### **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.

RI	RISK VISION												
Adn	ninistration	Users	Events										
Serv	er Administratio	n Extern	al Authentication	Login Integration	Notifications	Connectors	Email Templates	Queued Jobs	Scheduled Jobs	Document Repository		About this page	
🖏 Cor	nectors												
1-2 of 2													
Details	Delete										Filter by - S	ihow all - 👻 Refresh	
	Status Health Type Name Description Version												
	•	1	FireEye ISight	t Connector			internal		FireEye ISight Cor	nector		9.0.7408.147	
🔲 🐗 🧹 CrowdStrike Falcon Intelligence Connector int						1	Internal CrowdStrike Fi			on 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**.

💐 Connector: Crowd Stril	xe Falcon Intelligence Connector	🕑 Edit 🗞 😑 🗆 🕽
	Configuration Credentials Key mmm	
	Socret Koy *****	
Information		
Configuration >		
Commands		
Events		

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.

RI	SK	VIS	ION								Administration	•	Administrator	User Settings	Configure UI	Help   Log Out
Ad	ministr	ation Us	sers Events													
Se	ver Admi	inistration	External Authentication	Login Integration	Notifications	Connectors	Email Templates	Queued Jobs	Scheduled Jobs	Document Repository						
Q 50	cheduled	Jobs														
1-20 0	59 Show	av 20 🔻 ro	wrs												Page 1 2 3	Go to 1 Go
Deta	is Del	lete Run	Activate Deactivate	)											Filter by - Show all	Refresh
	Active	System	Job Group	Job Name						<ul> <li>Next Execution</li> </ul>		Current Statu	5	Description		
	1	1	System Jobs	Affected Entities M	Notification Sende	br				2019-06-06 09:16:33		Not Executing		Sends notification f or updated vulneral	or the affected entitie bilities.	es of newly imported
	1	1	System Jobs	Alert Rule Proces	sor					2019-06-07 05:00:00		Not Executing		Evaluates alert rule compliance scores	s. Sends notification crossed thresholds.	s if risk or
	1		Project Recurrence Jobs	Always On Asses	ssments 2-5-16 (al	II)				2019-06-07 01:00:00		Not Executing		Project recurrence 16	for project: Always O	in Assessments 2-5-
	1	1	System Jobs	Assessment Obje	ects Carry Forward	d				2019-06-06 23:00:00		Not Executing		Gets snapshot of a	ssessment related of	bjects
	1	1	System Jobs	Control Results U	Jpdater					2019-06-06 11:18:03		Not Executing		Updates control res	ults from other source	ces.
	1	1	System Jobs	CrowdStrike Falco	on Intelligence Co	onnector				2019-06-07 00:00:00		Not Executing		CrowdStrike Falcor intelligence reports	Intelligence Connect and persist into Risk	tor Job to pull Vision 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.

RI	SK VI	Administrator   User Settings   Help   Log Out									
Adr	ninistration	Users	Events								
Serv	er Administratio	on Extern	al Authentication	Login Integration	Notifications	Connectors	Email Templates	Queued Jobs	Scheduled Jobs	Document Repository	About this page
🖏 Coi	inectors										
1-2 of 2											
Details	Delete										Filter by - Show all - 👻 Refresh
	Status	Health	🔻 Туре				Name		Description		Version
	ф	1	FireEye ISight	Connector		1	internal		FireEye ISight Cor	inector	9.0.7408.147
	ф.	1	CrowdStrike F	alcon Intelligence Conn	ector	1	internal		CrowdStrike Falce	on Intelligence Connector	9.0.7408.147

The Connectors page.

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



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.

RI	SK	VIS	ON								Administration	✓ Administrat	or   User Settings   📝 Configure UI   Help   Log Ou
Ad	ministra	ation Us	sers Events										
Ser	ver Admi	nistration	External Authentication	Login Integration	Notifications	Connectors	Email Templates	Queued Jobs	Scheduled Jobs	Document Repository			
Q 50	heduled	Jobs											
1-20 of	59 Show	v 20 🔻 ro	vrs										Page 1 2 3 Go to 1 Go
Detai	is Del	ete Run	Activate Deactivate										Filter by - Show all - V Refres
	Active	System	Job Group	Job Name						Next Execution		Current Status	Description
	1	1	System Jobs	Affected Entities	Notification Send	a.				2019-06-06 09:16:33		Not Executing	Sends notification for the affected entities of newly importe or updated vulnerabilities.
	1	1	System Jobs	Alert Rule Proces	isor					2019-06-07 05:00:00		Not Executing	Evaluates alert rules. Sends notifications if risk or compliance scores crossed thresholds.
	1		Project Recurrence Jobs	Always On Asses	sments 2-5-16 (a	I)				2019-06-07 01:00:00		Not Executing	Project recurrence for project: Always On Assessments 2-5 16
	1	1	System Jobs	Assessment Obje	ects Carry Forwar	t i				2019-06-06 23:00:00		Not Executing	Gets snapshot of assessment related objects
	1	1	System Jobs	Control Results L	lpdater					2019-06-06 11:18:03		Not Executing	Updates control results from other sources.
	1	1	System Jobs	CrowdStrike Falc	on Intelligence C	nnector				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.



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

# To import exploits through the Exploit Database Connector:

1 Install and run the Explait DP Connector

- I. Install and full 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 ron 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.