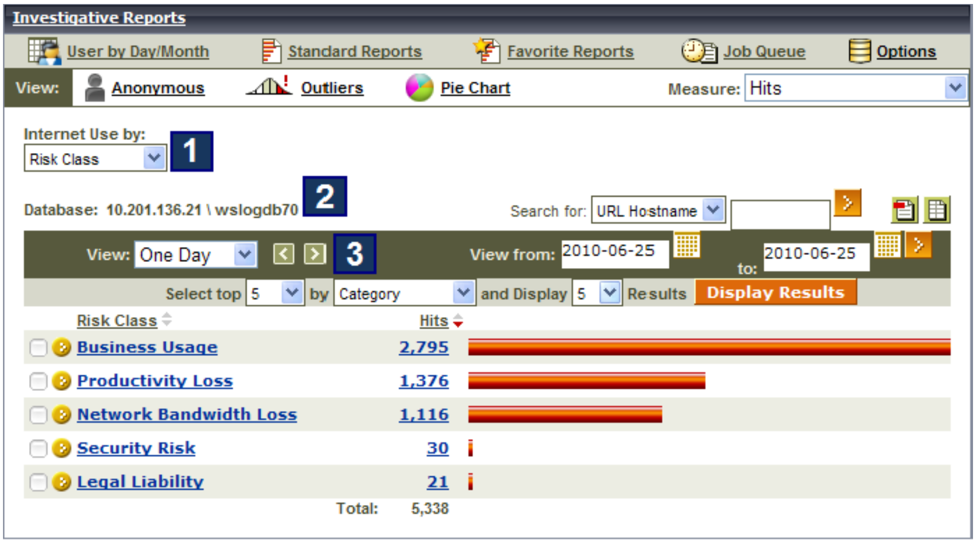
Investigative Reporting Quick Start

Investigative Reporting Quick Start | TRITON RiskVision | v7.8.x

Use investigative reports to review Internet monitoring and analysis activity in an interactive way.

When you first open the **Reporting > Investigative Reports** page in the TRITON RiskVision manager, a high-level summary report is displayed.



By default, this initial view shows activity:

1. Grouped by risk class

   Risk classes are groupings of categories used to suggest possible types or levels of vulnerability posed by sites in those categories.

2. That has occurred since midnight today

Tip

You can click **Options** at the top of the page to change the default time period.

3. Recorded in the specified Log Database

Only activity that you are authorized to see is displayed.

- For many delegated administrators, this is information about your managed clients.
- For some administrators, this is information for your entire organization.

Use this overview as a quick check for areas of potential concern. Are there a high number of Security Risk requests? Does the overall amount of activity seem appropriate?

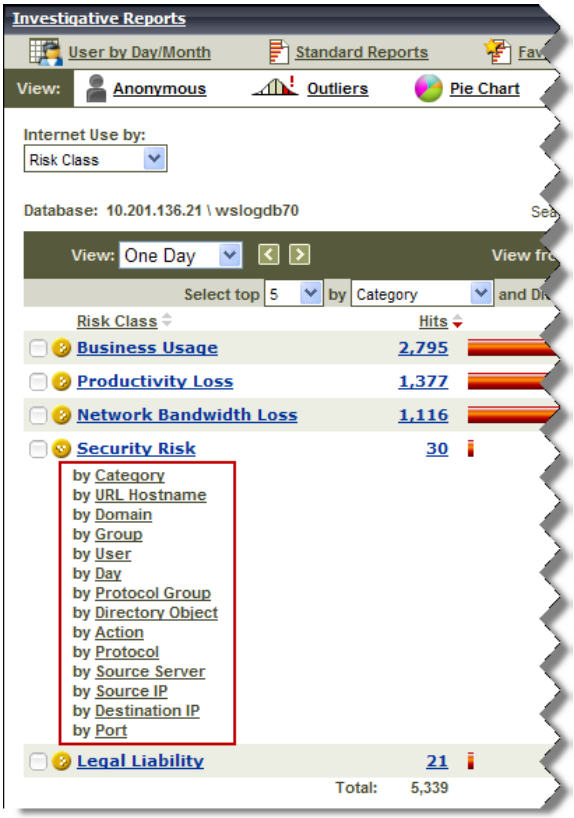
From here, you have several options:

- If the high-level summary shows areas of potential concern, *Drill down to find details*, page 3.
- *Use standard reports*, page 6, to get a targeted view of Internet monitoring and analysis activity.
- *Customize summary reports*, page 8, or *Customize detail reports*, page 10, to create a report that better reflects your needs.
- For quick reference explaining the types of data that can be included in an investigative reports, see *What information can I see in a report?*, page 13.
- *Create Favorite reports*, page 15, to minimize the work required to get to the data you need, and optionally schedule reports to run at regular intervals.

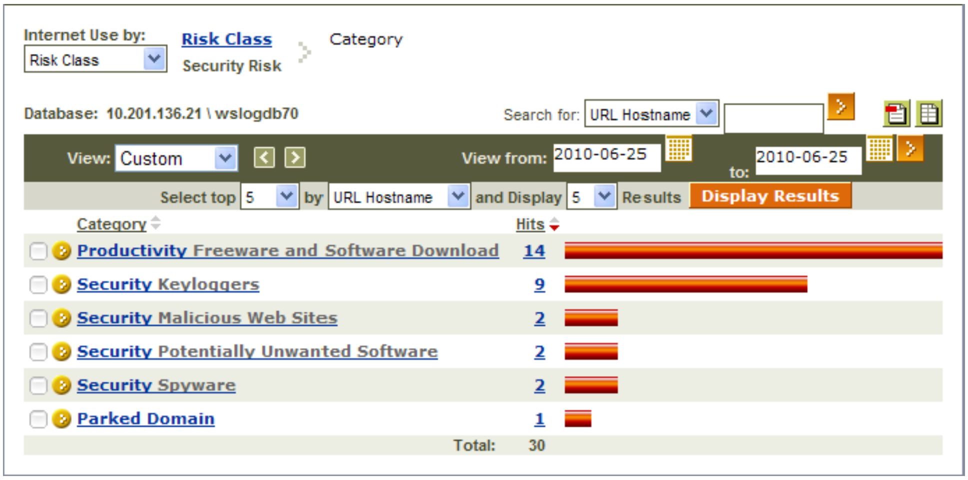
Drill down to find details

If a summary report shows information that you want to investigate further, you have several options for drilling down into the data.

Using the initial Internet use by risk class summary report as a starting point, you can, for example, click a risk class name see a list of additional details to view. For more information about the available details, see *What information can I see in a report?*, page 13.

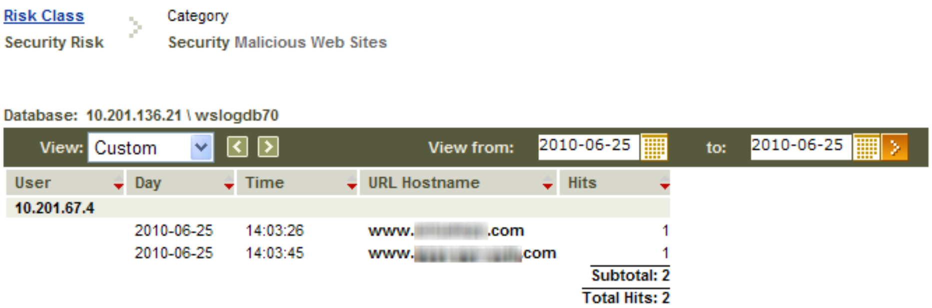


Click the **Category** link to see which categories in the Security Risk class were accessed.



From here, you can click a category name to again see a list of additional details, or click the number or bar next to a category name to see a detail report showing the requested sites in the category.

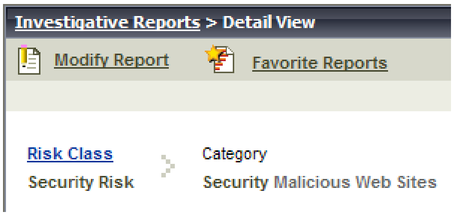
Clicking the bar next to **Security Malicious Web Sites** opens a detail page, showing which sites were requested.



Tip

You can click **Options** at the top of the main Investigative Reports page to change the default columns for a detail page.

From this point, it is possible to modify the report to show additional details, such as whether the site was flagged as blocked or permitted, or to go back to the previous summary view (in this example, a summary of requested categories in the selected risk class).



- To change the details shown in the report, click **Modify Report**.

  For more information about options for customizing a report, see *Customize summary reports*, page 8, or *Customize detail reports*, page 10.

- To return to the previous summary page, click the **Risk Class** link near the top of the page.

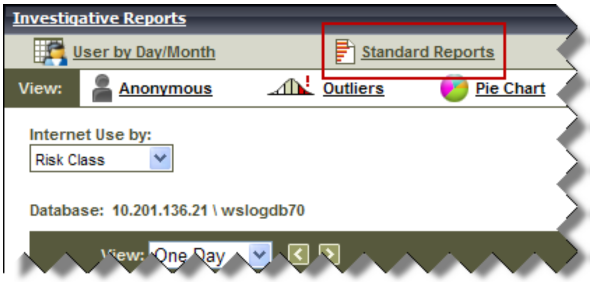
  On the summary page, you can click the **Risk Class** link next to the Internet Use by drop-down list to return to the initial, high-level summary of Internet use by risk class.

Although the details shown differ based on your selections, the principles of creating a report via drill-down are the same. Each selection you make results in more targeted information, and if your selection doesn't show the information you wanted, you can return to the previous view via a link near the top of the page.

Use standard reports

Investigative Reporting Quick Start | TRITON RiskVision | v7.8.x

Investigative reports includes a set of 18 **standard reports** to help you get to specific sets of information quickly, without having to drill down. Access the list of standard reports from a link at the top of the Investigative Reports page.



The list of available reports appears. The reports are grouped into 6 general areas, dealing with activity levels, bandwidth use, user time spent online, blocked sites and categories, security risks, and legal liability. Each report description is a link.

Click a link to see the corresponding report (for example, **Top categories posing a security risk**). The report displays in the main investigative reports window.

Once the report displays, you can change the time period displayed, drill down into the results, and otherwise customize the report until it shows the information that is most useful to you. See:

- *Drill down to find details*, page 3
- *Customize summary reports*, page 8
- *Customize detail reports*, page 10
- *What information can I see in a report?*, page 13

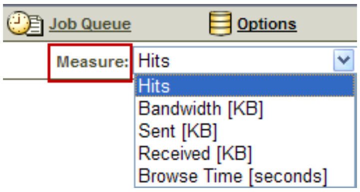
If you get to a set of data that is particularly valuable, you can save that view as a **Favorite Report**. Favorite reports make it easy to run the same report again, or to schedule the report to run on at regular intervals. See *Create Favorite reports*, page 15.

Customize summary reports

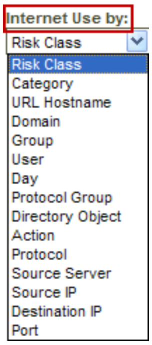
Investigative Reporting Quick Start | TRITON RiskVision | v7.8.x

In addition to drilling down into data to find details of interest, you can customize the information that appears in investigative reports in a number of ways. In a summary report, you can, for example:

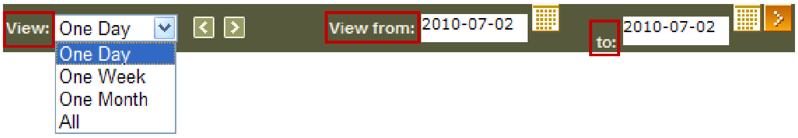
- Change the measuring unit from the default **hits** (or **visits**, depending on which your environment is configured to record) to bandwidth (in kilobytes), KB sent, KB received, or seconds of browse time.



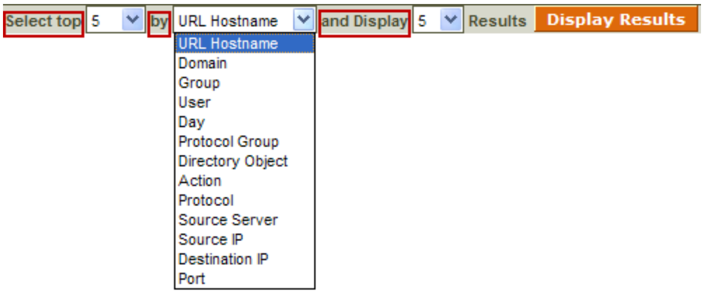
- Change the data grouping from the default **risk class** to category, URL hostname, domain, group, user, day, protocol group, directory object, action, protocol, source server IP address, source IP address, destination IP address, or port. For more information about these options, see *What information can I see in a report?*, page 13.



- Change the time period from the default **one day** to a standard period (week, month, or all) or specific date range.



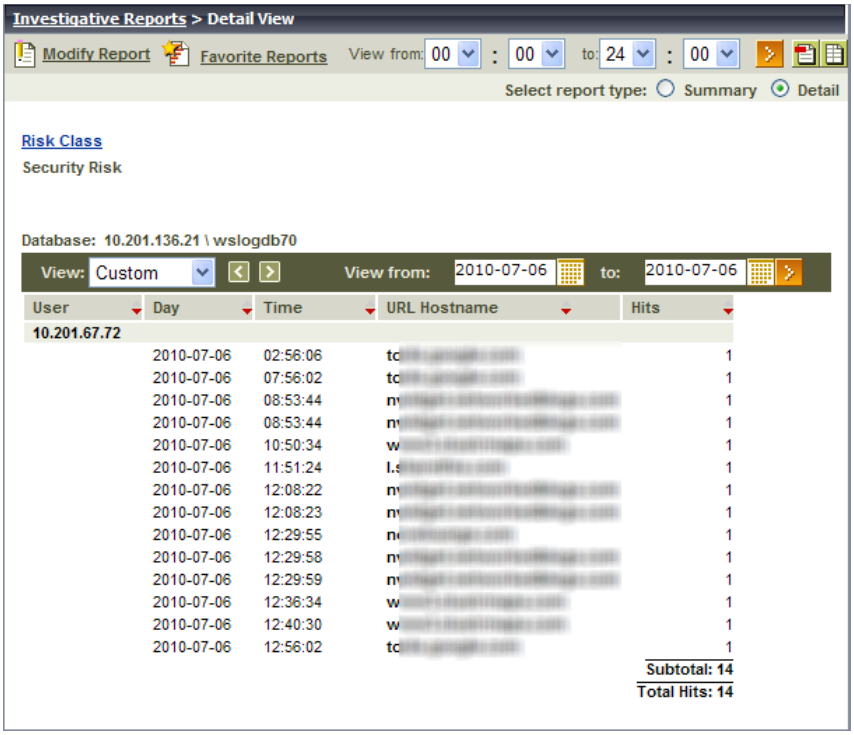
- Combine a high-level summary with an overview of details by creating a top N report. While looking at the default summary of requests by risk class, you might add additional detail by also displaying the top 5 sites (URL hostnames) requested in all 5 risk classes. For more information about the options in the “by” list, see *What information can I see in a report?*, page 13.



Customize detail reports

When you drill deeper into summary information, the results display on a Detail View page, and are called detail reports. Detail reports use a multi-column table format that does not include drill-down options. You can, however, modify both the columns of data that appear in the detail report, and the time range covered by the report.

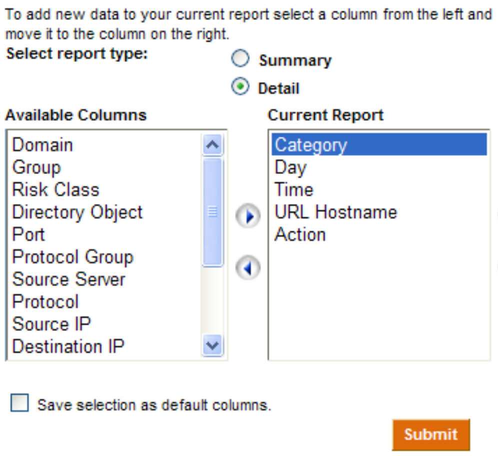
For example, in the default summary report (Internet Use by Risk Class), click the number next to a risk class (for example, Security Risk) to open a Detail View page showing sites requested in the risk class.



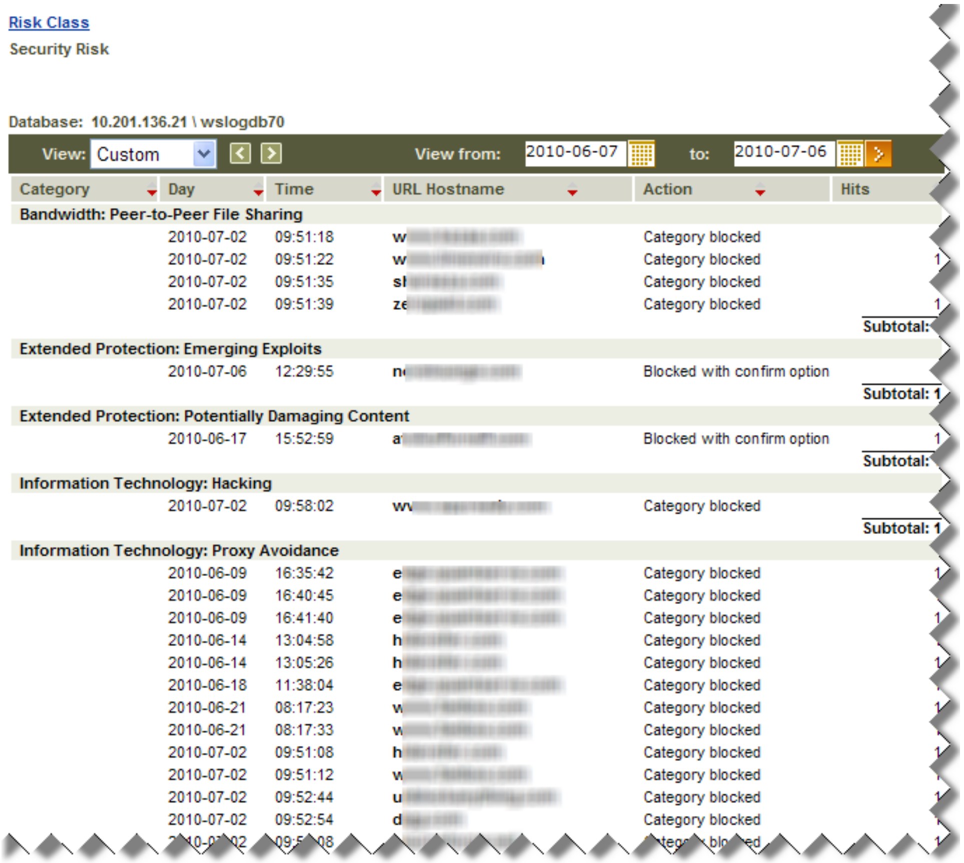
From here, you can:

- Change the time period (top toolbar) or date range (bottom toolbar) included in the report.

- Click **Modify Report** to change the columns included in the report. For more information about the available columns, see *What information can I see in a report?*, page 13.



For example, when the detail report above is modified to include the columns shown, and expanded to a longer period, the first results look like this:



Once you have created a report that includes all of the data that you want to see, you can save the report as a Favorite so that you can easily run the report again later. See *Create Favorite reports*, page 15.

What information can I see in a report?

Investigative Reporting Quick Start | TRITON RiskVision | v7.8.x

When you customize an investigative report (see *Customize summary reports*, page 8, or *Customize detail reports*, page 10), the information that you can select for display depends on what elements are already selected. If you are looking at requests by user, for example, you cannot add group information. Likewise, if you are looking at a report by category, you cannot simultaneously view risk class data.

In addition, the reporting permissions granted to your account can determine what information is available. User-identifying information may not be available to all reporting administrators.

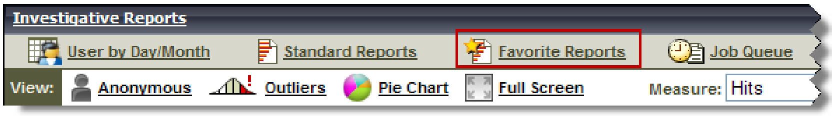
The table below lists all types of data that can be displayed in an investigative report. If you have drilled down into the data to create a detail report, these are the columns that you can add to the report to create a custom view of the data.

Column Name	Description
User	Name of the user who made the request. User information must be available in the Log Database to include it on reports. Group information is not available in user-based reports.
Day	Date the Internet request was made.
URL Hostname	Domain (host) name of the requested site.
Domain	Directory service domain for the directory-based client (user or group, domain, or organizational unit) that made the request.
Group	Name of the group to which the requestor belongs. Individual user names are not given on group-based reports. If the user who requested the site belongs to more than one group in the directory service, the report lists multiple groups in this column.
Risk Class	Risk class associated with the category to which the requested site belongs. If the category is in multiple risk classes, all relevant risk classes are listed.
Directory Object	Directory path for the user who made the request, excluding the user name. Typically, this results in multiple rows for the same traffic, because each user belongs in multiple paths. If you are using a non-LDAP directory service, this column is not available.
Disposition	Action flag TRITON RiskVision applied to the request (for example, category permitted or category blocked).
Source Server	IP address of the machine sending requests to Filtering Service. This is the Content Gateway or Network Agent IP address.
Protocol	Protocol of the request (for example, HTTP or FTP).
Protocol Group	Master Database group in which the requested protocol falls (for example, Remote Access or Streaming Media).

Column Name	Description
Source IP	IP address of the machine from which the request was made.
Destination IP	IP address of the requested site.
Full URL	Domain name and path for the requested site (example: http://www.mydomain.com/products/itemone/). If you are not logging full URLs, this column is blank.
Month	Calendar month the request was made.
Port	TCP/IP port over which the user communicated with the site.
Bandwidth	The amount of data, in kilobytes, contained in both the initial request from the user and the response from the website. This is the combined total of the Sent and Received values.
Bytes Sent	Number of bytes sent as the Internet request. This represents the amount of data transmitted, which may be a simple request for a URL, or may be a more significant submission if the user is registering for a website, for example.
Bytes Received	Number of bytes received from the Internet in response to the request. This includes all text, graphics, and scripts that make up the site. If the log record is created as a result of Content Gateway analysis, the bytes received represents the size of the page scanned.
Time	Time of day the site was requested, shown in the HH:MM:SS format, using a 24-hour clock.
Category	Category to which the request was assigned. This may be a category from the Master Database or a custom category.

Create Favorite reports

You can save most investigative reports as Favorites. This includes reports you generate by drilling down, standard reports, and detail reports that you have modified to meet your specific needs. You can run a Favorite report at any time, or schedule it to run on specific days and times.



Not all delegated administrators have permission to save and schedule Favorite reports. If you don't see the Favorite Reports link, talk to your Super Administrator for access.

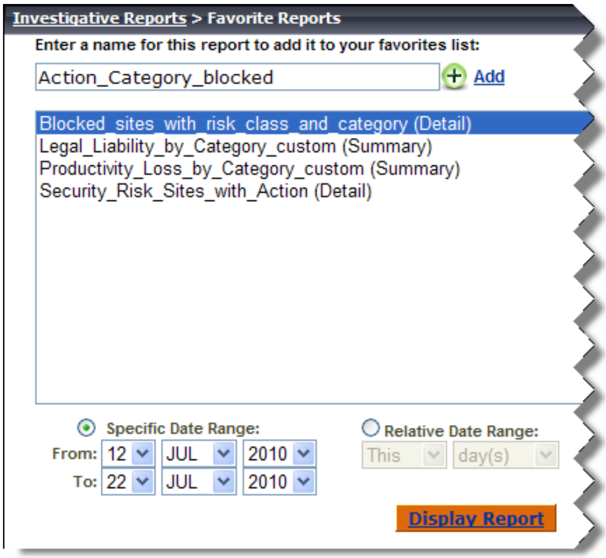
Save a report as a Favorite

1. Generate an investigative report with the desired format and information.
2. Click the Favorite Reports link in the toolbar at the top of the screen.
3. Enter a descriptive name for the report. The name may contain letters, numbers and underscore characters (_). No blanks or other special characters can be used.
4. Click **Add**. The report name is added to the list of Favorites.

Run a Favorite report immediately

Once a report has been added as a favorite, it is easy to run it again:

1. Select a report from the list, and then click **Run Now**.



2. Specify the date range that you want to include in the report, and then click **Display Report**.
3. When the report is complete, the results are displayed in the content pane.

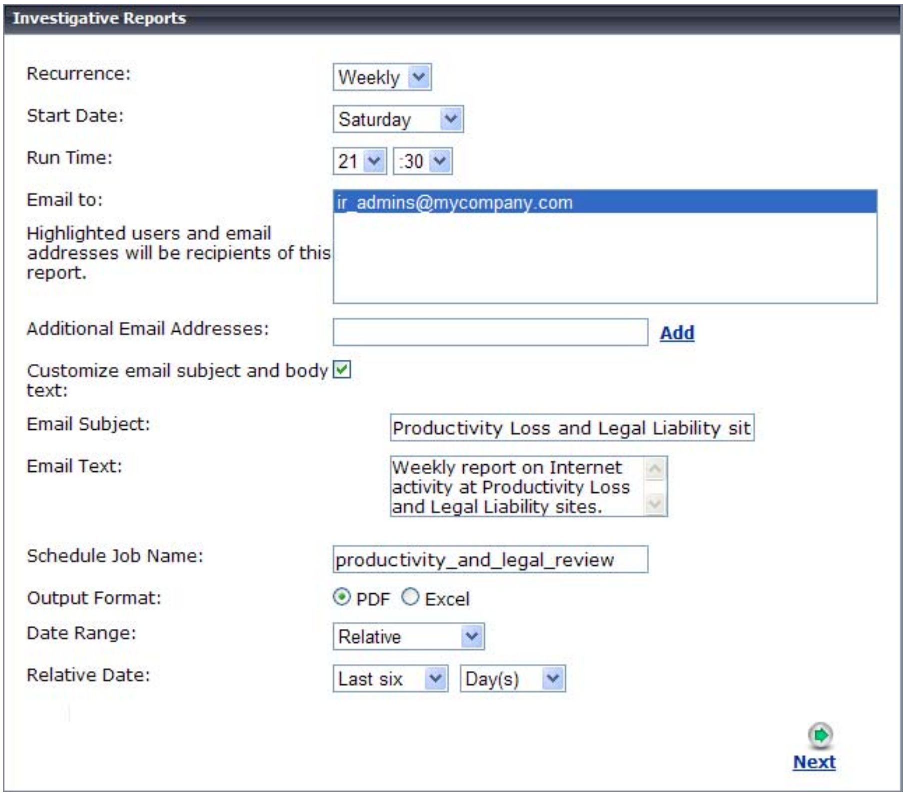
Schedule a Favorite report to run at a future time

You can also schedule Favorite reports to run later, or on a regular schedule:

1. If you are not already on the Favorite Reports page, click the **Favorite Reports** link.

2. Highlight up to 5 reports to schedule as part of the same job. (You can review the status of scheduled report jobs on the Investigative Reports > Job Queue page.)

3. Click **Schedule**. You are prompted to specify when the report will be run, how the report will be delivered, and how long a time period the report will cover.



4. Provide the following information to schedule the report, and then click **Next**:

Field	Description
Recurrence	How often (Once, Daily, Weekly, Monthly) the report job runs.
Start Date	The day of the week or calendar date the job first runs.
Run Time	The time of day the job runs.
Email to	Recipients of the completed report. Deselect any email addresses that should not be used. The report is sent only to highlighted email addresses.
Additional Email Addresses	Enter an email address, and then click **Add** to put it on the **Email to** list. The new email address is automatically highlighted with the other selected email addresses.
Customize email subject and body text	Indicates whether default or custom text is used when the completed report is sent to email recipients.
Email Subject	Enter custom text for the subject line of the email message containing the completed reports. The default subject reads: “Investigative Reports scheduled job.”

Field	Description

Email Text	Enter custom body text for the email message containing the completed reports.
	The email reads as follows:
	`Report scheduler generated the attached file or files on` *`<date time>`*`.`
	`<CUSTOM TEXT>`
	`To view the generated report(s), click on the following link(s).`
	`Note: The link will not work if the recipient does not have access to the web server from which the job was sent.`

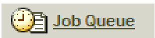
Schedule Job Name	Assign a unique name for the scheduled job. The name identifies this job in the Job Queue.
Output Format	Choose the file format for the scheduled reports: (Adobe) **PDF** or (Microsoft) **Excel**.
Date Range	Set the date range to be covered by reports in this job. **All Dates**: all available dates in the Log Database. **Relative**: Choose a time period (Days, Weeks, or Months) and the specific period to include (This, Last, Last 2, and so on). **Specific**: set specific dates or a date range for the reports in this job.

5. A summary page lists the scheduled job details, as well as any warnings. Click **Save** to schedule the report, or click **Previous** to make changes.

Clicking Save takes you to the Job Queue page, where you can:

- Review scheduled jobs.
- Make changes to scheduled jobs.
- Delete scheduled jobs. (This does not delete the Favorite report.)
- Find status and error information for jobs in progress and recently completed, or for jobs that could not be completed.

The Job Queue page can also be accessed from most investigative reports pages.



When a scheduled report is run, the completed report is saved in the following directory on the TRITON management server machine:

```
<install_path>\webroot\Explorer\<recipient_name>\
```

By default, the <*install_path*> is C:\Program Files (x86)\Websense\Web Security\bin. <*recipient_name*> is the portion of the recipient (Email to) email address before the @

symbol. If the report has multiple recipients, the reports are saved in a directory called **Other**.

Tips

- Recipients must have read access to the report directory to open the report.
- All reports saved from a repeating job use the same file name. If you want to save files for longer than a single cycle, be sure to change the file name or copy the file to another location.
- Depending on the size and number of reports scheduled, the Explorer directory could become very large. Super Administrators should clear the directory periodically, eliminating unneeded report files.