate Control Results**: Automatically import questionnaires and check results into assessments of the **To** entity.

- **Propagate Risk Score**. Shows aggregated scores of all **From** entity assessments in assessments of the To entity.

  Use score with propagate controls**.**

Only set propagation for policies, results, and scores in one direction of a relationship pair. For example, enable propagation on either the **Parent of** or the **Child of** relationship to avoid looping**.**



□ From Type	▲ To Type	Description	Propagate Control Results	Propagate Risk Score	Inherit Tag	Criticality
□ Can be accessed by	Has access to	Access relationship between entities	No	No	No	No inherit
□ Child of	Parent of	Parent child relationship between entities	No	No	No	No inherit
□ Consists of	Part of	Composition relationship between entities	No	No	No	No inherit
□ Consumes	Provides	Service provider relationship between entities	No	No	No	No inherit
□ Contains	Is inside	Containment relationship between entities	No	No	No	No inherit

The Relationships tab of the Entity Configuration screen.

To configure entity relationships:

1. Go to **Configuration** > **Entity Configuration**.
2. On the **Relationships** tab, select any of the relationship types.
3. Click **Edit**. The **Relationship Type** dialog displays.
4. Modify the settings, click **OK**, and click **Save**.

Programs and scores for entities with the relationship are updated immediately.

Predefined Relationship Types

The following types and their inverse are defined by RiskVision. That is, a relationship pair such as Child of/Parent of is specified in either direction. A source entity can have either the Child of or the Parent of relationship with a target entity. In the following table, the Relationship Type can be swapped with the Inverse Type.

Relationship type	Inverse type	Description
Can be accessed by	Has access to	Access relationship between entities
Child of	Parent of	Parent-child relationship between entities
Consists of	Part of	Composition relationship between entities
Contains	Is inside	Containment relationship between entities
Depends on	Needed by	Dependency relationship between entities
Deployed on	Hosting	Deployment relationship between entities
Entity Collection	Member of Entity Collection	Membership relationship between entities and entity collections
For	Has	Requirement relationship between entities
Group	Member of Group	Membership relationship between entities
Member of Program	Program	Membership relationship between entities and programs
Owned by	Owner of	Owner-ownee relationship between entities
Consumes	Provides	Service provider relationship between entities

Create Entity Relationships

Relationships can be defined between entities and entity collections.

Because entity relationships are always bi-directional, defining a relationship from one entity to another automatically defines the inverse relationship. When you define a relationship from one entity to another, two relationships are created. You can define a relationship between one source entity and more than one target entity, in which case several relationships are created. If you relate one source to three targets, six relationships are created.

For example, if you set the relationship of a user to 'Access to' an application, the system automatically adds the 'Accessed by' relationship to the application. Removing either 'Access to' or 'Accessed by' removes both definitions.

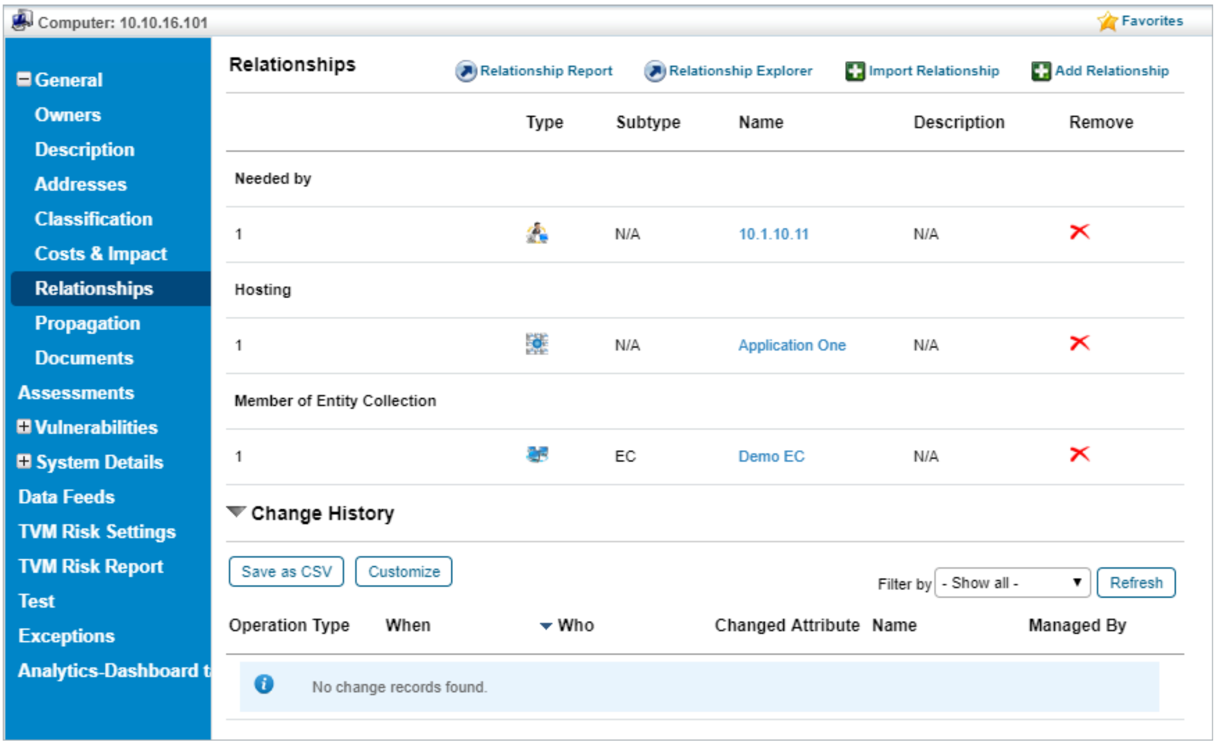
Relationships immediately affect assessments in progress and are visible in reports and dashboards the next time they run.

By default, control and score propagation settings are disabled. See Configuring Entity Relationship Attributes for more information.

> **EXAMPLE**
>
> You want to establish a parent-child relationship between entity A and entity B. As an entity owner, you know that an entity A must be the parent of entity B. In this case, you must add a 'Child of' relationship type on the Relationship tab of entity B and select entity A.

To establish a relationship between entities:

1. Go to **Entities** > **Entities**.
2. Click an entity to open.
3. Click the **Relationships** tab.



Computer: 10.10.16.101

Favorites

General
- Owners
- Description
- Addresses
- Classification
- Costs & Impact
- Relationships
- Propagation
- Documents

Assessments
Vulnerabilities
System Details
Data Feeds
TVM Risk Settings
TVM Risk Report
Test
Exceptions
Analytics-Dashboard t

Relationships

Relationship Report | Relationship Explorer | Import Relationship | Add Relationship

	Type	Subtype	Name	Description	Remove
Needed by					
1		N/A	10.1.10.11	N/A	✕
Hosting					
1		N/A	Application One	N/A	✕
Member of Entity Collection					
1		EC	Demo EC	N/A	✕

Change History

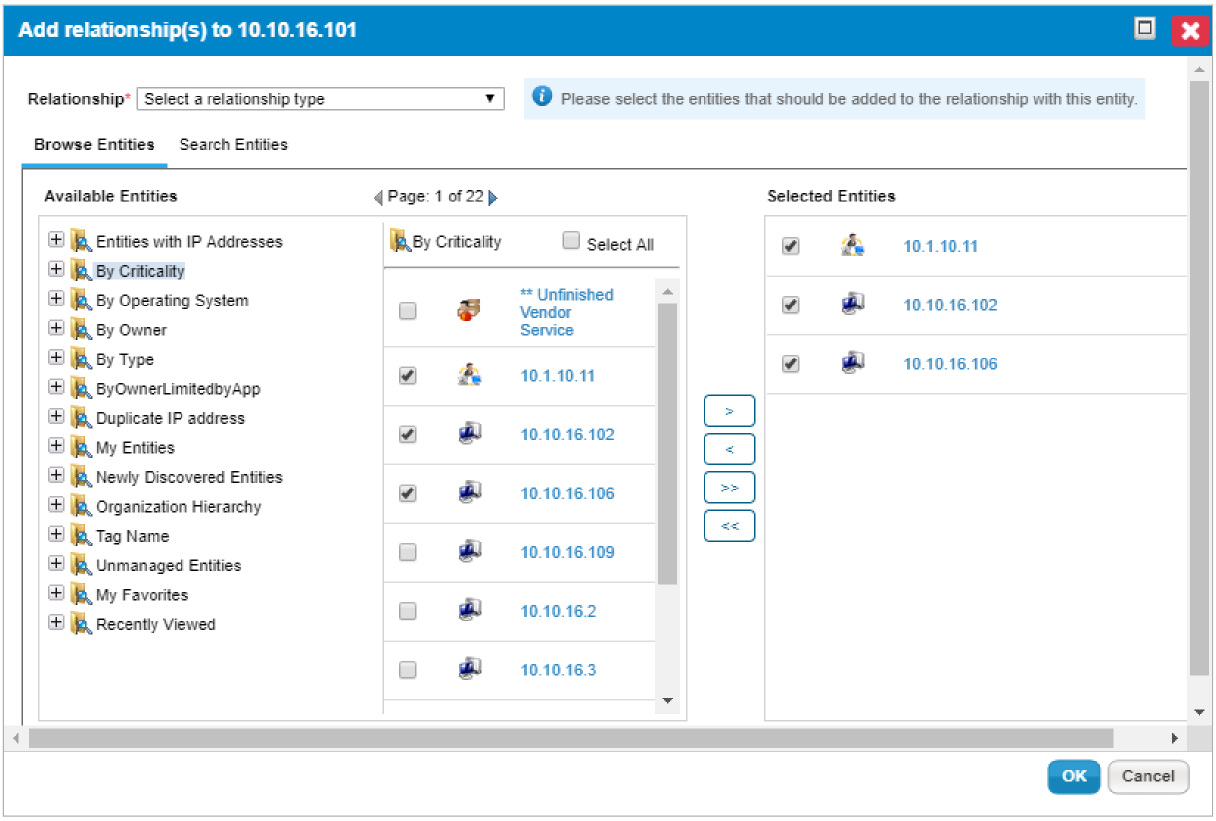
Save as CSV | Customize

Filter by - Show all - | Refresh

Operation Type	When	Who	Changed Attribute	Name	Managed By
No change records found.					

The Relationships table on the Relationships tab.

4. Click **Add relationship**.



Add relationship(s) to 10.10.16.101

Relationship* Select a relationship type

Please select the entities that should be added to the relationship with this entity.

The Add relationships dialog.

5. Click **Relationship** and choose a relationship type.

6. Select an entity group in the **Available Entities** box, or click **Search** to find a particular entity using the search criteria. To specify search criteria, select a field in the first dropdown box, then select a condition in the second dropdown box, and enter the search value in the box. Click **+** to add a new search condition. Click **Search** to retrieve the results for selecting entity(s). To select specific entities, check the box next to entity(s), or dynamic group, or **Select All**.

7. Click **OK**.

The specified relationship is added, as well as the inverse relationship from the target(s) to the original entity.

When a relationship is established with a dynamic group or its member(s):

- Selecting only specific entities within a dynamic group will create a relationship with only those entities.

- **Select All** will create a relationship with all the selected entities within a dynamic group, but not the dynamic group. Therefore, when members are added or removed from a dynamic group, the relationship of those entities with the entity collection are not affected.

- Selecting **dynamic group** will create a relationship with dynamic group itself. This selection creates a dynamic relation with members of the dynamic group. You must be careful with this selection because when members are added or removed from a dynamic group, their relationship with other entities is affected.

- Even though a member is shown on the**Entities** tab of entity collection, the **Relationship** tab will not show the EC Member or the Member of EC relationship type**.**

To remove a relationship:

1. Go to **Entities**> **Entities** and select an entity to open.

2. Click the **Relationships** tab.

3. Find a the relationship and click**X** in the **Remove** column.

4. Click **OK** .

The inverse relationship is automatically removed from the related entity.

Creating and Deleting Relationship Types

Beginning with version 7.0, RiskVision provides the ability to create and delete a relationship type when com.agiliance.asset.enableCreateRelationshipTypes=true property is added to the agiliance.properties file. You can only delete the relationship types you have created, if the relationship type is not in use.

To create a new relationship type

1. In the RiskVision application, go to **Configuration** > **Entity Configuration**. The **Relationships** tab details are displayed.
2. Click **New**. The **Create New Relationship** dialog appears.
3. In the dialog, enter the following fields.
    - **Relationship Name**. Name of the relation between entities
    - **Inverse of Relationship**. Name of the reverse relation
    - **Description**. Information that helps demonstrate the purpose of creating the relationship type
4. Click **OK**. The new relationship type is created.

User-defined relationship type allows the establishment of the relation only between the entities.

To delete a relationship:

1. In the RiskVision application, go to **Configuration** > **Entity Configuration**. The **Relationships** tab details are displayed.
2. In the **Relationships** tab, select the custom relationship type that is not in use, and click **Delete**. The relationship is deleted

Importing Relationships

You will need the **EntityRelationshipImportTemplate.xls** file to import relationships between entities and entity collection.

To import relationships:

1. In the RiskVision application, use one of the following navigation:
    - Go to **Entities** > **Entities** and select an entity to open its details page.
    - Go to **Entities** > **Entity Collections** and select an entity collection to open its details page.
2. Click the **Relationships** tab and click **Import Relationship**.
3. The **Import Entity Relationships** dialog appears. Click **Browse**, select the EntityRelationshipImportTemplate.xlsfile, click **Open**, and click **OK**.
4. The relationships are added.

Visualizing Relationships

Relationship visualization allows you to view associations between entities and entity collections for multiple levels of relationships. The Relationships Report provides the relationships of entity collections with entities, entity collections with other entity collections, and entities with other entities in graphical form.

To visualize entity relationships:

1. On the **Entities** menu, Click **Entities**. The **Entities** grid is displayed.
2. From within the Entities tree, expand the group containing the entity you want to visualize its relationships, and select the entity to open its details page.
3. On the entity details page, click the **Relationships** tab. The **Relationships** tab details are displayed.
4. Click **Relationship Report**. The web browser opens the **Relationship Report** in a new window.

To visualize entity collection relationships:

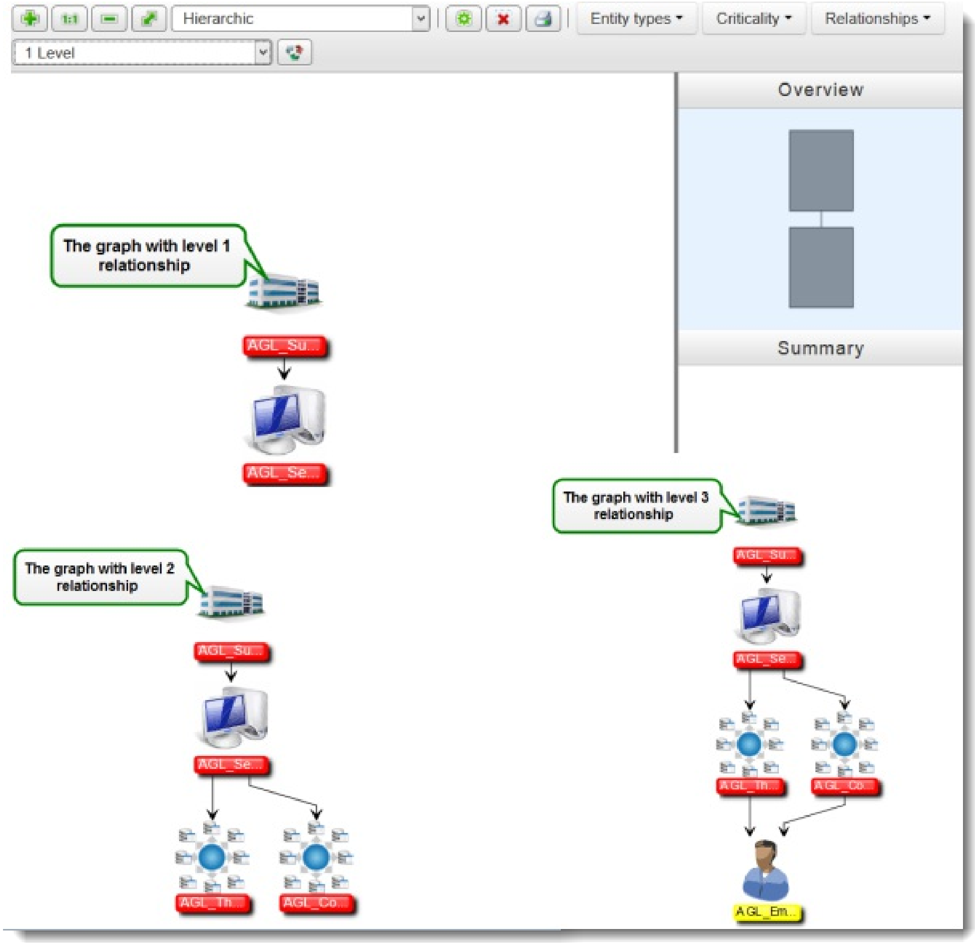
1. On the **Entities** menu, Click **Entity Collections**. The **Entity Collections** grid is displayed.
2. From within the Entity Collections tree, expand the group containing the entity collection you want to visualize its relationships, and select the entity to open its details page.
3. On the entity collection details page, click the **Relationships** tab. The **Relationships** tab details are displayed.
4. Click **Relationship Report**. The web browser opens the **Relationship Report** in a new window.

Relationship Report

The Relationship Report is displayed in a window in which different visualization tools are available to study relationships at varying depths from level 1 through level 6. In the Relationship Report, you can use filters, such as Entity Types, Criticality, and Relationships to exclude the leftover items not selected in the filter types. The default graphical view includes all of the entity types, criticalities, relationship types, and level 1 relationships the entity or entity collection has established with other entities and/or entity collections. The Level 1 relationship is one that is directly related to the source entity or entity collection. The graph also displays the criticality colors for the related entity and entity collections.

For each relationship type, the entities will be grouped based on the entity type when the count exceeds the value set in the com.agiliance.web.visulization.maxentitycountofsametype property.

The image below shows graphical layouts of level 1, level 2, and level 3 relationships.

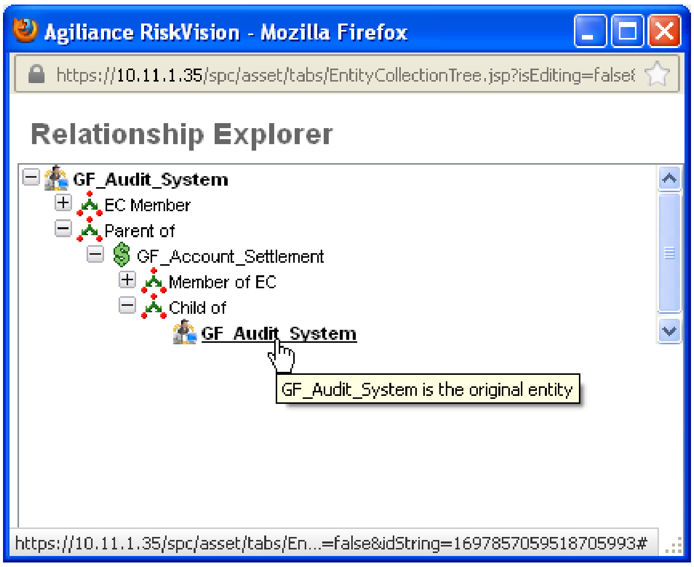


In the graphical layout shown above, the arrows indicate the relationships, the label colors associated with entities or entity collections indicate the criticality ratings, and double-clicking an entity or entity collection displays the details page.

Relationship Explorer

The **Relationships** tab for an entity or entity collection shows only the direct relationships of an entity or entity collection and not the indirect relationships. That is, the relationships of one or more entities or entity collections that are related to other entity or entity collection. The **Relationship Explorer** window allows you to drill down into a context of interdependence with other entities and entity collections and can be used to show all of the dependencies that a particular entity collection or entities, and not just those that are one level removed from that entity collection.

To open the **Relationship Explorer** window, select an entity or entity collection to open its details page, click the**Relationships** tab, and then click **Relationship Explorer** at the top right corner of the view.


Agiliance RiskVision - Mozilla Firefox
https://10.11.1.35/spc/asset/tabs/EntityCollectionTree.jsp?isEditing=false&
Relationship Explorer
GF_Audit_System
EC Member
Parent of
GF_Account_Settlement
Member of EC
Child of
GF_Audit_System
GF_Audit_System is the original entity
https://10.11.1.35/spc/asset/tabs/En...=false&idString=1697857059518705993#

At the top of the **Relationship Explorer** window, you will notice the entity (or entity collection) as a root. When you expand the root, any established relationships will appear. Expand each relationship type to see with what entities that the root entity is associated. You can also expand other entities to see if those entities have a relationship with any other entities, and so forth. This will provide an overview of the dependencies of the root entity or entity collection with the other entities or entity collections.

Assigning Vulnerabilities

To assign vulnerabilities to RiskVision objects, such as entities, tickets, controls and subcontrols, select the vulnerabilities by entering the search criteria. The **Select Vulnerabilities** interface has search elements with a text box or a check box that you can choose to narrow search results.

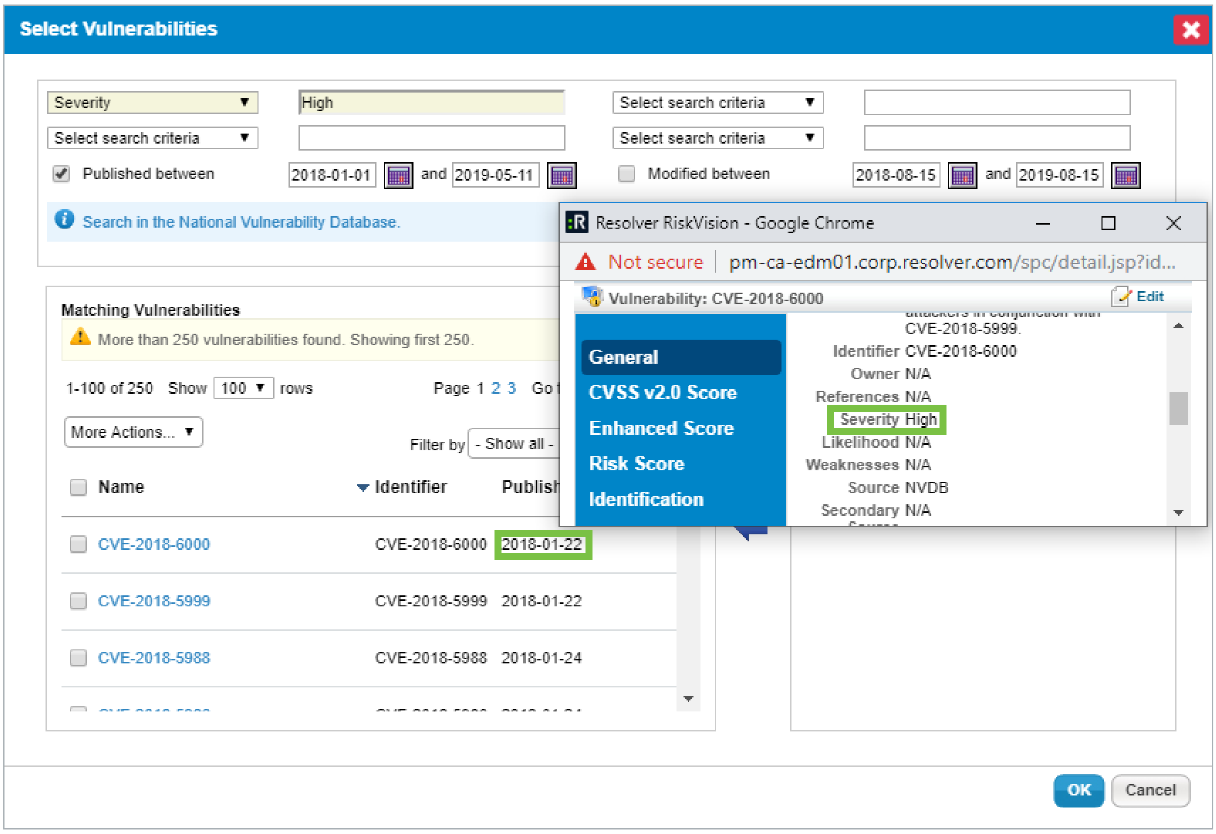
Search Element	Description
Title	Input the title text to search for vulnerabilities.
Identifier	Input the alphanumeric character to search for vulnerabilities.
Description	Input the vulnerability description to search for vulnerabilities.
Severity	Search for vulnerabilities based on their severity, such as low, medium, or high. Specify the complete string to search vulnerabilities based on the severity. For example, "med" will not return any results.
Source	Search for vulnerabilities based on their source, such as NVDB or Nessus.
Secondary Source	Search for vulnerabilities based on a secondary source, such as a scanner.
Technology	Search for vulnerabilities that are associated with a technology, such as Microsoft, Symantec, or Oracle.
Patch Name	Search for resolved vulnerability instances for which a patch has been applied.
CWE	Input the CWE value to search for vulnerabilities.
Other Identifiers	Search for vulnerabilities identified from a vulnerability database other than NVDB, such as MLIST or Security Focus.
CVSS Score less than	Search for vulnerabilities with a CVSS score less than a specified value.
CVSS Score greater than	Search for vulnerabilities with a CVSS score greater than a specified value. Use CVSS Score less than and greater than to find vulnerabilities between a score range.
Published between	Search for NVDB vulnerabilities and user-created vulnerabilities published between a specified period of time.
Modified between	Search for vulnerabilities modified between a specified period of time.

To assign a vulnerability:

1. Follow with the navigation in the following table for the desired object type:

Object	Navigation
Entity	Go to **Entities** > **Entities**, then select an entity to open. Click the **Vulnerabilities List** tab > **Assign**.
Control and Subcontrol	Go to **Content** > **Controls** and Questionnaires, then click a control or subcontrol to open. Click the **References** tab > **More Actions** > **Map to Vulnerability**.
Ticket	Go to **Home** > **Tickets**, then click a ticket to open. Click **Linked To** > **Vulnerabilities** tab > **Assign**.
Technology	Open RiskVision Threat and Vulnerability Manager. Go to **Vulnerabilities** > **All Technologies**, then click a technology to open. Click **Vulnerabilities** > **Link to Existing Vulnerabilities**.
Chart	Go to **Analytics** > **Charts**. Click a chart. Go to the **Filters** tab, then click +.

2. Search for vulnerabilities. Click **Select Search Criteria** and select search elements, or click the **Published between** or **Modified between** checkbox to select a date range. Click **Search**.



Select Vulnerabilities

Severity: High

Select search criteria

Select search criteria

Select search criteria

☑ Published between 2018-01-01 and 2019-05-11

□ Modified between 2018-08-15 and 2019-08-15

Search in the National Vulnerability Database.

Matching Vulnerabilities

More than 250 vulnerabilities found. Showing first 250.

1-100 of 250 Show 100 rows Page 1 2 3 Go t

Filter by - Show all -

□ Name	Identifier	Publish
□ CVE-2018-6000	CVE-2018-6000	2018-01-22
□ CVE-2018-5999	CVE-2018-5999	2018-01-22
□ CVE-2018-5988	CVE-2018-5988	2018-01-24

Resolver RiskVision - Google Chrome

Not secure | pm-ca-edm01.corp.resolver.com/spc/detail.jsp?id...

Vulnerability: CVE-2018-6000

CVE-2018-5999.

Identifier CVE-2018-6000

Owner N/A

References N/A

Severity High

Likelihood N/A

Weaknesses N/A

Source NVDB

Secondary N/A

Searching for elements in the Select Vulnerabilities dialog.

Search results are returned using:

- The "*AND*" operator - If the search criteria is applied to the different search elements.
- The "*Contains*" operator - If the input text is entered for a single search element.
- The "*Or*" operator - If the search criteria is a comma separated value for the Identifier search element.

- Select the check box next to the vulnerability, then use the right arrow to move the vulnerability into vulnerabilities to assign pane, and then click **OK**. To remove the selection, use the left arrow.

Operating Systems

Operating systems are available on the Computer, Network Device, and Mobile Device entity types. You can add a new operating system or use an existing one.

To add an operating system

1. In the **Entity Details** page, click the **System Details** tab.
2. Click **New**. The **Operating System** dialog appears.
3. In the Operating System dialog, enter the following fields:
   - **Full Name**. Enter the application name. This must be a relevant name.
   - **Description.** Enter any information that describes the operating system.
   - **Product**. Enter the product name. This is a short name for the operating system.
   - **Version**. Enter the version number of the operating system. This helps you notice the differences between the new version and old version.
   - **Vendor**. Enter the organization's name that is providing the operating system.
   - **Update**. Enter the software revision number, if available. You can derive this field if your operating system includes the most recent fix.
   - **Edition**. Enter the edition, such as standard, professional, or enterprise, if applicable.
   - **Language**. Enter the language if the operating system is procured for non-native English users.
   - **Version name**. Enter the version name, if available.
   - **Serial number**. Enter the unique number that identifies the operating system.
4. Click **OK**. The operating system is added.

To assign a predefined operating system:

1. In the entity details page, click the **System Details** tab.
2. Click **Add**. The **Choose Operating Systems** dialog appears.
3. In the dialog, use the following fields to search the application:
   - Title. Enter the operating system's title.
   - Version. Enter the operating system's version number.
   - Vendor. Enter the vendor's name.
     - The fields above can be used in combination to narrow the search results.
4. Click **Search** after entering the search field(s).
5. The results are returned and displayed in the **Known Operating Systems** box. If the search returns too many operating systems, use the scroll-bar to find the operating system.
6. After you locate the operating system, select the operating system in the **Known Operating Systems** box, and click the arrow pointing towards downward to move the operating system into the **Selected Operating Systems** box.
7. Click **OK**. The predefined operating system is added.

To edit an operating system:

1. In the entity details page, click the **System Details** tab.
2. Select the box in the corresponding operating system row. You can edit only the user-defined and scanner-imported operating systems.
3. Select **Edit** in the More Actions drop-down list. The **Operating System** dialog appears, where changes to the operating system can be made.
4. After the completion of changes, click **OK**.

To delete an operating system

1. In the entity details page, click the **System Details** tab.
2. Select the box in the corresponding operating system row and click **Delete**. The selected operating system is removed from the entity.

Applications

Applications installed can be found on the Computer, Network Device, and Mobile Device entity types. Typically, this data is brought in from scanners, but there may be times when you may want to manually update the data.

To add an application:

1. In the entity details page, click + to expand the **System Details** tab, and click **Applications**.
2. Click **New**. The **Application** dialog appears.
3. In the **Application** dialog, enter the following fields:
    - Full Name. Enter the application name. This must be a relevant name.
    - Description. Enter any information that describes the application.
    - Product. Enter the product name. This is a short name for the application.
    - Version. Enter the version number of the application or product. This helps you notice the differences
    - between the new version and old version.
    - Vendor. Enter the organization's name that offers the application.
    - Update. Enter the software revision number, if available. You can derive this field if your application
    - includes the most recent fix.
    - Edition. Enter the edition, such as standard, professional, or enterprise, if applicable.
    - Language. Enter the language if the application is procured for non-native English users
    - System Component: Select 'Yes' if the application is a system component.
4. Click **OK**. The application is added.

To assign a predefined application:

1. In the entity details page, click + to expand the System Details tab, and click Applications.
2. Click Add. The Choose Applications dialog appears.
3. In the dialog, use the following fields to search the application:

- Title. Enter the application's title.
- Version. Enter the application's version number.
- Vendor. Enter the vendor's name.

The fields above can be used in combination to narrow the search results.

4. Click **Search** after entering the search field(s).

5. The results are returned and displayed in the **Known Applications** box. If the search returns too many applications, use the scroll-bar to find the application.

6. After you locate the application, select the application in the **Known Applications** box, and click the arrow pointing downward to move the application into the **Selected Applications** box.

7. Click **OK**. The predefined application is added.

To edit an application

1. In the entity details page, click + to expand the **System Details** tab, and click **Applications**.
2. Select the box in the corresponding application row. You can edit only the user-defined and scanner-imported applications, since the applications that come from the NVD are not meant to be changed.
3. Select **Edit** in the More Actions drop-down list. The **Application** dialog appears, where changes to the application can be made.
4. After the completion of changes, click **OK**.

To delete an application:

1. In the entity details page, click + to expand the **System Details** tab, and click **Applications**.

2. Select the box in the corresponding application row and click **Delete**. The selected application is removed from the entity.

Ports

Ports are available on the Computer, Network Device, and Mobile Device entity types. Typically, ports are automatically imported into RiskVision by a vulnerability scanner, such as the Tenable Nessus Connector or the Qualys QualysGuard Connector. However, there may be times when you may want to manually modify port data.

To add a port

1. In the entity details page, click + to expand the **System Details** tab, and click **Ports**.
2. Click **New**. The **Port** dialog appears.
3. In the **Port** dialog, enter the following fields:
   - **Name**. Enter the port name.
   - **Protocol**. Enter the type of protocol, such as UDP and TCP.
   - **Protocol Number**. Enter the port number.
   - **Description.** Enter the information that helps understand the purpose of adding the port.
4. Click **OK**. The port is added.

To assign a predefined port:

1. In the entity details page, click **+** to expand the **System Details** tab, and click **Ports**.
2. Click **Add**. The **Choose Ports** dialog appears.
3. In the dialog, use the following fields to search the port:
   - Port Name. Enter the port's name.
   - Port Number. Enter the port's number.
   - Protocol. Enter the protocol, such as TCP or UDP.
4. The fields above can be used in combination to narrow the search results.
5. Click **Search** after entering the search field(s).
6. The results are returned and displayed in the **Known Ports** box. If the search returns too many ports, use the scroll-bar to find the port.
7. After you locate the port, select the port in the **Known Ports** box, and click the arrow pointing downwards to move the port into the **Selected Ports** box.
8. Click **OK**. The predefined port is added.

To edit a port:

1. In the entity details page, click **+** to expand the **System Details** tab, and click **Ports**.
2. Select the box in the corresponding port row. You can edit only the user-defined and scanner-imported ports
3. Select **Edit** in the More Actions drop-down list. The **Port** dialog appears, where changes to the port can be made.
4. Click **OK** after the completion of changes.

To delete a port:

1. In the entity details page, click **+** to expand the **System Details** tab, and click **Ports**.
2. Select the box in the corresponding port row and click **Delete**. The selected port is removed from the entity.

Manually modified port information will be overwritten by scanner data if the scanner data pertains to the same entity.

Performing Entity Actions

Entities can be managed using actions available in the **Entities** and **Entity Collection** grids. Entity actions are visible only if you have the Entity View and Entity Manage permissions. The actions provide a convenient way to update all of entities in a dynamic group where multiple entity attributes can be updated simultaneously, newly discovered entities can be allowed to participate in assessments, and entities can be excluded from participating in assessments.

The following table lists different actions and their purpose:

Action	Description
Manage Entities	Entities imported into RiskVision application must be managed before you include them in assessments.
Unmanage Entities	Refrains entities from participating in assessments.
Add Operating System to Entities	Adds operating system information to entities. Use the**Choose Operating System** dialog to search and select the operating system. For information about how to add the operating system to entities, see Operating Systems.
Remove Operating System from Entities	Removes operating system information from entities.
Add Application to Entities	Adds application(s) to entities. Use the **Choose Applications** dialog to search and select the applications. For information about how to add the application to entities, see Applications.
Remove Application from Entities	Removes application(s) from entities.
Copy Entity	Creates a copy of an entity into the selected assessment. While copying choose whether to copy an entity's attributes. Or use this action to copy an entity's data to other entities.
Batch Edit Entities	Select multiple entities to update common attributes simultaneously.
Save as CSV	Export entities out of the RiskVision application in Excel format.
Show Relationship Graph	Display a graph showing the relationship between the selected entities.
Run Contextual Report	View a contextual report of the selected entities.

The **Export Entities** option is configurable. If you have a lot entities, you can choose to turn off the **Export Entities** option. This can be done by modifying the property `ui.asset.grid.export.enable`

If `ui.asset.grid.export.enable` = True, then **Export Entities** appears in the **More Actions** drop-down.

If grid.csvexport.all = True, then the users will be able to export entities to CSV files.

Working with Contextual Reports of Entities

You can generate reports on more than a single entity or entity collection. For example, you can see all of the vulnerabilities that exist on a dynamic group containing your Windows and Linux servers. Or, you can generate a consolidated report showing the compliance status of all servers that a specific employee is responsible for.

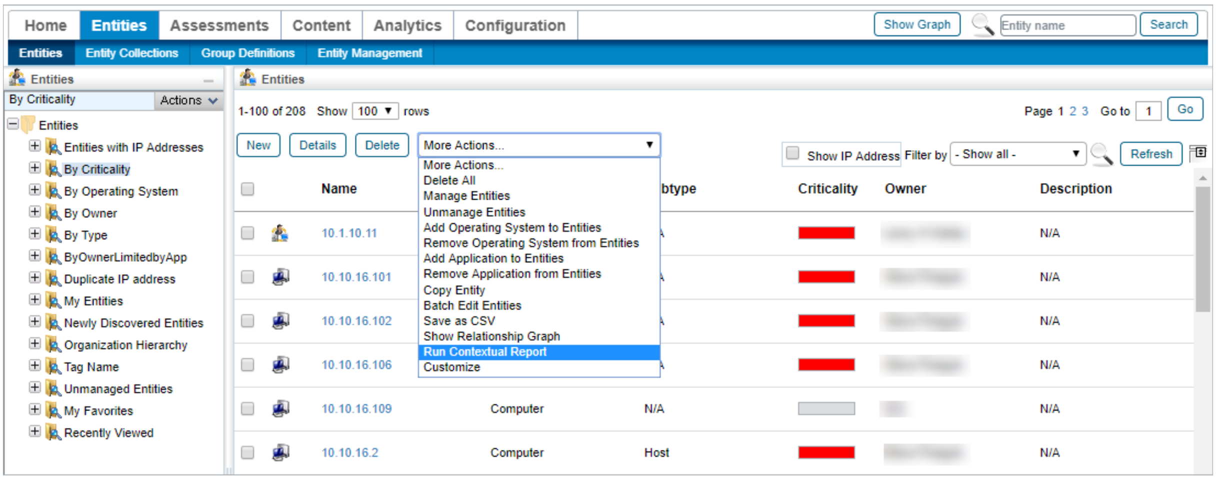
With contextual reports you can:

- View reports on dynamic groups. For example, it would be easy to create a contextual report on a given owner’s entities and entity collections, a given type of entity, or any other attribute that can be represented by a dynamic group.
- Use the **Advanced Search** to precisely define the list of entities or entity collections you want to see and then create a contextual report on these entities or entity collections. For example, you can search by IP address, discovery source, and entity risk, and then run a contextual report.

The contextual reporting feature works with both reports that come with RiskVision and reports you define yourself.

To view a contextual report:

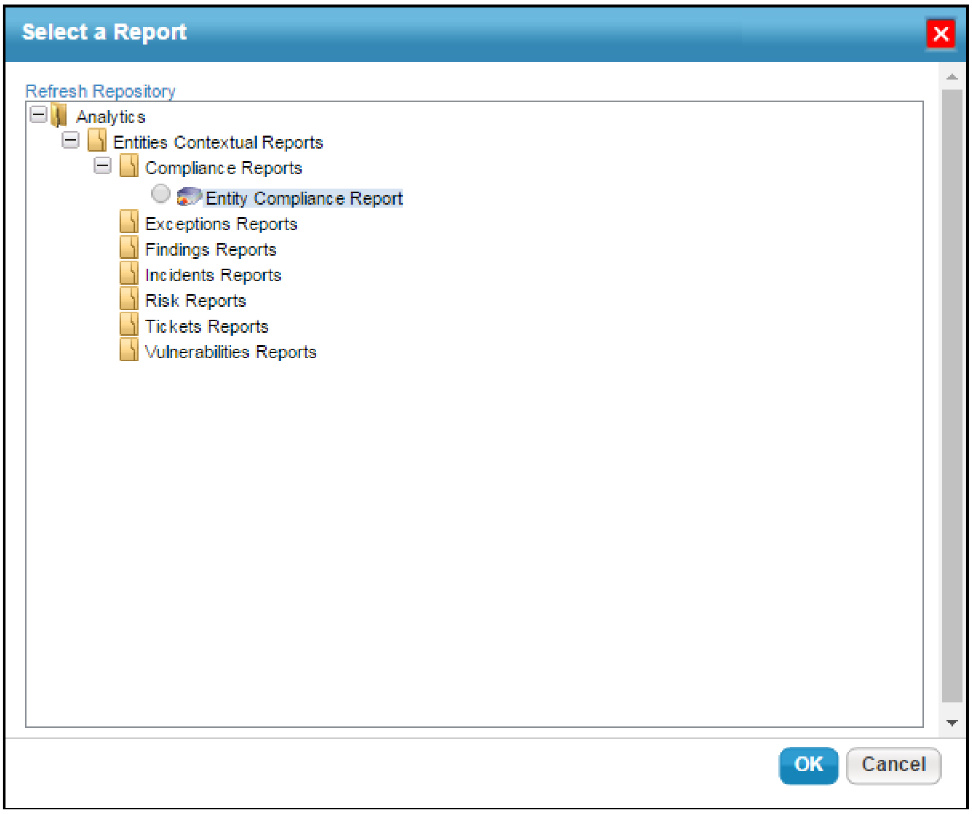
1. Open the Entities page.
2. Select the required entities, then click **More Actions** > **Run Contextual Report**.



Name		btype	Criticality	Owner	Description
10.1.10.11			🟥	[redacted]	N/A
10.10.16.101			🟥	[redacted]	N/A
10.10.16.102			🟥	[redacted]	N/A
10.10.16.106			🟥	[redacted]	N/A
10.10.16.109	Computer	N/A	⬜	[redacted]	N/A
10.10.16.2	Computer	Host	🟥	[redacted]	N/A

Running a contextual report.

3. Browse and select the required report. These reports can also be created in JasperReports and run directly from the **Entities** page.



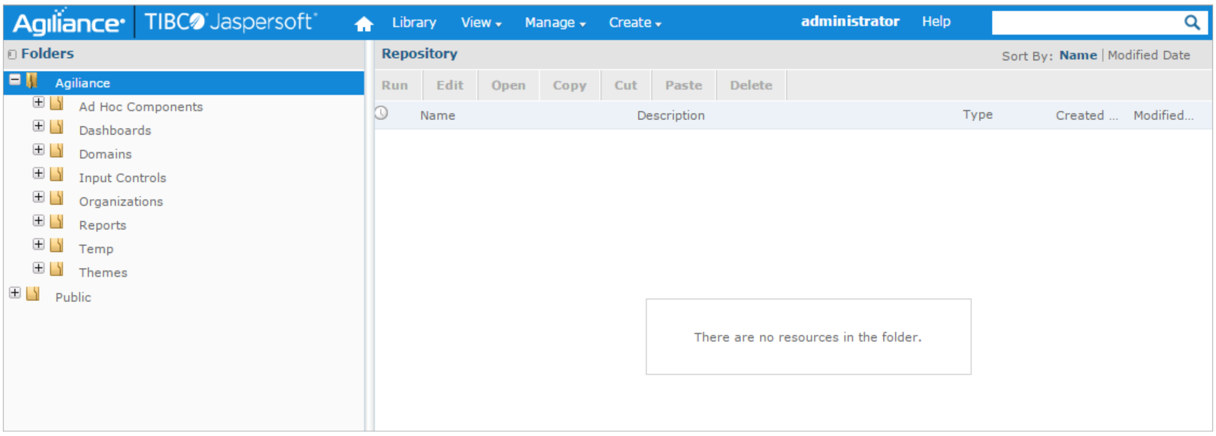
Selecting a report in the Select a Report dialog.

A contextual report related to the selected entities is generated based on the parameters configured for the selected report in JasperReports Server. The entities you have selected are passed to the report as parameters.

Create a Contextual Report in JasperReports Server

To create a contextual report to report against entities:

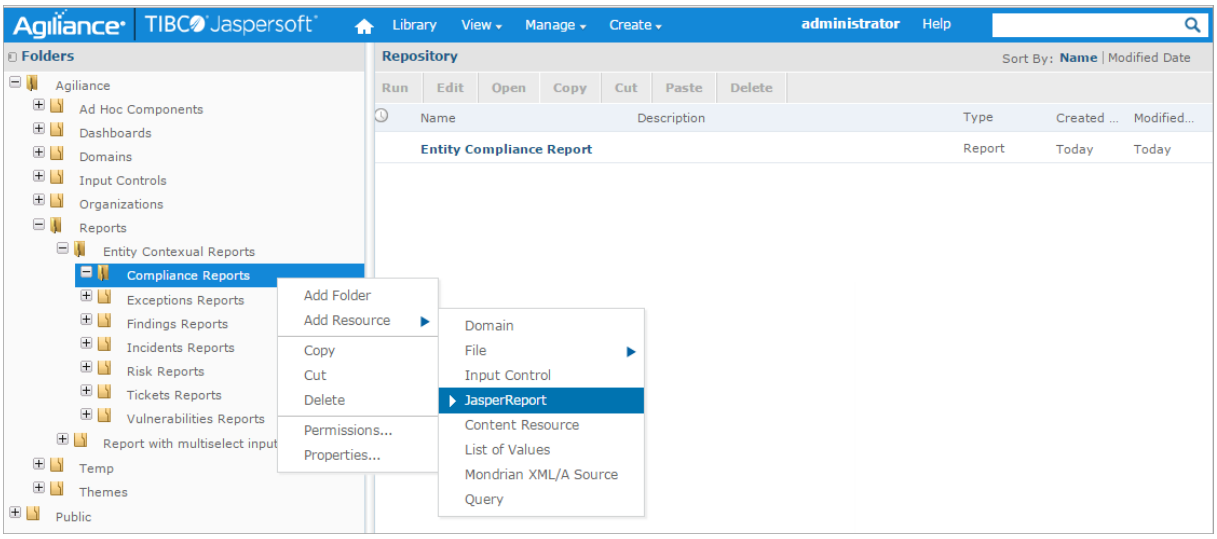
1. Click **Analytics** > **R7 charts** to open the **JasperReports Server** page.
2. Click **View > Repository**.



There are no resources in the folder.

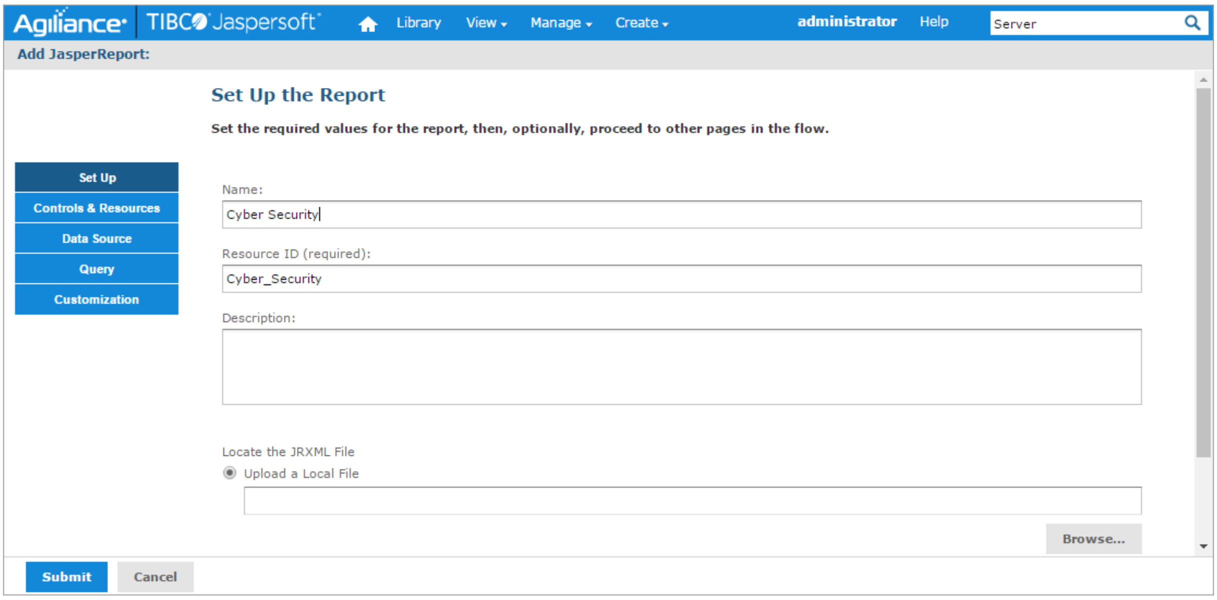
The Repository page.

3. Click **RiskVision** > **Reports** > **Entity Contextual Reports**.
4. Right-click on the type of contextual report that you want to create, then click **Add Resource** > **JasperReport**.



Name	Description	Type	Created ...	Modified...
Entity Compliance Report		Report	Today	Today

5. Follow the onscreen instructions to create a new report.



Set Up the Report

Set the required values for the report, then, optionally, proceed to other pages in the flow.

Name: Cyber Security

Resource ID (required): Cyber_Security

Description:

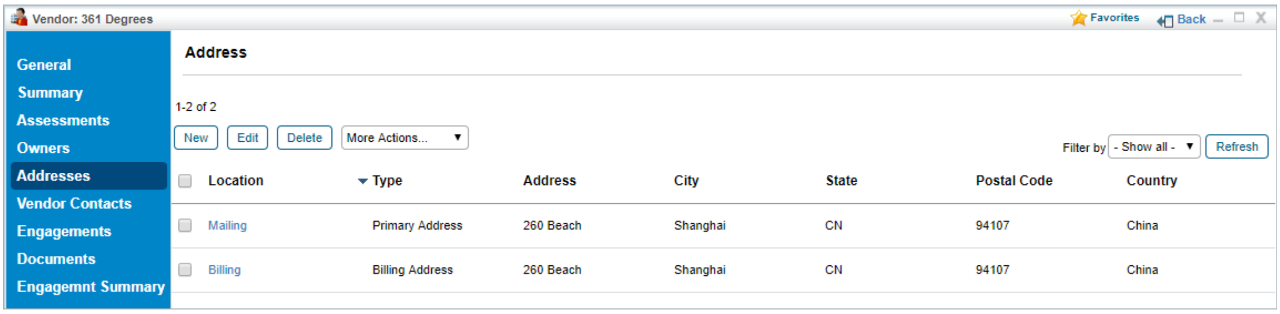
Locate the JRXML File

● Upload a Local File

After you have created a report, you can generate this contextual report from the **Select a Report** pop-up.

Entity Attribute Screens

This section provides the list of **Entity** attribute screens in RiskVision.

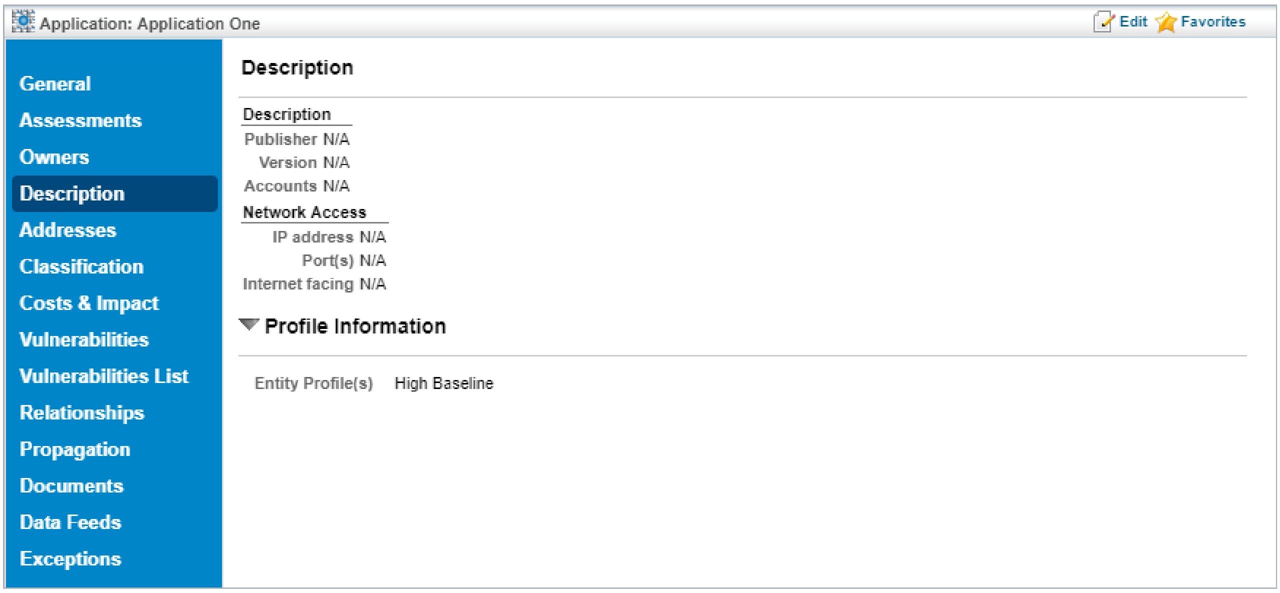


Address

1-2 of 2

	Location	Type	Address	City	State	Postal Code	Country
□	Mailing	Primary Address	260 Beach	Shanghai	CN	94107	China
□	Billing	Billing Address	260 Beach	Shanghai	CN	94107	China

The Addresses tab of a vendor.



Description

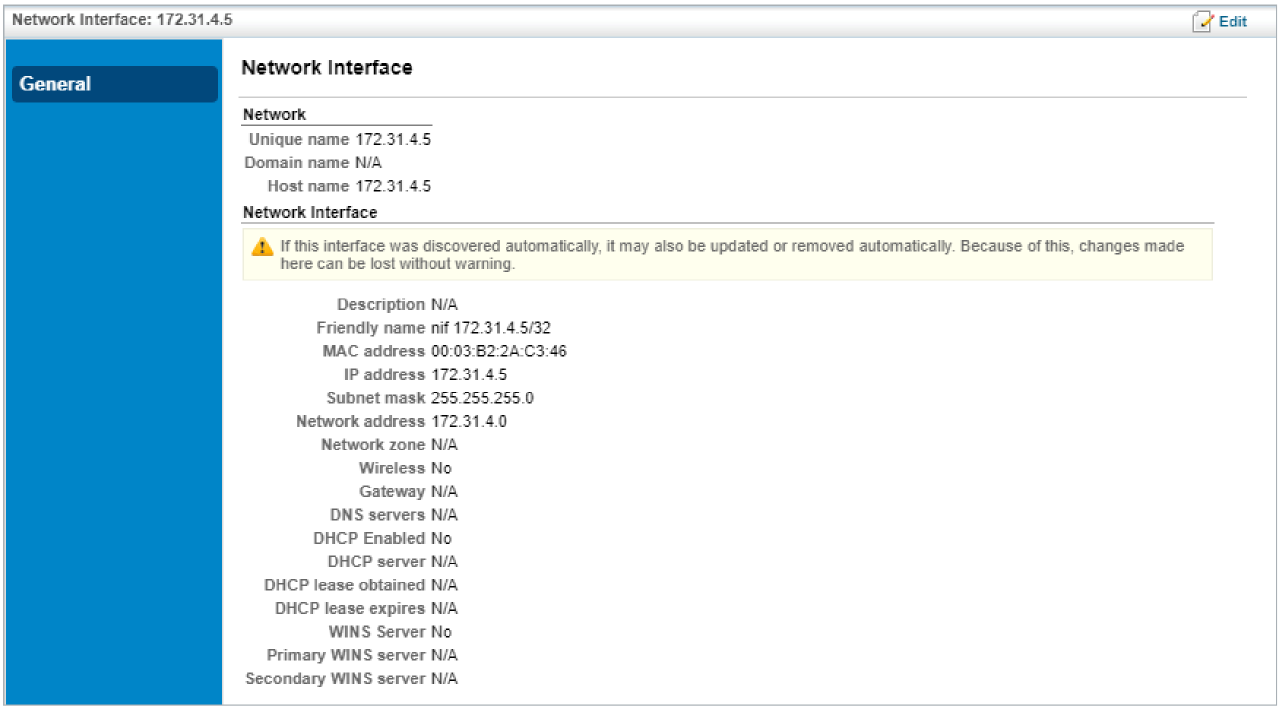
Description
Publisher N/A
Version N/A
Accounts N/A

Network Access
IP address N/A
Port(s) N/A
Internet facing N/A

Profile Information

Entity Profile(s) High Baseline

The Description tab of an application type entity.



Network Interface: 172.31.4.5

Network Interface

Network

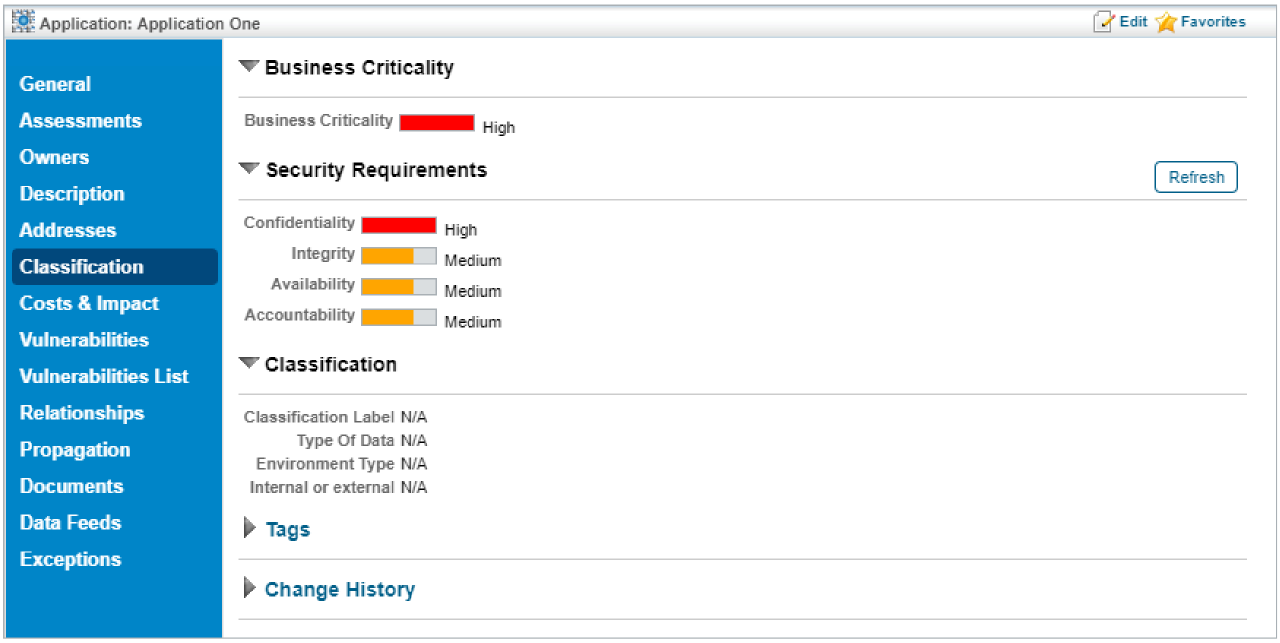
Unique name 172.31.4.5
Domain name N/A
Host name 172.31.4.5

Network Interface

⚠ If this interface was discovered automatically, it may also be updated or removed automatically. Because of this, changes made here can be lost without warning.

Description N/A
Friendly name nif 172.31.4.5/32
MAC address 00:03:B2:2A:C3:46
IP address 172.31.4.5
Subnet mask 255.255.255.0
Network address 172.31.4.0
Network zone N/A
Wireless No
Gateway N/A
DNS servers N/A
DHCP Enabled No
DHCP server N/A
DHCP lease obtained N/A
DHCP lease expires N/A
WINS Server No
Primary WINS server N/A
Secondary WINS server N/A

The General tab of a network interface.



Application: Application One

Business Criticality

Business Criticality 🟥 High

Security Requirements

Confidentiality 🟥 High
Integrity 🟧 Medium
Availability 🟧 Medium
Accountability 🟧 Medium

Classification

Classification Label N/A
Type Of Data N/A
Environment Type N/A
Internal or external N/A

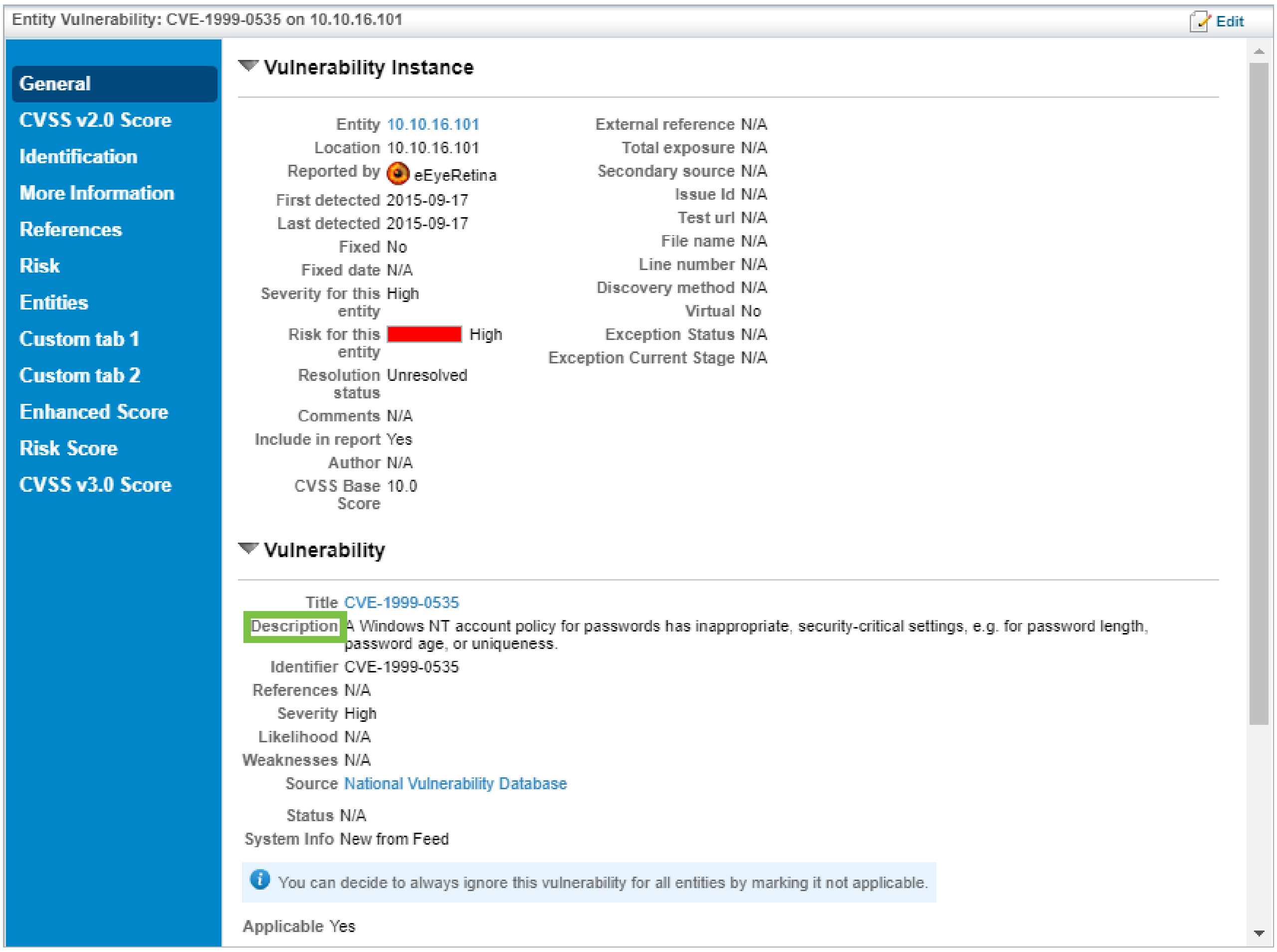
Tags

Change History

The Classification tab of an application type entity.

Clicking the **Refresh** button will:

- Update the criticality based on the classification survey; and
- Update any changes made to the classification through the entity user interface.


Entity Vulnerability: CVE-1999-0535 on 10.10.16.101

Vulnerability Instance

Entity 10.10.16.101
Location 10.10.16.101
Reported by eEyeRetina
First detected 2015-09-17
Last detected 2015-09-17
Fixed No
Fixed date N/A
Severity for this entity High
Risk for this entity 🟥 High
Resolution status Unresolved
Comments N/A
Include in report Yes
Author N/A
CVSS Base Score 10.0

External reference N/A
Total exposure N/A
Secondary source N/A
Issue Id N/A
Test url N/A
File name N/A
Line number N/A
Discovery method N/A
Virtual No
Exception Status N/A
Exception Current Stage N/A

Vulnerability

Title CVE-1999-0535
Description A Windows NT account policy for passwords has inappropriate, security-critical settings, e.g. for password length, password age, or uniqueness.
Identifier CVE-1999-0535
References N/A
Severity High
Likelihood N/A
Weaknesses N/A
Source National Vulnerability Database
Status N/A
System Info New from Feed

You can decide to always ignore this vulnerability for all entities by marking it not applicable.

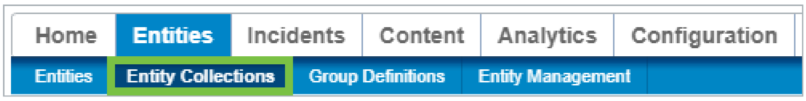
Applicable Yes

The Description of an Entity Vulnerability.

Using Entity Collections

An entity collection system is a type of entity (or asset) that behaves as an entity, but refers to a set of entities, such as a system, process, or department. If you prefer to use a name other than entity collection, for example, "System," you can rename the term in the UIDictionary.xml file.

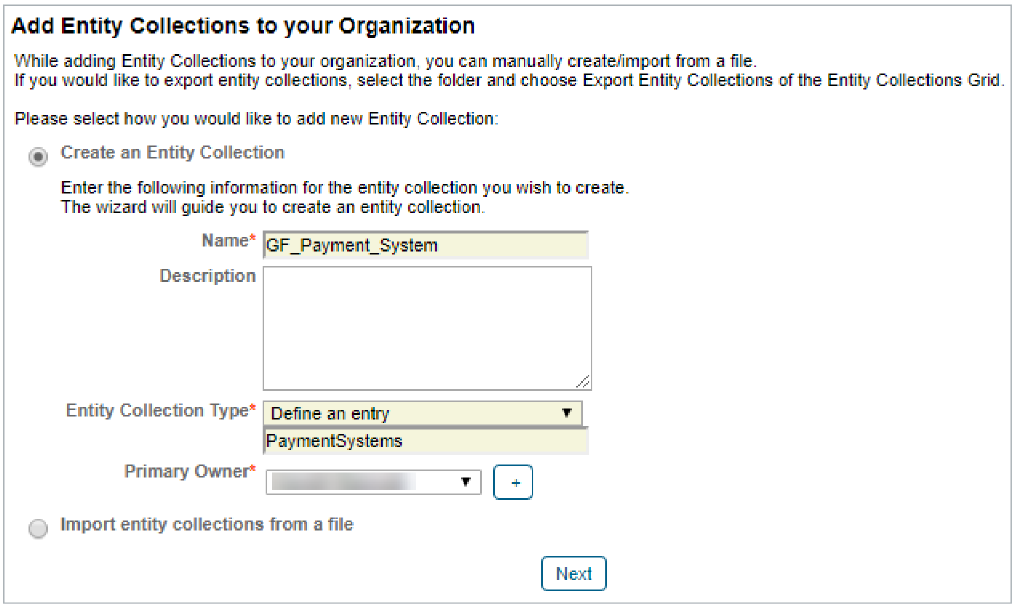
Dynamic groups and organization hierarchy containers with entity collections as members will appear in the navigation pane. An entity collection will appear in the **By Criticality**, **By Type**, or **Organization Hierarchy** pre-configured groups in the **Entity Collections** grid, by default. To add more pre-configured groups to the **Entity Collections** grid, go to **Entities** > **Group Definitions**, click **Add Pre-Configured Groups**, check the box next to the dynamic groups, and then click **Add Groups**.



The Entity Collections tab.

To create an entity collection:

1. Go to **Entities** > **Entity Collections** and click **New**.



Add Entity Collections to your Organization

While adding Entity Collections to your organization, you can manually create/import from a file.
If you would like to export entity collections, select the folder and choose Export Entity Collections of the Entity Collections Grid.

Please select how you would like to add new Entity Collection:

● Create an Entity Collection

Enter the following information for the entity collection you wish to create.
The wizard will guide you to create an entity collection.

Name* GF_Payment_System

Description

Entity Collection Type* Define an entry ▼
PaymentSystems

Primary Owner* [redacted] ▼ +

○ Import entity collections from a file

Next

The Add Entity Collections to your Organization screen.

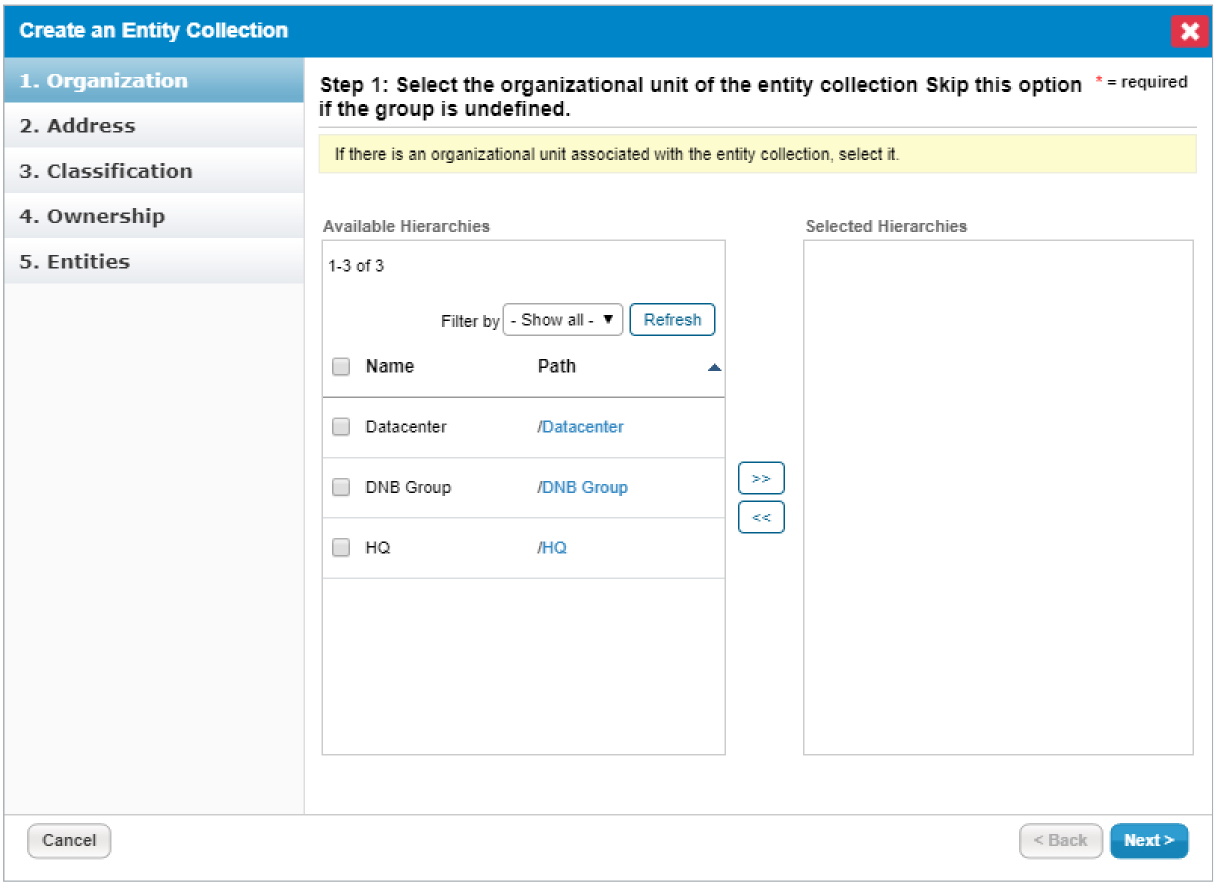
2. Enter a name in the **Name** field.

3. **Optional:** Enter a description in the **Description** field.

4. Click the **Entity Collection** Type dropdown and select a sub type, or define a new subtype. As a logged in user, you will be the primary owner for the entity collection by default. To change the primary owner, choose a name from the **Primary Owner** dropdown list or click **+**.

5. Click **Next**.

6. Select an organizational hierarchy container from the **Available Hierarchies** section, if available.



Create an Entity Collection

Step 1: Select the organizational unit of the entity collection Skip this option if the group is undefined.

* = required

If there is an organizational unit associated with the entity collection, select it.

Available Hierarchies

1-3 of 3

Filter by - Show all -

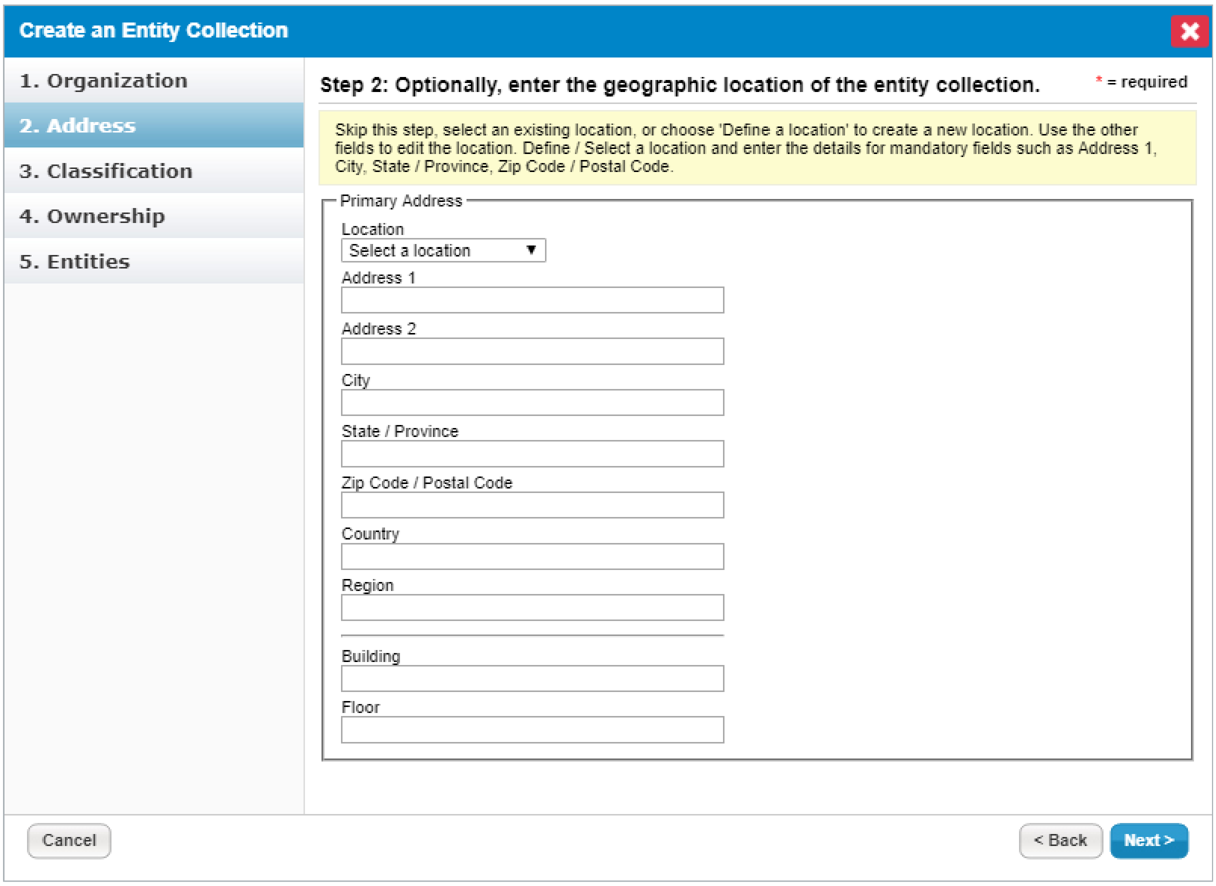
□	Name	Path
□	Datacenter	/Datacenter
□	DNB Group	/DNB Group
□	HQ	/HQ

Selected Hierarchies

The Organization step of the Create an Entity Collection wizard.

7. Click **Next**.

8. **Optional:** Enter the entity collection's geographic location.



Create an Entity Collection

Step 2: Optionally, enter the geographic location of the entity collection.

* = required

Skip this step, select an existing location, or choose 'Define a location' to create a new location. Use the other fields to edit the location. Define / Select a location and enter the details for mandatory fields such as Address 1, City, State / Province, Zip Code / Postal Code.

Primary Address

Location: Select a location

Address 1

Address 2

City

State / Province

Zip Code / Postal Code

Country

Region

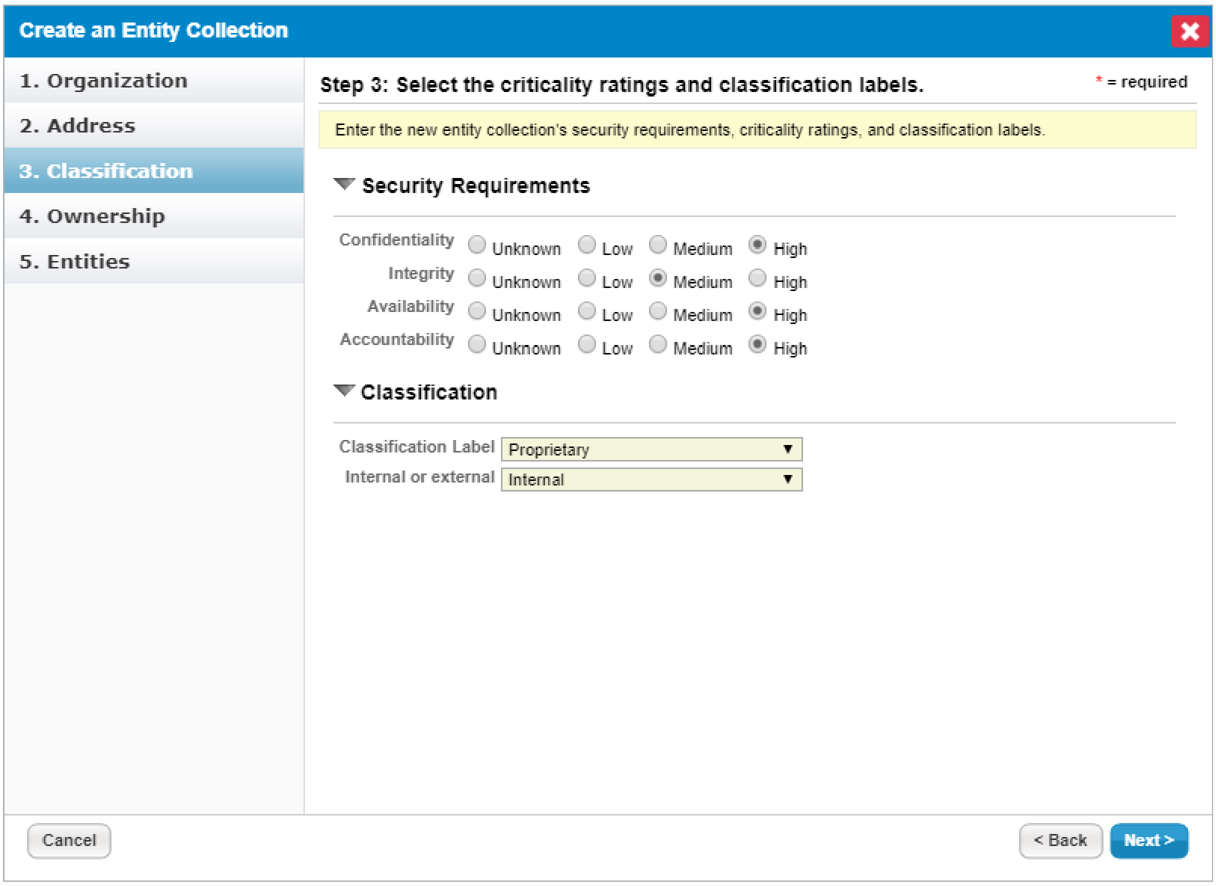
Building

Floor

The Address step of the Create an Entity Collection wizard.

9. Click **Next**.

10. Classify the new entity collection in terms of confidentiality, integrity, availability, accountability, and classification, and specify if it's internal or external.



Create an Entity Collection

1. Organization
2. Address
3. Classification
4. Ownership
5. Entities

Step 3: Select the criticality ratings and classification labels.

* = required

Enter the new entity collection's security requirements, criticality ratings, and classification labels.

Security Requirements

Confidentiality	○ Unknown	○ Low	○ Medium	● High
Integrity	○ Unknown	○ Low	● Medium	○ High
Availability	○ Unknown	○ Low	○ Medium	● High
Accountability	○ Unknown	○ Low	○ Medium	● High

Classification

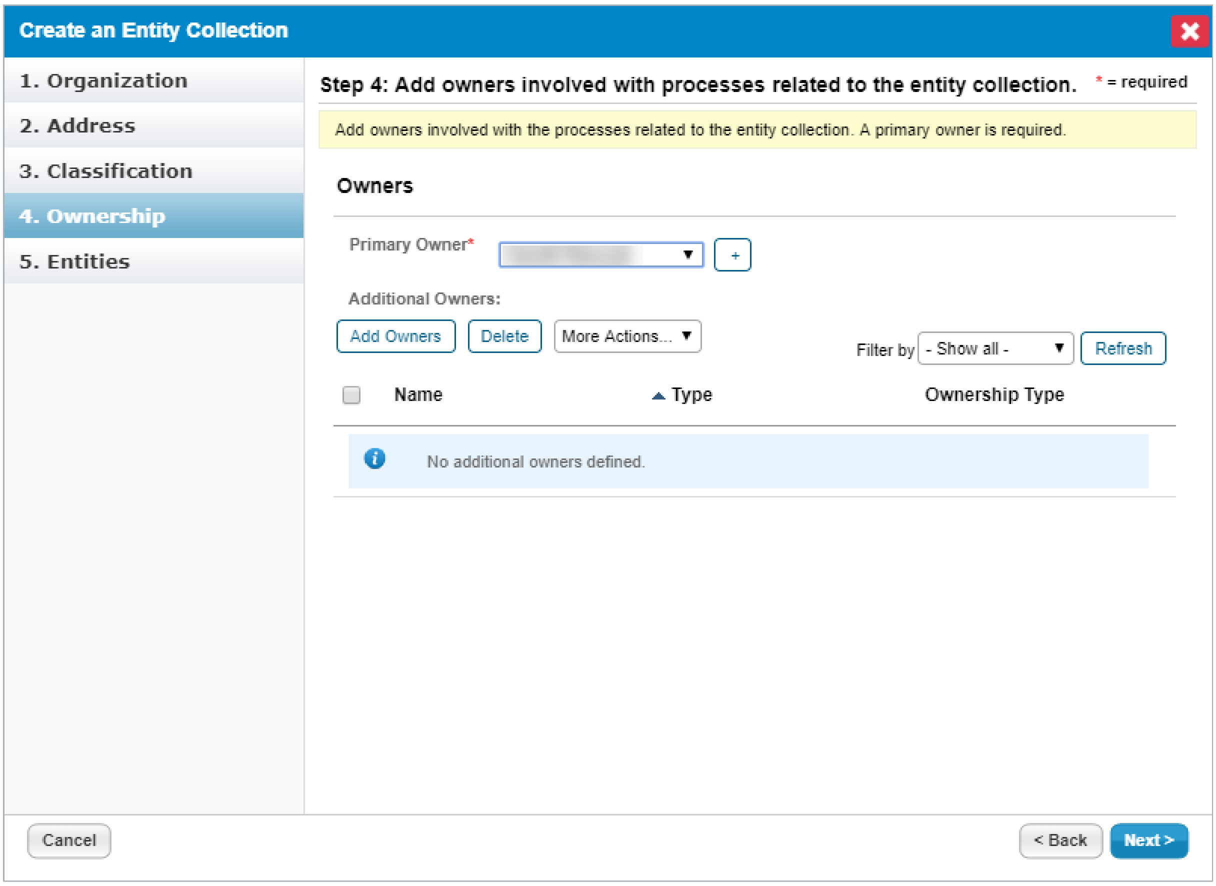
Classification Label: Proprietary

Internal or external: Internal

The Classification step of the Create an Entity Collection wizard.

11. Click **Next**.

12. Select a different primary owner, if appropriate. The entity collection must have a primary owner. You can also specify additional owners.



Step 4: Add owners involved with processes related to the entity collection. * = required

Add owners involved with the processes related to the entity collection. A primary owner is required.

Owners

Primary Owner*

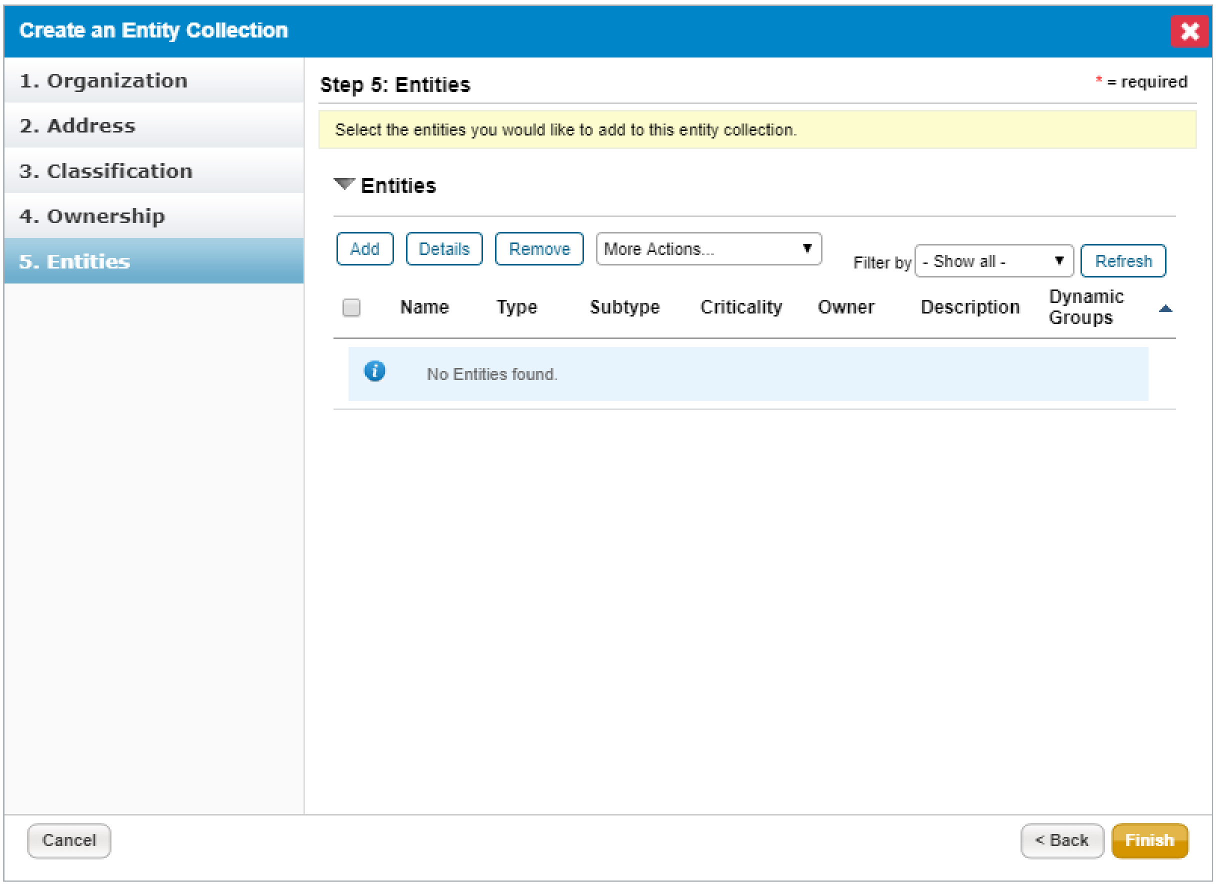
Additional Owners:

□	Name	▲ Type	Ownership Type
	No additional owners defined.		

The Ownership step of the Create an Entity Collection wizard.

13. Click **Next** to continue.

14. Click **Add**.



Create an Entity Collection

1. Organization
2. Address
3. Classification
4. Ownership
5. Entities

Step 5: Entities

* = required

Select the entities you would like to add to this entity collection.

Entities

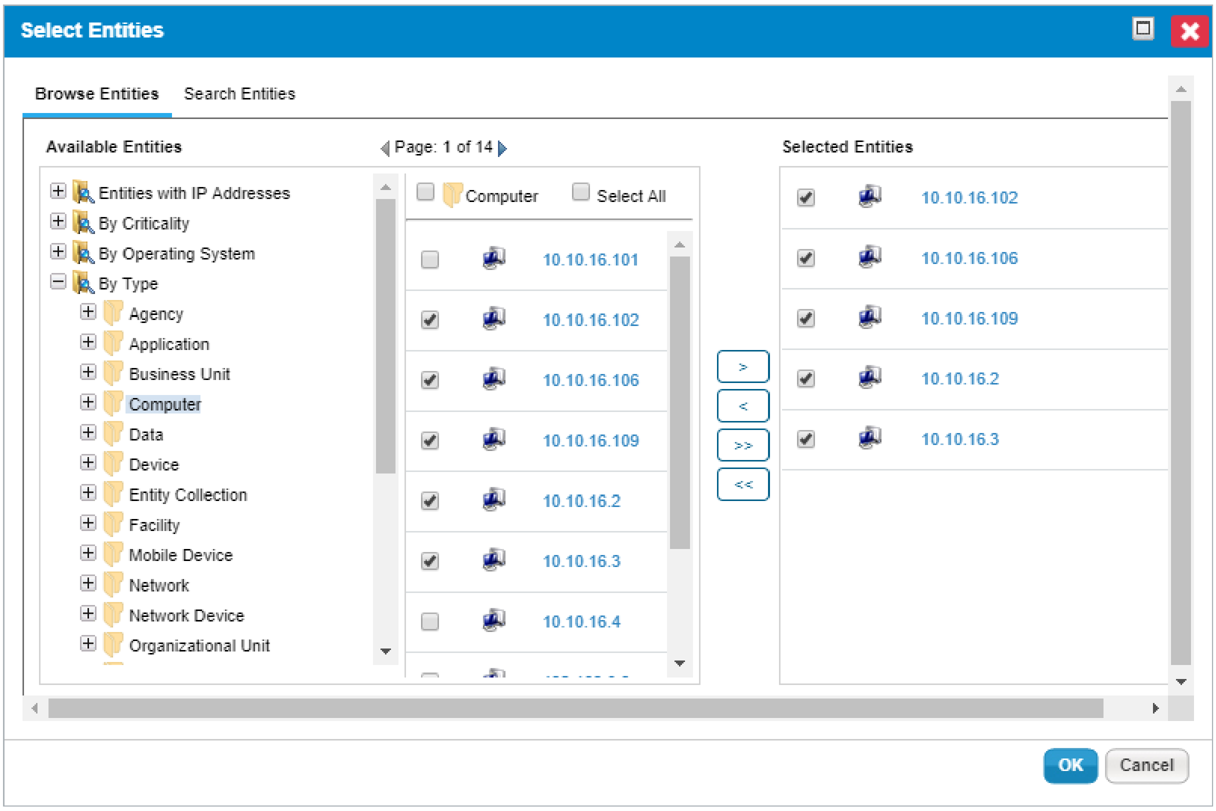
□	Name	Type	Subtype	Criticality	Owner	Description	Dynamic Groups

No Entities found.

The Entities step of the Create an Entity Collection wizard.

15. Go to the **Browse Entities** tab > **Available Entities** and select a group. Or, click **Search** to search for an entity. After the entity(s) or group is found, select any appropriate entities, or **Select All**, or select the dynamic group.

16. Click **>>** to move the entity(s) or group to the **Selected Entities** box, then click **OK**.



The Select Entities dialogue.

When adding a dynamic group or its members:

- Selecting only specific entities within a dynamic group will associate only those entities as members of an entity collection.
- Selecting a dynamic group will associate all entities as members of an entity collection. When members are added or removed from a dynamic group, those dynamic members within an entity collection are updated automatically.
- Select All will associate all entities as members of an entity collection, but not the dynamic group. When members of a dynamic group are added or removed, those dynamic group members within the entity collection are not updated.
- Entities that are a part of more than one dynamic group will be added only once to an entity collection, even if you add all dynamic groups containing that entity.

17. Click **Finish**.The new entity collection will be an 'entity collection' type entity.

To edit an entity collection:

1. Go to **Entities** > **Entity Collections** and locate the entity collection that you want to edit using the tree and grid views.
2. Click an entity collection name to open.
3. Select the tab with the information that needs to be edited, such as**General**, **Entities**, **Description**, or **Classification**.
4. Click **Edit** and make changes as needed.
5. Click **Save**.

To delete an entity collection:

Entity collections that are not associated with an assessment can be deleted.

1. Go to **Entities** > **Entity Collections** and locate the entity collection to be deleted using the tree and grid views.
2. Select the checkbox next to the entity collection to be deleted.
3. Click **Delete**, then click **OK**.

Entity collection task limitations

There is currently no predefined template for importing entity collections into RiskVision, so they must be entered manually.

Understanding Entity Collection Details

Unlike with entities, entity collection details tabs do not vary. When you create an entity collection, it's created as 'entity collection' type entity in RiskVision. As a result, tabs, such as General, Assessments, Owners, Description, Addresses, Classification, Cost & Impact, Relationships, Documents, and Data Feeds that are commonly available in details page of various entity types can also be found in the entity collection details page. As a primary owner of an entity collection, it is important to understand the following tabs to configure and manage an entity collection.

Tab	Description
Composition	Displays the number of objects grouped by type that constitutes an entity collection. Click an entity type to drill down into all the entities of that type.
Entities	Displays the objects available in an entity collection. The Entities tab allows you to manage entity collection members, such as, entities and dynamics groups. Use Remove option to remove entities that are a part of dynamic group or entity collection and choose Remove Dynamic Groups from the More Actions drop-down list to remove a dynamic group.

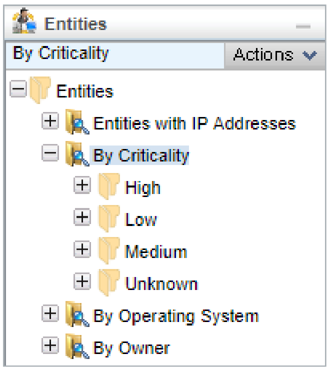
About Dynamic Groups

Dynamic groups include entities based on matching attribute values and filter conditions. Dynamic groups are used for assessments, displays and reporting. This feature is useful for managing very large collections of entities, called entity collections.

Dynamic group folders contain dynamic groups and child groups. Dynamic groups are displayed in a pane to the left of the entities and entity collections grid. For assessments and reports, you can select dynamic groups and child folders, but not top level folders.

Dynamic groups can contain entities and entity collections. When viewing dynamic groups in the **Entities** grid, you will only see entities. Similarly, when viewing dynamic groups in the **Entity Collections** grid, you will only see entity collections. Along these lines, if a dynamic group only has entities, then you will not see it in the **Entity Collections** grid, and if a dynamic group only has entity collections, you won't see it in the **Entities** grid.

The following example shows the default By Criticality group:



The default By Criticality group.

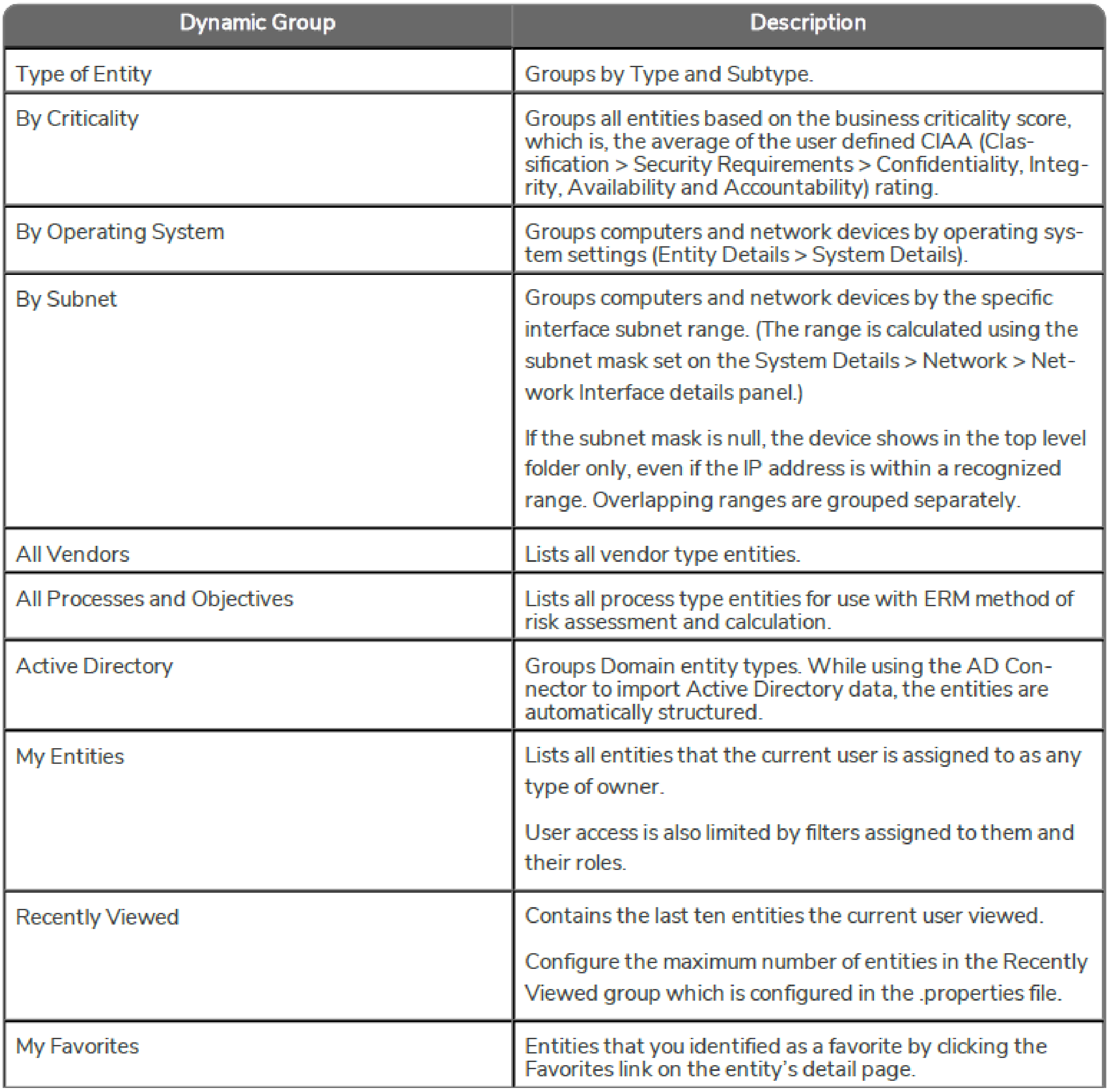
RiskVision automatically creates High, Low, Medium, and Unknown groups.

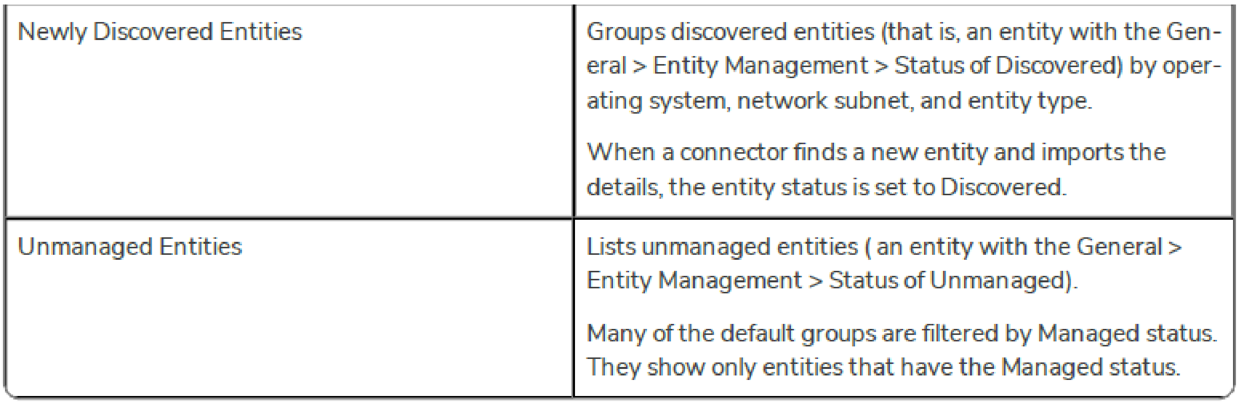
Performance Note

Be careful when creating dynamic groups that will create thousands of folders, because user interface performance will suffer. For example, do not create a dynamic group for "By Owner" in a system with 20,000 entities and 10,000 owners. This would create 10,000 folders, which would cause the system to respond slowly, making it difficult to scroll to the desired folder.

Default Dynamic Groups

The following table provides a brief description of the default groups available. To add, update or delete a custom defined dynamic group or a pre-configured group, you must have the Entity View and Entity Manage permissions.





Dynamic Group	Description
Type of Entity	Groups by Type and Subtype.
By Criticality	Groups all entities based on the business criticality score, which is, the average of the user defined CIAA (Classification > Security Requirements > Confidentiality, Integrity, Availability and Accountability) rating.
By Operating System	Groups computers and network devices by operating system settings (Entity Details > System Details).
By Subnet	Groups computers and network devices by the specific interface subnet range. (The range is calculated using the subnet mask set on the System Details > Network > Network Interface details panel.) If the subnet mask is null, the device shows in the top level folder only, even if the IP address is within a recognized range. Overlapping ranges are grouped separately.
All Vendors	Lists all vendor type entities.
All Processes and Objectives	Lists all process type entities for use with ERM method of risk assessment and calculation.
Active Directory	Groups Domain entity types. While using the AD Connector to import Active Directory data, the entities are automatically structured.
My Entities	Lists all entities that the current user is assigned to as any type of owner. User access is also limited by filters assigned to them and their roles.
Recently Viewed	Contains the last ten entities the current user viewed. Configure the maximum number of entities in the Recently Viewed group which is configured in the .properties file.
My Favorites	Entities that you identified as a favorite by clicking the Favorites link on the entity's detail page.
Newly Discovered Entities	Groups discovered entities (that is, an entity with the General > Entity Management > Status of Discovered) by operating system, network subnet, and entity type. When a connector finds a new entity and imports the details, the entity status is set to Discovered.
Unmanaged Entities	Lists unmanaged entities (an entity with the General > Entity Management > Status of Unmanaged). Many of the default groups are filtered by Managed status. They show only entities that have the Managed status.

Configuring the Dynamic Grouping

The RiskVision solution automatically creates a subgroup based on the selected entity attributes.

Grouping Applications

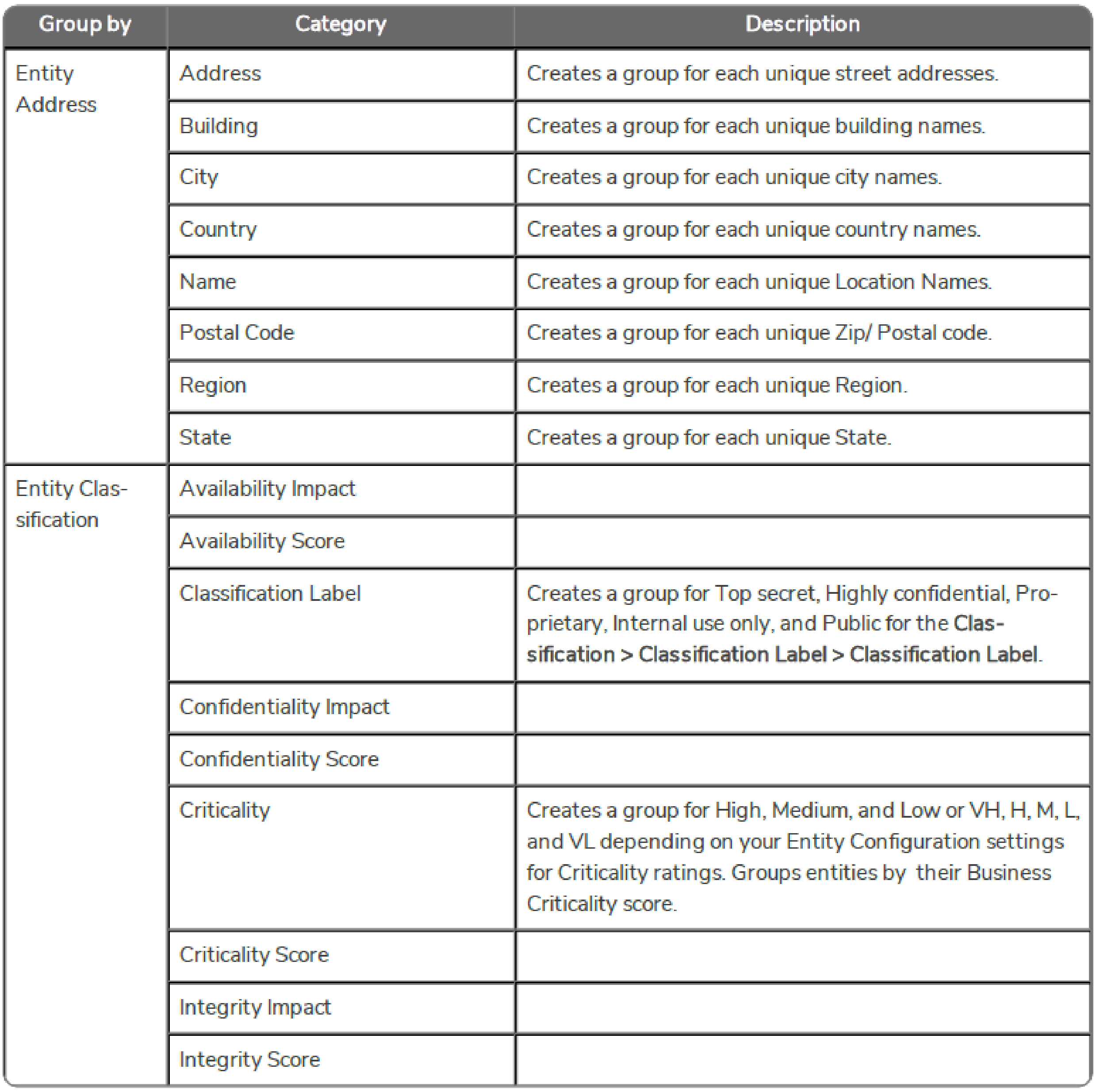
The following table describes the group-by options for Entity type applications:

Group by	Category	Description
ApplicationSystem Flags	Internet Facing	Creates True, False, and Unknown groups that include Entities of type application based on the Description > Network Access > Internet Facing attribute.

Grouping Entities By Attributes

The Entity options allow you to create groups by attributes that are common to all entity types. Use filters to limit the Entities by type.

The following table describes the group-by options for Entities:



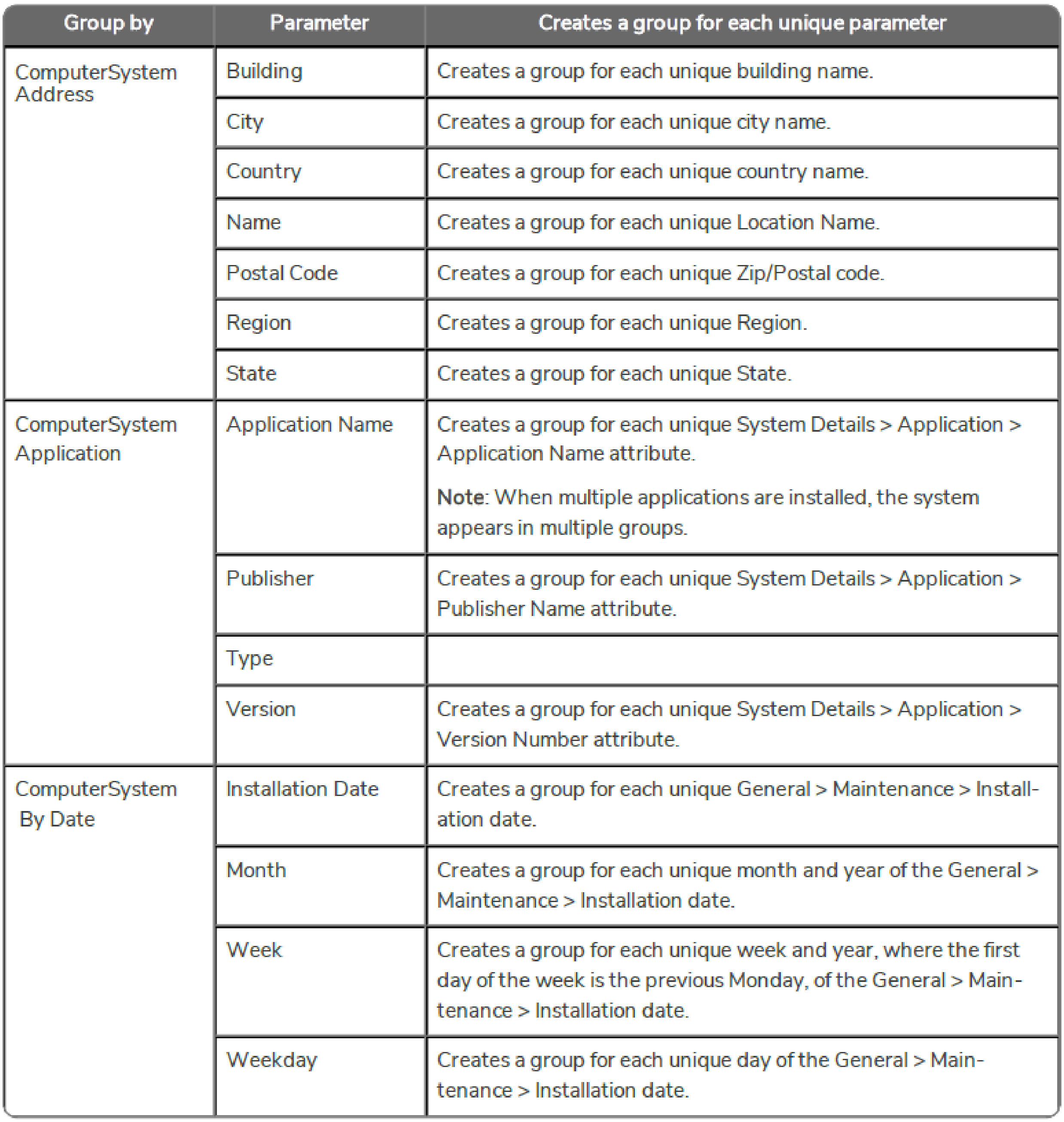
Group by	Category	Description
Entity Address	Address	Creates a group for each unique street addresses.
	Building	Creates a group for each unique building names.
	City	Creates a group for each unique city names.
	Country	Creates a group for each unique country names.
	Name	Creates a group for each unique Location Names.
	Postal Code	Creates a group for each unique Zip/ Postal code.
	Region	Creates a group for each unique Region.
	State	Creates a group for each unique State.
Entity Classification	Availability Impact	
	Availability Score	
	Classification Label	Creates a group for Top secret, Highly confidential, Proprietary, Internal use only, and Public for the **Classification > Classification Label > Classification Label**.
	Confidentiality Impact	
	Confidentiality Score	
	Criticality	Creates a group for High, Medium, and Low or VH, H, M, L, and VL depending on your Entity Configuration settings for Criticality ratings. Groups entities by their Business Criticality score.
	Criticality Score	
	Integrity Impact	
	Integrity Score	

Group by	Category	Description
Entity Description	Compliance Level	
	Container Level1	Custom option that structures user-defined attributes.
	Container Level2	
	Container Level3	
	Container Level4	
	Container Level5	
	Container Level6	
	Division	Creates a group for each unique General > Organization > Division attribute. **Note:** Used in the structured Organization default dynamic group folder.
	Domain	Creates a group for each entity type Domain **General > Domain** attribute. Used for an Active Directory DN (distinguished name).
	Installation Date	**Organizational Unit, Domain, Computer, Network Devices**: Creates a group for each unique General > Maintenance > Installation date. Account: Creates a group for each unique Description > Create attribute.
	Internal or External	Create an Internal, Public Facing, and unknown group sorts by the Classification > Classification Label selection.
	Inventory Tag	
	Manufacturer	Creates a group for each unique General > Information > Manufacturer attribute.
	Model	
	Organization	
	Risk Assessment Status	
	Risk Assessment Next Review Date (by Month)	
	Sub Division	
	Subtype Type	Creates a structured group Type/subtype for each unique General > Information > Subtype.

Group by	Category	Description
Entity Ownership	User Id - All Owners	Creates a group, that has the **User & Roles > User > Username** field as the group name, for each user who owns an entity regardless of the ownership role.
	User Id - Direct Ownership	Creates a group, that has the **User & Roles > User > Username** field as the group name, for each primary owner.
	User Id - Indirect Ownership (through a team)	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each user who owns an entity through a team regardless of ownership role.
	User Name - All Owners	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each user who owns an entity regardless of the ownership role, including users who own the entity through a team.
	User Name - Direct Ownership	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each primary owner.
	User Name - Indirect Ownership (through a team)	Creates a group that has the **User & Roles > User > First and Last Name** fields as the group name, for each user who owns an entity through a team regardless of ownership role.
Entity Stage	Stage	
Entity Tag	Name	
Entity Vulnerability	CVSS Score	Creates a group for each vulnerability CVSS score of vulnerabilities assigned to computer and device entities. **Note:** Use a filter to match only entities with vulnerabilities, such as an entity filter with the Vulnerability Name Not Null condition. Otherwise, the unknown group includes both entities without vulnerabilities and entities with vulnerabilities that do not have the CVSS score set.
	CVSS Vector	
	Description	Creates a group for each unique vulnerability description, see Vulnerability > Vulnerability List > Vulnerability Details > General > Vulnerability.
	Likelihood	
	Severity	Creates a group for each severity level of a vulnerability.
	Source	Creates a group for each vulnerability author or source.
	Type	Creates a group for each type of vulnerability.

Grouping Computer And Network Devices

The following table describes the group-by for Computer and Network Device type entities:



Group by	Parameter	Creates a group for each unique parameter
ComputerSystem Address	Building	Creates a group for each unique building name.
	City	Creates a group for each unique city name.
	Country	Creates a group for each unique country name.
	Name	Creates a group for each unique Location Name.
	Postal Code	Creates a group for each unique Zip/Postal code.
	Region	Creates a group for each unique Region.
	State	Creates a group for each unique State.
ComputerSystem Application	Application Name	Creates a group for each unique System Details > Application > Application Name attribute. **Note**: When multiple applications are installed, the system appears in multiple groups.
	Publisher	Creates a group for each unique System Details > Application > Publisher Name attribute.
	Type	
	Version	Creates a group for each unique System Details > Application > Version Number attribute.
ComputerSystem By Date	Installation Date	Creates a group for each unique General > Maintenance > Installation date.
	Month	Creates a group for each unique month and year of the General > Maintenance > Installation date.
	Week	Creates a group for each unique week and year, where the first day of the week is the previous Monday, of the General > Maintenance > Installation date.
	Weekday	Creates a group for each unique day of the General > Maintenance > Installation date.

Group by	Parameter	Creates a group for each unique parameter
ComputerSystem Classification	Availability Impact	
	Confidentiality Impact	
	Criticality	Creates a group for High, Medium, and Low or VH, H, M, L, and VL depending on your Entity Configuration settings for Criticality ratings. Groups entities by their Business Criticality score.
	Integrity Impact	
ComputerSystem Description	Domain	Creates a group for each unique Description > Identification > Domain Name attribute. **Note**: The System Details > Network Domain Name field is the same attribute.
	Host Name	Creates a group for each unique System Details > Network Domain Name attribute.
	Installation Date	Creates a group for each unique General > Maintenance > Installation date.
	Inventory Tag	
	Manufacturer	Creates a group for each unique General > Information > Manufacturer attribute. **Note**: The General > Information > Manufacturer and Description > Physical Description Manufacturer field are the same.
	Subtype	Creates a group for each unique General > Information > Subtype. **Note**: Computer and Network Device entity types are grouped together unless you set a filter.
ComputerSystem Network	Subnet	Creates a group for each unique subnet range. The subnet range is automatically calculated from the address settings in the System Details > Network > Network Interface Card dialog. **Note**: Overlapping ranges are grouped separately.
	Subnet Mask	Creates a group for each unique subnet mask of the System Details > Network > Network Interface Card > Subnet Mask.

Group by	Parameter	Creates a group for each unique parameter
ComputerSystem OperatingSystem	OS Name	Creates a group for each unique System Details > Operating System > Name attribute.
	OS Version	Creates a group for each unique System Details > Operating System > Version attribute. **Note**: Some connector discovered computers have the version number in the OS name field.
	OS Version Name	Creates a group for each unique System Details > Operating System > Version Name attribute.
ComputerSystem Vulnerability	CVSS Score	Creates a group for each vulnerability CVSS score of vulnerabilities assigned to computer and device entities. **Note**: Use a filter to match only entities with vulnerabilities, such as an entity filter with the Vulnerability Name Not Null condition. Otherwise, the unknown group includes both entities without vulnerabilities and entities with vulnerabilities that do not have the CVSS score set.
	CVSS Vector	
	Description	Creates a group for each unique vulnerability description, see Vulnerability > Vulnerability List > Vulnerability Details > General > Vulnerability.
	Likelihood	
	Severity	Creates a group for each severity level.
	Source	Creates a group for each vulnerability author or source.
	Type	Creates a group for each vulnerability type.

Configure Dynamic Group Folders

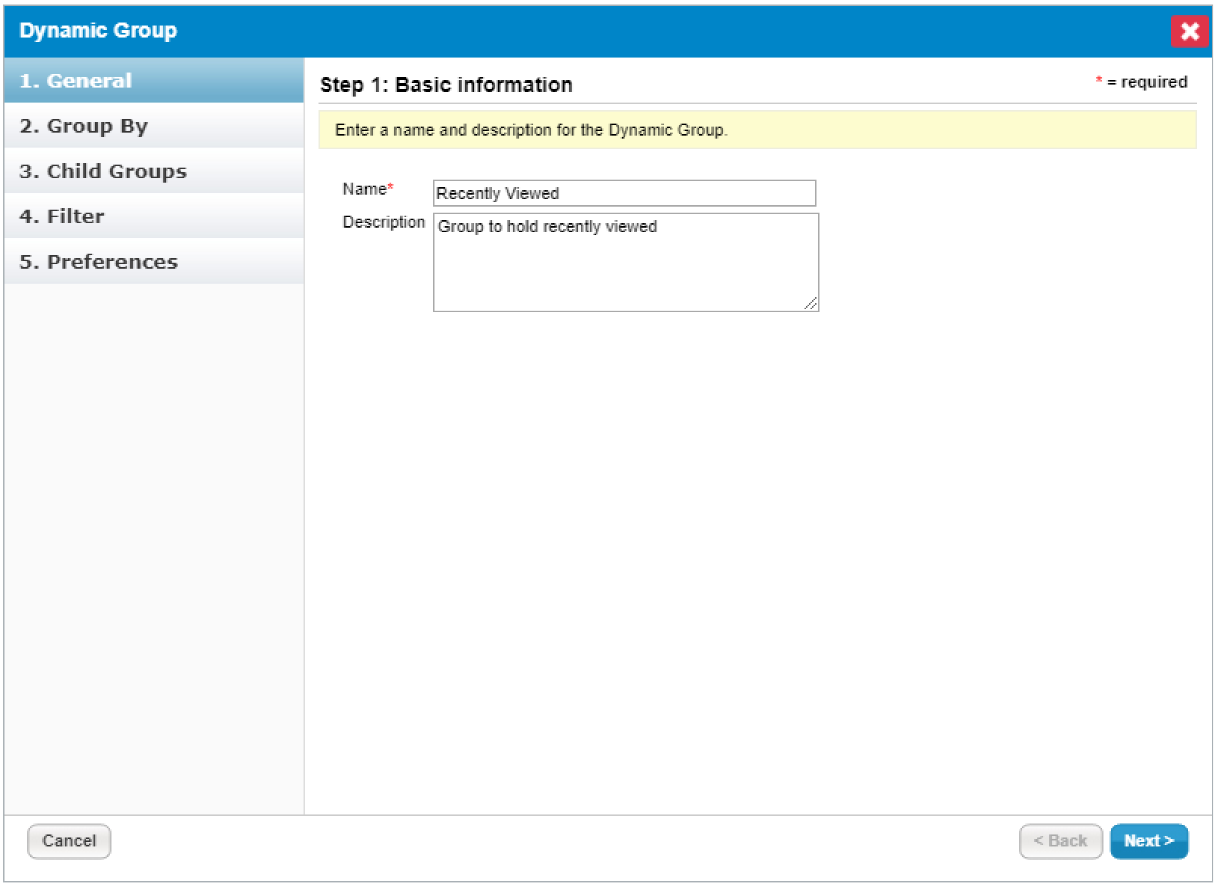
Modifications to an existing folder take effect immediately. When a group or child folder is part of an assessment, the newly matching entities are automatically added to the assessment. If the modification removes entities from the group or child folder, the assessments for the entities are automatically removed from the program. In order to modify an existing dynamic group or create a dynamic group, you must have Entity View and Entity Manage permissions.

To modify an existing group:

1. Go to **Entities** > **Group Definitions**.

2. Click the group, then click **Edit** to open the **Dynamic Group** wizard.

3. Enter a Name and Description.



Enter a name and description for the Dynamic Group.

Name* Recently Viewed

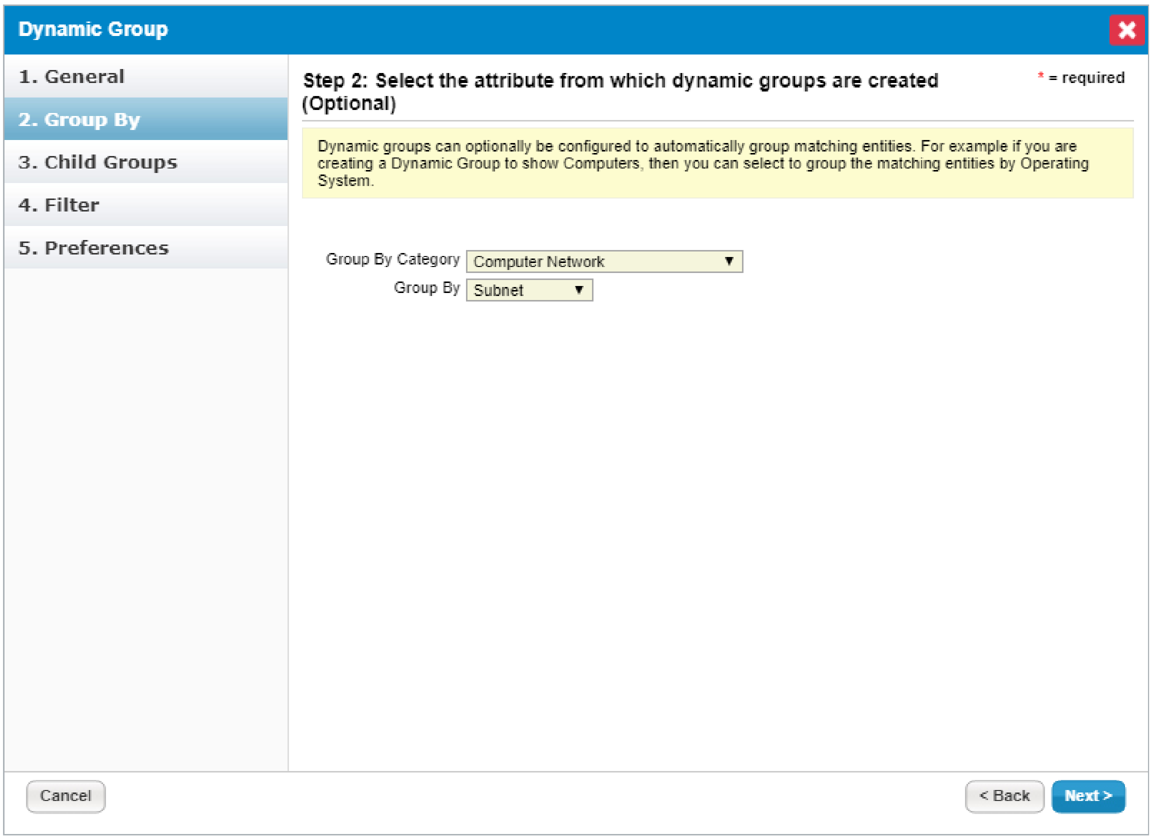
Description Group to hold recently viewed

Step 1 of the Dynamic Group wizard.

4. Click **Next**.

5. **Optional**: Configure the dynamic group settings:

   - To group applications by flags, click the **Application System Flags** and **Internet Facing** checkboxes.
   - To group entities by an attributes, select the options from the Grouping Entities table.
   - To group computer and network devices, select the options from the Grouping Computer and Network Device table.
   - If you skip this option, the folder will display a list of the entities that match the filters.



Step 2: Select the attribute from which dynamic groups are created (Optional)

* = required

Dynamic groups can optionally be configured to automatically group matching entities. For example if you are creating a Dynamic Group to show Computers, then you can select to group the matching entities by Operating System.

Group By Category: Computer Network

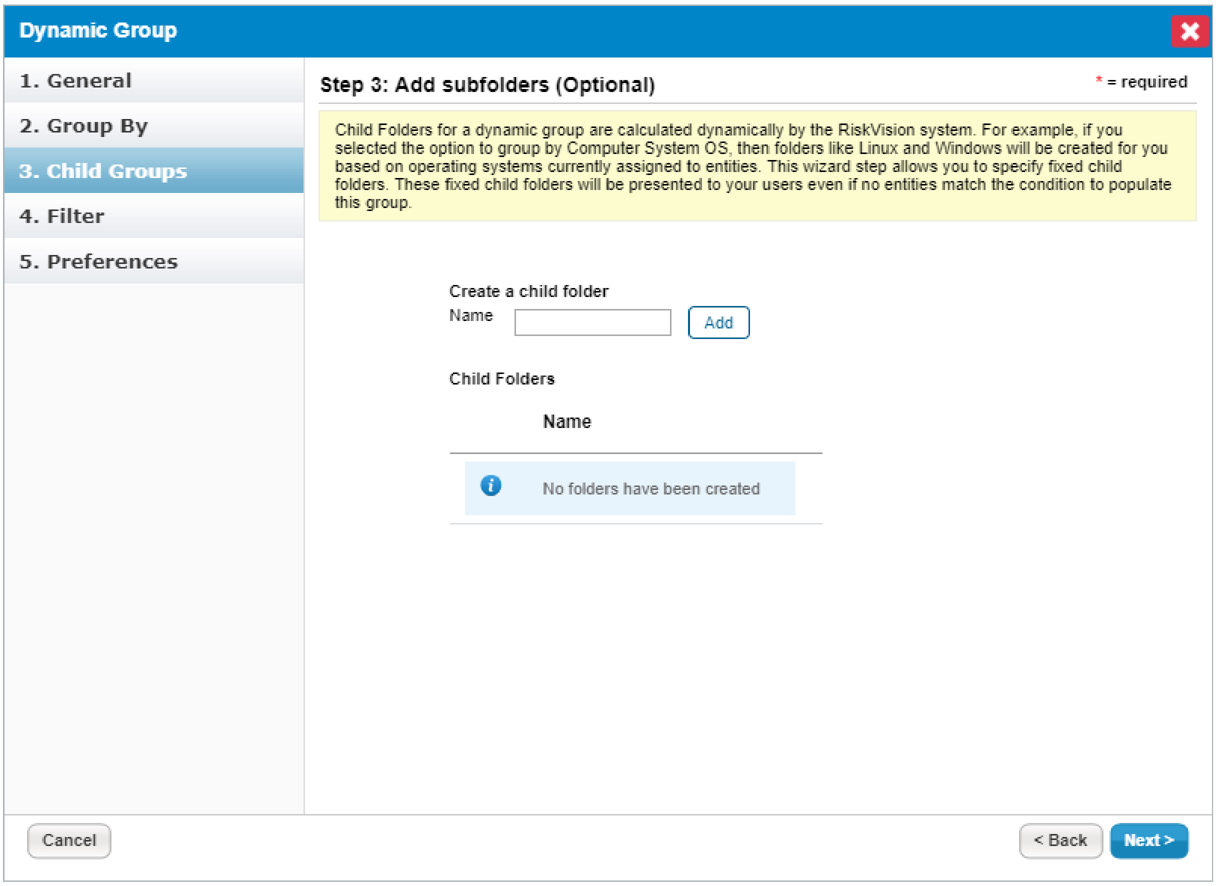
Group By: Subnet

Step 2 of the Dynamic Group wizard.

6. Click **Next**.

7. Enter a name that's similar to the value of the attribute that you want to match, then click **Add**.

   The child folder will appear in the **Entity** and **Program Wizard Entity** selection trees. RiskVision sorts entities with a matching attribute value into the appropriate folder and allows prepopulation of values during entity creation for organizations. For example, if you create a Division child folder called Engineering, the Engineering folder displays on the Organization page of the Entity Wizard. When it is selected, the Entity Organization/Division is automatically set to Engineering.



Step 3: Add subfolders (Optional)

* = required

Child Folders for a dynamic group are calculated dynamically by the RiskVision system. For example, if you selected the option to group by Computer System OS, then folders like Linux and Windows will be created for you based on operating systems currently assigned to entities. This wizard step allows you to specify fixed child folders. These fixed child folders will be presented to your users even if no entities match the condition to populate this group.

Create a child folder

Name

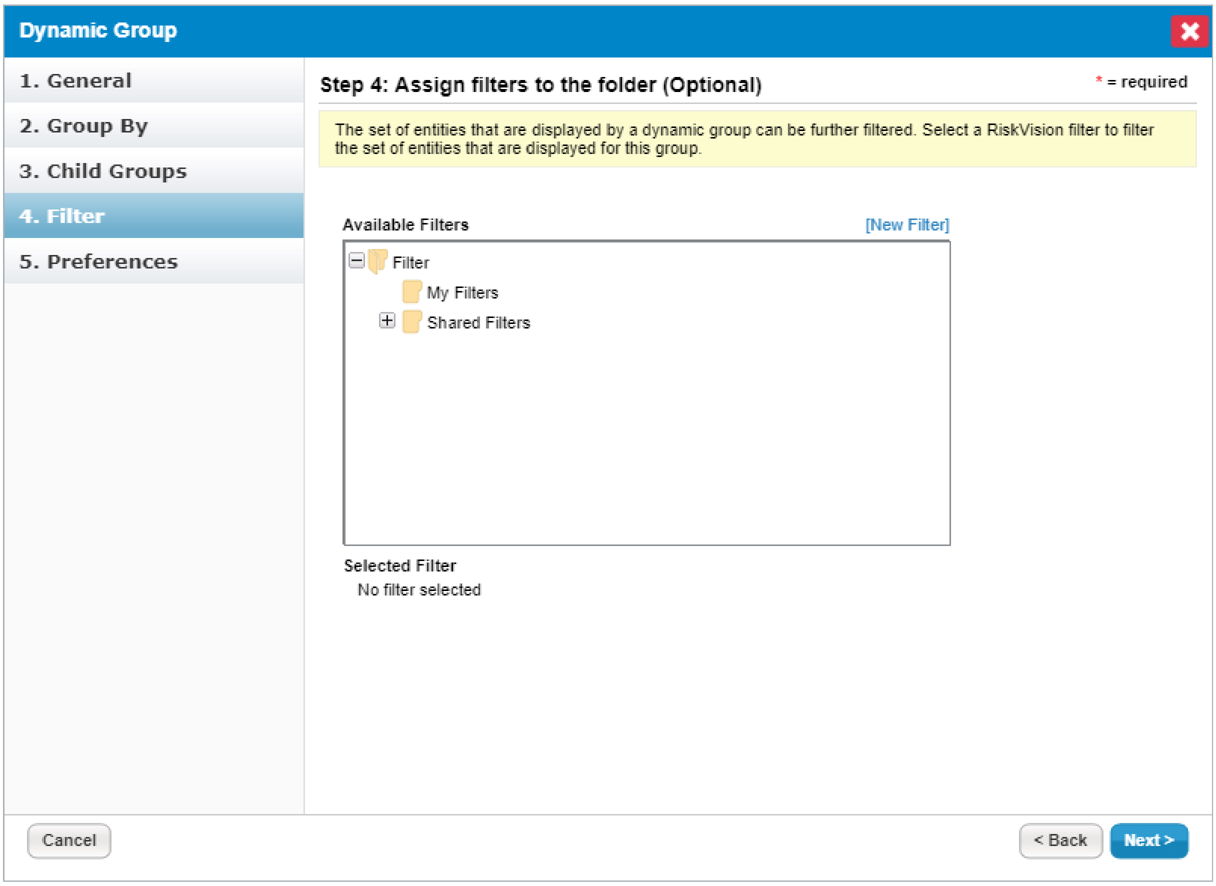
Child Folders

Name
No folders have been created

Step 3 of the Dynamic Group wizard.

8. Click **Next**.

9. Select a filter to limit the entities grouped or listed. You can select one filter. To use the Match Filter option to combine multiple filters, see Configuring filters.



Step 4: Assign filters to the folder (Optional)

* = required

The set of entities that are displayed by a dynamic group can be further filtered. Select a RiskVision filter to filter the set of entities that are displayed for this group.

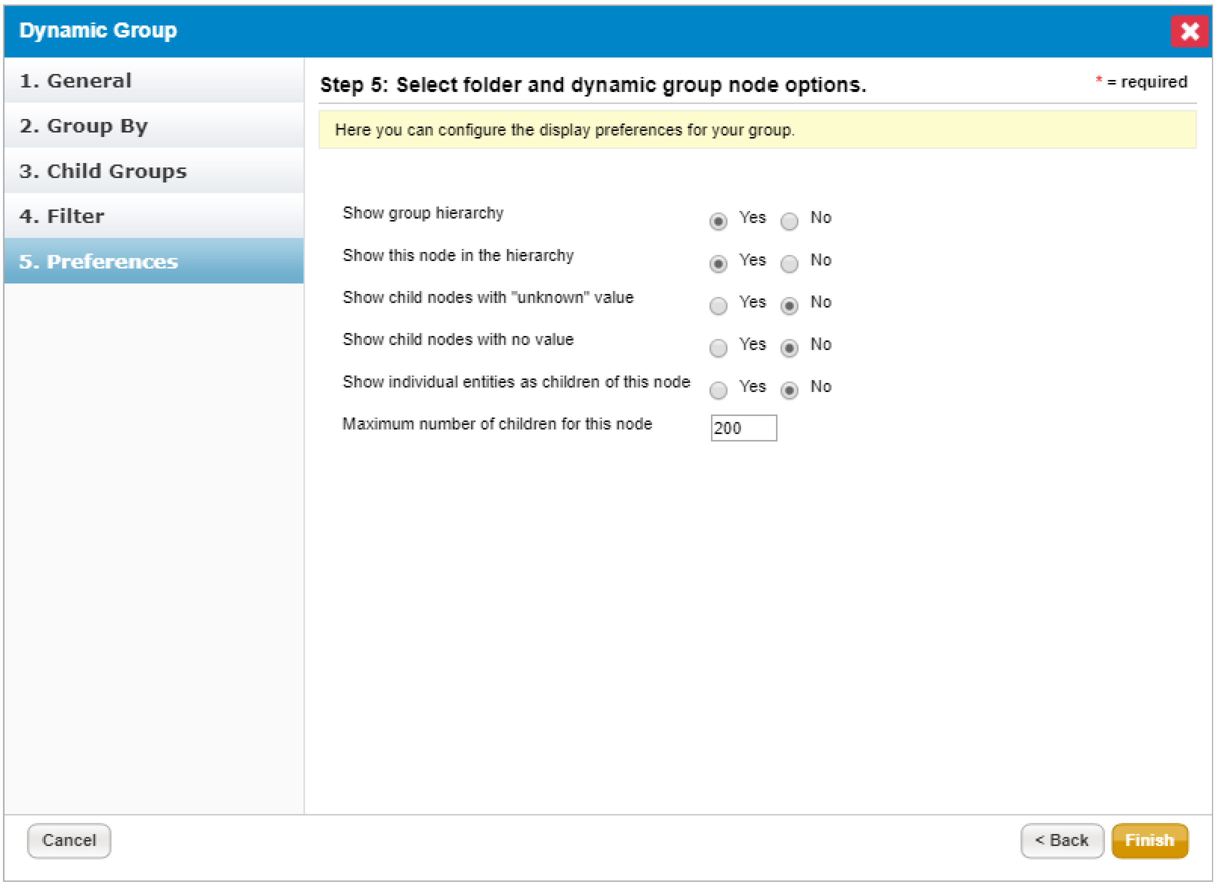
Selected Filter

No filter selected

Step 4 of the Dynamic Group wizard.

10. Click **Next**.

11. Select the folder and dynamic group settings, then click **Finish**.



Step 5: Select folder and dynamic group node options.

* = required

Here you can configure the display preferences for your group.

Show group hierarchy ● Yes ○ No

Show this node in the hierarchy ● Yes ○ No

Show child nodes with "unknown" value ○ Yes ● No

Show child nodes with no value ○ Yes ● No

Show individual entities as children of this node ○ Yes ● No

Maximum number of children for this node 200

Step 5 of the Dynamic Group wizard.

The dynamic group folder displays in the list and entities matching the settings are dynamically grouped on the **Entities** page.

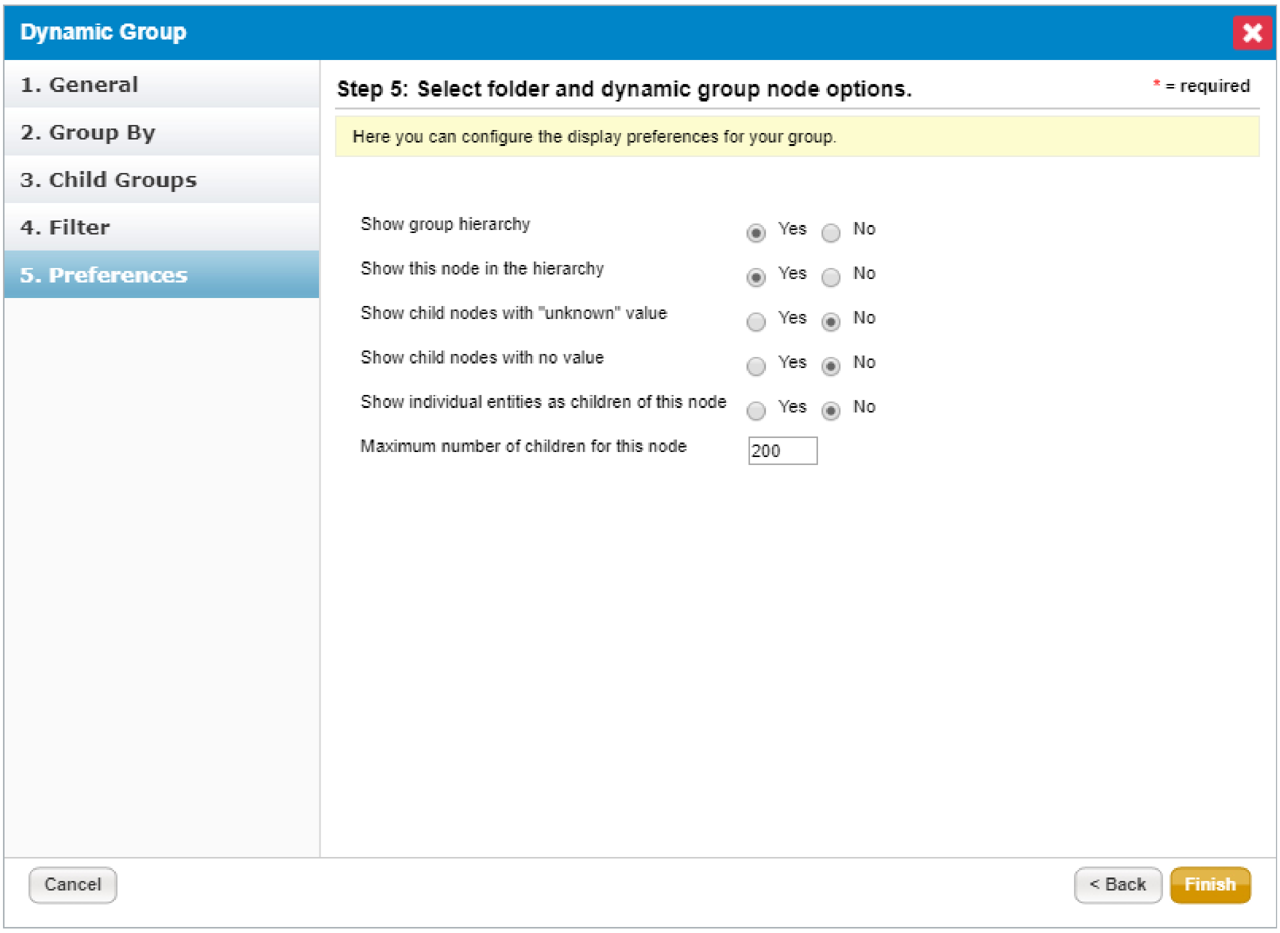
Setting the Name and Description

Specify the following fields:

- Name. Identifies the folder that contains the dynamic groups and/or child groups.
- Description. The Summary that displays on the Group Entities page.

Setting Folder and Grouping Preferences

Folder preferences control how dynamic and child groups display in the **Entities** tree and **Program Wizard Entity** selection tree.



Step 5: Select folder and dynamic group node options.

* = required

Here you can configure the display preferences for your group.

Show group hierarchy ● Yes ○ No

Show this node in the hierarchy ● Yes ○ No

Show child nodes with "unknown" value ○ Yes ● No

Show child nodes with no value ○ Yes ● No

Show individual entities as children of this node ○ Yes ● No

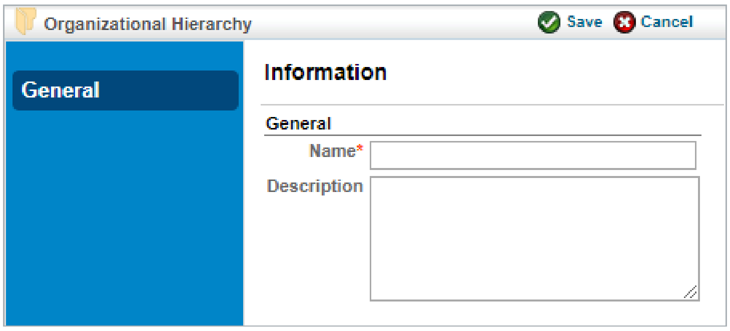
Maximum number of children for this node 200

The folder and grouping preferences in the Dynamic Group wizard.

SETTING	DESCRIPTION
Show group hierarchy	Displays dynamic groups in the folder. If disabled, the group will be hidden from users.
Show this node in the hierarchy	Hides the folder that contains the dynamic groups in the Entity and Program Wizard pages.
Show child node with Unknown value	Displays Unknown group that contains entities that the group by category attribute that matches Unknown.
Show child node with no value	Displays N/A group that contains entities for which the matching group by category attribute is not defined.
Show individual entities as children of this node	Displays entities in the Entities and Program Wizard Entities tree.

Understanding Organizational Hierarchy

The names and relationships of divisions, departments, and other organizational units within an enterprise can be modeled in RiskVision, and individual organizational units can be associated with other components of the system.



The New Organization Group screen.

Organizational units represent a "tree" of nodes. Each node has a single parent node and may have child nodes.

When adding an organization hierarchy node to a profile or other component, use 'Contains.' Do not use the '==' operator**.**

Organization Hierarchy Actions

Each node and its child nodes in an organization hierarchy tree can be moved, copied, or deleted using the Actions pull-down menu that appears when you select a node, or, when you use the Actions drop-down box that appears on the top right-hand corner of the General tab when you open a node's details.

To add an organization hierarchy node:

1. On the **Entities** menu, click **Group Definitions**.On the **Vendors** menu, click **Group Definitions**.

2. In the **Organization Hierarchy** tree, search the node, and then select it. Any child nodes that are available, appear in the child hierarchies section.

3. If you want to move all the child nodes of a node, choose **Cut** from the Actions pull-down menu of the organizational hierarchy tree. Select a node to which you want to move a node and then choose **Paste** from the **Actions** pull-down list of the organizational hierarchy tree.

4. To move a child node, select the node to open its details. Choose **Move To** from the **Actions** drop-down box, and then click **Go**. The **Move Hierarchy** dialog appears. Select a hierarchy and click **OK**.

To delete an organization hierarchy node:

1. On the **Entities** menu, click **Group Definitions**. On the **Vendors** menu, click **Group Definitions.**
2. Find the node to delete in the **Organization Hierarchy** tree.
3. To delete a root node, select a node in the organization hierarchy tree, choose Delete from the Actions pull-down menu and then confirm the action. To delete a child node, select the node to open its details. Choose **Delete** from the **Actions** drop-down box, click **Go** and then confirm the action. This provides the ability to retain the significant child nodes if you do not want to delete the complete node from the organization hierarchy tree.

To copy and paste an organization hierarchy node

1. On the **Entities** menu, click **Group Definitions**. On the **Vendors** menu, click **Group Definitions**.
2. In the **Organization Hierarchy** tree, search the node, and then select it. Any child nodes that are available, appear in the child hierarchies section.
3. If you want to copy all the child nodes of a particular node, choose **Copy** from the **Actions** pull-down menu of the organizational hierarchy tree. Select a desired node to which you want to copy a node and then choose Paste from the Actions pull-down list of the organizational hierarchy tree.
4. To copy a child node, select the node to open its details. Choose **Copy To** from the **Actions** drop-down box and then click **Go**. The Copy Hierarchy dialog appears. Select a hierarchy and click **OK**.

To move an organization hierarchy node:

1. On the **Entities** menu, click **Group Definitions**. On the **Vendors** menu, click **Group Definitions**.
2. In the **Organization Hierarchy** tree, search the node, and then select it. Any child nodes that are available, appear in the child hierarchies section.
3. If you want to move all the child nodes of a node, choose **Cut** from the Actions pull-down menu of the organizational hierarchy tree. Select a node to which you want to move a node and then choose **Paste** from the Actions pull-down list of the organizational hierarchy tree.
4. To move a child node, select the node to open its details. Choose **Move To** from the **Actions** drop-down box, and then click **Go**. The Move Hierarchy dialog appears. Select a hierarchy and click **OK**.

Enabling the Organization Hierarchy Selection

When you create a node under the organization hierarchy tree, by default, the nodes are not visible for you to make a selection in the entity wizard or when you want to assign an organization group to an existing entity. Configure the following properties to enable the selection for RiskVision users.

1. **entity.organization.assignment.through.hierarchy= [true |false]**

   This property displays the new organization hierarchy in entity details pane when it is set to true. By default, the property is set to false.

2. **entity.organization.through.hierarchy= [true |false]**

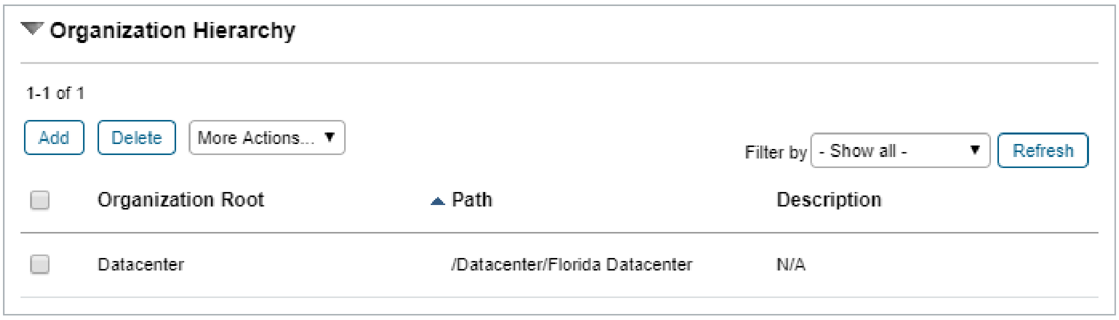
   This property allows you to select new organization hierarchy in entity wizard when it is set to true. By default, the property is set to false.

Defining a New Organization

Entities can be associated with multiple nodes in an enterprise's organizational hierarchy. For example, the hierarchy might be defined by location and division. An entity might belong to a particular department and may be located in a particular facility.

In previous versions of RiskVision, each entity had single-value fields for organization, division, and subdivision.

Associated nodes are in the organizational hierarchy with an entity on the **General** tab of the entity.



□	Organization Root	Path	Description
□	Datacenter	/Datacenter/Florida Datacenter	N/A

The Organization Hierarchy in the General tab of an entity.

Your organizational hierarchy defines your enterprise. You can define various hierarchies and combine them to cross-categorize your entities. For example, your organizational trees might be defined based on:

- Organization: Division, subdivision, department, group.
- Location: Country, region, facility, building, floor, section.
- Function: Retail/b2b, industry, market.

To create an organization node:

1. Go to **Entities** > **Group Definitions** and click **Organizational Hierarchy** in the tree.
2. Click **New Organization Group**, or navigate to an existing node and click **Actions** > **New Child**.
3. Click **Go** and enter the new child node's name and description.
4. Click **Save**.

Note:

- Nodes can also be copied, moved, and deleted using the **Actions** dropdown menu.
- From release 6.5 SP1 HF3 on, the organizational hierarchy supports a maximum number of 15 nodes.

Entity Management

The **Entity Management** page provides on-going information about entities present in the RiskVision system using dashboards that are available on each tab. To view dashboards, you must have the Entity View and Entity Manage permissions. The following table lists the tabs available on the **Entities** > **Entity Management** menu and describes what information each tab represents.

Tab	Description
Summary	Displays dashboards that provides you the managed, unmanaged, discovered, and entity type wise count of entities.
Reconciliation	Displays a vertical bar chart that provides you the count of entities that came from multiple sources, for example, scanner and other sources, and user created.
Manage	Displays a grid for entity types that provides you the count of discovered, managed and unmanaged entities for each entity type.
Classification	Displays dashboards that provides information on managed entities' classification, criticality and ownership data. Each dashboard shows "Yes" and "No" followed by a count of entities. The "Yes" followed by a count denotes that many managed entities have classification, criticality, and ownership. And the "No" followed by a count denotes that many managed entities have no classification, criticality, and ownership.
Assessment Progress	Displays a dashboard that provides the workflow stage wise count of entities.
Vulnerabilities	Displays a dashboard that provides the count of entities affected by the vulnerabilities and entities that have no vulnerabilities.
Controls & Questions	Displays a dashboard that provides you the count of entities that have controls and questionnaires assigned to them.

Entity Management

The **Entity Management** page provides on-going information about your entities using dashboards that are available on each tab. To view dashboards, you must have the Entity View and Entity Manage permissions. The following table lists the tabs available on the **Entities** > **Entity Management** menu and describes what information each tab represents.

TAB	DESCRIPTION
Summary	Displays dashboards that provides you the managed, unmanaged, discovered, and entity type wise count of entities.
Reconciliation	Displays a vertical bar chart that provides you the count of entities that came from multiple sources, for example, scanner and other sources, and user created.
Manage	Displays a grid for entity types that provides you the count of discovered, managed and unmanaged entities for each entity type.
Classification	Displays dashboards that provides information on managed entities' classification, criticality and ownership data. Each dashboard shows "Yes" and "No" followed by a count of entities. The "Yes" followed by a count denotes that many managed entities have classification, criticality, and ownership. And the "No" followed by a count denotes that many managed entities have no classification, criticality, and ownership.
Assessment Progress	Displays a dashboard that provides the workflow stage wise count of entities.
Vulnerabilities	Displays a dashboard that provides the count of entities affected by the vulnerabilities and entities that have no vulnerabilities.
Controls & Questions	Displays a dashboard that provides you the count of entities that have controls and questionnaires assigned to them.

Incidents

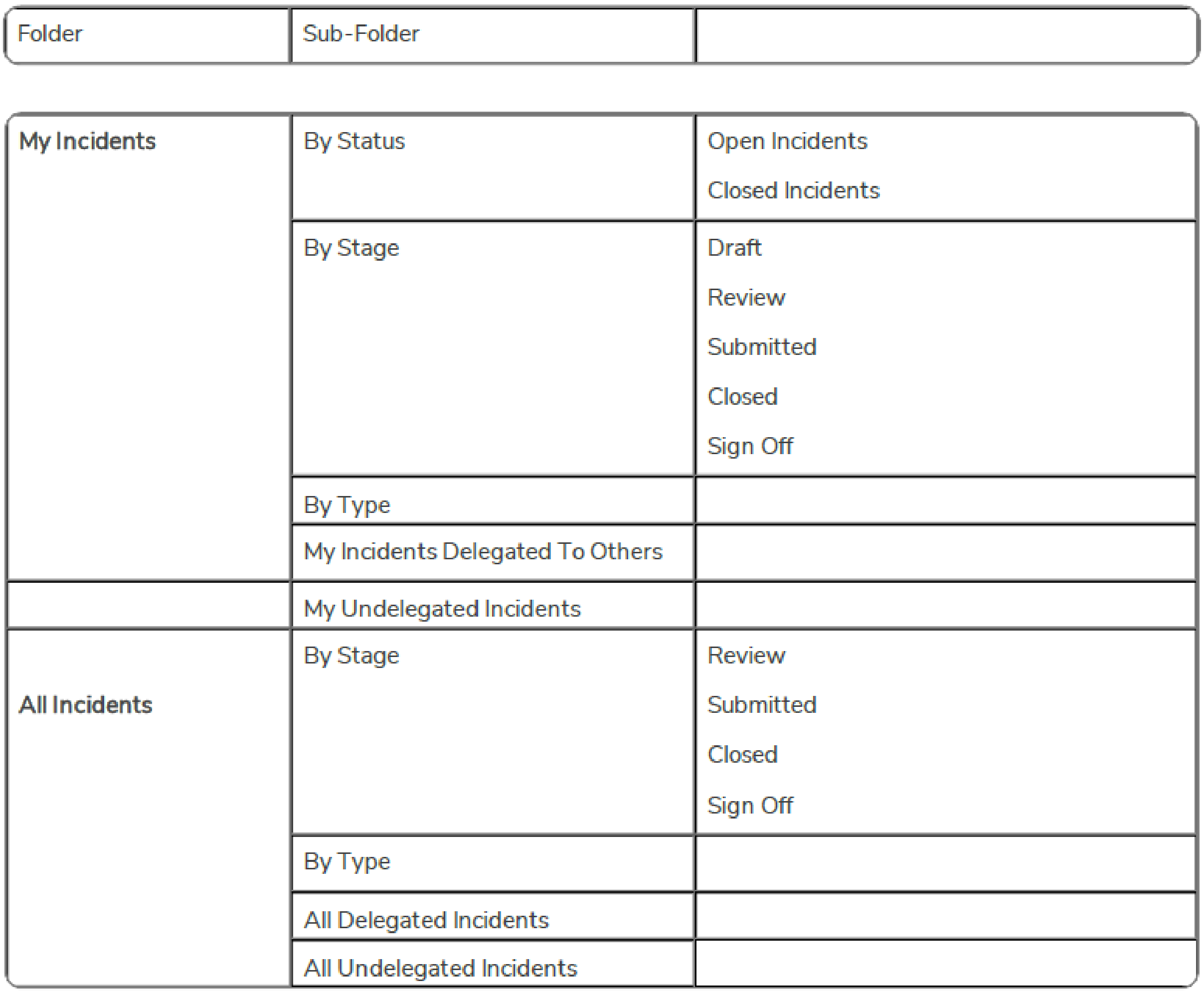
Incidents allow you to record events that occur outside the RiskVision solution. Incidents have a type and subtype and can be linked to specific entities in the organization.

Incidents have a list of Actions taken and can be associated with one or more Tickets and Controls. Incidents also have associated workflows that record the progress of the response to the incident.

Incidents can be created without logging in to the RiskVision solution. See Anonymous Incident Reporting for more information.

The **Incidents** > **Incidents** page provides the Incidents tree in a separate pane on the left-side. This tree, by default, includes My Incidents, By Status, By Stage, My Incidents Delegate To others folders.

- **My Incidents** folder represents those incidents for which you are the submitter.
- **By Status** folder categories the incidents based on the status being open or closed.
- **By Stage** folder helps you track those incidents, which you have submitted. This folder segregates incidents based on the workflow stage and at a minimum, it contains the Draft folder. More folders appear under the **By Stage** folder, representing the workflow stage name when an incident advances to other workflow stages.
- **My Incident Delegated To Others** folder contains the logged in users incidents that are delegated to the other users



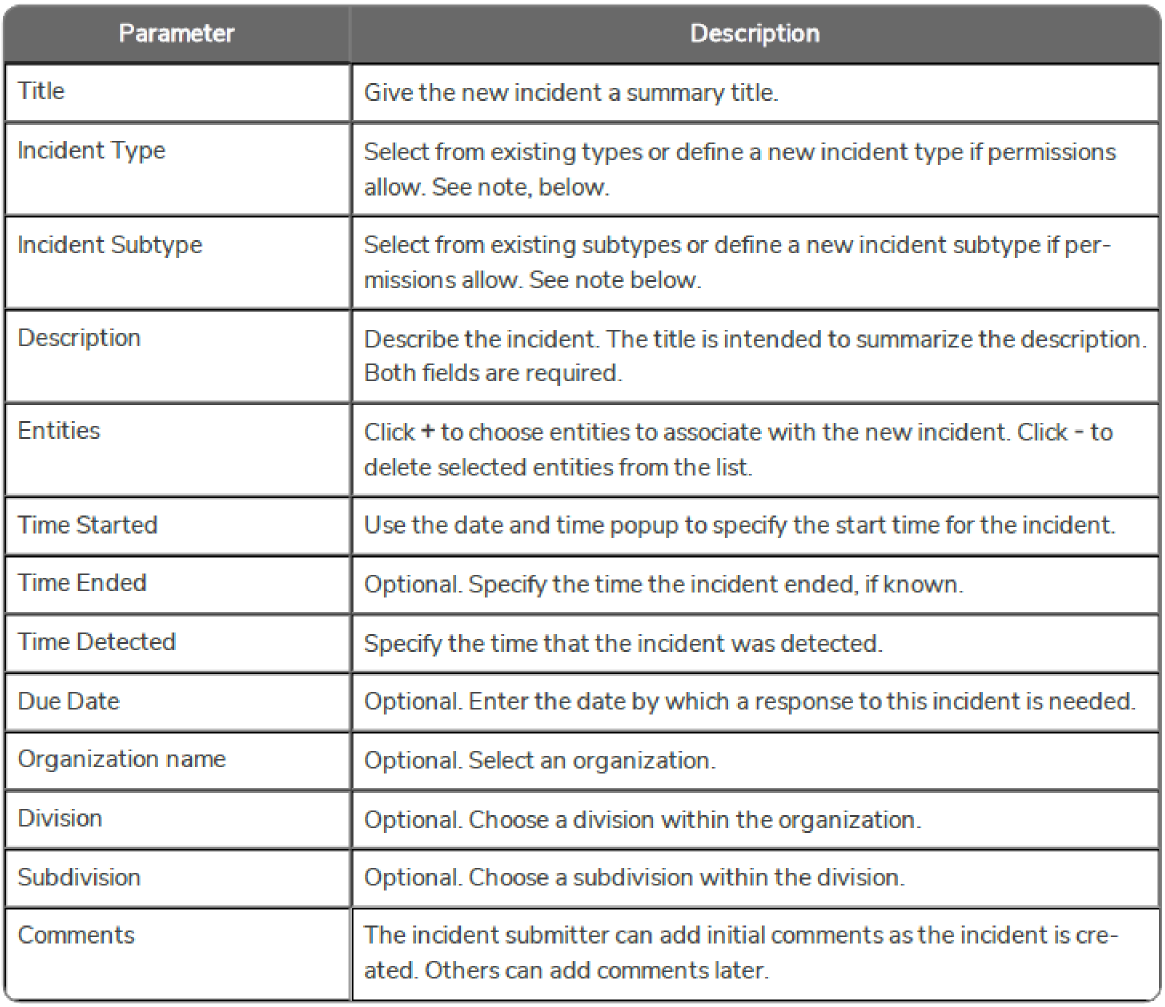
Folder	Sub-Folder	
My Incidents	By Status	Open Incidents Closed Incidents
	By Stage	Draft Review Submitted Closed Sign Off
	By Type	
	My Incidents Delegated To Others	
	My Undelegated Incidents	
All Incidents	By Stage	Review Submitted Closed Sign Off
	By Type	
	All Delegated Incidents	
	All Undelegated Incidents	

Creating a New Incident

Create a new incident to record an event that affects your organization and track the response to the event and the eventual resolution of the incident. You can create a new incident if you have the Incident View and Incident Create or Incident View and Incident Manage permissions. Unless you have the Incident View permission, the incidents are not visible to you if you are the owner of an incident. The Incident View permission is required in order to use permissions, such as Update and Manage in the Incident permissions hierarchy.

To create a new incident:

1. Click **Incidents** > **Incidents**. The **Incidents** page is displayed.
2. Click **New**. The **New Incident** dialog appears.
3. Enter the following fields:



Parameter	Description
Title	Give the new incident a summary title.
Incident Type	Select from existing types or define a new incident type if permissions allow. See note, below.
Incident Subtype	Select from existing subtypes or define a new incident subtype if permissions allow. See note below.
Description	Describe the incident. The title is intended to summarize the description. Both fields are required.
Entities	Click **+** to choose entities to associate with the new incident. Click **-** to delete selected entities from the list.
Time Started	Use the date and time popup to specify the start time for the incident.
Time Ended	Optional. Specify the time the incident ended, if known.
Time Detected	Specify the time that the incident was detected.
Due Date	Optional. Enter the date by which a response to this incident is needed.
Organization name	Optional. Select an organization.
Division	Optional. Choose a division within the organization.
Subdivision	Optional. Choose a subdivision within the division.
Comments	The incident submitter can add initial comments as the incident is created. Others can add comments later.

4. Click **Finish** to create the new incident.

By default, the RiskVision application assigns an appropriate workflow and immediately starts the workflow in the Submitted stage (first stage) after an incidents is created. Set the com..incident.autoLaunchIncidentproperty to "false" if you want a workflow not to start on its own.

The option of defining a new Incident Type or Subtype can be limited to users with the Incident Manage privilege by setting the global property: allow.incident.type.subtype.creation.toIncidentManagePermissionOnly = true

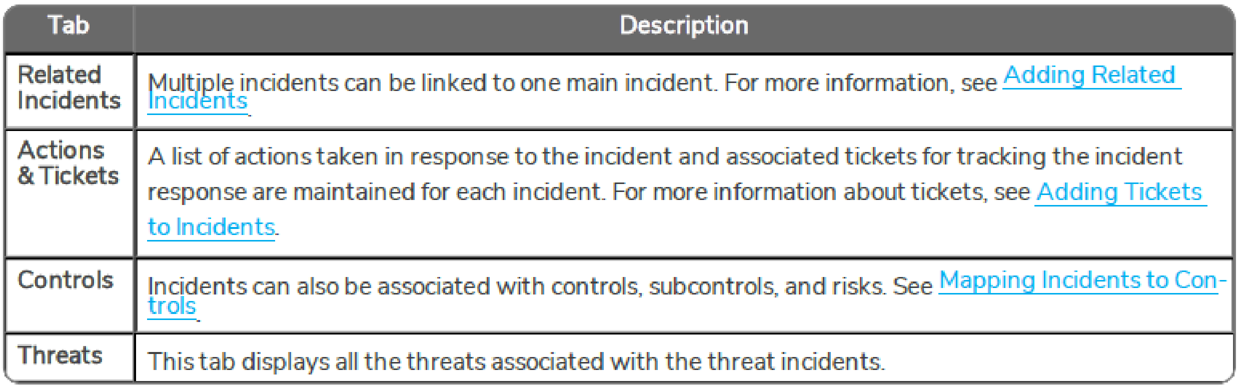
Adding Details to Incidents

Incidents have several categories of associated additional information. In addition to **General** and **Additional Details** tabs, incidents have:

- Related Incidents
- Actions & Tickets
- Controls
- Threats

Adding more details to incidents requires you to have the Incident View, and Update or Manage permissions. If you have Incident Update permission, then you can update your own incidents. If you have the Incident Manage permission, you will be able to update any incidents irrespective of the ownership.

The following table lists different tabs that are available on the **Incident** details page.



Tab	Description
Related Incidents	Multiple incidents can be linked to one main incident. For more information, see Adding Related Incidents
Actions & Tickets	A list of actions taken in response to the incident and associated tickets for tracking the incident response are maintained for each incident. For more information about tickets, see Adding Tickets to Incidents.
Controls	Incidents can also be associated with controls, subcontrols, and risks. See Mapping Incidents to Controls
Threats	This tab displays all the threats associated with the threat incidents.

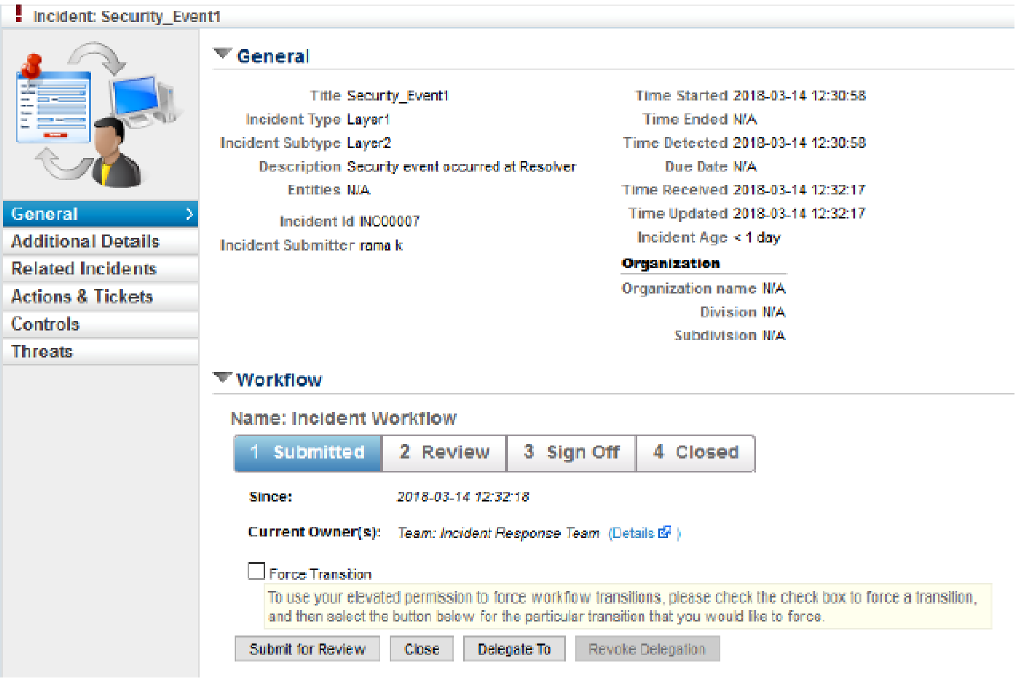
Adding Related Incidents

In order to track incidents that are related to each other, RiskVision provides a Related Incidents tab to show incidents that are related to the current incident. For example, if you believe that the same perpetuator who tried a denial of service attack last week attempted a similar attack a month ago, you might want to add the earlier incident as a related incident. This will provide you a means to track the resolution of all of the incidents together. To be able to add related incidents no matter who owns the incident, you must have the Incident Manage permission.

To add related incidents:

1. In the Incident Manager application, go to Incidents > Incidents.

2. Expand the Incidents tree, locate the desired incident group, and select the incident to open the details, showing the information in the General tab.



Incident: Security_Event1

General

Title Security_Event1
Incident Type Layer1
Incident Subtype Layer2
Description Security event occurred at Resolver
Entities N/A
Incident Id INC00007
Incident Submitter rama k

Time Started 2018-03-14 12:30:58
Time Ended N/A
Time Detected 2018-03-14 12:30:58
Due Date N/A
Time Received 2018-03-14 12:32:17
Time Updated 2018-03-14 12:32:17
Incident Age < 1 day

Organization
Organization name N/A
Division N/A
Subdivision N/A

Workflow

Name: Incident Workflow

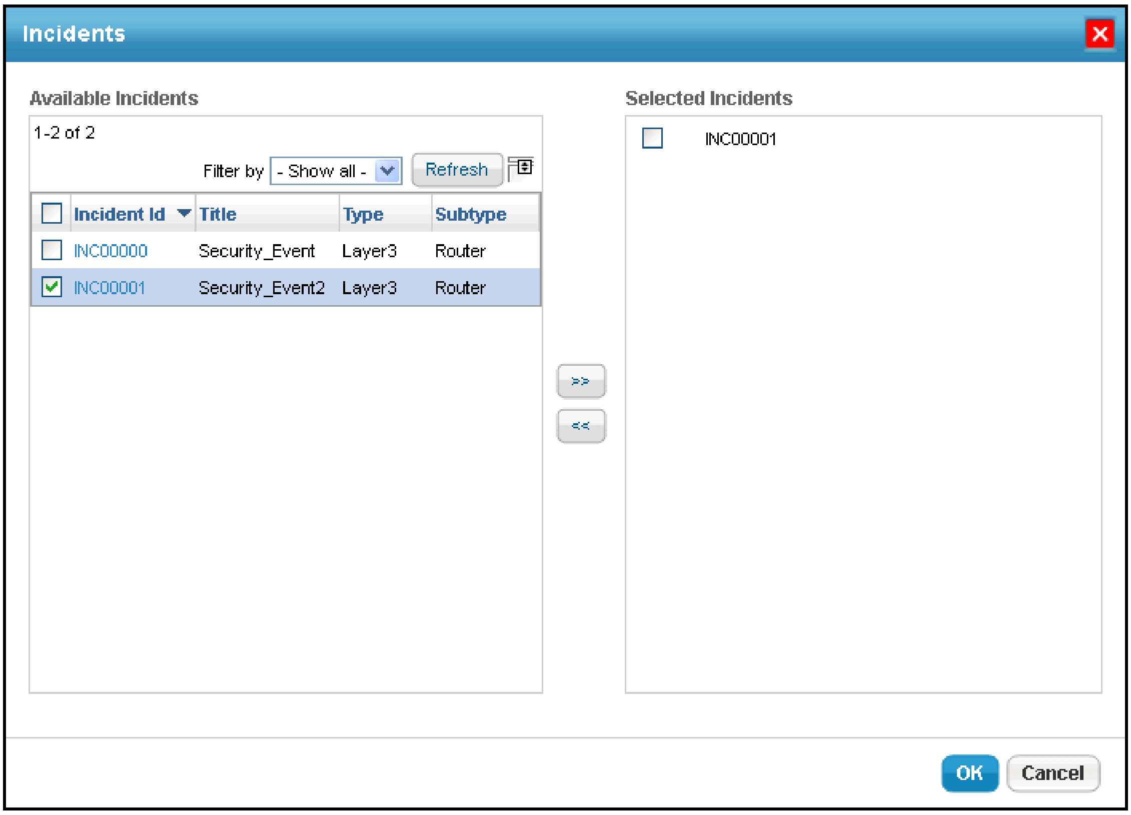
Since: 2018-03-14 12:32:18

Current Owner(s): Team: Incident Response Team (Details)

□ Force Transition

To use your elevated permission to force workflow transitions, please check the check box to force a transition, and then select the button below for the particular transition that you would like to force.

3. Click the **Related Incidents** tab and click **Add**. The **Incidents** dialog appears.



1-2 of 2

Filter by - Show all -

□	Incident Id	Title	Type	Subtype
□	INC00000	Security_Event	Layer3	Router
☑	INC00001	Security_Event2	Layer3	Router

□ INC00001

4. Depending on the roles and permissions, you will be allowed to view the incidents in the **Available Incidents** box. Check the box next to each incident Id to select only the specific incidents or check the box next to Incident Id header to select all of the incidents in the grid, and then click **>>** to move the incidents to the **Selected Incidents** box.

5. Click **OK** after you finish adding the related incidents and to exit the Incidents dialog.

Adding Tickets to Incidents

Tickets can be added to incidents to help track the organization's response to the event that initiated the incident.

To add a new ticket to an incident:

1. Click **Incidents > Incidents. The Incidents page displays.**
2. Use the navigation tree on the left to locate the dynamic folders containing the incident. Check the box next to the desired incident.
3. Click Details to display the details of the selected incident.
4. Click **Actions & Tickets. Under Incident Tickets, click New. See** Creating a New Ticket.

To add existing tickets to an incident:

1. Click Incidents > Incidents.
2. Use the navigation tree on the left to locate the dynamic folders containing the incident. Check the box next to the desired incident.
3. Click Details to display the details of the selected incident.
4. Click Actions & Tickets. Under **Incident Tickets**, click Add Tickets.
5. Search for applicable tickets by name or description. Click OK.

Adding Actions To Incidents

To add a new action to an incident:

1. Click **Incidents** > **Incidents**. The Incidents page displays.
2. Use the navigation tree on the left to locate the dynamic folder containing the incident. Select the checkbox next to the desired incident.
3. Click **Details** to display the details of the selected incident.
4. Click **Actions & Tickets**. Under Incident Actions, click **New**.
5. The **Add Incident Action** wizard appears, enter the *Action Summary, Action Time, Status, Resolution* and *Action Description*.
6. Click **OK**. A new incident action is added in the Incident Action section.

To edit the action associated to an incident

1. Click **Incidents** > **Incidents**.
2. Use the navigation tree on the left to locate the dynamic folder containing the incident. Select the checkbox next to the desired incident.
3. Click **Details**, to display the details of the selected incident.
4. Click **Actions & Tickets** and under **Incident Actions**, click **Edit**. The Edit Incident Action wizard appears.
5. Edit the required data and click **OK**.

Mapping Incidents to Controls

Incidents can be mapped directly to the set of controls that would have prevented the incident.

To map an incident to a control:

1. Go to **Incidents** > **Incidents** and then select an incident to open its details page.

2. Click the **Controls** tab, then click **Map to Control.**

3. Select the control to map to the incident. Note that mapping is not transitive--that is, mapping an incident to a control does not automatically map it to the control's parent or children in the hierarchy.

To disassociate a control with an incident:

1. Go to **Incidents** > **Incidents** and then select an incident to open its details page.

2. Click the Controls tab, select the control and click **Unmap**.

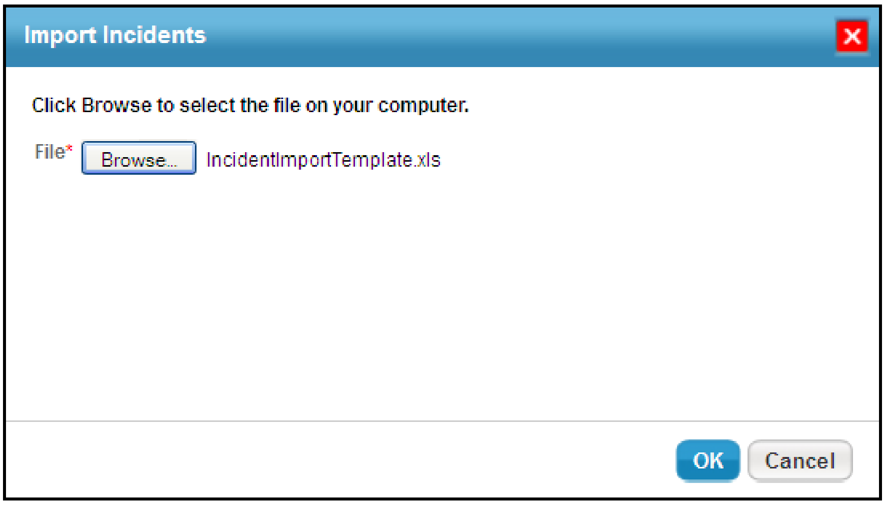
Importing Incidents

Incidents can be described in Excel spreadsheets (.xls file) and bulk imported into the RiskVision solution for tracking, prioritization, risk assessment, and mitigation. A user with Incident Manage permission can import the incidents.

To import incidents:

1. Go to **Incidents** > **Incidents**. The **Incidents** page appears.

2. In the **Incidents** tree pane, select **My Incidents** folder, and choose **Import** from the **More Actions**drop-down list. The **Import Incidents** dialog appears.



Import Incidents

Click Browse to select the file on your computer.

File* Browse... IncidentImportTemplate.xls

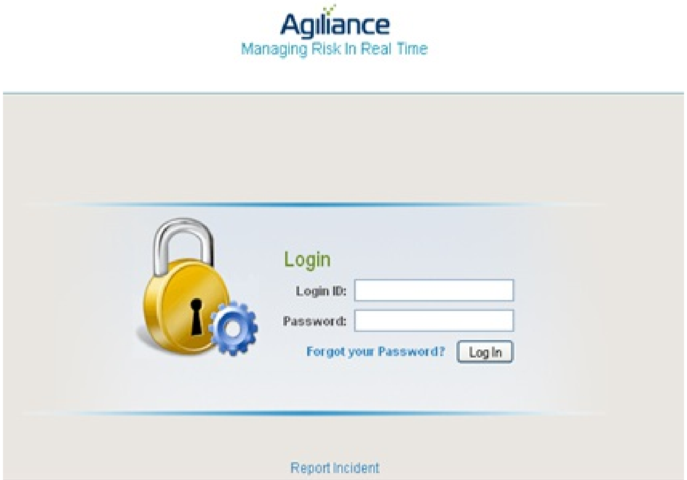
3. Click **Browse**, select the file, click **Open**, and click **OK**. Allow sufficient time to complete the import process.

Anonymous Incident Reporting

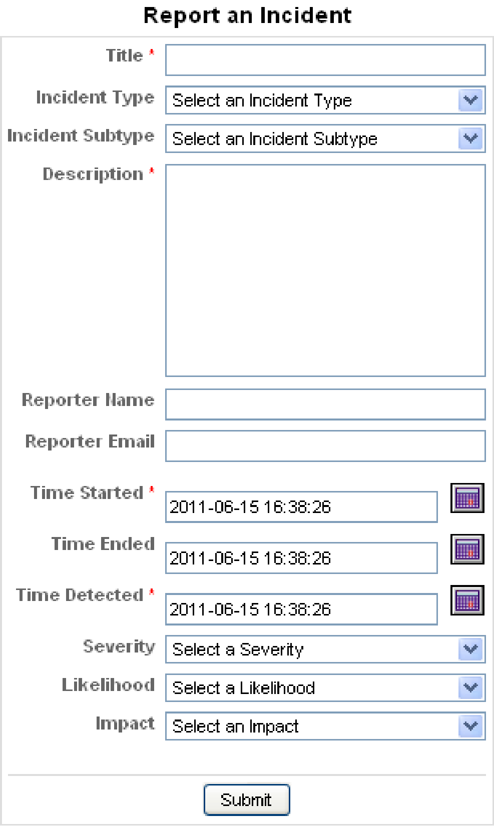
Users can report incidents without logging in to the RiskVision solution. By default, you will not be able to access this feature. To allow users to report anonymous incidents, you should add the following property in the `.properties` file.

```
com..incident.anonymous.reporting.enabled=true
```

To report an incident without logging in to RiskVision:

1. Open a browser and enter the RiskVision URL.
2. After the login page appears, click the Report Incident link.
3. 

4. The following page appears. The Reporter Name and Reporter E-mail fields are optional.



Report an Incident

Title *

Incident Type: Select an Incident Type

Incident Subtype: Select an Incident Subtype

Description *

Reporter Name

Reporter Email

Time Started *: 2011-06-15 16:38:26

Time Ended: 2011-06-15 16:38:26

Time Detected *: 2011-06-15 16:38:26

Severity: Select a Severity

Likelihood: Select a Likelihood

Impact: Select an Impact

5. Click **Submit** to report the incident.

An incident submitted anonymously will follow the same path as incidents submitted from a logged in session. An incident administrator will be able to associate the incident with the appropriate workflow, specify additional information, and so on.

Incident Management

The following properties are associated with incident management:

1. **com..incident.globalIncidentProject.name**

   This property is used to set global incident program name. If it is not set to a program name, by default "Incident Assessments" name is used.

2. `com..incident.autoLaunchIncident` = [true |**false]**

   If this property is true, the system will automatically assign the appropriate workflow and start the workflow. By default, it is true.

3. `com..incident.reconciliationCriteria` = Title,Description,IncidentType

   Based on the properties of Incident, supplied as comma-separated values to the above property, RiskVision decides whether to update an existing Incident or create a new one. There are three properties:

   - Title
   - Description
   - IncidentType

4. allow.incident.type.subtype.creation.toIncidentManagePermissionOnly = [true | `false`]

   This property is used to allow creation of type, sub type of incident. If the property is false, users with Incident Create permission will be able to create types and subtypes of incident. If the property is true, then only users with Incident Manage permission will be able to create type and subtype. The default value of the property is false.

   Note: By default, all users with the Incident Manage permission can create new incident types and subtypes. If you want to restrict users with the Incident Manage permission from creating new incident types and subtypes, you can use the allow.incident.type.subtype.creation.toRole=User_Role property value to require that, in addition to having to have Manage permissions, users have a specific role in order to be able to create new incident types and subtypes.

5. com..incident.workflow.allowToLaunchNewIncidentWF = [true | false]

   This property is used to allow launching a new workflow that will be picked up, based on the propertycom..incident.workflow.type, whenever any underlying incident property value changes. The default value of the propety is true.

**To create an
incident workflow:**

1. Create a new workflow and check the box next to theEnable Risk Assessmentoption in the stage from where you will want to start the assessment.

2. In the **Selection** tab of the workflow, set the criteria based on the incident type, division, or riskLevel so that the creation of incident automatically picks the required workflow.

3. If you want to start assessing risk from first stage, enable the **Enable Risk Assessment**option in the initial, "Submitted," stage.

Custom Incident Forms

Incident forms are searched in the order specified in the properties. If a form exists that matches **type_division_stage, it will be used. If it does not exist, a form that matches type_division** will be used if it is found. Otherwise, a form that matches **type_stage** will be used, followed by a form that matches type. Edit the properties file to reorder or remove items from the search list.

If no custom form is found, the default general form will be used. Incident forms can use custom properties defined using the "Configure UI" facility.

Custom Property Examples

Incidents can have different forms (each displaying a different set of attributes) based on incident type and workflow stage.

incidentFormSelection = (type, division, stage); (type, division); (type, stage); (type); (default)

This property's value is a semi-colon-delimited list of items. Each item describes components of a form name.

(type, division, stage)

First, the system tries to find a form with Incident_typeValue_divisionValue_stageValue. If found, it displays the "Incident Details" tab (with id "MoreInformation") contents from the selected component.

If stageValue is null (incident not submitted), it will ignore the triplet and falls back to the next item (type, division). However, if (type, division, null) is found in the triplet itself, the system will try to pick a component with Incident_typeValue_divisionValue.

If nothing matches, the system falls back to the next item (type, division) and then to (type) and, finally, the system uses the default form to display the contents.

(type, division)

The system tries to find the component with Incident_typeValue_divisionValue. If divisionValue is null, it tries to find a component with "Incident_typeValue". Because type is mandatory, typeValue cannot be null.

(stage, division)

First, the system tries to find a component with "Incident_stageValue_divisionValue". If stageValue is null, try to find Incident_divisionValue, else if divisionValue is null, the system tries to find Incident_stageValue. If nothing is found, it falls back to the next item in the token (type, stage).

incidentReadOnlyFormSelect = (type, division, "ReadOnly"); (type, "ReadOnly"); (default, "readonly")

(type, division,"ReadOnly")

First, the system tries to find a component with "Incident_typeValue_divisionValue" so that it can reuse the existing form in read-only mode. If not found, it tries to find Incident_typeValue_divisionValue_ReadOnly component. If this is not found, the system falls back to the next item in the mapping (type,"ReadOnly").

If Incident_typeValue is found, the system will use it. Otherwise, it tries to find Incident_typeValue_ReadOnly. At last, if no match is found, it will fall back to the default.

Note that divisionValue could be null. If it is, the system will try to find Incident_typeValue component. If not found, it tries to find Incident_typeValue_ReadOnly. If not found, it falls back to the next item in the list.

Customizing Incident Management

RiskVision version 4.1 and later supports a hook that allows custom-scripted asset manipulation during the classification process.

The general interface for this hook is:

```
package com..survey.asset;
```

```
import com..common.ALException;
```

```
import com..dal.model.Asset;
```

```
public interface EntityScriptUpdater {
```

```
/**
```

```
  * update the asset attributes
```

```
  * @param asset
```

```
  * @throws ALException
```

```
  */
```

```
public void updateEntity(Asset asset) throws ALException;
```

```
}
```

The hook is controlled by these properties in the .properties file:

```
classification.post.script.enabled=true
```

classification.entity.update.groovy.source=file:D://main/config/CustomerAssetUpdater.groovy

The first property enables or disables the hook and the second property specifies the custom groovy script. The default implementation without specifying the groovy source is

```
classification.entity.update.groovy.source=classpath:com//risk/
```

DefaultRiskUpdater.groovy

A good use case for this functionality is to customize the incident risk score calculation after the incident is done with classification, as the implementation of incident classification is performed through a hidden asset and the asset is associated with the incident by Asset#getIncident() or Incident#getAsset().

Here are the steps (these are all one-time steps):

1. Save the custom groovy file (based on the interface above) to a folder such as `server/config`.
2. Set the following properties in the `.properties` file, update based on your deployment:
3. `classification.post.script.enabled=true`

   `classification.entity.update.groovy.source=file:D://main/config` `/CustomerAssetUpdater.groovy`
4. Restart the RiskVision Tomcat service, or click Reload in the Configuration section of **Administration** > **Server Administration** menu.

Example

This default groovy script calculates the risk:

```
import com..dal.model.*
import com..survey.asset.*
import com..common.*
public class DefaultRiskUpdater implements EntityScriptUpdater{
public void updateEntity(Asset asset) throws ALException {
if (asset==null) return;
// calculate the risk
if (asset.getLikelihood()!=null && asset.getImpact()!=null) {
float risk = (float) (asset.getLikelihood() * asset.getImpact());
asset.setRisk(risk);
}
}
}
```

This custom groovy script illustrates a more comprehensive example:

```
package com..risk
import com..dal.dao.*
import com..dal.model.*
import com..survey.asset.*
import com..common.*
public class DefaultRiskUpdater implements EntityScriptUpdater{
public void updateEntity(Asset asset) throws ALException {
if (asset==null) return;
// calculate the risk
if (asset.getLikelihood()!=null && asset.getImpact()!=null) {
float risk = (float) (asset.getLikelihood() * asset.getImpact());
asset.setRisk(risk);
}
if(asset.getIncident() != null &&
asset.getCustomAttributes() != null &&
asset.getCustomAttributes.getString1() != null) {
Incident incident = asset.getIncident();
if (incident.getCustomAttributes()==null) {
CustomAttributes attr = new CustomAttributes();
new CustomAttributesDAO().save(attr);
incident.setCustomAttributes(attr);
}
asset.getIncident().getCustomAttributes()
.setString1(asset.getCustomAttributes().getString1());
}
}
}
```

Using the Document Repository

A document repository is used for storing critical documents, such as audit material, security plans and sensitive information pertaining to each domain in your organization. You can also refer stakeholders to useful information on the Internet or your intranet using web references. If your user role has sufficient permissions, you can upload files of any kind to share in the repository as well as you can refer to specific websites.

Typically, the document repository is available on the Content, Risks, or Administration menu in RiskVision application.

In addition to the shared document repository, documents and weblinks/ network paths can be uploaded and associated with various RiskVision objects, including entities, controls, programs, contracts, policy documents and so on. These objects have a **Documents** tab in their detail pages. The user permissions control the associated documents to view, upload, or perform any action.

Document Repository Structure

A document repository contains groups and document collections. Typically, a group represents a domain and a document collection is a container that can hold files, and web/ network path references. The document repository supports multiple file uploads of various file formats and image extensions. A user maintaining the document repository has to create at least one group or one document collection to upload documents. This enables you to store all the documents, web and network path references pertaining to your organization. However, creating a single group or document collection will grant other users unrestricted access to all documents, some of which are not relevant to their domain. Use groups to segregate documents based on specific domains, and then create separate groups and document collections within the top-level group with the ownership defined at the group or document collection level.

To support different file format extension, enable the following property `propertycom.agiliance.esapi.allowed.attachment.file.extensions=true.` Here the Default Value = true.

The lists of file formats supported by Document Repository are:

- PDF
- XLS
- XLSX
- DOC
- DOCX
- PPT
- PPTX
- TXT
- JPG
- JPEG
- PNG
- BMP
- MPP
- MPPX
- VSD
- VSDX
- MSG

Linkages for files attached directly to an object (e.g. to an assessment as evidence or to an entity, a finding, etc.) shall be maintained for files moved within the Document Repository. This consists of the following scenarios:

- When moving a file that is linked directly to an object from one Document Collection to another.
- When moving a Document Collection in which the file that was linked directly to an object resides from one Group to another.

Linkages for Document Collections attached directly to an object shall be maintained in the following scenarios:

- When moving a Document Collection into another Document Collection.
- When moving a Document Collection to a different group.

When a Document Collection is attached to an object and files are moved out of the Document Collection, these files shall no longer be linked to the objects they were previously linked to as a result of their membership in the Document Collection that they are no longer part of.

For more information about assigning ownership to a group or document collection, see Document Repository Ownership.

To create a group:

1. Open RiskVision Incident Manager.
2. Go to **Content** > **Document Repository**.
3. Select the **Document Repository** node or locate a group, select to display its details, and then click **New Group**. The **New Group** dialog appears.
4. Enter **Name** and **Description.**
5. Click **OK**.

To create a Document Collection:

1. Open RiskVision Incident Manager.
2. Go to **Content** > **Document Repository**.
3. Go to **Risks** > **Document Repository**.
4. Select the **Document Repository** node or locate a group, select to display its details and then click **New Document Collection**. The **New Document Collection** dialog appears.
5. Enter Name and Description.
6. Click **OK**.

For information about adding a document or a web reference to a document collection, see Attaching Documents.

Document Repository Ownership

The Reader and Writer document repository ownership roles control user access and limit the actions that can be performed by users in a document repository. Using a role, you can define an ownership at the group or document collection level.

Action	Ownership	Permission
Cut	Writer	View + Create + Update or Manage only
Paste	Writer	View + Create + Update or Manage only
Delete	Writer	View + Delete or Manage only
Move to	Writer	View + Create + Update or Manage only

Note: Users can attach and delete documents on entities as long as they have entity view, create, and update permissions. However, the Global Document Repository feature also requires document repository-related permissions and ownership to attach documents from the Document Repository to an entity.

Modifying Ownership

When you create a group or document collection, all RiskVision users are assigned with the Reader ownership type, by default.

To assign ownership to a group:

1. Open RiskVision Incident Manager.
2. Go to **Content > Document Repository**.
3. Select a group in the **Document Repository** node to display its details.
4. Select **Assign ownership** in the **Group actions**drop-down list and then perform step 4 and step 5 for assigning the ownership to a document collection.

To assign ownership to a Document Collection:

1. Open RiskVision Incident Manager.
5.
2. Go to **Content > Document Repository**.
6.
3. Locate the group in the **Document Repository** node and click the document collection of interest to display its details.
4. Click the **Ownership** tab.

   Click **Add Owners**. The **Add additional owners** dialog box appears.

   Select the ownership type from the *Owner Type* dropdown list. To assign the ownership, select a single user in the Individual Owner dropdown list or a team in the Team Owner dropdown list, and click **OK**. Optionally, click **+** to search a user based on role if the user that you intend to assign the ownership is not in the list.

A group can have nested groups, whereas a document collection can hold only the files and web links/network links. You cannot create a group in a document collection.

To delete ownership:

1. Open RiskVision Incident Manager.
2. Go to **Content > Document Repository**.
3. To delete the group ownership, locate and select the group, select **Assign ownership** in the **Group actions** drop-down list. Select the owner(s) and then click **Delete**.
4. To delete the document collection ownership, locate and select the document collection, and click the **Ownership** tab. Select the owner(s) and click **Delete**.

Document Repository Actions

You can perform an action on a group or document collection using the actions drop-down list of document repository root node or using the **More Actions** drop-down list which appears when the details are displayed. To perform an action on a document, or web or network path reference, use the **More Actions** drop-down list from the document collection details page.

The linkage between a RiskVision object and Document Repository object (Document Collection, Document) will be preserved only when we add and move the same type of items, but not when we add one type of item and try moving the other type.

- The linkage is maintained, when you add Document Collection to an object and move document collection from one group to another group or when you add the document to an object and move document(s) from one Document Collection to another Document Collection.
- The linkage is not maintained when you add Document Collection to an object and move document out of it because linking to Document Collection means we documents will be shown at the current point of time in the Documents tab of the linked object.

Move

Documents can be moved to any group within the document repository node if you have the appropriate ownership and permission. You can use cut and paste to move a group or document collection. Use the move action to move an individual document or a web/ network path reference.

To move an object:

1. Open RiskVision Incident Manager.
2. Go to **Content > Document Repository**.
3. Select the group or document collection in the **Document Repository** tree.
4. Click **Actions > Cut**.
5. Select the new location, then click **Actions > Paste**.

To move a document or web reference:

1. Open a document collection.
2. Select a document or web reference.
3. Click **More Actions > Move to**.
4. Select the document collection the item will be moved to.
5. Click **OK.**

Delete

To delete an object:

1. In the RiskVision application, go to **Content** > **Document Repository**. In RiskVision, go to **Risks** > **Document Repository**. In the Administration application, go to **Administration** > **Document Repository**.
2. To delete a group or document collection, select the object, and choose to **Delete** in the **Actions** drop-down list.
3. To delete a document or web reference, locate the document collection, and then select to display its details. Select the object and click **Delete**.

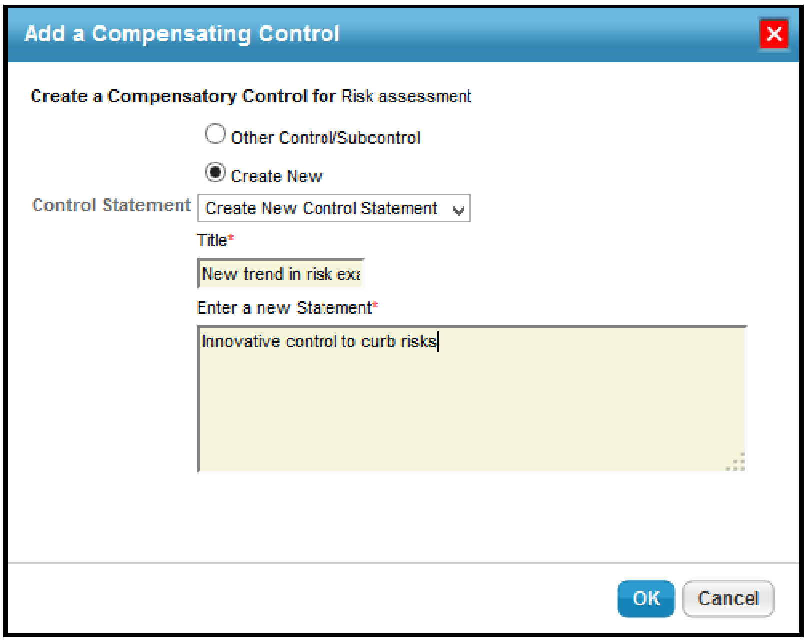
Documents that are linked to objects, such as entities and policies, cannot be deleted. Archive the linked documents by moving them to other groups.

Compensating Controls

Compensating controls are applied when an entity does not comply with one or more controls due to technical or business constraints. Putting the compensatory controls in place mitigates the associated risk; however, you must run an internal audit to confirm that there are no deficiencies. To compensate the non-performing controls, you can create a new control or select an existing control from your organization's controls library.

To add a compensating control

1. Select an assessment, that your stakeholders have responded to the controls, to open its details page.
2. On the **Assessment Details** page, click the **Control Results** tab.
3. Select a control and then select **New Compensating Control** in the **Actions** drop-down list.
4. The **Add a Compensating Control** dialog appears.



Add a Compensating Control

Create a Compensatory Control for Risk assessment

○ Other Control/Subcontrol

● Create New

Control Statement: Create New Control Statement

Title*: New trend in risk exa

Enter a new Statement*: Innovative control to curb risks

Do one of the following:

- By default, the **Create New** option is selected in the dialog. Enter a title and statement. This will create a new compensating control.
- Select **Other Control/Subcontrol** and click +.
- The **Select a Controls/Subcontrols** dialog appears. Expand the groups or content packs beneath the **Controls/SubControls** folder, locate and select the compensating control, and then click **OK** to exit the **Select a Controls/Subcontrols** dialog. This will add an existing control from the controls library
- Click **OK**. The compensating control is added.

There are three error conditions we need to check for when a user tries to add a compensating control to a control:

1. The same control as that which is being compensated cannot be added as a compensating control to itself.
2. A compensating control that is identical to one already present for a given control should not be able to be added.
3. A compensating control should not be able to compensate a control that itself is compensated.