# Contents

**Introduction** .................................................................................................................. 1

**ERS Settings** .................................................................................................................. 2

**Working with Reports** ..................................................................................................... 3
  - Accessing the Report Manager ......................................................................................... 3
  - Using the Report Manager .............................................................................................. 4
  - Creating a New Report .................................................................................................... 5
  - Choosing the Report Type .............................................................................................. 6
  - Choosing Report Search Criteria
    - Search Criteria: Application Detailed Report ............................................................ 10
    - Search Criteria: Application Statistics Report .......................................................... 12
    - Search Criteria: Web Detailed Report ........................................................................ 14
    - Search Criteria: Web Statistics and Web Hourly Statistics Reports ......................... 17
    - Search Criteria: Web Session Report ......................................................................... 19
    - Search Criteria: Web Top Domains and Web Top Hosts Reports .............................. 21
  - Finishing the Report ........................................................................................................ 23
  - Selecting the Date Range ............................................................................................... 24
  - Editing a Report ............................................................................................................. 24
  - Deleting a Report ........................................................................................................... 25

**Running a Report** ........................................................................................................... 27
  - Viewing a Report ............................................................................................................ 28
  - Drilling Down in a Report .............................................................................................. 30
  - Saving a Generated Report ............................................................................................ 31

**Scheduling a Report** ....................................................................................................... 32
  - Editing a Report Schedule ............................................................................................. 33
  - Deleting a Report Schedule ......................................................................................... 33

**iPrisms List** ..................................................................................................................... 34

**Monitoring in Real-Time** ............................................................................................... 36
  - Using the Real-Time Monitor ......................................................................................... 36
  - Editing the Real-Time Monitor Settings .................................................................... 38

**Frequently Asked Questions** ......................................................................................... 40
Introduction

iPrism is the award-winning Internet filtering appliance that secures your organization from Internet-based threats such as malware, spyware, IM, P2P, and inappropriate content at the perimeter, while it helps enforce your acceptable use and security policies. This guide will help you understand the reporting capabilities of your iPrism as well as get you started using them.

The iPrism reporting engine, Enterprise Reporting Server (ERS), provides consolidated reporting for up to 30 iPrism systems. This high-powered system is able to quickly and easily process large amounts of data from your iPrism and produce consolidated reports.

The key features of the ERS system are:

- Dedicated high performance reporting engine and powerful dual Intel Xeon microprocessors enable reports to be produced quickly and easily.
- Collects and indexes up to 60 million web and application events a day.
- Provides one terabyte storage and can store up to two billion events in its database.
- Background scheduling of reports for delivery by email or FTP at a later time.
- Real-time, graphical status monitoring
- An easy-to-use Report Wizard
- Drill-down ability in text reports
- Support for multiple simultaneous users
- The ability to run reports immediately or schedule them to run later in batch mode
- The ability to export graphic and text reports in PDF format; text reports can also be exported as text files or as comma-separated data, suitable for use in Microsoft Excel or Crystal Reports.
ERS Settings

There are two global values for ERS:

- Historical data

  This is the number of days after which old data is removed from ERS. For example, if this value is set to 30 days, data older than 30 days is purged from ERS. Data is also purged if the disk limit is reached, regardless of this value. If you only want ERS to purge data when the disk is full, select Purge data only when disk is full.

- Time zone

  If a time zone is selected it will be used for all times shown on reports. Otherwise, the default will be used.

To modify either of these settings:

1. Click Modify.
2. Make changes as needed, then click OK.
Working with Reports

The Reports Manager allows access to the iPrism’s reporting features. You can create and customize reports, define report grouping and sorting, select the deliverable format, and schedule reports for later use.

Multiple users may use the Reports Manager at the same time. The following access rights can be set by the iPrism administrator to determine the information users can access:

- Full
- Access to information about a certain profile (e.g., BlockOffensive)
- Access to information about a certain IP address range (e.g., the Marketing subnet)

Users with limited access can only generate reports on the authorized information.

Accessing the Report Manager

1. From the iPrism Home Page, select **Reporting**, then **Report Manager**.
2. Click **iPrism Reports** to launch the Report Manager.
Figure 1. Reports Manager

Using the Report Manager

From the Report Manager, you can define, run, and view reports using options in the Navigation Menu at left or the shortcuts.

The Navigation menu in the left sidebar provides quick access to the different areas of the reporting system:

- **Welcome** displays the Welcome screen.
- **Settings** displays the ERS settings.
• **Reports** displays the main Report Manager screen, from which you can create, run, view, edit, and delete reports.

• **Schedules** displays the main Scheduling screen, from which you can create, edit, and delete report schedules.

• **iPrisms** displays the list of iPrisms on the network that are available for reporting.

• **Real-time Monitor** displays the Real-Time Monitor screen, from which you can monitor Internet and IM/P2P use in real time, as well as edit your monitoring configuration.

The following shortcuts are available from the Welcome screen:

• **Create a report** launches the New Report Wizard, where you can create, run, and/or schedule a report.

• **Run a report** enables you to run and view an existing report.

• **Schedule a report** launches the Schedule Report Wizard, where you can schedule reports and set delivery options.

• **Exit** closes the Report Manager application.

**Creating a New Report**

This section explains the entire new report creation process. The individual steps, such as selecting a report type, are explained in further detail in separate sections.

To create a report:

1. From the Report Manager welcome screen, either select **Reports > Create New Report** from the navigation menu, or **Create a report** from the shortcuts. The New Report Wizard opens.

   ![Note: When you select Reports from the navigation menu, you can also edit, run, and delete reports.]

2. Select an option:
   - Create a new report from scratch: Selecting this option allows you to specify all of the options you want to include in the report.
   - Create a new report based on a pre-existing report: Selecting this option allows you to select an existing report from the list.
3. Click **Next**.

4. In the Type tab, select the type of report you want to create and click **Next**.

5. If you selected Web Statistics, Web Hourly Statistics, Web Top (Grouped), or IM/P2P Statistics in the Type tab, the Grouping tab appears. Select Grouping options and click **Next** to go to the Sorting tab.

6. Select Sorting options and click **Next**.

7. Select the report criteria on the Criteria tab and click **Next**.

8. On the Finish tab, follow the instructions for naming and processing your report, then click **Finish**.

9. If you selected to run the report immediately, select the date range and click **Run**.

**Choosing the Report Type**

The type of report you select determines the general type of information that is included in your report: web access statistics, application use, top-access lists, and so on. iPrism provides several main report types, as described in the following table. Grouping and Sorting options by Report Type are also listed.

**Notes:**

Grouping options (via the Grouping tab) are available only for Web Statistics, Web Hourly Statistics, Web Top by Group or Application Statistics reports.

Sorting options (via the Sorting tab) are available after you select a Web Detailed report type, or after you select Grouping options for Web Statistics, Web Hourly Statistics or Application Statistics report types.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Grouping Options</th>
<th>Sorting Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Detailed</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Report Type</td>
<td>Grouping Options</td>
<td>Sorting Options</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application Statistics</td>
<td>Protocol Protocol and IP Address Protocol and Profile Protocol and User Name User Name User Name and Protocol IP Address IP Address and Protocol Profile Profile and Protocol iPrism Hostname iPrism Hostname and Protocol iPrism Hostname and IP Address iPrism Hostname and Profile iPrism Hostname and User Name</td>
<td>Static - available to all groupings Passed Blocked Dynamic - based on selected grouping IP Address Profile User Name Protocol</td>
</tr>
<tr>
<td>Web Detailed</td>
<td>N/A</td>
<td>Date &amp; Time IP Address, Date &amp; Time User Name, Date &amp; Time Profile, User Name, Date &amp; Time Action, Date &amp; Time Bandwidth, Date &amp; Time Rating, Date &amp; Time URL, Date &amp; Time</td>
</tr>
<tr>
<td>Web Hourly Statistics</td>
<td>Hour Hour and IP Address Hour and User Name Hour and iPrism Host Name Hour and Profile</td>
<td>Static - available to all groupings Passed Blocked Overridden Override Initiated Warned Quota Notified Quota Reached Hits Pages Bandwidth</td>
</tr>
<tr>
<td>Report Type</td>
<td>Grouping Options</td>
<td>Sorting Options</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web Session</td>
<td>N/A</td>
<td>Hits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bandwidth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Duration*</td>
</tr>
<tr>
<td>Web Statistics</td>
<td>Category</td>
<td>Static - available to all groupings</td>
</tr>
<tr>
<td></td>
<td>Category and User Name</td>
<td>Passed</td>
</tr>
<tr>
<td></td>
<td>Category and IP Address</td>
<td>Blocked</td>
</tr>
<tr>
<td></td>
<td>Category and Profile</td>
<td>Overridden</td>
</tr>
<tr>
<td></td>
<td>Category and Domain</td>
<td>Override Initiated</td>
</tr>
<tr>
<td></td>
<td>User Name</td>
<td>Warned</td>
</tr>
<tr>
<td></td>
<td>User Name and Category</td>
<td>Quota Notified</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Quota Reached</td>
</tr>
<tr>
<td></td>
<td>IP Address and Category</td>
<td>Hits</td>
</tr>
<tr>
<td></td>
<td>Profile</td>
<td>Pages</td>
</tr>
<tr>
<td></td>
<td>Profile and Category</td>
<td>Bandwidth</td>
</tr>
<tr>
<td></td>
<td>Domain</td>
<td>Duration*</td>
</tr>
<tr>
<td></td>
<td>Domain and Category</td>
<td>Dynamic - based on selected grouping</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Category</td>
</tr>
<tr>
<td></td>
<td>Location and Category</td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Profile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Name</td>
</tr>
<tr>
<td>Web Top</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Web Top by Group</td>
<td>User Name</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Profile</td>
<td></td>
</tr>
</tbody>
</table>
* Duration applies to local as well as remote events, which are calculated the same way.

Choosing Report Search Criteria

The Criteria tab allows you to specify search options for a report. For example, you could create a report that highlights activity in one particular profile, or that focuses only on a certain set of categories. The default settings include all data.

The criteria are additive, meaning that the data in the report reflects all the criteria, not just one. For example, if you restrict the report to a certain range of IP addresses and a given filtering category, then the report will only contain data for activity in that category originating from those IP addresses. It will not contain activity originating from those IP addresses in other categories, or activity in those categories by other IP addresses.

The options on the Criteria tab vary by report type.
Search Criteria: Application Detailed Report

The following search criteria are available for the Application Detailed report.

![Search Criteria for Application Detailed Report](image)

**Figure 2. Search Criteria for Application Detailed Report**
<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Host            | Returns data from the hosts that match the pattern you specify. Select an option and then enter the serial number or pattern. You can choose from the following options:  
  • Host Name Pattern: displays data from all iPrisms on the network with names that match the pattern you enter  
  • Host Serial No: displays data only from the one specific iPrism you specify  
  • Host Tag Pattern: displays data from all iPrisms on the network with tags that match the pattern you enter |
| Location        | Returns data on the locations you specify; they can be local locations and/or remote locations. You can choose from the following options:  
  • Local only: displays data only from local users  
  • Remote only: displays data only from remote users who are using iPrism’s Remote Filtering capabilities  
  • Both Local and Remote Filtering Data: displays data from both local and remote users |
| IP Address Range| Returns data on the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation. |
| User            | Returns data on a certain user name. The default is all users. You may also enter multiple user names separated by commas. If you do not know the user name of the person whose activity you wish to check, try entering their IP address. |
| Profile         | Returns data on the following profiles:  
  • All (default)  
  • BlockIMP2P: profiles that are blocked from using any Instant Messaging or Peer-to-Peer services  
  • BlockP2P: profiles that are blocked from using any Peer-to-Peer services  
  • PassIMP2P: profiles that are allowed to use Instant Messaging and Peer-to-Peer services  
  • Any user-defined profiles created in your company to which you have access |
<p>| Protocol        | Returns data on the protocol or protocols you select. The default is all protocols. |</p>
<table>
<thead>
<tr>
<th><strong>Search Criteria</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Start and End Time</td>
<td>Returns data on the time range that you enter.</td>
</tr>
</tbody>
</table>

**Search Criteria: Application Statistics Report**

The following search criteria are available for the Application Statistics report.

![Choose the search criteria](image)

*Figure 3. Search Criteria for Application Statistics Report*
<table>
<thead>
<tr>
<th><strong>Search Criteria</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
</table>
| Host                | Returns data from the hosts that match the pattern you specify. Select an option and then enter the serial number or pattern. You can choose from the following options:  
  - Host Name Pattern: displays data from all iPrisms on the network with names that match the pattern you enter  
  - Host Serial No: displays data only from the one specific iPrism you specify  
  - Host Tag Pattern: displays data from all iPrisms on the network with tags that match the pattern you enter |
| Location            | Returns data on the locations you specify; they can be local locations and/or remote locations. You can choose from the following options:  
  - Local only: displays data only from local users  
  - Remote only: displays data only from remote users who are using iPrism's Remote Filtering capabilities  
  - Both Local and Remote Filtering Data: displays data from both local and remote users |
| IP Address Range    | Returns data on the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation. |
| User                | Returns data on a certain user name. The default is all users. You may also enter multiple user names separated by commas If you do not know the user name of the person whose activity you wish to check, try entering their IP address. |
| Profile             | Returns data on the following profiles:  
  - All (default)  
  - BlockIMP2P: profiles that are blocked from using any Instant Messaging or Peer-to-Peer services  
  - BlockP2P: profiles that are blocked from using any Peer-to-Peer services  
  - PassIMP2P: profiles that are allowed to use Instant Messaging and Peer-to-Peer services  
  - Any user-defined profiles created in your company to which you have access |
| Protocol            | Returns data on the protocol or protocols you select. The default is all protocols. |
### Search Criteria: Web Detailed Report

The following search criteria are available for the Web Detailed report.

<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start and End Time</td>
<td>Returns data on the time range that you enter.</td>
</tr>
</tbody>
</table>

**Figure 4. Search Criteria for Web Detailed Report**
<table>
<thead>
<tr>
<th><strong>Search Criteria</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
</table>
| **Host** | Returns data from the hosts that match the pattern you specify. Select an option and then enter the serial number or pattern. You can choose from the following options:  
  - Host Name Pattern: displays data from all iPrisms on the network with names that match the pattern you enter  
  - Host Serial No: displays data only from the one specific iPrism you specify  
  - Host Tag Pattern: displays data from all iPrisms on the network with tags that match the pattern you enter |
| **Location** | Returns data on the locations you specify; they can be local locations and/or remote locations. You can choose from the following options:  
  - Local only: displays data only from local users  
  - Remote only: displays data only from remote users who are using iPrism’s Remote Filtering capabilities  
  - Both Local and Remote Filtering Data: displays data from both local and remote users |
| **IP Address Range** | Returns data on the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation. |
| **User** | Returns data on a certain user name. The default is all users. If you do not know the user name of the person whose activity you wish to check, try entering their IP address. |
| **Profile** | Returns data on the following profiles:  
  - All (default)  
  - Block offensive: profiles that are not allowed to view sites that contain pornography, profanity, violence, bomb-making, and other topics that are deemed offensive  
  - Pass all: profiles that are allowed to view any site without restriction (browsing is monitored)  
  - Any user-defined profiles created in your company to which you have access |
<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Action**      | Returns data on the following types of access attempts:  
|                 | • All (default)  
|                 | • Passed: all accesses that are permitted in your system  
|                 | • Blocked: all accesses that are blocked in your system  
|                 | • Overridden: all accesses that were blocked and then overridden by the user  
|                 | • Override Initiated: all accesses that were blocked and to which the user requested access  
|                 | • Warned: all accesses that occurred after a quota warning  
|                 | • Quota Notified: all accesses that occurred after a quota notification  
|                 | • Quota Blocked: all accesses that blocked because the quota was exceeded |
| **Category**    | Returns data on the category or categories you select. The default is all categories. |
| **URL Pattern** | Does a partial search and returns URLs that match the words you enter. For example, if you enter playboy.com, it returns all pages in the playboy.com domain. It also includes all substring matches, such as www.playboy.com. |
| **Include Media** | Returns the images, scripts, style sheets, and other things included on the page. |
| **Start and End Time** | Returns data on the time range that you enter. |
Search Criteria: Web Statistics and Web Hourly Statistics Reports

The following search criteria are available for the Web Statistics and Web Hourly Statistics reports.

![Search Criteria for Web Statistics and Web Hourly Statistics Reports](image)

**Figure 5. Search Criteria for Web Statistics and Web Hourly Statistics Reports**
<table>
<thead>
<tr>
<th><strong>Search Criteria</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
</table>
| Host               | Returns data from the hosts that match the pattern you specify. Select an option and then enter the serial number or pattern. You can choose from the following options:  
  • Host Name Pattern: displays data from all iPrisms on the network with names that match the pattern you enter  
  • Host Serial No: displays data only from the one specific iPrism you specify  
  • Host Tag Pattern: displays data from all iPrisms on the network with tags that match the pattern you enter |
| Location           | Returns data on the locations you specify; they can be local locations and/or remote locations. You can choose from the following options:  
  • Local only: displays data only from local users  
  • Remote only: displays data only from remote users who are using iPrism’s Remote Filtering capabilities  
  • Both Local and Remote Filtering Data: displays data from both local and remote users |
| IP Address Range   | Searches on the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation if you do not know the user name of the person who uses it. |
| User               | Returns data on activity generated by a certain user. The default is all users. If you do not know the user name of the person whose activity you wish to check, try entering their IP address. |
| Profile            | Returns data on the following profiles:  
  • All (default)  
  • Block offensive: profiles that are not allowed to view sites that contain pornography, profanity, violence, bomb-making, and other topics that are deemed offensive  
  • Pass all: profiles that are allowed to view any site without restriction  
  • Any user-defined profiles created in your company to which you have access |
| Category           | Returns data on the category or categories you select. The default is all categories. |
| Start and End Time | Returns data on the time range that you enter. |
Search Criteria: Web Session Report

The following search criteria are available for the Web Session report.

![Choose the search criteria]

Figure 6. Search Criteria for Web Session Report
<table>
<thead>
<tr>
<th><strong>Search Criteria</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
</table>
| **Host**            | Returns data from the hosts that match the pattern you specify. Select an option and then enter the serial number or pattern. You can choose from the following options:  
  • Host Name Pattern: displays data from all iPrisms on the network with names that match the pattern you enter  
  • Host Serial No: displays data only from the one specific iPrism you specify  
  • Host Tag Pattern: displays data from all iPrisms on the network with tags that match the pattern you enter |
| **Location**        | Returns data on the locations you specify; they can be local locations and/or remote locations. You can choose from the following options:  
  • Local only: displays data only from local users  
  • Remote only: displays data only from remote users who are using iPrism’s Remote Filtering capabilities  
  • Both Local and Remote Filtering Data: displays data from both local and remote users |
| **IP Address Range**| Returns data on the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation. |
| **User**            | Returns data on a certain user name. The default is all users. If you do not know the user name of the person whose activity you wish to check, try entering their IP address. |
| **Profile**         | Returns data on the following profiles:  
  • All (default)  
  • Block offensive: profiles that are not allowed to view sites that contain pornography, profanity, violence, bomb-making, and other topics that are deemed offensive  
  • Pass all: profiles that are allowed to view any site without restriction (browsing is monitored)  
  • Any user-defined profiles created in your company to which you have access |
<p>| <strong>Category</strong>        | Returns data on the category or categories you select. The default is all categories. |</p>
<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Pattern</td>
<td>Does a partial search and returns domains that match the words you enter. For example, if you enter playboy.com, it returns all pages in the playboy.com domain. It also includes all substring matches, such as <a href="http://www.playboy.com">www.playboy.com</a>.</td>
</tr>
<tr>
<td>Start and End Time</td>
<td>Returns data on the time range that you enter.</td>
</tr>
</tbody>
</table>

Search Criteria: Web Top Domains and Web Top Hosts Reports

The following search criteria are available for the Web Top Domains and Web Top Hosts reports.

![Choose the search criteria](image)

*Figure 7. Search Criteria for Web Top Domains and Web Top Hosts Reports*
<table>
<thead>
<tr>
<th><strong>Search Criteria</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
</table>
| **Host**            | Returns data from the hosts that match the pattern you specify. Select an option and then enter the serial number or pattern. You can choose from the following options:  
  • Host Name Pattern: displays data from all iPrisms on the network with names that match the pattern you enter  
  • Host Serial No: displays data only from the one specific iPrism you specify  
  • Host Tag Pattern: displays data from all iPrisms on the network with tags that match the pattern you enter |
| **Location**        | Returns data on the locations you specify; they can be local locations and/or remote locations. You can choose from the following options:  
  • Local only: displays data only from local users  
  • Remote only: displays data only from remote users who are using iPrism’s Remote Filtering capabilities  
  • Both Local and Remote Filtering Data: displays data from both local and remote users |
| **IP Address Range**| Returns data on the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation. |
| **User**            | Returns data on a certain user name. The default is all users. You may enter multiple user names, separated by commas. If you do not know the user name of the person whose activity you wish to check, try entering their IP address. |
| **Profile**         | Returns data on the following profiles:  
  • All (default)  
  • Block offensive: profiles that are not allowed to view sites that contain pornography, profanity, violence, bomb-making, and other topics that are deemed offensive  
  • Pass all: profiles that are allowed to view any site without restriction (browsing is monitored)  
  • Any user-defined profiles created in your company to which you have access |
<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Action**      | Returns data on the following types of access attempts:  
|                 | • All (default)  
|                 | • Passed: all accesses that are permitted in your system  
|                 | • Blocked: all accesses that are blocked in your system  
|                 | • Overridden: all accesses that were blocked and then overridden by the user  
|                 | • Override Initiated: all accesses that were blocked and to which the user requested access  
|                 | • Warned: all accesses that occurred after a quota warning  
|                 | • Quota Notified: all accesses that occurred after a quota notification  
|                 | • Quota Blocked: all accesses that blocked because the quota was exceeded |
| **Category**    | Returns data on the category or categories you select. The default is all categories. |
| **Count**       | Select from the following options:  
|                 | • Top Domains by Requests (default)  
|                 | • Top Domains by Bandwidth  
|                 | • Top Domains by Duration  
|                 | • Top Domains by Pages  
|                 | • Top Hosts by Requests  
|                 | • Top Hosts by Bandwidth  
|                 | • Top Hosts by Duration  
|                 | • Top Hosts by Pages |
| **Start and End Time** | Returns data on the time range that you enter. |

**Finishing the Report**

1. If you plan to save or schedule this report, type a title in the text box. The title must be unique within this report user account. Other report users may create reports with the same titles.

2. Select Yes or No to indicate whether this report should be shared. If you select Yes, the report will appear the next time other report users log in.
3. Select one of the following options for the report:
   • Save and run this report interactively now: The report will be saved and will run immediately in the foreground.
   • Save and run this report in the background: The report will be saved and will run immediately in the background.
   • Save this report. I will run it later: The report will be saved. When you want to run it, select Run a report from the Welcome screen and open the saved report.
   • Save and schedule this report to run at a later date. If you select this option, the Choose Scheduling Options dialog box appears.
   • Run this report now without saving. If you select this option, the Choose Date Range dialog box appears. The report settings will not be saved. If you want to run the report again, you will need to recreate it from scratch.

4. Click Finish.

Selecting the Date Range

You can select a default date range or create a date range. Only the data within the specified date and time will appear on the report.

The following options are available:

   • Today: Includes data from midnight (12am) to 11:59pm of the current day.
   • Yesterday: Includes data from midnight (12am) to 11:59pm of the previous calendar day.
   • Last Week: Includes data from midnight (12am) Monday to 11:59pm Sunday - the last full week before the current date.
   • Last Month: Includes data from midnight (12am) on the first of the month to 11:59pm on the last day of the calendar month before the current month.
   • Custom Range: Allows you to enter any date and time range.

Editing a Report

You can edit any of the user-defined reports that have been created on your system. Predefined reports cannot be edited.
To edit a report:

1. From the Navigation menu, click **Reports**.

2. Select a report from the list. The columns are as follows:
   - **Name**: The name of the report. If this is a user-defined report, you defined the title in the Finish tab of the New Report Wizard.
   - **Type**: The type of report. For more information, see “Choosing a report type”.
   - **Owner**: The report user who created the report. Predefined indicates a predefined report built into iPrism.
   - If you have a long list of reports, you may want to use the Filter field. When you type a string such as “Statistics” into the Filter field, the report list automatically filters down to only those reports that contain the word “Statistics” in the Name, Type, or Owner column.
   - To clear the filter and see the whole list again, click ![Clear Filter](image)

3. Click **Edit Report**. The Editing Report dialog box appears and the settings that currently define the report are displayed. The contents of the dialog box depend on the report type.

4. Type or select new values in any of the rows that you want to change.

5. To exit the Editing Report dialog box and use the New Report Wizard instead, click **Use Wizard**. If you do this, you must finish editing the report in the wizard, or come back to the Editing Report dialog box from the Reports screen.

6. When you are finished editing the report, click **Save**.

Deleting a Report

You can delete any of the user-defined reports that have been created on your system. When you delete a report, any associated schedules will be deleted also. Predefined reports cannot be deleted.

1. Click **Reports** in the Navigation menu.

2. Select a report from the list. Options are as follows:
   - **Name**: The report title. If this is a user-defined report, you defined the title in the Finish tab of the New Report Wizard.
   - **Type**: The report type. For more information, see “Choosing a report type”.
• Owner: The report user who created the report. “Predefined” indicates a report that was built into iPrism.

• If you have a long list of reports, you may want to use the Filter field. When you type a string into the Filter field, such as “Statistics”, the report list automatically filters down to only those reports that contain the word “Statistics” in the Name, Type, or Owner column.

• To clear the filter and see the whole list again, click .

3. Click **Delete Report**. A confirmation dialog box appears.

4. Click **OK** to delete the report. Any associated schedules will also be deleted.

**Warning:** You cannot undo this action.
Running a Report

You can run and view a report immediately or run the report in the background to be delivered by email or FTP. Reports run in the background are not limited to 25,000 records.

To run a report immediately:

1. From the Welcome page, select **Reports** in the Navigation menu.
2. Select a report in the list, and click **Run & View Report**.

   ![Figure 8. Report List](image)

   **Figure 8. Report List**

3. Choose a date range, and click **Run**.

The Administrator can view the status of the scheduled reports via the Schedule screen. One-time reports are listed as “one-time” as opposed to a periodic report, such as daily, weekly, or monthly.
• Click **Refresh** to update and view the current status of all scheduled reports.

To run a report in the background:

1. From the Welcome page, select **Reports** in the Navigation menu.
2. Select a report in the list, and click **Run in Background**.
3. Choose a date range, and click **Next**.
4. Select how the report will be delivered:
   - If you want the report delivered by email, select Email and type the email address to which you want the report delivered. Use a comma to separate multiple email addresses.
   - If you want the report delivered by FTP, select FTP and type the locations of the FTP Host and FTP Directory, and the FTP Username and Password.
5. Select the format for the report.
6. Click **Finish**.

**Viewing a Report**

After you run a report, it opens automatically in the iPrism Report Viewer. iPrism provides column sorting and drill-down functionality.

The report header shows the report type, date, and criteria.

---

![Report Header](image)

**Figure 9. Report Header**
The report details section shows a chart of the selected data, followed by the report detail in list form. To change the data that shows on the chart, click on a column heading in the list below the chart. The selected column is highlighted.

**Figure 10. Report Details**

For example, clicking Passed in the above report generates the following.
Drilling Down in a Report

When you run a report interactively (i.e., select Run & View Report), iPrism text reports include full drill-down functionality to provide additional information about any section of the report.

When the report is displayed on your screen, click any field to see drill-down options for that field. A context menu shows the drilldown options.
The example above shows the drill-down options available in the Corporate Marketing category section of a Web Statistics by Category report.

- **User name**: Lists each user’s accesses to sites in a given category.
- **IP address**: Lists all accesses made to sites in a given category by workstation (IP address).
- **Profile**: Lists all accesses made to sites in a given category, by profile.
- **Domain**: Lists all accesses made to sites in a given category, by domain.
- **Details**: Generates a Web Detailed report on accesses made to sites in a given category; due to its detailed nature, this may take time to run.

**Saving a Generated Report**

After generating a report, you can save it in PDF, CSV, or CSV with Headings format from the Report Viewer. If you have drilled down in the report, the Report Viewer saves the tab you are currently viewing.

To save a report

1. Click **Save** in the Report Viewer toolbar.
2. Select a folder and enter a name for the report.
3. Select the file type.
4. Click **Save**.
Scheduling a Report

You can schedule reports to be generated at regular intervals. They can then be emailed to one or more recipients or stored on an FTP server.

To schedule a report:

1. From the Report Manager welcome screen:
   - Select Reports from the navigation menu, select a report, and click Schedule Report.
   OR
   - From the shortcuts, click Schedule a Report, click Next, select a report, and click Next again.

2. Select how often you want the report to run:
   - Daily: The report runs at midnight every day.
   - Weekly: The report runs at midnight every Sunday.
   - Monthly: The report runs at midnight on the first day of every month.

   Depending on their size, reports are usually delivered in the early morning after they have been generated.

3. Select how the report will be delivered:
   - If you want the report delivered by email, select Email and type the email address to which you want the report delivered. Use a semicolon (;) to separate multiple email addresses.
   - If you want the report delivered by FTP, select FTP and type the locations of the FTP Host and FTP Directory, and the FTP Username and Password.

   **Warning:** The FTP password you enter here is transmitted over the network “in the clear” (i.e., not encrypted). Therefore, do not use a privileged account for the FTP dropbox.

4. Select the format for the report.

5. Click OK or Finish.
Editing a Report Schedule

To change a report schedule:

1. From the Report Manager welcome screen, select Schedules from the navigation menu. The list of scheduled reports appears.

2. To filter the list, type a string (such as Daily) in the Filter field.

   To clear the filter and see the complete list again, click .

3. Select a report in the list and click Edit Schedule.

4. Type or select new values in any of the fields that you want to change.

5. Click Save.

Deleting a Report Schedule

To delete a report schedule:

1. From the Report Manager welcome screen, select Schedules from the navigation menu. The list of scheduled reports appears.

2. To filter the list, type a string (such as Daily) in the Filter field.

   To clear the filter and see the complete list again, click .

3. Select a report in the list and click Delete Schedule.

4. Click OK to confirm.
iPrisms List

- The iPrisms List window provides information about all iPrisms that have sent data to ERS. The iPrisms Inventory List displays each iPrism serial number, tag, DNS host name, and the last event ERS received from the iPrism.

- Serial No: iPrism serial number.

- Tag: The tag enables the administrator to group iPrisms meaningfully in order for the search criteria to limit the scope of reports. For example, you could group California universities, by tagging them by state, then city, then school. For example, ca:sd:sdsu (California, San Diego, San Diego State University), ca:sd:ucsd (California, San Diego, University of California, San Diego), ca:la:usc (California, Los Angeles, University of Southern California), ca:la:ucla (California, Los Angeles, University of California, Los Angeles) etc. Administrators can specify the tag pattern "ca:sd" in the search criteria to focus only on the schools in San Diego.

- Host Name: iPrism hostname.

- Last Event Received: The timestamp of the latest event received from that particular iPrism.

Selecting an iPrism in the list displays more specific information about it. The details are shown in the Selected iPrism Details frame at the bottom of the window. The information displayed includes:

- Number of web events as of yesterday: The total number of web access events from this iPrism that are stored on ERS.

- Number of application events as of yesterday: The total number of application access events from this iPrism that are stored on ERS.

- Description: The user description of this iPrism.

- Time zone: The time zone this iPrism is in.

- Oldest event processed: The oldest event from this iPrism that has been processed and stored in ERS.

- Newest event processed: The newest event from this iPrism that has been processed and is stored in ERS.

To modify the description and tag:

1. Select an iPrism
2. Click **Modify**.

3. Enter or change the description and the tag.

4. Click **OK**.

5. Click **Refresh** on the iPrism Settings screen to display the updates.

   **Note:** If ERS has not received any updates from an iPrism for the last 24 hours, a warning icon displays at the bottom of the iPrism Settings page, alerting the administrator to take action.
Monitoring in Real-Time

The real-time monitor lists system activity - web and application access - as it happens.

Using the Real-Time Monitor

To view system activity in real-time:

1. From the Report Manager welcome screen, select **Real-time Monitor** from the navigation menu.
2. Click **Start Monitoring**.

To pause and restart monitoring:

1. Click **Pause Monitoring**.
2. When you are ready to start again click **Start Monitoring**.

The real-time monitor shows the monitored activity on your system. Like reports, the monitor can hold up to 25,000 entries at a time. When it reaches the limit, it deletes the oldest entries to make room for new ones. As activities appear on the monitor, the bar scrolls. To stop the scrolling, double-click a site. To restart the scrolling, drag the vertical scroll bar all the way to the bottom.

Tips:

- Click and drag to resize or move any of the columns.
- Double-click the URL to access a site.
- To view a subset of the activities, type a string, such as “business” into the Filter field to automatically filter the list to all lines that contain that string in any column.
- To clear the filter and see the entire list again, click ![Clear Filter](image).

The following information is shown:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>When the access occurred.</td>
</tr>
<tr>
<td>Setting</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>The type of access: Web or application.</td>
</tr>
<tr>
<td>User &amp; IP Address</td>
<td>The user name and IP address of the login and computer that initiated the request.</td>
</tr>
<tr>
<td>Profile</td>
<td>The profile controlling this access attempt.</td>
</tr>
<tr>
<td>Action</td>
<td>The action iPrism took in response to the access attempt (pass, block, monitor, override, override initiated).</td>
</tr>
<tr>
<td>Rating/Protocol</td>
<td>For Internet/Web access, this shows the rating category, such as entertainment or business. For applications, this shows the protocol, such as AIM or Kazaa.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL being accessed.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The bytes required for this activity.</td>
</tr>
</tbody>
</table>

The summary information is as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests</td>
<td>The total number of events currently contained in the RTM.</td>
</tr>
<tr>
<td>Web</td>
<td>The number of Web events.</td>
</tr>
<tr>
<td>Application</td>
<td>The number of application events.</td>
</tr>
<tr>
<td>Users</td>
<td>The number of unique user/IP address combinations contained in the RTM.</td>
</tr>
<tr>
<td>Passed</td>
<td>The number of events passed.</td>
</tr>
<tr>
<td>Blocked</td>
<td>The number of events blocked.</td>
</tr>
<tr>
<td>Overridden</td>
<td>The number of events overridden.</td>
</tr>
<tr>
<td>Override Initiated</td>
<td>The number of events override initiated.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The bandwidth used by all events currently contained in the RTM.</td>
</tr>
</tbody>
</table>
Editing the Real-Time Monitor Settings

To edit the real-time monitor settings:

1. From the Report Manager welcome screen, select **Real-time Monitor** from the navigation menu.

2. Click **Edit Monitor Settings**.

3. Type or select new values as needed.

4. Click **OK**.

The settings are as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address Range</td>
<td>Monitors the range of IP addresses that you enter. The default is all IP addresses. Entering an IP address enables you to get information on a single workstation.</td>
</tr>
<tr>
<td>Setting</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>Returns data on a certain user name. The default is all users. You may also enter multiple user names separated by commas. If you do not know the user name of the person whose activity you wish to check, try entering their IP address.</td>
</tr>
</tbody>
</table>
| Profile   | Returns data on the following Web profiles:  
  - All (default)  
  - BlockOffensive  
  - Pass All  
Returns data on the following Application profiles:  
  - All (default)  
  - BlockIMP2P: profiles that are blocked from using any Instant Messaging or Peer-to-Peer services  
  - BlockP2P: profiles that are blocked from using any Peer-to-Peer services  
  - PassIMP2P: profiles that are allowed to use Instant Messaging and Peer-to-Peer services  
  - Any user-defined profiles created in your company to which you have access |
| Action    | Returns data on the following types of access attempts:  
  - All (default)  
  - Passed: all accesses that are permitted in your system  
  - Blocked: all accesses that are blocked in your system  
  - Overridden: all accesses that were blocked and then overridden by the user  
  - Override Initiated: all accesses that were blocked and to which the user requested access |
| Include Media | Returns the images, scripts, style sheets, and other things included on the page.                                                                                                                               |
| Category   | Returns data on the category or categories you select. The default is all categories.                                                                                                                      |
| Protocol   | Returns data on the protocol or protocols you select. The default is all protocols.                                                                                                                        |
Frequently Asked Questions

Why do my reports sometimes run slowly?

Usually it is because your report is queued behind someone else’s. Two people cannot run the same report simultaneously. If you try to run a report that is already running, iPrism queues your request and executes it after the first report concludes.

In addition, some reports, such as the Web Top reports, use a high level of system resources; however, any report may take a long time to run if the date range is quite large. When there is a high demand for system resources, iPrism also queues reports. Wait a few minutes to allow the system to free up.

How many days of information does iPrism store?

iPrism stores up to 120 million records at a time. The amount of time it takes to accumulate this many records may vary from company to company.

How many entries can a report hold?

No limit is placed on scheduled reports. Large reports are broken into several smaller documents of a manageable size (65,000 records) before being delivered by email or FTP. All other report types can hold up to 25,000 entries. Limits should be placed on reports running interactively (i.e., when Run & View Report is selected).

The Real-time Monitor is not working and I received the error message, "Unable to receive real-time events”. Why?

iPrism sends access events to the Real-time Monitor using the UDP protocol. If for some reason these messages are not able to reach your workstation, the Real-time Monitor will not function.

In many cases this is caused by a firewall, or by a router configured to not allow UDP packets. You will need to configure your firewall or router to allow the following UDP ports used by the Real-Time Monitor: PORT 51231 and PORT 51232.

For additional information and help configuring your firewall, see the Knowledgebase article “Unable to Receive Real-Time Events”.

I did not receive my scheduled report in email.

Some email systems limit the size of the attachments you can receive. Some PDF reports are quite large, and may exceed the file size limits.

Try any of the following:

- Edit the schedule so that iPrism delivers your reports via FTP rather than email.
- Edit the schedule so that iPrism saves the report in CSV format. Large CSV reports are automatically split up into multiple email messages.
- Edit your report so that the saved report is smaller. Web Statistics and Application Statistics typically generate smaller files than the other report types.
- Ask your system administrator if it is possible to reconfigure the email system to accept larger attachments.

The Real-time Monitor is not showing all of the application or web activity that I know is occurring.

The Real-time Monitor only shows monitored web sites. If your profile does not monitor the web sites you are accessing, they will not appear in the Real-time Monitor or on any reports.

When I log in to the Report Manager, it pauses at 84%. Why?

iPrism typically pauses at this stage to authenticate Windows domains. Wait a few moments for the system to finish starting up.