Threat Intelligence Connector

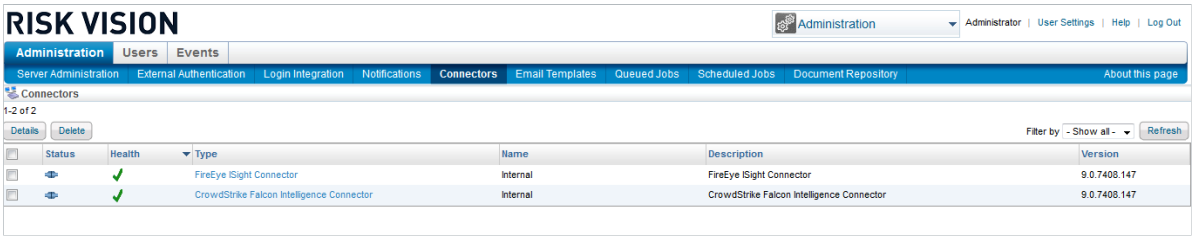
RiskVision integrates with threat intelligence services through connectors. Customers with a valid license can access the CrowdStrike Falcon Intelligence Connector, the FireEye ISight Connector, and the Exploit Database Connector data in the Connectors page.

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:

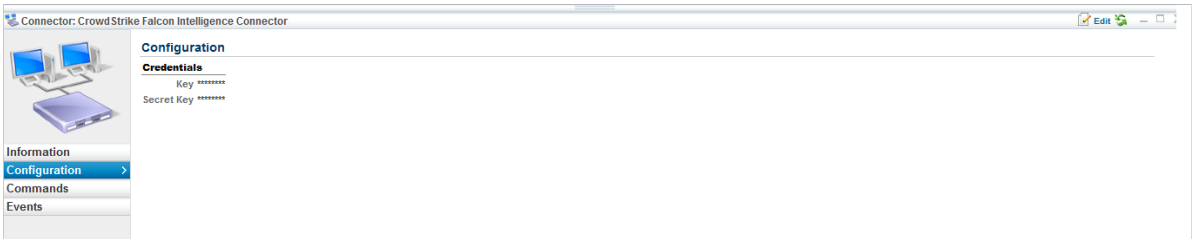
```
Proxy.useProxyServer = true
Proxy.serverHost = Server Hostname
Proxy.serverPort = 3128
Proxy.httpType = http
```

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



The Connectors page.

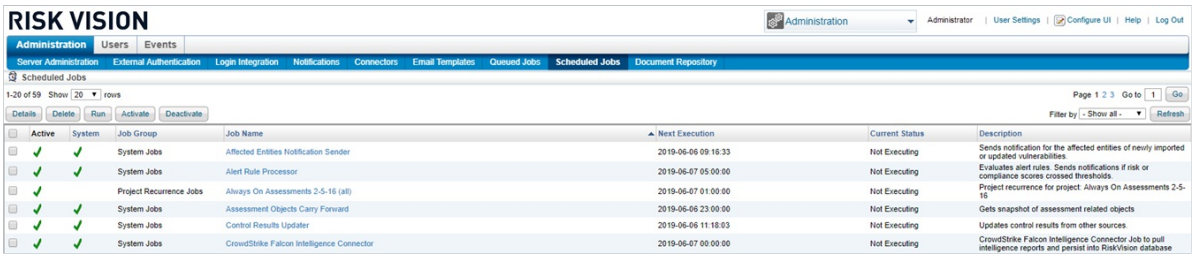
6. Click on **CrowdStrike Falcon Intelligence Connector** and then click **Details**.
7. Click on the **Configuration** tab and then **Edit**.



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.



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".

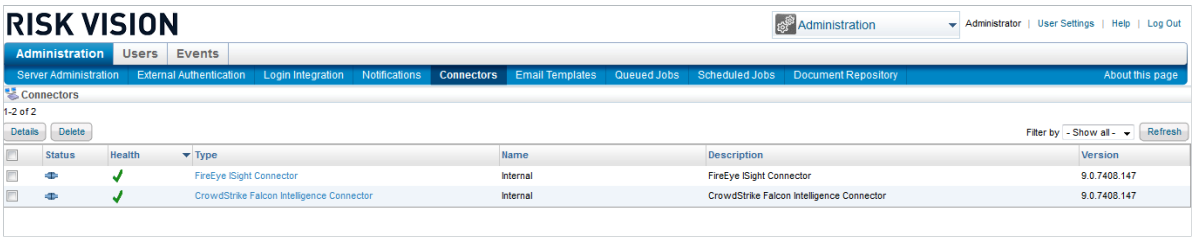
11. After successfully importing threats, click **Deactivate**.

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:

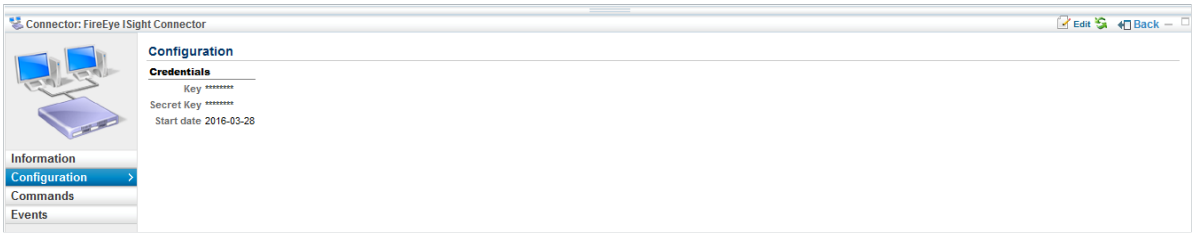
```
Proxy.useProxyServer = true
Proxy.serverHost = Server Hostname
Proxy.serverPort = 3128
Proxy.httpType = http
```

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



The Connectors page.

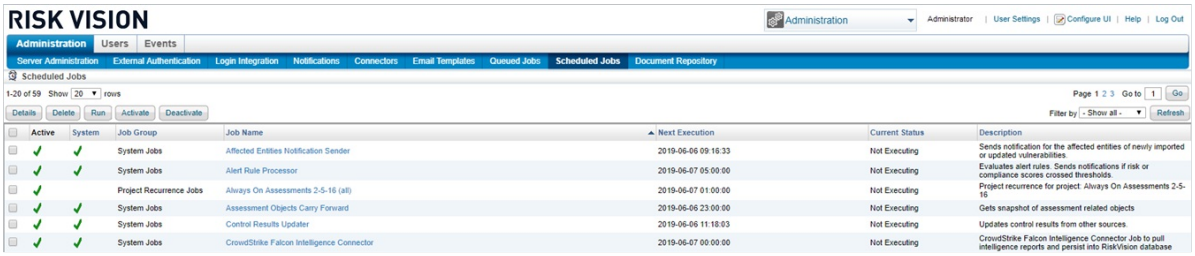
6. Click on **FireEye ISight Connector**.
7. Click on the **Configuration** tab and then **Edit**.



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.



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**

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.