TRITON® RiskVision™ Setup Guide

v7.8.1

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2013
Printed in the United States and Ireland

Trademarks

Contents

1 Introducing Websense TRITON RiskVision

Websense 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 Websense Advanced Classification Engine (ACE) analytics within Websense 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.
- ThreatScope Cloud Services provide sandboxing to find advanced malware threats in suspicious files. Administrators can:
  - Receive ThreatScope alerts when file analysis is complete.
  - Access online ThreatScope 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 Security 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 RiskVision manager.

In some circumstances, it may be desirable for administrators 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. 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 Websense Content Gateway, TRITON RiskVision also offers:

- Data analysis of information sent over web channels (Web DLP), configured in the Data Security 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 ThreatScope Analysis in the TRITON RiskVision manager.

  When files are sent for sandboxing, administrators receive a report on the outcome of the analysis. If threats are found, the 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 RiskVision manager or Data Security manager reports.

What traffic is analyzed?

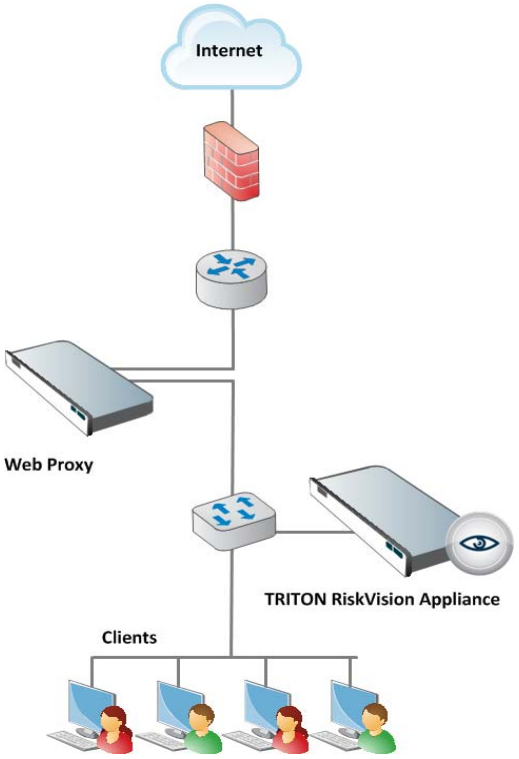
The ACE analytics within Websense Content Gateway are applied only to HTTP traffic, and decryption and inspection of SSL decryption is not available.

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

More information about Network Agent configuration is provided in the installation and configuration sections of this Setup Guide.

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:

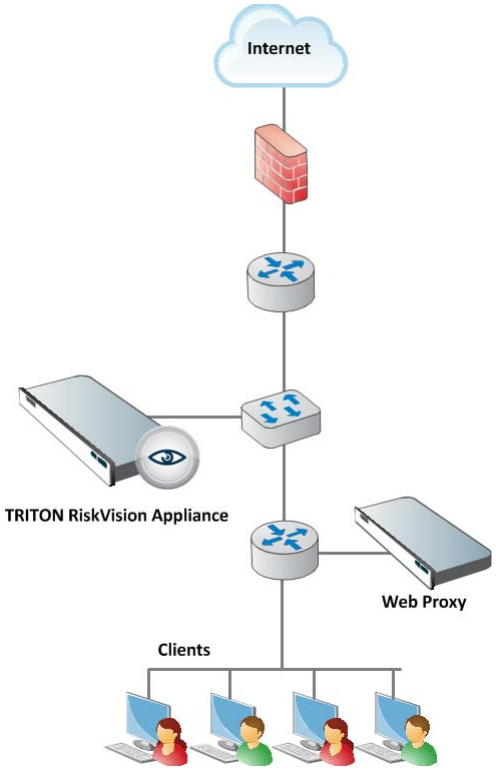
- URL categorization and outbound data protection performed by the upstream proxy does not affect TRITON RiskVision.
- If the upstream proxy blocks HTTP **responses** from origin servers, TRITON RiskVision does not see those responses. TRITON RiskVision does not have an opportunity to analyze blocked 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 46.
- 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 46.

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 TRITON RiskVision, 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 TRITON RiskVision. See *Configure TRITON RiskVision to work with a downstream proxy*, page 44.

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

Setup process overview

TRITON RiskVision Setup Guide | Websense TRITON RiskVision | v7.8.1

The installation and deployment process for TRITON RiskVision has 3 basic stages, broken into a series of steps. Use this guide to ensure that you complete the entire process.

1. *Set Up the Appliance*
   - *Step 1: Set up the appliance hardware*
   - *Step 2: Run the firstboot script*
   - *Step 3: Configure basic appliance settings*
   - *Step 4: Configure RiskVision component interaction*
   - *Step 5 (optional): Deploy additional appliances*
2. *Create a Management Server*
   - *Step 1: Download the installer and start installation*
   - *Step 2: Install TRITON Infrastructure*
   - *Step 3: Install the TRITON RiskVision manager*
   - *Step 4: Install Data Security 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*

2 Set Up the Appliance

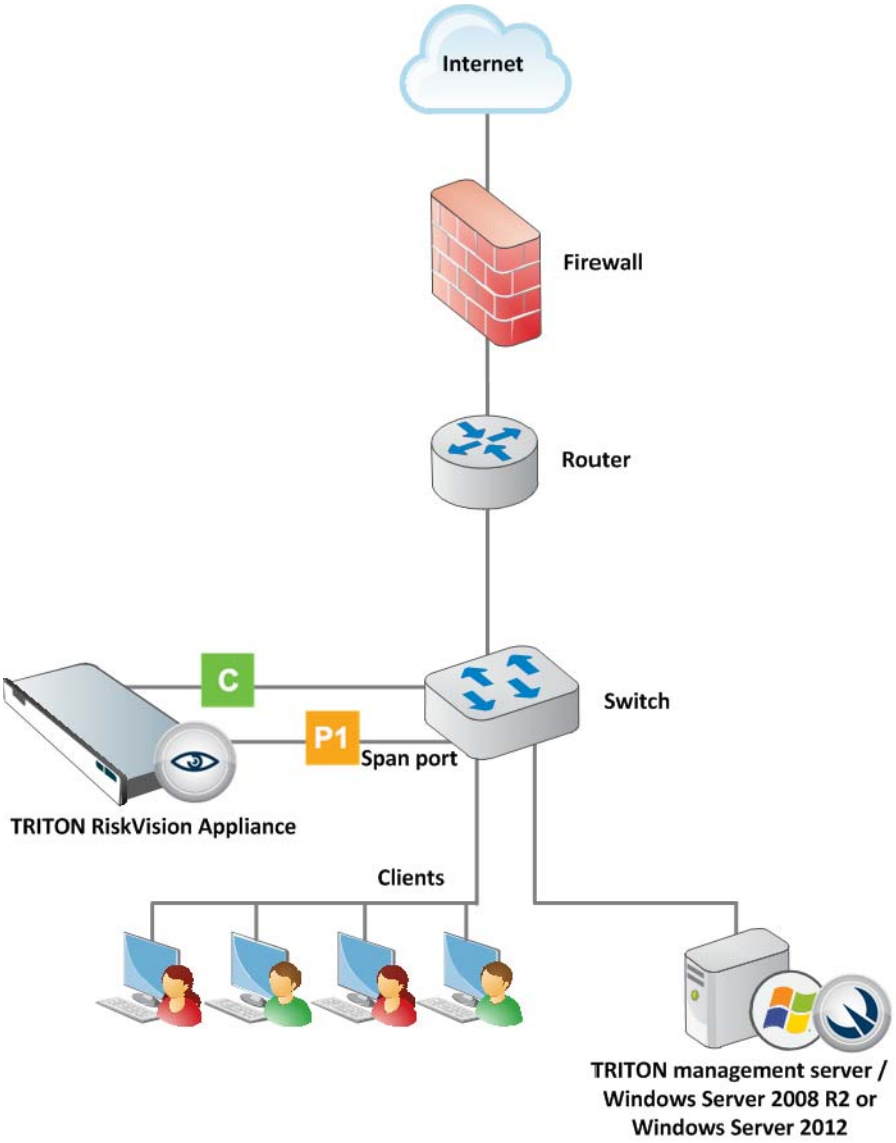
To deploy TRITON® RiskVision™, start by setting up the appliance hardware and performing basic appliance configuration, as outlined below.

- *Step 1: Set up the appliance hardware* (rack and cable the appliance).
- *Step 2: Run the firstboot script* (activates the appliance).
- *Step 3: Configure basic appliance settings* (set date and time, and add an appliance description).
- *Step 4: Configure RiskVision component interaction* (verify which components run on the appliance).
- *Step 5 (optional): Deploy additional appliances* (if needed).

Once your TRITON RiskVision appliances are racked, connected, and configured, continue to the next sections of this guide to *Create a Management Server* and *Configure TRITON RiskVision*.

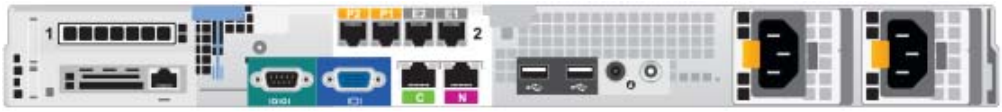
Step 1: Set up the appliance hardware

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.

V10000 G3 appliance:



V5000 G2R2 appliance:

Network **interface C** provides communication for appliance modules and handles database downloads. 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 P1** connects either to a span or mirror port on the switch or to a network tap that supports aggregation. This allows Websense 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.

V10000 G3 appliance:

V5000 G2R2 appliance:

An activation script, called **firstboot**, runs when you start 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 the **firstboot** script. After you approve the settings, initial appliance configuration occurs.

Later, if you want to change settings, you can do so through the Appliance manager, a graphical management interface accessed through a web browser.

Gather the following information before running the **firstboot** script.

Security mode	**Web**
Which subscription?	**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 for network interface C (IP address) *Optional*	
Tertiary DNS server for network interface C (IP address) *Optional*	
Password (8 to 15 characters, at least 1 letter and 1 number) This password is for the **admin** account used to access: • Appliance manager • Content Gateway manager	
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Websense to help improve the accuracy of traffic analysis and classification.

Run the initial command-line configuration script (**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** to launch the **firstboot** activation script.

   To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. Follow the on-screen instructions to provide the information collected in the table above.

After the script finishes running, continue with the next section.

Step 3: Configure basic appliance settings

TRITON RiskVision appliance settings are configured in the Appliance manager, a web-based interface. Use the Appliance manager to view system status, configure network and communication settings, and perform general appliance administration.

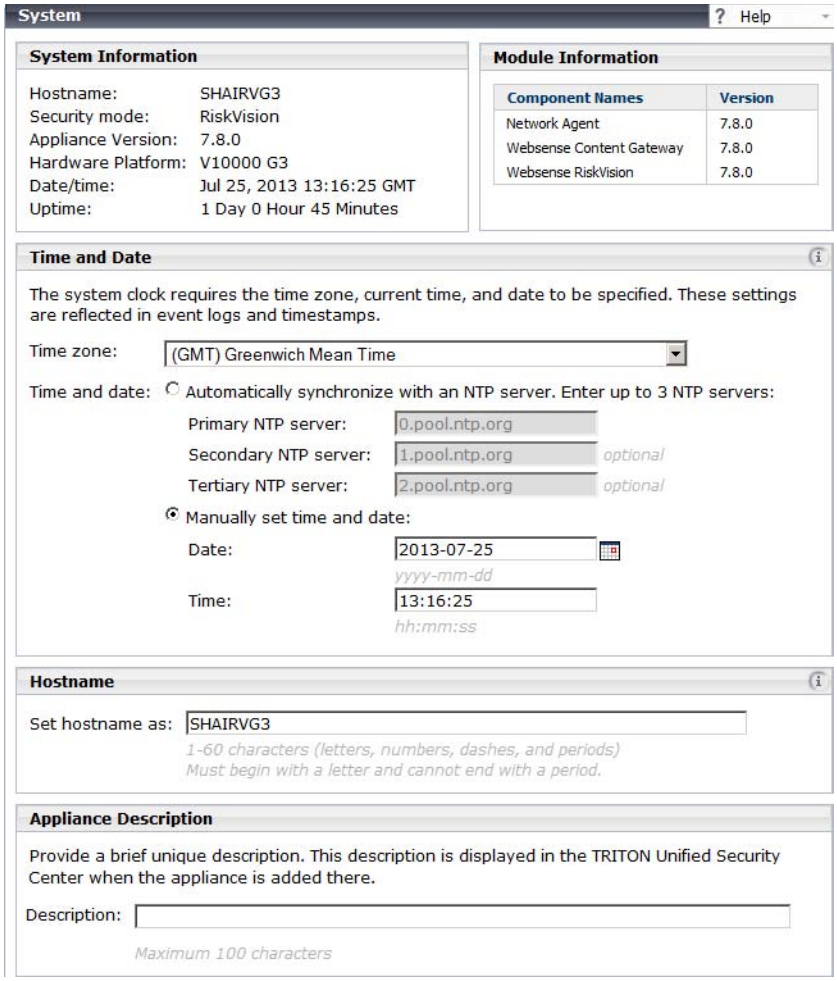
To configure the basic settings needed to get started with TRITON RiskVision:

1. Open a supported browser (Internet Explorer 8 or 9, Microsoft Internet Explorer 10 in Desktop mode, 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 initial appliance configuration.

3. Use the left navigation pane to navigate 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.

   GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.

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 RiskVision 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. Create or edit a unique appliance **Description** to help you identify and manage the system, particularly when there will be multiple appliances deployed.

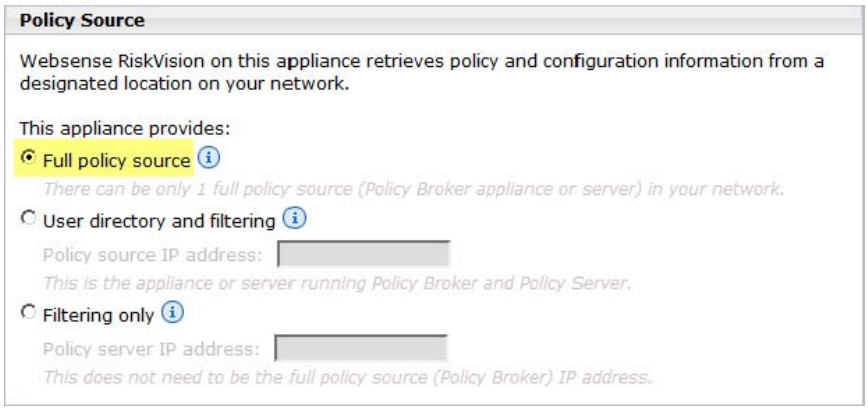
   The description is displayed in the appliance list in the TRITON Unified Security Center when the appliance is added there.

7. Click **OK** to save your changes.

Step 4: Configure 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 that you are installing, select **Full policy source**.

     The first TRITON RiskVision appliance that 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.

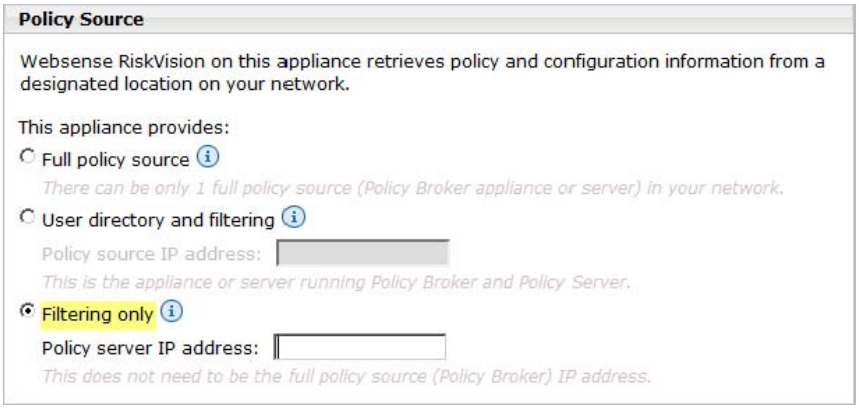
     When you configure a user directory and filtering appliances, you are prompted for the location of the policy source.
3. Click **OK** to save and apply your changes.

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 8.

When you reach *Step 4: Configure 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.



Note

Content Gateway for TRITON RiskVision cannot be configured into a cluster (a synchronized set of Content Gateway proxies). Therefore, 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: *Create a Management Server*, page 17.

3 Create a Management Server

After performing initial appliance configuration, install management and reporting components on a Windows Server 2008 R2 or Windows Server 2012 machine, as described in the sections that follow.

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 RiskVision 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 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.

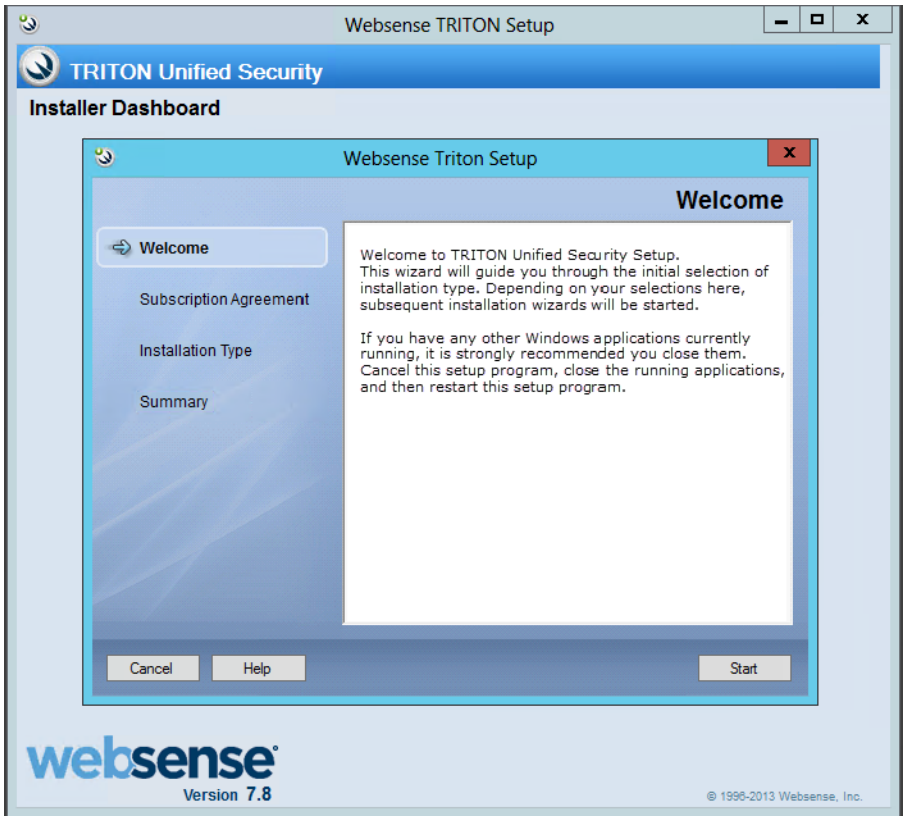
  You can install the required version or versions of .NET Framework via the Server Manager, or download it from www.microsoft.com.
- Disable any antivirus software on the machine prior to installing TRITON RiskVision components. Be sure to re-enable antivirus software after installation.
- Synchronize the clocks on all TRITON RiskVision appliances and machines where TRITON RiskVision components are installed. It is a good practice to point the machines to the same Network Time Protocol server.

Once the management server has been created, continue to the final section of this guide to *Configure TRITON RiskVision*.

Step 1: Download the installer and start installation

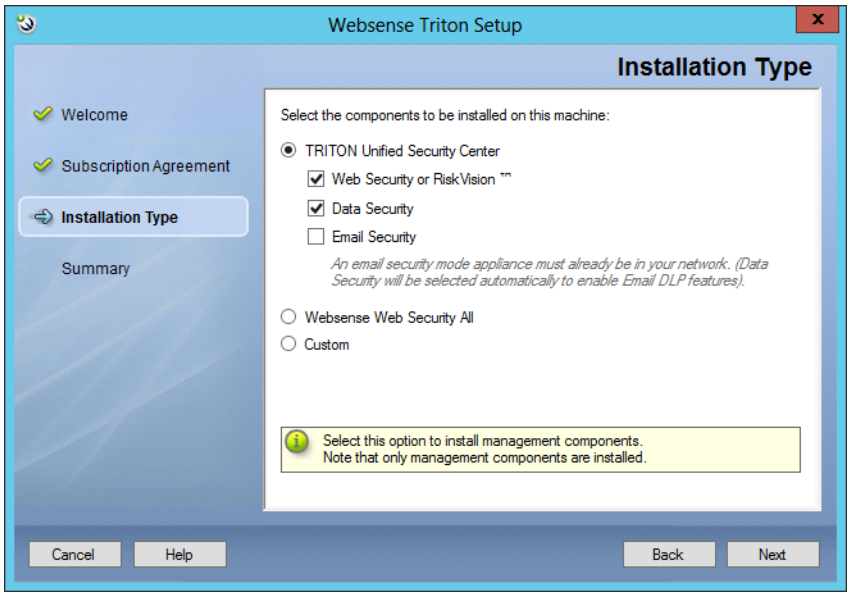
1. Download the **TRITON RiskVision Installer** from the **Downloads** tab of mywebsense.com.
   - The file name is **WebsenseTRITON781Setup.exe**.
   - The version is **7.8.1**.
   - When extracted, the installation files occupy about 2 GB of disk space.
2. Double-click the installer executable to launch the **Websense TRITON Setup** program.

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



4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.

5. On the **Installation Type** screen, select **TRITON Unified Security Center**, then mark the **Web Security or RiskVision** and **Data Security** check boxes, as shown below.



When you are finished, click **Next**.

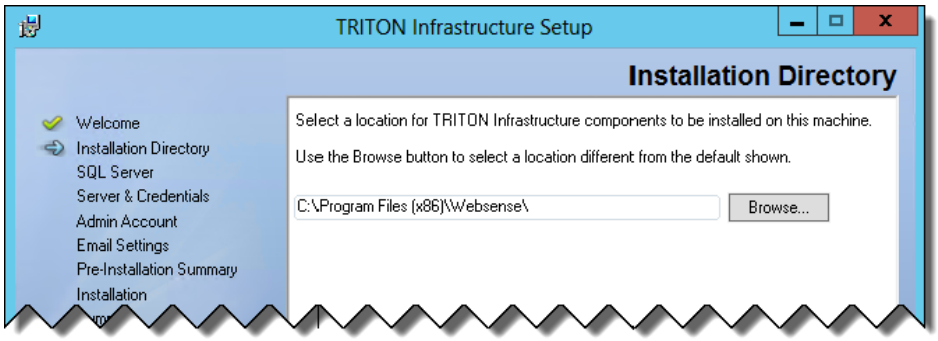
6. On the **Summary** screen, click **Next** to continue the installation.

The TRITON Infrastructure Setup program launches. Continue with the next section.

Step 2: Install TRITON Infrastructure

TRITON Infrastructure is the platform on which Websense TRITON management components are built. When the infrastructure components have been installed, the TRITON RiskVision installer launches automatically to install the TRITON RiskVision management components.

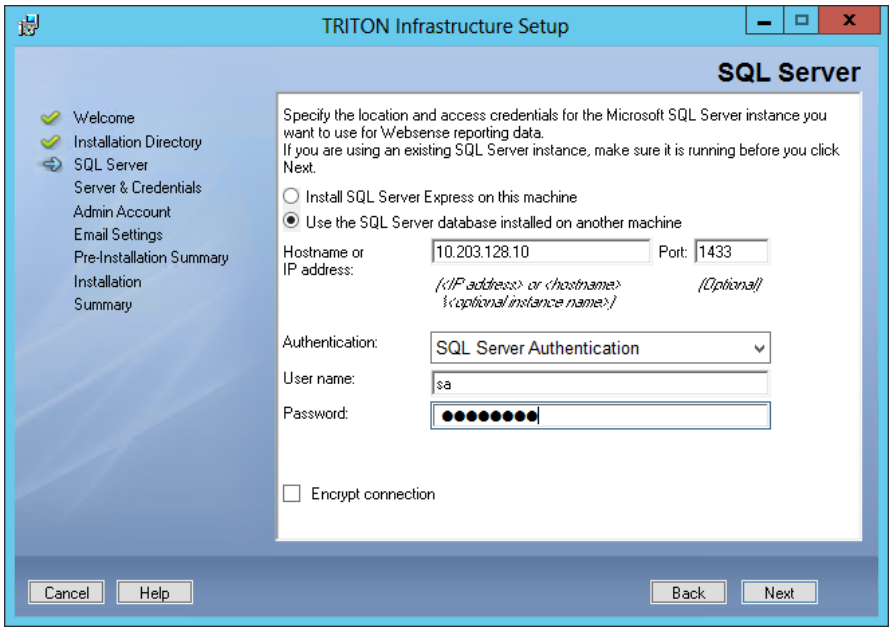
1. On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
2. On the **Installation Directory** screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.



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**.

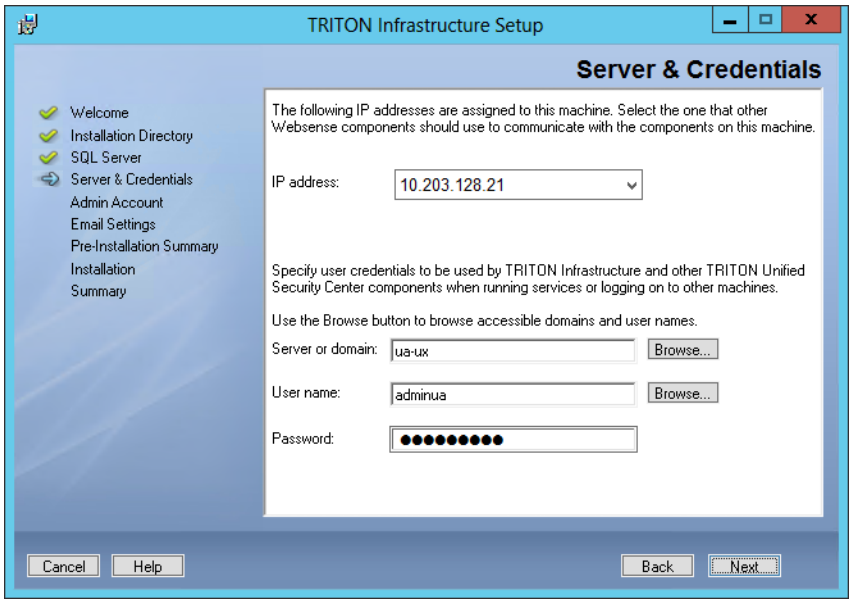
   When you are finished, click **Next** to verify the connection to the database.

   - 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.

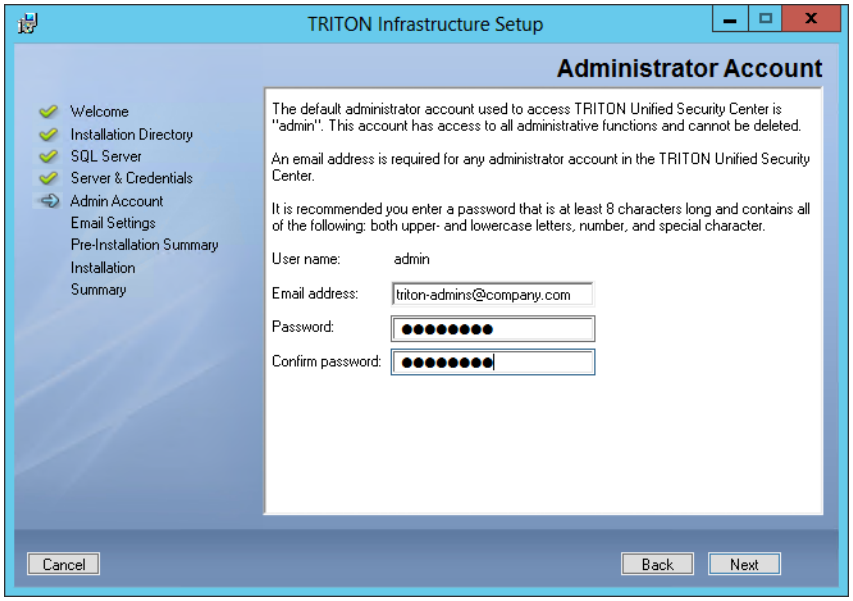
5. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Unified Security Center.



   - 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 Unified Security Center services. The server/host name cannot exceed 15 characters.
- Specify the **User name** of the account that you want to use to run the TRITON Unified Security Center services.
- Enter the **Password** for the specified account.

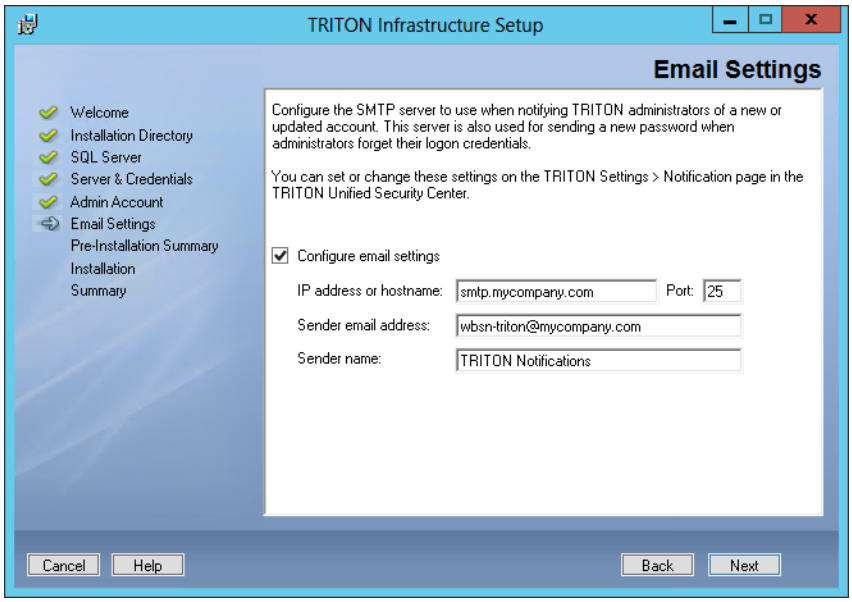
6. On the **Administrator Account** screen, enter an email address and password for the default TRITON console administration account: **admin**. When you are finished, click **Next**.



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

Define a strong password as described on the screen.

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 after installation in the TRITON console.



   - **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 console.

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 'Websense 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 Security component installer launches. Continue with the next section.

Step 3: Install the TRITON RiskVision 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 - Web Security (the primary component supporting the TRITON RiskVision 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).

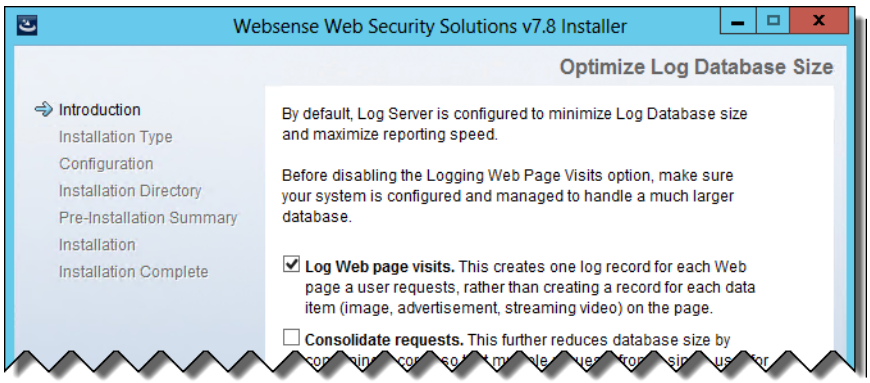
   When you are finished, click **Next**.

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.

   When you are finished, click **Next**.

5. On the **Optimize Log Database Size** screen, select **Log Web page visits**.



This results in fewer log records for each URL by combining information for secondary elements on a website (like graphics) into a single record. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities.

When you are finished, 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**).

   When you are finished, click **Next**.

7. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

8. Click **Next** to start the installation. The **Installing Websense** progress screen is displayed. Wait for installation to complete.
9. On the **Installation Complete** screen, click **Next**.

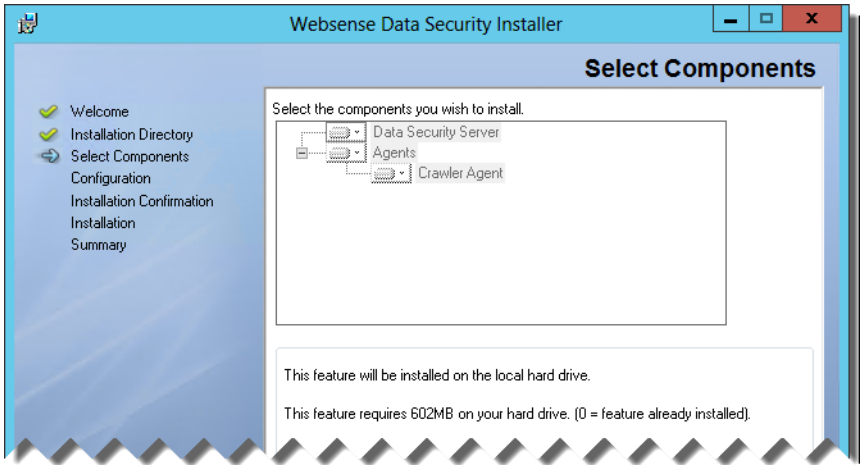
Continue with the next section to install Data Security management components.

Step 4: Install Data Security components

All TRITON RiskVision subscriptions include Web DLP, used for data loss monitoring over web channels. Data loss monitoring is performed by Data Security components installed on the management server, and configured in the Data Security module of the TRITON console.

To install the Data Security management components:

1. When the Data Security component installer launches, and the Welcome screen is displayed, 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 Data Security components.
8. If the following message appears, click **Yes** to continue the installation:

   ```
   Data Security 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 Data Security installer.

You have completed installation of the TRITON management server. Continue with the next section to enter a subscription key and activate Websense TRITON RiskVision.

Step 5 (optional): Install a transparent identification agent

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

- Websense 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.
- Websense Logon Agent identifies users as they log on to Windows domains. Its associated logon application runs on Windows or Mac clients.

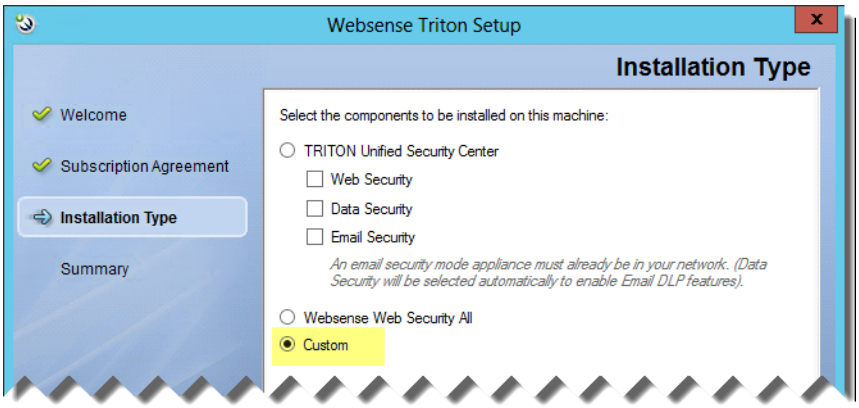
  Note that with Logon Agent, you must both install the agent and deploy the logon application to client machines.
- Websense RADIUS Agent can be used in conjunction with either Windows- or LDAP-based directory services. The agent works with a RADIUS server and client to identify users logging on from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

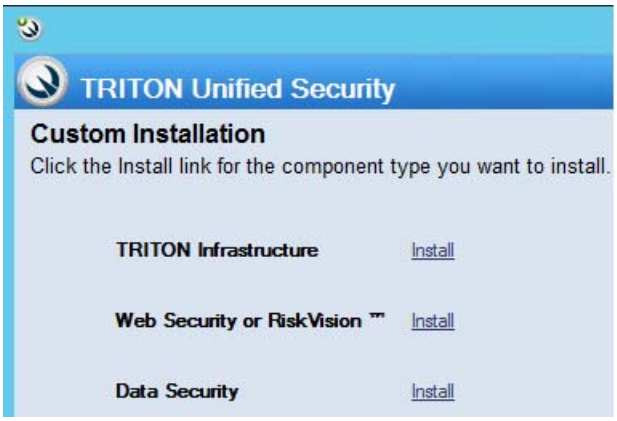
1. Launch the TRITON Unified Installer on the machine that will host the transparent identification agent:
   - To add the component to the management server, launch the TRITON Unified Installer executable again. On the Modify Installation dashboard, click the **Modify** link for **Web Security or RiskVision**.

- 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:

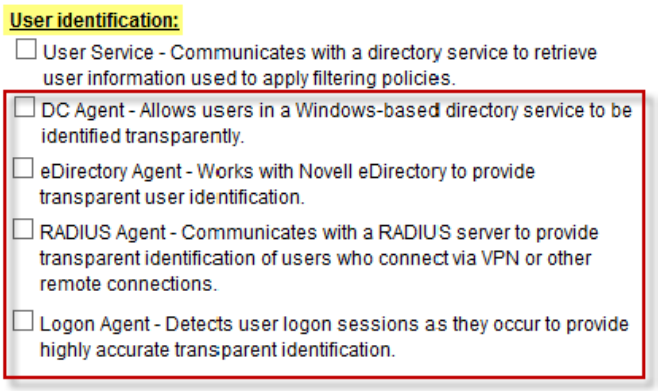
  a. Select the **Custom** radio button at the bottom of the page, instead of the TRITON Unified Security Center radio button.



  b. On the Custom Installation screen, select the **Install** link next to **Web Security or RiskVision**.



2. On the Select Components screen, scroll down to the User Identification section, then mark the check box next to the transparent identification agent that you want to install, then 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 console and enter your TRITON RiskVision subscription key. Do not make any configuration changes to the Content Gateway component until after the TRITON RiskVision subscription key has been entered.

1. Open a preferred browser (Mozilla Firefox 5 and later or Google Chrome 13 and later), and enter the following URL in the address bar:

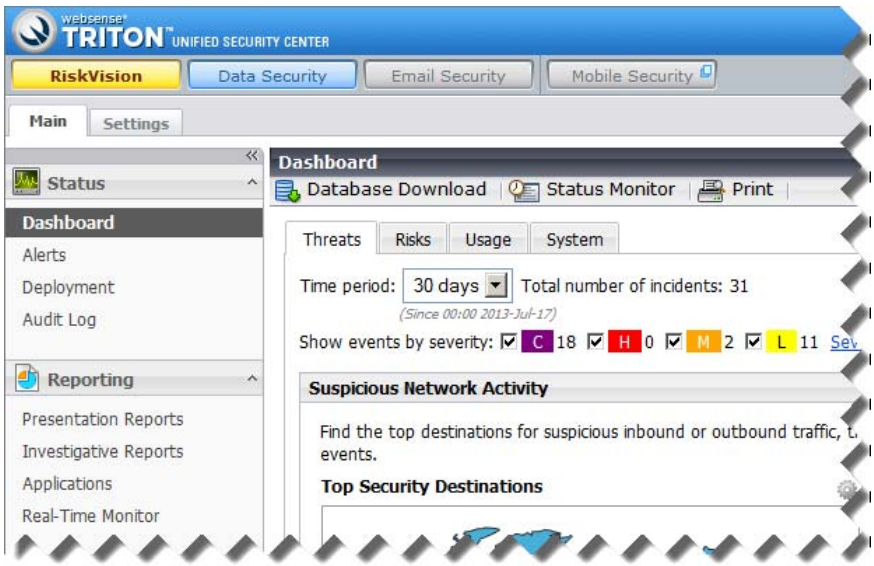
   ```
   https://<IP-address-of-management server>:9443/triton/
   ```

   Internet Explorer 8, 9, and 10 (not Compatibility View) are also supported.
2. Enter the user name **admin** and the password set during installation, then click **Log On**.

   You are logged on to the TRITON console and automatically connected to the Web Security management module.
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 the TRITON console and continue with the next section of this document.

   The next time you log on to the TRITON console, you are connected to the TRITON RiskVision manager, instead of the Web Security manager.



4 Configure TRITON RiskVision

After setting up the TRITON® RiskVision™ appliance and creating a TRITON management server, you are ready to use TRITON RiskVision to begin monitoring traffic. This involves the following procedures:

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 decide 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.

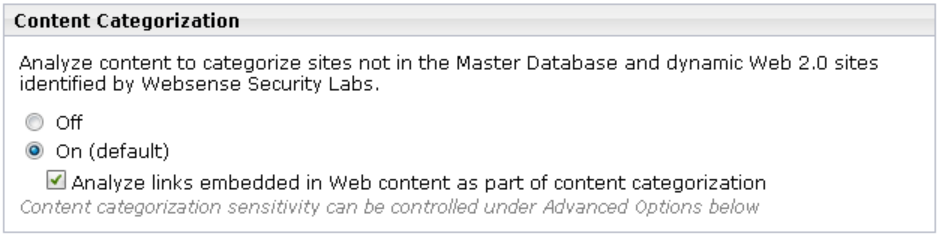
- If any policies that you configure (including the Default policy) use only the Monitor Only filters, all traffic goes to Content Gateway, and reports do not show any blocked requests.
- If your policies include filters that block categories (explained in the next section), any requests flagged as blocked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

assigned to Master Database categories blocked by the filter) are not forwarded to the proxy.

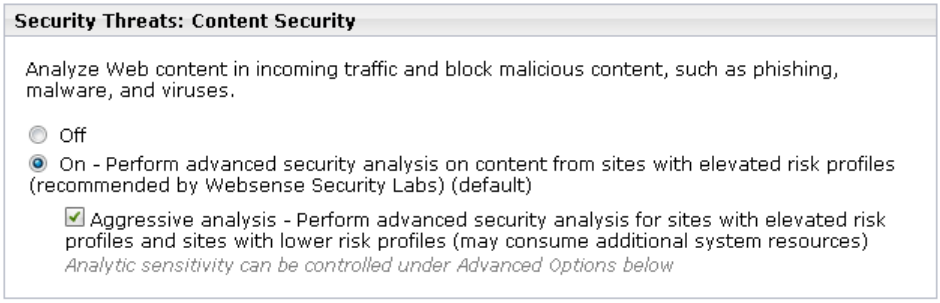
In other words, even though no actual block occurs, the request is treated **as if it had been blocked** based on Master Database categorization, and no further analysis is performed.

To configure how Content Gateway analyzes traffic:

1. Log on to the TRITON console as **admin**, using the password created during installation. You are connected to the TRITON RiskVision manager 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.

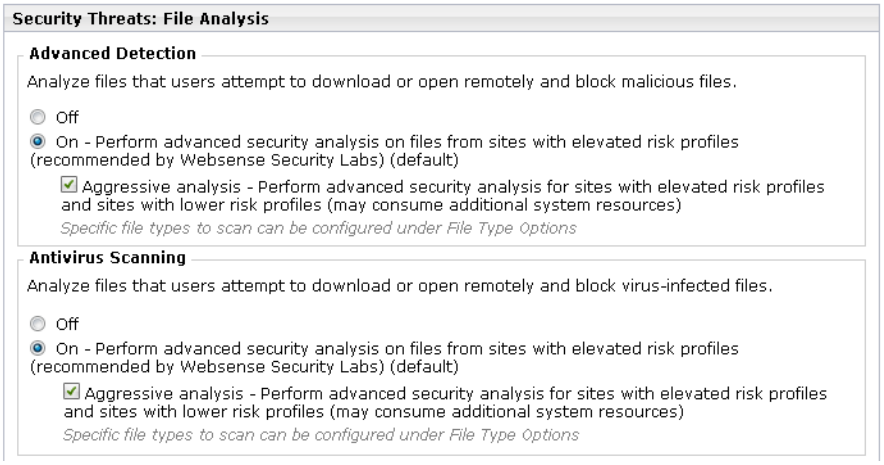


4. Under Tunneled Protocol Detection, make sure that the **On** radio button is selected.
5. Under Security Threats: Content Security, make sure that the **On** radio button is selected, and the **Aggressive analysis...** check box is marked.

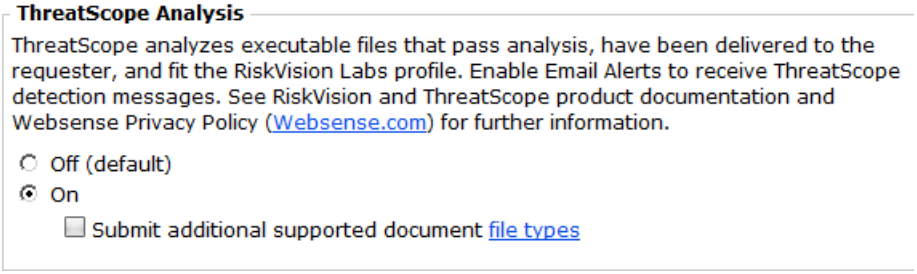


6. Under Security Threats: File Analysis:
   - Under Advanced Detection, make sure that the **On** radio button is checked, and the **Aggressive analysis...** check box is marked.

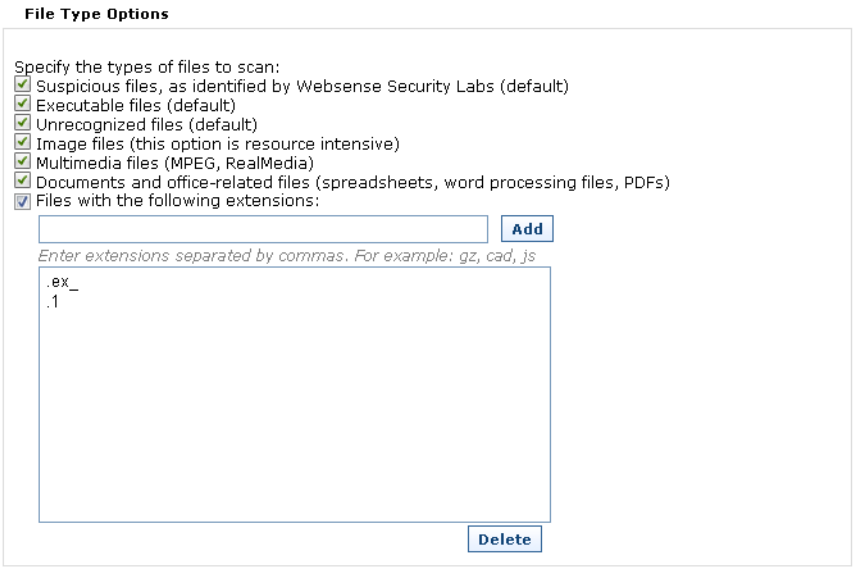
- Under Antivirus Scanning, make sure that the **On** radio button is checked, and the **Aggressive analysis...** check box is marked.



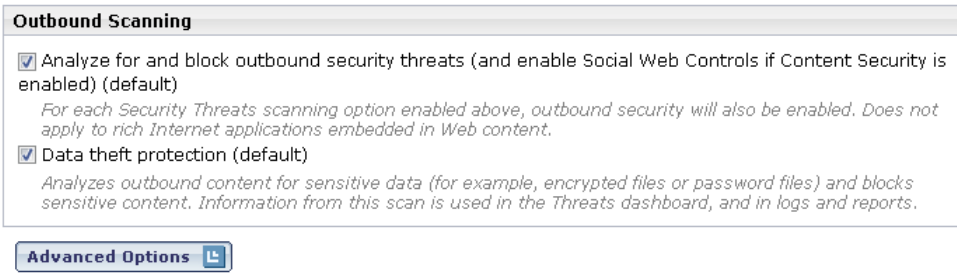
- Under ThreatScope Analysis, select the **On** radio button to have suspicious executable files sent to ThreatScope Cloud Services for sandboxing and extended analysis.



- Expand the **File Type Options** button, then mark all of the file type check boxes.



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. 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. See *Use the default policy setup*, page 48, for more information.

If your organization requires custom policies, they are configured in the TRITON RiskVision manager on the **Policy Management** > **Policies** page. See the TRITON RiskVision Help (accessed from the Help menu in the TRITON RiskVision 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 Data Security 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 TRITON console and 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 **Data Security**, then make sure that the **Integrated on-box** radio button is selected (the default).
4. Click **Apply**.

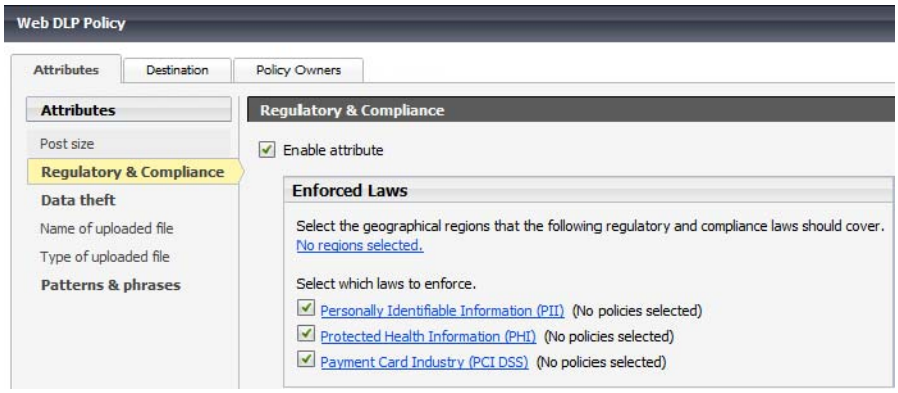
Continue with *Step 4: Configure Web DLP policies* to complete the registration process and start monitoring data loss activity.

Step 4: Configure Web DLP policies

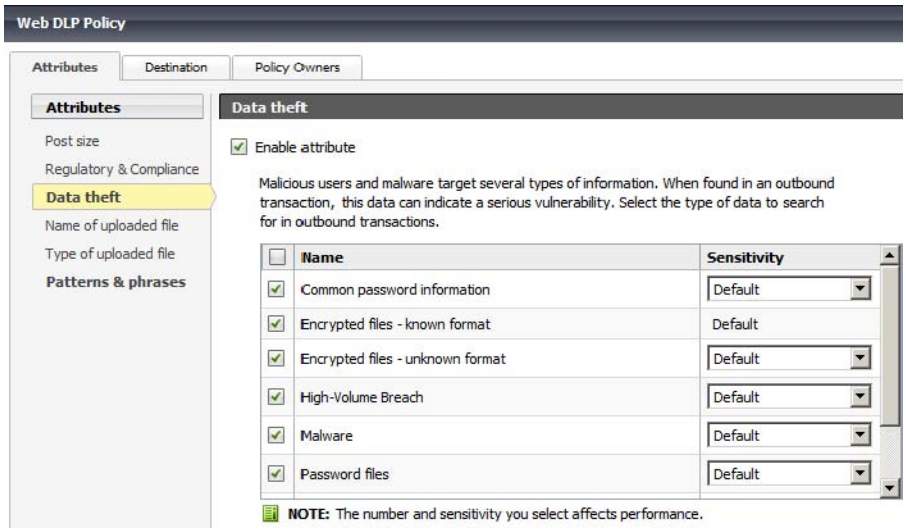
In addition to standard TRITON RiskVision policies, you can also configure Web DLP policies to detect data leaving your organization through web channels (for example, in files uploaded to the Internet).

Use the Data Security manager to configure Web DLP policies:

1. Select the **Data Security** module of the TRITON console.
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



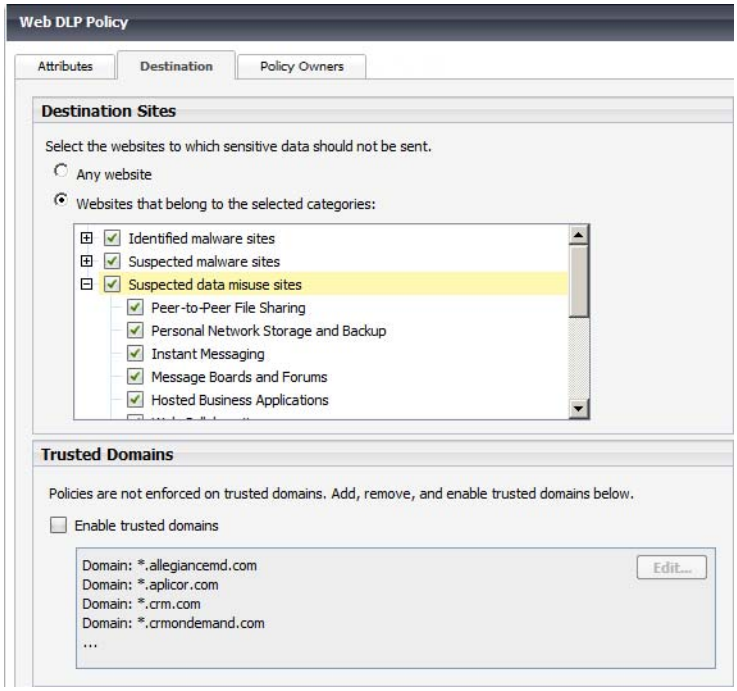
   - Data theft attributes, like password information and encrypted files



   - 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 Data Security 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 the Data Security Help (accessed from the Help menu in the Data Security manager) for more information about Web DLP policies.

Step 5: Configure reporting behavior

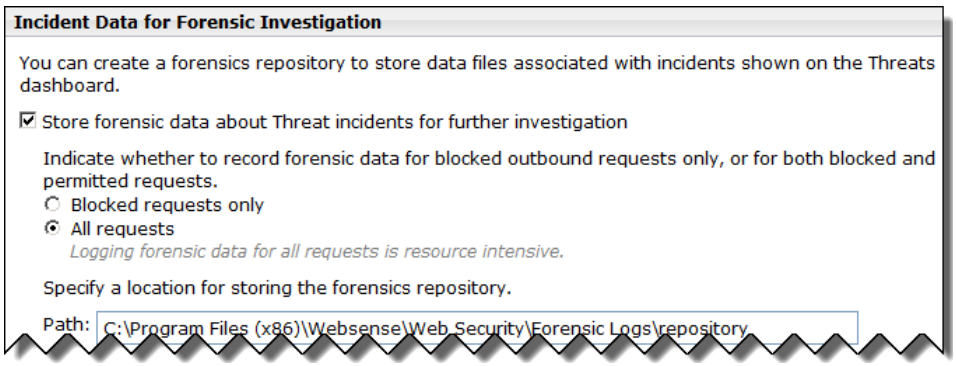
Forensic data capture

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 console and select the **RiskVision** 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.

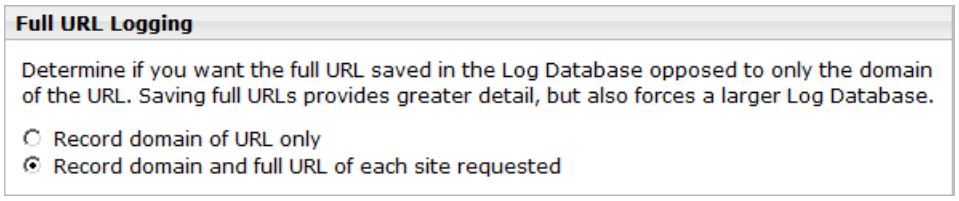
Logging full URLs

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 console and select the **RiskVision** 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 RiskVision manager, you must configure Websense 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 RiskVision manager.

Find full instructions for each supported directory in the TRITON RiskVision Help, accessed through the Help menu in the TRITON RiskVision 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 Security 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 the Data Security 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 RiskVision 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 44
- *Configure TRITON RiskVision to work with an upstream proxy*, page 46

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 48

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 TRITON RiskVision 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 RiskVision Help, accessed from the Help menu in the TRITON toolbar.
- In the Data Security 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 Data Security 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 delve into your data. See the TRITON RiskVision Reporting Guide for instructions.

5 Working with upstream and downstream proxies

Important

Install the TRITON® RiskVision™ manager, enter a subscription key, and restart the RiskVision appliance **before** performing any Content Gateway configuration.

- 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 48.
- 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.

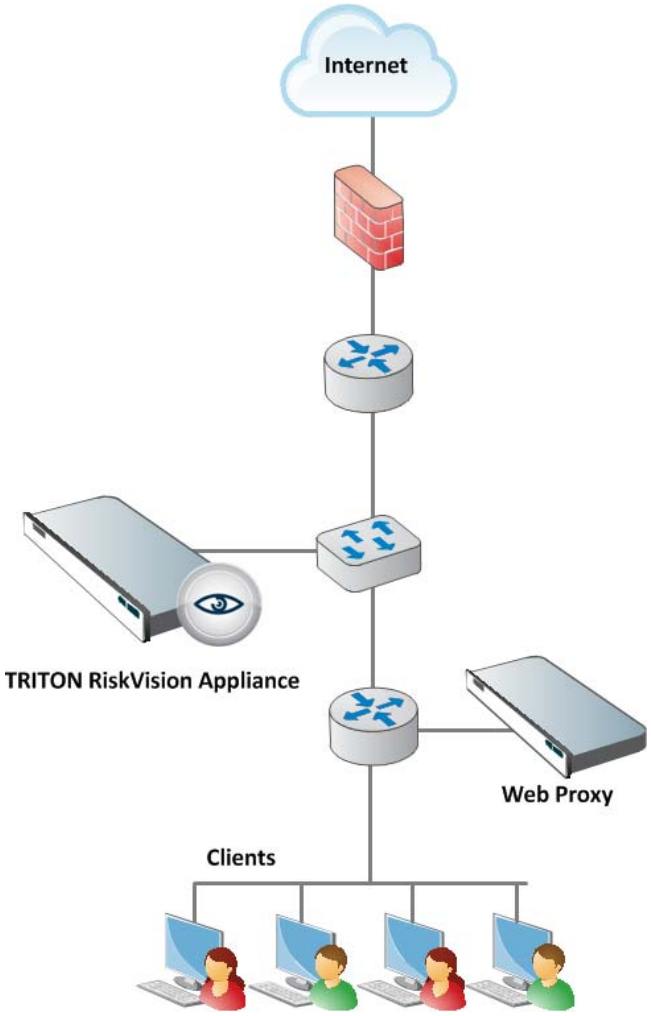
    (For more about the effects of upstream and downstream position in the network, see *What is the effect of positioning TRITON RiskVision downstream or upstream of an active web proxy?*, page 3.)
  - Uses explicit or transparent (interception redirect) methods to direct client traffic to the web proxy

  See:

  - *Configure TRITON RiskVision to work with a downstream proxy*, page 44
  - *Configure TRITON RiskVision to work with an upstream proxy*, page 46

Configure TRITON RiskVision to work with a downstream proxy

If your network includes a web proxy, the TRITION 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

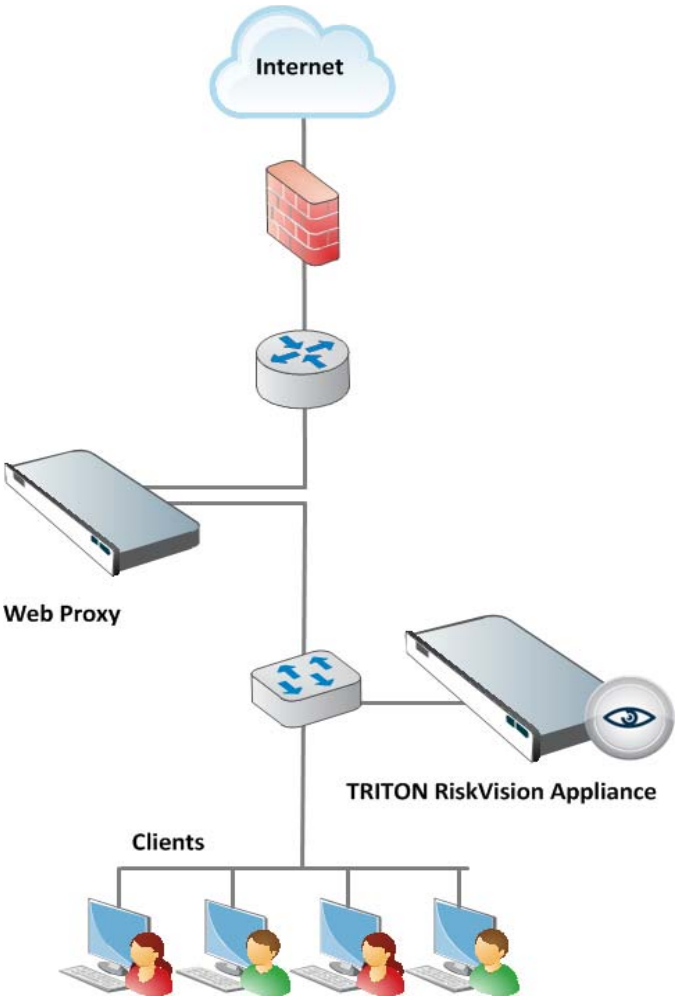
If the downstream proxy performs user authentication and has the ability to insert **X-Authenticated-User** headers (the *de facto* field for passing the authenticated user name), TRITON RiskVision can be configured to read the value and include it in transaction handling.

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 TRITION 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 Websense 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 RiskVision 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	