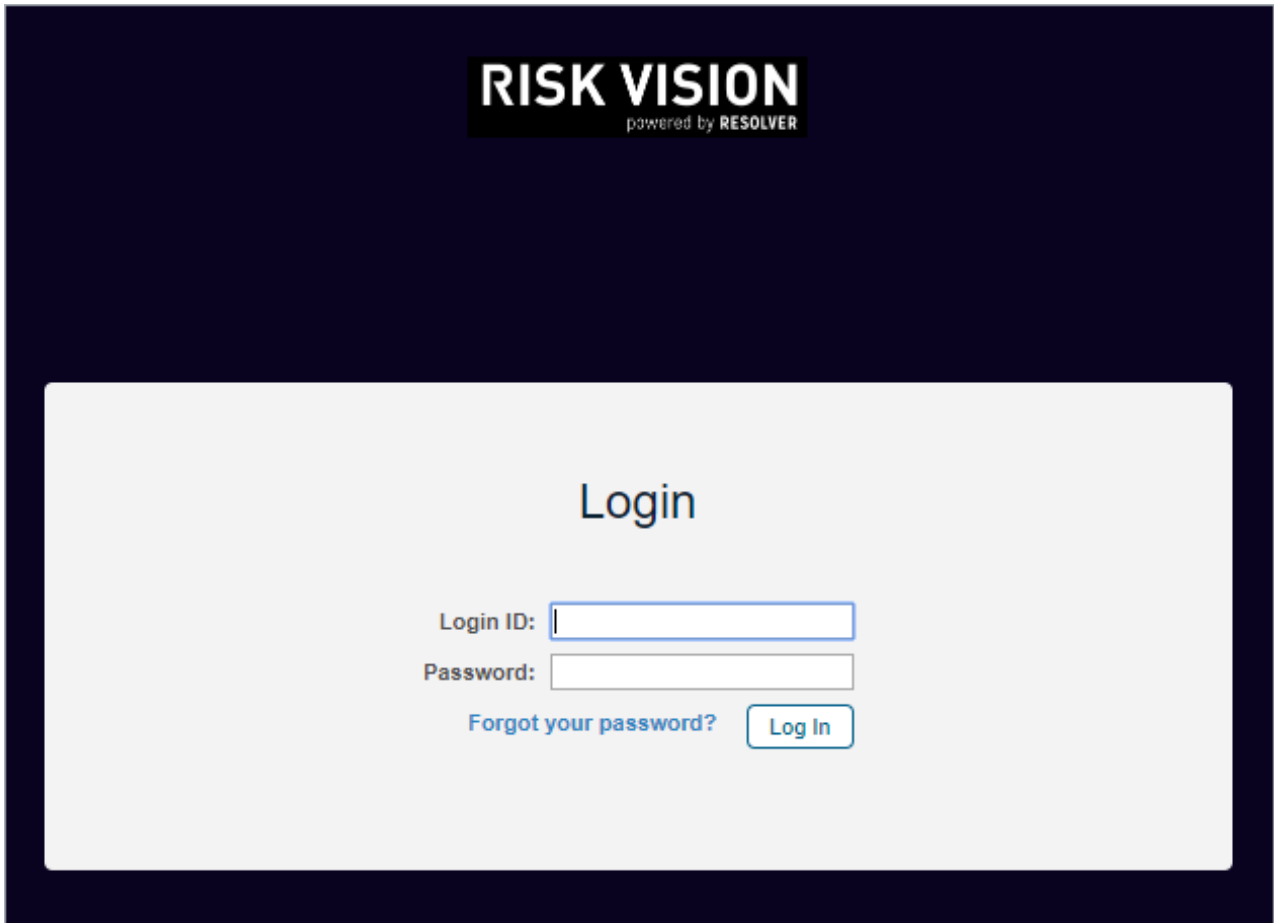


Version 9.3 Release Notes

User Interface Modernization

Enhancements to RiskVision's user interface provide a clean, modern look that is easier to navigate. Changes to the UI include a new login page, a new landing page, new application icons, and cleaner looking grids and tabs.



RISK VISION

Compliance Manager | User Settings | Configure UI | Help | Log Out

Home **Entities** Assessments Content Analytics Configuration

Show Graph Entity name

Entities Entity Collections Group Definitions Entity Management

Entities

- Entities
 - Entities with IP Addresses
 - Active Directory
 - All Processes and Objectives
 - By Criticality
 - By Operating System
 - By Type
 - DG1
 - DG2
 - My Entities
 - Newly Discovered Entities
 - Organization Hierarchy
 - Unmanaged Entities
 - My Favorites
 - Recently Viewed

Entities

1-6 of 6

New Details Delete More Actions...

Show IP Address Filter by - Show all - Refresh

Name	Type	Subtype	Criticality	Owner	Description
abc	Application	N/A			sfs
Default Engagement	Vendor Service	N/A			This is the default engagement provided by this vendor
E123	Computer	N/A			N/A
RRV-2909	Computer	N/A			RRV-2909
tyryy	Computer	N/A			tytytyt
v12333	Vendor	N/A			ff

Computer: RRV-2909 Edit Favorites

General

- Owners
- Description
- Addresses
- Classification
- Costs & Impact
- Relationships
- Propagation
- Documents
- Assessments
- Vulnerabilities
- System Details
- Data Feeds
- Exceptions

Information

Information

Name RRV-2909
 Description RRV-2909
 Entity type Computer
 Entity subtype N/A
 Manufacturer N/A
 Serial number N/A
 Product name N/A

Maintenance

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

Entity Management

Tracked since 2019-07-16
 Status Managed
 Data source(s) Manual entry
 Created by
 Created on 2019-07-16
 Discovery N/A source

Organization Hierarchy

Add Delete More Actions...

Filter by - Show all - Refresh

Organization Root	Path	Description
No assigned Hierarchies found.		

National Vulnerability Database (NVD) CVSS v3.0 Tab Population

The CVSS v3.0 Score tab on the [vulnerabilities details](#) page will now populate from NVD data.

Vulnerability: CVE-2019-0001

- 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

▼ **Base Score Metrics v3.0**

Exploitability Metrics	Impact Metrics
Attack Vector Network	Confidentiality None
Attack High	Integrity None
Complexity	Availability High
Privileges None Required	
User None	
Interaction	
Scope	
Scope Unchanged	

▼ **Environmental Score Metrics v3.0**

Base Modifiers	Security Requirements
Modified Attack Vector N/A	Confidentiality Requirement N/A
Modified Attack Complexity N/A	Integrity Requirement N/A
Modified Privileges N/A Required	Availability Requirement N/A
Modified User Interaction N/A	
Impact Metrics	
	Modified Confidentiality N/A
	Modified Integrity N/A
	Modified Availability N/A
Scope	
Modified Scope N/A	

▼ **Temporal Score Metrics v3.0**

Exploit Code Maturity N/A
 Remediation Level N/A
 Report Confidence N/A

▼ **CVSS v3.0 Score**

CVSS v3.0 Base Score 5.9
 Impact Subscore 3.6
 Exploitability Subscore 2.2
 CVSS Temporal Score N/A
 CVSS Environmental Score N/A
 Overall Score 5.9

▼ **About CVSS**

Common Vulnerability Scoring System (CVSS)

i The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Following are useful links related to CVSS.

National Vulnerability Database CVSS Link <https://nvd.nist.gov/cvss/v3-calculator?vector=CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H>

National Vulnerability Database CVSS [Version 3](#) Calculator

[Version 2](#)

[Version 1](#)

Groovy Support

Batch Edit Tickets

[Batch ticket editing](#) now works for customers who are leveraging groovy scripting to control elements of the ticket UI.

Batch Workflow Transitions

[Batch workflow transitioning](#) now works with tickets, findings, exceptions, and incidents that are using groovy with their workflows.

HTML in Custom Text Attributes

Custom text attributes being used in notifications can now have their HTML formatting properly displayed within notifications, allowing for enhanced readability within the notifications. This may be used, for example, to provide greater context to a ticket by showing information about a related vulnerability.

Topic: WordPress wp_delete_attachment() Code Execution Vulnerability
Status: New
Category: New vulnerability with high publicity
Description: WordPress wp_delete_attachment() Code Execution Vulnerability
Attack vector: local user to run exploit code to get root privileges
Impacted SW / HW / Assets: Red Hat 6, Red Hat 7 (Red Hat 5 not impacted);
Severity: CVSS Score: 6.5 (https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE: CVE-2018-14634
Exploit: PoC

Import Content Packs

RiskVision now allows users to import content packs using the [Content Pack Import Template](#). This will speed up the process of adding controls and subcontrols to content packs.

The screenshot shows the RiskVision Administration interface. The top navigation bar includes 'Administration', 'Users', and 'Events'. Below this, a secondary navigation bar lists 'Server Administration', 'External Authentication', 'Login Integration', 'Notifications', 'Connectors', 'Email Templates', 'Queued Jobs', and 'Scheduled Jobs'. The main content area is titled 'Server Administration' and features a left-hand sidebar with categories: Information, Configuration, Commands, Support, Health Report, Documentation (highlighted), and About. The 'Documentation' section is expanded, showing 'General documentation' with a link to 'Download user guides here.' and 'Sample templates' including: Entity Import Template, User Import Template, Finding Import Template, Incident Import Template, Control Import Template, Risk Assessment Import Template, Entity Relationship Import Template, Vulnerability Risk Score Entity Criticality Factor Formula Definition, Vulnerability Risk Score Entity Criticality Factor Attribute Mappings, and Core Content Import Template. The 'Core Content Import Template' is highlighted with a green box.

New Password Change Process

Users with administration privileges are no longer able to change the passwords of other users. Administrators must now [request users to change their password](#) by clicking the **Reset Password** checkbox on the **User Details** page.

System User: user 2

Information

Information

i Passwords must be at least 8 characters long, they must contain at least one lower case letter, they must contain at least one number.

Login ID user2

Reset User Password

First Name* user

Middle Name

Last Name* 2

Email Address* user2@idcagl.com

Picture N/A

Manager

Last Login Location N/A

Authentication Type Internal

RiskVision Status Active

LDAP Status Not Applicable

JasperReports Server v7.1.1

JasperReports Server has been upgraded to version 7.1.1, delivering the following enhancements:

- Ad hoc views – Improvements include a message being generated when fields have been deleted from a related domain, balance calculations for time series data with beginning and ending balances, and day-of-week time series grouping.
- Jasper Studio – Enhancements include the ability to develop reports when offline and various improvements that speed up working with fields and parameters.
- Configurations – Oracle 12c is now supported as the database for the Jasper repository.

NVD Connector Upgrade

NVD is end-of-living its XML feed and will only be compatible with JSON. Customers will need to [upgrade their NVD connector](#) to be able to download the JSON feed and continue to access NVD data.