

# Table of Contents

<b>RiskVision Help</b>	8
<b>RiskVision Threat &amp; Vulnerability Manager</b>	8
<b>About Threat and Vulnerability Manager</b>	8
About Threat and Vulnerability Manager	8
<b>About Threat Management</b>	9
About Threat Management	9
Vulnerabilities from Virtual Scans	10
Categorizing Vulnerabilities	11
<b>Vulnerability Risk Score</b>	12
Vulnerability Risk Score	12
Calculate an Entity Criticality Factor	13
Calculate a Vulnerability Risk Factor	14
Reporting Vulnerabilities	17
Other RiskVision Applications	18
Log into RiskVision	20
Log In as a Delegate	21
<b>Reset Your Password</b>	22
Reset Your Password	22
Log in With Your New Password	23
<b>Get Started</b>	24
Get Started with RiskVision	24
<b>Navigate RiskVision</b>	25
Navigation Overview	25
Using the Tree and Grid View	26
<b>The Grid View</b>	28
Grid View Overview	29
Limiting the Number of Rows	30
Pagination	31
Change the Grid Header Mode	32
Actions	33
Details	34
Customizing the Columns	35
<b>Common Features</b>	36
Common Features Overview	36
Changing the Grid Header Mode	37
Advanced Searching	38
Control Object Visibility	44
Rich Text Editor Overview	45
Batch Workflow Transitions	48
<b>Object Visualization</b>	51
Object Visualization Overview	51
Move the Layout	52
Bulk Exporting Evidence	53
<b>Bulk Export Documents</b>	54
Bulk Exporting Documents	54
Maximum Zip File Download Size	55
User Picker	56
Actions	58

Documents .....	60
<b>About the Welcome Page</b> .....	63
About the Welcome Page .....	63
Message Center .....	64
Quick Links Overview .....	65
Understanding the Message Center .....	66
<b>About Tickets Page</b> .....	67
About the Tickets Page .....	67
Creating a New Ticket .....	68
Batch Edit Tickets .....	69
About the Exception Requests Page .....	72
R6 Report License .....	73
<b>Configurations Overview</b> .....	74
Understanding Configurations .....	74
<b>Threat Management Preferences</b> .....	75
Threat Management Preferences .....	75
Entity Groupings .....	77
<b>Create a Grouping</b> .....	79
Create a Grouping .....	79
Vulnerability Status Configuration Options .....	81
<b>Workflows</b> .....	82
Workflows .....	82
<b>Modify Stage Settings</b> .....	83
Modify Stage Settings .....	83
Renaming The Stage .....	84
Configure Stage Transitions & Actions .....	85
Configuring Stakeholder Settings .....	89
Assigning Stakeholders .....	90
Allowing Stakeholders To Delegate .....	92
Allowing Stakeholders to Add Other Stakeholders .....	93
Send to Next Stage .....	94
Deleting Workflow Stages .....	95
Other Stage Options .....	98
<b>Stakeholder Escalations and Reminders</b> .....	101
Send Escalations and Reminders to Stakeholders .....	101
Send Reminders and Escalations to Task-Aware Stakeholders .....	102
Delegation & Delegation Revocation .....	103
<b>Force Stage Transitions</b> .....	105
Force a Stage Transition .....	105
Determining Stage Transition Mode .....	106
Manage Workflow Escalations .....	107
<b>Specify Multiple Workflows</b> .....	108
Specify Multiple Workflows .....	108
<b>Complex Selection Conditions</b> .....	109
Define More Complex Selection Conditions .....	109
Specify Sub-Conditions .....	110
Visualize Workflows .....	111
<b>Escalation</b> .....	113
Escalation Overview .....	113
Create an Escalation Configuration .....	114
<b>About Email Templates</b> .....	115

About Email Templates .....	115
Default Email Templates .....	116
<b>Configure Email Templates</b> .....	120
Configure an Email Template .....	120
Add A Customized Email Template .....	121
Update an Email Template .....	122
<b>Email Template Variables</b> .....	123
Email Template Variables .....	123
Alert Email Templates .....	124
Analytics Email Templates .....	125
Exception Email Templates .....	126
Risk Email Templates .....	127
Ticket Email Templates .....	128
Vendor Email Templates .....	129
More Variables .....	130
Modify the Variable Displaying Date .....	131
Add Object Fields to Email Templates .....	132
Add Custom Attributes to Email Templates .....	133
Getting Familiar with Email Notifications .....	134
<b>Filters</b> .....	137
Filters .....	137
Add a Filter .....	138
Modify Filter Conditions .....	139
Remove a Filter .....	140
<b>Group Filters</b> .....	141
Group Filters .....	141
Create a New Group .....	142
Delete a Group .....	143
About Complex Filters .....	144
User Variables .....	146
Configure a Threshold Range for Calculating Vulnerability Scores .....	147
About Ticket Management Preferences .....	149
Exception Management Preferences .....	150
<b>Essential Objects in RiskVision</b> .....	154
<b>Entities</b> .....	154
Entity Types .....	154
Create a New Entity .....	156
Create a New Computer Type Entity .....	161
Set the Name, Type, and Owner for an Entity .....	167
About Discovered Entities .....	168
<b>Display Entity Details</b> .....	169
Display Entity Details .....	169
Entity Details Tabs .....	171
<b>About Ownership Types</b> .....	173
About Ownership Types .....	173
Add A New Ownership Type .....	174
Delete an Ownership Type .....	175
Change the Ownership Type Settings .....	176
Configure Owners .....	177
Configure Entity Compliance and Criticality Ranges .....	179
Set the Criticality Rating .....	180

<b>About Entity Relationships</b> .....	182
About Entity Relationships .....	182
About Relationship Types .....	183
Relationship Types Overview .....	183
Predefined Relationship Types .....	184
Create Entity Relationships .....	185
Create and Delete Relationship Types .....	188
Import a Relationship .....	189
Visualize Relationships .....	190
Visualize a Relationship .....	190
Relationship Report .....	191
Relationship Explorer .....	192
Assign a Vulnerability .....	193
Operating Systems .....	196
Applications .....	198
Ports .....	200
<b>Vulnerability Compensating Controls</b> .....	201
Add Compensating Controls .....	201
Batch Edit Compensating Controls .....	205
Remove Compensating Controls .....	209
Entity Actions .....	212
Entity Attribute Screens .....	213
Contextual Reports of Entities .....	216
<b>About Entity Collections</b> .....	219
About Entity Collections .....	219
About Entity Collection Details .....	227
<b>About Dynamic Groups</b> .....	228
About Dynamic Groups .....	228
Default Dynamic Groups .....	229
<b>Configure a Dynamic Grouping</b> .....	230
Group Entity Applications .....	230
Group Computer And Network Devices .....	231
<b>Configure Dynamic Group Folders</b> .....	234
Configure Dynamic Group Folders .....	234
Set the Name and Description .....	239
Set Folder and Grouping Preferences .....	240
<b>About the Organizational Hierarchy</b> .....	241
Organizational Hierarchy Overview .....	241
Organization Hierarchy Actions .....	242
Enable the Organization Hierarchy Selection .....	243
Define a New Organization .....	244
Entity Management .....	245
<b>Vulnerabilities</b> .....	246
Vulnerabilities .....	246
My Vulnerabilities .....	247
Vulnerabilities from Scanners or Users .....	248
Inferred Vulnerabilities .....	249
Scanner & Inferred Vulnerabilities .....	250
All Vulnerabilities .....	251
Recent Vulnerabilities .....	252
Recent Vulnerabilities of Interest .....	253

<b>Actions in Vulnerabilities Grids</b> .....	255
Perform Actions in Vulnerabilities Grids .....	255
Use More Actions in Vulnerabilities Grids .....	256
Manage Scan Results .....	257
<b>About Vulnerability Details</b> .....	258
Vulnerability Details Overview .....	258
About the More Information Tab .....	261
<b>Link Tickets to Vulnerabilities</b> .....	263
Link Tickets to Vulnerabilities .....	263
Link Tickets Automatically .....	264
Link Tickets Manually .....	265
<b>Exceptions for Vulnerabilities</b> .....	266
Add Exceptions to Vulnerabilities .....	266
Vulnerability Compensating Controls on Exceptions .....	270
Exceptions and Vulnerability Instances .....	272
Vulnerability Archiving .....	273
<b>Threats</b> .....	274
Threats .....	274
<b>Threat Pages</b> .....	275
My Threats .....	275
Recent Threats .....	276
All Threats .....	277
Threat Intelligence .....	278
Malware .....	279
Threat Actors .....	280
Vulnerability Reports .....	281
<b>Threat Object Pages</b> .....	282
Threat Object Pages .....	282
General .....	283
Report .....	285
Vulnerabilities .....	286
Targeted Entities .....	289
Tickets .....	290
Incidents .....	291
Exploits .....	294
<b>Technologies</b> .....	296
Technologies .....	296
All Technologies .....	297
Recent Technologies .....	298
Search for Technologies .....	299
Review Non-Validated Technologies .....	301
Create a Technology .....	302
<b>Technology Details</b> .....	303
About Technology Details .....	303
Weaknesses .....	306
Patches .....	307
<b>Exception Requests</b> .....	308
Vulnerability Exception Details Overview .....	308
Create a Vulnerability Exception Request .....	310
Exception Request Basic Details .....	312
Exception Request Attachments .....	315

Transition Exception Requests .....	316
Link Exception Requests with Vulnerabilities .....	317
Default Exception Workflow .....	318
Edit an Exception .....	319
Affected Instances .....	320
<b>Tickets</b> .....	321
About Tickets .....	321
About Ticket Flow .....	323
Link a Ticket to an Entity .....	325
Start and Transition the Ticket Process .....	326
Change the Default Ticket Workflow .....	327
Assign a Ticket to Another User .....	328
Delegate an Object to Another User .....	329
Setting General Ticket Information .....	331
Link a Ticket to a Vulnerability .....	333
Delete a Ticket .....	335
Automatic Ticket Archiving .....	336
Link a Ticket to a Compensating Control .....	337
Create a Vulnerability Exception on a Ticket .....	339
Exceptions on Tickets .....	343
<b>The Document Repository</b> .....	344
About the Document Repository .....	344
Document Repository Structure .....	345
Document Repository Ownership .....	347
Modify Ownership .....	348
<b>Document Repository Actions</b> .....	349
Document Repository Actions .....	349
Move .....	350
Delete .....	351
<b>Vulnerability Compensating Controls</b> .....	352
Vulnerability Compensating Controls .....	352
Create Categories, Sub Categories & Compensating Controls .....	354
Edit or Delete Categories, Sub Categories & Compensating Controls .....	357
Move Sub Categories & Compensating Controls .....	361
Add a Compensating Control to a Vulnerability .....	363
Edit a Compensating Control Attached to a Vulnerability .....	366
Remove a Compensating Control From a Vulnerability .....	368
Export & Import Categories & Sub Categories .....	369
<b>Frequently Asked Questions</b> .....	371
Data Correlation .....	371
Owner Stakeholder Assignment .....	372
Customize or Configure .....	373
Assets .....	374
Risk Scoring with Threat Modeling .....	375
Workflow & Ticketing .....	376
Create a Technology .....	379
Integration .....	380



## About Threat and Vulnerability Manager

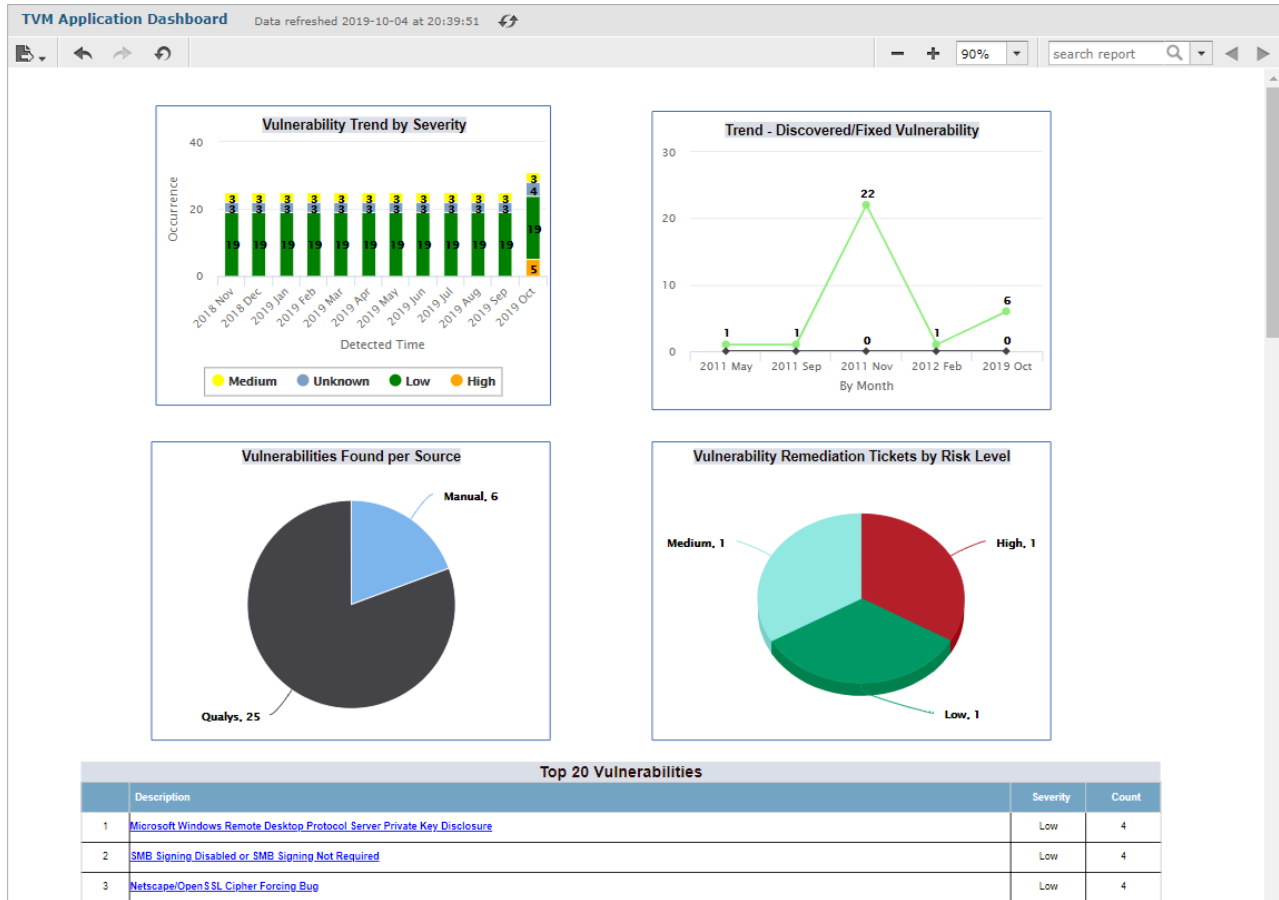
Threat and Vulnerability Manager allows organizations to consolidate their threat and vulnerability programs on a single platform. This application integrates with vulnerability, early warning, and exploit data feeds, such as those from iDefense, the National Vulnerability Database, and Offensive Security. 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 entity database, mitigating risks for entities that aren't reachable by vulnerability scanners. Once detected, vulnerabilities are assessed and resolved using the system's workflow for true closed-loop vulnerability management.



## About Threat Management

Threat management means being aware of known [vulnerabilities](#) that may apply to your entities and technologies.

The National Vulnerability Database (NVD) tracks thousands of vulnerabilities, most identified by a unique CVE (Common Vulnerabilities and Exposures) number.



*The Threat & Vulnerability Manager Application Dashboard.*

Not all vulnerabilities will apply to your organization. The NVD and other subscription feeds, such as VeriSign iDefense Labs, provide vulnerability definitions (VD). When a VD targets your entities or [technologies](#), the system identifies a vulnerability instance (VI). VIs can be inferred (reported by a feed) or actual.

RiskVision works with vulnerability scanners, such as Qualys, that identify vulnerability instances. RiskVision can also create VIs on its own, based on VDs and the [technologies catalog](#) known as the Common Platform Enumeration (CPE). VIs are usually identified by CVE numbers. The same VI may be reported more than once for a given entity.

## Vulnerabilities from Virtual Scans

If you have a source of vulnerabilities, such as the iDefense connector, the Vulnerabilities grid will include virtual scans. Virtual scans produce inferred vulnerabilities. While the iDefense connector is a major source of CVE to CPE mapping, the NVD is the primary source. Vulnerabilities can also be created manually.

## Categorizing Vulnerabilities

Vulnerabilities fall into specific categories identified by the [Common Weakness Enumeration](#) (CWE) that are useful for grouping threats and remediation efforts. In addition, each vulnerability definition has a Common Vulnerability Scoring System (CVSS) score. A specific VI's CVSS score can be adjusted based on local conditions, entity criticality, and other environmental factors.

In addition to tracking possible [vulnerabilities](#) and identified vulnerability instances, RiskVision tracks remediation efforts using [Tickets](#). Because many entities can be affected by a single VI, tickets are created for each entity group. You can mark one or more entities in the group as 'fixed' (mitigated), and when all entities have been mitigated and the ticket has been closed, the VI itself is marked as mitigated. For information about how to link tickets for reported vulnerabilities, see [Linking Tickets to Vulnerabilities](#).

## Vulnerability Risk Score

Most organizations have many more vulnerabilities than they can patch. Vulnerability risk scores are used to prioritize these vulnerabilities so you can make intelligent decisions about which vulnerabilities to patch first.

Vulnerability risk scoring uses the following terms:

- **Entity Criticality Factor** – Portion of the Vulnerability Risk Score formula that represents the relative importance of an entity. It is derived from the entity's Business Criticality value.
- **Enhanced Risk Score** – A calculation of a risk factor that indicates the relative likelihood of a vulnerability to be exploited.
- **Vulnerability Definition Risk Score** – The sum of the risk scores of all of the instances of the vulnerability.
- **Vulnerability Risk Factor** – A value that is used in the Vulnerability Instance Risk Score equation that indicates the relative likelihood of a vulnerability being exploited.
- **Risk Reduction %** – The sum of the risk reduction percentage points of each vulnerability compensating control attached to the vulnerability. If the vulnerability has an approved exception, this value equals 0.
- **Vulnerability Instance Risk Score** – The risk a vulnerability instance, which is a vulnerability on an entity, poses to an organization. It comprises both an element of the importance of an entity and another element of the likelihood that the vulnerability will be exploited on that entity. This risk score uses the following formula:

$$\text{Vulnerability Instance Risk Score} = (\text{Entity Criticality Factor} * \text{Vulnerability Risk Factor}) * (1 - \text{Risk Reduction \%})$$

## Calculate an Entity Criticality Factor

The Entity Criticality Factor is meant to approximate the relative importance of an entity.

By default, the Entity Criticality Factor is equal to the criticality of an entity. Typically, this will take one of the following values:

- High = 10
- Medium = 6
- Low = 3
- Unknown (not set) = Null

You can modify the Entity Criticality Factor equation to have a maximum of four variables. Therefore, you can add up to the three additional criteria to the entity criticality attribute, or if you remove the entity criticality, you can add up to four additional criteria. These criteria are custom attribute string values. You can assign a corresponding number that determines the weight of that variable for each of these values.

The Entity Criticality Factor can be calculated with the following formula:

```
Entity Criticality Factor = Entity Criticality * Custom Attribute String 1 * Custom  
Attribute String 2 * Custom Attribute String 3
```

Or

```
Entity Criticality Factor = Custom Attribute String 1 * Custom Attribute String 2 *  
Custom Attribute String 3 * Custom Attribute 4
```

There cannot be more than 4 arguments in a formula, but you can use operations other than multiplication. The Custom Attribute Strings must have a number associated with each possible value.

For example, if you used PCI as a custom attribute, and the possible values were "Yes" and "No", then you may decide to make "Yes" = 1 and "No" = .5, so that if an entity is not in scope for PCI, then the risk of any vulnerabilities on that entity would be reduced, all other factors being the same, as compared to an entity that is in scope for PCI.

Another example of how a custom attribute can be used in the calculation of an entity criticality factor is if you had a custom attribute that represented an entity location within a network. For example, you could use the following scale:

- DMZ = 2
- Internal network – edge = 1
- Internal network – core = .5

Note that this would only approximate the location, and other factors of the Entity Criticality Factor equation could, and probably will, result in some entity that are in the core of the network, and therefore behind multiple firewalls, having a higher entity criticality factor.

For a discussion about how to equate the labels of a custom attribute with numerical values, please see the section "Assigning Numerical Values to Custom Attributes."

## Calculate a Vulnerability Risk Factor

The Vulnerability Risk Factor estimates the likelihood of a vulnerability instance being exploited on an entity. There are two mutually exclusive ways to set a vulnerability risk factor:

1. CVSS v2.0 score
2. Enhanced score

Your administrator chooses whether to use the CVSS v2.0 score or the Enhanced score as the Vulnerability Risk Factor. The CVSS v2.0 score is more difficult to use. Although it's possible to change your selection, we recommend you don't change methods.

If you use the CVSS v2.0 score, it will be used as the Vulnerability Risk Factor, and will be multiplied by the Entity Criticality Factor to determine the Vulnerability Instance Risk Score. The CVSS score works on a 0-10 scale.

The CVSS score will come from the scanner that reports the vulnerability. In contrast, the Enhanced score takes into account the following variables:

1. CVSS v2.0 Confidentiality Impact Vector.  
The possible values are:
  - None: 0.
  - Partial: 1
  - Complete: 2
2. CVSS v2.0 Integrity Impact Vector.  
The possible values are:
  - None: 0.
  - Partial: 1
  - Complete: 2
3. CVSS v2.0 Availability Impact Vector.  
The possible values are:
  - None: 0.
  - Partial: 1
  - Complete: 2
4. CVSS v2.0 Access Complexity.  
The possible values are:
  - Low: 1
  - Medium: 3
  - High: 5
5. CVSS v2.0 Access Vector.  
The possible values are:
  - Local: 1
  - Adjacent Network: 3
  - Network: 5.
6. CVSS v2.0 Authentication Vector.  
The possible values are:
  - Multiple: 1
  - Single: 3
  - None: 5
7. The number of days a vulnerability has been open: Calculated as the difference between the current date and the date the CVE vulnerability was published. This number is significant because the longer a vulnerability has been open, the more likely it is to be exploited.
8. Exploit Factor: Whether there is a known exploit for the vulnerability, and its exploit type. When more than one exploit maps to a vulnerability, the equation will select the exploit with the highest Exploit Factor. The possible values are:
  - Local: Local access to the computer in question is required to exploit the vulnerability. Value = .6.
  - Remote: The exploit can be conducted across a network. Value = 1.
  - Shellcode: Value = .6
  - WebApp: A web application. Value = 1
  - DOS: Results in a Denial of Service attack. Value = .5
  - No matching exploit: Value = .25

The formula for the Enhanced Vulnerability Risk Score is:

$$\text{Enhanced Score} = (\text{Numerator} / \text{Denominator}) \times \text{Threat factor} \times \text{Exploit Factor} \times \text{SQRT}(\text{Days Known}^*)$$

where:

$$\text{Numerator} = \text{Factorial}(\text{Confidentiality} + \text{Integrity} + \text{Availability})$$

and

$$\text{Denominator} = \text{Square}(\text{Access Complexity} + \text{Authentication} + \text{Access Vector})$$

- Days Known is capped at 730 days, which equates to 2 years. The above data shows the actual number of days the vulnerability has been known, but the formula does not allow the Days Known value to exceed 730.
- If there is a threat that matches the vulnerability, the default value is 2. If there is no matching threat, then the default value is 1.

The Enhanced Score is calculated for each CVE that maps to a scanner-reported vulnerability. For example, McAfee Vulnerability Manager ID 140978, Red Hat Enterprise Linux RHSA-2015-2506 Update Is Not Installed, has 19 CVEs that map to it. An Enhanced Score will be calculated for each of the 19 CVEs that map to it, then the Enhanced Scores for these 19 CVEs that map to the scanner-reported vulnerability will be summed up to create the total Enhanced Score for the scanner-reported vulnerability.

### Placement of the Vulnerability Risk Score in the RiskVision UI

The Vulnerability Risk Score appears in the following locations within the RiskVision user interface:

- The following vulnerability grids have a new risk score column: Vulnerabilities from Scanners or Users, Scanner & Inferred Vulnerabilities, All Vulnerabilities, Recent Vulnerabilities, and Recent Vulnerabilities of Interest.

Primary Source	Secondary Sources	Type	Identifier	Title	Description	Severity	CVSS v2.0 Score	Risk Score	Date Published	Applicable	Exploits	Status	Owner	Entities Affected	Entities With Tickets	Entities with Exceptions	Unresolved Entities	Latest Patch Date
NVDB	N/A	Vulnerability	CVE-2012-0251 CVE-2012-0251		license.php in system-portal before 1.6.2 in op5 Monitor and op5 Appliance before 5.5.3 allows remote attackers to execute arbitrary commands via shell metacharacters in the timestamp parameter for an install action.	High	10.0	3928.98	2014-01-01	Yes	No	N/A	kalpona g	1	0	0	1	N/A

- The vulnerability definition and vulnerability instance user interfaces have two new tabs: Enhanced Score and Risk Score. The Enhanced Score tab shows the components of the Enhanced Risk Score as well as the overall Enhanced Score. The Risk Score tab shows the components of the Entity Criticality Factor, Vulnerability Risk Factor, and Vulnerability Risk Score. For the vulnerability definition, these tabs show the totals across all instances of the vulnerabilities, while the instance only shows the scores for that instance.

Vulnerability: CVE-2012-1972

[dr]public/System\_Reports/Enhanced\_Score\_For\_Vulnerability

**Enhanced Score For Vulnerability** Data refreshed 2018-04-02 at 15:52:51

CVE	Confidentiality	Integrity	Availability	Numerator	Access Complexity	Authentication	Access Vector	Denominator	Days Known	Exploit Factor	Threat Factor	Enhanced Score
CVE-2012-1972	2	2	2	720	1	1	1	9	2042	0.25	1	£40.37
<b>Total Enhanced Vulnerability Score</b>												£40.37

Enhanced Score=(Numerator/Denominator) X Threat Factor X Exploit Factor X SQRT(Days Known<sup>2</sup>)  
 where:  
 Numerator = Factorial(Confidentiality + Integrity + Availability) and  
 Denominator = Square(Access Complexity + Authentication + Access Vector)

\* Days Known is capped at 730 days, which equates to 2 years. The above data shows the actual number of days the vulnerability has been known, but the formula does not allow the Days Known value to exceed a quantity of 730.

Vulnerability: CVE-2012-1972

[dr]public/System\_Reports/Risk\_Score\_For\_Vulnerability

**Risk Score For Vulnerability** Data refreshed 2018-04-02 at 15:57:06

Entity Criticality	Number of Vulnerability Instances	Entity Criticality Factor	Vulnerability Risk Factor	Vulnerability Risk Score
High	2	9.0	10.0	180
<b>Total Vulnerability Risk Score</b>				180

- The Vulnerabilities List tab that appears in certain types of entities, such as computers and applications, has a new Risk Score column. Additionally, it shows an aggregate vulnerability Risk Score for the entity at the top of the tab, above the grid.

Computer: Active Directory

**Vulnerabilities Found by Scanners or Users**

Vulnerabilities : 2 Vulnerability Risk Score : 180.0

1-2 of 2

Assign New Filter Delete More Actions...

Filter by - Show all - Refresh

Title	Severity	CVSS Score	Risk Score	First Reported	Last Reported	Interfaces	Reported By	Status	Patch Status	Test URL	Secondary Source	File Name	Line Number
CVE-2012-1972	High	10.0	90.0	2018-04-02	2018-04-02	10.10.30.4		Unresolved	N/A	N/A	N/A	N/A	N/A
CVE-2015-5581	High	10.0	90.0	2018-04-02	2018-04-02	10.10.30.4		Unresolved	N/A	N/A	N/A	N/A	N/A

## Null Values

When a variable that's used for the vulnerability risk score calculation is not present, this results in a null value, which will nullify the result of the vulnerability risk score equation. The only exception to this is when a vulnerability does not have any mapped exploits, in which case the Exploit Factor of the Enhanced Score is given a value of .25.

Null values are displayed in the **Enhanced Score** and **Risk Score** tabs as "N/A."

## Configuring the Vulnerability Risk Score Calculations

Please refer to the Administrative Guide for the instructions regarding configuring vulnerability risk score calculations.



## Reporting Vulnerabilities






### To view threat management reports:

1. Click the **Analytics** tab.
2. Click **Reports**.
3. Navigate to **Reports > Shared Reports > Threat and Vulnerability Management**

Reports in this folder are further categorized as feeds, technology, and weakness reports.

## Other RiskVision Applications

Other RiskVision applications are listed in the table below:

ICON	APPLICATION	DESCRIPTION
	Compliance Manager	Compliance Manager 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. Evidence and control results can be automatically collected through connectors or questionnaire results from business users. Data classification, ownership configuration, compliance assessment, mitigation, and reporting are all enabled. Compliance Manager also supports popular frameworks, standards, and regulations such as ISO 27002, CIS, HIPAA and PCI. This application improves process efficiency and integrity, as well as data quality and reliability.
	Enterprise Risk Manager	Enterprise Risk manager is a comprehensive risk lifecycle management solution. It allows organizations to identify, assess, and mitigate risks 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. Enterprise Risk Manager features rich reports and dashboards, as well as easy to use risk assessment tools that enable organizations to understand and monitor their enterprise risk posture. It also includes out-of-the-box support for popular risk methodologies such as COSO, AZ/NZS 4360 and ISO.
	Vendor Risk Manager	Vendor Risk Manager enables organizations to audit and manage third-party risks, as mandated by regulations and standards such as ISO 27001, PCI, and FISMA. It 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 that are used to apply applicable controls. Delegated administration and automation features enable Vendor Risk Manager to scale to large vendor populations.
	Policy Manager	Policy Manager enables the management of enterprise policies on a single centralized platform. Organizations can enforce policy and process standards across different locations, departments, and programs. It also 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.
	Incident Manager	Incident Manager enables organizations to collect, classify, and manage multiple IT and non-IT incidents. It's a single collection point for all incidents that are manually and automatically reported. 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 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 risks to provide closed-loop feedback for policy and control assessment and risk monitoring. Incidents are rated based on their criticality so that organizations can respond based on the impact to the business.

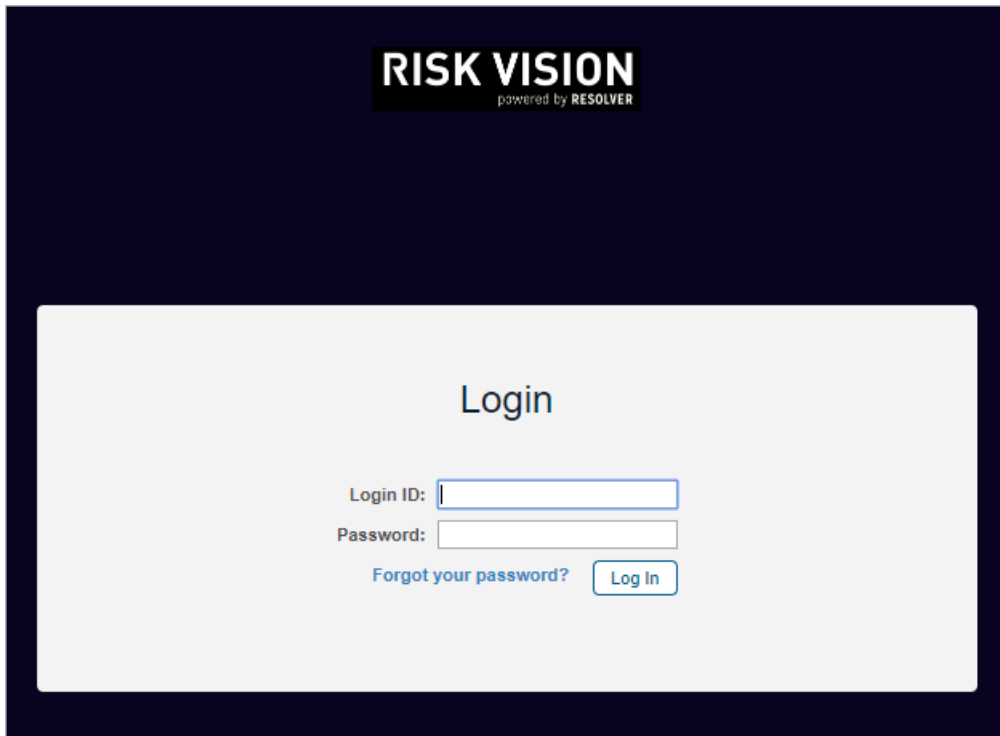
## Log into RiskVision

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.

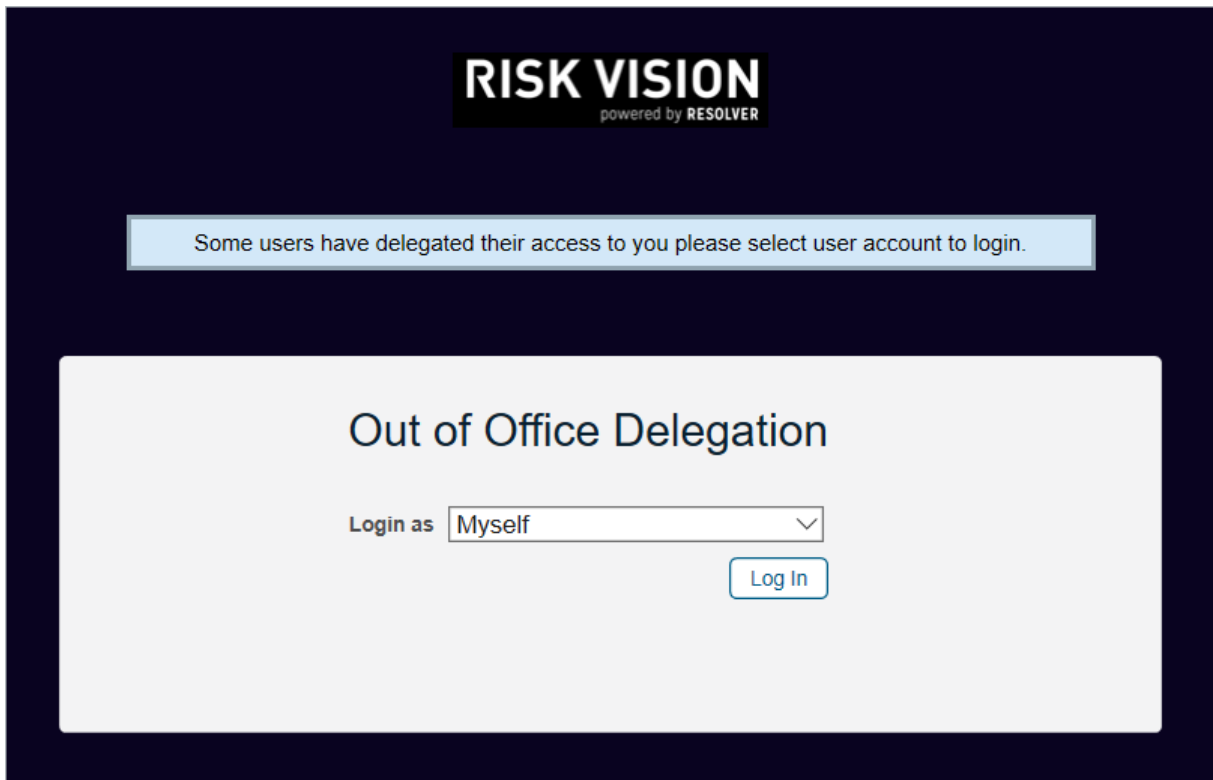
4. Click **Accept** to continue. The **Welcome** page is displayed.

## Log 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.



*The Out of Office Delegation screen.*

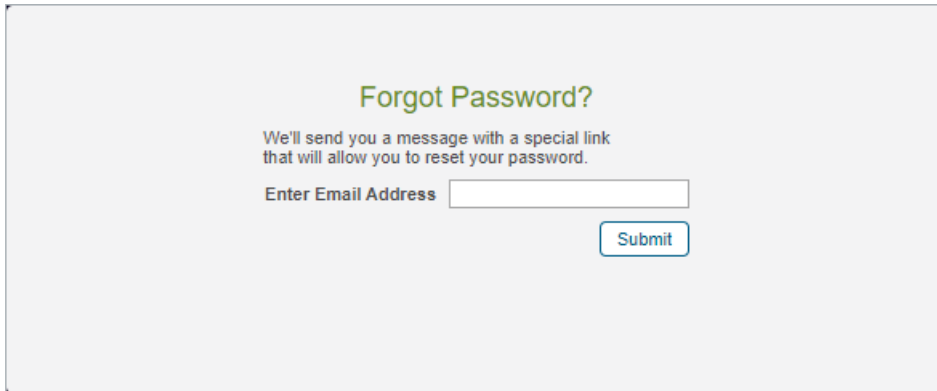
When you are logged into a delegated user account, you can perform any task permitted by that user's account permissions on behalf of that user. When the delegated user logs into RiskVision, the **Current User** will appear as **Logged in as: delegated by [username]**.

## Reset Your Password

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

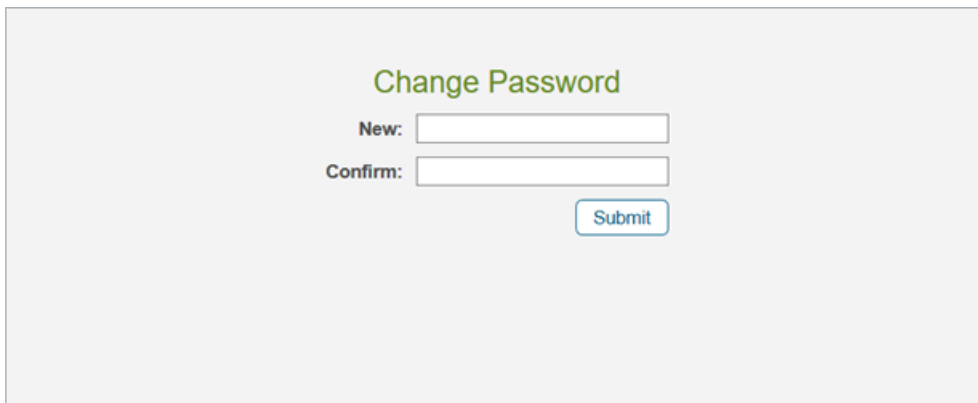
### To reset your password:

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.



*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.



*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](#).

## Log in With Your New Password

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

## Get Started with RiskVision

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're not a stakeholder on any tasks, you won't see any links in the sections.

By default, each section will show up to five items. 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.

This is 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**

These pages will help you to view, edit, and update the list of items. The user interface of each page can be customized to fit the needs of your business goal.

We recommend familiarizing yourself with the navigation, tree and grid, actions, user settings, and advanced search. For more information, see [Navigating the RiskVision System](#).



## Navigation Overview

RiskVision pages use a consistent interface to easily navigate from any page in the application.



*The navigation ribbon in the Threat & Vulnerability Manager.*

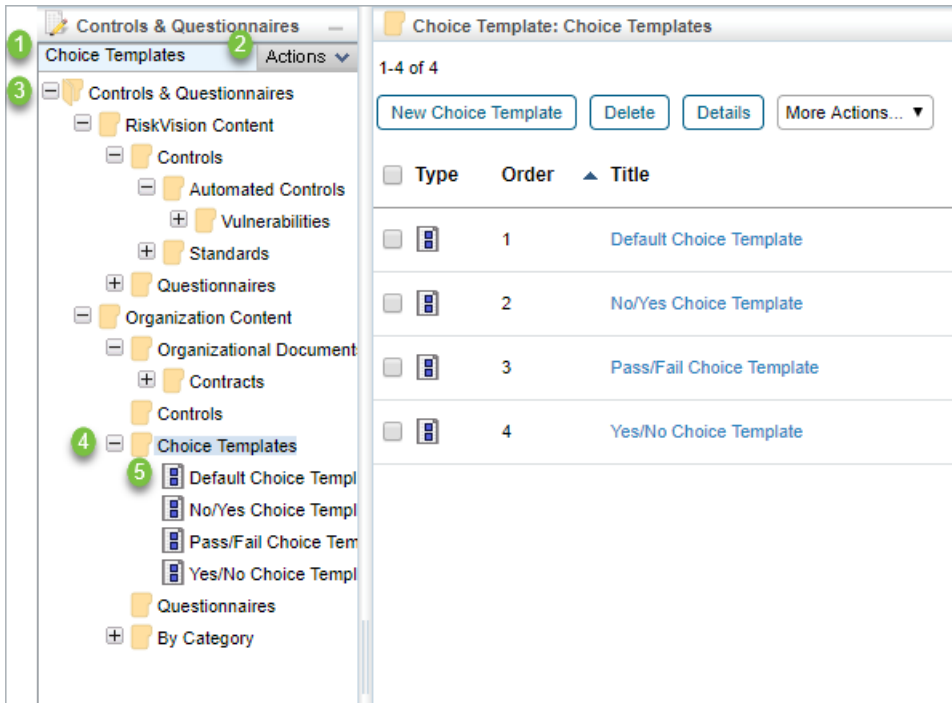
Selecting a different application will change the available menus. The specific menus and submenu choices available depend on the permissions assigned to your user role.

Hovering your mouse over a menu item displays a dropdown submenu. You can quickly view a snapshot of the available pages by moving the mouse over each menu.

## 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](#).



*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.

Object Target	Description
	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.

## 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.

## Grid View Overview

The grid view displays 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.

## Sort 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](#).

## Refresh

The table represents a snapshot of the underlying data at the time it was first displayed. Some data, such as Charts, 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

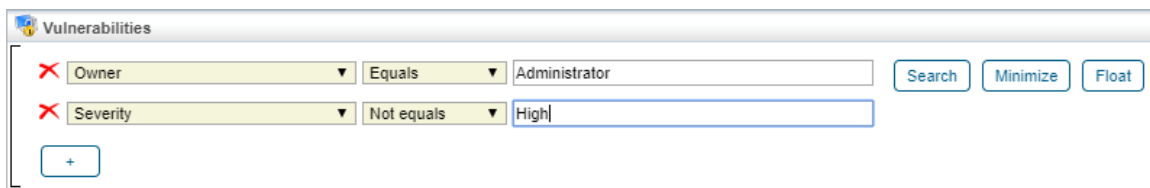
Certain grids, such as Entities, Vendors, and all grids on the Vulnerabilities menu, contain the Advanced Filter to help you locate the objects using one or more advanced search conditions.

### 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.



*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.

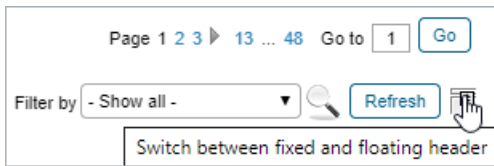


*RiskVision's pagination controls.*

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.

## Change the Grid Header Mode

A RiskVision object grid can have various numbers of rows on any page. As a result, you can only view a certain number of rows in a browser, whose dimensions vary according to your monitor's size. When you scroll down the grid in a browser to view the remaining objects, the grid header row moves along with other rows.



*Click the icon next to Refresh to select a fixed header.*

To prevent the header row from moving, click the icon next to the **Refresh** button.



## 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.

To create objects, click **New**. To delete objects, check the box to select the rows to remove and click **Delete**. The **More Actions...** dropdown 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 can be done multiple ways:

- Open the grid view and check the box to select the desired object, then click **Details**.
- Open the **More Actions...** dropdown list, then click **Details**.
- Click the object's name or title.

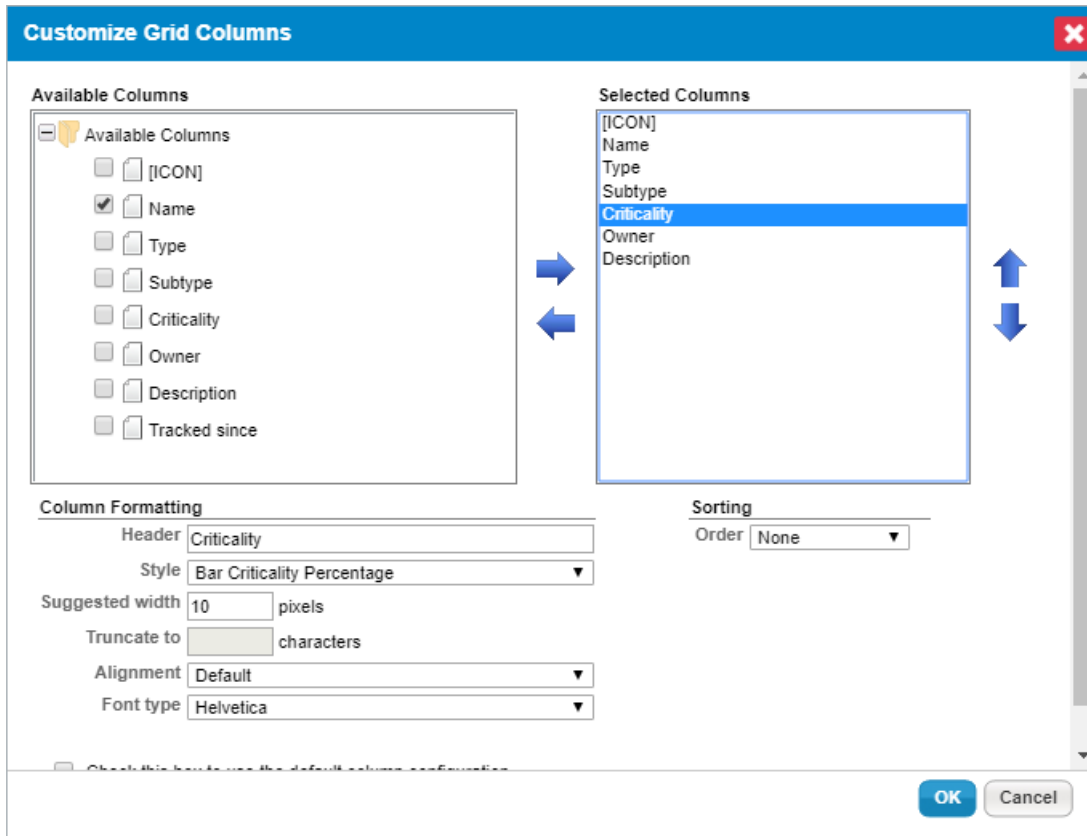
Some kinds of objects do not have details. Some, such as the **Home > Questionnaires** view, have links to more than one kind of object (in this case, entities and questionnaires). Details can be displayed in the lower half of the grid view in a popup window, or the details view can replace the entire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

## Customizing 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**.



*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.

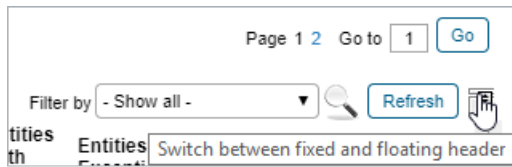
## Common Features Overview

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."

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

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

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

### Additional Information

For more information about the advanced searching features built in to RiskVision, see [Apache Lucene - Query Parser Syntax](#).

Using special characters to search objects might not return correct results. Instead, you can use the Advance Filter in the Filter by dropdown 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
- attachments.name [Note misspelling]
- attachments.pathId [Note misspelling]
- attachments.url [Note misspelling]
- attachments.version [Note misspelling]
- customAttributes.string1 (to) customAttributes.string25
- customAttributes.text1 (to) customAttributes.text2
- customAttributes.date1 (to) customAttributes.date3

- customAttributes.boolean1 (to) customAttributes.boolean5
- customAttributes.long1 (to) customAttributes.long3
- customAttributes.lstring1 (to) customAttributes.lstring3
- customAttributes.extendedCustomAttributes.string1 (to) .string25
- customAttributes.extendedCustomAttributes.text1 (to) .text2
- customAttributes.extendedCustomAttributes.date1 (to) .date3
- customAttributes.extendedCustomAttributes.boolean1 (to) .boolean5
- customAttributes.extendedCustomAttributes.long1 (to) .long3

#### Vulnerability ID

- captionDB (vulnerability title)
- identifier (use title if available)
- description
- abstractText
- analysis
- recovery
- defaultSeverity
- cvssVector (matches value to first ':')
- likelihood
- source
- sourceFlags (string from int; for example, 3 is 'nvdbidefense')
- assessmentCheckSystem
- assessmentCheckName
- assessmentCheckHref
- recordType
- vulnerableProducts.description
- vulnerableProducts.title
- vulnerableProducts.vendor
- vulnerableProducts.version
- data.data
- tags.name
- tags.description
- tags.type
- tags.referenceType

#### Vendor ID

Kind of Asset/Entity; adds:

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

## Control Object Visibility

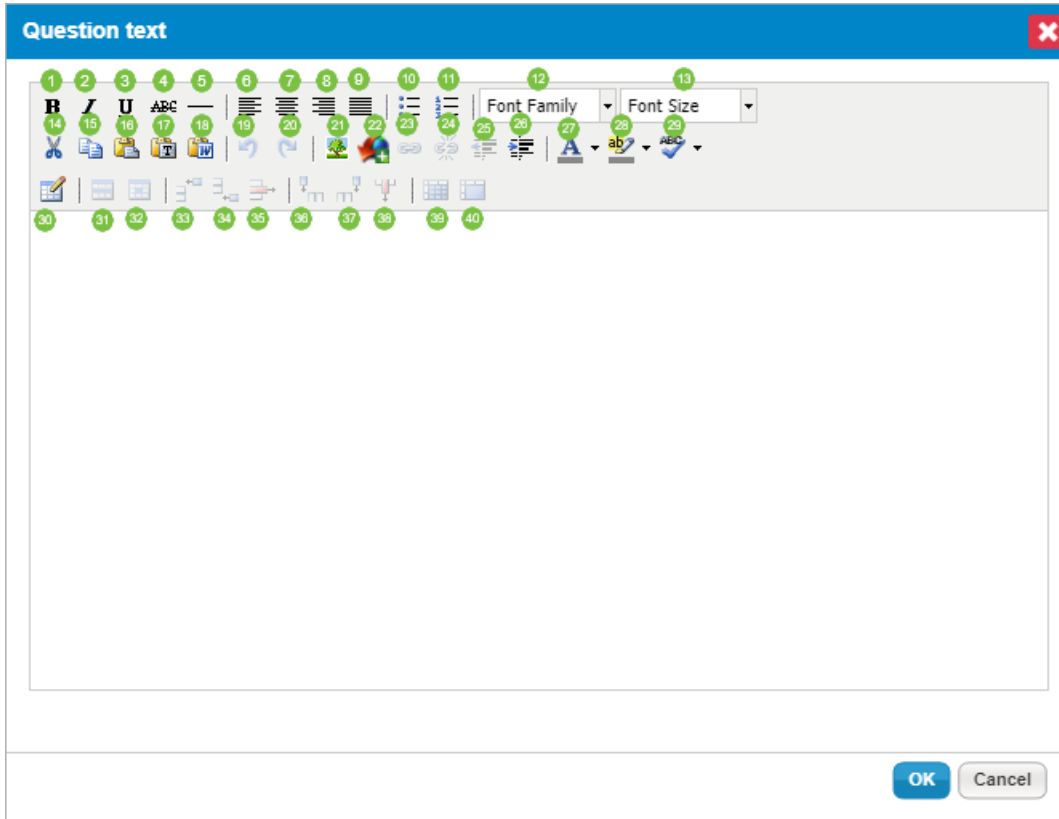
Many default and user-defined objects have an **Applications** tab to help you control the visibility of an object in the RiskVision applications. Even with sufficient permissions to access the application and the menu item, the object will not be visible to you if the applications is not selected as described below.

### To control an object's visibility:

1. Select an object.
2. Click the **Applications** tab.
3. Click **Edit** and select the checkbox next to application(s).
4. Click **Save**. The object is now visible in the application(s) you have selected in the previous step.

## Rich Text Editor Overview

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.

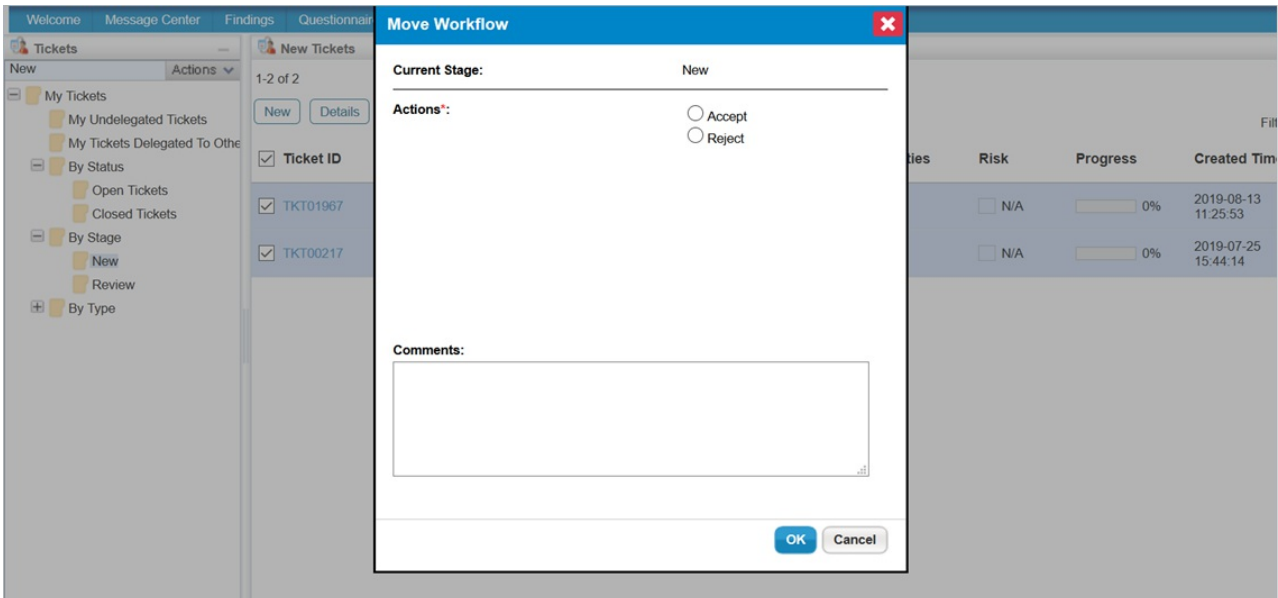
## Batch Workflow Transitions

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.



*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.

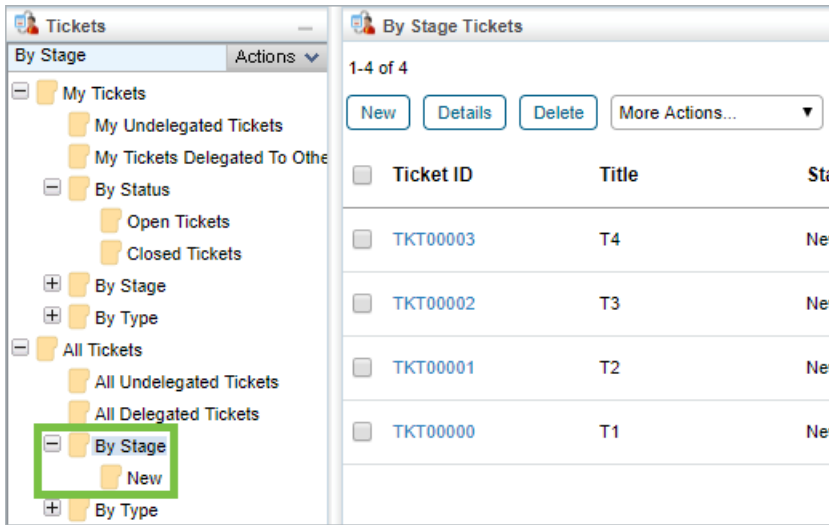
### To bulk-transition objects:

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



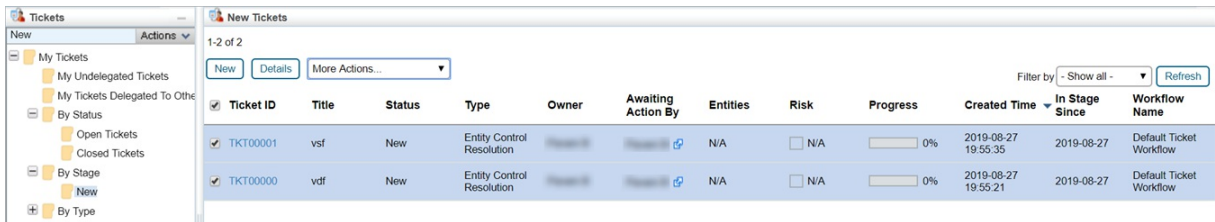
Exceptions, or Incidents).

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



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.



Selected objects in the **New** sub-folder.

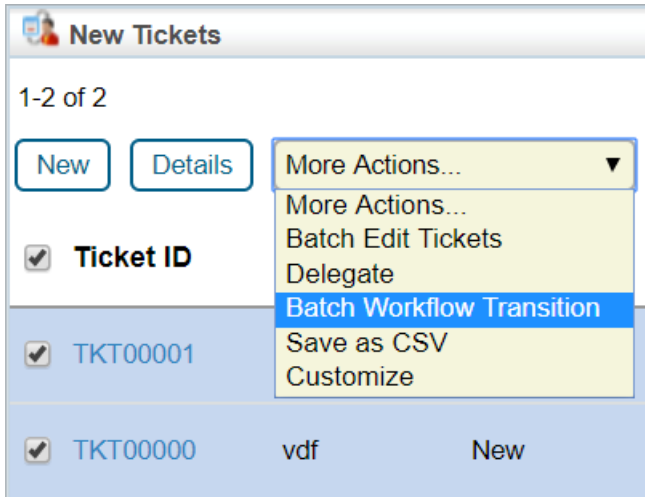


When selecting objects in bulk, review the **Workflow Name** column on the far-right of the grid to ensure all objects belong to the same workflow definition. If a workflow's name was recently modified, the workflow must be synchronized before it will display its current name in the column.



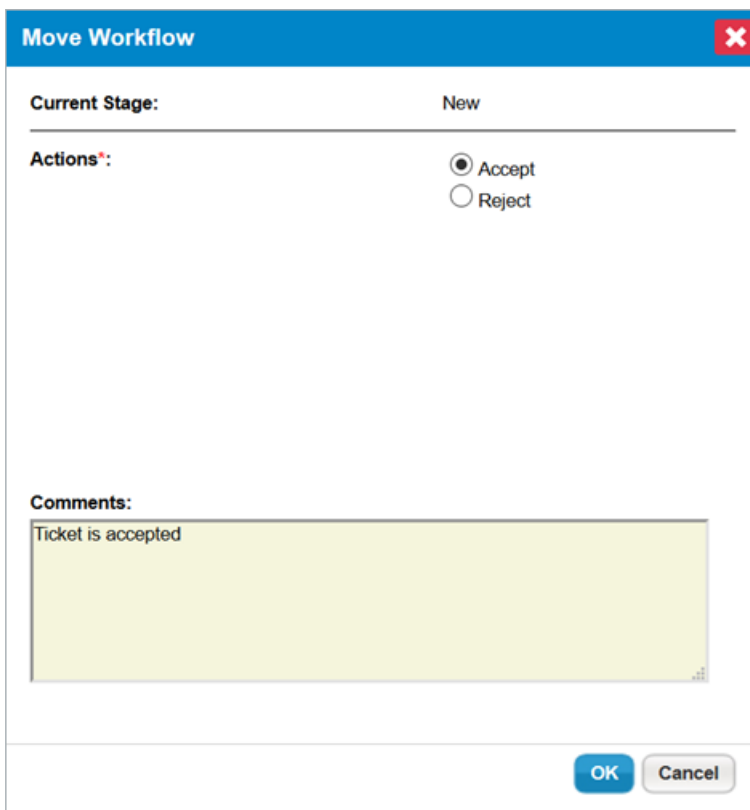
A maximum of 50 objects can be selected for a single bulk transition. Closed objects cannot be selected.

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.



The Move Workflow window.









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

## Object Visualization Overview

This section provides an overview of visualization tool options available in RiskVision. For case-specific information about how the RiskVision visualization tool helps understand the pattern with respect to workflows and relationships, see [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's also displayed by clicking on Stages tab for workflows.

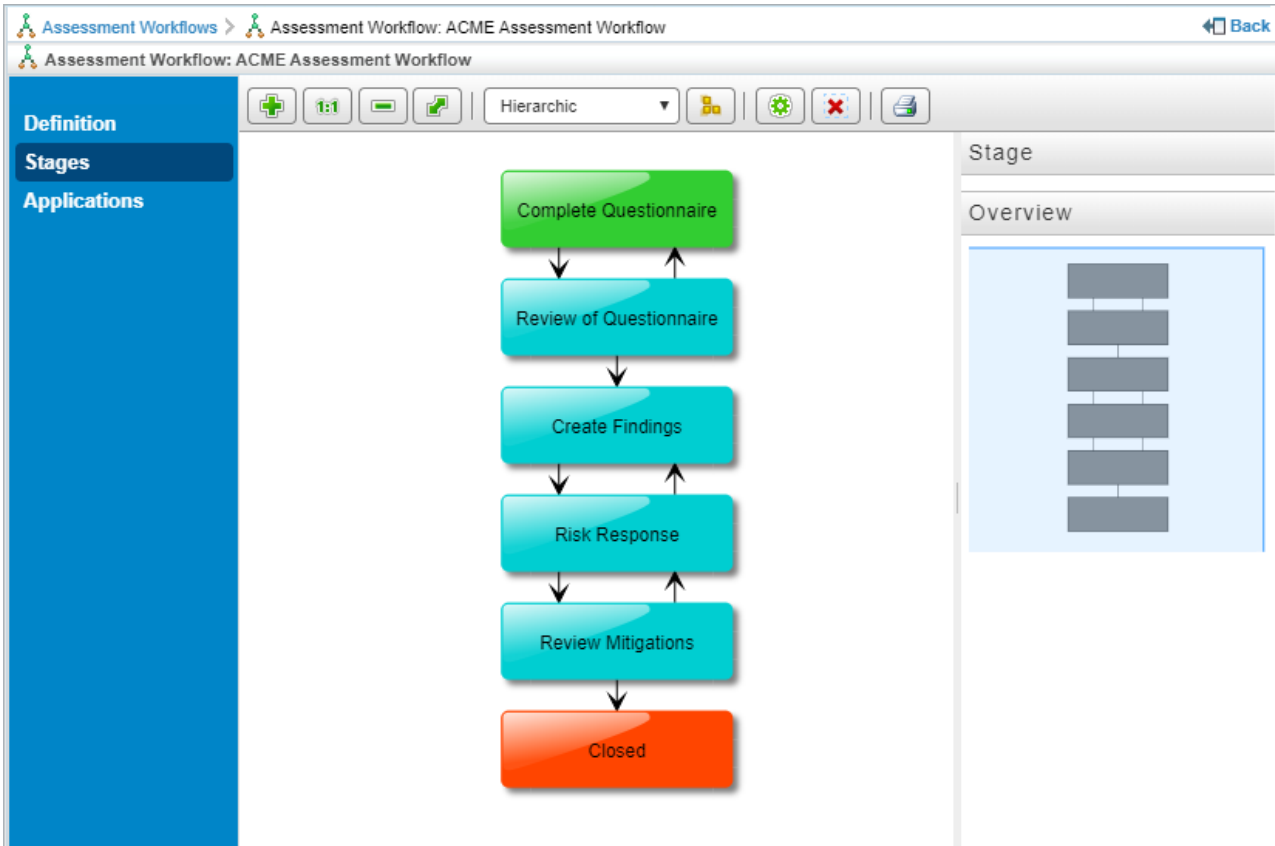
The following tool options are available to enhance your visual experience:

Option	Description
	Click to magnify the layout. Continue selecting this icon until you have achieved the desired magnification level.
	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.

Note: To visualize workflows in RiskVision, you need a web browser with HTML5 support.

## Move 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.

The screenshot displays the 'Assessment: RRV-2909' interface. The left sidebar contains navigation options: General, Summary, Control Results, Workflow, Findings, Tickets, Responses, Exceptions, Comp Controls, Charts, Logs, Evidence Log (selected), Workflow Log, and Archives. The main content area is divided into two sections: 'Evidence' and 'Evidence Change Log'.

**Evidence Section:**

- 1-1 of 1
- More Actions... dropdown menu is open, showing options: More Actions..., Export All Evidence (highlighted), Save as CSV, and Customize.
- Filter by: Show all - Refresh
- Table columns: Description, Owner, Documents, Controls.
- Table content:
 

Description	Owner	Documents	Controls
wsr	Document Repository	Linked from Document Repository	1. Survey - RRV-2909, question - RRV-2909_Subcontrol

**Evidence Change Log Section:**

- Results as of 2019-07-24 11:26:38
- 1-37 of 37 Show 50 rows
- Buttons: Save as CSV, Customize
- Filter by: Show all - Refresh
- Table columns: Change, Who, When
- Table content:
 

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

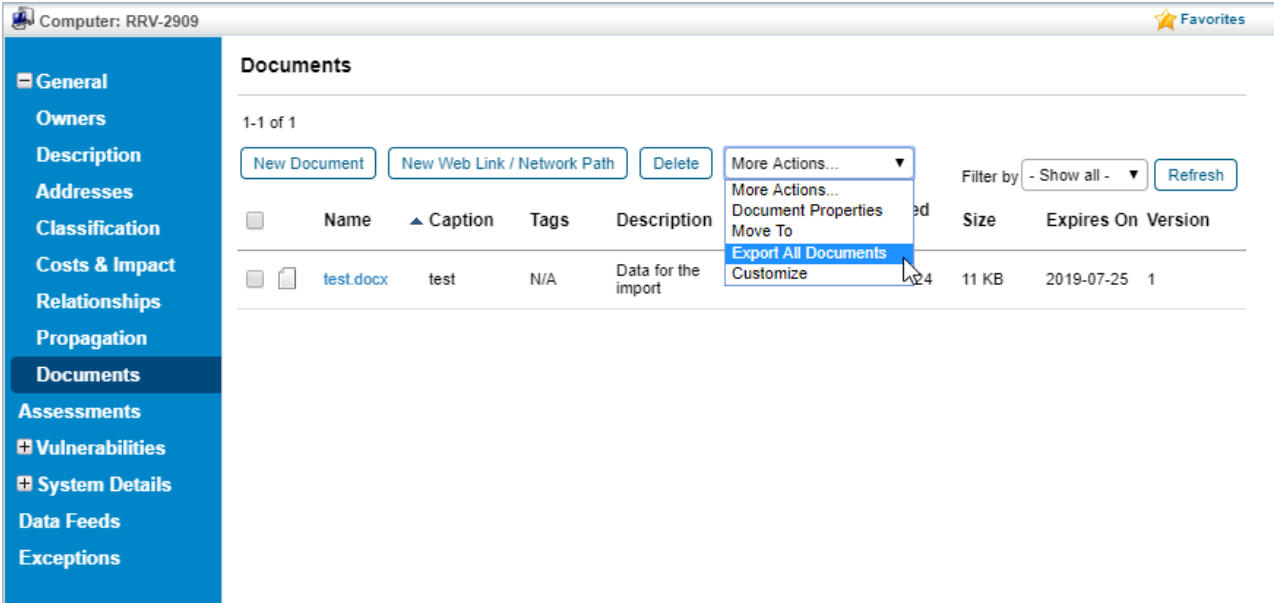
*The Evidence Log tab on the Assessment Details page.*

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.



The screenshot displays the 'Documents' tab for the object 'Computer: RRV-2909'. The left sidebar contains a navigation menu with options: General, Owners, Description, Addresses, Classification, Costs & Impact, Relationships, Propagation, Documents (selected), Assessments, Vulnerabilities, System Details, Data Feeds, and Exceptions. The main content area shows a table of documents. The table has columns for Name, Caption, Tags, Description, Size, Expires On, and Version. A single document is listed: 'test.docx' with a caption of 'test', tags of 'N/A', and a description of 'Data for the import'. The size is 11 KB, the expiration date is 2019-07-25, and the version is 1. Above the table, there are buttons for 'New Document', 'New Web Link / Network Path', and 'Delete'. A 'More Actions...' dropdown menu is open, showing options: 'More Actions...', 'Document Properties', 'Move To', 'Export All Documents' (highlighted), and 'Customize'. There are also 'Filter by - Show all -' and 'Refresh' buttons.

*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.

*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

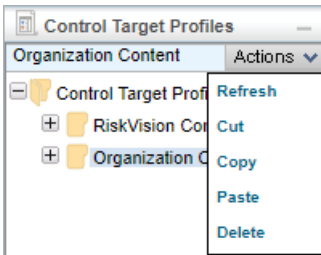
1. Search results are filtered using an AND condition between the fields
2. Depending on the Source selected internal users or LDAP users, the use of the wildcard character is different:
  - For Internal Users, the search field supports a single word in which the wildcard of "\*" can be used before and/or 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



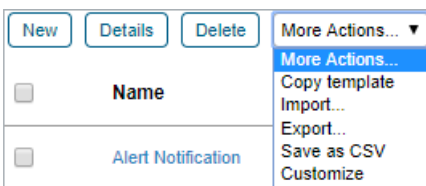
- Note: If you are not making a wildcard search, your search terms will be exact match terms for each of the terms you are using.

## 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 the [Batch 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:

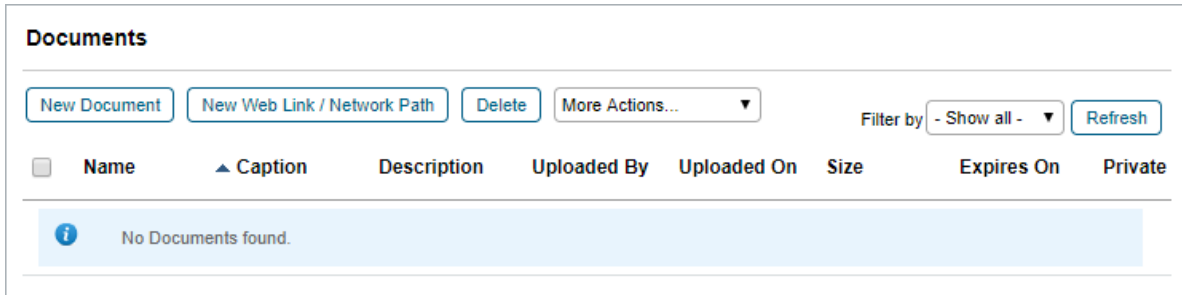
1. Open the page of interest in which the More Actions drop-down list containing the **Import** option is available.
2. Select **Import** in the More Actions drop-down list. An import dialog sensitive to the object type appears. For example, if you are importing an email template, the **Import Email 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.

## 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.

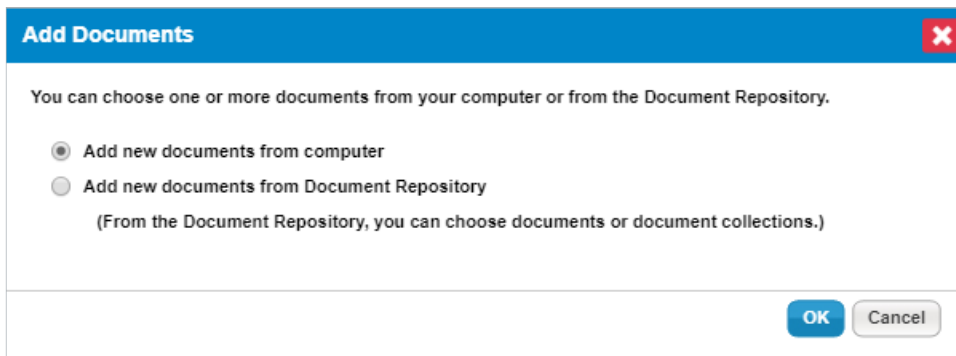


*The Documents window.*

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.

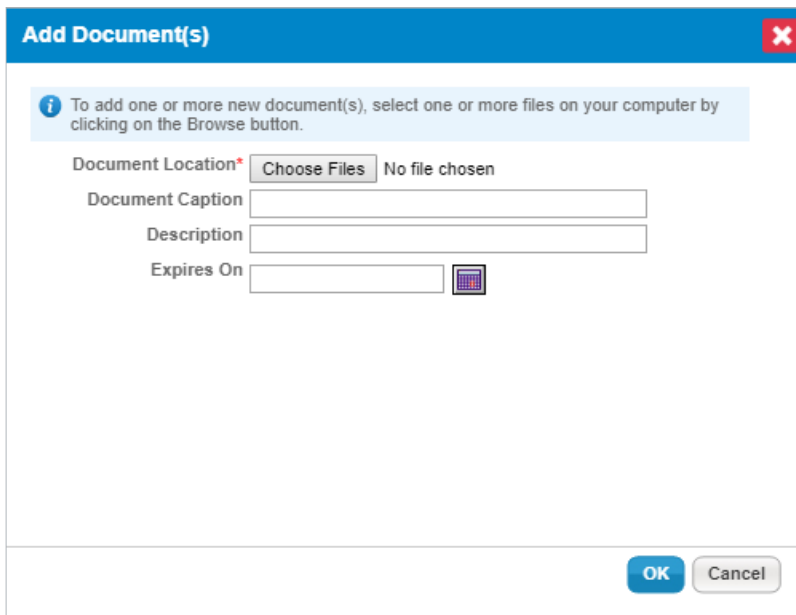
## To attach a document:

1. Select an object to open its details page, then click the **Documents** tab.
2. Click **New Document**. Select one of the following options:



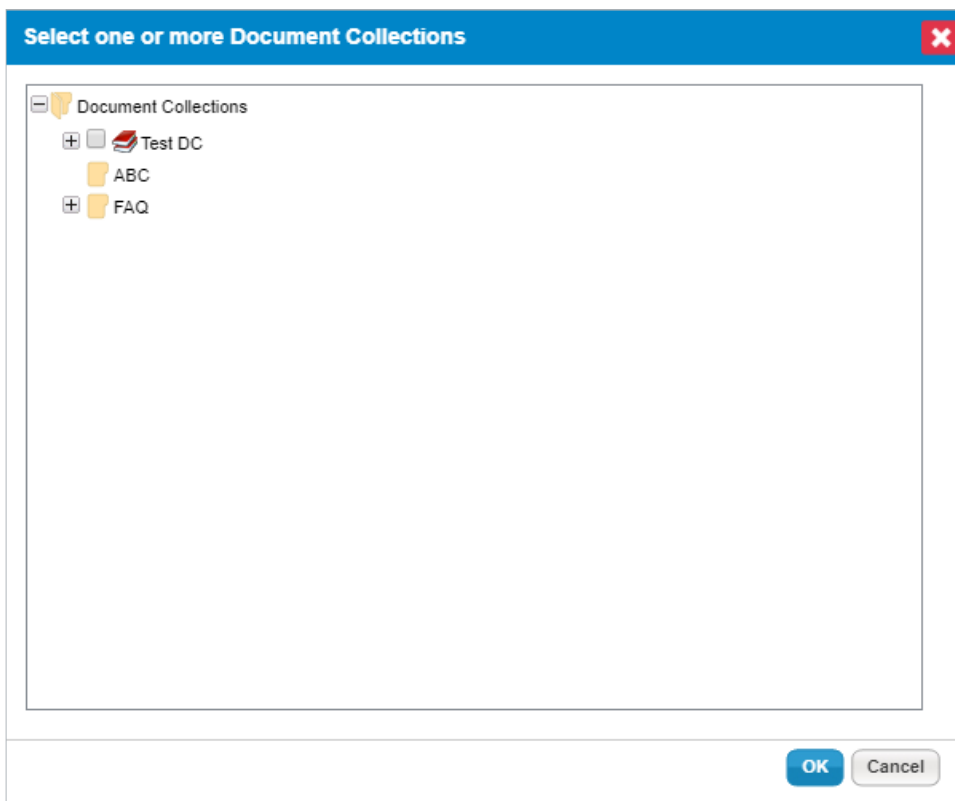
*The Add Documents window.*

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



*The Add new documents from computer window.*

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



*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\*

Link Caption

Description

Expires On

**OK** **Cancel**

*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.


## About the Welcome Page

Each RiskVision application has a **Welcome** page that can be customized for each individual user and their specific roles. The components of this page change based on the selected application.

When you log in, a summary of items assigned to you, such as questionnaires, tickets, exceptions, and notifications, will be displayed. Clicking on any of these items on the **Welcome** page opens a navigation pane with details specific to your selection.

## Message Center

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

 <b>Message Center</b>	
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
<a href="#">Go to the message center</a>	

*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](#).










## Quick Links Overview

Quicklinks is a component of the [Welcome page](#) that provides a categorized set of links to other pages in the RiskVision system. The set of links change depending on the selected application and your role.

### Quicklinks

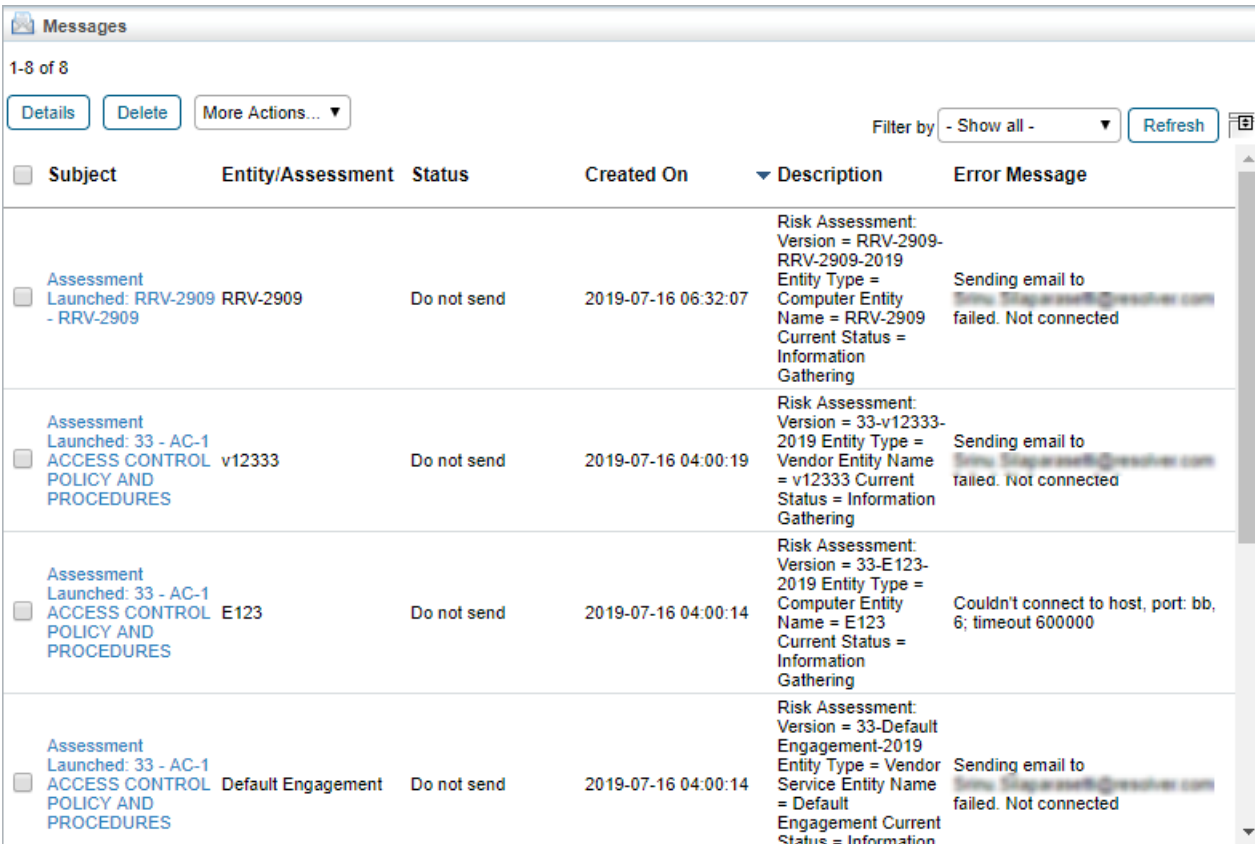
- Entities** [Entities](#) | [Entity Collections](#) | [Group Definitions](#) | [Entity Management](#)
- Assessments** [Assessments](#) | [Programs](#) | [Notifications and Alerts](#) | [Data Feeds](#)
- Content** [Controls and Questionnaires](#) | [Control Target Profiles](#) | [Risks](#) | [Document Repository](#)
- Analytics** [R6 Dashboards and Reports](#) | [R6 Charts](#) | [R6 Report Templates](#) | [R6 Report Status](#) | [R7 Analytics \(Early Release\)](#)
- Configuration** [Workflows](#) | [Questionnaire Presentation Options](#) | [Email Templates](#) | [Escalation](#) | [Ticket Management Preferences](#) | [Filters](#) | [Ownership Types](#) | [Assessment Configuration](#) | [Entity Configuration](#) | [Findings Configuration](#)

### Quicklinks

 1209 unread Messages	 499 Tickets	 12 Assessments	 177 Questionnaires	 94 Entities	 2 Risk Responses	 1 Risks
---	--	---	---	---	---	--

## 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.



The screenshot shows the Message Center interface with a table of messages. The table has the following columns: Subject, Entity/Assessment, Status, Created On, Description, and Error Message. There are four rows of messages, each with a checkbox in the Subject column. The interface includes a 'Messages' header, '1-8 of 8' count, and buttons for 'Details', 'Delete', and 'More Actions...'. A 'Filter by' dropdown is set to '- Show all -' and a 'Refresh' button is present.

<input type="checkbox"/>	Subject	Entity/Assessment	Status	Created On	Description	Error Message
<input type="checkbox"/>	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]@reseller.com failed. Not connected
<input type="checkbox"/>	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]@reseller.com failed. Not connected
<input type="checkbox"/>	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
<input type="checkbox"/>	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]@reseller.com 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 the Tickets Page

The **Tickets** page displays a grid of all tickets in which you are a stakeholder. If you own the responsibility of managing the tickets in your organization, you can view all the tickets regardless of ownership. Depending on your user permissions, you can use the **Tickets** page to perform the following tasks:

- [Create a new ticket](#)
- Open a ticket to view the details and perform the following tasks:
  - [Update the general information](#);
  - [Transition the workflow](#);
  - Add comments;
  - Manage attachments;
  - [Link or detach entities and vulnerabilities](#); and
  - 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 your active and closed tickets. Tickets can be segregated by the groups By Status, Stage, Type, and My Tickets Delegated To Others. For example, you can click the **Review** group under the Tickets tree to work on the tickets that have 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.

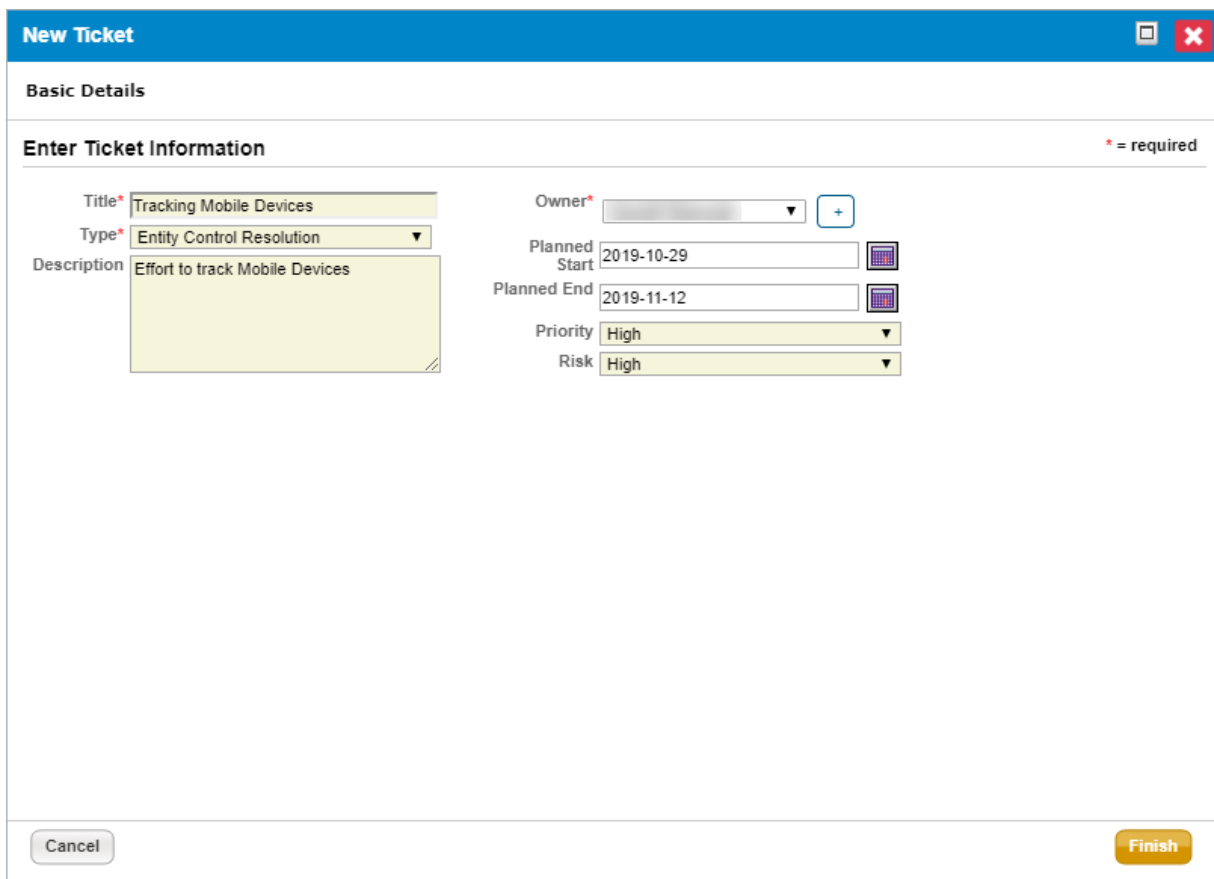
## Creating a New Ticket

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.



The screenshot shows a window titled "New Ticket" with a blue header bar. Below the header is a section labeled "Basic Details". Underneath is a form titled "Enter Ticket Information" with a legend indicating that an asterisk (\*) denotes required fields. The form contains the following fields:

- Title\***: Text input field containing "Tracking Mobile Devices".
- Type\***: Dropdown menu showing "Entity Control Resolution".
- Description**: Text area containing "Effort to track Mobile Devices".
- Owner\***: Dropdown menu with a "+" button next to it.
- Planned Start**: Date input field containing "2019-10-29" with a calendar icon.
- Planned End**: Date input field containing "2019-11-12" with a calendar icon.
- Priority**: Dropdown menu showing "High".
- Risk**: Dropdown menu showing "High".

At the bottom of the window, there are two buttons: "Cancel" on the left and "Finish" on the right.

*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.

The screenshot shows the 'Tickets' interface. On the left is a tree view with folders: 'My Tickets', 'My Undelegated Tickets', 'My Tickets Delegated To Other', 'By Status' (containing 'Open Tickets' and 'Closed Tickets'), 'By Stage' (containing 'New'), 'By Type', and 'All Tickets'. The 'All Tickets' folder is selected. On the right is a grid titled 'All Tickets' showing 1-4 of 4 tickets. The grid has columns for 'Ticket ID', 'Title', 'Status', and 'Type'. Each row has a checkbox in the left margin.

<input type="checkbox"/>	Ticket ID	Title	Status	Type
<input type="checkbox"/>	TKT00003	T4	New	Entity Control Resolution
<input type="checkbox"/>	TKT00002	T3	New	Entity Control Resolution
<input type="checkbox"/>	TKT00001	T2	New	Entity Control Resolution
<input type="checkbox"/>	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
<input type="checkbox"/> TKT00003	T4	New	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:46:21	2019-07-04
<input checked="" type="checkbox"/> TKT00002	T3	New	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:46:09	2019-07-04
<input checked="" type="checkbox"/> TKT00001	T2	New	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:45:59	2019-07-04
<input type="checkbox"/> TKT00000	T1	New	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> 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.

- 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
<input type="checkbox"/> TKT00003	T4	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:46:21	2019-07-04
<input checked="" type="checkbox"/> TKT00002	T3	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:46:09	2019-07-04
<input checked="" type="checkbox"/> TKT00001	T2	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:45:59	2019-07-04
<input type="checkbox"/> TKT00000	T1	Entity Control Resolution	Prakash ch	Prakash ch	N/A	<input type="checkbox"/> N/A	0%	2019-07-04 01:45:45	2019-07-04

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

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

**Editing Multiple Tickets: 2 Tickets** Edit

**General**

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 N/A

Custom String 4 E123

Owner Prakash ch

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

**Comments**

No comments have been entered.

*The Editing Multiple Tickets window.*

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

Editing Multiple Tickets: 2 Tickets Save Cancel

General

**General**

<p>Description <input style="width: 100%; height: 40px;" type="text"/></p> <p>Type <span style="border: 1px solid #ccc; padding: 2px;">Select a ticket type</span></p> <p>Status New</p> <p>Export Status Not exported to external system</p> <p>Category <input style="width: 100%;" type="text"/></p> <p>Disposition <span style="border: 1px solid #ccc; padding: 2px;">-- Select --</span></p> <p>Progress <input style="width: 100%; height: 15px;" type="range" value="25"/> 25</p> <p>Submitted By N/A</p> <p>Custom String 10 <input style="width: 100%;" type="text"/></p> <p>Custom String 4 <span style="border: 1px solid #ccc; padding: 2px;">E123</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">+</span>  <span style="border: 1px solid #ccc; padding: 2px 5px;">-</span></p>	<p>Owner <span style="border: 1px solid #ccc; padding: 2px;">Select a user</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">+</span></p> <p>Start <span style="border: 1px solid #ccc; padding: 2px;">2019-07-24</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">📅</span></p> <p>Expiration date <span style="border: 1px solid #ccc; padding: 2px;">2019-07-31</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">📅</span></p> <p>Planned Start <input style="width: 100%;" type="text"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">📅</span></p> <p>Planned End <input style="width: 100%;" type="text"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">📅</span></p> <p>Exception Expiration Date <input style="width: 100%;" type="text"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">📅</span></p> <p>Priority <span style="border: 1px solid #ccc; padding: 2px;">Medium</span></p> <p>Risk <span style="border: 1px solid #ccc; padding: 2px;">Low</span></p> <p>Ticket Age N/A</p>
---	---

**Comments**

Applied a medium priority and low risk

View 0

i No comments have been entered.

*Editing the fields of multiple tickets.*

## About the 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 you perform in this grid depend on the permissions assigned to your role. You can use the **Exception Requests** page to perform one or more of the following tasks:

- [Create a global exception](#);
- Update the [general](#) information;
- Transition the workflow;
- View workflow history;
- Enter additional comments;
- [Manage attachments](#);
- Synchronize the changes made to the workflow of an exception; and
- Delete an exception.

Exception ID	Exception Name	Global	Entity Names	Exception Type	Object Name	Risk	Current Stage	Status	Status Modified By	Requestor	Awaiting Action By	Start	End	In Stage Since
EXP00726	applied	✓	5432_H	Vulnerability	VULN-225	N/A	Closed	Cancelled				2020-06-29	N/A	2020-06-29
EXP00221	vulin2	✓	N/A	Vulnerability	VULN-62, VULN-67	N/A	Review	Review	N/A			2020-04-15	N/A	2020-06-17
EXP00236	exceptionvulcve1	✓	N/A	Vulnerability	VULN-96	N/A	Review	Review	N/A			2020-04-16	N/A	2020-06-17

*The Exception Request page.*

Local exceptions can be created in the **Questionnaire** window or the **Control Results** tab of the **Assessment Details** page. For more information, see the [Questionnaire Responder's Guide](#).



## 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	<ul style="list-style-type: none"> <li>Analytics and Reporting</li> <li>R6 Dashboards and Reports</li> <li>R6 Charts</li> <li>R6 Report Templates</li> <li>R6 Report Status</li> </ul>	<ul style="list-style-type: none"> <li>Analytics and Reporting</li> </ul>
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	<ul style="list-style-type: none"> <li>To create R6 Charts, enable <code>allowNewReport=true</code></li> <li>To create R6 Dashboards and Reports, enable <code>allowNewDashboard=true</code></li> </ul>	<ul style="list-style-type: none"> <li>To create R6 table-type charts with custom queries, enable <code>allowNewReport=true</code></li> </ul>
Viewing R6 Charts, Dashboards, and Reports	Users can access R6 Dashboards and Reports, R6 Report Templates, and R6 Report Status.	<ul style="list-style-type: none"> <li>To view archived R6 Charts, enable <code>showArchivedReports=true</code></li> <li>To view archived R6 Dashboards and Reports, enable <code>showDashboardPage=true</code></li> </ul>
<b>New Group and Export Group</b> Actions	Users can select <b>New Group</b> and <b>Export Group</b> under <b>My Charts</b> and <b>My Dashboards</b> .	Users cannot execute <b>New Group</b> or <b>Export Group</b> .

Home	Entities	Assessments	Content	Analytics	Configuration
Analytics and Reporting	R6 Dashboards and Reports	R6 Charts	R6 Report Templates	R6 Report Status	

*The Analytics tab with an R6 License.*

Home	Entities	Assessments	Content	Analytics	Configuration
Analytics and Reporting	R6 Charts				

*The Analytics tab without an R6 License.*

## Understanding Configurations

Any assessments you run in RiskVision involve objects from on the **Configuration** menu. Objects may need to be configured differently for each assessment, depending on your business needs. The following objects must be configured before launching an assessment:

- Workflows;
- Escalations;
- Email Templates;
- Filters;
- Ownership Types;
- Assessment Configuration;
- Entity Configuration;
- Findings Configuration;
- Vulnerability Risk Configuration;
- Incident Configuration;
- Questionnaire Presentation Options; and
- Ticket Management Preferences.

The following describes how to configure some of the above options:

- **Workflows:** You can choose a workflow other than the default workflow using the assessment and policy creation wizards. If you want an exception, ticket, finding, and incident to follow a workflow pattern other than the default workflow, 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:** Sent to the requestor, owner, or manager when a ticket is overdue. For more information, see [Creating an Escalation Configuration](#) and [Managing Escalation Configurations](#).
- **Email Templates:** Used to notify stakeholders about an event. Several default email templates are available. If your organization prefers to follow a particular procedure for its internal communications, you can design an email template. For more information, see [Configuring E-mail Templates](#).
- **Filters:** A set of conditions used by reports to match records, and by dynamic groups to limit membership, user access, and more. Filter types include Assessment, Dynamic Group, Entity, Exception Request, Incident, Program, Response, Risk, and others. 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 approvals 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](#).
- **Assessment Configuration, Entity Configuration, Findings Configuration, Vulnerability Risk Configuration, and Incident Configuration:** Depending on the RiskVision application, a common threshold range criteria can be established for assessments, findings, vulnerabilities, risks 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:** Configure your preferences for sending ticket escalations. For more information on setting the ticket preferences, see [About Ticket Management Preferences](#).

## Threat Management Preferences

The **Threat Management Preferences** page is where you control email alert notifications of new vulnerabilities and other features of the **Threat and Vulnerability Manager**. You can choose the recipients and email templates for threat management alerts. Alerts are optionally sent after each vulnerability scan and when updates are received from vulnerability feeds. Tickets can be automatically created for newly updated vulnerabilities. **Threat Management Preferences** is also where you manage groupings and dynamic groups of entities (entities) based on their shared properties. You can set the **Threat Management Preferences** only if you have the Threats and Vulnerabilities View and Manage permissions.

PREFERENCE		DESCRIPTION
Send notification when a vulnerability matches my environment	To Recipients	Select a team of users to receive alerts by email.
	Using Email Template	Choose <b>No Email</b> , or select an alert template (such as Threats Advisory Alerts).
	Vulnerabilities from Scanners	Include vulnerabilities from scanners in email notifications.
	Vulnerabilities from Feeds	Include vulnerabilities from feeds in email notifications.
When a vulnerability is assigned to a user, send notification using:	Email Template	Choose <b>No Email</b> , or select an alert template (such as Threats Advisory Alerts).
When vulnerabilities are updated:	Automatically create tickets	Check the box to automatically create tickets
	Create tickets only if no patch is available for the affected entity	Check the box to create a ticket if a patch is unavailable for the affected entity.
	CVSS Score >=	Create a ticket when vulnerabilities have a CVSS score greater or equal to a specified value.
	Acknowledge the vulnerability when tickets are automatically created	Check the box to automatically acknowledge vulnerabilities when tickets are created.
	and assign the vulnerability to	Select a user the vulnerability will be assigned to.
Ticket default due dates based on vulnerability risk level	High	Default: 10 days after today
	Medium	Default: 30 days after today
	Low	Default: 90 days after today
Ticket Reminders	Send reminder to owners	Check to send a reminder to ticket owners.
	After	Specify the percentage of ticket timespan to have elapsed before sending reminder. Default is 50%.
	Using Email Template	Choose <b>No Email</b> , or select an alert template (such as Threats Advisory Alerts).
Send a notification to the vulnerability owner when all its tickets are closed	For Vulnerability severity level	Choose <b>All, High-only, Medium and High</b> , or <b>None</b> .

Using E-mail Template

Choose **No Email**, or select an alert template (such as Threats Advisory Alerts).

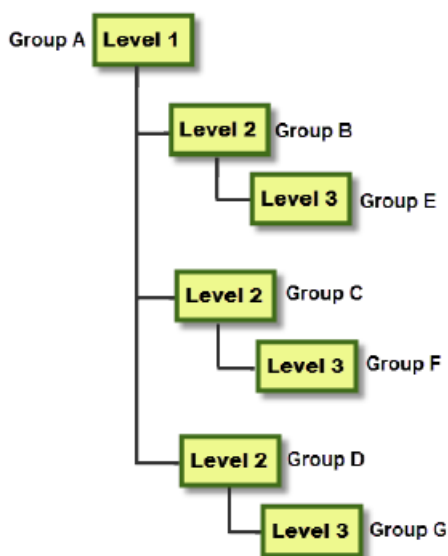
## Entity Groupings

The **Groupings** tab on the **Threat and Vulnerability Preferences** page lets you view entities affected by a vulnerability, grouped by attributes. Entities can be grouped by:

- App Vendor;
- App OS;
- App Version;
- Entity Type;
- Entity Subtype;
- Criticality;
- Custom String 1-25;
- Hierarchy Level 1-15;
- Owner;
- OS Name;
- OS Vendor;
- OS Version.

This allows you to analyze a vulnerability from different many different perspectives to check the effect of a vulnerability.

You can combine different attributes or select one or more hierarchy levels to create a grouping. Creating a grouping using one or more hierarchy levels requires an understanding of the groupings behavior for each hierarchy level.



*The organization hierarchy levels.*

- Selecting entities to group by organizational hierarchy level displays the affected entities in that level and below that level. For example, if you select Level 1, the affected entities will be grouped by Group A, Group B, Group C, Group D, Group E, Group F, and Group G.
- Selecting entities grouped by levels that are adjacent to each other will display the affected entities in separate groups for each path. For example, if you select hierarchy Level 1 to Level 3, the affected entities are displayed in the following groups: Group A, Group B, and Group E; Group A, Group C, and Group F; Group A, Group D, and Group G.
- Selecting entities grouped by levels that are not adjacent to each other will display the affected entities in the lowest hierarchical level group. For example, if you select Level 1 and Level 3, the affected entities are displayed in the following groups: Group E, Group F, and Group G.
- Affected entities belonging to one or more groups appear multiple times, one for each subgroup to which it belongs.
- Rebuild Grouping Cache: Allows you to rebuilds all entity groups from the beginning.
- Update Grouping Cache: Allows you to update all entity groups from the last timestamp.



## Create a Grouping

You can create a grouping using any attribute combination you want. For example, you can create a grouping using the Entity Type and Owner.



If a user who is using a version of RiskVision below 9.0 upgrades to version 9.0 or higher, their custom groupings will be deleted and will need to be recreated.

### To create a grouping:

1. In the RiskVision Threat and Vulnerability Manager application, go to **Configuration > Threat Management Preferences**. The **Threat Management Preferences** page is displayed by default.
2. Click the **Groupings** tab. The **Grouping of Entities** grid is displayed.

Name	Description
Criticality	Template using entity criticality for grouping.
Default	Default using OS title/vendor/version with entity owner and criticality.
EHOCOC	Testing the custom grouping
EPCAT	N/A
Test	N/A

*The Grouping of Entities grid.*

3. Click **New**. The **New Grouping** dialog appears.

**Name:**

**Description:**

**Attributes**

- Entity Type
- Entity Subtype
- Hierarchy Level1
- Hierarchy Level2
- Hierarchy Level3
- Hierarchy Level4
- Hierarchy Level5
- Hierarchy Level6
- Hierarchy Level7
- Hierarchy Level8
- Hierarchy Level9
- Hierarchy Level10

**Selected Attributes**

**OK** **Cancel**

*The New Grouping dialog.*

4. Enter the **Name** and **Description**.

- In the **Attributes** box, select the attribute(s) of interest, and click the arrow pointing right. The attribute(s) appears in the **Selected Attributes** box. Use the arrows pointing up and down to change the sequence of the selected attributes.
- Click **OK**.
- Click the **Rebuild Grouping Cache** button. This will reset all groups and create tables for newly created groups.

The screenshot shows the 'Configuration' section of the RiskVision interface, specifically the 'Grouping of Entities' page. The navigation bar includes 'Home', 'Entities', 'Vulnerabilities', 'Threats', 'Technologies', 'Content', 'Analytics', and 'Configuration'. Under 'Configuration', there are sub-tabs for 'Threat Management Preferences', 'Workflows', 'Email Templates', 'Escalation', 'Ticket Management Preferences', 'Filters', 'Ownership Types', 'Entity Configuration', and 'Vulnerability Risk Configuration'. The 'Grouping of Entities' page has a left sidebar with 'General', 'Groupings', and 'Vulnerability Status'. The main content area shows a table of grouping templates with columns for 'Name' and 'Description'. The 'Rebuild Grouping Cache' button is highlighted with a green box. The table contains the following data:

Name	Description
Criticality	Template using entity criticality for grouping.
Default	Default using OS title/vendor/version with entity owner and criticality.
EHOCCO	Testing the custom grouping
EPCAT	N/A
Test	N/A

*The Rebuild Grouping Cache*



After creating a new custom group, its data will not appear in a vulnerability **Affected Entities** tab if the user is running RiskVision version 9.0 or higher. **TW reports** need to be created first.



## Vulnerability Status Configuration Options

To configure vulnerability status in the Threat & Vulnerability Manager, go to **Configuration > Threat Management Preferences** and click the **Vulnerability Status** tab.

PARAMETER	DESCRIPTION
Vulnerability Status Dispositions	Manage the list of dispositions. To add a disposition, click <b>Add</b> , then enter the name, then click <b>OK</b> . To update, click <b>Edit</b> on the desired row. To delete, click <b>Delete</b> on the desired row.
Resolved status is set to	Choose a disposition.
Acknowledged status is set to	Choose a disposition.
Auto Resolver Vulnerabilities based on Installed Fixes	Yes or no.

## 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 default workflows. The type of workflow that you see on the **Configuration > Workflows** menu depends on which RiskVision application you're using.

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.

## Modify 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 synchronization 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.

## 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.

## 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
<code>workflow.min.transitions=</code>	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.
<code>workflow.max.transitions=</code>	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.



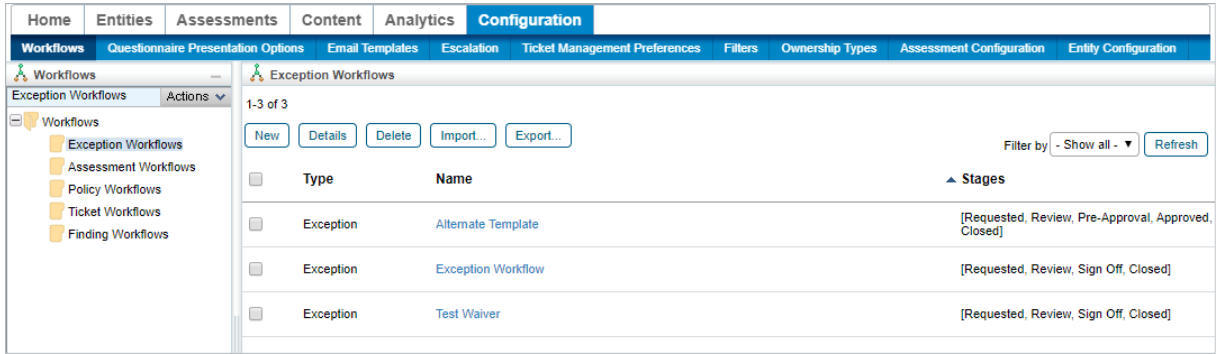
Only users with **Workflow View** and **Workflow Update** permissions can modify workflows.



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.

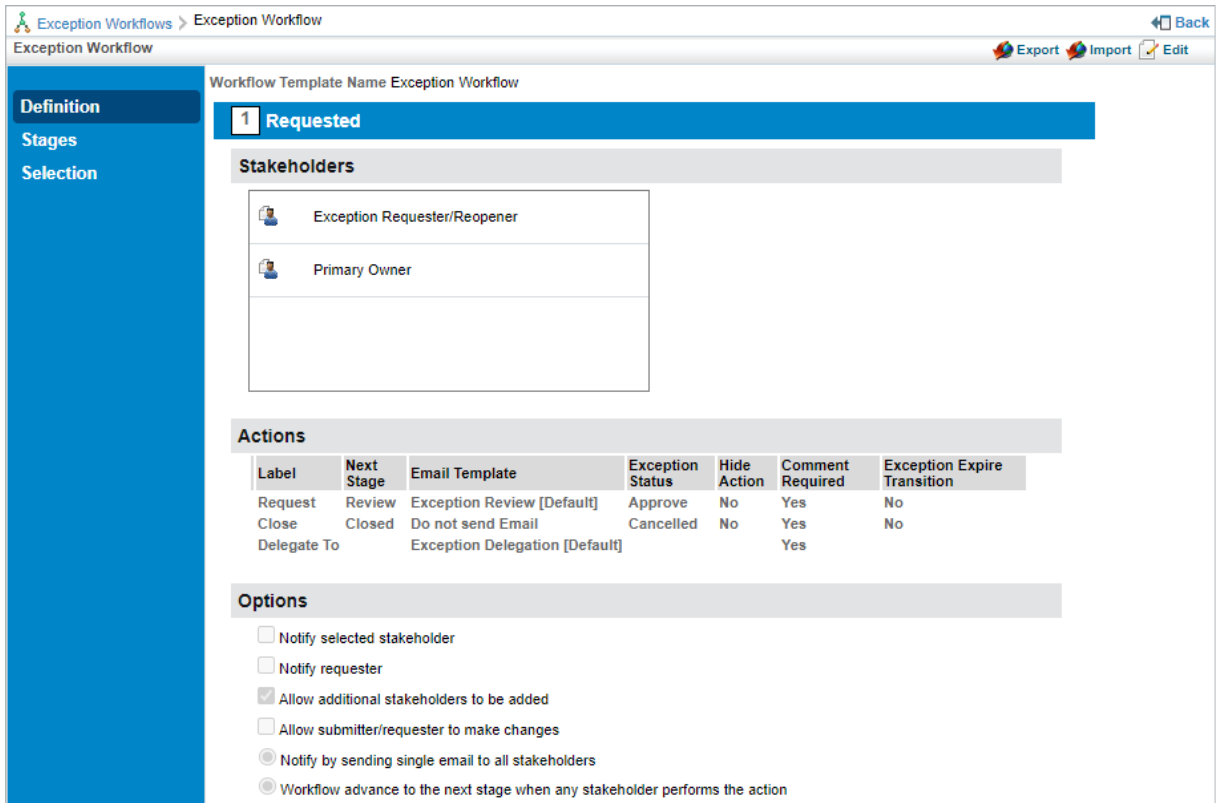
### To configure a workflow's transitions and actions:

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.



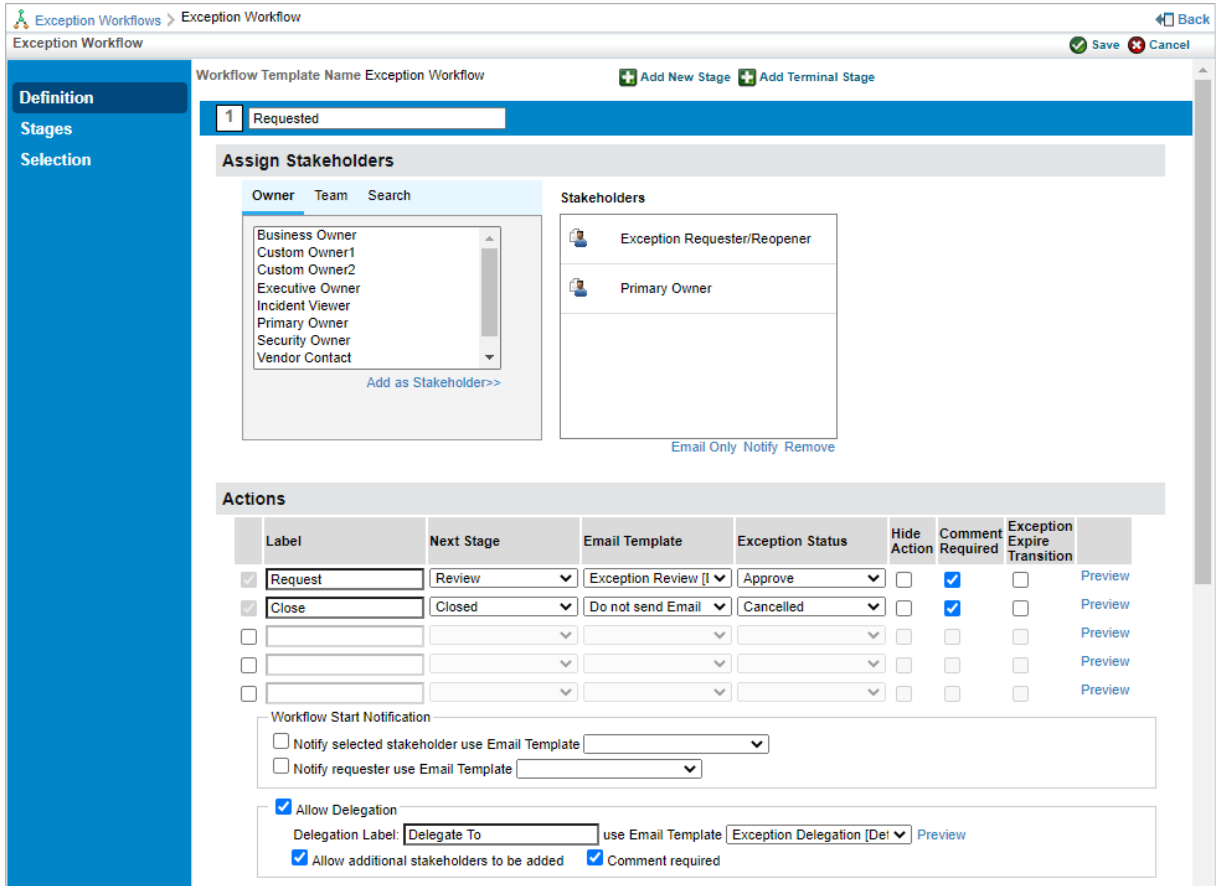
The Workflow settings in Configuration.

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



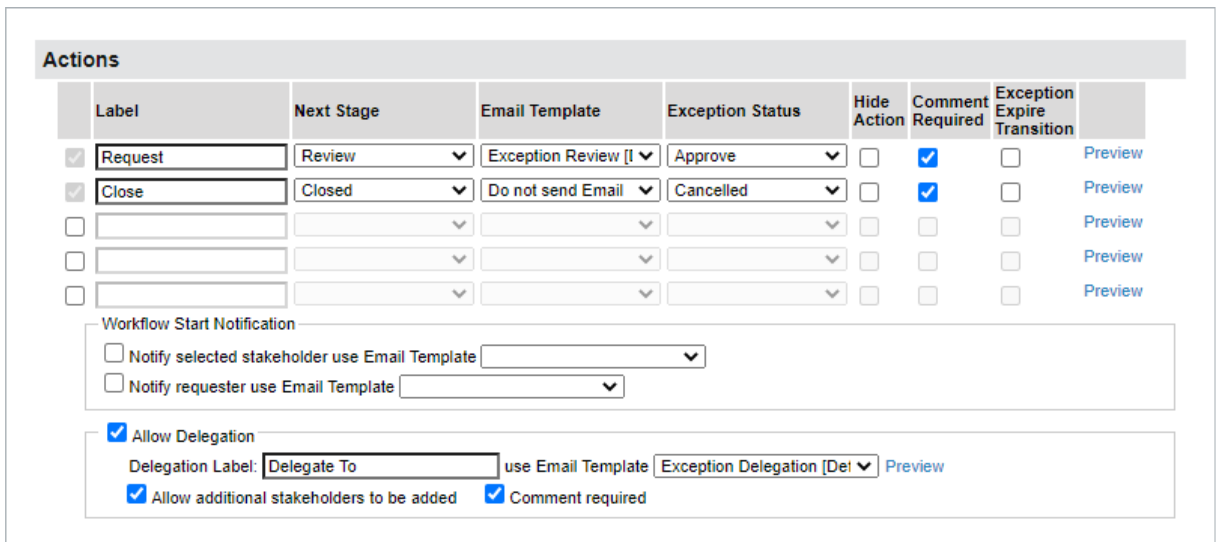
Workflow details.

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



The Workflow edit screen.

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



The Actions settings.

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

- 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.
- 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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Preview
Cancelled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Preview
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Preview
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Preview
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Preview

*The Hide Action and Comment Required checkboxes.*

- Optional:** Click **Preview** if you selected an email template in step 8 above and you wish to preview it.
- Repeat steps 5 to 12 to modify the settings of additional stages as needed.
- 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.



## 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:

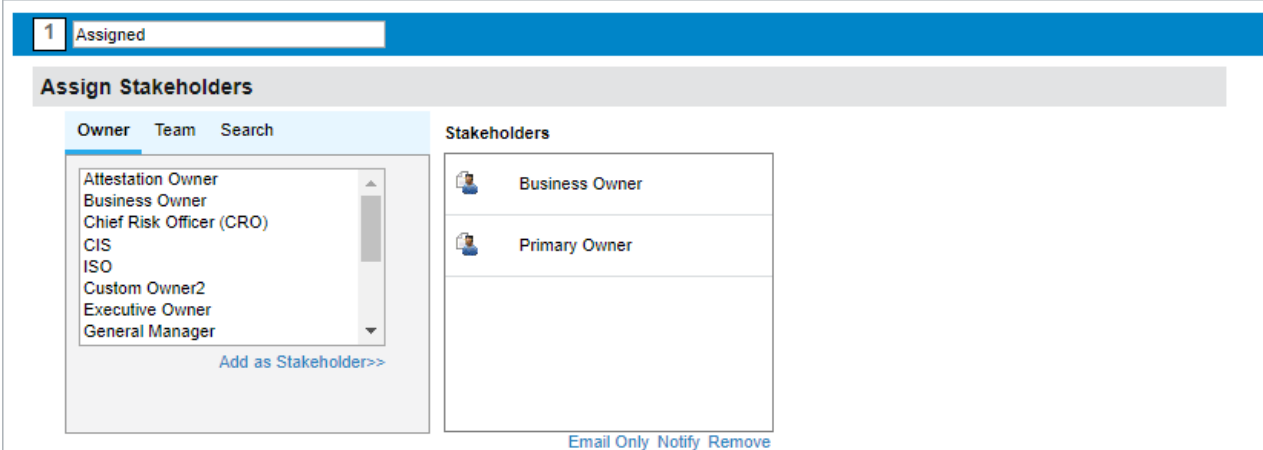
1. Task-performing stakeholders
2. Task-aware stakeholders

**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:

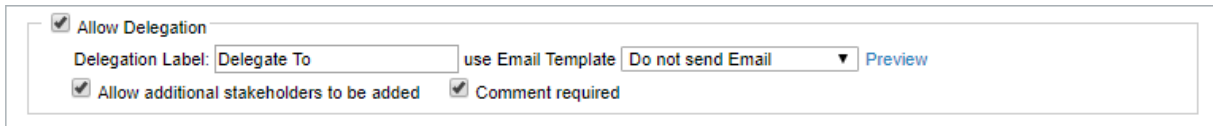
1. Select a workflow.
2. Click **Edit** at the top-right corner of the workflow **Details** page.
3. Select a stage.
4. Under **Assign Stakeholders**, select the stakeholder, and click **Remove**. To remove multiple stakeholders within a stage, press and hold **CTRL** button on your keyboard, click the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



The screenshot shows a configuration panel for 'Allow Delegation'. It includes a checked checkbox for 'Allow Delegation', a text input field for 'Delegation Label' containing 'Delegate To', a 'use Email Template' checkbox, a dropdown menu for 'Do not send Email', a 'Preview' link, and two other checked checkboxes: 'Allow additional stakeholders to be added' and '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
Allows incomplete submission	Allows responders to submit the questionnaire even if all questions have not been answered.
Automatically move assessments to the next stage when all Questionnaires are complete	<p>If checked, the workflow automatically advances to the next stage only when all questionnaires have been completed and the user submits the questionnaire by clicking the <b>Submit</b> link.</p> <p>This option works effectively when an assessment has only one questionnaire. In the case of multiple questionnaires, the workflow stage must have branching capability.</p>
Automatically submit Questionnaires that are answered by automated controls	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.

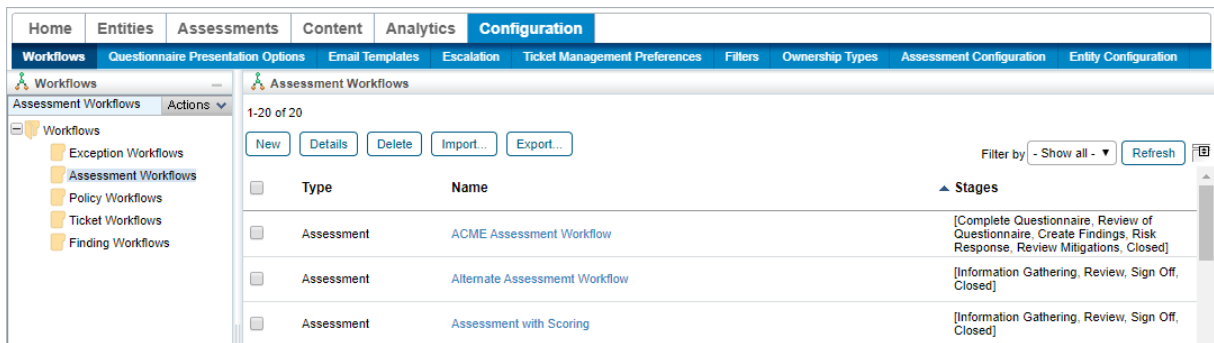
Prevent this page from creating additional dialogs

OK

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

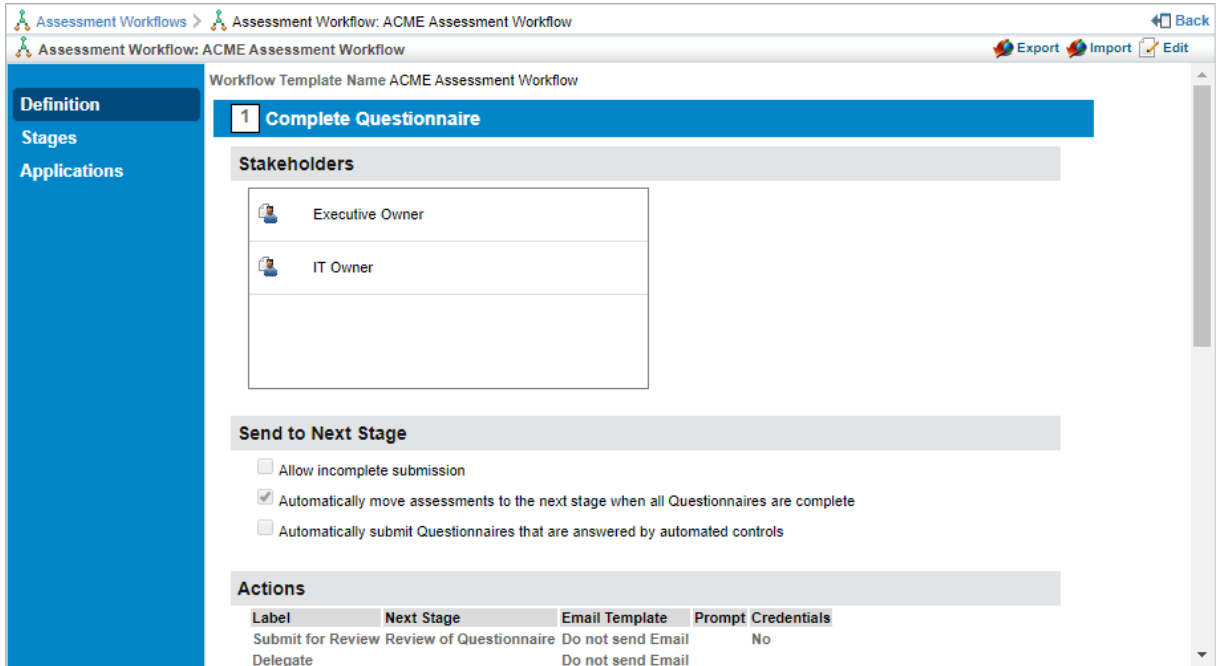
## To delete a workflow stage:

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



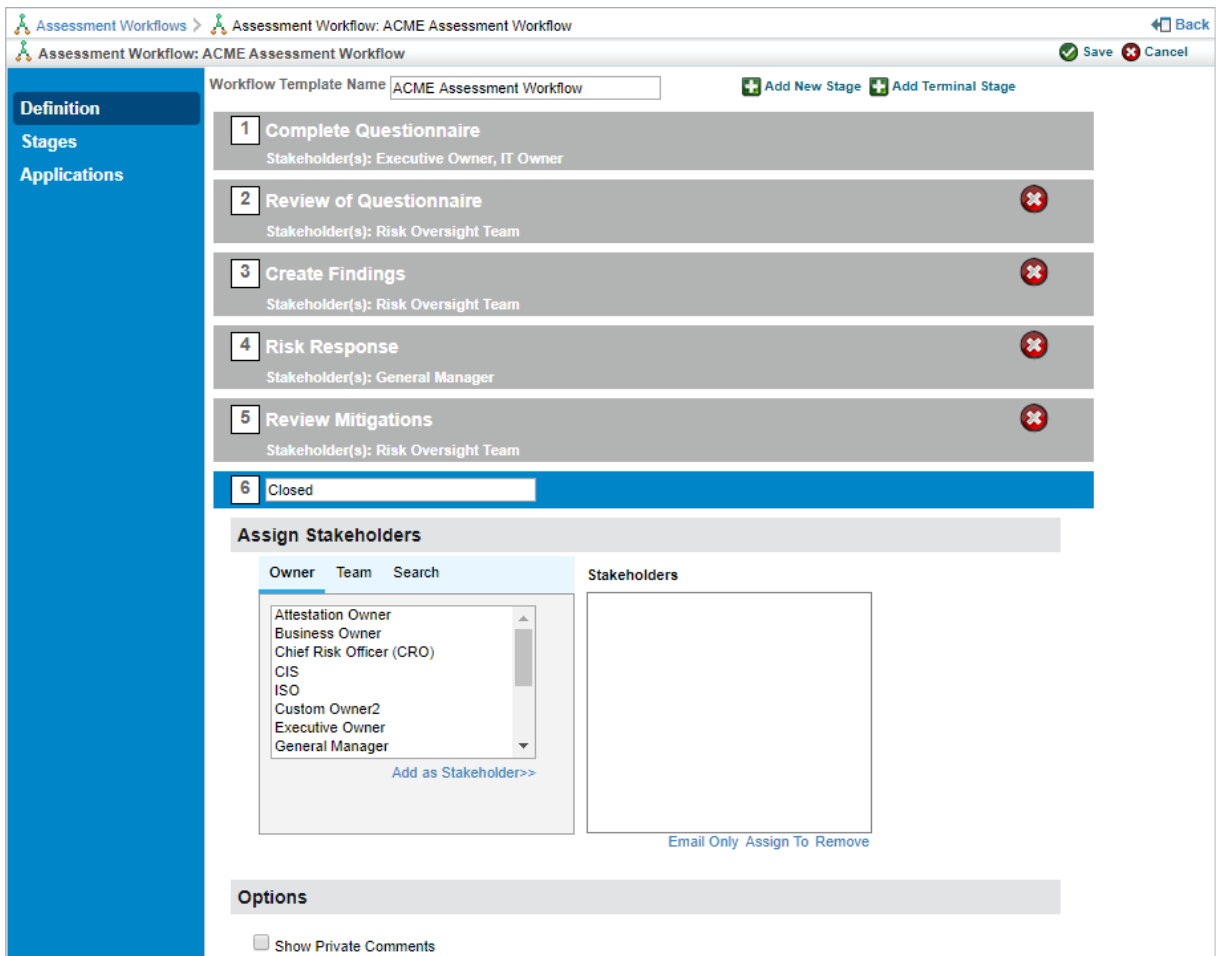
*The Workflow settings in Configuration.*

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.



The Workflow Details page.

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



The workflow edit screen.

- Click the  icon next to any stage to delete it.



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

## Other Stage Options

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

OPTION	WORKFLOW TYPE	Description
Notify selected stakeholder	Ticket, Policy, Finding, and Exception	Notify the stakeholder selected in this stage.
Notify owner	Ticket, Finding, and Exception	Notify object owners regarding the object creation.
Allow submitter/requester to make changes	Ticket and Exception	<p>If checked, the original submitter or requester can change the ticketer exception request.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The workflow option has no bearing on the ticket's owner, who can always make changes to the ticket.</li> <li>• 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.</li> </ul>
Allow additional stakeholders to be added	Ticket and Finding	If checked, allow additional stakeholders to add to the stage.
Allow owner to make changes	Finding	<p>If checked, allow owners to make changes in the findings.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• If a user has the Object Manage permission or is a stakeholder, they will be able to make changes to the object regardless of whether the option is checked.</li> <li>• The workflow option will only be applicable if there are stakeholders mapped.</li> </ul>
Add Option	All	Click to add reminder and escalation options. For more information, see <a href="#">Sending Reminders and Escalations to Stakeholders</a> .
Notify by sending...	All	<p>Notify by sending an email to each stakeholder individually, or by sending a single email to all stakeholders.</p> <p>For example, if a workflow stage has two normal stakeholders and three email stakeholders:</p> <ul style="list-style-type: none"> <li>• <b>Notify by sending email individually to each stakeholder:</b> Two emails are sent to normal stakeholders in the TO list with no one on the CC</li> </ul>

		<p>list and one email is sent to email only stakeholders on the CC list with no one in the TO list.</p> <ul style="list-style-type: none"> <li>• <b>Notify by sending single email to all stakeholders:</b> One email is sent which includes two normal stakeholders in the TO list and three email-only stakeholders in the CC list.</li> </ul>
Allow each questionnaire to advance workflow stages...	Assessment Only	Allow each questionnaire to advance independently, or require that all questionnaires must advance together. Specify "branch" and "join" stages that mark the beginning and ending of independent transition zones in a workflow. For more information, see <a href="#">Allowing Independent Stage Transitions</a> .
Enable preferred user matching	Assessment only	If this option is checked, RiskVision will send questionnaires to preferred users. If a preferred user is not found for a particular entity, a related option specifies whether to send a questionnaire. For information about how to set up the preferred ownership, see <a href="#">Preferred Ownership</a> .
Allow Control test authoring	Assessment only	If checked, respondents can author control tests.
Allow Control test authoring	Assessment only	If checked, respondents can evaluate control tests.
Read Only Stage	Assessment only	Click and select to prevent modification of the entire questionnaire or answers. For more information, see <a href="#">Locking Answers in a Questionnaire</a> .
Notify primary owner when assessment is accessed	Assessment only	If checked, sends the primary owner of the entity or asset an email when the assessment is accessed. For configuration steps, see <a href="#">Notifying Assessment Owner</a> .
Show Private Comments	Assessment only	If checked, show private comments.
Allow all question scoring	Assessment only	If checked, allow all question scoring.
This is Review Stage	Assessment only	Check to indicate that the status of the current stage is in review.
Auto Advance after n days; Action	Assessment only	Advance the assessment workflow automatically using the specified action if it is still in this stage the specified number of days since the start.
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.



## Send Escalations and Reminders to Stakeholders

RiskVision Server allows you to send of escalations and/or reminders to stakeholders when a workflow does not move forward within a specified time. These notifications can be sent from any stage of any type of workflow. In each workflow stage, you can add a combination of up to ten reminder and escalation options. 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 as follows:

WORKFLOW	ESCALATE/REMIND OPTIONS	DATE TYPES
Assessment	Remind Stakeholder, Escalate to program owner, and Escalate to stakeholder's manager	Due date, Recurrence date, Stage start date, and custom dates
Exception	Remind Stakeholder and Escalate to stakeholder's manager	Expiration, Start, Stage start date, and custom dates
Finding	Remind Stakeholder, Escalate to owner, and Escalate to stakeholder's manager	Last modified date, 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
Policy	Remind Stakeholder, Escalate to owner, and Escalate to stakeholder's manager	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

## Send Reminders and Escalations to Task-Aware Stakeholders

By default, the configured reminder and escalation options are sent only to task-performing stakeholders and not to task-aware stakeholders, who receive emails only and cannot transition workflows.

To copy task-aware stakeholders on all reminder and escalation notifications, 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 & 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.

1 Assigned

2 In Progress

3 Review

4 Closed

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.

Accept
Reject
Delegate To
Revoke Delegation

▶ **Comments**

---

▶ **Documents**

---

▶ **Linked To**

---

▼ **Workflow History**

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): <span style="background-color: #d9d9d9; padding: 0 5px;">[redacted]</span>	N/A	No	<span style="background-color: #d9d9d9; padding: 0 5px;">[redacted]</span>	<span style="background-color: #d9d9d9; padding: 0 5px;">[redacted]</span>	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:

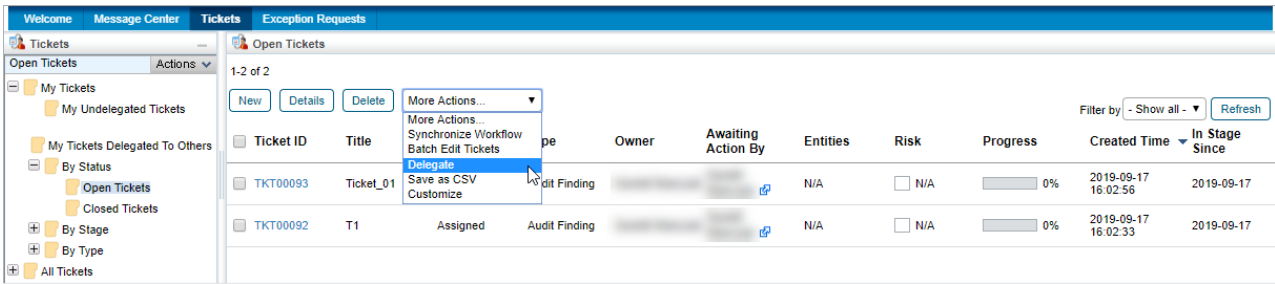


Not all of the below objects will be available in each application.

- 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.

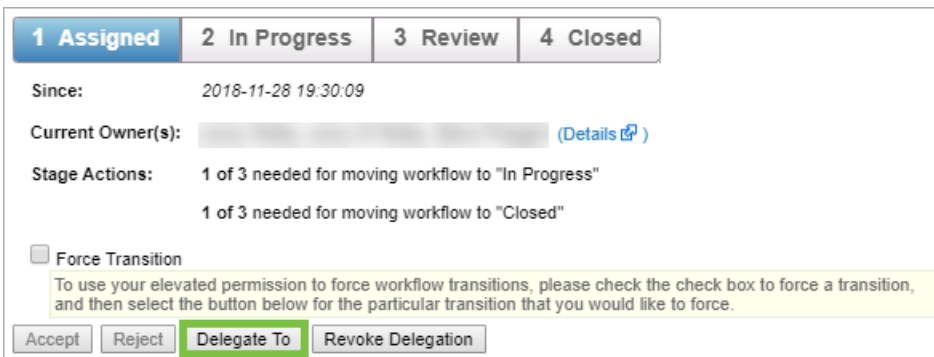
For **Tickets**, **Findings**, **Incidents**, and **Exception Requests**, stakeholders can perform bulk delegation and delegation revocation from the **More Actions** dropdown list.



The Delegate option in the More Actions dropdown.

## Delegation

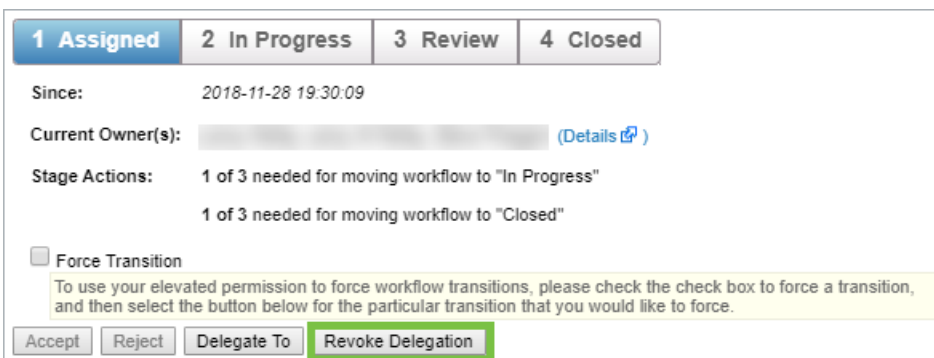
Any stakeholder of a stage that permits delegation can delegate to another user. The workflow designer can allow team Delegation at each stage. For example, the **In Progress** and **Review** stages may allow for delegation, whereas the **Approval** stage might be designed not to allow delegation. The 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.



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.



The Revoke Delegation button.



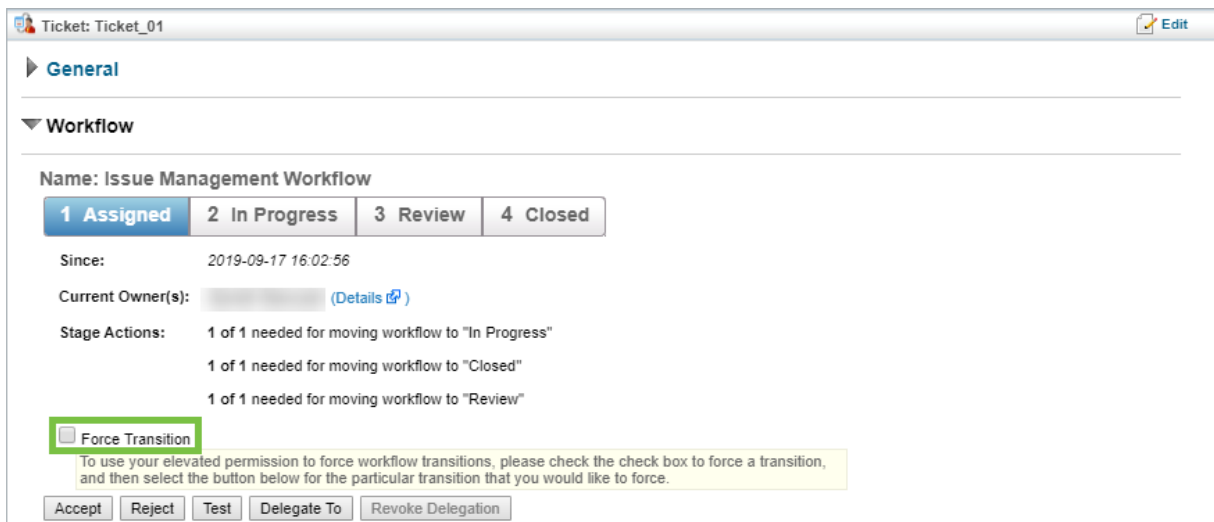
## Force a Stage Transition

Any user with appropriate permissions can force the stage transition of a workflow for objects such as tickets, exceptions, or incidents, when the stage stakeholder fails to transition the workflow to the next stage in time. To force the stage transition in a policy workflow, the user must be a primary owner of the policy. This can allow you to move the workflow stage forward, even if all stage requirements have not been met. 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

### To force a stage transition:

1. Select the object to open its details page.
2. In the **Workflow** section, click the **Force Transition** checkbox and click the desired action to complete the transition.



The screenshot shows a web interface for a ticket titled "Ticket: Ticket\_01". The "Workflow" section is expanded, showing a workflow named "Issue Management Workflow" with four stages: "1 Assigned", "2 In Progress", "3 Review", and "4 Closed". Below the stages, there are details for "Since" (2019-09-17 16:02:56), "Current Owner(s)", and "Stage Actions". A checkbox labeled "Force Transition" is highlighted with a green box. Below the checkbox, a yellow tooltip reads: "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." At the bottom of the workflow section, there are buttons for "Accept", "Reject", "Test", "Delegate To", and "Revoke Delegation".

*The Force Transition checkbox.*

## 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.

▼ Workflow History							
1-1 of 1							
Date	▼ Stage	Action	To Stage	Force Transition	User	Target User	Comment
2019-09-17 16:02:56	N/A	Start Workflow	Assigned	No		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						
<input type="button" value="Add Option"/>						
Remind Stakeh ▼	2	days	after ▼	Stage start date ▼	Email Template: Default Ticket Assig ▼	Preview ✕
Escalate to ownr ▼	7	days	after ▼	Stage start date ▼	Email Template: ▼	Preview ✕
Escalate to stake ▼	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 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**.

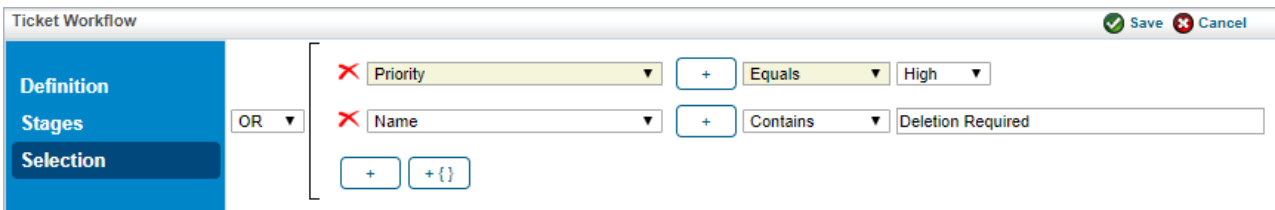
## Specify Multiple Workflows

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.



The screenshot shows the 'Ticket Workflow' configuration window. On the left, there is a sidebar with three tabs: 'Definition', 'Stages', and 'Selection'. The 'Selection' tab is selected and highlighted in blue. To the right of the sidebar, there is a list of selection conditions. The first condition is 'Priority Equals High' and the second is 'Name Contains Deletion Required'. Each condition has a red 'X' icon to its left, indicating it can be removed. There are also buttons for adding (+) and removing (X) conditions, and a plus sign button with curly braces (+ {}).

*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.

## Define 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**  $\neq$  **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.

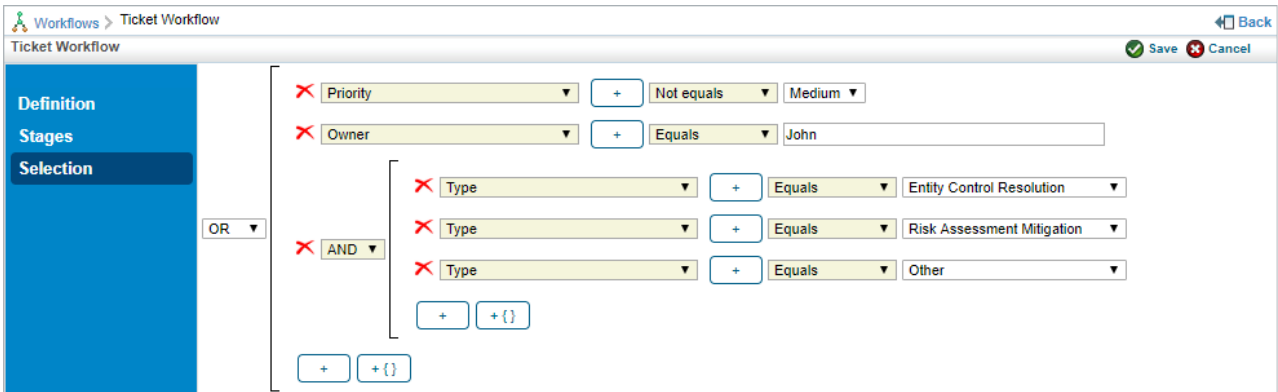
The screenshot shows the 'Selection' tab of the 'Ticket Workflow' editor. On the left, a blue sidebar contains 'Definition', 'Stages', and 'Selection'. The main area shows three conditions: 'Priority' (Not equals Medium), 'Owner' (Equals John), and 'Type' (Equals Audit Finding). A dropdown menu is set to 'OR'. There are 'Save' and 'Cancel' buttons at the top right, and '+' and '+ {}' buttons at the bottom left.

*The Selection Criterion editor.*

## Specify Sub-Conditions

### EXAMPLE

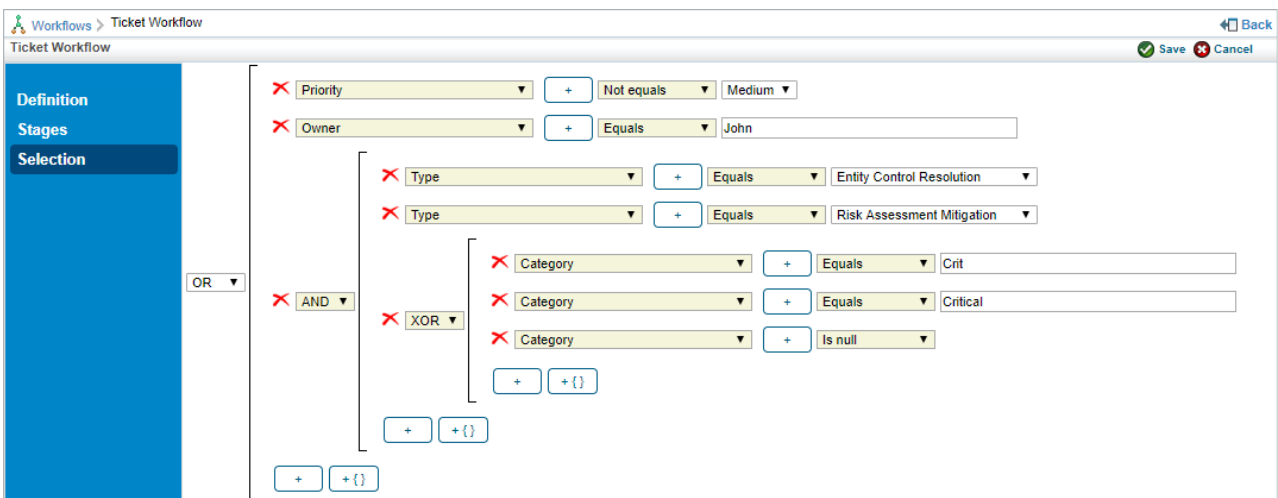
You want to select this workflow when **Priority** > **Medium**, when **Owner** is **John**, or when **Type** is **Entity Control Resolution**, **Risk Assessment Mitigation**, or **Other**. To specify the last three sub-conditions, you use the + { } button.



The screenshot shows the 'Selection Criterion editor' for a 'Ticket Workflow'. The interface includes a sidebar with 'Definition', 'Stages', and 'Selection' tabs. The main area displays a logical expression for selection criteria. The expression is: **Priority** Not equals **Medium** OR **Owner** Equals **John** OR **AND** ( **Type** Equals **Entity Control Resolution** OR **Type** Equals **Risk Assessment Mitigation** OR **Type** Equals **Other** ). The 'AND' operator is used to group the three 'Type' conditions, and the 'OR' operator is used to group the 'Priority', 'Owner', and the 'AND' group.

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.



The screenshot shows the 'Selection Criterion editor' for a 'Ticket Workflow'. The interface includes a sidebar with 'Definition', 'Stages', and 'Selection' tabs. The main area displays a logical expression for selection criteria. The expression is: **Priority** Not equals **Medium** AND **Owner** Equals **John** AND **AND** ( **Type** AND ( **Type** AND ( **Category** Equals **Crit** OR **Category** Equals **Critical** ) XOR **Category** Is null ). The 'AND' operator is used to group the 'Priority', 'Owner', and the inner 'AND' group. The inner 'AND' group contains 'Type' AND ( 'Type' AND ( 'Category' Equals 'Crit' OR 'Category' Equals 'Critical' ) XOR 'Category' Is null ).

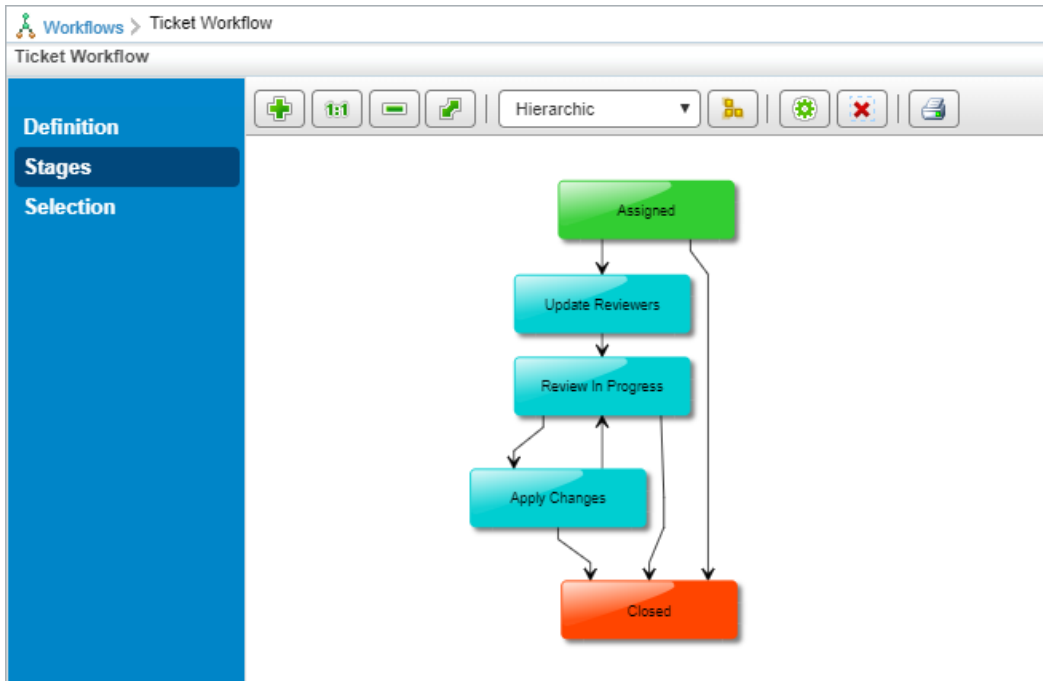
The Selection Criterion editor with two layers of sub-conditions.

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.

## Visualize 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.

Workflows > Ticket Workflow Back

Ticket Workflow

Definition

Stages

Selection

Hierarchic

```

graph TD
    Assigned[Assigned] --> UpdateReviewers[Update Reviewers]
    UpdateReviewers --> ReviewInProgress[Review In Progress]
    ReviewInProgress --> ApplyChanges[Apply Changes]
    ApplyChanges --> Closed[Closed]
    UpdateReviewers --> Closed
    ReviewInProgress --> Closed
  
```

Stage

Name: Apply Changes

Action	Next Stage
Changes Complete	Review In Progress
Reject	Closed

Overview

*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, see [Moving the Layout](#).



## Escalation Overview

Escalation configurations allow you to control the email notifications that are sent when a Ticket is overdue. Three levels of escalation are supported, each with distinct evaluation criteria, recipients, and email templates.

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

For more information about the email template associated with each level of an escalation, see [About E-mail Templates](#).

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

## Create an Escalation Configuration

[Escalation configurations](#) define what happens when a ticket is overdue. Selected recipients are notified using an email template.

If your escalation will require a custom email template, [create the email template](#) first.

### To create a new escalation configuration:

1. Go to **Configuration > Escalation**.
2. Click **New**.
3. Enter the general settings:
  - **Name:** Type the display name that users will use to identify this escalation configuration
  - **Description:** Type 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, if desired.
5. Enter escalation settings:
  - **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.
  - **Email Template:** Select from the list of available email templates. Click **Preview** to see how the email will look.
  - **Escalation Date:** The number of days after the ticket is due to trigger this message. Level 1 might be triggered 1 day after a ticket's due date; Level 2 a few days later. Level 3, if required, would be triggered later still.
  - **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 email templates to include organization-specific details in messages sent to stakeholders during assessments, ticket resolution, and other processes.

RiskVision 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.
Assessment Launch	Assessment	Notifies users that a new assessment has been launched.
Assessment Launch Status	Assessment	Notifies program owners of assessment launch success or failure.
Assessment Recurrence	Assessment	Notifies program owners that an assessment that is configured for recurrence is about to be restarted.
Assessment Review	Assessment	Sends email when an assessment is sent out for review.
Assessment Review Rejection	Assessment	This template is used when an assessment you sent out for review was rejected.
Assessment Signoff	Assessment	Sends email when an assessment is sent for sign-off.
Assessment Signoff Rejection	Assessment	This template is used when an assessment that you sent out for sign-off was rejected.
Classification Assessment Launch	Assessment	This template is used when a new risk classification assessment has been launched.
Content Pack Delegation	Control	This template is used when a Content Pack is delegated from one user to another user.
Content Pack Deployed	Control	This template is used when a Content Pack is deployed.
Content Pack Escalation	Control	This template is used to alert users that a Control's due date is passed.
Content Pack Reminder	Control	This template is used to remind the user about upcoming due dates.
Content Pack Review	Control	This template is used when a Control is ready for review.
Content Pack Review Rejection	Control	This template is used when a Control is rejected during the review.

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.
ERM Assessment Launch	Assessment	This template is used when a new ERM assessment has been launched.
ERM Risk Opinion Review Request	Risk	This template is used to notify users to request an ERM risk opinion.
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 the 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 the 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 the 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.
Finding Closed	Finding	This template is used when a finding is closed.
Finding Delegation	Finding	This template is used when a finding is delegated from one user to another.
Finding Escalation	Finding	This template is used by the system to notify an assignor that a finding that they have assigned has not been worked on and is nearly past the due date.
Finding Reminder	Finding	This template is used to remind users about upcoming due dates on findings.
Finding Review	Finding	This template is used when a finding is ready for review.
Finding Review Rejection	Finding	This template is used when a finding is rejected during the review.
Finding Update Notification	Finding	This template is used to notify the finding owner when the finding is updated.

New Finding	Finding	This template is used to notify stakeholders when a finding is created.
New Vendor Contact Notification	Vendor	This template is used for notifying a new vendor contact that his/her login account has been created.
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 the 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 the review.
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.
Questionnaire Assignment	Assessment	Used for data gathering to notify users that a questionnaire has been assigned to them.
Questionnaire Change Notification	Assessment	Used to notify assessment stakeholders that the questionnaire has been changed.
Questionnaire Delegation	Assessment	Used to notify a user that another user delegated a questionnaire to them.
Questionnaire Escalation	Assessment	Used to alert users that the questionnaire assigned to them is past the due date.
Questionnaire Reminder	Assessment	Used for reminding users of questionnaire due dates.
Report or Dashboard Delivery	Analytics	This template is used when a report or dashboard is sent to the user.
Response Notification Error	System	An HTML template used to send notification that a user request was not successfully processed.
Response Notification		An HTML template used to send notification that a user request was successfully

Success	System	processed.
Response to Password Reset Request	System	Sent when a user requests their password to be reset.
Risk Assessment Launch	Assessment	This template is used to notify stakeholders that a new risk assessment has been launched.
Risk Identified	Risk	This template is used to notify owners that a new risk is identified.
Scheduled Job Completed Successfully	System	Sends a job success notification.
Scheduled Job Failed	System	Sends a job failure notification.
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 a notification that a ticket was closed.
Ticket Delegation	Ticket	Sends a 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 a notification that a ticket is ready for review.
Ticket Review Rejection	Ticket	Sends a notification that a ticket was rejected during the review.
Vulnerability Assignment Notification	Alert	Used to notify a user that they have become the owner of a vulnerability.

## Configure an Email Template

This section explains how to create, delete, and modify an email 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.

### Available email template types:

- **Access Delegation.** Used when notifying users of assigned access delegations.
- **Assessment.** Available for selection in assessment workflows.
- **Analytics.** Available for selection in the Administration application when a report or dashboard is sent to the user.
- **Control .** Available for selection in the policy workflow.
- **Ticket.** Available for selection in the ticket workflow.
- **Incident.** Available for selection in the incident workflow.
- **Exceptions.** Available for selection in the exception workflow.
- **Finding.** Available for selection in the finding 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.
- **Vendor.** Used to notify primary vendor contact of changes.



## Add A Customized Email Template

Users with sufficient privileges can create new email templates for later use.

### To create an email template:

1. Go to **Configuration > Email Templates**. Or, in **Administration**, 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**: Send notifications without sequencing and/or merging. See also Sequencing and Merging of Email Notifications.
  - **High Priority**: Send notifications with high importance. By default, all escalation email templates are sent with high priority.
  - **Sender Email Account**: Select the email account that will send the notifications. The administrator email account is used by default.
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](#).

## Update an Email Template

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**.

## 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, <code>details.alertRule</code> 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 <code>details.alertRule.name</code> .
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.
exceptionName	The name of the exception (Exception expire template only).
exceptionEndDate	The expiration date of the exception (Exception expire template only). See <a href="#">Modifying a Variable Displaying Date</a> .
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.

## Risk 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.
projectName	The name of the Program associated with this notification.
projectDescription	The description of the Program associated with this notification.
riskNames	The name of the risk associated with the program for which you are sending the notification.
entityName	The name of the entity associated with the risk.
appurl	The URL of the RiskVision application.

## Ticket Email Templates

The following variables are available for this email template:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the <code>setSubject</code> 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. See <a href="#">Modifying a Variable Display Date</a> .
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.



## Vendor Email Templates

The following variables are available for these email templates:

VARIABLE	DESCRIPTION
email	The email object gives the designer access to the setSubject method, which takes a string that can include other variables.
vendorName	Name of the vendor to whom the account details are sent.
userName	Recipient of the email, usually a stakeholder in the current workflow.
userId	Username of the vendor account.
password	Password for the vendor account user.
details	Additional details sent for the vendor account.
senderName	Name of the user who will send this notification.
appurl	RiskVision URL.

In addition to the variables above, you can also use the `$NT.getValue(".- workflowTransitionComment")` variable to notify stakeholders of the workflow stage comments.

## 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("RAPProject").
\$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.

## Modify the Variable Displaying 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)`

## Add Object Fields to Email 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	<code>\$NT.getValue(".customAttributes.")</code>
Number	<code>\$NT.getValue(".customAttributes.")</code>
Boolean	<code>\$NT.getValue(".customAttributes.")</code>
Date	<code>\$NT.getValue(".customAttributes.")</code>

## 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	<code>\$NT.getValue(".customAttributes.")</code>	The date and time in the YYYY-MM-DD HH:MM:SS format by default.
Encrypted string	<code>\$NT.getValue(".customAttributes.")</code>	A string value in encrypted format.
Flag	<code>\$NT.getValue(".customAttributes.")</code>	Boolean values.
Image	<code>\$NT.getValue(".customAttributes.")</code>	An image that can be displayed in the email.
Number	<code>\$NT.getValue(".customAttributes.")</code>	Positive and negative numbers, including zero.
Rational number	<code>\$NT.getValue(".customAttributes.")</code>	Positive and negative integers displayed as fractions.
String	<code>\$NT.getValue(".customAttributes.")</code>	Multiple characters.
Text	<code>\$NT.getValue(".customAttributes.")</code>	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  <b>Do Not Send Email</b> is the default.	Exception requester is the only stakeholder if <b>Notify selected stakeholder</b> is checked.
Ticket Workflow Started	Optional  No pre-defined templates.	If <b>Notify selected stakeholder</b> 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 <code>ticket.exception.expired.notification.template</code> 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 by dynamic groups to limit membership and user access. Filter types include Assessment, Dynamic Group, Entity, Exception Request, Incident, Program, Response, Risk, and others.

The following options are available 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.
- **Conjunction:** Joins operands in truth tables.

## Add a Filter

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

### To create a new filter:

1. Open Threat and Vulnerability Manager.
2. Go to **Configuration > Filters**.
3. Expand the **Filter** groups.
4. Select a group to which a filter will be added.
5. Click **New**.
6. Add a Name and Description.
7. Select the filter type.
8. Click **OK**.

The filter is available for assignment.

## Modify 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:

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**.

## Remove 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. Go to **Configuration > Filters**. Or, in the **Administration** application, go to **Users > Filters**.
2. Expand the **Filters** tree and locate to select the filter.
3. Click **Delete**.

## Group 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**.

The group displays in the list.

## Delete 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. Go to **Configuration > Filters**.
2. Select the group you want to delete. The group will display in the **Filter** list.
3. Click **Delete**.

The group and any subgroups and filters are removed.

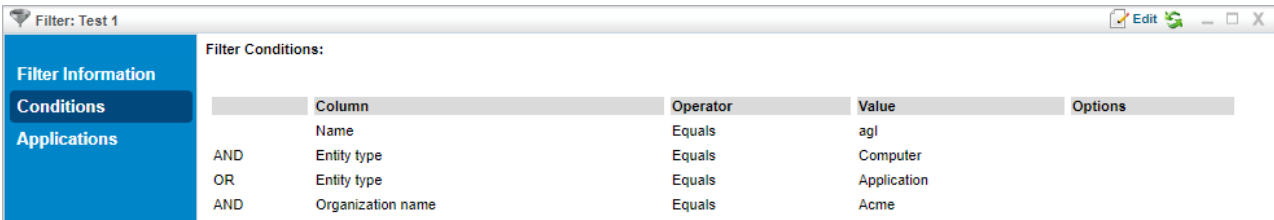
## About Complex Filters

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:



	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:

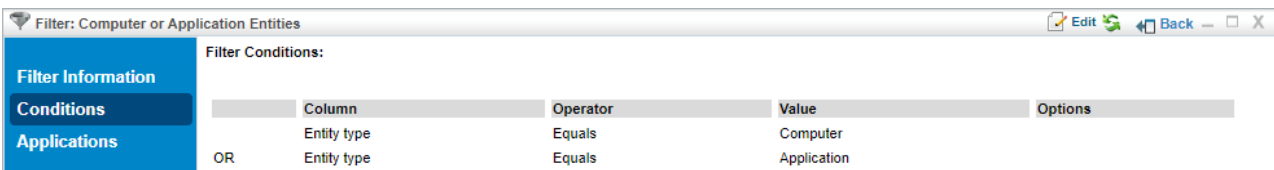
```
(Entity Name starts with agl AND Entity Type = Computer) OR (Entity Type = Application AND Organization name = Acme)
```

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)`.



	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: Test 1

Filter Conditions:

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

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: Test 1

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.

## Configure a Threshold Range for Calculating Vulnerability Scores

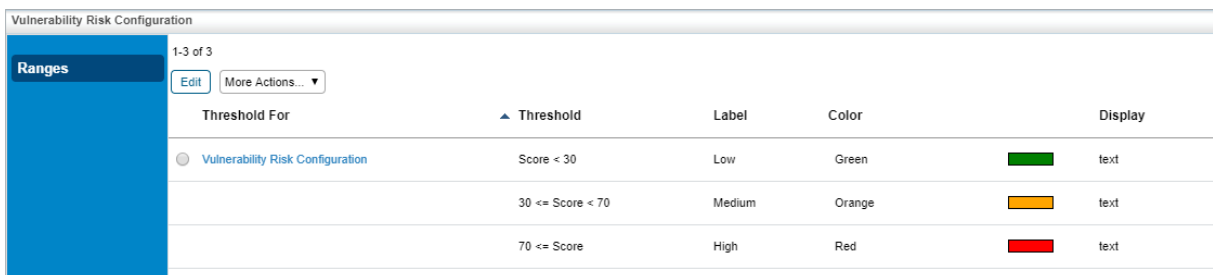
A common threshold range criteria must be established for vulnerability scores related to the vulnerability object. When assessments are run, vulnerability scores are derived according to the threshold range. Before running an assessment, ensure that the threshold range is configured to meet your assessment's auditing guidelines and policies.

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 Vulnerability Risk Configuration:

1. Open the Threat and Vulnerability Manager.
2. Go to **Configuration > Vulnerability Risk Configuration**.

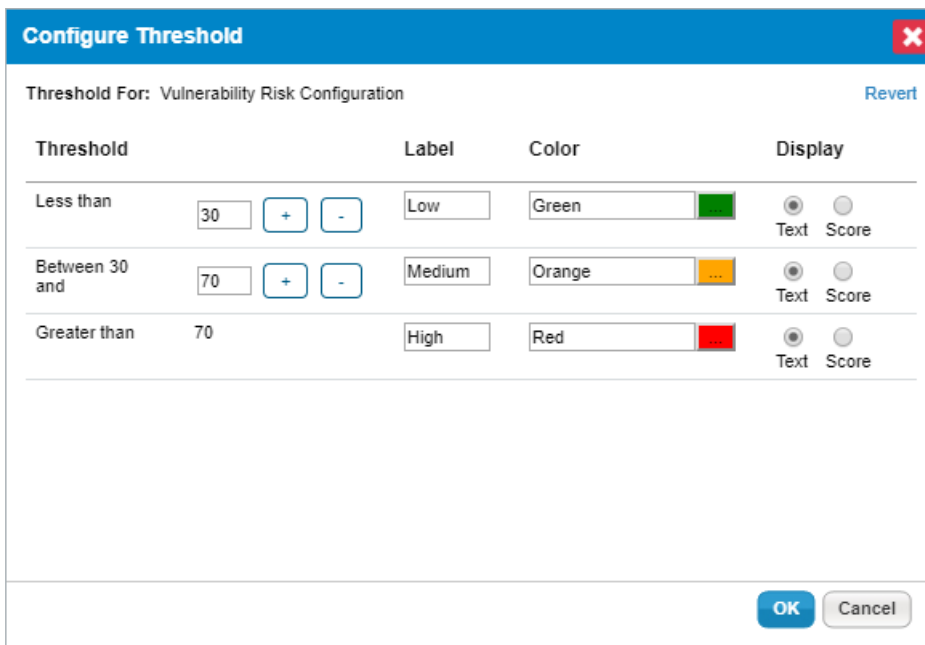


The screenshot shows the 'Vulnerability Risk Configuration' interface. On the left, there is a sidebar with a 'Ranges' section. The main area displays a table with the following columns: 'Threshold For', 'Threshold', 'Label', 'Color', and 'Display'. The table contains three rows of configuration data.

Threshold For	Threshold	Label	Color	Display
Vulnerability Risk Configuration	Score < 30	Low	Green	text
	30 <= Score < 70	Medium	Orange	text
	70 <= Score	High	Red	text

*The Vulnerability Risk Configuration tab.*

3. Select **Vulnerability Risk Configuration** and click **Edit**.



The screenshot shows the 'Configure Threshold' dialog box. It has a title bar with a close button. The main content area is titled 'Threshold For: Vulnerability Risk Configuration' and includes a 'Revert' link. Below this, there are three rows of configuration options, each with a 'Threshold' field, a 'Label' field, a 'Color' field, and a 'Display' field. The 'Threshold' field includes a numeric input and '+'/'-' buttons. The 'Color' field includes a color picker. The 'Display' field has radio buttons for 'Text' and 'Score'.

Threshold	Label	Color	Display
Less than 30	Low	Green	Text (selected)
Between 30 and 70	Medium	Orange	Text (selected)
Greater than 70	High	Red	Text (selected)

*The Configure Threshold 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**.
- Choose the **Text** or **Score** option to display the threshold label or the value for the risk after the assessment is run.

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

## 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 is overdue, it's automatically escalated to additional stakeholders via email notification. 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 a ticket disposition:

1. Go to **Configuration > Ticket Management Preferences**, then click **Edit**.
2. Click **Add**.
3. Enter a new disposition in the **Ticket Dispositions** text box, then click **OK**.
4. Click **Refresh** to update the **Do not escalate when disposition is set to** dropdown list.
5. Click **Save**.

### To change a ticket disposition:

1. Go to **Configuration > Ticket Management Preferences**, then click **Edit**.
2. Select the disposition name.
3. Update the name, then click **OK**.
4. Click **Refresh** to update the **Do not escalate when disposition is set to** dropdown list.
5. Click **Save**.

### To delete a ticket disposition:

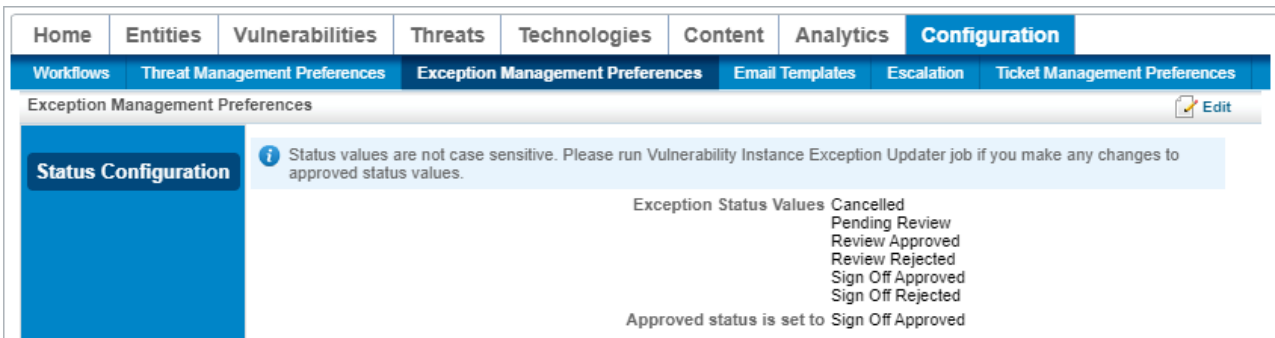
1. Go to **Configuration > Ticket Management Preferences** and then click **Edit**.
2. Select the disposition, click **Delete**, and confirm the action.
3. Click **Refresh** to update the Do not escalate when disposition is set to drop-down list.
4. Click **Save** after you finish modifying a ticket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

## Exception Management Preferences

The **Exception Management Preferences** page is where users with the Exception Manage permission can view all of the workflow statuses an exception can be set to. In addition, users can create new statuses as well as delete ones that have gone obsolete. Users can set new approved statuses on this page as well.



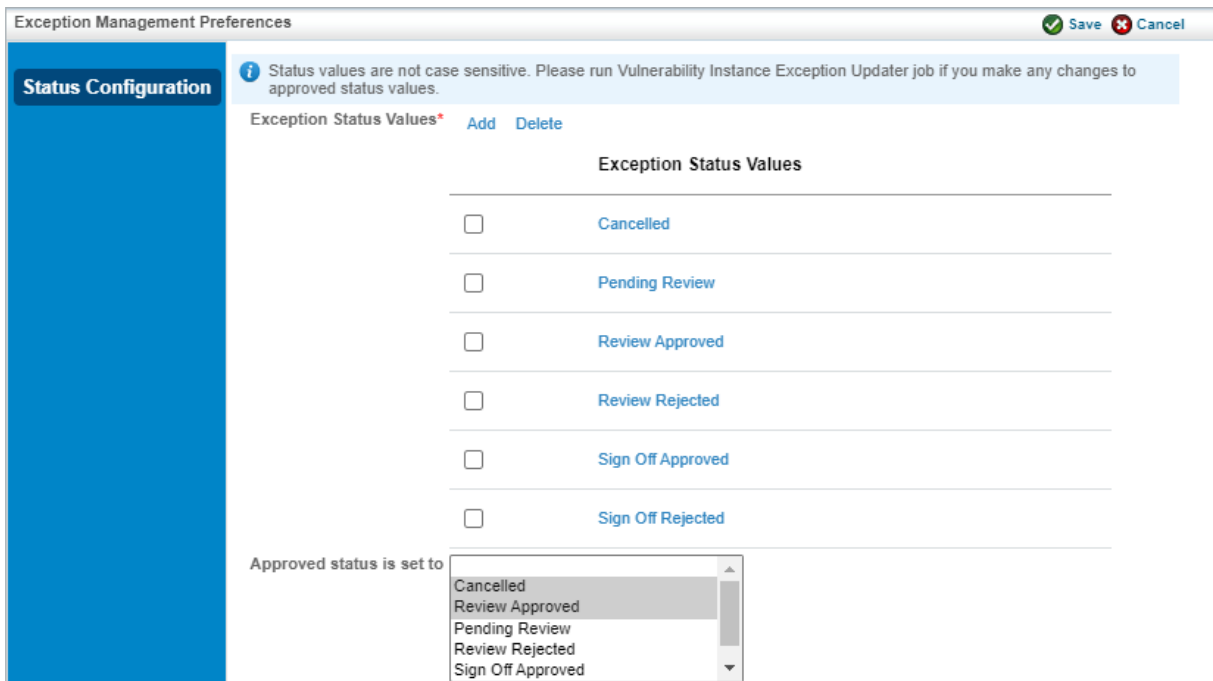
The Exception Management Preferences page.



After upgrading to RiskVision version 9.5 or higher, each RiskVision instance must have at least one approved status mapped before performing any action in Riskvision. New installations at version 9.5 or higher will have a default mapping already provided that can be changed if desired.

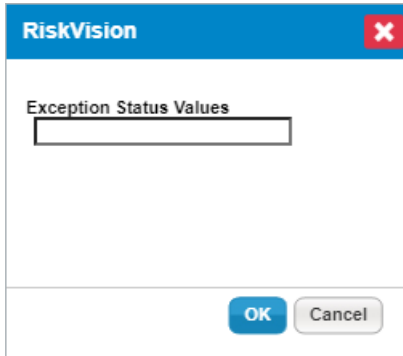
### To add a new exception status value:

1. In any RiskVision application, navigate to **Configuration > Exception Management Preferences**.
2. Click **Edit** to open the **Edit Exception Management Preferences** page.



The Edit Exception Management Preferences page.

3. Click **Add** to open the **Add Exception Status Values** dialogue.

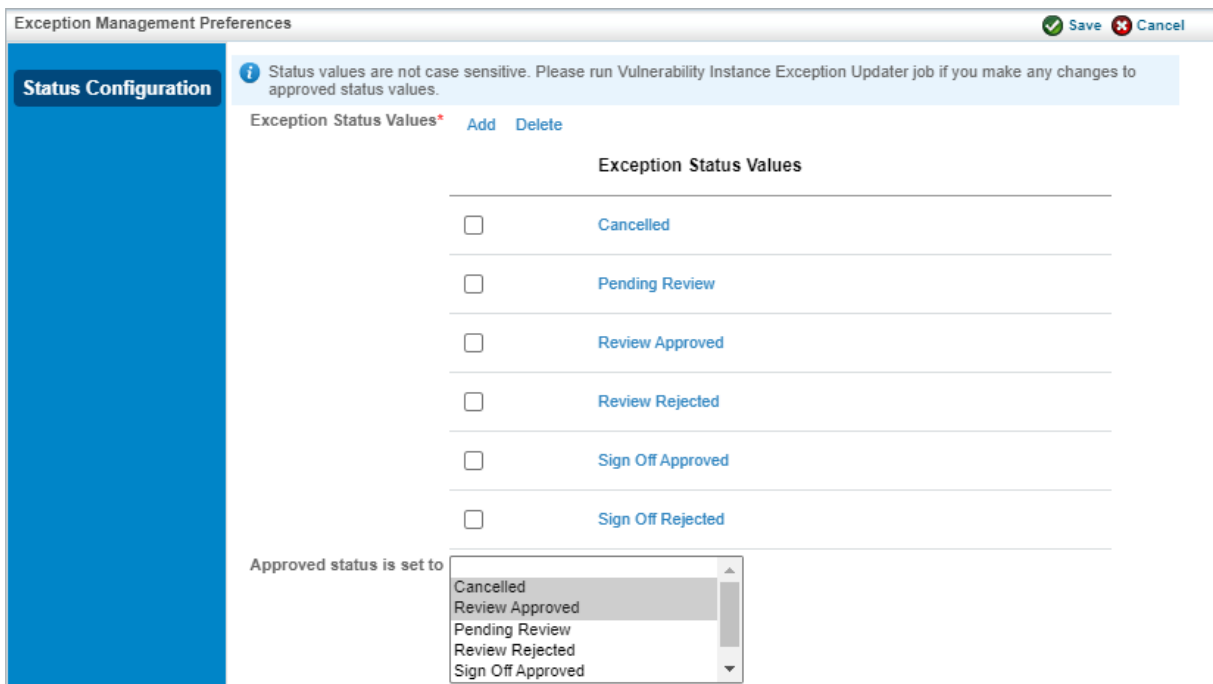


The Add Exception Status Values dialogue.

4. Type the name of the new status value and click **OK**.
5. Repeat steps 3 and 4 as many times as required and click **Save**.

## To delete exception status values:

1. In any RiskVision application, navigate to **Configuration > Exception Management Preferences**.
2. Click **Edit** to open the **Edit Exception Management Preferences** page.



The Edit Exception Management Preferences page.

3. Select each exception status value to be deleted and click **Delete**.

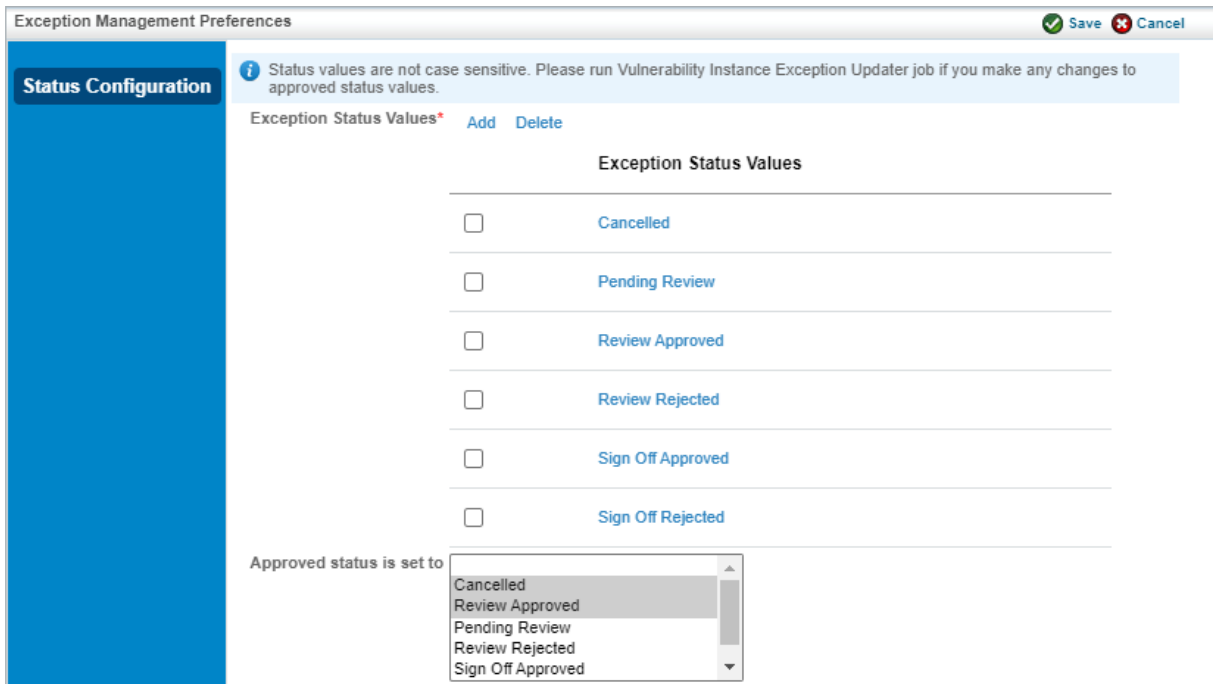


Users cannot delete an exception status value that is being used in the current or previous statuses of a workflow (whether or not it is being used by an exception), or that is selected in the **Approved status is set to** field. Those statuses must first be deleted from their respective workflows. If the workflow in question is being used by an exception, it must be deleted from it first.

4. Click **Save**.

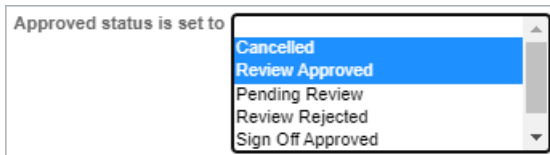
## To set a new approved status:

1. In any RiskVision application, navigate to **Configuration > Exception Management Preferences**.
2. Click **Edit** to open the **Edit Exception Management Preferences** page.



*The Edit Exception Management Preferences page.*

3. Scroll down to the **Approved status is set to** field and click on any status you wish to have mapped to Approved. Hold the **Ctrl** key while you click to select multiple statuses. Any value(s) you select to map to an approved status value will result in risk reduction taken against the object an exception is applied to when an exception possesses those status values.

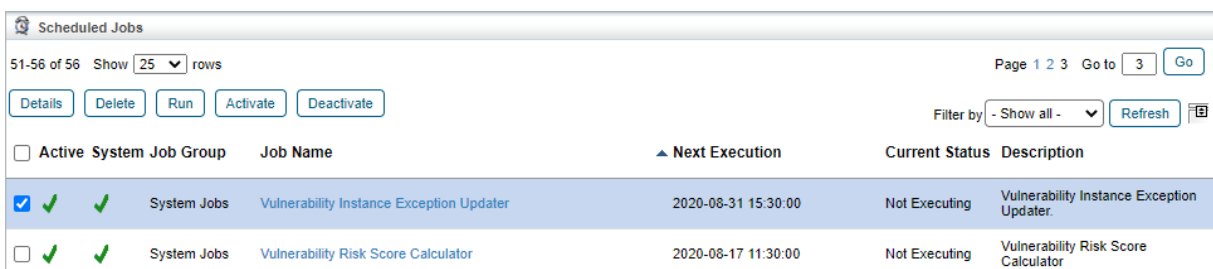


*The Approved status is set to field.*

4. Click **Save**.

If the newly set approved status values relate to vulnerability exceptions, you will need to run a job to recalculate all approved vulnerability exceptions. Running this job requires a user to be a RiskVision administrator. To run this job, see the following steps:

1. Log on with an administrator account.
2. Open the **Administration** application.
3. Navigate to **Administration > Scheduled Jobs**.
4. Select the **Vulnerability Instance Exception Updater** job and click **Run**.



*The Vulnerability Instance Exception Updater job.*
























## Entity Types

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

## 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
	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.

## Create 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\* jason B

Import Entities from a file

Next

*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

<input type="checkbox"/> Name	Path
<input checked="" type="checkbox"/> Datacenter	/Datacenter
<input checked="" type="checkbox"/> DNB Group	/DNB Group
<input type="checkbox"/> HQ	/HQ

Selected Hierarchies

Datacenter  
 DNB Group

>>  
<<

Cancel
< Back
Next >

*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.

Create a Computer
✕

<b>1. Organization</b> <b>2. Computer</b> <b>3. Address</b> <b>4. Classification</b> <b>5. Ownership</b>	<div style="background-color: #0070C0; color: white; padding: 5px; font-weight: bold;"> <b>Step 3: Optionally, enter the geographic location of the entity.</b> <span style="float: right; font-size: 0.8em;">* = required</span> </div> <div style="background-color: #FFF9C4; padding: 5px; margin-top: 5px; font-size: 0.9em;">             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.           </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><b>Primary Address</b></p> <p>Location  <input type="text" value="Headquarters"/></p> <p>Address 1  <input type="text" value="123 Main Street"/></p> <p>Address 2  <input type="text"/></p> <p>City  <input type="text" value="Washington"/></p> <p>State / Province  <input type="text" value="DC"/></p> <p>Zip Code / Postal Code  <input type="text" value="20401"/></p> <p>Country  <input type="text" value="US"/></p> <p>Region  <input type="text"/></p> <hr/> <p>Building  <input type="text"/></p> <p>Floor  <input type="text"/></p> </div>
<div style="display: flex; justify-content: space-between; align-items: center;"> <span style="border: 1px solid #ccc; border-radius: 5px; padding: 5px 15px; background-color: #D3D3D3;">Cancel</span> <span style="display: flex; gap: 10px;"> <span style="border: 1px solid #ccc; border-radius: 5px; padding: 5px 15px; background-color: #D3D3D3;">&lt; Back</span> <span style="border: 1px solid #ccc; border-radius: 5px; padding: 5px 15px; background-color: #0070C0; color: white;">Next &gt;</span> </span> </div>	

*The Address wizard page.*

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

**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  ▼

Internal or external  ▼

Cancel
< Back
Next >

*The Classification wizard page.*

7. Select the [criticality setting](#). The **Ownership** page is displayed.

**Create a Computer**
✕

1. Organization

2. Computer

3. Address

4. Classification

5. Ownership

**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\*

Additional Owners:

Filter by

☐	Name	▲ Type	Ownership Type
i	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.



## Create 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\*

Entity type\*

Entity subtype

Description

Primary Owner\*

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**
✕

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

<input type="checkbox"/> Name	Path
<input checked="" type="checkbox"/> Datacenter	/Datacenter
<input checked="" type="checkbox"/> DNB Group	/DNB Group
<input type="checkbox"/> HQ	/HQ

>>
<<

Selected Hierarchies

Datacenter

DNB Group

Cancel
< Back
Next >

*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.

Create a Computer
✕

<p><b>1. Organization</b></p> <p><b>2. Computer</b></p> <p><b>3. Address</b></p> <p><b>4. Classification</b></p> <p><b>5. Ownership</b></p>	<div style="text-align: right; font-size: 0.8em; color: #0070C0;">* = required</div> <p><b>Step 2: Define the network identification and physical properties of the computer or device.</b></p> <div style="background-color: #FFF2CC; padding: 5px; margin-top: 10px;">             Enter the network identification and other information, if desired.         </div> <p><b>Identification</b></p> <p>Name DesktopID1012</p> <p>Host name* <input type="text" value="DesktopID1012"/></p> <p>Domain name <input type="text"/></p> <p><b>Computer Details</b></p> <p>Manufacturer <input type="text"/></p> <p>Version <input type="text"/></p> <p>Serial number <input type="text"/></p> <p>Product name <input type="text"/></p> <p>Chassis Type <input type="text" value="laptop"/></p> <p>Processor name <input type="text"/></p>
---	---

Cancel
< Back
Next >

*The Computer wizard page.*

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

Create a Computer
✕

<b>1. Organization</b> <b>2. Computer</b> <b>3. Address</b> <b>4. Classification</b> <b>5. Ownership</b>	<div style="text-align: right; font-weight: bold; font-size: 1.1em;">Step 3: Optionally, enter the geographic location of the entity. <span style="font-size: 0.8em;">* = required</span></div> <div style="background-color: #FFF9C4; padding: 5px; margin-top: 10px;"> <p style="font-size: 0.9em; margin: 0;">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.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><b>Primary Address</b></p> <p>Location  <input type="text" value="Headquarters"/></p> <p>Address 1  <input type="text" value="123 Main Street"/></p> <p>Address 2  <input type="text"/></p> <p>City  <input type="text" value="Washington"/></p> <p>State / Province  <input type="text" value="DC"/></p> <p>Zip Code / Postal Code  <input type="text" value="20401"/></p> <p>Country  <input type="text" value="US"/></p> <p>Region  <input type="text"/></p> <hr/> <p>Building  <input type="text"/></p> <p>Floor  <input type="text"/></p> </div>
<input type="button" value="Cancel"/>	<input type="button" value=" &lt; Back"/> <input style="background-color: #0070C0; color: white;" type="button" value=" Next &gt;"/>

*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

Internal or external

Cancel
< Back
Next >

*The Classification wizard page.*

8. Select the [criticality setting](#). The **Ownership** wizard page appears.

**Create a Computer**
✕

1. Organization

2. Computer

3. Address

4. Classification

5. Ownership

**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\*

Additional Owners:

Filter by

<input type="checkbox"/> Name	<input type="checkbox"/> Type	Ownership Type
<div style="display: flex; align-items: center;"> <div style="font-size: 1.2em; margin-right: 5px;">i</div>           No additional owners defined.         </div>		

*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.

## Set 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\*

Entity type\*  ▼ +

Entity subtype  ▼

Description

Primary Owner\*  ▼ +

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	<a href="#">Default entity types</a>	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, application, computer, and so on. Entities first show up in the Discovered dynamic group when they are discovered by a connector or created from imported entities.

### To move discovered or unmanaged entities to the Managed group:

- Click **Manage** in the **Status** dropdown list in the **General Detail** display for a particular entity.  
OR
- Click the **Manage** node or any **Manage** node subgroup and click **Start Managing These Entities**.  
OR
- Click **Manage Entities** from the **More Actions** menu.

Entities require a minimum of a hostname or IP and a domain to be included in the display of discovered or managed entities.



## Display Entity Details

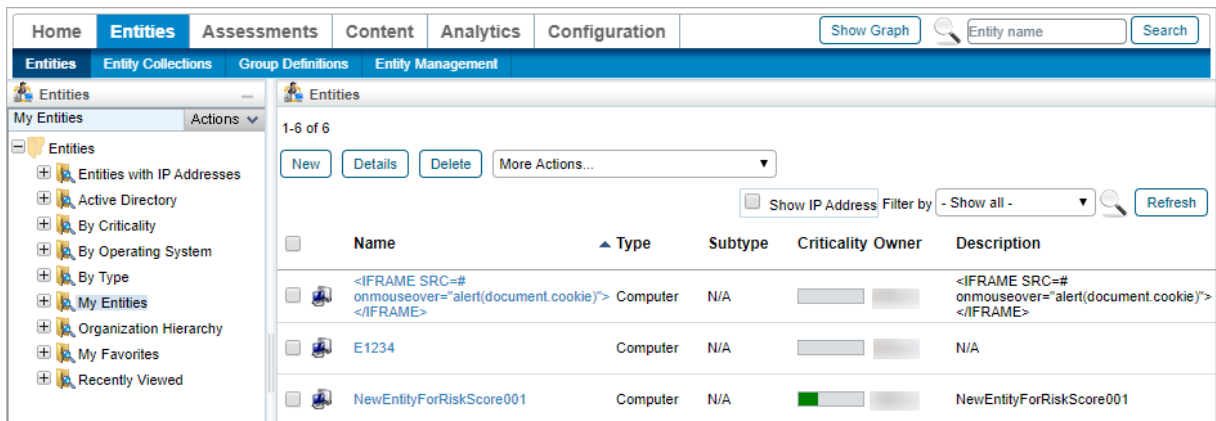
There are a few ways to open the entity details pane from other menus, such as opening the **Assessment Details** page. This section explains how to open the details pane from the **Entities** menu. To view and search an entity, you must have the Entity View permission. In general, entities are visible 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.



*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> Edit ★ Favorites

**General**

Owners

Description

Addresses

Classification

Costs & Impact

Relationships

Propagation

Documents

Assessments

⊕ Vulnerabilities

⊕ System Details

Data Feeds

Exceptions

### Information

<p><b>Information</b></p> <p>Name &lt;IFRAME SRC=# onmouseover="alert(document.cookie)"&gt;&lt;/IFRAME&gt;</p> <p>Description &lt;IFRAME SRC=# onmouseover="alert(document.cookie)"&gt;&lt;/IFRAME&gt;</p> <p>Entity type Computer</p> <p>Entity N/A subtype</p> <p>Manufacturer N/A</p> <p>Serial N/A number</p> <p>Product N/A name</p> <p><b>Entity Management</b></p> <p>Tracked since 2020-04-27</p> <p>Status Managed</p> <p>Data source(s)  Manual entry</p> <p>Created by srinu s</p> <p>Created on 2020-04-27</p> <p>Discovery source N/A</p>	<p><b>Maintenance</b></p> <p>Installation date N/A</p> <p>Last maintenance date N/A</p> <p>Maintenance reference N/A</p> <p>Warranty expiration date N/A</p> <p>Warranty reference N/A</p>
--	--

**Organization Hierarchy**

Add Delete More Actions... ▼

Filter by - Show all - ▼ Refresh

<input type="checkbox"/>	Organization Root	▲ Path	Description
<span>i</span> 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: <code>com.agilance.asset.deleteAddress=true</code> .
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 <a href="#">Relationship Explorer</a> .  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 <a href="#">Assigning Vulnerabilities</a> .  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	<p>Certain types and subtypes of entity, such as Computers, have a number of tabs organized under the heading 'System Details.' These tabs include:</p> <ul style="list-style-type: none"> <li>• Network</li> <li>• Ports</li> <li>• Services</li> <li>• Applications</li> <li>• Patches</li> <li>• Network Shares</li> <li>• User Accounts</li> <li>• Membership</li> </ul>
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 the Tenant Configure permission.

## Add 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**.
3. Enter the ownership configuration:
  - **Name:** Type a name that uniquely identifies the ownership type.
  - **Display Name:** 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.
  - **Type:**
    - **Entity:** Assign to Entities and the Assessment, Ticket, Exception, and Incident workflows.
    - **Policy:** Assign to policy packs and policy workflows.
  - **Role:** limit which users can be assigned to 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.

## Delete 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.

## Change the Ownership Type Settings

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

### To modify an ownership type settings:

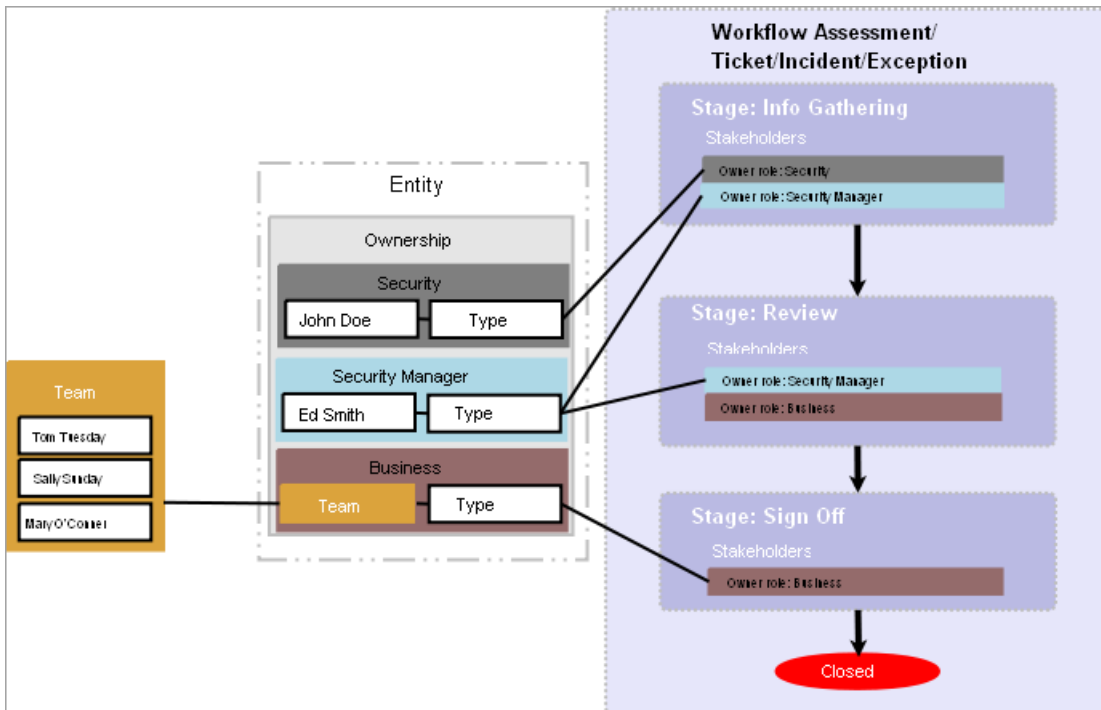
1. Go to **Configuration > Ownership Types**.
2. Select the ownership type.
3. Click **Edit**. The **Configure Ownership Type** dialog appears.
4. Modify the configuration and click **OK**.

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**.

The screenshot shows the 'Select Owners' dialog box. It has a blue header with the title 'Select Owners' and a close button. Below the header, there are three sections: 'Owner Type\*' with a dropdown menu set to 'Business Owner'; 'Individual Owner\*' with a dropdown menu showing 'John D' and an add button; and 'Team Owner' with a dropdown menu and a 'Details' link. At the bottom, there are 'OK' and 'Cancel' buttons.

*The Add Additional Owners dialog.*

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**.

## Configure 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.

### To modify a range:

1. Go to **Configuration > Entity Configuration**.
2. Click **Ranges**.
3. Choose **Entity Criticality Configuration**, then click **Edit**.

Threshold	Label	Color	Display
Less than 0 [ + ]	Unknown	Gray	<input type="radio"/> Text <input checked="" type="radio"/> Score
Between 0 and 6 [ + ] [ - ]	Low	Green	<input checked="" type="radio"/> Text <input type="radio"/> Score
Between 6 and 8 [ + ] [ - ]	Medium	Gold	<input type="radio"/> Text <input type="radio"/> Score
Greater than 8	High	Red	<input type="radio"/> Text <input type="radio"/> Score

*The Configure Threshold dialogue.*

4. Select one of the following options:
  - Click + to increase the threshold range,
  - Click - to decrease the threshold range.
5. Click **OK**.

## Set the Criticality Rating

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

Application: E1 Save Cancel Favorites

**General**  
**Assessments**  
**Owners**  
**Description**  
**Addresses**  
**Classification**  
**Costs & Impact**  
**Vulnerabilities**  
**Vulnerabilities List**  
**Relationships**  
**Propagation**  
**Documents**  
**Data Feeds**  
**Exceptions**

**Business Criticality**

Business Criticality

**Security Requirements** Refresh

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

**Classification**

Classification Label   
 Type Of Data   
 Environment Type   
 Internal or external

**Tags**

**Change History**

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.

Name	Type	Subtype	Criticality	Owner	Description
DesktopID1012	Computer	N/A	<input type="text" value="Unknown"/>	pavani B	N/A
E1	Application	N/A	<input type="text" value="Unknown"/>	pavani B	N/A

The Entities list.

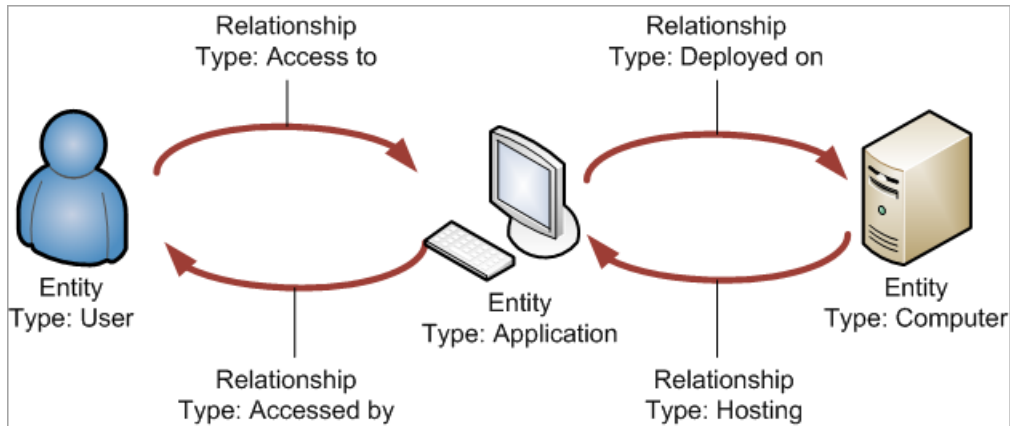
3. Select an entity, then click **Details**.
4. Click the **Classification** tab, then click **Edit**.
5. Select the desired radio button in the **Security Requirements** section.
6. Click **Save**.

Related scores and settings are immediately updated.

## About Entity Relationships

Entities are related to one another, usually in obvious 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 are bidirectional. If an application is deployed on a computer, the computer hosts the application.



Entity relationships allow risks to propagate from entity to entity.

### 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.

## Relationship Types Overview

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.

<input type="checkbox"/> From Type	▲ To Type	Description	Propagate Control Results	Propagate Risk Score	Inherit Tag	Criticality
<input type="checkbox"/> Can be accessed by	Has access to	Access relationship between entities	No	No	No	No inherit
<input type="checkbox"/> Child of	Parent of	Parent child relationship between entities	No	No	No	No inherit
<input type="checkbox"/> Consists of	Part of	Composition relationship between entities	No	No	No	No inherit
<input type="checkbox"/> Consumes	Provides	Service provider relationship between entities	No	No	No	No inherit
<input type="checkbox"/> 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.

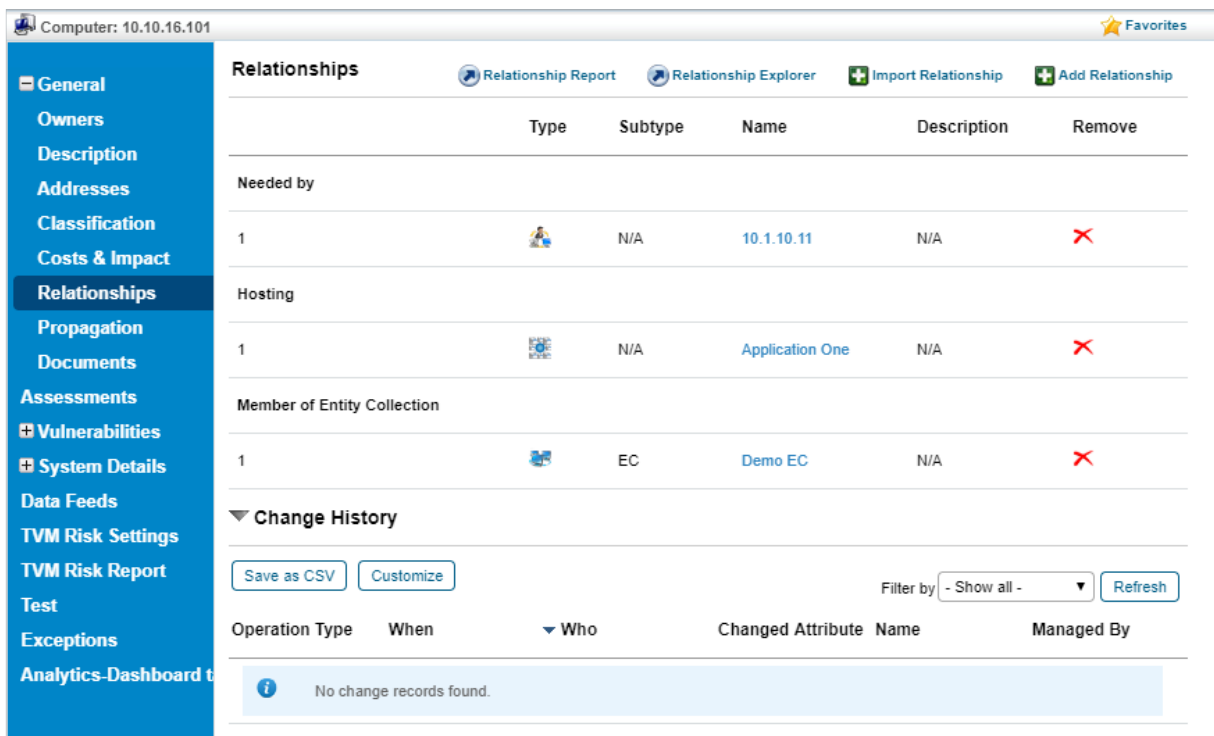
By default, control and score propagation settings are disabled. See [Configuring Entity Relationship Attributes](#) for more information.

### 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.



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

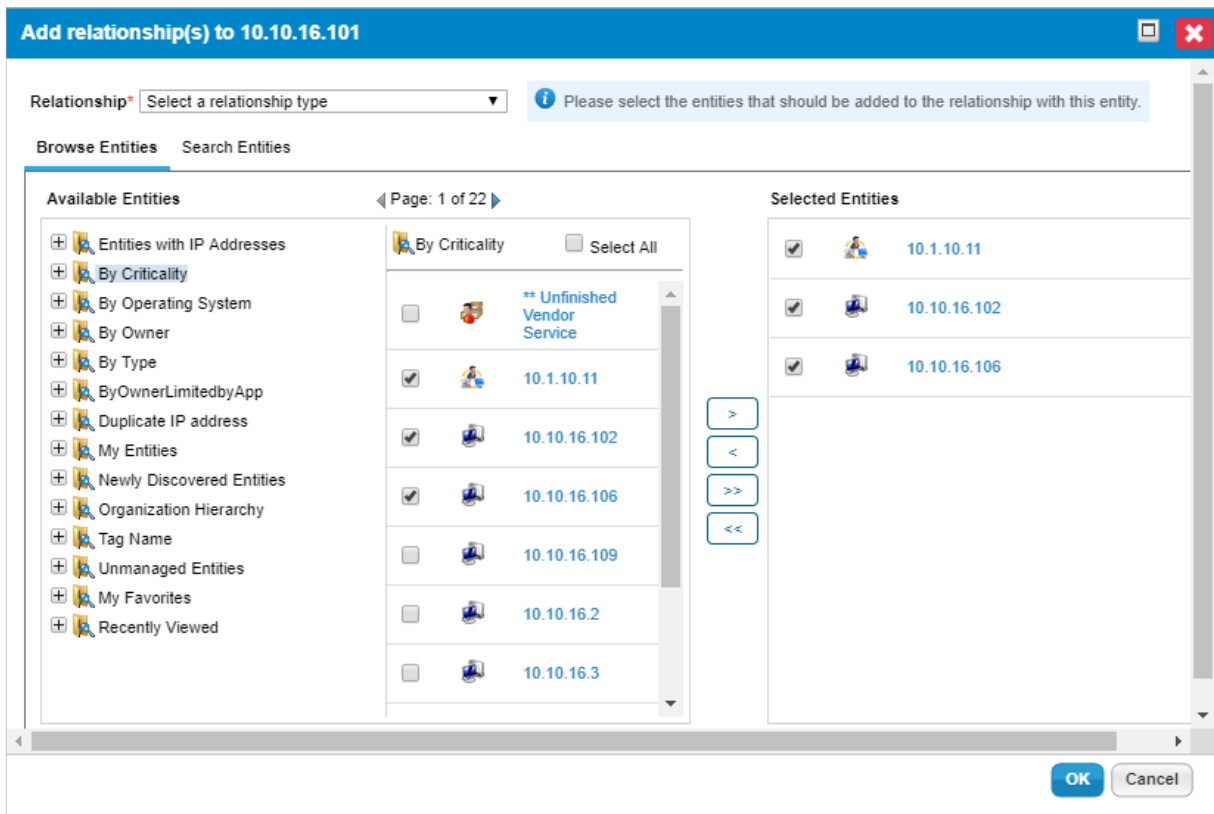
**Change History**

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**.



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.



## Create and Delete Relationship Types

Started in version 7.0, RiskVision provides the ability to create and delete a relationship type when `com.agilance.asset.enableCreateRelationshipTypes=true` property is added to the `agilance.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. 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**: The purpose of creating the relationship type.
4. Click **OK**.

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

### To delete a relationship:

1. Go to **Configuration > Entity Configuration**.
2. Select a custom relationship type.
3. Click **Delete**.

## Import a Relationship

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, then click **Import Relationship**.
3. Click **Browse**, select the EntityRelationshipImportTemplate.xls file, click **Open**, and then click **OK**.

## Visualize a Relationship

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. Click **Entities** on the Entities menu.
2. Expand the group containing the entity you want to visualize, then select an entity.
3. Click the **Relationships** tab.
4. Click **Relationship Report**. The web browser opens the **Relationship Report** in a new window.

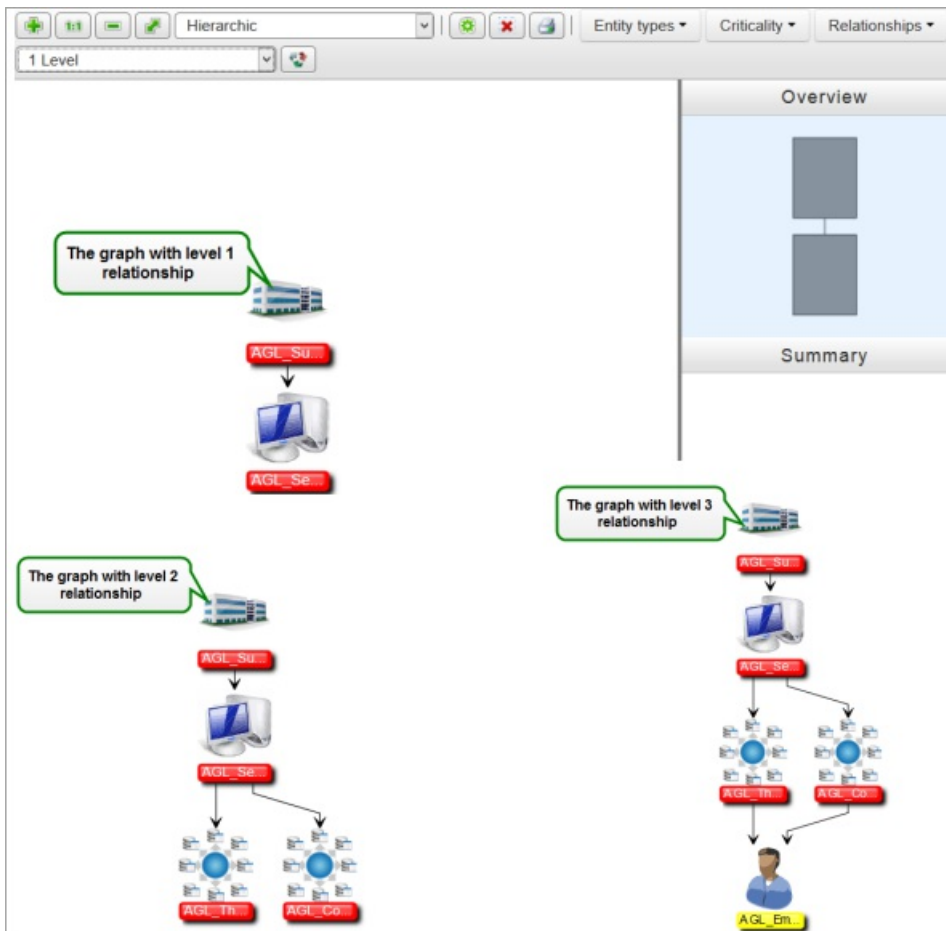
### To visualize entity collection relationships:

1. Open the **Entities** menu.
2. Click **Entity Collections**.
3. Expand the group containing the entity collection you want to visualize, then select an entity.
4. Click the **Relationships** tab.
5. Click **Relationship Report**.

## Relationship Report

The Relationship Report is displayed in a window in which different visualization tools are available to study relationships from level 1 to level 6. In the Relationship Report, you can use filters, such as entity type, criticality, and relationships, to exclude items. The default view includes all 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 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.agilance.web.visualization.maxentitycountofsametype` property.



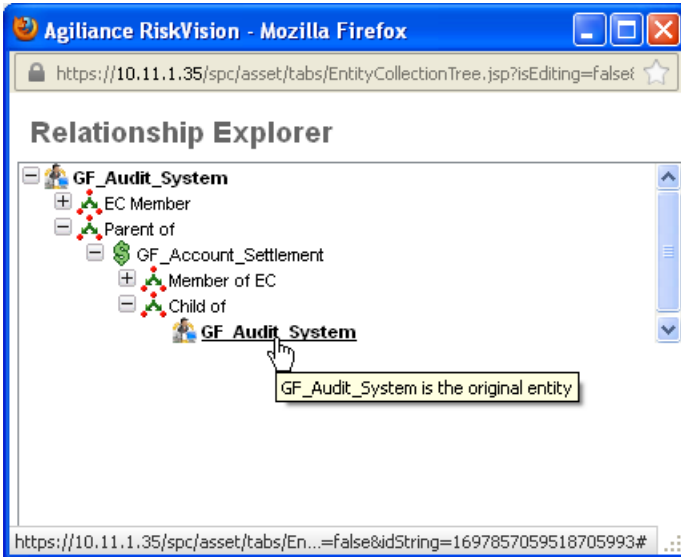
*Layouts of level 1, 2, and 3 relationships.*

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. For more information about visualization and its tool options, please see [Visualizing Objects](#).

## Relationship Explorer

The **Relationships** tab for an entity or entity collection only shows its direct relationships. That is, the relationships of one or more entities or entity collections that are related to other entities or entity collections. The **Relationship Explorer** window allows you to drill down into relationships with other entities and entity collections. It can also be used to show all the dependencies of a particular entity collection or entities, not just those that are one level removed from that entity collection.

To open the **Relationship Explorer** window, click an entity or entity collection to open, click the **Relationships** tab, and then click the **Relationship Explorer**.



*The Relationship Explorer window.*

At the top of the **Relationship Explorer** window, you will see the entity (or entity collection) as a root. When you expand the root, any established relationships will appear. Expand each relationship type to see the entities associated with the root entity. 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.



## Assign a Vulnerability

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 <b>Entities</b> > <b>Entities</b> , then select an entity to open. Click the <b>Vulnerabilities List</b> tab > <b>Assign</b> .
Control and Subcontrol	Go to <b>Content</b> > <b>Controls</b> and Questionnaires, then click a control or subcontrol to open. Click the <b>References</b> tab > <b>More Actions</b> > <b>Map to Vulnerability</b> .
Ticket	Go to <b>Home</b> > <b>Tickets</b> , then click a ticket to open. Click <b>Linked To</b> > <b>Vulnerabilities</b> tab > <b>Assign</b> .
Technology	Open RiskVision Threat and Vulnerability Manager. Go to <b>Vulnerabilities</b> > <b>All Technologies</b> , then click a technology to open. Click <b>Vulnerabilities</b> > <b>Link to Existing Vulnerabilities</b> .
Chart	Go to <b>Analytics</b> > <b>Charts</b> . Click a chart. Go to the <b>Filters</b> 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**.

The screenshot shows the 'Select Vulnerabilities' dialog box. At the top, there are search criteria fields: 'Severity' set to 'High', and 'Published between' dates '2018-01-01' and '2019-05-11'. Below this is a table of 'Matching Vulnerabilities' with columns for Name, Identifier, and Publish Date. The first row is 'CVE-2018-6000' with a publish date of '2018-01-22'. A detail pane for 'Vulnerability: CVE-2018-6000' is open, showing 'Severity High' in a green box. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

*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 for 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. Open the **Entity Details** page.
2. Click the **System Details** tab.
3. Click **New**.
4. 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.
  - **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.
5. Click **OK**. The operating system is added.

### To assign a predefined operating system:

1. Open the **Entity Details** page.
2. Click the **System Details** tab.
3. Click **Add**.
4. Search the application. The following fields can be used in combination to narrow the search results:
  - **Title:** Enter the operating system's title.
  - **Version:** Enter the operating system's version number.
  - **Vendor:** Enter the vendor's name.
5. Click **Search**.
6. Select the operating system in the **Known Operating Systems** box, and click the arrow pointing down to move the operating system into the **Selected Operating Systems** box.
7. Click **OK**.

### To edit an operating system:

1. Open the **Entity Details** page.
2. Click the **System Details** tab.
3. Select the box in the corresponding operating system row. You can edit only the user-defined and scanner-imported operating systems.
4. Click **Edit** in the **More Actions** dropdown list. The **Operating System** dialog appears, where changes to the operating system can be made.
5. After the completion of changes, click **OK**.

### To delete an operating system

1. Open the **Entity Details** page.
2. Click the **System Details** tab.
3. Select the box in the corresponding operating system row and click **Delete**. The selected operating system is removed from the entity.



## Applications

Installed applications can be found on the Computer, Network Device, and Mobile Device entity types. Typically, this data is imported from scanners, but there may be times when you may want to manually update the data.

### To add an application:

1. Open the **Entity Details** page.
2. Click **+** to expand the **System Details** tab, then click **Applications**.
3. Click **New**.
4. Enter the following fields in the **Application** dialog,
  - **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.
5. Click **OK**. The application is added.

### To assign a predefined application:

1. Open the **Entity Details** page.
2. Click **+** to expand the **System Details** tab, then click **Applications**.
3. Click **Add**.
4. Search the application using the following fields to narrow the search results:
  - **Title**. Enter the application's title.
  - **Version**. Enter the application's version number.
  - **Vendor**. Enter the vendor's name.
5. Click **Search**.
6. 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.
7. 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.
8. Click **OK**. The predefined application is added.

### To edit an application:

1. Open the **Entity Details** page.
2. Click **+** to expand the **System Details** tab, then click **Applications**.
3. 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.
4. Click **Edit** in the **More Actions** dropdown list. The **Application** dialog appears, where changes to the application can be made.
5. After the completion of changes, click **OK**.

### To delete an application:

1. Open the **Entity Details** page.
2. Click **+** to expand the **System Details** tab, then click **Applications**.
3. Select the box in the corresponding application row, then click **Delete**.

## 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.

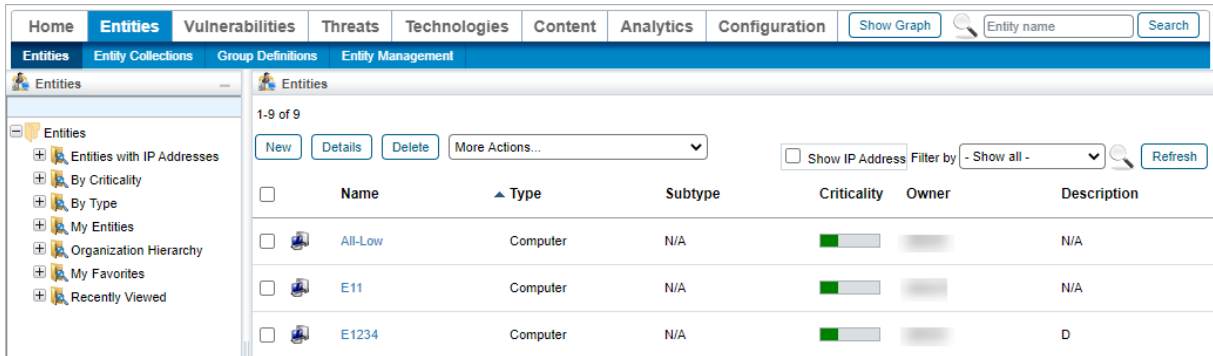


## Add Compensating Controls

Users with the Entity View, Threats and Vulnerabilities View, and Vulnerability Compensating Control Update permissions can add vulnerability compensating controls directly to an entity to reflect vulnerability risk mitigations applied to one or more entities. Alternatively users with the Entity View, Entity Manage, Threats and Vulnerability View, and Vulnerability Compensating Controls Update permissions can add vulnerability compensating controls to multiple entities.

### To add vulnerability compensating controls to a single entity:

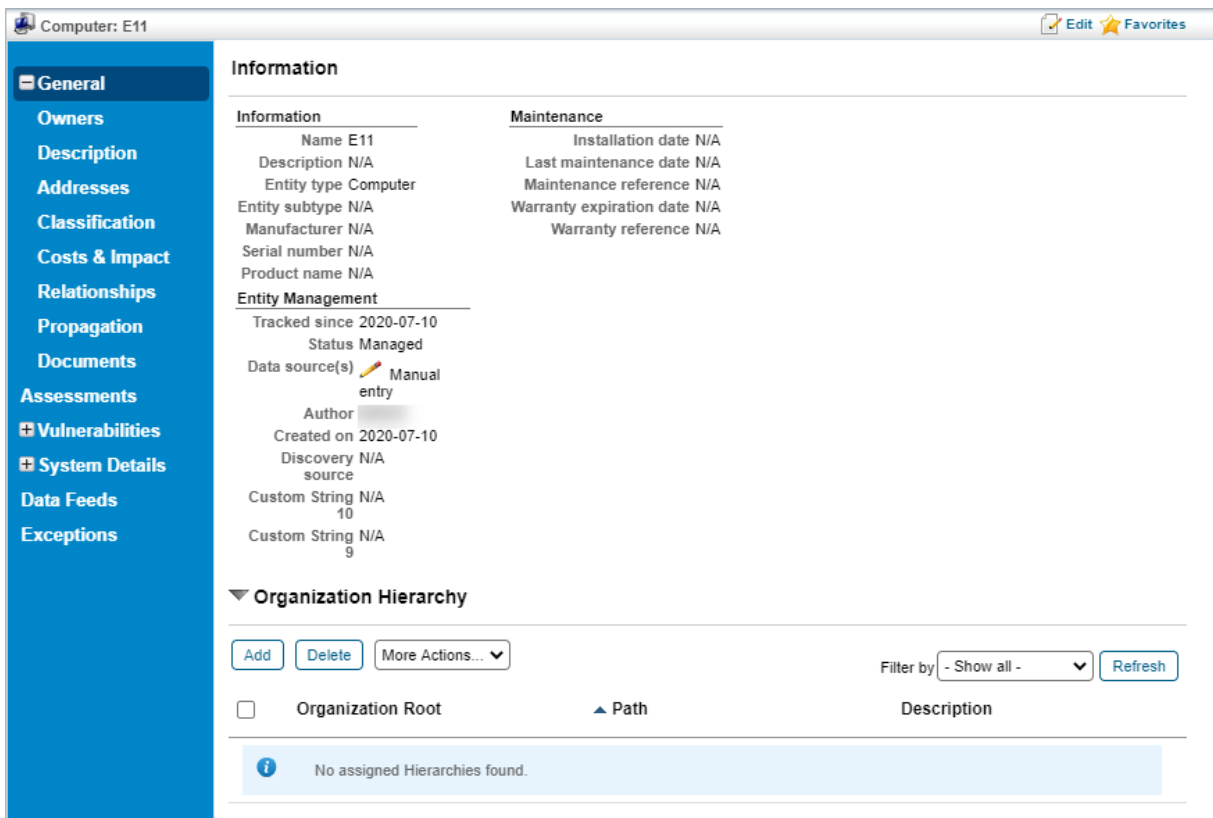
1. In the Threat & Vulnerability Manager application, navigate to **Entities > Entities**.



The screenshot shows the Threat & Vulnerability Manager application interface. The top navigation bar includes tabs for Home, Entities, Vulnerabilities, Threats, Technologies, Content, Analytics, and Configuration. The main content area is titled 'Entities' and displays a list of 9 entities. The list has columns for Name, Type, Subtype, Criticality, Owner, and Description. The entities listed are All-Low, E11, and E1234, all of which are of type 'Computer' and have a criticality of 'N/A'. The 'All-Low' entity has a description of 'N/A', 'E11' has 'N/A', and 'E1234' has 'D'. There are also buttons for 'New', 'Details', 'Delete', and 'More Actions...' at the top of the list.

*The Entities list.*

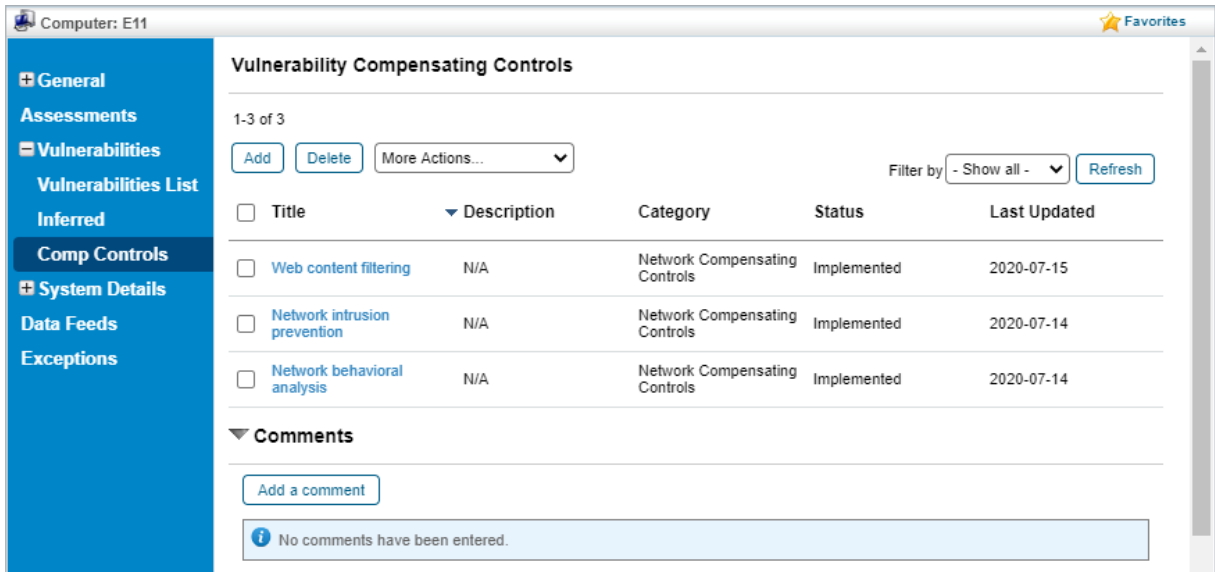
2. Click an entity you wish to add vulnerability compensating controls to.



The screenshot shows the 'Entity Details' page for 'Computer: E11'. The page is divided into several sections: 'General' (selected), 'Owners', 'Description', 'Addresses', 'Classification', 'Costs & Impact', 'Relationships', 'Propagation', 'Documents', 'Assessments', 'Vulnerabilities', 'System Details', 'Data Feeds', and 'Exceptions'. The 'Information' section is expanded, showing details for 'Information' and 'Maintenance'. The 'Information' section includes fields for Name (E11), Description (N/A), Entity type (Computer), Entity subtype (N/A), Manufacturer (N/A), Serial number (N/A), and Product name (N/A). The 'Maintenance' section includes fields for Installation date (N/A), Last maintenance date (N/A), Maintenance reference (N/A), and Warranty expiration date (N/A). The 'Entity Management' section includes fields for Tracked since (2020-07-10), Status (Managed), Data source(s) (Manual entry), Author, Created on (2020-07-10), Discovery source (N/A), Custom String 10 (N/A), and Custom String 9 (N/A). The 'Organization Hierarchy' section is also visible, showing a table with columns for Organization Root, Path, and Description. A message at the bottom of the hierarchy section states 'No assigned Hierarchies found.'

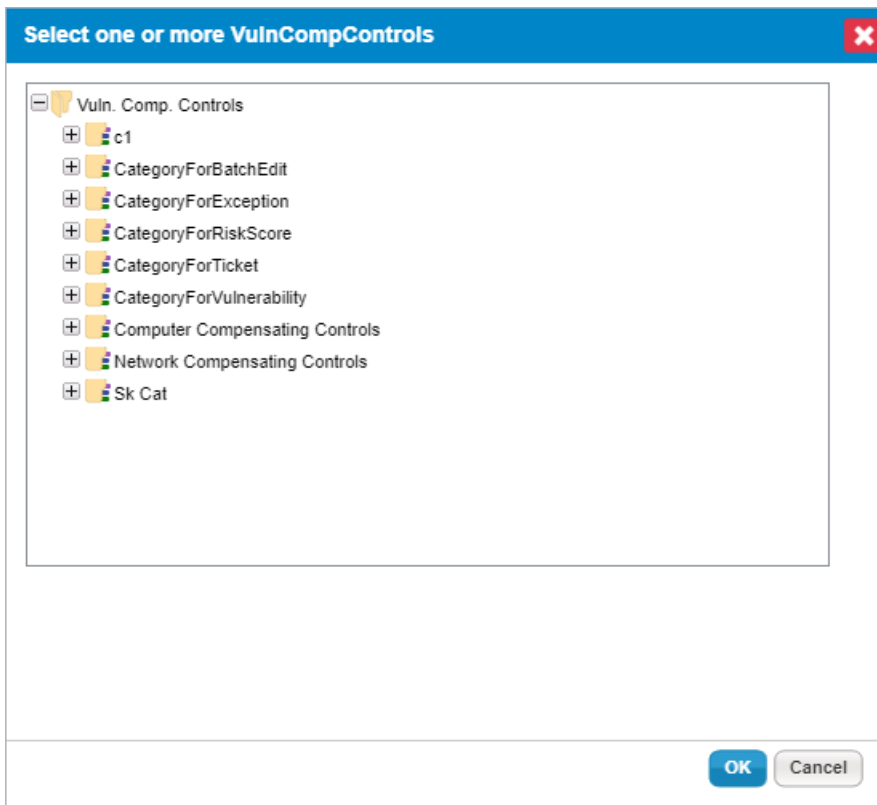
*The Entity Details page.*

3. Navigate to the **Comp Controls** tab under the **Vulnerabilities** tab.



The Comp Controls tab.

4. Click Add.



The Add Vulnerability Compensating Controls dialogue.

5. Click + next to any category you wish to open.
6. Click the checkbox next to any vulnerability compensating controls you wish to add to the entity.
7. Click OK.

## To add vulnerability compensating controls to multiple entities:

1. In the Threat & Vulnerability Manager application, navigate to **Entities > Entities**.

Name	Type	Subtype	Criticality	Owner	Description
All-Low	Computer	N/A	100%		N/A
E11	Computer	N/A	50%		N/A
E1234	Computer	N/A	50%		D

The Entities list.

2. Select each entity you wish to add vulnerability compensating controls to and click **Batch Edit Entities**.

The Editing Multiple Entities page.

3. Navigate to the **Comp Controls** tab.

Editing Multiple Entities: 2 Entities

General  
 Owners  
 Description  
 Addresses  
 Classification  
 Costs & Impact  
**Comp Controls**

### Vulnerability Compensating Controls

1-3 of 3

Filter by - Show all -

<input type="checkbox"/>	Title	Description	Category	Status	Last Updated
<input type="checkbox"/>	Web content filtering	N/A	Network Compensating Controls	Implemented	2020-07-15
<input type="checkbox"/>	Network intrusion prevention	N/A	Network Compensating Controls	Implemented	2020-07-14
<input type="checkbox"/>	Network behavioral analysis	N/A	Network Compensating Controls	Implemented	2020-07-14

The Comp Controls tab.

4. Click Add.

**Select one or more VulnCompControls**
✕

Vuln. Comp. Controls

c1

CategoryForBatchEdit

CategoryForException

CategoryForRiskScore

CategoryForTicket

CategoryForVulnerability

Computer Compensating Controls

Network Compensating Controls

Sk Cat

The Add Vulnerability Compensating Controls dialogue.

5. Click + next to any category you wish to open.
6. Click the checkbox next to any vulnerability compensating controls you wish to add to the entity.
7. Click OK.

## Batch Edit Compensating Controls

Users with the Entity View, Threats and Vulnerabilities View, and Vulnerability Compensating Control Update permissions can use the **Batch Edit VCC** action to edit the status of multiple vulnerability compensating controls attached to a single entity. Alternatively, users with the Entity View, Entity Manage, Threats and Vulnerability View, and Vulnerability Compensating Controls Update permissions can edit vulnerability compensating controls attached to multiple entities.



Batch editing vulnerability compensating controls across multiple entities can only be done for compensating controls that the entities have in common.

## To batch edit vulnerability compensating controls on a single entity:

1. In the Threat & Vulnerability Manager application, navigate to **Entities > Entities**.

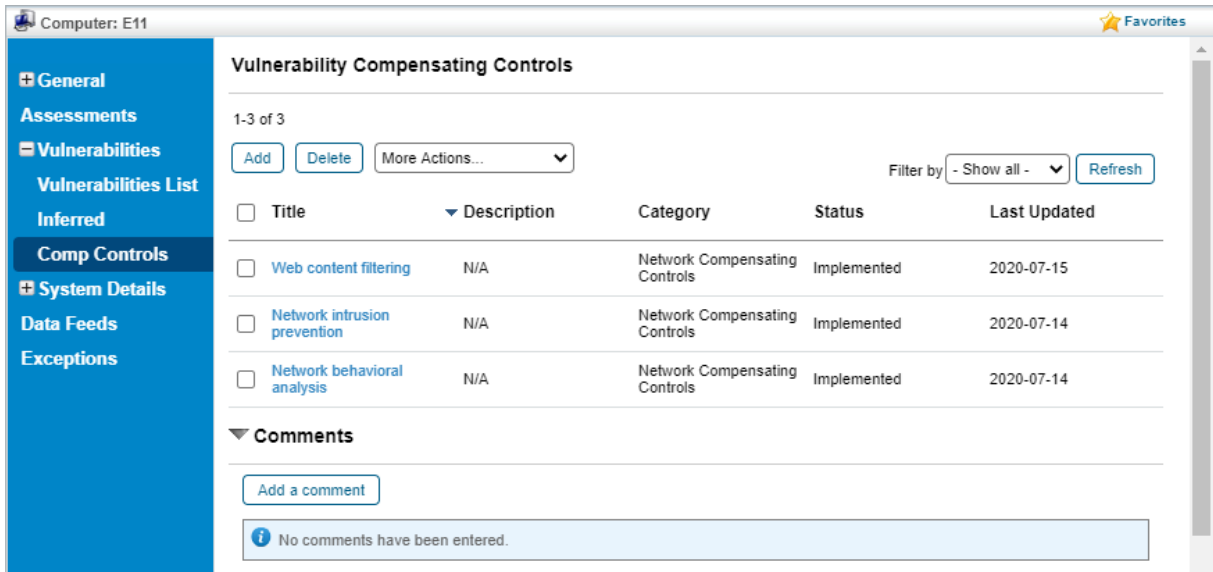
Name	Type	Subtype	Criticality	Owner	Description
All-Low	Computer	N/A	Green bar	[Redacted]	N/A
E11	Computer	N/A	Green bar	[Redacted]	N/A
E1234	Computer	N/A	Green bar	[Redacted]	D

The Entities list.

2. Click the entity that contains the vulnerability compensating control or controls that you wish to edit.

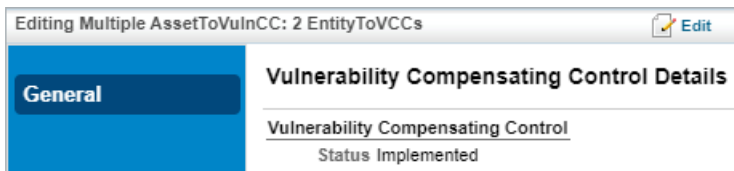
The Entity Details page.

3. Navigate to the **Comp Controls** tab under the **Vulnerabilities** tab.



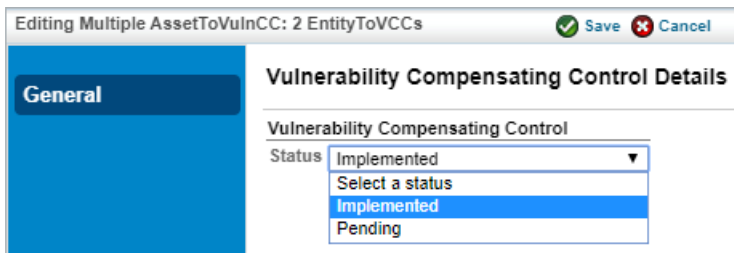
The Comp Controls tab.

4. Select each compensating control to be edited and select **Batch Edit VCC** from the **More Actions...** select list.



The Editing Multiple Vulnerability Compensating Controls page.

5. Click **Edit**.
6. Select the status the compensating controls should be set to in the **Status** select list.

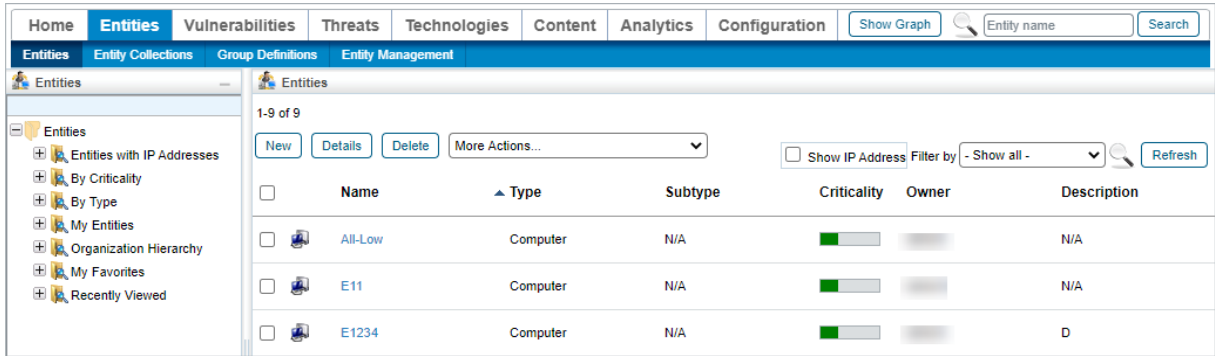


The Status select list.

7. Click **Save**.

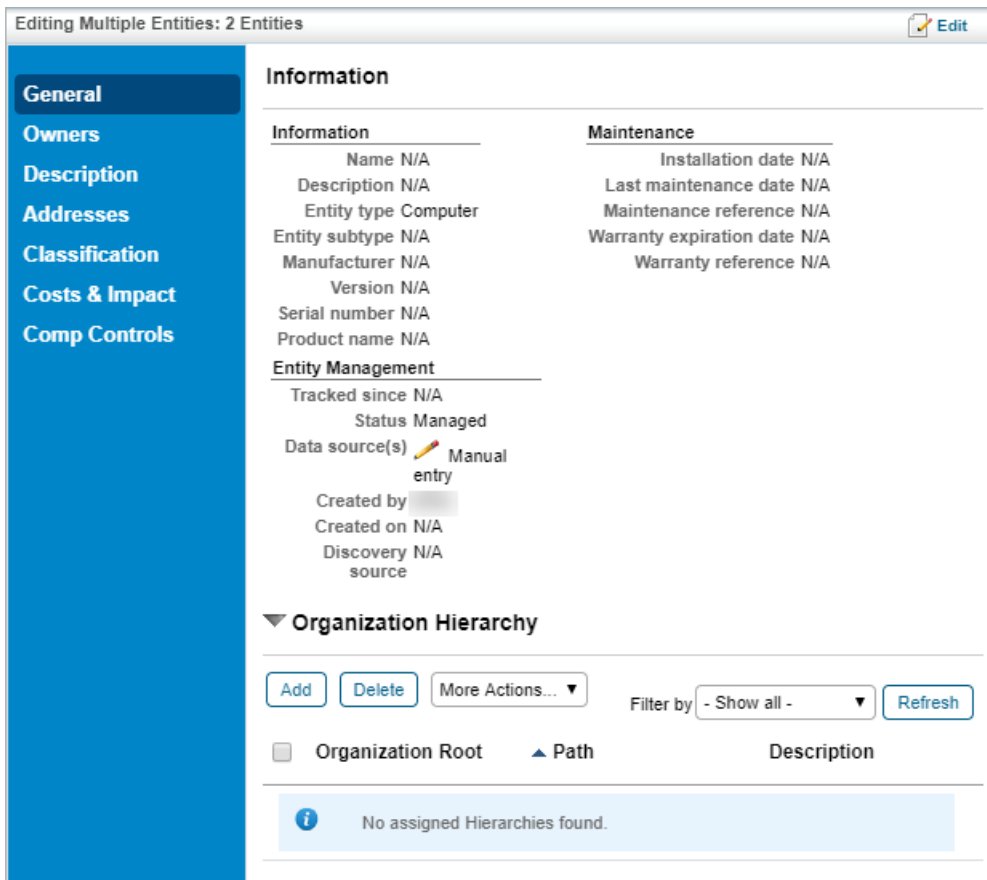
## To batch edit vulnerability compensating controls across multiple entities:

1. In the Threat & Vulnerability Manager application, navigate to **Entities > Entities**.



The Entities list.

2. Select each entity that contains the vulnerability compensating control or controls that you wish to edit and click **Batch Edit Entities**.



The Editing Multiple Entities page.

3. Navigate to the **Comp Controls** tab.

Editing Multiple Entities: 2 Entities

**Vulnerability Compensating Controls**

1-3 of 3

Filter by

<input type="checkbox"/>	Title	Description	Category	Status	Last Updated
<input type="checkbox"/>	Web content filtering	N/A	Network Compensating Controls	Implemented	2020-07-15
<input type="checkbox"/>	Network intrusion prevention	N/A	Network Compensating Controls	Implemented	2020-07-14
<input type="checkbox"/>	Network behavioral analysis	N/A	Network Compensating Controls	Implemented	2020-07-14

The Comp Controls tab.

- Select each compensating control to be edited and select **Batch Edit VCC** from the **More Actions...** select list.

Editing Multiple AssetToVulnCC: 8 EntityToVCCs

**General**

**Vulnerability Compensating Control Details**

Vulnerability Compensating Control  
Status Implemented

The Edit Multiple Vulnerability Compensating Controls page.

- Click **Edit**.
- Select the status the compensating controls should be set to in the **Status** select list.

Editing Multiple AssetToVulnCC: 8 EntityToVCCs

**General**

**Vulnerability Compensating Control Details**

Vulnerability Compensating Control  
Status

- Select a status
- Implemented
- Pending

The Status select list.

- Click **Save**.



## Remove Compensating Controls

If a vulnerability compensating control has been added to an entity in error or is no longer applicable to an entity, it can be removed by users with the Entity View, Threats and Vulnerabilities View, and Vulnerability Compensating Control Update permissions. Alternatively, users with the Entity View, Entity Manage, Threats and Vulnerability View, and Vulnerability Compensating Controls Update permissions can remove vulnerability compensating controls from multiple entities. Removing the vulnerability compensating control from the entity will not delete it.



Removing vulnerability compensating controls across multiple entities can only be done for compensating controls that the entities have in common.

### To remove a vulnerability compensating control from an entity:

1. In the Threat & Vulnerability Manager application, navigate to **Entities > Entities**.

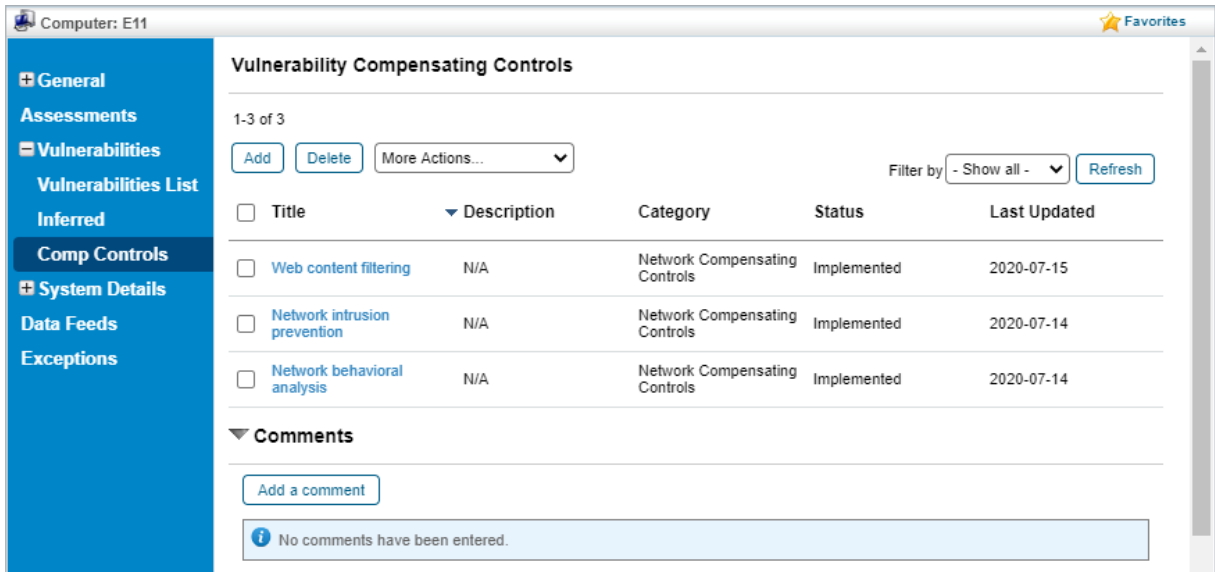
Name	Type	Subtype	Criticality	Owner	Description
All-Low	Computer	N/A	Green bar	[Redacted]	N/A
E11	Computer	N/A	Green bar	[Redacted]	N/A
E1234	Computer	N/A	Green bar	[Redacted]	D

The Entities list.

2. Click the entity that contains the vulnerability compensating control or controls that you wish to remove.

The Entity Details page.

3. Navigate to the **Comp Controls** tab under the **Vulnerabilities** tab.

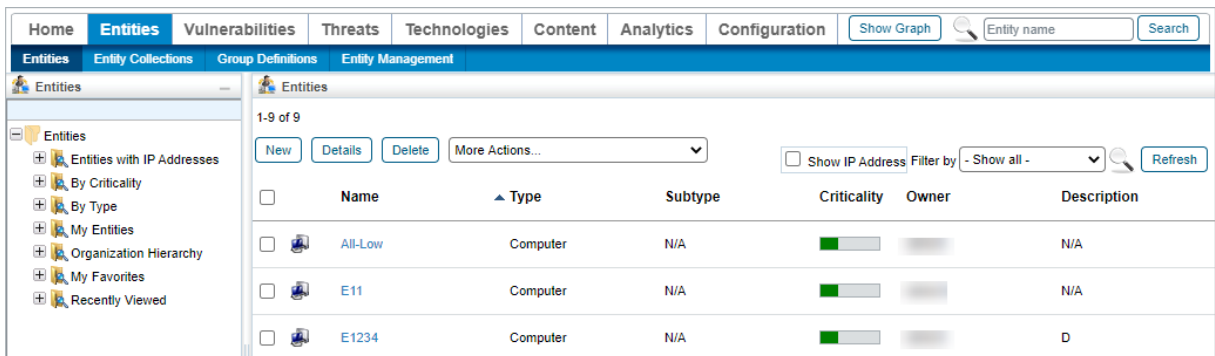


The Comp Controls tab.

4. Select each compensating control to be deleted and click **Delete**.
5. Click **OK**.

## To remove vulnerability compensating controls from multiple entities:

1. In the Threat & Vulnerability Manager application, navigate to **Entities > Entities**.



The Entities list.

2. Select each entity that contains the vulnerability compensating control or controls that you wish to edit and click **Batch Edit Entities**.

Editing Multiple Entities: 2 Entities Edit

**General**

Owners

Description

Addresses

Classification

Costs & Impact

Comp Controls

### Information

---

**Information**

Name N/A

Description N/A

Entity type Computer

Entity subtype N/A

Manufacturer N/A

Version 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 N/A

Status Managed

Data source(s) Manual entry

Created by

Created on N/A

Discovery N/A source

---

**Organization Hierarchy**

---

Filter by

Organization Root     Path    Description

---

No assigned Hierarchies found.

The Editing Multiple Entities page.

- Navigate to the **Comp Controls** tab.

Editing Multiple Entities: 2 Entities

General

Owners

Description

Addresses

Classification

Costs & Impact

**Comp Controls**

### Vulnerability Compensating Controls

1-3 of 3

Filter by

<input type="checkbox"/>	Title	Description	Category	Status	Last Updated
<input type="checkbox"/>	Web content filtering	N/A	Network Compensating Controls	Implemented	2020-07-15
<input type="checkbox"/>	Network intrusion prevention	N/A	Network Compensating Controls	Implemented	2020-07-14
<input type="checkbox"/>	Network behavioral analysis	N/A	Network Compensating Controls	Implemented	2020-07-14

The Comp Controls tab.

- Select each compensating control to be deleted and click **Delete**.
- Click **OK**.

## Entity Actions

Entities can be managed 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 <b>Choose Operating System</b> dialog to search and select the operating system. For information about how to add the operating system to entities, see <a href="#">Operating Systems</a> .
Remove Operating System from Entities	Removes operating system information from entities.
Add Application to Entities	Adds application(s) to entities. Use the <b>Choose Applications</b> dialog to search and select the applications. For information about how to add the application to entities, see <a href="#">Applications</a> .
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 of 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.

## Entity Attribute Screens

This section provides the list of **Entity** attribute screens in RiskVision.

The screenshot shows the 'Addresses' tab for a vendor named '361 Degrees'. The left sidebar contains a menu with options: General, Summary, Assessments, Owners, Addresses (selected), Vendor Contacts, Engagements, Documents, and Engagemnt Summary. The main content area is titled 'Address' and shows a table with 2 rows of address data. The table has columns for Location, Type, Address, City, State, Postal Code, and Country. There are also buttons for 'New', 'Edit', 'Delete', and 'More Actions...' at the top left, and a 'Filter by' dropdown set to '- Show all -' with a 'Refresh' button at the top right.

Location	Type	Address	City	State	Postal Code	Country
<input type="checkbox"/> Mailing	Primary Address	260 Beach	Shanghai	CN	94107	China
<input type="checkbox"/> Billing	Billing Address	260 Beach	Shanghai	CN	94107	China

*The Addresses tab of a vendor.*

The screenshot shows the 'Description' tab for an application type entity named 'Application One'. The left sidebar contains a menu with options: General, Assessments, Owners, Description (selected), Addresses, Classification, Costs & Impact, Vulnerabilities, Vulnerabilities List, Relationships, Propagation, Documents, Data Feeds, and Exceptions. The main content area is titled 'Description' and contains sections for 'Description', 'Network Access', and 'Profile Information'. The 'Description' section lists 'Publisher N/A', 'Version N/A', and 'Accounts N/A'. The 'Network Access' section lists 'IP address N/A', 'Port(s) N/A', and 'Internet facing N/A'. The 'Profile Information' section shows 'Entity Profile(s) High Baseline'. There are 'Edit' and 'Favorites' buttons at the top right.

*The Description tab of an application type entity.*

Network Interface: 172.31.4.5 Edit

General

### 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 Edit Favorites

General
Assessments
Owners
Description
Addresses
Classification
Costs & Impact
Vulnerabilities
Vulnerabilities List
Relationships
Propagation
Documents
Data Feeds
Exceptions

### Business Criticality

Business Criticality  High

---

### Security Requirements

Refresh

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.

## General

CVSS v2.0 Score

Identification

More Information

References

Risk

Entities

Custom tab 1

Custom tab 2

Enhanced Score

Risk Score

CVSS v3.0 Score

## ▼ Vulnerability Instance

Entity	10.10.16.101	External reference	N/A
Location	10.10.16.101	Total exposure	N/A
Reported by	eEyeRetina	Secondary source	N/A
First detected	2015-09-17	Issue id	N/A
Last detected	2015-09-17	Test url	N/A
Fixed No		File name	N/A
Fixed date	N/A	Line number	N/A
Severity for this entity	High	Discovery method	N/A
Risk for this entity	High	Virtual	No
Resolution status	Unresolved	Exception Status	N/A
Comments	N/A	Exception Current Stage	N/A
Include in report	Yes		
Author	N/A		
CVSS Base Score	10.0		

## ▼ 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

**i** You can decide to always ignore this vulnerability for all entities by marking it not applicable.

Applicable Yes

*The Description of an Entity Vulnerability.*

## Contextual Reports of Entities (parent)

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

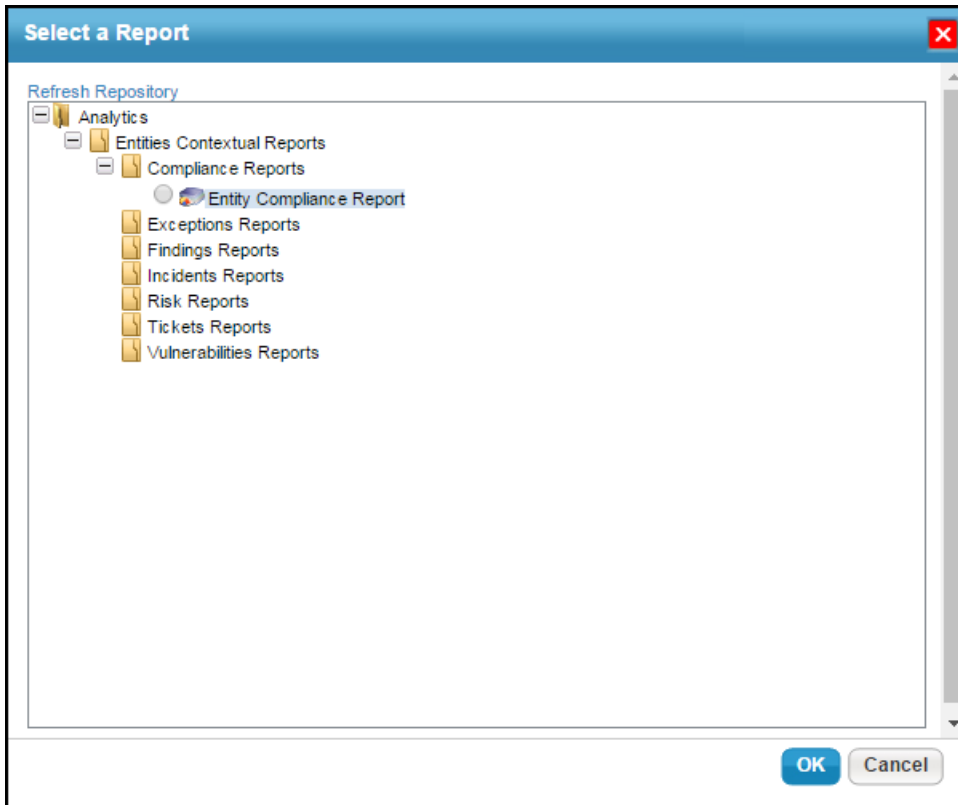
1. Open the Entities page.
2. Select the required entities, then click **More Actions > Run Contextual Report**.

Name	btype	Criticality	Owner	Description
10.1.10.11		High		N/A
10.10.16.101		High		N/A
10.10.16.102		High		N/A
10.10.16.106		High		N/A
10.10.16.109	Computer	Low		N/A
10.10.16.2	Computer	High	Host	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.





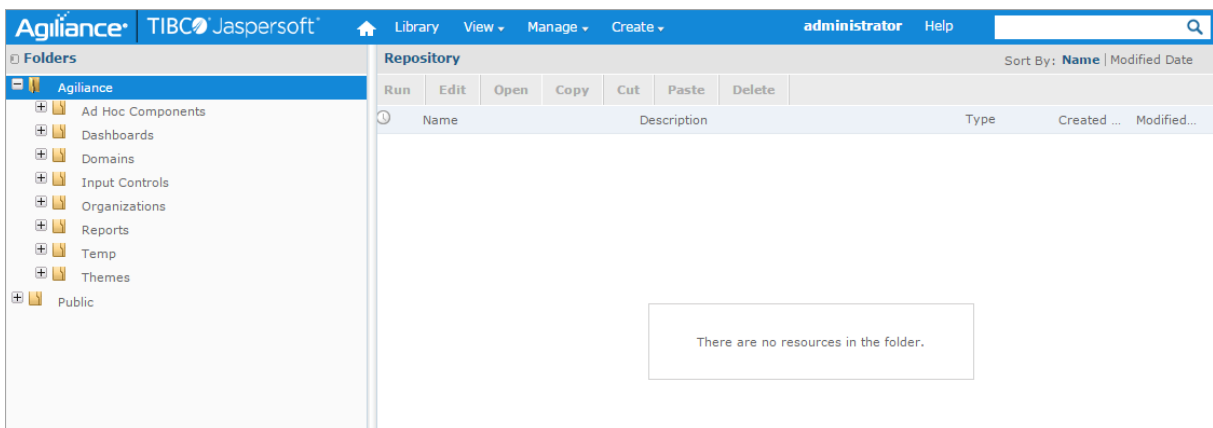
*Selecting a report in the Select a Report dialog.*

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

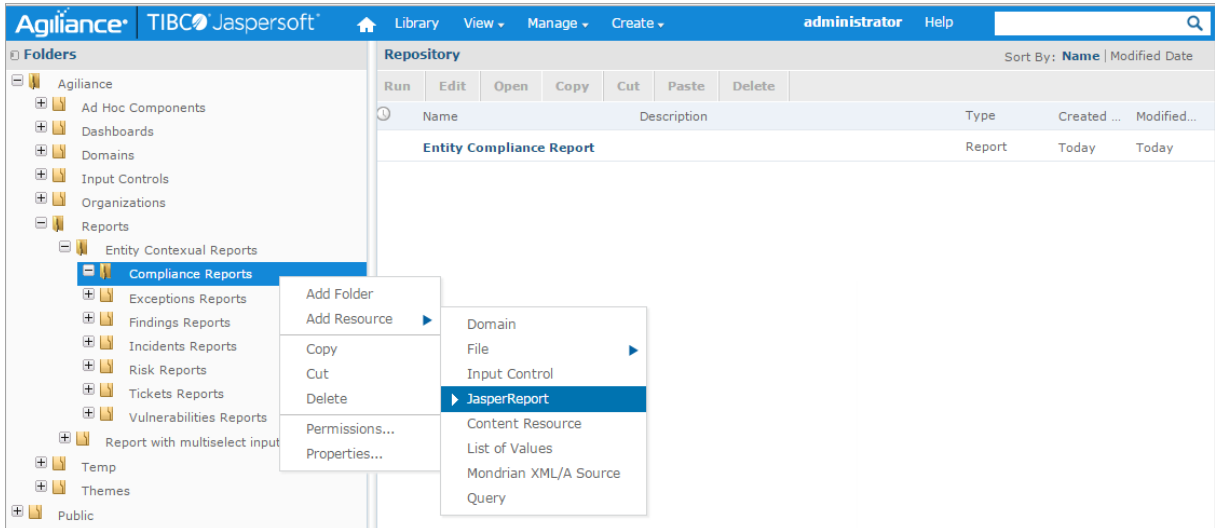
### To create a contextual report to report against entities:

1. Click **Analytics > R7 charts** to open the JasperReports Server page.
2. Click **View > Repository**.

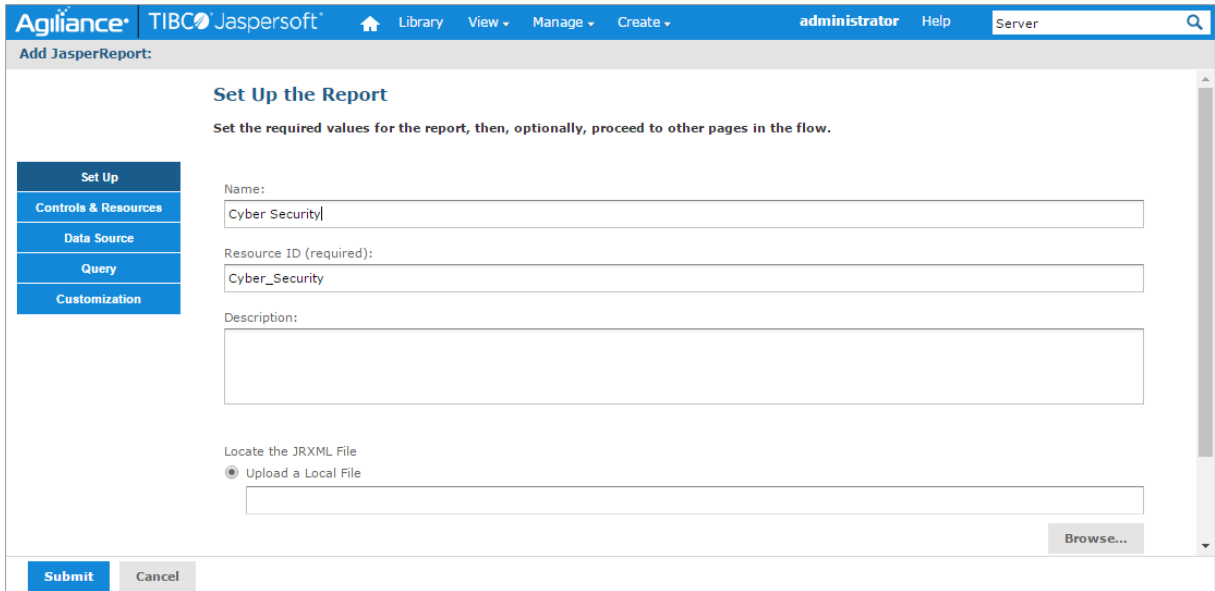


*The Repository page.*

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**.



5. Follow the onscreen instructions to create a new report.



After you have created a report, you can generate this contextual report from the **Select a Report** pop-up.

## About 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**.

A screenshot of a web form titled "Add Entity Collections to your Organization". The form contains the following elements:

- Introductory text: "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."
- Section header: "Please select how you would like to add new Entity Collection:"
- Radio button: "Create an Entity Collection" (selected).
- Text: "Enter the following information for the entity collection you wish to create. The wizard will guide you to create an entity collection."
- Form fields:
  - "Name\*" text input field containing "GF\_Payment\_System".
  - "Description" text area.
  - "Entity Collection Type\*" dropdown menu with "Define an entry" selected and "PaymentSystems" listed below it.
  - "Primary Owner\*" dropdown menu with a plus sign button next to it.
- Radio button: "Import entity collections from a file" (unselected).
- "Next" button at the bottom right.

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

1. Organization

**Step 1: Select the organizational unit of the entity collection** Skip this option \* = required if the group is undefined.

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

Available Hierarchies

1-3 of 3

Filter by - Show all - ▾ Refresh

<input type="checkbox"/> Name	Path
<input type="checkbox"/> Datacenter	/Datacenter
<input type="checkbox"/> DNB Group	/DNB Group
<input type="checkbox"/> HQ	/HQ

Selected Hierarchies

>>
<<

Cancel
< Back
Next >

*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
✕

<b>1. Organization</b> <b>2. Address</b> <b>3. Classification</b> <b>4. Ownership</b> <b>5. Entities</b>	<p><b>Step 2: Optionally, enter the geographic location of the entity collection.</b> * = required</p> <p style="background-color: #FFF9C4; padding: 5px;">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.</p> <div style="border: 1px solid #ccc; padding: 10px;"> <p>Primary Address</p> <p>Location  <input type="text" value="Select a location"/></p> <p>Address 1  <input type="text"/></p> <p>Address 2  <input type="text"/></p> <p>City  <input type="text"/></p> <p>State / Province  <input type="text"/></p> <p>Zip Code / Postal Code  <input type="text"/></p> <p>Country  <input type="text"/></p> <p>Region  <input type="text"/></p> <p>Building  <input type="text"/></p> <p>Floor  <input type="text"/></p> </div>
<input type="button" value="Cancel"/>	<input type="button" value=" &lt; Back"/> <input style="background-color: #0070C0; color: white;" type="button" value=" Next &gt;"/>

*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

Internal or external

Cancel
< Back
Next >

*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.

Create an Entity Collection
✕

1. Organization

2. Address

3. Classification

4. Ownership

5. Entities

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:

Filter by

<input type="checkbox"/> Name	<input type="checkbox"/> Type	Ownership Type
<span style="font-size: 1.2em; color: #0070C0; font-weight: bold;">i</span> 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**

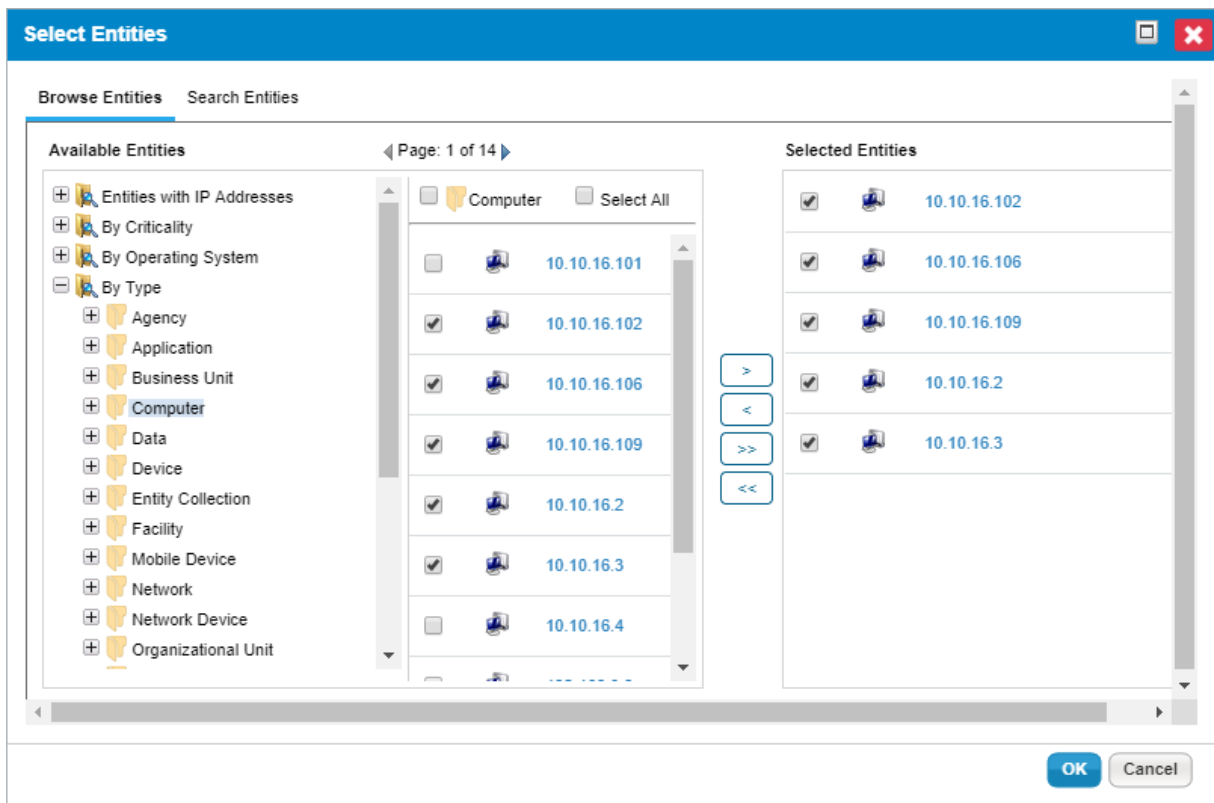
Filter by - Show all -

<input type="checkbox"/>	Name	Type	Subtype	Criticality	Owner	Description	Dynamic Groups
<div style="display: flex; align-items: center;"> <span style="font-size: 1.2em; margin-right: 5px;">i</span> <span>No Entities found.</span> </div>							

*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.

## About Entity Collection Details

Unlike an entity, the tabs in entity collection details do not change. When you create an entity collection, it's created as 'entity collection' type entity in RiskVision . As a result, tabs, such as General, Assessments, 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 the Remove option to remove entities that are a part of dynamic group or entity collection and choose Remove Dynamic Groups from the More Actions dropdown list to remove a dynamic group.

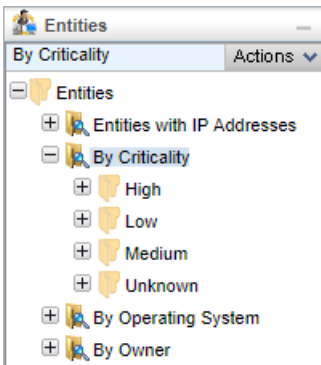
## About Dynamic Groups

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: 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 the 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 users and 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 (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).

## Group Entity 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.

## Group 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 System Details > Application > Version Number attribute.
	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 date of the General > Maintenance > Installation date.
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

Group by	Parameter	Details
	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.
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



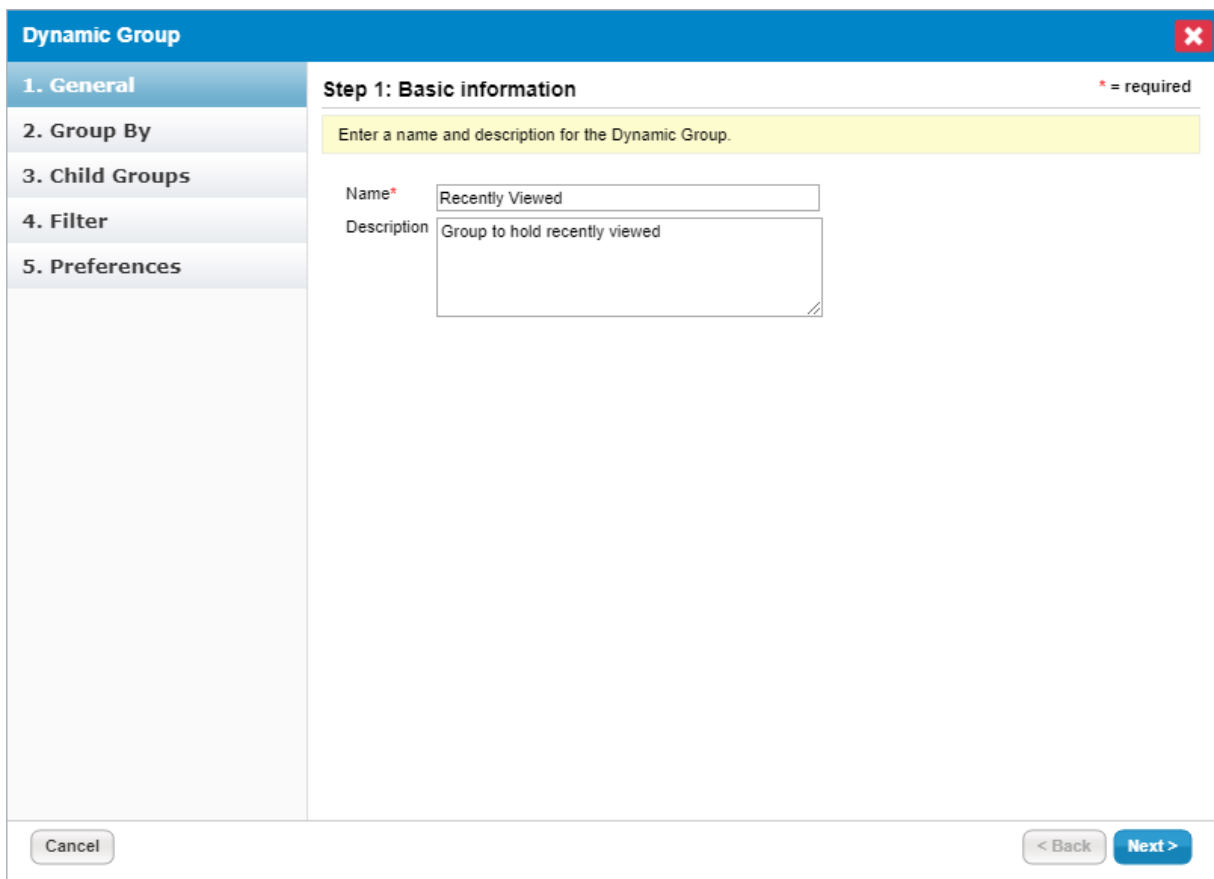
Group by	Parameter	Creates a group description. See parameter
		Vulnerability > Vulnerability List > Vulnerability Details > General > Vulnerability.
	Likelihood	Creates a group for each likelihood.
	Severity	Creates a group for each severity level.
	Source	Creates a group for each vulnerability author 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**.



The screenshot shows the 'Dynamic Group' wizard interface. The title bar is blue with the text 'Dynamic Group' and a red close button. On the left is a vertical navigation pane with five items: '1. General' (selected), '2. Group By', '3. Child Groups', '4. Filter', and '5. Preferences'. The main area is titled 'Step 1: Basic information' with a red asterisk and '= required' to its right. Below the title is a yellow instruction bar: 'Enter a name and description for the Dynamic Group.' There are two input fields: 'Name\*' with the text 'Recently Viewed' and 'Description' with the text 'Group to hold recently viewed'. At the bottom are three buttons: 'Cancel', '< Back', and 'Next >'.

*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.

**Dynamic Group**
✕

**1. General**

**2. Group By**

**3. Child Groups**

**4. Filter**

**5. Preferences**

**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 ▼

Cancel
< Back
Next >

*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.

**Dynamic Group**
✕

**1. General**

**2. Group By**

**3. Child Groups**

**4. Filter**

**5. Preferences**

**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
<div style="background-color: #e1f5fe; padding: 5px; display: flex; align-items: center;"> <span style="font-size: 1.2em; margin-right: 5px;">i</span> <span>No folders have been created</span> </div>

*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](#).

### Dynamic Group ✕

- 1. General
- 2. Group By
- 3. Child Groups
- 4. Filter
- 5. Preferences

#### 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.

Available Filters [\[New Filter\]](#)

- Filter
  - My Filters
  - + Shared Filters

Selected Filter  
No filter selected

Cancel< BackNext >

Step 4 of the Dynamic Group wizard.

10. Click **Next**.
11. Select the folder and dynamic group settings, then click **Finish**.

**Dynamic Group**
✕

**1. General**

**2. Group By**

**3. Child Groups**

**4. Filter**

**5. Preferences**

**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

Cancel
< Back
Finish

*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.

## Set 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 will display on the **Group Entities** page.

## Set Folder and Grouping Preferences

Folder preferences control how dynamic and child groups display in the **Entities** tree and **Program Wizard Entity** selection tree.

**Dynamic Group**
✕

**1. General**

**2. Group By**

**3. Child Groups**

**4. Filter**

**5. Preferences**

**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

Cancel
< Back
Finish

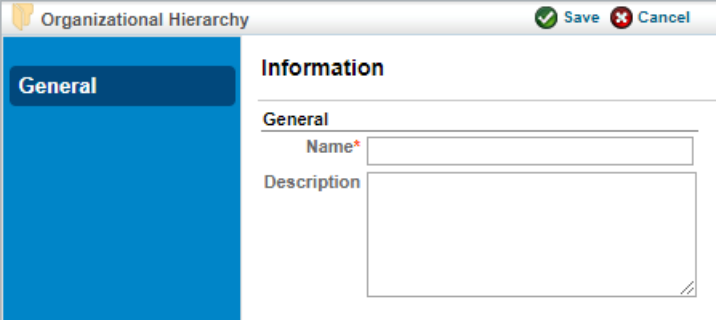
*The folder and grouping preferences in the Dynamic Group wizard.*

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.



## Organizational Hierarchy Overview

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 screenshot shows a window titled "Organizational Hierarchy" with a "Save" button (green checkmark) and a "Cancel" button (red X). On the left is a blue sidebar with a "General" tab selected. The main area is titled "Information" and contains a "General" section with two input fields: "Name\*" (a single-line text box) and "Description" (a multi-line text area).

*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** dropdown menu that appears when you select a node, or by opening a node's details page and going to the **General** tab > **Actions**.

### To add an organization hierarchy node

1. Open the **Entities** menu, then click **Group Definitions**.
2. Click a node in the **Organization Hierarchy** tree. Any child nodes that are available appear in the child hierarchies section.
3. **Optional:** To move all the child nodes of a node, open the organizational hierarchy tree. Click **Actions**, then click **Cut**. Select the node you want to move the nodes to, then click **Paste** from the **Actions** dropdown.
4. **Optional:** To move a child node, select the node. Click **Actions**, then click **Move To**, and then click **Go**. Select a hierarchy and click **OK**.

### To delete an organization hierarchy node

1. Open the **Entities** menu, then click **Group Definitions**.
2. Click a node in the **Organization Hierarchy** tree.
3. Perform one of the following actions:
  - To delete a root node, select a node in the organization hierarchy tree. Click **Actions**, then click **Delete**.
  - To delete a child node, select a node. Click **Actions**, then click **Delete**. Click **Go** a This provides the ability to retain specific child nodes if you don't want to delete the complete node from the organization hierarchy tree.

### To copy and paste an organization hierarchy node

1. Click **Group Definitions** on the **Entities** or **Vendors** menu.
2. Click a node in the **Organization Hierarchy** tree. Any child nodes that are available appear in the child hierarchies section.
3. Perform one of the following actions:
  - To copy all the child nodes of a particular node, open the organizational hierarchy tree. Click **Actions**, then click **Copy**. Select a desired node to which you want to copy move the node. Click **Actions**, then click **Paste**.
  - To copy a child node, select the node. Click **Actions**, then click **Copy To**, and then click **Go**. Select a hierarchy, then click **OK**.

### To move an organization hierarchy node

1. Click **Group Definitions** on the **Entities** or **Vendors** menu.
2. Select a node in the **Organization Hierarchy** tree. Any child nodes that are available will appear in the child hierarchies section.
3. Perform one of the following actions:
  - To move all the child nodes of a node, click **Actions**, then click **Cut**. Select a node to which you want to move the node. Click **Actions**, then click **Paste**.
  - To move a child node, select the node to open its details. Click **Actions**, then click **Move To**, and then click **Go**. Select a hierarchy and click **OK**.

## Enable the Organization Hierarchy Selection

When you create a node under the organization hierarchy tree, the nodes are not visible in the entity wizard or for assigning 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.

## Define 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.



<input type="checkbox"/>	Organization Root	▲ Path	Description
<input type="checkbox"/>	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 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.

## Vulnerabilities

Vulnerabilities represent a potential hole in your system that can be exploited and used for malicious purposes. Feeds, such as the National Vulnerability Database (NVD) or iDefense, report new vulnerability definitions on a regular basis. Vulnerability definitions are usually mapped to descriptions in the Common Vulnerabilities Enumeration (CVE), but sometimes definitions arrive without CVE identifiers as "early warnings."

Vulnerabilities that apply to your specific entities and technologies are considered actual, rather than inferred, vulnerabilities. When you acknowledge a new vulnerability definition as applying to your system, you will be the owner of the vulnerability instance. You can assign a different owner as needed.

The Threat Management menu includes predefined vulnerability reports, such as:

- [My Vulnerabilities](#)
- [Vulnerabilities from Scanners or Users](#)
- [Inferred Vulnerabilities](#)
- [Scanner & Inferred Vulnerabilities](#) (includes user-entered vulnerabilities)
- [Exploits](#)
- [All Vulnerabilities](#)
- [Recent Vulnerabilities](#)
- [Recent Vulnerabilities of Interest](#)

In addition, the **Vulnerabilities Dashboard** provides an overview of new vulnerabilities and their resolution.

## My Vulnerabilities

The **My Vulnerabilities** page is a grid available on the **Vulnerabilities** menu within the Threat and Vulnerability Manager. This grid displays vulnerabilities for which you are the owner. To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).

## Vulnerabilities from Scanners or Users

The **Vulnerabilities from Scanners or Users** page is a grid available on the **Vulnerabilities** menu within the Threat and Vulnerability Manager. It's only visible if you have the Threats and Vulnerabilities View permission. This grid contains vulnerabilities reported by scanners as well as users. The vulnerabilities reported by users appear in this grid only when a vulnerability affects an entity. To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).



## Inferred Vulnerabilities

The **Inferred Vulnerabilities** page is a grid available on the **Vulnerabilities** menu. An inferred vulnerability is created when RiskVision correlates an existing National Vulnerability Database vulnerability definition with an entity within your system. The vulnerabilities are inferred because they have not been actually discovered by a scanner. Vulnerabilities can also be inferred from iDefense data.

To view inferred vulnerabilities, you must have the Threats and Vulnerabilities View permission. The **Inferred Vulnerabilities** grid contains vulnerabilities that are implicitly associated with entities in your organization.

To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).

## Scanner & Inferred Vulnerabilities

The **Scanners and Inferred Vulnerabilities** page is a grid available on the **Vulnerabilities** menu within the Threat and Vulnerability Manager. It's only visible to users with the Threats and Vulnerabilities View permission. This grid contains vulnerabilities reported by all of your scanners and those that are implicitly associated with entities.

To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).

## All Vulnerabilities

The **All Vulnerabilities** page is a grid available on the **Vulnerabilities** menu within the Threat and Vulnerability Manager. This grid is visible only if you have the Threats and Vulnerabilities View permission. There are three sources of vulnerabilities in this grid:

- Vulnerabilities published by the NVD, which are added when the product is installed;
- Vulnerabilities imported by scanners; and
- Vulnerabilities added by users.

This grid displays vulnerabilities that are published in the year 2013, by default. To view past vulnerabilities, select an year ranging from 1988 to 2013 in the **Show** dropdown list in the upper right-hand portion of the page.

To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).

## Recent Vulnerabilities

The **Recent Vulnerabilities** page is a grid available on the **Vulnerabilities** menu within the Threat and Vulnerability Manager. By default, this grid displays vulnerabilities that are imported, created manually, and modified in the last month. You can use the **Show** dropdown list to view vulnerabilities up to the last year. This grid is visible only if you have the Threats and Vulnerabilities View permission.

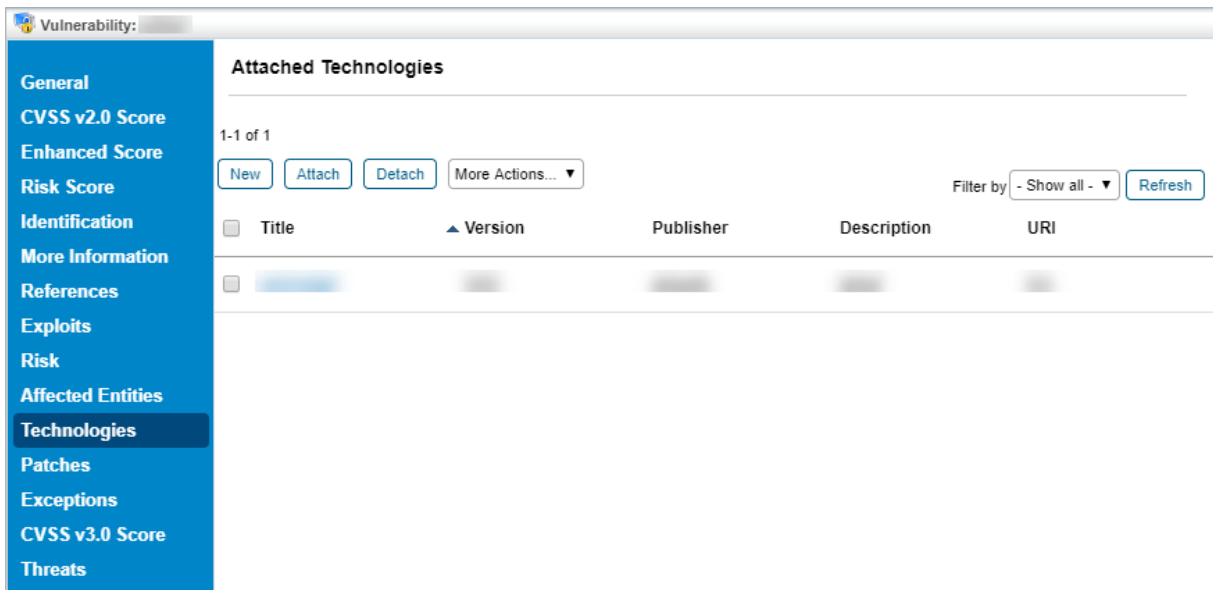
To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).

## Recent Vulnerabilities of Interest

Scanning entities regularly will ensure that all configurations and patches are up to date. Some technologies have a high number of vulnerabilities, with new ones reported frequently to the NVD. You can mark a technology 'Of Interest' to track vulnerabilities that are imported through scanners or data feeds. Marking a technology 'Of Interest' will help you understand how often a technology has been affected by threats in the past. In the Threat and Vulnerability manager, the **Recent Vulnerabilities of Interest** report lists vulnerabilities that were modified in the NVD over a period of one year.

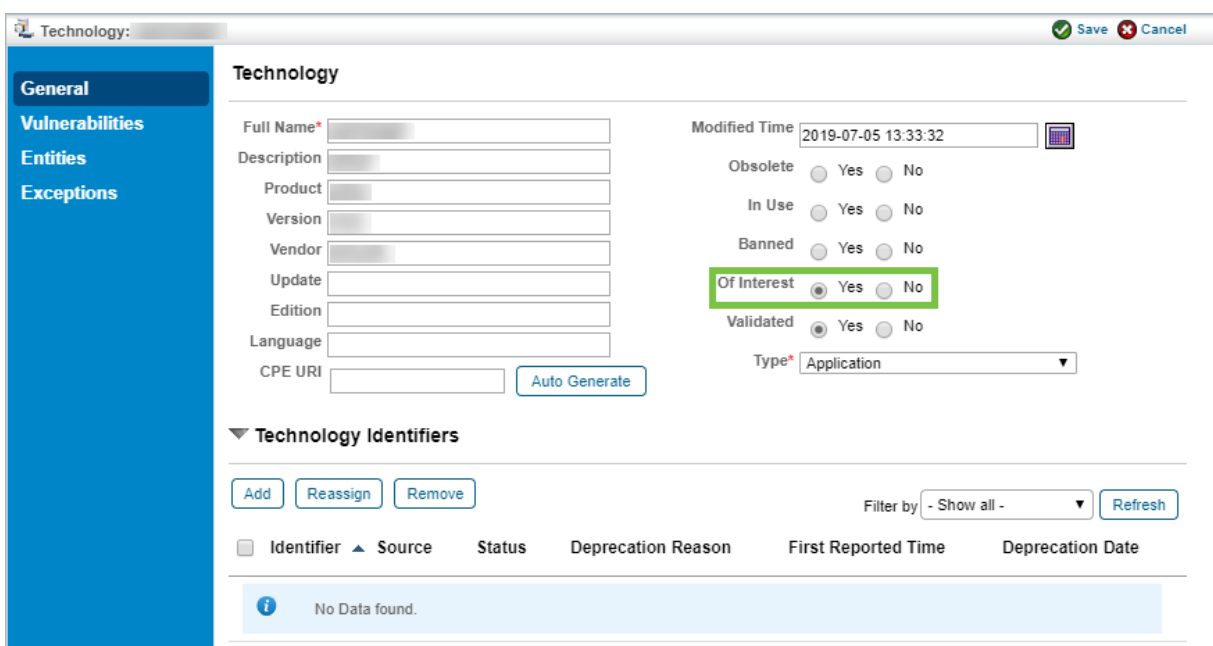
### To flag a vulnerability 'of interest':

1. Go to **Vulnerabilities > My Vulnerabilities**.
2. Select a specific vulnerability, then click **Details**.
3. Go to the **Technologies** page, then click the title of the attached technology.



The Technologies page.

4. Click the **General** tab of the technology details page.
5. Click **Edit**, then click **Yes** next to **Of Interest**.



The Edit Technology page.

6. Click **Save**.

Go to **Vulnerabilities > Recent Vulnerabilities of Interest** to view vulnerabilities that are marked **Of Interest**. To view recent or historical vulnerabilities related to a technology, click **Show**, then select a time frame. Click **Refresh**.

If the Recent Vulnerabilities of Interest report does not provide any results, we recommend running the Update Vulnerability Summary job from the **More Actions** dropdown list.

OR

In the **Recent Vulnerabilities of Interest** page, select vulnerabilities for which the updated report is required. Click **More Actions > Update Vulnerability Summary**.

To view the actions available in this grid, see [Performing Actions in Vulnerabilities Grids](#).

## Perform Actions in Vulnerabilities Grids

Within the vulnerabilities grids, you can create, update, delete, and use action options. The table below lists the vulnerability actions available when you visit the grids on the Vulnerability menu, as well as the required user permissions.

Action	Grid	Permission
Create	My Vulnerabilities, All Vulnerabilities, Recent Vulnerabilities, Recent Vulnerabilities of Interest	Threats and Vulnerabilities Create
Update	My Vulnerabilities, Vulnerabilities from Scanners or Users, Scanner & Inferred Vulnerabilities, All Vulnerabilities, Inferred Vulnerabilities, Recent Vulnerabilities, Recent Vulnerabilities of Interest	Threats and Vulnerabilities Update
Delete	Vulnerabilities from Scanners or Users, All Vulnerabilities, Inferred Vulnerabilities, Recent Vulnerabilities, Recent Vulnerabilities of Interest	Threats and Vulnerabilities Delete
More Actions  To learn about the action options, see <a href="#">Using More Actions in Vulnerabilities Grids</a> .	Vulnerabilities from Scanners or Users, My Vulnerabilities, Inferred Vulnerabilities, All Vulnerabilities, Scanner & Inferred Vulnerabilities, Recent Vulnerabilities, Recent Vulnerabilities of Interest	Threats and Vulnerabilities Manage

## Use More Actions in Vulnerabilities Grids

This section describes the vulnerability actions available in the **More Actions** dropdown list for vulnerability grids. Vulnerability actions can be performed simultaneously on multiple vulnerabilities. They can be used to automate actions, such as Acknowledge Vulnerability or Assign Vulnerability Owner, to kick-off the remediation process as soon as the vulnerabilities are reported.

The following table summarizes different vulnerability actions:

Action	Description
Assign Vulnerability Owner	Assign an owner manually to a vulnerability when they are reported.
Assign Entities	Assign more entities to a vulnerability if you believe that a vulnerability is going to affect multiple entities.
Assign Vulnerability	All reported vulnerabilities must be acknowledged before initiating the remediation process. If scanner results are imported after you acknowledge vulnerabilities, the status is automatically changed to as "Updated After Acknowledged" for those vulnerabilities instances which the scanner had reported earlier. The "Updated After Acknowledged" status will help you understand whether any new technologies are affecting the acknowledged vulnerabilities.
Unacknowledge Vulnerability	Unacknowledge a vulnerability if you have proper evidence to show that a reported vulnerability does not apply
Update Vulnerability Summary	Perform this action to update the vulnerabilities grid with the latest import results.



## Manage Scan Results

After you import scan results into RiskVision user interface, you'll need to manage the newly discovered entities and create tickets to resolve related vulnerabilities. For information on creating tickets manually, see [Linking Tickets Manually](#). The manual ticket creation process is available in Compliance Manager, Enterprise Risk Manager, and Vendor Risk Manager, and is ideal for enterprises managing a small number of vulnerabilities. For large enterprises with multiple entities and large amounts of data, we recommend using the ticket automation feature in RiskVision Threat and Vulnerability Manager. This feature allows you to prioritize the vulnerability response based on the CVSS score.

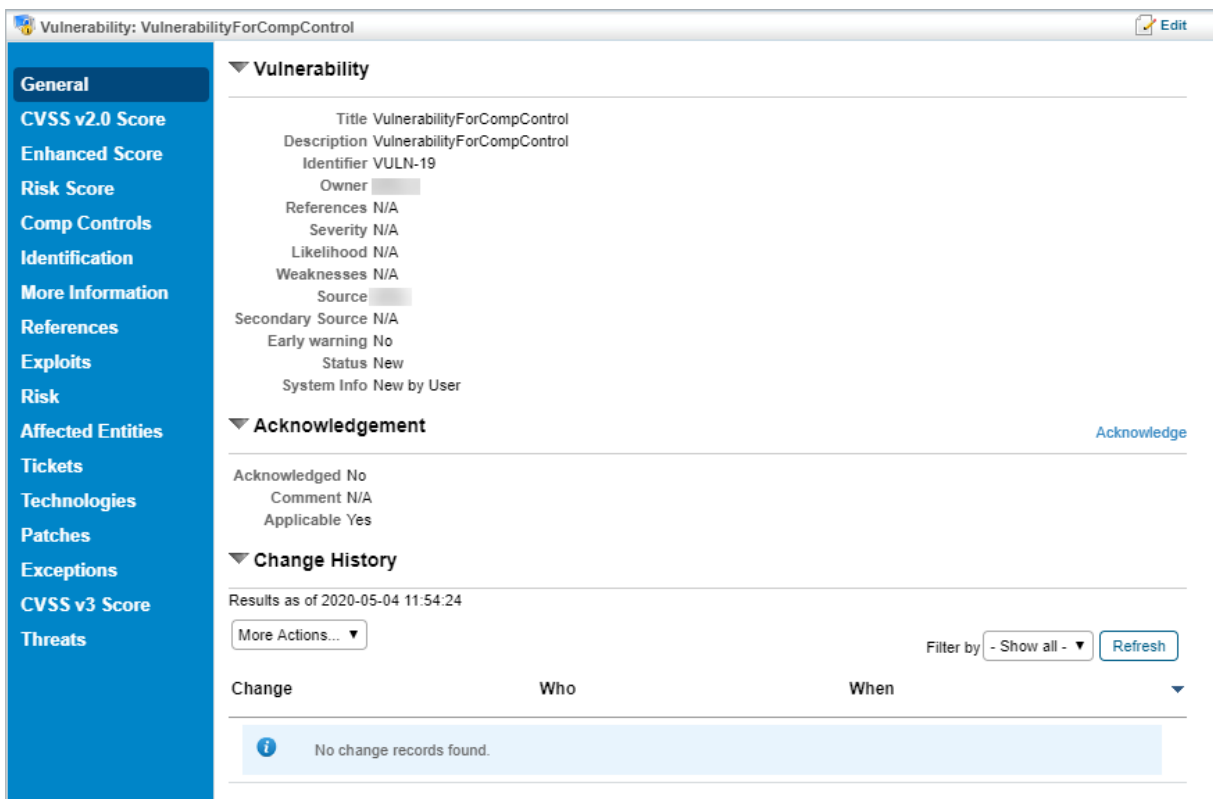
## Vulnerability Details Overview

The **Vulnerability Details** page contains assorted information to help you manage your remediation effort. This page contains a series of tabs that are used to:

- Acknowledge vulnerabilities to mark them as applicable or duplicate;
- Provide substantiation to remediate, examine, or work around vulnerabilities; and
- Create tickets to resolve related vulnerability instances. Vulnerability instances represent the individual occurrences of the vulnerability on each affected entity.

### To expand a vulnerability:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities**, **Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Select a vulnerability.



*The Vulnerability Details page.*

To update the information available on the various tabs of the **Vulnerability Details** page, you must have the Threats and Vulnerabilities View and Threats and Vulnerabilities Update permissions. The following table summarizes the different tabs available in the **Vulnerability Details** page.

TAB	DESCRIPTION
General	Displays information, such as severity, likelihood, and source. Allows users to assign an owner and status to the vulnerability.
CVSS v2.0 Score	The Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of IT vulnerabilities. RiskVision displays each vulnerability's CVSS score in detail, breaking down the base score, impact, and

	exploitability sub-scores, as well as the temporal and environmental scores.
CVSS v3 Score	CVSS v3 will provide a better indication of the relative severity of vulnerabilities, because it better reflects the true impact of the vulnerability being rated in software components, such as database servers or middleware.
Enhanced Score	Displays the Enhanced Score of a vulnerability. For scanner-reported vulnerabilities, it is not uncommon that the vulnerability will map to multiple CVE's. When this happens, the Enhanced Score tab will have several lines, one for each mapped CVE, and the Enhanced Score will be the sum of the Enhanced Scores for each of the mapped CVE's.
Risk Score	<p>Displays all of the input vectors used to calculate the Entity Criticality Factor in columns, with their appropriate values. Also displays the Vulnerability Risk Factor and resultant Risk Score.</p> <p>Risk Scores are calculated at the following levels:</p> <ul style="list-style-type: none"> <li>● Risk Score of vulnerability instance</li> <li>● Risk Score of vulnerability definition</li> <li>● Risk Score of an entity</li> </ul> <p>This tab uses all possible groupings of the Risk Score formula that use Entity Criticality to calculate the Entity Criticality Factor portion of the Current Risk Score.</p>
Comp Controls	Displays all of the vulnerability compensating controls attached to a vulnerability. Allows users to add existing controls to a vulnerability and to edit the detection and protection values of a control.
Identification	Provides vulnerability IDs that have been identified together for a vulnerability, such as when you're using multiple scanners.
More Information	Shows attached information using the rich text editor interface to provide more information related to the vulnerability, such as how it affects your organization and any available workarounds.
References	Shows mapped vulnerabilities to organization and industry-defined controls.
Exploits	Displays exploits linked to vulnerabilities.
Risks	Displays risks associated with vulnerabilities in your environment.
	Shows the entity groups that have technology affected by the vulnerability. These groupings are defined in Threat

Affected Entities	<p>Management Preferences. To view specific entities, select one or more groups and click View Entities. You can create a ticket or add to an existing ticket for entities collections on this tab.</p> <p>If the user has a filter preventing him or her from viewing all of the individual entities attached to an entity group, he or she will see the following message at the top of the screen:</p> <ul style="list-style-type: none"> <li>You are not able to see all the entities on this page because you are restricted from seeing [number of hidden entities] entities.</li> </ul>
Tickets	Displays tickets associated with a specific vulnerability.
Technologies	Lists the technologies associated with the vulnerability. Use this tab to create and manage technologies.
Patches	Once vulnerabilities have been disseminated to vulnerability administrators, the vulnerability instances are fixed with a patch, usually provided by the vendor. Connectors such as the IBM Tivoli Endpoint Manager Connector can provide information about available patches.
Exceptions	Shows exceptions associated with a specific vulnerability. Users can also create new exceptions and add them to the vulnerability.
Threats	Lists the threats associated with this vulnerability.

## About the More Information Tab

The **More Information** tab supports multiple links for sections, such as Diagnosis, Exploits, Workarounds, and Remediation.

### To add details on the More Information tab of a vulnerability:

1. Click any vulnerability.
2. Click the **More Information** tab.

Vulnerability: CVE-2008-0082

**General**  
CVSS v2.0 Score  
Enhanced Score  
Risk Score  
Identification  
**More Information**  
References  
Exploits  
Risk  
Affected Entities  
Tickets  
Technologies  
Patches  
Exceptions  
CVSS v3.0 Score  
Threats

**Diagnosis**

New Edit Delete Filter by - Show all - Refresh

Name	Data	Links
No Diagnosis found.		

**Exploits**

New Edit Delete Filter by - Show all - Refresh

Name	Data	Links
No Exploit found.		

**Workarounds**

New Edit Delete Filter by - Show all - Refresh

Name	Data	Links
No Workaround found.		

**Remediation**

New Edit Delete Filter by - Show all - Refresh

Name	Data	Links
No Remediation found.		

*The More Information screen.*

3. Click **New** under each section to open the **New Vulnerability Data** window.

*The New Vulnerability Data window.*

4. Enter the name, data, and add multiple links separated by a comma, then click **OK**.

If you want to add multiple links in other sections, repeat steps 4 to 6. Multiple links will be added and the links are active. These links will allow you to browse the respective URL.

**When multiple links are reported from a connector, the links will be displayed properly.**

## Link Tickets to Vulnerabilities

You can create a ticket manually or automatically to establish a single link between a vulnerability and an entity group or a one-to-one link between a vulnerability and an entity. A ticket that is linked to a vulnerability will help you track the affected entities and remediation procedures to fix a vulnerability.

## Link Tickets Automatically

You can automatically create tickets for vulnerabilities reported by scanners. In addition, a criteria can be set to create tickets based on vulnerabilities' CVSS Score or when there is no patch associated with the vulnerability for affected entities. Tickets created automatically are applied only to vulnerabilities associated with an entity group.

To create tickets separately for each entity, see [Linking Tickets Manually](#).

### To create tickets automatically:

1. Open RiskVision Threat and Vulnerability Manager.
2. Click **Threat Management Preferences** on the **Configuration** menu.
3. Click **Edit** in the upper right-hand corner of the screen.
4. Click **Automatically create tickets** to create tickets automatically when vulnerabilities are reported using scanners.

**Ticket Management**

When vulnerabilities are updated

Automatically create tickets

Create ticket only if no patch is available for the affected entity

CVSS Score >=

Acknowledge the vulnerability when tickets are automatically created

and assign the vulnerability to

*The Ticket Management settings.*

5. **Optional:**
  - **Create ticket only if no patch is available for the affected entity** Automatically create tickets when the reported vulnerability does not contain a patch for affected entities.
  - **CVSS Score>=:** Automatically create tickets when the reported vulnerabilities' CVSS score is greater than or equal to value specified.
  - **Acknowledge the vulnerability when tickets are automatically created** Acknowledge all reported vulnerabilities. Select an owner in the **and assign the vulnerability to** dropdown box.
6. Add the following property to the `.properties` file:

```
com.agilance.job.affectedAssetsNotificationSenderJob.disable=false
```



## Link Tickets Manually

You can create a new ticket and add an existing ticket to a vulnerability. To create a ticket manually, you must have the Ticket Create and Threats and Vulnerabilities View and Manage permissions or View and Update permissions.

Adding an existing ticket and to a vulnerability requires only the View permission.

### To create tickets manually:

1. Open RiskVision Threat and Vulnerability Manager.
2. Click **My Vulnerabilities**, or click any page on the **Vulnerabilities** menu. Click a vulnerability to open.
3. Click the **Affected Entities** tab to view entities that are affected by the vulnerability, then perform the following:
  - To create a new ticket:
    - Select an entity group and click **Create Ticket** to create a single ticket for all affected entities in that group. You can also select multiple entity groups to create a single ticket.
  - To create individual tickets for each entity in a group:
    - Click **View Entities** in the entity group that has more than one entity. Select an entity, then click **Create Ticket**.
  - To add an existing ticket:
    - Select an entity group, then click **Add to existing Ticket**. Select a ticket in the **Select a Ticket** dialog, then click **OK**. You can also select multiple entity groups to add an existing ticket.
    - For entities in a group, click **View Entities** in the entity group row that has more than one affected entity. Select an entity, then click **Add to existing Ticket**. Select a ticket, then click **OK**.

Vulnerability: CVE-2006-4691

**Vulnerable entity groups**

The following entity groups have a technology affected by this vulnerability.

1-1 of 1

[Create Ticket](#) [Add to existing Ticket](#) [Create Exception](#) [Add to existing Exception](#) [View Entities](#) [More Actions...](#)

Filter by: - Show all - [Refresh](#)

<input type="checkbox"/>	OS Name	OS Vendor	OS Version	Owner	Criticality	Risk Level	Total Affected	Scanner Reported	Without Ticket	Without Ticket and Exception	Patch Installed
<input type="checkbox"/>	Windows 2000 Release	N/A	N/A				1	1	1	1	0

*The Affected Entities tab.*

If you automate the ticket creation and vulnerability acknowledgment process, ensure that the Affected Entity Notification Sender system job is not deactivated. This process will create tickets automatically and acknowledges reported vulnerabilities.

## Add Exceptions to Vulnerabilities

You can create or add an existing exception manually to establish a single link between a vulnerability and an entity group or a one-to-one link between a vulnerability and an entity. An exception that is linked to a vulnerability will help you track the affected entities and mitigation procedures to fix a vulnerability.

Existing exceptions can only be added through a vulnerability's **Affected Entities** tab, while new exceptions can also be created in the **Exceptions** tab. To create an exception manually, you must have the Exception View, Request, and Threats and Vulnerabilities View permissions. Adding an existing ticket or exception to a vulnerability requires the View and Request permissions.

### To create an exception in Affected Entities:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities**, **Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Click a vulnerability.

The screenshot shows a web interface for a vulnerability. On the left is a blue sidebar with navigation tabs: General (selected), CVSS v2.0 Score, Enhanced Score, Risk Score, Comp Controls, Identification, More Information, References, Exploits, Risk, Affected Entities, Tickets, Technologies, Patches, Exceptions, CVSS v3 Score, and Threats. The main content area is titled 'Vulnerability: SSL Certificate - Signature Verification Failed Vulnerability' and has an 'Edit' button in the top right. It is divided into three sections: 'Vulnerability' with fields for Title, Description, Identifier, Owner, References, Severity, Likelihood, Weaknesses, Source, Secondary Source, Early warning, Status, and System Info; 'Acknowledgement' with fields for Acknowledged, Comment, and Applicable, and an 'Acknowledge' button; and 'Change History' with a date filter, a 'More Actions...' dropdown, a 'Filter by' dropdown set to 'Show all', and a 'Refresh' button. Below these is a table with columns 'Change', 'Who', and 'When', which is currently empty with a message 'No change records found.'

*The Vulnerability details page.*

4. Click the **Affected Entities** tab.

Vulnerability: SSL Certificate - Signature Verification Failed Vulnerability

**Vulnerable entity groups**

The following entity groups have a technology affected by this vulnerability.

1-6 of 6

Filter by:

<input type="checkbox"/>	OS Name	OS Vendor	OS Version	Owner	Criticality	Risk Score	Total Affected	Scanner Reported	Without Ticket	Without Ticket and Exception	Patch Installed
<input type="checkbox"/>	advanced_core_operating_system	a10networks	2.7.1			30	1	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			9	2	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			21	4	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			30	1	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A	N/A		21	1	1	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			30	2	0	0	0	0

*The Affected Entities tab.*

5. Perform any one of the following actions:

- To create a new exception:
  - Select an entity group and click **Create Exception** to create a single exception for all affected entities in that group. You can also select multiple entity groups to create a single exception.
- To create individual exception for each entity in a group:
  - Click **View Entities** in the entity group that has more than one entity, select an entity, and then click **Create Exception**.
- To add an existing exception
  - Select an entity group, then click **Add to existing Exception**. Select an exception, then click **OK**. You can also select multiple entity groups to add an existing exception.
  - For entities in a group, click **View Entities** in the entity group row that has more than one affected entity. Select an entity, then click **Add to existing Exception**. Select a ticket, then click **OK**.

## To create an exception in Exceptions:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities**, **Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Click a vulnerability.

The screenshot shows the 'Vulnerability' details page. The left sidebar contains navigation tabs: General, CVSS v2.0 Score, Enhanced Score, Risk Score, Comp Controls, Identification, More Information, References, Exploits, Risk, Affected Entities, Tickets, Technologies, Patches, Exceptions, CVSS v3 Score, and Threats. The main content area is titled 'Vulnerability' and includes sections for 'Vulnerability', 'Acknowledgement', and 'Change History'. The 'Vulnerability' section shows details like Title, Description, Identifier, Owner, References, Severity, Likelihood, Weaknesses, Source, Secondary Source, Early warning, Status, and System Info. The 'Acknowledgement' section shows Acknowledged status, Comment, and Applicability. The 'Change History' section shows results as of 2020-06-08 13:01:09 and a table with columns for Change, Who, and When. A message indicates 'No change records found.'

The Vulnerability details page.

4. Click the Exceptions tab.

The screenshot shows the 'Exceptions' tab selected in the sidebar. The main content area is titled 'Exceptions' and shows a table with columns: Exception ID, Exception Name, Global Entity Names, Current Stage, Status, Status Modified By, Requestor, Start, End, and Total Entities. There is one entry with ID EXP00218, Name entity, a green checkmark, Global Entity Names qa103,qa100,qa102,qa101, Current Stage Sign Off, Status Approve1, Status Modified By, Requestor, Start 2020-04-15, End N/A, and Total Entities 4. The sidebar navigation tabs are the same as in the previous screenshot, with 'Exceptions' highlighted.

The Exceptions tab.

5. Click New to create a single exception that will use the selected vulnerability as its vulnerability scope and definition.

Exception Request
✕

1. Basic Details

2. Attach File

### Step 1: Enter Exception Request Information

\* = required

Title\*

Vulnerability Scope Vulnerability Definition(s)

Vulnerability Definition(s) [SSL Certificate - Signature Verification Failed Vulnerability](#)

Entities Scope\*

Reason for Exception

Start Date

End Date

Next Review Date

Cancel
< Back
Next >
Finish

*The Exception Request wizard.*

Users creating an exception from the **Exceptions** tab will not be able to modify the vulnerability scope.

For more information on creating a new exception, see [Create an Exception Request](#). For information on creating an exception from a ticket object, see [Create a Vulnerability Exception on a Ticket](#)

## Vulnerability Compensating Controls on Exceptions

Vulnerability compensating controls can be attached to vulnerability exceptions to help justify the exception request if compensating controls are in place or in the process of being put in place. These compensating controls can be added by users with the Exception Create and Threats and Vulnerabilities View and Manage permissions or View and Update permissions. They can be added and viewed from the vulnerability exception's Information tab.

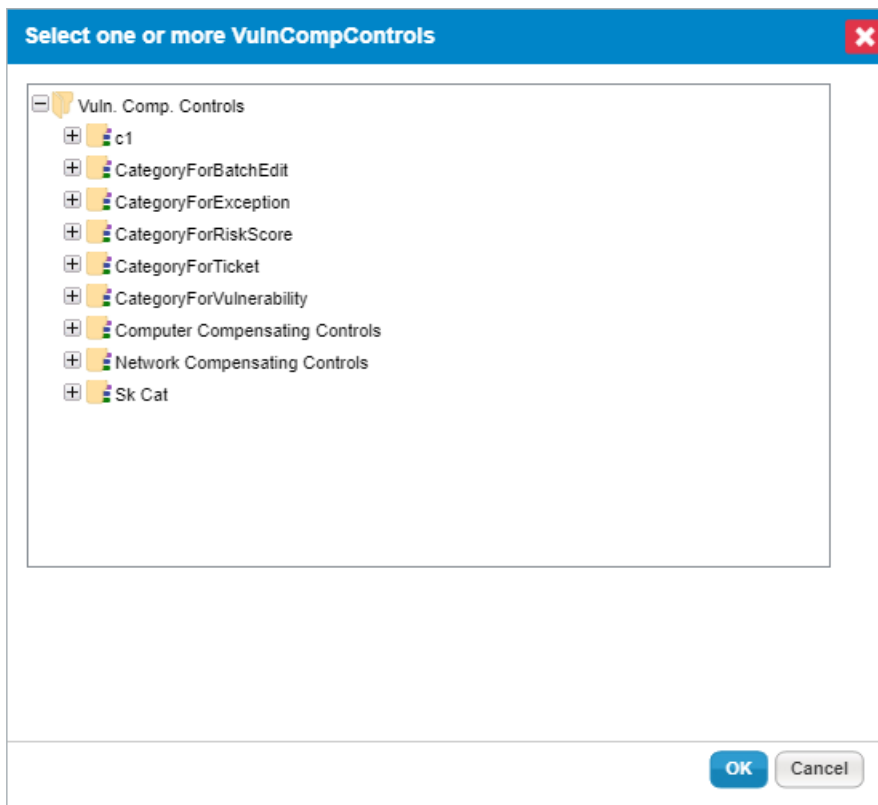
The Information tab.

The **Comp Controls** tab of a vulnerability exception will show the vulnerability compensating controls for each entity the exception is attached to. It will only show vulnerability compensating controls in the **Implemented** or **Pending** status, and is read-only.

The Comp Controls tab.

## To add vulnerability compensating controls:

1. Navigate to **Home > Exception Requests**.
2. Click on the exception you want to add a vulnerability compensating control to to display its **Information** tab.
3. In the **Vulnerability Compensating Control** section, click **Add**.



*The Add Vulnerability Compensating Controls dialogue.*

4. Click + next to any category you wish to open and click the checkbox next to any compensating controls you wish to add to the exception.
5. Click **OK**.

## To delete vulnerability compensating controls:

1. Navigate to **Home > Exception Requests**. Click on the exception you want to delete a vulnerability compensating control from to display its **Information** tab.
2. In the **Vulnerability Compensating Control** section, click the checkbox next to each compensating control you wish to remove from the exception and click **Delete**.
3. Click **OK**.

## Exceptions and Vulnerability Instances

Once a vulnerability instance has been created within a vulnerability definition that an exception has been applied to, the exception will be applied to the instance. Vulnerability instances with an exception applied will have their risk scores reduced to 0 until there are no longer any valid approved exceptions applied to them.

In order for an exception to be applied to a vulnerability instance, it must first be approved. In order for an exception to be approved, the exception must be in a workflow status specified in the **Approved status is set to** field on the [Exception Management Preferences](#) page. While multiple approved exceptions can be attached to a single vulnerability instance, only the one with the latest expiration date will be applied. If there are multiple exceptions with the same expiration date, the one that was created latest will be applied.

When an exception expires, the system will check if there are any further exceptions that can be applied to the instance. The applied exception will be marked with a checkmark in the **Is Applied** column of the vulnerability instance's **Exceptions** tab.


Entity Vulnerability: CVE-2018-11937 on 5432_H										
General CVSS v2.0 Score Enhanced Score Risk Score Identification More Information References Risk Entities CVSS v3 Score Exceptions	Exceptions									
	1-5 of 5									
	More Actions...	Filter by - Show all - Refresh								
	Exception ID	Exception Name	Global	Current Stage	Status	Status Modified By	Requestor	Start	End	Is Applied
	EXP00324	excefrom affecttab	✓	Review	Review			2020-04-24	N/A	
	EXP00325	exceptionfromexcptab	✓	Review	Review			2020-04-24	N/A	
	EXP00335	testcpe	✓	Review	Review			2020-04-24	N/A	
	EXP00361	ehtest1	✓	N/A	Approve	N/A		2020-04-28	N/A	✓
	EXP00363	tab	✓	Review	Review			2020-04-28	N/A	

The Exceptions tab of a vulnerability instance.



## Vulnerability Archiving

### To Enable Automatic Vulnerability Archiving:

1. Go to **Administration>Server Administration**.
2. Select the Configuration module.
3. Click  **Edit**
4. Click **Yes** to enable archiving in the Vulnerabilities Archiving and Tickets Archiving sections.
5. Enter the number of days you want the archival period to last.

<b>Enable Archiving Vulnerabilities</b> <input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Vulnerabilities archival period in days since last updated date</b> <input type="text" value="90"/>

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

## Threats

A threat is an indication of impending danger or the possibility that something bad or harmful could happen. Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging risk to entities that can be used to inform decisions regarding the subject's response to that threat.

RiskVision allows you to import threat intelligence to:

- Assign risk level to threats;
- Attribute incidents to threats;
- Associate entities with threats;
- Mitigate threats by creating tickets against the threats; and
- Prioritize vulnerabilities by auto-correlating threats to vulnerabilities.

These functions will be discussed in more detail later in this section.

The RiskVision user interface features threats grids and pages. The Threats grids are:

- **My Threats:** Threats the logged in user owns.
- **Recent Threats:** Threats from the last month. This can be configured to show different time periods.
- **All Threats:** Shows all threats.
- **Threat Intelligence:** Data imported from threat intelligence services, excluding malware, threat actors, and vulnerability intelligence. Includes periodic reports, such as weekly and monthly updates, and alerts on important topics.
- **Malware:** Shows threat intelligence on malware.
- **Threat Actors:** Shows threat intelligence on threat actors.
- **Vulnerability Reports:** Shows threat intelligence on vulnerabilities

The Threats grids provide the following information:

- **Source:** Name of the threat intelligence service.
- **Identifier:** The ID that the threat intelligence service assigns to the threat information.
- **Title:** Title assigned by the threat intelligence provider.
- **Type:** Type of report assigned by the threat intelligence provider.
- **Status:** Values can be New, Acknowledged, Investigating, Ignore, Mitigating, and Mitigated.
- **Owner:** Owner of the threat.
- **Risk:** Risk level associated with the threat.
- **Published Date:** Date the threat information was first released.
- **Last Updated Date:** Date the threat information was last updated.
- **Entities at Risk:** Count of entities associated with the threat information. Entities attached to a threat's targeted vulnerabilities will appear in this count, as will entities that have been manually assigned to the threat.
- **Targeted Vulnerabilities:** Count of vulnerabilities associated with the same CVE as the threat.
- **Related Incidents:** Incidents that have been linked to the threat. RiskVision automatically correlates threats with vulnerabilities when such correlation is provided by the threat intelligence provider.
- **Related Tickets:** Tickets that have been filed for the threat information.

The following are threat-related properties that can be added to `%AGILIANCE_HOME%\config\agiliance.properties` if needed:

- **com.agiliance.threatObject.fireEye.forceUpdate=true:** This property is set to **false** by default; however, users can force updates to the existing threat data that has already been imported into RiskVision from FireEye by setting it to **true**.
- **com.agiliance.fireeye.requestRange.inDays=90:** This property controls the maximum age for threat intelligence reports retrieved from FireEye. The default and maximum supported value of this property is **90** (days); however, users can reduce the number of days by adjusting this property.

# My Threats

The My Threats page shows threats that belong to the logged in user based on ownership.

The screenshot shows the 'My Threats' page in a web application. At the top, there is a navigation bar with tabs for Home, Entities, Vulnerabilities, Threats (selected), Technologies, Content, Analytics, and Configuration. Below this is a sub-navigation bar with links for My Threats, Recent Threats, All Threats, Threat Intelligence, Malware, Threat Actors, and Vulnerability Reports. The main content area displays a list of threats. The table has 14 columns: Source, Identifier, Title, Threat Type, Status, Owner, Risk, Published Date, Last Updated, Entities At Risk, Targeted Vulnerabilities, Related Incidents, and Related Tickets. Two threats are listed: one with Identifier 2139 and Title FANCY BEAR, and another with Identifier 2135 and Title VICEROY TIGER. Both are of type Actor and status New. The table also includes a filter dropdown set to '- Show all -' and a Refresh button.

Source	Identifier	Title	Threat Type	Status	Owner	Risk	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets
CrowdStrike	2139	FANCY BEAR	Actor	New		N/A	2014-11-03	2019-09-17	17	19	0	0
CrowdStrike	2135	VICEROY TIGER	Actor	New		N/A	2013-05-01	2019-09-17	17	7	0	0

The My Threats page.

The default sorting is by Entity at Risk, then Targeted Vulnerabilities, then Related Incidents, and finally by Risk, in descending order. Each of the columns is sortable in ascending or descending order.

## Recent Threats

The **Recent Threats** page displays a list of threats in order of most to least recent. A threat will not appear on this page if the logged in user has already viewed it.

Home	Entities	Vulnerabilities	Threats	Technologies	Content	Analytics	Configuration						
My Threats	Recent Threats	All Threats	Threat Intelligence	Malware	Threat Actors	Vulnerability Reports							
Threats													
1-100 of 136 Show 100 rows Page 1 2 Go to 1 Go													
<input type="button" value="Details"/> <input type="button" value="Customize"/> <input type="button" value="Save as CSV"/> <input type="button" value="More Actions..."/>													
Show Last One Month Filter by - Show all - Refresh													
<input type="checkbox"/>	Source	Identifier	Title	Threat Type	Status	Owner	Risk	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets
<input type="checkbox"/>	CrowdStrike	65728	CSA-191132 Spam Delivers QakBot via Compromised WordPress Sites	Notice	N/A	N/A	N/A	2019-09-19	2019-09-19	N/A	N/A	N/A	N/A
<input type="checkbox"/>	CrowdStrike	65731	CSA-191133 Western Cryptocurrencies Face Uneven Competition from China's State-Backed Cryptocurrency	Notice	N/A	N/A	N/A	2019-09-19	2019-09-19	N/A	N/A	N/A	N/A
<input type="checkbox"/>	CrowdStrike	65700	CSA-191130 Emerging Brazilian Malware Family Links Two Previously Unrelated Malware Clusters	Notice	N/A	N/A	N/A	2019-09-18	2019-09-18	N/A	N/A	N/A	N/A
<input type="checkbox"/>	CrowdStrike	65697	CSIT-19170 Leaked Materials Link REMIX KITTEN to Iranian Ministry of Intelligence and Security	Tipper	N/A	N/A	N/A	2019-09-18	2019-09-18	N/A	N/A	N/A	N/A
<input type="checkbox"/>	CrowdStrike	65673	CSA-191131 Emotet Spam Continues with English-Language Lures	Notice	N/A	N/A	N/A	2019-09-18	2019-09-18	N/A	N/A	N/A	N/A
<input type="checkbox"/>	CrowdStrike	65672	IMPERIAL KITTEN	Actor	New	N/A	N/A	2019-09-18	2019-09-18	0	0	0	0

*The Recent Threats page.*

By default, all threats created in the last month are displayed, but other time periods can be selected using the **Show** dropdown list in the upper right-hand corner.

# All Threats

The All Threats page shows all the threats.

Threats														
1-100 of 4701 Show 100 rows Page 1 2 3 13 ... 48 Go to 1 Go														
Filter by - Show all - Refresh														
Source	Identifier	Title	Threat Type	Status	Owner	Risk	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets		
<input type="checkbox"/>	CrowdStrike	2139	FANCY BEAR	Actor	New		N/A	2014-11-03	2019-09-17	17	19	0	0	
<input type="checkbox"/>	CrowdStrike	2135	VICEROY TIGER	Actor	New		N/A	2013-05-01	2019-09-17	17	7	0	0	
<input type="checkbox"/>	CrowdStrike	1826	Hammer Panda	Actor	New	N/A	N/A	2015-09-24	2018-04-26	17	5	0	0	
<input type="checkbox"/>	CrowdStrike	1751	ENERGETIC BEAR	Actor	New		N/A	2013-04-19	2018-12-17	16	7	0	0	
<input type="checkbox"/>	CrowdStrike	1759	Pitty Panda	Actor	New	N/A	N/A	2013-04-22	2017-03-29	16	3	0	0	
<input type="checkbox"/>	CrowdStrike	150	CSA-14032 ENERGETIC BEAR Using Document Reader Exploits CVE-2013-2729 and CVE-2014-1761	Notice	New	N/A	N/A	2014-06-18	2017-03-07	16	3	0	0	
<input type="checkbox"/>	CrowdStrike	806	CSIT-14097	Tipper	New	N/A	N/A	2014-10-21	2014-10-21	16	3	0	0	
<input type="checkbox"/>	FireEye	16-00003616	Oracle October 2015 Critical Patch Update Summary - Java SE	Vulnerability	New	N/A	N/A	2016-03-17	N/A	4	26	0	0	
<input type="checkbox"/>	CrowdStrike	1768	VIXEN PANDA	Actor	New		Very High	2013-04-22	2019-02-05	4	12	1	0	
<input type="checkbox"/>	CrowdStrike	1746	Aurora Panda	Actor	New	N/A	N/A	2013-04-15	2018-06-25	4	10	0	0	
<input type="checkbox"/>	FireEye	16-00003558	Oracle July 2015 Critical Patch Update Summary - Java SE	Vulnerability	New	N/A	N/A	2016-03-17	N/A	0	24	0	0	

The All Threats page.

The default sorting is by Entity at Risk, then Targeted Vulnerabilities, then Related Incidents, and then Risk in descending order. Each of the columns is sortable in ascending or descending order.

## Threat Intelligence

The **Threat Intelligence** page is a catch-all to show data imported from threat intelligence services that is not malware, threat actors, or vulnerability intelligence.

Home	Entities	Vulnerabilities	Threats	Technologies	Content	Analytics	Configuration						
My Threats	Recent Threats	All Threats	Threat Intelligence	Malware	Threat Actors	Vulnerability Reports							
Threats													
1-100 of 1592 Show 100 rows Page 1 2 3 13 ... 16 Go to 1 Go													
<input type="button" value="Details"/> <input type="button" value="Customize"/> <input type="button" value="Save as CSV"/> <input type="button" value="More Actions..."/>													
Filter by - Show all - <input type="button" value="Refresh"/>													
<input type="checkbox"/>	Source	Identifier	Title	Report Type	Status	Risk	Owner	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets
<input type="checkbox"/>	CrowdStrike	806	CSIT-14097	Tipper	New	N/A	N/A	2014-10-21	2014-10-21	16	3	0	0
<input type="checkbox"/>	CrowdStrike	45232	CSIT-19005 ThreadKit and VenomKit Comparison of Exploit Builders	Tipper	New	N/A	N/A	2019-01-21	2019-01-21	0	8	0	0
<input type="checkbox"/>	CrowdStrike	8454	CSIT-16131 Badnews Malware Leverages Exploit Documents to Target Asian Victims	Tipper	New	N/A	N/A	2016-11-30	2018-02-05	0	3	0	0
<input type="checkbox"/>	CrowdStrike	12191	CSMR-17004 Global Threat Analysis Cell Monthly Report - April 2017	Periodic Report	New	N/A	N/A	2017-05-17	2018-04-26	0	3	0	0
<input type="checkbox"/>	CrowdStrike	17822	CSWR-18001 GTAC Weekly Wrap-Up: Week of 1/13/2018	Periodic Report	New	N/A	N/A	2018-01-19	2018-03-27	0	3	0	0
<input type="checkbox"/>	CrowdStrike	18375	CSWR-18003 GTAC Weekly Wrap-Up: Week of 1/27/2018	Periodic Report	New	N/A	N/A	2018-02-02	2018-02-02	0	3	0	0
<input type="checkbox"/>	CrowdStrike	53735	CSWR-19014 GTAC Weekly Wrap-Up: Week of 4/6/2019	Periodic Report	New	N/A	N/A	2019-04-12	2019-04-12	0	3	0	0

*The Threat Intelligence page.*

The default sorting is by Entity at Risk, then Targeted Vulnerabilities, then Related Incidents, and then Risk in descending order. Each of the columns is sortable in ascending or descending order.

RiskVision integrates with threat intelligence services through connectors.

# Malware

The Malware page shows threat intelligence on malware.

Home	Entities	Vulnerabilities	Threats	Technologies	Content	Analytics	Configuration					
My Threats	Recent Threats	All Threats	Threat Intelligence	Malware	Threat Actors	Vulnerability Reports						
Threats												
1-18 of 18												
Details		Customize	Save as CSV	More Actions...		Filter by - Show all -		Refresh				
<input type="checkbox"/>	Source	Identifier	Title	Status	Owner	Risk	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets
<input type="checkbox"/>	FireEye	16-00003688	Indicator Report: Domain Generation Algorithm (DGA) Activity Report (Jan. 20 to 27, 2016)	New	N/A	N/A	2016-03-17	N/A	0	0	0	0
<input type="checkbox"/>	FireEye	16-00003706	Indicator Report: KOL BP Network Activity Report (Jan. 28 to Feb. 4, 2016)	New	N/A	N/A	2016-03-17	N/A	0	0	0	0
<input type="checkbox"/>	FireEye	17-00004611	CLONE-Mirai Malware Profile	New	N/A	N/A	2017-05-10	N/A	0	0	0	0
<input type="checkbox"/>	FireEye	16-00003628	Indicator Report: Smoke Loader Activity Report (Nov. 27 to Dec. 4, 2015)	New	N/A	N/A	2016-03-17	N/A	0	0	0	0
<input type="checkbox"/>	FireEye	16-00003698	Freeloader Malware Family	New	N/A	N/A	2016-03-17	N/A	0	0	0	0
<input type="checkbox"/>	FireEye	16-00003546	Punkye POS: Malware Capabilities, Behavior and Communications	New	N/A	N/A	2016-03-17	N/A	0	0	0	0
<input type="checkbox"/>	FireEye	17-00004635	CLONE-Indicator Report: Pony Activity Report (Feb. 22 to March 1, 2017)	New	N/A	N/A	2017-05-10	N/A	0	0	0	0

The Malware page.

The default sorting is by Entity at Risk, then Targeted Vulnerabilities, then Related Incidents, and then Risk in descending order. Each of the columns is sortable in ascending or descending order.

# Threat Actors

The Threat Actors page shows threat intelligence on threat actors.

Threats													
1-100 of 118 Show 100 rows Page 1 2 Go to 1 Go													
Filter by - Show all - Refresh													
Source	Identifier	Title	Status	Owner	Risk	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets		
CrowdStrike	2139	FANCY BEAR	New		N/A	2014-11-03	2019-09-17	17	19	0	0		
CrowdStrike	2135	VICEROY TIGER	New		N/A	2013-05-01	2019-09-17	17	7	0	0		
CrowdStrike	1826	Hammer Panda	New	N/A	N/A	2015-09-24	2018-04-26	17	5	0	0		
CrowdStrike	1751	ENERGETIC BEAR	New		N/A	2013-04-19	2018-12-17	16	7	0	0		
CrowdStrike	1759	Pitty Panda	New	N/A	N/A	2013-04-22	2017-03-29	16	3	0	0		
CrowdStrike	1768	VIXEN PANDA	New		Very High	2013-04-22	2019-02-05	4	12	1	0		
CrowdStrike	1746	Aurora Panda	New	N/A	N/A	2013-04-15	2018-06-25	4	10	0	0		
CrowdStrike	2134	Numbered Panda	New	N/A	N/A	2013-04-21	2017-10-04	0	8	0	0		
CrowdStrike	21976	SHADOW CRANE	New	N/A	N/A	2018-05-10	2018-11-07	0	8	0	0		

The Threat Actors page.

The default sorting is by Entity at Risk, then Targeted Vulnerabilities, then Related Incidents, and then Risk in descending order. Each of the columns is sortable in ascending or descending order.



# Vulnerability Reports

The Vulnerability Reports page shows threat intelligence on vulnerabilities.

Home	Entities	Vulnerabilities	Threats	Technologies	Content	Analytics	Configuration						
My Threats	Recent Threats	All Threats	Threat Intelligence	Malware	Threat Actors	Vulnerability Reports							
Threats													
1-37 of 37 Show 100 rows													
<input type="button" value="Details"/> <input type="button" value="Customize"/> <input type="button" value="Save as CSV"/> <input type="button" value="More Actions..."/>			Filter by - Show all - <input type="button" value="Refresh"/>										
<input type="checkbox"/>	Source	Identifier	Title	Status	Owner	Risk	Published Date	Last Updated	Entities At Risk	Targeted Vulnerabilities	Related Incidents	Related Tickets	
<input type="checkbox"/>	FireEye	16-00003616	<a href="#">Oracle October 2015 Critical Patch Update Summary - Java SE</a>	New	N/A	N/A	2016-03-17	N/A	4	26	0	0	
<input type="checkbox"/>	FireEye	16-00003558	<a href="#">Oracle July 2015 Critical Patch Update Summary - Java SE</a>	New	N/A	N/A	2016-03-17	N/A	0	24	0	0	
<input type="checkbox"/>	FireEye	16-00003652	<a href="#">Mozilla Network Security Services 3.19.2 RSA-MD5 Downgrade Cryptographic Issues Vulnerability</a>	New	N/A	N/A	2016-03-17	N/A	0	4	0	0	
<input type="checkbox"/>	FireEye	16-00003554	<a href="#">Adobe Flash Player 18.0.0.161 Vector Object Handling Heap-based Buffer Overflow Vulnerability</a>	New	N/A	N/A	2016-03-17	N/A	0	2	0	0	
<input type="checkbox"/>	FireEye	16-00003600	<a href="#">ISC BIND 9.10.2-P3 DNSSEC Key Unspecified Vulnerability</a>	New	N/A	N/A	2016-03-17	N/A	0	1	0	0	
<input type="checkbox"/>	FireEye	16-00003564	<a href="#">QEMU 2.4.0 Emulated RTL8139 Network Card Input Validation Vulnerability</a>	New	N/A	N/A	2016-03-17	N/A	0	1	0	0	
<input type="checkbox"/>	FireEye	16-00003536	<a href="#">Linux Kernel 3.19.2 exec.c Race Condition Vulnerability</a>	New	N/A	N/A	2016-03-17	N/A	0	0	0	0	

The Vulnerability Reports page.

The default sorting is by Entities at Risk, then Targeted Vulnerabilities, then Related Incidents, and then Risk in descending order. Each of the columns is sortable in ascending or descending order.

## Threat Object Pages

Click on any threat to open its related detail pages in a new window.

The screenshot shows a web interface for a threat object named 'Hammer Panda'. The page has a blue sidebar on the left with navigation tabs: General (selected), Report, Vulnerabilities, Targeted Entities, Tickets, and Incidents. The main content area is divided into three sections: Threat Information, Mitigation Status, and Change History. The Threat Information section includes fields for Type Actor, Source CrowdStrike, Identifier 1826, Title Hammer Panda, and a detailed Description. The Mitigation Status section shows Status New and Comment N/A. The Change History section shows results as of 2019-09-17 14:45:51, with a 'Save as CSV' button, a 'Filter by' dropdown set to '- Show all -', and a 'Refresh' button. Below this is a table with columns: Changed Attribute, Old Value, New Value, Who, and When. The table currently displays a message: 'No change records found.'

Threat: Hammer Panda Edit

**General**

Report

Vulnerabilities

Targeted Entities

Tickets

Incidents

**Threat Information**

Type Actor

Source CrowdStrike

Identifier 1826

Title Hammer Panda

Description CrowdStrike Intelligence tracks HAMMER PANDA activity back to at least 2013. This adversary has leveraged a range of malicious tools including PlugX, NetTraveler, Saker, and DarkSt malware. Older activity from 2013/2014 appeared to focus on India and related targets while a shift in targeting at the end of 2014 into 2015 showed a clear focus on Russian-related issues. Campaigns appear to focus on defense-related geopolitical issues which indicates primary targeting in the government and defense sectors, but CrowdStrike Intelligence is aware of limited targeting of financial firms as well.

Published 2015-09-24

Date

Last 2018-04-26

Updated

Owner N/A

Severity N/A

Likelihood N/A

Risk N/A

Risk Rating N/A

Exploit N/A

Rating

Exploitation N/A

InTheWild

**Mitigation Status**

Status New

Comment N/A

**Change History**

Results as of 2019-09-17 14:45:51

[Save as CSV](#)

Filter by - Show all - Refresh

Changed Attribute	Old Value	New Value	Who	When
No change records found.				

*A threat object.*

The tabs displayed for the Threats pages are:

- General
- Report
- Vulnerabilities
- Targeted Entities
- Tickets
- Incidents

## General

Threat: Hammer Panda Edit

**General**

Report

Vulnerabilities

Targeted Entities

Tickets

Incidents

**Threat Information**

Type Actor

Source CrowdStrike

Identifier 1826

Title Hammer Panda

Description CrowdStrike Intelligence tracks HAMMER PANDA activity back to at least 2013. This adversary has leveraged a range of malicious tools including PlugX, NetTraveler, Saker, and DarkSt malware. Older activity from 2013/2014 appeared to focus on India and related targets while a shift in targeting at the end of 2014 into 2015 showed a clear focus on Russian-related issues. Campaigns appear to focus on defense-related geopolitical issues which indicates primary targeting in the government and defense sectors, but CrowdStrike Intelligence is aware of limited targeting of financial firms as well.

Published 2015-09-24

Date

Last 2018-04-26

Updated

Owner N/A

Severity N/A

Likelihood N/A

Risk N/A

Risk Rating N/A

Exploit N/A

Rating

Exploitation N/A

InTheWild

**Mitigation Status**

Status New

Comment N/A

**Change History**

Results as of 2019-09-17 14:45:51

[Save as CSV](#)

Filter by  [Refresh](#)

Changed Attribute	Old Value	New Value	Who	When
No change records found.				

*The General tab.*

The **General** tab of the **Threat** object pop-up displays the following fields:

- **Report Type:** Type of report that RiskVision imported.
- **Source:** Threat feed provider.
- **Identifier:** ID assigned by threat intelligence provider.
- **Title:** Descriptive name of the threat intelligence.
- **Description:** Summary of the threat intelligence.
- **Owner:** The person responsible for analyzing or mitigating the threat.
- **Severity:** Severity of the threat. You need to manually select this field. Possible values include:
  1. Informational (score = 1)
  2. Low (score = 2)
  3. Medium (score = 3)
  4. High (score = 4)
  5. Critical (score = 5)
- You need to manually select this field. The Likelihood values are ordered as follows:
  1. Unlikely (score = 1)
  2. Possible (score = 2)
  3. Likely (score = 3)
  4. Almost Certain (score = 4)
  5. Certain (score = 5)

- **Risk:** The risk posed by the threat. This is a calculated field and cannot be edited. Calculated Risk = (Severity \* Likelihood). Risk values are as follows:
  1. Very Low (1 score)
  2. Low (2 - 5 score)
  3. Medium (6 - 11 score)
  4. High (12 - 19 score)
  5. Very High (20 - 25 score)
- **Status:** Potential values are as follows:
  1. New
  2. Acknowledged
  3. Investigating
  4. Ignore
  5. Mitigating
  6. Mitigated

## Report

The **Report** tab provides the text from the related threat intelligence report.

The screenshot shows a web interface for a threat intelligence report. The title bar reads "Threat: Hammer Panda". On the left is a blue sidebar with navigation tabs: "General", "Report" (selected), "Vulnerabilities", "Targeted Entities", "Tickets", and "Incidents". The main content area displays the following information:

- Threat Actor:** Hammer Panda
- Source:** CrowdStrike
- Published On:** 2015-09-24 15:22:24
- Executive Summary:** CrowdStrike Intelligence tracks HAMMER PANDA activity back to at least 2013. This adversary has leveraged a range of malicious tools including PlugX, NetTraveler, Saker, and DarkSt malware. Older activity from 2013/2014 appeared to focus on India and related targets while a shift in targeting at the end of 2014 into 2015 showed a clear focus on Russian-related issues. Campaigns appear to focus on defense-related geopolitical issues which indicates primary targeting in the government and defense sectors, but CrowdStrike Intelligence is aware of limited targeting of financial firms as well.
- Alias:** Temp.Zhenbao
- Origins:**
  - China
- Motivations:**
  - Espionage
- Target Countries:**
  - India
  - Russian Federation
  - United States
  - Uzbekistan
- Target Industries:**
  - Aerospace & Defense

*The Report tab.*

## Vulnerabilities

Threat: Hammer Panda

General  
 Report  
**Vulnerabilities**  
 Targeted Entities  
 Tickets  
 Incidents

### Vulnerabilities

1-5 of 5

Filter by - Show all - Refresh

<input type="checkbox"/> Identifier	Title	Description	CVSS v2.0 Score	Exploits	Entities Affected	Entities Without Tickets
<input type="checkbox"/> 10114	10114	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.	2.3	0	16	0
<input type="checkbox"/> CVE-2012-0158	CVE-2012-0158	The (1) ListView, (2) ListView2, (3) TreeView, and (4) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0 Runtime allow remote attackers to execute arbitrary code via a crafted (a) web site, (b) Office document, or (c) .rtf file that triggers "system state" corruption, as exploited in the wild in April 2012, aka "MSCOMCTL.OCX RCE Vulnerability."	9.3	1	0	0

The Vulnerabilities tab.

The **Vulnerabilities** tab shows every targeted vulnerability attached to the threat. When one or more CVE is associated with a threat, RiskVision will display any vulnerabilities mapped to those CVEs here.

The **Vulnerabilities** grid displays the following columns:

- Identifier - The ID that the threat intelligence service assigns to the threat information
- Caption - Title assigned by the threat intelligence provider to the information
- Description - A short description assigned by the threat intelligence provider to the information
- CVSS 2.0 Score - The CVSS 2.0 score of the vulnerability
- Exploits - The number of exploits as a result of the vulnerability
- Instances - The number of vulnerability instances
- Instances Without Tickets - The number of vulnerability instances without a ticket

Click and select a vulnerability identifier to view the vulnerability details.

Vulnerability: 10114 [Edit](#)

**General**

CVSS v2.0 Score

Identification

More Information

References

Risk

Affected Entities

Tickets

Technologies

Patches

Custom tab

Enhanced Score

Risk Score

Exploits

Exceptions

CVSS v3.0 Score

Threats

**▼ Vulnerability**

---

Title 10114

Description The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Identifier 10114

Owner [Redacted]

References N/A

Severity Low

Likelihood N/A

Weaknesses N/A

Source connector.remote.nessus

Secondary Source Scanner

Early warning No

Status Acknowledged

System Info Acknowledged

**▼ Acknowledgement** [Unacknowledge](#)

---

Acknowledged Yes

Comment This vulnerability was automatically acknowledged when a ticket was created by [Redacted]

Applicable Yes

**▼ Change History**

---

Results as of 2019-09-17 15:25:01

[More Actions...](#) Filter by [- Show all -](#) [Refresh](#)

Change	Who	When
No change records found.		

The Vulnerability Details page.

Select the **Threats** tab to view a list of threats from the selected vulnerability.

Vulnerability: 10114

**General**

CVSS v2.0 Score

Identification

More Information

References

Risk

Affected Entities

Tickets

Technologies

Patches

Custom tab

Enhanced Score

Risk Score

Exploits

Exceptions

CVSS v3.0 Score

**Threats**

**Threats**

---

1-7 of 7

[Details](#) [Create Ticket](#) [Add To Existing Ticket](#) Filter by [- Show all -](#) [Refresh](#)

	Source	Identifier	Title	Threat Type	Risk	Status	Owner	Last Updated
<input type="checkbox"/>	CrowdStrike	806	CSIT-14097	Tipper	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	N/A	2014-10-21 13:11:18
<input type="checkbox"/>	CrowdStrike	1759	Pitty Panda	Actor	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	N/A	2017-03-29 11:53:44
<input type="checkbox"/>	CrowdStrike	2139	FANCY BEAR	Actor	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	[Redacted]	2019-09-17 11:24:18
<input type="checkbox"/>	CrowdStrike	1751	ENERGETIC BEAR	Actor	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	[Redacted]	2018-12-17 09:11:51
<input type="checkbox"/>	CrowdStrike	2135	VICEROY TIGER	Actor	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	[Redacted]	2019-09-17 11:24:35
<input type="checkbox"/>	CrowdStrike	150	CSA-14032 ENERGETIC BEAR Using Document Reader Exploits CVE-2013-2729 and CVE-2014-1761	Notice	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	N/A	2017-03-07 19:52:25
<input type="checkbox"/>	CrowdStrike	1826	Hammer Panda	Actor	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	New	N/A	2018-04-26 07:32:11

The Threats tab.

The threat details include:

- Source - Threat feed provider.

- Identifier - ID assigned by threat intelligence provider.
- Title - Title provided by threat intelligence provider.
- Threat Type - The type of threat.
- Risk - The severity of risk from the threat.
- Status - The current status of the threat.
- Owner - The owner responsible for taking action on the threat.
- Last Updated - The date when the threat was last updated.



## Targeted Entities

The screenshot shows a web interface for a threat named "Hammer Panda". On the left is a navigation menu with options: General, Report, Vulnerabilities, Targeted Entities (selected), Tickets, and Incidents. The main area is titled "Targeted Entities" and shows "1-17 of 17" entities. There are three buttons: "Details", "Assign", and "Remove". A "Filter by" dropdown is set to "- Show all -" and a "Refresh" button is present. Below is a table with columns: Name, Type, Subtype, and Criticality. The table lists three computer entities with IP addresses 192.168.0.6, 192.168.0.9, and 192.168.0.3. The first has a yellow criticality bar, the second and third have red bars.

<input type="checkbox"/>	Name	Type	Subtype	Criticality
<input type="checkbox"/>	192.168.0.6	Computer	N/A	
<input type="checkbox"/>	192.168.0.9	Computer	N/A	
<input type="checkbox"/>	192.168.0.3	Computer	N/A	

*The Targeted Entities tab.*

The **Targeted Entities** tab displays all target entities attached to the threat. There are two kinds of targeted entities:

1. Entities that are attached to any of the threat's targeted vulnerabilities; and
2. Entities that have been manually assigned to the threat by users.

The **Targeted Entities** tab consists of a grid with the following columns:

1. **Name:** The name of the entity
2. **Type:** The entity type
3. **Subtype:** The entity subtype
4. **Criticality:** The criticality of the entity

Users can perform the following actions:

1. **Details:** Brings up the details of the selected entity.
2. **Assign:** Allows the user to assign a new threat to the entity.
3. **Delete:** Removes the threat association with the selected entity



If the user has a filter preventing him or her from viewing all of the individual entities attached to an entity group, he or she will see the following message at the top of the screen: **You are not able to see all the entities on this page because you are restricted from seeing [number of hidden entities] entities.**

## Tickets

<input type="checkbox"/>	Ticket ID	Title	Status	Type	Owner	Entities	Risk	Progress	Description	Created Time
<input type="checkbox"/>	TKT00093	Ticket_01	Assigned	Audit Finding		0	<input type="checkbox"/> N/A	<div style="width: 0%;"></div> 0%	N/A	2019-09-17
<input type="checkbox"/>	TKT00092	T1	Assigned	Audit Finding		0	<input type="checkbox"/> N/A	<div style="width: 0%;"></div> 0%	N/A	2019-09-17

*The Tickets tab.*

The **Tickets** tab shows a grid with the following details:

- **Ticket ID:** The ID of the ticket. Click on this link to view the ticket details
- **Title:** The ticket title
- **Status:** The current status of the workflow associated with the ticket
- **Type:** The ticket type
- **Owner:** The owner of the ticket
- **Entities:** The entities affected by the ticket
- **Risk:** The severity of the risk
- **Progress:** The current progress made on the resolution of the ticket
- **Description:** A short description of the ticket
- **Created Time:** The time when the ticket was created

Click **New** to create a new ticket.

Select a ticket and click:

- **Assign** to associate an existing ticket to the threat
- **Remove** to disassociate a ticket from the threat
- **Details** to view the ticket details
- **Customize** to modify the columns displayed in the grid

# Incidents

<input type="checkbox"/>	Incident ID	Title	Severity	Type	Detected Date	Submitter	Awaiting Action By	Status	Risk
<input type="checkbox"/>	INC00015	TestIncident02	N/A	Breach	2019-09-17 16:13:02		Team: Incident Response Team	Submitted	<input type="checkbox"/> N/A
<input type="checkbox"/>	INC00016	TestIncident03	N/A	Investigation	2019-09-17 16:13:49		N/A	Draft	<input type="checkbox"/> N/A
<input type="checkbox"/>	INC00014	TestIncident01	N/A	Theft	2019-09-17 16:11:59		Team: Incident Response Team	Submitted	<input type="checkbox"/> N/A

*The Incidents tab.*

The **Incidents** tab shows a grid with the following details.

- Incident ID - The ID of the incident. Click on this link to view the incident details.
- Title - The ticket title.
- Severity - Severity of the incident.
- Type - The incident type.
- Detected Date - Date the incident was first observed.
- Submitter - Name of the person who recorded the incident.
- Awaiting Action By - Name of the person with pending action.
- Status - Current status of the workflow associated with the incident.
- Risk - Severity of the risk.

Click **New** to create a new incident

Select an incident and click:

- **Assign** to associate an existing incident with the selected threat.
- **Remove** to disassociate an incident from the threat.

Select an incident to view the **Incident Details** window.

Incident: TestIncident02

- General
- Additional Details
- Related Incidents
- Actions & Tickets
- Controls
- Threats

### Workflow

Name: Incident Workflow

1 Submitted 2 Review 3 Sign Off 4 Closed

Since: 2019-09-17 16:13:41

Current Owner(s): Team: Incident Response Team (Details)

Stage Actions: 1 of 5 needed for moving workflow to "Review"  
1 of 5 needed for moving workflow to "Closed"

Documents

Workflow History

Change History

### General

Title TestIncident02	Time Started 2019-09-17 16:13:02
Incident Type Breach	Time Ended N/A
Incident Subtype Data	Time Detected 2019-09-17 16:13:02
Description Test	Due Date N/A
Entities N/A	Time Received 2019-09-17 16:13:41
Incident Id INC00015	Time Updated 2019-09-17 16:13:41
Incident Submitter	Incident Age < 1 day

**Images**

Custom Image 1 N/A  
Custom Image 2 N/A  
Custom Image 3 N/A  
Custom Image 4 N/A

**Organization**

Organization N/A  
Division N/A  
Subdivision N/A

### Comments

Add a comment

No comments have been entered.

The Incident Details window.

Select the **Threats** tab to view a list of threats arising from the incident. Threats must be manually assigned to incidents.

Incident: TestIncident02

- General
- Additional Details
- Related Incidents
- Actions & Tickets
- Controls
- Threats

### Threat Incidents

1-1 of 1

More Actions...

Filter by - Show all - Refresh

Source	Identifier	Title	Threat Type	Risk	Status	Owner	Last Updated
<input type="checkbox"/>	CrowdStrike 1826	Hammer Panda	Actor		New	N/A	2019-09-17

The Threat Details page.

The **Threat Details** page includes the following information:

- Source - Threat feed provider.
- Identifier - ID assigned by threat intelligence provider.
- Title - Descriptive name of the threat intelligence.
- Threat Type - The type of threat.
- Risk - The severity of risk from the threat.

- Status - The current status of the threat incident.
- Owner - The owner responsible for taking action on the threat incident.
- Last Updated - The date when the threat incident was last updated.

## Exploits

Exploits detail the ways in which a vulnerability can be taken advantage of by stealing data or otherwise inflicting harm on an organization. Visibility of the number and types of exploits facilitates the prioritization of vulnerabilities. The **Exploits** page shows exploits that have been imported into RiskVision.

Exploits are usually mapped to vulnerabilities through CVEs, although the exploit may have additional identifiers it is mapped to, depending on the data source.

**Exploits** is a grid available in the **Vulnerabilities** menu, which is visible only if you possess the Threats and Vulnerabilities View permission. This grid contains exploits imported from the **Administrator** application.

Source	Identifier Name	Description	Platform	Type	CVE	Vulnerability Instances	Date Published	Date Added	Last Updated Date
Exploit DB 44493	exploits/xml/webapps/44493.txt	"Geist WatchDog Console 3.2.2 - Multiple Vulnerabilities"	xml	webapps	CVE-2018-10079,CVE-2018-10078,CVE-2018-10077	0	2018-04-17	N/A	2018-04-17
Exploit DB 44492	exploits/php/webapps/44492.txt	"Joomla! Component JS Jobs 1.2.0 - Cross-Site Request Forgery"	php	webapps	N/A	0	2018-04-17	N/A	2018-04-17
Exploit DB 44491	exploits/multiple/dos/44491.txt	"RSVG 2.40.13 / 2.42.2 - '.svg' Buffer Overflow"	multiple	dos	N/A	0	2018-04-17	N/A	2018-04-17
Exploit DB 44484	exploits/php/webapps/44484.txt	"Rvsitebuilder CMS - Database Backup Download"	php	webapps	N/A	0	2018-04-17	N/A	2018-04-17
Exploit DB 44488	exploits/hardware/webapps/44488.py	"Lultron Quantum 2.0 - 3.2.243 - Information Disclosure"	hardware	webapps	CVE-2018-8880	0	2018-04-17	N/A	2018-04-17
Exploit DB 44485	exploits/windows/remote/44485.py	"Easy File Sharing Web Server 7.2 - Stack Buffer Overflow"	windows	remote	CVE-2018-9059	0	2018-04-17	N/A	2018-04-17
Exploit DB 44490	exploits/linux/dos/44490.txt	"PDFunite 0.41.0 - '.pdf' Local Buffer Overflow"	linux	dos	N/A	0	2018-04-17	N/A	2018-04-17

The Exploits grid.



The **Date Added** and **Last Updated Date** columns are not default. They can be added by using the **Customize** action from the **More Actions** dropdown.

## To expand an exploit:

1. Open the **Vulnerabilities** menu.
2. Click the **Exploits** page and click an exploit to open.

Tab	Description
General	<p><b>Exploit</b></p> <p>Name exploits/xml/webapps/44493.txt</p> <p>Description "Geist WatchDog Console 3.2.2 - Multiple Vulnerabilities"</p> <p>Platform xml</p> <p>Type webapps</p> <p>Port N/A</p> <p>CVE Reference CVE-2018-10079;CVE-2018-10078;CVE-2018-10077</p> <p>Date Added N/A</p> <p>Date Published 2018-04-17</p> <p>Last Updated Date 2018-04-17</p> <p>Source URL <a href="https://www.exploit-db.com/exploits/44493">https://www.exploit-db.com/exploits/44493</a></p>

The Exploits Details page.

The following table summarizes different tabs available in the **Exploits Details** page:

Tab	Description
General	Displays detailed exploit information, including the name, description, platform, type of exploit, port used by the exploit, CVEs the exploit maps to, the date the exploit was published or submitted, and

Tab	Description
Vulnerabilities	<p>the dates the exploit was added and last updated.</p> <p>Displays the vulnerabilities associated with the exploit.</p> <ul style="list-style-type: none"> <li>• Vulnerabilities by Identifier: Displays the following columns: Identifier, Severity, CVSS Score, Total Entities, Without Tickets, and Without Patches.</li> <li>• Vulnerabilities by Entity Criticality: Displays the Entity Criticality, Total Affected, and Without Tickets.</li> </ul>

## Technologies

Technologies include platforms, such as operating systems, and applications, such as web browsers. Whenever you deploy technologies there is the potential for vulnerabilities.

The Common Platform Enumeration (CPE) provides a central database of possible technologies. By mapping your entities to CPE, RiskVision can automatically determine some of the vulnerabilities that apply to your situation.

Use predefined reports under the **Threat Management** menu to view:

- **All Technologies;** and
- **Recent Technologies.**



## All Technologies

The **All Technologies** page, on the **Technologies** menu, is a grid consisting of manually and automatically created technologies in RiskVision Threat and Vulnerability Manager.

You can perform the following operations in the **All Technologies** page:

- Search technologies by vendor, product, keyword, unassigned, and non-validated. For information about how to search technologies, see [Searching Technologies](#). For information about how to search non validated technologies, see [Reviewing Non Validated Technologies](#).
- Create a new technology using the **New** option. This action requires the Threats and Vulnerabilities Create permission.
- Update a technology. This action requires the Threats and Vulnerabilities Update permission.
- Use actions in the **More Actions** dropdown list. This action requires the Threats and Vulnerabilities Manage permission.
- Delete a technology using the Delete option. This action requires the Threats and Vulnerabilities Delete permission.

## Recent Technologies

The **Recent Technologies** page, on the **Technologies** menu, is a grid consisting of technologies that are manually created and modified in the last month. However, you can select a value in the **Show** dropdown list to view technologies up to the last year.

You can perform the following operations in the **Recent Technologies** page:

- Create a new technology using the **New** option. This action requires the Threats and Vulnerabilities Create permission.
- Update a technology. This action requires the Threats and Vulnerabilities Update permission.
- Use actions in the **More Actions** dropdown list. This action requires the Threats and Vulnerabilities Manage permission.
- Delete a technology using the **Delete** option. This action requires the Threats and Vulnerabilities Delete permission.

## Search for Technologies

When using Threat and Vulnerability Manager, you may find you need to search for specific technologies among the thousands your organization has procured. You can use the **All Technologies** page, available on the **Technologies** menu, to search technologies. In the **All Technologies** grid, the technology names are sorted alphabetically by default. This grid contains a search pane that allows you to perform a search based on product or vendor. In addition, you can also review non-validated technologies that are imported by connectors.

*The Search Technologies pane.*

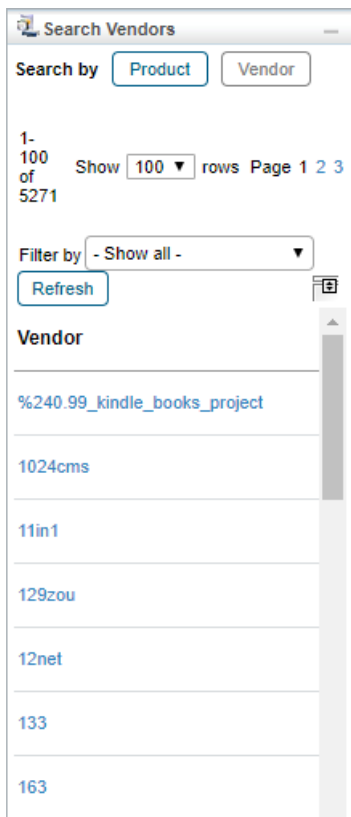
### To search technologies by product:

Perform one of the following actions:

- By first letter:
  1. Verify that the **Search Technologies** pane is enabled; click **Product** if it is disabled.
  2. Click any letter under **Browse by Product Name**. Use the pagination buttons to navigate between the search results. For more information about pagination, see *Using the Grid View*.
- Search by Vendor:
  1. Enter a vendor name in the **Search by Vendor** field.
  2. Click **Search**.
- Search by Keyword:
  1. Enter a keyword in the **Search by Keyword** field.
  2. Click **Search**.
- View un-assigned technologies:
  1. Click **Search** under the **Un-Assigned Technologies** option.

### To search technologies by Vendor:

1. Click **Vendor** to enable the **Search Vendors** pane.



*The Search Vendors pane.*

2. Click a vendor to view the technologies provided by the vendor.
3. **Optional:** If you're looking for a specific vendor, click **Filter by**, then click either **Vendor** or **Number of Technologies**. Enter your search criteria, then click **Refresh**.

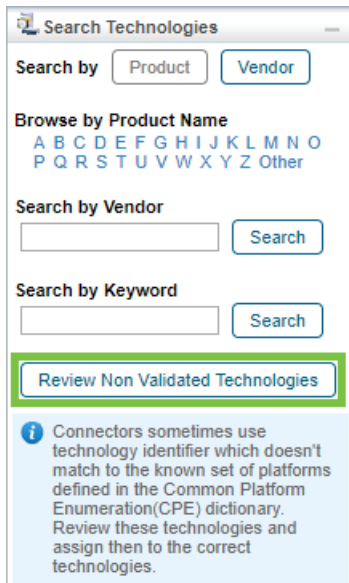
You can also search the **Technologies** page to find all technologies that do not have a vendor by using 'N/A' in the **Search By Vendor** field.

## Review Non-Validated Technologies

The National Vulnerability Database (NVD) uses Common Platform Enumeration (CPE) identifiers to represent information technology systems, software, and packages. Whenever an identifier is brought into RiskVision, such as from a vulnerability scanner, with identifiers that differ from the NVD identifiers, RiskVision treats these technologies as non-validated technologies. Before these non-validated identifiers can be mapped to a technology, you will first need to review them.

### To review non-validated technologies:

1. Open Threat and Vulnerability Manager.
2. Go to **Technologies > All Technologies**.
3. Click **Review Non Validated Technologies**. The technologies with validated flag 'No' will appear.



*The Search Technologies pane.*

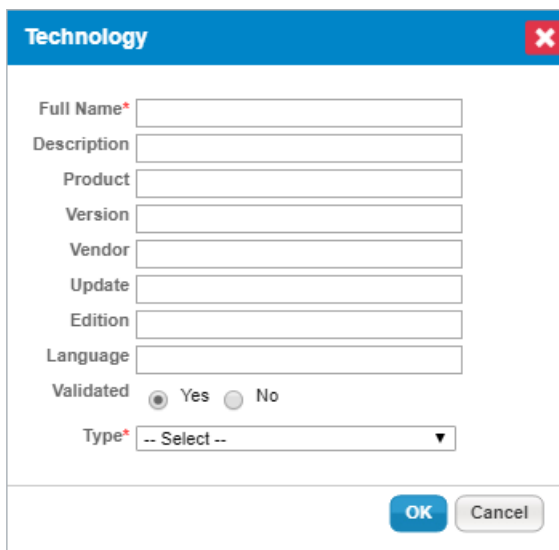
4. Click a technology to open its details page.
5. Click **Edit** in the upper right-hand corner of the window.
6. Click the **General** tab.
7. Click **Yes** next to the Validated option.
8. Click **Save**.

## Create a Technology

A large number of commonly used vulnerabilities are shipped along with Threat and Vulnerability Manager that can be immediately attached to vulnerabilities and entities, if required. You will need to create a new technology if your organization is using a technology that is not available in the application.

### To create a new technology:

1. Open Threat and Vulnerability Manager.
2. Go to **Technologies > All Technologies**, or **Technologies > Recent Technologies**.
3. Click **New**.
4. The **Technology** dialogue box appears. Enter the details as follows:
  - **Full Name:** The name of a technology. This must be a relevant name.
  - **Description:** Any additional information that describes a technology.
  - **Product:** The short name of a technology.
  - **Version:** The version number of a technology or product.
  - **Vendor:** The name of an organization providing the technology.
  - **Update:** The information of an update if the technology includes the most recent fixes.
  - **Edition:** The edition of a technology or product. This can be standard, professional, enterprise, and more.
  - **Language:** The technology language if procured for non-native English users.
  - **Type:** Select whether a technology is a software application, a hardware component, or an operating system.



The Technology dialogue box contains the following fields and controls:

- Full Name\***: Text input field (required).
- Description**: Text input field.
- Product**: Text input field.
- Version**: Text input field.
- Vendor**: Text input field.
- Update**: Text input field.
- Edition**: Text input field.
- Language**: Text input field.
- Validated**: Radio buttons for **Yes** (selected) and **No**.
- Type\***: Dropdown menu with **-- Select --** and a downward arrow (required).
- OK** and **Cancel** buttons at the bottom right.

*The Technology dialogue box.*

## About Technology Details

More information related to a technology is available on the **General**, **Vulnerability**, **Entities**, and **Exceptions** tabs of **Technology** details page. The details of a technology can be viewed when a technology is selected in the **All Technologies** or **Recent Technologies** grid. You can also view technology details within the **Vulnerability** details page if a technology is present on a vulnerability.

The screenshot shows the 'Technology' details page for 'AB Google Map Travel project AB Google Map Travel for WordPress 3.4'. The page has a blue sidebar with navigation tabs: 'General' (selected), 'Vulnerabilities', 'Entities', and 'Exceptions'. The main content area is titled 'Technology' and contains the following information:

Full Name	AB Google Map Travel project AB Google Map Travel for WordPress 3.4	Modified Time	N/A
Description	N/A	Obsolete	N/A
Product	ab_google_map_travel	In Use	N/A
Version	3.4	Banned	N/A
Vendor	ab_google_map_travel_project	Of Interest	N/A
Update	N/A	Validated	Yes
Edition	~~~wordpress~~	Type	Application
Language	N/A		
CPE URI	cpe:/a:ab_google_map_travel_project:ab_google_map_travel:3.4:~~~wordpress~~		

Below the technology details is the 'Technology Identifiers' section, which includes buttons for 'Add', 'Reassign', and 'Remove'. It also features a 'Filter by' dropdown menu set to '- Show all -' and a 'Refresh' button. A table header is visible with columns: 'Identifier', 'Source', 'Status', 'Deprecation Reason', 'First Reported Time', and 'Deprecation Date'. The table currently displays 'No Data found.'

*The Technology details page.*

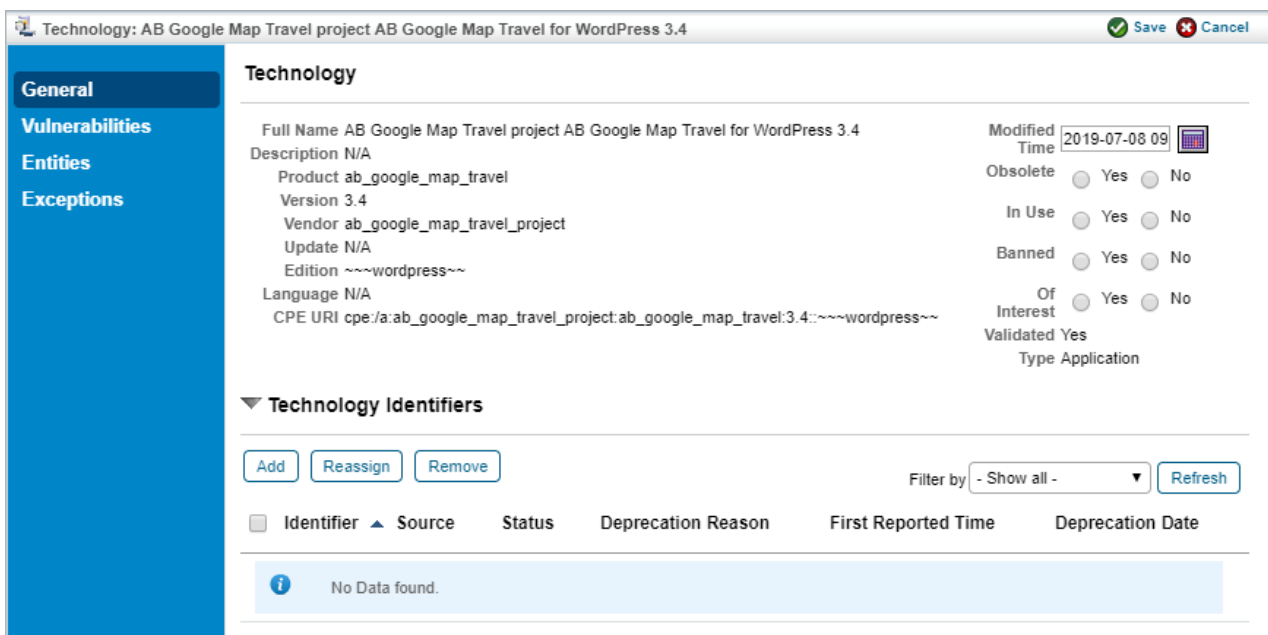
## General Tab

The **General** tab includes **Technology** and **Technology Identifiers** sections, and allows updating the fields under those sections.

All of the fields available under the **Technology** section can be updated if you have manually created a technology. Default technologies will only allow you to update the following fields:

- **Obsolete.** Select 'Yes' if a technology is no longer used in your organization.
- **Banned.** Select 'Yes' if a technology is prohibited by your organization.
- **In Use.** Select 'Yes' if a technology is in use.
- **Of Interest.** Select 'Yes' if a technology is widely used, and is frequently affected by vulnerabilities.

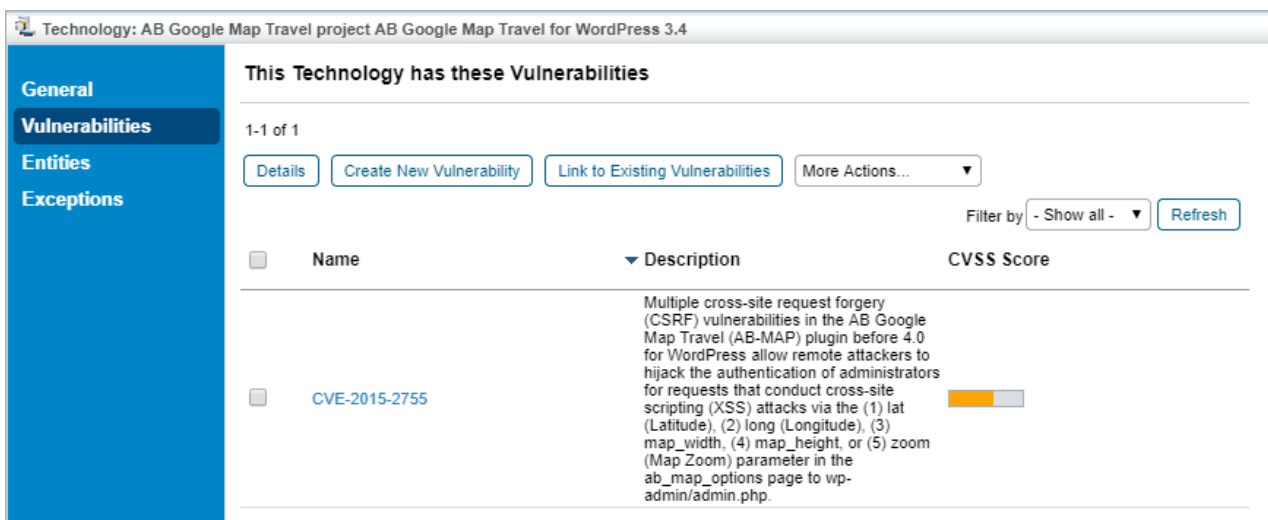
The **Technology Identifiers** section shows the technologies that are no longer in use.



The Edit General Information screen.

## Vulnerabilities Tab

The vulnerabilities attached to a technology are listed in the **Vulnerabilities** tab. Using this tab, you can update a vulnerability, create a new vulnerability, link to an existing vulnerability, and remove vulnerabilities from a technology.



The Vulnerabilities tab.

## Entities Tab

A software application or a hardware component installed on an entity, such as computer or mobile, signifies that a technology is present on that entity. This tab shows entities the technology is attached to.



Technology: AB Google Map Travel project AB Google Map Travel for WordPress 3.4

**General**  
**Vulnerabilities**  
**Entities**  
 Exceptions

**This Technology is Present on these Entities**

Customize Filter by - Show all -

Name	Type	Subtype	Criticality	Owner	Description
No entities found.					

The Entities tab.

## Exceptions Tab

Attaching an exception to a [Common Platform Enumeration \(CPE\)](#) can save users a lot of time. This tab shows the exceptions attached to the CPE the technology is mapped to.

Technology: AB Google Map Travel project AB Google Map Travel for WordPress 3.4

**General**  
**Vulnerabilities**  
**Entities**  
**Exceptions**

**Exceptions**

More Actions... Filter by - Show all -

Exception ID	Exception Name	Global	Entity Names	Current Stage	Status Modified By	Requestor	Start	End	Total Entities
No exception found.									

The Exceptions tab.

## Weaknesses

Weaknesses, as defined by the Common Weakness Enumeration (CWE), provide a set of categories for vulnerabilities. For example, Hard-Coded Password (CWE ID 259) describes a weakness that is common to many specific vulnerability definitions.

Name	Number of Entities	Number of Vulnerabilities
.NET Misconfiguration: Use of Impersonation	0	0
Absolute Path Traversal	0	0
Acceptance of Extraneous Untrusted Data With Trusted Data	0	0
Access of Memory Location After End of Buffer	0	0
Access of Memory Location Before Start of Buffer	0	0
Access of Resource Using Incompatible Type ('Type Confusion')	0	0
Access of Uninitialized Pointer	0	0
Access to Critical Private Variable via Public Method	0	0
Addition of Data Structure Sentinel	0	0

*The Weaknesses grid view.*

The RiskVision All Weaknesses report shows the kind of vulnerabilities that are most frequent, for example, and allow you to track remediation efforts in a summary form.

## Patches

Patches are remedial changes made available by software vendors and security agencies. RiskVision tracks Name, Version, Type, Severity, Publisher, affected entities and other properties for available patches.

Patch information comes from external sources such as BigFix(R) or subscription vulnerability feeds such as iDefense Labs.

## Vulnerability Exception Details Overview

The **Exception** details page contains general information on a selected RiskVision exception.

*The Exception details page.*

The following table summarizes the tabs available on the **Exception** details page.

TAB	DESCRIPTION
Information	Displays information such as the vulnerability and entity scope, the affected entities, and the current stage. Users may also add or delete vulnerability compensating controls to the exception.
Workflow	Shows the current workflow stage of the exception, as well as the workflow history. Users can also force a transition to another stage or delegate access to the exception to another user.
Comments	Allows users to review and add comments to the exception
Affected Instances	Displays the entities, vulnerabilities, and tickets that the exception is attached to.
Documents	Displays all of the documents or web links attached to the exception. Users can add or delete documents or web links.

Comp Controls

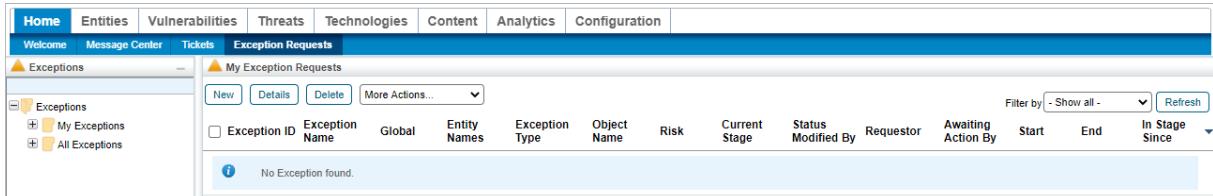
Displays the current vulnerability compensating controls in the **Pending** or **Implemented** status attached to the exception, and the status values for each entity listed in their **Entities** sections.

## Create a Vulnerability Exception Request

Vulnerability instances with approved exceptions will have their risk scores reduced to 0 until there are no longer any valid exceptions applied to them.

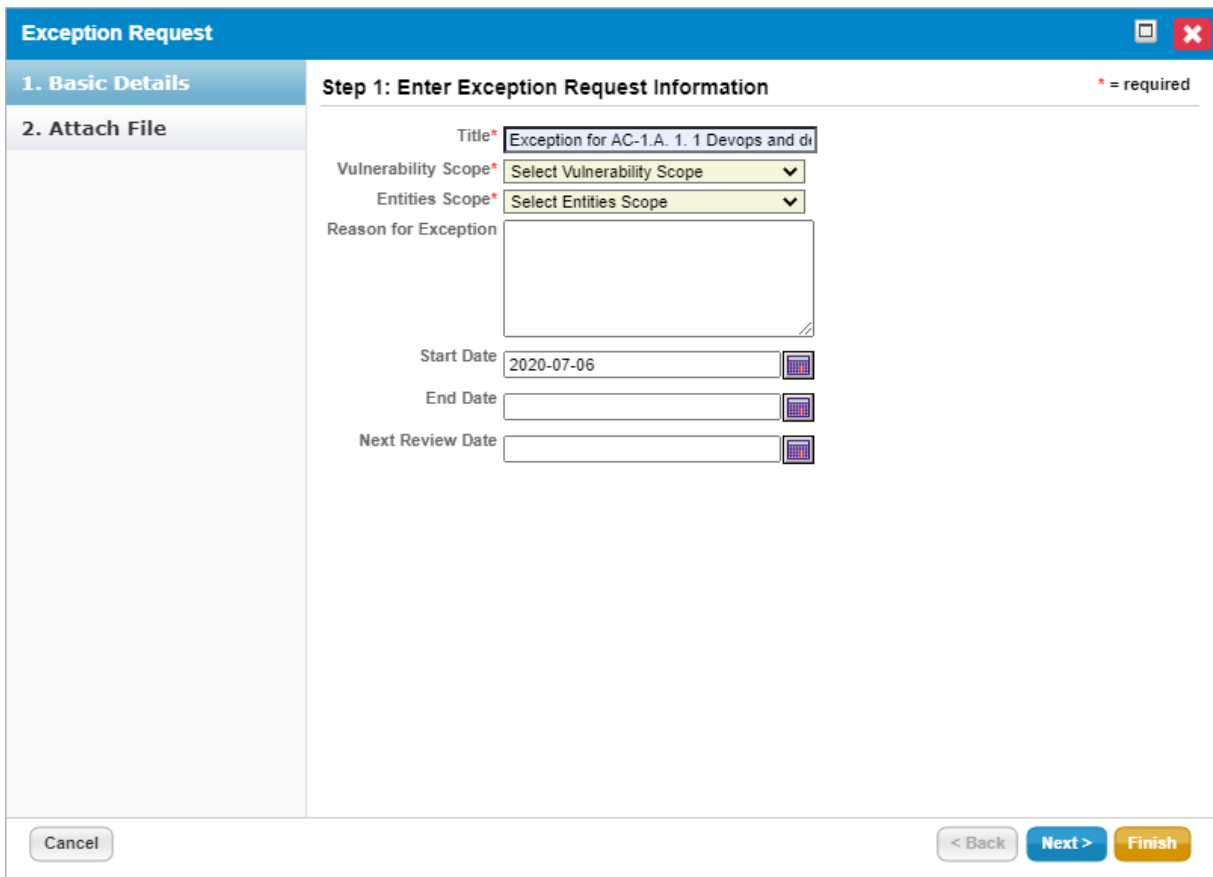
### To create an exception:

1. Open the RiskVision Threat and Vulnerability Manager.
2. Go to Home > Exception Requests.



*The Exception Requests tab.*

3. Click **New** to launch the **Exception Request** wizard.

The screenshot shows the 'Exception Request' wizard, Step 1: Enter Exception Request Information. The wizard has a blue header with the title 'Exception Request' and a close button. The left sidebar shows two sections: '1. Basic Details' (selected) and '2. Attach File'. The main content area contains the following fields:

- Title\***: Text input field containing 'Exception for AC-1.A. 1. 1 Devops and di'
- Vulnerability Scope\***: Dropdown menu with 'Select Vulnerability Scope' selected.
- Entities Scope\***: Dropdown menu with 'Select Entities Scope' selected.
- Reason for Exception**: Large text area for providing details.
- Start Date**: Date picker showing '2020-07-06'.
- End Date**: Date picker.
- Next Review Date**: Date picker.

At the bottom, there are three buttons: 'Cancel', '< Back', and 'Next > Finish'.

*The Basic Details section of the Exception Request wizard.*

4. Enter the [basic details](#) of the exception, then click **Next**.
5. **Optional:** Add a document, link to a document in the repository, or provide a 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\*  
 No file chosen

Document Caption

Description

Expires On

Add a link to a document in repository

Add a web link

Add a Network Path

Added Documents and Links

▼

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

*The Attach File section of the Exception Request wizard.*

If you cancel the attachment, it will initially appear as if the entire exception request has been cancelled. Wait a few moments and the exception request will reappear.

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

## Exception Request Basic Details

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

- **Title**: Enter the text to name the exception request.
- **Vulnerability Scope**: Click to view a list of options. When you select an option the **Exception Request Basic Details** page will alter depending on your selection.
  - **Vulnerability Definition(s)**: Use this option to create an exception for one or more vulnerability definitions. This will apply an exception for one or more vulnerabilities across a range of entities.

The screenshot shows a software window titled "Exception Request" with a blue header bar. On the left, there is a sidebar with two tabs: "1. Basic Details" (selected) and "2. Attach File". The main content area is titled "Step 1: Enter Exception Request Information" and includes a legend "\* = required". The form contains the following fields:

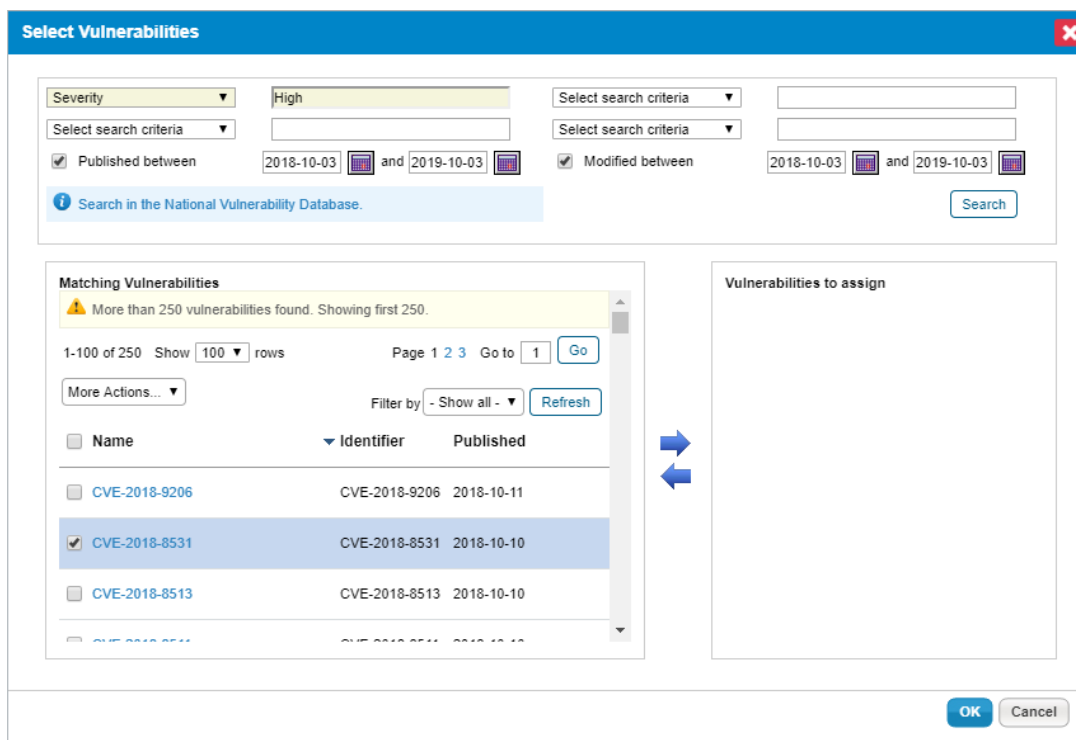
- Title\***: A text input field containing "Exception for AC-1.A. 1. 1 Devops and di".
- Vulnerability Scope\***: A dropdown menu with "Select Vulnerability Scope" selected.
- Entities Scope\***: A dropdown menu with "Select Entities Scope" selected.
- Reason for Exception**: A large text area for providing details.
- Start Date**: A date input field with "2020-07-06" and a calendar icon.
- End Date**: An empty date input field with a calendar icon.
- Next Review Date**: An empty date input field with a calendar icon.

At the bottom of the window, there are three buttons: "Cancel", "< Back", and "Next > Finish".

*The Basic Details page of the Exception Request wizard.*

- **Optional**: Click + to open the **Select Vulnerabilities** dialog to browse for one or more vulnerabilities. The exception will be linked to any vulnerabilities selected.





The Select Vulnerabilities dialog.

- **Common Platform Enumeration(s)**: Creating an exception for a CPE can save you a lot of time if you have a technology that you are unable to patch that has multiple CVEs. This allows you to create a single exception for the CPE, instead of an exception for each vulnerability tied to the CPE. For example, if a version of your router operating system embeds an outdated Java version, you can create an exception for the router OS, and therefore not be required to patch the outdated Java version until a router OS patch is available.

 Selecting this option will apply the exception to all new and existing vulnerabilities attached to all new and existing CVEs mapped to the selected CPE.

- **Apply To All Vuln Definitions for selected Entity(s)**: The exception will apply to all vulnerability definitions for the selected entities and entity collections options. This option is useful for servers that you don't want to apply any patches to. For example, an e-commerce provider may restrict that its servers are not allowed to be patched during the holiday shopping season.
- **Entities Scope**: Click this field to view a list of options to define the vulnerability scope on the entities:
  - **Apply to All Instances**: Applies the exception to all instances of the vulnerability or CPE.

 Selecting this option along with **Vulnerability Definitions** or **Common Platform Enumeration(s)** in the **Vulnerability Scope** field will make the exception automatically apply to all new and existing vulnerabilities created with the specified definitions.

- **Select Entities**: Confines the exception to the chosen entities.

 Selecting this option along with **Apply To All Vuln Definition for selected Entity(s)** in the **Vulnerability Scope** field will make the exception automatically apply to all new and existing vulnerabilities created with the specified definitions.

- **Others**: Add the scope in a text description if you're not able to select specific entities.
- **Reason for Exception**: Explain why the exception is required.
- **Compensatory Controls**: Select compensating controls, if applicable, that will offset the risk of the vulnerabilities.

- **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 this field empty if the exception is on-going.
- **Next Review** : Select the date and time that the exception should be reviewed by next. This is just a memo field and will not send any notification.
- **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.

## 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.

## Link Exception Requests with Vulnerabilities

RiskVision provides the ability to link your exceptions to vulnerabilities or vulnerability instances. This feature provides the following types of vulnerability exceptions:

- Exempt all instances of one or more vulnerability definitions;
- Exempt some instances of one or more vulnerability definitions; and
- Exempt one or more entities or entity collections from all vulnerability instances on those chosen entities and/or entity collections.

Valid combinations of Vulnerability and Entity Scope Settings:

Vulnerability Scope	Entity Scope	Result
Vulnerability Definition(s)	Apply the exception to all instances of vulnerability definitions or CPEs	The exception covers all instances of the chosen vulnerability definition.
	Other	Vulnerability definitions for the scope that the user typed in the Other field will be covered by the exception. Since this is a text field, there will not be any linkage to specific instances.
Common Platform Enumerator(s)	Apply the exception to all instances of vulnerability definitions or CPEs	The exception covers all instances of the chosen CPEs. Note that all vulnerabilities that map to the selected CPEs will be covered by the exception.
	Entities	The exception covers just the CPE instances that belong to the selected entities or entity collections.
	Other	The exception covers specified instances of the CPE. Since this is a text field, there are no direct linkages to the specific instances.
Apply the exception to all vulnerability definitions for the selected entities and entity collections	Apply the exception to all instances of vulnerability definitions or CPEs	This exception covers all vulnerability definitions and all instances of the vulnerability.
	Entities	This exception covers all vulnerability definitions for the selected entities and entity collections.
	Other	This exception covers all vulnerability definitions for the text scope provided in the Other field. Since this is a text field there will be no linkages with entities or entity collections.

You can also create exceptions for inferred vulnerabilities. If you have an inferred vulnerability, and if you do not already have a vulnerability instance for it, RiskVision will automatically create a vulnerability instance. Automatically created vulnerability instances (created when an exception is created) will be treated as a manually created vulnerability instance, and they need to be manually resolved. These exceptions can be combined with vulnerability instances from scanners and manually created vulnerability instances within the same exception request. If you create an exception for a vulnerability definition that is applied to all instances of the vulnerability definition, then the exception applies to vulnerability instances originated by scanners, users, and inferred vulnerabilities.

## 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.  <b>Note:</b> 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.  <b>Note:</b> 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	Rejected	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](#).

## Affected Instances

Exceptions attached to vulnerabilities will have an **Affected Instances** tab which allows users to view the entities and vulnerabilities that the exception applies to.

Exception Request: entity

**Affected Vulnerability Instances**

1-22 of 22 Show 100 rows

More Actions... Filter by - Show all - Refresh

Entity	Vulnerability Title	Vulnerability Status	Vulnerability Risk Score	Ticket ID	Ticket Status
qa100	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure	Unresolved	N/A	TKT00086	New
qa100	SMB Signing Disabled or SMB Signing Not Required	Unresolved	N/A	TKT00088	New

*The Affected Instances tab.*

The **Affected Vulnerability Instances** grid contains the following information:

- **Entity:** The name of all entities attached to the exception.
- **Vulnerability Title:** The title of each vulnerability attached to the exception's entities.
- **Vulnerability Status:** The current status of each vulnerability.
- **Vulnerability Risk Score:** The current risk score of each vulnerability.
- **Ticket ID:** The ID of each ticket attached to the exception's vulnerabilities.
- **Ticket Status:** The current status of each ticket.



## About Tickets

RiskVision provides a ticket management system that lets you create and track tickets for tasks, risk assessment mitigation and remediation, and entity control resolution - that is, findings. Tickets are also used for [vulnerability](#) resolution. In addition, sites may deploy and integrate RiskVision 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 Type	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.

## About 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

Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
TKT00093	Ticket_01	Assigned	Audit Finding			N/A	N/A	0%	2019-09-17 16:02:56	2019-09-17
TKT00092	T1	Assigned	Audit Finding			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.override**: Names the exception status that cannot be further modified by a scanner or other source reporting the same vulnerability instance again.

Vulnerability: CVE-1999-0594

General

CVSS v2.0 Score

Enhanced Score

Risk Score

Identification

More Information

References

Exploits

Risk

Affected Entities

**Tickets**

Technologies

Patches

Exceptions

CVSS v3.0 Score

Threats

### Tickets

1-1 of 1

Filter by - Show all -

<input type="checkbox"/>	Ticket ID	Title	Status	Type	Owner	Entities	Risk	Progress	Description	Created Time
<input type="checkbox"/>	TKT00040	CVE-1999-0594	New	Vulnerability Resolution		2	<span style="color: red;">■</span> High	<div style="width: 0%; height: 10px; background-color: #ccc;"></div> 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()
```

## Link 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. Select a ticket you want to link, then click **Details**.
3. Open the **Linked To** section.
4. Click **Add Entities**.
5. Select a type of entity and click **Search**.
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](#).

## Start and Transition 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 by clicking **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**.
4. Click an action button, such as **Accept**, to transition to the next stage or **Reject** to send it back to the previous stage.
5. Enter your transition message and click **OK**.

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

## Change the Default Ticket Workflow

When a ticket is created, which can be an automatic or a manual process, the new ticket will use the Default Ticket Workflow if there is no appropriate custom 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. See [Creating a New Ticket](#) for more information.
2. Open the file `%AGILIANCE_HOME%\config\agiliance.properties` 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.

## Assign 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**.

The screenshot displays the 'Issue Management Workflow' interface. At the top, it shows the name 'Name: Issue Management Workflow' and a progress bar with four stages: '1 Assigned' (highlighted in blue), '2 In Progress', '3 Review', and '4 Closed'. Below the progress bar, the 'Since' date is '2019-09-17 16:02:56'. The 'Current Owner(s)' is shown as a redacted name with a '(Details)' link. Under 'Stage Actions', it lists: '1 of 1 needed for moving workflow to "In Progress"', '1 of 1 needed for moving workflow to "Closed"', and '1 of 1 needed for moving workflow to "Review"'. There is a 'Force Transition' checkbox which is currently unchecked. A yellow tooltip box contains the text: '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.' At the bottom, there are five buttons: 'Accept', 'Reject', 'Test', 'Delegate To', and 'Revoke Delegation'.

*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.

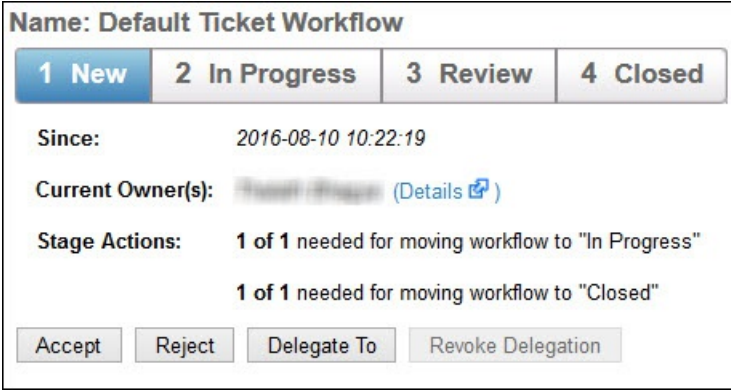


## Delegate an Object to Another User

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 and 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.
3. Assign the user or team using one of the following methods:
  - **More Action** dropdown:
    - Click **More Action > Delegate**.
    - Click the **Select User** or **Select Team** field and select the user or team that you want to assign the ticket to.
    - Click **Comment** field and add a comment.
    - Click **OK**.
  - **Details**:
    - Click **Details**.
    - Click the **General** tab.
    - Click the **Workflow** section.
    - Click **Delegate To**.
    - Locate the user or team that you want to assign.



**Name: Default Ticket Workflow**

<b>1 New</b>	<b>2 In Progress</b>	<b>3 Review</b>	<b>4 Closed</b>
--------------	----------------------	-----------------	-----------------

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

**Current Owner(s):** [David Brown](#) (Details [↗](#))

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

1 of 1 needed for moving workflow to "Closed"

- Enter a comment in the **Comment** field.
- Click **OK**.

The ticket ownership will transfer from the old list of owners to the new list and the **Revoke Delegation** button will be enabled.

## Revoking A Delegated Object

Revoke delegation will change the ownership of current and subsequent workflow stages. The **Revoke Delegation** option is not enabled for delegated tickets unless you have Ticket View and Ticket Manage permissions.

### To revoke an assigned ticket:

1. Go to **Home > Tickets**.
2. Click the ticket you want to revoke.
3. Revoke delegation using one of the following methods:
  - **More Action** dropdown:

- Click **More Action > Revoke Delegation**.
  - Enter the reason or comment for revoking delegation access.
  - Click **OK**.
- **Details:**
- Click **Details** to open the **Ticket** details page.
  - Click the **General tab > Workflow**. If the ticket is already delegated, then the **Revoke Delegation** button will be enabled.

1 New	2 In Progress	3 Review	4 Closed
<b>Since:</b> 2016-08-10 10:22:19			
<b>Current Owner(s):</b> [Avatar] (Details <a href="#">↗</a> )			
<b>Stage Actions:</b> 1 of 1 needed for moving workflow to "In Progress"			
1 of 1 needed for moving workflow to "Closed"			
<input type="checkbox"/> <b>Force Transition</b>			
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.			
<div style="display: flex; justify-content: space-between; width: 100%;"> <span>Accept</span> <span>Reject</span> <span>Delegate To</span> <span>Revoke Delegation</span> </div>			

- Click **Revoke Delegation**.
- Enter the reason or comment for revoking delegation access.
- Click **OK**.

## 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.

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.agilance.ticket.update.email.enabled=false`

Parameter	Description
Title	Identifies the ticket
Description	Text description for the ticket
Type	Ticket types include: <ul style="list-style-type: none"> <li>• Entity Control Resolution</li> <li>• Incident Response</li> <li>• Risk Assessment Mitigation</li> <li>• Risk Assessment Remediation</li> <li>• Vulnerability Resolution</li> </ul>
Status	Current workflow stage
Export Status	Indicates whether the ticket is linked to a remote ticket system, such as Remedy

Parameter Category	Description Label that you can run reports on
Disposition	Ticket disposition, as specified in <a href="#">Ticket Management Preferences</a>
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

## Link a Ticket to a Vulnerability

Links between vulnerabilities and tickets are permanent.

### To link a ticket to a vulnerability:

1. Go to Home > Tickets.

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

*The Tickets page.*

2. Locate the ticket, select the ticket and click **Details**.
3. Open the **Linked To** section and click the **Vulnerabilities** tab.

Name	Type	Identifier	Published Date	Modified Date
None.				

*The Vulnerabilities tab of the Linked To section.*

4. Click **Add**.

✕
Select Vulnerabilities

Published between  and

Modified between  and

Search in the National Vulnerability Database.

⚠ More than 250 vulnerabilities found. Showing first 250.

1-100 of 250 Show  rows Page 1 2 3 Go to

Filter by

<input type="checkbox"/> Name	▼ Identifier	Published
<input type="checkbox"/> CVE-2018-9206	CVE-2018-9206	2018-10-11
<input checked="" type="checkbox"/> CVE-2018-8531	CVE-2018-8531	2018-10-10
<input type="checkbox"/> CVE-2018-8513	CVE-2018-8513	2018-10-10
<input type="checkbox"/> CVE-2018-8514	CVE-2018-8514	2018-10-10

**Vulnerabilities to assign**

*The Select Vulnerabilities dialog.*

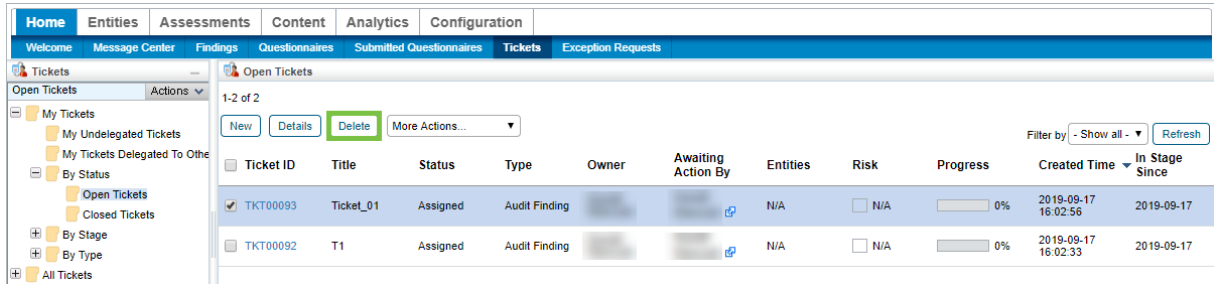
5. Enter the required search criteria for the vulnerability and then click **Search**.
6. Select a vulnerability and click the down arrow to move it to the **Vulnerabilities to assign** field.
7. Click **OK**.

## Delete 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**.



The screenshot shows the 'Tickets' page in a software application. The 'Delete' button is highlighted in green. The table below shows two tickets:

Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
<input checked="" type="checkbox"/> TKT00093	Ticket_01	Assigned	Audit Finding	[Avatar]	[Avatar]	N/A	N/A	0%	2019-09-17 16:02:56	2019-09-17
<input type="checkbox"/> TKT00092	T1	Assigned	Audit Finding	[Avatar]	[Avatar]	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.

The screenshot shows the 'Server Administration' page with the 'Configuration' tab selected. The left sidebar contains a navigation menu with 'Configuration' highlighted. The main content area is titled 'Configuration' and contains several sections: 'Server Name' (with fields for Operating system, Local hostname, Local IP address(es), and Public hostname or IP address), 'Session Timeout' (with a text input field and a help icon), 'Health Report' (with a radio button for 'Automatically send the Health Report to Resolver' and a text input for 'Interval to send the Health Report(Days)'), 'Archiving' (with a radio button for 'Enable Archiving Vulnerabilities' and a text input for 'Vulnerabilities archival period in days since last updated date'), and 'Tickets Archiving' (with a radio button for 'Enable Archiving Tickets' and a text input for 'Archival period in days since last updated date').

*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.

The screenshot shows the 'Tickets Archiving' section of the 'Edit Configuration' screen. It features a radio button for 'Enable Archiving Tickets' with 'Yes' selected. Below it is a text input field for 'Archival period in days since last updated date' with the value '90' entered. A help icon and text are visible at the bottom: '\*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.



## Link a Ticket to a Compensating Control

While vulnerability compensating controls cannot be added to a ticket directly, they can be linked to the ticket so will be automatically attached to each of the ticket's linked entities.

When the ticket is created, all attached vulnerability compensating controls will be added with a **Pending** status to the ticket's attached entities. If a vulnerability compensating control already exists on an attached entity in the **Implemented** status, the status will not change. Closing the ticket will change all attached compensating controls to the **Implemented** status.



A vulnerability compensating control cannot be linked to a ticket unless it already has entities attached to it. If an entity is added to the ticket after a vulnerability compensating control has been linked to it, the compensating control will be applied to that entity.

## To link a ticket to a vulnerability compensating control:

1. Go to Home > Tickets.

Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
TKT00020	sddddd	New	Compensating Control Implementation			1	N/A	100%	2020-04-22 05:09:48	2020-04-27

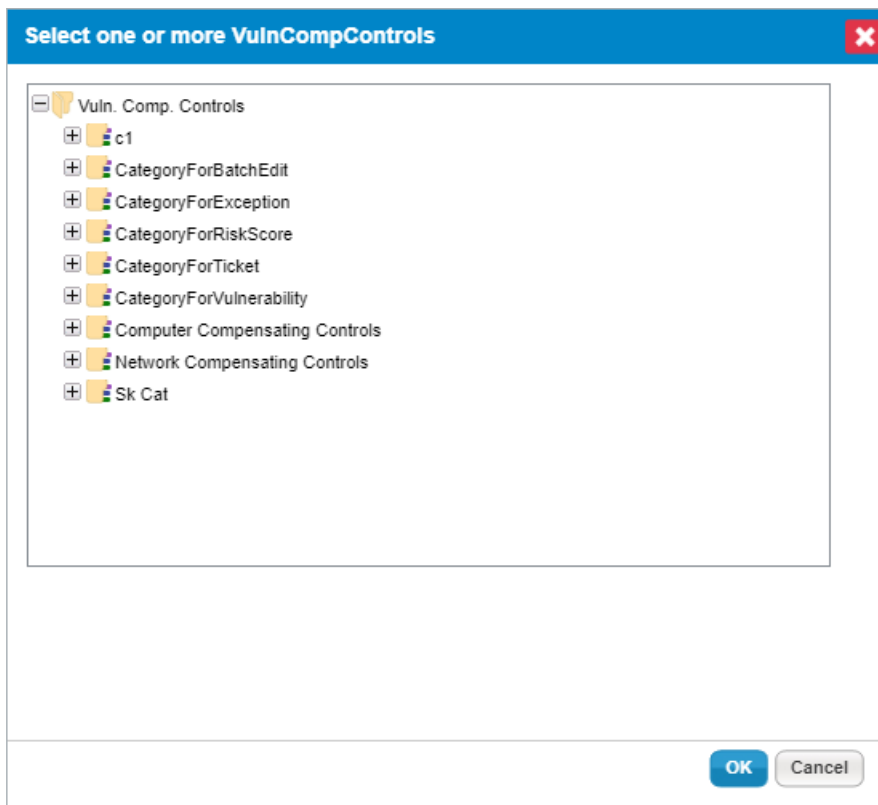
The Tickets page.

2. Click the ticket you wish to link to a vulnerability compensating control.
3. Expand the **Linked To** section and click the **Compensating Controls**.

Name	Type	Entity	Status	Last Updated Time
VCCForRiskScore	Vulnerability Compensating Control	NewEntityForRiskScore001	Pending	2020-04-27 23:18:36.0

The Compensating Controls tab of the Linked To section.

4. Click **Add**.



*The Add Vulnerability Compensating Controls dialogue.*

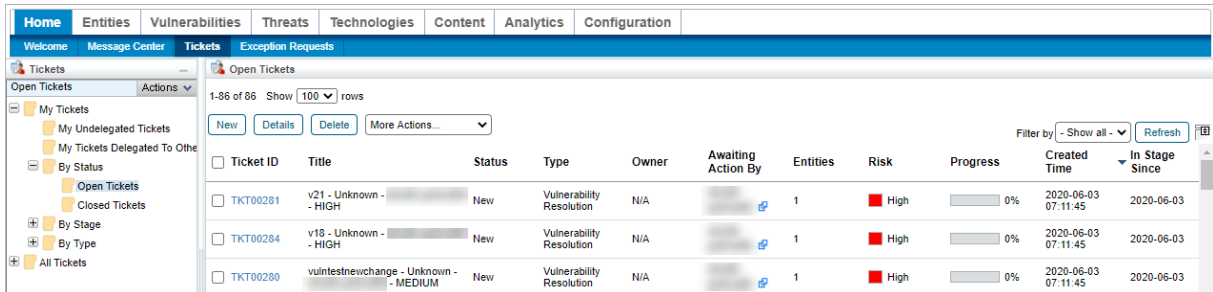
5. Click + next to any category you wish to open and click the checkbox next to any vulnerability compensating controls you wish to add to the ticket.
6. Click **OK**.

## Create a Vulnerability Exception on a Ticket

If required, users can request an exception to be placed on specific vulnerability instances attached to a ticket.

### To create a vulnerability exception from a ticket:

1. Go to Home > Tickets.

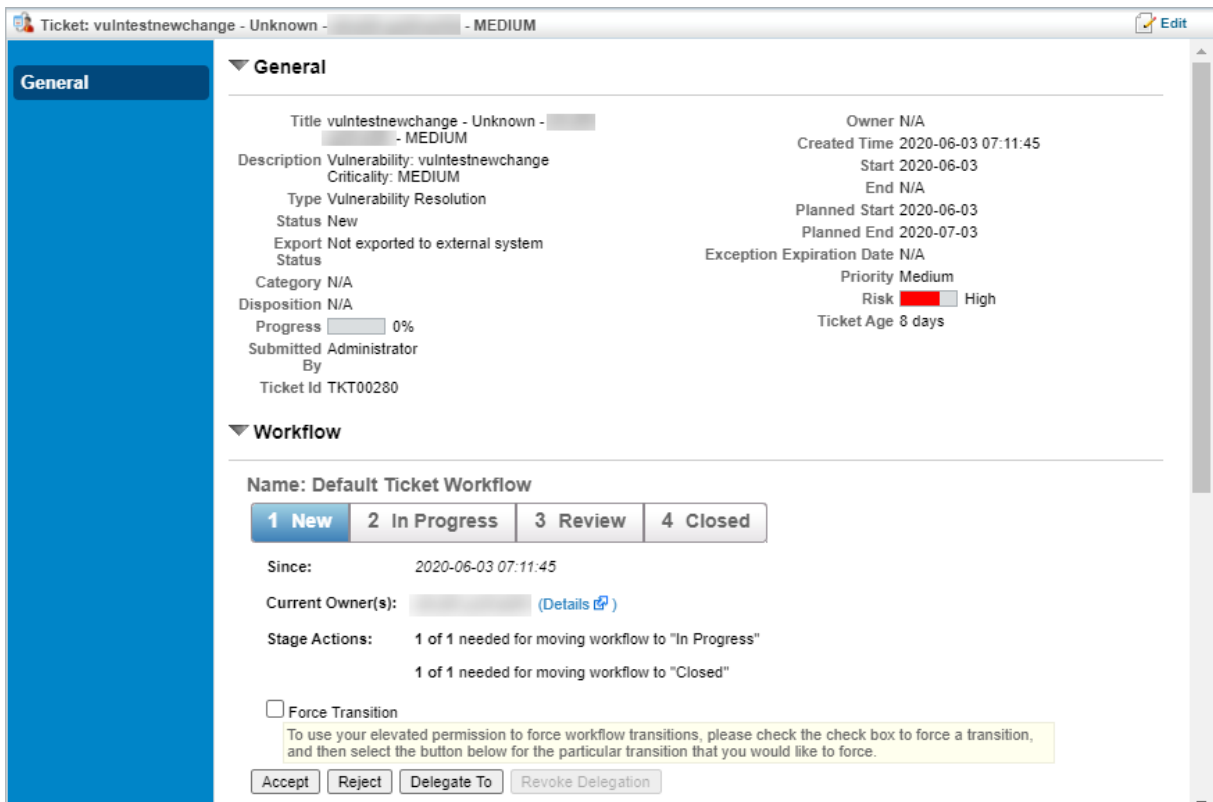


The screenshot shows the 'Tickets' page in a web application. The top navigation bar includes 'Home', 'Entities', 'Vulnerabilities', 'Threats', 'Technologies', 'Content', 'Analytics', and 'Configuration'. Below this is a sub-navigation bar with 'Welcome', 'Message Center', 'Tickets', and 'Exception Requests'. The main content area displays a table of 'Open Tickets' with 1-86 of 86 rows shown. The table has columns for Ticket ID, Title, Status, Type, Owner, Awaiting Action By, Entities, Risk, Progress, Created Time, and In Stage Since. Three tickets are visible:

Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
TKT00281	v21 - Unknown - HIGH	New	Vulnerability Resolution	N/A		1	High	0%	2020-06-03 07:11:45	2020-06-03
TKT00284	v18 - Unknown - HIGH	New	Vulnerability Resolution	N/A		1	High	0%	2020-06-03 07:11:45	2020-06-03
TKT00280	vulntestnewchange - Unknown - MEDIUM	New	Vulnerability Resolution	N/A		1	High	0%	2020-06-03 07:11:45	2020-06-03

The Tickets page.

2. Select the desired ticket and click **Details**.



The screenshot shows the 'Ticket: vulntestnewchange - Unknown - MEDIUM' details page. The page is divided into sections: 'General' and 'Workflow'. The 'General' section contains the following information:

- Title: vulntestnewchange - Unknown - MEDIUM
- Description: Vulnerability: vulntestnewchange, Criticality: MEDIUM
- Type: Vulnerability Resolution
- Status: New
- Export Not exported to external system
- Category: N/A
- Disposition: N/A
- Progress: 0%
- Submitted Administrator: [Name]
- Ticket Id: TKT00280
- Owner: N/A
- Created Time: 2020-06-03 07:11:45
- Start: 2020-06-03
- End: N/A
- Planned Start: 2020-06-03
- Planned End: 2020-07-03
- Exception Expiration Date: N/A
- Priority: Medium
- Risk: High
- Ticket Age: 8 days

The 'Workflow' section shows the 'Name: Default Ticket Workflow' with stages: 1 New, 2 In Progress, 3 Review, 4 Closed. It also displays the 'Since' time (2020-06-03 07:11:45), 'Current Owner(s)', and 'Stage Actions' (1 of 1 needed for moving workflow to "In Progress" and 1 of 1 needed for moving workflow to "Closed"). There is a 'Force Transition' checkbox and a warning message: '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.' Below this are buttons for 'Accept', 'Reject', 'Delegate To', and 'Revoke Delegation'.

The Tickets Details page.

3. Open the **Linked To** section and click the **Vulnerability Instances** tab.

▼ **Linked To**

Entities Vulnerabilities **Vulnerability Instances** Exceptions All Others

1-1 of 1

Resolve Create Exception More Actions... Filter by - Show all - Refresh

<input type="checkbox"/>	Name	Vulnerability Title	Severity	Vulnerability Risk Score	Resolution	Approved Exception Status
<input type="checkbox"/>	5432_M	vulntestnewchange	N/A	N/A	Unresolved	N/A

The Vulnerability Instances tab.

- Select the vulnerability instance you wish to add an exception to and click **Create Exception**.

**Exception Request** [Close]

**1. Basic Details** | **Step 1: Enter Exception Request Information** \* = required

**2. Vuln Instances**

**3. Attach File**

Title\*

Reason for Exception

Start Date  [Calendar]

End Date  [Calendar]

Next Review Date  [Calendar]

Cancel < Back Next > Finish

The Basic Details section of the Exception Request wizard.

- Enter the [basic details](#) of the exception, then click **Next**.

**i** Because this exception is being applied to specific vulnerability instances, there are no **Vulnerability Scope** or **Entities Scope** fields in this version of the Exception Request wizard.

- Review the vulnerability instances the exception will be applied to and click **Next**.

**Exception Request**
✕

1. Basic Details

2. **Vuln Instances**

3. Attach File

**Step 2: Review Vulnerability Instances**

1-1 of 1

\* = required

Filter by

- Show all -

Refresh

Entity Name	▼ Vulnerability Identifier	Severity	Risk Score	Resolution
5432_M	VULN-116	N/A	<input type="checkbox"/> N/A	Unresolved

Cancel

< Back

Next >

Finish

*The Vuln Instances section of the Exception Request wizard.*

7. **Optional:** Add a document from your desktop, link to a document in the repository, or add a URL. For more information, see [Exception Request Attachments](#).

**Exception Request** ✕

1. Basic Details

2. Vuln Instances

3. Attach File

**Step 3: Optionally Attach File**

\* = required

Add a Document or Link

Add a document

Document Location\*  
 No file chosen

Document Caption

Description

Expires On

Add a link to a document in repository

Add a web link

Add a Network Path

Added Documents and Links

▾

Name	Caption	Tags	Description	Uploaded By	Uploaded On	Size	Expires On	Version
<span style="color: blue; font-weight: bold;">i</span> No Documents found.								

*The Attach File section of the Exception Request wizard.*

8. Click Finish.

## Exceptions on Tickets

The exceptions attached to a ticket's assets or vulnerabilities can be viewed in the **Exceptions** tab of the ticket's **Linked To** section.

▼ **Linked To**

Entities Vulnerabilities Vulnerability Instances **Exceptions** All Others

1-1 of 1

Filter by

Exception ID ▲	Exception Name	Entity Names	Exception Type	Object Name(s)	Current Stage	Requester	Is Applied
<a href="#">EXP00726</a>	applied	5432_H	Vulnerability	CMP	Closed	afest	

*A ticket's Exceptions tab.*

The Exceptions tab displays the following information:

- **Exception ID:** The exception's ID automatically generated ID number.
- **Exception Name:** The name the user gave the exception.
- **Entity Names:** The names of the entities the exception has been attached to.
- **Exception Type:** The exception's type.
- **Object Name(s):** The names of the object the exception has been attached to.
- **Current Stage:** The workflow stage that the exception is currently in.
- **Requester:** The user who requested the exception.
- **Is Applied:** Whether or not the exception has been applied to one of its entities.

## About 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 refer to specific websites.

Typically, the document repository is available on the **Content**, **Risks**, and **Administration** menus in RiskVision.

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

The 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. You can 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 extensions, enable the following property:

```
propertycom.agiliance.esapi.allowed.attachment.file.extensions=true.
```

The default value is true.

The Document Repository supports the following file formats:

- 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.) are maintained for files moved within the Document Repository. This applies to 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 moves from one group to another.

Linkages for document collections attached directly to an object are 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 are no longer linked to objects in the document collection.

For more information about assigning ownership to a group or document collection, see [Document Repository Ownership](#).

### To create a group:

1. Open RiskVision Threat and Vulnerability 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 Threat and Vulnerability 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 Document Collection**. The **New Document Collection** dialog appears.

4. Enter Name and Description.

5. 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.

## Modify Ownership

When you create a group or document collection, all RiskVision users are assigned Reader ownership by default.

### To assign ownership to a group:

1. Open RiskVision Threat and Vulnerability 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** dropdown 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 Threat and Vulnerability Manager.
5. Go to **Content > Document Repository**.
6. 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 Threat and Vulnerability 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

Document repository actions, such as delete, cut, and download link, allow you to manage documents and external information for your organization. A combination of document repository permissions and ownership type determines who can view, delete, cut, paste and move the objects in a document repository.

You can perform an action on a group or document collection using the actions dropdown list of a document repository root node, or using the **More Actions** dropdown list. To perform an action on a document or web or network path reference, use the **More Actions** dropdown list from the document collection details page.

The link between a RiskVision object and document repository object (Document Collection, Document) will be preserved only when you add and move the same type of items, but not when you add one type of item and try moving the other type.

- The link is maintained when you add a document collection to an object and move the document collection from one group to another group, and when you add documents to an object and move the documents from one document collection to another.
- The link is not maintained when you add a document collection to an object and move a document out of it. Linking to a document collection means the 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 Threat and Vulnerability 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 from the Document Repository:

1. Go to **Content > Document Repository**.
2. To delete a group or document collection, select the object, then click **Actions > Delete**.
3. To delete a document or web reference, locate the document collection, click the object, and then click **Delete**.

Documents that are linked to objects, such as entities and policies, cannot be deleted. Archive linked documents by moving them to other groups.

## Vulnerability Compensating Controls

Vulnerability compensating controls are measures taken to mitigate the likelihood or impact of the damage that can be caused by an exploited vulnerability. In order to help an organization plan, track, and measure the implementation of compensating controls on a vulnerability, RiskVision enables users to create and assign vulnerability compensating controls.

While users can create their own vulnerability compensating controls and categories to hold them, RiskVision comes with the following by default:

- Computer Compensating Controls (category)
  - Antivirus
  - Application whitelisting
  - Data loss prevention
  - Encryption (at rest)
  - Endpoint detection and response
  - Host Intrusion Prevention
  - IP blacklist
  - IP whitelist
  - Multi-factor authentication
  - Network access control
  - Web application firewall
- Network Compensating Controls (category)
  - Firewall rules (category)
    - Example rule 1
    - Example rule 2
  - Network behavioral analysis
  - Network intrusion prevention
  - Segmentation
  - Web content filtering

Vulnerability compensating controls can be viewed from the **Vulnerability Compensating Controls** grid in the **Content** menu by users with the Threats and Vulnerabilities View or Manage permissions. However, the root menu can only contain categories. Click on a category to view or create vulnerability compensating controls or sub categories.



Home	Entities	Vulnerabilities	Threats	Technologies	Content	Analytics	Configuration
Vulnerability Compensating Controls		Document Repository					
Vulnerability Compensating Con ...		Categories					
<ul style="list-style-type: none"> <li>By Category           <ul style="list-style-type: none"> <li>5140cat1</li> <li>5140cat-2</li> <li>&lt;IFRAME SRC=# onmous</li> <li>&lt;svg onResize svg onRes</li> <li>adfdf</li> <li>C1</li> <li>C1</li> <li>c2</li> <li>c3</li> <li>c4</li> <li>c4</li> <li>c4</li> <li>c4</li> <li>c4</li> <li>c4</li> <li>c5</li> <li>category-1</li> <li>CategoryForBatchEdit</li> <li>CategoryForException</li> <li>CategoryForException1</li> </ul> </li> </ul>		1-43 of 43 Show 100 rows New Category Delete Category More Actions... Filter by - Show all - Refresh					
Type	Title	Description	Created By	Last Updated			
	C1	C1	N/A	N/A			
	c2	c2	N/A	N/A			
	c3	c3	N/A	N/A			
	c4	N/A	N/A	N/A			
	c4	N/A	N/A	N/A			
	c4	N/A	N/A	N/A			
	c4	N/A	N/A	N/A			
	c5	N/A	N/A	N/A			
	Computer Compensating Controls	N/A	N/A	N/A			
	Network Compensating Controls	N/A	N/A	N/A			

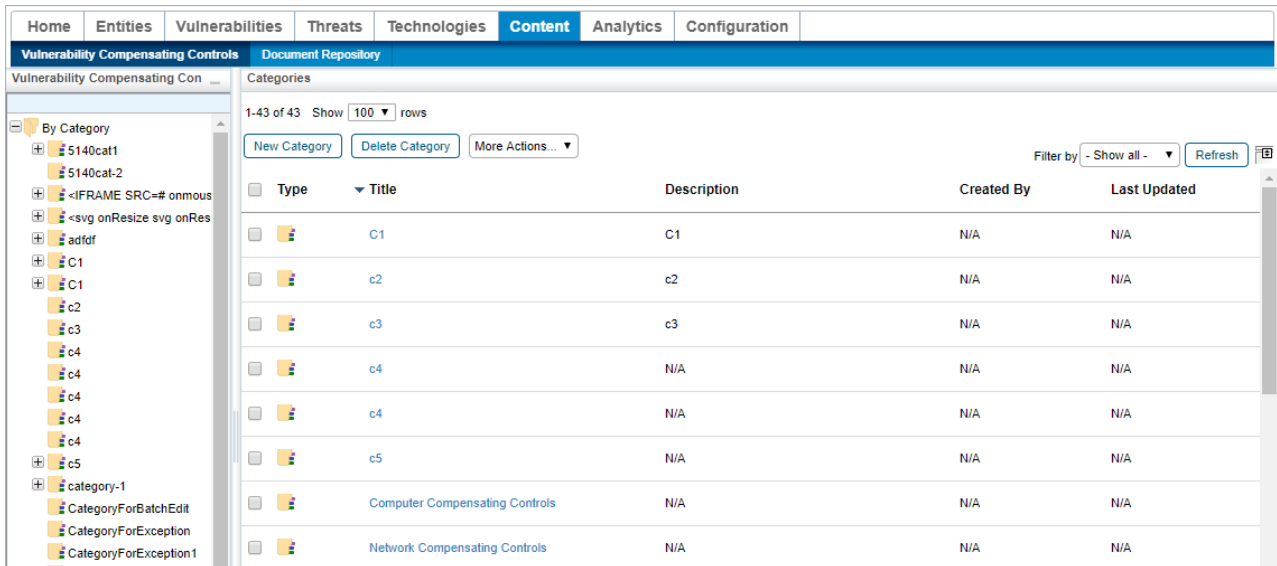
*The Vulnerability Compensating Controls grid.*

The Vulnerability Compensating Controls grid provides the following information:

- **Type:** Whether the item is a category ( ) or a compensating control ( ).
- **Title:** The name of the category or compensating control.
- **Description:** A short description of the category or compensating control.
- **Created By:** Who created the category or compensating control.
- **Last Updated:** When the category or compensating control was last edited.

## Create Categories, Sub Categories & Compensating Controls

Users with the Threats and Vulnerabilities Manage permission can create categories, sub categories, and vulnerability compensating controls on the **Vulnerability Compensating Controls** grid. Vulnerability compensating controls are attached to vulnerabilities in order to mitigate risk, and categories are the containers used to organize the compensating controls or sub categories. As the root page only contains categories, each vulnerability compensating control must belong to a category.

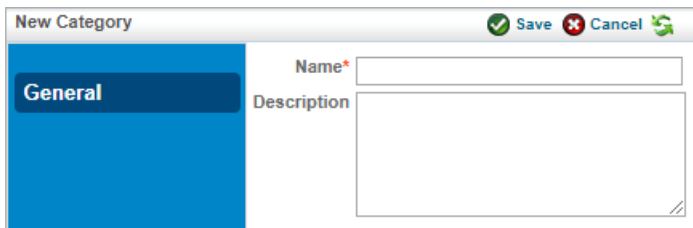


Type	Title	Description	Created By	Last Updated
	C1	C1	N/A	N/A
	c2	c2	N/A	N/A
	c3	c3	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c5	N/A	N/A	N/A
	Computer Compensating Controls	N/A	N/A	N/A
	Network Compensating Controls	N/A	N/A	N/A

The Vulnerability Compensating Controls grid.

### To create a new category:

1. In the Threat & Vulnerability Manager application, click **Vulnerability Compensating Controls** in the **Content** menu.
2. Click **New Category**.

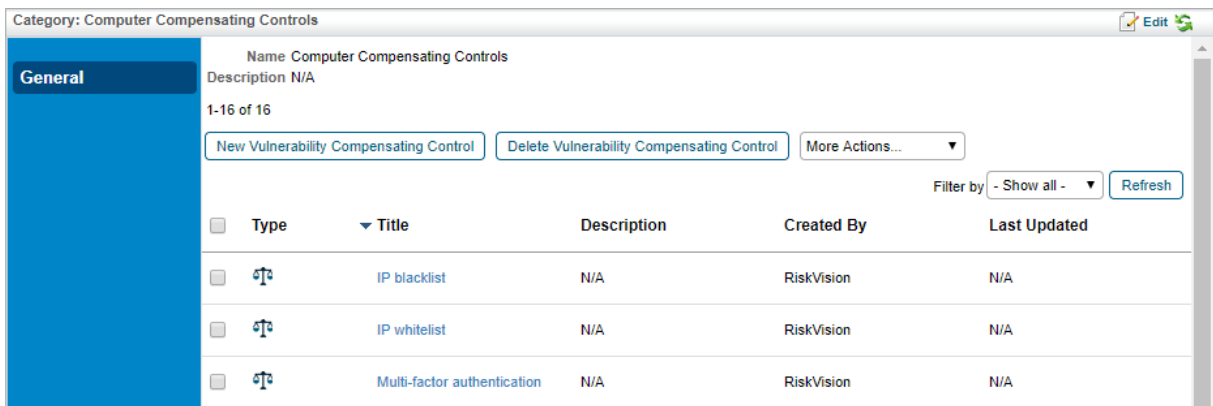


The New Category page.

3. Enter a name in the **Name** field.
4. **Optional:** Enter a description in the **Description** field.
5. Click **Save**.

### To create a new sub category:

1. In the Threat & Vulnerability Manager application, click **Vulnerability Compensating Controls** in the **Content** menu.
2. Click the category you wish to add a sub category to to open its **Category** page.

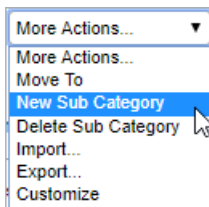


The Category page.

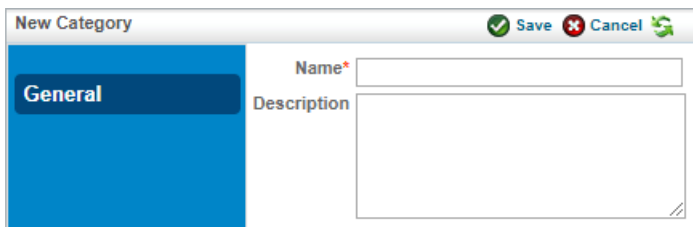


If desired, a sub category can be added to a pre-existing sub category. There is no limit to the number of sub category levels each category can contain.

3. Select **New Sub Category** from the **More Actions...** select list.



The More Actions...  
select list.

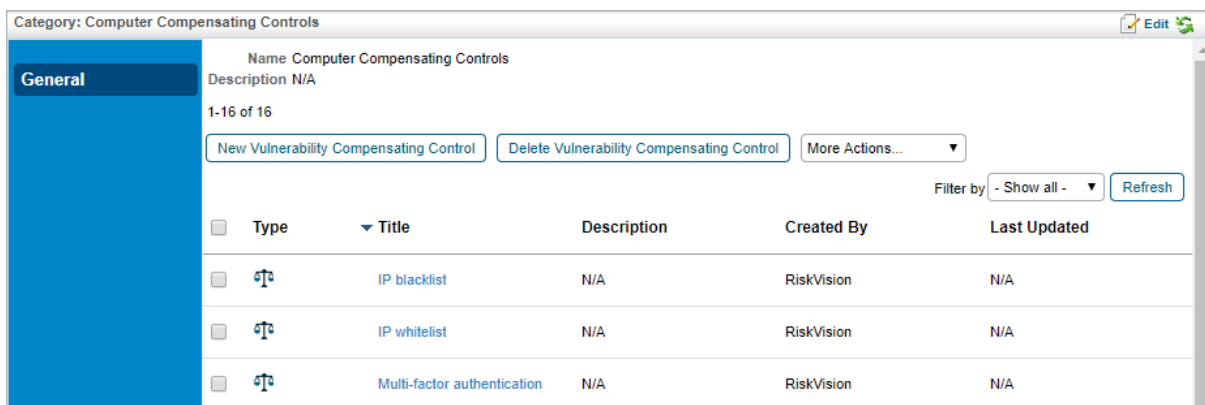


The New Category page.

4. Enter a name in the **Name** field.
5. **Optional:** Enter a description in the **Description** field.
6. Click **Save**.

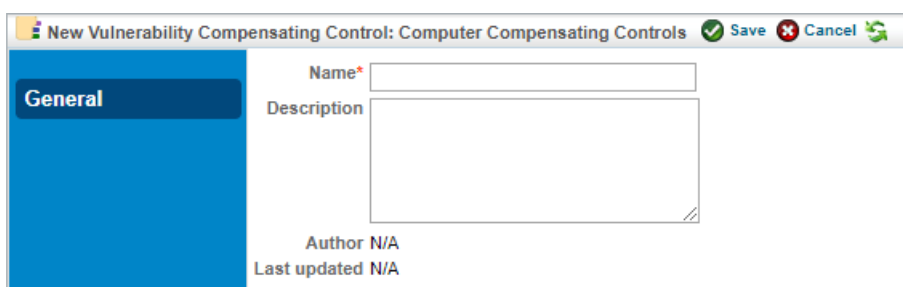
## To create a new vulnerability compensating control:

1. In the **Threat & Vulnerability Manager** application, click **Vulnerability Compensating Controls** in the **Content** menu.
2. Click one of the available categories to open the corresponding **Category** page.



The Category page.

3. Click New Vulnerability Compensating Control.



The New Vulnerability Compensating Control page.

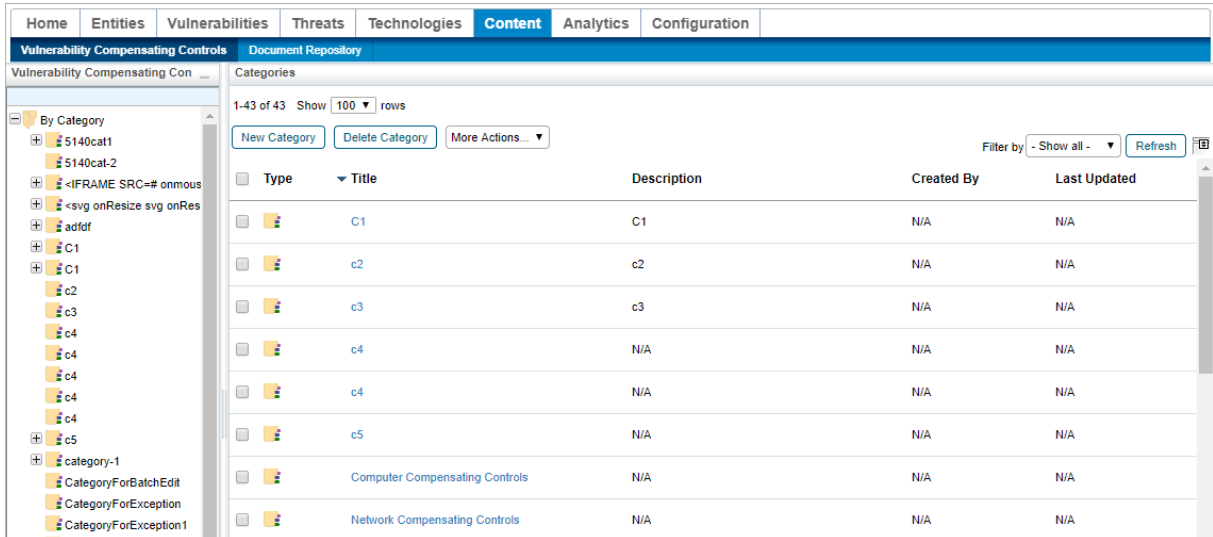
4. Enter a name in the **Name** field.
5. **Optional:** Enter a description in the **Description** field.
6. Click **Save**.

## Edit or Delete Categories, Sub Categories & Compensating Controls

Users with the Threats and Vulnerabilities Manage permission can edit or delete categories, sub categories, and vulnerability compensating controls on the **Vulnerability Compensating Controls** grid.

### To edit or delete categories:

1. In the **Threat & Vulnerability Manager** application, click **Vulnerability Compensating Controls** in the **Content** menu.



Type	Title	Description	Created By	Last Updated
	C1	C1	N/A	N/A
	c2	c2	N/A	N/A
	c3	c3	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c4	N/A	N/A	N/A
	c5	N/A	N/A	N/A
	Computer Compensating Controls	N/A	N/A	N/A
	Network Compensating Controls	N/A	N/A	N/A

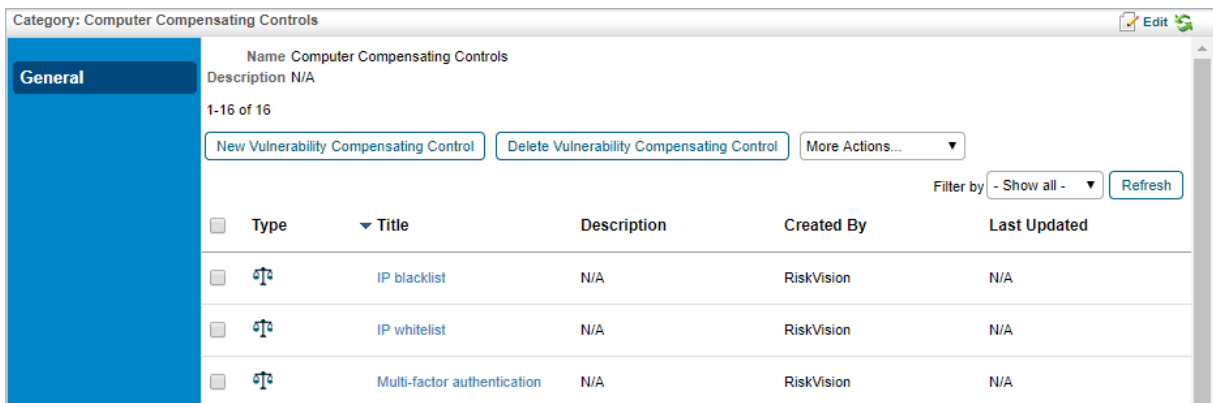
*The Vulnerability Compensating Controls grid.*

2. **Optional:** Click the checkbox next to any categories you wish to delete and click **Delete Category**.



Deleting a category will delete all the sub categories and vulnerability compensating controls attached to it.

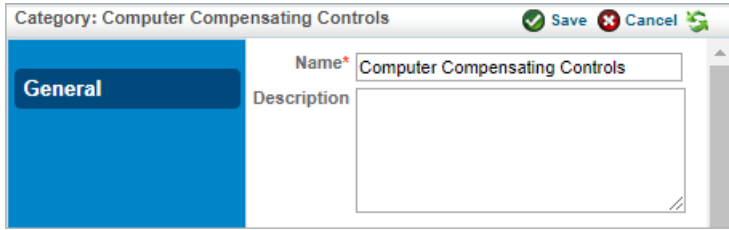
3. Click the category you wish to edit to open its **Category** page.



Type	Title	Description	Created By	Last Updated
	IP blacklist	N/A	RiskVision	N/A
	IP whitelist	N/A	RiskVision	N/A
	Multi-factor authentication	N/A	RiskVision	N/A

*The Category page.*

4. Click **Edit**.

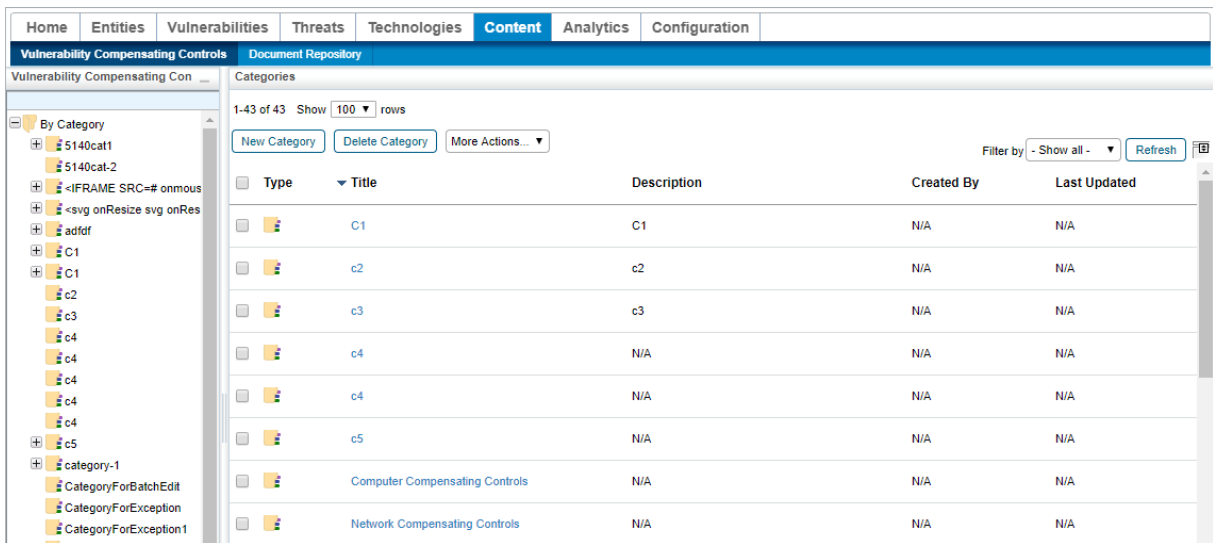


The Edit Category page.

5. Change the **Name** or **Description** of the category as desired.
6. Click **Save**.

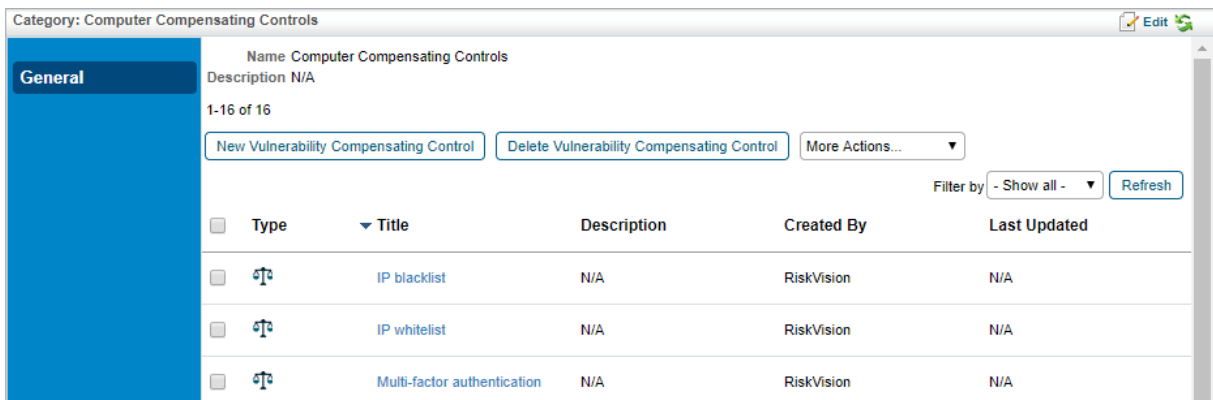
## To edit or delete a sub category:

1. In the **Threat & Vulnerability Manager** application, click **Vulnerability Compensating Controls** in the **Content** menu.



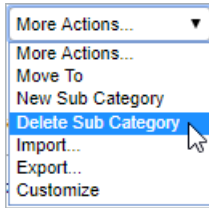
The Vulnerability Compensating Controls grid.

2. Click the category containing the sub category you wish to edit or delete to open its **Category** page.




The Category page.

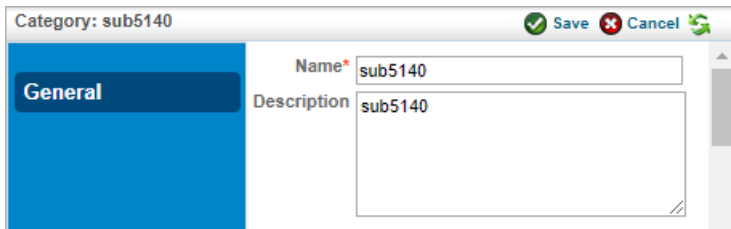
3. **Optional:** Click the checkbox next to any sub categories you wish to delete and select **Delete Sub Category** from the **More Actions...** select list.



The More Actions select list.

 Deleting a sub category will delete all the sub categories and vulnerability compensating controls attached to it.

4. Click the sub category you wish to edit.
5. Click **Edit**.

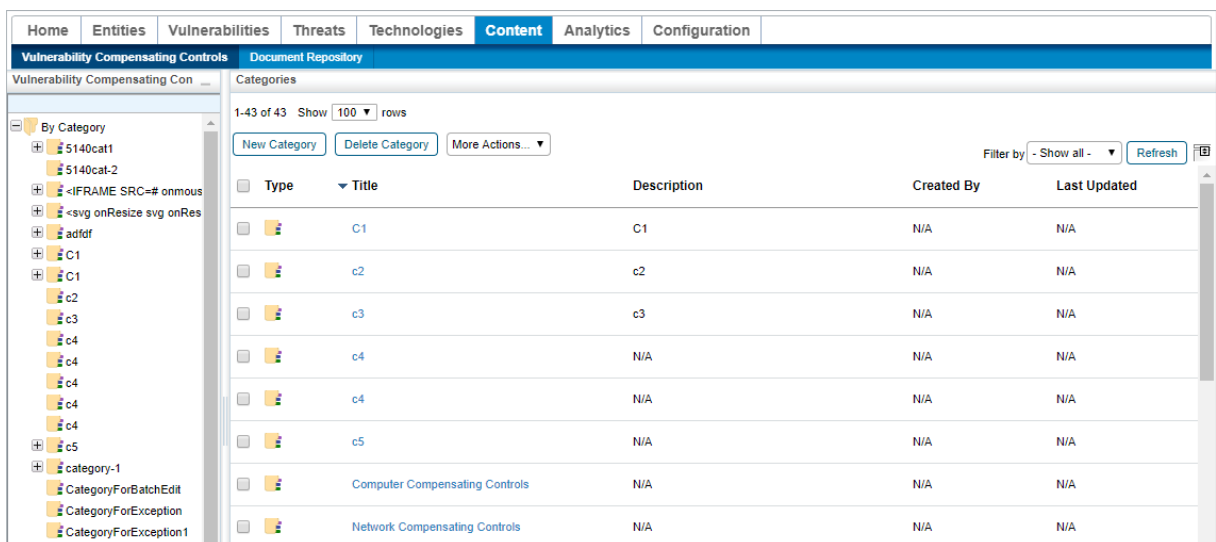


The Edit Sub Category page.

6. Change the **Name** or **Description** of the category as desired.
7. Click **Save**.

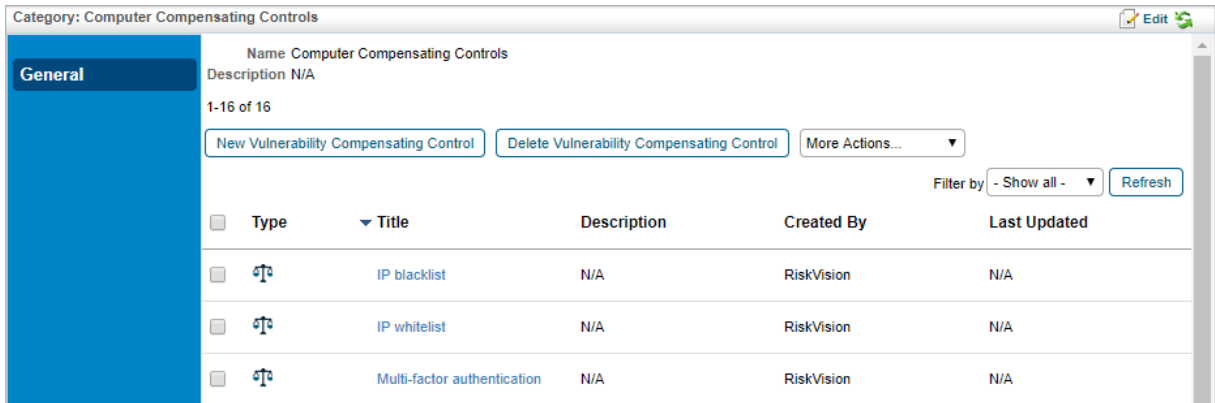
## To edit or delete a vulnerability compensating control:

1. In the Threat & Vulnerability Manager application, click **Vulnerability Compensating Controls** in the **Content** menu.



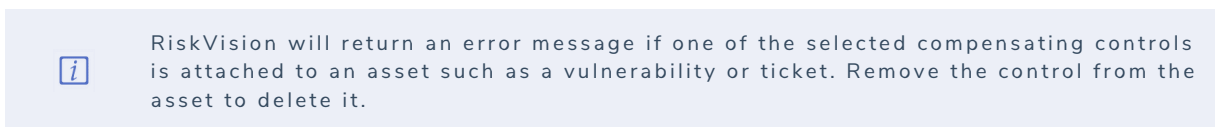
The Vulnerability Compensating Controls root page.

2. Click the category that contains the control or controls you wish to edit or delete to open its **Category** page.

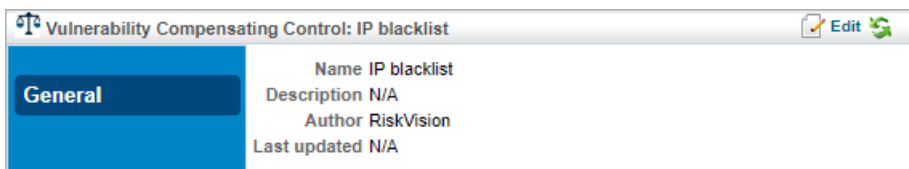


The Category page

- Optional: Click the checkbox next to any compensating controls you wish to delete and click **Delete Vulnerability Compensating Control**.

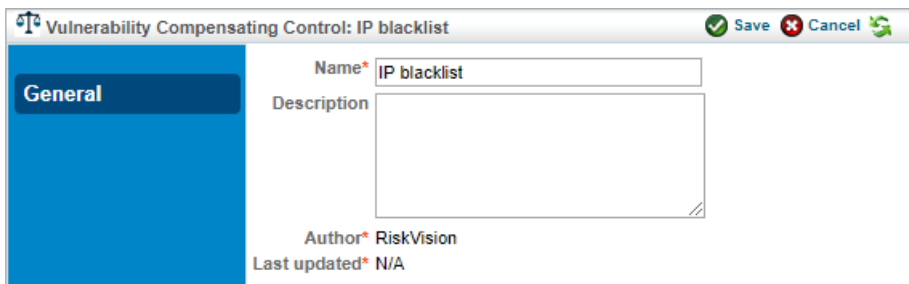


- Click the control you wish to edit to open its **Vulnerability Compensating Control** page.



The Vulnerability Compensating Control page.

- Click **Edit**.



The Edit Vulnerability Compensating Control page.

- Change the **Name** or **Description** of the control as desired.
- Click **Save**.

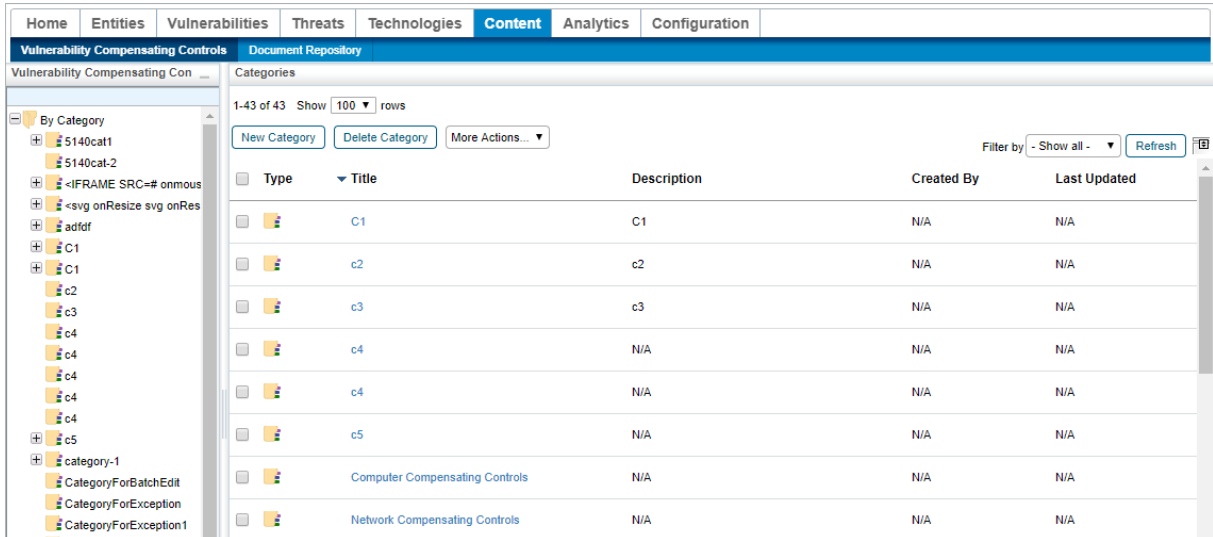


## Move Sub Categories & Compensating Controls

Users with the Threats and Vulnerabilities Manage permission can move sub categories and vulnerability compensating controls from one category to another. Top-level categories cannot be moved.

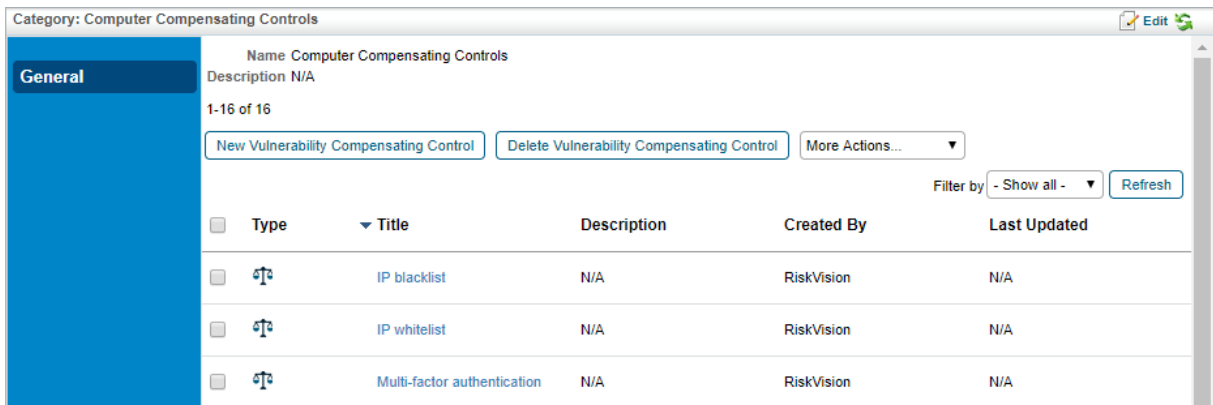
### To move a sub category or compensating control:

1. In the Threat & Vulnerability Manager application, click **Vulnerability Compensating Controls** in the **Content** menu.



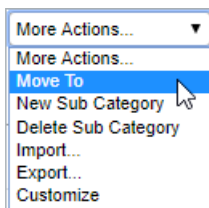
*The Vulnerability Compensating Controls root page.*

2. Click on the category that contains the sub categories or compensating controls you wish to move.



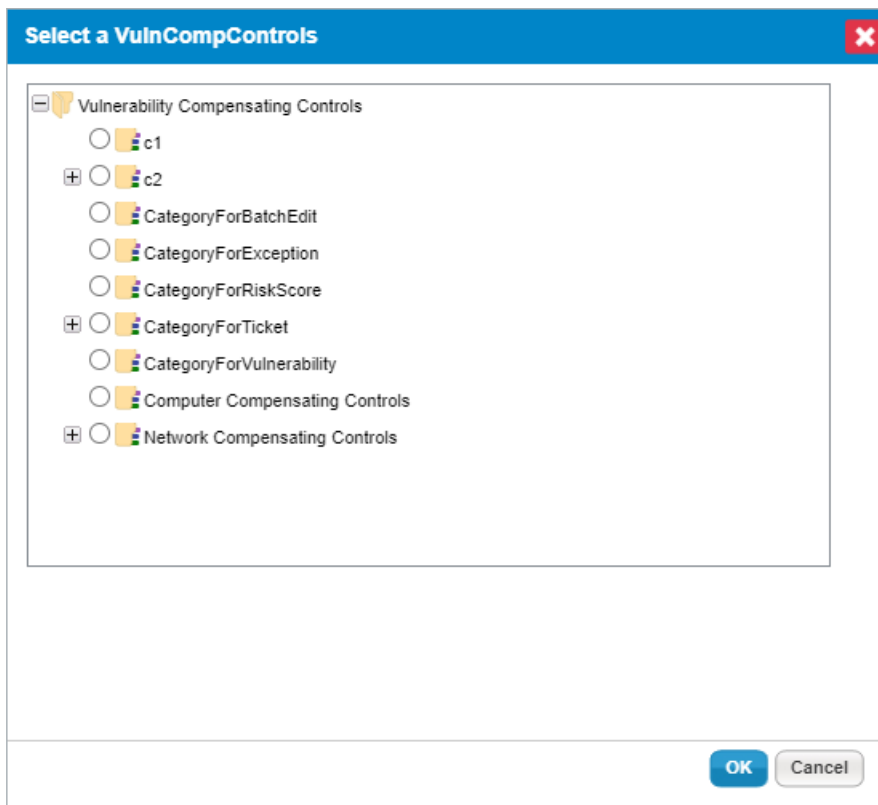
*The Category page.*

3. Click the checkbox next to each sub category or compensating control you wish to move and select **Move To** from the **More Actions...** select list.



*The More Actions... select list.*

4. Click the radio button next to the category or sub category you wish to move the selected items to.



*The Select a VulCompControls dialogue.*

5. Click **OK**.

## Add a Compensating Control to a Vulnerability

Once a vulnerability compensating control has been [created](#), it must be added to a vulnerability to have an effect. Vulnerability compensating controls can be added from a vulnerability's **Vulnerability Compensating Controls** tab by a user with the Threats and Vulnerabilities View and Update permissions.

### To add a vulnerability compensating control to a vulnerability:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities**, **Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Click a vulnerability.

The screenshot shows the 'Vulnerability: VulnerabilityForCompControl' page. The left sidebar contains navigation options: General, CVSS v2.0 Score, Enhanced Score, Risk Score, Comp Controls, Identification, More Information, References, Exploits, Risk, Affected Entities, Tickets, Technologies, Patches, Exceptions, CVSS v3 Score, and Threats. The main content area is divided into three sections: **Vulnerability** (Title: VulnerabilityForCompControl, Description: VulnerabilityForCompControl, Identifier: VULN-19, Owner: [redacted], References: N/A, Severity: N/A, Likelihood: N/A, Weaknesses: N/A, Source: [redacted], Secondary Source: N/A, Early warning: No, Status: New, System Info: New by User), **Acknowledgement** (Acknowledged: No, Comment: N/A, Applicable: Yes, with an 'Acknowledge' button), and **Change History** (Results as of 2020-05-04 11:54:24, More Actions... dropdown, Filter by: - Show all -, Refresh button). A table with columns 'Change', 'Who', and 'When' is shown below, with a message 'No change records found.'

*The Vulnerability details page.*

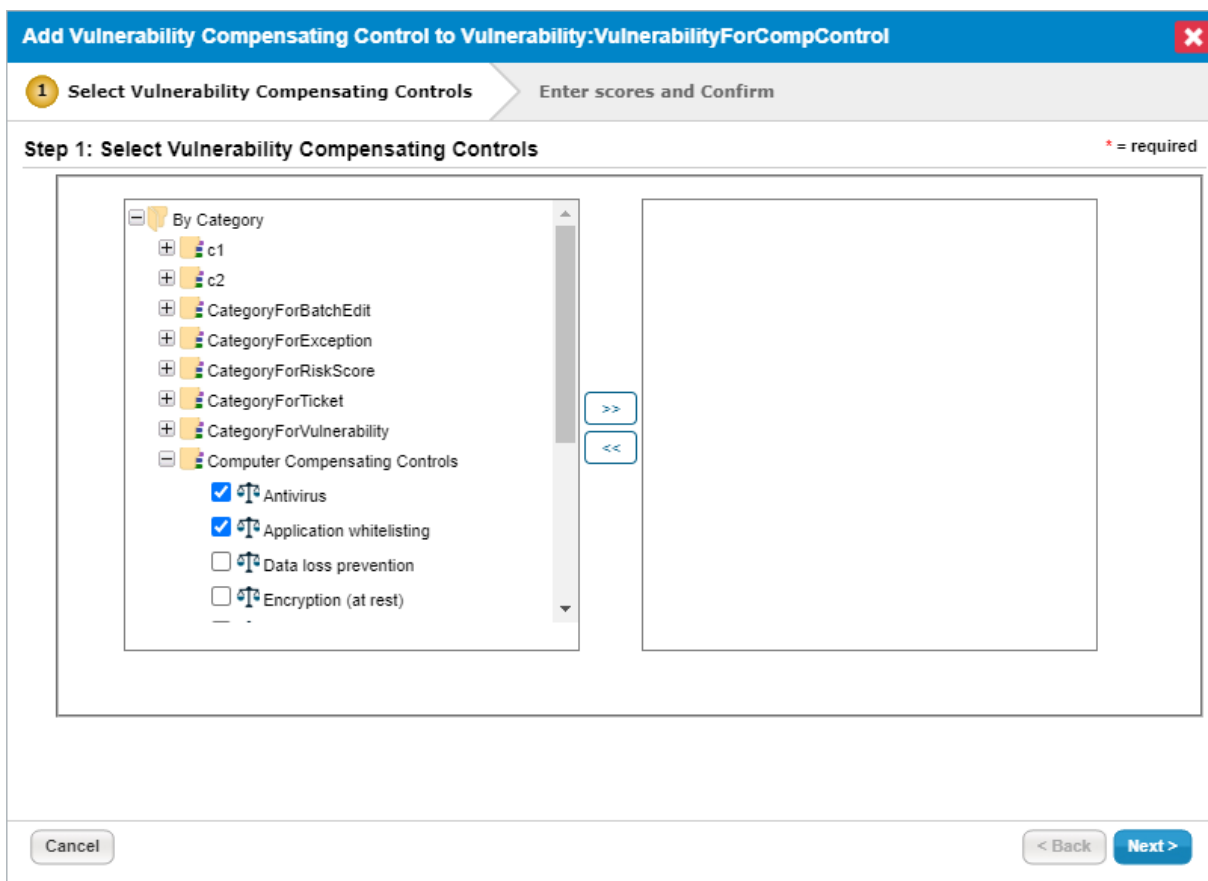
4. Click **Comp Controls** to open the **Vulnerability Compensating Controls** tab.

The screenshot shows the 'Vulnerability Compensating Controls' tab for 'Vulnerability: VulnerabilityForCompControl'. It displays '1-1 of 1' control. There are 'Add', 'Delete', and 'Edit' buttons. A table lists the control with columns: Title, Description, Category, Detection %, Protection %, and Total %. The control is 'VCCForVulnerability' with a description 'VCCForVulnerability', category 'CategoryForVulnerability', 10% detection, 20% protection, and 30% total. There are also 'Filter by: - Show all -' and 'Refresh' buttons.

Title	Description	Category	Detection %	Protection %	Total %
<input type="checkbox"/> VCCForVulnerability	VCCForVulnerability	CategoryForVulnerability	10	20	30

*The Vulnerability Compensating Controls tab.*

5. Click **Add**.
6. In the left window, click + next to each category you wish to open and click the checkbox next to each vulnerability compensating control you wish to add to the vulnerability.



Step 1 of the Add Vulnerability Compensating Control to Vulnerability dialog.

7. Click >> to add the selected vulnerability compensating controls to the right window.
8. Click **Next**.
9. Enter the initial **Detection %** and **Protection %** for each of the vulnerability compensating controls. These values can be changed later. The sum of a single vulnerability compensating control's fields cannot exceed 100%. However, the total sum of all compensating controls may exceed 100%.

✕
**Add Vulnerability Compensating Control to Vulnerability:VulnerabilityForCompControl**

1
Select Vulnerability Compensating Controls
Enter scores and Confirm

**Step 2: Enter scores and Confirm** \* = required

Please enter detection and protection reduction scores for each selected Vulnerability Compensating Control

1-2 of 2

Name	Detection %	Protection %
Antivirus	<input style="width: 30px;" type="text" value="20"/>	<input style="width: 30px;" type="text" value="30"/>
Application whitelisting	<input style="width: 30px;" type="text" value="40"/>	<input style="width: 30px;" type="text" value="20"/>

Cancel
< Back
Finish

*Step 2 of the Add Vulnerability Compensating Control to Vulnerability dialogue.*

10. Click Finish.

## Edit a Compensating Control Attached to a Vulnerability

Once a vulnerability compensating control has been added to a vulnerability, its **Detection %** and **Protection %** values can be edited at any time by a user with the Threats and Vulnerabilities View and Update permissions.

### To edit the values of a vulnerability compensating control attached to a vulnerability:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities**, **Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Click a vulnerability.

The screenshot shows the 'Vulnerability: VulnerabilityForCompControl' page. The left sidebar contains navigation options: General, CVSS v2.0 Score, Enhanced Score, Risk Score, Comp Controls, Identification, More Information, References, Exploits, Risk, Affected Entities, Tickets, Technologies, Patches, Exceptions, CVSS v3 Score, and Threats. The main content area is divided into three sections:
 

- Vulnerability:** Fields include Title (VulnerabilityForCompControl), Description (VulnerabilityForCompControl), Identifier (VULN-19), Owner, References (N/A), Severity (N/A), Likelihood (N/A), Weaknesses (N/A), Source, Secondary Source (N/A), Early warning (No), Status (New), and System Info (New by User).
- Acknowledgement:** Fields include Acknowledged (No), Comment (N/A), and Applicable (Yes). An 'Acknowledge' button is present.
- Change History:** Shows results as of 2020-05-04 11:54:24. A table with columns 'Change', 'Who', and 'When' is shown, but it contains the message 'No change records found.'

The Vulnerability details page.

4. Click **Comp Controls** to open the **Vulnerability Compensating Controls** tab.

The screenshot shows the 'Vulnerability Compensating Controls' tab for the same vulnerability. It displays a table with one row of controls. The table has columns for Title, Description, Category, Detection %, Protection %, and Total %. The 'Vulnerability Compensating Controls' section includes 'Add', 'Delete', and 'Edit' buttons, a filter dropdown set to '- Show all -', and a 'Refresh' button.

Title	Description	Category	Detection %	Protection %	Total %
VCCForVulnerability	VCCForVulnerability	CategoryForVulnerability	10	20	30

The Vulnerability Compensating Controls tab.

5. Click either **Edit** or in the **Detection %** or **Protection %** fields of a vulnerability compensating control to open the **Edit Vulnerability Compensating Controls** page.

Vulnerability: VulnerabilityForCompControl

**Vulnerability Compensating Controls**

1-1 of 1

Filter by

<input type="checkbox"/>	Title	Description	Category	Detection %	Protection %	Total %
<input type="checkbox"/>	VCCForVulnerability	VCCForVulnerability	CategoryForVulnerability	<input type="text" value="10"/>	<input type="text" value="20"/>	30

*The Edit Vulnerability Compensating Controls page.*

6. Make any changes to the **Detection %** or **Protection %** fields as required. The sum of a single row cannot exceed 100%. Because some vulnerability compensating controls may be used by multiple assets, the total sum of all fields may exceed 100%.
7. Click **Save Changes** to save your edits and continue editing, or **Save and Exit** to save your edits and return to the **Vulnerability Compensating Controls** tab.

## Remove a Compensating Control From a Vulnerability

If a vulnerability compensating control has been added to a vulnerability in error, or if it no longer applies to the vulnerability, it can be removed by a user with the Threats and Vulnerabilities View and Update permissions. Removing the vulnerability compensating control from a vulnerability will not delete it, but it will clear the assigned **Detection %** and **Protection %** values for this vulnerability.

### To remove a vulnerability compensating control from a vulnerability:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities**, **Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Click a vulnerability.

The screenshot shows the 'Vulnerability: VulnerabilityForCompControl' page. The left sidebar contains a navigation menu with options like 'General', 'CVSS v2.0 Score', 'Enhanced Score', 'Risk Score', 'Comp Controls', 'Identification', 'More Information', 'References', 'Exploits', 'Risk', 'Affected Entities', 'Tickets', 'Technologies', 'Patches', 'Exceptions', 'CVSS v3 Score', and 'Threats'. The main content area is divided into sections: 'Vulnerability' (Title: VulnerabilityForCompControl, Description: VulnerabilityForCompControl, Identifier: VULN-19, Owner: [redacted], References: N/A, Severity: N/A, Likelihood: N/A, Weaknesses: N/A, Source: [redacted], Secondary Source: N/A, Early warning: No, Status: New, System Info: New by User), 'Acknowledgement' (Acknowledged: No, Comment: N/A, Applicable: Yes, with an 'Acknowledge' button), and 'Change History' (Results as of 2020-05-04 11:54:24, More Actions... dropdown, Filter by: - Show all -, Refresh button). A table with columns 'Change', 'Who', and 'When' is shown below, with a message 'No change records found.'

*The Vulnerability details page.*

4. Click **Comp Controls** to open the **Vulnerability Compensating Controls** tab.

The screenshot shows the 'Vulnerability Compensating Controls' tab for 'Vulnerability: VulnerabilityForCompControl'. It displays '1-1 of 1' controls. There are 'Add', 'Delete', and 'Edit' buttons. A table lists the controls with columns: Title, Description, Category, Detection %, Protection %, and Total %. The table contains one row: 'VCCForVulnerability' with Description 'VCCForVulnerability', Category 'CategoryForVulnerability', Detection % '10', Protection % '20', and Total % '30'. There is a checkbox next to the title and a 'Filter by' dropdown set to '- Show all -' with a 'Refresh' button.

*The Vulnerability Compensating Controls tab.*

5. Click the checkbox next to each vulnerability compensating control you wish to delete.
6. Click **Delete** and then **OK**.

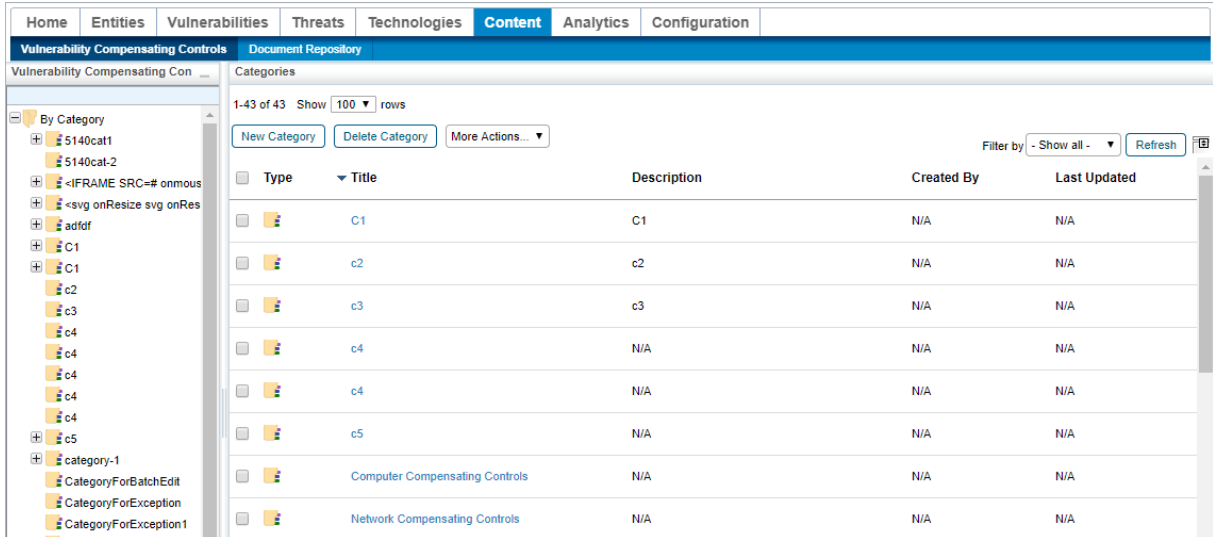


## Export & Import Categories & Sub Categories

While individual vulnerability compensating controls cannot be exported or imported, RiskVision does allow for the importing and exporting of categories and sub categories as .xml files. This allows for the categories, the sub categories, and their related compensating controls attached to them to be transferred between servers.

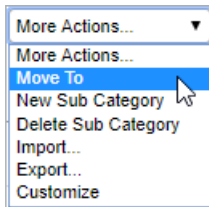
### To export categories and sub categories:

1. In the Threat & Vulnerability Manager application, click **Vulnerability Compensating Controls** in the **Content** menu.



*The Vulnerability Compensating Controls root page.*

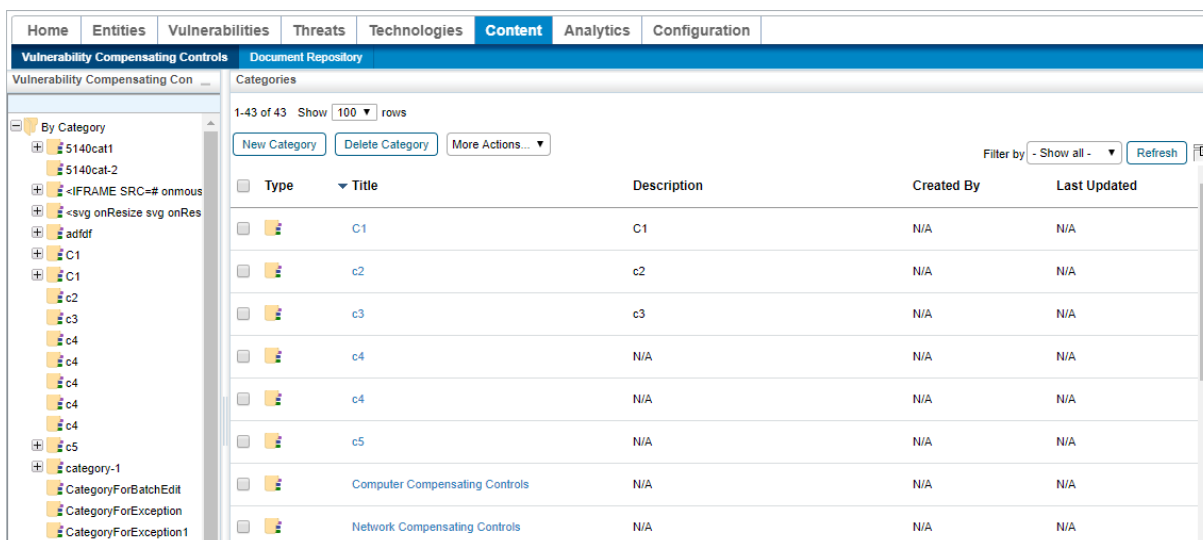
2. **Optional:** If you just wish to export a sub category, click on the category that contains the sub category you wish to export.
3. Click the checkbox next to each category or sub category you wish to export and select **Export** from the **More Actions...** select list.



*The More Actions...  
select list.*

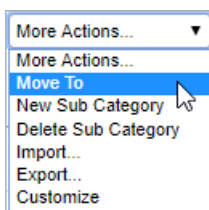
### To import categories and sub categories:

1. In the Threat & Vulnerability Manager application, click **Vulnerability Compensating Controls** in the **Content** menu.



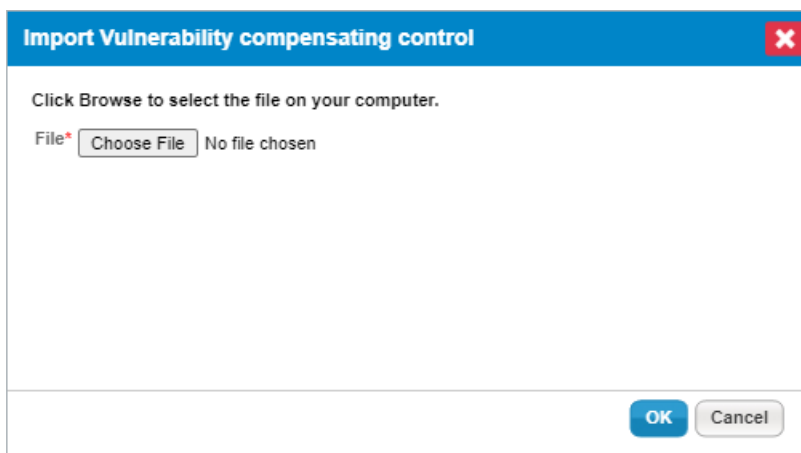
The Vulnerability Compensating Controls root page.

2. **Optional:** If you wish to import a category or sub category into an existing category, click on the desired category.
3. Click the checkbox next to each sub category or compensating control you wish to transfer and select **Import** from the **More Actions...** select list.



The More Actions... select list.

4. Click Choose File.



The Import Vulnerability Compensating Control window.

5. Select the .xml file you wish to import and click **Open**.
6. Click **OK**.

## Data Correlation

- Vulnerability Deduplication: How are vulnerabilities caught by a scanner and by the patch management tool correlated?
  - Deduping is done by CVE per asset per port.

### EXAMPLE

You have two Tomcat servers on a machine and two vulnerability scanners. Your scanners would show four total vulnerabilities, but RiskVision would dedupe so that it would only show as two vulnerabilities, one for each instance of Tomcat.

- How is the many-to-many CVE-patch relationship managed?
  - We can correlate on a per CVE basis. See previous question.
- Is risk measured at the CVE or patch level?
  - RiskVision scores risk at the vulnerability instance level. A patched risk is equal to the sum of the risks of the vulnerability instances that the patch remediates. Patched risks are not currently displayed in the user interface; however, the data relationships are available to generated this information in reports.
- How are discrepancies managed? For example, the vulnerability scanner says there's a MS17-010 vulnerability, but patch management says it's already been applied.
  - If a Patch Management tool says a patch has been applied and scanner hasn't seen the patch, there are two possible scenarios:
    1. A timing difference (example, no updated scan since the patch was applied). We recommend that the ticket is updated when a patch is applied. However, we don't close the vulnerability or ticket until another scan is run and RiskVision has verified that the vulnerability is no longer present on that host.
    2. The scanner could be erroneously missing the patch. We recommend that you label the vulnerability as a false positive using the **Status** field of the vulnerability, or create a vulnerability exception.
- Are all of the above configurable?
  - Generally, yes. For more information, contact [Resolver Support](#).
- Is manual correlation occasionally required? For example, do I need to update correlation rule sets as new patches/vulnerabilities are released?
  - As long as the data sources that are being sent to RiskVision do not have errors (e.g. CMDB repositories, vulnerability scanners, threat intelligence feeds, etc.), manual correlation should not be required. RiskVision provides two types of automated vulnerability-related correlation:
    1. **By CVE:** Vulnerability scanners typically identify vulnerabilities using their own IDs (e.g. Qualys QID, Nessus Plug-In #). When the source scanner provides CVE cross-references, RiskVision automatically correlates CVE associations with assets. Once RiskVision has asset-to-CVE associations, the system can perform vulnerability instance deduplication when multiple scanners report the same vulnerabilities. This allows RiskVision to infer threats and exploits, both of which are highly useful to automate vulnerability risk scoring. This also facilitates patch-to-asset correlation.
    2. **By CPE:** This is used when RiskVision is aware of a vulnerability definition, but doesn't know which assets the vulnerability applies to. A common scenario where this might occur is a zero-day vulnerability, which by definition will not be caught by any scanner. A vulnerability advisory service would typically indicate which technologies are affected and the steps to exploit the vulnerability. Through CPE correlation, RiskVision can identify the assets affected by a zero-day vulnerability.

CPE correlation is also valuable when assets can only be scanned on a low-frequency basis (e.g. due to difficulty of obtaining credentials for credentialed scans or due to performance effects on critical assets). Using CPE correlation, RiskVision can take vulnerability definitions from the National Vulnerability Database or another vulnerability advisory service and correlate these definitions to the assets that are affected by the vulnerabilities.

## Owner Stakeholder Assignment

- How are asset owners and other involved stakeholders correlated? For example, if one person is responsible for ticket but other people own the associated risk. Please demonstrate how this can be managed (CMDB, Active Directory OU, internally managed asset lists, etc.)
  - Asset ownership is easy to configure in RiskVision. You can specify one owner for an asset, another owner for a ticket, and another owner for any identified risk. Entities, such as assets or apps, can have multiple stakeholders, and we can integrate your Active Directory OU to use your existing role structure. Although this is all out of the box configuration, because of the flexibility in the tool, it's important to think through how you model this structure. For example, you may want to model both hardware components and software components as assets, each of which have owners. Once modeled, you can integrate with your existing technologies like your CMDB to perform the following operations:
    - Import your entities
    - Import the relationship of those entities to each other (i.e. Server1 hosts DB1 and App1),
    - Import the organizations hierarchy.
- How granular can stakeholder assignment be? For example, one piece of software on a particular asset might have a different responsible party than another piece of software on that same asset.
  - Multiple owners can be assigned to assets, such as the primary owner, business owner, and executive owner. The types of ownership allows you to easily set up workflows and assign different owner types to different stages of the workflow. The ownership types are completely configurable.

## Customize or Configure

- How many tiers are available for risk visibility?
  - Up to 15 levels of organizational hierarchy plus lots of flexibility in how you structure it.
- Are devices correlated to employees and organizational structures?
  - Yes. Once you have your org structure configured, you simply assign your entities to the appropriate hierarchy level.
- Given a data source that provides employee IDs with their supervisor's ID, and logic that can determine an asset's primary user's ID, can visibility be given based on org chart? For example, could I see the risks for workstations of those who report to me?
  - Yes. This can be done two ways:
    1. Reporting: Create a query that pulls the user's manager from the user record along with all assets those users own and the associated risk of each asset.
    2. Model Manager as a custom attribute. This all comes down to how you model your organizational structure and how you prefer to keep your data in sync.

## Assets

- How are assets correlated between sources?
  - RiskVision provides very flexible reconciliation methods that will accommodate virtually any deployment scenario, including those where an organization is using DHCP and IoT devices. In DHCP environments where the IP address is always changing, our customers typically reconcile by MAC address.
- Criticality/impact: where and how is this determined?
  - Business Criticality is set at the entity level by setting the Confidentiality, Integrity and Availability ratings. There is also an entity import template that allows you to import your pre-defined criticality data. This is a low amount of effort to do.
  - To create an exception in RiskVision, you select a vulnerability and some or all of the assets associated with it and create a due date and owner of the exception. You can also create an exception on a single asset and the associated vulnerabilities on that asset. Those are just two approaches, but there are other approaches, all of which are standard out of the box configuration.

Computer: DesktopID1012 Save Cancel 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

**Business Criticality**

Business Criticality  Low

**Security Requirements** Refresh

Confidentiality  Unknown  Low  Medium  High

Integrity  Unknown  Low  Medium  High

Availability  Unknown  Low  Medium  High

Accountability  Unknown  Low  Medium  High

**Classification**

Type Of Data

Environment Type

Classification Label

Internal or external

**Tags**

**Change History**

Top secret

Highly confidential

Proprietary

Internal use only

Public

*Using the Classification Label settings to set the Business Criticality.*

## Risk Scoring with Threat Modeling

- What knobs / dials exist that allow us to tailor a model to specific threats targeting our organization? For example, if a line of service is being targeted and that actor is known to use certain methods, could we increase the risk score on those assets that are vulnerable?
  - There are two types of knobs / dials you can use to control vulnerability prioritization expressed in terms of risk score:
    - **Vulnerability Risk Factor:** You can control the magnitude of the Threat Factor, which signifies whether there is a threat targeting a vulnerability. There is an Exploit Factor that is auto-selected based on the type of exploit, with remotely executed exploits getting the highest weighting. This is not currently adjustable out of the box, but the values do automatically change based on the type of exploit.
    - **Asset Criticality Factor** - You can model virtually any attribute of the asset on which a vulnerability is found, such as the line of business it belongs to, whether it is Internet-facing, and the type of data that is stored on the asset. Each attribute value is associated with a weighting that will influence the Asset Criticality Factor, and therefore the risk score.

## Workflow & Ticketing

- How are vulnerabilities grouped into tickets?
  - Out of the box, RiskVision supports virtually any grouping that maps to the way in which your organization chooses to fix vulnerabilities. For example, vulnerabilities can be grouped by BU, operating system, asset criticality, and/or asset owner.
- Are multiple vulnerabilities allowed on the same asset?
  - Yes
- Can multiple assets be associated with the same vulnerability?
  - Yes
- Can you have multiple assets with multiple vulnerabilities in the same application (or patch)?
  - Yes
- If multiple criteria above are employed, how is duplication between them handled? For example, would we potentially see one ticket for asset A that includes vulnerability B, and another ticket for vulnerability B that includes asset A?
  - RiskVision can support virtually any vulnerability grouping criteria. However, groups should be mutually exclusive, similar to the out-of-the-box groupings shipped with the system. This prevents vulnerability duplication.
- Can ticketing thresholds be configured to automatically create a ticket when a risk score goes above a certain level and automatically close a ticket if it goes lower than another number.
  - Yes

## Patching Operations vs. Vulnerability Risk

Out of the box, you can group the tickets created for patching in whatever way aligns with your current patching process. However, there is a little bit of work required to set up the integration with the ticketing system if you're interfacing with one. Typically that effort is just a few days.

- Can we ticket/track patching deadlines for newly released patches?
  - The due date of the ticket is typically set based on the patching deadline that your organization establishes, however, the due date can also be based off of other criteria.
- Can we ticket/track vulnerability management risk remediation with separate deadlines/thresholds?
  - Yes. You can set the deadline for a vulnerability at the ticket level so each separate ticket can have a different deadline. You can also define different time frames that tickets have to be addressed within based on ticket attributes, such as the risk score of linked vulnerabilities.
- Do connectors with patch management tools allow action to be taken from within RiskVision tickets?
  - RiskVision can be easily configured to send patching commands to external systems, but whether the patch management system can accept the patching command will be dependent upon whether the patching tool provides an API to accept the patching command and initiate a patch.



Ticket: Ticket\_01 Edit

**General**

Name Ticket_01	Owner [Redacted]
Description N/A	Created 2019-09-17 16:02:56
Type Audit Finding	Start 2019-09-17
Status Assigned	Expiration date N/A
Export Status Not exported to external system	Planned Start N/A
Category N/A	Planned End N/A
Disposition N/A	Exception Expiration N/A
Progress <input type="text"/> 0%	Date
Submitted By [Redacted]	Priority N/A
Ticket Id TKT00093	Risk <input type="text"/> Unknown
<b>Custom Attributes</b>	Ticket Age 20 days
Custom String 10 N/A	
Custom Text 1 N/A	

**Workflow**

Name: Issue Management Workflow

1 Assigned | 2 In Progress | 3 Review | 4 Closed

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.

Accept | Reject | Test | Delegate To | Revoke Delegation

**Comments**

[Add a comment](#)

*No comments have been entered.*

**Documents**

All | Files | Web Links

[New Document](#) | [New Web Link / Network Path](#) | [Delete](#) | [More Actions...](#)

Filter by: [- Show all -](#) [Refresh](#)

Name	Caption	Tags	Description	Uploaded By	Uploaded On	Size	Expires On	Version
<i>No Documents found.</i>								

A ticket's Details page.

## Ticket Ownership vs. Asset Ownership

Computer: DesktopID1012 Save Cancel 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

### Owners

Primary Owner\*  +

Additional Owners:  
1-3 of 3

Filter by

	Name	Type	Ownership Type
<input type="checkbox"/>	[blurred]	User	Executive Owner
<input type="checkbox"/>	[blurred]	User	Business Owner
<input type="checkbox"/>	[blurred]	User	Security Owner

The Edit Owners screen.

## Create a Technology

A large number of commonly used vulnerabilities are shipped along with the Threat and Vulnerability Manager application that you can use immediately to attach vulnerabilities and entities, if required. You will need to create a new technology if your organization is using a technology that is not available in the application.

### To create a technology:

1. Open RiskVision Threat and Vulnerability Manager.
2. Go to **Technologies > All Technologies**, or **Technologies > Recent Technologies**.
3. Click **New**.
4. Enter the following details:
  - Full Name. The name of a technology. This must be a relevant name.
  - Description. Any additional information that describes a technology.
  - Product. The short name of a technology.
  - Version. The version number of a technology or product.
  - Vendor. The name of an organization providing the technology.
  - Update. The information of an update if the technology includes the most recent fixes.
  - Edition. The edition of a technology or product. This can be standard, professional, enterprise, and more.
  - Language. The technology language if procured for non-native English users.
  - Type. Select whether a technology is a software application, a hardware component, or an operating system.

## Integration

### Custom threat intel

- What is the level of effort (pro-serv \$) to integrate a custom threat intel feed in XML format that is used to drive patching deadlines and inform vulnerability risk?
  - Typically, new integrations are in the 1-2 week range, but we recommend contacting [Resolver Support](#) for more information.

### Hadoop & Big Data

In general, we support reading from and outputting to Hadoop and big data environments. Contact [Resolver Support](#) for more specific information.

- Can TVM pull from a central big-data repository rather than individual integrations? How much does this impact deployment effort?
  - While this is certainly possible, it adds some complexity. For instance, vulnerability definitions and the asset instance data from the vulnerability scanner could be pulled.
- Can TVM's data be piped into a big-data repository for use by other analytic tools?
  - Yes. Contact [Resolver Support](#) for assistance.

