websense®

TRITON® RiskVision™ Setup Guide

v2.0

Contents

1 | Introducing TRITON RiskVision

Websense® TRITON® RiskVision™ uses advanced analytics—including rules, signatures, heuristics, and file sandboxing—to provide real-time analysis of files transferred in web and email traffic.

TRITON RiskVision monitors TCP traffic by connecting to a SPAN or mirror port on a switch, or to a network tap that supports aggregation.

◆ Files identified in HTTP and SMTP traffic are analyzed by the solution in real time, using Websense Advanced Classification Engine (ACE) analytics on the local machine, to identify suspicious and malicious software.

◆ Potentially suspicious files are forwarded to the cloud-based file sandboxing service to identify advanced malware threats. Administrators can:

   ■ Find status information in the Local Manager to track the status of file sandboxing.

   ■ Access online file sandboxing reports to learn more about analyzed files, the threats associated with them, and the steps needed for remediation.

◆ Transaction data is analyzed to find violations of regulatory policies related to transfer of Personally Identifiable Information (PII), Protected Health Information (PHI), and Payment Card Industry (PCI) data within file content.

Positioning TRITON RiskVision in the network

RiskVision positioned downstream from a web proxy

In most cases, it is best to position the RiskVision appliance between clients and the proxy. This ensures that RiskVision components see:

◆ Unaltered TCP traffic from clients

◆ The client IP address associated with requests
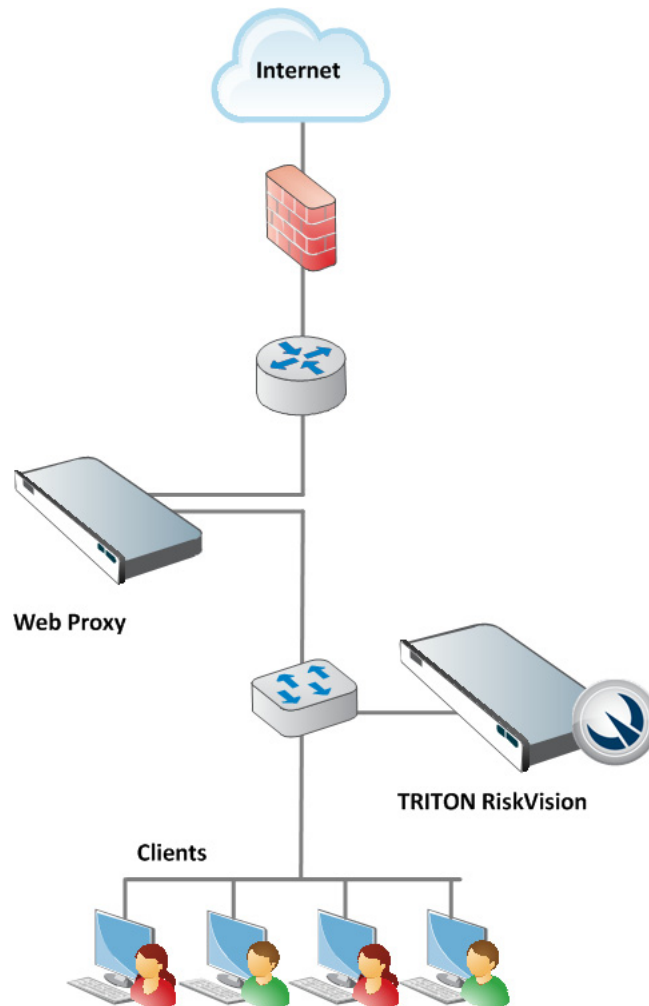
Outbound data protection performed by the upstream proxy does not affect RiskVision, but if the upstream proxy blocks **responses** from origin servers, RiskVision does not see those responses.

RiskVision positioned upstream from a web proxy

When RiskVision is positioned closer to the Internet egress point:

◆ RiskVision sees origin server responses before they are processed by the web proxy. This allows unrestricted application of the real-time analytic features.

◆ If the downstream proxy blocks outbound requests, however, RiskVision will not see those requests and cannot analyze or log them.
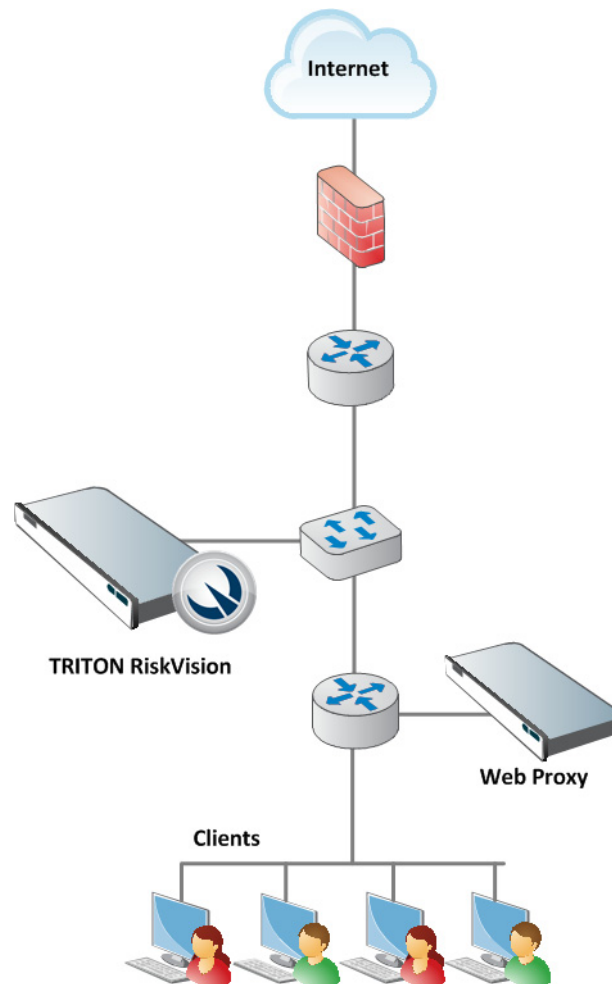
In this configuration, because outbound traffic goes through the downstream proxy before being seen by RiskVision, the source IP address of all requests is the web proxy IP address.

To address this issue, configure the downstream proxy to add **X-Forwarded-For** to HTTP headers. RiskVision automatically parses the X-Forwarded-For information and includes both the source IP address (the proxy) and the forwarded for IP address (the client) in its reporting output.

RiskVision and SSL decryption

If your network includes a product that provides SSL decryption, RiskVision can be configured to monitor and analyze the decrypted traffic.

Deployment details vary based on the product providing the decryption. In general terms, however, RiskVision analyzes a read-only copy of the decrypted traffic via a monitor or SPAN port.
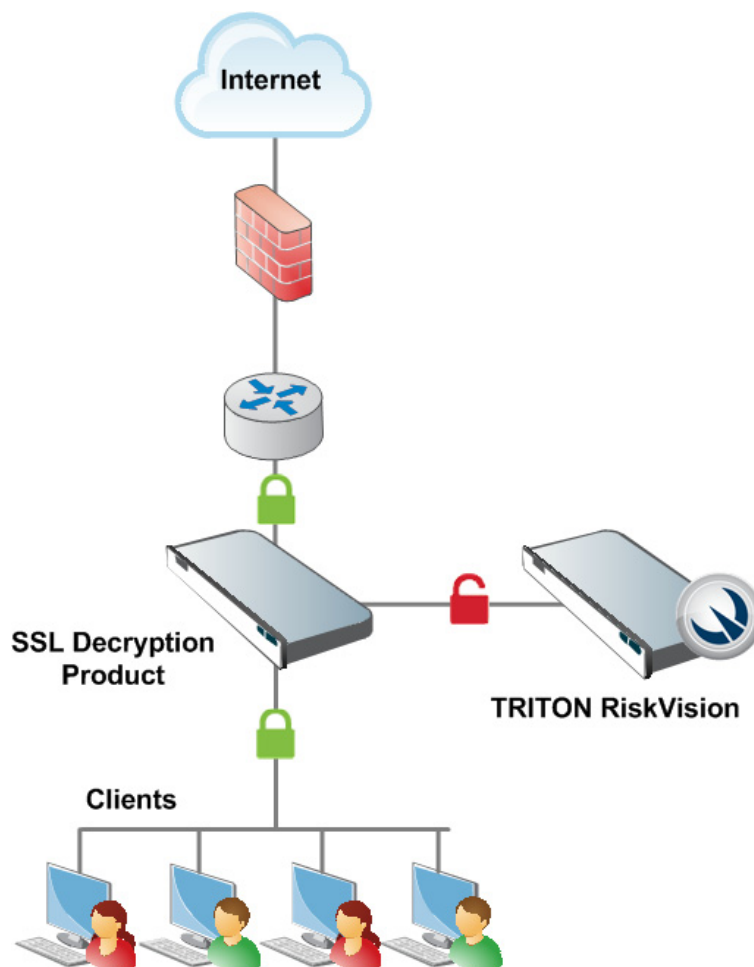
How does RiskVision work?

The RiskVision monitoring and analysis process works as follows:

1. **Capture** monitors IP packets from a single network interface and stores them in memory.

2. **Assembler** reads the pcap files provided by Capture and:
   - Identifies HTTP and SMTP transactions
   - Properly orders packets and removes duplicates
   - Writes HTTP and SMTP request and response data to disk for further processing

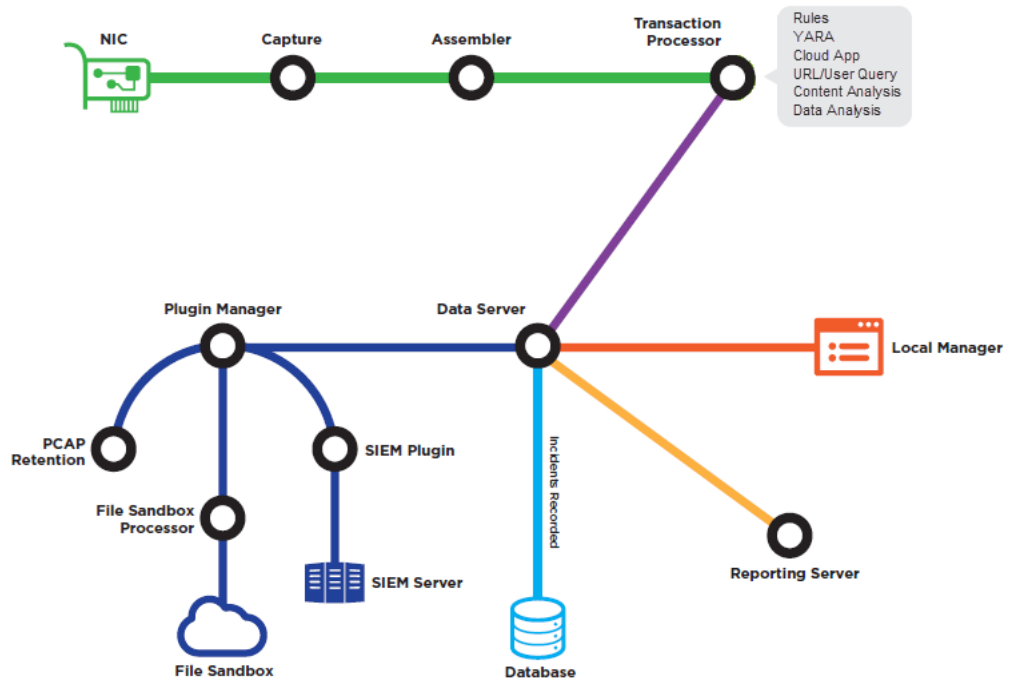3. **Transaction Processor** takes the request and response files provided by Assembler and provides them to each of the Local Analysis plugins on the appliance.
   - If any plugin identifies a transaction as malicious, suspicious, or violating a data loss or data theft policy an incident is created.
   - If any plugin recommends that a transaction receive Cloud Analysis, an incident is created.
   - By default, if no incident is created, the transaction is discarded.

4. **Data Server** is responsible for storing, retrieving, and analyzing data in the Incident and Reporting Database. It also makes data available to other services for further analysis (Plugin Manager), display to administrators (Local Manager), and report generating (Reporting Server).

5. **Plugin Manager** allows its plugins to observe, add to, or modify incident data for incidents created by Transaction Processor and its plugins.

   Plugin Manager plugins are responsible for managing communication with the File Sandboxing cloud service, pcap storage, and logging to syslog and third-party SIEM products.

6. **Local Manager** displays incident data to administrators to help them investigate malicious, suspicious, data loss, and data theft activity in their network. It also offers diagnostic information for system monitoring and troubleshooting, as well as a variety of other features.

Setup process overview

2

Installation

Step 1: Set up your V-Series appliance hardware

The diagram below gives a simple overview of TRITON RiskVision deployment. All local RiskVision components, including management and reporting components, reside on the Websense V-Series appliance.
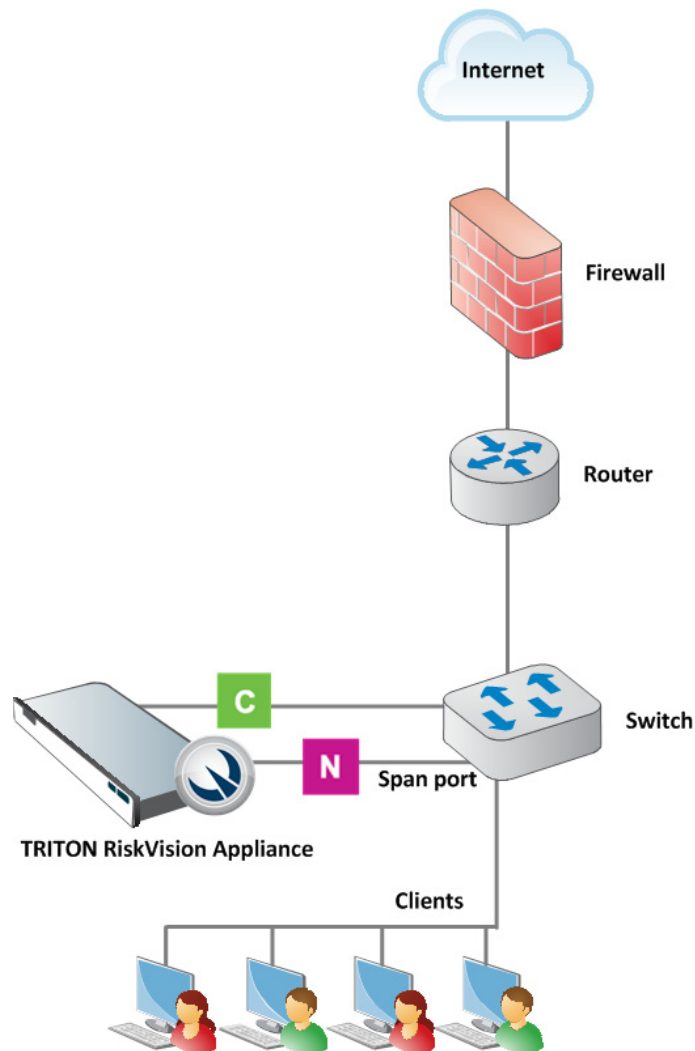
Connect the C (eth0) and N (eth1) appliance interfaces as described below. Cat 5E cables (or better) are required. Do not use crossover network cables.

Management console communication, analytic database downloads, and system updates use network **interface C**. The interface:

◆ Must be able to access a DNS server

◆ Has continuous access to the Internet

Ensure that interface C is able to access the download servers at **download.websense.com**. This URL must be permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.

Network **interface N** connects either to a port mirror on the switch or to a network tap that supports aggregation. This allows RiskVision to monitor and analyze HTTP and SMTP traffic on all ports.

Step 2: Set up the RiskVision appliance software

You can attach a monitor and keyboard to the appliance, or access the appliance via the iDRAC, to complete this procedure.

1. Power on the appliance.

   The CentOS 6.6 operating system and TRITON RiskVision software are pre-installed on the appliance. (If you need to re-install the operating system and RiskVision software, see Reinstalling RiskVision from a USB Drive.)

2. Log in as **root** with the default password **websense123**, then immediately create a new password, as prompted.

3. If DHCP is enabled in your network, the startup process automatically acquires an IP address for the C interface. If you are not using DHCP, or if you want to configure a specific IP address:

   a. Use the **system-config-network** command to update your eth0 configuration.

   b. Use the **service network restart** command to restart your network interfaces.

   c. Use the **/opt/websense/rvadmin.sh restart** command to restart all of the TRITON RiskVision services.

4. Optionally also:

   ■ Set the system timezone using the **timezone** command.

   ■ Configure your keyboard or language settings with the **system-config-keyboard** and **system-config-language** commands.

Continue with the next chapter of this guide to activate, verify, and configure your RiskVision deployment.

3

Initial Setup

Step 3: Configure the system

When installation is complete, use the RiskVision Local Manager to enter your subscription key and verify the system.

Verify your network interface configuration

During installation, the Capture service is configured to use the **C interface** (eth0) for communication and the **N interface** (eth1) to monitor traffic. If DHCP is enabled in your network, the C interface is automatically assigned an IP address during installation.

To verify your current network interface configuration, and change the traffic capture interface (if needed):

1. Select the **System > Network** tab in the Local Manager.

2. Verify that an IP address is assigned to interface C, and that the link status is **Up**.
3. Verify that the N interface is being used for **Traffic Capture**, and that the link status is **Up**.

If you need to change the interface used to monitor traffic, use the **Traffic capture interface** drop-down list to select the new interface.

Enable RiskVision analysis

When you enter your subscription key in the Local Manager, RiskVision connects to Websense servers to validate the subscription. This is required to download analytic databases, connect to the File Sandboxing cloud service, and retrieve reporting information from Websense Security Labs.

To enter your key:

1. Open an instance of Mozilla Firefox or Google Chrome and navigate to:

   ```
   https://<C_interface_IP_address>:8443
   ```

2. Log on to the Local Manager with user name **admin** and password **admin**.

3. Immediately select the **admin** menu in the toolbar at the top of the page, then click **Change Password**.
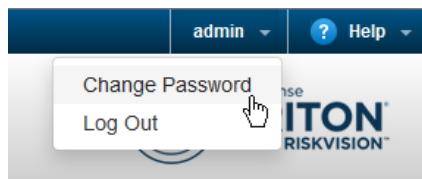
4. Enter and confirm the new password for the admin account, then click **Change Password**.

   - As a best practice, enter a strong password containing a combination of uppercase and lowercase characters, numbers, and special characters.

   - The password must be between 4 and 255 characters long.

5. Select the **System** page in the RiskVision toolbar.

6. If C interface traffic from the RiskVision appliance must go through an explicit proxy to access the Internet:

   a. Select the **Proxy** tab.

   b. Toggle **Enable proxy settings** to **ON**

   c. Enter the connection details.

   d. Click **Apply**.
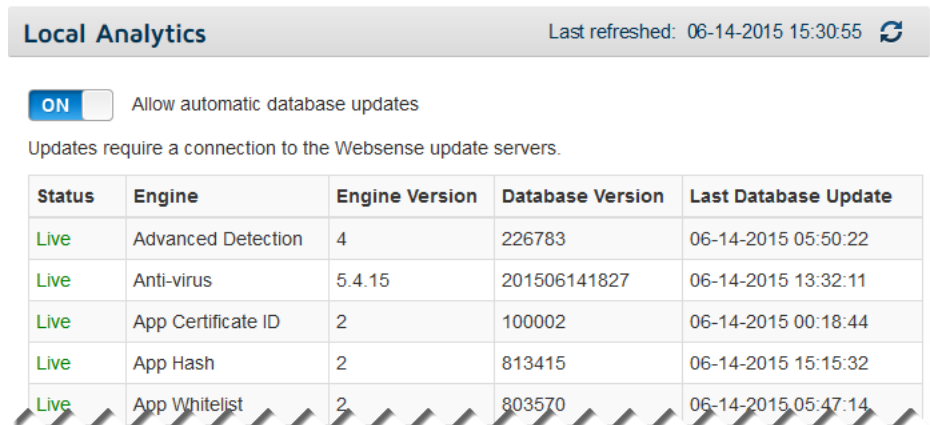

7. Select the **Account** tab.

8. Enter your subscription key into the field at the top of the page, then click **Apply**.

   If you do not click Apply, the field will be cleared when you accept the subscription agreement, and you will need to enter your key again.

9. Under Subscription Agreement, read and accept the agreement to activate your product.

Update the analytic databases

On-box analytics use several databases to facilitate detection of malicious and suspicious software.

To check the status of your on-box analytic databases:

1. Select the **System > Analytics** tab in the Local Manager.
2. Scroll to the **Local Analytics** section.
3. Make sure that **Allow automatic database updates** is set to **ON**.

4. Use the table beneath the toggle switch to check the status of each analytic database.

   The information updates automatically every 5 minutes.

Note that after a new installation, each database will need to be downloaded. Download progress is shown on the screen, and when the update is complete, the database version and last update time are displayed.

Check for system updates

RiskVision systems use the Linux **yum** tool for both operating system and RiskVision software hotfixes, patches, and upgrades. The **System > Updates** tab in the Local Manager indicates whether updates are available, and offers a single-button mechanism for downloading and installing the updates.

As a best practice, check for and apply any available updates to your newly-deployed system:

1. Select the **System > Updates** tab in the Local Manager.

2. If updates are available, click **Start Update**.

   A warning message indicates that the update will include a system restart.

3. Click **OK** to start the update.

4. When the system has restarted, log back in to the Local Manager to finish setting up the system.

Configure data storage

By default, RiskVision is configured to store up to 400,000 incident records and up to 2 million sessions in its database. RiskVision is also configured not to store pcap files for captured traffic.

To customize data storage settings:

1. Select the **System > Local Storage** tab in the Local Manager.

2. Use the **Incident Storage** box to configure:

   ■ The maximum number of threat or data loss incident records to store in the database

   ■ Whether database cleanup occurs automatically

      Note that if you disable database cleanup, when the database is full, new records will be discarded. Database cleanup deletes the oldest records to make room for new records.

   ■ How long to keep incident records

If the maximum number of incident records is reached before the oldest records reach the obsolescence period that you select, and database cleanup is enabled, the oldest records will still be deleted to make room for newer records.

Likewise, even if the database is not full, records older than the period specified will be deleted by the cleanup job.

3. Use the **Session Storage** box to configure:

   ■ The maximum number of sessions to store in the database

   Session data is stored only when the **Log all sessions** option is enabled on the **Diagnostics** page. Session logging is generally enabled only for troubleshooting, and disabled when the troubleshooting process is complete.

   ■ Whether database cleanup occurs automatically

   Because session data is typically used for troubleshooting, it is a best practice to allow the automated database cleanup process to remove data that is no longer needed.

   ■ How long to keep session data

   The default is 3 days.

4. Use the **Pcap Retention** box to configure:

   ■ Whether or not to store pcap files for threat and data loss incidents in your network

   Storing pcap files can quickly use a large volume of disk space, so pcap files are not retained by default.

   ■ If pcap files are being retained, configure the maximum amount of disk space to use for pcap file storage (120 GB, by default).

   ■ If pcap files are being retrained, also configure whether to delete the oldest files or stop storing new files when the storage size reaches 90% of maximum capacity.

Enable traffic capture

By default, traffic capture starts immediately upon startup. If the appliance interfaces are not properly configured, however, the Capture process may stop.

To make sure that traffic capture is enabled:

1. Select the **System > Analytics** tab in the Local Manager.
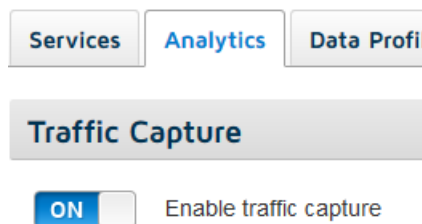
2. Make sure **Enable traffic capture** is **ON**.

Verify the RiskVision services

You can monitor the status of the local RiskVision services on the **System > Services** page in the Local Manager.

The Service Manager table should show a status of **Running** for all services.

Status	Name	Uptime	CPU Use (1.50% / 24 Cores)	Memory Use (4.12 GB)	Service Restart
Running	Assembler	0d - 18h:19m:35s	0% / 5 Cores	28.8 MB	⏻
Running	Capture	0d - 18h:19m:37s	0% / 3 Cores	66.7 MB	⏻
Running	Data Analysis Engine	0d - 18h:17m:34s	0% / 23 Cores	294.0 MB	⏻
Running	Data Server	0d - 18h:17m:34s	0% / 21 Cores	651.0 MB	⏻
Running	Database	0d - 18h:17m:44s	0.50% / 10 Cores	44.3 MB	⏻
Running	Event Log Processor	0d - 18h:19m:40s	0% / 2 Cores	2.5 MB	⏻
Running	Feedback	0d - 18h:17m:49s	0% / 3 Cores	4.3 MB	⏻
Running	File Sandbox Processor	0d - 18h:17m:32s	0.50% / 19 Cores	325.8 MB	⏻
Running	Local Analysis	0d - 18h:18m:06s	0% / 1 Core	1.07 GB	⏻
Running	Local Manager	0d - 18h:17m:29s	0% / 21 Cores	787.0 MB	⏻
Running	Reporting Server	0d - 18h:17m:35s	0% / 23 Cores	238.3 MB	⏻
Running	Splice Plugin Manager	0d - 18h:17m:34s	0% / 24 Cores	308.1 MB	⏻
Running	Transaction Processor	0d - 18h:19m:38s	0.50% / 11 Cores	34.4 MB	⏻
Running	URL Database Query	0d - 18h:19m:40s	0% / 4 Cores	342.2 MB	⏻

◆ If a single service is stopped, use the icon in the **Service Restart** column of the table to restart that service.

> **Important**
>
> If the service that is stopped is **Local Analysis**, the problem may be that the analytics databases have not finished downloading.
>
> Check download status on the **System > Analytics** page, and restart the service or services when the databases have finished downloading.

◆ If multiple services are stopped, or if you have changed the IP address or hostname of your RiskVision appliance, use the **Restart All Services** icon above the table to restart all RiskVision services.

When you use the Restart All option, you are automatically logged out of the Local Manager. Give the Local Manager services about a minute to finish restarting before you attempt to log in again.

Step 4: Verify RiskVision monitoring

To make sure that TRITON RiskVision is able to monitor traffic from all expected sources:

1. In the Local Manager, click **Diagnostics** in the toolbar at the top of the page, then select the **Sessions** tab.

2. Scroll down to the **Session Details** section of the page, then switch **Log all sessions** to **ON**.

Session Details

When all sessions are logged, details for each session are displayed in the table below, regardless of wh...

ON Log all sessions

6 most recent sessions   April 23, 2015 15:01:05 to Present   4 unique sources   4 unique destinations

Filter	

Drag and drop column headers into this area to group your data

Session ID	Start	Duration	Transport	Protocol	Source IP	Destinatio
595	2015-06-14 1...	1m1s	TCP/IP	None	10.64.134.76	10.204.82.
592	2015-06-14 1...	1m977ms	TCP/IP	None	10.64.134.76	10.204.82.
602	2015-05-07 1...	199ms	TCP/IP	HTTP	10.212.7.13	209.99.60.
601	2015-05-06 0...	26s	TCP/IP	HTTP	10.34.50.224	74.125.22.
600	2015-05-05 1...	1m305ms	TCP/IP	HTTP	10.34.50.224	74.125.22.
599	2015-04-23 1...	1ms	TCP/IP	HTTP	10.34.50.47	10.34.50.2

3. To make sure that traffic is originating from the clients or subnets that you want to verify, check the IP addresses in the **Source** column of the Session Details table.

   To make it easier to verify that all expected traffic is being seen, you can drag the column headers to reorder the table, or click the down arrow icon at the top of the table ( ) to select which columns appear in the table.

4. When you are done verifying the traffic sources that are being monitored, toggle the full session logging switch to **OFF**. Summary information will continue to be collected for all traffic, but only threat-related sessions and files will be saved. This helps to optimize use of disk space.

Step 5: Using TRITON RiskVision

Use the **Incidents** page in the RiskVision Local Manager to track the results of RiskVision file analysis.

Tips for using the table:

◆ Click on a column header and drag it up one row (into the space that says "Drag a column header here and drop it to group by that column") to group results by the selected field.

◆ Click the arrow icon ( ) next to **Show/Hide Columns** at the top, right corner of the table to see all of the columns that can be displayed.

Understanding the process of analysis:

1. When RiskVision identifies files in HTTP or SMTP transactions, it sends them to the local, on-box analytics to determine whether the files contain suspicious or malicious content.

2. File content is analyzed by the Data Analysis Engine to identify potentially sensitive information that is being transferred out of your network.

   The policies and rules used to identify sensitive content are based on the profile that you configure on the **System > Data Profile** page in the Local Manager. By default, data analysis is used to identify Payment Card Industry (PCI) information in file content.

3. Files whose formats are supported by the cloud File Sandbox are also submitted for sandboxing analysis, which uses virtual machines to replicate the behavior of those files when opened. File sandboxing can be used to analyze:

   ■ Executable files

   ■ PDF files

   ■ Microsoft Office files (like DOCX, XLSX, and so on)

4. Both on-box and cloud analytics return a **Threat Level** of malicious, suspicious, or no threat detected for each file analyzed.

   When the result is returned from the cloud File Sandbox, the Threat Level value is a link to a cloud-based report with detailed information about the analysis that was performed and the reason for the threat level that was assigned.

5. The File Analysis table is also updated with data analysis results that show any identified policy violations, including information about some of the strings that triggered the violation.

You can export the data shown on the Incidents page to a CSV file to perform further analysis in third-party reporting tools.

In addition, you can use the **Reporting** page in the Local Manager to generate PDF or RTF reports with information about specific types of malicious activity (like exploit

kits and call home traffic), as well as more detailed information about potential data loss violations discovered by RiskVision.