FORCEPOINT
POWERED BY Raytheon

TRITON® RiskVision Setup Guide

v8.2.x, v8.1.x

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

R060816820

Published 2016
Printed in the United States and Ireland

Trademarks

Contents

1 TRITON RiskVision

TRITON® RiskVision | 11-August-2016

This guide is for Sales Engineers (SEs) preparing TRITON RiskVision for use with TRITON AP-WEB to support proof-of-concept (PoC) engagements.

> **Important**
> TRITON RiskVision is available for versions 8.2.x and 8.1.x on V10000 and V5000 G2R2 and higher appliances.

If you are upgrading a v7.8.x RiskVision appliance to v8.2.x or v8.1.x, see the knowledge base article titled v8.2.x and v8.1.x TRITON RiskVision for PoCs.

This guide has 3 parts

- *Feature summary*, page 2 – Provides descriptive information helpful to prospects and customers.
- *Installation and Configuration Summary*, page 7 – Can be used as a checklist by those familiar with the process.
- *Installation and Configuration Detail*, page 13 – Step-by-step detail, including explanations of features and recommended settings.

Installation and Configuration Summary sections link to their corresponding detail sections.

Feature summary

These sections provide an overview of TRITON RiskVision.

TRITON RiskVision Overview

TRITON RiskVision uses advanced analytics—including rules, signatures, heuristics, and application behaviors—to provide real-time Internet traffic analysis. This analysis is used to:

- Proactively discover security risks.
- Detect access to proxy avoidance and hacking sites, adult content, botnets, keyloggers, sites related to phishing attacks, spyware, and many other types of unsafe content.
- Report on potential vulnerabilities and active threat activity in your network.
- Categorize new sites and dynamic content.

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

- Requests and responses monitored by the solution are analyzed in real time by Advanced Classification Engine (ACE) analytics within Content Gateway. Administrators can:
  - Use dashboard charts, reporting tools, and Real-Time Monitor to investigate and understand the results of this analysis.
  - Enable suspicious activity and usage alerts to be notified about types of detected Internet activity of interest to the organization.
- The cloud-hosted File Sandboxing service can identify advanced malware threats in suspicious files. Administrators can:
  - Receive File Sandboxing alerts when file analysis is complete.
  - Access online File Sandboxing reports to learn more about analyzed files, the threats associated with them, and steps needed for remediation.
  - Use investigative reports to find more information about Internet activity on machines where threat-related files were downloaded.
- Web DLP analyzes data leaving your network to detect data exfiltration activity. Administrators can:
  - Create Web DLP policies that target the types of data loss activity that they want to monitor.

- Use dashboard charts and incident reports in the Data module of the TRITON Manager to investigate data loss activity.

Understanding TRITON RiskVision behavior

TRITON RiskVision is an advanced traffic analysis tool used to investigate your organization's Internet activity. It does not block any Internet requests or responses.

By default, the only Internet monitoring policy configured for TRITON RiskVision applies the "permit" flag to all requests from all clients. In most deployments, no further policy configuration needs to be performed in the TRITON Manager.

In some circumstances, it may be desirable for administrators to configure policies that apply a "blocked" flag to some requests. Such policies are not used for enforcement. Instead, they can be used to highlight types of Internet activity that are of interest to the organization in reports. However, this can lead to unintended side-effects.

- If a policy "blocks" a request based on category or URL, the request is not sent to Content Gateway for analysis.
- Once a request receives the "block" flag, subsequent requests by the user for content internal to that website (for example, clicking through content on the site) may not appear in reports.

  This happens because TRITON RiskVision components do not know that the "block" is virtual. They act as though the user was stopped from viewing the website, and close the connection to the request.

In addition to the ACE analysis offered by Content Gateway, TRITON RiskVision also offers:

- Data analysis of information sent over web channels (Web DLP), configured in the Data module of the TRITON Manager.

  Web DLP policies, like Internet monitoring policies, can be configured to flag some requests as blocked. In this case, a "blocked" flag appears in reports, but no enforcement occurs.
- Sandboxing of suspicious files to identify threats, enabled under File Analysis in the Web module of TRITON Manager.

  When files are sent for sandboxing, if the file is found to be malicious the administrator receives a report. Reports include information that can help with remediation on machines infected by the files.

  The files are not given a "block" flag or other special highlighting in TRITON Manager reports.

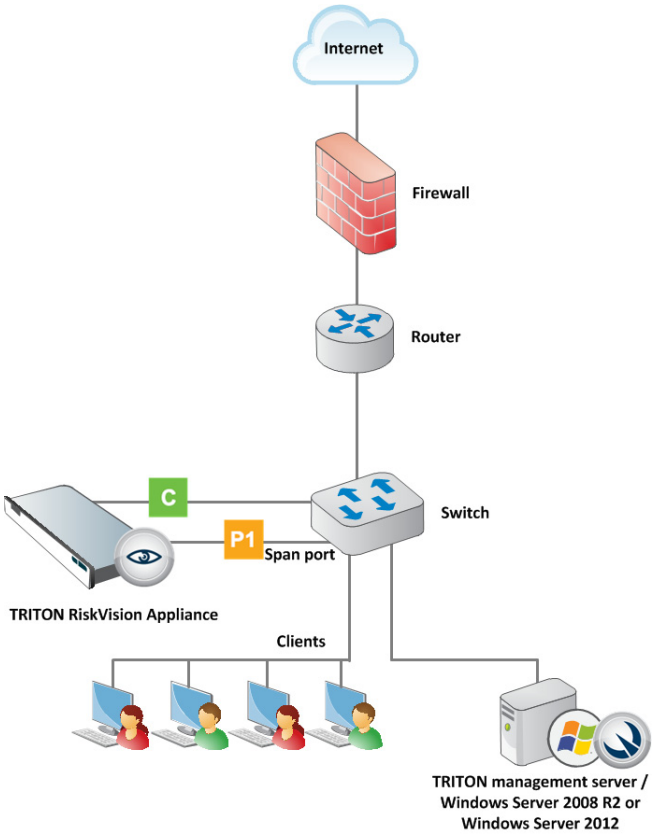
What traffic is analyzed?

The ACE analytics within Content Gateway are applied only to HTTP traffic. Decryption and inspection of HTTPS traffic is not available.

However, Network Agent can be configured to perform simple protocol classification of non-HTTP traffic, to help administrators understand Internet traffic patterns within their organization.

What is the effect of positioning TRITON RiskVision downstream or upstream of an active web proxy?

TRITON RiskVision positioned downstream from the web proxy:



When TRITON RiskVision is positioned downstream from the web proxy, between the clients and the proxy, TRITON RiskVision components see:

- Unaltered HTTP requests from clients
- The client IP address of requests

  These can be mapped to user names if a transparent identification agent is deployed.

Note that:

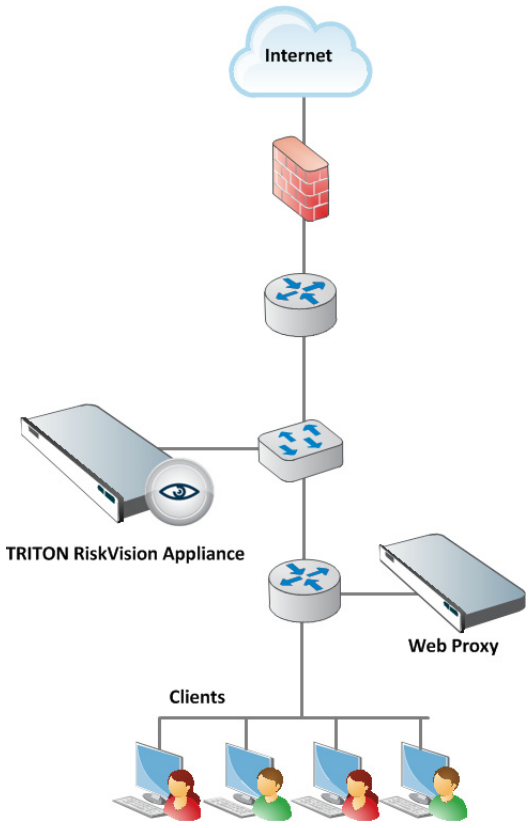
- URL categorization and outbound data protection performed by the upstream proxy does not affect TRITON RiskVision.
- If the upstream proxy blocks HTTP **responses** from origin servers, TRITON RiskVision does not see those responses. TRITON RiskVision does not have an opportunity to analyze blocked response traffic.

Depending on your proxy setup, TRITON RiskVision may require an additional configuration step to ensure that it monitors traffic correctly.

- If the web proxy is an explicit proxy (client browsers are configured to explicitly send HTTP requests to the web proxy), TRITON RiskVision requires a special configuration setting (--parent-proxy) to ensure that requests going to different sites on the same connection (multiplexed connections) are seen. See *Configure TRITON RiskVision to work with an upstream proxy*, page 36.
- If the web proxy is a transparent proxy using WCCP and GRE tunneling, TRITON RiskVision requires a special configuration setting (--gre) to ensure that GRE packets are seen and properly handled. See *Configure TRITON RiskVision to work with an upstream proxy*, page 36.

This positioning of TRITON RiskVision is recommended when looking for threats that were not detected by the web proxy.

TRITON RiskVision positioned upstream from the web proxy:



When TRITON RiskVision is positioned upstream from a web proxy, closer to the Internet egress point:

- TRITON RiskVision sees origin server responses before they are processed by the web proxy. This allows unrestricted application of the real-time analytic features.
- Limitation: If the downstream proxy blocks outbound requests, for example due to URL filtering or outbound scanning, TRITON RiskVision will not see those requests and cannot log them.
- Limitation: If the downstream proxy serves some content from a local cache, TRITON RiskVision may log what appears to be an incorrect category for the URL. An indication of this is “TCP_REFRESH_HIT” entries in the Content Gateway event log (squid.log by default; see “Event log file” in the Content Gateway Manager Help).
- Limitation: Because HTTP requests go through the downstream proxy before being seen by the TRITON RiskVision appliance, the source IP address of all of the requests is the web proxy IP address; this makes it difficult to collect end user information. One solution is to configure the downstream proxy to send X-Forwarded-For and/or X-Authenticated-User HTTP headers and enable “Read authentication from child proxy” in the Content Gateway module of the TRITON RiskVision appliance. See *Configure TRITON RiskVision to work with a downstream proxy*, page 34.

This positioning of the TRITON RiskVision appliance is recommended when you are looking for analysis and trends on all inbound traffic.

2 Installation and Configuration Summary

TRITON® RiskVision | 11-August-2016

Links below connect to step-by-step detail.

System requirements

- V10000 or V5000 G2 R2 or higher
- Microsoft SQL Server 2008, 2008 R2, or 2012 installation; this system must be ready before installing TRITON management and reporting components
- Windows Server 2008 R2 or Windows Server 2012 machine for TRITON management and reporting components
- Switch with span port or mirror port, or a network tap that supports aggregation

Set up the V-Series appliance

Requirements:

- Access to a DNS server
- Continuous access to the Internet
- C interface access to **download.websense.com**

1. Set up the appliance hardware (*Step 1: Set up the appliance hardware*)
   - Rack and power the appliance
   - Cable ports C and P1

- Power on the appliance; the process starts **firstboot**, pausing at the subscription agreement

2. Complete **firstboot** (*Step 2: Run the firstboot script*)
   - At the **Security Mode** prompt select **TRITON AP-WEB**.
   - At the following prompt -- “Do you want to continue?” -- enter “rv”.

   Also be prepared with:
   - The hostname
   - IPv4 address of C
   - DNS server IP address
   - Strong password
3. Configure basic appliance settings (*Step 3: Configure basic appliance settings*)

   After **firstboot** has completed and the appliance has rebooted, log on to the Appliance Manager and:
   - Set the time; NTP is recommended
   - Add a unique system description
4. Configure TRITON RiskVision component interaction (*Step 4: Configure TRITON RiskVision component interaction*)
   - In the Appliance Manager, set the Policy Source
5. Deploy additional appliances (*Step 5 (optional): Deploy additional appliances*)

Create a TRITON Management Server

Before you begin, confirm that:

- Microsoft SQL server is running and that the TRITON management server can connect to it
- The TRITON management server has at least 4 cores (2.5 GHz), 8 GB RAM, 146 GB disk
- All Windows Server updates have been applied
- On Windows Server 2008 R2 machines, .NET Framework 2.0 is installed
- On Windows Server 2012, .NET Framework 2.0 and 3.5 are installed
- Antivirus is disabled for the duration of the install, and then re-enabled
- Clocks on all TRITON RiskVision appliances and servers are synchronized

1. Download the installer **(TRITON8xxSetup.exe)** and start installation. (*Step 1: Download the installer and start installation*)
   - On the **Installation Type** screen, select **TRITON Manager**, then mark the **TRITON AP-WEB or Web Filter & Security** and **TRITON AP-DATA** check boxes.
2. Install TRITON Infrastructure (*Step 2: Install TRITON Infrastructure*).

- On the **SQL Server** screen, select **Use existing SQL Server on another machine**. Enter the **Hostname** or **IP address** of the SQL Server machine, including the instance name, if any.
- Select the **Authentication** method to use for database connections.
- On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Infrastructure and TRITON Manager.
- On the **Administrator Account** screen, enter an email address and password for the default TRITON Manager administration account: **admin**.

3. Install TRITON Manager (*Step 3: Install the TRITON Manager*).
   - On the **Select Components** screen, select **Log Server**, **Linking Service**, **Real-Time Monitor**

     TRITON - AP-WEB is selected by default and cannot be deselected.
   - On the **Policy Server Connection** screen, enter the IP address of the **appliance C interface** and port **55806**.
   - If prompted, allow the installer to include Microsoft SQL Server Native Client and related tools.
   - On the **Log Database Location** screen, specify the IP address or hostname of the SQL Server instance that will host the reporting database.
   - On the **Optimize Log Database Size** screen, select **Log Web page visits**.
   - On the **Filtering Service Communication** screen, enter the IP address of the **appliance C interface** and port **55806**.
4. Install TRITON AP-DATA (*Step 4: Install TRITON AP-DATA components*).
   - On the **Select Components** screen, all required components are selected by default.
   - If prompted, accept that services such as ASP.NET and SMTP will be enabled.
   - If the **Local Administrator** screen appears, specify credentials.
   - If the following message appears, click **Yes** to continue the installation:

     ```
     TRITON AP-DATA needs port 80 free.
     In order to proceed with this installation, DSS will free
     up this port.
     Click Yes to proceed OR click No to preserve your
     settings.
     ```

     A similar message for port 443 may appear. Click **Yes** to continue.
5. Optionally, install a transparent identification agent (*Step 5 (optional): Install a transparent identification agent*).
   - To add the component to the management server, launch the TRITON Installer again. On the **Modify Installation** dashboard, click the **Modify** link for **TRITON AP-WEB or Web Filter & Security**.

- To install the component on another machine, download and launch the installer as described in *Step 1: Download the installer and start installation*. When you get to step 5:
  a. Select the **Custom** radio button at the bottom of the page (not the TRITON Manager radio button).
  b. On the **Custom Installation** screen, select the **Install** link next to **TRITON AP-WEB or Web Filter & Security**.
- On the **Select Components** screen, select the transparent identification agent you want to install.

  eDirectory Agent cannot be installed on the same machine as DC Agent or Logon Agent.
- On the **Policy Server Connection** screen, enter the C interface of the RiskVision full policy source or user directory and filtering appliance.
- If you are installing DC Agent or Logon Agent:
  a. On the **Active Directory** screen, indicate whether you use Active Directory to authenticate users.
  b. On the **Computer Browser** screen, if it not already running, launch the Computer Browser Service.
  c. On the **Directory Service Access** screen, enter a domain admin account to use for connecting to the directory service.

6. Enter a TRITON AP-WEB subscription key and download the Master Database (*Step 6: Enter a key and download the Master Database*).
   - After management server installation is complete, log on to the TRITON Manager and enter the TRITON AP-WEB subscription key.

     Do not make any configuration changes to Content Gateway.
   - If Internet requests originating from the **appliance C interface** must go through a proxy to reach the Internet, provide the proxy details at the same time you enter the key.

Note

Note that when you log on to the TRITON Manager there is nothing to indicate that the installation is TRITON RiskVision mode.

Configure TRITON RiskVision

Configuration includes:

1. Configure Content Gateway (Scanning Options) analysis (*Step 1: Configure Content Gateway analysis*)
2. Understand TRITON RiskVision policies (*Step 2: Understand TRITON RiskVision policies*)

3. Enable Web DLP monitoring (*Step 3: Enable Web DLP monitoring*)
4. Configure Web DLP policies (*Step 4: Configure Web DLP policies*)
5. Configure reporting behavior (*Step 5: Configure reporting behavior*)
6. Configure user directory connections (*Step 6: Configure user directory connections*)
7. Configure a transparent user identification agent (*Step 7 (optional): Configure a transparent user identification agent*)
8. Restart the appliance

Configure for non-standard HTTP ports and for an upstream or downstream proxy

9. If HTTP traffic is sent to a port other than 80 or 8080, you must configure a NAT rule in the Content Gateway manager to ensure that traffic is monitored. (*Create a NAT rule to ensure all traffic is monitored*, page 38)
   - NAT rules are added on the **Configure** > **Networking > ARM** page. After the rule is added, restart Content Gateway.
10. If the traffic analyzed by TRITON RiskVision is managed by a downstream proxy, user identification requires special consideration. (*Configure TRITON RiskVision to work with a downstream proxy*)

    When the downstream web proxy can be configured to insert **X-Forwarded-For** headers or **X-Authenticated-User** headers, TRITON RiskVision can be configured to read the value and include it in transaction handling.
    - Configure the web proxy to insert **X-Forwarded-For** or **X-Authenticated-User** headers.
    - In Content Gateway manager, go to **Configure > My Proxy > Basic** and enable **Read authentication from child proxy**.
    - **Restart** Content Gateway.
11. When traffic analyzed by TRITON RiskVision is managed by an upstream proxy (*Configure TRITON RiskVision to work with an upstream proxy*)
    - *Configure user identification*
    - *Configure TRITON RiskVision for explicit proxy*, or
    - *Configure TRITON RiskVision for transparent proxy with GRE*
    - If you have not already done so, *Create a NAT rule to ensure all traffic is monitored*

    It is highly recommended that you *Use the default policy setup*.

3 Installation and Configuration Detail

TRITON® RiskVision | 11-August-2016

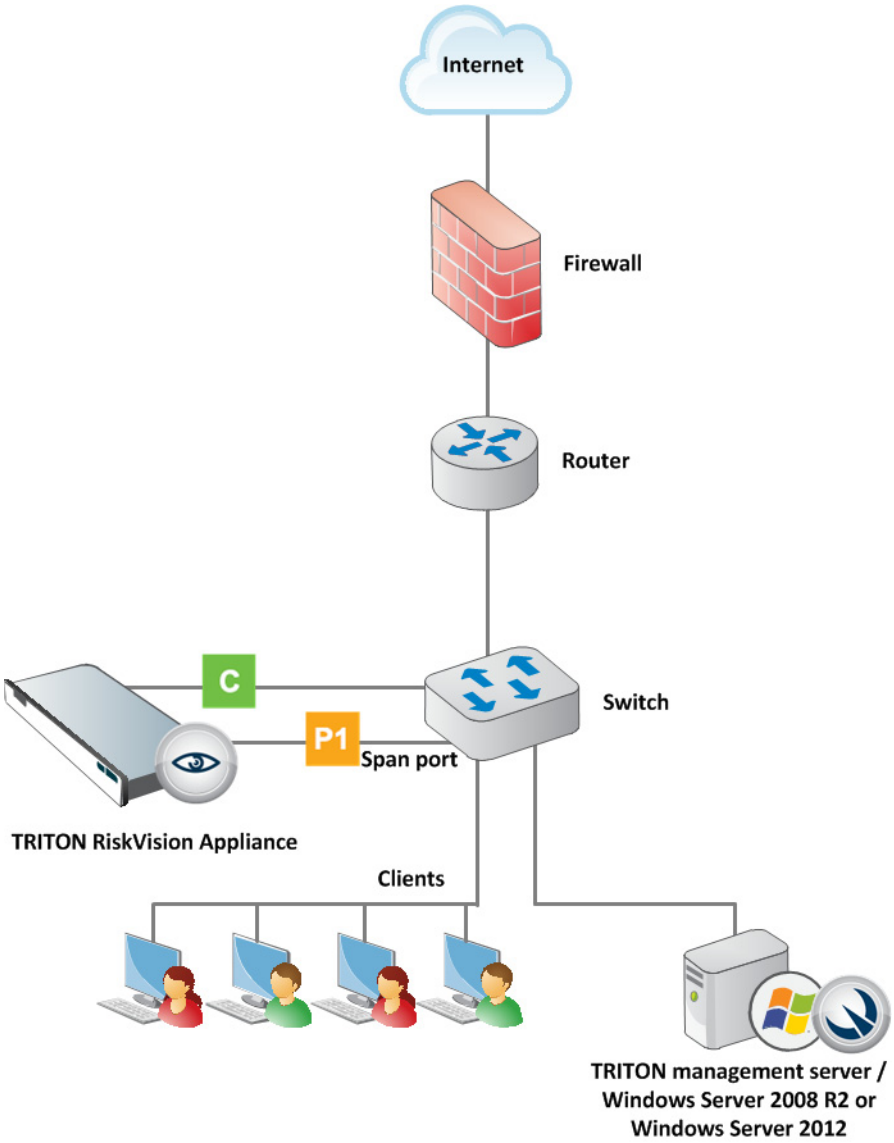
Step-by-step detail.

1. *Set up the V-Series appliance*
   - *Step 1: Set up the appliance hardware*
   - *Step 2: Run the firstboot script*
   - *Step 3: Configure basic appliance settings*
   - *Step 4: Configure TRITON RiskVision component interaction*
   - *Step 5 (optional): Deploy additional appliances*
2. *Install TRITON Management Server*
   - *Step 1: Download the installer and start installation*
   - *Step 2: Install TRITON Infrastructure*
   - *Step 3: Install the TRITON Manager*
   - *Step 4: Install TRITON AP-DATA components*
   - *Step 5 (optional): Install a transparent identification agent*
   - *Step 6: Enter a key and download the Master Database*
3. *Configure TRITON RiskVision*
   - *Step 1: Configure Content Gateway analysis*
   - *Step 2: Understand TRITON RiskVision policies*
   - *Step 3: Enable Web DLP monitoring*
   - *Step 4: Configure Web DLP policies*
   - *Step 5: Configure reporting behavior*
   - *Step 6: Configure user directory connections*
   - *Step 7 (optional): Configure a transparent user identification agent*
4. *Working with upstream and downstream proxies*
   - *Configure TRITON RiskVision to work with a downstream proxy*
   - *Configure TRITON RiskVision to work with an upstream proxy*
   - *Create a NAT rule to ensure all traffic is monitored*

Set up the V-Series appliance

Step 1: Set up the appliance hardware

The diagram below gives a simple overview of a TRITON RiskVision deployment. In addition to the appliance, a Windows Server 2008 R2 or Windows Server 2012 machine is required to host management and reporting components. The management and reporting components must be configured to connect to a Microsoft SQL Server 2008, 2008 R2, or 2012 installation within your network.



Connect the C and P appliance interfaces as described below. Cat 5E cables (or better) are required. Do not use crossover network cables.

Network **interface C** provides communication for appliance modules and handles database downloads. Interface C:

- Must be able to access a DNS server
- Must have 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 P1** connects either to a span or mirror port on the switch or to a network tap that supports aggregation. This allows Content Gateway and Network Agent to monitor client Internet requests.

Step 2: Run the firstboot script

After hardware setup, connect directly to the TRITON RiskVision appliance through the serial port or the monitor and keyboard ports.

An activation script, called **firstboot**, runs when you power up the appliance. The firstboot script prompts you to:

- Supply settings for the network interface labeled C.
- Enter a few other general items, such as hostname and password.

You are given the opportunity to review and change these settings before you exit **firstboot**. After you approve the settings, initial appliance configuration occurs.

Later, if you want to change settings, you can do so through the Appliance Manager.

Know the following information before running **firstboot**.

Security mode	**TRITON AP-WEB** **IMPORTANT:** At the next prompt -- "**Do you want to continue?**" -- enter "**rv**"
Proxy configuration	Select **RiskVision**
Hostname (example: appliance.domain.com) ● 1 - 60 characters long. ● The first character must be a letter. ● Allowed: letters, numbers, dashes, or periods. ● The name cannot end with a period.	
IPv4 address for network interface C	
Subnet mask for network interface C	
Default gateway for network interface C (IP address)	

Primary DNS server for network interface C (IP address) Secondary DNS server IP address (Optional) Tertiary DNS server IP address (Optional)	
Strong password (8 to 15 characters)	
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Forcepoint to help improve the accuracy of traffic analysis and classification.

Run **firstboot** as follows.

1. Access the appliance through a USB keyboard and monitor, or a serial port connection.

   Note

   For serial port activation, use:

   - 9600 baud rate
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes**.
4. **Important:** When prompted to select a security mode, select option 1, **TRITON AP-WEB**.
5. Firstboot follows with

   ```
   You have selected [TRITON AP-WEB].
   Do you want to continue? [yes/no]
   ```

   Important: To the yes/no prompt, enter **rv**.
6. Firstboot then prompts to select a proxy configuration, select **RiskVision**.
7. Follow the on-screen instructions.

After the script completes, continue with the next section.

Note

It's possible to convert a TRITON RiskVision appliance to TRITON AP-WEB. The procedure is:

- Configure interface P1 for in-line traffic handling.
- Enter a standard AP-WEB subscription key.
- Re-run firstboot, and choose TRITON AP-WEB.

When firstboot is complete and the appliance has restarted, the security mode is TRITON AP-WEB. Reconfigure the appliance, Content Gateway, and TRITON components as needed.

Step 3: Configure basic appliance settings

Appliance settings are configured in the Appliance Manager.

1. Open a supported browser (Internet Explorer 8-11, Mozilla Firefox 5 and later, or Google Chrome 13 and later), and enter the following URL in the address bar:

   ```
   https://<IP-address-of-C-interface>:9447/appmng
   ```

2. Log on with the user name **admin** and the password set during **firstboot**.
3. Go to the **Configuration > System** page.
4. Under **Time and Date**, use the **Time zone** list to select the time zone to be used on this system.
5. Use the **Time and date** radio buttons to indicate how you want to set the date.

   Time is set and displayed using 24-hour notation. Make sure that the time and date are synchronized on all TRITON RiskVision appliances, and other machines hosting TRITON components.

   - To synchronize with an Internet Network Time Protocol (NTP) server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

Important

If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

- To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.

6. Enter an appliance **Description**. This is especially important if multiple appliances will be deployed. The description is displayed in the appliance list in the TRITON Manager when the appliance is added there.
7. Click **OK** to save your changes.

Step 4: Configure TRITON RiskVision component interaction

Still in the Appliance Manager:

1. Navigate to the **Configuration > RiskVision Components** page to specify which TRITON RiskVision components are active on the appliance, and where the appliance gets configuration and Internet policy information.
2. Select a **Policy Source** mode:

   - If you are installing only one TRITON RiskVision appliance, or if this is the first TRITON RiskVision appliance you are installing, select **Full policy source**.

     The first TRITON RiskVision appliance you install hosts Policy Broker, which is responsible for global configuration and policy data.

   If you install additional TRITON RiskVision appliances, they may be either:

   - **Filtering only** appliances, which include only components used for Internet access monitoring.

     When you configure a filtering only appliance, you are prompted for the location of a Policy Server instance. This may be either the full policy source appliance or a user directory and filtering appliance.
   - **User directory and filtering** appliances, which include both components used for user identification and components used for Internet access monitoring.

     When you configure a user directory and filtering appliances, you are prompted for the location of the policy source.
3. Click **OK** to save and apply your changes.

Step 5 (optional): Deploy additional appliances

If you are deploying more than one TRITON RiskVision appliance, repeat the steps in this section for each appliance, beginning with *Step 1: Set up the appliance hardware*, page 14.

When you reach *Step 4: Configure TRITON RiskVision component interaction*, instead of selecting **Full policy source** as the Policy Source mode for the appliance, select **Filtering only** or **User directory and filtering**.

In most cases, it is preferable to deploy secondary appliances in filtering only mode.

Important

Content Gateway with TRITON RiskVision cannot be configured into a cluster. When a Content Gateway configuration change is needed, the change must be made in the Content Gateway module on each appliance.

When you are finished deploying appliances, continue with the next topic: *Install TRITON Management Server*, page 19.

Install TRITON Management Server

After setting up the appliance, install management and reporting components on a Windows Server 2008 R2 or Windows Server 2012 machine.

- *Step 1: Download the installer and start installation*
- *Step 2: Install TRITON Infrastructure*
- *Step 3: Install the TRITON Manager*
- *Step 4: Install TRITON AP-DATA components*
- *Step 5 (optional): Install a transparent identification agent*
- *Step 6: Enter a key and download the Master Database*

Before you begin:

- Make sure that Microsoft SQL Server 2008, 2008 R2, or 2012 is installed and running in your network, and that the network is configured to allow the TRITON management server machine to connect to the SQL Server machine.
- Make sure that Windows Server 2008 R2 or Windows Server 2012 machine that will become the TRITON management server has at least 4 CPU cores (2.5 GHz), 8 GB RAM, and 146 GB of disk space available.
- Make sure all Microsoft updates have been applied on the management server machine. There should be no pending updates, especially any requiring a restart of the system.
- The Microsoft .NET Framework is required to run the Windows installer:
  - On Windows Server 2008 R2 machines, .NET Framework 2.0 is required.
  - On Windows Server 2012, .NET Framework 2.0 and 3.5 are both required.

  You can install the required version or versions via the Server Manager, or download it from www.microsoft.com.
- Synchronize the clocks on all TRITON RiskVision appliances and machines on which TRITON components are installed. It is a good practice to point the machines to the same Network Time Protocol server.
- Disable any antivirus software on the machine prior to installing TRITON components. Be sure to re-enable antivirus software after installation.
- Disable any firewall on the machine before starting the TRITON installer and then re-enable it after installation. Open ports as required by the TRITON components you have installed, and make sure that required ports are not being used by other local services on the machine. Some ports are used only during installation and can be closed once installation is complete. See the Web tab of the TRITON Ports spreadsheet for more information about ports.

After the management server is installed, continue to *Configure TRITON RiskVision*, page 26.

Step 1: Download the installer and start installation

1. Log on to the machine with domain admin privileges.
2. Download the **TRITON Installer** from the **Downloads** tab of My Account (formerly mywebsense.com).
   - The file name is **TRITON8xxSetup.**exe.
   - The version is 8.2.x or 8.1.x; the version must match the version installed on the appliance.
   - When extracted, the installation files occupy about 3 GB of disk space.
3. Double-click the installer executable to launch the **TRITON Setup** program.

   A progress dialog box is displayed as files are extracted. This may take several minutes.
4. On the **Welcome** screen, click **Start**.

5. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
6. On the **Installation Type** screen, select **TRITON Manager**, then mark the **TRITON AP-WEB or Web Filter & Security** and **TRITON AP-DATA** check boxes.

   Click **Next**.
7. Do not install Email Gateway virtual appliance.
8. On the **Summary** screen, click **Next** to continue. The TRITON Infrastructure Setup program launches. Continue with the next section.

Step 2: Install TRITON Infrastructure

Still in the installer:

1. On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
2. On the **Installation Directory** screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.

   Important

   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

3. On the **SQL Server** screen, select **Use existing SQL Server on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

   Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any.

   - If you are using a named instance, the instance must already exist.
   - If you are using SQL Server clustering, enter the virtual IP address of the cluster.

     Also provide the **Port** used to connect to the database (1433, by default).
4. Select the **Authentication** method to use for database connections: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).

   a. Provide the **User Name** or **Account** and **Password** for a database account with system administrator rights in SQL Server, then click **Next**.

   b. If your SQL Server installation is already configured to use SSL encryption to secure communication with the database, mark **Encrypt connection**.

   When you are finished, click **Next** to verify the connection to the database.

   - If the connection test is successful, the next installer screen appears.
   - If the test is unsuccessful, the following message appears:

     ```
     Unable to connect to SQL
     Make sure the SQL Server you specified is currently
     ```

```
running. If it is running, verify the access
credentials you supplied.
```

Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

5. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Infrastructure and TRITON Manager.
   - Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.
   - Specify the **Server or domain** of the user account that you want to use to run the TRITON Infrastructure and TRITON Manager services. The server/host name cannot exceed 15 characters.
   - Specify the **User name** of the account that you want to use to run TRITON services.
   - Enter the **Password** for the specified account.
6. On the **Administrator Account** screen, enter an email address and password for the default TRITON Manager administration account: **admin**. When you are finished, click **Next**.

   System notification and password reset information is sent to the email address specified (once SMTP configuration is done; see next step).

   Specify a strong password.
7. On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications and then click **Next**. You can also configure these settings in the TRITON Manager after installation.
   - **IP address or hostname**: IP address or host name of the SMTP server through which email alerts should be sent. In most cases, the default **Port** (25) should be used. If the specified SMTP server is configured to use a different port, enter it here.
   - **Sender email address**: Originator email address appearing in notification email.
   - **Sender name**: Optional descriptive name that can appear in notification email. This can help recipients identify this as a notification email from the TRITON Manager.
8. On the **Pre-Installation Summary** screen, verify the information and then click **Next** to begin the installation.
9. Next, the **Installation** screen appears. Wait until all files have been installed.

   If the following message appears, check whether port 9443 is already in use on this machine:

   ```
   Error 1920. Server 'TRITON Central Access'
   (EIPManagerProxy) failed to start. Verify that you have
   sufficient privileges to start system services.
   ```

   If port 9443 is in use, release it and then click **Retry** to continue installation.
10. On the **Installation Complete** screen, click **Finish**.

The TRITON Infrastructure Setup program closes and the web component installer launches. Continue with the next section.

Step 3: Install the TRITON Manager

1. On the **Select Components** screen, select the following components to install, and then click **Next**.
   - **Log Server**
   - **Linking Service** (selected by default)
   - **Real-Time Monitor**

   Note that TRITON AP-WEB (the primary component supporting the TRITON Manager) is selected by default and cannot be deselected.
2. On **Policy Server Connection** screen, enter the IP address and port used by Policy Server (the IP address of the **appliance C interface** and **55806**, by default), and then click **Next**.
3. If the management server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components. Follow the on-screen prompts to complete this process.
4. Use the **Log Database Location** screen to specify the IP address or hostname of the SQL Server instance that will host the reporting database (if prompted), and provide a path for the database files, and then click **Next**.
5. On the **Optimize Log Database Size** screen, select **Log Web page visits**, and then click **Next**.
6. On the **Filtering Service Communication** screen, provide the IP address and port used by Filtering Service (the IP address of the **appliance C interface** and **15868**), and then click **Next**.
7. On the **Pre-Installation Summary** screen, verify the information shown.
8. Click **Next** to start the installation. The installation progress screen displays. Wait for installation to complete.
9. On the **Installation Complete** screen, click **Next**.

Continue with the next section to install TRITON AP-DATA components.

Step 4: Install TRITON AP-DATA components

TRITON RiskVision includes Web DLP. Data loss monitoring is performed by TRITON AP-DATA components installed on the TRITON management server, and configured in the Data module of the TRITON Manager.

To install the TRITON AP-DATA components:

1. When the TRITON AP-DATA installer Welcome screen displays, click **Next**.
2. On the Select Components screen, all required components are selected by default and the selections cannot be changed. Click **Next**.

3. If prompted, click **OK** to accept that services such as ASP.NET and SMTP will be enabled.
4. On the Fingerprinting Database screen, accept the default location or click **Browse** to specify a different location (local path only).
5. Use the Temporary Folder Location Screen to provide the name of a folder to use for temporary files created during archive processing and system backup and restore. Also indicate:
   - Whether to **Enable incident archiving and system backup** to archive old or aging incidents and perform system backup or restore.
   - Use the **From SQL Server** field to enter the UNC path that the SQL Server should use to access the temporary folder. Make sure the account used to run SQL has write access to this folder.
   - Use the **From TRITON Management Server** field to enter the UNC path the management server should use to access the temporary folder. Enter a user name and password for a user who is authorized to access this location.
6. If the Local Administrator screen appears, provide credentials for a local administrator account for Web DLP components to use, then click **Next**.
7. In the Installation Confirmation screen, click **Install** to begin installing TRITON AP-DATA components.
8. If the following message appears, click **Yes** to continue the installation:

   ```
   TRITON AP-DATA needs port 80 free.
   In order to proceed with this installation, DSS will free
   up this port.
   Click Yes to proceed OR click No to preserve your
   settings.
   ```

   A similar message for port 443 may appear. Click **Yes** to continue.
9. The Installation progress screen appears. Wait for the installation to complete.

   When the Installation Complete screen appears, click **Finish** to close the installer.

You have completed installation of the TRITON management server.

Step 5 (optional): Install a transparent identification agent

If you want your TRITON RiskVision reports to include user information, you can install a transparent identification agent. There are 4 agents to choose from:

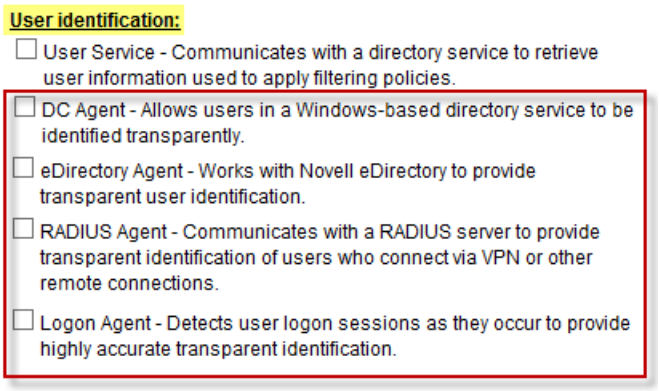
- DC Agent is used with a Windows-based directory service. The agent periodically queries domain controllers for user logon sessions and polls client machines to verify logon status.
- Logon Agent identifies users as they log on to Windows domains. Its associated logon application runs on Windows or Mac clients.

  Note that with Logon Agent, you must both install the agent and deploy the logon application to client machines.
- RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services. The agent works with a RADIUS server and client to identify users logging on from remote locations.

- eDirectory Agent uses Novell eDirectory authentication to map users to IP addresses.

You can install the transparent identification agent on your TRITON management server, or on another Windows Server 2008 R2 or Windows Server 2012 machine in your network.

1. Launch the TRITON Installer on the machine that will host the transparent identification agent:
   - To add the component to the management server, launch the TRITON Installer executable again. On the Modify Installation dashboard, click the **Modify** link for **TRITON AP-WEB or Web Filter & Security**.
   - To install the component on another machine, download and launch the installer as described in *Step 1: Download the installer and start installation*. When you get to step 5 of the procedure:
     a. Select the **Custom** radio button at the bottom of the page (not the TRITON Manager radio button).
     b. On the Custom Installation screen, select the **Install** link next to **TRITON AP-WEB or Web Filter & Security**.
2. On the Select Components screen, scroll down to the User Identification section, mark the check box next to the transparent identification agent that you want to install, and click **Next**.



   Note that eDirectory Agent cannot be installed on the same machine as DC Agent or Logon Agent.
3. On the Policy Server Connection Screen, enter the **Policy Server IP address** (the IP address of the C interface of a TRITON RiskVision full policy source or user directory and filtering appliance), then click **Next**.
4. If you are installing DC Agent or Logon Agent:
   a. On the Active Directory screen, you are asked whether you are using Active Directory to authenticate users in your network. Respond, then click **Next**.
   b. On the Computer Browser screen, you are prompted to launch the Computer Browser Service, if it not already running. Click **Next**.

c. On the Directory Service Access screen, you are prompted to enter a domain admin account to use for connecting to the directory service. Enter a user name and password, then click **Next**.

5. On the Installation Directory screen, accept the default installation path, or click **Choose** to enter a different path. When you are finished, click **Next**.
6. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.
7. On the Installation Complete screen, click **Done**.

Step 6: Enter a key and download the Master Database

After the management server installation is complete, log on to the TRITON Manager and enter your TRITON AP-WEB subscription key. Do not make any configuration changes to the Content Gateway component until after the TRITON AP-WEB subscription key has been entered.

1. Open a supported browser and enter the following URL in the address bar:

   ```
   https://<IP-address-of-management server>:9443/triton/
   ```

2. Enter the user name **admin** and the password set during installation, then click **Log On**.
3. The Initial Setup Checklist prompts you to enter your key. If Internet requests originating from the **appliance C interface** must go through a proxy to reach the Internet, provide the proxy details at the same time you enter the key, and before clicking **OK**.
4. To monitor the progress of the Master Database download, do either of the following:
   - Click the **Database Download** button on any tab of the **Status > Dashboard** page.
   - Watch the **Health Alerts** list on the **System** dashboard.
5. When the download is complete, log off of TRITON Manager and continue with the next section.

   Note that when you log on to the TRITON Manager there is nothing to indicate that the installation is in TRITON RiskVision mode.

Configure TRITON RiskVision

Step 1: Configure Content Gateway analysis

Administrators can adjust the settings that determine how TRITON RiskVision components analyze Internet traffic.

This section describes how to enable the highest available level of traffic analysis. This configuration maximizes the number of requests sent through ACE analysis, but also increases the performance demands on your TRITON RiskVision appliances.

After collecting some initial TRITON RiskVision data, you may want to tune these settings for a better balance of security reporting and system performance.

Note that even with the highest level of analysis enabled, not all traffic may be sent to Content Gateway for analysis.

- If any policies that you configure (including the Default policy) use only the Monitor Only filters, all traffic goes to Content Gateway, and reports do not show any blocked requests.
- If your policies include filters that block categories (explained in the next section), any requests flagged as blocked **before analysis** (that is, any requests for URLs assigned to Master Database categories blocked by the filter) are not forwarded to the proxy.

  In other words, even though no actual block occurs, the request is treated **as if it had been blocked** based on Master Database categorization, and no further analysis is performed.

To configure how Content Gateway analyzes traffic:

1. Log on to the TRITON Manager as **admin**. You are connected to the Web module by default.
2. Select the **Settings** tab of the left navigation page, then navigate to the **Scanning > Scanning Options** page.
3. Under Content Categorization, make sure that the **On** radio button is selected, and that the **Analyze links embedded in Web content** check box is marked.
4. Under Tunneled Protocol Detection, make sure that the **On** radio button is selected.
5. Under Security Threats: Content Security, make sure that the **On** radio button is selected, and the **Aggressive analysis** check box is marked.
6. Under Security Threats: File Analysis:
   - Under Advanced Detection, make sure that the **On** radio button is checked, and the **Aggressive analysis** check box is marked.
   - Under Antivirus Scanning, make sure that the **On** radio button is checked, and the **Aggressive analysis** check box is marked.
7. Under Outbound Scanning, make sure that both the **Analyze for and block outbound security threats** and **Data theft protection** check boxes are marked.
8. Under File Sandboxing:
   a. Select the **On** radio button to have suspicious executable files sent to the cloud-hosted file sandbox for behavioral analysis.
   b. On the Settings > Alerts > Enable Alerts page, enable **Email Alerts**, then on the Settings > Alerts > Suspicious Activity page, enable **File Sandboxing Alerts**.
9. Click **OK** to cache your changes, then click **Save and Deploy** to implement them.

Continue to the next section to find out more about TRITON RiskVision policies.

Step 2: Understand TRITON RiskVision policies

When users access the Internet, TRITON RiskVision logs the activity so that it can be reviewed in reports.

After installation, TRITON RiskVision includes a **Default** policy, in effect 24 hours a day, 7 days a week. Initially, this policy is configured to use the **Monitor Only** category filter, which flags all Internet requests as permitted, and applies to all requests from all clients.

This configuration ensures that:

- Requests are sent to Content Gateway for analysis as expected.
- Internet activity is logged fully.
- Reporting tools accurately reflect how Internet traffic was treated by TRITON RiskVision components.

In many cases, it is not necessary to customize the Default policy or create other TRITON RiskVision policies.

It is, however, possible to configure TRITON RiskVision policies to flag some types of traffic as "blocked" to make them stand out more easily in reports.

When you create policies that include "blocking":

- Regardless of how strict the policies are that you create, no requests are actually blocked.
- Requests that Filtering Services flags as "blocked" based on your policies and Master Database categorization are not sent to Content Gateway for analysis.
- When Filtering Service flags a request as "blocked," all components drop their connection to that request. As a result, if the user visits other pages within the "blocked" site, that activity is not logged and does not appear in reporting tools.

Important

If your TRITON RiskVision appliance is located between clients in your network and a third-party proxy, and explicit proxy is used to direct client requests, do not configure policies that assign the "block" flag.

Instead, use the default configuration provided with TRITON RiskVision v1.0. See *Use the default policy setup*, page 38, for more information.

If your organization requires custom policies, they are configured in the Web module of TRITON Manager on the **Policy Management > Policies** page. See Help (accessed from the Help menu in the TRITON Manager) for detailed instructions.

Step 3: Enable Web DLP monitoring

TRITON RiskVision includes the ability to monitor how and where users post sensitive data via HTTP connections.

Before Web DLP policies for data loss detection can be configured and deployed, you must first enable communication between the Content Gateway and TRITON AP-DATA components.

To do this:

1. Log on to the Content Gateway manager:

   ```
   https://<appliance_C_interface>:8081
   ```

   The logon name is **admin** and the password is the same one used to log on to the Appliance Manager.
2. Navigate to the **Configure > My Proxy > Basic** page (the page that appears by default when you click the Basic tab).
3. Under Networking, mark the **On** radio button next to **Web DLP**, then make sure that the **Integrated on-box** radio button is selected (the default).
4. Click **Apply** and restart Content Gateway.

Continue with *Step 4: Configure Web DLP policies* to complete the registration process and start monitoring data loss activity.

Step 4: Configure Web DLP policies

In addition to standard TRITON RiskVision policies, you can also configure Web DLP policies to detect data leaving your organization through web channels (for example, in files uploaded to the Internet).

Use the Data module in TRITON Manager to configure Web DLP policies:

1. Select the **Data** module of the TRITON Manager.
2. On the Main tab, navigate to the **Policy Management > DLP Policies > Web DLP Policy** page.
3. On the Attributes tab, select and enable the attributes to monitor, such as:
   - Regulatory and compliance attributes, like protected health information
   - Data theft attributes, like password information and encrypted files
   - Uploaded files with specified names or file types
   - Custom patterns and phrases appropriate to your organization or industry

   When the settings you configure are matched, the policy is triggered.
4. Select the **Destination** tab, then specify the websites where you do not want your data sent.
5. Select the **Policy Owners** tab, then identify an administrator as the owner for the policy. The policy owner can be configured to receive notifications associated with Web DLP policy violations.
6. Click **OK**, then click **Deploy**.

When you click Deploy, the TRITON AP-DATA components complete their registration with the Content Gateway component (initialized when you completed *Step 3: Enable Web DLP monitoring*) and activate the policies that you configured.

See TRITON AP-DATA Help (accessed from the Help menu in the Data module of TRITON Manager) for more information about Web DLP policies.

Step 5: Configure reporting behavior

Forensic data capture

By default, TRITON RiskVision reporting components only capture file-related forensic data for threat incidents flagged as blocked. Because many deployments use policies that apply only the permit flag to requests, as a best practice, change this setting when you configure your deployment.

To do this:

1. Log on to the TRITON Manager and select the **Web** module.
2. Navigate to the **Settings > Reporting > Dashboard** page.
3. Under Incident Data for Forensic Investigation, make sure the **Store forensic data about Threats incidents...** check box is marked, then select the **All requests** radio button.
4. Click **OK** to cache your change, then click **Save and Deploy** to implement it.

Logging full URLs

By default, in order to reduce the size of the reporting database, TRITON RiskVision reporting components record the domain portion of requested URLs, but not the entire URL.

If your Microsoft SQL Server installation has the resources to host large databases, or if you do not need to store data for long periods of time, you can configure TRITON RiskVision to record the entire URL string for requests by enabling full URL logging.

To do this:

1. Log on to the TRITON Manager and select the **Web** module.
2. Navigate to the **Settings > Reporting > Log Database** page.
3. Scroll down to the **Full URL Logging** section.
4. Select the **Record domain and full URL of each site requested** radio button.
5. Click **OK** to cache your changes, then click **Save and Deploy** to implement them.

Step 6: Configure user directory connections

Before you can add directory clients (users, groups, and OUs) in the TRITON Manager, you must configure User Service to retrieve information from your directory service. User Service also:

- Maps users to groups when you use a transparent identification agent to identify users
- Ensures that user names are reported correctly when the TRITON RiskVision appliance is upstream from a third-party proxy, and X-Authenticated-User HTTP headers are being used

You must also configure user directory settings separately to enable user-based reporting on Web DLP policy application.

User Service directory settings

Configure the User Service connection to the directory on the **Settings > General > Directory Services** page in the TRITON Manager.

Find full instructions for each supported directory in the TRITON Manager Help, accessed through the Help menu in the TRITON Manager.

Note that if User Service will connect to Active Directory in native mode, you must configure the WINS settings on the Active Directory (Mixed Mode) page before adding global catalog connections on the Active Directory (Native Mode) page.

Web DLP directory settings

To resolve user details during analysis and enhance the details displayed in reporting, configure Web DLP directory settings in the Data module of TRITON Manager.

1. Navigate to the **Settings > General > System** page.
2. Click the **User Directories** option, then click **New** in the toolbar.
3. Click **Help > Explain This Page** to open TRITON AP-DATA Help and find instructions for completing this task.
4. When you are finished, click **OK**, then click **Deploy**.

Step 7 (optional): Configure a transparent user identification agent

Depending on which transparent identification agent you have chosen to install, additional configuration may need to be performed:

- In the TRITON Manager
- In your network, to enable communication between the agent and your user directory
- On client machines

Use the links below to access comprehensive configuration information for the transparent identification agent that you have installed:

- Using DC Agent for Transparent User Identification
- Using Logon Agent for Transparent User Identification

- Using eDirectory Agent for Transparent User Identification
- Using RADIUS Agent for Transparent User Identification

Next steps

Working with third-party proxies

If you are using TRITON RiskVision in a network that also includes a third-party proxy, continue with the appropriate section:

- *Configure TRITON RiskVision to work with a downstream proxy*, page 34
- *Configure TRITON RiskVision to work with an upstream proxy*, page 36

If HTTP traffic in your network goes through a non-standard port, you need to create a NAT rule to ensure that TRITON RiskVision monitors Internet traffic on that port. See:

- *Create a NAT rule to ensure all traffic is monitored*, page 38

Configuring alerts

You can configure TRITON RiskVision and its Web DLP component to send alerts to specified administrators when specific types of traffic or incidents reach thresholds that you configure.

- In the Web module of TRITON Manager, navigate to the **Settings > Alerts > Enable Alerts** page to enable alerting via email, SNMP, or both.

  Once at least one alerting channel is configured, use the **Suspicious Activity**, **Category Usage**, and **Protocol Usage** settings pages to set up the alerts that you want to receive.

  Detailed instructions can be found in the TRITON AP-WEB Help, accessed from the Help menu in the TRITON toolbar.
- In the Data module of TRTION Manager, navigate to the **Settings > General > System** page and click **Alerts**.

  Here, you can both select the conditions that you want to have trigger alerts, and configure email settings to determine how alert messages are sent.

  Detailed instructions can be found in the TRITON AP-DATA Help, accessed from the Help menu in the TRITON toolbar.

Using reports

TRITON RiskVision includes a number of reporting tools that you can use to verify your setup, uncover threat activity, and explore your data. See the TRITON RiskVision Reporting Guide for instructions.

Working with upstream and downstream proxies

- If traffic on your network uses one or more non-standard ports for HTTP traffic, you need to create a Content Gateway NAT rule to configure Content Gateway to monitor those ports. See *Create a NAT rule to ensure all traffic is monitored*, page 38.
- If the traffic analyzed by TRITON RiskVision is managed by a web proxy, some additional configuration may be needed on the TRITON RiskVision appliance.

  Configuration requirements differ depending on whether the TRITON RiskVision appliance:

  - Is upstream (closer to the Internet egress point) or downstream (closer to your clients/users) from the web proxy.

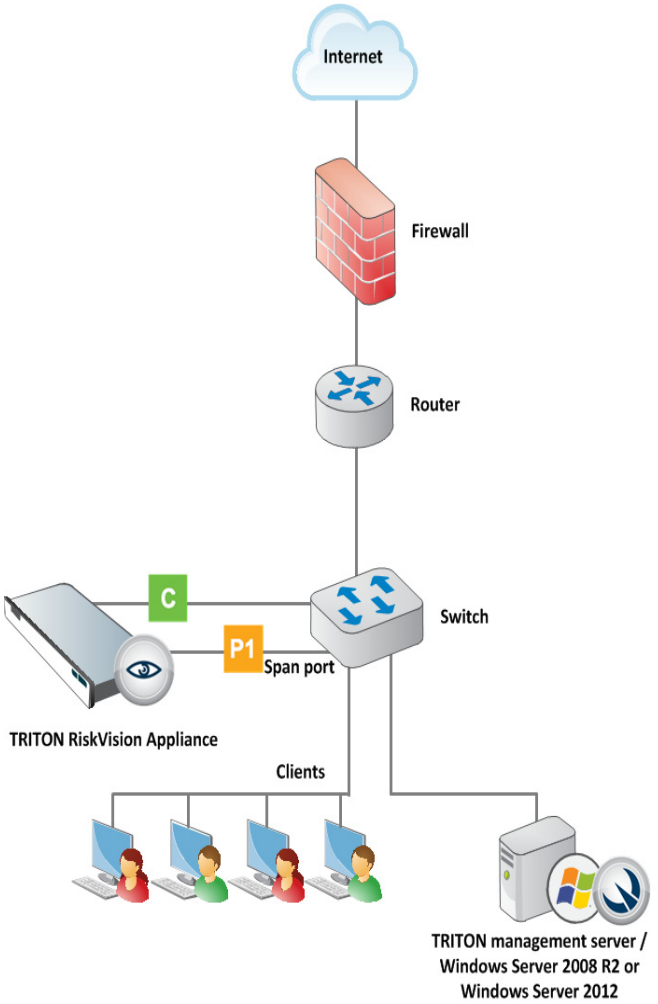
    (For more about the effects of upstream and downstream position in the network, see *What is the effect of positioning TRITON RiskVision downstream or upstream of an active web proxy?*, page 4.)
  - Uses explicit or transparent (interception redirect) methods to direct client traffic to the web proxy

  See:

  - *Configure TRITON RiskVision to work with a downstream proxy*, page 34
  - *Configure TRITON RiskVision to work with an upstream proxy*, page 36

Configure TRITON RiskVision to work with a downstream proxy

If your network includes a web proxy, the TRITON RiskVision appliance may be deployed between the proxy and the Internet, as shown below:



User identification

In this deployment, user identification is the only function that requires special consideration.

Unless IP spoofing is used by the web proxy, it is usual for requests flowing through the web proxy to have the original source IP address replaced with the proxy's IP address. Because of this, unless special provisions are made on the downstream proxy, it impossible to determine the requestor's user name or IP address.

If the downstream proxy is configured for IP spoofing, TRITON RiskVision will see the originating IP address and use it for logging. If a transparent user identification agent is deployed, an attempt is made to map the IP address to a user name.

When the web proxy can insert X-Forwarded-For

When the web proxy can be configured to insert **X-Forwarded-For** headers (the *de facto* field for identifying the originating IP address), TRITON RiskVision can be configured to read the value and include it in transaction handling. If a transparent user identification agent is deployed, an attempt is made to map the IP address to a user name.

To implement the solution:

1. Configure the web proxy to insert **X-Forwarded-For** headers.
2. Log on to the Content Gateway manager and go to **Configure > My Proxy > Basic**.
3. At the bottom of the page, enable **Read authentication from child proxy** and click **Apply**.
4. At the top of the page, click **Restart**.
5. Run some test traffic and check the reports and logs for IP addresses and user names.

When the web proxy performs user authentication

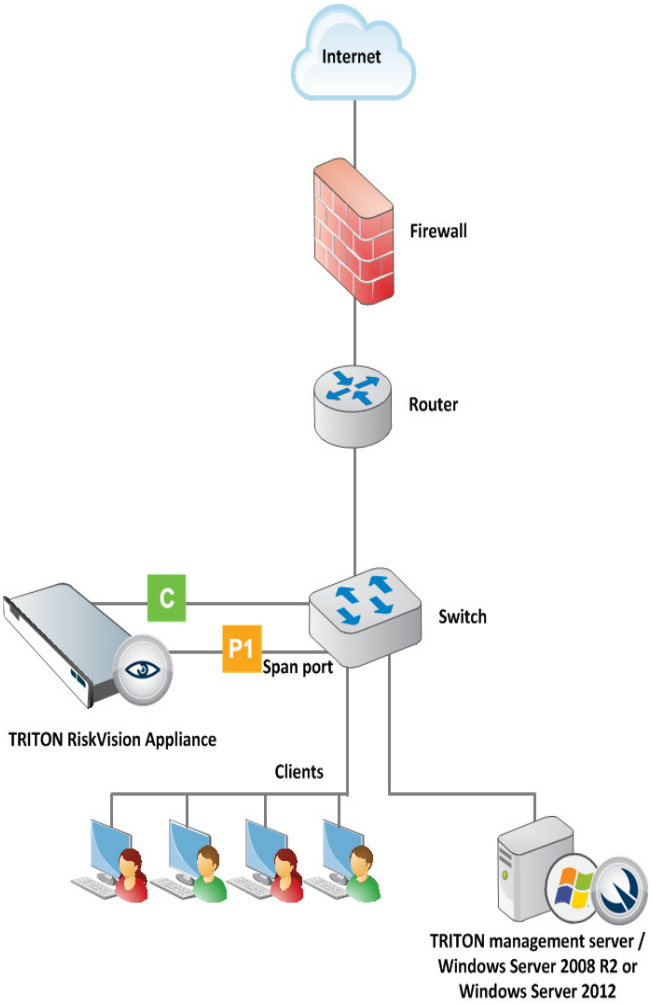
If the downstream proxy performs user authentication and has the ability to insert **X-Authenticated-User** headers (the *de facto* field for passing the authenticated user name), TRITON RiskVision can be configured to read the value and include it in transaction handling.

To implement the solution:

1. Configure the web proxy to insert **X-Authenticated-User** headers.
2. Log on to the Content Gateway manager and go to **Configure > My Proxy > Basic**.
3. At the bottom of the page, enable **Read authentication from child proxy** and click **Apply**.
4. At the top of the page, click **Restart**.
5. Run some test traffic and check the reports and logs for user names.

Configure TRITON RiskVision to work with an upstream proxy

If your network includes a web proxy, the TRITON RiskVision appliance may be deployed in the network between the proxy and clients, as shown below:



In this deployment:

1. *Configure user identification*
2. *Configure TRITON RiskVision for explicit proxy*
3. *Configure TRITON RiskVision for transparent proxy with GRE*
4. *Create a NAT rule to ensure all traffic is monitored*

It is highly recommended that you also *Use the default policy setup*.

Configure user identification

In this configuration, although requests that require proxy authentication can be monitored, you must deploy a transparent user identification agent to see user information in reports.

- TRITON RiskVision sees the source (client) IP address
- TRITON RiskVision components cannot obtain user information from authentication messages.
- If no transparent user identification agent is deployed, TRITON RiskVision components log only client IP addresses.

Configure TRITON RiskVision for explicit proxy

If client applications are configured to explicitly send Web requests to the web proxy, there is an additional configuration step. This step ensures that multiplexed requests to different websites via a single client/proxy connection are handled correctly.

To perform the necessary configuration step:

1. Ensure that Appliance Manager **Remote Access** is enabled. (In the Appliance Manager, go to **Administration > Toolbox** and enable **Remote Access**.)
2. Use SSH to connect to the C IP address of the TRITON RiskVision appliance.
3. At the logon prompt, enter the same credentials you use to log on to the Appliance Manager.
4. In the command line interface (CLI), enter the following command:

   ```
   monitor-config --parent_proxy 1
   ```

5. You will be asked if you want to restart Content Gateway. Respond 'Yes' and wait while the appliance configuration is updated and Content Gateway restarts.
6. Logout to close the SSH session.

After you run this command, the TRITON RiskVision appliance can still monitor Internet requests that go directly to the Internet without passing through the web proxy.

Configure TRITON RiskVision for transparent proxy with GRE

If your network transparently redirects Internet requests with WCCP and GRE tunneling, an additional configuration setting is required.

To perform the necessary configuration step:

1. Ensure that **Remote Access** is enabled. (In the Appliance Manager, go to **Administration > Toolbox** and enable **Remote Access**.)
2. Use SSH to connect to the C IP address of the TRITON RiskVision appliance.
3. At the logon prompt, enter the same credentials you use to log on to the Appliance Manager.
4. In the command line interface (CLI), enable GRE handling with the following command:

   ```
   monitor-config --gre 1
   ```

5. You will be asked if you want to restart Content Gateway. Respond 'Yes' and wait while the appliance configuration is updated and Content Gateway restarts.
6. Logout to close the SSH session.

Use the default policy setup

When TRITON RiskVision is deployed with an upstream web proxy, it is best to avoid customizing policies in the TRITON Manager. Instead, use the default configuration:

- The Default policy is assigned to all requests.
- The Default policy uses the Monitor Only category and protocol filters.
- All requests are flagged as permitted in reports.

If you create custom policies that apply the block flag to some requests, your reporting data will be incomplete. Due to the type of multiplexing that occurs in a parent proxy configuration, when a request is flagged as blocked, other requests from the same client IP address to different websites are not seen.

Create a NAT rule to ensure all traffic is monitored

If HTTP traffic is sent to a port other than 80 or 8080, you must configure a NAT rule in the Content Gateway manager to ensure that traffic is monitored appropriately.

1. Log on to the Content Gateway manager and select the **Configure** tab of the left navigation pane.
2. On the **Configure** tab, select **Networking > ARM**, and then click **Edit File** under the Network Address Translation (NAT) table.
3. Next to Ethernet Interface, enter **eth0**, and keep the default Connection Type (**tcp**).
4. Enter **0.0.0.0** as the Destination IP address and leave the Destination CIDR blank.
5. Enter the custom port used by the web proxy as the Destination Port.
6. Enter **169.254.254.1** as the Redirected Destination IP address.
7. Enter **8080** as the Redirected Destination port.
8. Click **Add**, then click **Apply**.
9. Click **Close** to return to the ARM page. To view the new rule in the NAT table, click **Refresh**.
10. Go to **Configure > My Proxy > Basic** and click **Restart** to restart Content Gateway.

The new rule takes effect when the restart is complete.

Network Address Translation (NAT)

Ethernet Interface	Connection Type	Destination IP	Destination CIDR (Optional)	Destination Port	Redirected Destination IP	Redirected Destination Port	User Protocol (Optional)
eth0	tcp	0.0.0.0	0	80	169.254.254.1	8080	
eth0	tcp	0.0.0.0		5050	169.254.254.1	8080	