Table of Contents

Intended Audience

The Resolver RiskVision Administrator's Guide will help you customize and configure the user interface in Resolver RiskVision applications. This guide is intended for developers who are experienced in complex customization of applications using APIs. This guide includes several Java methods which you can use as a reference when writing scripts for customizing a page, tab, menu, wizard, or dialog. The guide also demonstrates how to customize the UI, as well as where groovy scripts can be used for UI customization.

Other RiskVision Applications

Other RiskVision applications are listed in the table below:

Icon	Application	Description
☑	Compliance Manager	Compliance Manager allows organizations to effectively manage and measure compliance programs across multiple regulations, standards, and frameworks. It also automates the compliance process through general computer controls (GCC) and questionnaires. The evidence and control results can be automatically collected through connectors or questionnaire results from business users. Copmliance enables data classification, ownership configuration, compliance assessment, mitigation, and reporting. It supports popular frameworks, standards, and regulations such as ISO 27002, CIS, HIPAA and PCI, and others. Compliance Manager improves process efficiency and integrity as well as data quality and reliability.
🌐	Enterprise Risk Manager	Enterprise Risk Manager is a comprehensive risk lifecycle management solution. Organizations can use this application to identify, assess, and mitigate risks using an appropriate risk treatment plan. Its flexible risk model supports both qualitative and quantitative methodologies, including the calculation of inherent risk, current risk, and residual risk within the context of mitigating controls. It features rich reports and dashboards, as well as easy to use risk assessment tools and will help your orgnization understand and monitor its enterprise risk posture. Enterprise Risk Manager includes out-of-the-box support for popular risk methodologies, such as COSO, AZ/NZS 4360 and ISO.
⚠	Threat and Vulnerability Manager	Threat and Vulnerability Manager will help you consolidate your threat and vulnerability programs onto a single platform. It integrates with vulnerability and early warning data feeds from iDefense and National Vulnerability, and correlates these feeds with vulnerability scanner results to eliminate false positives and report incidents. Inferred scans are performed by correlating the vulnerability data feeds to a company's RiskVision asset database, mitigating risks for assets not reachable by vulnerability scanners. Once detected, vulnerabilities are assessed and remediated using the system's workflow for true closed-loop vulnerability management.
📄	Policy Manager	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 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 helps organizations collect, classify, and manage multiple IT and non-IT incidents. It is 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 workflows and automatically created and classified based on rules that are tracked throughout the incident's lifecycle. Incidents are tied to controls, policies, and risk to provide closed-loop feedback for policy and control assessment and risk monitoring. Incidents are rated based on their criticality

so that organizations can respond based on the impact to the business.

Icon	Application	Description

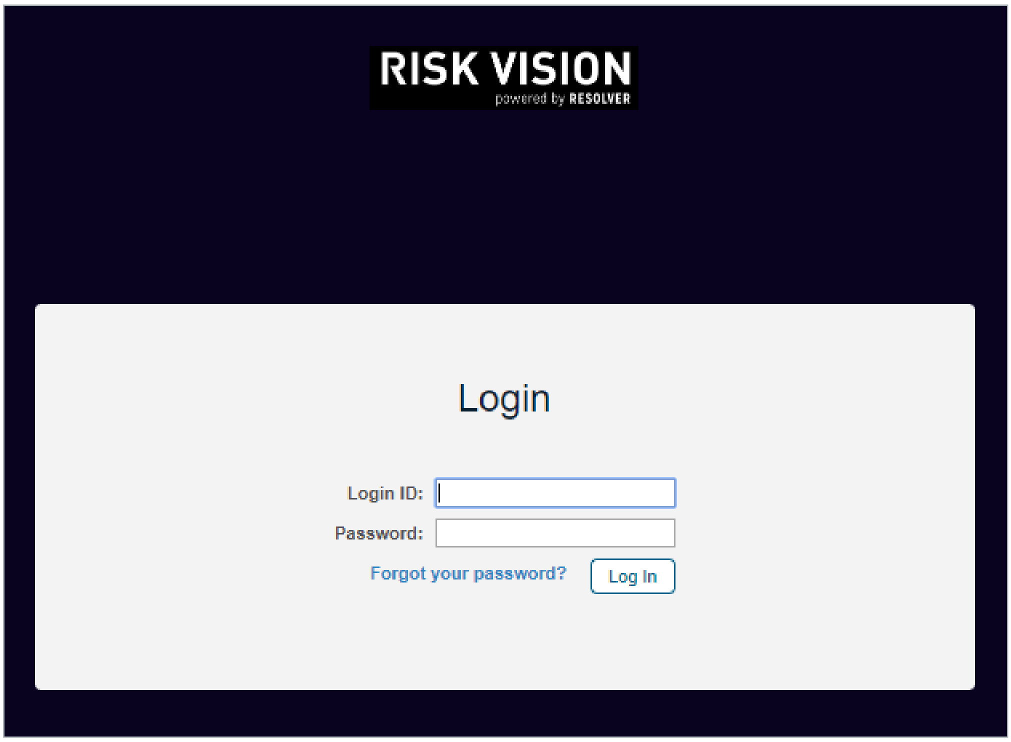
Logging in to RiskVision Application

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

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

To access the application using a web browser:

1. Open a browser and enter the RiskVision URL.



The RiskVision login screen.

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

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

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

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

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

Logging in as a Delegate

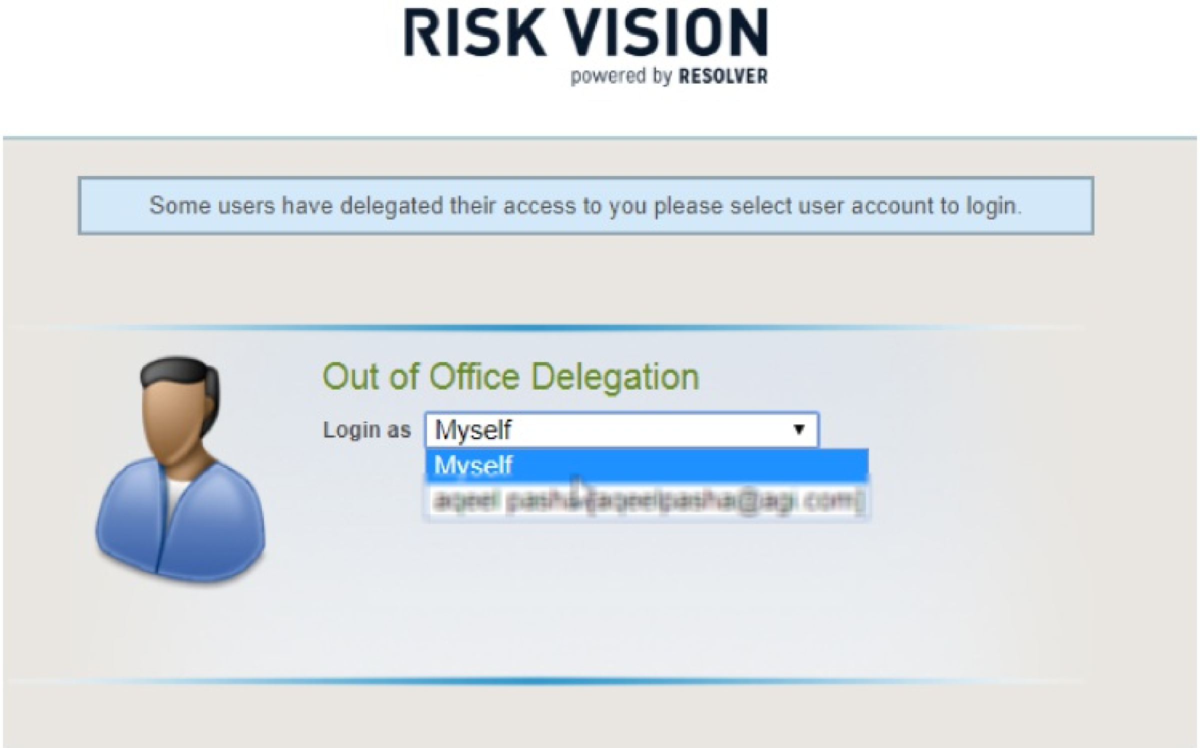
You can log into the account of another user if that user or a RiskVision administrator nominates you to access the delegation. To learn how to delegate your RiskVision user account, see Delegating Your RiskVision User Account.

To access the delegated user account:

1. Open a browser and enter the RiskVision server URL.

2. Enter your RiskVision credentials: Login ID and Password, and click **Log In**.

3. The **Out of Office Delegation** page appears. In the Login as drop-down list, select the user account other than **Myself**, and click **Log In**. You would select **Myself** to log in to your user account.



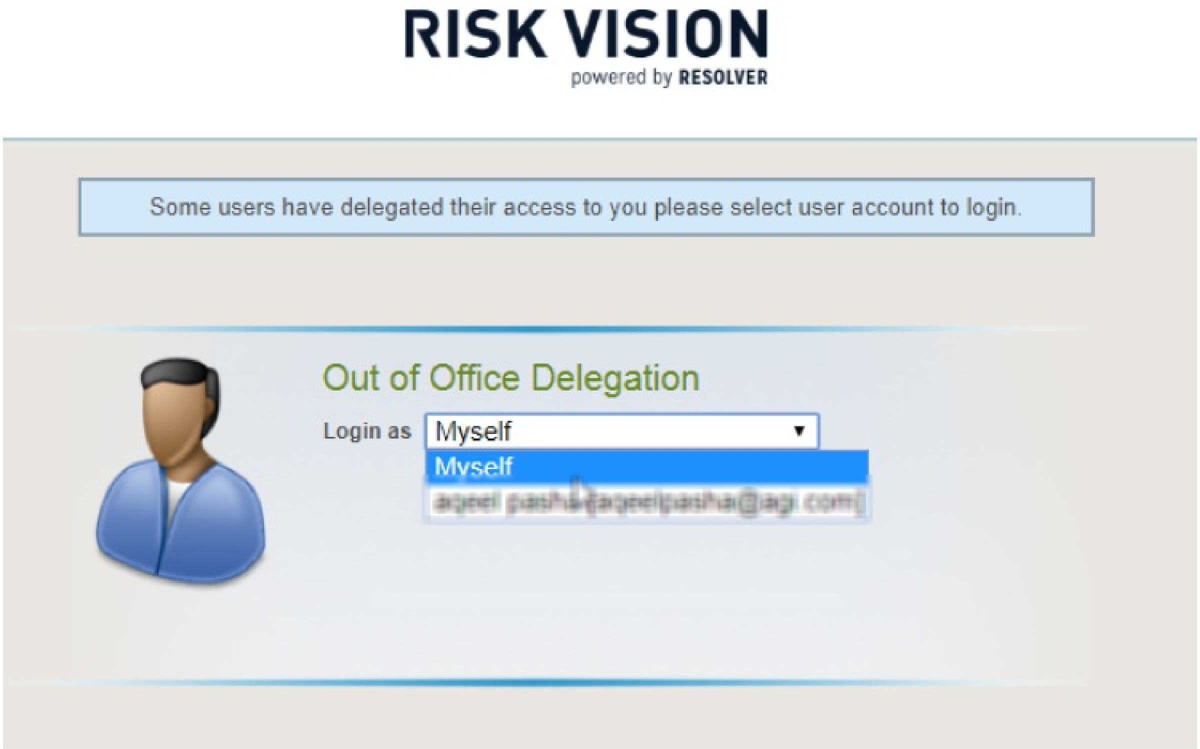
Some users have delegated their access to you please select user account to login.

Out of Office Delegation

Login as: Myself

After you log into the delegated user's account, you become eligible to perform any task that the user who delegated the access can perform on behalf of that user.

When the delegated user logs into the RiskVision application, the **Current User** displays the Logged in as: **delegated by username.**



RISK VISION

powered by RESOLVER

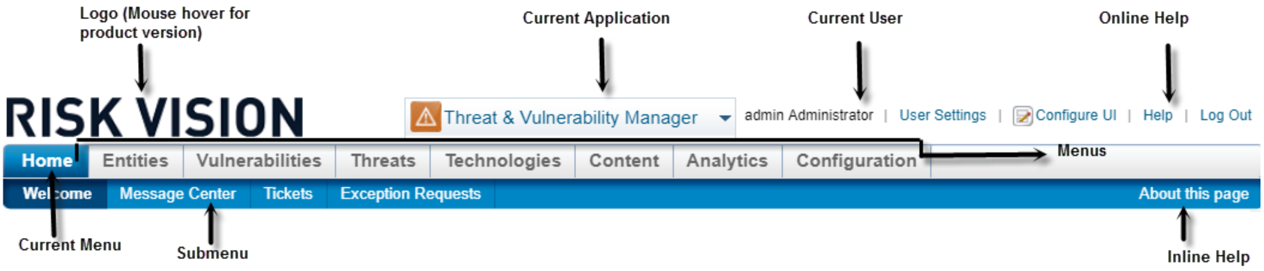
Some users have delegated their access to you please select user account to login.

Out of Office Delegation

Login as: Myself

Navigating the RiskVision System

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



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

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

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

Controlling Object Visibility

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

To control an object's visibility:

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

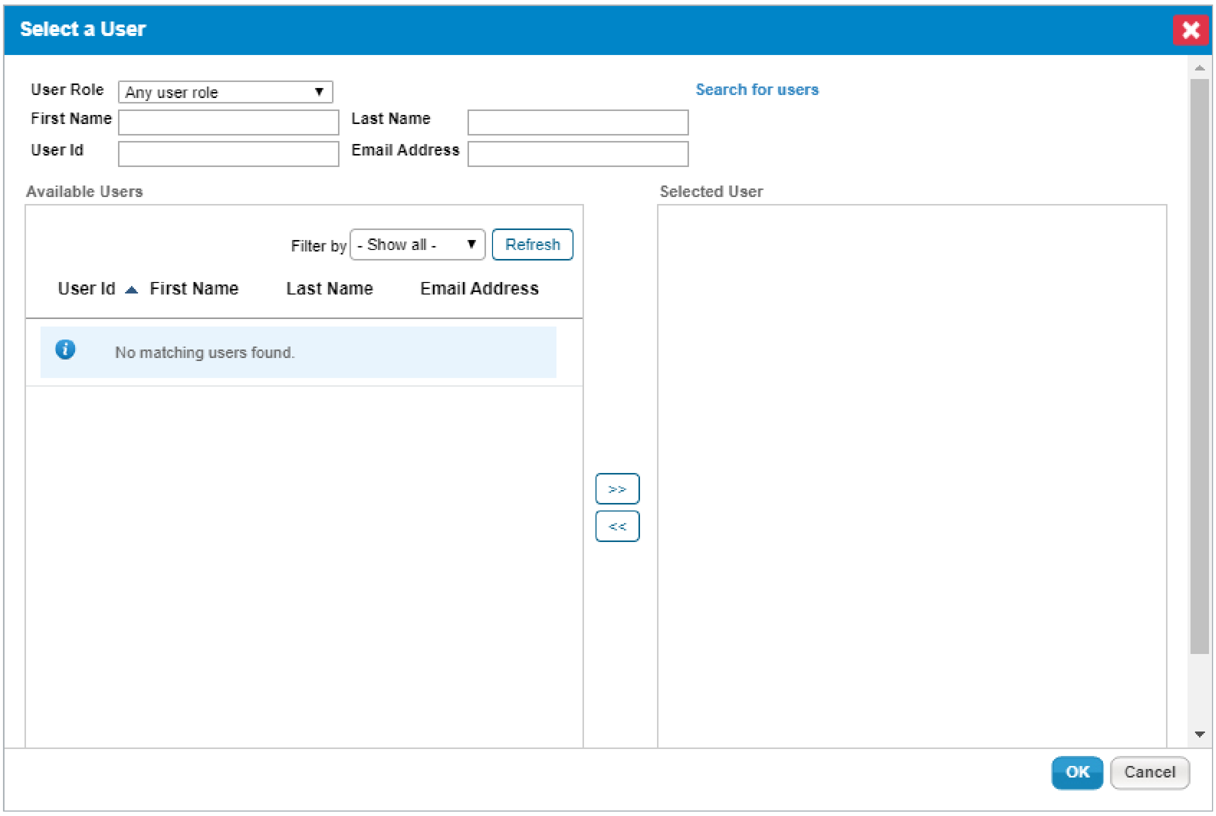
User Picker

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.



Select a User

User Role: Any user role

Filter by: - Show all -

No matching users found.

The User Picker window.

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

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

Using Search Criteria

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

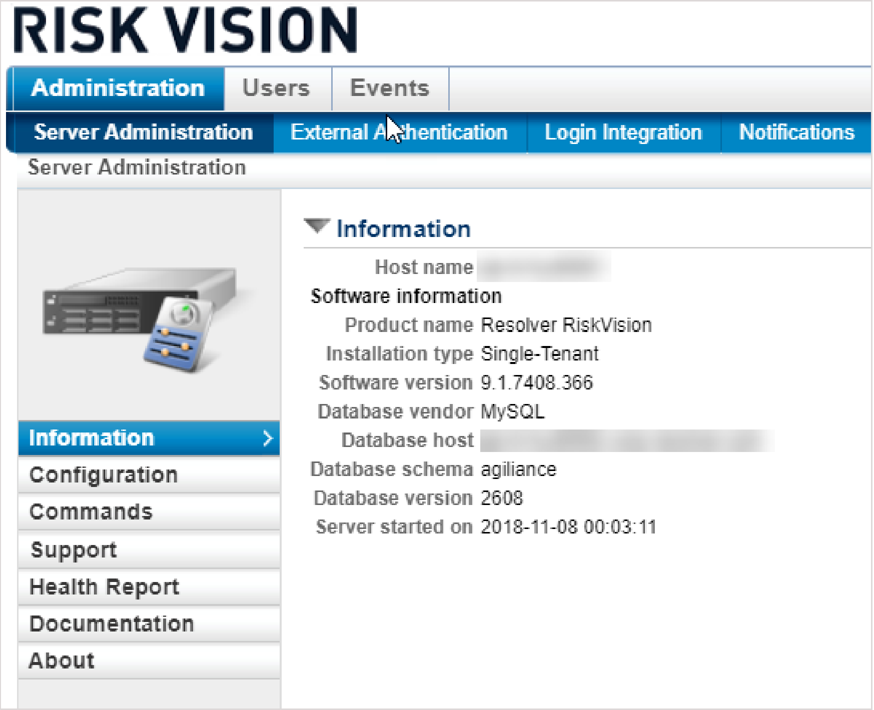
   - For Internal Users, the search field supports a single word in which the wildcard of "*" can be used before and/or after the search term. For example: *test* , *test, test * and test

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

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

Server Administration

The **Server Administration** page provides version, status, and other resource usage information and settings for the RiskVision solution. The default Administrator role in RiskVision allows you to view and modify the settings on tabs that are available on the **Administration** > **Server Administration** menu. If you require another user to manage the settings, you must assign the Server Manage permission to that user.



Information

Host name [redacted]

Software information

Product name Resolver RiskVision

Installation type Single-Tenant

Software version 9.1.7408.366

Database vendor MySQL

Database host [redacted]

Database schema agiliance

Database version 2608

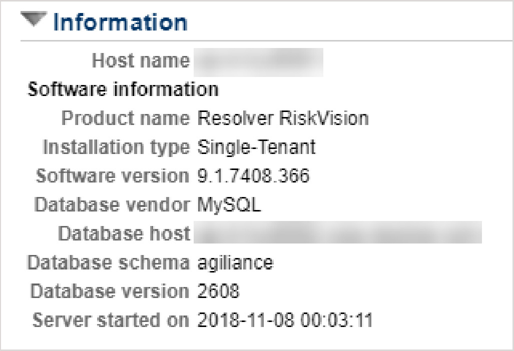
Server started on 2018-11-08 00:03:11

The following tabs are available on the **Server Administration** menu:

- **Information:** Product version, installation location, user activity, health monitoring, and system resource usage metrics.
- **Configuration:** IP addresses, notification e-mail web address, and integration user name, password, and token information.
- **Commands:** Provides the commands to run system configuration operations, releasing memory without interrupting service, and importing system files and configuration information.
- **Support:** Commands to run maintenance operations, configure e-mail notification settings, test charts, save system logs for printing, and perform other support-related operations.
- **Health Report:** General information, applications, deployment, connectors, key object count, programs, and top 20 pages to view and download.
- **Documentation:** Provides a list of available Resolver documentation, and links to download Adobe Acrobat PDF copies of each document.
- **About:** Software credits and copyright information, including embedded third-party software.

Information Tab

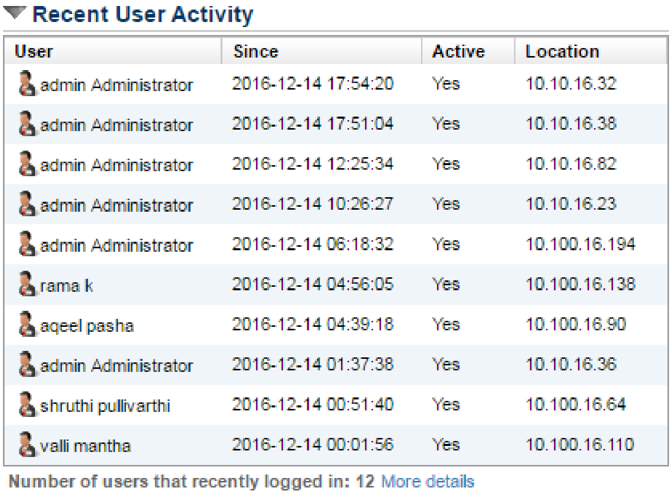
The Server Administration **Information Tab** shows product version and location information in the **Information** drop-down.



Information

Host name	[redacted]
Software information	
Product name	Resolver RiskVision
Installation type	Single-Tenant
Software version	9.1.7408.366
Database vendor	MySQL
Database host	[redacted]
Database schema	agiliance
Database version	2608
Server started on	2018-11-08 00:03:11

The **Recent User Activity** pane displays the recent activity of logged in users.



Recent User Activity

User	Since	Active	Location
admin Administrator	2016-12-14 17:54:20	Yes	10.10.16.32
admin Administrator	2016-12-14 17:51:04	Yes	10.10.16.38
admin Administrator	2016-12-14 12:25:34	Yes	10.10.16.82
admin Administrator	2016-12-14 10:26:27	Yes	10.10.16.23
admin Administrator	2016-12-14 06:18:32	Yes	10.100.16.194
rama k	2016-12-14 04:56:05	Yes	10.100.16.138
aqeel pasha	2016-12-14 04:39:18	Yes	10.100.16.90
admin Administrator	2016-12-14 01:37:38	Yes	10.10.16.36
shruthi pullivarthi	2016-12-14 00:51:40	Yes	10.100.16.64
valli mantha	2016-12-14 00:01:56	Yes	10.100.16.110

Number of users that recently logged in: 12 More details

This pane can be used to keep track of the users that have logged in and if they are still active.

- If a user logs out, the Active column shows "*No*".
- The "Since" column is the time at which the user logged in.
- The "Location" is to differentiate user sessions using the same account at the same time, but from different computers.

Health Monitoring

The **Health Monitoring** section of the **Information** tab displays information about:

- **System memory**. Total size and percentage used. If the system memory usage continues to display in the red color for a longer duration, you should consider upgrading the RAM on the RiskVision Server.

- **Processors**. The number of processors and CPU cores. The CPUs are named sequentially from CPU 1 to CPU 4 and displays the average load on each CPU.

- **Storage**. The total size and percentage used by the hard disk drive where the RiskVision Server is installed. If the RiskVision Server is installed on a single tier and the storage continues to display in the red color, consider increasing the disk space. You may also want to delete large temporary files created by the MySQL database to free up a lot of disk space.

Resources

The **Resources** section of the **Information** tab displays information about memory usage, threads, and database connections.

Non-Heap Memory Usage

This section describes the memory that is managed by the Java Virtual Machine (JVM), which may or may not be subject to compaction. The non-heap area is used for method data, shared among all threads.

Heap Memory Usage

Memory used by the JVM for class instances and arrays. Heap memory is reclaimed by an automatic memory management system known as a garbage collector. The "Used" Heap memory usage bar indicates how much memory is utilized. If the "Used" Heap memory bar continues to display in the red color for a long duration, you should consider increasing the Heap memory. Expect occasional spikes in the red color.

The table below outlines the usage types for both Heap and Non-heap memory.

Type	Description
Init*	The initial amount of memory that the JVM requests from the operating system during start-up.
Used*	The amount of memory already in use.
Committed*	The amount of memory that will be available for use by the JVM. This memory may change. The Committed memory will always be greater than or equal to Used memory.
Max*	The maximum amount of memory available for use by the JVM. The Used memory plus the Committed memory will be less than or equal to Max memory.

*Memory in megabytes.

MySQL and Tomcat require a special configuration to make use of additional memory. Most likely, the situation to change the heap memory size arises on the Tomcat. For example, running Java Virtual Machine applications such as Tomcat with the parameter -Xmx5120m establishes a maximum heap size of 5GB for Tomcat's use. Make sure to specify a maximum heap size that is well under the physical memory of the server.

For information about changing the heap size for Tomcat, please follow the steps given below:

1. Go to the `%AGILIANCE_HOME%\Tomcat\bin` directory and double-click the file `tomcat8w.exe` to launch the RiskVision Tomcat Properties dialog.
2. Click the **Java** tab and enter a value, in megabyte as required, in the Maximum memory pool field.
3. Click **Apply** and click **OK** to save and close the dialog.
4. Restart the RiskVision Tomcat service to apply the latest changes.

Also, you may want to change the MySQL configuration to utilize the system memory of the host in which you have installed the MySQL database. If you have deployed the MySQL database on a host with at least 8 GB of system memory, run the script `%AGILIANCE_HOME%\install\mysql\use_4CPU_8GB_mysql_ini.bat` . Otherwise, change the %AGILIANCE_HOME%\install\mysql\my.ini file.

Run the script `%AGILIANCE_HOME%\install\mysql\use_default_mysql_ini.bat` if you want to revert the changed MySQL configuration to the default configuration.

Memory Managers

For each memory manager in use, RiskVision displays the manager name, the total number of collections that have occurred and the approximate accumulated collection elapsed time in milliseconds.

Threads

The number of active threads.

Database Connections

The total number of connections including busy and idle. Ideally, there will be zero Unclosed connections.
The information mentioned above should help you monitor the RiskVision Server and take an appropriate action when required; however, if you have encountered an unusual situation in that you are unable to resolve the problem on your own, then please contact your Resolver Customer Support Representative.

Currently Running Jobs

This section of the Server Administration **Information** tab shows information about active jobs.

- Currently Running Jobs: Active jobs on the server and for how long they have been running.
- Slow Running Queries: Queries that have been running for more than 30 seconds. If you are using an Oracle database, SELECT ANY DICTIONARY permissions must be given to the agiliance schema for queries to appear on the Server Administration page.
- Recent Connector Activity: Connectors that have imported data in the last 30 minutes. The data in the grid can be filtered on following options:
    1. Type
    2. Name
    3. Time Started
    4. Time Finished
    5. Duration

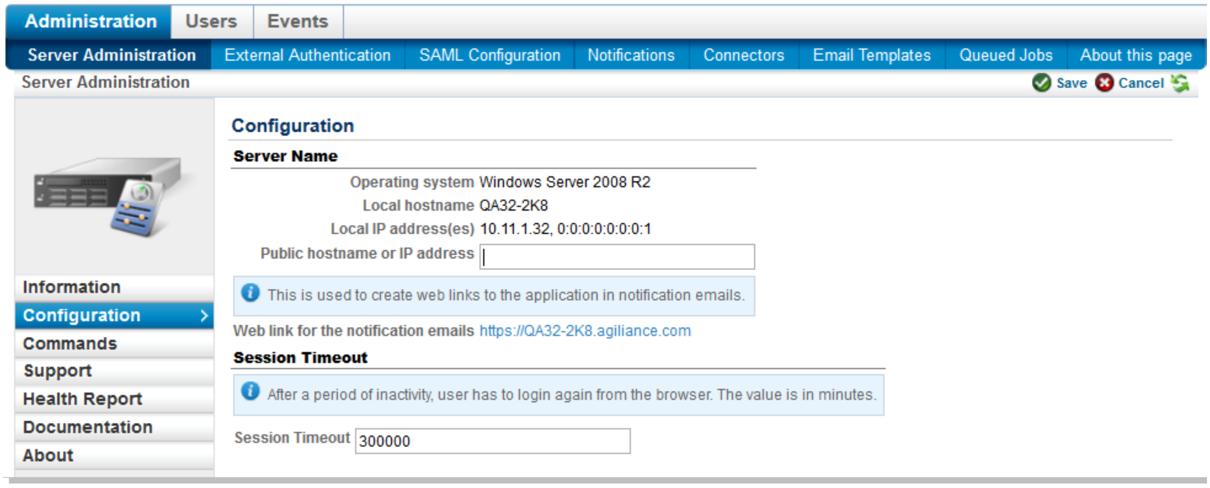
You can view further information about active server jobs by going to**Administration>Scheduled Jobs**. The **Current Status** column shows the status of scheduled jobs. When a job is triggered, its status will change to “Executing from ‘xx’” seconds. Finished jobs have a status of “Not Executing.”

Setting the Host Name

The RiskVision solution inserts the public hostname or IP address value in e-mails/notifications that use the application URL variable $appurl. Enter a fully qualified domain name or Internet hostname if users access the RiskVision solution.

To set the host name:

1. **In the Administration application, go to Administration > Server Administration > Configuration.**
2. Click **Edit**.



Configuration

Server Name

Operating system Windows Server 2008 R2

Local hostname QA32-2K8

Local IP address(es) 10.11.1.32, 0:0:0:0:0:0:0:1

Public hostname or IP address |

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

Web link for the notification emails https://QA32-2K8.agiliance.com

Session Timeout

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

Session Timeout 300000

3. In the **Public hostname or IP address**field, type the IP address in dotted quad format (such as `127.0.0.1`).
4. Click **Save**.

   The web link for Notification E-mails URL is updated.

5. Click on the URL to test the link.

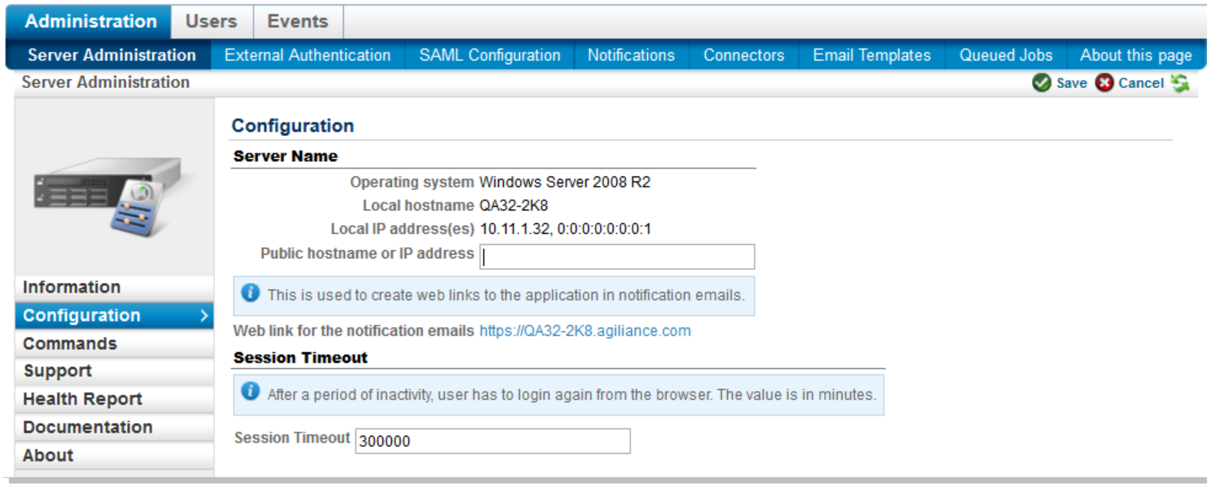
Setting User Session Timeout

By default, the RiskVision solution logs out inactive sessions after 30 minutes. Session time-out is a system-wide setting. The session time-out period is set when the session is opened. Changing this setting does not affect open sessions.

To change the time-out setting:

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

2. Click Edit.



Configuration

Server Name

Operating system Windows Server 2008 R2
Local hostname QA32-2K8
Local IP address(es) 10.11.1.32, 0:0:0:0:0:0:0:1
Public hostname or IP address

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

Web link for the notification emails https://QA32-2K8.agiliance.com

Session Timeout

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

Session Timeout 300000

3. In the **Session Timeout** field, enter the interval in minutes.

4. Click **Save**.

All sessions opened after you saved the setting will have the new time-out period.

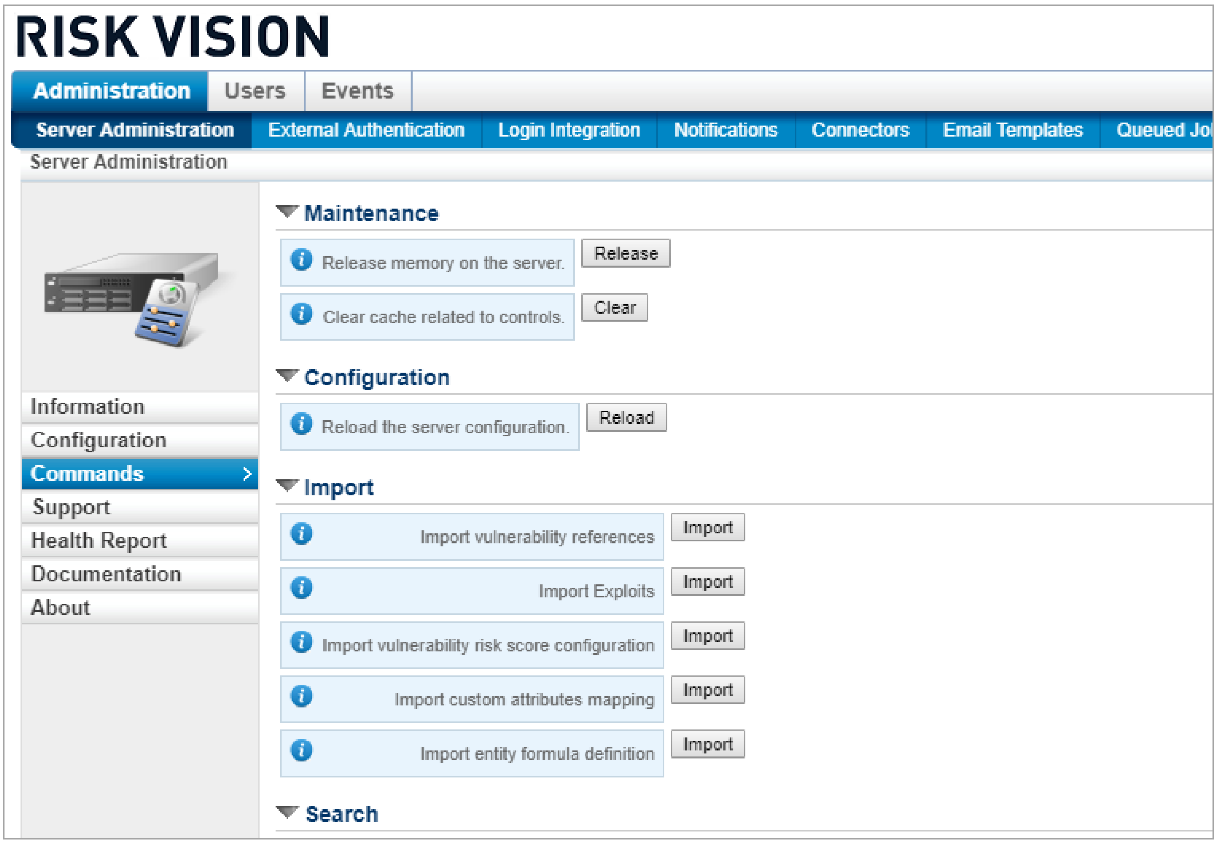
Release Server Memory

The RiskVision solution allows you to release memory from the RiskVision solution or clear the control-related cache without interrupting user sessions.

To release memory or clear the control-related cache:

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

2. In the **Maintenance** section, click **Release** to release the server memory <u>**OR**</u> click **Clear** to clear the control cache.



3. Click **Information** to review and verify the system health status.

Importing Configuration Files

The RiskVision solution allows you to import system configuration files such as properties files, vulnerabilities references and the exploit files without interrupting user sessions.

To import files:

1. In the **Administration** application, go to **Administration** > **Server Administration** > **Commands**.
2. Click **Import** button, the Import wizard appears and then click**browse** button, to view and select the required file to be imported.
3. Click **OK** button, to confirm importing the file.

The list of configuration files that can be imported in the **Commands** tab, is given below:

Importing File	Description
Properties	This file allows importing properties file.
Vulnerabilities References	This file allows importing the NVDB data.
Exploits	This file allows importing the exploit data.

Reloading Application Configuration

Some customization requires the RiskVision solution to reload configuration and properties files. You can implement the changes without interrupting service (some changes will take effect when the server next starts).

Customization file	Description
`.properties`	Properties that control many aspects of the system
`TargetSelectionObjects.xml`	Customize the objects and fields that can be used to build the target selection criteria
`UICustomization.xml`	Customize the look and feel
`UIDictionary.xml`	Customize terms used in the user interface
`UIHelpTopics.xml`	Customize the 'About this Page' panels
`UIWorkspace.xml`	Customize the look and feel of individually-licensed applications
`Grids.xml`	Customize most grids

To implement customization:

1. Place the customized file in the correct location on the host computer. Your custom files are located in the folder:

   ```
   %AGILIANCE_HOME%\config\
   ```

2. In the Administration application, go to **Administration** > **Server Administration** > **Commands**.
3. Expand the **Commands** tab and click the **Reload** button in the **Configuration** section.

When the process completes, the 'reloaded configuration' message displays.

System Event Notifications

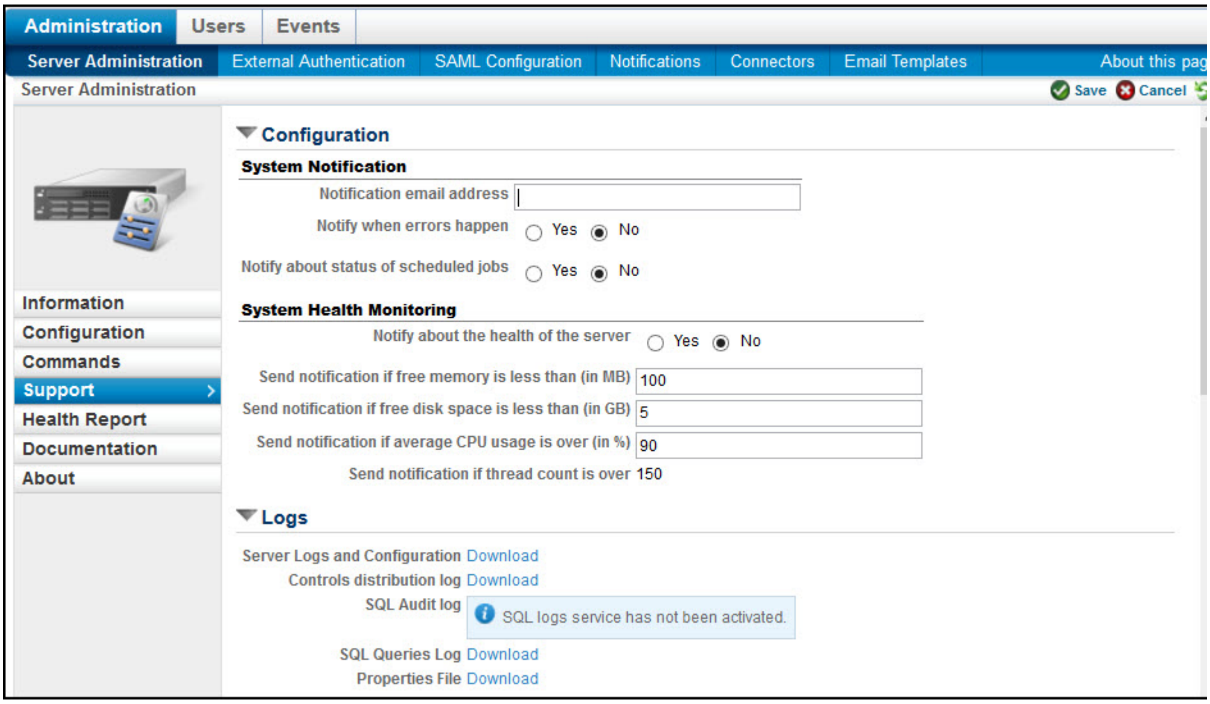
You can configure the RiskVision solution to send a notification to an e-mail address when a system event occurs. The notification events include the status of scheduled jobs, errors, and license expiration.

Sending e-mail notification requires the RiskVision e-mail connector and SMTP service.

To configure event notification:

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

   The **Support** tab details are displayed.



Configuration

System Notification

Notification email address

Notify when errors happen ○ Yes ● No

Notify about status of scheduled jobs ○ Yes ● No

System Health Monitoring

Notify about the health of the server ○ Yes ● No

Send notification if free memory is less than (in MB) 100

Send notification if free disk space is less than (in GB) 5

Send notification if average CPU usage is over (in %) 90

Send notification if thread count is over 150

Logs

Server Logs and Configuration Download

Controls distribution log Download

SQL Audit log SQL logs service has not been activated.

SQL Queries Log Download

Properties File Download

2. Click **Edit**.

3. Expand the **Configuration** section and change the system event notification settings.

   E-mail. Type an e-mail address. If you enable notification for any events, this field is required.

   Errors. Select yes to send an e-mail if a system error occurs.

   Health. Select yes to send an e-mail if a system resource status becomes critical.

   Scheduled Jobs. Select yes to send an e-mail if a queued job fails or when the queue reaches a certain size.

4. Click **Save**.

A notification is sent if any of the events occur.

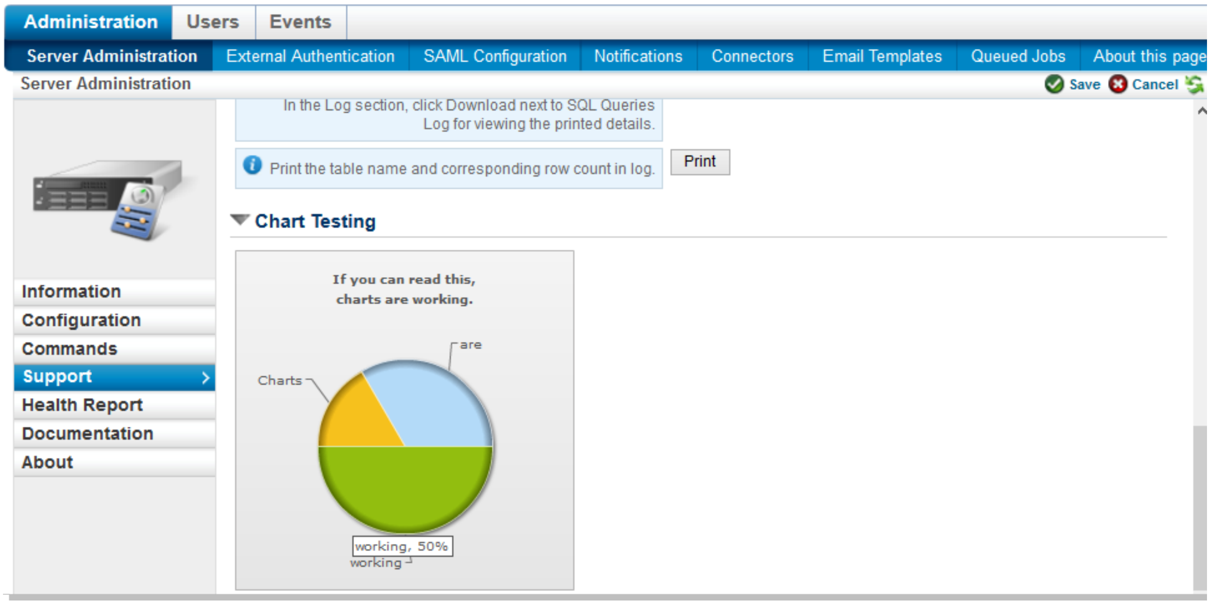
Testing Charts

The RiskVision solution requires Adobe Flash to render charts. Use the Chart display to verify that Flash is installed and rendering charts.

To test charts:

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

   The **Support** tab details are displayed.



In the Log section, click Download next to SQL Queries Log for viewing the printed details.

Print the table name and corresponding row count in log.

If you can read this, charts are working.

2. Double click the **Chart Testing** text to expand the section.

As the screen explains, if you can see the image, the charts are working correctly.

Maintaining Indexed Database Searches

The RiskVision solution uses indexes to improve performance when searching for information, such as content and entities, in its database. The index maintenance tool requires additional disk space on the host computer. The amount of additional space depends on the size of the database.

Creating Search Indexes

By default, index searching is 'disabled.' During regularly scheduled server maintenance, you must update the index. Create an index after enabling the tool for the first time.

To create search indexes:

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

2. In the Search section, click **Recreate** associated with any search index type. To create all search indexes at once, click**Recreate** associated with the Recreate all search indexes option.

   A job is created to rebuild the index. Depending on the amount of data, allow sufficient time to complete creating the search index. You can monitor the progress by navigating to the **Queued Jobs** page on the **Administration** menu.

RiskVision Log Files

The Logs section on the Support tab of the**Administration** > **Server Administration** menu has different types of log files of the components installed in your environment. The files and logs available for download are listed in the table below.

Component	Logs/Files
RiskVision Server	Config folder, Health Report
RiskVision Job Manager	.log, .log.1 through .log.10
RiskVision MySQL	.errors, mysql-slow.log
RiskVision Apache	access.log, error.log, https_error.log, mod_jk.log
RiskVision Tomcat	agentmanager.log, .log, auditquery.log, catalina.log (Server log), commons-daemon.yyyy-mm-dd.log, dbquerypl.log (SQL queries log), dbtablerowcount.log, error.log, hibernate.log, host-manager.yyyy-mm-dd.log, localhost.yyyy-mm-dd.log, manager.yyyy-mm-dd.log, pdperror.log (controls distribution log), tomcat8-stderr.yyyy-mm-dd.log, tomcat8-stdout.yyyy-mm-dd.log

Enabling the SQL Audit Log Link

By default, the download link for SQL Audit log is disabled. To enable the download link, configure the Tomcat server properties files that are specific to the database installed in your environment. The properties files are located in the %AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes directory.

If your database is MySQL, follow the steps given below to enable the SQL Audit Log download link:

# if you want to turn the SQL Audit logs, use below the warper driver and comment the jdbc driver.

```
database.mysql.driver=com.p6spy.engine.spy.P6SpyDriver
```

```
#database.mysql.driver=com.mysql.jdbc.Driver
```

1. Go to the %AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classesdirectory and open the .default.system.properties file using a text editor.

2. Uncomment the following line:

3. Comment the following line:

4. Restart the RiskVision Tomcat service to affect the latest changes.

If your database is Oracle, follow the steps given below to enable the SQL Audit Log download link:

1. Go to the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` directory and open the file `.default.system.properties` using a text editor.

2. Edit the following lines in the database connection information:

    - Comment the following lines:

      ```
      #database.mysql.driver=com.p6spy.engine.spy.P6SpyDriver
      ```

      ```
      #database.mysql.driver=com.mysql.jdbc.Driver
      ```

      ```
      #database.oracle.driver=oracle.jdbc.driver.OracleDriver
      ```

    - Add the following line:

      ```
      database.oracle.driver=com.p6spy.engine.spy.P6SpyDriver
      ```

3. Save the file `.default.system.properties` .

4. Go to the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` directory and open the `spy.properties` files using a text editor

    - Edit the database driver information by commenting and uncommenting the lines as shown below:

      ```
      # oracle driver
      ```

      ```
      realdriver=oracle.jdbc.OracleDriver
      ```

      ```
      realdriver2=oracle.jdbc.driver.OracleDriver
      ```

      ```
      #realdriver3=
      ```

      ```
      # mysql Connector/J driver
      ```

      ```
      #realdriver=com.mysql.jdbc.Driver
      ```

      ```
      #realdriver2=
      ```

      ```
      #realdriver3=
      ```

5. Save the file `spy.properties` .

6. Restart the RiskVision Tomcat service to affect the latest changes.

SQL Queries Log

The SQL Queries Log identifies long-running SQL queries in the database. You can view the start time of a query, statements that consume more time, the end time of a query, and more. Unlike SQL Audit Log, the SQL Queries Log allows printing the latest information straightforwardly so that information can be viewed or saved at the same moment. When you print the SQL Queries Log, the file `dbquerypl.log` is saved in the directory `%AGILIANCE_HOME%\Tomcat\logs\`, by default. You can also save the file `dbquerypl.log` in a different directory using the following property, which is found in the file `.default.system. properties`.

```
log.dbquerypl={.home}/../dbquerypl.log
```

Downloading Logs

The steps to download a log file are given below.

1. In the Administration application, go to **Administration**>Server Administration, then click **the Support** tab.

   The **Support** tab details are displayed.

2. Expand the **Logs** section.

3. Click **Download** next to the log type.

4. A dialog for the log file type appears. Select **Open** and the program that you want to use or select **Save** to save the file.

Printing Database Tables

The file `dbtablerowcount.log` lists all the tables and the corresponding row count. You can use this information to monitor fast-growing tables in your database. Identifying the rapidly growing tables help you manage the space in your database. When you print this information, by default, the file `dbtablerowcount.log` is saved in the directory `%AGILIANCE_HOME%\Tomcat\logs\`. You can also save the file `dbtablerowcount.log` in a different directory using the following property, which is found in the file `.default.system. properties`.

```
log.dbtablerowcount={.home}/.../dbtablerowcount.log
```

Locating Installation Logs

The Install.log file in the %AGILIANCE_HOME%\Install directory records the result of the installation script.

Printing Logs

You can print logs, such as the server log, or the controls distribution log, from the RiskVision solution.

To print server logs:

1. In the Administration application, go to **Administration>Server Administration**, then click the **Support** tab.

   The **Support** tab details are displayed.

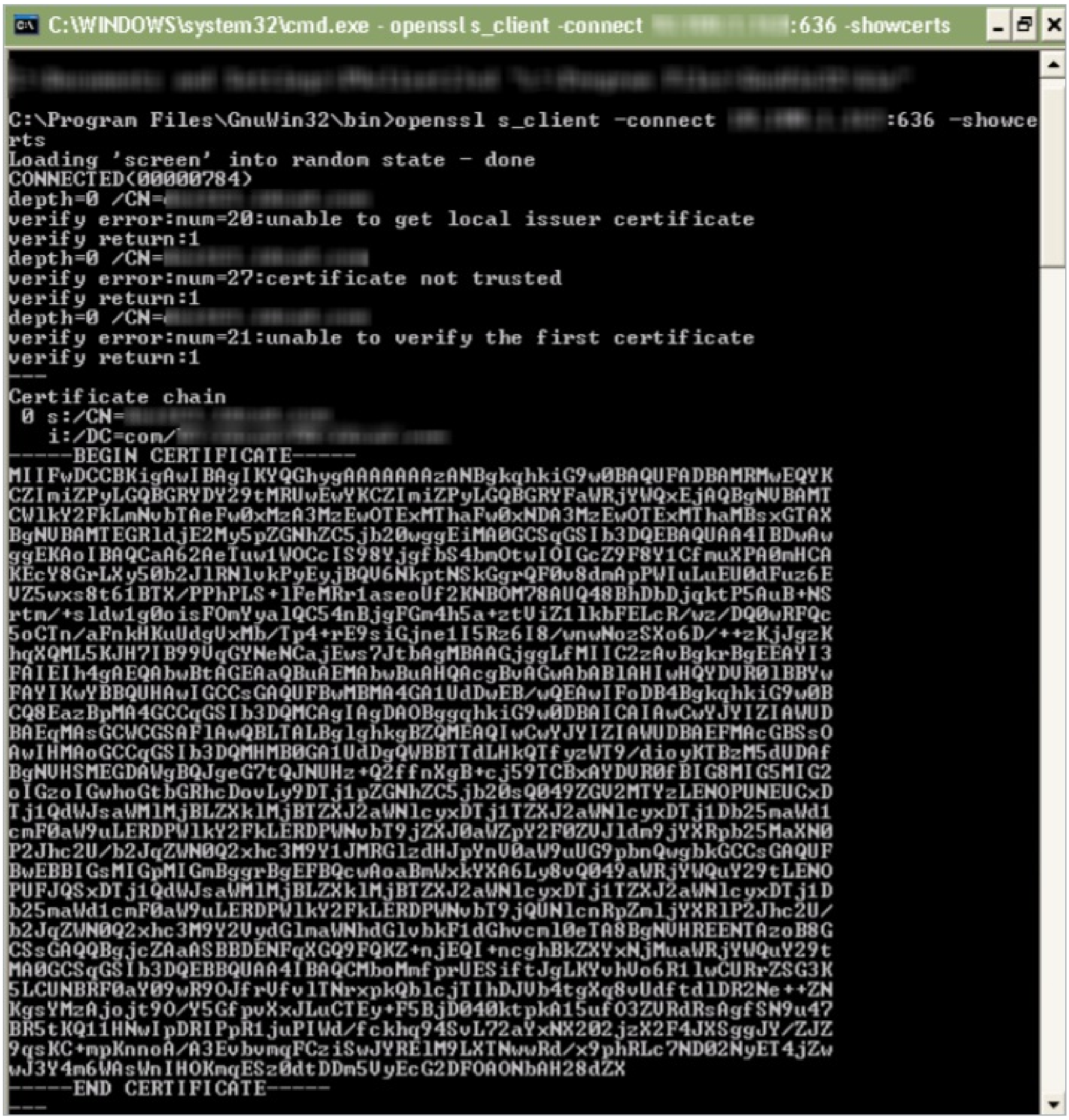
2. Click **Print** next to the desired log.

Prerequisites to Configure Secure LDAP Service

The following steps must be met in order to configure the secure LDAP service.

To prepare your machine for the LDAP service:

1. Back up the default trust store file cacerts located in the **%AGILIANCE_HOME%\Java\jre\lib\security** directory.
2. Create an empty file with any name to store the AD certificate in the machine where RiskVision is installed. For example, **C:\SecureLDAP\keystore.cer**.
3. Open the command prompt and navigate to the path where OpenSSL is installed. For example, **C:\Program Files\GnuWin32\bin**.
4. Run the following command to generate the certificate from the AD server where you want the secure LDAP service to be.
    - `openssl s_client -connect :636 -showcerts`



C:\WINDOWS\system32\cmd.exe - openssl s_client -connect [redacted]:636 -showcerts

```
[redacted]

C:\Program Files\GnuWin32\bin>openssl s_client -connect [redacted]:636 -showce
rts
Loading 'screen' into random state - done
CONNECTED(00000784)
depth=0 /CN=[redacted]
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 /CN=[redacted]
verify error:num=27:certificate not trusted
verify return:1
depth=0 /CN=[redacted]
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/CN=[redacted]
   i:/DC=com/[redacted]
-----BEGIN CERTIFICATE-----
MIIFwDCCBKigAwIBAgIKYQGhygAAAAAAAzANBgkqhkiG9w0BAQUFADBAMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFaWRjYWQxEjAQBgNVBAMT
CWlkY2FkLmNvbTAeFw0xMzA3MzEwOTExMThaFw0xNDA3MzEwOTExMThaMBsxGTAX
BgNVBAMTEGRldjE2My5pZGNhZC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCaA62AeTuw1WOCcIS98YjgfbS4bmOtwIOIGcZ9F8Y1CfmuXPA0mHCA
KEcY8GrLXy50b2J1RNlvkPyEyjBQU6NkptNSkGgrQF0v8dmApPWIuLuEU0dFuz6E
UZ5wxs8t61BTX/PPhPLS+1FeMRr1aseoUf2KNBOM78AUQ48BhDbDjqktP5AuB+NS
rtm/+sldw1g0oisFOmYyalQC54nBjgFGm4h5a+ztViZ1lkbFELcR/wz/DQ0wRFQc
5oCTn/aFnkHKuUdgUxMb/Tp4+rE9siGjne1I5Rz6I8/wnwNozSXo6D/++zKjJgzK
hqXQML5KJH7IB99UqGYNeNCajEws7JtbAgMBAAGjggLfMIIC2zAvBgkrBgEEAYI3
FAIEIh4gAEQAbwBtAGEAaQBuAEMAbwBuAHQAcgBvAGwAbABlAHIwHQYDVR0lBBYw
FAYIKwYBBQUHAwIGCCsGAQUFBwMBMA4GA1UdDwEB/wQEAwIFoDB4BgkqhkiG9w0B
CQ8EazBpMA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAWUD
BAEqMAsGCWCGSAF1AwQBLTALBglghkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcGBSsO
AwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQWBBTTdLHkQTfyzWT9/dioyKTBzM5dUDAf
BgNVHSMEGDAWgBQJgeG7tQJNUHz+Q2ffnXgB+cj59TCBxAYDVR0fBIG8MIG5MIG2
oIGzoIGwhoGtbGRhcDovLy9DTj1pZGNhZC5jb20sQ049ZGU2MTYzLENOPUNEUCxD
Tj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1
cmF0aW9uLERDPWlkY2FkLERDPWNvbT9jZXJ0aWZpY2F0ZUJldm9jYXRpb25MaXN0
P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQwgbkGCCsGAQUF
BwEBBIGsMIGpMIGmBggrBgEFBQcwAoaBmWxkYXA6Ly8vQ049aWRjYWQuY29tLENO
PUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPWlkY2FkLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/
b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTA8BgNVHREENTAzoB8G
CSsGAQQBgjcZAaASBBDENFqXGQ9FQKZ+njEQI+ncghBkZXYxNjMuaWRjYWQuY29t
MA0GCSqGSIb3DQEBBQUAA4IBAQCMboMmfprUESiftJgLKYvhUo6R1lwCURrZSG3K
5LCUNBRF0aY09wR9OJfrUfvlTNrxpkQblcjTIhDJUb4tgXq8vUdftdlDR2Ne++ZN
KgsYMzAjojt9O/Y5GfpvXxJLuCTEy+F5BjD040ktpkA15ufO3ZURdRsAgfSN9u47
BR5tKQ1iHNwIpDRIPpR1juPIWd/fckhq94SvL72aYxNX202jzX2F4JXSggJY/ZJZ
9qsKC+mpKnnoA/A3EvbvmqFCziSwJYRE1M9LXTNwwRd/x9phRLc7ND02NyET4jZw
wJ3Y4m6WAsWnIHOKmqESz0dtDDm5UyEcG2DFOAONbAH28dZX
-----END CERTIFICATE-----
---
```

An example of a generated certificate.

5. Copy and paste the text between **-----BEGIN CERTIFICATE-----**and **-----END CERTIFICATE-----**into the file that was created in step 2.
6. Verify if the content is corrupted by using the following command:
    - `openssl x509 -in \keystore.cer -text`

> If the content has been corrupted, you will need to repeat steps 1-6.

7. Navigate to the location where keytool is installed (E.g., **%AGILIANCE_HOME%\java\bin**).

8. Import the AS certificate file made in step 5 into the**jre\lib\security\cacerts** certificate file by running the following command in one line.
    - `keytool -import -alias ldap1 -keystore %AGILIANCE_HOME%\Java\jre\lib\security\cacerts -trustcacerts -file \keystore.cer`

> The system will require a keystore password in order to import the certificate. The default password for cacerts is **changeit**.

9. Restart the Tomcat server and test the secure LDAP connection in RiskVision by configuring the Authentication Connector.

Configuring LDAP Service

In addition to using the built-in RiskVision solution authentication mechanism, you can configure a local LDAP directory service for authentication. When using LDAP for authentication, the RiskVision solution prompts the user to type a login user name and password. Once the user is authenticated by LDAP (credentials validated with the underlying AD or LDAP directory service), the RiskVision solution retrieves the corresponding user's attributes and permissions based on mapping roles stored in the RiskVision database.

Providing LDAP authentication for the RiskVision solution requires installation of the following:

- A supported LDAP Directory service such as Active Directory (AD).
- Optionally, if LDAP users will be imported into the RiskVision database , login names defined for LDAP users that you want to grant access to the RiskVision solution.

AD or LDAP users are assigned initial roles with access to the Console based on settings and roles defined on the Administration > Login Integration page in the Administration application.

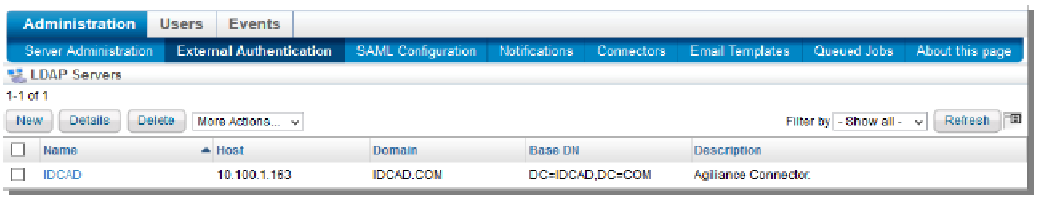
If you want to allow a user to configure an LDAP service, you should assign the System User Manage permission. This permission is assigned to the default Administrator role in RiskVision.

To set up the LDAP service connection:

1. (Note: In a multi-tenant environment, only the 'sysadmin' user in the system tenant space can access the Authentication Connector.)

   In the Administration application, go to **Administration > External Authentication**.

   The **LDAP Servers** page is displayed.

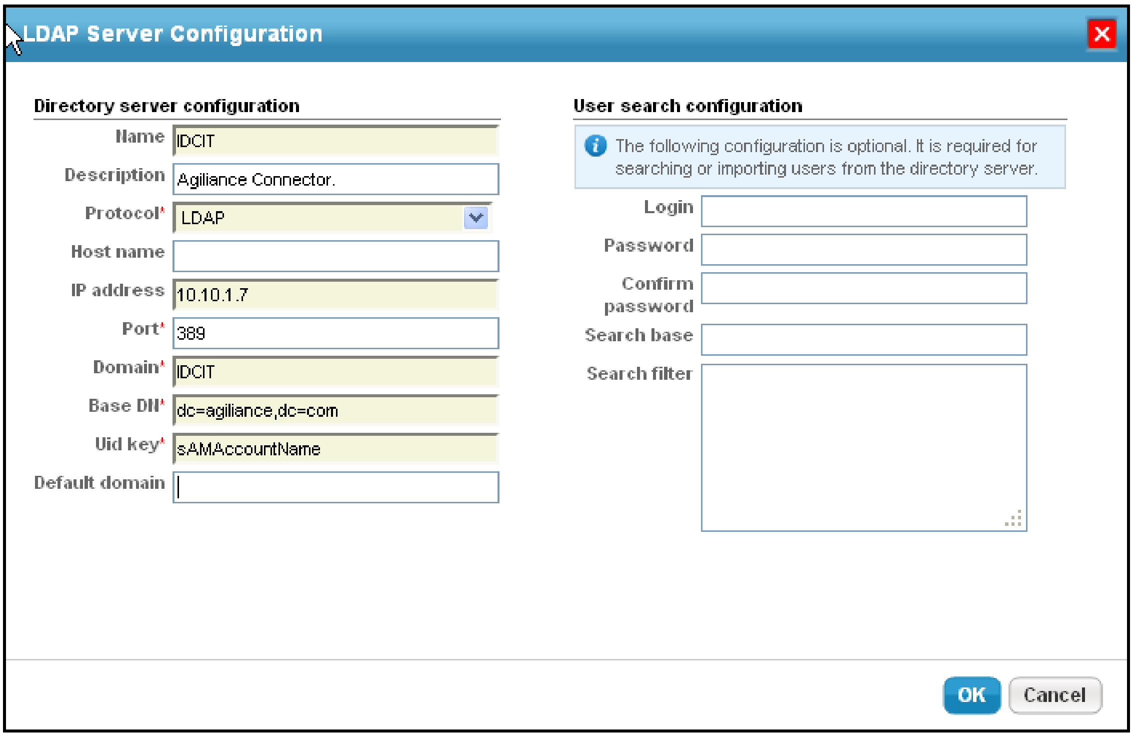


LDAP Servers

1-1 of 1

□	Name	Host	Domain	Base DN	Description
□	IDCAD	10.100.1.163	IDCAD.COM	DC=IDCAD,DC=COM	Agiliance Connector.

2. A default Authentication Connector is available for you to set up an LDAP service. Modify the default LDAP setup or click **New** to create a new LDAP server. When you click new, the **LDAP Server Configuration** dialog appears.



Directory server configuration

Name: IDCIT
Description: Agiliance Connector.
Protocol*: LDAP
Host name:
IP address: 10.10.1.7
Port*: 389
Domain*: IDCIT
Base DN*: dc=agiliance,dc=com
Uid key*: sAMAccountName
Default domain:

User search configuration

The following configuration is optional. It is required for searching or importing users from the directory server.

Login:
Password:
Confirm password:
Search base:
Search filter:

3. Enter the configuration information.
   - Name: Specify the LDAP name.
   - Description: Provide information explaining the purpose to set up an LDAP.

  - Protocol: Select the connection type.
  - Host name: Enter the host name or the IP address.
  - IP address: Enter the IP address.
  - Port: Enter the connection port, the default is 389 (LDAP) or 636 (Secure LDAP).
  - Domain: Specify the domain name. Display domain name for users to select while logging in to RiskVision.
  - Base DN: Enter the base domain such as dc=,dc=com.
  - Uid key: Enter the name of the field that specifies the unique user identifier, For example, uid for standard LDAPs or sAMAccountName for AD.
  - Default domain: Enter the domain name to use as default domain when there multiple configured domains

4. Enter the connection and search details.

   - Login: Optional, enter the account information that the application should use to authenticate users against the LDAP service. The account requires at least read access to the DN and search base.
   - Password: Optional, enter the account password.
   - Confirm password: Verifies if you have entered the correct password when you save.
   - Search base: Used for large directories to prevent time outs, this field is combined with the base DN; for example enter OU=Security.
   - Search filter: Limit the scope of the search to certain objects, for example to search only user in AD enter ObjectClass=User.

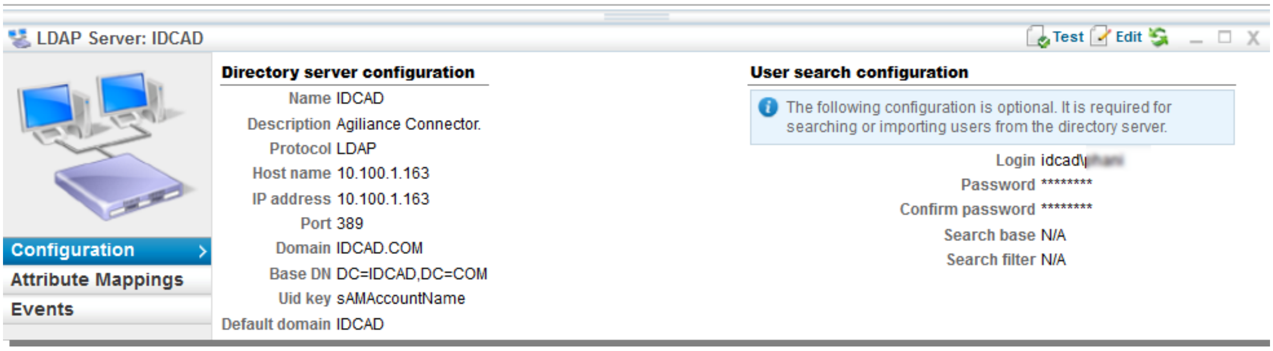
5. Click **OK**.

Next, test the connection.

Testing the Authentication Connector

Use the following instructions to test the connection and ability of the RiskVision solution to authenticate users against the configured LDAP directory.

To test LDAP authentication:



LDAP Server: IDCAD

Directory server configuration

Name IDCAD
Description Agiliance Connector.
Protocol LDAP
Host name 10.100.1.163
IP address 10.100.1.163
Port 389
Domain IDCAD.COM
Base DN DC=IDCAD,DC=COM
Uid key sAMAccountName
Default domain IDCAD

User search configuration

The following configuration is optional. It is required for searching or importing users from the directory server.

Login idcad\[redacted]
Password ********
Confirm password ********
Search base N/A
Search filter N/A

1. In the Administration application, go to **Administration** > **External Authentication**. The **LDAP Servers** page is displayed

2. Select an LDAP server and click **Details**. The LDAP server details are displayed below on the same page.

3. At the top-right corner of LDAP details, click **Test**. If the user search information is unavailable, click **Edit** and enter a username and password for a user within the base group and search base that matches the search filter and then click **Save**.

The Authentication success or failure message is displayed.

Configuring Attribute Mappings

When you create a new LDAP server configuration, the default attribute mappings that you see is a replica of settings on the Login Integration page. Use Attribute Mappings to set up authentication, external roles, and user attributes separately for each LDAP server. This provides an opportunity to create up to ten domain controllers and/or global catalogs and appropriate criteria can be determined for users logging into RiskVision application using each LDAP server.

To configure attribute mappings:

1. In the Administration application, go to **Administration** > **External Authentication**. The **LDAP Servers** page is displayed.
2. Select an LDAP server and click **Details**. The LDAP server details are displayed below on the same page.
3. Click **Attribute Mappings**. The tab details are displayed.
4. To change the settings on each tab, click **Edit**.
5. When you finish configuring, click **Save**.

Health Report

The RiskVision Health Report is intended to provide you information on the status of your RiskVision deployment. You can use this information to better understand how the RiskVision system is being used, the deployment architecture, and whether you possess the proper license entitlements.

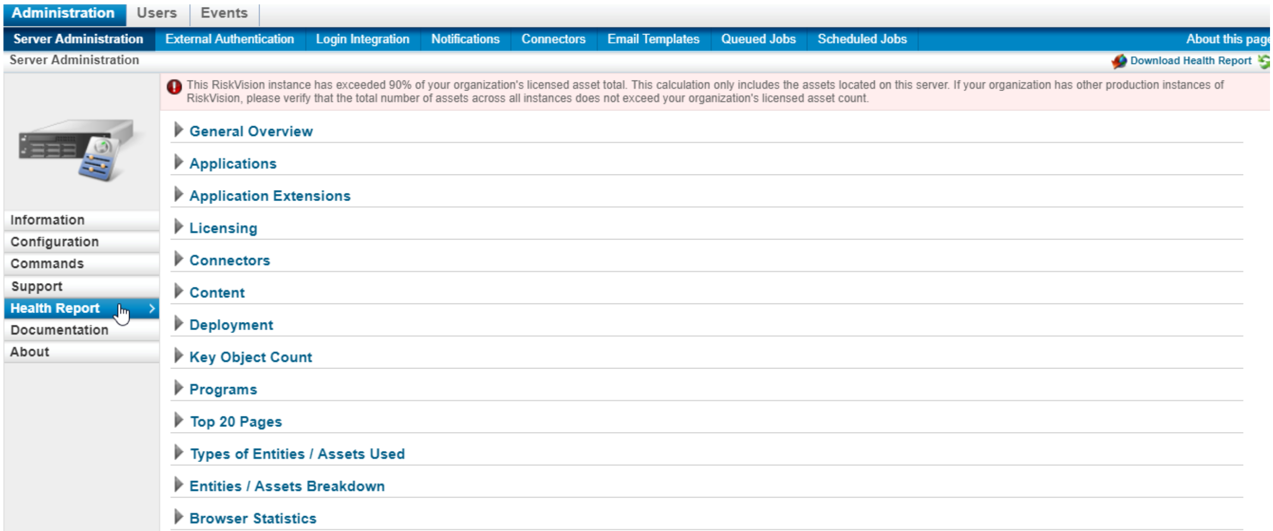
You can also send the data in the Health Report to Resolver Support to help with troubleshooting issues that you are experiencing.

Change How Often Health Reports Are Sent:

1. Go to **Administration**>**Server Administration**.
2. Select the **Configuration** tab.
3. Click Edit
4. In the **Interval to send the Health Report (Days)** field, enter the interval by which Health Reports should be sent.
5. To disable sending Health Reports to Resolver, select No.
6. Click ✓ Save

View the Health Report:

In the **Administration** application, go to **Administration** > **Server Administration**, and click **Health Report** tab.



This RiskVision instance has exceeded 90% of your organization's licensed asset total. This calculation only includes the assets located on this server. If your organization has other production instances of RiskVision, please verify that the total number of assets across all instances does not exceed your organization's licensed asset count.

The Health Report contains the following information that you can view and download:

- **General Information**. Provides the basic details, such as your organization name, domain name, and entity licensing information.
- **Applications**. Provides a list of RiskVision licensed applications and the number of licensed users. It helps in tracking the application status that is installed in your environment and also the number of users using the application. An icon signifies ✓ that an application is licensed and an icon signifies ✖ that an application is not installed; because you do not possess the application.
- **Application Extension**: Provides a list of RiskVision extended applications that are installed in your environment and helps you keep track of extended application's license status. An icon signifies ✓ that the extended application is licensed and an icon signifies ✖ that an application is not enabled.
- **Licensing**. Provides a count of connectors, assets, and vendors that are licensed, active and delta.
- **Connectors**. Provides a list of RiskVision licensed Connectors that are used and unused. The connectors that are in use allows you to view the physical location details, such as version and hostname, and activity details, such as entities import count and last updated.
- **Content**. Provides a list of all the content under the RiskVision group in the content tree.

- **Deployment**. Provides details about the RiskVision deployment. Data, such as version, operating system, hostname, IP address, domain name, and last started on provides the location of RiskVision Server, database server, Report server, or Services. If you have moved any of the RiskVision installed components to a new host, the deployment section will reflect the details of the component correctly after you restart the services specific to that relocated component. For example, when you deploy the database server on a new host, you must restart the RiskVision Tomcat service to obtain the latest deployment details. Any obsolete deployment details of a component remain in the deployment section. To delete such components, check the box next to a component, and click **Delete**.

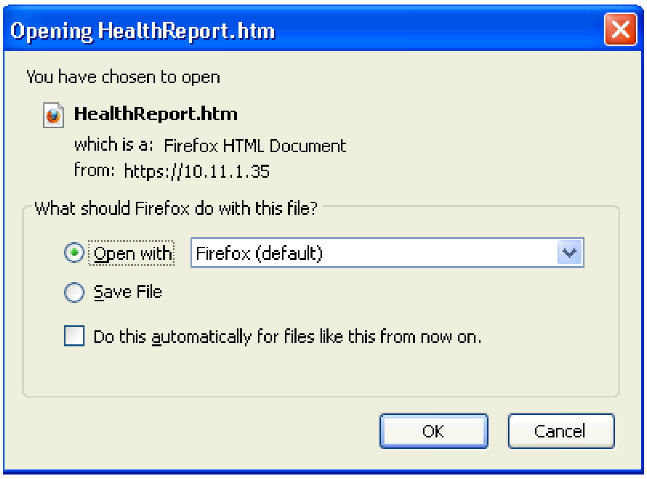
  For MySQL database that is deployed on a separate machine other than the RiskVision server, the operating system value is displayed as "N/A.' Because an underlying firewall that exists between the RiskVision server machine and the database machine may not provide access to the operating system details of the database.

- **Key Object Count**. Provides a list of object count for each key object type across all RiskVision applications.
- **Programs**. Provides a list of programs grouped by application. Each program summarizes the count of assessments, controls, and control results. In addition, any programs that were using draft content in a version earlier than 8.0 will appear in the Programs Using Draft Content section. Programs using draft content are shown in red and have a number of issues associated with them. Hence, the draft content used on all such programs must be migrated to the latest version. For step-by-step information on how to migrate draft content, contact Customer Support to obtain the *Migrating Draft Content* technical notes.
- **Documents**: Shows the number of attachments and their size.
- **Top 20 Pages**. Provides a list of top 20 pages with a metric value displaying the number of times a page is accessed.
- **Types of Entities/Assets Used**: Provides a list of entities/assets available in the RiskVision application.
- **Entities/Assets Breakdown**. Provides a count of entities category wise. The available entity categories are discovered, unmanaged, managed, non-vendor, and vendor.
- **Browser Statistics**. Displays a list of web browsers and the number of times the web browser was used by users for accessing the RiskVision applications.

Downloading Health Report

To download the Health Report:

1. **In the Administration application, go to Administration > Server Administration, and click the Health Report tab.**
2. Click **Download Health Report** at the top right corner of the pane.
3. The **Opening HealthReport.htm** pop-up appears prompting you to choose open or save the Health Report.



Opening HealthReport.htm

You have chosen to open

HealthReport.htm

which is a: Firefox HTML Document

from: https://10.11.1.35

What should Firefox do with this file?

● Open with Firefox (default)

○ Save File

□ Do this automatically for files like this from now on.

4. Select Save File to save the report. The Health Report is downloaded to the local directory.

Introduction

Security Assertion Markup Language (SAML) is a single sign-on login standard that RiskVision uses to authenticate and authorize users. For more information on SAML, see the OASIS technical overview.

These technical notes will cover how to

- Install and configure the Shibboleth Service Provider;
- Configure the SAML Identity Provider, Apache, and Tomcat;
- Activate and configure connectors in RiskVision;
- Enable Single Sign-On Login in SAML; and
- Establish and manage roles in RiskVision.

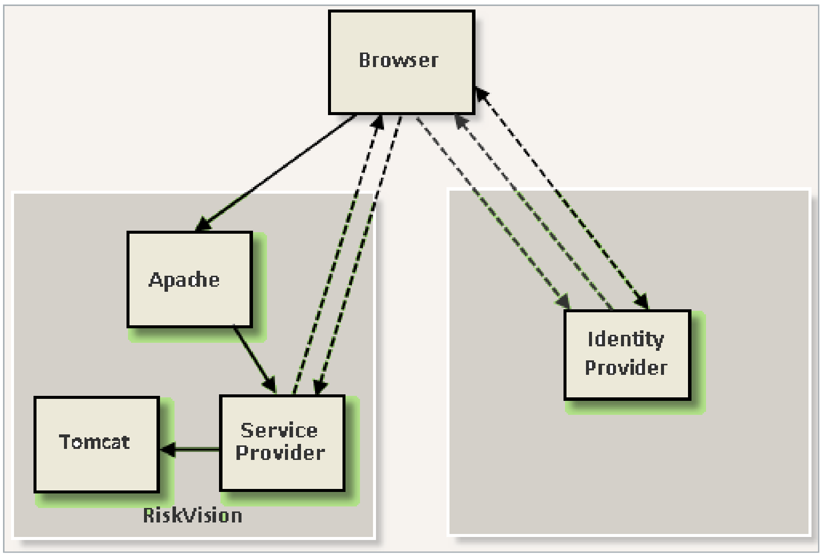
Supported Versions

Resolver supports Shibboleth version 2.5.3 and below in RiskVision versions 7.5 to 9.3. What if RiskVision upgrades to above 9.3? Should we say something more inclusive? These technical notes only cover the installation of Shibboleth on Windows platforms.

This article seems very short now. I'm thinking I should combine it with the Introduction article.

Understanding SAML

When a user attempts to log in to RiskVision, the browser first sends a request to the Apache server. The request is redirected to the SAML Service Provider, which will verify the authentication token against the Identity Provider (IdP). The browser will display the login page so that the login credentials can be provided to the IdP.



A visual overview of how SAML handles authentication information.

If the authentication is successful, the IdP will generate and redirect the SAML response to the Tomcat server through the browser and Service Provider. RiskVision will verify the user in the system and log him or her in if available. However, if a user is not available in RiskVision, he or she will first be created in RiskVision and then be logged in.

Identity Provider Pre-Requisites

I created this article as per your request. I'm not terribly familiar with this subject so please let me know if it is missing anything or if it should be in another location. Also, should we mention in this article that Resolver does not support IdP anymore and that the user has to configure it him or herself?

In order to configure RiskVision SSO, the Identity Provider (IdP) must provide the following information:

- IdP metadata
- SAML attributes:
  - **uid**
  - **surname**
  - **givenName**
  - **mail**
- IdP entity ID

In addition to the above, it is also necessary that the Service Provider (SP) provide the following to the IdP:

- Assertion Consumer Service URL
- SP entity ID
- SP metadata

If any of the above elements are missing, contact your IdP or SP.

Install the Shibboleth Service Provider

Communication with the SAML Identity Provider requires installing and configuring the Shibboleth service provider (SP). The Shibboleth SP is an open source software solution for web single sign-on and is available for both Windows (32-bit and 64-bit). Install the suggested version of the Shibboleth SP for Apache by downloading the appropriate Shibboleth SP installer from here. Ensure the SP is downloaded for 64-bit Windows XP, Windows Server 2003, Windows Server 2008, or Windows Server 2012.

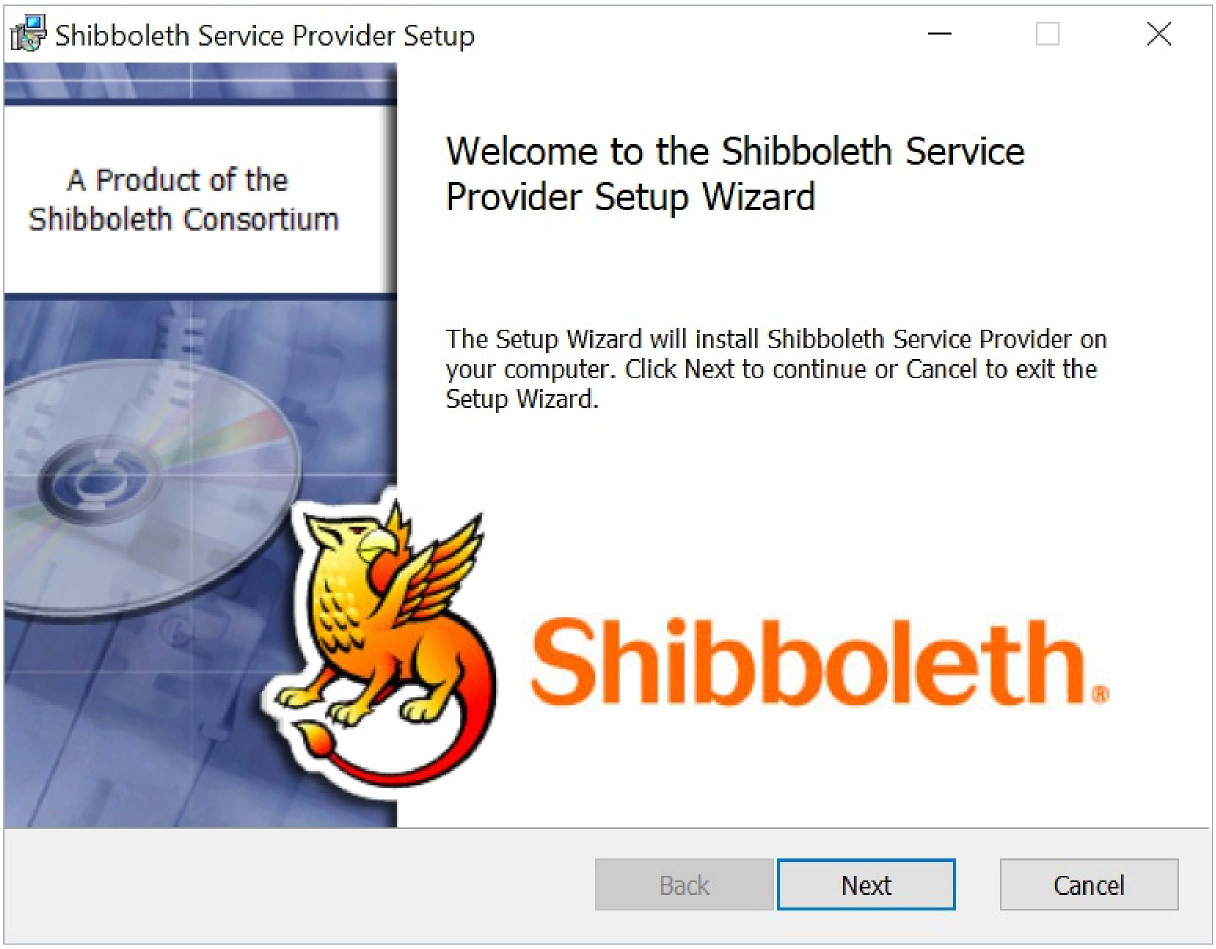
> Resolver recommends installing the Shibboleth SP on a Windows Server 2008 R2 - machine that has a 64-bit Apache Web Server.

To install the Shibboleth service provider:

1. Download the Shibboleth installer.

2. Run the installer file to launch the setup wizard.

3. Click **Next**. I've kept the screenshots at the original size, but would you like me to shrink them down? Personally I like them at this size.



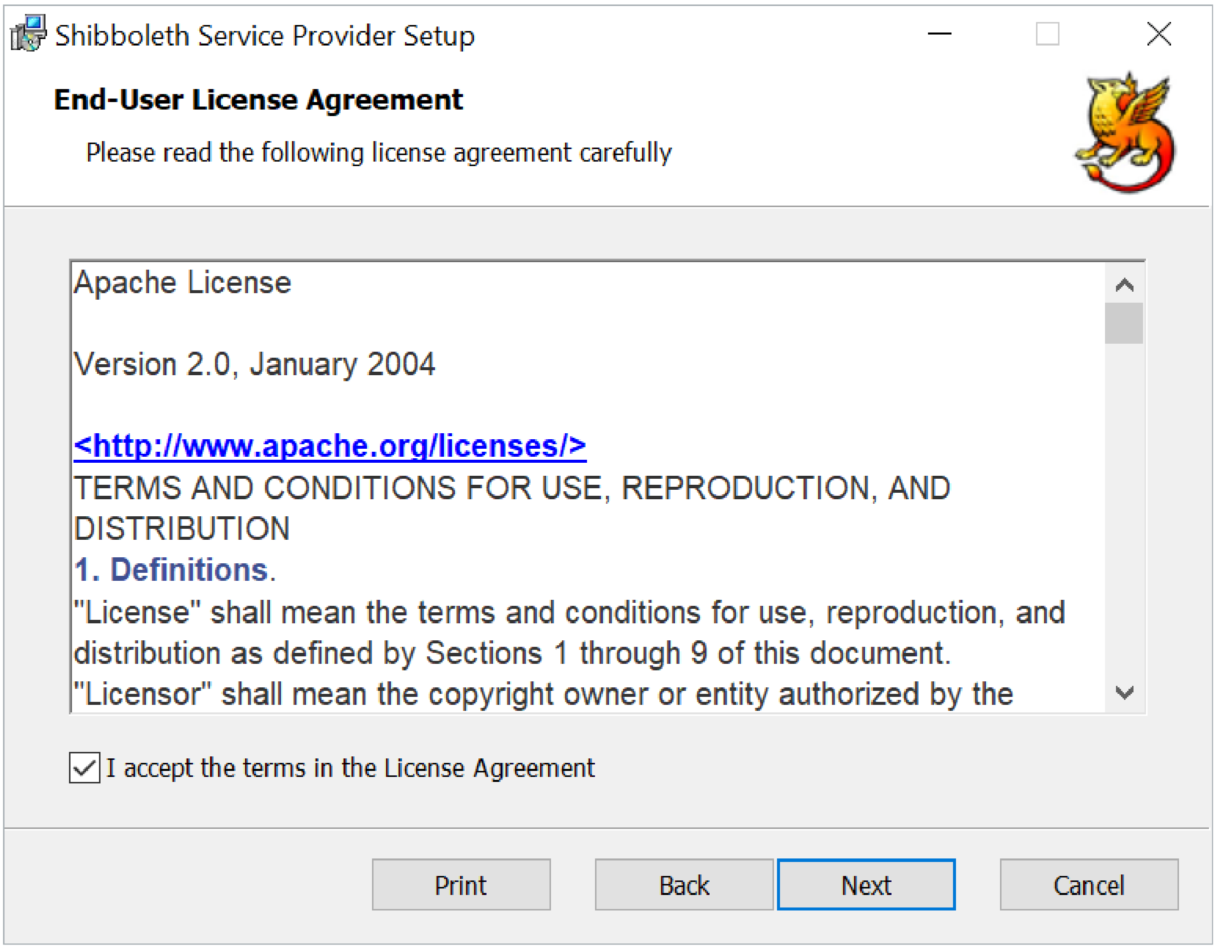
Shibboleth Service Provider Setup

Welcome to the Shibboleth Service Provider Setup Wizard

The Setup Wizard will install Shibboleth Service Provider on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

The Shibboleth Service Provider Setup Wizard.

4. Click the **I accept the terms in the License Agreement** checkbox and click **Next**.



End-User License Agreement

Please read the following license agreement carefully

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.
"Licensor" shall mean the copyright owner or entity authorized by the

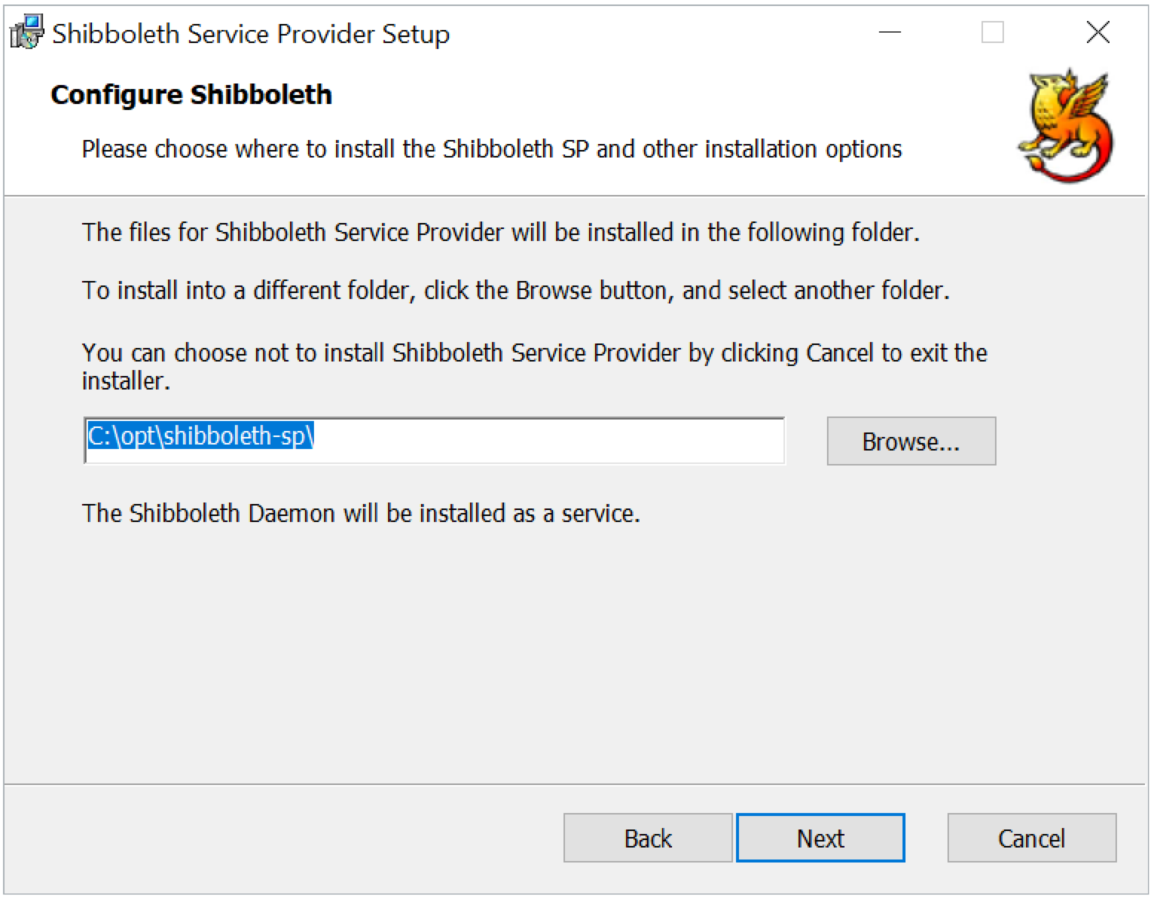
☑ I accept the terms in the License Agreement

The End-User License Agreement.

5. To select the installation path:

   a. Click **Browse** to select where you would like to install the service provider.

   b. Click **Next**.



Shibboleth Service Provider Setup

Configure Shibboleth

Please choose where to install the Shibboleth SP and other installation options

The files for Shibboleth Service Provider will be installed in the following folder.

To install into a different folder, click the Browse button, and select another folder.

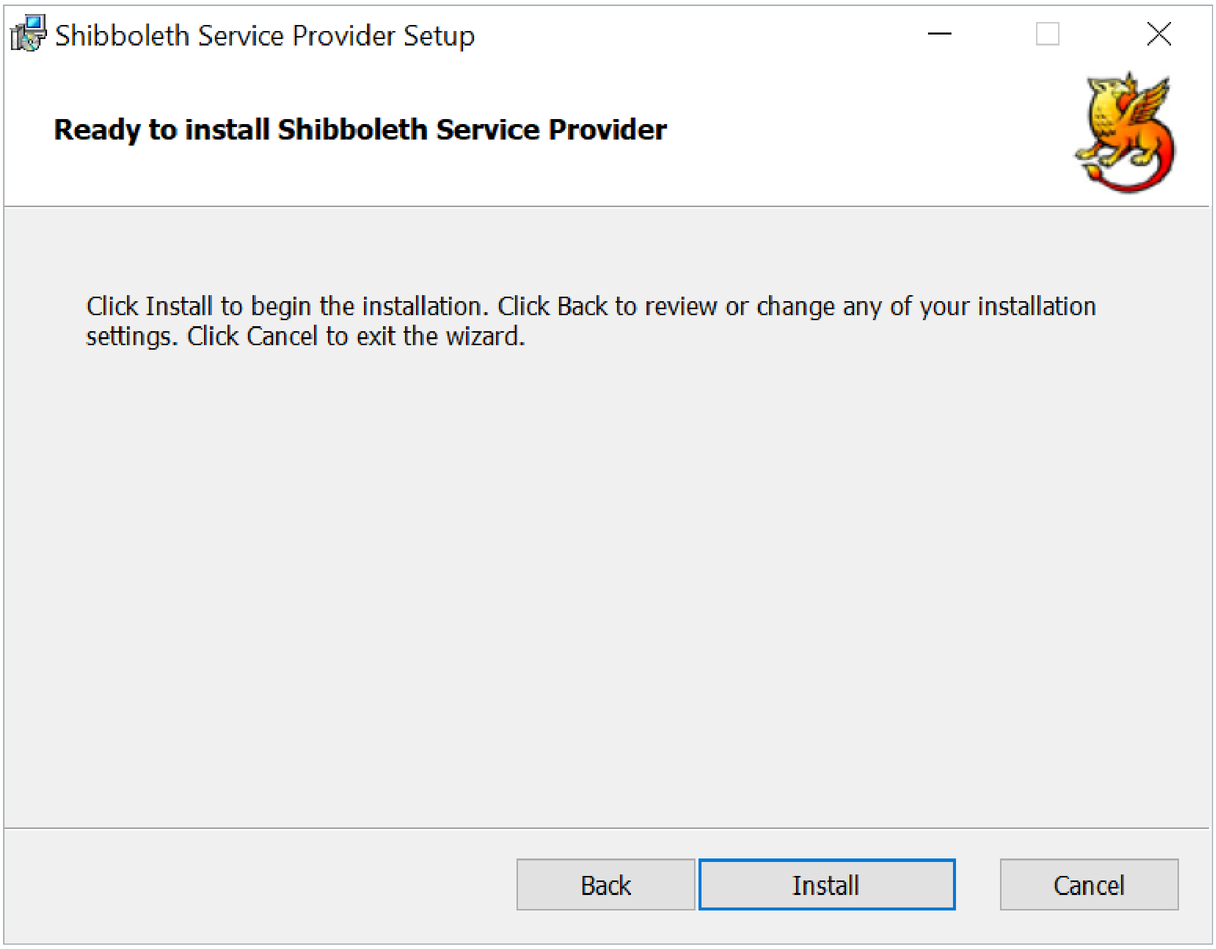
You can choose not to install Shibboleth Service Provider by clicking Cancel to exit the installer.

C:\opt\shibboleth-sp\

The Shibboleth Daemon will be installed as a service.

The Installation Path selection screen.

6. Click **Install**.

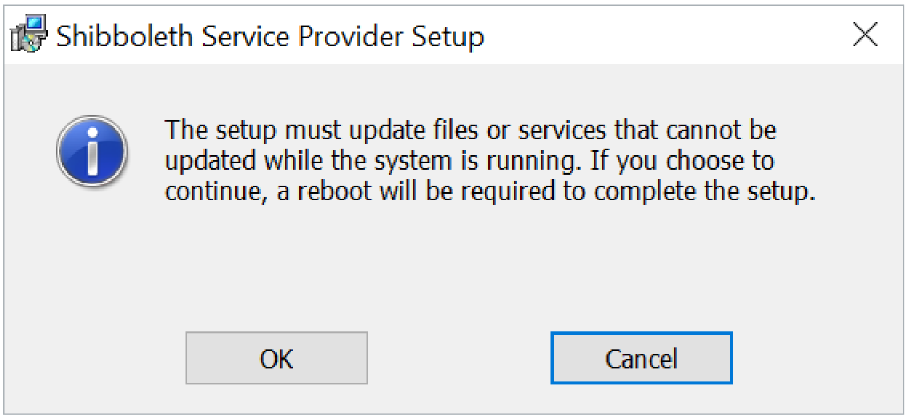

Shibboleth Service Provider Setup

Ready to install Shibboleth Service Provider

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

The Ready to Install screen.

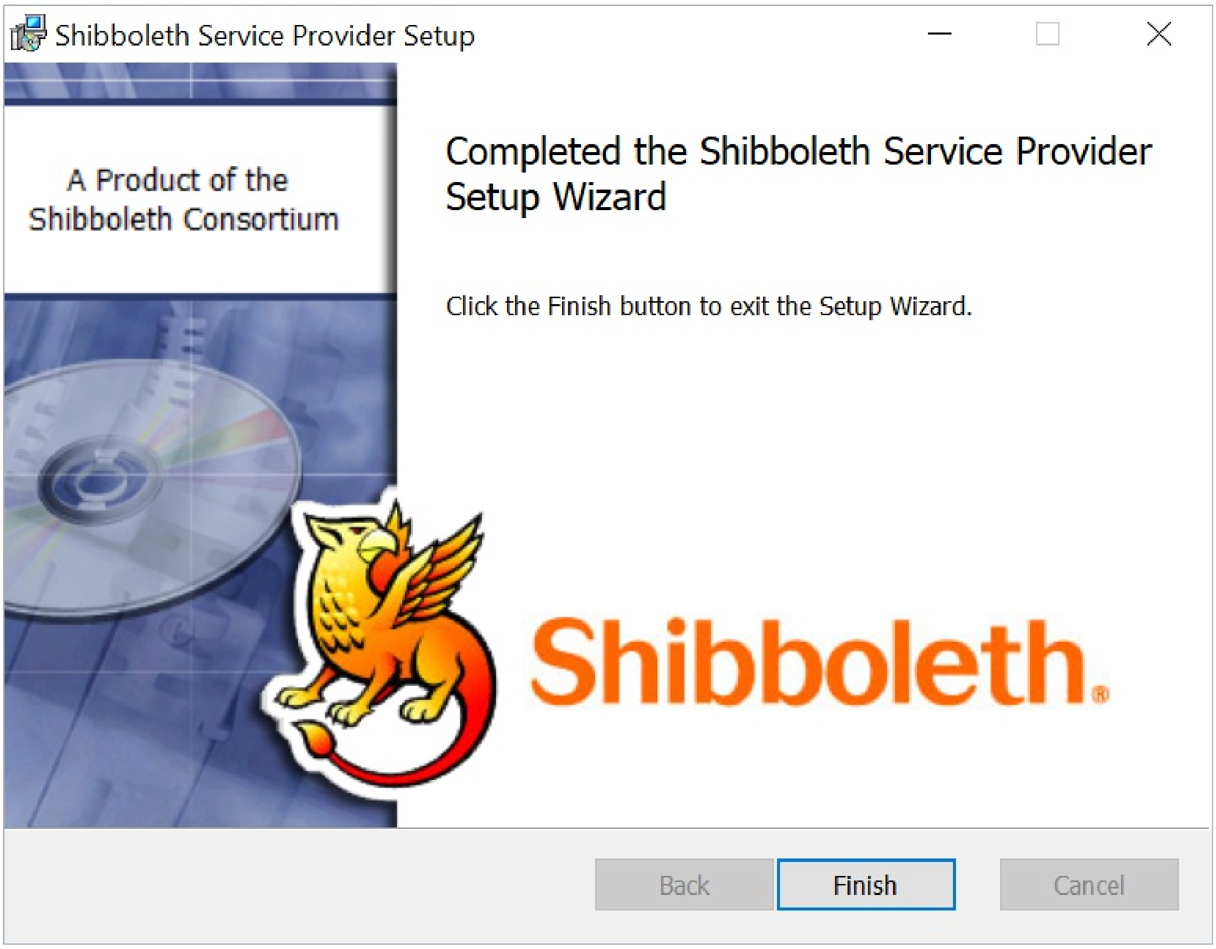
7. Ensure all work has been saved, then click **OK** on the pop-up window.


Shibboleth Service Provider Setup

The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

The Reboot Warning pop-up.

8. Click **Finish** to exit the wizard once installation is complete.


Shibboleth Service Provider Setup

A Product of the Shibboleth Consortium

Completed the Shibboleth Service Provider Setup Wizard

Click the Finish button to exit the Setup Wizard.

The Completion screen.

9. Restart your computer before you use the Shibboleth SP. Should the user still do this step if the computer reset on its own as part of the installation process in step 7?

Configure the RiskVision Apache Web Server

In order to configure Apache to provide RiskVision with SAML authenticated single sign-on, the following actions must be performed:

- Copy the SAML configuration files
- Configure the **httpd.conf** file
- Configure the **httpd-ssl.conf** file
- Configure the **httpd-ssl-saml.conf** file
- Configure the **hosts** file

Once you have performed all of these actions, you should restart Apache in order for the changes to take effect.

> In these technical notes,**%_AGILIANCE_HOST_NAME_%** refers to the required virtual hostname without SAML authentication, and **%_SAML_MACHINE_HOSTNAME_%** refers to the required virtual hostname with SAML authentication. For example, **%_AGILIANCE_HOST_NAME_%** could be `qa143-vendor.idcagl.com:443` and **%_SAML_MACHINE_HOSTNAME_%** could be `qa143.idcagl.com:443`. I decided to put the examples up here rather than every instance mentioned below. I think this would make it easier to read for customers. Let me know if you would prefer I do it the other way.

To copy the SAML configuration files:

1. Navigate to the **%AGILAINCE_Home%\apache2\conf\SAML\extra** folder and copy the below files:
    - **httpd-ssl.conf**
    - **httpd-ssl-saml.conf**
    - **agiliance-saml.conf**
2. Paste the files into **%AGILAINCE_Home%\apache2\conf\extra**.

To configure the httpd.conf file:

1. Navigate to the **%AGILIANCE_HOME%\apache2\conf\extra** folder and open the **httpd.conf** file using a text editor.
2. Uncomment the following line:

```
ServerName Localhost:80
```

To configure the httpd-ssl.conf file:

1. Navigate to the **%AGILIANCE_HOME%\apache2\conf\extra** folder and open the **httpd-ssl.conf** file using a text editor.
2. Configure the file to listen to **%_AGILIANCE_HOST_NAME_%** and **%_SAML_MACHINE_HOSTNAME_%**:
    a. Add the following lines to the file: I changed the host names as specified in your document. Let me know if I misunderstood anything.

```
NameVirtualHost %_AGILIANCE_HOST_NAME_%
NameVirtualHost %_SAML_MACHINE_HOSTNAME_%
```

    b. Specify the appropriate RiskVision hostname:

```
: 443>
```

    c. Specify the server name:

```
: 443>
# The default character set if UTF-8 AddDefaultCharset UTF-8
ServerName <%_AGILIANCE_HOST_NAME_%>
```

d. Uncomment the following line:

```
Include conf/extra/httpd-ssl-saml.conf
```

To configure the httpd-ssl-saml.conf file:

1. Navigate to the **%AGILIANCE_HOME%\apache2\conf\extra** folder and open the **httpd-ssl.conf** file using a text editor.

2. Run the hostname command (`sethostname`) to specify the **%_SAML_MACHINE_HOSTNAME_%**. I'm not sure I understood the screenshot. Just to be sure I understand, would you like me to delete this step?

3. Specify the hostname as shown below:

```
 : 443>
# The default character set if UTF-8 AddDefaultCharset UTF-8
ServerName <%_SAML_MACHINE_HOSTNAME_%>
..
```

4. Specify the Shibboleth home directory:

```
 Include /etc/shibboleth/apache24.config
```

5. Enable multi-tier architecture by inputting the following:

```
 ProxyPass /spc ajp://localhost:8009/spc
 ProxyPassReverse /spc ajp://localhost:8009/spc
```

To configure the hosts file:

1. Navigate to the **%WinDir%/system32/drivers/etc/** folder and open the **hosts** file using a text editor.

2. Map **%_SAML_MACHINE_HOSTNAME_%** to **%MACHINE_HOSTNAME%**. I try not to use screenshots of code. If you think users will understand these steps then I will leave it. If you think we need the screenshot, I will add it.

Configure the Shibboleth Service Provider

Once Shibboleth has been installed, you must navigate to the **%SHIBBOLETHSP_HOME%\etc\shibboleth** folder and configure the following XML files:

- **shibboleth2.xml**
- **attribute-map.xml**
- **attribute-policy.xml**

> For the sake of convenience, the service provider server location will be referred to as **SP_SERVERNAME** and the identity provider server location will be referred to as **IdP_SERVERNAME**.

To configure shibboleth2.xml:

1. Configure the following settings in the **shibboleth2.xml** file:

   a. **Entity ID:** Ensure that the element matches the following:

   ```
   entityID= "https:///shibboleth" REMOTE_USER="eppn persistent-id targeted-id" signing="true"
   encryption="true" attributePrefix="AJP_">
   ```

   > If the `encryption` and `attributePrefix` values are not present in this file, they must be added as specified above.

   b. **MetadataProvider:**

      i. Ensure that the **MetadataProvider** elements match the following:

      ```

      uri=https://:/idp/shibboleth backingFilePath="federation-metadata.xml"
      reloadInterval="7200" />
      ```

      ii. You must also ensure that the **entityID** and **Location** elements of the **idp-metadata.xml** file match the URL of the identity provider metadata. However, at times you may have to configure the identity provider metadata file when the port number is missing or the URL points to the local host.

      > In the event that the Shibd daemon fails to update the metadata, Resolver recommends manually copying the **idp-metadata.xml** file into the **SP_SERVERNAME** location. If this happens, you must replace the URI with the **<%SHIBBOLETHSP_HOME%>\etc\shibboleth\idp-metadata.xml** file.

   c. **CredentialResolver:** Ensure that the **key** and **certificate** of this element match the following: Would you mind clarifying your notes on c and d for me? Are you saying that these steps are no longer required since Shibboleth will update them automatically?

   ```
   I have already told the user to make the checkAddress attribute "true" in the below instructions.
   ```

   ```
    handlerURL="/Shibboleth.sso" handlerSSL="false" cookieProps="; path=/; secure"
   exportLocation="http://localhost/Shibboleth.sso/GetAssertion" exportACL="127.0.0.1"
   idpHistory="false" idpHistoryDays="7">
   ```

`To configure attribute-map.xml:`

1. `Open the` **`attribute-map.xml`** `file and uncomment the attributes that you want to use. At a minimum, you should uncomment the following:`

   - **`cn`**
   - **`surname`**
   - **`sAMAccountName`**
   - **`givenname`**

- `uid`
- `mail`

To configure attribute-policy.xml:

1. Open the **attribute-policy.xml** file and ensure that it has the following at minimum:

```
  xmlns="urn:mace:shibboleth:2.0:afp:mf:basic"
xmlns:basic="urn:mace:shibboleth:2.0:afp:mf:basic"
xmlns:afp="urn:mace:shibboleth:2.0:afp" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

2. **Optional:** Delete or comment all other elements or attributes in this file.

Obtain the Metadata File

Metadata is used by SAML to ensure a secure connection with the service provider. In the case of the Shibboleth Service Provider, a metadata file from the Shibboleth website must be obtained.

To obtain the Shibboleth metadata file:

1. Start the Apache server.
2. Enter the URL: **https:///Shibboleth.sso/Metadata**.
3. Select **File > Save As** to save the file.

Configure the RiskVision Tomcat Application Server

In order for Tomcat to be be able to handle authenticated requests from Shibboleth, the following files must be configured:

- **agiliance.properties**
- **applicationContext-security.xml**
- **server.xml**

After the below changes have been made, reset the Tomcat service.

To configure agiliance.properties:

1. Navigate to the **%AGILIANCE_HOME%\config** folder and open the **agiliance.properties** file using a text editor.
2. Add the `com.agiliance.SAML.configured=true` property to the file.
3. Specify the SAML hostname at `virtual.host = %AGILIANCE_HOST_NAME%`.

To configure applicationContext-security.xml:

1. Navigate to the **%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF** folder and open the **applicationContext-security.xml** file.

   > Resolver recommends that you back up this file before making any changes. You may need to revert the file to its original settings for role maintenance.

2. Comment the first element and uncomment the second one as shown below:

Activate a Connector in RiskVision Using SAML

Legacy connectors installed in RiskVision will not be able to establish communication using SAML SSO. In order for SAML to work, these connectors must first be activated.

To activate a connector:

1. Navigate to the **%AGILIANCE_HOME%\Connectors\Server- side\cfg** directory open the **connector.properties** file.
2. Set `server_host` as %_AGILIANCE_HOST_NAME_%.
3. Restart the connector services to affect the latest changes.

Configure a Web Services Connector

In order for a Web Services connector to work with RiskVision, You must configure the following properties: I guessed this from the original document, but is it correct? The original mentioned something about RiskVision release versions that I did not understand.

- **itgrcxml-ws-client-configuration**
- **agiliance-heartbeat-client-configuration**
- **WebServicesClient.properties** The original document said these last two items are "for 6.5 and after releases". What does that mean?
- **agiliance.default.system** The original document said "Refer to the previous section". Which previous section?

To configure itgrcxml-ws-client-configuration:

1. Navigate to the **%WebservicesClient_HOME%\etc\conf** folder and open the **itgrcxml-ws-client-configuration** file using a text editor.
2. Change the URL of the element as specified below:

To configure agiliance-heartbeat-client-configuration:

1. Navigate to the **%WebservicesClient_HOME%\plugins\com.agiliance.itgrcxml.heartbeat.plugin\conf** folder and open the **agiliance-heartbeat-client-configuration** file using a text editor.
2. Change the URL of the element as specified below:

To configure WebServicesClient.properties:

1. Navigate to the **%WebservicesClient_HOME%>\etc\conf** folder and open the **WebServicesClient.properties** file using a text editor.
2. Change the URL of the element as specified below:

```
agilianceWebServiceUrl=https\://%AGILIANCE_HOST_NAME%:443/spc/services/agiliancews
```

3. Change the URL of the element as specified below:

```
itgrcxmlWebServiceUrl=https\://%AGILIANCE_HOST_NAME%/itgrcxml/services/itgrcxmlws
```

To configure agiliance.default.system:

Not sure what to put here. Is it the same as WebServicesClient.properties but with the file name changed?

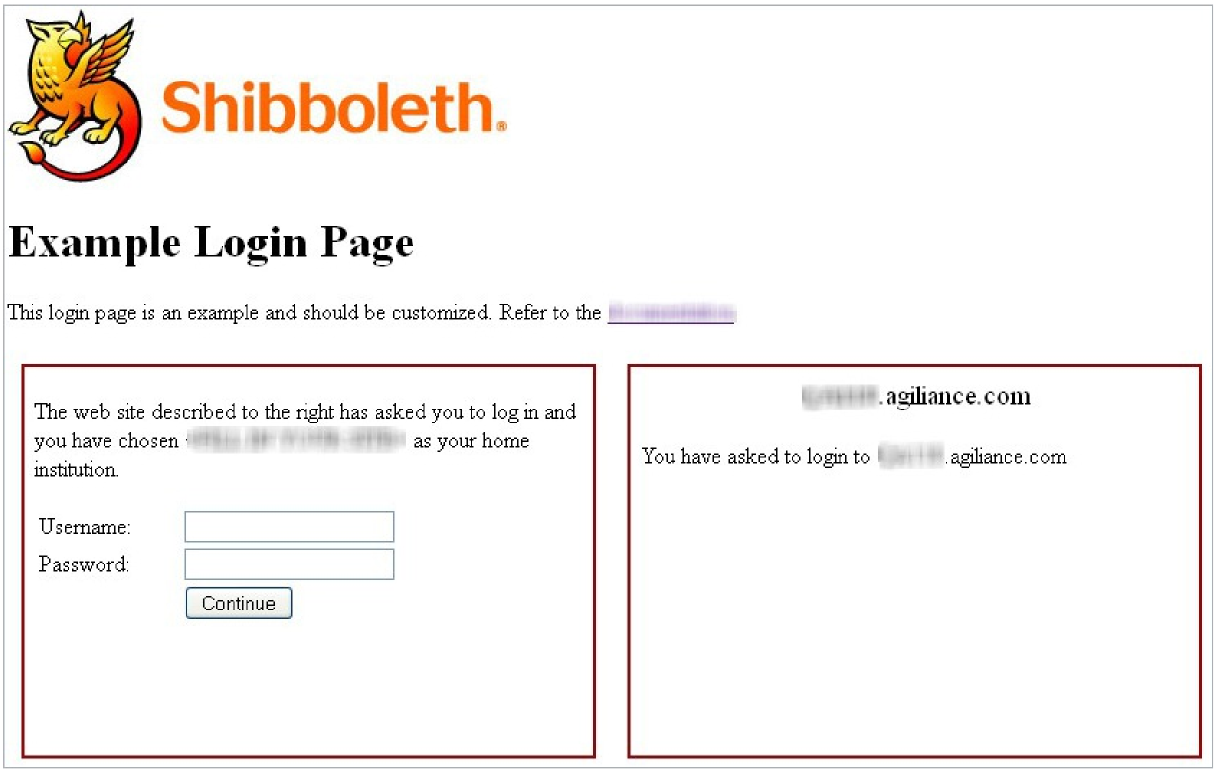
SAML Login/Logout

Once you have installed and configured the SAML Web SSO profile, your users should be able to log in and out of RiskVision using SAML.

To log in to RiskVision:

1. Enter the URL of your company's domain into the web browser of your choice to access the RiskVision login screen.

> Depending on your identity provider's environment, your login page may appear different. The example below is a sample login page from an environment that uses the Shibboleth service and identity providers.



Example Login Page

This login page is an example and should be customized. Refer to the [redacted]

The web site described to the right has asked you to log in and you have chosen [redacted] as your home institution.

Username:

Password:

[redacted].agiliance.com

You have asked to login to [redacted].agiliance.com

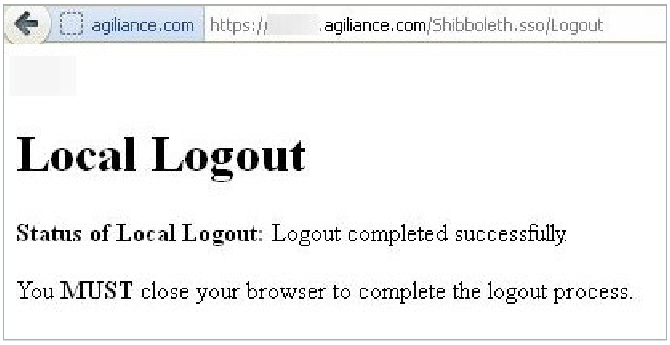
An example of a login page that uses the Shibboleth service and identity providers.

2. Enter your username and password into the **Username** and **Password** fields.

3. Click **Continue**.

To log out of RiskVision

Click **Logout** from the SAML page (is this RiskVision?).



Local Logout

Status of Local Logout: Logout completed successfully.

You **MUST** close your browser to complete the logout process.

An example of a logout page that uses the Shibboleth service and identity providers.

Configure the Local Logout

I would like to put a context paragraph here. Why would an administrator want to configure the local logout?

To configure the local logout:

1. Navigate to the **%SHIBBOLETHSP_HOME%\etc\shibboleth** folder and open the **shibboleth2.xml** file using a text editor.

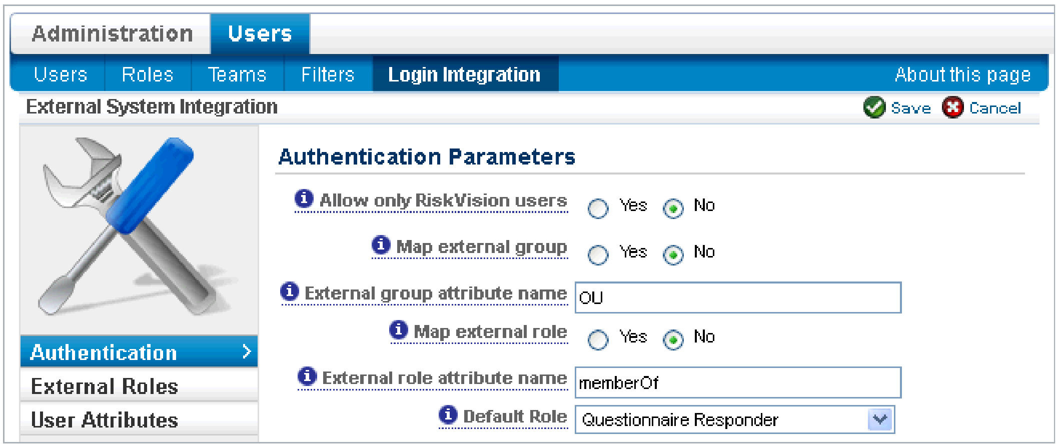
2. Set the **LogoutInitiator** to **Local** as shown below:

3. **Optional:** To customize your local logout screen, update the **localLogout.html** file in the **%SHIBBOLETHSP_HOME%\etc\shibboleth** folder. Users who log out of RiskVision will be taken to whatever is in the **localLogout.html** file.

4. Restart the Shibboleth 2 Daemon to put these changes into effect.

Establishing and Managing Roles

In RiskVision, new users can be created manually or by importing them. When SAML has been configured properly, a user will beautomatically created in RiskVision when logging in through an identity provider for the first time. Newly created users will be assigned the default role that has been set in the **Login Integration** tab of the **Users** menu.



Authentication Parameters

Allow only RiskVision users ○ Yes ● No

Map external group ○ Yes ● No

External group attribute name: OU

Map external role ○ Yes ● No

External role attribute name: memberOf

Default Role: Questionnaire Responder

The Login Integration tab of the Useers Menu in RiskVision.

A SAML user that has been assigned to the **administrator** role can perform user management tasks such as importing users, changing the default tole in the **Login Integration** tab, and changing the roles and permissions for users in general.

If at least one SAML user has not been granted an **administrator** role, a system administrator must bypass the normal SAML SSO login in order to grant access. I didn't really understand how this was phrased in the original document and this is my interpretation of it. Is this correct?

To bypass the SAML SSO login:

1. Disable SAML by reverting the **applicationContext-security.xml** file to its original settings before you configured it.
2. Restart Tomcat to put the above changes into effect.
3. Log in to RiskVision.
4. Access the **Administration** application to assign roles and permissions to the SAML users. Ensure that one or more SAML users has been assigned to the **administrator** role.
5. Reconfigure the **applicationContext-security.xml** file to enable users to login using SAML SSO.

SAML Error Codes

IDP/SP/ Server	Status	Error on UI	Log File	Reason	Steps to Overcome Errors
IDP	Login Failure	Credentials not recognized	idpprocess.-log	LDAP details not properly configured in login.config file of IDP NOTE: Error Message is observed in logs only if format is incorrect. In case of incorrect details, no logs will be generated	Go to login.cofig in IDP and provide LDAP details as in below :- edu.vt.middleware. ldap.jaas.LdapLoginModule required ldapUrll=" ldap://10.100.1.37:389" baseDn- ="OU= Saml,DC=qaad,DC=com" bindDn="CN=kalpana one,OU- =Saaml, DC=QAAD,DC=com" ssl="false" tls="false" subtreeSearch= true" user- Filter="sAMAccountName= {0}" bindCredential=" welcome@123";
IDP	Login Failure	When valid credentials of user (who's present in AD)are given in Shibboleth SSO, user navigates from Shibboleth SSO to RV login page and 'Login Failed' is displayed NOTE: Vendor site works fine	catalina log	When attributes are not properly set in attributeresolver file. Ex: Only surname is given	Go to attribute-resolver.xml in IDP and make sure the following attributes are uncommented: xsi:type="ad:Simple" id="cn" sourceAttributeID="cn"> myLDAP" /> AttributeEncoder xsi:type="enc:SAML1String" namee=" urn:mace:dir:attributedef: cn" /> xsi:type="enc:SAML2String" name="urn:oid:2.5.4.3" friendlyName="cn" /> AttributeDefinition> xsi:type="ad:Simple" id="suurname" sourceAttributeID=" sn"> myLDAP" /> AttributeEncoder xsi:type="enc:SAML1String" namee=" urn:mace:dir:attributedef: sn" /> xsi:type="enc:SAML2String" name="urn:oid:2.5.4.4" friendlyName="sn" /> AttributeDefinition> xsi:type="ad:Simple" id="uid" sourceAttributeID=" sAMAccountName"> myLDAP" /> AttributeEncoder xsi:type="enc:SAML1String" namee=" urn:mace:dir:attribute-def:sAMAccou /> xsi:type="enc:SAML2String" name- ="urn:oid:0.9.2342.192003- 00.100.1.1" friendlyNamee=" sAMAccountName" /> AttributeDefinition> xsi:type="ad:Simple" id=- ="mail" sourceAttributeID=" mail"> myLDAP" /> AttributeEncoder xsi:type="enc:SAML1String" namee=" urn:mace:dir:attributedef: mail" /> xsi:type="enc:SAML2String" name- ="urn:oid:0.9.2342.192003- 00.100.1.3" friendlyName="mail" /> AttributeDefinition>

					xsi:type="ad:Simple" id=-="givenName" sourceAttributeID=" givenName"> myLDAP" /> AttributeEncoder xsi:type="enc:SAML1String" namee=" urn:mace:dir:attributedef: givenName" /> xsi:type="enc:SAML2String" name="urn:oid:2.5.4.42" friendlyName="givenName" /> AttributeDefinition>
IDP	Login Failure	Credentials not recognized	idpprocess.-log	Incorrect or Invalid Credentials provided in SSO page	Provide valid credentials(of users present in AD) in Shibboleth SSO page
IDP	Shibboleth error upon login	ERROR An error occurred while processing your request. Please contact your helpdesk or user ID office for assistance. This service requires cookies. Please ensure that they are enabled and try your going back to your desired resource and trying to login again. Use of your browser's back button may cause specific errors that can be resolved by going back to your desired resource and trying to login again. If you think you were sent here in error, please contact technical support	idpprocess.-log	When some changes are done in configuration, if TOMCAT APACHE and SHIBBOLETH services are not restarted in SP but TOMCAT is restarted in IDP	Tomcat apache and shibboleth service should be restarted on IDP as well as SP after making any changes
IDP	Page Loading Failed	HTTP Status 404 -	idpprocess.-log	Incorrect LDAP details are provided in attribute resolver file of IDP	Go to attribute-resolver.xml in IDP and make sure correct Ldap details are provided and are in the following format: DataConnector xsi:-type="dc:LDAPDirectory" id="myLDAP" ldapURLL=" ldap://10.100.1.37:389" baseDN-="oou= Saml,dc=qaad,dc=com" principal="qaad\kalpana1" principalCredential=" welcome@123"> [CDATA[(sAMAccountName=$ requestContext.principalName)]]>
IDP	Page Loading Failed	HTTP Status 404 -	idpprocess.-log	LDAP details not properly configured in attribute resolver file i.e. in this particular case xsi:-type="LDAPDirectory" is given instead of xsi:-type="dc:LDAPDirectory"	Go to attribute-resolver.xml in IDP and make sure correct Ldap details are provided and are in the following format: DataConnector xsi:-type="dc:LDAPDirectory" id="myLDAP" ldapURLL=" ldap://10.100.1.37:389" baseDN-="oou= Saml,dc=qaad,dc=com" principal="qaad\kalpana1" principalCredential=" welcome@123"> [CDATA[(sAMAccountName=$ requestContext.principalName)]]>
IDP	Page Loading Failed	HTTP Status 404 -	idpprocess.-log	LDAP details not properly configured in attribute resolver file i.e. in this particular case and are given instead of and	Go to attribute-resolver.xml in IDP and make sure correct Ldap details are provided and are in the following format: DataConnector xsi:-type="dc:LDAPDirectory" id="myLDAP" ldapURLL=" ldap://10.100.1.37:389"

					baseDN- ="oou= Saml,dc=qaad,dc=com" principal="qaad\kalpana1" principalCredential=" welcome@123"> [CDATA[(sAMAccountName=$ requestContext.principalName)]]>
IDP	Login Failure	When valid credentials of user (who's present in AD)are given in Shibboleth SSO, user navigates from Shibboleth SSO to RV login page and 'Login Failed' is displayed NOTE: Vendor site works fine	catalina log	LDAP details not properly configured in attribute resolver file i.e. Period is missing in this particular case sAMAccountName=$ requestContextprincipalName is given instead of sAMAccountName=$ requestContext.principalNam	Go to attribute-resolver.xml in IDP and make sure correct Ldap details are provided and are in the following format: DataConnector xsi:- type="dc:LDAPDirectory" id="myLDAP" ldapURLL=" ldap://10.100.1.37:389" baseDN- ="oou= Saml,dc=qaad,dc=com" principal="qaad\kalpana1" principalCredential=" welcome@123"> [CDATA[(sAMAccountName=$ requestContext.principalName)]]>
IDP	Login Failure	When valid credentials of user (who's present in AD)are given in Shibboleth SSO, user navigates from Shibboleth SSO to RV login page and 'Login Failed' is displayed NOTE: Vendor site works fine	catalina log	Attribute-filter.xml file doesn't contain required Attribute Filter Policy	In attribute-filter.xml of IDP make sure following tags are present in attributefilterpolicygroup tags : xsi:type="basic:ANY" /> givenName"> type="basic:ANY" /> uid"> xsi:type="basic:ANY" /> attributeID=" cn"> type="basic:ANY" /> surname"> xsi:type="basic:ANY" /> attributeID=" mail"> type="basic:ANY" />
IDP	Page Loading Failed	HTTP Status 404 -	idpprocess.- log	Attribute-filter.xml file contain incorrect details in required AttributeFilterPolicy tags i.e. 'basic:any' is given instead of 'basic:ANY'	In attribute-filter.xml of IDP make sure following tags are present in attributefilterpolicygroup tags : xsi:type="basic:ANY" /> givenName"> type="basic:ANY" /> uid"> xsi:type="basic:ANY" /> attributeID=" cn"> type="basic:ANY" /> surname"> xsi:type="basic:ANY" /> attributeID=" mail"> type="basic:ANY" />
IDP	Page Loading Failed	HTTP Status 404 -	idpprocess.- log	afp:AttributeFilterPolicy tags were not ended properly	In attribute-filter.xml of IDP make sure following tags are present in attributefilterpolicygroup tags : xsi:type="basic:ANY" /> givenName"> type="basic:ANY" /> uid"> xsi:type="basic:ANY" /> attributeID=" cn"> type="basic:ANY" /> surname"> xsi:type="basic:ANY" /> attributeID=" mail"> type="basic:ANY" />
IDP	Page Loading	opensaml:: FatalProfileException The system	shibd. log	Server details are incorrectly provided in	In relying-party.xml make sure the details(i.e. Url's) are

	Failed	encountered an error at Mon Oct 19 14:48:54 2015 To report this problem, please contact the site administrator at root@localhost. Please include the following message in any email: opensaml:: FatalProfileException at (https://idcws079. idcagl. com/Shibboleth.sso/SAML2/POST) Unable to establish security of incoming assertion.			correctly provided in
IDP	Page Loading Failed	HTTP Status 404 -	idpprocess.-log	Incorrect location for metadata(IDP/SP) was given in relying-party.xml	Correct location for metadata (IDP/SP) should be given in relying-party.xml under tags
SP	Login Failure	When valid credentials of user (who's present in AD)are given in Shibboleth SSO, user navigates from Shibboleth SSO to RV login page and 'Login Failed' is displayed NOTE: Vendor site works fine	catalina log	In attribute-map.xml, id in is incorrect or in different case or required attributes tags are missing	Make sure attribute tags are properly added in attribute map, attribute resolver and attribute filter
SP	Page Loading Failed	ERROR An error occurred while processing your request. Please contact your helpdesk or user ID office for assistance. This service requires cookies. Please ensure that they are enabled and try your going back to your desired resource and trying to login again. Use of your browser's back button may cause specific errors that can be resolved by going back to your desired resource and trying to login again. If you think you were sent here in error, please contact technical support Error Message: Message did not meet security requirements	idpprocess.-log	Entity ID was given wrong in shibboleth2.xml file	In shibboleth2.xml, under application tags make sure details are correctly given in the following format, id="default" policyId="default" entityID-="https:// idcws079.idcagl.com/shibboleth" REMOTE_USER="eppn persistent-id targeted-id" signing="true" encryption=" true" attributePrefix=" AJP_">
SP	Page Loading Failed	ERROR An error occurred while processing your request. Please contact your helpdesk or user ID office for assistance. This service requires cookies. Please ensure that they are enabled and try your going back to your desired resource and trying to login again. Use of your browser's back button may cause specific errors that can be resolved by going back to your desired resource and trying to login again. If you think you were sent here in error, please contact technical support Error Message: Message did not meet security requirements	idpprocess.-log	signing="true" is not present in Name> tag	In shibboleth2.xml, under application tags make sure details are correctly given in the following format, id="default" policyId="default" entityID-="https:// idcws079.idcagl.com/shibboleth" REMOTE_USER="eppn persistent-id targeted-id" signing="true" encryption=" true" attributePrefix=" AJP_">
SP	Login Failure	When valid credentials of user (who's present in AD)are given in Shibboleth SSO, user navigates from Shibboleth SSO to RV login page and 'Login Failed' is displayed NOTE: Vendor site works fine	catalina log	attributePrefix="AJP_" is not present in Name> tag	In shibboleth2.xml, under application tags make sure details are correctly given in the following format, id="default" policyId="default" entityID-="https:// idcws079.idcagl.com/shibboleth" REMOTE_USER="eppn persistent-id targeted-id" signing="true" encryption=" true" attributePrefix=" AJP_">
SP	Page Loading Failed	shibsp::ListenerException The system encountered an error at Tue Oct 20 16:33:53 2015 To report this problem, please contact		Commenting is not properly done in in shibboleth2.xml file	In Shibboleth2.xml, make sure the following tags are present inside tag:

		the site administrator at root@localhost. Please include the following message in any email: shibsp:: ListenerException at (https://idcws079. idcagl. com/spc/page.jsp) Cannot connect to shibd process, a site adminstrator should be notified.			type="Chaining" Location="/ Logout" relayStatee=" cookie"> type="SAML2" template=" localLogout.html"/> Local"/>
SP	Page Loading Failed	opensaml:: saml2md::MetadataException The system encountered an error at Tue Oct 20 17:00:26 2015 To report this problem, please contact the site administrator at root@localhost. Please include the following message in any email: opensaml:: saml2md::MetadataException at (https://idcws079. idcagl. com/spc/page.jsp) Unable to locate metadata for identity provider (https://idp. example.org/shibboleth)	shibd. log	and tags are missing in tag group of shibboleth2.xml file	In Shibboleth2.xml, make sure the following tags are present inside tag: Chaining" Location="/ Login" isDefault="true" id="FarmFed" relayStatee=" cookie" entityID- ="https://idcws080.idcagl.com/idp/sh type="SAML2" acsIndex="1" templatee=" bindingTemplate.html"/> Shib1" acsIndex="5"/> Chaining" Location="/ Logout" relayState="cookie"> SAML2" template=" localLogout.html"/> Local"/>
SP	Page Loading Failed	shibsp::ListenerException The system encountered an error at Tue Oct 20 17:21:38 2015 To report this problem, please contact the site administrator at root@localhost. Please include the following message in any email: shibsp:: ListenerException at (https://idcws079. idcagl. com/spc/page.jsp) Cannot connect to shibd process, a site adminstrator should be notified.		SAML2 Local Was not commented in shibboleth2. xml file	In shibboleth2.xml, make sure the following tags are commented: SAML2 Local
SP	Page Loading Failed	shibsp::ConfigurationException The system encountered an error at Tue Oct 20 17:30:45 2015 To report this problem, please contact the site administrator at root@localhost. Please include the following message in any email: shibsp:: ConfigurationException at (https://idcws079. idcagl. com/spc/page.jsp) No MetadataProvider available.	shibd. log	Metadata provider details provided in shibboleth2. xml file are not changed into required format	In shibboleth2.xml, make sure correct details of IDP are given in the following tags and tags are present in following format: type="Chaining"> XML" uri- ="https://idcws080.idcagl.com/idp/sh backingFilePath=" federationmetadata. xml" reloadInterval="7200">
Server	Page Loading Failed After Entering credentials in SSO page	HTTP Status 404 -	catalina log	SAML Bean not uncommented in applicationContext- security.xml	Go to Tomcat\ webapps\spc\WEBINF\ applicationContextsecurity. xml, and then uncomment SAML related bean and comment regular bean
Server	Page Loading Failed	Secure Connection Failed An error occurred during a connection to idcws079.idcagl. com. SSL received a record that exceeded the maximum permissible length. (Error code: ssl_error_rx_record_too_long) The page you are trying to view cannot be shown because the authenticity of the received data could not be verified. Please contact the website owners to inform them of this	catalina log	URL details are not properly given in httpd-ssl.conf and httpd-ssl-saml.conf files	Navigate to Server- \apache2\conf\extra and give correct URL's in httpd-ssl.- conf and httpd-ssl-saml.conf files

		problem.			

Introduction

Active Directory Federation Services (AD FS) is a Microsoft specific solution meant to accompany Active Directory. It is used to grant federation identity protocols (including SAML SSO services) across organizational boundaries. By using AD FS, organizations can authenticate users for RiskVision using their SAML identity providers.

This guide will explain how to configure AD FS to work with RiskVision's Shibboleth SAML service provider.

System Prerequisites

Before you can configure AD FS, you must ensure that your AD FS identity provider and Active Domain are located in the same location. In addition, Active Directory should be on the IP address 10.100.1.144-QATEAM, and AD FS should be on the IP address 10.100.1.72. Are these IP addresses? Should we be mentioning them here? The username and password for both is **administrator** and **Ag1|1ance** respectively. Is this right? It was in the original document, but I'm not sure about it.

Another set for AD and AD FS- I really didn't understand this in the original document so I pasted it just as it was. What is "Another set" referring to?

10.100.1.41- AD and AD FS are installed.

Machine hostname (QA41-2K12.qatest.com-10.100.1.41)

Qatest-Domain

adfsuser@qatest.com/welcome@123 Is this login information?

> Make sure AD FS 2.0 is already installed on 10.100.1.72 and has an associated self-signed certificate. Should we include steps on how one can get a self-signed certificate?

You must also ensure that you have obtained the Shibboleth metadata file, and that you have tested Shibboleth's installation before you proceed.

I did not include the following from the original document:

"Note- Shibboleth2.xml file, not included the following

AssertionConsumerService and Logout initiators *as these 2 are required only when Shibboleth is used as IPD as well.*

Log4j properties-log4j.logger.com.agiliance.web.security=DEBUG'

Because it doesn't seem to fit in with the rest of the document. Is this information important?

Create Federation Metadata File

Before you can configure AD FS, you must ensure that you have federation metadata. This will allow you to add a Relying Party Trust and will generally make using AD FS easier.

To create the federation metadata file:

1. Open AD FS.

2. Navigate to **AD FS > Services > End Points**and verify the path for **FederationMetadata/2007-06/FederationMetadata.xml** under the metadata section. How does the user verify the path? Should we include steps? Also, I'm not entirely sure I understand what this step is asking us to do. Are we creating a place to put the metadata file once we download it in step 3?

3. Download the federation metadata file and install it in the location specified in step 2. This link does not work. Is there a more recent link?

Overview

This section will instruct you in configuring AD FS 2.0 as your identity provider. By doing this, you will be able to grant the domain administrator federated access to RiskVision using Shibboleth as the service provider. The original text mentions that this uses the SAML 2.0 POST profile. Should that be included here?

Add a Relying Party Trust Using Metadata

Should there be screenshots for this article?

A relying party trust is a configuration that is used to identify the partner organization. In order for AD FS 2.0 to be used as the identity provider for Shibboleth, a relying party trust must be set up. While this can be done manually, it is easier to do so by importing the federation metadata file. Should we include steps for doing it manually?

To add a relying party trust using metadata:

1. Navigate to the console tree of AD FS 2.0.
2. Right-click on the **Relying Party Trusts** folder and click on **Add Relying Party Trust...** to start the Add Relying Party Trust Wizard.
3. Click **Start**.
4. Select **Import data about the relying party from a file** on the **Select Data Source** page.
5. In the **Federation metadata file location** field, type **navigate to the Metadata file provided by Agiliance**, and then click **Next**.
6. Click **OK** to acknowledge the warning.
7. On the **Specify Display Name** page, enter a descriptive name in the **Display name** field, and any notes in the **Notes** field.
8. Click **Next**.
9. On the **Multifactor Authentication Configuration** page, leave **default** selected.
10. On the **Choose Issuance Authorization Rules** page, leave the default **Permit all users to access the relying party** selected and click **Next**.
11. Click **Next**, and then **Close** to complete adding the relying party trust.

Edit Claim Rules for Relying Party Trust

Do we need screenshots for this article?

Claim rules describe how AD FS 2.0 determines what data should reside inside the federation security tokens that it generates. The claim rule in this section describes how data from Active Directory will be inserted in the security token that is created for Shibboleth.

Shibboleth expects inbound SAML attributes to use a different name format (E.g., urn:oasis:names:tc:SAML:2.0:attrname-format:uri) than the format AD FS 2.0 uses by default (e.g., urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified). For these reasons, we will use the AD FS 2.0 custom rule language to generate Shibboleth-compliant claims.

To configure claims for sending to a relying party trust:

1. Navigate to **Relying Party Trusts** in the AD FS 2.0 center pane.

2. Right-click **shib.adatum.com**, and click **Edit Claim Rules**.

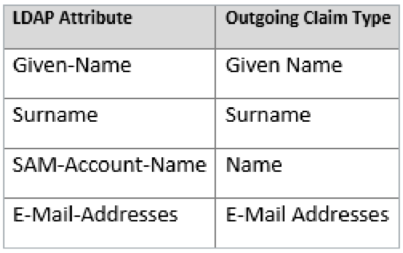
3. Click **Add Rule** on the **Issuance Transform Rules** tab.

4. On the **Select Rule Template** page, select **Send LDAP Attributes as Claims**, and then click **Next**.

5. On the **Configure Rule** page, type **Get Data** in the **Claim rule name** box.

6. Select **Active Directory** from the **Attribute Store** list.

7. Create the following mappings in the **Mapping of LDAP attributes** section.



LDAP Attribute	Outgoing Claim Type
Given-Name	Given Name
Surname	Surname
SAM-Account-Name	Name
E-Mail-Addresses	E-Mail Addresses

The required mappings for the Mapping of LDAP attributes section.

8. Click **Finish**.

There are more steps in the source document, but they are in red and it says to ignore if using ADFSv2.0 and above. Should we leave them out?

Configuring External User Authorization

RiskVision can be configured to use an external directory to authorize access. By default, even if the Authentication connector has been established and configured correctly, only RiskVision users can access the RiskVision console.

You can import users from the external directory into RiskVision, or you can configure RiskVision to automatically create users based on information in the external directory whenever a user first logs in to RiskVision. As usual, there is a trade-off between convenience and security. Requiring that users be manually imported is more secure than creating users automatically.

If you want to allow a user to configure the external authorization, you should assign the System User Manage permission. This permission is assigned to the default Administrator role in RiskVision.

To configure authorization policy:

1. In the Administration application, go to **Administration** > **SAML Configuration** and click the **Authentication** tab.
2. Click **Edit** at the upper-right corner.
3. To automatically create RiskVision users when externally-authorized users first log in, choose **No** for the **Allow only RiskVision users**question.

   To limit logins to pre-existing RiskVision users only, choose **Yes** for the **Allow only RiskVision users**question. Choose **Yes** if you do not plan to use an external directory, or if you plan to import users from the external directory manually.
4. Click **Save** to update the configuration, or **Cancel** to exit without saving changes.

Mapping External User Attributes

When a user is imported from an external directory, or when a RiskVision user is automatically created at first login using external authentication, attributes of the external user record are copied, and in some cases converted (mapped), into RiskVision user attributes.

Roles

Every RiskVision user needs a role in order to establish privileges in the system. The Roles page is shown only if you have the System User Manage permission. A user with no assigned role cannot log in, because they lack permission to view or edit anything. RiskVision includes a set of default roles, and organizations may define their own.
Anticipating that roles defined in the external directory may not be applicable to RiskVision, the system provides a way to specify a default role rather than using the role attribute from the external directory. Also, the user attribute which specifies the user's role in the organization is likely not named "role" in an LDAP directory. For example, it might be the "memberOf" attribute.

A role that has the System User Manage permission allows a user to view the Login Integration page to manage authentication parameters, external roles, and the external user attributes.

To specify role policy:

1. In the Administration application, go to **Administration** > **SAML Configuration** and click the **Authentication** tab.
2. Click **Edit** at the upper-right corner of the **Authentication** tab.
3. To use the external directory's role attribute when a user is imported or automatically created, choose **Yes** for the question Map external role.

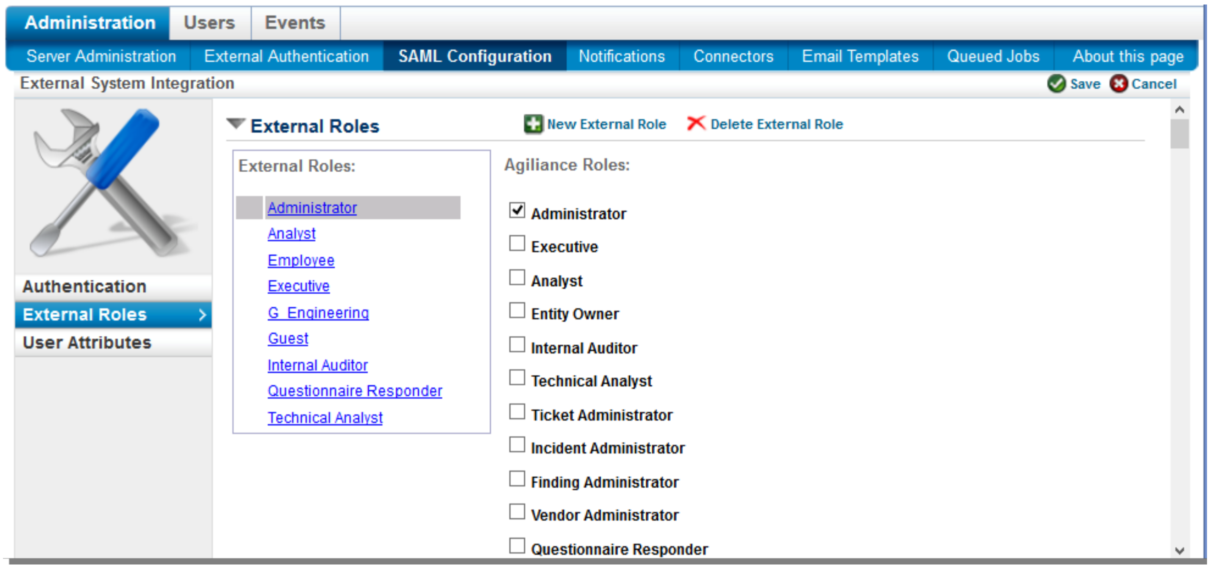
   To use a default RiskVision role rather than the role attribute in the external directory, choose **No**.
4. If you chose **Yes** for Map external role, specify the External role attribute name.
5. Specify a default RiskVision role, such as Questionnaire Responder, to use either all the time (if you chose No for Map external role) or when no role mapping is available.
6. Click **Save** to update the policy, or **Cancel** to exit without saving changes.

To convert external directory roles to RiskVision roles, you will need to specify a mapping, even if the role names are the same. External roles can be mapped to zero, one, or more RiskVision roles. For example, the LDAP-defined role "IT Analyst" might be mapped to RiskVision roles "Questionnaire Responder" and "Technical Analyst."

When no mapping exists--either because the external user does not have a role, or because the role is not found in the RiskVision mapping table--the new RiskVision user is created with the default role specified by role policy.

To manage role mapping:

1. In the Administration application, go to **Administration** > **SAML Configuration**, and click the **External Roles** tab.
2. Click **Edit** at the upper-right corner of the **External Roles** tab.



External Roles:

- Administrator
- Analyst
- Employee
- Executive
- G_Engineering
- Guest
- Internal Auditor
- Questionnaire Responder
- Technical Analyst

Agiliance Roles:

☑ Administrator
□ Executive
□ Analyst
□ Entity Owner
□ Internal Auditor
□ Technical Analyst
□ Ticket Administrator
□ Incident Administrator
□ Finding Administrator
□ Vendor Administrator
□ Questionnaire Responder

3. The External Roles list on the left must include every role that you expect to map. Click **New External Role** to add additional role names. To delete invalid external roles, click the role to select it, then click **Delete External Role**.
4. To assign an external role to a RiskVision role, click the external role to select it, then check the box next to the (RiskVision) role or roles that make sense.

   This role mapping only affects the initial, automatic mapping when a user is automatically created or imported from an external directory. Any user's roles can be adjusted at any time.

5. Click **Save** to update the role mappings, or **Cancel** to exit without saving changes.

Teams

RiskVision can automatically create teams based on external directory user group attributes. The assignment is performed user-by-user. If a new user (imported or automatically created) belongs to group X, RiskVision will create a team X, if it does not yet exist, and assign the new user to that team.

Be careful, because this feature can create many one-member teams if a wrong group attribute is chosen. For example, the OU attribute (organizational unit) is usually appropriate for team membership. Specifying the middle initial attribute would eventually create 26 meaningless teams in RiskVision**.**

To configure team creation:

1. In the Administration application, go to **Administration** > **SAML Configuration** and click the **Authentication** tab.
2. Click **Edit** at the upper-right corner of the **Authentication** tab.
3. To disable automatic team creation and assignment, choose **No** for the question **Map external group**. To enable automatic team creation and assignment, choose **Yes** for the question **Map external group**.
4. If you chose Yes, specify the name of the LDAP attribute in the **External group attribute name** field. The values in this field will be used to create RiskVision teams.
5. Click **Save** to update the team creation setting, or **Cancel** to exit without saving changes.

The team membership will be periodically synchronized, but LDAP groups that are deleted or renamed will not be updated in RiskVision.

Other LDAP User Attributes

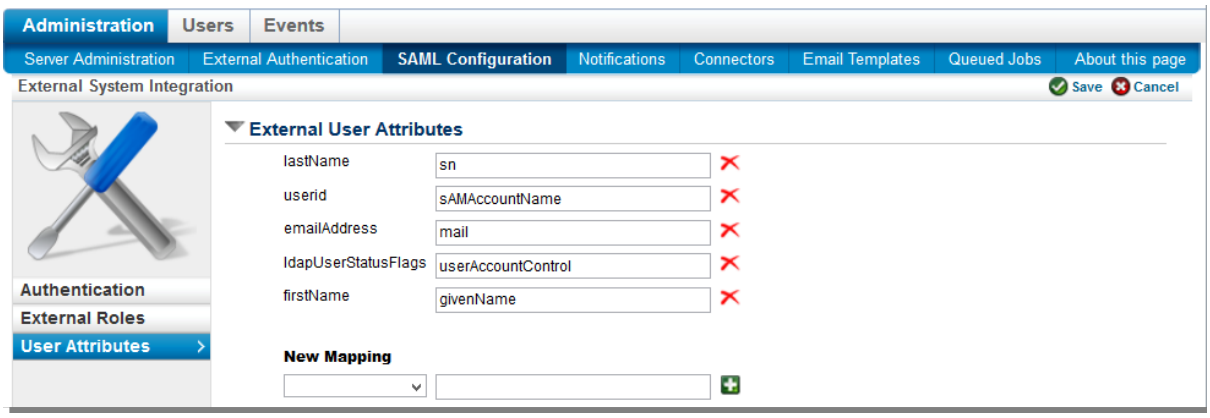
RiskVision can be configured to copy information from the LDAP user record when a new user is automatically created or manually imported. Arbitrary LDAP attributes can be mapped to the following RiskVision user properties:

RiskVision User Property	Description
address	Street address
city	City name
country	Country
dn	Distinguished name
emailAddress	User's e-mail address
fax	Fax number
firstName	User's given the name
lastName	User's surname
localeCountry	User's country (such as 'us')
localeLanguage	User's language (such as 'en')
middleInitial	User's middle name
mobile	Mobile phone number
state	State, province, or district
status	Synchronize user account status.
timezone	Time zone
userid	Login name (such as ' flastname') **Note**: It is important that the external field be globally unique. Duplicate userids will cause problems.
phone	Phone number
zip	Zipcode or postal code

Properties shown in **bold** are required.

To manage attribute mapping:

1. In the Administration application, go to **Administration** > **SAML Configuration**, and click the **User Attributes** tab.
2. Click **Edit** at the upper-right corner of the **User Attributes** tab.



External User Attributes

lastName	sn
userid	sAMAccountName
emailAddress	mail
ldapUserStatusFlags	userAccountControl
firstName	givenName

New Mapping

3. Enter the name of the LDAP attribute that corresponds with the RiskVision user property.

   To create a new mapping, select the RiskVision user property from the drop-down list, enter the name of the LDAP attribute, and click **+**. To delete a mapping, click **X** in red color at the right.

4. Click **Save** to update the role mappings, or **Cancel** to exit without saving changes.

Managing External User Accounts

During Active Directory maintenance, it is likely that your Windows administrator may change attributes of an user account or may simply disable an user account. When an account is disabled in the Active Directory, the RiskVision administrator has the responsibility to secure the RiskVision domain by ensuring that a user is not be able to access the RiskVision application when an inactive user is imported into RiskVision. Anticipating that these changes can cause security breach, the RiskVision administrator can make use of an external user attribute called "Status" to affect the changes made in Active Directory to reflect in RiskVision. By default, each LDAP Server has Status attribute set to “userAccountControl.”

If you have upgraded to RiskVision 6.5, you must manually add the Status attribute by setting the value to "userAccountControl" for the existing LDAP server. This attribute can be added on the External User Attributes tab of Administration > SAML Configuration page. To get updates from the Active Directory, run the LDAP User Synchronization system job manually.

It is necessary to familiarize yourself with the behavior of user accounts that are made active or inactive in the Active Directory before or after the user accounts are imported into RiskVision.

- A deactivated user in Active Directory when imported into RiskVision will be shown as deactivated.
- From Active Directory, importing an active user into RiskVision will be shown as active.
    - Afterwards, if the same user is deactivated in Active Directory and when the LDAP Users Synchronization system job is run, the user account status is changed to as inactive in RiskVision.
    - Afterwards, if the same user is deactivated in RiskVision and when the LDAP Users Synchronization system job is run, the user account status remains inactive in RiskVision.

Importing Users from an External Directory

RiskVision users can be created based on the available LDAP servers and the selected user records in an external directory.

The LDAP server must be configured correctly before importing users. The LDAP test facility may be helpful, as well. The Base DN configured for the LDAP server will be used as the root of the external directory tree.

To import users from an external directory:

1. In the Administration application, navigate to Users > Users.
2. In the More Actions drop-down menu, select Import from a Directory. The Import Users from a Directory dialog appears.
3. Select the desired domain from the domain drop-down list.
4. Enter a search base, such as OU=IT. This base will be joined with the base DN configured for the Authentication connector. Put another way, only tree nodes under the base DN node can be specified as the search base.
5. Enter a search filter to avoid being overwhelmed with names.

   Click **Search** to query the external directory and populate the Available Users list.

6. In the **Available Users** list, select users to be imported by clicking on the name. Use shift+click to select a range of users. Use ctrl+click to select another name without deselecting the first. Click the → arrow to move users from the **Available Users** list to the **Selected Users** list.

7. To import the selected users, click **OK,** or click **Cancel** to return to the table of users without importing

Authenticating Across Trusted Domains

RiskVision solution supports multiple LDAP servers that span over different domains. Typically, an enterprise will have all user accounts stored within one primary Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) top-level domain or forest. User accounts may be dispersed into many organizational units under the domain.

In a large enterprise, especially those with global reach, users interfacing with the RiskVision solution may be located in multiple AD domains with trusted relationships. In this instance, connecting to one AD domain may not be sufficient for importing all necessary users. The authentication connector can be referred to the enterprise's global catalog as a solution to this problem.

To facilitate this scenario, the RiskVision solution administrator must use these settings when configuring a connector:

Setting	Value
Protocol	LDAP
Hostname/IP	IP or hostname of a global catalog server
Port	3268 (standard)
Base DN	Top-level domain shared by all trusted domains
UID Key	sAMAccountName or mail
Default Domain	Any existing domain will suffice

RiskVision will require a valid ID with read access to the external directory to perform user search. The search base does not have to be completed here. When the RiskVision solution administrator begins to import users from AD or LDAP, the search base field can be populated with any additional domain or OU details.

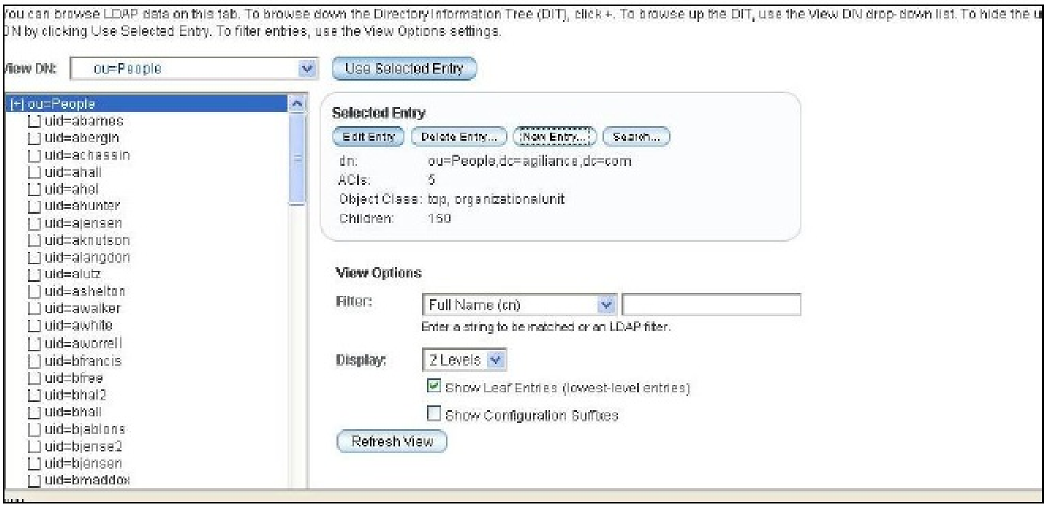
Allow users logging in for the first time using their email address by specifying the UID key field as 'mail' on the LDAP server Configuration tab and also, the 'userid' must be set to as 'mail in the User Attributes page of Attribute Mappings tab of LDAP server. Further, the following property must also be enabled: `com..authenticate.ldap.user.using.email=true`

RiskVision does not authenticate the users with same email IDs when UID key is set to as 'mail.'

Example Sun Directory Server Configuration

Your configuration will depend upon your organization's directory structure and policies. This example illustrates using the Authentication Connector to connect RiskVision with the Sun Directory Server.

If we assume that the organizational unit (ou) 'People' contains a user identifier (uid) for 'abarnes', the Sun Directory Server's LDAP data will look something like this:



ou can browse LDAP data on this tab. To browse down the Directory Information Tree (DIT), click +. To browse up the DIT, use the View DN drop-down list. To hide the u
N by clicking Use Selected Entry. To filter entries, use the View Options settings.

iew DN: ou=People

[+] ou=People
- □ uid=abarnes
- □ uid=abergin
- □ uid=achassin
- □ uid=ahall
- □ uid=ahel
- □ uid=ahunter
- □ uid=ajensen
- □ uid=aknutson
- □ uid=alangdon
- □ uid=alutz
- □ uid=ashelton
- □ uid=awalker
- □ uid=awhite
- □ uid=aworrell
- □ uid=bfrancis
- □ uid=bfree
- □ uid=bhal2
- □ uid=bhall
- □ uid=bjablons
- □ uid=bjense2
- □ uid=bjensen
- □ uid=bmaddox

Selected Entry

dn: ou=People,dc=agiliance,dc=com
ACIs: 5
Object Class: top, organizationalunit
Children: 150

View Options

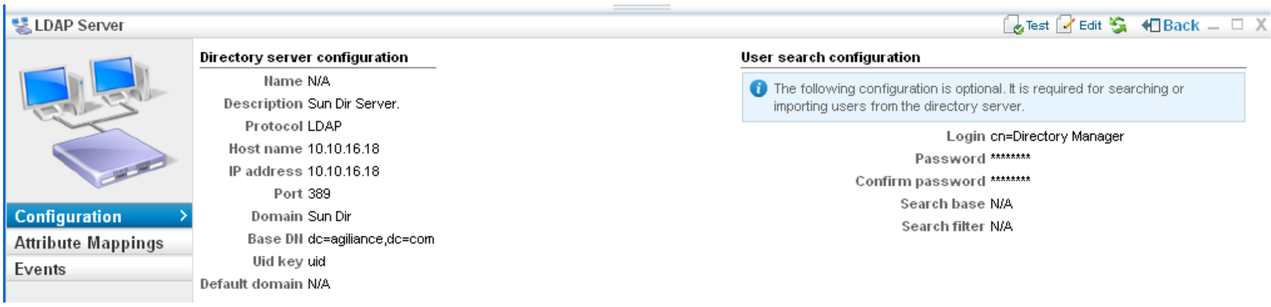
Filter: Full Name (cn)
Enter a string to be matched or an LDAP filter.

Display: 2 Levels

☑ Show Leaf Entries (lowest-level entries)

□ Show Configuration Suffixes

We configure the RiskVision Authentication connector to use 'uid' (as found on Sun Directory Server) as the Uid key. The base distinguished name (DN) establishes the root of the LDAP tree. In this case, it is `dc=,dc=com` .



Directory server configuration

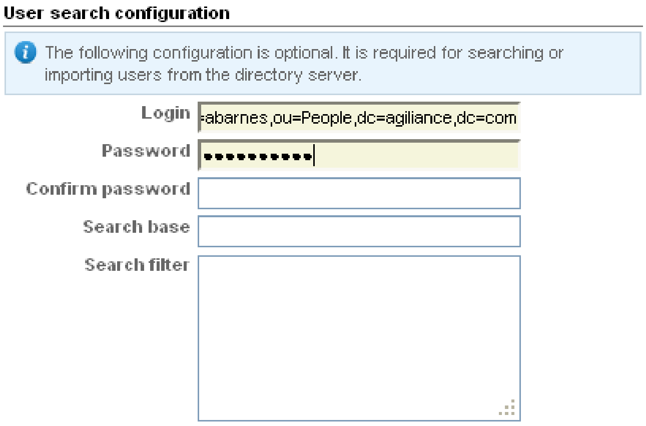
Name N/A
Description Sun Dir Server.
Protocol LDAP
Host name 10.10.16.18
IP address 10.10.16.18
Port 389
Domain Sun Dir
Base DN dc=agiliance,dc=com
Uid key uid
Default domain N/A

User search configuration

The following configuration is optional. It is required for searching or importing users from the directory server.

Login cn=Directory Manager
Password ********
Confirm password ********
Search base N/A
Search filter N/A

We test the connection by logging in as `uid=abarnes,ou=People,dc=,dc=com` , specifying user abarnes' password.



User search configuration

The following configuration is optional. It is required for searching or importing users from the directory server.

Login =abarnes,ou=People,dc=agiliance,dc=com
Password •••••••••••
Confirm password
Search base
Search filter

Resolve Login Issues

With RiskVision version 9.5 and above, beyond Apache Web Server version 2.4.39, some users have been unable to log in using SAML and receive the following error message: **HTTP Status 403 – Forbidden**. In order to resolve this issue, users must follow the steps below:

To fix SAML login issues:

1. Navigate to the **\apache2\conf\extra** folder and open the **httpd-ssl-saml.conf** file.
2. Comment the following lines:
    - `ProxyPass /spc ajp://localhost:8009/spc`
    - `ProxyPassReverse /spc ajp://localhost:8009/spc`
3. Save your changes.
4. Restart the RiskVision Apache service and try again.

If the above steps do not work, contact resolver support.

About Connectors

Connectors are used to discover and collect information about various entities on the network, distribute and enforce controls, and return results for managed entities, among other things. Connectors help RiskVision fit into\ an organization's unique context.

Once installed, the application queries the connectors, sends updated controls, and returns results or status of control checks for managed computers or other resources.

Displaying Connectors

Refer to the connector documentation for connector specific information. This section provides an overview of the RiskVision solution connector page.

If you want other users to view and modify the connector configuration, you must assign the Connector Manage permission. This permission is assigned to the default Administrator role in RiskVision. When you have the sufficient permissions, go to the Administration application and click Connectors on the Administration menu to view the currently configured RiskVision connectors, The top-right pane lists all installed RiskVision connectors. Selecting a connector displays additional details in the lower bottom pane.

The e-mail connector, authentication connector, and server connector display only for users with the system administrator role (sysadmin or administrator, or, in multi-tenant deployments, the sysadmin user in the system tenant space).

About the Connector Tables

The table contains the following information:

- For status, the plug indicates whether or not the server received a heartbeat within the specified interval of time.
- For health, a green checkmark indicates authentication was successful and Red circle the connector failed authentication or another error was detected.
- Click a heading to sort the table.

To view the currently configured RiskVision connectors, go to Administration > Connectors. The top-right panelists all installed RiskVision Connectors. Selecting a connector displays additional details in the lower bottom pane. The bottom detail pane provides three different tab views to display general information, configuration, and commands available for specific connectors.

About Connector Details

If the Authentication status field on the Information detail menu tab displays a status of “Not authenticated,” click the corresponding **Authenticate** button to authenticate the connector with the Server. From the Configuration detail menu, set the username and password used to authenticate the connector and to access other computers the connector manages or collects information from. You can store different individual usernames and passwords at the entity detail level, to set the username and password for administrative access to other computers managed by the RiskVision server.

The bottom detail pane provides the following information:

Option	Description
Information	Describes general information about the connector including the host IP address and computer or machine name, and status information such as the connector’s last “heartbeat” communication with the Server.
Configuration	Varies by the type of connector. Displays and provides capabilities, such as the ability to specify authentication credentials and update heartbeat frequency, and set the interval of communication with the server.
Commands	Execute commands available for a specific connector.

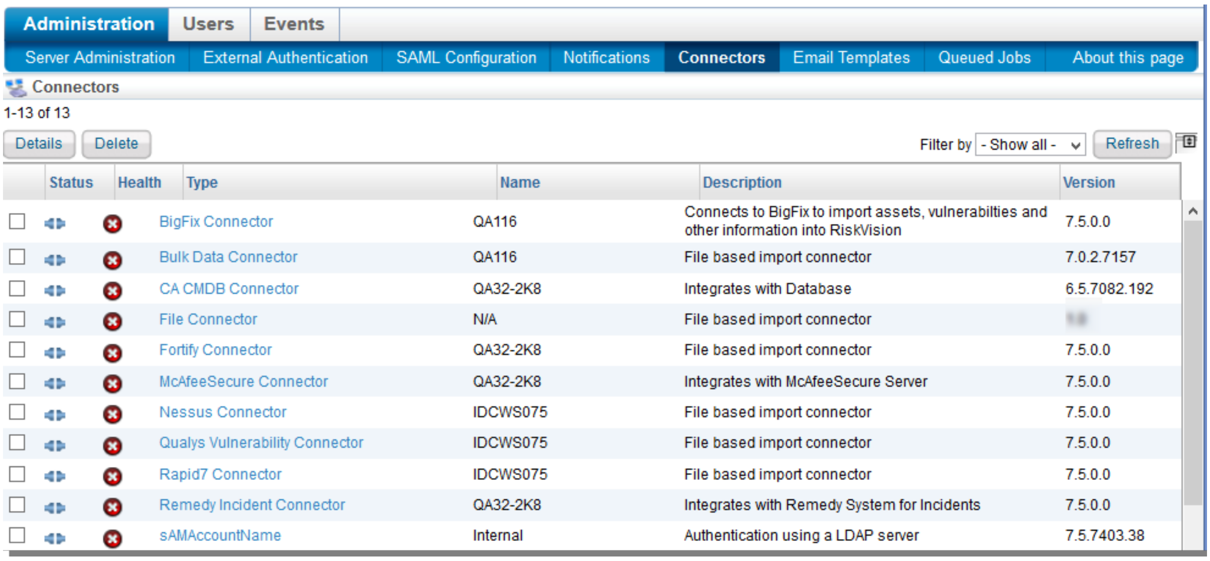
Modifying the Connector Configuration

Users with sufficient privileges can modify a connector configuration.

To change the connector configuration:

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

   The **Connectors** page is displayed.

	Status	Health	Type	Name	Description	Version
□	◂▸	⊗	BigFix Connector	QA116	Connects to BigFix to import assets, vulnerabilties and other information into RiskVision	7.5.0.0
□	◂▸	⊗	Bulk Data Connector	QA116	File based import connector	7.0.2.7157
□	◂▸	⊗	CA CMDB Connector	QA32-2K8	Integrates with Database	6.5.7082.192
□	◂▸	⊗	File Connector	N/A	File based import connector	[redacted]
□	◂▸	⊗	Fortify Connector	QA32-2K8	File based import connector	7.5.0.0
□	◂▸	⊗	McAfeeSecure Connector	QA32-2K8	Integrates with McAfeeSecure Server	7.5.0.0
□	◂▸	⊗	Nessus Connector	IDCWS075	File based import connector	7.5.0.0
□	◂▸	⊗	Qualys Vulnerability Connector	IDCWS075	File based import connector	7.5.0.0
□	◂▸	⊗	Rapid7 Connector	IDCWS075	File based import connector	7.5.0.0
□	◂▸	⊗	Remedy Incident Connector	QA32-2K8	Integrates with Remedy System for Incidents	7.5.0.0
□	◂▸	⊗	sAMAccountName	Internal	Authentication using a LDAP server	7.5.7403.38

2. Select a connector.

   The Connector details pane displays below the table.

3. Click the **Configuration** tab.

4. Click **Edit**.

5. Change the settings as appropriate.

6. Click **Save**.

For more information about configuring and troubleshooting a specific connector type, please contact Customer Support to obtain the connector guide.

Connector Healthcheck Alert

Connector Health-check alert allows users to automate alerts if the connectors are not running as expected, or if they are flagging errors that need attention.

Configuration required to send an email notification are:

1. Configure the email connector
2. Install a connector and set the property `Alert.sendError = true` in the `connector.file.properties` file
3. Set the property `connector.alert.email=true` in the `%AGILIANCE_HOME%\Server\config` folder in the agiliance.properties file

Threat Intelligence Connector

RiskVision integrates with threat intelligence services through connectors. Customers with a valid license can access the CrowdStrike Falcon Intelligence Connector, the FireEye ISight Connector, and the Exploit Database Connector data in the Connectors page.

To set up and run the CrowdStrike Falcon Intelligence connector:

1. Navigate to the **\config** folder and add a valid license with the `connector.remote.crowdstrike.falconintelligence` connector set to true.

2. Download the SQUID Proxy.

3. Install the **SQUID Proxy** server onto the machine that will be using RiskVision.

4. To enable the proxy:

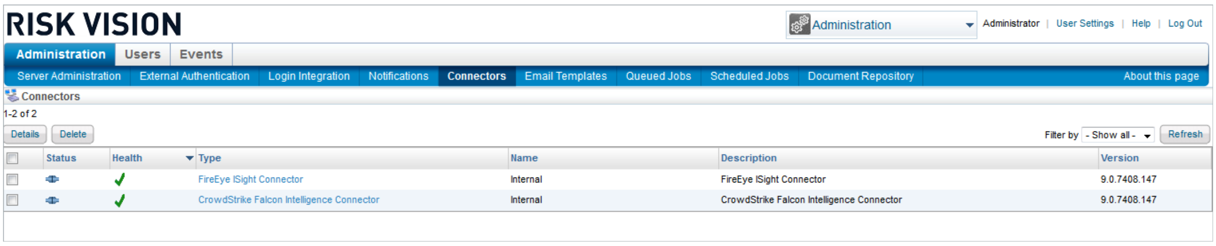
    a. Navigate to **\config\agiliance.properties**.

    b. Make the following changes to the file:

    ```
    Proxy.useProxyServer = true
    Proxy.serverHost = Server Hostname
    Proxy.serverPort = 3128
    Proxy.httpType = http
    ```

    c. Restart the RiskVision Tomcat service to apply these change.

5. In the **RiskVision Administration** application, click on **Administration**, then **Connectors**.

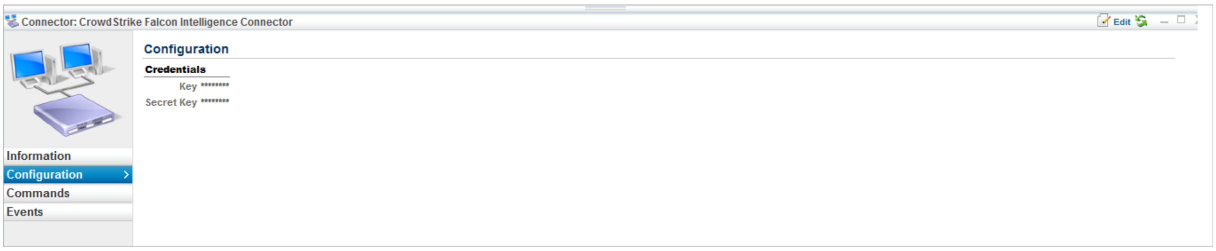


☐	Status	Health	Type	Name	Description	Version
☐		✓	FireEye ISight Connector	Internal	FireEye ISight Connector	9.0.7408.147
☐		✓	CrowdStrike Falcon Intelligence Connector	Internal	CrowdStrike Falcon Intelligence Connector	9.0.7408.147

The Connectors page.

6. Click on **CrowdStrike Falcon Intelligence Connector** and then click **Details**.

7. Click on the **Configuration** tab and then **Edit**.



Configuration

Credentials

Key ********

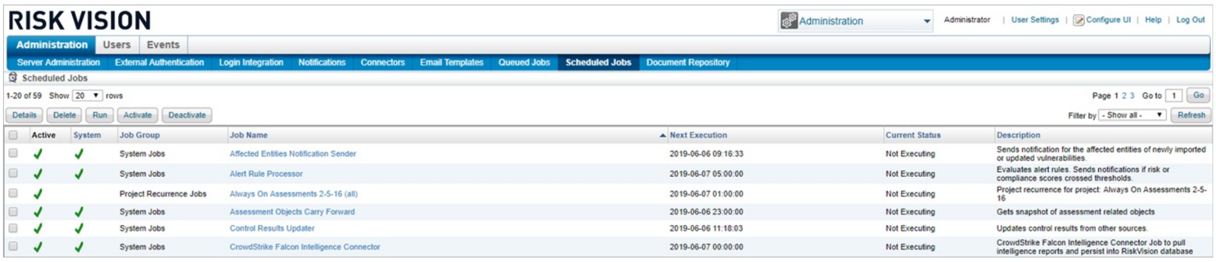
Secret Key ********

The Configuration tab for the CrowdStrike Falcon Intelligence Connector.

    a. Enter the **Key** and **Secret Key**.

8. Click **Save**.

9. Click on the **Scheduled Jobs** tab.



□	Active	System	Job Group	Job Name	Next Execution	Current Status	Description
□	✓	✓	System Jobs	Affected Entities Notification Sender	2019-06-06 09:16:33	Not Executing	Sends notification for the affected entities of newly imported or updated vulnerabilities.
□	✓	✓	System Jobs	Alert Rule Processor	2019-06-07 05:00:00	Not Executing	Evaluates alert rules. Sends notifications if risk or compliance scores crossed thresholds.
□	✓		Project Recurrence Jobs	Always On Assessments 2-5-16 (all)	2019-06-07 01:00:00	Not Executing	Project recurrence for project: Always On Assessments 2-5-16
□	✓	✓	System Jobs	Assessment Objects Carry Forward	2019-06-06 23:00:00	Not Executing	Gets snapshot of assessment related objects
□	✓	✓	System Jobs	Control Results Updater	2019-06-06 11:18:03	Not Executing	Updates control results from other sources.
□	✓	✓	System Jobs	CrowdStrike Falcon Intelligence Connector	2019-06-07 00:00:00	Not Executing	CrowdStrike Falcon Intelligence Connector Job to pull intelligence reports and persist into RiskVision database

The Scheduled Jobs page.

10. Select the **CrowdStrike Falcon Intelligence Connector** scheduled job and click **Activate**, then **Run**. This will import threats through the proxy into RiskVision.

> If the proxy has been turned off or configured improperly, you will see a message that reads: "Connection refused for proxy server: java.net.ConnectException: Connection refused: connect".

11. After successfully importing threats, click **Deactivate**.

To perform a threats import through the FireEye ISight connector:

1. Navigate to the **\config** folder and add a valid license with the `connector.remote.fireeye.isight` connector set to true.

2. Download the SQUID Proxy.

3. Install the **SQUID Proxy** server onto the machine that will be using RiskVision.

4. To enable the proxy:

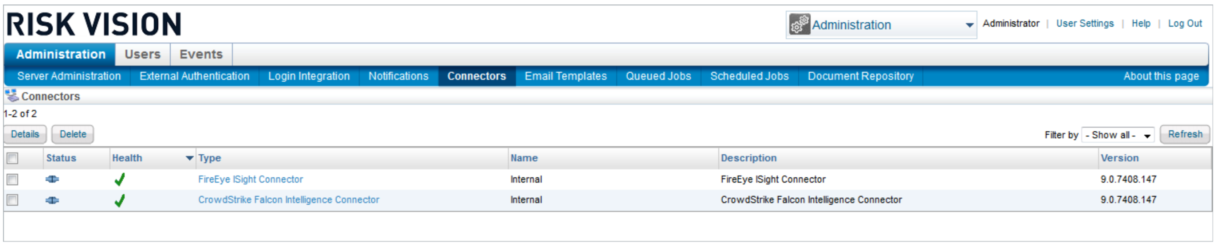
    a. Navigate to **\config\agiliance.properties**.

    b. Make the following changes to the file:

    ```
    Proxy.useProxyServer = true
    Proxy.serverHost = Server Hostname
    Proxy.serverPort = 3128
    Proxy.httpType = http
    ```

    c. Restart the RiskVision Tomcat service to apply these change.

5. In the **RiskVision Administration** application, click on **Administration**, then **Connectors**.

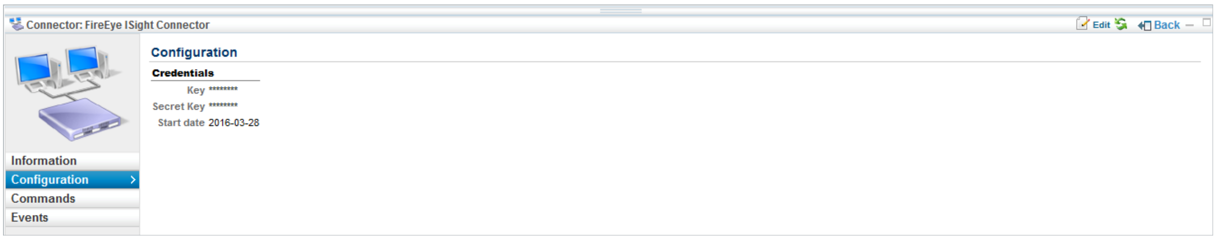


□	Status	Health	Type	Name	Description	Version
□		✓	FireEye ISight Connector	Internal	FireEye ISight Connector	9.0.7408.147
□		✓	CrowdStrike Falcon Intelligence Connector	Internal	CrowdStrike Falcon Intelligence Connector	9.0.7408.147

The Connectors page.

6. Click on **FireEye ISight Connector**.

7. Click on the **Configuration** tab and then **Edit**.



Configuration

Credentials

Key *********

Secret Key *********

Start date 2016-03-28

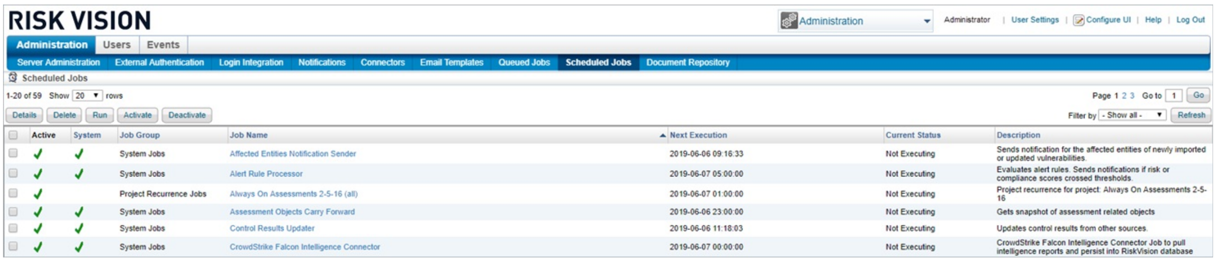
The Configuration tab for the FireEye ISight Connector.

   a. Enter the **Key** and **Secret Key**.

   b. Specify the start date from which the threat data should be downloaded.

8. Click **Save**.

9. Click on the **Scheduled Jobs** tab.



1-20 of 59 Show 20 rows

Page 1 2 3 Go to 1

Filter by - Show all -

□	Active	System	Job Group	Job Name	Next Execution	Current Status	Description
□	✓	✓	System Jobs	Affected Entities Notification Sender	2019-06-06 09:16:33	Not Executing	Sends notification for the affected entities of newly imported or updated vulnerabilities.
□	✓	✓	System Jobs	Alert Rule Processor	2019-06-07 05:00:00	Not Executing	Evaluates alert rules. Sends notifications if risk or compliance scores crossed thresholds.
□	✓		Project Recurrence Jobs	Always On Assessments 2-5-16 (all)	2019-06-07 01:00:00	Not Executing	Project recurrence for project: Always On Assessments 2-5-16
□	✓	✓	System Jobs	Assessment Objects Carry Forward	2019-06-06 23:00:00	Not Executing	Gets snapshot of assessment related objects
□	✓	✓	System Jobs	Control Results Updater	2019-06-06 11:18:03	Not Executing	Updates control results from other sources.
□	✓	✓	System Jobs	CrowdStrike Falcon Intelligence Connector	2019-06-07 00:00:00	Not Executing	CrowdStrike Falcon Intelligence Connector Job to pull intelligence reports and persist into RiskVision database

The Scheduled Jobs page.

10. Select the **FireEye ISight Connector** scheduled job and click **Activate**, then **Run**. This will import threats through the proxy into RiskVision.

> ⚠ If the proxy has been turned off or configured improperly, you will see a message that reads: "Connection refused for proxy server: java.net.ConnectException: Connection refused: connect".

11. After successfully importing threats, click **Deactivate**.

To import exploits through the Exploit Database Connector:

1. Install and run the **Exploit DB Connector**.

2. Authenticate the Exploit Database in RiskVision.

3. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy file.

4. To enable the proxy:

   a. Navigate to the **\cfg** directory.

   b. Open **connector.file.properties**.

   c. Make the following changes to the file:

```
Proxy.useProxyServer = true
Proxy.serverHost = Server Hostname
Proxy.serverPort = 3128
Proxy.httpType = http
```

   d. Save the file.

5. To retrieve the Exploit Database connector file from Rackspace:

   a. Run the following expressions for five minutes:

```
exploit.cron.expression= 0 0/5 * 1/1 * ?
exploit.encryption.secret.key=Enter Secret Key
riskvision.server.url=Url should be entered correctly
```

> You can retrieve the cron.expression from the Cron Maker website.

b. Save the file.

6. Go to the location where Java is installed on your machine and place the Advanced Encryption Standard supported **local_policy.jar** and **US_export_policy.jar** files in the **$JDK_FOLDER/jre/lib/security** directory.

Troubleshooting Connectors

Each connector has a document (available from Resolver Support) that describes the specifics of the software to which it connects and how to install and configure the connector. In some cases, the connector documentation has troubleshooting tips that will be more relevant than the general advice found in this section.

Does the connector appear in the RiskVision Administrator application?

The connector must be a configured hostname host name (or IP address) of the RiskVision server, and the server must be accessible on the port specified. In addition, the connector must be configured with proper RiskVision credentials. To test credentials, try logging in to the console manually.

Has the connector been authenticated?

Each connector must be manually authenticated through the RiskVision console by a user with sufficient privileges. The connector's health shows green in the connector table when the connector has been authenticated and its "heartbeat" has been received.

Is the third-party software running?

Connectors connect to third-party software. Is this software the correct version, as described in the connector documentation? Is that system up and running, and is the server accessible to the connector host? The connector must be configured with the correct hostname and login credentials for the third-party software.

Did you allow enough time?

Third-party software sometimes takes longer than expected to send data. In addition, the connector sometimes throttles a high-bandwidth data stream and buffers a sporadic one. The connector configuration may affect the timing of the data flow, for example, by specifying a polling frequency.

Have you checked the connector logs?

The connector log will describe connection issues with RiskVision or third-party software, for example.

Did the RiskVision server report any errors with the connector?

The RiskVision log and notifications may help pinpoint a source of connector problems.

Did you upgrade to the current connector without uninstalling the previous version?

Connector installation requires that any previous version is uninstalled first.

Does the problem still occur?

Contact Resolver Support.

Configuring JSON Support for the NVD Connector

The National Vulnerability Database (NVD) would previously publish their list of vulnerabilities, known as Common Vulnerabilities and Exposures (CVE), in XML format through their CVE XML feed. Recently though, the NVD introduced a JSON feed and announced their XML support will be end-of-lifed on October 9, 2019. As a result, customers must upgrade their NVD Connector to be compatible with the NVD JSON feed.

Starting September 9, 2019, the JSON 1.1 feed will be available for the NVD connector. Customers must download this feed in order to continue receiving vulnerability information from the JSON feed.

In addition to the JSON feed, customers who upgrade their NVD connector will gain access to the CPE Match Feed. This feed explicitly states which Common Platform Enumerators (CPE) are affected by which CVEs instead of just stating ranges of CPEs, as is often done in the JSON CVE file. This allows for increased accuracy when performing CPE matching.

If customers are upgrading to RiskVision version 9.3 or above, they must upgrade the NVD connector using the steps below. Customers who do not upgrade their RiskVision server must apply the NVD patch which can be received from the Resolver Support Team along with installation instructions. The NVD patch will make the user's NVD connector compatible with the JSON feed without needing to upgrade the RiskVision server.

To upgrade the NVD connector:

> Unless otherwise stated in one of the below steps, it is good practice to delete the previous connector files.

1. Navigate to **C:\Program Files (x86)\Agiliance\NVD Connector\cfg**.
2. Keep a backup of this folder.
3. Reinstall the NVD connector.
4. Open the **connector.file.properties** file and make sure it matches the file you backed up in step 2.
5. Set the following properties:
    - `SupportedFormatExtensions = .xml,.json`
    - `cve.fromYear = [insert year connector should start importing datafeeds (e.g. 2002)]` This defaults to the year 2002, but it is recommended that you set it to the year before the current year.
    - `cve.toYear = [insert year connector should stop importing datafeeds (e.g. 2019)]` This defaults to the current year.
    - `NvdCveUrl=https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-[YEAR].json.zip` (only if `requestAutoFeed` is set to `true`)
        - The `[YEAR]` property will be automatically filled in based on the range of the `cve.fromYear` and `cve.toYear` properties.
        - If the `requestAutoFeed` property is set to `true`, the connector will contact the NVD website specified in the `NvdCveUrl` property and download the JSON files. If the property is set to `false`, any valid JSON file downloaded by the customer can be placed and immediately processed in the following location: **C:\Program Files (x86)\Agiliance\NVD Connector\data\connector.remote.cve\new**. This is useful for customers who wish to download their own CVE files.
    - `NvdCpeMatchFeedURL=https://nvd.nist.gov/feeds/json/cpematch/1.0/nvdcpematch-1.0.json.zip`

    > An NVD connector that has been configured for JSON will not run without the Match Feed provided by the above property.

6. Open the **File_wrapper.conf** file.
7. Set the connector's memory as:
    - `wrapper.java.maxmemory=4096MB`

> Users may need to increase their RAM by at least 500 MB in order to support this upgrade.

8. Restart the NVD connector.
9. To forcefully update the pre-existing vulnerabilities' CVSS scores when upgrading to RiskVision version 9.3 or above:

   > This step can be skipped for any version of RiskVision below 9.3 as those versions do not support CVSS v3.0 scores.

   a. Disable the following RiskVision jobs before importing the NVD data:

      - Vulnerabilities Affected Entities Incremental Updates
      - Vulnerability Risk Score Calculator
      - Vulnerability Risk Score Initiator
      - Vulnerability Summary Update
      - Search Indexes Builder

   b. Navigate to **%AGILIANCE_HOME%/config**.

   c. Open the **agiliance.properties** file.

   d. Set the following property to `true`:

      - `com.agiliance.agent.nvd.cve.forceUpdate`

        > If this property is not set to true, the NVD will only be updated if there is a difference between the vulnerability's published date in the JSON file and the vulnerability's published date in the database. Setting the property to true will bring in CVSS v3.0 data for unchanged vulnerabilities. Once this step has been completed, Resolver recommends changing the value back to **False**.

        > CVSS 3.0 scores **will not** be populated for **CVEs prior to 12/20/2015**. Some legacy vulnerabilities, however may get updated with CVSS 3.0 scores under special circumstances. Further information on CVSS can be found here.

   e. Set the above property to false and resume the activities from step 9a once the CVSS values have been updated.

10. To re-authenticate the NVD Connector.

    a. Open the Administration application in RiskVision.

    b. Navigate to **Administration > Connectors**.

    c. Click on the NVD Connector in the connectors list.

    d. Under the Status section, click **Deny Access**.

    e. Click **Authenticate**. NVD will now exclusively download JSON files rather than XML files.

11. Once the import is done, re-enable the jobs listed in step 9a.

NVD Data Map Overview

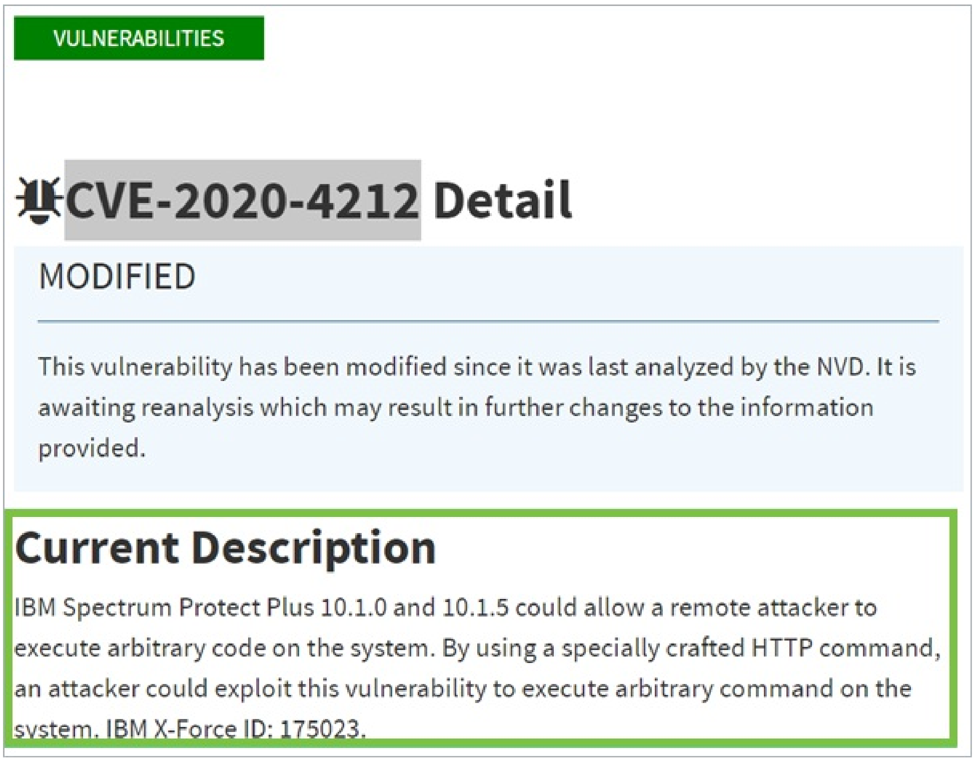
When importing a .json file into RiskVision, the NVD Connector will populate different fields depending on which data feed the file comes from.

When Importing CVE Files

RiskVision will capture the following from the NVD website:

Description

The **Current Description** and **Analysis Description** will be uploaded to the **Description** field of a vulnerability's **General** tab.



VULNERABILITIES

CVE-2020-4212 Detail

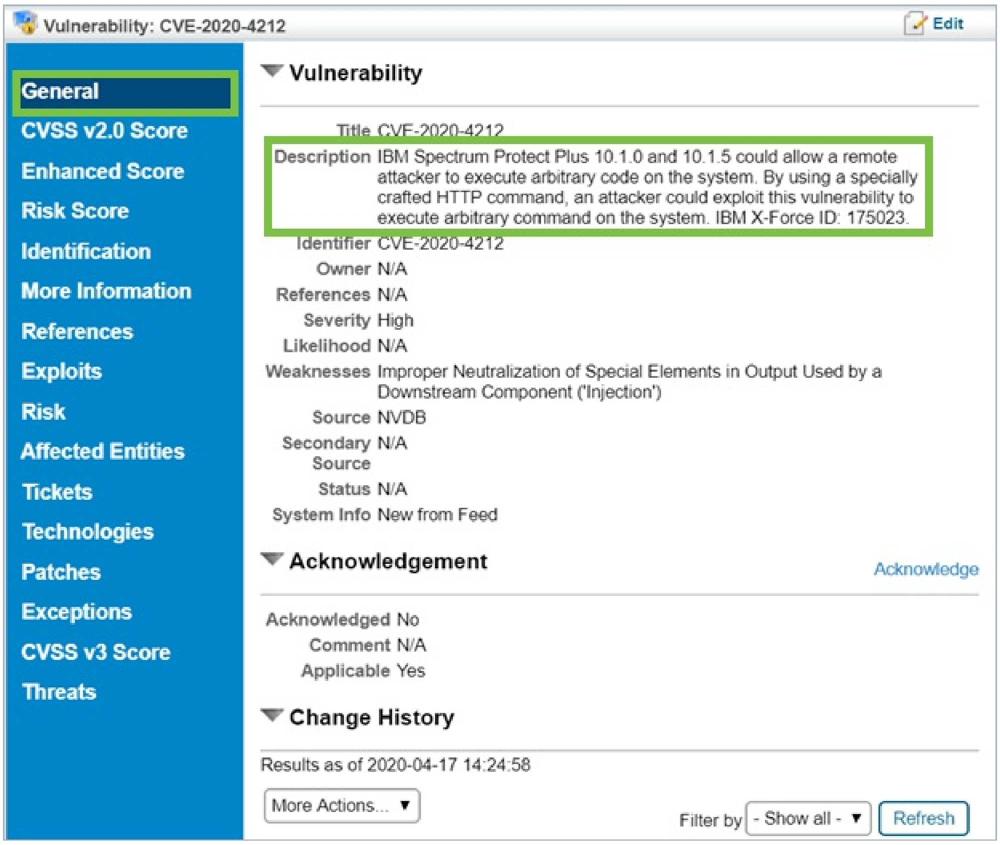
MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.

The Current Description of a CVE file.



Vulnerability

Title CVE-2020-4212
Description IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.
Identifier CVE-2020-4212
Owner N/A
References N/A
Severity High
Likelihood N/A
Weaknesses Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
Source NVDB
Secondary Source N/A
Status N/A
System Info New from Feed

Acknowledgement

Acknowledged No
Comment N/A
Applicable Yes

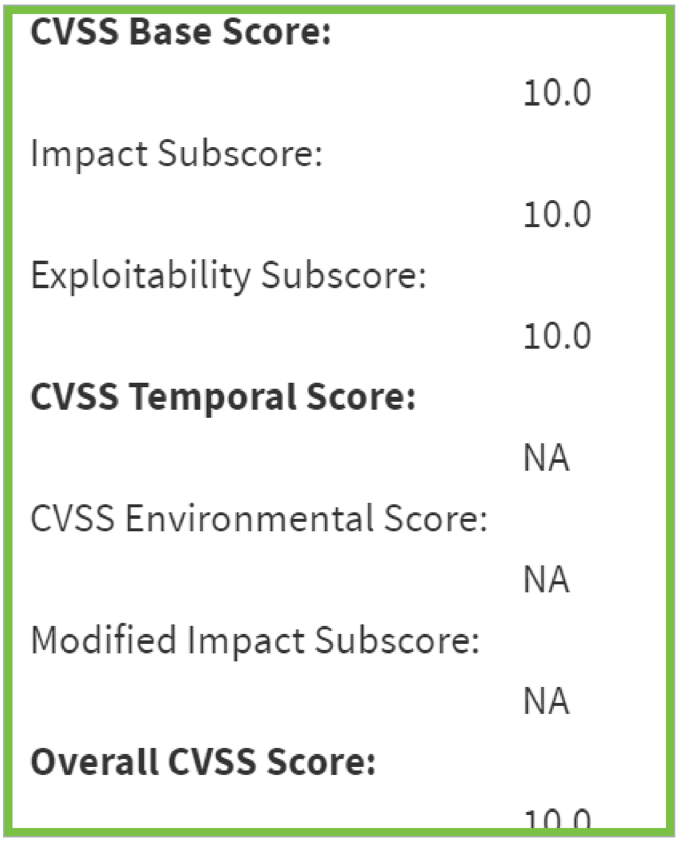
Change History

Results as of 2020-04-17 14:24:58

The CVE's description captured by the Description field in RiskVision.

Severity

The vulnerability's **CVSS v2.0 Score** tab will capture all scores from the file's**CVSS Score** section.



CVSS Base Score:

10.0

Impact Subscore:

10.0

Exploitability Subscore:

10.0

CVSS Temporal Score:

NA

CVSS Environmental Score:

NA

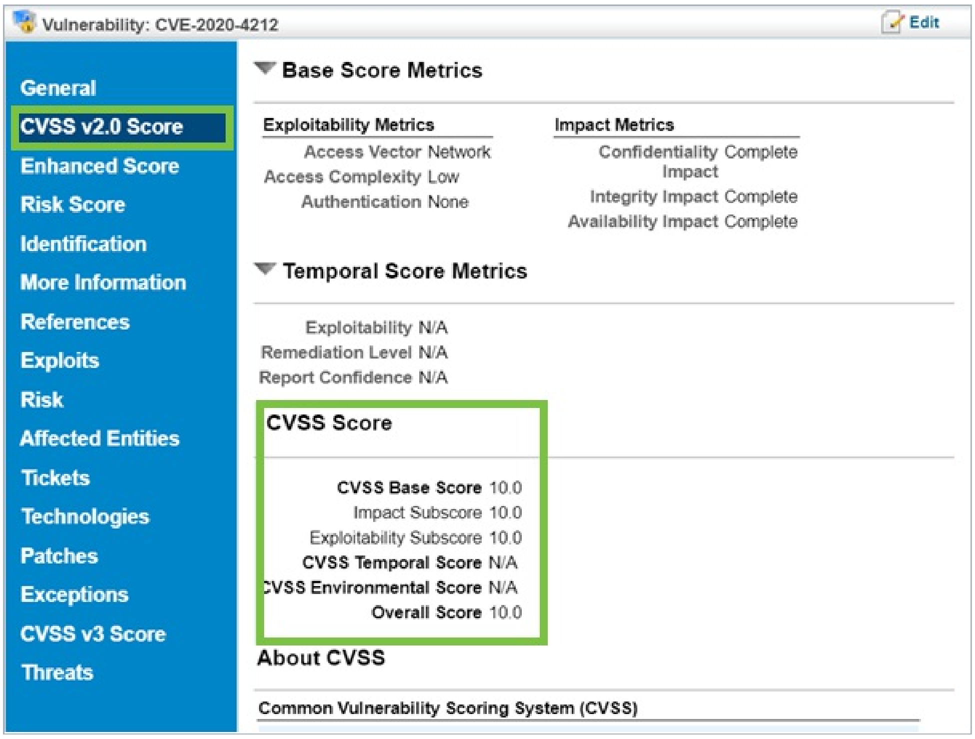
Modified Impact Subscore:

NA

Overall CVSS Score:

10.0

The CVSS Score section of a CVE file.



Base Score Metrics

Exploitability Metrics

Access Vector Network
Access Complexity Low
Authentication None

Impact Metrics

Confidentiality Impact Complete
Integrity Impact Complete
Availability Impact Complete

Temporal Score Metrics

Exploitability N/A
Remediation Level N/A
Report Confidence N/A

CVSS Score

CVSS Base Score 10.0
Impact Subscore 10.0
Exploitability Subscore 10.0
CVSS Temporal Score N/A
CVSS Environmental Score N/A
Overall Score 10.0

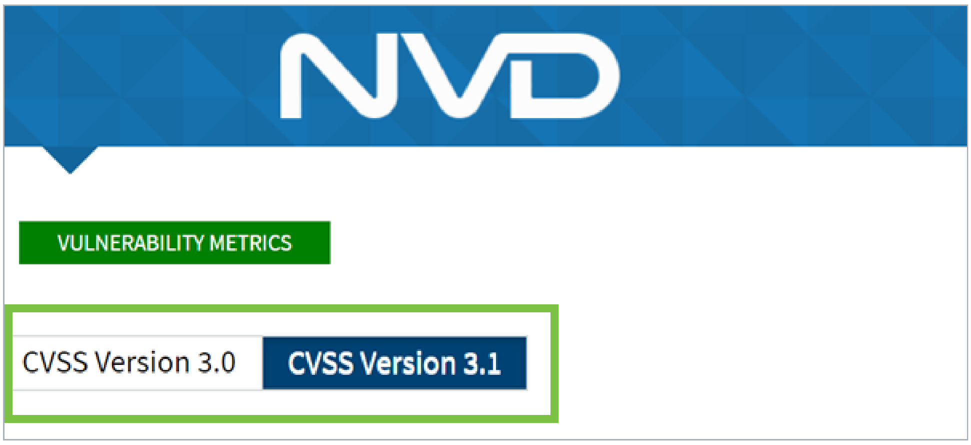
About CVSS

Common Vulnerability Scoring System (CVSS)

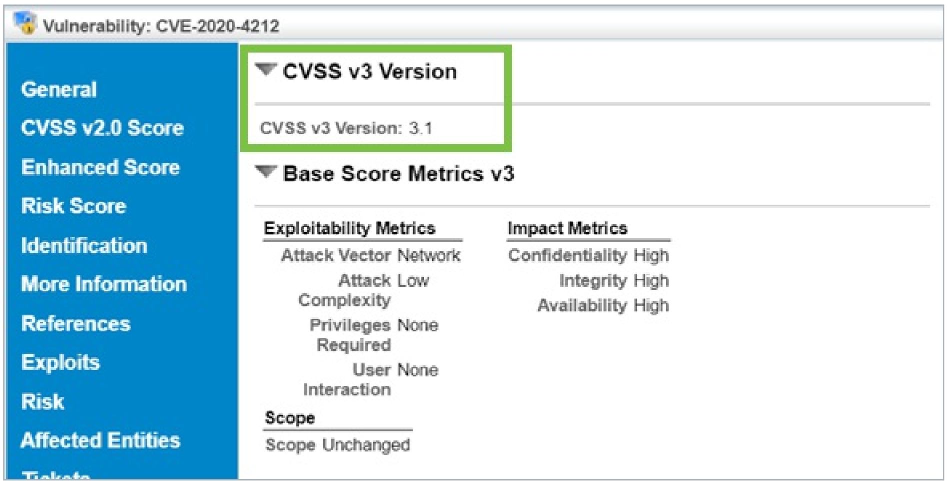
The CVE's severity scores captured by the CVSS Score field in RiskVision.

The **CVSS v3 Score** tab will capture all fields and values in the following sections of the .json file:

- **CVSS v3 Version**



The CVSS version of a CVE file.



CVSS v3 Version: 3.1

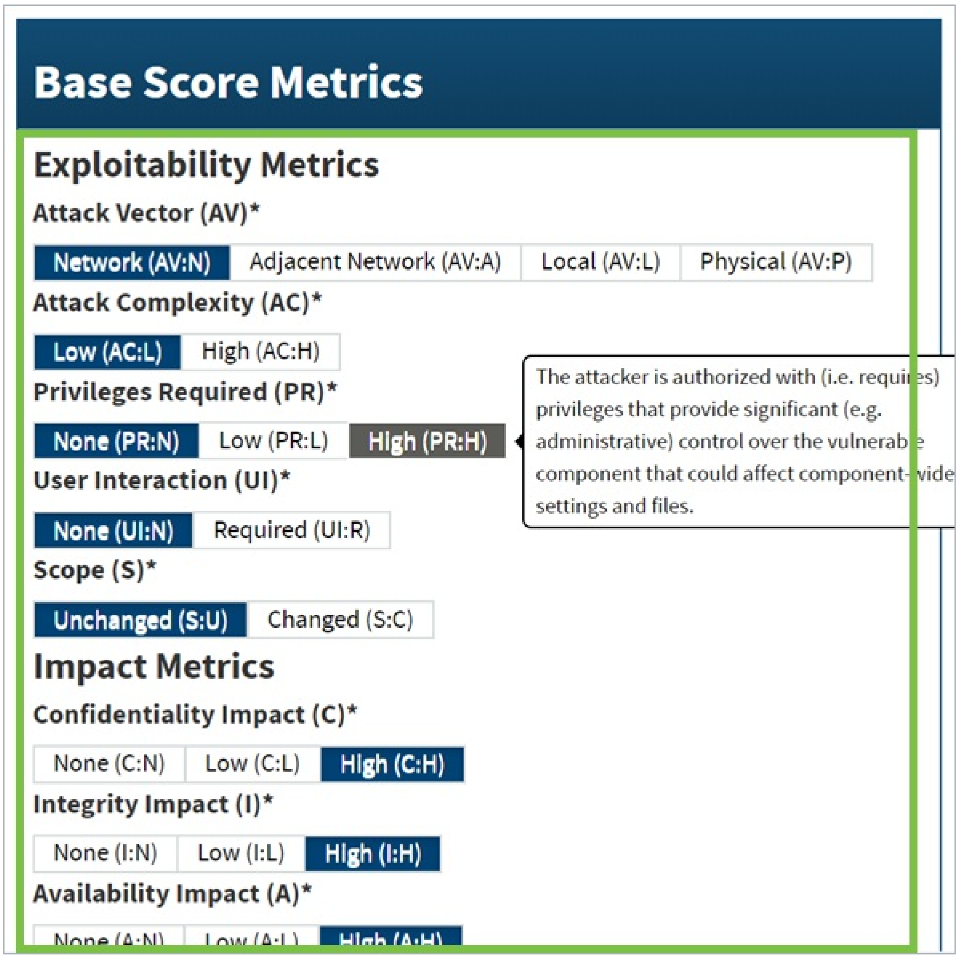
Attack Vector Network
Attack Complexity Low
Privileges Required None
User Interaction None

Confidentiality High
Integrity High
Availability High

Scope Unchanged

The CVE's CVSS v3 Version captured in RiskVision.

- Base Score Metrics v3



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*

[✓ None (PR:N)] Low (PR:L) High (PR:H)

The attacker is authorized with (i.e. requires) privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

User Interaction (UI)*

[✓ None (UI:N)] Required (UI:R)

Scope (S)*

[✓ Unchanged (S:U)] Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) [✓ High (C:H)]

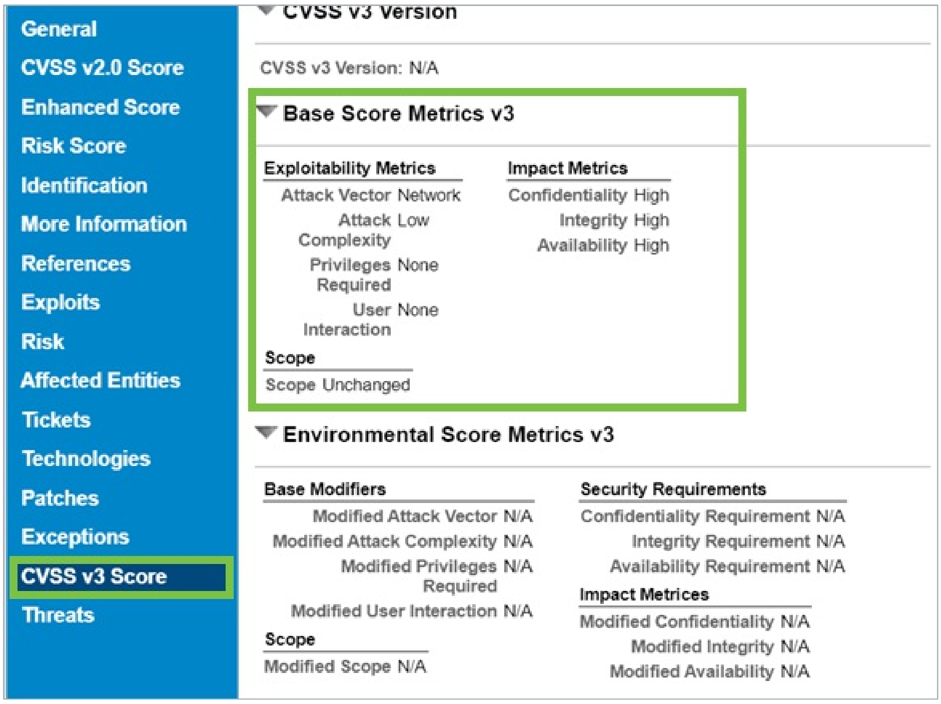
Integrity Impact (I)*

None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*

None (A:N) Low (A:L) [✓ High (A:H)]

The Base Score Metrics of a CVE file.



CVSS v3 Version

CVSS v3 Version: N/A

Base Score Metrics v3

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

Scope

Scope Unchanged

Environmental Score Metrics v3

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

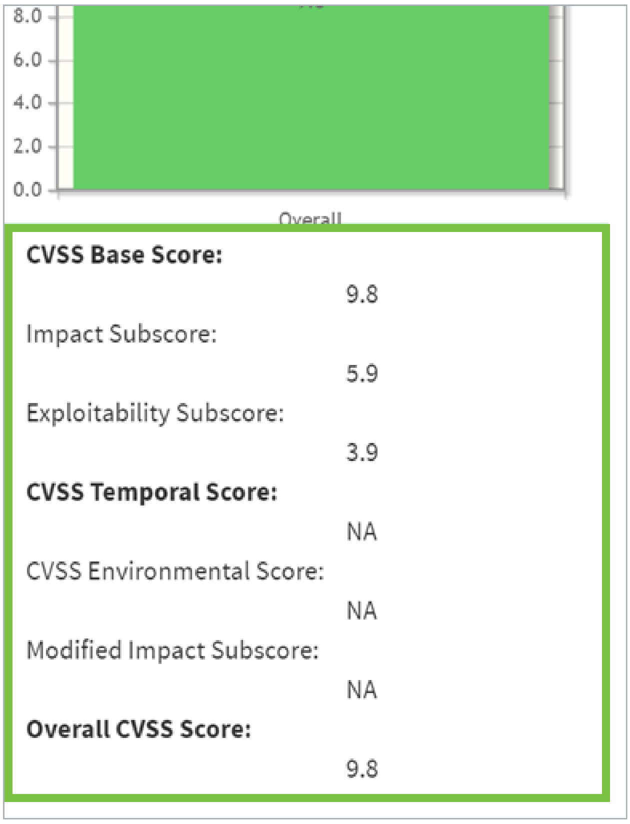
Impact Metrices	
Modified Confidentiality	N/A
Modified Integrity	N/A
Modified Availability	N/A

Scope

Modified Scope N/A

The CVE's Base Score Metrics captured in RiskVision.

- CVSS v3 Score



CVSS Base Score: 9.8

Impact Subscore: 5.9

Exploitability Subscore: 3.9

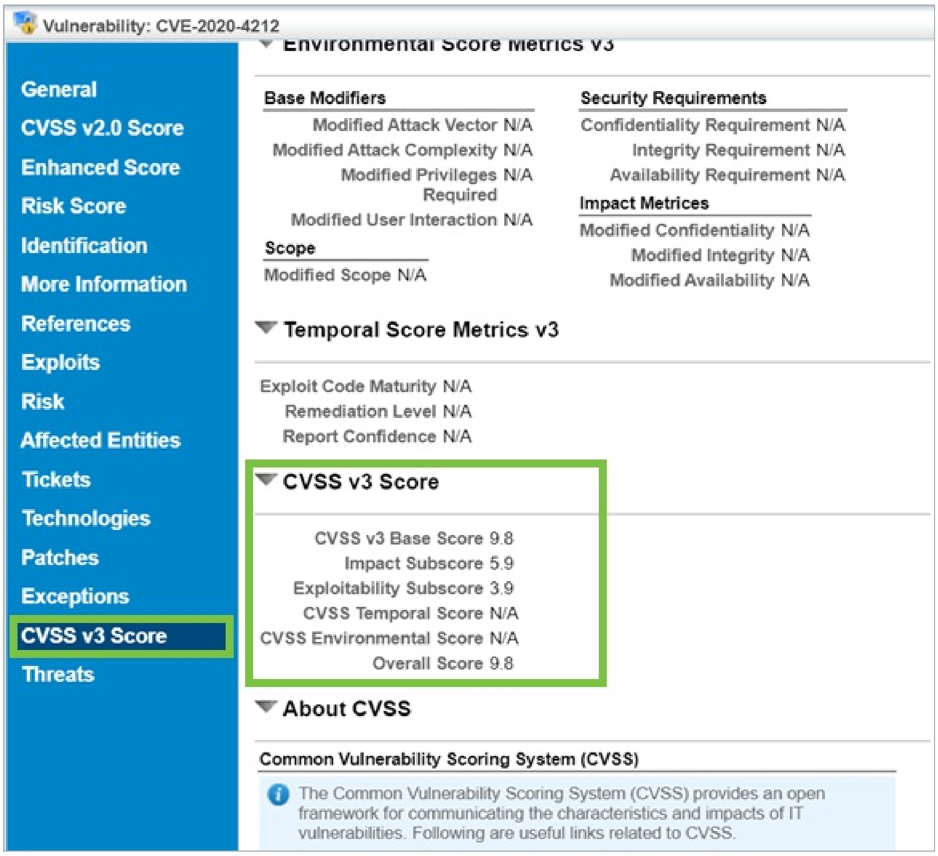
CVSS Temporal Score: NA

CVSS Environmental Score: NA

Modified Impact Subscore: NA

Overall CVSS Score: 9.8

The CVSS V3 Scores of a CVE file.



Base Modifiers

Modified Attack Vector N/A
Modified Attack Complexity N/A
Modified Privileges Required N/A
Modified User Interaction N/A

Scope

Modified Scope N/A

Security Requirements

Confidentiality Requirement N/A
Integrity Requirement N/A
Availability Requirement N/A

Impact Metrices

Modified Confidentiality N/A
Modified Integrity N/A
Modified Availability N/A

Temporal Score Metrics v3

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

CVSS v3 Score

CVSS v3 Base Score 9.8
Impact Subscore 5.9
Exploitability Subscore 3.9
CVSS Temporal Score N/A
CVSS Environmental Score N/A
Overall Score 9.8

About CVSS

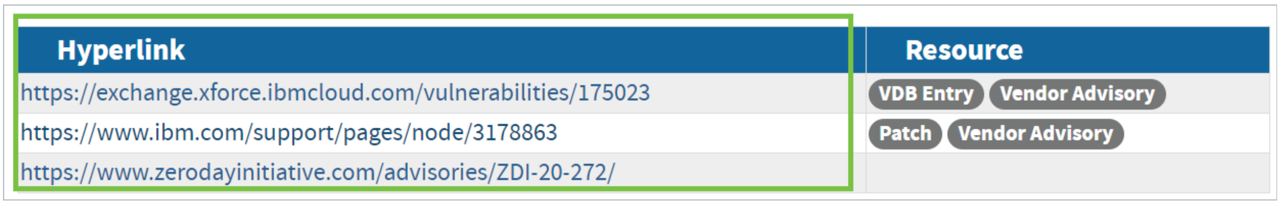
Common Vulnerability Scoring System (CVSS)

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.

The CVE's CVSS v3 Score captured in RiskVision.

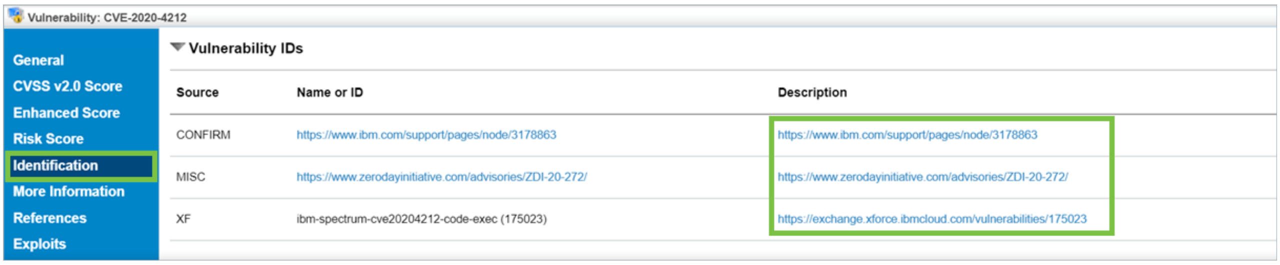
Hyperlinks

All related hyperlinks will be captured in the **Description** field of the vulnerability's **Identification** tab.



Hyperlink	Resource
https://exchange.xforce.ibmcloud.com/vulnerabilities/175023	VDB Entry Vendor Advisory
https://www.ibm.com/support/pages/node/3178863	Patch Vendor Advisory
https://www.zerodayinitiative.com/advisories/ZDI-20-272/	

The Hyperlink section of a CVE file.

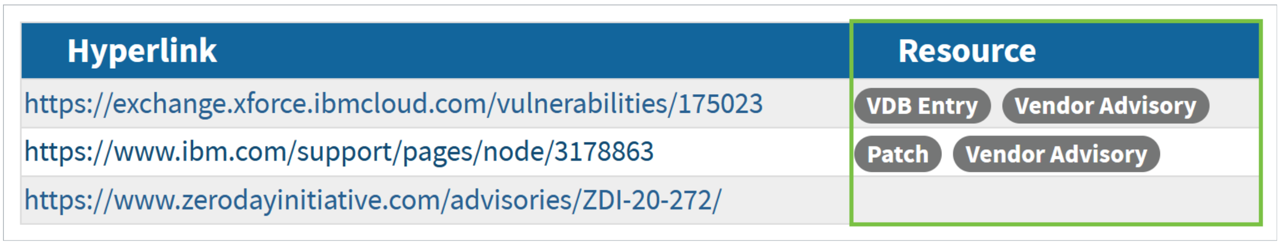


Source	Name or ID	Description
CONFIRM	https://www.ibm.com/support/pages/node/3178863	https://www.ibm.com/support/pages/node/3178863
MISC	https://www.zerodayinitiative.com/advisories/ZDI-20-272/	https://www.zerodayinitiative.com/advisories/ZDI-20-272/
XF	ibm-spectrum-cve20204212-code-exec (175023)	https://exchange.xforce.ibmcloud.com/vulnerabilities/175023

The CVE's hyperlinks captured in the Description field in RiskVision.

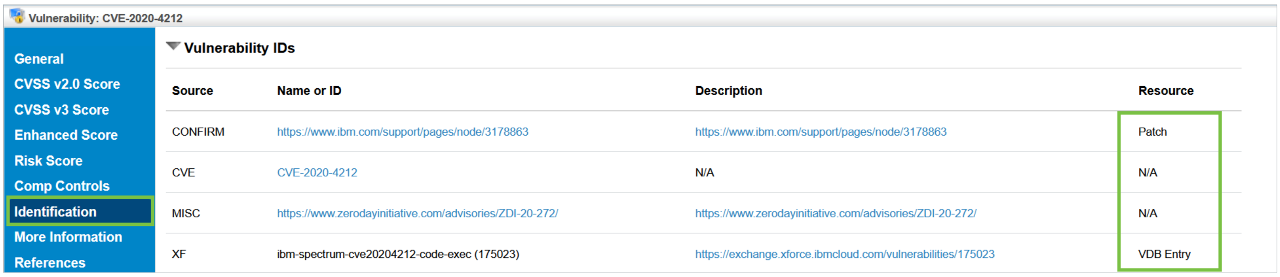
Resources

All related resources will be captured in the **Resource** field of the vulnerabilities **Identification** tab.



Hyperlink	Resource
https://exchange.xforce.ibmcloud.com/vulnerabilities/175023	VDB Entry Vendor Advisory
https://www.ibm.com/support/pages/node/3178863	Patch Vendor Advisory
https://www.zerodayinitiative.com/advisories/ZDI-20-272/	

The Resource section of a CVE file.

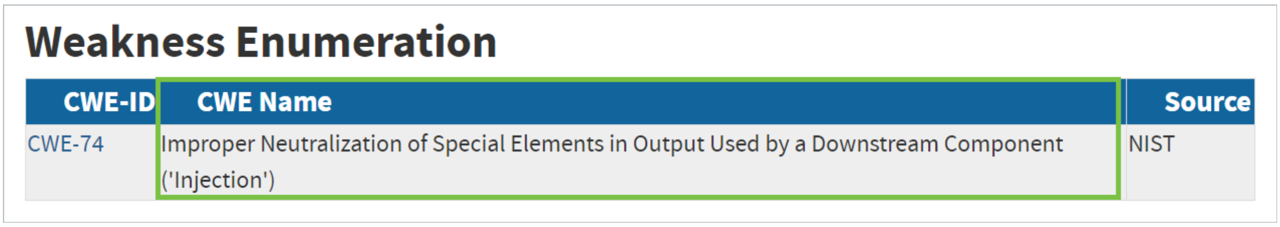


Source	Name or ID	Description	Resource
CONFIRM	https://www.ibm.com/support/pages/node/3178863	https://www.ibm.com/support/pages/node/3178863	Patch
CVE	CVE-2020-4212	N/A	N/A
MISC	https://www.zerodayinitiative.com/advisories/ZDI-20-272/	https://www.zerodayinitiative.com/advisories/ZDI-20-272/	N/A
XF	ibm-spectrum-cve20204212-code-exec (175023)	https://exchange.xforce.ibmcloud.com/vulnerabilities/175023	VDB Entry

The CVE's resources captured in the Resource field in RiskVision.

Weakness Enumeration

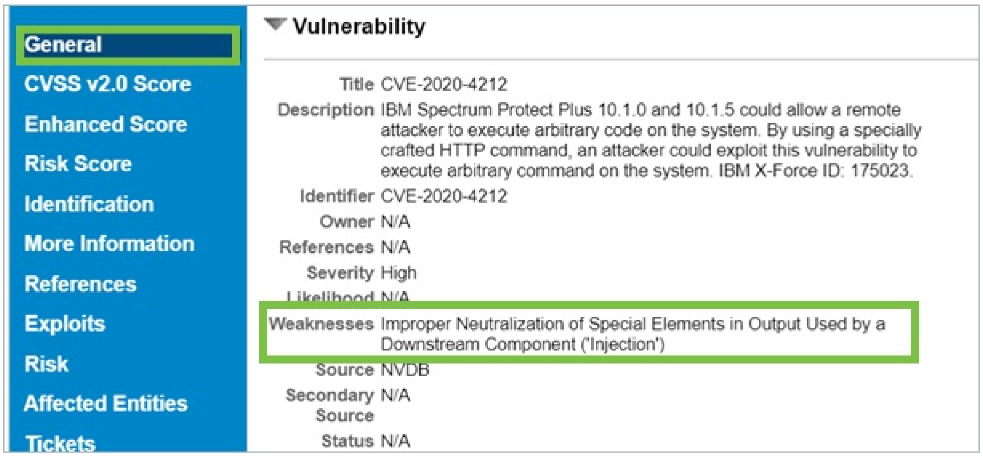
The .json file's **CWE Name** will be captured in the **Weaknesses** field of the vulnerability's **General** tab. The **CWE-ID** and **Source** will not be captured.



Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	NIST

The CWE Name of a weakness in a CWE file.



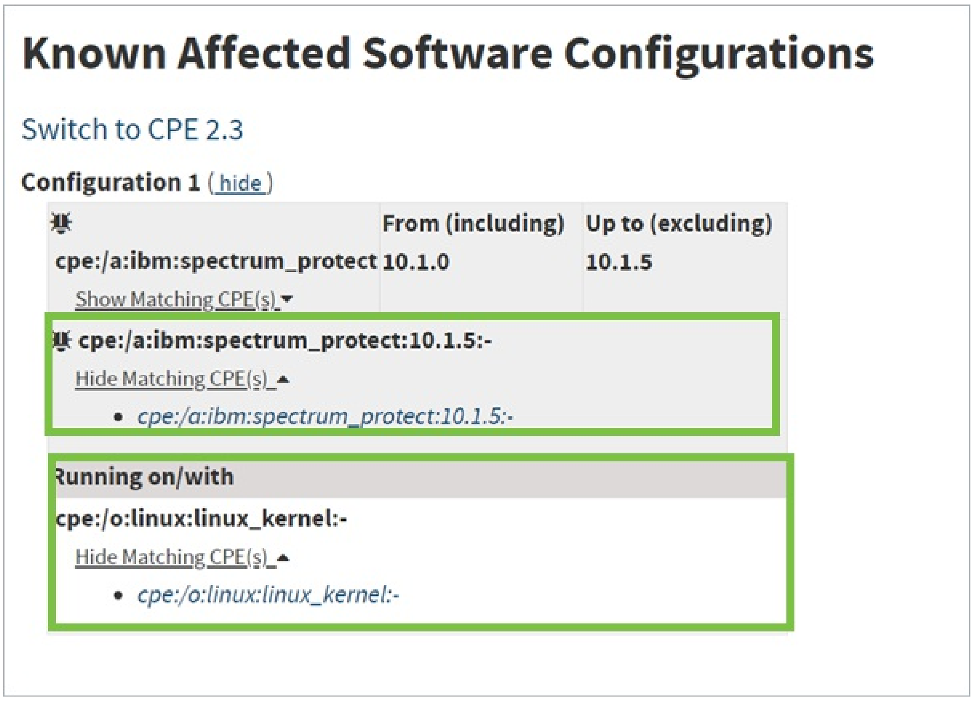
Vulnerability

Title CVE-2020-4212
Description IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.
Identifier CVE-2020-4212
Owner N/A
References N/A
Severity High
Likelihood N/A
Weaknesses Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
Source NVDB
Secondary Source N/A
Status N/A

The CWE Name captured in the Weaknesses field in RiskVision.

Known Affected Software Configurations

These will be captured in the vulnerability's **Technologies** tab.



Known Affected Software Configurations

Configuration 1 (hide)

	From (including)	Up to (excluding)
cpe:/a:ibm:spectrum_protect Show Matching CPE(s)	10.1.0	10.1.5
cpe:/a:ibm:spectrum_protect:10.1.5:- Hide Matching CPE(s) • cpe:/a:ibm:spectrum_protect:10.1.5:-		

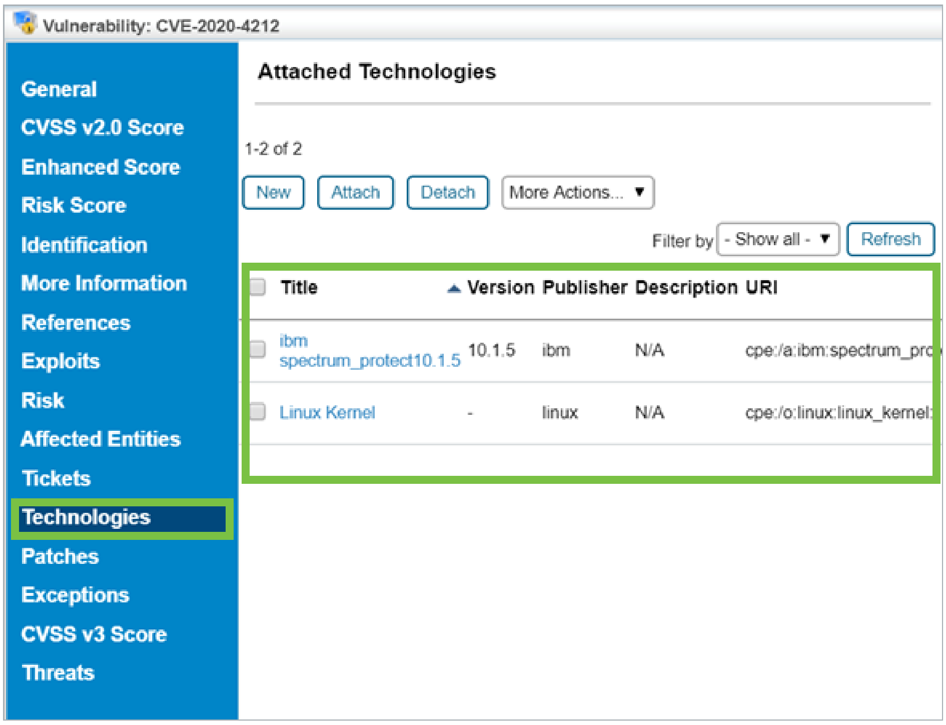
Running on/with

cpe:/o:linux:linux_kernel:-

Hide Matching CPE(s)

- cpe:/o:linux:linux_kernel:-

The Known Affected Software Configurations of a CVE file.


Vulnerability: CVE-2020-4212

Attached Technologies

1-2 of 2

□	Title	Version	Publisher	Description	URI
□	ibm spectrum_protect10.1.5	10.1.5	ibm	N/A	cpe:/a:ibm:spectrum_pro
□	Linux Kernel	-	linux	N/A	cpe:/o:linux:linux_kernel:

The CVE file's Known Affected Software Configurations captured in RiskVision.

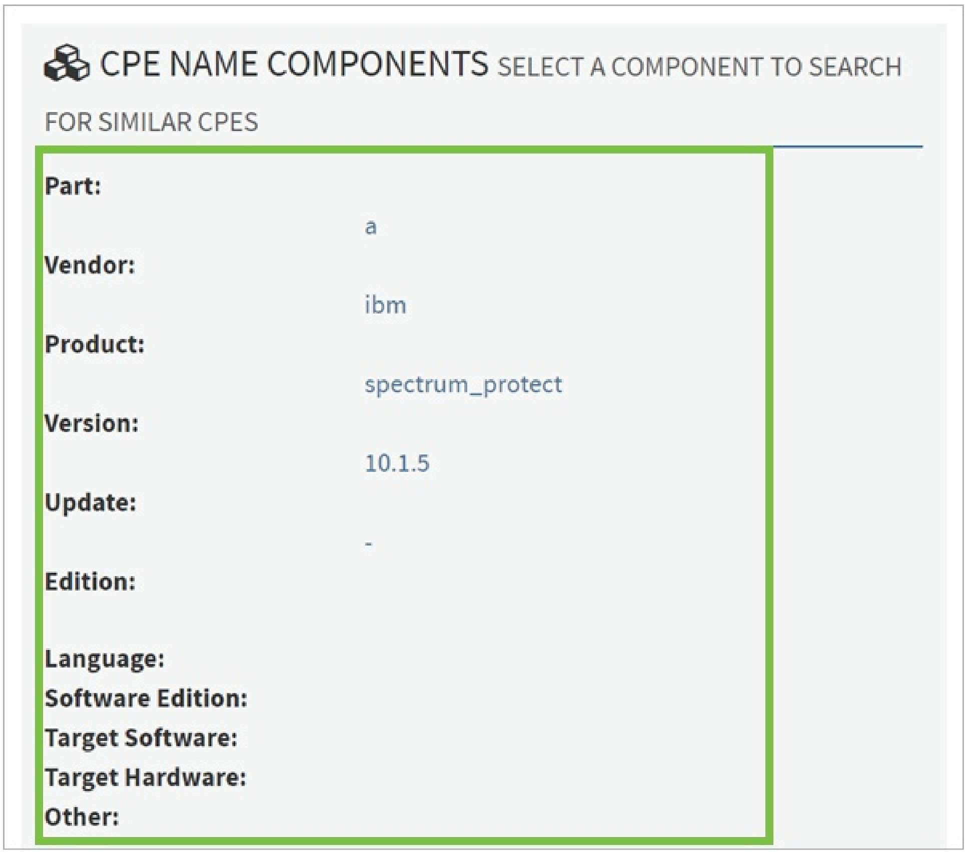
When Importing CPE Files

RiskVision will capture the following from the NVD website:

CPE Names

RiskVision can only import names from version 2.2 of CPE. The following components will be captured by the**General** tab of a technology:

- Part
- Vendor
- Product
- Cloud-init
- Version
- Update
- Edition
- Language



CPE NAME COMPONENTS SELECT A COMPONENT TO SEARCH FOR SIMILAR CPES

Part: a

Vendor: ibm

Product: spectrum_protect

Version: 10.1.5

Update: -

Edition:

Language:

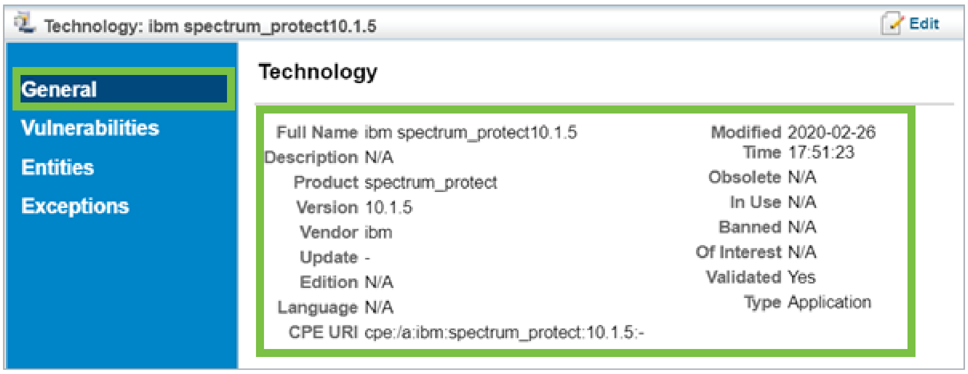
Software Edition:

Target Software:

Target Hardware:

Other:

The Name Components of a CPE file.



Technology

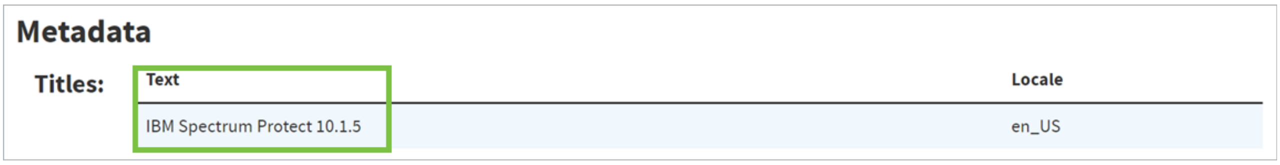
Full Name ibm spectrum_protect10.1.5
Description N/A
Product spectrum_protect
Version 10.1.5
Vendor ibm
Update -
Edition N/A
Language N/A
CPE URI cpe:/a:ibm:spectrum_protect:10.1.5:-

Modified 2020-02-26
Time 17:51:23
Obsolete N/A
In Use N/A
Banned N/A
Of Interest N/A
Validated Yes
Type Application

The CPE name components captured in RiskVision.

Metadata

The **Text** title will be captured by the**Full Name** field in a technology's **General** tab, but the **Locale** title will not.

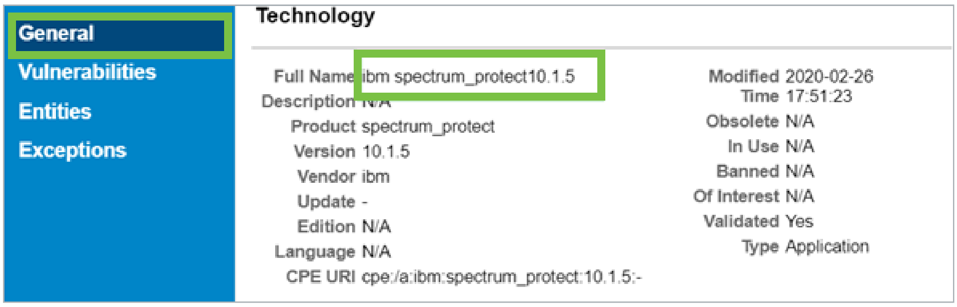


Metadata

Titles:

Text	Locale
IBM Spectrum Protect 10.1.5	en_US

The Text title in a CPE file.



Technology

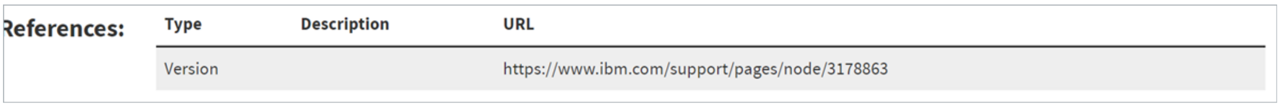
Full Name ibm spectrum_protect10.1.5
Description N/A
Product spectrum_protect
Version 10.1.5
Vendor ibm
Update -
Edition N/A
Language N/A
CPE URI cpe:/a:ibm:spectrum_protect:10.1.5:-

Modified Time 2020-02-26 17:51:23
Obsolete N/A
In Use N/A
Banned N/A
Of Interest N/A
Validated Yes
Type Application

The CPE's Text title captured by the Full Name field in RiskVision.

References

This section is not captured as they contain **Change Log** data.



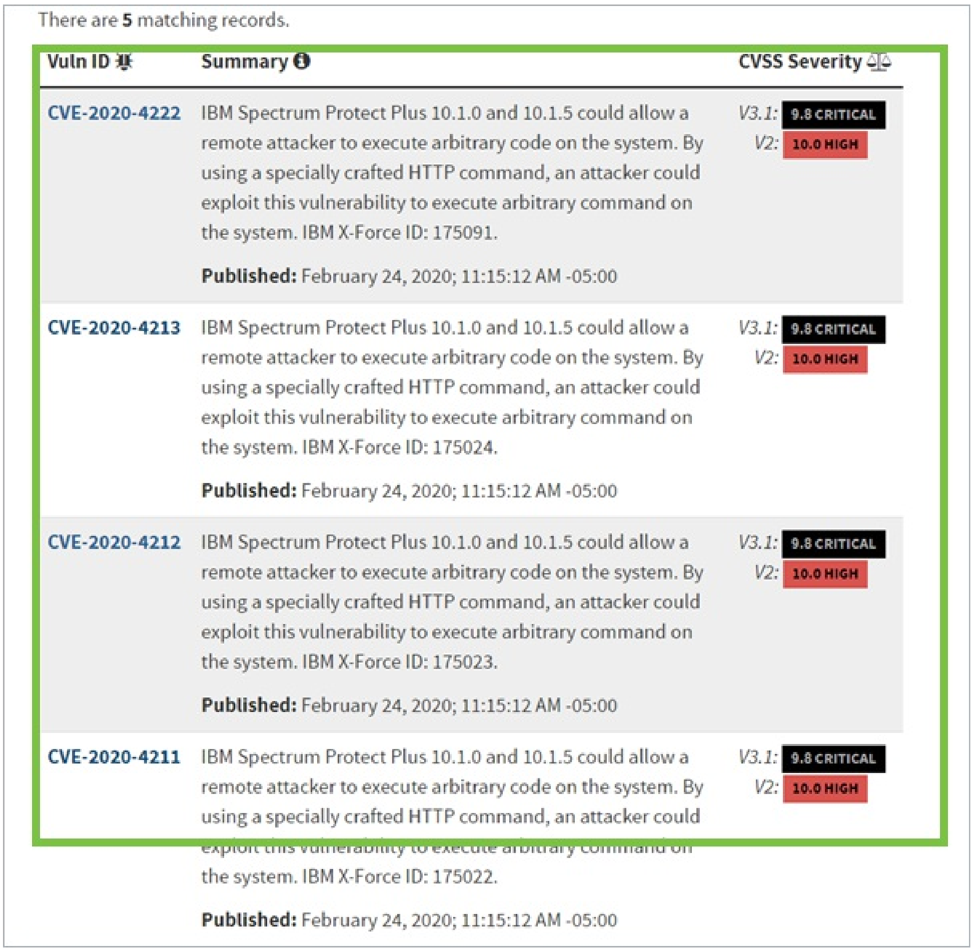
References:

Type	Description	URL
Version		https://www.ibm.com/support/pages/node/3178863

The References section of a CPE file.

CPE Usage

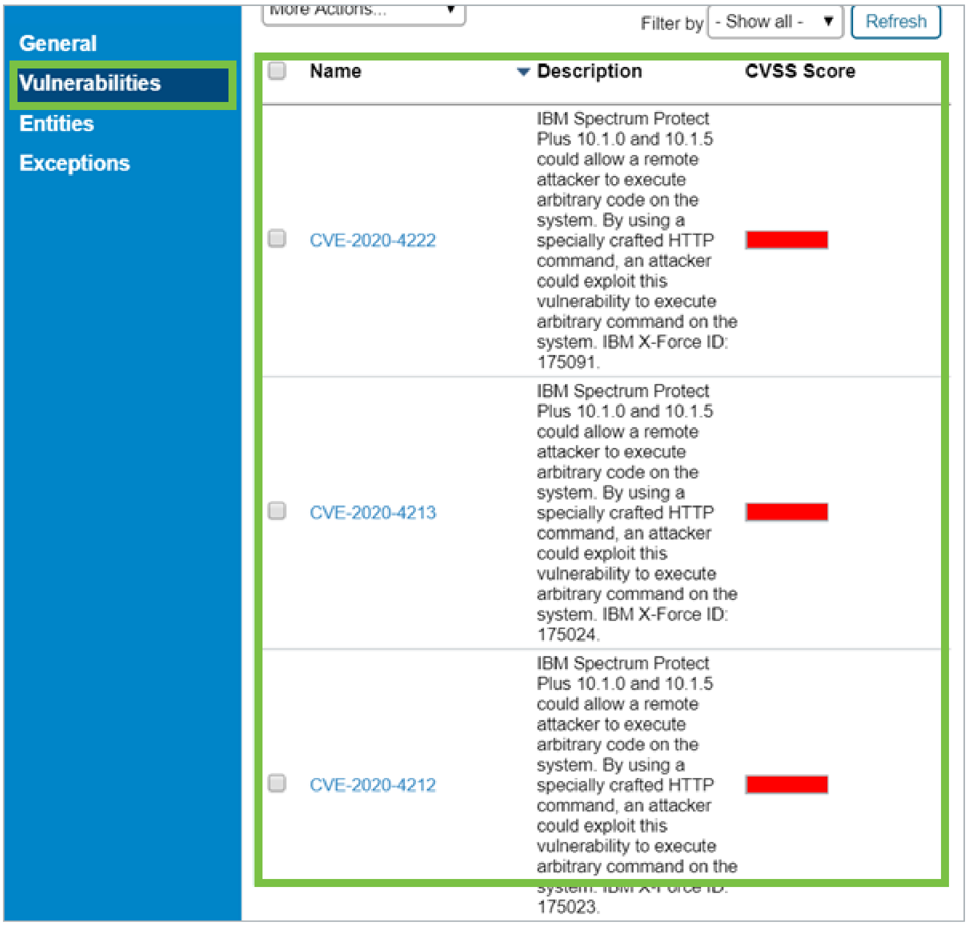
View and Associated vulnerabilities will be captured in RiskVision's **Vulnerabilities** tab for threats and technologies.



There are **5** matching records.

Vuln ID	Summary	CVSS Severity
CVE-2020-4222	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175091. **Published:** February 24, 2020; 11:15:12 AM -05:00	*V3.1:* 9.8 CRITICAL *V2:* 10.0 HIGH
CVE-2020-4213	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175024. **Published:** February 24, 2020; 11:15:12 AM -05:00	*V3.1:* 9.8 CRITICAL *V2:* 10.0 HIGH
CVE-2020-4212	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023. **Published:** February 24, 2020; 11:15:12 AM -05:00	*V3.1:* 9.8 CRITICAL *V2:* 10.0 HIGH
CVE-2020-4211	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175022. **Published:** February 24, 2020; 11:15:12 AM -05:00	*V3.1:* 9.8 CRITICAL *V2:* 10.0 HIGH

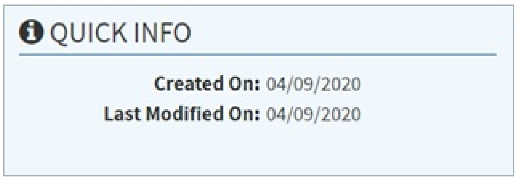
Vulnerabilities in a CPE file.



	Name	Description	CVSS Score
□	CVE-2020-4222	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175091.	🟥
□	CVE-2020-4213	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175024.	🟥
□	CVE-2020-4212	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.	🟥

The CPE's Vulnerabilities captured in RiskVision.

The connector will not capture the file's quick info such as published dates and last modified dates.

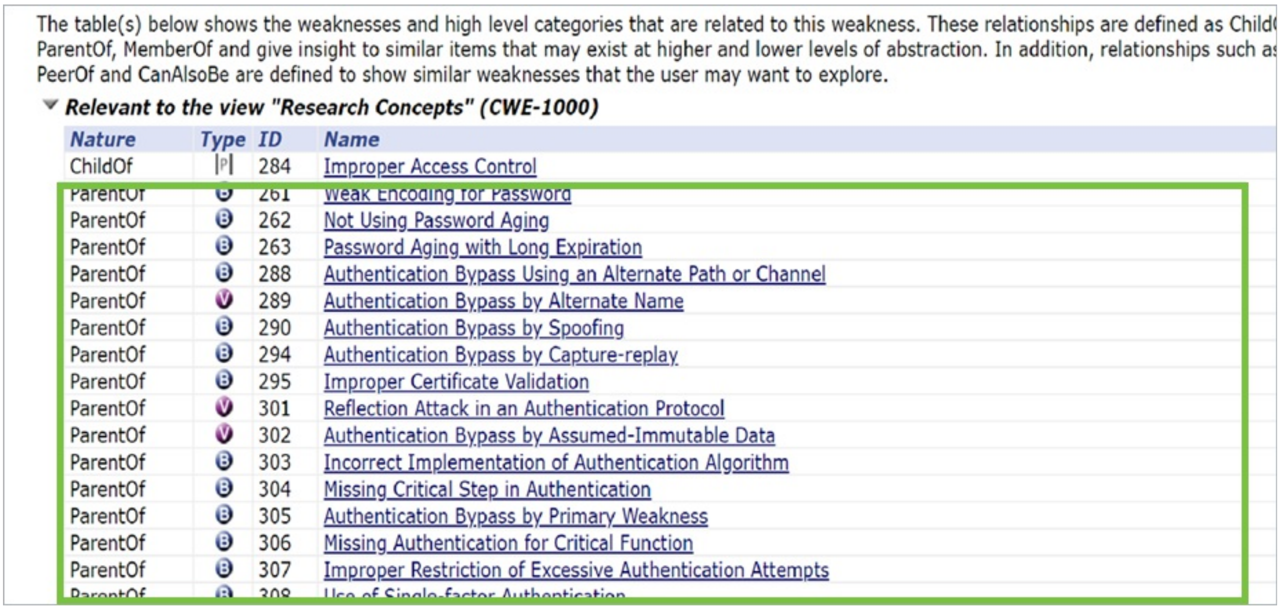

QUICK INFO

Created On: 04/09/2020
Last Modified On: 04/09/2020

The Quick Info of a CPE file.

When Importing CWE Files

While the NVD connector will import files from the CWE datafeed, it will import data from adifferent site than the NVD site. As of now, RiskVision will only capture **Parent Of** information from CWE files in the **General** tab of a weakness.

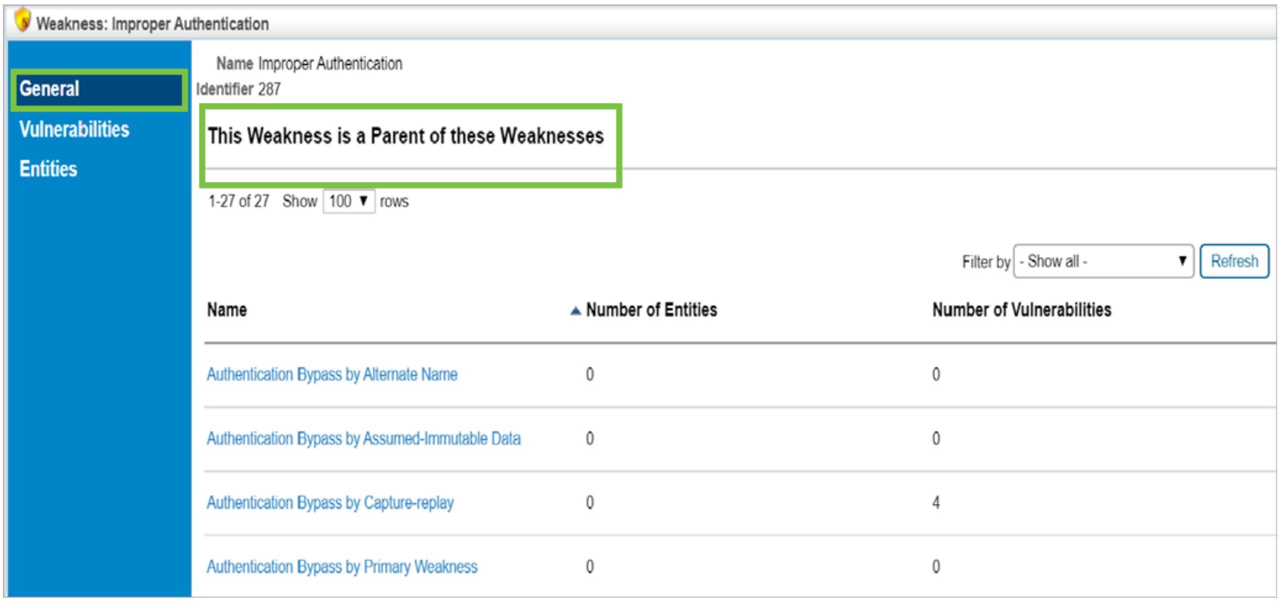


The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as Child ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such a PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	P	284	Improper Access Control
ParentOf	B	261	Weak Encoding for Password
ParentOf	B	262	Not Using Password Aging
ParentOf	B	263	Password Aging with Long Expiration
ParentOf	B	288	Authentication Bypass Using an Alternate Path or Channel
ParentOf	V	289	Authentication Bypass by Alternate Name
ParentOf	B	290	Authentication Bypass by Spoofing
ParentOf	B	294	Authentication Bypass by Capture-replay
ParentOf	B	295	Improper Certificate Validation
ParentOf	V	301	Reflection Attack in an Authentication Protocol
ParentOf	V	302	Authentication Bypass by Assumed-Immutable Data
ParentOf	B	303	Incorrect Implementation of Authentication Algorithm
ParentOf	B	304	Missing Critical Step in Authentication
ParentOf	B	305	Authentication Bypass by Primary Weakness
ParentOf	B	306	Missing Authentication for Critical Function
ParentOf	B	307	Improper Restriction of Excessive Authentication Attempts
ParentOf	B	308	Use of Single-factor Authentication

The Parent Of information in a CWE file.



Name Improper Authentication
Identifier 287

This Weakness is a Parent of these Weaknesses

1-27 of 27 Show 100 ▾ rows

Filter by - Show all - ▾

Name	▲ Number of Entities	Number of Vulnerabilities
Authentication Bypass by Alternate Name	0	0
Authentication Bypass by Assumed-Immutable Data	0	0
Authentication Bypass by Capture-replay	0	4
Authentication Bypass by Primary Weakness	0	0

The Parent Of information from a CWE file captured in RiskVision.

Exploit Database Connector Overview

In order for the Exploits grid to provide users with information, it must first be populated with data. Resolver RiskVision uses the Exploit Database connector to achieve this purpose. Once a day, this connector automatically accesses the Exploit Database and downloads the data into a customer-specific CSV file. This file is imported back into RiskVision and used to populate the Exploits grid.

In addition to downloading information from the Exploit Database, the connector also correlates this data to its corresponding vulnerability, making it easy for users to identify any weaknesses. It also factors into the risk scoring of vulnerabilities to help users prioritize which vulnerabilities should be addressed first.

Exploit Database Connector Prequisites

Before installing the Exploit Database connector, ensure that the following prerequisites are met on the machine that:

- Windows 2008 Standard Edition or Windows 2012 platform
- Resolver RiskVision version 8.5 or higher
- The **RiskVisionExploitDatabaseConnector.msi** file obtained from Resolver Support
- **JAVA_HOME** must be set as an environmental parameter for Java

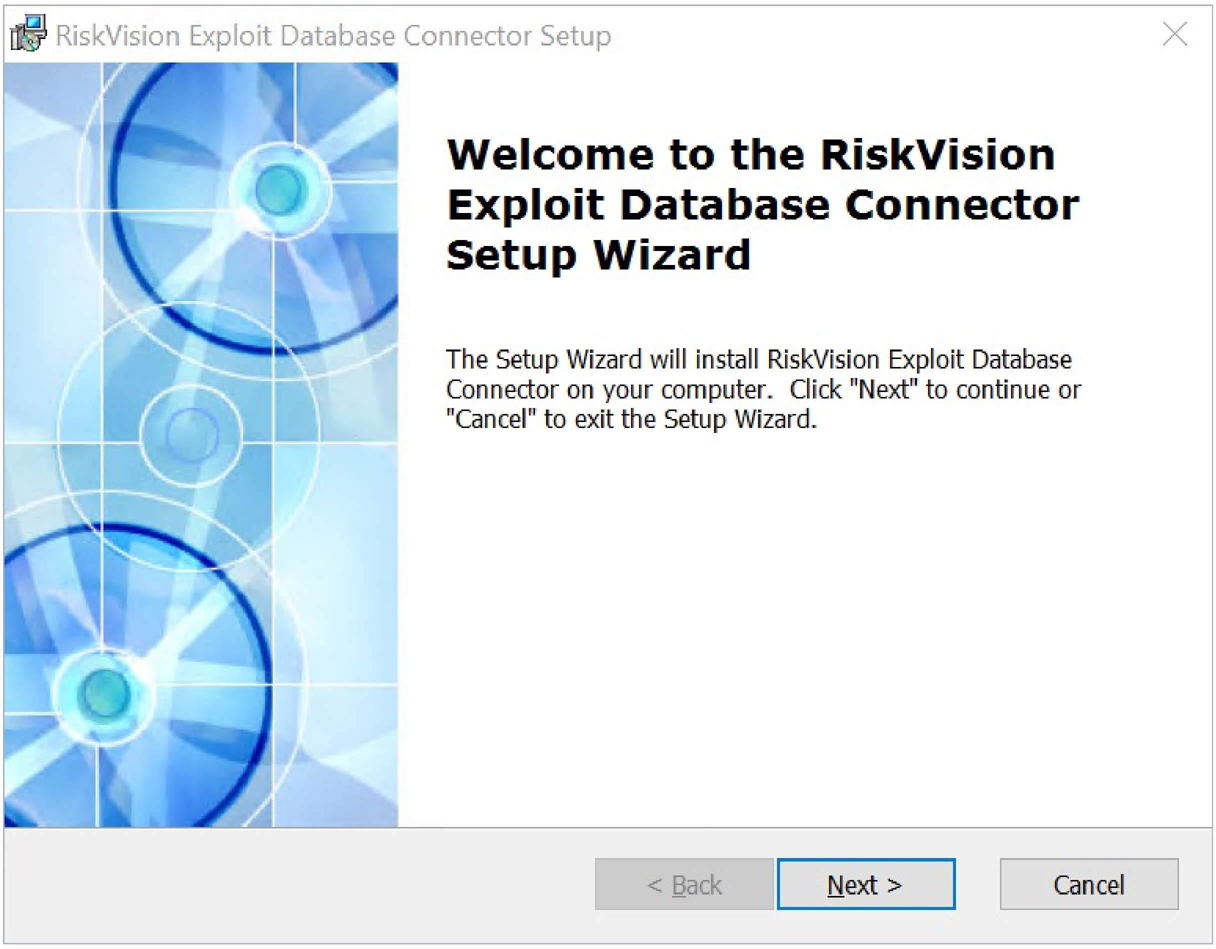
Install the Exploit Database Connector

Resolver recommends that the Exploit Database connector be installed on the same machine as RiskVision. If this is not possible, it can be installed on a remote host server that it has sufficient privileges to connect with the RiskVision server.

Before installing the connector, ensure that all prerequisites are in place on the desired machine.

To install the Exploit Database connector:

1. Download the **RiskVisionExploitDatabaseConnector.msi** file on the computer where the connector will be installed.
2. Run the file to launch the setup wizard.



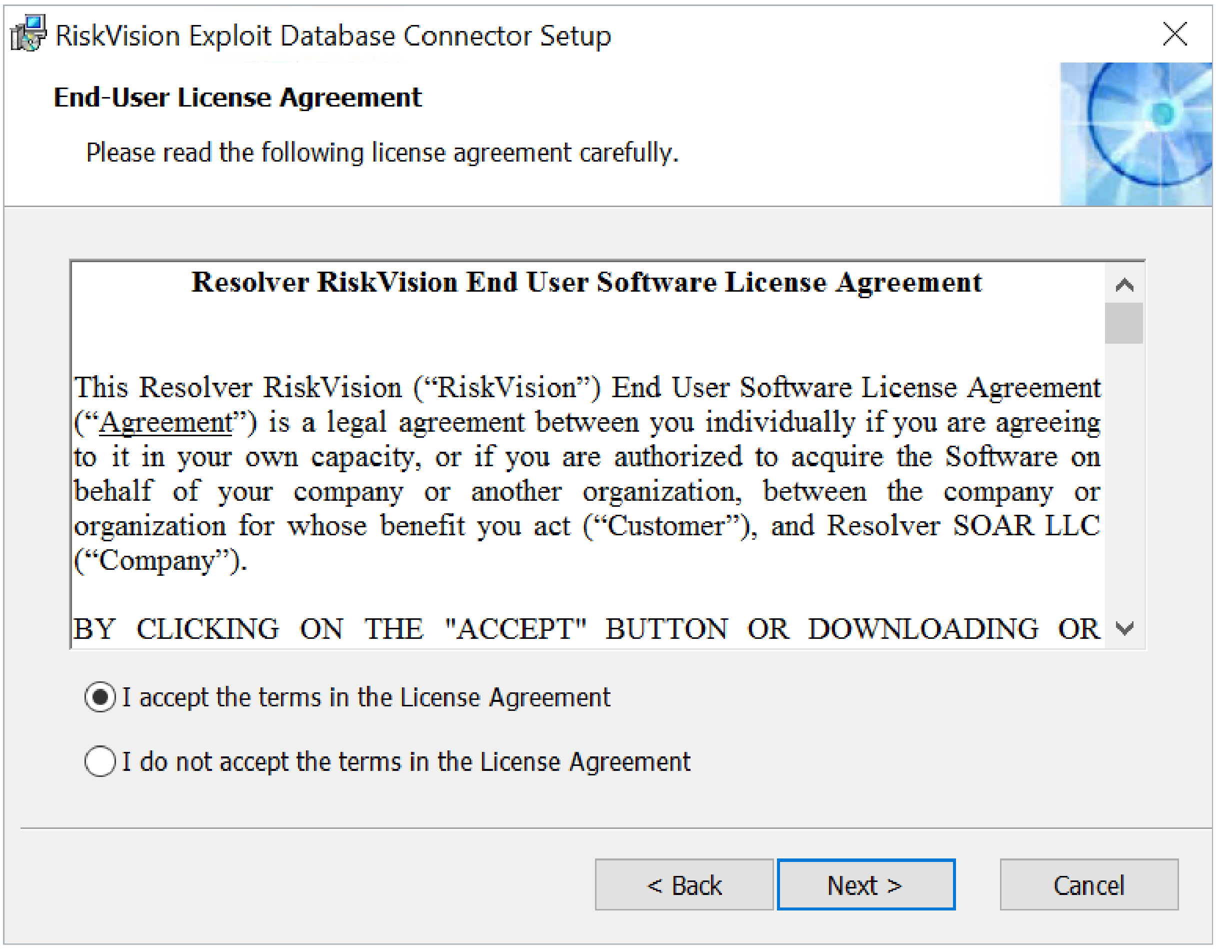
RiskVision Exploit Database Connector Setup

Welcome to the RiskVision Exploit Database Connector Setup Wizard

The Setup Wizard will install RiskVision Exploit Database Connector on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

The Exploit Database Connector Setup wizard.

3. Click **Next**.
4. Click **I accept the terms in the License Agreement**



RiskVision Exploit Database Connector Setup
End-User License Agreement
Please read the following license agreement carefully.

Resolver RiskVision End User Software License Agreement

This Resolver RiskVision ("RiskVision") End User Software License Agreement ("Agreement") is a legal agreement between you individually if you are agreeing to it in your own capacity, or if you are authorized to acquire the Software on behalf of your company or another organization, between the company or organization for whose benefit you act ("Customer"), and Resolver SOAR LLC ("Company").

BY CLICKING ON THE "ACCEPT" BUTTON OR DOWNLOADING OR

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

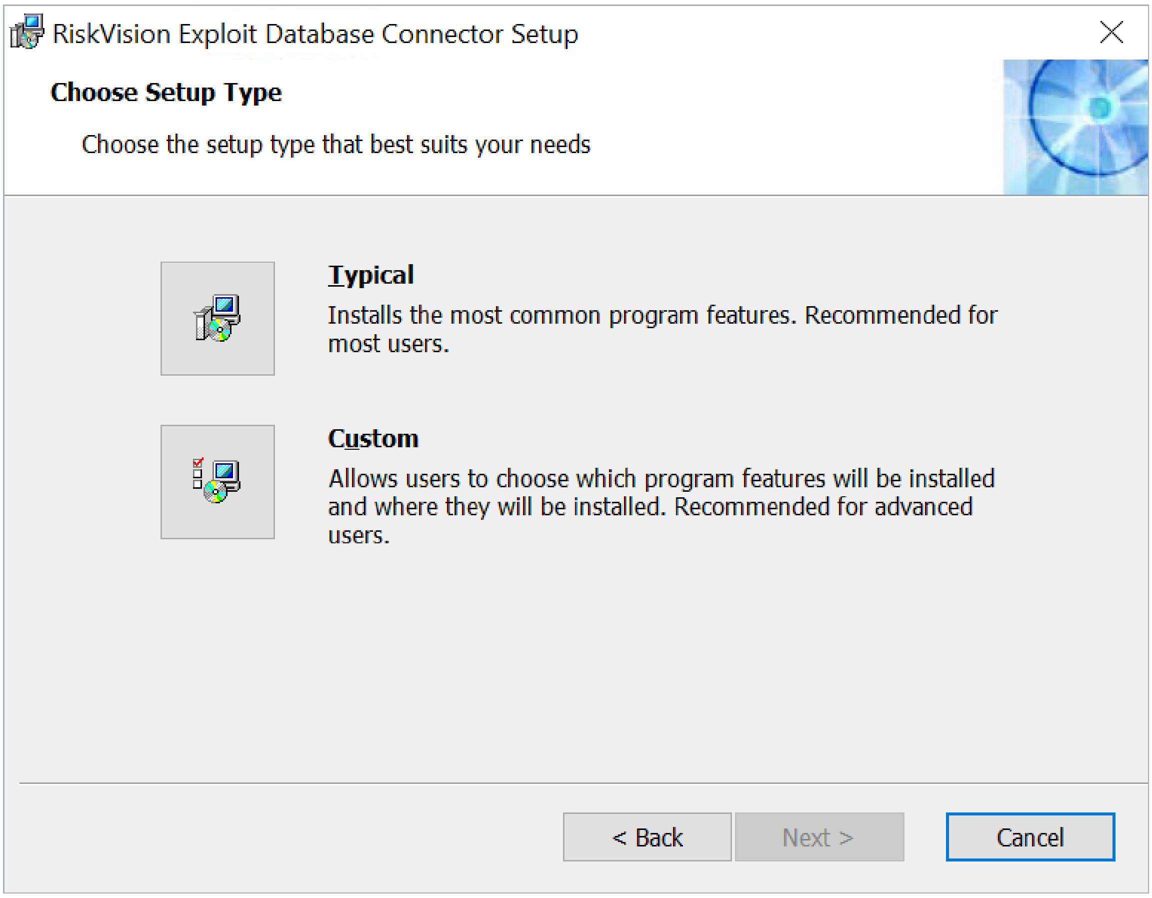
The End-User License Agreement.

5. Click **Next**.

6. Choose one of the following:

   - **Typical**: Installs the connector in the **C:\Program Files (x86)\Agiliance\** folder by default.

   - **Custom**: Specify the desired location of the connector.


RiskVision Exploit Database Connector Setup

Choose Setup Type

Choose the setup type that best suits your needs

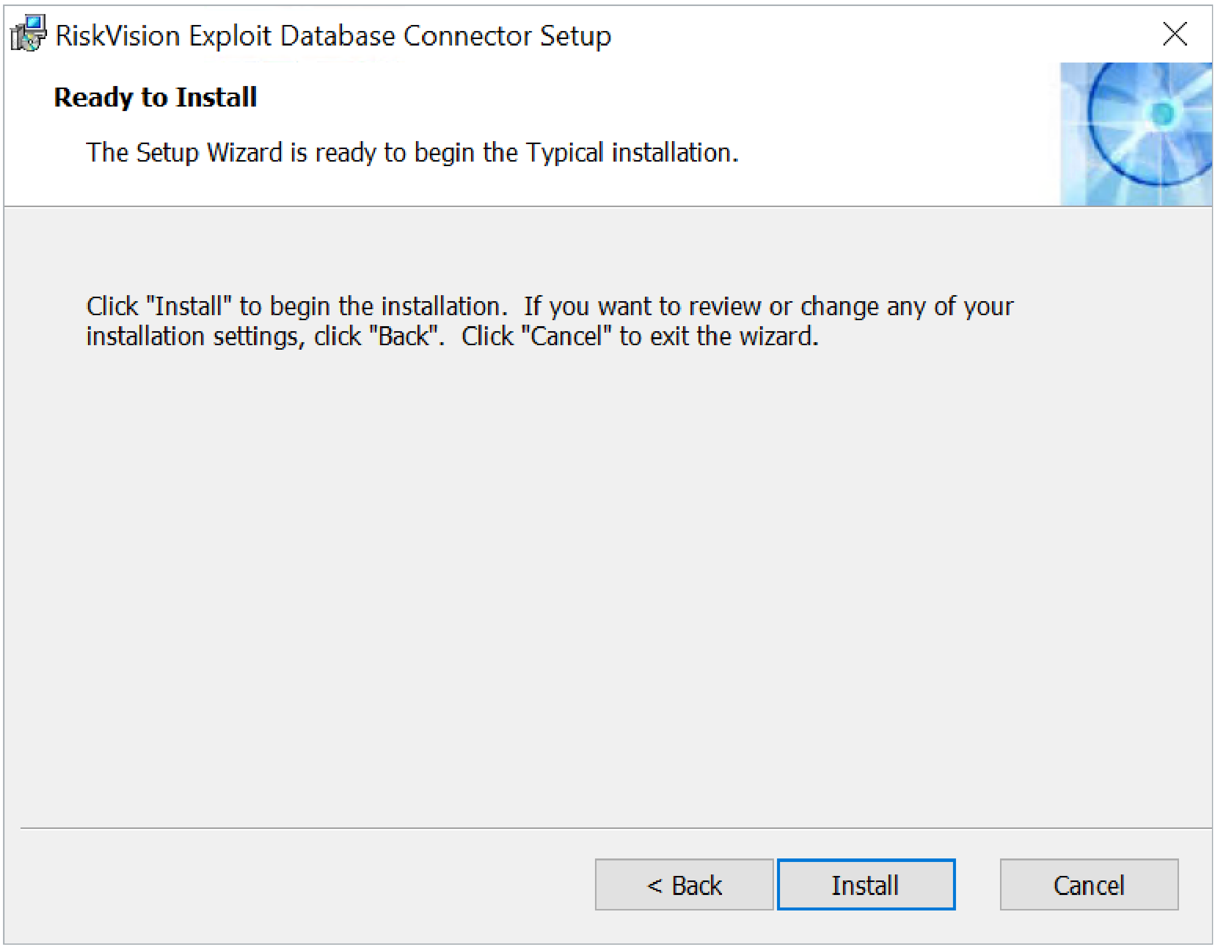
Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

The Choose Setup Type screen.

7. Click **Next**.

8. Click **Install**.



RiskVision Exploit Database Connector Setup

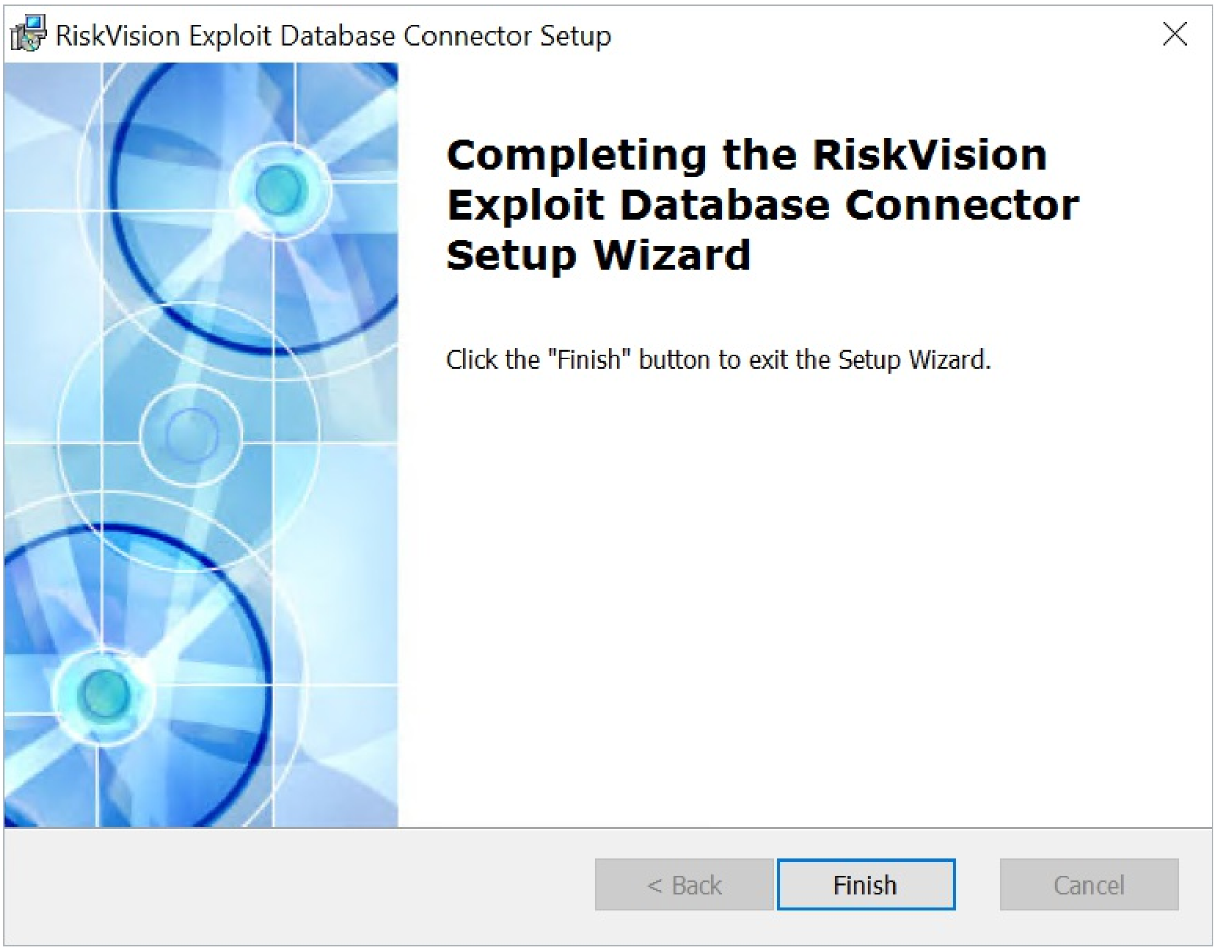
Ready to Install

The Setup Wizard is ready to begin the Typical installation.

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

The Ready to Install screen.

9. Click **Finish** to exit the wizard once the installation is complete.



RiskVision Exploit Database Connector Setup

Completing the RiskVision Exploit Database Connector Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

The Completion screen.

Starting, Stopping, & Restarting the Exploit Database Connector

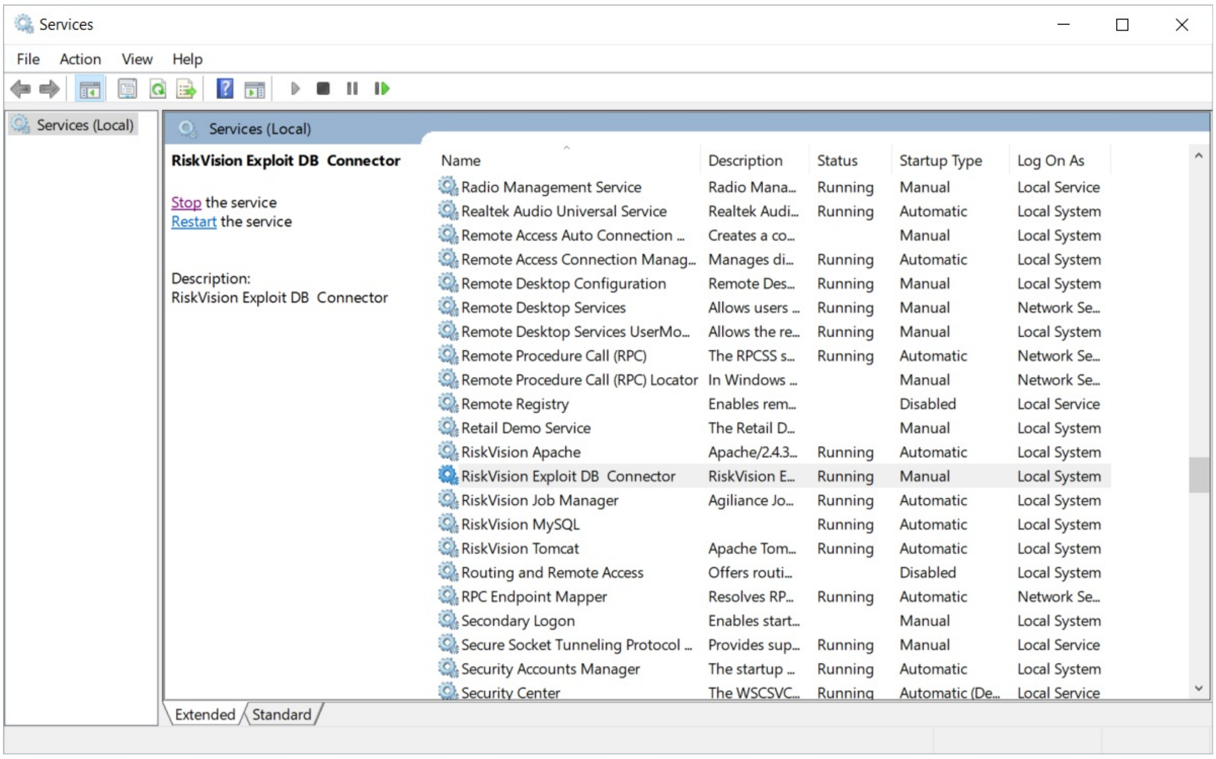
Installing the Exploit Database connector sets it up as a Microsoft Windows service; however, by default, the Microsoft Windows service will not be started. In order to start, stop, or restart the service, certain steps must be taken.

To start, stop, or restart the Exploit Database connector:

1. Go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools**.

2. Click **Services**.

3. Right-click **RiskVision Exploit DB Connector**, and select either **Start**, **Stop**, or **Restart**.



RiskVision Exploit DB Connector

Stop the service
Restart the service

Description:
RiskVision Exploit DB Connector

Name	Description	Status	Startup Type	Log On As
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Realtek Audio Universal Service	Realtek Audi...	Running	Automatic	Local System
Remote Access Auto Connection ...	Creates a co...		Manual	Local System
Remote Access Connection Manag...	Manages di...	Running	Automatic	Local System
Remote Desktop Configuration	Remote Des...	Running	Manual	Local System
Remote Desktop Services	Allows users ...	Running	Manual	Network Se...
Remote Desktop Services UserMo...	Allows the re...	Running	Manual	Local System
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network Se...
Remote Procedure Call (RPC) Locator	In Windows ...		Manual	Network Se...
Remote Registry	Enables rem...		Disabled	Local Service
Retail Demo Service	The Retail D...		Manual	Local System
RiskVision Apache	Apache/2.4.3...	Running	Automatic	Local System
RiskVision Exploit DB Connector	RiskVision E...	Running	Manual	Local System
RiskVision Job Manager	Agiliance Jo...	Running	Automatic	Local System
RiskVision MySQL		Running	Automatic	Local System
RiskVision Tomcat	Apache Tom...	Running	Automatic	Local System
Routing and Remote Access	Offers routi...		Disabled	Local System
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network Se...
Secondary Logon	Enables start...		Manual	Local System
Secure Socket Tunneling Protocol ...	Provides sup...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSVC...	Running	Automatic (De...	Local Service

The RiskVision Exploit DB Connector in Services.

Configuring the RiskVision Host Settings

If you installed the connector on the same host as RiskVision, the connector will automatically display on the**Administration** > **Connectors** page. By default, the connector uses loopback (localhost) on port 443 to communicate with the RiskVision server. When you install the connector on a different host or use a port other than 443, you must configure the RiskVision application host information.

To change the RiskVision host settings:

1. Open the **/Exploit Database Connector/cfg/connector.properties** file in the connector host.
2. Point the `server_host` property to the RiskVision host name or IP adress.
3. Save the file.
4. Restart the connector service.

Connector Authentication

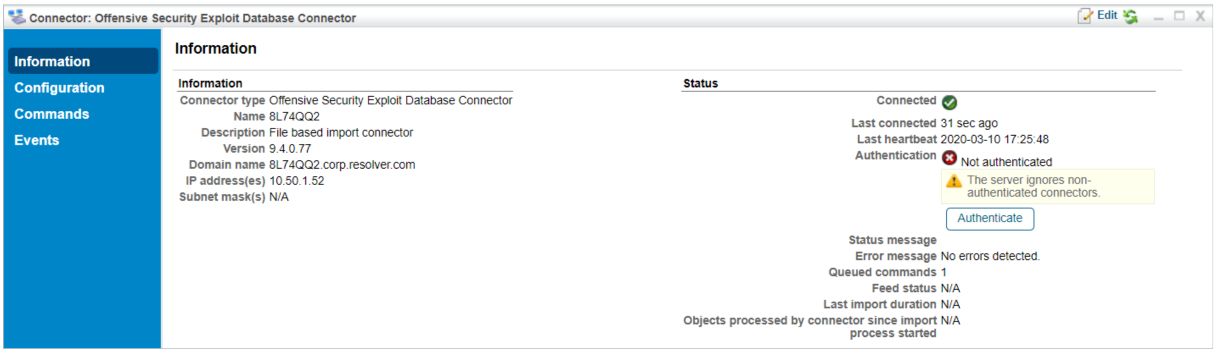
Before the Exploit Database connector can send any messages to the RiskVision Server, it must first be manually authenticated.

To authenticate the connector:

1. In the **RiskVision Administration** application, click on **Administration** > **Connectors**.

2. Select the **Exploit DB Connector** to open its details page. The **Information** tab will open by default.

3. Click Authenticate on the right-hand side of the screen.



Information

Information
Connector type Offensive Security Exploit Database Connector
Name 8L74QQ2
Description File based import connector
Version 9.4.0.77
Domain name 8L74QQ2.corp.resolver.com
IP address(es) 10.50.1.52
Subnet mask(s) N/A

Status
Connected ✓
Last connected 31 sec ago
Last heartbeat 2020-03-10 17:25:48
Authentication ✗ Not authenticated
⚠ The server ignores non-authenticated connectors.
Status message
Error message No errors detected.
Queued commands 1
Feed status N/A
Last import duration N/A
Objects processed by connector since import process started N/A

The Exploit Database Connector's details page.

Downloading Encrypted CSV Files

To download the CSV files:

1. Stop the RiskVision Exploit DB connector.
2. Navigate to **\cfg** and open the **connector.file.properties** file.
3. Enter values for the below properties as shown:
    - `exploit.encryption.secret.key` = Enter the value received from Resolver Support.
    - `exploit.cron.expression` = This value represents the interval of time the connector will download the encrypted files. By default, it is set for 1 AM, but it can be configured as desired.
    - `riskvision.server.url` = Enter the value received from Resolver Support.
4. Restart the **services.msc** Exploit DB connector.
5. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy file.

    > ⓘ Ensure the latest version has been downloaded.

6. Extract the file and copy the **local_policy.jar** and **US_export_policy.jar** files into the **JAVA_HOME/jre/lib/security directory** folder in the connector.

Troubleshooting the Exploit Database Connector

In the event that a user runs into problems while using the Exploit Database connector, there are a few steps that can be taken. The below steps should help resolve most common errors that the user will encounter.

To troubleshoot most common issues:

1. Ensure that the connector is authenticated.
2. Confirm that there are no errors or exceptions in the connector's log.
3. Confirm that the RiskVision server did not report any connector errors. In the event of an error, resolve them by providing proper configuration details.
4. In the event of a decryption error, verify that the connectors are using the latest JCE file and the latest `exploit.encryption.secret.key` .

If problems persist:

1. Stop the connector.
2. Delete all files from the **\data\old** folder.
3. Copy the correct file in the **\data\new** folder. GS: What is the correct file and what should the user do with it once they copy it?
4. Start the connector and provide a couple of heartbeat cycles to see if hierarchies start showing up in the connector log as well as in RiskVision itself.

If all of the above steps fail, contact Resolver Support.

Enable Proxy Server

By setting up a proxy server, the connector will operate at a faster speed and save on bandwidth. This will cause the Exploit Database connector to run smoother and reduce the strain put on RiskVision as a whole.

To enable the proxy server:

1. Navigate to and open the **/Exploit Database Connector/cfg/connector.file.properties** file.

2. Ensure the following properties are displayed as follows:

```
Proxy.useProxyServer = true
Proxy.serverHost = Server Hostname
Proxy.serverPort = 3128
Proxy.httpType = http
```

3. Save the file.

4. Restart the Exploit Database connector.

NVD Connector Overview

The National Vulnerability Database (NVD) connector integrates with the Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE), and Common Vulnerabilities and Exposures (CVE) data feeds. The NVD connector provides standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). Asset and vulnerability data from NVD is sent to RiskVision, and this data can be used for threat and vulnerability management.

The NVD connector connects to the NIST database and automatically pulls vulnerabilities to populate RiskVision's vulnerabilities section. GS: I know it can be configured to do more, but how often does it do this by default? The connector automatically maps the NVD vulnerability field to target fields. CVE ID, patch, exploits, and other vulnerability-specific information is imported and mapped automatically to RiskVision's target fields. Remediation workflow helps organizations prioritize each vulnerability and fix them in time.

NVD Connector Prerequisites

Before installing the Exploit Database connector, ensure that the following prerequisites are met: GS: I'm not sure about some of these (especially the third one). Are they all correct?

- Windows 2008 Standard Edition or Windows 2012 platform
- Resolver RiskVision version 6.5 SP1 or higher
- Access to the NVD data directory
- The **RiskVisionNVDConnector.msi** file obtained from Resolver Support
- **JAVA_HOME** must be set as an environmental parameter for Java

Install the NVD Connector

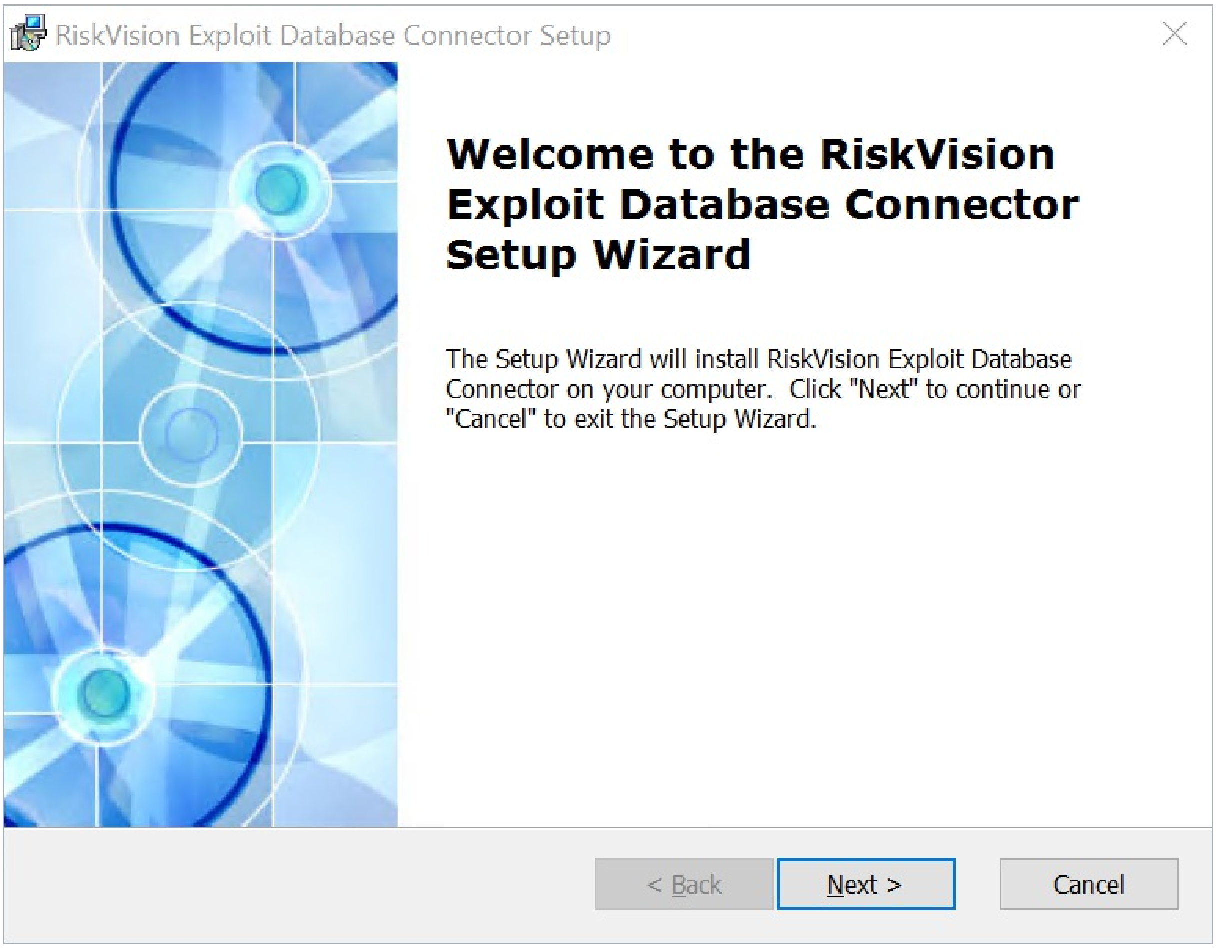
Resolver recommends that the NVD connector be installed on the same machine as RiskVision. If this is not possible, it can be installed on a remote host server that it has sufficient privileges to connect with the RiskVision server.

Before installing the connector, ensure that all prerequisites are in place on the desired machine. GS: I copied the below instructions and screenshots from the Exploit Database connector guide since the steps are all the same, but the screenshots all say Exploit Database on them. Can I get some screenshots that are relevant to the NVD connector please?

To install the NVD connector:

1. Download the **RiskVisionNVDConnector.msi** file on the computer where the connector will be installed.

2. Run the file to launch the setup wizard.



RiskVision Exploit Database Connector Setup

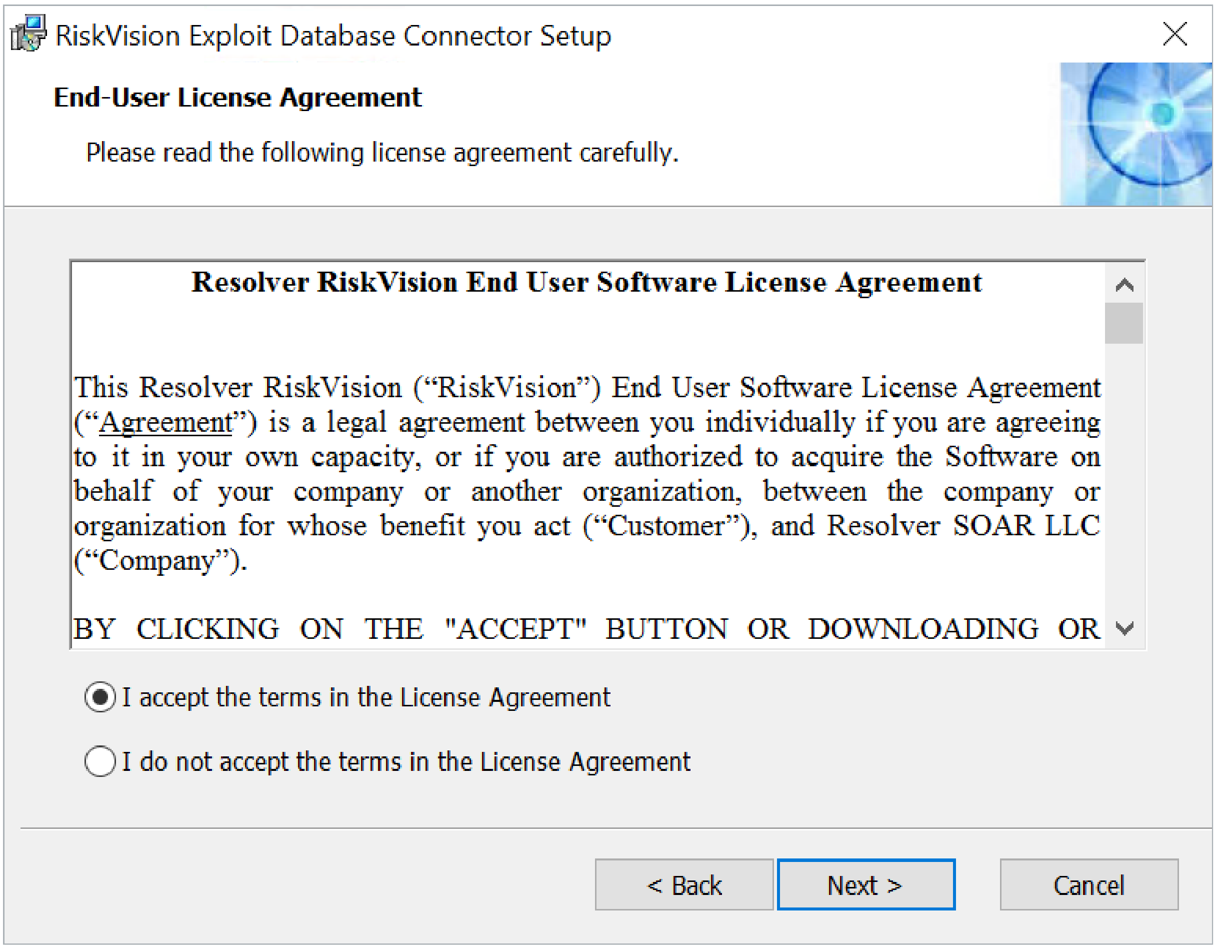
Welcome to the RiskVision Exploit Database Connector Setup Wizard

The Setup Wizard will install RiskVision Exploit Database Connector on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

The Exploit Database Connector Setup wizard.

3. Click **Next**.

4. Click **I accept the terms in the License Agreement**


RiskVision Exploit Database Connector Setup

End-User License Agreement

Please read the following license agreement carefully.

Resolver RiskVision End User Software License Agreement

This Resolver RiskVision ("RiskVision") End User Software License Agreement ("Agreement") is a legal agreement between you individually if you are agreeing to it in your own capacity, or if you are authorized to acquire the Software on behalf of your company or another organization, between the company or organization for whose benefit you act ("Customer"), and Resolver SOAR LLC ("Company").

BY CLICKING ON THE "ACCEPT" BUTTON OR DOWNLOADING OR

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

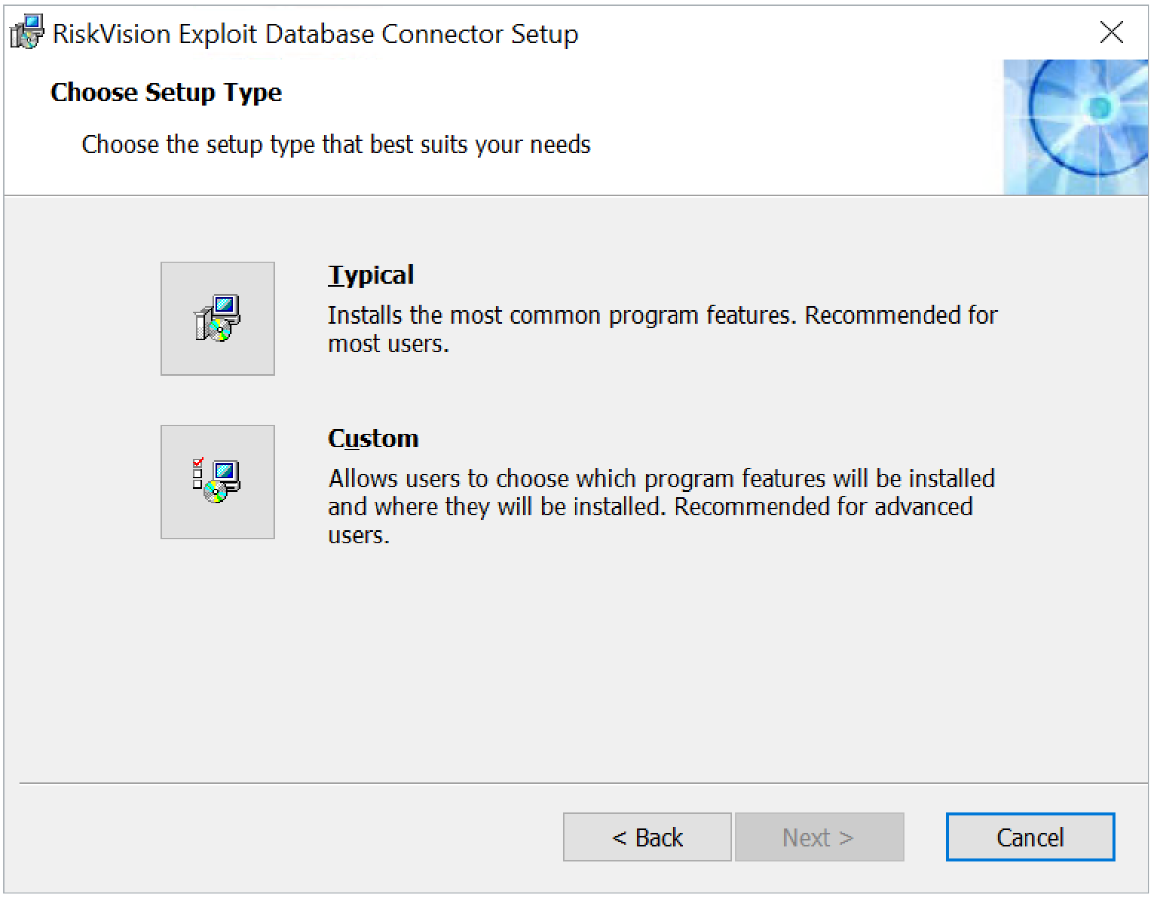
The End-User License Agreement.

5. Click **Next**.

6. Choose one of the following:

    - **Typical**: Installs the connector in the **C:\Program Files (x86)\Agiliance\** folder by default.

    - **Custom**: Specify the desired location of the connector.



RiskVision Exploit Database Connector Setup

Choose Setup Type

Choose the setup type that best suits your needs

Typical

Installs the most common program features. Recommended for most users.

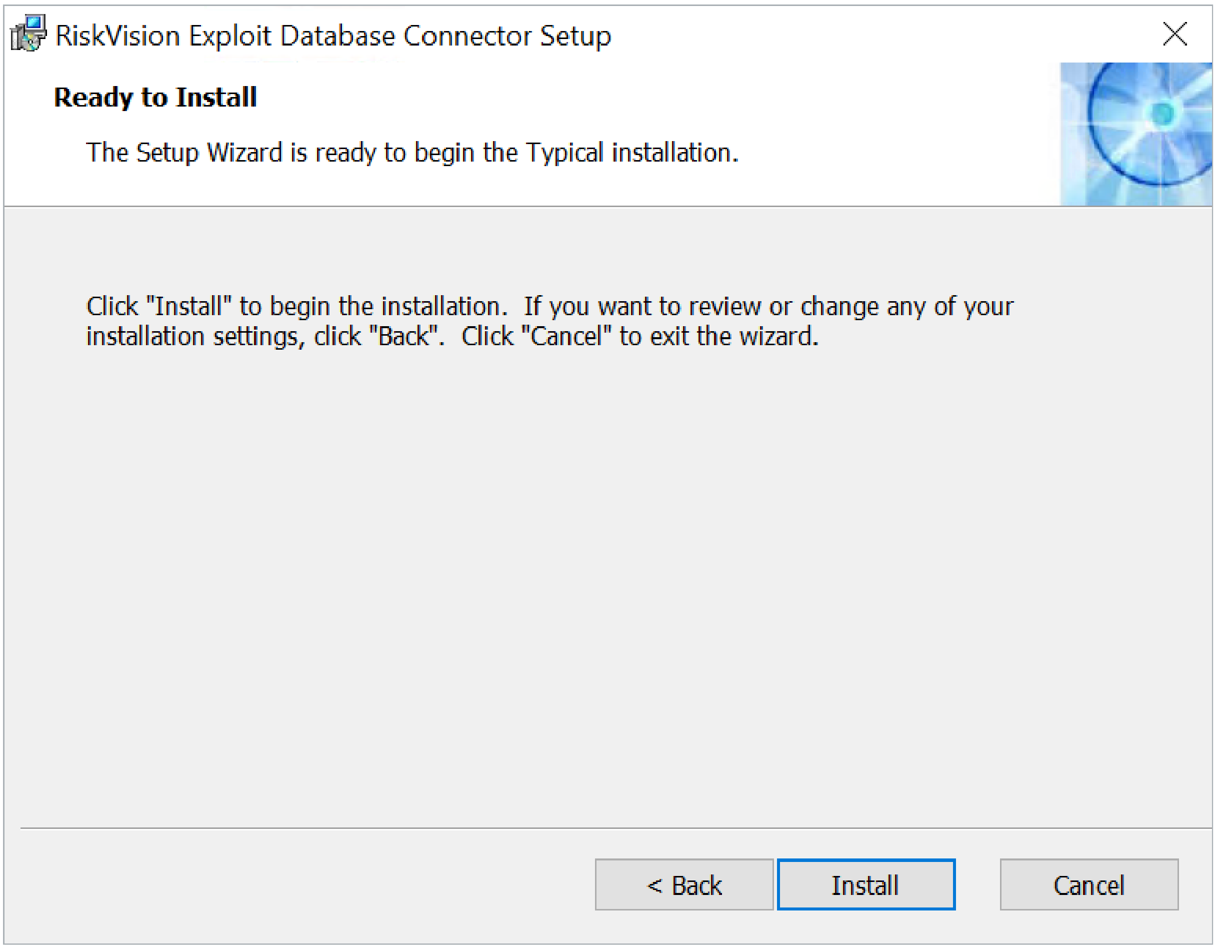
Custom

Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

The Choose Setup Type screen.

7. Click **Next**.

8. Click **Install**.



RiskVision Exploit Database Connector Setup

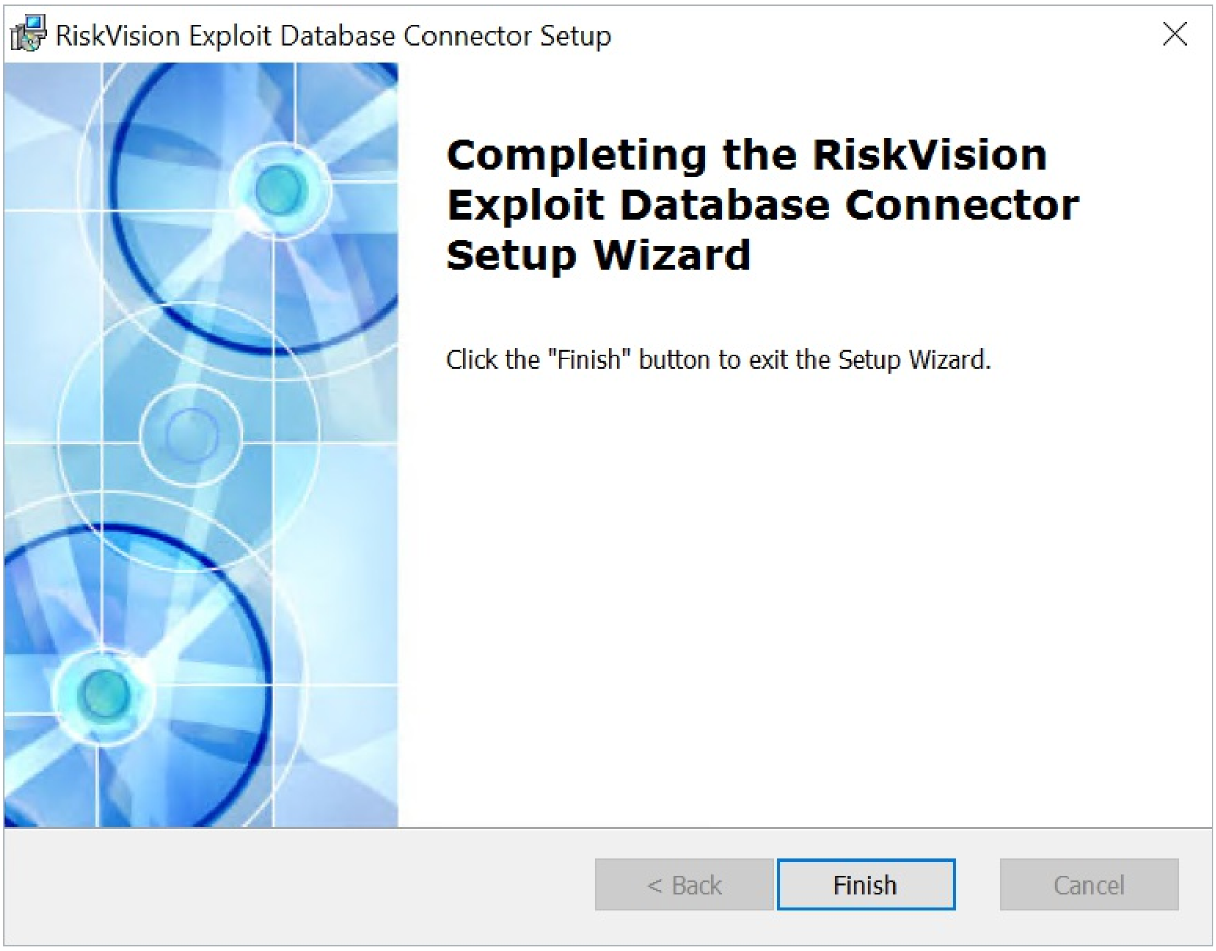
Ready to Install

The Setup Wizard is ready to begin the Typical installation.

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

The Ready to Install screen.

9. Click **Finish** to exit the wizard once the installation is complete.


RiskVision Exploit Database Connector Setup

Completing the RiskVision Exploit Database Connector Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

The Completion screen.

Uninstall the NVD Connector

GS: Do we need this article? The Exploit Database connector guide doesn't have one, and it seems like common sense to me. If we do need it, should I put a version of it in the Exploit Database connector guide?

In order to upgrade from an older version of the NVD connector to the newest one, customers must first uninstall their current version of the connector. Once the old version has been removed, the user must install the latest version of the **RiskVisionNVDConnector.msi** file obtained from Resolver Support.

To uninstall the NVD connector:

1. Open the **Control Panel** on the computer where the connector has been installed.

2. Click **Programs and Features**.

3. Select **Resolver NVD Connector** and click **Uninstall**. GS: Is this the right name?

4. Click **Yes**.

Starting, Stopping & Restarting the NVD Connector

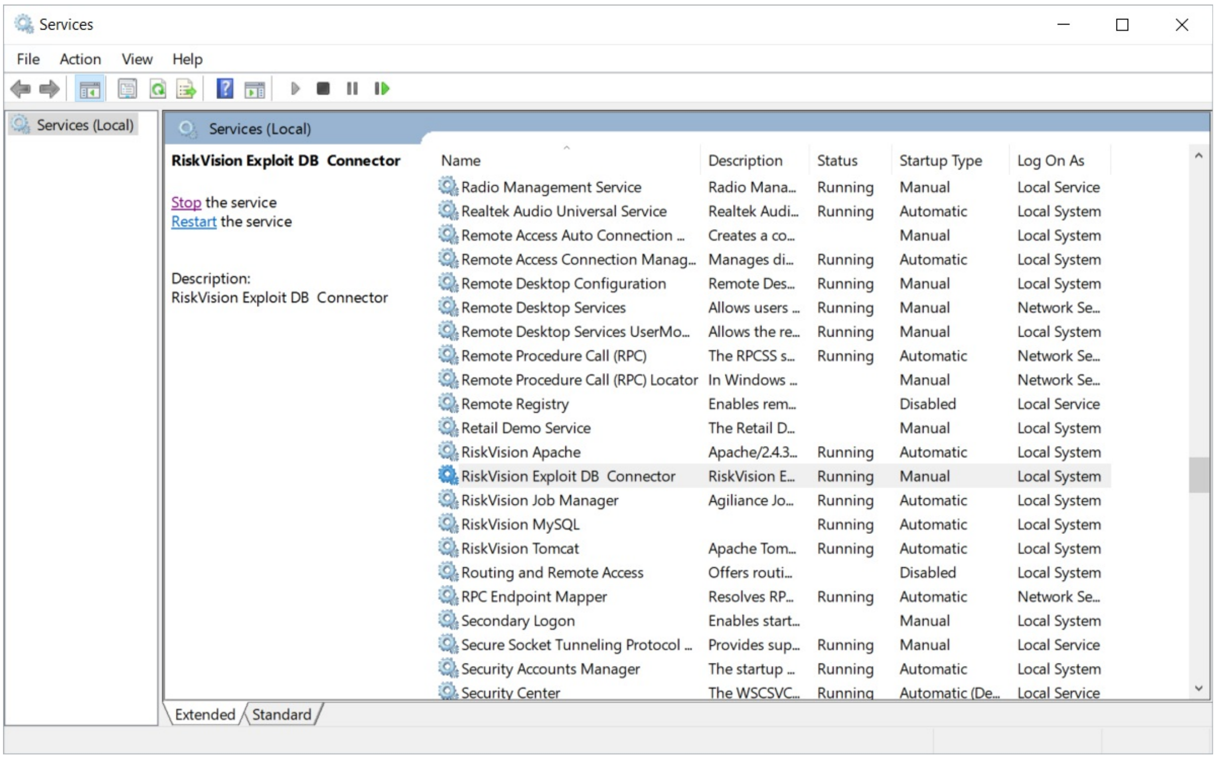
Installing the NVD connector sets it up as a Microsoft Windows service; however, by default, the Microsoft Windows service will not be started. In order to start, stop, or restart the service, certain steps must be taken. GS: These steps were copied from the Exploit Database connector guide because Mounika had updates to make from the pdf guide. Are these steps still correct for NVD?

To start, stop, or restart the NVD connector:

1. Go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools**.

2. Click **Services**.

3. Right-click **RiskVision NVD Connector**, and select either **Start**, **Stop**, or **Restart**. GS: Can I get a screenshot with the NVD Connector in it (preferably a similar size to this one)?



RiskVision Exploit DB Connector

Stop the service
Restart the service

Description:
RiskVision Exploit DB Connector

Name	Description	Status	Startup Type	Log On As
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Realtek Audio Universal Service	Realtek Audi...	Running	Automatic	Local System
Remote Access Auto Connection ...	Creates a co...		Manual	Local System
Remote Access Connection Manag...	Manages di...	Running	Automatic	Local System
Remote Desktop Configuration	Remote Des...	Running	Manual	Local System
Remote Desktop Services	Allows users ...	Running	Manual	Network Se...
Remote Desktop Services UserMo...	Allows the re...	Running	Manual	Local System
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network Se...
Remote Procedure Call (RPC) Locator	In Windows ...		Manual	Network Se...
Remote Registry	Enables rem...		Disabled	Local Service
Retail Demo Service	The Retail D...		Manual	Local System
RiskVision Apache	Apache/2.4.3...	Running	Automatic	Local System
RiskVision Exploit DB Connector	RiskVision E...	Running	Manual	Local System
RiskVision Job Manager	Agiliance Jo...	Running	Automatic	Local System
RiskVision MySQL		Running	Automatic	Local System
RiskVision Tomcat	Apache Tom...	Running	Automatic	Local System
Routing and Remote Access	Offers routi...		Disabled	Local System
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network Se...
Secondary Logon	Enables start...		Manual	Local System
Secure Socket Tunneling Protocol ...	Provides sup...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSVC...	Running	Automatic (De...	Local Service

The RiskVision Exploit DB Connector in Services.

Configuring the RiskVision Host Settings

If you installed the connector on the same host as RiskVision, the connector will automatically display on the**Administration** > **Connectors** page. By default, the connector uses loopback (localhost) on port 443 to communicate with the RiskVision server. When you install the connector on a different host or use a port other than 443, you must configure the RiskVision application host information. GS: The below instructions were copied from the Exploit Database connector guide, due to their similarity. Let me know if any step of these are wrong.

To change the RiskVision host settings:

1. Open the **/NVD Connector/cfg/connector.properties** file in the connector host.
2. Point the `server_host` property to the RiskVision host name or IP adress.
3. Save the file.
4. Restart the connector service.

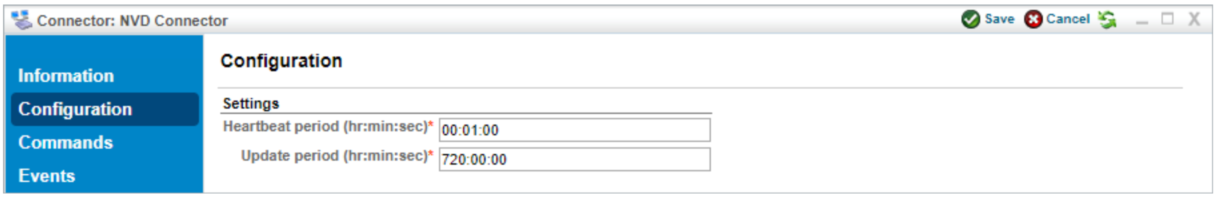
Configuring the NVD Connector

Before the NVD connector can send any messages to the RiskVision Server, it must first be manually authenticated. Users may also wish to edit the connectors heartbeat and update settings. A description of each setting is below:

SETTING	DEFAULT VALUE	DESCRIPTION
Heartbeat period (hr:min:sec)	1 minute	Send messages, if any, and report the health of the connector.
Update period (hr:min:sec)	720 hours	Scan the file where the range is 60 and above.

To configure the connector:

1. In the **RiskVision Administration** application, click on **Administration** > **Connectors**.
2. Select the **NVD Connector** to open its details page.
3. Click the **Configuration** tab.
4. Click **Edit** to change the **Heartbeat period** and **Update period** as desired.

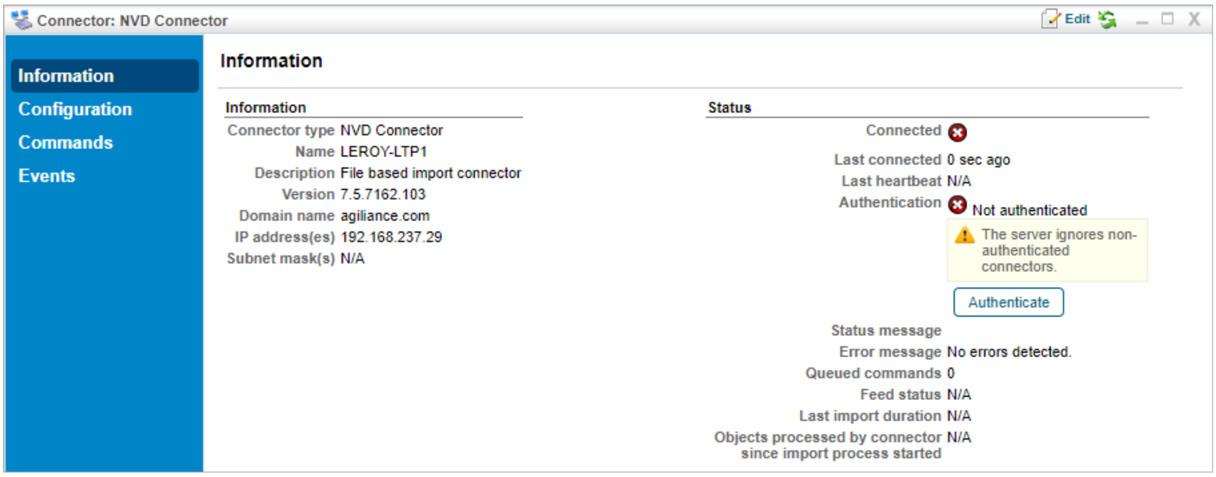


Heartbeat period (hr:min:sec)* 00:01:00

Update period (hr:min:sec)* 720:00:00

The Edit Configuration page.

5. Navigate to the **Information** tab.
6. Click **Authenticate** on the right-hand side of the screen.



Connector type NVD Connector

Name LEROY-LTP1

Description File based import connector

Version 7.5.7162.103

Domain name agiliance.com

IP address(es) 192.168.237.29

Subnet mask(s) N/A

Connected ☒

Last connected 0 sec ago

Last heartbeat N/A

Authentication ☒ Not authenticated

The server ignores non-authenticated connectors.

Status message

Error message No errors detected.

Queued commands 0

Feed status N/A

Last import duration N/A

Objects processed by connector since import process started N/A

The NVD Connector's details page.

Using the Connector.properties File

GS: What properties does this file maintain? The original pdf guide didn't say.

The actions that can be taken with the **connector.properties** file depend on where the file was installed:

- **Installed on the same host as the Resolver RiskVision server:** The default settings should work unless the https server port is set to a number other than 443. GS: What should the user do if it is set to a different number?
- **Remotely installed:** Edit the **connector.properties** file as desired by using a text editor. Uncomment any desired settings, edit the `server_host` property settings, and specify the RiskVision server IP or hostname (should be resolvable to an IP over the network). Reset the connector for the changes to take effect.

Using the Connector.file.properties File

The **connector.file.properties** file maintains monitoring folder, server queue size, filter, and auto downloading of CPE, CVE, and CWE. The following show how these properties can be edited.

Monitor Folder

By default the **folder_monitor_folder** is located in **/Agiliance/NVD Connector/data**. However, this location can be changed. GS: Is this the only way the user can edit the Monitor Folder setting?

To edit the monitor folder's location:

1. Open the **connector.file.properties** file with a text editor.
2. Change the following setting as desired:
   - `folder_monitor_folder =`
3. Reset the connector for changes to take effect.

Queue Size

By default, the NVD connector will not send an import request to the server until the queue size is over twenty. This number can be changed.

To edit the queue size:

1. Open the **connector.file.properties** file with a text editor.
2. Change the following setting as desired:
   - `server_queue_size = 20`
3. Reset the connector for changes to take effect.

Filter

By default, the filter xml file will be installed in **/Agiliance/NVD Connector/filter**. All files from the NVD connector will be stored in this location before being processed. To change this location, move the xml file to the desired location. Reset the connector for changes to take effect.

Automatic Download of CPE, CVE & CWE Files

GS: Why would a user want to automatically download this information? The original documentation didn't say.

To enable the automatic download of CPE, CVE, and CWE files:

1. Open the **connector.file.properties** file with a text editor.
2. **Optional:** To automatically download the CPE, CVE, or CWE files, uncomment the following line:
   - `file_listeners=com.agiliance.connector.nvd.CveListener com.agiliance.connector.nvd.CpeListener com.agiliance.connector.nvd.CweListener`
3. **Optional:** To only download one of the above files, uncomment the following line: GS: Can they only download CPE files, or can they choose any file type to download?
   - `file_listeners= com.agiliance.connector.nvd.CpeListener`
4. Set the following lines as desired:
   - `autoFeedOption=`

- `NvdCveUrl=[YYYY].xml" class="external-link" rel="nofollow">[YYYY].xml" class="external-link" rel="nofollow">http://static.nvd.nist.gov/feeds/xml/cve/nvdcve-2.0-[YYYY].xml`

- `NvdCpeUrl=http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.3.xml`

- `NvdCweUrl=http://cwe.mitre.org/data/xml/cwec_v2.5.xml.zip`

- `fromYear=`

- `toYear=`

5. Reset the connector for changes to take effect.

CVE Download Interval

The NVD connector can be configured to download CVE files at a rate of every two hours. Because the connector is not capable of auto-identifying newly added CVEs in NVD websites and processes unless it reaches the next download interval, two hours is considered the optimal interval time.

To change the CVE download interval:

1. Open the **connector.file.properties** file with a text editor.

2. Change the following setting as shown:

    - `updatePeriod = 7200000`

3. Reset the connector for changes to take effect.

Using the Log4j.properties File

The **log4j.properties** file maintains the connector's logging properties. In order to keep the connector running as normal, it is recommended that the user debugs this file periodically. GS: Are the below steps correct?

To debug the log4j.properties file:

1. Open the **log4j.properties** file with a text editor.
2. Change the following setting as as shown:
    - `Log4j.rootLogger=DEBUG,C,F`
3. Reset the connector for the changes to take effect.

Using the Fileconnector.metadata File

The **fileconnector.metadata** file provides additional, static information about the parsed data that is not available within the report files. GS: I didn't understand the below text so I copied it as is. Please let me know if anything needs to be corrected.

In all file based connectors to load the metadata properties, use **java.util.Properties** class. It will treat the backslash as (\) escape character. If you try entering the folder path as `<\workshop>` , it will render the path as .

If you use double slash (\\) or forward slash (/), the property will not throw any exception. This will work only if the path is root.

Example for root drive:

If the root path is , then the path will be `/workshop/test.groovy` .

The condition above is not applicable if the path is other than root drive.

Example for drives other than the root drive:

If the path is , then the path will be .

The following metadata properties are available:

NAME	DESCRIPTION
ScriptName	This flag sets the script name for groovy based parser. For example, `ScriptName=NessusScript.groovy`
ScriptFolder	Introduced since 3.x; this flag sets the path for scripting parser to look for groovy scripts. For example, `ScriptFolder=C:/server/cfg/scripts.` If this flag is not set, the parser will look at the default location to get the scripts (**NVD Connector/cfg**).

NVD Connector Directories

When the NVD connector is started, it creates a directory structure of sub-directories to hold the third-party files for processing. The NVD connector's default directory structure is as follows:

- `connector.remote.cve`
    - `new/`
    - `old/`
    - `wip/`

During folder creation, the installer will add a default metadata file (**fileconnector.metadata**) and an ip/host lookup file (**ip_lookup.csv**) in each of the new folders.

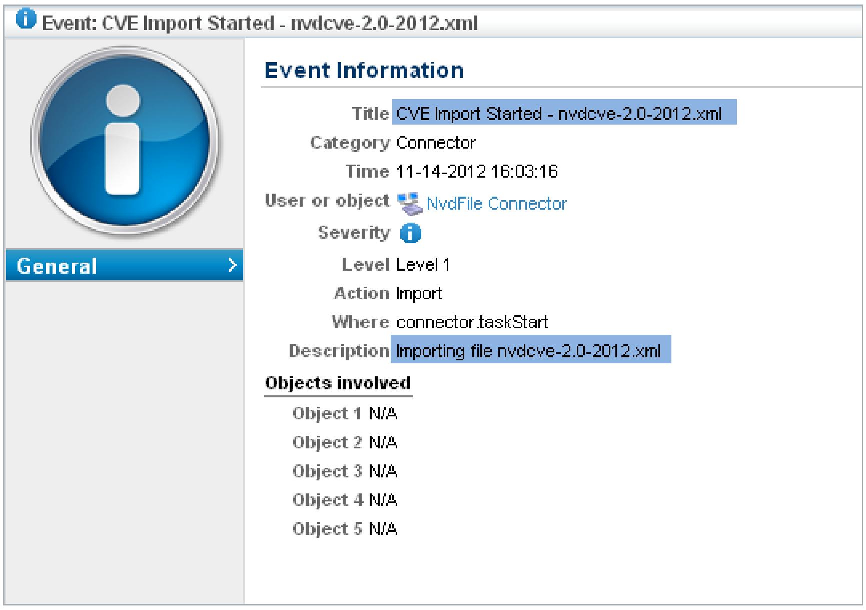
During the processing of transferred files, a copy of the file is moved from the **new** directory to the **wip** directory for processing. The **old** directory is used to archive transfer files that have already been processed. Copy the new integration files to the **new** folder under the appropriate NVD folder. GS: I don't understand this last sentence, but is this correct?

NVD Connector Events

The NVD connector makes use of two new connector events to aid in reconciling the data being sent to the RiskVision server. The two events are **CVE Import Started** and **CVE Import Completed** and will only appear for the NVD connector. GS: The below screenshots are placeholders. Can I please have updated screenshots with the new UI?

CVE Import Started

This event is triggered as soon as the import starts. It displays the name of the imported file and time.



Event: CVE Import Started - nvdcve-2.0-2012.xml

Event Information

Title CVE Import Started - nvdcve-2.0-2012.xml

Category Connector

Time 11-14-2012 16:03:16

User or object NvdFile Connector

Severity

Level Level 1

Action Import

Where connector.taskStart

Description Importing file nvdcve-2.0-2012.xml

Objects involved

Object 1 N/A

Object 2 N/A

Object 3 N/A

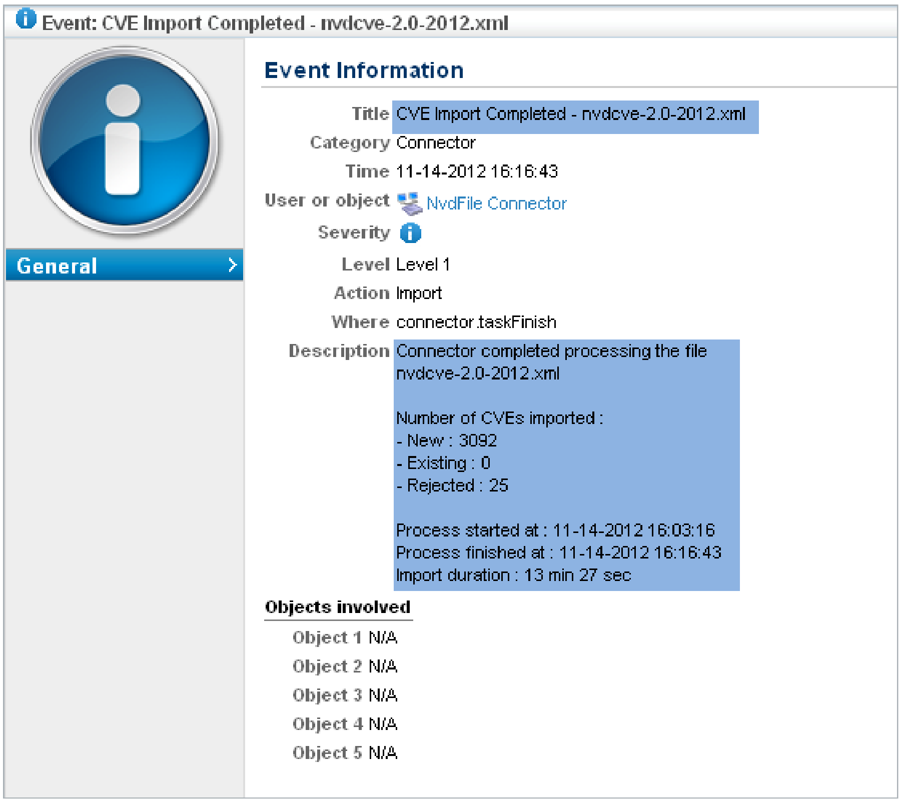
Object 4 N/A

Object 5 N/A

The CVE Import Started event.

CVE Import Completed

This event provides detailed data on the number of vulnerabilities received by the RiskVision server. GS: What triggers it?



Event: CVE Import Completed - nvdcve-2.0-2012.xml

Event Information

Title	CVE Import Completed - nvdcve-2.0-2012.xml
Category	Connector
Time	11-14-2012 16:16:43
User or object	NvdFile Connector
Severity	ⓘ
Level	Level 1
Action	Import
Where	connector.taskFinish
Description	Connector completed processing the file nvdcve-2.0-2012.xml Number of CVEs imported : - New : 3092 - Existing : 0 - Rejected : 25 Process started at : 11-14-2012 16:03:16 Process finished at : 11-14-2012 16:16:43 Import duration : 13 min 27 sec

Objects involved

Object 1	N/A
Object 2	N/A
Object 3	N/A
Object 4	N/A
Object 5	N/A

The CVE Import Completed event.

Understanding the InterfaceSubnet Property

GS: Does this article belong in the Connector Operation folder? It feels like kind of a random inclusion and like it would belong more in the table in the fileconnector.metadata article. If the below information is correct, can I move it there?

The InterfaceSubnet property is a metadata property that indicates the range of user subnets. This property may include multiple subnets strings separated by a comma. For example, the property could read 192.*.*.*/24, 10.10.*.*/16.

Troubleshooting the NVD Connector

In the event that a user runs into problems while using the NVD connector, there are a few steps that can be taken. The below steps should help resolve most common errors that the user will encounter.

To troubleshoot most common issues:

1. Ensure that the connector is authenticated.
2. Ensure that the correct file been used to import data.
3. Confirm that there are no errors or exceptions in the connector's log.
4. Allow approximately two minutes for the connector to collect all required information from the file.
5. Confirm that the RiskVision server did not report any connector errors. In the event of an error, resolve them by providing proper configuration details.

If problems persist:

1. Stop the connector.
2. Delete all the files from the **\data\old** folder.
3. Copy the correct file in the **\data\new** folder. GS: What is the correct file?
4. Start the connector and provide a couple of heartbeat cycles to see if hierarchies start showing up in the connector log as well as in RiskVision itself.

If all of the above steps fail, contact Resolver Support.

The FireEye ISight Connector

Once a day, the FireEye ISight connector accesses the FireEye database and imports a .json file containing a risk report to populate RiskVision's Threats table. Users can change the frequency of this import using the **FireEye ISight Connector** job if required.

The ISight connector is used to import the following threat types: **Threats**, **Vulnerabilities**, and **Malware**. The connector fills in the following fields for each threat:

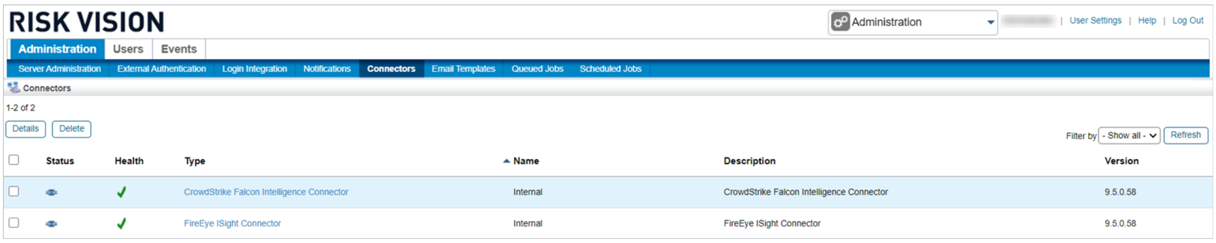
- **Type**
- **Source**
- **Identifier**
- **Title**
- **Description**
- **Published Date**
- **Last Updated**
- **Owner**
- **Severity**
- **Likelihood**
- **Risk**
- **Risk Rating**
- **Exploit Rating**
- **Exploitation in the Wild**

To set up and run the FireEye ISight connector:

1. Navigate to the **\config** folder and add a valid license with the `connector.remote.fireeye.isight` connector set to true.
2. ~~Download the SQUID Proxy.~~
3. ~~Install the **SQUID Proxy** server onto the machine that will be using RiskVision.~~
4. ~~To enable the proxy:~~
   a. ~~Navigate to **\config\agiliance.properties**.~~
   b. ~~Make the following changes to the file:~~

```
~~Proxy.useProxyServer = true~~
~~Proxy.serverHost = Server Hostname~~
~~Proxy.serverPort = 3128~~
~~Proxy.httpType = http~~
```

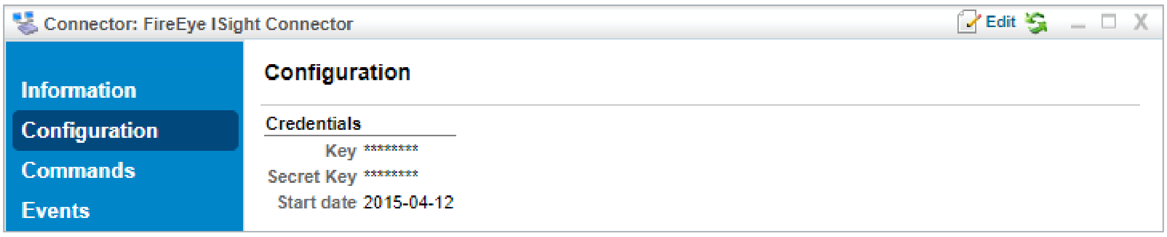
   c. ~~Restart the RiskVision Tomcat service to apply these change.~~
5. In the **RiskVision Administration** application, click on **Administration**, then **Connectors**.



☐	Status	Health	Type	▲ Name	Description	Version
☐		✓	CrowdStrike Falcon Intelligence Connector	Internal	CrowdStrike Falcon Intelligence Connector	9.5.0.58
☐		✓	FireEye ISight Connector	Internal	FireEye ISight Connector	9.5.0.58

The Connectors page.

6. Click on **FireEye ISight Connector** and then click **Details**.
7. Click on the **Configuration** tab and then **Edit**.



Configuration

Credentials

Key ********

Secret Key ********

Start date 2015-04-12

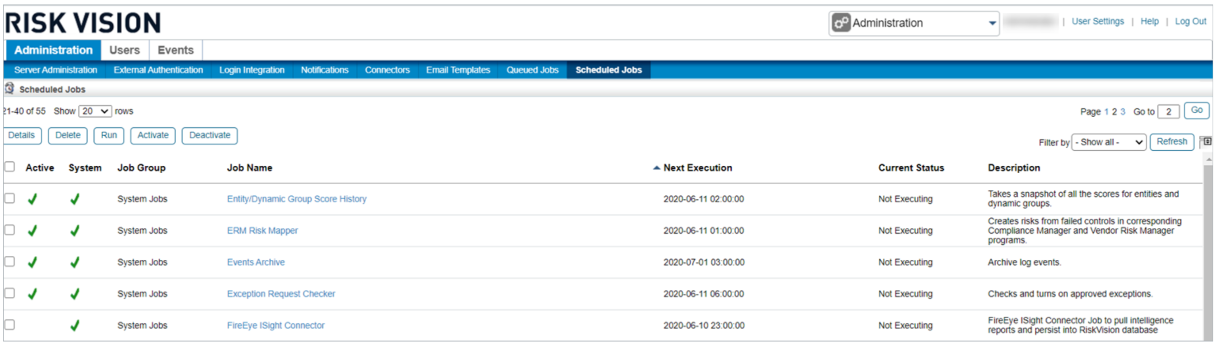
The Configuration tab for the FireEye ISight Connector.

a. Enter the **Key** and **Secret Key**.

b. Specify the start date from which the threat data should be downloaded.

8. Click **Save**.

9. Click on the **Scheduled Jobs** tab.



21-40 of 55 Show 20 rows

Page 1 2 3 Go to 2

Filter by - Show all -

□	Active	System	Job Group	Job Name	Next Execution	Current Status	Description
□	✓	✓	System Jobs	Entity/Dynamic Group Score History	2020-06-11 02:00:00	Not Executing	Takes a snapshot of all the scores for entities and dynamic groups.
□	✓	✓	System Jobs	ERM Risk Mapper	2020-06-11 01:00:00	Not Executing	Creates risks from failed controls in corresponding Compliance Manager and Vendor Risk Manager programs.
□	✓	✓	System Jobs	Events Archive	2020-07-01 03:00:00	Not Executing	Archive log events.
□	✓	✓	System Jobs	Exception Request Checker	2020-06-11 06:00:00	Not Executing	Checks and turns on approved exceptions.
□		✓	System Jobs	FireEye ISight Connector	2020-06-10 23:00:00	Not Executing	FireEye ISight Connector Job to pull intelligence reports and persist into RiskVision database

The Scheduled Jobs page.

10. Select the **FireEye ISight Connector** scheduled job and click **Activate**, then **Run**. ~~This will import threats through the proxy into RiskVision.~~

11. After successfully importing threats, click **Deactivate**.

To enable a proxy server:

1. Navigate to **\config\agiliance.properties**.

2. Make the following changes to the file:

```
Proxy.useProxyServer = true
Proxy.serverHost = Server Hostname
Proxy.serverPort = 3128
Proxy.httpType = http
```

3. Restart the RiskVision Tomcat service to apply these change.

> ⚠ If the proxy has been turned off or configured improperly, you will see a message that reads: "Connection refused for proxy server: java.net.ConnectException: Connection refused: connect".

To troubleshoot common issues:

1. Ensure that the connector is authenticated.

2. Confirm that there are no errors or exceptions in the RiskVision Catalina log.

3. If there are any errors in the RiskVision Catalina log, verify that the connector is using the correct key and secret key to access the reports.

The CrowdStrike Falcon Intelligence Connector

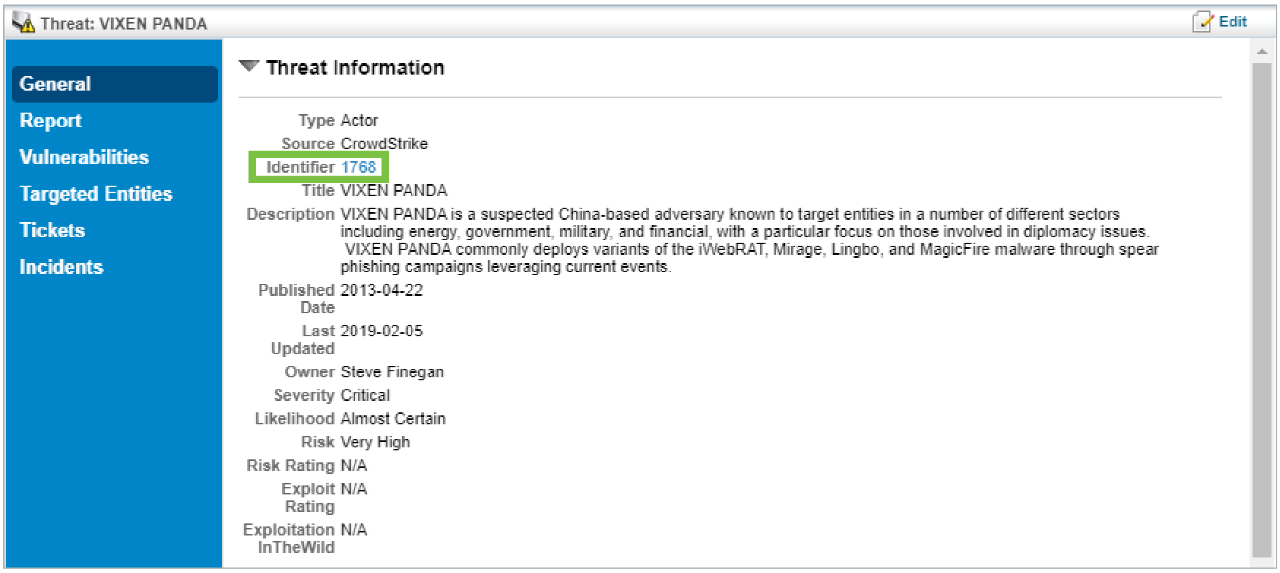
Once a day, the CrowdStrike Falcon Intelligence connector accesses the CrowdStrike database and imports a .json file containing a risk report to populate RiskVision's Threats table. Users can change the frequency of this import using the **CrowdStrike Falcon Intelligence Connector** job if required.

The Falcon Intelligence connector is used to import the following threat types: **Actors**, **Intelligence**, **Tippers**, **Notices**, and **Periodic Reports**. The connector fills in the following fields for each threat:

- Type
- Source
- Identifier
- Title
- Description
- Published Date
- Last Updated
- Owner
- Severity
- Likelihood
- Risk

While the **Risk Rating**, **Exploit Rating**, and **Exploitation in the Wild** fields will be present in RiskVision, the CrowdStrike Falcon Intelligence connector will not fill them in.

The Falcon Intelligence connector only provides RiskVision with an annotated report. In order to view the full report, click the Identifier number on the Threat's General page to log into the CrowdStrike webpage.



Type Actor
Source CrowdStrike
Identifier 1768
Title VIXEN PANDA
Description VIXEN PANDA is a suspected China-based adversary known to target entities in a number of different sectors including energy, government, military, and financial, with a particular focus on those involved in diplomacy issues. VIXEN PANDA commonly deploys variants of the iWebRAT, Mirage, Lingbo, and MagicFire malware through spear phishing campaigns leveraging current events.
Published Date 2013-04-22
Last Updated 2019-02-05
Owner Steve Finegan
Severity Critical
Likelihood Almost Certain
Risk Very High
Risk Rating N/A
Exploit Rating N/A
Exploitation InTheWild N/A

The Identifier number on a Threat's General page.

To set up and run the CrowdStrike Falcon Intelligence connector:

1. Navigate to the **\config** folder and add a valid license with the `connector.remote.crowdstrike.falconintelligence` connector set to true.
2. ~~Download the SQUID Proxy.~~
3. ~~Install the **SQUID Proxy** server onto the machine that will be using RiskVision.~~
4. ~~To enable the proxy:~~

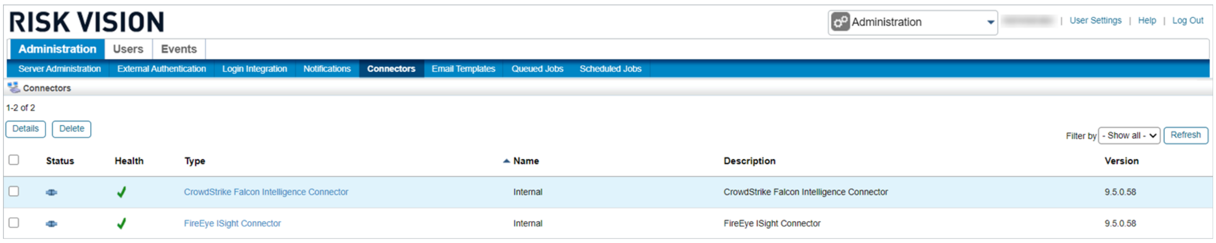
   a. ~~Navigate to \config\agiliance.properties.~~

   b. ~~Make the following changes to the file:~~

```
~~Proxy.useProxyServer = true~~
~~Proxy.serverHost = Server Hostname~~
~~Proxy.serverPort = 3128~~
~~Proxy.httpType = http~~
```

   c. ~~Restart the RiskVision Tomcat service to apply these change.~~

5. In the **RiskVision Administration** application, click on **Administration**, then **Connectors**.

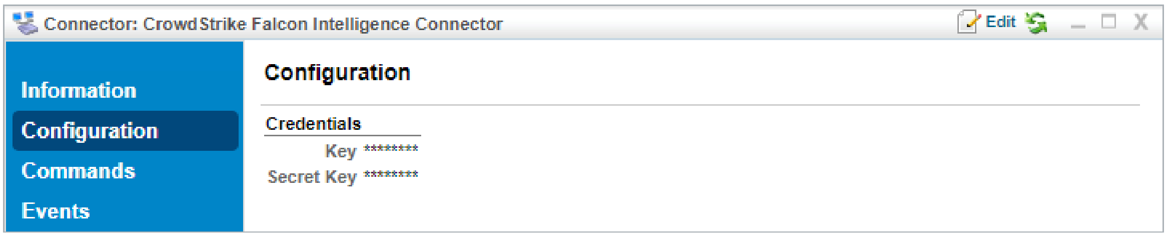


☐	Status	Health	Type	▲ Name	Description	Version
☐		✓	CrowdStrike Falcon Intelligence Connector	Internal	CrowdStrike Falcon Intelligence Connector	9.5.0.58
☐		✓	FireEye ISight Connector	Internal	FireEye ISight Connector	9.5.0.58

The Connectors page.

6. Click on **CrowdStrike Falcon Intelligence Connector** and then click **Details**.

7. Click on the **Configuration** tab and then **Edit**.



Configuration

Credentials

Key ********

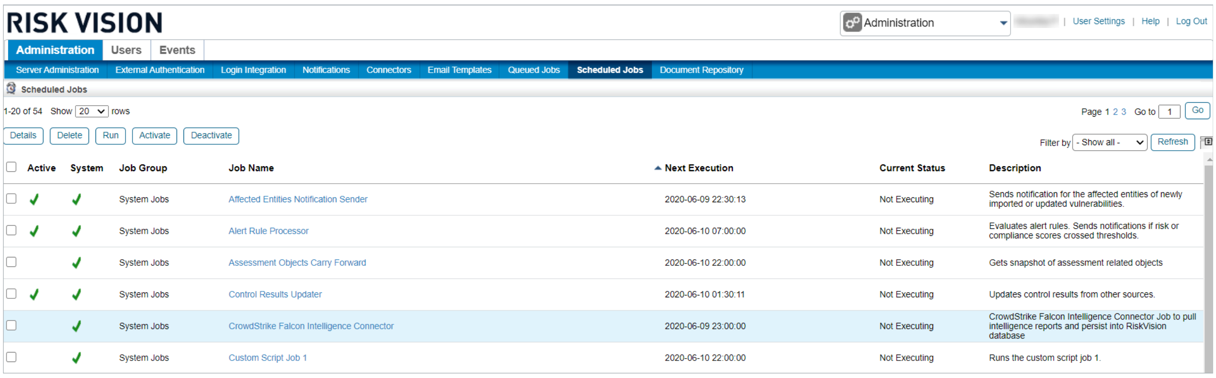
Secret Key ********

The Configuration tab for the CrowdStrike Falcon Intelligence Connector.

   a. Enter the **Key** and **Secret Key**.

8. Click **Save**.

9. Click on the **Scheduled Jobs** tab.



☐	Active	System	Job Group	Job Name	▲ Next Execution	Current Status	Description
☐	✓	✓	System Jobs	Affected Entities Notification Sender	2020-06-09 22:30:13	Not Executing	Sends notification for the affected entities of newly imported or updated vulnerabilities.
☐	✓	✓	System Jobs	Alert Rule Processor	2020-06-10 07:00:00	Not Executing	Evaluates alert rules. Sends notifications if risk or compliance scores crossed thresholds.
☐		✓	System Jobs	Assessment Objects Carry Forward	2020-06-10 22:00:00	Not Executing	Gets snapshot of assessment related objects
☐	✓	✓	System Jobs	Control Results Updater	2020-06-10 01:30:11	Not Executing	Updates control results from other sources.
☐		✓	System Jobs	CrowdStrike Falcon Intelligence Connector	2020-06-09 23:00:00	Not Executing	CrowdStrike Falcon Intelligence Connector Job to pull intelligence reports and persist into RiskVision database
☐		✓	System Jobs	Custom Script Job 1	2020-06-10 22:00:00	Not Executing	Runs the custom script job 1.

The Scheduled Jobs page.

10. Select the **CrowdStrike Falcon Intelligence Connector** scheduled job and click **Activate**, then **Run**. ~~This will import threats through the proxy into RiskVision.~~

11. After successfully importing threats, click **Deactivate**.

To enable a proxy server:

1. Navigate to **\config\agiliance.properties**.

2. Make the following changes to the file:

   ```
   Proxy.useProxyServer = true
   Proxy.serverHost = Server Hostname
   Proxy.serverPort = 3128
   Proxy.httpType = http
   ```

3. Restart the RiskVision Tomcat service to apply these change.

   > ⚠ If the proxy has been turned off or configured improperly, you will see a message that reads: "Connection refused for proxy server: java.net.ConnectException: Connection refused: connect".

To troubleshoot common issues:

1. Ensure that the connector is authenticated.

2. Confirm that there are no errors or exceptions in the RiskVision Catalina log.

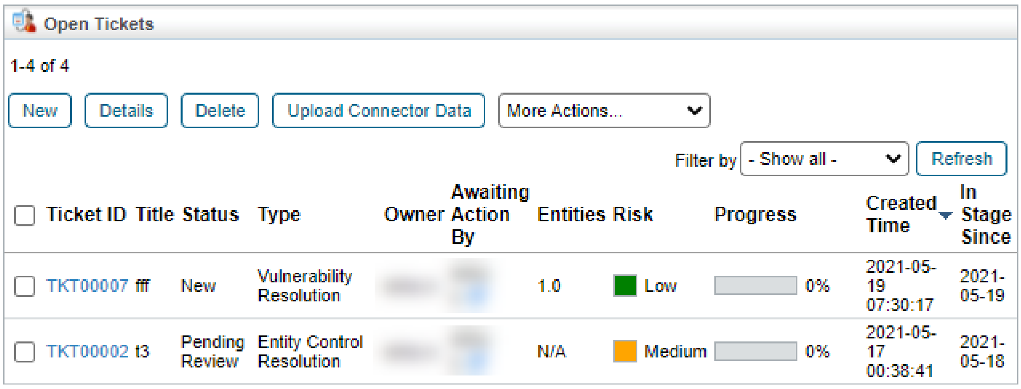
3. If there are any errors in the RiskVision Catalina log, verify that the connector is using the correct key and secret key to access the reports.

Upload Connector Data

Connector input files can be manually uploaded to a specified folder in RiskVision. This is useful in the event that a particular file was missed by the connector syncing, or if it needs to be urgently uploaded to RiskVision before the next scheduled sync. Only users with the **Threats and Vulnerabilities - Manage** permission can upload connector data.

To upload connector data:

1. Open **agiliance.properties** file.
2. Change the following properties as listed below:
   - `ConnectorImport.enableConnectorDataUpload=true`
   - `ConnectorImport.allowedDataFileTypes=xml,csv`
   - `ConnectorImport.allowedSourceTypes=`
   - `ConnectorImport.destinationFolder.=`
3. Open RiskVision.
4. Navigate to **Home** > **Tickets**.

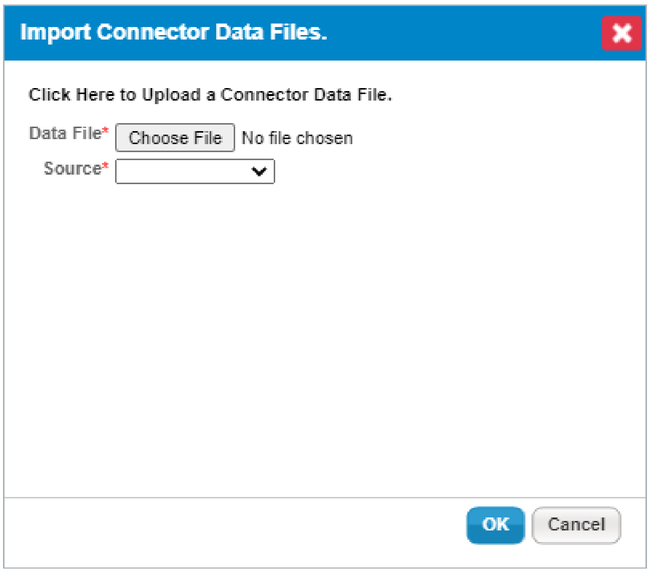


Filter by - Show all -

☐	Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
☐	TKT00007	fff	New	Vulnerability Resolution	[redacted]	[redacted]	1.0	🟩 Low	0%	2021-05-19 07:30:17	2021-05-19
☐	TKT00002	t3	Pending Review	Entity Control Resolution	[redacted]	[redacted]	N/A	🟧 Medium	0%	2021-05-17 00:38:41	2021-05-18

The Tickets page.

5. Click **Upload Connector Data** to open the **Import Connector Data Files** window.



Click Here to Upload a Connector Data File.

Data File* No file chosen

Source*

The Import Connector Data Files window.

6. Click **Choose File** to browse for the desired input file on your computer.

7. Select the file source from the **Source** field.

8. Click **OK**.

9. Verify that the desired file has been uploaded to the destination folder.

Viewing Queued Jobs

Queued Jobs are jobs--such as reports--that are currently in progress or that will be performed in the future. And to view queued jobs, the Queued Job View permission is assigned to the default Administrator role in RiskVision.

To view queued jobs:

1. In the Administration application, go to **Administration > Queued Jobs**.
2. The display shows all queued jobs, with columns for **Type**, **Submitted by**, **Status**, **Progress**, **Priority**, **Result**, and **Is Persistent**. Click a column heading to sort the table by that column.
3. To view a subset of table rows, select from the **Filter By** drop-down list. You can filter on **Type**, **Submitted by**, **Status**, **Priority**, or **Result**.
4. Click **Refresh** to display the current contents of the database if other users may have added jobs while you have been viewing the queue.

Displaying Queued Job Details

Queued Jobs are jobs--such as reports--that are currently in progress or that will be performed in the future. The Queued Jobs page shows some information about all Queued Jobs, but you can drill down to see more detail.

To display the details of a queued job:

- In the Administration application, go to **Administration** > **Queued Jobs**.
- The display shows all queued jobs. Check the box next to the job of interest.
- Click **Details**.

  The queued job details are displayed.

About Scheduled Jobs

Jobs include running a report, creating a new policy and control framework, or other task that may take a significant amount of time to complete.

Run a report manually or schedule a report to run at a specific time or interval to create a report job. The Queued Jobs page displays information about pending jobs. For more information, see Viewing Queued Jobs.

About System Jobs

System Jobs are regularly-scheduled tasks that the RiskVision solution performs routinely in the background. Jobs in the System Jobs group can be viewed along with other queued jobs, such as reports. Jobs including system jobs and scheduled reports can be accessed by other users if they have a user role with the Scheduled Job View permission. In order to activate, deactivate, delete, run, or reschedule a job, you will need to have the Scheduled Job Manage permission along with the Scheduled Job View permission.

To run a system job now, check the System Job and click **Run**.

To enable or disable a system job, check the System Job and click **Activate/Deactivate**.

Click on an active system job to view more details, including:

- **Job Start**. When the job was created
- **Last Executed**. When the job was last run
- **Next Executions**. A list of upcoming dates and times when the job will be run

Default System Jobs

System job	Description	Job Details
Affected Entities Notification Sender	Sends notification for the affected entities of newly imported or updated vulnerabilities.	From the "Threat Management preferences" page: If Automatically create ticket is set to**Yes**, then this job creates tickets for each vulnerability (which has affected entities). If Acknowledge the vulnerability when the tickets are automatically created is set to **Yes**, then this job will acknowledge each vulnerability (which has affected entities). For all the affected entities , system notifications will be sent. Default value **= "enabled"** To enable this job set com..job.effectedEntities NotificationSenderJob.disable= true
Alert Rule Processor	Evaluates alert rules and sends notifications if risk or compliance scores have crossed set thresholds.	
Assessment Objects Carry Forward	Gets snapshot of assessment related objects	The Assessment Objects Carry Forward job is required to archive questionnaire data and objects attached to the assessment, such as findings, tickets, exceptions, and to carry forward these objects to the continued assessment.
Control Results Updater	Updates control results from the Connectors that are in use. RiskVision has the capability to pull information/data from connectors. When such data is populated, this job updates all results (such as - passed, failed, scores etc) in their respective tables.	This job updates the assessment (**agl_apc) with vulnerability data. Based on this data, scores and updated scores will be calculated for this APC entry.** This job reads the survey question results table and updates the compliance level score for assessments (agl_apctable). This job also updates the vulnerability links related to the entity. This job updates control responses from the Common Control Framework (see Additional Program Options settings of automatically answering unanswered controls using results from related controls.). This job applies compliance score from the related controls and applies answers from the related controls when controls have exactly the same set of choices. Vulnerabilities are related to the following Additional Program Options: • Automatically fail controls when vulnerabilities, mapped to the controls, are reported in the entity. • Automatically pass controls when vulnerabilities, mapped to the controls, are

System job	Description	Job Details
		not present or closed in the entity. • Automatically update controls when data feeds, mapped to the controls, are reported in the entity.
CrowdStrike Falcon Intelligence Connector	CrowdStrike Falcon Intelligence Connector pulls intelligence reports and persists into RiskVision Database.	Downloads threat intelligence data from the CrowdStrike Falcon Intelligence service, parses the data, places it into the RiskVision database, and correlates it with the National Vulnerability Database CVE data, if CVE references are provided by CrowdStrike Falcon Intelligence.
Daily Server and Database Hot Backup	Performs RiskVision Server, database, JasperReports Server, and Jaspersoft repository backup to a folder. The Jasper Repository contains Jasper Report repository internal data. This is a feature provided by Jaspersoft itself.	This job performs: • A Server files backup (data folder etc). • Database backup. If the database is Oracle, then specify "SYSTEM" user encrypted password for property "database.oracle.admin.password.encrypted" and also set `com.agiliance.admin.backup.BackupManager.skipOracleBackup=true` `Default Value = "false."` • Jasper database backup, and • Jasper repository backup. You can save a database backup in .exe file format. Note that running the Daily Server and Database Hot Backup jobs at the same time as other jobs may result in the database backup jobs failing. When this happens, an error message that reads "The database backup job failed as it could not get the following tables ..." will be returned in the **catalina.log**. For RiskVision version 9.3.5 or later, add the `com.agiliance.admin.backup.BackupManager.IgnoredDatabaseTableNames=` property to a**giliance.properties**. Then restart the Tomcat and rerun the database backup job. This will allow for the Daily Server and Database Hot Backup jobs to run at the same time as other jobs without causing the database backup jobs to fail. For customers using a version below 9.3.5, the only workaround is to stop all jobs and then run the database backup jobs. Also note that running the Daily Server and Database Hot Backup jobs on a multi-tier setup may return the following error message in the logs: "BackupManager - Database backup failed due to error: com.agiliance.common.ALException:". If this happens, install Microsoft Visual C++ 2013 at the application's server side for smoother database backup. See the RiskVision System Requirements for further details.
Database Statistics Updater	Updates MySQL database table statistics. This system job is disabled by default. It is recommended that this job is enabled for MySQL. The duration needs to set appropriately since this activity takes a lot of time and effects all other operations. only recommends turning on this job when advised to by Support to troubleshoot an issue. This job is not available when using the Oracle database. Instead, use the DBMS_STATS.GATHER_SCHEMA_STATS	This job updates all the required hashing techniques that are used to retrieve the objects, internal index tables etc. These statistics are used by optimizers for better performance. For example - performance, When doing collect stats on fields/indexes , the system collects the information like: total row counts of the table, how many distinct values are there in the column, how many rows per value, is the column indexed, if so unique or non unique etc.

System job	Description	Job Details
	procedure to gather statistics for all objects in a schema.	
Detailed Compliance and Risk History for Entities and Dynamic Groups	Takes a snapshot of compliance scores and risk scores for entities and dynamic groups. The scores are computed for each control, questionnaire, sub-control, question, and so on, for all entities and dynamic groups.	This job updates: Asset compliance risk history table (agl_assetcompliancerisk history) with the contents of entity compliance risk table (agl_assetcompliancerisk). Virtual group compliance risk history table (**agl_vgcompliancerisk history) with the contents of virtual group compliance risk table (agl_virtualgroupcompliancerisk).** This follows a retention policy based on the property com.agiliance.admin.scheduler AssetAndVirtualGroupCompliance RiskScoreHistoryUpdateJob.maximum HistoryRetentionTime". Default Value = 2 years. (Which means any data more than 2 years old is removed from each table respectively.)
Dynamic Group Entity Map Builder	Completely rebuilds the Dynamic Group Entity Map and updates policy assignments.	This job rebuilds the Dynamic Group entity mapping for new dynamic groups
Dynamic Group Entity Map Updater	Updates the Dynamic Group Entity Map and policy assignment for all entity changes.	This job rebuilds the Dynamic Group entity mapping for new dynamic groups, by updating the existing association.
Entity/Dynamic Group Score History	Takes a snapshot of all entities and Dynamic Group's risk and compliance scores.	The 'Entity/Dynamic Group Score History' uses the classification criticality to calculate assessment's compliance score and the Dynamic Group's score. This job then updates this to the Dynamic Group history table (agl_virtualgroupscorehistory). Similarly the entity score history table (agl_assetscorehistory) is also updated with required scores such as compliance, risk, confidentiality and integrity etc.
ERM Risk Mapper	Creates risks from failed controls in related Compliance Manager and Vendor Risk Manager programs.	To use this job, enable the featureAutomatically identify risks from failed controls for the following Compliance Manager or Vendor Risk Manager programand set its value as true.
Events Archive	Archives events that are more than three months old.	This job archives events which are of more than three months old. This duration is not editable.
Exception Request Checker	Checks for the time stamp before processing exceptions.	If the exception "**start time**" is between the last execution time and current day end time **11:59 AM**, it is marked as approved. If the "**end time**" is between one day after the execution and the current day time **12:00 AM**, the exception is marked as expired. Assessments are also marked with required expiration of exceptions.
FireEye ISight Connector	FireEye ISight Connector pulls intelligence reports and persists into RiskVision	Downloads threat intelligence data from the FireEye iSight service, parses the data, places it into the RiskVision database, and correlates it with the National Vulnerability

System job	Description	Job Details
Connector	Database	Database CVE data, if CVE references are provided by the FireEye iSight service.
LDAP Teams Synchronization	Synchronizes Team membership with group affiliations in an external LDAP directory, such as Active Directory.	This job synchronizes users for teams that are imported from LDAP, with the SystemUsertable.
LDAP Users Synchronization	Synchronizes user attributes for users that are imported from LDAP.	This job synchronizes user attributes for users that are imported from LDAP, with the SystemUsertable.
Notification Escalator	Responsible for sending out workflow escalations and reminders.	By default the job is executed only once per day and is controlled by the property **com..scheduledJob.reminderOrEscalationJobs.runOnlyOnceADay= true** Default Value = true. This job will run checks based on the following properties: **com.agiliance.notification.assessmentAdvanceChecker.enabled=true** com.agiliance.notification.ticketEscalationChecker.enabled=true com.agiliance.notification.exceptionWFAlertChecker.enabled=true com.agiliance.notification.surveyWFAlertChecker.enabled=true com..notification.ticketReminderChecker.enabled=true Depending on the property, respective checker is called. For example, if com..notification.assessmentAdvanceChecker.enabled=true, then AssessmentAdvanceCheckeris invoked. **AssessmentAdvanceChecker**moves the workflow based on workflow configuration. When you customize a workflow, the **Auto Advance**check-box in workflow options must be enabled. Ticket escalation escalates tickets, Exception alert checker checks for exceptions which are "expired" and sends notifications, Survey checker checks for alerts (which are already defined), and matches them with the workflow alerts. Ticket reminder checks for tickets for which reminders have to be sent.
Notification Sender	Sends e-mail notifications other than escalations and reminders.	
Patch Status Updater	Updates the patch status of vulnerability instances for newly created or updated patches and vulnerabilities.	
Program	Updates Dynamic Group entities in programs automatically. This job will flag entities which have been added to or	To execute the job, the options Add entity automatic and Remove entity automatic should be enabled while creating a project.

System job	Description	Job Details
Updater	removed from Dynamic Groups for addition to or deletion for assessment creation or deletion.	If they are enabled and if any entity added to Dynamic Group or removed from group, corresponding assessments are created and updated.
Purge Job Queue	Purges old and non-active jobs in the job queue database.	This job will purge the jobs in the queue - the ones that not new or not started yet. This job checks for the status of the jobs along with duration. This job will purge jobs which are in "Suspended", "Done" or "Error" state. This job enforces the property **com..dal.dao.JobPersistenceDAO.keepNDays=7** Default Value = 7. Any job after 7 days is removed.
Questionnaire Change Notification Sender	Sends questionnaire change notifications by e-mail.	
Report Summary Builder	Builds report summaries.	This job populates the tables and views which are used for reporting.
Risk Analysis Calculator	Calculates risk analysis metrics.	The job updates scores at the assessment level. Examples of attributes updated include confidentiality, integrity, availability, overall risk score and also overall compliance score of an assessment are updated.
Scan Summary Update	Updates the scan summary, summarizing the information about the data that is part of a scan. Scan summary job updates summary information per scan for findings e.g. total findings, number of passed/failed, number of mapped to control/entity for current scans only.	This job updates the summary information per scan for findings. This job updates agl_scantable. Scan is linked to finding table and the fields like **passed findings** and **failed findings** and so on are updated.
System Monitoring	Monitors the health of the system. Provides health monitoring information, which is displayed on the Server Administration page. All the metrics displayed in Health Report are calculated by this job.	This job provides the health monitoring information, that is displayed on the**Server Administration** page. This job also provides information on resources, license expiration date and sent notifications.
System User Maintenance	Performs system user maintenance, such as unlocking user accounts. A user account can be locked out due to a password policy violation, For example - after n number of failed log in attempts. The 'System Monitoring Job' unlocks the user after a certain wait period.	This job performs system user maintenance. Currently, the maintenance job includes unlocking user accounts. If a user account is locked out due to password policy violations, such as consecutive number of failed logins, this job will unlock it after the wait period. The property to set password unlock is**password.unlockWaitPeriod=12.** Default Value = 12 hours.

System job	Description	Job Details
Search Index	Automatically recreates search indexes.	This job periodically checks the various RiskVision pages to determine if any search indexes are out of sync. If they are, then the job rebuilds the search indexes for the pages that are out of sync.
Threat Summary Update	Updates the Entities at Risk, Related Tickets, Targeted Vulnerabilities and Related Incidents columns of the Threats Grid.	This job updates Entities at Risk, Related Tickets, Targeted Vulnerabilities and Related Incidents columns of the Threats
Trending Data Collection for Ad Hoc Views	Collects metrics based on Ad Hoc queries.	The Trending Data Collection for Ad Hoc Views job provides a means to trend data that can be collected using a user written query.
Trending Data Collection for CM Dashboard	Collects trending metrics from ad hoc queries for the Compliance Manager dashboard.	The Trending Data Collection for CM Dashboard job provides a means to collect trend data specifically for Compliance Manager dashboard.
Trending Data Collection for Tickets	Collects ticket trending metrics	The Trending Data Collection for Tickets job provides a means to collect trend data specifically for tickets
Update Objects	Runs object update tasks such as entity classification propagation.	This job updates the Entity classification and profile evaluation for a given entity.
Update Questionnaire	Updates questionnaires to help quickly render the Home > Questionnaires grid.	
Upload Repository Cleaner	Cleans up temporary files created by the upload component.	
Update Questionnaires for Always On Assessments	Updates the Home -> Questionnaires page for Always On-restarted assessments.	The Update Questionnaires for Always On Assessments job is required to ensure that the questionnaires for Always On Assessments appear on the Home -> Questionnaires page of each user who is assigned questions for the continued assessment.
Vulnerability Summary Update	Updates vulnerability summaries, including information such as affected entities count.	This job updates the vulnerability and the CPE summary, including information such as affected entites, affected entites with tickets, and unresolved affected entitesetc. The job updates the agl_vulnerability, agl_vulnerabilityExtensionand **agl_CPE** tables and their corresponding link tables. Entity group totals are not updated. Only the affected entites are updated.
Vulnerability Affected Entities Incremental updates Job	Vulnerability Affected Entities Incremental updates Job	This job is used to call the daily update of affected entities.
Vulnerability Risk Score Calculator	Vulnerability Risk Score Calculator	The job only recalculates risk scores for entities whose vulnerabilities or relevant entity attributes have changed, but RiskVision recommends first testing the performance impact of the job in your environment if you decide to run it multiple times per day.
Vulnerability		If you want to apply change of score system throughout the application, then the

System job	Description	Job Details
Risk Score Initiator	Vulnerability Risk Score Initiator	Vulnerability Risk Score Initiator job will refresh the scores and re-calculate everything based on new score system.
Weekly Backup of Attachments	Performs backup of ticket and policy document attachments.	This job creates a complete back-up of the attachment directory. Weekly Backup of attachments will only create a backup of the attachments folder. All the evidence are stored as attachments.
Workflow Reminder	Sends workflow reminders by e-mail.	

Further details of the system jobs are explained in the table below:

System job	Recommended Schedule	Demand On System Resources	Required
Affected Entites Notification Sender	Every 30 minutes	Medium	Not required for customers who do not have Threat and Vulnerability Manager or vulnerability notifications.
Alert Rule Processor	Daily at 5:30 p.m.	Low	Not required by customers who are not using compliance or risk score alerting.
Control Results Updater	Every 5 hours	High	Only required by customers using Compliance Manager and Enterprise Risk Manager.
Daily Server and Database Hot Backup	Daily at 6:30 a.m.	High	Yes. strongly recommends leaving this job enabled.
Database Statistics Updater	Weekly, Sunday at 1:30 p.m.	Low	No. You cannot run the Database Statistics Updater job during the execution of the Daily Server and Database Hot Backup job.
Detailed Compliance and Risk History for Entities and Dynamic Groups	Monthly, on the 1st, at 2:30 p.m.	Medium	No, but if this job is disabled you will not be able to trend on risk and compliance scores.
Dynamic Group Entity Map Builder	Daily at 2:30 p.m.	High	Yes. This job is required for Dynamic Groups to work and Dynamic Groups are essential to the functioning of the product.
Dynamic Group Entity Map Updater	Every 15 minutes	High	Yes. This job is required for Dynamic Groups to work and Dynamic Groups are essential to the functioning of the product.
Entity/Dynamic Group Score History	Daily at 12:30 p.m.	Medium	No.
ERM Risk Mapper	Daily at 11:30 a.m.	Medium	No. This job is only required by customers using the auto-risk identification feature.
Events Archive	Monthly at 7:00 p.m	Medium	Yes. This job is required to prevent logs from taking up a lot of space in the database.
Exception Request Checker	Daily at 6:30 p.m.	Medium	No. This job is required by customers using exceptions.
LDAP Teams	Daily at		No. This job is required by customers who are using teams and are managing teams

System job	Recommended Schedule	Demand On System Resources	Required
Synchronization	5:30 p.m.	High	by syncing them to LDAP.
LDAP Users Synchronization	Weekly, Friday at 10:30 a.m.	High	No. This job is required by customers who have users authenticating against their LDAP directory.
Notification Escalator	Daily at 3:30 p.m.	Low	No. This job is required by customers who are using the escalation feature and the reminder feature of workflows.
Notification Sender	Every 15 minutes	Low	No. This job is required by customers using notifications.
Patch Status Updater	Every 30 minutes	High	No. This job is only required by customers who are using Threat and Vulnerability Manager and who are tracking patches via Threat and Vulnerability Manager.
Program Updater	Every 2 hours	High	No. This job is only required by customers who are assigning dynamic groups to programs.
Purge Job Queue	Daily at 5:30 p.m.	Low	Yes. This job should be run to maintain the efficiency and performance of the database.
Questionnaire change Notification Sender	Every 30 minutes	Low	No. Customers only need this when they want to send out questionnaire change notifications to let users who are responsible for answering questions know when the content in the questions has changed or new questions has been added.
Report Summary Builder	Daily at 11:30 a.m.	High	No. Customers who are using legacy RiskVision reports and Jasper reports are the only ones who require this job.
Risk Analysis Calculator	Daily at 6:30 p.m.	High	No. This job is only required by customers who are using the Enterprise Risk Manager application.
Scan Summary Update	Daily at 1:00 p.m.	Medium	No. This job is only required by customers who are using Threat and Vulnerability Manager application.
System Monitoring	Every 5 minutes	Low	Yes. This job is used to monitor the health of the RiskVision server.
System User Maintenance	Every 30 minutes	Low	Yes.
Search Index	Every 4 Hours	High	Yes. This job runs at regular intervals to make sure that the search index is updated. If the search index is being rebuilt from the Admin user interface, then this job will be idle and will not try rebuilding the search all over again. Search indexes are only rebuilt when they are out of sync.
Update Objects	Every 10 minutes	Medium	Yes.
Update Questionnaire	Every 4 hours	High	Yes.
Upload Repository Cleaner	Every 30 minutes	Low	Not required, but recommended to clean up temporary files.
Vulnerability Summary	Every 60		

System job	Recommended Schedule	Demand On System Resources	Required
Update	minutes	High	No. This job is only required for customers using Threat and Vulnerability Manager.
Weekly Backup of Attachments	Weekly, Sunday at 6:30 a.m.	Medium	No. This is not required for customers who are performing their own backups of attachments.
Workflow Reminder	Daily at 3:30 p.m.	Low	No. This is only required for customers who are using the reminder feature of workflows.
Assessment Objects Carry Forward	Daily Once	Low	Yes. This is used for Assessments Snapshot process. It is a light weight job assuming there will be very few assessments queued up for snapshot process per execution.
Update Questionnaires for Always On Assessments	Daily Once	Low	This is a post-update step run after assessments snapshot process. Correct data will be visible in My Questionnaires page after this job execution which also releases lock on Assessments for edits.
Vulnerability Risk Score Calculator	Daily Once	Low	Yes. This is used to process enhanced risk score for vulnerabilities.
Vulnerability Risk Score Initiator	Daily Once	High	Yes. This job processes enhanced risk score for all the vulnerabilities and entities and so resource intensive.
Vulnerability Affected Entities Incremental Updates Job	Once	Low	Yes. This is used for vulnerability entities grouping.
CrowdStrike Falcon Intelligence Connector	Daily Once	Medium	Yes. This job is required to get the threat object information.
FireEye ISight Connector	Daily Once	Medium	Yes. This job is required to get the threat object information.
Threat Summary Update	Hourly	Low	Yes. This job allows to update the related tickets, entitys at risk and targeted vulnerabiltiy count.
Trending Data Collection for Ad Hoc Views	Daily Once	High	Yes. This job is required to enable any trend data collection.
Trending Data Collection for Tickets	Daily Once	High	Yes. This job is required to enable any trend data collection for ticket.
Trending Data Collection for CM Dashboard	Daily Once	High	Yes. This job is required to enable any trend data collection for " Average Compliance Score, Open Assessments, Open Mitigations, Open Findings/Open Tickets/Open Exceptions, and Program Compliance Score Trend".

About Scheduled Jobs

Jobs include running a report, creating a new policy and control framework, or other task that may take a significant amount of time to complete.

Run a report manually or schedule a report to run at a specific time or interval to create a report job. The**Queued Jobs** page displays information about pending jobs.

Custom Script Jobs

Custom Script jobs replace the groovy script that is implemented in a system job to automate routine actions. There are a total of five Custom Script system jobs that are available on the Administration > Scheduled Jobs menu, named sequentially from Custom Script Job 1 to Custom Script Job 5. One file can be assigned to each custom job, but there can be multiple groovy scripts within each file. There are five custom jobs so that you can batch your groovy scripts to run at different intervals.

To use a Custom Script job:

1. Create a groovy script file with the required logic.
2. Name the groovy script file with the same name as the Custom Script job.
3. Copy the groovy script file to the `%AGILIANCE_HOME%\Config\scripts` directory.
4. Restart the RiskVision Tomcat service or reload the server configuration.
5. Go to the **Administration > Scheduled Jobs**.
6. Check the box next to the Custom Script system job and click Activate. For example, if you have named the groovy script file as "CustomScriptJob1," then activate the Custom Script Job 1 system job. Note that there can be no spaces when naming the groovy script file.
7. Optional. Click the Custom Script system job to open its details page. And, click Reschedule to revise the execution time and to set the recurrence.

Example groovy script:

```
/**
This Groovy file should be placed in {customizations.folder}/scripts folder.
*/
import com.agiliance.admin.scheduler.CustomScriptJob.ScriptJob
import com.agiliance.web.customization.scripting.CustomizationBase
import java.lang.StringBuilder;
import java.util.Map;
/**
* This is an example of script class written in Groovy that can be used as a template for
a script based job.
* The class must implement ScriptJob interface. If it extends CustomizationBase class,
then the logging (info, warn, error) and other methods are also available.
*/
public class CustomScriptJob1 extends CustomizationBase implements ScriptJob {
/**
* The method gets called from 'CustomScriptJob' system job.
* @param namedParams Job data
* @return
*/
public void execute(Map namedParams)
{
// The following helper methods can be used for logging:
info("CustomScriptJob: info() method!")
// warn("CustomScriptJob: warn() method!")

// error("CustomScriptJob: error() method!")

// Log all job named parameters
logAllNamedParameters(namedParams);
// For more detailed info about all available helper methods take a look at CustomizationBase
//Java class that this class extends.
}
private void logAllNamedParameters(Map namedParams) {
StringBuilder sb = new StringBuilder();
// Log all script job parameters
sb.append("Job Named Parameters: [ ");
for (Map.Entry e : namedParams.entrySet())
{
sb.append(e.getKey()).append(": ").append(e.getValue()).append(" ");
}
sb.append("]");
info(sb.toString());
}
}
```

Rescheduling Jobs

The **Scheduled Job** details page allows you to reschedule system jobs and the user-defined recurring tasks, such as updating programs and charts. Depending on the nature of each system job, has set the execution time of these jobs to run at regular intervals. Some system jobs run frequently and concludes in a short time, whereas other jobs recur less frequently. When modifying the schedule of any system job, recommends not to set the same start time for long running jobs.

To reschedule a job:

1. Go to **Administration** > **Scheduled Jobs**.
2. The **Scheduled Jobs** page appears. Click a job to open its details page and click **Reschedule Job**.
3. The **Revise Schedule** dialog appears. Choose one of the following Frequency options: **Daily, Weekly, Monthly, Hourly, or Minutes,** and then select or enter the options, given below in the table, that appear based on the type of frequency. Note that not all jobs can be rescheduled using the Minutes frequency.

Parameter	Description
Frequency	Choose Daily, Weekly, Monthly, Hourly, or Minutes
Start Time	Enter the time to run the job
Start Date	Enter the date the job must begin
Select the Days of the Week (Weekly)	Select the days of week to run the job
Select the day of the month and the months (Monthly)	Select the day: First, Last, Fifteenth, or enter a particular day (such as the 10th) and month(s) to run the job
Perform this task (Daily)	Select how often to run the job. Choose Every Day, Weekdays, or Weekends
Hourly Interval	Enter the frequency in hours to repeat the job
Interval (minutes)	Enter the frequency in minutes to repeat the job

4. Click **OK**. The job is rescheduled.

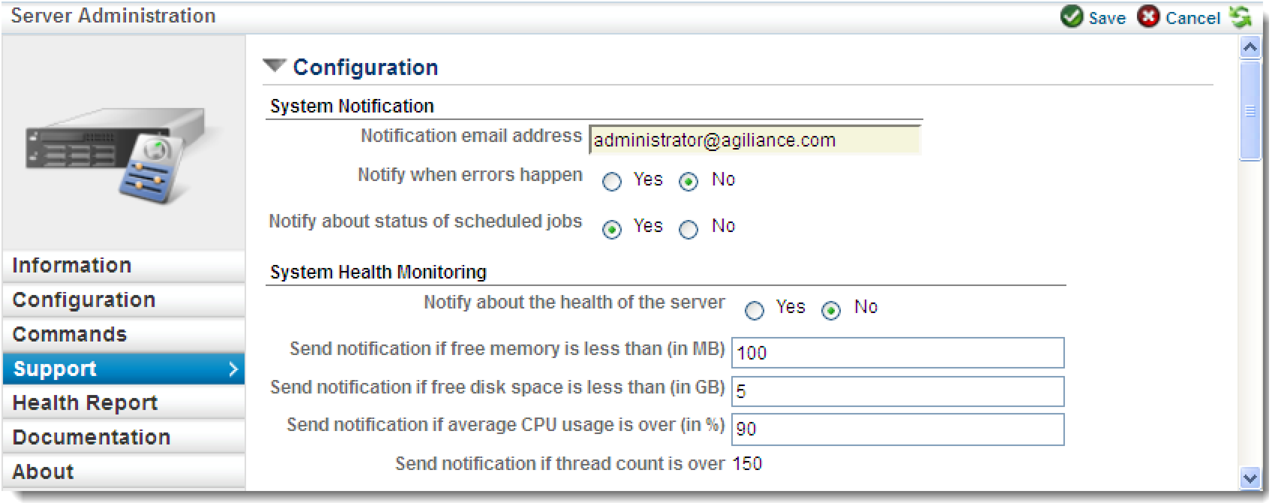
Scheduled Job Status Notification

The job scheduler can send notifications about the status of scheduled jobs. For each scheduled job, you can get notifications for success, failure, or both. The job successful notification informs you of the details, such as Time job started, Time job completed, Job duration, and the next execution date and time. Whereas the job failure notification informs you of the details, such as Time job started, Time job interrupted Job runtime before error(s), and the description of the error(s).

To specify the notification information for a scheduled job

1. In the RiskVision Administration application, go to **Administration** > **Server Administration**, and click the Support tab.
2. Click Edit at the upper right corner of the Server Administration page.
3. Under the System Notification of Configuration section, enter an email ID in the Notification email address field to which you want to receive the notifications, and select Yes next to the Notify about the status of scheduled jobs option.

   You can enter only one email ID. Also, no contact group is allowed to send email notifications to multiple recipients.



System Notification

Notification email address administrator@agiliance.com

Notify when errors happen ○ Yes ● No

Notify about status of scheduled jobs ● Yes ○ No

System Health Monitoring

Notify about the health of the server ○ Yes ● No

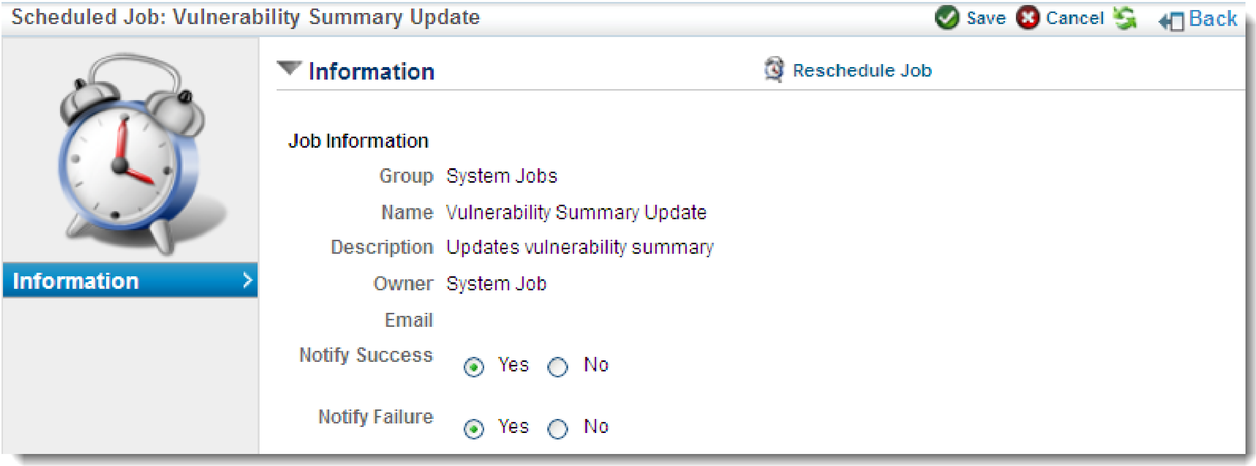
Send notification if free memory is less than (in MB) 100

Send notification if free disk space is less than (in GB) 5

Send notification if average CPU usage is over (in %) 90

Send notification if thread count is over 150

4. Click **Save**, and then go to **Administration** > **Scheduled Jobs**.
5. In the **Scheduled Jobs** page, select a job to open its details pane below the**Scheduled Jobs** page, and click **Edit** at the upper right corner of the pane.
6. Under the Job Information of Information section, Select **Yes** next to the following options:
   - Notify Success. Receive a notification that a job is successfully executed.
   - Notify Failure. Receive a notification that a job is failed.



Job Information

Group System Jobs

Name Vulnerability Summary Update

Description Updates vulnerability summary

Owner System Job

Email

Notify Success ● Yes ○ No

Notify Failure ● Yes ○ No

7. Click **Save** at the upper right corner of the details pane.

Chart Status

The Chart Status page displays information about charts in progress. To cancel a chart, select it in the grid and click Cancel.

Chart Status

The **Chart Status** page displays information about charts in progress.

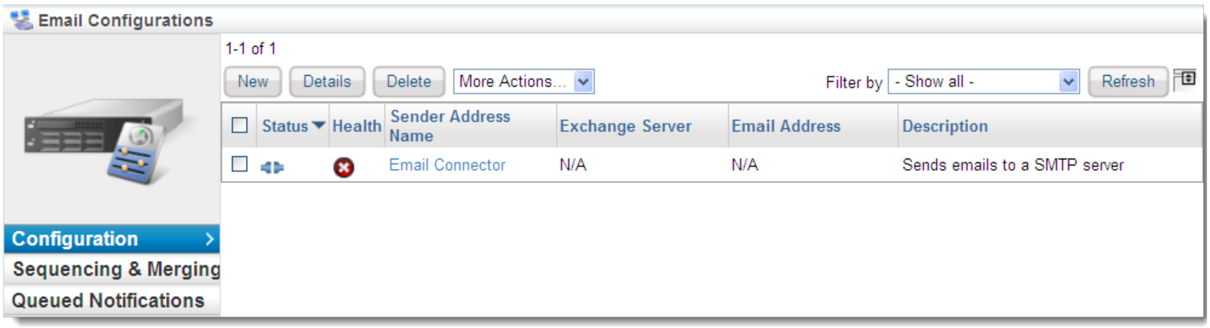
To cancel a chart, select it in the grid, and click Cancel.

Configuring Email Accounts to Send Notifications

The default email configuration sends notifications to a local SMTP service for email distribution. With default email configuration, all notifications are sent out using one email address. You can add multiple email configurations to send out notifications from more than one email account. You might do this for users tasked with the administration of RiskVision objects, such as assessments, findings, incidents, and tickets so that stakeholders can directly reach out to those users. Once you configure multiple email configurations, the email addresses are available for selection in the **Sender Email Account** field of email templates to send out notifications using different email addresses. If no sender account is selected in the email template, the notifications are sent out using the default email configuration.

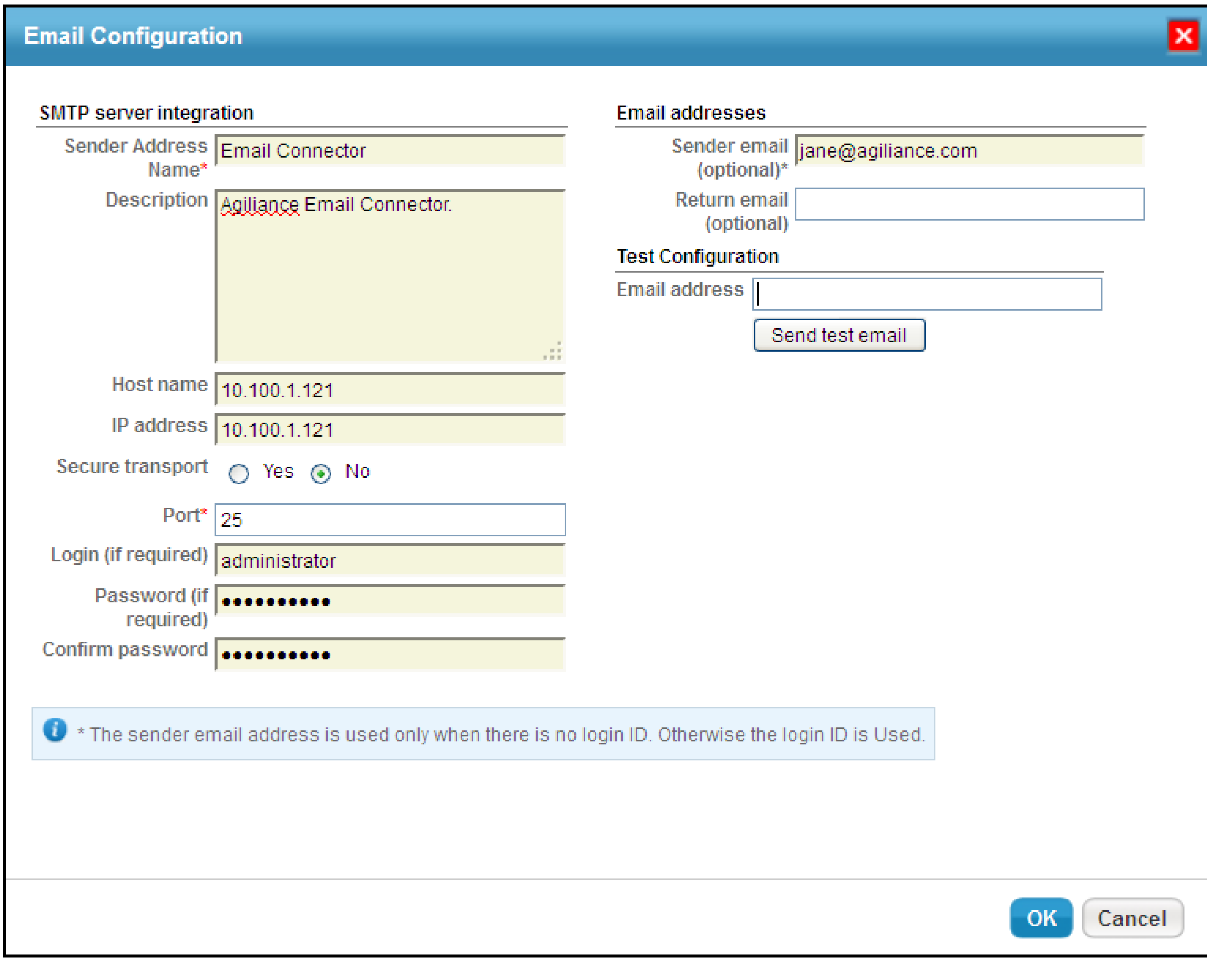
To set up the email configuration:

1. In the **RiskVision Administration** application, go to **Administration** > **Notifications**, and click the **Configuration** tab. The default notification sender account is displayed.



□	Status	Health	Sender Address Name	Exchange Server	Email Address	Description
□		☒	Email Connector	N/A	N/A	Sends emails to a SMTP server

2. Select the default notification sender account to open the sender account or click**New** to add a sender account.



Sender Address Name*	Email Connector
Description	Agiliance Email Connector.
Host name	10.100.1.121
IP address	10.100.1.121
Secure transport	○ Yes ● No
Port*	25
Login (if required)	administrator
Password (if required)	••••••••••
Confirm password	••••••••••
Sender email (optional)*	jane@agiliance.com
Return email (optional)	
Email address	

* The sender email address is used only when there is no login ID. Otherwise the login ID is Used.

3. Enter the following fields to update the configuration:

    - **Sender Address Name.** Enter the sender's name using which you will want to send the email notifications.

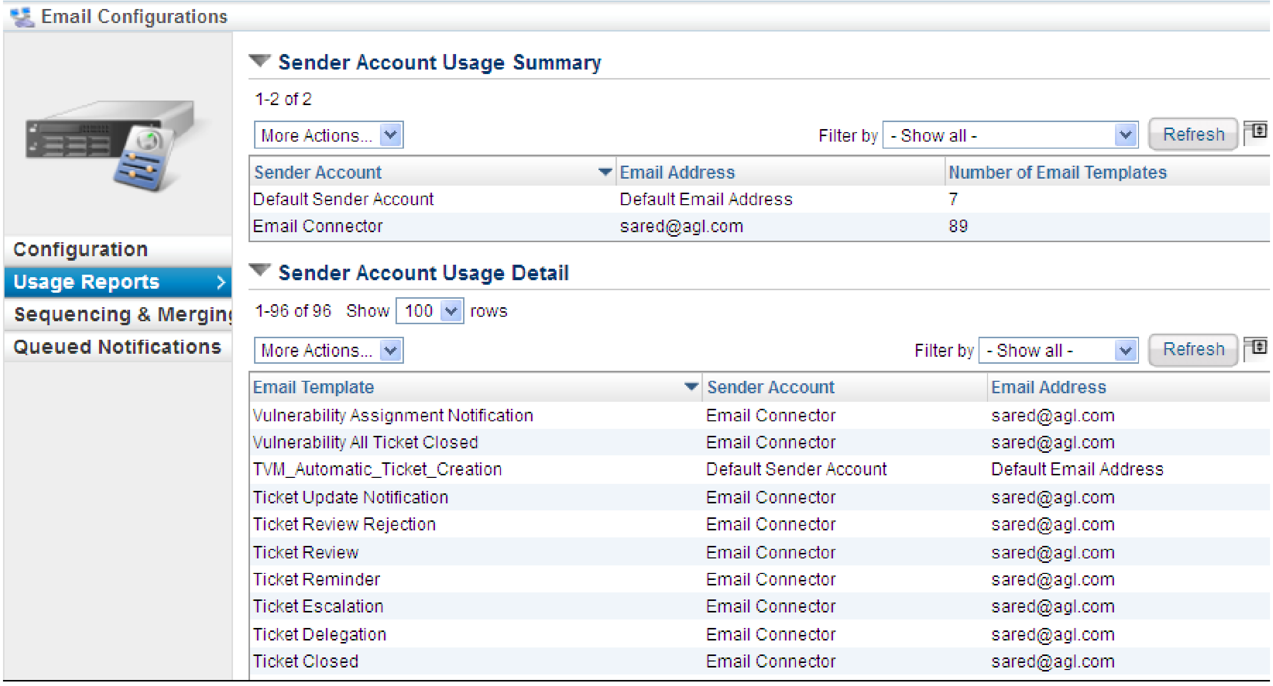
- **Description**. Any additional information to help understand the use of exchange server.
- **Host Name**. Enter the fully qualified Domain Name of the SMTP host.
- **IP address**. Enter the IP address of the SMTP host
- **Secure transport**. Choose Yes or No.
- **Port**. Enter the SMTP listening port (default value is 25).
- **Login** (if required). Enter the username for SMTP service if the service requires authentication. By default, the email configuration uses the Login ID entered here to send out notifications.
- **Password** (if required). Enter the password if the SMTP service requires authentication.
- **Confirm password**. Enter the password again for confirmation.
- **Sender email** (optional). Enter an email address using which you will want to send the email notifications rather than using the Login ID.
- **Return email** (optional). Enter the email address where you want to receive email replies.

4. To test the configuration, enter a valid email Id in theEmail address field, and click **Send test email**. If the configuration entered is correct, you will receive an email notification.

5. Click **OK** to save and exit the dialog.

Email Usage Reports

When you set up multiple sender accounts to send notifications from different email addresses, you will want to know from which sender accounts the RiskVision Server is sending the notifications. To help with this information has added the Usage Reports tab to the **Administration** > **Notifications** menu.



Sender Account Usage Summary

1-2 of 2

Sender Account	Email Address	Number of Email Templates
Default Sender Account	Default Email Address	7
Email Connector	sared@agl.com	89

Sender Account Usage Detail

1-96 of 96 Show 100 rows

Email Template	Sender Account	Email Address
Vulnerability Assignment Notification	Email Connector	sared@agl.com
Vulnerability All Ticket Closed	Email Connector	sared@agl.com
TVM_Automatic_Ticket_Creation	Default Sender Account	Default Email Address
Ticket Update Notification	Email Connector	sared@agl.com
Ticket Review Rejection	Email Connector	sared@agl.com
Ticket Review	Email Connector	sared@agl.com
Ticket Reminder	Email Connector	sared@agl.com
Ticket Escalation	Email Connector	sared@agl.com
Ticket Delegation	Email Connector	sared@agl.com
Ticket Closed	Email Connector	sared@agl.com

With **Usage Reports** tab, you can see which sender accounts are in use and both the quantity and list of the email templates that are being sent from the sender accounts. The reports available in this tab are:

Sender Account Usage Summary. This report displays the configured sender accounts and the count of email templates that are using a particular sender account to send email notifications.

Sender Account Usage Detail. This report lists the breakdown of all the email templates that send notifications from a sender account.

Sequencing and Merging of Email Notifications

Beginning with version 7.0, introduces the following two new features to handle email notifications:

- Sequencing
- Merging

Sequencing

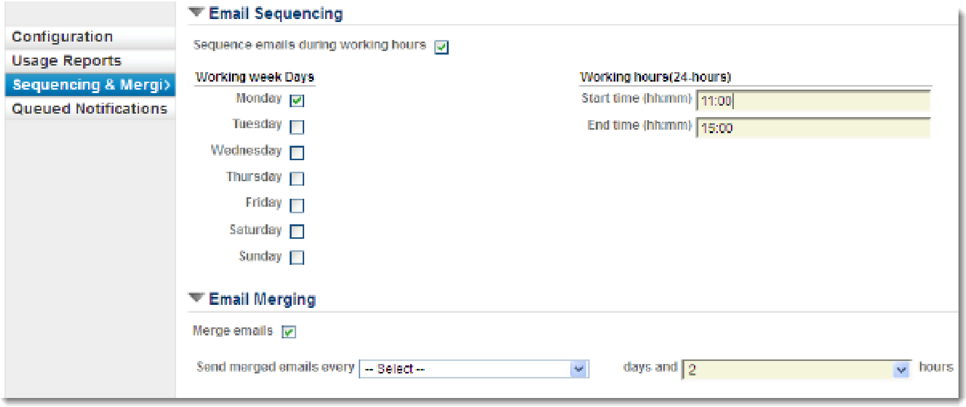
The email sequencing feature allows administrators to choose to avoid sending notifications during peak business hours. When enabling this feature, you can define peak business hours by days of the week and hours of the day.

The purpose of this feature is to allow your organization to reduce the load on the RiskVision server that can happen when users click on the links in the notifications they receive. Many users click on the link shortly after receiving the notification. By delaying the sending and receiving of these notifications until off-peak hours, your organization can reduce the load on the RiskVision server during peak hours.

The only emails that are sent during the sequencing period are those emails that are derived from notifications templates that are marked as “Send Immediately.”

To enable sequencing:

1. In the Administration application, go to **Administration > Notifications**, and click the **Sequencing & Merging** tab.



Email Sequencing

Sequence emails during working hours ☑

Working week Days

- Monday ☑
- Tuesday □
- Wednesday □
- Thursday □
- Friday □
- Saturday □
- Sunday □

Working hours(24-hours)

- Start time (hh:mm) 11:00
- End time (hh:mm) 15:00

Email Merging

Merge emails ☑

Send merged emails every -- Select -- days and 2 hours

2. Click **Edit** and then check the box next to Sequence emails during working hours option under the **Email Sequencing** section.
3. Under **Working week Days**, check the box next to days of week as applicable, and under **Working hours (24-hours)**, enter a start time in the Start time (hh:mm) field when the sequencing must begin and an end time in the End time (hh:mm) field when the sequencing must begin.

   For example, you run certain assessments every Monday between 11 AM and 3 PM. You will not want to do anything in this period to accelerate RiskVision logons, and therefore would want to delay sending notifications during these hours. To achieve this objective, you will enable the sequencing, check the box next to Monday, and select the Start time (hh:mm) as 11:00 and the End time (hh:mm) as 15:00.

4. Click **Save**.

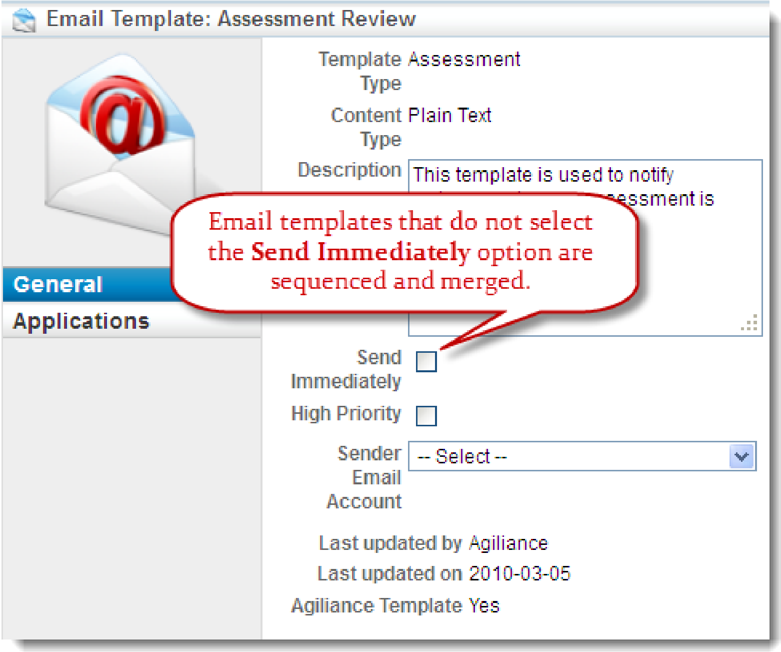
Merging

Emails are merged to combine the contents of all the notifications, intended for each user, into a single email notification in order to minimize the number of messages that users receive and for convenient reading. With merging, the notifications are stored in the queue for the chosen time interval before they are sent to the recipients.

The email merging feature can work in conjunction with the email sequencing feature. The sending time of merged emails is calculated as detailed in the bulleted list below. When it is time to send a merged email, RiskVision checks to see if this is during sequencing hours. If it is during sequencing hours, then the merged email will not be sent until the sequencing hours are over.

The merging uses the following guidelines when sending notifications to recipients:

- Assembles all the email notifications that are not marked as "Send Immediately."



Email Template: Assessment Review

Template Type Assessment

Content Type Plain Text

Description This template is used to notify ...essment is

Email templates that do not select the **Send Immediately** option are sequenced and merged.

Send Immediately □

High Priority □

Sender Email Account -- Select --

Last updated by Agiliance

Last updated on 2010-03-05

Agiliance Template Yes

- Segregates all the email notifications according to the recipient and sender email accounts in their own queue.

- Continues to hold all messages for each sender-recipient pair until the oldest message in the queue has exceeded the merging period. When the oldest message exceeds the merging period, then all of the messages are sent.

- The queue for that sender-recipient pair starts to accumulate again until the oldest message exceeds the merging period.

To enable merging:

1. In the Administration application, go to **Administration** > **Notifications**, and click the **Sequencing & Merging** tab
2. Click **Edit** and then check the box next to the **Merge emails** option under the **Email Merging** section.
3. Select the days in the first drop-down box and select the hours in the second drop-down box to recurringly send the merged emails after that many days and hours.

Example

This example shows you how notifications are sent when both sequencing and merging are enabled. To configure this scenario, In this context, enable the sequencing on Monday between 11 AM and 4 PM and set the merging to send notifications every 2 hours. Then, consider the following data in the table.

Template	Sender	Recipient	In queue (hours)
N1	Tom (tom@agl.com)	Nathan	5
N2	Martin (martin@agl.com)	Paul	4

Template	Sender	Recipient	In queue (hours)
N3	Tom (tom@agl.com)	Nathan	3
N4	Martin (martin@agl.com)	David	4
N5	Martin (martin@agl.com)	Nathan	5
N6	Jane (Jane@domain.com)	Mary	2

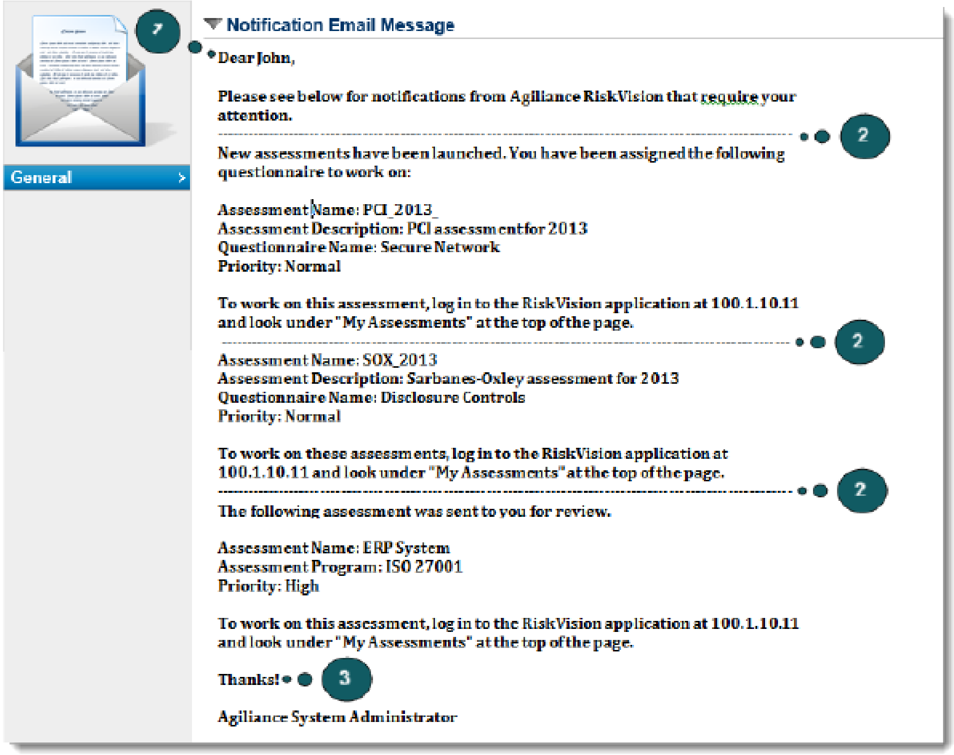
In the table above, the notifications N1 through N6 are queued because the email templates are marked as not to send immediately and the sequencing and merging are enabled. When notifications are triggered on Monday between 11 AM and 4 PM, they are stored in a queue until 4 PM and only then the notifications are sent. As you can see in the table that the notification N1 for user 'Nathan' is in the queue for 5 hours, the RiskVision Server marks that notification for sending to the intended recipient. Since merging is enabled, the RiskVision Server attempts to locate other notifications intended for the user 'Nathan' from the sender 'Tom.' When multiple notifications for a user from the same sender are found, the notifications are merged though other notifications for that user has been in the queue for less than 5 hours. In this case, there are two notifications to be sent from Tom to Nathan; one being in the queue for 5 hours and the other one for 3 hours. The content of these two notifications is merged and sent using a single notification. Since there is one more notification N5 to be sent from Martin to Nathan, the notification is sent using a separate email since the email template is configured to send from the sender email account 'Martin.'

Setting the Salutation and Signature for Merged Emails

Merged emails within RiskVision currently show up as an aggregation of the individual emails that comprise the merged email. For example, if a merged email has 5 notifications within the merged email, there will be 5 salutations and endings within the merged email, once for each notification. Adding the following properties to the . `properties` file will result in the merging placing a global salutation and signature for all the merged notifications and appending a separator at the beginning of each notification to demarcate the individual notifications within the email.

- `com.agiliance.notification.useGlobalSalutationAndSignature` – Setting this property to true allows using the universal salutation and signature.
- `com.agiliance.notification.globalSalutation` – Setting this property applies the universal salutation for all the merged and non-merged emails.
- `com.agiliance.notification.globalSignature` – Setting this property applies the universal signature for all the merged and non-merged emails.
- `com.agiliance.notification.messageSeparator` – Setting this property to true appends a separator (use special characters, such as -, *, ^, #, and more) at the beginning of each notification in the merged emails. This will not be used for notifications from templates that are marked as Send Immediately.

The graphic below illustrates a merged email with universal salutation and signature, and separator:



Dear John,

Please see below for notifications from Agiliance RiskVision that require your attention.

New assessments have been launched. You have been assigned the following questionnaire to work on:

Assessment Name: PCI_2013_
Assessment Description: PCI assessment for 2013
Questionnaire Name: Secure Network
Priority: Normal

To work on this assessment, log in to the RiskVision application at 100.1.10.11 and look under "My Assessments" at the top of the page.

Assessment Name: SOX_2013
Assessment Description: Sarbanes-Oxley assessment for 2013
Questionnaire Name: Disclosure Controls
Priority: Normal

To work on these assessments, log in to the RiskVision application at 100.1.10.11 and look under "My Assessments" at the top of the page.

The following assessment was sent to you for review.

Assessment Name: ERP System
Assessment Program: ISO 27001
Priority: High

To work on this assessment, log in to the RiskVision application at 100.1.10.11 and look under "My Assessments" at the top of the page.

Thanks!

Agiliance System Administrator

1. *The universal salutation "Dear"*
2. *The separator "hyphen (-)"*
3. *The universal signature "Thanks!"*

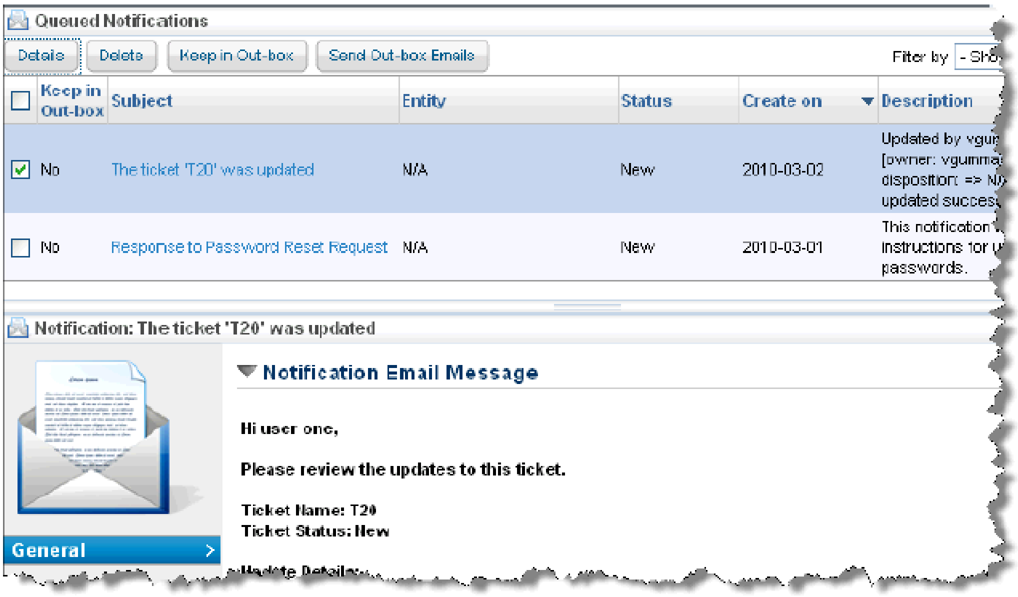
In addition to the properties mentioned above, you must also delete the salutation and signature from all of the email templates including the ones that are marked as Send Immediately.

recommends only to use the properties mentioned above when merging is enabled. However, if you decide to use the properties when merging is not enabled, please be aware of the following behavior:

There will be multiple salutations and signatures shown in each merged email, one from the global setting and one from the email template if the salutation and signature are not deleted from the email templates.

About the Out-box

Notification messages that have not yet been sent are displayed on the **Queued Notifications** page.



□	Keep in Out-box	Subject	Entity	Status	Create on	Description
☑	No	The ticket 'T20' was updated	N/A	New	2010-03-02	Updated by vgu [owner: vgumma disposition: => N/ updated succes
□	No	Response to Password Reset Request	N/A	New	2010-03-01	This notification instructions for u passwords.

Notification: The ticket 'T20' was updated

Notification Email Message

Hi user one,

Please review the updates to this ticket.

Ticket Name: T20
Ticket Status: New

Update Details:

Unlike the Message Center, the **Queued Notifications** page only displays messages that have not yet been sent. When e-mail notifications are sent (see System Jobs), all messages for which **Keep in Outbox** is marked 'No' will be sent and removed from the **Queued Notifications** page.

To postpone sending a notification:

1. In the Administration application, go to **Administration** > **Notifications**, and click the**Queued Notifications** tab.
2. Check the box to select the notification to postpone. Click **Keep in Outbox**. The **Keep in Outbox** column for the selected notification changes to 'Yes.'

To clear the Keep in Outbox flag:

1. In the Administration application, go to Administration > **Notifications**, and the **Queued Notifications** tab.
2. Check the box to select the notification of interest. Click **Send Out-box Emails**. The **Keep in Outbox** column for the selected notification changes to 'No.'

Viewing Queued Notifications

As a RiskVision administrator, you are able to view and perform actions on the queued notifications because the Queued Notification View permission is granted to the predefined Administrator role. If you need other users to access the Queued Notifications page, assign that user role with the Queued Notification View permission.

To view Queued Notifications:

1. In the Administration application, navigate to **Administration**> **Notifications**, and click the **Queued Notifications** tab.
2. The display shows all queued notifications, with columns for **Subject**, **Entity**, **Status**, **Create on**, **Assessment**, and **Description**. Click a column heading to sort the table by that column.
3. To view a subset of table rows, select from the **Filter By**drop down list. You can filter on **Subject**, **Entity**, **Status**, **Create on**, **Assessment**, and **Description**.
4. Click **Refresh** to display the current contents of the database if new notifications may have been added while you have been viewing the queue.

Displaying Queued Notification Details

Notifications are queued (saved) for later viewing.

To display the details of a Queued Notification:

1. In the Administration application, navigate to **Administration** > **Notifications**, and click the **Queued Notifications** tab.

2. The display shows all queued notifications. Check the box next to the notification of interest.

3. Click **Details**.

About Email Templates

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

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

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

Configuring Email Templates

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

The following describes the available email template types:

- **Access Delegation**. Used when notifying users of assigned access delegations.
- **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.

Updating Email Template

Modifications to email templates take effect immediately.

To update an e-mail template:

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

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

The new template is now available.

Adding A New Customized E-mail Template

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

To create an e-mail template:

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

2. Click **New**.

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

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

   - **Template Type.** Select the workflow type.

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

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

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

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

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

4. Enter the message content.

   Resolver recommends basing new templates on one of the defaults.

5. Click **Save**.

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

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

Getting Familiar with Email Notifications

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

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

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

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

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

Escalation

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

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

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

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

Creating an Escalation Configuration

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

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

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

To create a new escalation configuration:

1. Go to **Configuration** > **Escalation**.

2. Click **New**.

3. Enter the **General** settings as follows:

   - Name. Enter the display name that users will use to identify this escalation configuration.

   - Description. Enter a summary that will be visible only on the escalation page.

4. Create an escalation for Level 1 by clicking **New** in the **Escalations** section. You can repeat these steps to create escalations for Level 2 and 3 later, if desired.

5. Enter the **Escalation** settings as follows:

   - Escalation Level. Choose 1 for the first response to an overdue ticket. To create a different response if the ticket remains overdue, create a second Escalation with Level 2.

   - E-mail Template. Select from the list of available e-mail templates. Click Preview to see how the e-mail will look.

   - Escalation Date. The number of days after the ticket is due that triggers this message. Level 1 might be triggered 1 day after a ticket's due date while Level 2 is triggered a few days later. Level 3, if required, would be triggered later.

   - Recipients. Check Requester, Owner Manager, or select individuals or teams to receive this message.

6. Click **OK**.

7. Click **Save** to save the new escalation configuration.

Using the Document Repository

A document repository is used for storing critical documents, such as audit material, security plans and sensitive information pertaining to each domain in your organization. You can also refer stakeholders to useful information on the Internet or your intranet using web references. If your user role has sufficient permissions, you can upload files of any kind to share in the repository as well as you can refer to specific websites.

Typically, the document repository is available on the Content, Risks, or Administration menu in RiskVision application.

In addition to the shared document repository, documents and weblinks/ network paths can be uploaded and associated with various RiskVision objects, including entities, controls, programs, contracts, policy documents and so on. These objects have a **Documents** tab in their detail pages. The user permissions control the associated documents to view, upload, or perform any action.

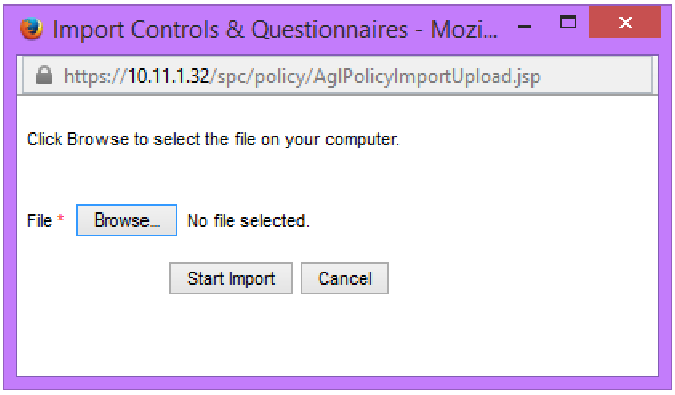
Import Content

RiskVision supports a variety of checklists, frameworks, methodologies, regulations, and standards that are referred to as "content." Over fifty content sources are mapped to RiskVision Frameworks that support over ten thousand operational and technical controls. Visit our website for a complete list of provided content.

This content is created in tree and must be imported into RiskVision as the sysadmin user. Once imported, the content can be copied to the **Organizational** tree. To import policy documents in XML format, you must have Policy View and Policy Manage permissions.

To import XML policy documents:

1. Log into RiskVision as the sysadmin user. The default password is “compliance”. This password will have to be changed after initial login.
2. Go to **Content** > **Controls and Questionnaires**.
3. Click **Import Policies (XML)**.
4. Click **Browse** to select the file, and then click **Start Import**.

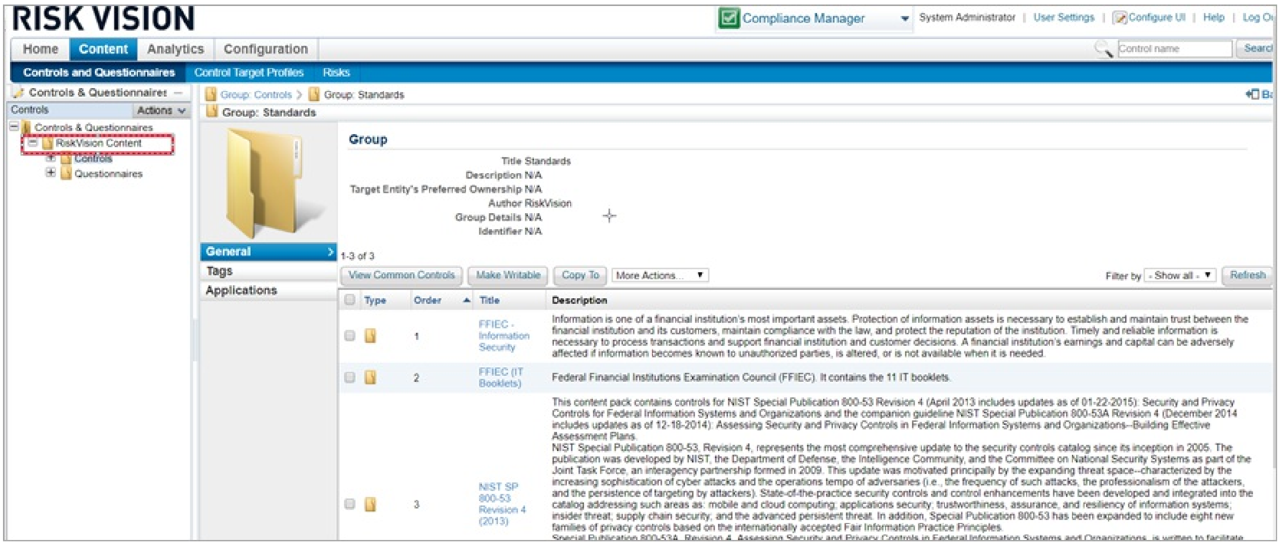

Import Controls & Questionnaires - Mozi...
https://10.11.1.32/spc/policy/AglPolicyImportUpload.jsp
Browse...
Start Import
Cancel

Click Browse to select the file on your computer.

File * No file selected.

The Import Controls & Questionnaires window.

Once the import has been completed, the **Import Policies** window will display details about the imported file, such as content count. Content imported by the sysadmin user can be found in the **Hierarchy Tree** > **RiskVision Content** folder.



Group

Title Standards
Description N/A
Target Entity's Preferred Ownership N/A
Author RiskVision
Group Details N/A
Identifier N/A

1-3 of 3

Type	Order	Title	Description
	1	FFIEC - Information Security	Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support financial institution and customer decisions. A financial institution's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.
	2	FFIEC (IT Booklets)	Federal Financial Institutions Examination Council (FFIEC). It contains the 11 IT booklets.
	3	NIST SP 800-53 Revision 4 (2013)	This content pack contains controls for NIST Special Publication 800-53 Revision 4 (April 2013 includes updates as of 01-22-2015): Security and Privacy Controls for Federal Information Systems and Organizations and the companion guideline NIST Special Publication 800-53A Revision 4 (December 2014 includes updates as of 12-18-2014): Assessing Security and Privacy Controls in Federal Information Systems and Organizations--Building Effective Assessment Plans. NIST Special Publication 800-53, Revision 4, represents the most comprehensive update to the security controls catalog since its inception in 2005. The publication was developed by NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force, an interagency partnership formed in 2009. This update was motivated principally by the expanding threat space--characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat. In addition, Special Publication 800-53 has been expanded to include eight new families of privacy controls based on the internationally accepted Fair Information Practice Principles. Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, is written to facilitate

The RiskVision Content folder.

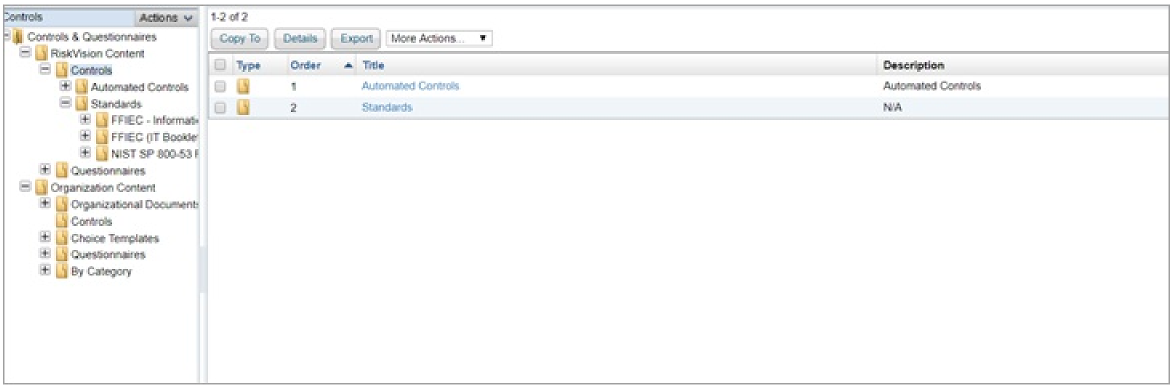
Moving Content

Content imported by the sysadmin user can be found in the **RiskVision Content** folder. It's good practice to copy this content to the **Organizational** content folder prior to making modifications and deploying the content.

> Content provided by Resolver can only be imported by the sysadmin user. Content that is created by you and your team can be exported and imported by a user with administrative permissions.

To move content:

1. Log into RiskVision as a user that's been added to an administrative role, such as the administrator.
2. Go to **Content** > **Controls and Questionnaires**.
3. Expand **Controls and Questionnaires**, then expand **RiskVision Content** and **Organization Content**.
4. Go to **RiskVision Content > Controls >Standards**, then select the content you want to copy.



□	Type	Order	Title	Description
□		1	Automated Controls	Automated Controls
□		2	Standards	N/A

5. Click **Actions** > **Copy**.
6. Select a folder under the **Organizational Content** folder to paste the content into.
7. Click **Actions** > **Paste**.
8. Modify and deploy the new content, as needed.

Advanced Backup Retention

The backup retention properties allow you to determine the number of daily, weekly, and monthly backups to preserve. The daily backups are by default kept for 7 days, and are used for the weekly and monthly backups that are retained. There are also properties that govern the day of week for the weekly backup and the date of the month for monthly backup.

Below are the relevant backup properties.

Property	Description
com.agiliance.admin.backup.BackupManager.MaxRetainedBackups	Allows backup based on the execution of the Daily Backup Job, the default value is set as "7"
com.agiliance.backup.dayofWeekToBackupdatabase	Allows backup on the day of the week to be considered, the default value is set as "Friday"
com.agiliance.backup.MaxRetainedWeeklyBackups	Allows backup on weekly bases, the default value is set as "5"
com.agiliance.backup.MaxRetainedMonthlyBackups	Allows backup on monthly bases, the default value is set as "12"
com.agiliance.backup.dateOfMonthToBackupdatabase	Allows backup on which date of the month to be considered for backup the default value is set as "1"

For example, if you wish to keep **n** number of backup files, set the properties as below:

```
com.agiliance.admin.backup.BackupManager.MaxRetainedBackups=n
com.agiliance.backup.MaxRetainedWeeklyBackups=0
com.agiliance.backup.MaxRetainedMonthlyBackups=0
com.agiliance.backup.dayofWeekToBackupdatabase=Null
com.agiliance.backup.dateOfMonthToBackupdatabase=0
```

The above configurations will only back up data for the last n days. They will not back up data on a weekly or monthly basis as is default.

Setting Up Vulnerability Risk Scoring

By default, the Vulnerability Risk Score feature is set up to calculate risk scores for vulnerabilities in RiskVision. You do not need to do anything for the scores to be calculated, other than to ensure vulnerabilities with the required data are present in RiskVision.

When there are CVE mappings to vulnerabilities, data from these CVEs is used to calculate the Vulnerability Risk Factor. If no CVE mappings to the vulnerability exist, then RiskVision will use data that is available directly from the vulnerability instance, if sufficient data is available to calculate the Vulnerability Risk Factor.

The formula that RiskVision uses for the vulnerability risk score is as follows:

`Vulnerability Instance Risk Score = Entity Criticality Factor * Vulnerability Risk Factor`

For additional background on the Vulnerability Risk Score feature, please refer to the **Understanding Vulnerability Details** section of the *Threat and Vulnerability Manager User Guide*.

By default, the Entity Criticality Factor is set to be equal to the entity criticality values in the RiskVision database. If a Low-Medium-High value has not been set, then the entity criticality value will be null. A High entity criticality value usually equates to a numerical value of 10, Medium a 7, and Low a 3. However, the values in your database for some entities may differ from these values.

The Vulnerability Risk Factor can be set to be equal to the Enhanced Score or the CVSS Score. By default, it uses the CVSS v2 score. If you want to override this behavior, set the following property value in the `agiliance.properties` file: `vulnerability.risk.factor = enhanced_score`

Note: For the property value change to be recorded in the database, you will need to restart the server.

Changing the Default Vulnerability Risk Score Calculations

You can modify the default vulnerability risk score calculations. For the Entity Criticality Factor, you can change the formula used to calculate the Entity Criticality Factor result, including modifying the formula to add custom attribute variables and mapping numerical values to string values. For example, you could have a custom attribute for whether an entity is in scope for PCI, with a "yes" string value could be equal to 2 and a "no" to 1, such that the risk score would be twice as high if an entity was in scope for PCI.

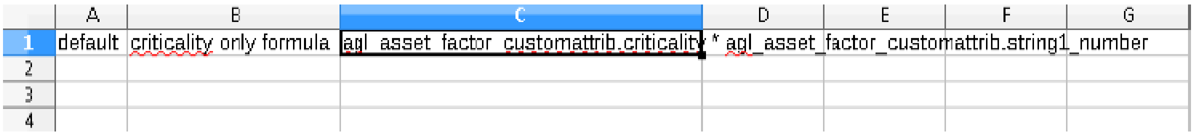
There are two files involved in the calculation of the Entity Criticality Factor. These are as follows:

- Vulnerability Risk Score Entity Criticality Factor Formula Definition - This file is used to define the formula used to calculate the Entity Criticality Factor. Please see the next section for the instructions to modify this file.
- Vulnerability Risk Score Entity Criticality Factor Attribute Mappings - This file is used to map integer values to string values for custom attributes. It is only required if your vulnerability risk score equation uses custom attributes that have string values. Adding and modifying data in this file will be discussed later in this guide.

Modifying the Entity Criticality Factor Equation

As mentioned in the previous section, you use the Vulnerability Risk Score Entity Criticality Factor Formula Definition file to determine the Entity Criticality Factor formula. The Vulnerability Risk Score Entity Criticality Factor Formula Definition file has three columns which define the formula name, description, and formula, respectively. The CSV file can have as many rows as you would like, but you must use the “default” name in column A for the formula that you want to be the active formula.

You can use any name you would like in column B.



	A	B	C	D	E	F	G
1	default	criticality only formula	agl_asset_factor_customattrib.criticality * agl_asset_factor_customattrib.string1_number				
2							
3							
4							

All variables in the formula need to have the following syntax: agl_asset_factor_customattrib .criticality and agl_ asset_factor_customattrib.string1_number, where agl_asset_factor_customattrib is the database table name. This table name, agl_asset_factor_customattrib must precede all the variables, such as criticality. Custom attributes have an additional syntax element. The string number must precede the characters “_number”, such as agl_asset_ factor_customattrib.string12_number and ;agl_asset_factor_customattrib.string25_number

The maximum character length for the formula field is 1,000 characters. The other fields have a maximum length of 20 characters. All fields are case-insensitive.

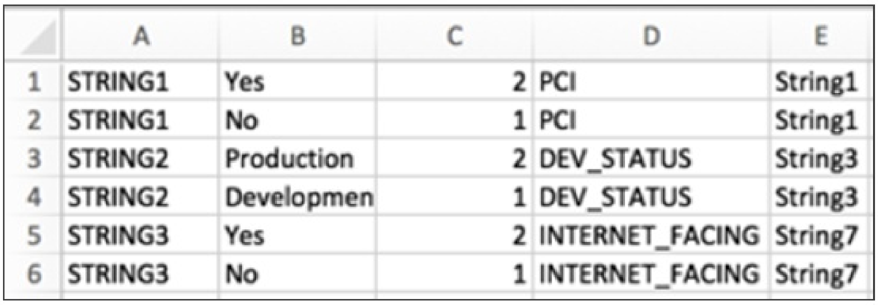
Modifying Custom Attribute String Value Mappings

If you use custom attributes in the vulnerability risk score equation, there is a good chance that these custom attributes will have string values, such as “yes’ and “no” for PCI. Because the vulnerability risk score equation requires numerical values, these string values must be mapped to numerical values. The Vulnerability Risk Score Entity Criticality Factor Attribute Mappings file provides a way to do this.

The Vulnerability Risk Score Entity Criticality Factor Attribute Mappings file allows you to assign numerical values to string values. It has the following four columns:

- String number, which is the string number in the spreadsheet. Since there can be a maximum of 4 strings, then the string number should not exceed 4. If criticality is being used in the Entity Criticality Factor, then there can be a maximum of 3 strings.
- String value, such as “yes” or “no”. This is the attribute value that will appear in the RiskVision user interface.
- Integer value that equates with each string value, such as 1 or 2. This will be the number used to calculate the Entity Criticality Factor for entities when the entity’s string has that value.
- User friendly name, such as PCI, DEV_STATUS, or INTERNET_FACING. Typically, this would be the label associated with the custom attribute location. You can use any name you would like for this field since the field exists for your convenience, and is not used in the risk score calculation or the RiskVision user interface. RiskVision recommends that you use the name that appears for the field in the RiskVision user interface.
- Number of the custom string attribute that represents this attribute. In the below example, String1 is used for PCI, String3 for DEV STATUS, and String 7 for INTERNET_FACING.

Following is an example of some values that you might populate in the CSV file:



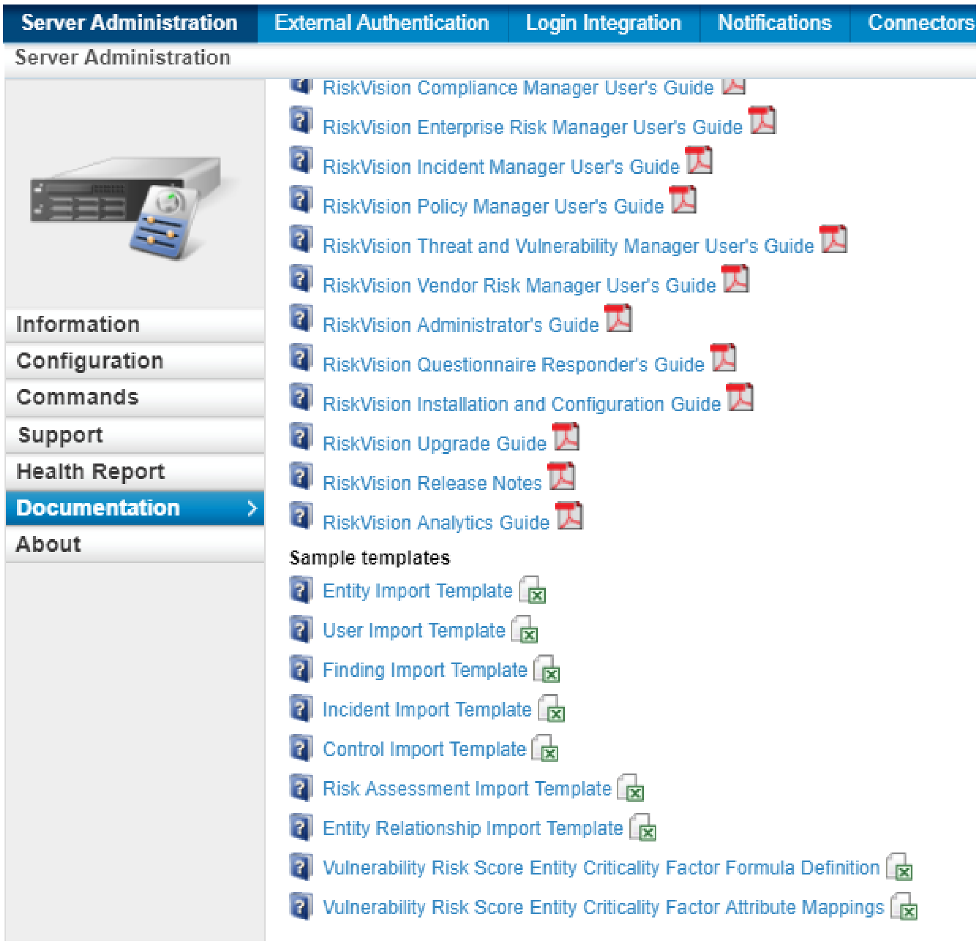
	A	B	C	D	E
1	STRING1	Yes	2	PCI	String1
2	STRING1	No	1	PCI	String1
3	STRING2	Production	2	DEV_STATUS	String3
4	STRING2	Developmen	1	DEV_STATUS	String3
5	STRING3	Yes	2	INTERNET_FACING	String7
6	STRING3	No	1	INTERNET_FACING	String7

The maximum character length for the above fields is 20 characters. All fields are case-insensitive.

Obtaining the Files

You can download the files two files from the **Administration** module in the **Server Administration > Documentation** tab, they are as follows:

1. Vulnerability Risk Score Entity Criticality Factor Formula Definition
2. Vulnerability Risk Score Entity Criticality Factor Attribute Mapping



RiskVision Compliance Manager User's Guide
RiskVision Enterprise Risk Manager User's Guide
RiskVision Incident Manager User's Guide
RiskVision Policy Manager User's Guide
RiskVision Threat and Vulnerability Manager User's Guide
RiskVision Vendor Risk Manager User's Guide
RiskVision Administrator's Guide
RiskVision Questionnaire Responder's Guide
RiskVision Installation and Configuration Guide
RiskVision Upgrade Guide
RiskVision Release Notes
RiskVision Analytics Guide

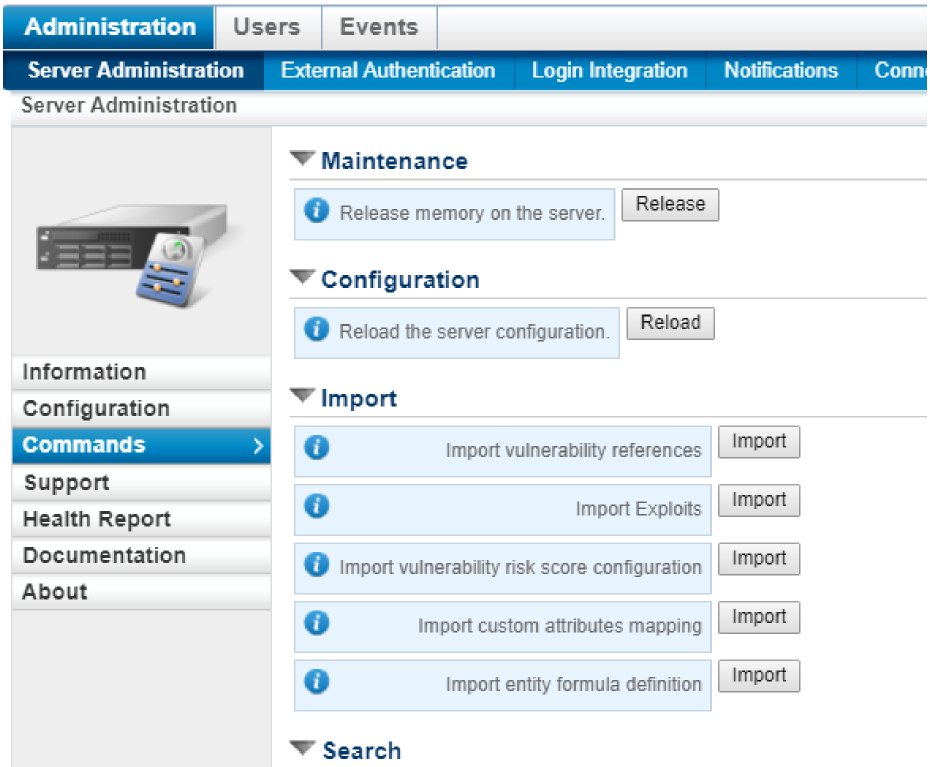
Sample templates

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

Uploading Files

To have the settings in the CSV files take effect, you will need to upload the files in the Administrator application. It is important not to change the names of the CSV files. Before uploading, verify that the names of the files are as follows:

- Vulnerability Risk Score Entity Criticality Factor Formula Definition
- Vulnerability Risk Score Entity Criticality Factor Attribute Mappings



Maintenance

Release memory on the server.

Configuration

Reload the server configuration.

Import

Import vulnerability references

Import Exploits

Import vulnerability risk score configuration

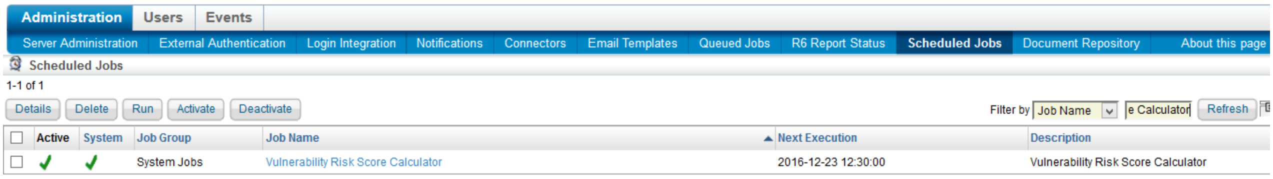
Import custom attributes mapping

Import entity formula definition

Search

Vulnerability Risk Score Calculator Job

Vulnerability risk score calculations are updated when the Vulnerability Risk Score Calculator job runs. By default, the job is set to run once per day at 11:00 PM. You can run the job more frequently. The job only recalculates risk scores for entities whose vulnerabilities or relevant entity attributes have changed, but RiskVision recommends first testing the performance impact of the job in your environment if you decide to run it multiple times per day.



Scheduled Jobs

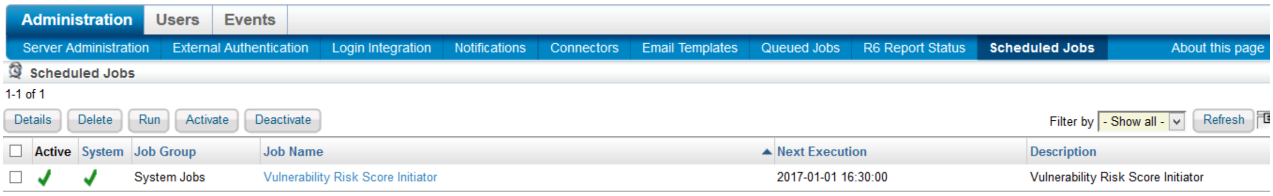
1-1 of 1

Filter by Job Name | e Calculator

□	Active	System	Job Group	Job Name	Next Execution	Description
□	✓	✓	System Jobs	Vulnerability Risk Score Calculator	2016-12-23 12:30:00	Vulnerability Risk Score Calculator

For Vulnerability Risk Factor processing , the property changes to pickup different score system or enhanced score gets picked up during next job run. However, new system will be applicable only to the vulnerabilities/instances changed after the property change. In this case there will be a mix of scores from old and new system.

If you want to apply change of score system throughout the application, then the Vulnerability Risk Score Initiator job will refresh the scores and re-calculate everything based on new score system.



Scheduled Jobs

1-1 of 1

Filter by - Show all -

□	Active	System	Job Group	Job Name	Next Execution	Description
□	✓	✓	System Jobs	Vulnerability Risk Score Initiator	2017-01-01 16:30:00	Vulnerability Risk Score Initiator

Set Default Severity Values

The default severity values of a vulnerability are as follows:

- **High** = 10
- **Medium** = 6
- **Low** = 3
- **N/A** = 10

However, some customers may prefer to use the following values:

- **Critical** = 10
- **High** = 8
- **Medium** = 6
- **Low** = 4
- **Informational** = 2

In order to set these values, users must follow the below steps:

To change the default severity values:

1. Navigate to the **%AGILIANCE_HOME%\config\** folder.
2. Open the **agiliance.properties** file.
3. Set the following properties as specified:
    - `com.Agiliance.Vulnerability.Severity.Assignment=false`
    - `vulnerability.severity.value=Critical,10;High,8;Medium,6;Low,4;Informational,2`
4. Close the file and restart RiskVision.

About System Users

The RiskVision application authenticates users against an internal user directory. You can add additional users and define user roles in the internal directory. Optionally, you can choose to integrate with an LDAP directory service, such as Active Directory.

The RiskVision application uses a role-based Access Control List (ACL) policy with granular permission configuration. It is possible to define new roles with permission to access specific objects and perform specific operations on those objects, such as view, create, update, and delete. In addition, filters can be used in conjunction with roles to restrict specific permissions for a user assigned one or more roles. So, when a user logs in, they are granted the combined permissions of the roles to which they assigned membership and restricted by any access filters that might also be attached to their user account.

The RiskVision solution has the following types of user accounts:

- **System administrator** : User accounts in the system space that manage the host computer settings.
- **System users**: Accounts that participate in assessments, manage assessment data, and connectors for their own space. This is the only type of user account that has roles you can customize.
- **Vendor users**: Limited-access accounts for questionnaire-taking and vendor user management only. Vendor accounts allow an organization to involve third-parties in the risk assessment process.

Assigning a Role to a User

A role allows a user to log in to the and determines the user's privileges, access rights, and the type of objects the user can own. The permission and access rights associated with roles are cumulative.

The user has the highest level of permission and all access rights granted by the roles assigned to them. For example, if the user had one role with Entity view and another with Entity manage, the user can manage entities.

To assign a role:

1. In the Administration application, go to **Users** > **Users**.
2. Select the user and click **Details**.
3. Click the **Roles** tab.
4. Click **Edit**.
5. Select a role from the **Available Role** list and click the right-arrow.

   The role moves into the **Assigned Roles** list.
6. Click **Save**.

Assigning an Access Filter

An access filter allows the user to perform actions, which their role permission allows, on entities. You can assign access filters directly to the user or by assigning a role with an access filter. Access filters rights are cumulative, the user can access all entities that match the conditions in the filters assigned to them.

For example,consider an user who has a role with Managed Entities access filter that limits them to see only managed entities. If this user is directly assigned a My Entities filter that constrains them to act on only entities that they own, the two access filters expand, rather than narrow, the number of entities the user can see. In the example, the user can perform actions on all managed entities and all the entities they own, even unmanaged entities that they own.

To assign an access filter:

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

2. Select the user and click **Details**.

3. Click the **Access Filter** tab.

4. Click **Edit** and then **Add Filters**.

5. Expand the folders and select all the **Entity Filters** you want to assign.

   The filter list displays Entity Filters only.

6. Click **OK**.

7. Click **Save**.

The access filter is applied the next time the user logs in.

Creating and Modifying User Accounts

You can create, activate, deactivate, update, or delete user accounts if you have the System User Manage permission.

You must assign a role to a user to allow them to log in to the RiskVision solution. A warning symbol displays next to users who are configured without a role.

To configure user account:

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

2. To create a new account, click **New**.

   To modify an existing account, select a user, click Details, and then click Edit.

3. Enter the user information:

   - User name: The user's login ID. Note that user name cannot be changed once the user account is created.

   - Password: A password for the RiskVision solution. Passwords must be at least eight characters long, and must contain at least one digit and at least one alphabetic character.

   - Confirm password: Retype the password.

   - First name: Type the user's first name as you want it to display in other fields of the RiskVision solution, such as Entity Ownership. Many default e-mail templates use the recipient's first name as a greeting.

   - Middle initial: Type a single letter.

   - Last name: Type the user's last name as you want it to display in the RiskVision solution.

   - E-mail address: Type the full e-mail address of the user. Users enter their e-mail address (or User name) when they log in to the RiskVision solution. They also receive notifications at this address.

   - Force Password Change: Check the box to require that the user change their password the next time they log in.

   - Allow user to access RiskVision: Activate or deactivate an user account. An user account that is deactivated (suspended) will not allow a user to access the RiskVision.

4. Click **OK** to add the user or **Save** if you are modifying an existing account.

The user is created and the details page displays.

Deleting Users

You can only delete unassigned users--that is, a user who does not own any active programs, entities, or content and is not assigned as a workflow stage stakeholder. You can choose to delete users one by one or all at once.

Note the following behavior when deleting users one by one:

- If you try to delete a user who has not performed any activities, a message to provide your confirmation to delete the user appears.
- If you try to delete a user who has performed more or less activities, a message listing all the objects owned by the user appears. In addition, it is recommended deactivating the user.

Note the following behavior when deleting multiple users at once:

- A message appears without listing any underlying objects owned by the users, but displays the users who can be deleted and deactivated.

To delete a user:

1. In the Administration application, go to **Users** > **Users**.
2. Select the user you want to remove.
3. Click **Delete**.
4. In the confirmation dialog, click **OK**.

The user account is removed from the system. If the user is logged in, their session is terminated.

Resetting A User's Password

Suspending User Accounts

You can suspend a user account to retain important assessment-related associations for closed assessments. You can choose to deactivate users one by one or many at once.

Note the following behavior when deactivating users one by one:

- If the user has not performed any activities, a message to provide your confirmation to deactivate the user appears.
- If the user has performed more or less activities, a message listing the objects owned by the user including any kind of activities the user has performed, with a confirmation to deactivate the user appears.

Note the following behavior when deactivating multiple users at once:

- A message appears without listing any underlying objects owned by the users, but displays the users who can be deactivated. In addition, it is recommended deactivating the users one by one to become aware of any underlying objects owned by the users.

To suspend multiple user accounts at a time:

1. In the Administration application, go to **Users** > **Users**.
2. Select a user and then select **Deactivate** in the More Actions... drop-down list.
3. When a confirmation box appears asking you whether to deactivate the user, then click **OK**. The icon next to user is grayed out.

To suspend user accounts one by one:

1. Select the user and click **Details**.
2. On the **Information** tab, click **Edit**.
3. Clear the box next to Allow user to access RiskVision field. The icon next to the user is grayed out.
4. Click **Save**.

The account is immediately suspended. If the user is logged in, their session is terminated.

Locking User Accounts

To reduce the chances that an unauthorized user will be able to compromise the account of an authorized RiskVision application user, suggests that you lock user accounts after a predefined number of consecutive login attempts. This is only applicable to internal users (users who authenticate against the RiskVision database), and does not apply to external users (users who authenticate against an LDAP source). RiskVision would then lock any user account that has a greater number of consecutive failed login attempts than the value set in the **password.disableAfterNFailedLogin** property. When an account is locked, the user will not be authenticated even if a user inputs the correct credentials. You will need to follow the steps mentioned below to unlock the user account.

To enable locking of user accounts:

1. Open the `agiliance.properties` file using a text editor
2. Add the `password.disableAfterNFailedLogin =` property.
3. Save the **agiliance.properties** file.
4. To apply the latest changes, do one of the following:
   - Reload the server configuration.
     1. Go to **Administration** > **Server Administration**
     2. Click the **Commands** tab.
     3. Expand the **Configuration** section and click **Reload**.
   - Restart the RiskVision Tomcat service.

Unlocking User Accounts

When you learn from the users that they can no longer access the RiskVision application due to a lock out, you will have to unlock the user accounts. You can unlock user account one at a time or through a batch operation.

Method 1: To unlock user accounts one at a time

1. In the Administration application, go to **Users > Users**. The **Users** page is displayed.
2. Select the user to open its details page, displaying the **Information** tab.
3. Click **Edit** at the upper right-hand corner of the Information tab.
4. Check the box next to the Allow users to access RiskVision option.
5. Click **Save**. The user is unlocked.

Method 2: To unlock user accounts through a batch operation

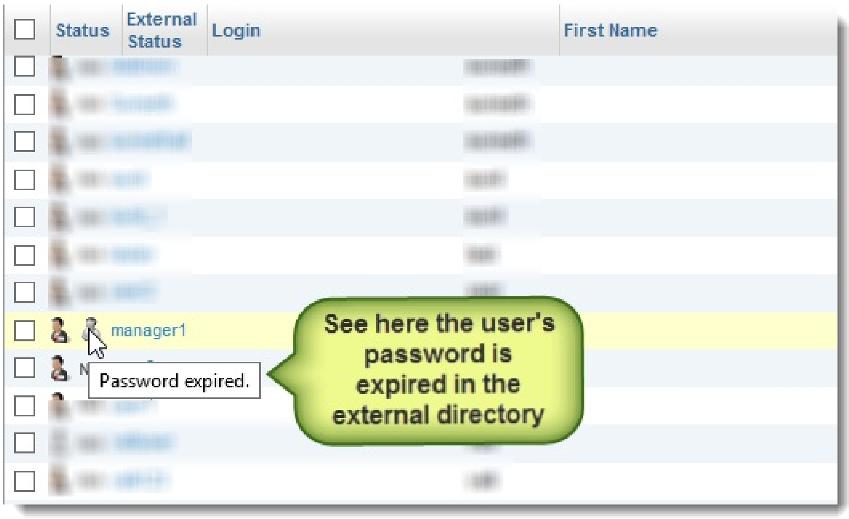
1. In the Administration application, go to **Users > Users**. The **Users** page is displayed.
2. Check the corresponding box in each user's row and select **Activate** in the More Actions drop-down list. The users are unlocked.

The method 2 can also be useful in unlocking the user accounts one at a time. It is entirely up to you, which method to prefer when unlocking the user accounts.

Understanding User Status

The Users grid lists internal and external users, and allows you to see which user is active and inactive. In this section, you will understand the representation of active and inactive user status. You will also understand how to determine the underlying reason for inactive status. All the active users are shown by the icon and inactive users are shown by the same icon in greyed out style. The icon in the **Status** column of a user row determines that you have authenticated an internal user and therefore the icon symbolizes that an internal user is active. Whereas the icons available in the **External Status** and **Status** columns of a user row determines that you have authenticated an external user and therefore the icons symbolize that an external user is active.

When an external user becomes inactive in an external authentication directory, that user becomes inactive in the RiskVision as well and the icon is automatically put back in the greyed out style. To know the underlying reason for inactiveness, hover on the icon available in the **External Status** column and read the tool tip that appears.



Status
External Status
Login
First Name
manager1
See here the user's password is expired in the external directory

Password expired.

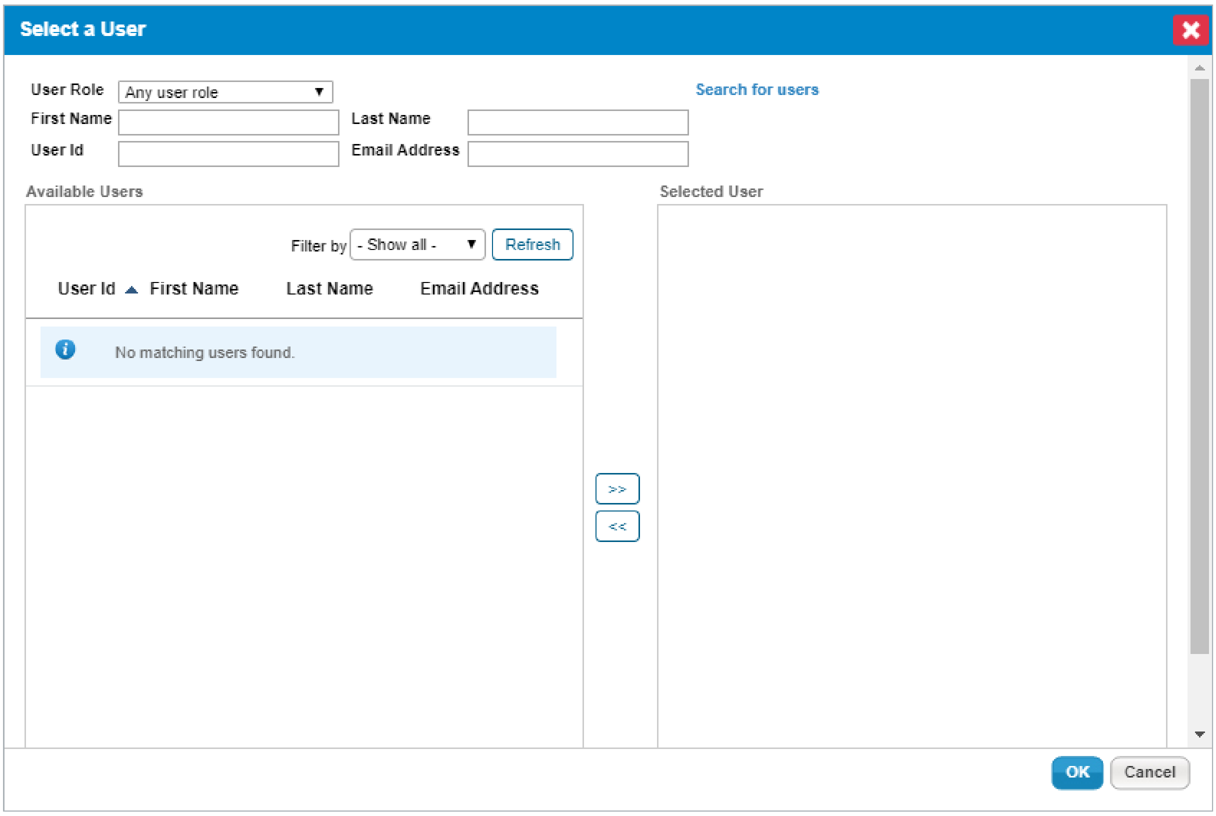
User Picker

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.



User Role: Any user role

Filter by: - Show all -

No matching users found.

The User Picker window.

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

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

Using Search Criteria

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

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

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

Importing Users

In the **RiskVision Administration** module, you can import users along with their roles in the .xls/.xlsx and .xml formats. The default behavior is to force users to change their passwords upon their initial logins to match the in effect password requirements.

Note:

The forcePasswordChange attribute must be entered on the import template if the user performing the import wants to override the default behavior of forcing the imported users to change their passwords upon their initial logins into the RiskVision system. The current default password requirements consist of at least 8 characters, one upper-case letter, one lower-case letter, one special character, and one number. Resolver recommends not overriding this default behavior.

About Roles and Permissions

Roles determine the permission level and access settings of a user. You must assign a role to a user before they can log into the RiskVision solution. The user only sees the RiskVision solution pages, menu options, and entities that are allowed by their role.

About Access to Entities

You can assign access filters to limit which entities a user can view, modify, and be assigned to as an owner. Access filters--that is, Entity type filters--can be assigned to roles as well as directly to a user. The access filters are cumulative, that is if a user has multiple filters assigned to them, they see all the entities that match each filter.

About Role Privileges and Permissions

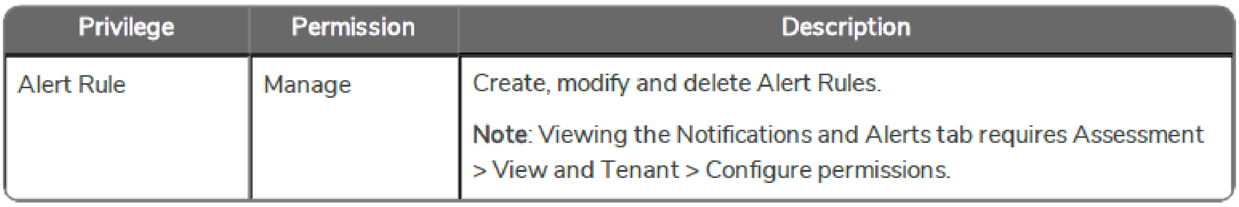
Role assignment determines the RiskVision solution user permissions. A privilege is an object or set of objects, typically associated with an RiskVision solution page. Permission is the type of action you can grant to the user. Role permissions are cumulative, that is a user is granted the highest level of permission for the privileges in all the roles assigned to them. For example, if a user is assigned two roles, the first has Assessment View and second has Assessment Manage, the user can manage assessments.

If you grant a role Manage privileges, also grant View privileges to avoid confusion. If a user has Manage but not View privileges, they will not be able to see objects, such as Findings, that they need to manage.

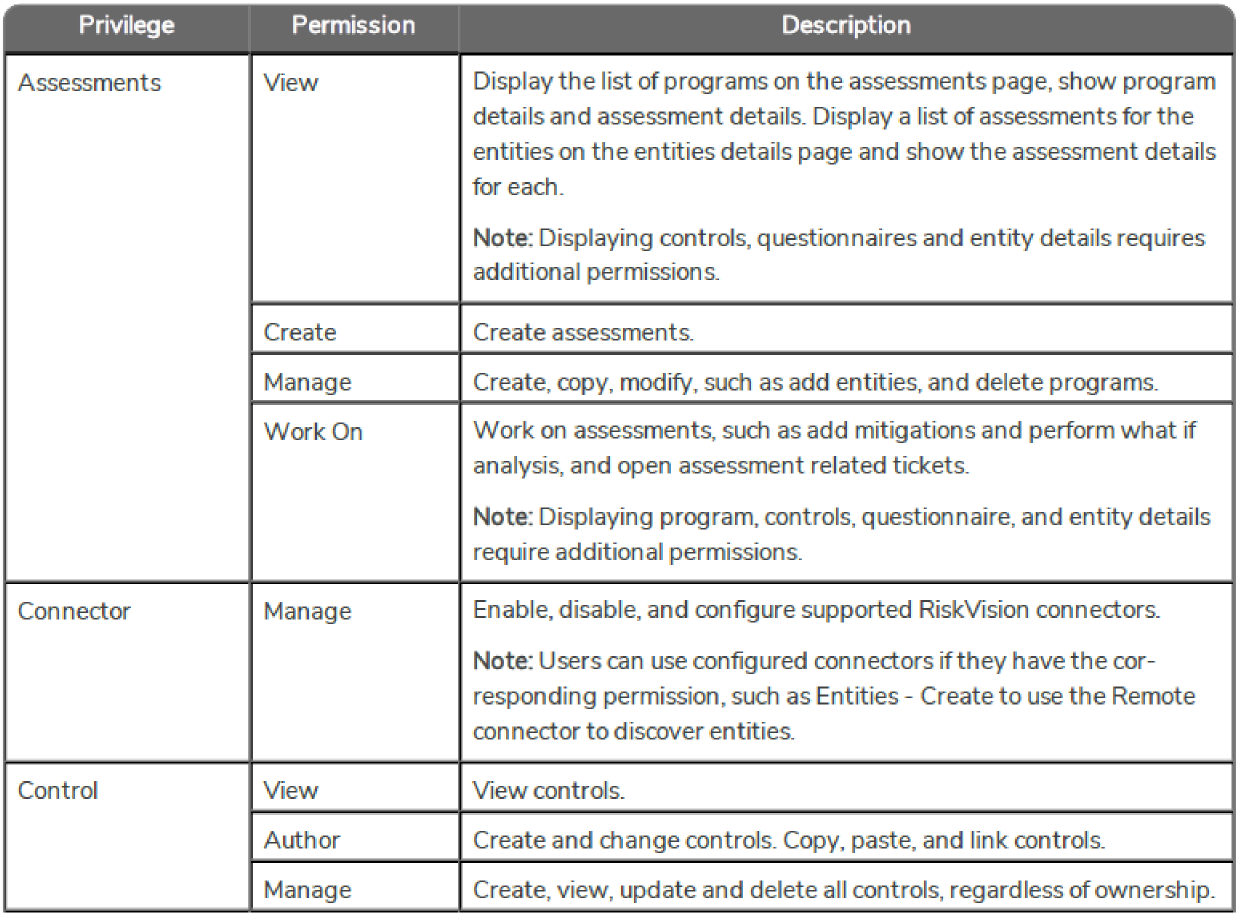
Permissions that are not assigned to any role are shown in **red**. In general, each permission must be assigned to at least one role that is, in turn, assigned to at least one user.

You cannot explicitly deny or restrict a privilege with respect to a user, only with respect to a role.

Your user role must have the System User Manage permission to create, modify, or delete a role.



Privilege	Permission	Description
Alert Rule	Manage	Create, modify and delete Alert Rules. **Note**: Viewing the Notifications and Alerts tab requires Assessment > View and Tenant > Configure permissions.



Privilege	Permission	Description
Assessments	View	Display the list of programs on the assessments page, show program details and assessment details. Display a list of assessments for the entities on the entities details page and show the assessment details for each. **Note:** Displaying controls, questionnaires and entity details requires additional permissions.
	Create	Create assessments.
	Manage	Create, copy, modify, such as add entities, and delete programs.
	Work On	Work on assessments, such as add mitigations and perform what if analysis, and open assessment related tickets. **Note:** Displaying program, controls, questionnaire, and entity details require additional permissions.
Connector	Manage	Enable, disable, and configure supported RiskVision connectors. **Note:** Users can use configured connectors if they have the corresponding permission, such as Entities - Create to use the Remote connector to discover entities.
Control	View	View controls.
	Author	Create and change controls. Copy, paste, and link controls.
	Manage	Create, view, update and delete all controls, regardless of ownership.

Custom Charts	Author	Create, edit, and delete custom charts.
Dashboards and Reports	View	Display reports.
	Author	Create, delete, modify, run, and schedule run time of reports.
	Save	Create reports that others can view, copy, and run.
Data Feed	View	View data feeds.
	Manage	Create new and delete data feeds.
Design Documents	View	View documents.
	Manage	Create, modify, and delete documents.
Design Test	View	View Control design tests.
	Manage	Create, modify, and delete Control design tests.

Privilege	Permission	Description
Document Repository	View	View shared documents in the document repository.
	Manage	Upload new documents, delete documents and modify ownership roles, regardless of ownership in the document repository.
	Create	Create documents or web references in the document repository.
	Update	Update the description of a group and the document collection.
	Delete	Delete groups and document collections.
	Note: To perform create, update or delete, view permission is required.	
Effectiveness Test	View	View Control effectiveness tests.
	Manage	Create, modify, and delete Control effectiveness tests.
E-mail Template	View	Display and export E-mail Templates.
	Manage	Create new templates, import and export templates, and modify and delete existing templates. **Note:** To display the Menu item and Dashboard Template page, view is required.

Privilege	Permission	Description
Entity	View	Display the list of entities on the entities page and view details of each. **Note:** To display the list of assessments the entity is in, grant Program and Assessments - View permission.
	Manage	Manage entities in dynamic groups. Create, modify, and delete dynamic groups.
	Update	Modify entities owned by this user..
	Update All	Update any entity, regardless of ownership.
	Create	Create new entities. This permission is also required to use a connector to discover entities.
	Delete	Remove entities.
Event	View	Display the Administration > Event page.
Exception	View	Display the exceptions assigned to you.
	Approve	Review an exception request and approve, delegate, or reject the request.
	Request	Open an exception request.
	Delete	Delete exceptions assigned to you.
Filter	View	Display filters.
	Update	Create new filters, modify existing filters, and add/remove filter groups.
Finding	View	View a list of findings.
	Manage	Create, update and delete a finding and its objects, such as response, ticket and exception.
	Update	Update existing findings, modify the general settings, risk assessment and attachments.
	Create	Create findings and responses.
	Delete	Delete findings and all its objects.
	Note: To perform create, update or delete, view permission is required.	
Incident	View	Display incidents assigned to the user.
	Update	Update existing incidents, modify the settings and manage attachments, add and remove actions, and open incident related tickets.
	Manage	Remove, import, and export incidents.
	Create	Open an incident and modify it until it is submitted.
Notification	View	Display the message center.

Privilege	Permission	Description
Policy	View	Display only the deployed policies.
	Author	Create and change policies.
	Manage	Create, edit, delete all policies, regardless of ownership.
Profile	View	Display a list of control target profiles and view details.
	Author	Create, delete, copy, and modify control target profiles.
Program	View	Display and run reports for all programs in the system.
	Update	Modify any program in the system.
	Manage	Manage any program in the system.
Questionnaire	View Submitted Questionnaires	Display grid of questionnaires that are submitted by the stakeholder.
	Answer	Display grid of Questionnaires that are assigned to the stakeholder. Respond to questionnaire questions.
	Author	Create, delete, copy, and modify questionnaire questions.
	Review	Accept, reject, and delegate the answers provided by questionnaire responders.
Questionnaire Preferences	View	Display a list of preferences that questionnaire authors can set.
	Manage	Create, delete, copy, and modify preferences that questionnaire authors can set for questionnaires.
Queued Job	View	Display a list of jobs that are waiting to run. Enables the Queued Jobs and Report Status tabs.
Queued Notification	View	Display a list of the notifications that are going to be sent.
Report Template	View	Display and export Report Templates. **Note:** To display the Report Templates under the Analytics menu, Dashboard Template view and Dashboards and Reports view is required.
	Manage	Create new templates, import and export templates, and modify and delete existing templates. **Note:** To manage the report templates, view is required.
Risk	View	Display the risk configurations and details of each risk.
	Author	Create, delete, copy, and modify risks.
Scheduled Job	View	Display a list of jobs that are scheduled to run.
	Manage	Cancel, delay, and reschedule jobs.

Server	Manage	Configure RiskVision solution settings.
System User	Manage	Create, delete, modify, import and active/suspend user accounts.
	Access Delegation	Allows delegating the user account to another user.
Team	View	Display a list of teams on the Administration > User & Roles page.
	Manage	Create, delete, add and remove members from Teams.
Tenant	Configure	Manage Ownership types, Policy Configuration, and Entity Configuration settings.
	Configure UI	Change labels and other aspects of the user interface. **Note**: This permission is disabled by default.

Privilege	Permission	Description
Threats and Vulnerabilities	View	Display a list of threats, vulnerabilities, weaknesses, and so on.
	Manage	Manage Threat & Vulnerability Manager settings.
	Update	Modify threats, vulnerabilities, weaknesses, and so on.
	Create	Create new objects.
	Delete	Delete tickets.
Ticket	View	Display a list of tickets.
	Manage	Create and modify tickets.
	Update	Modify the settings of a ticket.
	Create	Open new tickets.
	Manage Objects	Manage (add, remove) objects that are linked to tickets.
	Classify	Classify ticket objects.
	Delete	Delete ticket objects.
Vendor	View	Display a list of vendors.
	Update	Change an existing vendor's settings.
	Create	Add a new vendor.
	Delete	Remove a vendor.
	Configure	Configure vendors.

Vendor Service	View	Display a list of services provided by vendors.
	Manage	Create, delete, copy, and modify vendor services.
Vendor User	View	Display a list of the users in the vendor domain.
	Update	Modify the settings of users in the vendor domain.
	Create	Add users to a vendor domain.
	Delete	Remove users from a vendor domain.
Workflow	View	Display a list of workflows.
	Update	Change the settings of existing workflows.

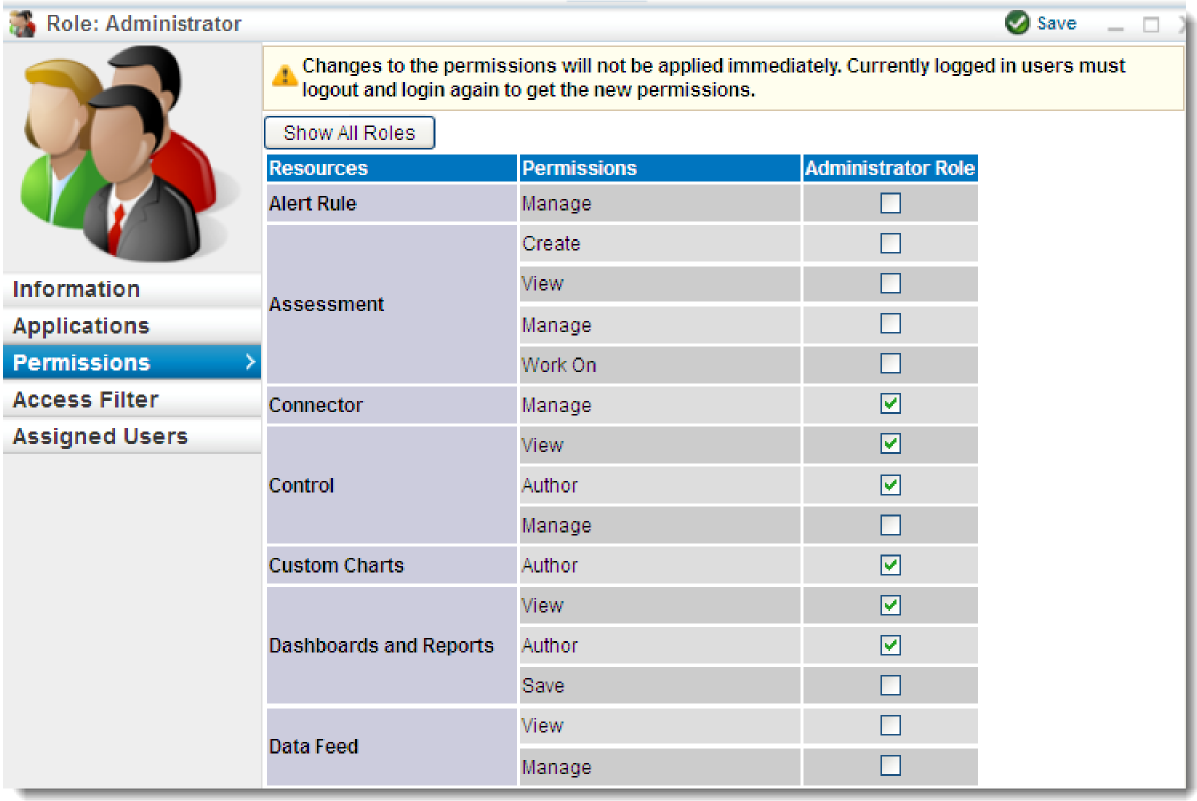
Configuring a Role

When you modify a role, users assigned to the role have the new privilege and access settings the next time they log in. If the user is logged in when you change the role, the new settings will apply within a few minutes.

If you assign more than one role to a user, the user has the highest level of permission in all the roles for each privilege and can access all the entities of each role.

To modify permissions:

1. In the Administration application, go to **Users** > **Roles**.
2. Select a role and click **Details**.
3. Go to the **Permissions** tab and click **Edit**.



Changes to the permissions will not be applied immediately. Currently logged in users must logout and login again to get the new permissions.

Resources	Permissions	Administrator Role
Alert Rule	Manage	□
Assessment	Create	□
	View	□
	Manage	□
	Work On	□
Connector	Manage	☑
Control	View	☑
	Author	☑
	Manage	□
Custom Charts	Author	☑
Dashboards and Reports	View	☑
	Author	☑
	Save	□
Data Feed	View	□
	Manage	□

1. To grant a permission to a role, check the box that is available next to the permission level of a resource type .
2. To remove a permission, clear the selection for that particular permission.
3. Click **Save** when you finish making the changes.

Warning: Clicking **X** at the top right corner of the pane, instead of clicking**Save**, changes the permissions.

To manage entity access for a role:

1. In the Administration application, go to **Users** > **Roles**.

2. Select a role, go to the **Access Filters** tab, and click **Add Filter**.

3. The **Filter** dialog appears. You can apply an **Entity** and **Incident** filter type for a role. Then select the filter type drop-down box to apply a filter based on an entity or an incident.

4. Expand the **Filter** tree to select the desired filter and then click **OK**.

   To delete a filter, select a filter and then click **Delete**.

To manage a role:

1. In the Administration application, go to **Users** > **Roles**.

2. Select a role, then go to the **Assigned Users** tab to view any users that are assigned to that role.

3. To add a user, click **Add**. The **Select Users** dialog appears. In the select user drop-down box, choose the same role that appears on the top-left side of the Role's pane or enter text in the **User Name** field and then click **Search** for users. Based on your search criteria, the usernames appear for you to make a selection. Select a user name and then click **OK**.

4. To remove a user, select a username and then click **Remove**.

Note: By default, all users with the Incident Manage permission can create new incident types and subtypes. If you want to restrict users with the Incident Manage permission from creating new incident types and subtypes, you can use the allow.incident.type.subtype.creation.toRole=User_Role property value to require that, in addition to having to have Manage permissions, users have a specific role in order to be able to create new incident types and subtypes

Create a New Role

A role defines what level of permissions the user has for each RiskVision application and which entities the user can access.

To create a new role:

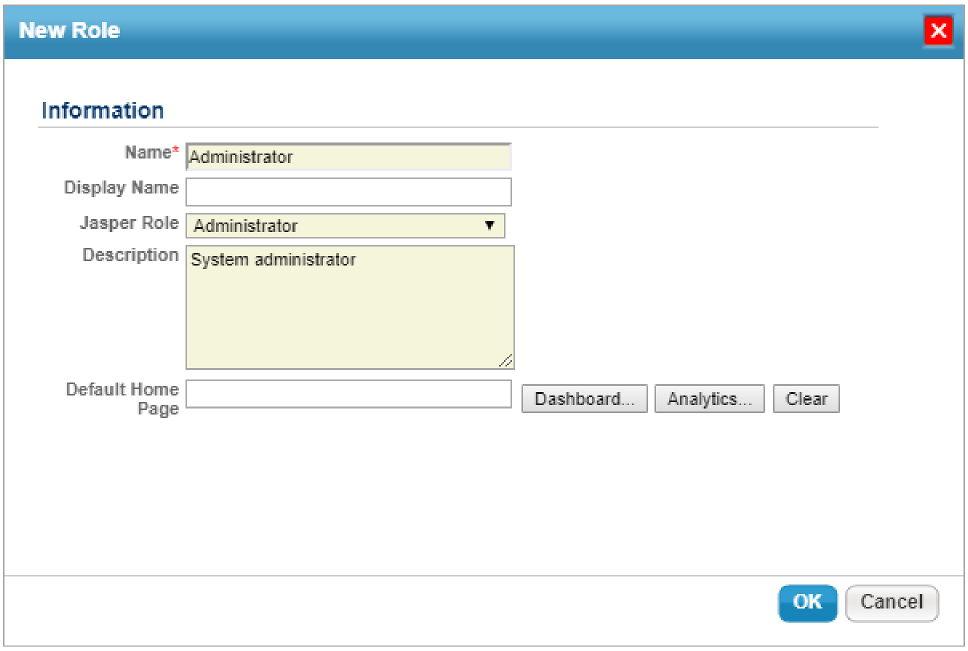
1. In the Administration application, go to **Users** > **Roles**, and click **New**.

2. Enter a name for the role in the **Name** field.

3. **Optional:** If needed, enter an alternate display name for the role in the **Display Name** field. If this field is left blank, the display name will automatically be assigned the role name.

4. **Optional:** If this user needs to access the JasperReports Server, select the applicable role from the**Jasper Role** dropdown menu.

5. **Optional:** Enter a summary of the role in the **Description** field.



New Role

Information

Name* Administrator

Display Name

Jasper Role Administrator

Description System administrator

Default Home Page

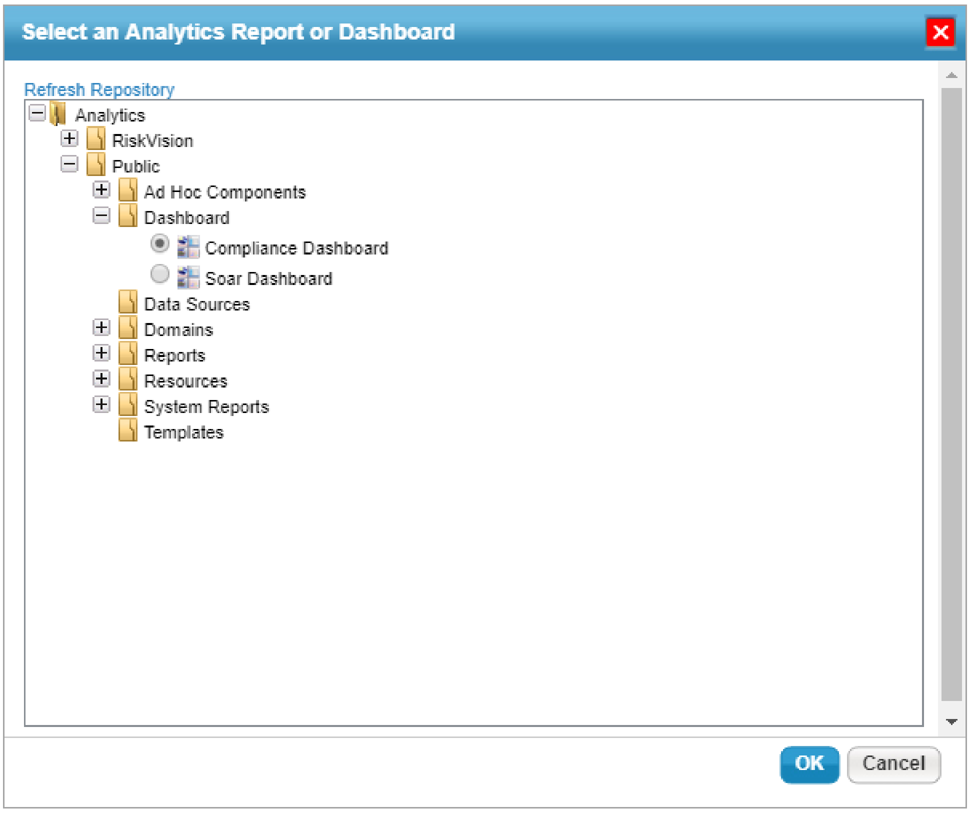
The New Role window.

6. **Optional:** To select a dashboard or report to display on the **Welcome** page for users in this role:

    a. Click the **Analytics...** button beside the **Default Home Page** field.

    b. Click the **+** icon beside a folder in the tree to display sub-folders as needed.

    c. Navigate to the location of the report or dashboard you wish to select, then click the radio button to select it. If the report was recently added and is not appearing in the tree, click **Refresh Repository** to load it.



d. Click **OK** to close the window.

> Any selections made by end-users in the Dashboards settings will override any default home page selections made by an administrator.

7. Click **OK** to save the role.

Once the role has been saved, you can modify its permissions. See the Configuring a Role article for more information.

Assigning JasperReports Server Role

Access to the JasperReports Server is controlled by the Server and Dashboards and Reports permissions that are assigned to a RiskVision role. The New Role dialog allows you to specifically assign a Jasper role. You can utilize this dialog to assign a default dual role when users are imported from an external directory. This makes it easier to administer RiskVision and Jasper roles together. Assign a role that is higher in the Jasper role hierarchy, or the Server Manage permission, to manage complex features, such as creating and managing domains, users, roles and permissions, manage repositories, and so on. In JasperReports Server, you can add, delete, enable or disable a Jasper role, or you can simply remove a Jasper role from a RiskVision role.

By default, provides the following Jasper roles to access JasperReports Server:

- User
- Author
- Power User
- Administrator

The following table lists the RiskVision roles that are equivalent to the JasperReports Server roles, and indicates what menus appear when you access the JasperReports Server using the specific permission assigned to a particular role.

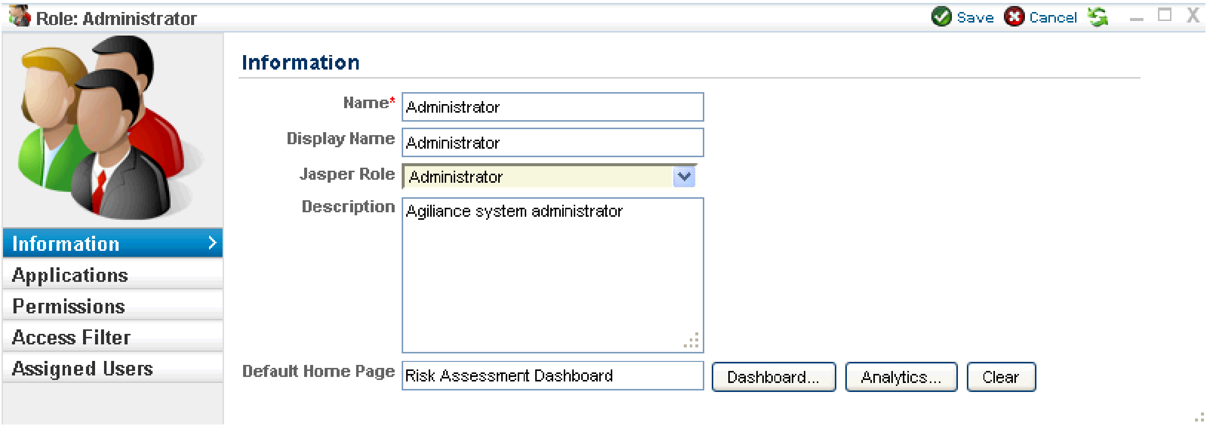
RiskVision Permission		Jasper role	Jaspersoft Feature	Jaspersoft Permission				
				Admin	Write	Read	Delete	Edit
Dashboard/ ReportView		ROLE_USER	Ad hoc			X		
			Report			X		
			Dashboard			X		
			Domain					X
			Input Control					X
			Data Source					X
Dashboard/Report Author		ROLE_AUTHOR	Ad hoc		X	X	X	
			Report		X	X	X	
			Dashboard		X	X	X	
			Domain			X		
			Input Control		X	X	X	
			Data Source			X		
Server Manage		ROLE_ADMINISTRATOR	Ad hoc	X				
			Report	X				
			Dashboard	X				
			Domain			X		
			Input Control	X				
			Data Source			X		
			Role	X				
			User	X				
Any RiskVision role can be mapped to any Jasper role within the Role Editor	User	ROLE_USER	Ad hoc			X		
			Report			X		
			Dashboard			X		
			Domain					X
			Input Control					X
			Data Source					X
	Author	ROLE_AUTHOR	Ad hoc		X	X	X	
			Report		X	X	X	
			Dashboard		X	X	X	
			Domain			X		
			Input Control		X	X	X	
			Data Source			X		
	Administrator	ROLE_ADMINISTRATOR	Ad hoc	X				
			Report	X				
			Dashboard	X				
			Domain	X				
			Input Control	X				
			Data Source			X		
			Role	X				
			User	X				

To assign a Jasper role:

The default and any custom defined roles appear.

The selected role appears in a pane below the list of other roles.

1. In the Administration application, go to **Users** > **Roles**.
2. Select a role and click **Details**.
3. Click **Edit**, select a role in the **Jasper Role** drop-down list, and then click **Save**.



Information

Name*	Administrator
Display Name	Administrator
Jasper Role	Administrator
Description	Agiliance system administrator
Default Home Page	Risk Assessment Dashboard

4. Optionally, click **Analytics**, select the report or dashboard from JasperReports Server to assign a default home page to the user role.

Default Role Settings

Resolver provides the default roles described in the tables below:

- Administrator
- Analyst
- Entity Owner
- Executive
- Finding Administrator
- Incident Administrator
- Internal Auditor
- Questionnaire Responder
- Technical Analyst
- Ticket Administrator
- Vendor Administrator

Administrator

Filter: None

Privileges	Permission
Entity	Manage
Connector	Manage
Control	View, Author
Custom Charts	Author
Dashboards and Reports	View, Author
Email Template	View, Manage
Event	View, Manage
Filter	View, Update
Notification	View
Profile	View, Author
Queued Job	View
Queued Notification	View
Report Templates	View, Manage
Risk	View, Author
Scheduled Job	View, Manage
Server	Manage

Privileges	Permission
Questionnaire	View, Author
Questionnaire Preferences	View, Manage
System User	Manage, Change Others Password
Team	View, Manage
Tenant	Configure
Threats and Vulnerabilities	All
Vendor	All except Configure
Vendor Service	All
Vendor User	All
Workflow	View, Update

Analyst

Filter: All Managed Entities

Privileges	Permission
Assessment	All
Entity	All
Control	Author, View
Exception	All
Filter	View, Update
Finding	View, Manage
Incident	All
Notification	View
Policy	All
Policy Document	All
Profile	View, Author
Queued Job	View
Queued Notification	View

Privileges	Permission
Report	All
Risk	View, Author
Scheduled Job	View
Questionnaire	All
Questionnaire Preferences	View, Manage
Team	View, Manage
Ticket	All
Workflow	View, Update

Entity Owner

Filter: All Managed Entities

Privileges	Permission
Assessment	View, Work On
Entity	View, Update All
Finding	View, Update, Create
Notification	View
Threats and Vulnerabilities	View, Update, Create, Delete
Ticket	View, Update, Create

Executive

Filter: All Managed Entities

Privileges	Permission
Entity	View
Dashboards and Reports	View
Design Documents	View
Design Test	View
Effectiveness Test	View
Notification	View
Threats and Vulnerabilities	View

Privileges	Permission

Finding Administrator

Filter: None

Privileges	Permission
Assessment	View, Work On
Entity	View
Finding	All

Incident Administrator

Filters: None

Privileges	Permission
Incident	All

Internal Auditor

Filter: All Managed Entities

Privileges	Permission
Entity	All
Assessment	All
Control	Author, View
Dashboards and Reports	All
Data Feed	View
Design Documents	All
Design Test	All
Document Repository	All
Effectiveness Test	All
Exception	View, Approve, Request
Finding	View, Update, Create
Notification	View

Privileges	Permission
Policy	View, Author
Policy Document	All
Profile	View, Author
Program	All
Queued Notification	View
Queued Job	View
Risk	All
Questionnaire	All
Team	View, Manage
Threats and Vulnerabilities	All
Ticket	View, Update, Create
Workflow	View, Update

Questionnaire Responder

Filter: All Managed Entities and My Entities

Privileges	Permission
Design Documents	View
Design Test	View
Effectiveness Test	View
Notification	View
Policy Document	View
Questionnaire	Answer, View Submitted Questionnaires

Technical Analyst

Filter: All Managed Entities

Privileges	Permission
Entity	All except Update
Assessment	View

Privileges	Permission
Data Feed	View
Design Documents	View
Design Test	View
Document Repository	View
Effectiveness Test	View, Manage
Exception	Request, Approve
Finding	View, Create, Update
Incident	View, Update, Create
Notification	View
Policy	View
Program	View
Questionnaire	Answer, View Submitted Questionnaires
Threat and Vulnerabilities	All
Ticket	View, Update, Create, Manage, and Classify
Vendor	All except Configure
Vendor Service	All
Vendor User	All

Ticket Administrator

Filter: None

Privileges	Permission
Ticket	All

Vendor Administrator

Filter: All Managed Entities and My Entities

Privileges	Permission
Entity	View, Update All
Design	

Privileges	Permission
Documents	View
Design Test	View
Effectiveness Test	View
Notification	View
Questionnaire	Answer, View Submitted Questionnaires
Vendor	View, Update, Configure
Vendor Service	View, Manage
Vendor User	All

Deleting a Role

You can only delete an unused role. That is, a role that is not assigned to a user or to an ownership type restriction.

To delete a role:

1. In the Administration application, go to **Users** > **Roles**.

2. Select the roles you want to remove.

3. Click **Delete**.

4. In the confirmation dialog, click **OK**.

The role is removed from the system.

To display assigned users, select the role, click **Details** and then click **Assigned Users**.

Managing Teams

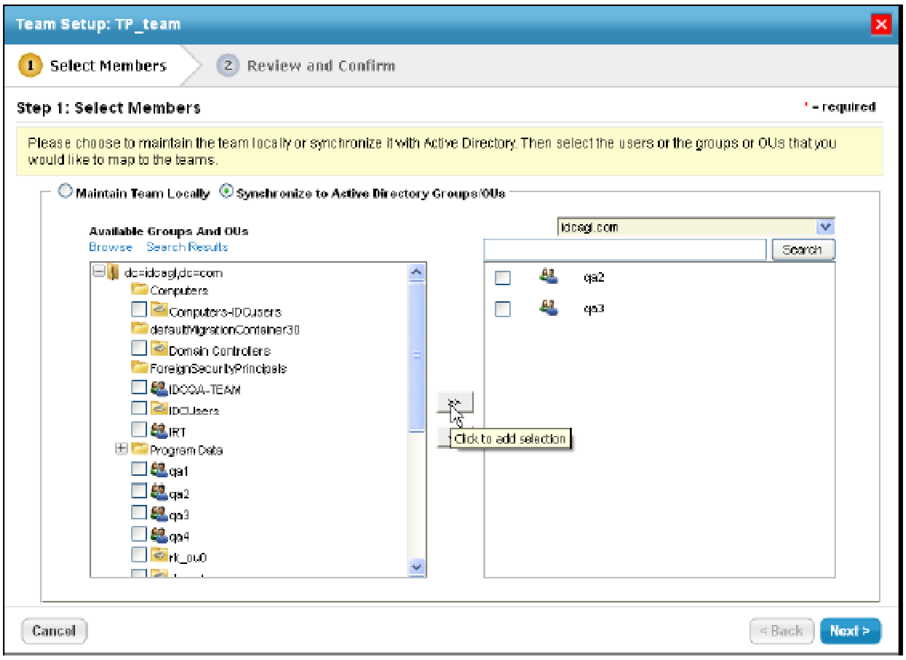
Teams are named groups of system users. Users with sufficient permissions can add and remove members to and from a team. The last member of a team can only be removed if the team is unassigned; that is, if the team is not a stakeholder in a workflow or an owner of an assessment, entity, and so on.

Teams can be synchronized with LDAP groups. For more information, see Mapping External User Attributes.

Note: To manage teams and their members, you must have Team View and Team Manage permissions.

To add members to a team:

1. Open the **Administration** application.
2. Go to **Users > Teams.**
3. Select a team and click **Details**.
4. Click **Add Team Members** to open the **Team Setup wizard.**



Team Setup: TP_team

1 Select Members 2 Review and Confirm

Step 1: Select Members * = required

Please choose to maintain the team locally or synchronize it with Active Directory. Then select the users or the groups or OUs that you would like to map to the teams.

○ Maintain Team Locally ● Synchronize to Active Directory Groups/OUs

Available Groups And OUs

idcagl.com

The Team Setup wizard.

5. Select team members using one of the following methods:
   - Choose **Maintain Team Locally.**
     1. Select a role from the **User Role** dropdown list, or enter the search text in the User Name text box, then click **Search** for users.
     2. Select the users you want to add. To select multiple users, use CTRL or SHIFT on your keyboard.
     3. Click **Next** to continue.
   - Choose **Synchronize to Active Directory Groups/OUs** to add external team members if you have configured an LDAP server.
     1. Select a domain from the drop-down list.
     2. Select a group or organization unit (OU). To find and select a particular group or OU, enter the search text and then click **Search**.
     3. Click the right arrow to make the selection.
     4. Click **Next** to continue.
6. Click the number of users hyperlink to see the members of a group or organization unit (OU) mapped using an LDAP directory.
7. Click **Finish** to exit the wizard.

To remove members:

1. Open the **Administration** application.
2. Go to **Users > Teams.**

3. Select a team and click **Details**.
4. Check the box next to the members you want to remove and click **Remove**.
5. Click **OK.**

Creating Teams

Creating Teams

A team is a group of system users that can be assigned as the owner of entities, policy packs, assessments, and as workflow stage stakeholders.

To assign a team to an assessment, every member of the team must have a role with Programs and Assessment Manage permission.

To create a new team:

1. In the Administration application, go to **Users** > **Teams** and click **New**.
2. The New Team dialog appears.
3. Enter the team information:
   - **Name** : Type the display name of the team. This is the name that displays in the team list on the user selection dialog.
   - **Display Name**: Enter a name to display in the team list on the user selection dialog.
   - **Description**: Enter details that describe the team.
4. Click **OK**.

The team is created.

See also

About Teams

Deleting Teams

You can only remove teams that are not assigned as an owner or stakeholder in an active assessment. Deleting an team does not affect the team member's individual user accounts.

To delete a team:

1. In the Administration application, go to **Users** > **Teams**.
2. Select the team.
3. Click **Delete**.

The team is no longer available for assignment.

About Vendors

A vendor is one or more persons outside your own enterprise who provide or manage goods (entities) or provide a service that you want to apply and monitor control compliance and calculate risk.

Vendor information is accessed, managed, and stored in the following manner:

- **Vendor entity**. An object to which you can assign controls and risks in an assessment.
- **Vendor contact**.Each vendor can have multiple accounts, each of which is referred to as a vendor contact. There will be one Primary Vendor Contact and 0 or more regular vendor contacts.
- **Vendor account**. A group of external users, managed by the vendor administrator, that can respond to questionnaires.
- **Vendor administrator**. The vendor administrator manages the account, including questionnaires, and delegates questionnaires and questions to vendor users.
- **Vendor engagement (Vendor Service)**. When users create a new vendor within the Vendor Risk Manager Application, by default an engagement or service is automatically created and associated with that vendor.

Other than the Primary Vendor Contact which is able to see responses to questions delegated to regular vendor users (i.e. contacts), regular vendor users for the same vendor are unable to see each other's questionnaire responses. In no case can vendor contacts from one vendor be able to see submissions of another vendor. Vendor contacts, even for the same vendor, cannot see each others questionnaires and responses, including evidence.

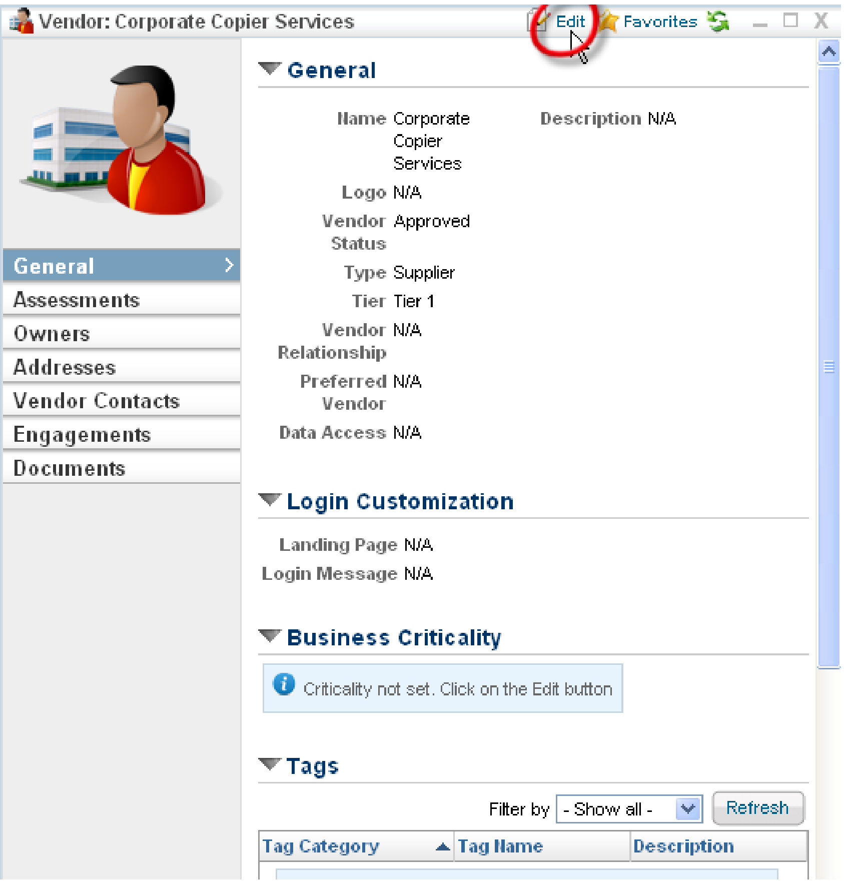
Configuring Vendor Accounts

Each vendor on the system is represented as an entity and has user account information on the Users page. When you add a vendor, the RiskVision solution creates an entity and a user account.

You can add, remove, and update general information for the vendor, such as name and address, from either the Entity page or the Users & Roles page.

To configure a vendor:

1. In the Vendor Risk Manager application, go to **Vendors** > **Vendors**, and select the desired vendor to open its details.



Vendor: Corporate Copier Services

General

Name Corporate Copier Services

Description N/A

Logo N/A

Vendor Status Approved

Type Supplier

Tier Tier 1

Vendor Relationship N/A

Preferred Vendor N/A

Data Access N/A

Login Customization

Landing Page N/A

Login Message N/A

Business Criticality

Criticality not set. Click on the Edit button

Tags

Filter by - Show all -

Tag Category	Tag Name	Description

2. Click a tab (General, Assessments, etc.) to open the corresponding pane.

3. Click **Edit**.

4. Change the settings.

5. Click **Save**.

Managing Vendor Users

The Vendor Contact manages vendor user accounts. The vendor contact can add, remove, and modify accounts and respond to and delegate questionnaires.

You can grant permission for vendor user management in any system user role.

Creating a New Vendor User

Create user accounts for people you want to delegate questionnaire or questionnaire questions.

Vendor users have the same permissions as the default Questionnaire Responder role. You cannot customize the vendor user role

To add a user:

1. Log in using the vendor administrator account.

2. In the Administration application, go to **Users** > **Users**.

3. Click **New**.

4. Enter the user information:

   - **User name. Type the user ID, you cannot modify this setting after the user is created.**

   - **Password. Type a password for the RiskVision solution , it must be at least eight characters long and contain a number or symbol.**

   - **Confirm password. Retype the password.**

   - **First name: Type the user's first name as you want it to display in other fields of the RiskVision solution , such as Entity Ownership.**

   - **Middle initial. Type a single letter.**

   - **Last name. Type the user's last name as you want it to display in the RiskVision solution.**

   - **E-mail address. Type the full e-mail address of the user. Users enter their e-mail address to log in to the RiskVision solution and receive notifications at this address.**

   - **Force password change. Requires the user to change their password the next time they log in.**

   - **Active. Enables and disables the account. A user with a suspended account is locked out of the system.**

5. Click **OK** to add the user.

The user is created and the details page displays.

Removing a User

You can only delete unassigned users. If a user is assigned to a questionnaire or question, you must reassign it.

To delete a user:

1. Log in using the vendor administrator account.

2. In the Administration application, go to **Users** > **Users**.

3. Select the users you want to remove.

4. Click **Delete**.

5. In the confirmation dialog, click **OK**.

The user accounts are removed from the system. If the user is logged in, their session is terminated.

Suspending a user account

You can suspend a user account to prevent them from logging into the RiskVision solution .

To suspend or activate an account:

1. Log in using the vendor administrator account.
2. In the Administration application, go to **Users** > **Users**.
3. Select the user and click **Details**.
4. Click **General**.
5. Click **Edit**.
6. Change Active to **No**.

   To reactivate the account select Yes.
7. Click **Save**.

The account is immediately suspended. If the user is logged in, their session is terminated.

Permitting Access to Vendors Page

Vendor users when set as primary contact automatically receives the Vendor Administrator role to access the RiskVision Application application with no permission to view the Vendors page, on the Home menu. You will need the `com..vendoradmin.permission=Object.VendorUser_` property, along with the permissions defined for the Vendor User object, to allow vendor primary contact users to access the **Home** > **Vendors** page. Adding the property with an appropriate permission enables the primary contact user to manage vendor users.

To add the property:

1. Go to the `%_HOME%\config` directory and open the `.properties` file using a text editor.
2. Add the following property and set one of these permissions: View, Create, Update, or Delete.

   ```
   com..vendoradmin.permission=Object.VendorUser_Update
   ```

   In the property above, the Vendor User Update permission is set. When this permission is set, also ensure that Vendor User View and Vendor User Update permissions are selected in the Permissions tab of Vendor Administrator role.

3. Reload the server configuration to affect the latest changes.

Filters

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

The following describes the options on the filter page:

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

Add a Filter

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

To create a new filter:

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

The filter is available for assignment.

Modifying Filter Conditions

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

To add a condition:

1. Go to **Configuration** > **Filters**.

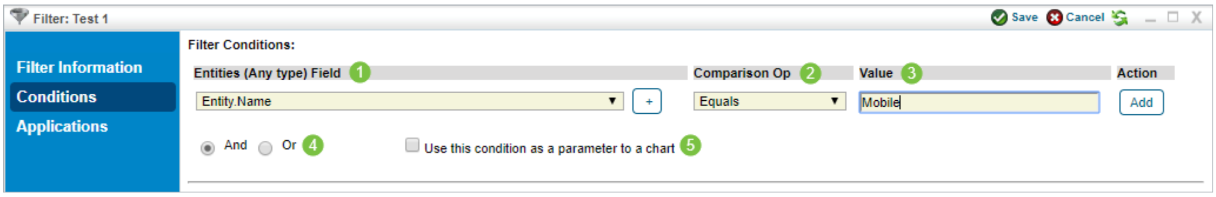
2. Expand the **Filters** tree.

3. Select a filter to open.

4. Click the **Conditions** tab.

5. Click **Edit**, then click **Add.**

6. Enter the Filter conditions as follows:



Filter Conditions:

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

● And ○ Or

□ Use this condition as a parameter to a chart

The Filter Conditions section.

   1. **Attribute**: Select the field where you want to filter the records.

   2. **Operator**: Select the type of operation you want to use to compare the attribute definition and value.

   3. **Value**: Enter a string or number, or select from the dropdown list.

   4. **Conjunctions**: Joins conditions to build an expression that is matched when returned true. Select the same type for all conditions in a filter. Matches filter to combine AND and OR expressions.

   5. **Use this condition as a parameter to a chart**Allow all users to create reports that can drill down to the record level of this field.

7. Click **Save**.

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

To remove a condition:

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

2. Expand the **Filters** tree.

3. Select a filter to open.

4. Click the **Conditions** tab.

5. Click **Edit**, then click the **Delete X** icon next to the condition.

6. Click **Save**.

Removing a Filter

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

To delete a filter:

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

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

3. Click **Delete**.

The filter is no longer available.

Grouping Filters

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

The navigation pane contains the following predefined groups:

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

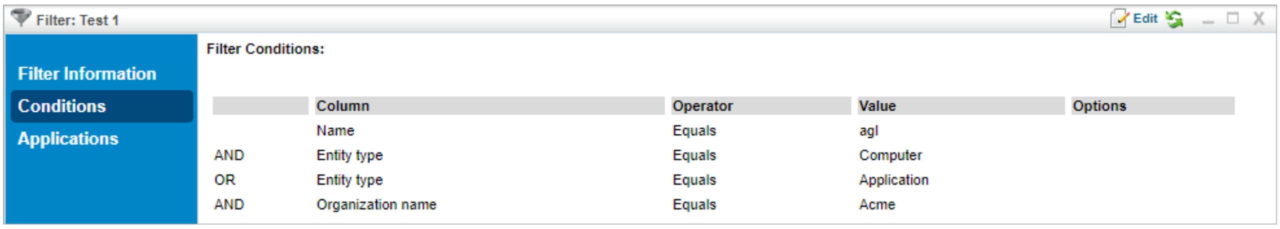
Understanding Complex Filters

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

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

Example

You have the following filter set up:



Filter Conditions:

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

The Conditions tab of a filter.

The filter in this example translates to:

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

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

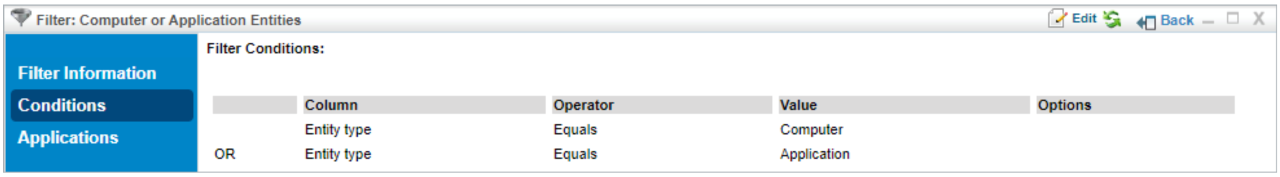
`(Entity Name starts with agl AND Entity Type = Computer) OR (Entity Type = Application AND Organization name = Acme)`

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

If you want this filter to evaluate as:

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

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



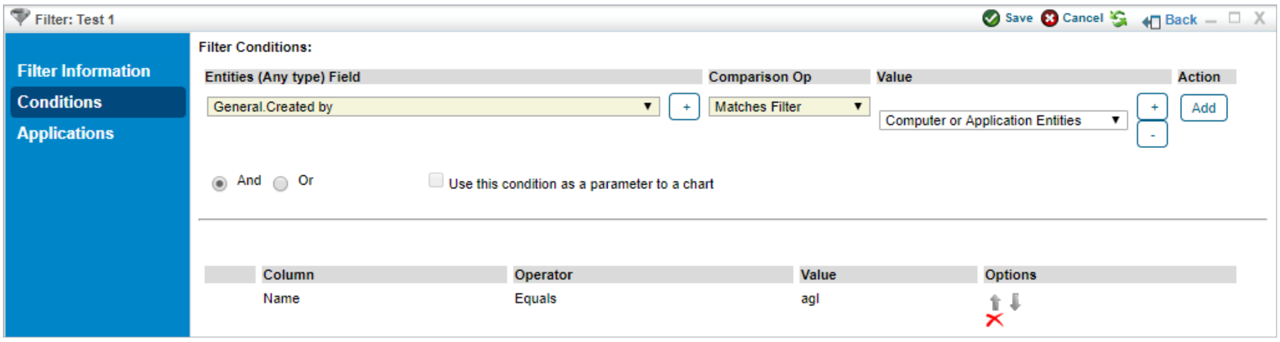
Filter Conditions:

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

A Computer or Application Entities filter.

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

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



Filter: Test 1

Filter Conditions:

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

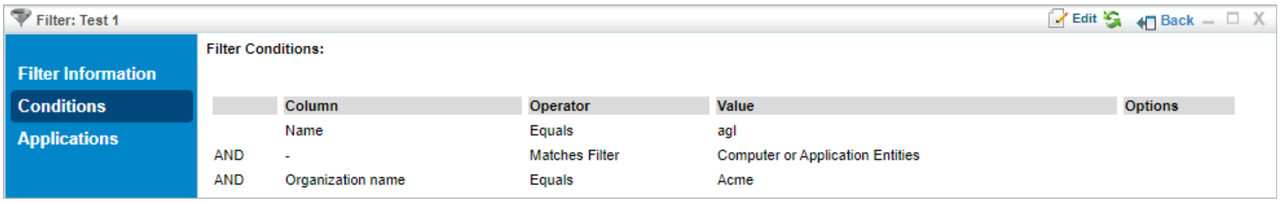
● And ○ Or

□ 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.

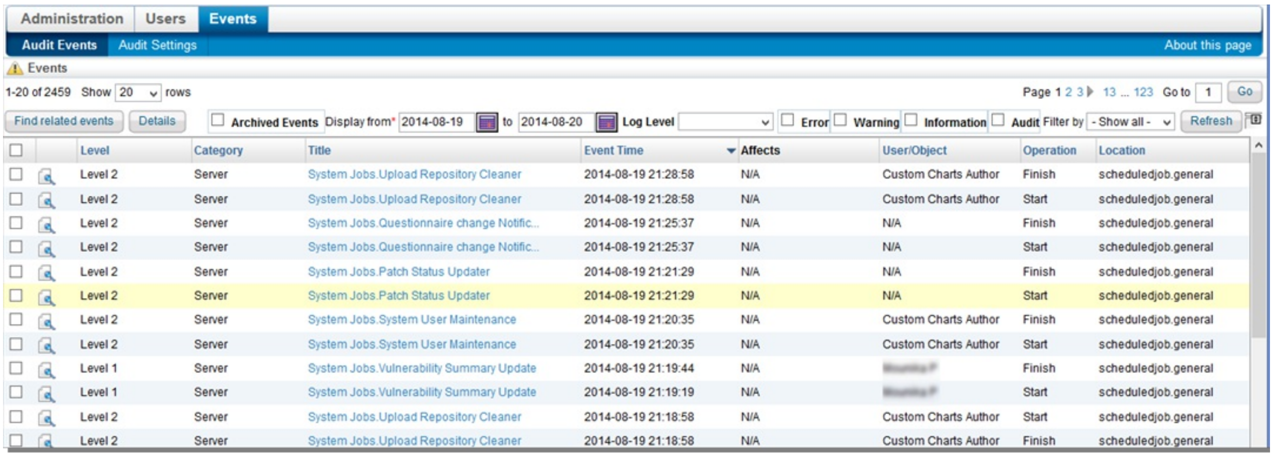
Events

Events are informational system messages that the RiskVision solution has logged. Each event is categorized as Console, Server, or Connector, and its Severity is classified in terms of Information, Warning, Audit, or Error.

An Event operation can be:

- Authentication
- Authorization
- Assessment
- Entity
- Connector
- Control
- File Export
- File Import
- Filter
- General
- Group
- Incident
- Policy
- Risk
- Schedule Job
- Server Admin
- UI Customization
- User
- Vendor

Events displayed in a tabular grid are shown below.



1-20 of 2459 Show 20 rows

Page 1 2 3 13 ... 123 Go to 1

□ Archived Events Display from* 2014-08-19 to 2014-08-20 Log Level □ Error □ Warning □ Information □ Audit Filter by - Show all -

□		Level	Category	Title	Event Time	Affects	User/Object	Operation	Location
□		Level 2	Server	System Jobs.Upload Repository Cleaner	2014-08-19 21:28:58	N/A	Custom Charts Author	Finish	scheduledjob.general
□		Level 2	Server	System Jobs.Upload Repository Cleaner	2014-08-19 21:28:58	N/A	Custom Charts Author	Start	scheduledjob.general
□		Level 2	Server	System Jobs.Questionnaire change Notific...	2014-08-19 21:25:37	N/A	N/A	Finish	scheduledjob.general
□		Level 2	Server	System Jobs.Questionnaire change Notific...	2014-08-19 21:25:37	N/A	N/A	Start	scheduledjob.general
□		Level 2	Server	System Jobs.Patch Status Updater	2014-08-19 21:21:29	N/A	N/A	Finish	scheduledjob.general
□		Level 2	Server	System Jobs.Patch Status Updater	2014-08-19 21:21:29	N/A	N/A	Start	scheduledjob.general
□		Level 2	Server	System Jobs.System User Maintenance	2014-08-19 21:20:35	N/A	Custom Charts Author	Finish	scheduledjob.general
□		Level 2	Server	System Jobs.System User Maintenance	2014-08-19 21:20:35	N/A	Custom Charts Author	Start	scheduledjob.general
□		Level 1	Server	System Jobs.Vulnerability Summary Update	2014-08-19 21:19:44	N/A	[redacted]	Finish	scheduledjob.general
□		Level 1	Server	System Jobs.Vulnerability Summary Update	2014-08-19 21:19:19	N/A	[redacted]	Start	scheduledjob.general
□		Level 2	Server	System Jobs.Upload Repository Cleaner	2014-08-19 21:18:58	N/A	Custom Charts Author	Start	scheduledjob.general
□		Level 2	Server	System Jobs.Upload Repository Cleaner	2014-08-19 21:18:58	N/A	Custom Charts Author	Finish	scheduledjob.general

Filtering Events

Because there can be a large number of events, you can filter events using a combination of following ways:

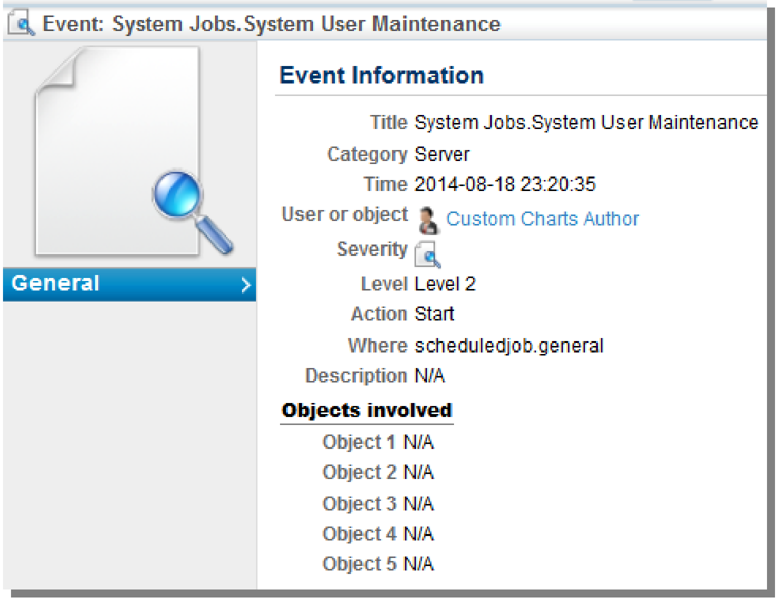
- Archived Events
- Filter by column value
- Restrict by date range
- Find related events (events involving the same resources)
- Log Level
- Error
- Warning
- Information
- Audit

Viewing Event Details

The Event View permission is assigned to the Administrator role, by default, to view event details. The Events grid displays the event information for all types of operation. Objects, such as users and connectors have an Events tab to particularly view the full cycle of information.

To view events:

1. On the **Events** menu, click **Audit Events**.
2. The **Events** page is displayed.



Event: System Jobs.System User Maintenance

Event Information

Title System Jobs.System User Maintenance
Category Server
Time 2014-08-18 23:20:35
User or object Custom Charts Author
Severity
Level Level 2
Action Start
Where scheduledjob.general
Description N/A

Objects involved

Object 1 N/A
Object 2 N/A
Object 3 N/A
Object 4 N/A
Object 5 N/A

3. After finding an event you want, check the box on that row and click **Details**.

Configuring Objects for Event Logging

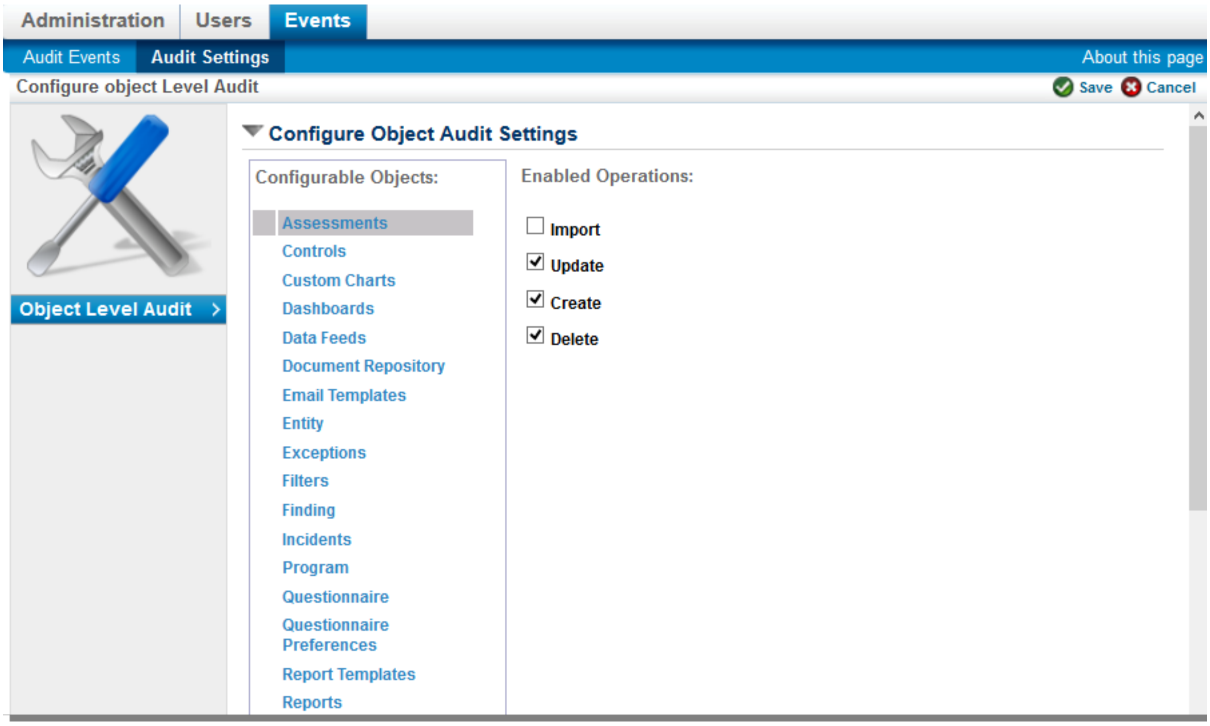
The **Audit Settings** page on the **Events** menu provides control over the event logging of most common objects found in the RiskVision application. You can configure operations for the various objects and make RiskVision write the information required. The default enabled operations of different objects are shown in the table below:

Object Type	Enabled Operations
Assessment, Controls, Custom Charts, Dashboards, Data Feeds, Document Repository, Email Templates, Entity, Exceptions, Filters, Findings, Incidents, Program, Questionnaire, Questionnaire Preferences, Report Templates, Reports, Risk, Risk Profiles, Sub Controls, Effectiveness Tests & Design Tests, System Users, Teams, Tenants, Threats, Tickets, Vulnerabilities, and Workflow	Create, Update, Delete, and Import
Scheduled Jobs	Start, Update, Create, Finish, Delete, and Run

The operations that are not enabled are not logged by the RiskVision Server and therefore those events are not available on the **Administration** > **Events** page and for reporting purposes.

To view enabled operations of objects that are logged:

1. In the **Administration** application, go to **Events** > **Audit Settings**. The **Audit Settings** page is displayed.
2.



Configure Object Audit Settings

Configurable Objects:

- Assessments
- Controls
- Custom Charts
- Dashboards
- Data Feeds
- Document Repository
- Email Templates
- Entity
- Exceptions
- Filters
- Finding
- Incidents
- Program
- Questionnaire
- Questionnaire Preferences
- Report Templates
- Reports

Enabled Operations:

☐ Import
☑ Update
☑ Create
☑ Delete

3. In the **Configurable Objects** box, select the object of interest to see the enabled operations on the right-hand side. Select the objects one by one to see the operations for which the events are logged by the RiskVision Server.

To configure objects for event logging:

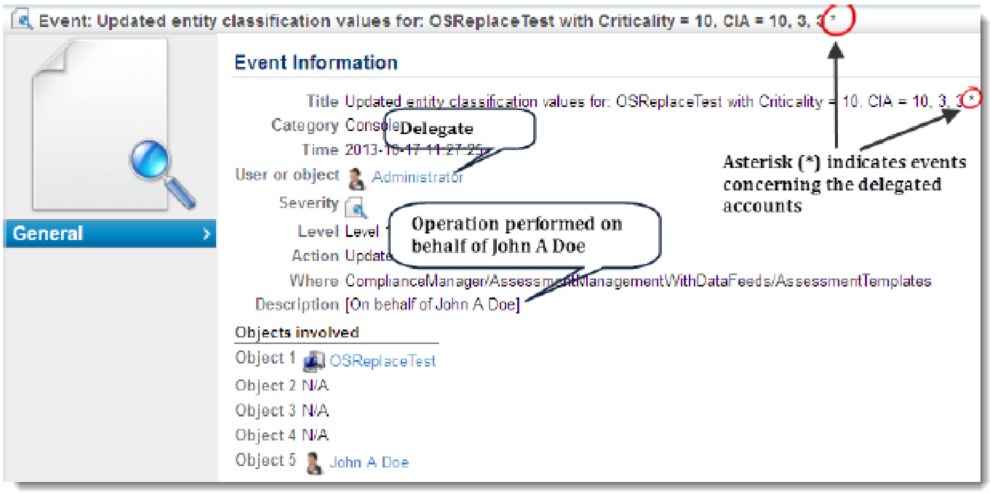
1. In the **Administration** application, go to **Events** > **Audit Settings**.The **Audit Settings** page is displayed.
2. Click **Edit** at the top-right corner of the page.

3. In the **Configurable Objects** box, select the object, and perform the tasks given below:
    1. Check the box next to the operation type if you want to log events for the operation.
    2. Clear the box next to the operation type if you don't want to log events for the operation.
4. Click **Save** after performing the desired changes.

The changes to event logging are applied.

Delegation Event Logging

The Events grid displays activities performed by users and the system in RiskVision applications. The User/Object column in the Events grid displays the user or object accountable for the execution of operations. When users delegate their user account to someone else, the delegates perform activities on behalf of the user from whom the delegation is received. The operations concerning the delegated user accounts are logged with an asterisk(*) in the Title column so that events performed by delegated users can be searched. The user in the User/Object column is the delegate. In addition, opening the event details shows the user, in the Description field, on behalf of whom the operation is performed.



Event: Updated entity classification values for: OSReplaceTest with Criticality = 10, CIA = 10, 3, 3*

Event Information

Title Updated entity classification values for: OSReplaceTest with Criticality = 10, CIA = 10, 3, 3*

Category Console

Time 2013-10-17 11:27:25

User or object Administrator

Severity

Level Level

Action Update

Where ComplianceManager/AssessmentManagementWithDataFeeds/AssessmentTemplates

Description [On behalf of John A Doe]

Objects involved

Object 1 OSReplaceTest

Object 2 N/A

Object 3 N/A

Object 4 N/A

Object 5 John A Doe

Delegate

Operation performed on behalf of John A Doe

Asterisk (*) indicates events concerning the delegated accounts

Customizing the User Interface

Installing RiskVision system will provide you a default pane, dialog, or a wizard depending on the object, and contains a set of attributes. Further, the Governance, Risk and Compliance (GRC) implementation team must analyze the RiskVision objects to provide a solution from audit perspective, and the suggested layout must expose attributes to stakeholders in a way that can provide insight to understand the inter-dependencies. This tailored approach helps you gain the detail view for building reports, which can be sufficient for meeting the GRC requirements.

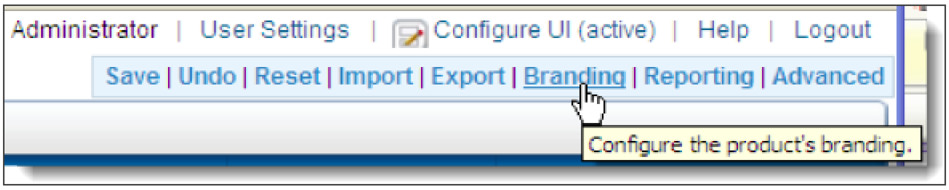
Starting with the image and text on the login page to the tab, layout, and attribute on any page in the RiskVision application, allows customization only if you have the Configure UI permission. The basic customization and configuration tasks can be accomplished easily using one or more combinations of a mouse button: left-click for making the selection, and holding the left-click and moving the mouse to drag-and-drop the tabs and attributes.

Configuring The Branding

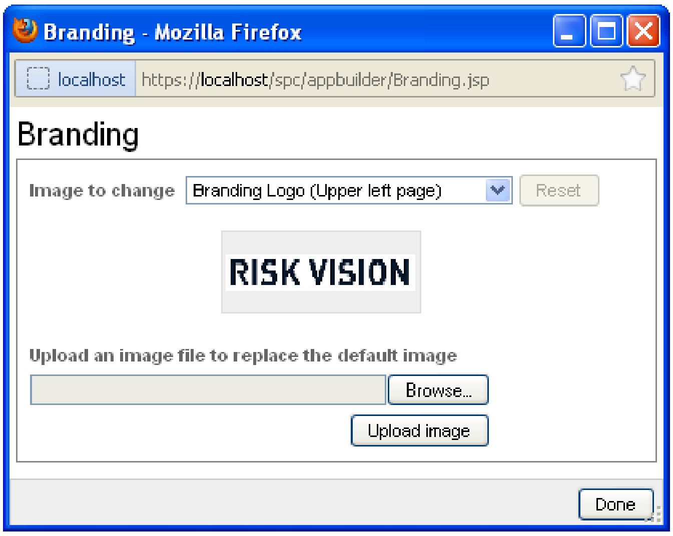
You can add your company's logo to the RiskVision system after you have logged in to the RiskVision application. To add an image from the RiskVision application, the administrator must have the Tenant Configure UI permission.

To incorporate the company logo:

1. Log in to the RiskVision application, click the Configure UI link to turn-on the configuration mode, and then click Branding.


Administrator | User Settings | Configure UI (active) | Help | Logout
Save | Undo | Reset | Import | Export | Branding | Reporting | Advanced
Configure the product's branding.

2. The **Branding** window appears. By default, the **Image to change**drop-down list selects the **Branding Logo (Upper left page)** option. To change the image, click **Browse**, select an image, click **Open**, and then click **Upload image**. Click **OK** to confirm that the image is uploaded successfully and then click **Done**.


Branding - Mozilla Firefox
localhost https://localhost/spc/appbuilder/Branding.jsp
Branding
Image to change
Branding Logo (Upper left page)
Reset
RISK VISION
Upload an image file to replace the default image
Browse...
Upload image
Done

3. Reload the browser to apply the changes.
4. To add a co-branding logo, select **Co-branding Logo (Upper right page)** from the **Image to change**drop-down list.
5. To revert back to the original image, click **Branding**, and then click **Reset** button on the **Branding** window. Click **Done**, and then reload the browser to apply the changes.When you change the Branding Logo (Upper left page) image, the image which appears on the top of the log in page will be changed.

When you change the Branding Logo (Upper left page) image, the image which appears on the top of the log in page will be changed.

Customizing the Login Page

The itemized customizations for RiskVision login page are:

- Login instructions
- Login information header and text
- Changing labels

Login instruction

Instructions about the login procedure, which appears between the username and password text box, can be changed using the following property:

`ui.login.instructions=`

The login information header and text, and labels can be customized by adding the properties, which are described under the respective sections, to the `.properties` file.

Login Information Header and Text

The login information header and text, which appears at the bottom of the log in page, can be changed using the following properties:

`ui.login.informationHeader=`

`ui.login.informationText=`

Changing Labels

The following labels on the log in page can be changed:

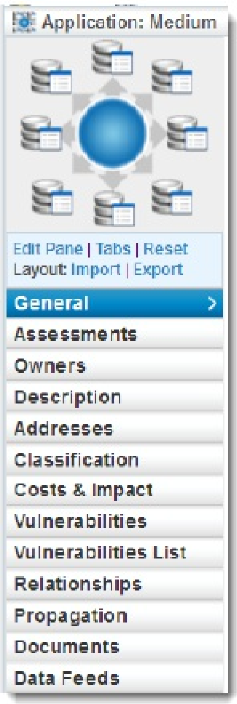
- **Log in label** - To change the **Log in** label, use the following property:
- `ui.login.userNameLabel=`
- **Forgot your Password** - To change the **Forgot your Password** label, use the following property:
- `ui.login.forgotPasswordLabel=`

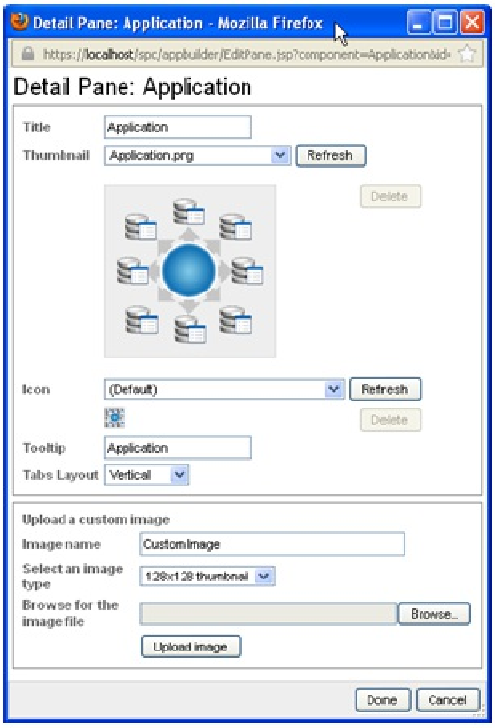
Customizing a RiskVision Object

Each RiskVision object is illustrated with a unique image that can help you identify the object easily among a group of several objects. Usually, this is helpful when a new object type is defined in RiskVision. For example, you can incorporate an image to represent the newly created entity type.

To change the object image:

1. In the RiskVision application, select any object to open its details and then click **Edit Pane**.




Detail Pane: Application - Mozilla Firefox

https://localhost/spc/appbuilder/EditPane.jsp?component=Application&id=

Detail Pane: Application

Title: Application

Thumbnail: Application.png

Icon: (Default)

Tooltip: Application

Tabs Layout: Vertical

Upload a custom image

Image name: Custom Image

Select an image type: 128x128 thumbnail

Browse for the image file

2. In the **Upload a custom image** section, enter **Image name, select an image type,** and click **Browse** to select an image**.** Selecting the **128x128 thumbnail** image type will change the image, which appears on top of object tabs, whereas selecting the 16x16 icon image type will change the image, which appears next to the object name, and in the breadcrumb, which appears on top of object details.

3. Click **Upload image** and select the newly added image in the Thumbnail drop-down list.

4. To add icon, repeat step 1 and step 2.

5. To delete custom images, click **Delete**.

6. An object's tabs appearance can be changed to display horizontally or vertically. To change the layout, select**Horizontal** or **Vertical** from the **Tabs Layout** drop-down list.

7. Click **Done** after all the changes have been made and then click **Save** to retain the customization permanently.

Customizing the Layout And Tab

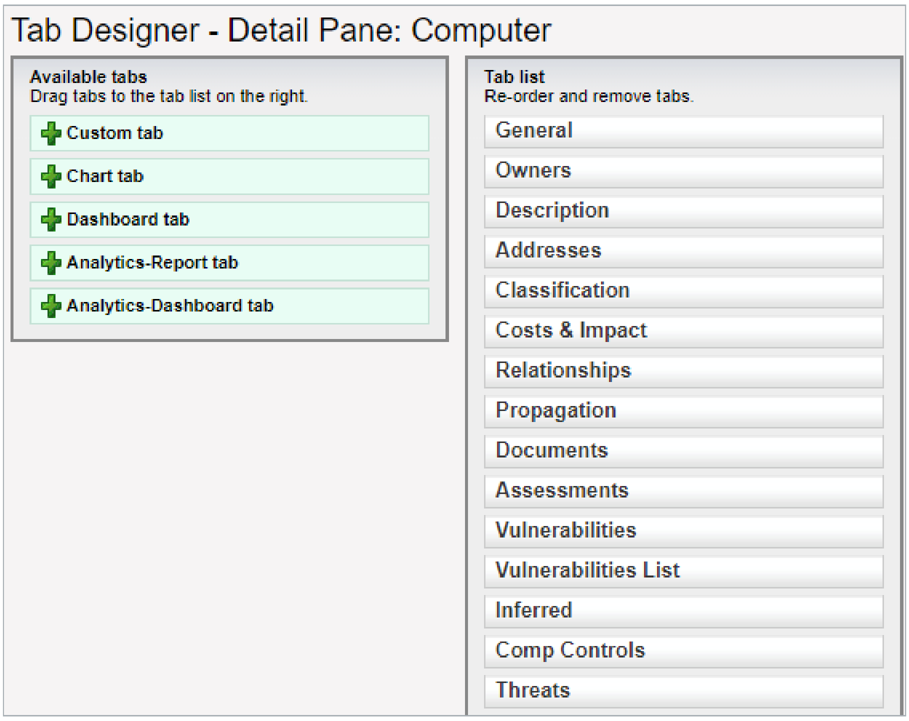
RiskVision allows you to customize a pane's layout and tab. A pane layout that you can customize includes tab, wizard page, and a dialog. At a minimum, all RiskVision objects has a tab associated with it and a menu with Tabs option, which appears above the object's first tab. Only those panes that contains a menu with the Edit Layout option at the top right side can be customized.

Before you start customizing the interface, it is strongly suggested to take a back up of the `UICustomization.xml` file, which is available in the following Tomcat web application directory:

`AGILIANCEHOME%\Tomcat\webapps\spc\WEB-INF\classes`

To customize tab:

1. In the RiskVision application, select an object to open its details, and then click **Tabs**.
2. The **Tab Designer – Detail Pane** window appears.



Tab Designer - Detail Pane: Computer

Available tabs
Drag tabs to the tab list on the right.

- Custom tab
- Chart tab
- Dashboard tab
- Analytics-Report tab
- Analytics-Dashboard tab

Tab list
Re-order and remove tabs.

- General
- Owners
- Description
- Addresses
- Classification
- Costs & Impact
- Relationships
- Propagation
- Documents
- Assessments
- Vulnerabilities
- Vulnerabilities List
- Inferred
- Comp Controls
- Threats

The Tab Designer - Detail Pane window.

Adding tabs - You can add default and custom tabs to the object view. To add a tab, hold the left-click of the mouse and drag the attribute from the Available tabs box to the Tab list box, and then release the left-click when the attribute is placed in the correct location.

Deleting tabs - To delete unwanted tabs on the object view, mouse hover the tab in the Tab list to highlight, and then click**X**.

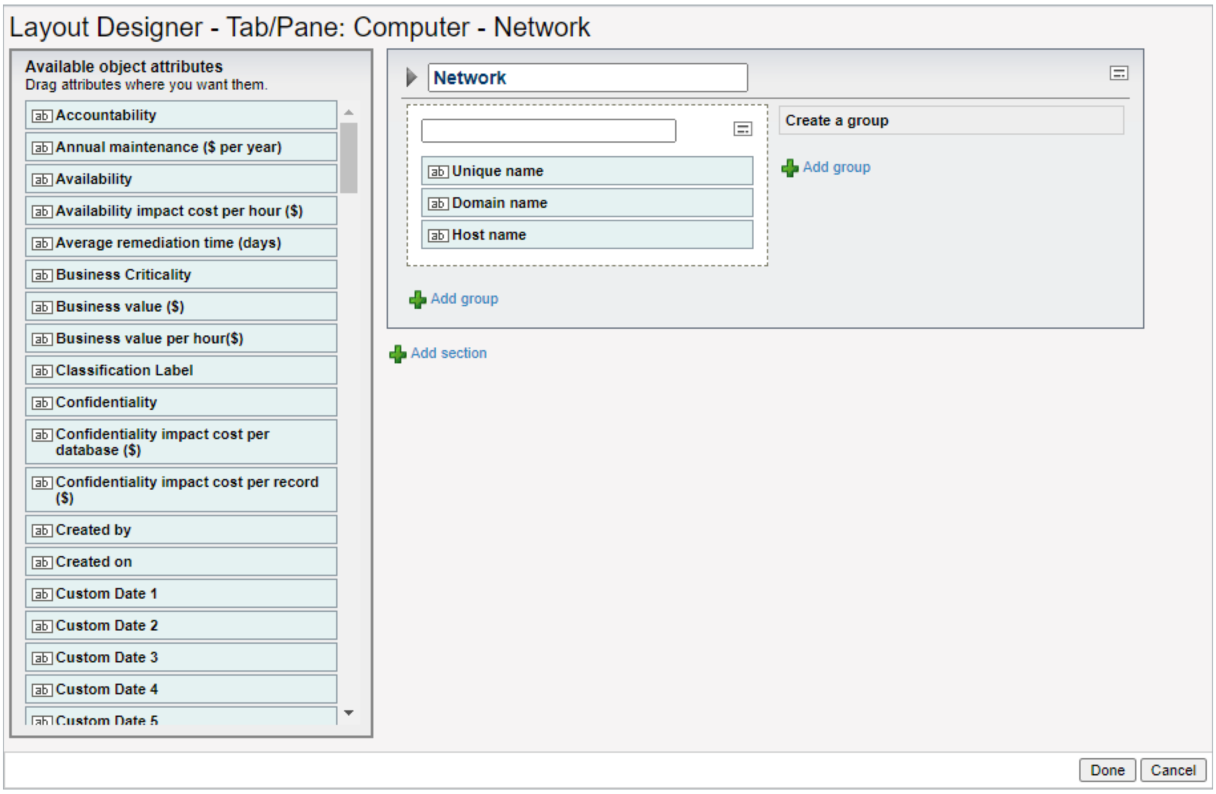
Renaming tabs - To rename a tab, mouse hover the tab, left-click the mouse in the tab area, and then change the text using the keyboard.

3. Click **Done** and then click **Save** to save your changes.

Since the fields on the General tab of a vulnerability instance are taken from a vulnerability definition, the customization of the General tab is not possible. Instead, add a new tab on a vulnerability instance and then add new attributes as appropriate.

To customize layout:

1. In the RiskVision application, select an object to open its details, and go to the page, tab, or dialog containing a menu on its right for editing the layout.
2. Click **Edit Layout** to open the **Layout Designer - Tab/Pane** window.
3. The **Available object attributes** lists the default as well as the custom attributes that you can add to the tab/pane of an object.


Layout Designer - Tab/Pane: Computer - Network
Available object attributes
Drag attributes where you want them.
Accountability
Annual maintenance ($ per year)
Availability
Availability impact cost per hour ($)
Average remediation time (days)
Business Criticality
Business value ($)
Business value per hour($)
Classification Label
Confidentiality
Confidentiality impact cost per database ($)
Confidentiality impact cost per record ($)
Created by
Created on
Custom Date 1
Custom Date 2
Custom Date 3
Custom Date 4
Custom Date 5
Network
Unique name
Domain name
Host name
Add group
Create a group
Add group
Add section
Done
Cancel

The Layout Designer - Tab/Pane window.

Adding attributes - To add attributes to a group or section present in the pane, hold the left-click of the mouse and drag the attribute from the Available object attributes scroll-box to the group or section on the right side, and then release the left-click when the attribute is placed in the correct location.

Adding groups and sections- To add a group for a particular section, click **+ Add group**, and to add a section, click **+ Add section**.

Groups can be created only as a part of section; you cannot create nested sections, that is sections within a section.

Hiding attributes - You can hide an individual attribute, group, or even a section from displaying in the object's pane. To hide, mouse hover the section, group, or attribute, and then click the hide button next to close button. To make it visible, click the hide button one more time.

Removing attributes - You cannot delete default sections of an object. However, RiskVision allows you to remove attributes from the section or group. To remove an attribute, mouse hover the attribute, and then click the close button.

4. After you finish customizing the layout, click **Done**, and then click **Save** to save your work.

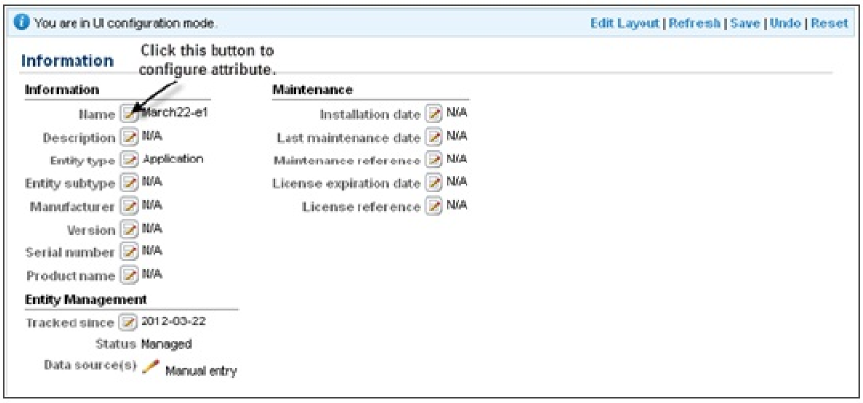
You can modify the UICustomization.xml file to display messages (such as info, warning, errors etc) in the tabs on the user interface. To do this, edit the tab in the UICustomization.xml file and set the value as *configurable='message-only'*.

Configuring Attributes

RiskVision provides flexibility to configure attributes on fly without requiring you to work in a separate window. Only those panes, which contains a menu to edit the layout and a configure button next to each attribute can be configured.

To configure attribute:

1. In the RiskVision application, select an object to open its details, go to the page, tab, or dialog containing a menu on its right for editing the layout, and then click the button next to attribute.


Edit Layout | Refresh | Save | Undo | Reset
Click this button to configure attribute.

You are in UI configuration mode.

Information

Information

Name March22-e1
Description N/A
Entity type Application
Entity subtype N/A
Manufacturer N/A
Version N/A
Serial number N/A
Product name N/A

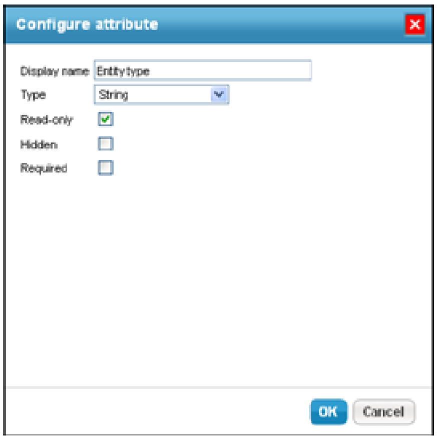
Entity Management

Tracked since 2012-03-22
Status Managed
Data source(s) Manual entry

Maintenance

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

2. The **Configure attribute** dialog appears. You can change the display name, choose whether the type of attribute must be **String, Email address, Drop-down list, Combo box, Multiple check boxes**, or **Multiple select**, and indicate whether the attribute is Read-only, Hidden, or Required.



Configure attribute

Display name Entity type
Type String
Read-only ☑
Hidden ☐
Required ☐

3. Click **OK** and then click **Save** to save your work.

Supported Custom Attributes in RiskVision

Attributes appear throughout an RiskVision application, you will find them on a page, on a wizard, on a tab, within a section of a tab, and more. The supported attribute types in an RiskVision application are date, encrypted string, flag, image, number, rational number, string, and text. Further, the attributes are classified into two categories: custom attributes and extended custom attributes.

The table below outlines the different available attribute types and their function:

Attributes	Description
Date	Stores date and time in the YYYY-MM-DD HH:MM:SS format by default
Encrypted string	Stores a string in encrypted format.
Flag	Stores Boolean values.
Image	Stores images
Number	Stores positive and negative numbers including zero.
Rational number	Stores an integer (positive and negative) as fraction.
String	Stores multiple characters.
Text	Stores character strings and HTML formatting tags.

Custom Attributes

Attributes that can be added directly from the user interface with Configure UI option are referred as custom attributes. The custom attributes that can be added are readily available on the Layout Designer - Tab/Pane window of an associated object. However, there is a limit on the number of attributes for each type that can be added to the user interface. For example, you can straightaway add up to a maximum of 4 Custom Text attributes, named sequentially from Custom Text 1 to Custom Text 4, to the user interface. For information about how to add custom attributes, see Adding attributes in the section, " Customizing the Layout and Tab."

Please note that the use of custom attributes may affect the scalability and performance of the RiskVision application. The magnitude of the effect will depend on various factors, such as the number of custom attributes added, the number of object instances of the object that will have the custom attributes added to it, and the specifications of the system on which you have installed RiskVision. RiskVision recommends that you test any changes before deploying them to production and that, if you are not already engaged with RiskVision Services or a partner, that you consider an engagement, depending on the magnitude of the considered changes.

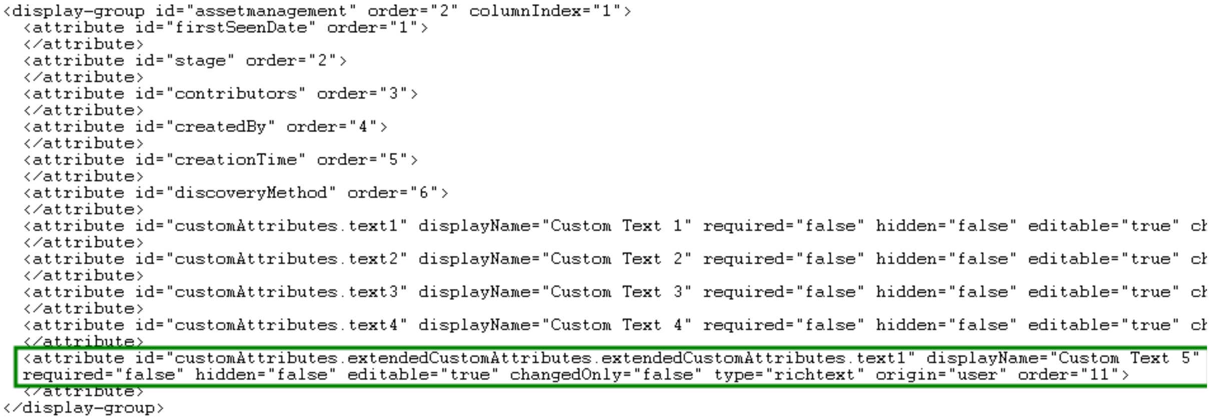
Extended Custom Attributes

In addition to the available count of custom attributes on the Layout Designer - Tab/Pane window, the RiskVision application supports many more attributes by customization of the exported user interface changes. The code changes to the exported user interface that will result in new attributes are referred as extended custom attributes. Now, you will learn how to add an extended attribute to an user interface. The steps that will walk you through the procedure to add an extended custom text attribute considers an entity details page.

To add an extended custom attribute

1. Turn on the advance UI configuration mode.
2. Select an entity to open its details page.
3. Click **Export** (Layout) at the left-hand side of the details page to export the current UI configuration changes in XML file format.
4. A dialog appears and prompts you whether to save or open the file. Save the file.
5. Open the saved XML file using a text editor, navigate to the group or section element where you want to add an extended custom attribute, and add the following code within the code context of that group or section element:
6.

   The following image demonstrates the code changes in the customization file:



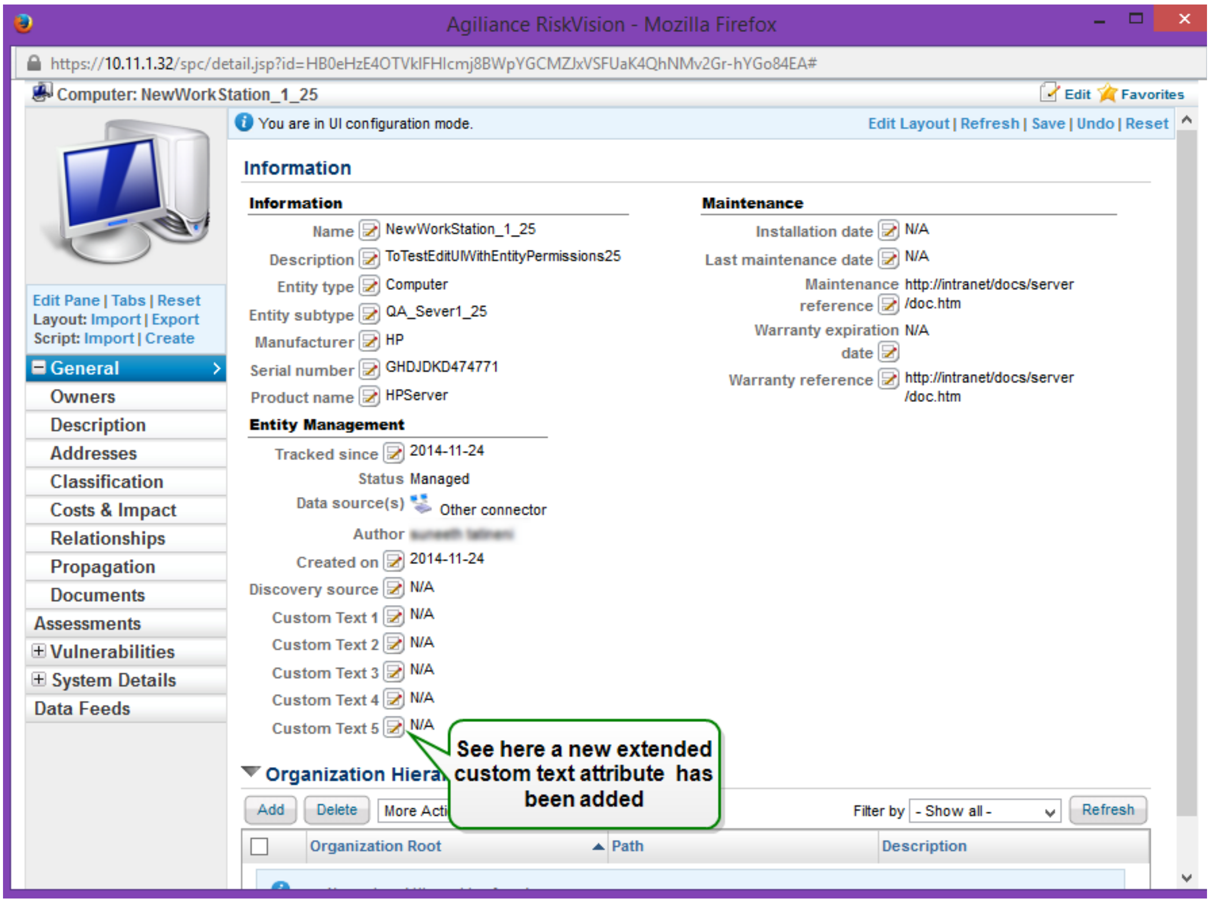
```
<display-group id="assetmanagement" order="2" columnIndex="1">
  <attribute id="firstSeenDate" order="1">
  </attribute>
  <attribute id="stage" order="2">
  </attribute>
  <attribute id="contributors" order="3">
  </attribute>
  <attribute id="createdBy" order="4">
  </attribute>
  <attribute id="creationTime" order="5">
  </attribute>
  <attribute id="discoveryMethod" order="6">
  </attribute>
  <attribute id="customAttributes.text1" displayName="Custom Text 1" required="false" hidden="false" editable="true" ch
  </attribute>
  <attribute id="customAttributes.text2" displayName="Custom Text 2" required="false" hidden="false" editable="true" ch
  </attribute>
  <attribute id="customAttributes.text3" displayName="Custom Text 3" required="false" hidden="false" editable="true" ch
  </attribute>
  <attribute id="customAttributes.text4" displayName="Custom Text 4" required="false" hidden="false" editable="true" ch
  </attribute>
  <attribute id="customAttributes.extendedCustomAttributes.extendedCustomAttributes.text1" displayName="Custom Text 5"
  required="false" hidden="false" editable="true" changedOnly="false" type="richtext" origin="user" order="11">
  </attribute>
</display-group>
```

7. Save the customization file.

8. From within the entity details page, click **Import** (Layout), browse and select the customization file, and click **OK**.

   The file is imported successfully and the extended custom text attribute is added.

   The following image demonstrates the extended custom text attribute in the entity details page.



Agiliance RiskVision - Mozilla Firefox

https://10.11.1.32/spc/detail.jsp?id=HB0eHzE4OTVklFHlcmj8BWpYGCMZJxVSFUaK4QhNMv2Gr-hYGo84EA#

Computer: NewWorkStation_1_25

You are in UI configuration mode.

Information

Information

Name NewWorkStation_1_25
Description ToTestEditUIWithEntityPermissions25
Entity type Computer
Entity subtype QA_Sever1_25
Manufacturer HP
Serial number GHDJDKD474771
Product name HPServer

Entity Management

Tracked since 2014-11-24
Status Managed
Data source(s) Other connector
Author [redacted]
Created on 2014-11-24
Discovery source N/A
Custom Text 1 N/A
Custom Text 2 N/A
Custom Text 3 N/A
Custom Text 4 N/A
Custom Text 5 N/A

Maintenance

Installation date N/A
Last maintenance date N/A
Maintenance reference http://intranet/docs/server/doc.htm
Warranty expiration date N/A
Warranty reference http://intranet/docs/server/doc.htm

See here a new extended custom text attribute has been added

Organization Hiera

□	Organization Root	Path	Description

Similarly, if you have to add other attribute types, follow the code syntax shown above.

For information about how to save the custom changes permanently, see Retaining the Custom Changes Permanently.

If problems arise due to customizations in your RiskVision environment, please contact your Customer Support Representative.

Retaining the Custom Changes Permanently

The changes you make to the layout or pane are applied permanently to all RiskVision user accounts and even when the users log in and log out of RiskVision several times. The layout or pane that is customized using the Configure UI permission are preserved and continue to work as expected because the changes are saved directly to the database.

When you modify the `UICustomization.xml` file present in the `%AGILIANCE_HOME%\Tomcat\ webapps\spc\WEB-INF\classes` directory, copy the `UICustomization.xml` file to the `%AGILIANCE_ HOME%\config` directory to ensure that the upgrade process picks the custom changes.

> RiskVision strongly recommends customizing the user interface with the Configure UI permission.

Only the changed XML blocks must be copied in the `UICustomization.xml` file in the `%AGILIANCE_HOME%\config` directory. And, remove all unchanged XML blocks. This makes upgrades much easier to do successfully and changes are easy to track down and update when needed.

Also, when RiskVision server is updated, the changes to the `UICustomization.xml` file need to be updated to match any UI changes in the newer version of RiskVision server by comparing with the new `UICustomization.xml` file of the `%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes` directory. Using an old `UICustomization.xml` file with a new RiskVision server version might cause problems, such as hiding new features in the UI. As a reason, the `UICustomization.xml` file is versioned and will be rejected if the version in the file header doesn't match.

However, if you configure the UI using the Configure UI feature in the UI, this is automatically handled by tracking the "changes" that were made and reapplying them to the new UI of the upgraded RiskVision server. It is the recommended method to make most UI configurations and using the `UICustomization.xml` file is a backup for corner cases.

Restoring the Default UI Settings

Customizing the interface can involve several changes across the RiskVision application. Reverting the changes to the original state requires you to remember each setting you made on all the layouts and panes, which is an inefficient and time consuming process. Instead, delete the `UICustomization.xml` file from the `%AGILIANCE_HOME%\config` directory and then restart the RiskVision Tomcat service to apply the default settings. When you log in to RiskVision, notice that the default changes are applied permanently.

Enable Custom SQL Dropdown List

In addition to the other custom attributes that can be added to RiskVision objects users can also add a dropdown list that is populated based on an SQL query. This list can be added to any object in RiskVision, but it must first be enabled.

To enable the SQL dropdown list:

1. Log in to RiskVision.
2. Create a role and enable the **Tenant Configure** and **Tenant Configure UI** permissions.
3. Assign the currently logged in user to the role.
4. Log out and back in again.
5. Click **Configure UI** in the top right corner and click **OK**.
6. Open the object you wish to add the dropdown to.
7. Drag and drop a custom string attribute into the object.
8. Export the **UIComponent-Ticket.xml**, append the customization file as below, and save the file:
    -
9. Import the **UIComponent-Ticket.xml** file.
10. Navigate to the **%AGILIANCE_HOME%\Tomcat\webapps\spc\WEB-INF\classes\sqlQueries.xml** file.
11. Place the below query at the bottom of the page and save it:
    -
12. Restart the tomcat service.
13. Log in to RiskVision again.
14. Navigate to the object in step 6.
15. Click on the dropdown of the custom string from step 7 which will display data based on the query written in**sqlQueries.xml**.

Appendix A: Configuring Custom Jasper Roles

This appendix contains information that allows you to make a custom Jasper role work as per the defined logic.

Jasper Roles Overview

The JasperReports Server comes with the following roles: Role_superuser, Role_administrator, Role_poweruser, Role_author and Role_user. These roles can be assigned to your users to provide access to various available features in the JasperReports Server. You can assign these pre-configured Jasper roles to RiskVision roles. You may also create custom Jasper roles in the JasperReports Server and assign them to RiskVision roles.

Note: This technical document assumes that you are familiar with the information about creating a custom role in the JasperReports Server and assigning a Jasper role to an role in the RiskVision application. For more information, please refer to the section, Assigning JasperReports Server Role.

File Settings for a Custom Jasper Role

These are the files in which the settings are required:

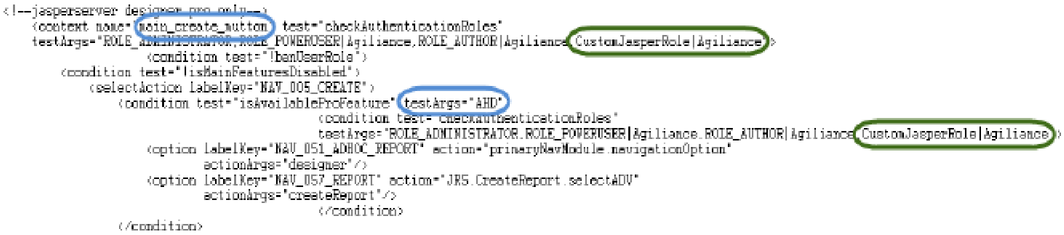
- `actionmodel-navigation.xml`
- `applicationContext-rest-services.xml`

The following scenario illustrates how to modify the file settings.

Scenario: A custom Jasper role allows a user to create an ad hoc view and a report in the JasperReports Server. Here, the Jasper role is referred as 'CustomJasperRole.'

To make a custom Jasper role function in accordance with your requirements, please follow the steps given below:

1. On the JasperReports Server host, go to the `%JASPERREPORTS_HOME\ReportServer\apache-tomcat\ webapps\jasperserver-pro\WEB-INF` , open the actionmodel-navigation.xml file using a text editor.
2. Locate the context element and add the custom Jasper role to the appropriate lines of code depending on the custom Jasper role functionality. For this scenario, add the custom Jasper role to the testArgs attribute within the context element. And then, add the custom Jasper role to the testArgs attribute within the element that is beneath the other element in which the value of testArgs attribute is **AHD**. The following graphic demonstrates the code changes.

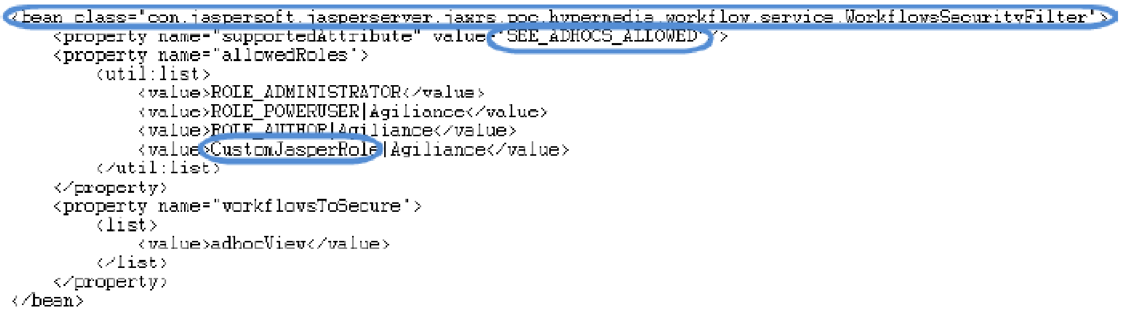


```
<!--jasperserver designer_pro_only-->
    <context name="main_create_button" test="checkAuthenticationRoles"
    testArgs="ROLE_ADMINISTRATOR,ROLE_POWERUSER|Agiliance,ROLE_AUTHOR|Agiliance,CustomJasperRole|Agiliance">
                    <condition test="!banUserRole">
        <condition test="!isMainFeaturesDisabled">
            <selectAction labelKey="NAV_005_CREATE">
                <condition test="isAvailableProFeature" testArgs="AHD">
                                        <condition test="checkAuthenticationRoles"
                                        testArgs="ROLE_ADMINISTRATOR,ROLE_POWERUSER|Agiliance,ROLE_AUTHOR|Agiliance,CustomJasperRole|Agiliance">
                    <option labelKey="NAV_051_ADHOC_REPORT" action="primaryNavModule.navigationOption"
                            actionArgs="designer"/>
                    <option labelKey="NAV_057_REPORT" action="JRS.CreateReport.selectADV"
                            actionArgs="createReport"/>
                                        </condition>
                </condition>
```

3. Locate the bean element within the bean element and add the custom Jasper role to the appropriate lines of code depending on the custom Jasper role functionality. For this scenario,add the following code beneath the element within the element of other element in which the value attribute is **SEE_ADHOCS_ALLOWED**.

```
<value>
                                                            CustomJasperRole|
  </value>
```

The following graphic demonstrates the code changes:



```
<bean class="com.jaspersoft.jasperserver.jaxrs.poc.hypermedia.workflow.service.WorkflowsSecurityFilter">
    <property name="supportedAttribute" value="SEE_ADHOCS_ALLOWED"/>
    <property name="allowedRoles">
        <util:list>
            <value>ROLE_ADMINISTRATOR</value>
            <value>ROLE_POWERUSER|Agiliance</value>
            <value>ROLE_AUTHOR|Agiliance</value>
            <value>CustomJasperRole|Agiliance</value>
        </util:list>
    </property>
    <property name="workflowsToSecure">
        <list>
            <value>adhocView</value>
        </list>
    </property>
</bean>
```

4. Restart the Jasper Tomcat service.