

iPrism Web Security



© 2001 - 2012 EdgeWave. All rights reserved. The EdgeWave logo, iPrism and iGuard are trademarks of EdgeWave Inc. All other trademarks and registered trademarks are hereby acknowledged.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

The iPrism software and its documentation are copyrighted materials. Law prohibits making unauthorized copies. No part of this software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into another language without prior permission of EdgeWave, Inc.

iPrismAdmin07.000.01

Contents

Chapter 1 Introduction	1
About iPrism.....	1
About this Guide.....	1
Who Should Use this Guide?.....	1
Knowledgebase, Tutorials and Technical Support.....	2
Installation Notes.....	2
Chapter 2 Overview	4
How iPrism Works.....	4
The Filtering Database.....	4
Deciding What Gets Blocked.....	4
Assigning Profiles.....	7
Getting Past Blocked Sites.....	7
How iPrism Filters Internet Activity.....	8
Introduction to Profiles.....	9
Proxy Mode.....	10
Bridge (Transparent) Mode.....	11
Using the Management Interface.....	12
Logging In and Out of iPrism.....	13
Restarting and Shutting Down iPrism.....	14
The iPrism Home Page.....	14
Chapter 3 Profiles & Filters	15
Custom Filters.....	15
Adding a Custom Filter.....	16
Editing a Custom Filter.....	18
Deleting a Custom Filter.....	18
Importing and Exporting Custom Filters.....	19
Profiles.....	19
How iPrism Uses Profiles.....	20
iPrism's Default Profiles.....	21
Web Profiles.....	21
Adding a Web Profile.....	22
Copying a Profile.....	23
Deleting a Profile.....	24
Application Profiles.....	24
Adding an Application Profile.....	25

Copying an Application Profile	27
Deleting an Application Profile	28
Authentication and Assigning Profiles to Users	28
Assigning Profiles to a Set of IP Addresses (Workstations)	28
Quotas and Warnings	28
Email Alerts	30
Adding an Email Alert	31
Editing an Email Alert	32
Deleting an Email Alert	33
Quotas	33
Adding a Quota	35
Editing a Quota	36
Deleting a Quota	37
Warnings	37
Adding a Warning	38
Editing a Warning	40
Deleting a Warning	40
Access Control Lists (ACLs)	40
Creating a New Web ACL	40
Creating a New Application ACL	42
Editing an ACL	43
Deleting an ACL	43
Lock ACL	43
Current Overrides	45
Pending Requests	46
Granting Requests	47
Denying Requests	47
Recent Blocks	48
Remote Filtering	48
Using Remote Filtering	49
Enabling Remote Filtering	49
Chapter 4 Users & Networks	53
Local Users	53
Adding Users	54
Editing a Local User	55
Deleting a Local User	56
Importing Users	56
Exporting Users	57

Groups	57
Adding a Group	58
Editing a Group	59
Deleting a Group	59
Mapping Groups to Profiles	59
Nested Groups	60
Privileges	61
Networks	63
Adding a Network Profile	64
Editing a Network Profile	67
Deleting a Network Profile	67
VLAN Management	67
Adding a VLAN Description	68
Editing a VLAN Description	69
Deleting a VLAN Description	69
Admin Roles	70
Adding an Admin Role	71
Editing an Admin Role	74
Deleting an Admin Role	75
Exceptions	75
Adding an Exception	75
Editing an Exception	77
Deleting an Exception	77
Remote Users	77
Adding a Remote User	79
Editing Remote Users	79
Deleting a Remote User	80
Importing Remote Users	80
Exporting Remote Users	81
Remote Upgrades	82
Chapter 5 Reporting	85
Chapter 6 Maintenance	86
Appliance Updates	86
Installing a New Hotfix	87
Rebooting after Installing Hotfixes	87
Uninstalling a Hotfix	87
Backup and Restore	88
Backing Up	88

Restoring.....	89
Restoring Your System from a Local Backup.....	89
Restoring iPrism to its Default (Factory) Configuration.....	89
Event Log.....	89
Deleting Access Event Records.....	90
Policy Test.....	90
Self Check.....	91
Send Test Email.....	92
Site Rating & Test.....	92
Support Tunnel.....	93
Test Directory Services.....	93
Chapter 7 System Settings.....	95
Central Management.....	95
Customizable Pages.....	95
Customizing Pages.....	96
Authentication, Access Denied, Quota Notification, and Warning Notification.....	
Pages.....	96
Customized HTML.....	96
Specified URL.....	97
All Other Pages.....	98
Reporting Logo.....	99
Customizable Page Tags.....	100
Directory Services.....	101
Choosing an Authentication Mechanism.....	102
Local Authentication.....	103
LDAP Authentication.....	103
Setting up the iPrism LDAP Client.....	103
Authentication from the User's Perspective.....	105
Microsoft Windows Active Directory Authentication (Active Directory 2000/2003).....	106
Assigning iPrism Profiles to Windows AD Global Groups.....	107
Microsoft Windows Active Directory Authentication (Active Directory 2008).....	107
Prerequisites.....	107
Setting up iPrism to authenticate against a Windows 2008 server.....	108
Migrating from AD 2003 to AD 2008.....	111
Enterprise Reporting.....	111
Event Logging.....	111
Syslog Export.....	111
Email Settings.....	112

FTP Settings.....	113
High Availability.....	113
Setup.....	114
Recovery.....	116
License Key.....	117
iPrism Certificates.....	117
Uploading Your License Key.....	119
Local Categories.....	119
Network ID.....	120
Network Services.....	125
Network Hardening (Protecting Against DoS Attacks).....	126
Enabling SNMP.....	126
The SNMP Community String.....	126
WCCP.....	127
Configuring WCCP Settings in iPrism.....	127
Configuring SMTP Relay Settings.....	128
Enabling the Co-Management Network.....	129
Pending Request Options.....	130
Ports.....	131
Proxy and Configuration Ports.....	132
Redirect and HTTPS Ports.....	133
Proxy.....	134
Slaving iPrism to a Parent Proxy (Proxy Mode).....	135
Enabling an Upstream Proxy in Bridge (transparent) Mode.....	136
HTML Header Handling.....	136
Configuring the Filter List/System Update Proxy Server.....	137
System Preferences.....	137
Backup Settings.....	138
Bypass Authentication.....	139
Current Date and Time.....	139
Filter Failover Mode.....	140
Setting or Changing the Supervisor Password.....	140
Filter List (iGuard) Updates.....	141
Scheduling Filter List (iGuard) Updates.....	141
Checking iPrism's Filter List Status.....	141
System Failover Mode.....	141
System Updates.....	142
Proxying for External Users.....	142
Scheduled Reboot.....	143

Unrated Pages (iARP).....	144
User Settings.....	145
Chapter 8 System Status.....	146
About.....	146
Administration Log.....	146
Configuration Summary.....	147
Connectivity.....	147
Pinging a Host.....	148
Tracing Network Activity.....	148
Perform a DNS Lookup.....	148
Refreshing the System Updates Server.....	148
Routing Table.....	148
Security Log.....	149
Status.....	149
Chapter 9 Central Management.....	151
Before You Begin.....	151
Setting Up a Master/Slave Configuration.....	152
Designating Slave Systems.....	152
Designating the Master System.....	153
Changing the Master System.....	155
Removing a Slave System.....	156
Using Standalone Mode.....	156
Upgrading iPrisms in a Central Management Configuration.....	156
Chapter 10 Override Management.....	158
Access Denied Page Options.....	158
Using Override Privileges.....	159
Overriding a Blocked Web Site.....	159
Using Access Requests.....	161
Requesting Access to a Site.....	161
Managing Override Access.....	162
Appendix A Filtering Categories.....	163
Site Rating Categories.....	163
Sex Category.....	163
Adult.....	163
Lingerie/Bikini.....	164
Nudity.....	164

Pornography.....	165
Sexuality.....	165
Questionable Activities Category.....	166
Copyright Infringement.....	166
Computer Hacking.....	166
Intolerance/Extremism.....	167
Miscellaneous Questionable.....	167
Profanity.....	167
Tasteless.....	168
Weapons/Bombs.....	168
Violence.....	169
Security Exploits Category.....	169
Phishing.....	169
Spyware/Adware.....	169
Malware.....	170
Society Category.....	170
Alt/New Age.....	170
Art/Culture.....	171
Family Issues.....	171
Government.....	172
Politics.....	172
Social Issues.....	173
Keywords.....	173
News.....	173
Classifieds.....	173
Religion.....	174
Cult.....	174
Alternative Lifestyle.....	175
Internet (Web) Category.....	175
Anonymizer.....	175
Discussion Forums.....	175
Online Chat.....	176
Translators.....	176
Image Host.....	176
File Host.....	176
Peer to Peer.....	177
Email Host.....	177
Safe Search Engine.....	177
Sharewares Download.....	177

Web Banners	178
Web Host	178
Web Search	178
Portals	179
High Bandwidth	179
Dynamically Detected Proxies	179
Business Category	180
Specialized Shopping	180
Dining/Restaurant	180
Real Estate	180
Automotive	180
Internet Services	180
Corporate Marketing	180
Finance	181
Job/Employment Search	181
Professional Services	182
Online Auctions	182
Education Category	182
Continuing Education/Colleges	182
History	183
K-12	183
Reference Sites	184
Sci/Tech	184
Sex Education	184
Health Category	185
Alcohol/Tobacco	185
Drugs	185
Health	186
Adult Sex Education	186
Recreation Category	187
Entertainment	187
Gambling	187
Games	188
Hobbies/Leisure	188
Mature Humor	189
Television/Movies	189
Music	189
Digital Media	189
Radio Stations	189

Social Networking/Dating.....	190
Special Interests.....	190
Sports.....	191
Travel.....	191
Web Log (Blog).....	192
Appendix B Configuring Browsers for Proxy Mode.....	193
Configuring Firefox for Proxy Mode.....	193
Configuring Safari (Mac OS X only) for Proxy Mode.....	193
Configuring Internet Explorer for Proxy Mode.....	194
Appendix C iPrism Error Messages.....	195
iPrism Rating Error.....	195
iPrism List Update.....	195
iPrism List Error.....	196
iPrism Filter Service Expired.....	196
Access Denied.....	196
Authentication is Required.....	197
Connection Failed.....	197
Unable to Determine IP Address.....	197
Invalid Request.....	198
Invalid URL.....	198
iPrism is in the Process of Reconfiguring Itself.....	198
Zero Sized Reply.....	198
Write Error / Broken Pipe.....	199

CHAPTER 1 Introduction

About iPrism

The iPrism Web Filter combines simplicity, performance and value to deliver unrivalled protection from Internet-based threats such as malware, viruses, spyware, anonymizers, IM, P2P, and inappropriate content. As a self-contained appliance-based solution, iPrism offers universal interoperability on any platform and in any network environment, delivering Internet security at the perimeter, to help enforce your Internet acceptable use and security policies. In addition, iPrism seamlessly integrates with your directory services to automate authentication for fast and easy deployment throughout your organization.

About this Guide

This guide is designed to provide you with both an overview of iPrism and the step-by-step processes for implementing it in your organization. It is important to have a thorough understanding of the iPrism appliance itself, as well as the bigger picture of how it functions within your network environment, to get the best performance possible from your appliance.

This section introduces you to how information is arranged and presented. It also provides information about how to access the iPrism tutorials and Knowledgebase, and contact information for Technical Support.

This guide does not include installation instructions. Refer to the *iPrism Installation and Configuration Guide* if you have not yet connected the iPrism to your network.

Who Should Use this Guide?

This guide was written for network administrators or those who are fulfilling that duty for their organizations. The requirements for understanding this manual include:

- An understanding of TCP/IP networking

- Knowledge of your network's topology
- The ability to configure networking settings on Windows workstations

Knowledgebase, Tutorials and Technical Support

If you are unable to resolve your issue using the manual, please check our Knowledgebase at:

www.edgewave.com/support/web_security/knowledgebases.asp

Embedded iLearn videos are a series of short task-oriented videos to help guide you through specific iPrism configuration scenarios. These tutorials are available at:

www.edgewave.com/support/web_security/recorded_webinars_ilearn.asp

You may also contact the iPrism support team at:

www.edgewave.com/forms/support/web_security.asp

When contacting tech support, include all relevant information about how the iPrism is configured on your network (e.g., topology, other hardware, networking software, etc.). Have your iPrism serial number and registration key information handy. Also, to help our support staff solve your problem, it is helpful if you can send us a network diagram showing the basic hardware that is in use on your network.

Installation Notes



Important: This guide assumes that you have already connected the iPrism appliance to your network using the instructions in the *iPrism Installation Guide*.

There are a few situations that can complicate an iPrism installation that are not addressed in the iPrism Installation Guide, such as:

- If other proxy servers are configured on your network.
- If you have a WAN serviced by a router that is also the Internet router.
- If you have a unique network setup, and you are unsure of its ability to interact with iPrism.

If one or more of these conditions exist on your network and you are not able to get iPrism to function properly, check the EdgeWave website. This site contains the most current support information for iPrism.

www.edgewave.com/support/web_security/default.asp

If you are still unable to find a solution, you may request assistance with your installation from the iPrism technical support team. See [Knowledgebase](#), [Tutorials](#) and [Technical Support](#).

If your network uses a firewall or other device that masks IP addresses, it is important to install iPrism inside the firewall/device. Otherwise, it may prevent iPrism from tracking individual users on the network, in which case it will not be possible to perform user tracking. If you are unable to configure iPrism inside the firewall, some iPrism features will not be available to you.

CHAPTER 2 Overview

This section describes how iPrism works and provides an overview of its features and capabilities.

How iPrism Works

In the simplest terms, iPrism is a filtering device that examines your Internet traffic stream for HTTP, HTTPS, IM, and P2P traffic. In the case of HTTP and HTTPS requests, each URL request is checked against a database in which URLs are classified into fixed categories, based on their content. The client's web request may be blocked or monitored by iPrism, depending on which categories the iPrism administrator has elected to place limits according to the rules in the user's Web Profile.

The Filtering Database

The process by which URLs are evaluated and categorized is a URL database. As part of the process, each website in question is submitted to an Internet analyst who reviews the site and makes the appropriate category designations (e.g., adult, nudity, profanity, government, religion, drugs, games, etc.). To ensure that each iPrism unit is always operating with the very latest filtering database, the iPrism appliance automatically connects to the EdgeWave server daily and downloads the most recent filtering database files. The URL database now contains more than 80 categories with millions of websites. See [Filtering Categories](#) for detailed information about categories.

Deciding What Gets Blocked

The first step in setting up your filter is to create an Access Control List (ACL). This is a list that tells iPrism what to do for each category of website. For example, you may want to block access to websites of an "adult" nature (and monitor any attempt to access them), monitor any accesses to sites categorized as "nudity" (and allow the user to access them), and let all other requests through unmonitored and unblocked.

To do this you need to create an ACL with the following settings:

Category	Monitor	Blocked
adult	Yes	Yes
nudity	Yes	No
everything else	No	No

The ACL controls what is blocked and monitored. iPrism needs to know when to apply the ACL and who to apply it to.

The schedule controls when an ACL is applied. Suppose the company policy is “No Shopping during working hours, but during lunch and after work, anything goes.” To implement this policy, you may create an ACL called NoShopping which blocks all shopping and online auction sites. You can also create an ACL called “WideOpen” which does not block any sites. You may want to apply the WideOpen ACL during a standard lunch hour timeframe such as 12 - 1 p.m., and after working hours.

Next, define a schedule that tells iPrism when to apply each of the two ACLs, as shown below.

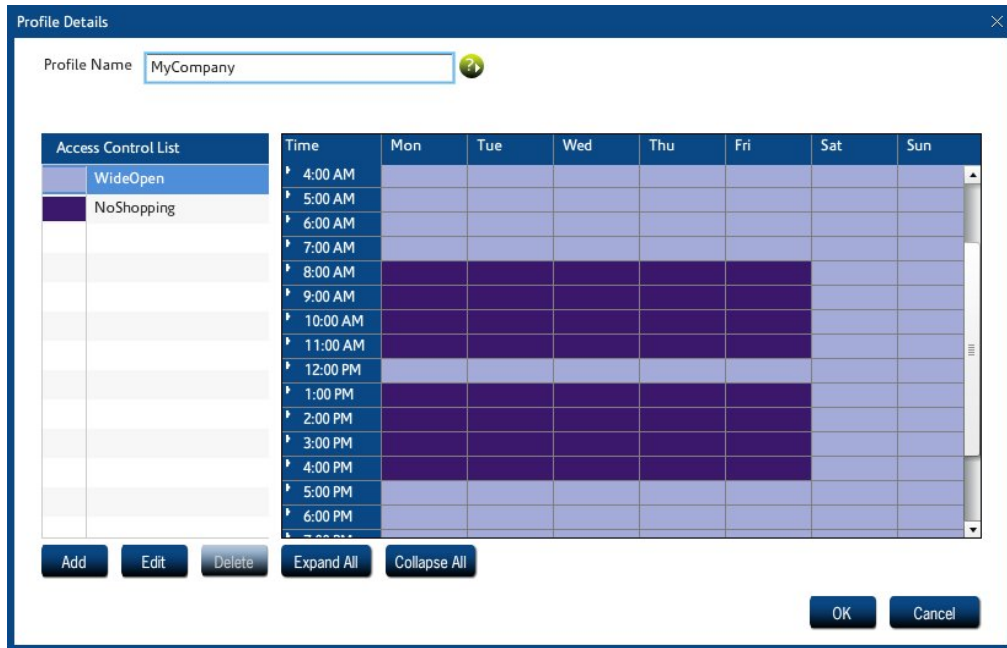


Figure 1. Profiles and Scheduling

In this example, the schedule applies to the entire company (Profile name = MyCompany). But sometimes you need to give different users different access rights. For example, the Purchasing department may legitimately need access to online shopping, and Finance may need access to online gambling. In addition, upper management and iPrism administrators may have access to everything.

iPrism uses two different types of profiles:

- Web Profiles are used to filter web surfing or HTTP/HTTPS traffic.
- Application Profiles filter IM and P2P usage.

Each profile is associated with a group of users. One way of identifying users is by the IP address of the machine they are using. For example, you can define a profile called “Sales”, which is mapped to the IP addresses in the range 192.168.77.0 to 192.168.77.255.

Users can also be identified by a username and password through an authentication process. There are a number of authentications available including NTLM (for Microsoft Windows users), Kerberos (for Microsoft Windows and Macintosh users) and LDAP (for Macintosh, UNIX, Linux, and Novell users).

Finally, you can manually add users to your iPrism. In practice, manual creation is usually only done for iPrism administrators and sub-administrators.

Assigning Profiles

Now that you have set up profiles, you need to learn how to associate a profile with the people to which it applies. The simplest way of doing this is to assign a profile to a set of IP addresses. Anyone using a machine which has one of these addresses will be assigned the same profile. This is useful when you have a lot of public or lab machines and wish to apply the same profile to everyone in the room. For example, if you're running a school, you can assign a profile called "KidSafe" to all the machines in the student lab, and assign a profile called "NoBlocking" to the teacher's offices.

You can also assign profiles to a set of authentication users. (Authentication means that you have a username to work with which has been validated by a password.) Although each web access message contains the IP address of the computer making the request, there is no user identification included in the message.



Note: This is not always true. If you configure your iPrism and user computers just right, you can create a system where each web access message will contain user identification. This complex form of configuration is discussed in [Users & Networks](#).

iPrism interfaces with Windows NTLM authentication as well as LDAP, which is used by UNIX, Linux, and Novell. If you want to use "user level" authentication, see [Users & Networks](#) for instructions on getting your iPrism working with your existing authentication system.

Getting Past Blocked Sites

Users have options when they encounter a blocked site. The Access Denied page provides two options for getting to a page that is being blocked by iPrism.

Override allows an administrator to log in. The administrator can then specify whether they want to override just the blocked page, the entire domain, or the whole blocked category. They can then select how long they want the override access to last before iPrism resumes normal blocking.

In addition, a user that has been granted override privileges (see [Managing Override Access](#)), can override the blocked page. Whether or not users can override blocked pages is configured and managed by the iPrism administrator.

If the user's request to unblock a site is granted, that site will be unblocked for all users if you are using a custom filter to grant access. See [Override Management](#) for detailed instructions on managing overrides and requests.

Request Access allows the user to “plead their case” to the iPrism administrator (or other authorized user with override privileges), who can subsequently grant or deny access to the page. The request is emailed to the iPrism administrator, who will then grant or deny the request (see [Granting Requests](#)).



Note: If Request Access is not available, then access is being denied by the active ACL in the current profile. You cannot request access to the site.

How iPrism Filters Internet Activity

iPrism filters both web traffic as well as IM and P2P services. Web traffic is filtered by checking each client's web request against an extensive database containing both URLs and IP addresses. This database also classifies sub-domains or specific URL paths, in addition to the top-level domain.

If the requested path belongs to a “blocked” category, then the user may see an “access denied” page instead (what the user sees is determined by how the iPrism administrator has chosen to handle requests to blocked categories; for specifics, see [Access Control Lists \(ACLs\)](#)). An Access Denied page notifies the client that the web page they tried to access belongs to a category which is currently being blocked.



Note: If the administrator has set General Options in the user's ACL to Deny all access to the web, the user will not see an Access Denied page.

The rules for IM and P2P filtering are based on protocols used by applications, but not by applications themselves. In other words, the iPrism will check the protocols used by applications to see if the traffic is permitted.



Note: Application filtering does not result in an Access Denied notification; the traffic is silently dropped. The administrator may want to communicate this behavior to end users, so they do not think the application is malfunctioning. IM/P2P activity can be viewed in the Application Detailed Report, available through the iPrism Report Manager (refer to the *iPrism Reporting Guide* at http://edgewave.com/support/web_security/documentation.asp).

Besides blocking web, IM, and P2P activity, the administrator also has the ability to simply monitor the traffic. For websites, you can select which categories are monitored and when this monitoring is to be done. For IM and P2P traffic, you can monitor based on the protocol used.

Monitoring allows you to see how your network is being used; for example, who visits which sites and how often. All the power to block or monitor access lies in the hands of the administrator. iPrism just gives them the means by which to do it.

Since a “one size fits all” approach to filtering is not suitable for most organizations, iPrism resolves the issue by using filtering profiles. The iPrism uses two different types of profiles - one for web traffic and another for non-web traffic. A profile tells iPrism which categories of traffic to block or monitor at a particular moment. You can create as many different profiles as you need and assign them to different users, or different networks and subnets.

How to create profiles and how to assign them to subnets or an entire network is covered in the following sections. Details on how to assign these profiles to users is covered in [Profiles & Filters](#).

Introduction to Profiles

Profiles are the elements within iPrism that determine what information is blocked, monitored, or passed through. There are two types of profiles:

- Web Profiles determine which websites are filtered.
- Application Profiles determine which instant message (IM) and peer to peer (P2P) traffic is allowed.

Profiles are at the very core of iPrism’s functionality. In addition to determining what gets blocked where, profiles also determine when traffic is blocked. Thus, you don’t have to manually change profiles to accommodate a situation where one group has access to the network for some part of the day and another group has access to it for another. The active profile can automatically switch the filtering criteria at a designated time of day, so you can be assured of having the protection you need, when you need it.

Profiles are flexible and accommodating, as each profile is actually made up of one or more individual filtering criteria, called an Access Control List (ACL). It is actually the ACL that specifies which traffic gets blocked or monitored. A profile can consist of a single ACL, which would provide the same degree of filtering all the time, or it can utilize several ACLs, allowing different degrees of filtering at specific times. This is how a single profile is able to provide a different level of filtering at various times of the day.

Proxy Mode

Proxy mode is the simplest, and is the preferred mode in which to operate an iPrism when testing, as well as when iPrism is installed “inside” a busy network with many different kinds of traffic. In proxy mode, the iPrism is installed right off the switch. End users and workstations are pointed to the iPrism via a proxy statement.

In proxy mode, iPrism uses a single internal interface to connect to the Internet. Only one (1) network (NIC) connection is used, as only the internal interface is connected to the local network. The iPrism acts as a filtering web proxy; web traffic that is explicitly directed to the iPrism is filtered.

In this configuration, HTTP and HTTPS requests are sent to the iPrism as proxy requests. The iPrism determines if the request should be allowed or blocked and, if it is allowed, forwards the request to the Internet. The reply goes back through the iPrism proxy to the user.

In this mode, the iPrism is not able to detect or regulate P2P traffic.

Proxy mode is best for testing, as since the iPrism is not placed in a network-critical location, any problems that occur will not jeopardize your company’s entire access to the Internet. You can fine-tune the profile and network settings and test the results before moving the system into a network-critical environment.

It also provides a way to demonstrate the capabilities of the iPrism before it is deployed for all users.

If you choose to deploy the system in proxy mode, all you have to do is to make the iPrism a proxy server for all your users. (This can be done through group policy settings, or through a system administrator edict.) You must also change your firewall rules to allow only the iPrism to access the Internet, preventing anyone who didn’t change their proxy settings from directly accessing the Internet.

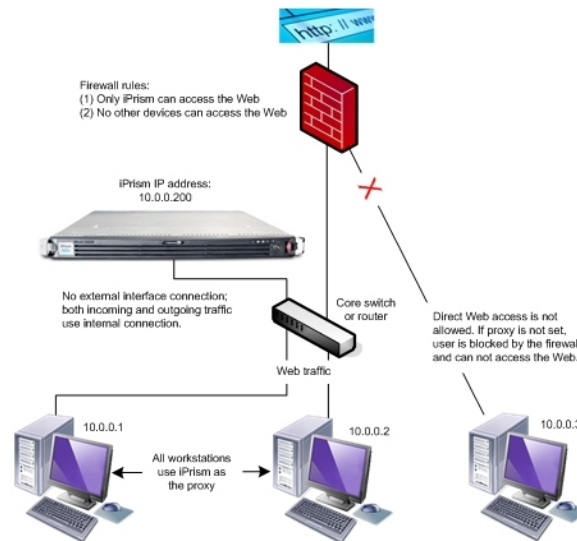


Figure 2. Deploying iPrism in Proxy Mode

Refer to the *iPrism Installation Guide* for detailed information.

Bridge (Transparent) Mode

In bridge (transparent) mode, the iPrism is an “in-line installation” which has 2 network (NIC) connections. This mode is recommended for full network production deployment.

In this mode, iPrism is installed between the firewall and the switch. All network traffic destined for the Internet (e.g., email and web) flows through the iPrism, and a single IP address is used by both interfaces. This is the preferred mode in which to deploy and operate an iPrism in production.

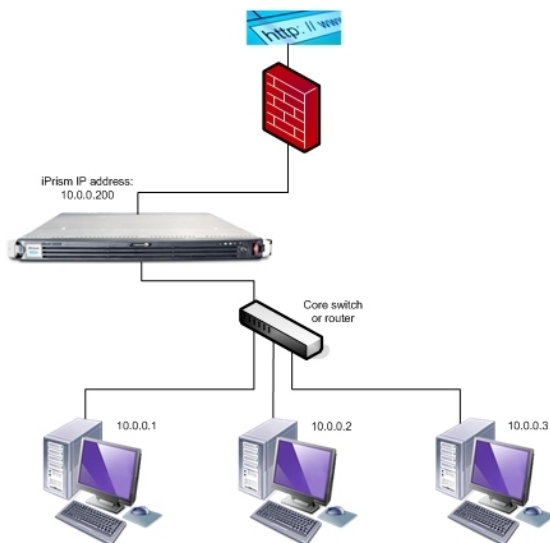


Figure 3. Deploying iPrism in Bridge (Transparent) Mode



Notes:

The iPrism can also act as a filtering web proxy when in bridge (transparent) mode. Users can configure their browsers to point at the iPrism, just as they do in proxy mode, although the iPrism is configured in bridge (transparent) mode. Web and Application traffic will be filtered for these users.

For instructions on how to configure a browser to point at the iPrism, refer to the *iPrism Installation Guide*.

Older versions of iPrism (Versions 3.6 and earlier) had an additional mode called Router mode. This mode had been discontinued. Bridge (transparent) mode is now used in all situations where the iPrism is used in an in-line network environment.

Using the Management Interface

The iPrism has a third network interface called the Management Interface. Normally you can administer your iPrism from any system connected to the internal network. You can configure the system to only accept configuration from the management interface. This allows you to create a secure subnet from which to control your iPrism.

Other uses of the management interface include:

- A secure way of transferring logging data from the iPrism to a management workstation. When you configure the iPrism to send you periodic reports or logging information, the information is transmitted in plain text. This means that anyone with a sniffer attached to your network could see that data. If you want to make your network extremely secure you can use the management interface to transfer this data on a secure network.
- High Availability. Paired iPrisms use the management interface to keep track of each other's current running status. Interrupting this link results in a situation where both iPrisms believe the other is not working, which results in both becoming active at the same time.

For more information on configuring and using the management interface, refer to the Knowledgebase article “How do I enable the Management Interface?” at www.edgewave.com/support/web_security/knowledgebases.asp.

Logging In and Out of iPrism

Logging into iPrism is done via the login page. It is recommended that you bookmark this page.

Within an iPrism session, you can log out via the Logout menu in the top right corner of the page. Select **Logout** from the dropdown menu.

Users on shared computers should log out when finished. If they do not, the next person who uses the machine will be able to access the Internet using the previous user's profile.



The image shows a login page for iPrism. At the top left is the EdgeWave logo, which consists of a blue square with a white stylized 'E' and the text 'EdgeWave™' to its right. Below this is the 'iPrism®' logo in a large, purple, sans-serif font. Underneath the logo is the word 'Login' in a smaller, blue font. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Below the password field is a blue link that says 'Forgotten Password'. To the right of the password field is a dark blue button with the word 'Login' in white text.

Figure 4. Logging in

Restarting and Shutting Down iPrism

- To restart iPrism, select **Restart** from the **Logout** menu in the top right corner of the page.
- To shut down iPrism, select **Shut Down** from the **Logout** menu in the top right corner of the page.

The iPrism Home Page

The primary method of administering the iPrism is via the configuration options available from the iPrism home page. This is available online through your iPrism after you have gone through the Installation Wizard (refer to the *iPrism Installation Guide* for steps on how to set up your iPrism through the Installation Wizard).

For the end users, the iPrism will remain invisible depending on how the administrator configures it in their network. The system may require them to authenticate themselves, and if they encounter a blocked site, it allows them to request that it be unblocked. But for the most part, it operates in the background, and users only become aware of it when they try to access a blocked site.

A variety of options are available from the iPrism home page which allow you to manage and administer the iPrism.

The following tools are available from the iPrism home page. Each tool has its own section in this guide:

- Profiles & Filters
- Users & Networks
- Reporting
- Maintenance
- System Settings
- System Status

For detailed information about and instructions how to use each tool, see the associated section.

CHAPTER 3 Profiles & Filters

This section describes how iPrism's profiles and filters work, and provides detailed procedures for creating and implementing your own filtering profiles. Instructions for controlling access to specific websites and other Internet services is also provided.

To access iPrism Profiles & Filters, click **Profiles & Filters** from the home page. A context menu lists the Filtering features.

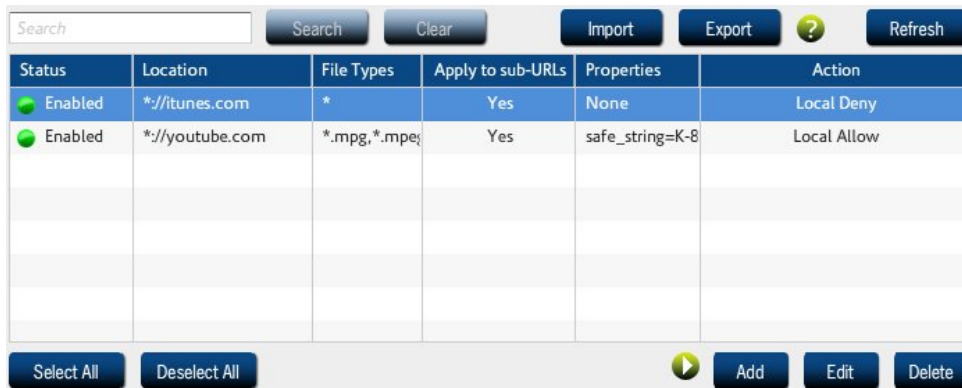
Custom Filters

Custom Filters provide a way of overriding or changing a specific site's rating on a long-term basis, and/or adding filters based on file extensions. A custom filter consists of one or more file extension types, and/or a site location (URL) and new rating, and will remain on the iPrism until deleted. Upon deletion, the URL will revert back to its original iGuard database rating. Custom filters allow you to restrict or allow access to any file type or website, not just those included in iPrism's URL database.

When you make a custom URL assignment, iPrism treats the URL as a member of that category and either allows or denies access to the site based on the active filtering profile.

In the Custom Filters section, you can import, add, edit, and delete custom filters. You can obtain the data for making a custom filter from several sources, including recent overrides or blocks, and personal requests made from users on the network. You can also create custom filters manually, entering the URL and ratings yourself.

1. From the iPrism home page, select **Profiles & Filters**, then **Custom Filters**.



Status	Location	File Types	Apply to sub-URLs	Properties	Action
Enabled	*://itunes.com	*	Yes	None	Local Deny
Enabled	*://youtube.com	*.mpg,*.mpeg	Yes	safe_string=K-8	Local Allow

Buttons: Select All, Deselect All, Add, Edit, Delete

Figure 5. Custom Filters

2. If you want to search for a custom filter, type all or part of the filter name and click **Search**.

Adding a Custom Filter

1. In the Custom Filters window click **Add**.

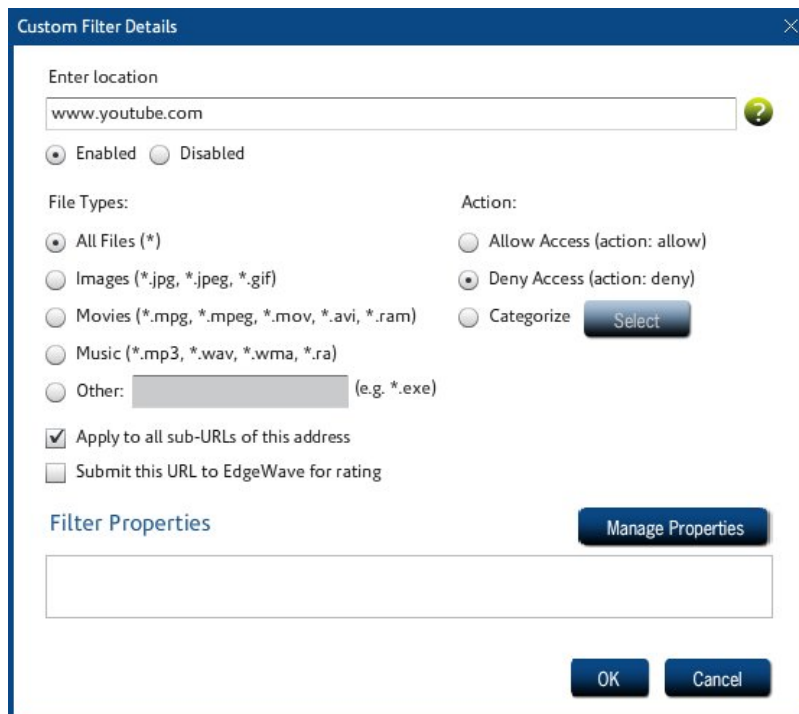


Figure 6. Filter Details

2. Make sure **Enabled** is selected, and type the URL to which this filter applies.
3. Select the file types to which this filter applies. If this filter applies to all file types, leave the default (**All Files (*)**) selected.
4. If all sub-URLs of this address are to be included in the filter, check **Apply to all sub-URLs of this address**.
5. If you want to have this URL submitted to the EdgeWave iGuard team for rating, check **Submit this URL to EdgeWave for rating**.
6. Select the appropriate action (**Allow Access**, **Deny Access**, or **Categorize**). If you select **Categorize**, click **Select** to assign this URL to an iGuard category.
7. If you want to specify properties for this filter, click **Manage Properties**. Select the applicable options and click **OK**.

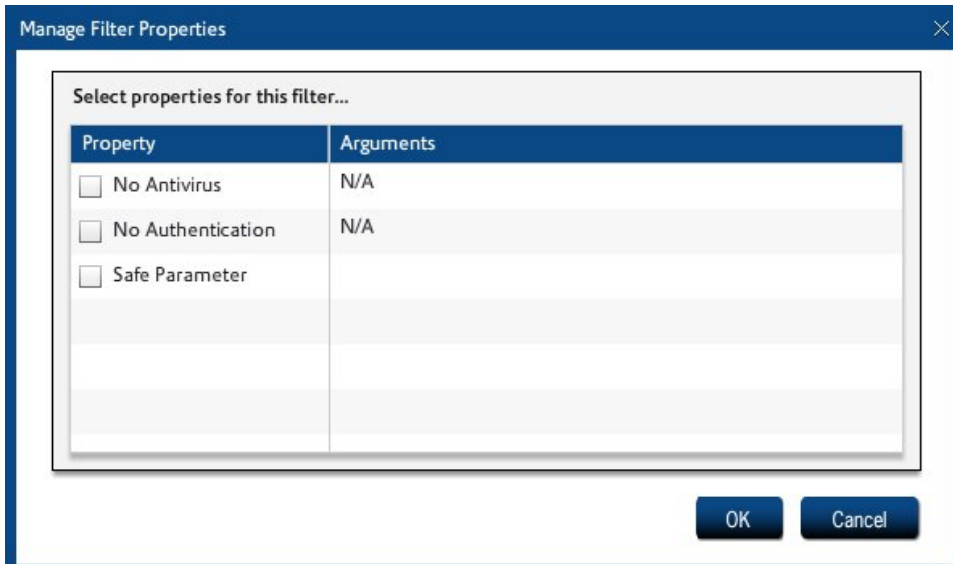


Figure 7. Manage Filter Properties

- **No Antivirus** - Turns off virus checking for this URL or file extension.
- **No Authentication** - Turns off authentication for this URL or file extension.
- **Safe Parameter** - Checks for the specified parameter and, if it matches this definition, allows the content. The safe parameter takes the form <parameter> = <definition> or just <definition>. Valid characters are: A-Z a-z 0-9 .!/_+=()[]{}@!#\$%*|-^

8. When you are finished, click **OK**.

Editing a Custom Filter

- Select a filter in the Custom Filters window and click **Edit**.

Deleting a Custom Filter

To delete a custom filter:

- In the Custom Filters window, select a filter and click **Delete**.

Importing and Exporting Custom Filters

To import a custom filter:

1. In the Custom Filters window, click **Import**.
2. Click **Yes** to confirm.
3. Locate the file and click **Open**.

To export a custom filter:

1. In the Custom Filters window, select a filter and click **Export**.
2. Enter a name for the file and click **Save**.

Profiles

Profiles allow or block requests or protocols. Profiles tell iPrism which categories of web or IM/P2P traffic to block and/or monitor at a particular moment, and allow different users to have different access rights. You can create as many different profiles as you need and assign them to groups of users, networks and users (local or remote).

Profiles assigned to a user are always applied to that user, regardless of which workstation they log into.

iPrism uses two types of profiles:

- Web profiles (for filtering web or HTTP traffic)
- Application profiles (for filtering IM/P2P traffic)

Profiles are the core of iPrism's functionality. In addition to determining what gets blocked where, profiles also determine when traffic is blocked. Thus, you don't have to manually change profiles to accommodate a situation where one group has access to the network for some part of the day and another group has access to it for another. The active profile can automatically switch the filtering criteria at a designated time of day, so you can be assured of having the protection you need, when you need it.

Profiles' flexibility stems from the fact that each profile is made up of one or more individual filtering criteria, called an Access Control List (ACL). An ACL tells iPrism what to do for each category of website and specifies which traffic gets blocked or monitored. For example, ACLs can block access to websites of an "adult" nature (and monitor any attempt to access them), monitor any accesses to site categorized as "nudity" (and allow the user to access them), and let all other requests through unmonitored and unblocked.

A profile can consist of a single ACL, which would provide the same degree of filtering all the time, or it can utilize several ACLs, allowing different degrees of filtering at specific times. This is how a single profile is able to provide a different level of filtering at various times of the day.

For detailed information about ACLs and how they work, see [Access Control Lists \(ACLs\)](#).

How iPrism Uses Profiles

There are different ways that iPrism can make use of a filtering profile, depending on how iPrism is configured on your network and whether or not you are using authentication:

- **Filtering by groups or local users, based on username.** This type of filtering associates a profile with a given user. It does not matter which machine they use, the user will always get the same profile, as it is based on their username.

User-level filtering works well in environments where you want some people to have significantly more (or less) access to the web than others. It also offers an additional layer of protection because the user's profile applies to them no matter which workstation they log into.

Before a user can access the Internet s/he must be authenticated. iPrism provides a variety of authentication methods and can access authentication servers like NTLM (for Microsoft Windows users), Kerberos (for Microsoft Windows and Macintosh users) and LDAP (for Macintosh, UNIX, Linux, and Novell users). See [Directory Services](#) for more information on authentication.

- **Network-level filtering, based on a range of IP addresses.** For network-level filtering, you specify a set of IP addresses and associate a profile with them. For example, if your iPrism is for a library, you can have one profile for the computers in the children's reading area, and another for the adult library users.



Note: If a user has been successfully authenticated and their username is not included in an iPrism group, iPrism will fall back to network-level filtering; i.e., they will be assigned a profile based on their workstation's IP address. Users that cannot be authenticated will be blocked from all Web requests and IM/P2P protocol traffic.

- **Machine-level filtering, based on Machine ID, that applies only to remote users.** The Machine ID identifies a particular remote machine and defines a policy for all users on that machine. It is treated like a username, and by default is the hostname of the machine when the client is installed. For detailed information, see [Remote Users](#).

iPrism's Default Profiles

iPrism ships with five preconfigured (default) profiles, two for web filtering and three for application filtering. This allows you to realize some level of filtering while you are learning how to create your own profiles. You may find these to be useful and decide to keep them or, once you start creating your own profiles, you may choose to edit or delete them. The preconfigured profiles are as follows:

- **PassAll:** This profile allows access to any site without monitoring.
- **BlockOffensive:** This web filtering profile blocks and monitors access to sites containing pornography, profanity, violence, bomb-making, etc.
- **BlockP2P:** Blocks all P2P traffic only.
- **BlockIMP2P:** Blocks all IM and P2P traffic.
- **PassIMP2P:** Blocks no IM or P2P traffic.

Web Profiles

Web profiles are used to filter web surfing or HTTP/HTTPS traffic.

To work with web profiles:

1. From the iPrism home page, select **Profiles & Filters**, then **Web Profiles**.
2. When you have finished working with web profiles, click **Save** to save your changes.
3. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Profile Name	ACLs
PassAll	ACL 1
BlockOffensive	ACL 1

Select All Deselect All  Add Copy Edit Delete

Figure 8. Web Profiles

Adding a Web Profile

To add a profile:

1. Click **Add** in the main Web Profiles window.
2. Enter a name for the profile.
3. Add new Access Control Lists (ACLs) or edit existing ACLs. For details, see [Access Control Lists \(ACLs\)](#)
4. For each ACL that is part of this profile, assign the days/times the ACL is in effect.
 - a. Select an ACL.
 - b. Click next to a time and drag to highlight the time blocks when the ACL is in effect.

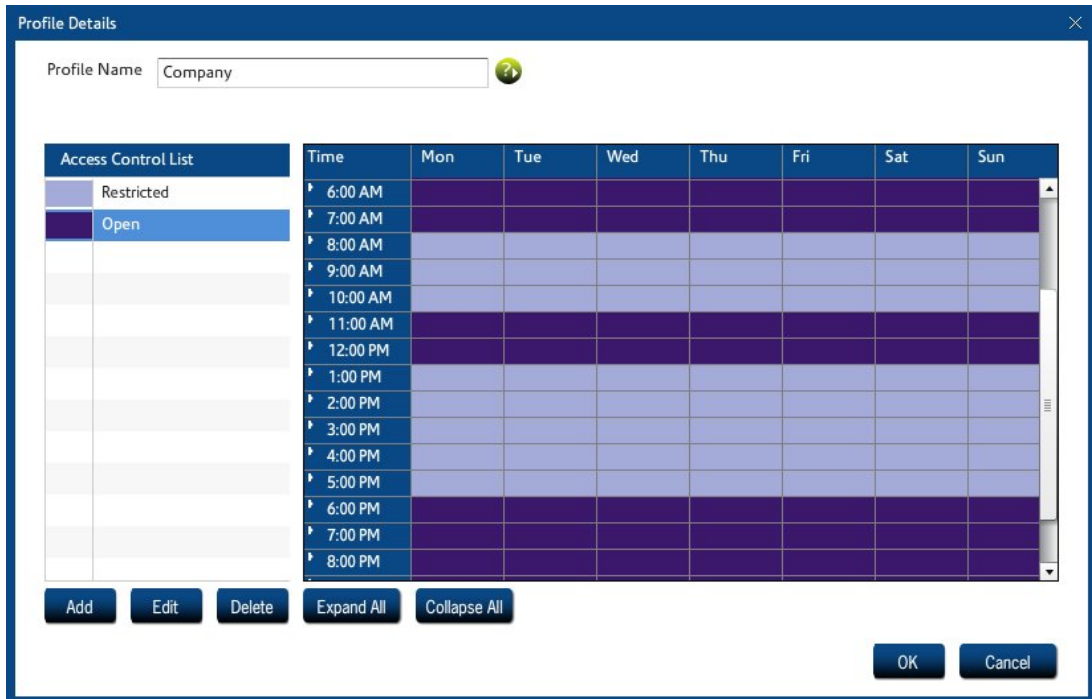


Figure 9. ACL Times

5. Click **OK** to add the web profile.

Copying a Profile

To create a new profile by copying an existing profile:

1. Select a profile in the main Web Profiles window and click **Copy**.
2. Enter a name for the new profile.
3. Add new Access Control Lists (ACLs) or edit the existing ACLs. For details, see [Access Control Lists \(ACLs\)](#)



Note: If any of the ACLs contain quotas and/or warnings, those are not copied. Quotas and warnings must be assigned to each ACL within the new profile.

4. For each ACL that is part of this profile, assign the days/times the ACL is in effect.
5. Click **OK** to add the web profile.

Deleting a Profile

When you delete a profile, you need to specify a replacement profile.

1. Select a profile in the main Web Profiles window and click **Delete**.
2. Select a replacement profile from the dropdown list and click **OK**.



Important: Assigning a different profile may dramatically change what the user sees. For specific information about the default profiles and what they allow and do not allow, see iPrism's Default Profiles.

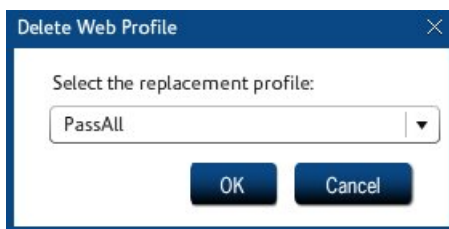


Figure 10. Deleting a Profile

Application Profiles

Application profiles filter IM and P2P usage.

To work with application profiles:

1. From the iPrism home page, select **Profiles & Filters**, then **Application Profiles**.
2. When you have finished working with application profiles, click **Save** to save your changes.
3. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Profile Name	ACLs
BlockP2P	ACL 1
BlockIMP2P	ACL 1
PassIMP2P	ACL 1

Select All Deselect All  Add Edit Copy Delete

Figure 11. Application Profiles

Adding an Application Profile

To add a profile:

1. In the Application Profiles window, click **Add**.
2. Enter a name for the profile.
3. Add new Access Control Lists (ACLs) or edit existing ACLs. For details, see [Access Control Lists \(ACLs\)](#)

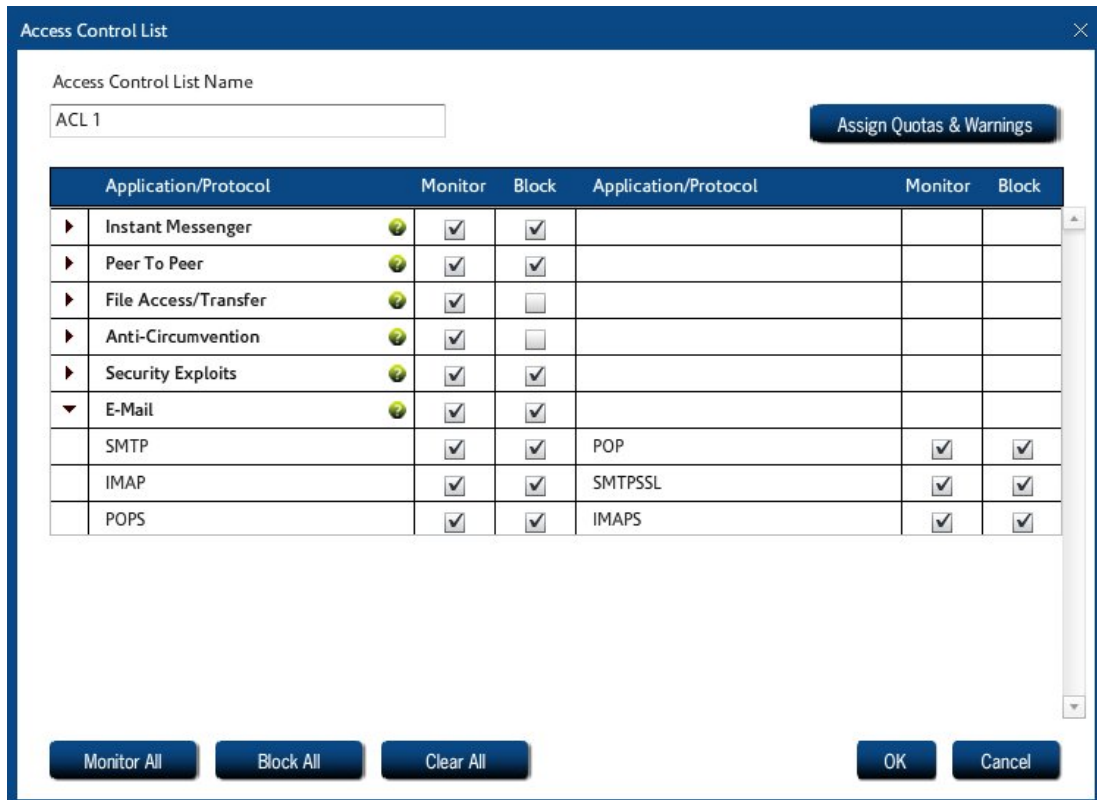


Figure 12. Application ACL

4. For each ACL that is part of this profile, assign the days/times the ACL is in effect.
 - a. Select an ACL.
 - b. Click next to a time and drag to highlight the time blocks when the ACL is in effect.

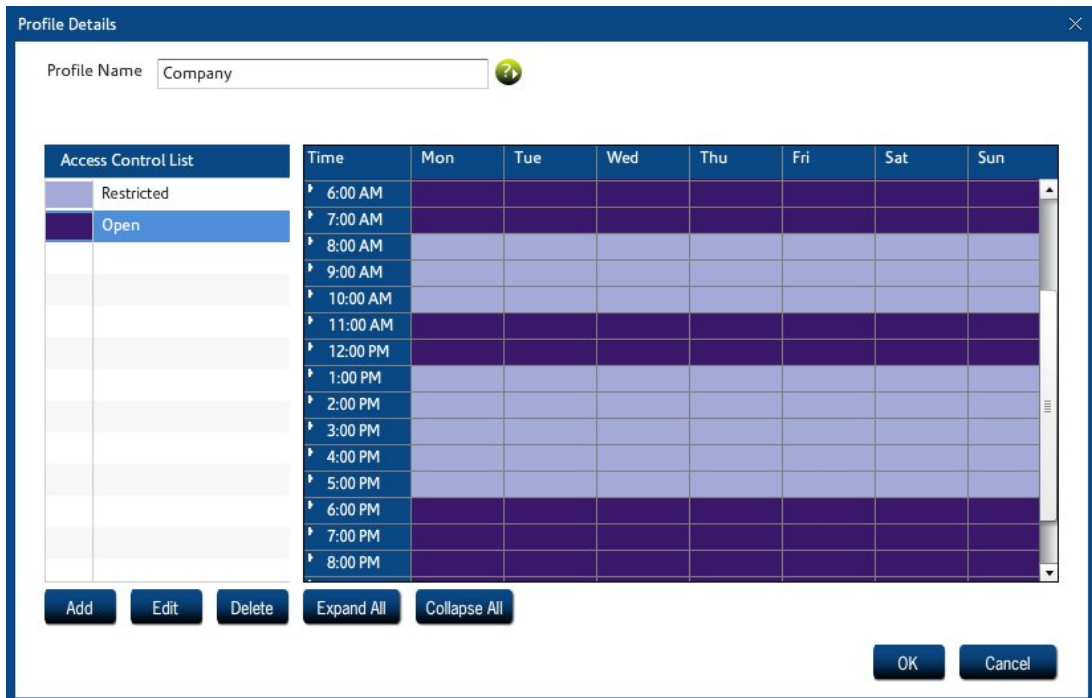


Figure 13. ACL Times

5. Click **OK** to add the application profile.

Copying an Application Profile

To create a new profile by copying an existing profile:

1. In the Application Profiles window, select a profile and click **Copy**.
2. Enter a name for the new profile.
3. Add new Access Control Lists (ACLs) or edit the existing ACLs. For details, see [Access Control Lists \(ACLs\)](#)
4. For each ACL that is part of this profile, assign the days/times the ACL is in effect.
5. Click **OK** to add the application profile.

Deleting an Application Profile

When you delete a profile, you need to specify a replacement profile.

1. In the Application Profiles window, select a profile and click **Delete**.
2. Select a replacement profile from the dropdown list and click **OK**.



Important: Assigning a different profile may dramatically change what the user sees. For specific information about the default profiles and what they allow and do not allow, see iPrism's Default Profiles.



Figure 14. Deleting a Profile

Authentication and Assigning Profiles to Users

Users can be authenticated on iPrism in a number of ways. See [Directory Services](#) for detailed information and instructions.

Assigning Profiles to a Set of IP Addresses (Workstations)

For detailed instructions on how to assign a profile to an individual IP address or a range of IP addresses, see [Networks](#).

For detailed instructions on how to assign a profile to remote or mobile users, see [Remote Filtering](#).

Quotas and Warnings

iPrism's Quotas and Warnings keep users and administrators aware of specific Internet-related events.

- Email Alerts send an email notification to one or more defined email addresses each time a certain type of event occurs.

Adding an Email Alert

1. From the Email Alerts window, click **Add**.
2. Enter a name for the email alert.
3. Select **Enabled** to turn on the alert or **Disabled** to turn it off (save for later use).
4. From the Monitoring dropdown list, select an option:
 - **Any**: The access of any user (or from any workstation) will be considered when determining if alert conditions are met.
 - **User**: Only the specified user will be tracked for alert consideration. Enter the user's iPrism username or the workstation's IP address in the associated field.
 - **Profile**: Only users monitored by the profile selected from the dropdown list will be considered.
 - **IP Range**: Only workstations that have an IP address within the specified IP range will be monitored for alert events. To track a single workstation, type the workstation's IP address in both the **IP Start** and **IP End** fields.
5. Check **Group Utilization for Monitoring Selection** if you want the threshold to be based on the total usage for all profiles or IPs in the selected range. Leave this unchecked for each individual profile or IP address to be subject to the threshold defined below.
6. In the **Threshold** frame, select the criteria, value, and time span that will cause an email alert to be sent.
 - **Bandwidth (KB)**: An email alert will be sent when the specified amount of data is accessed within the selected time span.
 - **Pages**: An email alert will be sent when the specified number of pages are accessed within the selected time span. A page is defined as an HTML access with a MIME content type of `text/*`. This includes blocked attempts as well.
 - **Hits**: An email alert will be sent when the specified number of web accesses of any content type occur within the selected time span. Generally, Pages are a more useful selection type than Hits, since Hits will track data for every access (images, etc.), even though they all fall within a single page.
 - **Session Duration (minutes)**: An email alert will be sent when the specified number of minutes are spent online within the selected time span. Since it is impossible for computer software alone to track exactly how long someone spends browsing at a particular site, real-world usage heuristics have been used to approximate the time spent browsing.

7. In the ACL Categories frame, click **Select** and choose the categories that will trigger the alert. Click **OK** to return to the Email Alerts window.
8. Type the email address(es) of the users to receive the email alert. Use commas to separate multiple email addresses.
9. Click **OK** to save this email alert.

Email Alert - Add

Name Enabled Disabled

Monitoring

Group Utilization For Monitoring Selection

Threshold

Criteria	Value	Time span
<input type="text" value="Pages"/>	<input type="text" value="5"/>	<input type="text" value="30 mins"/>

ACL Categories

Selected categories to count towards threshold

Currently Selected Categories

alt/new_age,art/culture,cult,family issues,government,news,politics,religion,social issues,classifieds,alternative

Email Notification

Email Recipients (Comma delimit multiple recipients)

Figure 17. Adding an Email Alert

Editing an Email Alert

1. In the Email Alerts window, select the alert to edit.
2. Click **Edit**.
3. Make changes as needed.
4. Click **OK** to save your changes.

Deleting an Email Alert



Note: If you might use the email alert later, you can deactivate it instead of deleting it. To deactivate an alert, click the green indicator on the far left. The indicator turns red to show the email alert is disabled.

To delete an email alert:

1. In the Email Alerts window, select the alert to delete.
2. Click **Delete**.
3. Click **Yes** to confirm.

Quotas

Quotas are defined limits for Internet-related events. You set them up based on the kinds of access you want to limit.

Once created, quota enforcement can be turned on and off as desired, so you can control when users are subject to each quota.

To configure quotas:

1. From the iPrism home page, select **Profiles & Filters**, then **Quotas & Warnings**.
2. Select the **Quotas** tab.

The requested page is restricted by a quota

Your organization has chosen to limit viewing of this site (http://oc-sge-master1.stbernard.com/html/test_uris/sports/test_sports_100k_page.html), due to the rating of its content (sports), and a quota value. If you choose to continue to the requested page, the content will be applied toward this quota.

The requested page is counted toward a quota for rating sports.

Time quota will be reevaluated: 2011-11-17 00:00:00.

Percentage of quota reached: 100

If you feel that you have received this page in error, please contact Your System Administrator with the following details:

- User = [Unknown]
- IP = 172.17.20.105

[Override / Request Access](#) [More Info](#)

Figure 20. Quota Reached

Adding a Quota

1. From the Quotas window, click **Add**.
2. Enter a name for the quota.
3. Select **Enabled** to turn on the quota or **Disabled** to turn it off (save for later use).



Note: When a quota is disabled, the ACL associations still appear even though the quota is not being enforced. iPrism will activate the quota enforcement for those ACLs when the quota is enabled.

4. In the **Threshold** frame, specify the quota parameters.
 - **Criteria:** Choose the measurement to be used for assessing the quota.
 - **Value:** Enter the number of units (depends on the criteria) for this quota.
 - **Reset:** Choose the duration of each unit for this quota. For example, if you chose Session Duration as the criteria, and 60 for the value, choosing 1 day for the reset value means the quota is reached if the user's session is 60 minutes in one day. The quota resets at the end of the day so that the user has up to 60 minutes each day.
 - **Relative threshold:** The user gets notified when this percentage of the quota has been reached.
5. In the ACL Categories frame, click **Select** and choose the categories to be applied to the quota. Click **OK** to return to the Quotas window.



Note: The quota calculation is a total of the usage in all the categories selected. For example, a 100KB quota for selected categories of games and sports will reach the quota if games is at 30KB and sports is at 70KB.

6. Type the email address(es) of the users to receive email notification when the quota has been reached. Use commas to separate multiple email addresses.
7. Click **OK** to save this quota.

Quota - Add

Name Enabled Disabled

Threshold	Reset Relative	Relative Threshold
Criteria	Threshold Level to	Level to Trigger
Session Duration [min]	0% Every:	Notification Page:
<input type="text" value="60"/>	<input type="text" value="1 day"/>	<input type="text" value="50%"/>

ACL Categories

Selected categories to count towards threshold

Currently Selected Categories

alt/new_age,art/culture,cult,family
issues,government,news,politics,religion,social issues,classifieds,alternative

Email Notification Enabled Disabled Note: Triggered once at 100% relative threshold level.

Email Recipients (Comma delimit multiple recipients)

Figure 21. Adding a Quota

Once the quota has been defined it can be assigned to an access control list. See [Creating a New Web ACL](#) for more information.

Editing a Quota

1. In the Quotas window, select the quota to edit.

2. Click **Edit**.
3. Make changes as needed.
4. Click **OK** to save your changes.

Deleting a Quota



Note: If you might use the quota later, you can deactivate it instead of deleting it. To deactivate a quota, click the green indicator on the far left. The indicator turns red to show the quota is inactive.

To delete a quota:

1. In the Quotas window, select the quota to delete.
2. Click **Delete**.
3. Click **Yes** to confirm.

Warnings

Warnings are notifications about specific Internet-related events. You define which events generate warnings and how often those warnings are shown to the user.

Once created, warnings can be turned on and off as desired, so you can control when the warning messages appear.

To configure warnings:

1. From the iPrism home page, select **Profiles & Filters**, then **Quotas & Warnings**.
2. Select the **Warnings** tab.

Status	Name	Frequency	ACL Categories	Profile/ACL Association
Enabled	Health	4 hrs	alcohol/tobacco,drugs,health,adu...	
Enabled	Recreation	2 hrs	entertainment,gambling,games,h...	

Figure 22. Warnings

When a user accesses a page that has a warning attached to it, the following message appears.

Viewing of the requested page will be reported to your administrator

Your organization has chosen to audit viewing of this site (http://oc-sge-master1.stbernard.com/html/test_urls/drugs/test_drugs_100k_page.html), due to the rating of its content (drugs).

If you choose to continue to the requested page, it will be listed in a report to your administrator.

If you feel that you have received this page in error, please contact Your System Administrator with the following details:

- User = [Unknown]
- IP = 172.17.20.105

Continue

Figure 23. Warning

This message can be customized. See [Customizable Pages](#).

Adding a Warning

1. From the Warnings window, click **Add**.
2. Enter a name for the warning.

3. Select **Enabled** to turn on the warning or **Disabled** to turn it off (save for later use).



Note: When a warning is disabled, the ACL associations still appear even though they are not affected. iPrism will activate the warnings for those ACLs when the warning is enabled.

4. In the **Frequency** frame, specify how often the trigger should reset. For example, 2 hrs means that, if the selected category generates a warning, the user will not receive another warning for 2 hours.
5. In the ACL Categories frame, click **Select** and choose the categories to be applied to the warning. Click **OK** to return to the Warnings window.



Note: The warning will appear the first time a page from any category on the list is accessed. It will not appear for pages in other categories from the same list, within the reset trigger timeframe. The warning notification lists all of the categories to which the warning applies.

6. Click **OK** to save this warning.

Warning - Add

Name Enabled Disabled

Frequency Note: Triggered once after first hit.

Reset Trigger for Warning Page Every: ▼

ACL Categories

Selected categories that apply towards this Warning

Currently Selected Categories

entertainment,gambling,games,hobbies/interest,sports,travel,mature humor,digital music,television/movies,music,Digital Media,radio

Figure 24. Adding a Warning

Once the warning has been defined it can be assigned to an access control list. See [Creating a New Web ACL](#) for more information.

Editing a Warning

1. In the Warnings window, select the warning to edit.
2. Click **Edit**.
3. Make changes as needed.
4. Click **OK** to save your changes.

Deleting a Warning



Note: If you might use the warning later, you can deactivate it instead of deleting it. To deactivate a warning, click the green indicator on the far left. The indicator turns red to show the warning is inactive.

To delete a warning:

1. In the Warnings window, select the warning to delete.
2. Click **Delete**.
3. Click **Yes** to confirm.

Access Control Lists (ACLs)

Access Control Lists (ACLs) are the building blocks that make up every filtering profile. They alone determine which types of traffic will get blocked, monitored and/or allowed to be accessed. Unlike profiles, ACLs are not assignable to users or networks; they only exist in the context of a profile.

When creating a new profile, a default ACL (called ACL 1) is always provided. When a profile is created, this is the default value used for all time blocks. You can create new ACLs and schedule them by applying them to the time grid in the profile.

For each category you have the option to monitor access or block it completely. You can use email alerts, quotas, and warnings to send notifications to the administrator and/or user, or to block access (quotas) based on time or bandwidth.

Creating a New Web ACL

1. Create or edit a web profile. For details, see [Web Profiles](#).
2. In the Profile Details window, click **Add**.

3. Enter a name for the ACL.

Access Control List Name

ACL 2

Assign Quotas & Warnings

General Options

Deny all access to the web

Force browsers to use safe search

Access Denied Page Options

Show these options when a page is blocked:

Override link Request access link

Category	Monitor	Block	Category	Monitor	Block
▶ sex	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ questionable activities	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ security exploits	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ society	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ internet	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ business	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ health	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ recreation	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ education	<input checked="" type="checkbox"/>	<input type="checkbox"/>			

Monitor All Block All Clear All OK Cancel

Figure 25. Web Access Control List

4. Select General Options.

- **Deny all access to the web:** No web traffic is allowed for this ACL. This is a quick way to set all categories (even local allowed) to **Blocked**. This is the equivalent of setting everything to **Blocked/Monitored**. If this option is selected, an Access Denied page will not be displayed to users when they access the Internet.
- **Force browsers to use safe search:** If this is enabled, the iPrism will enable safe search for Google, Yahoo, Alltheweb, Hotbot, Lycos, Dogpile, and Excite. Safe Search will be turned on even if the user tries to do a search with this feature turned off.

5. Select Access Denied Page Options (web profiles only). These determine what will be shown when a user encounters a blocked page.

- **Override link:** The Access Denied page will include an **Override** button, allowing users with override privileges to gain access to the page.
 - **Request access link:** The Access Denied page will include a **Request Access** button, allowing users to petition the administrator for access when they are blocked from a site.
6. If you want to assign quotas and warnings to this ACL, click **Assign Quotas & Warnings**, select the quotas and warnings to use, and click **Apply**. For more information about defining quotas and warnings see [Quotas and Warnings](#).



Note: For email alerts, quotas, or warnings to be in effect for a category, that category must be monitored.

7. Check the categories you want to monitor and/or block. You can select individual categories or block/monitor all categories.
- **Monitor:** Web pages are supplied to the user. Each access is recorded and can be viewed using the reporting system or the Real-Time Monitor. Click **Monitor All** to monitor all categories.
 - **Block:** Web traffic is blocked for this ACL. Click **Block All** to block all categories.
8. Click **OK** to save the new ACL.

Creating a New Application ACL

1. Create or edit an application profile. For details, see [Application Profiles](#).
2. In the Profile Details window, click **Add**.
3. Enter a name for the ACL.
4. Check the categories you want to monitor and/or block. You can select individual categories or block/monitor all categories.
 - **Monitor:** Applications are supplied to the user. Each access is recorded and can be viewed using the reporting system or the Real-Time Monitor. Click **Monitor All** to monitor all applications.
 - **Block:** Application is blocked for this ACL. Click **Block All** to block all applications.
5. Click **OK** to save the new ACL.

Editing an ACL

1. Create or edit a web profile or an application profile. For details, see [Web Profiles](#) or [Application Profiles](#)
2. In the Profile Details window, select the ACL to edit and click **Edit**.
3. Make your changes and then click **OK**.

Deleting an ACL

1. Create or edit a web profile or an application profile. For details, see [Web Profiles](#) or [Application Profiles](#)
2. In the Profile Details window, select the ACL to delete and click **Delete**
3. If you are prompted to confirm, click **Yes**.
4. Click **OK** to close the application profile.

Lock ACL

Lock ACL provides a way for the SuperUser and the Global Policy Administrator to globally enforce access restrictions on the same categories. By using Lock ACL, categories can be marked to be blocked and/or monitored (e.g., pornography or nudity). Lock ACL settings override those in individual profiles.


If a category is blocked and/or monitored in Lock ACL and a user requests an override for a blocked page in that category, it will show up as Locked in Pending Requests (see [Pending Requests](#)). Lock ACL will have to be turned off for that category before the Pending Request can be granted.



Note: Lock ACL is only available to the SuperUser, Global Policy Administrator, and Full Access Administrator.

To lock ACLs:

1. From the iPrism home page, select **Profiles & Filters**, then **Lock ACL**.

Category Locks 

You have the ability to lock settings of categories nobody will be able to modify. Any locks that you make to the Web or Application Access Control List (ACL) will be applied to all existing and new ACLs.

Lock ACLs in each profile

Web Lock ACL Application Lock ACL

Advanced

The denied page that results from a locked category access can also have the presence of the override and request access links locked OFF. Select the link preferences below:

Override link:

- block page gets no override link
- defer override link presence to Web profile setting
- defer override link presence to Web profile setting, but login only allowed for administrators with roles: Full Access, Global Policy Admin, OR Super Admin

Request access link:

- block page gets no request access link
- defer request access link presence to Web profile setting

Figure 26. Lock ACL

2. Check **Lock ACLs in each profile**.
3. Click **Edit** next to the type of ACL you want to lock (Web Lock ACL or Application Lock ACL).
4. Make your changes and then click **OK**.
5. Select whether the Override link will appear on the Access Denied page. You can specify that it does not appear, or you can specify that this is determined by the Web Profile setting (and restrict the login).
6. Select whether the Request access link will appear on the Access Denied page. You can specify that it does not appear, or you can specify that this is determined by the Web Profile setting.
7. Click **Save** to save your changes.
8. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Current Overrides

Override access allows users with the required privileges to be able to overrule the active filtering policy and gain access to web pages that would otherwise be blocked. In iPrism, override privileges are determined by a user's administrator level assignment.

To view current overrides:

- From the iPrism home page, select **Profiles & Filters**, then **Current Overrides**. The iPrism administrator can review all of the currently active overrides and revoke them, as desired.

Expires	Administrator	Profile	Rating Category	User(s)/Workstation	URL/Domain
10/05/09 3:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
11/05/09 4:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
12/05/09 5:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
13/05/09 6:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
14/05/09 7:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
15/05/09 8:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
16/05/09 9:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
17/05/09 10:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
18/05/09 11:00AM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
19/05/09 0:00PM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
20/05/09 1:00PM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
21/05/09 2:00PM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
22/05/09 3:00PM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
23/05/09 4:00PM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au
24/05/09 5:00PM	Admin	Any	News	Bob Smith (172.0.0.1)	http://www.news.com.au

Figure 27. Current Overrides

The following columns are available on the Current Overrides page:

- Expires:** The date and time at which the override will expire.
- Administrator:** The user who created the override. This is only relevant when using user authentication. The override is only valid for the indicated user. When user authentication is not used, or when the override is valid for all users, this column indicates Any.
- Profile:** The profile to which the override applies. If this column reads Any, the override applies to all profiles.

- **Rating Category:** The filtering profile affected by the override (e.g., News). This may be the name of the profile overridden by the user, or it may read Any if the override is relevant to a network, not a profile.
- **User(s)/Workstation:** The user, workstation, or range of workstations affected by the override, using the IP addresses. If only one workstation is affected, this column shows its IP address. If several workstations are affected, this column shows the IP network range.
- **URL/Domain:** The URL (single page or domain name) affected by the override. If the override was performed for a list of categories instead of a URL, the categories affected is displayed.

To revoke one or more overrides:

- In the Current Overrides window, select the override(s) and click **Revoke**.

Pending Requests

When a user is surfing the Internet and receives an Access Denied message for a blocked page they can click **Request Access** to send a message to the iPrism administrator to explain why they need access to the site (see [Overriding a Blocked Web Site](#)). The administrator can review the request and decide whether or not to grant access. No administration privileges are required to submit an access request. If a request is granted, the requesting user will be allowed to access the site.



Note: The Request Access link appears in the Access Denied message if the administrator has checked **Request Access link** when setting up the ACL. For details, see [Creating a New Application ACL](#)

To view a list of pending requests:

- From the iPrism home page, select **Profiles & Filters**, then **Pending Requests**.

Date/Time	URL/Domain	Category	User(s)/Workstation	Locked
2009-10-01 10:00 AM	http://www.news.com	News	Jane Doe (172.0.0.1)	
2009-10-01 11:00 AM	http://www.amazon.com	Consumer Shopping	Jane Doe (172.0.0.1)	
2009-10-01 12:00 PM	http://www.cnn.com	News	John Roe (172.0.1.1)	

Buttons: Select All, Deselect All, Refresh, Grant, Deny

Figure 28. Pending Requests

Granting Requests

1. In the Pending Requests window, select the request(s) and click **Grant**.



Note: You cannot grant requests that are locked, which will be indicated by the Locked column. Locked requests are set up via Lock ACL (see Lock ACL), and can only be unlocked if the administrator unlocks them via the Lock ACL.

2. In the **Grant Request** page, choose Override Options.
 - **Apply the override to:**
 - **User's current workstation:** Applies the override only to the given IP address
 - **Everyone:** Applies the override to everyone.
 - **Override duration:**
 - **Unlimited:** Allows override access for an unlimited period of time
 - **() days:** By typing a number in the box, specifies a certain number of days for which this override will be valid.
 - **Allow access to:**
 - **Path:** Allows access *only* to the given path
 - **Domain:** Allows access to everything within the given domain
3. Click **Grant** to grant the request(s).
4. Click **Save**.
5. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Denying Requests

To deny pending request(s):

1. In the Pending Requests window, select the request(s) and click **Deny**.
2. Click **Deny** to deny the request.
3. Click **Save**.

4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Recent Blocks

You can view a list of the 100 most recently blocked pages by selecting **Profiles & Filters**, then **Recent Blocks**.

If you want to allow access to any of these blocked pages, select the page and click **Allow Access**.

Remote Filtering

iPrism provides comprehensive Internet security for off-premises flexible policy enforcement and robust reporting.

- Once the iPrism Remote Filtering Client software is installed (see the *iPrism Remote Filtering Client Guide*), mobile laptop and remote users are easily managed by iPrism without the client being connected directly to a network containing iPrism. There's no need to set up a DMZ deployment or access the iPrism via VPN; thus, there is low latency and minimal impact on network bandwidth.
- After mobile laptop and/or remote users are provisioned (see [Remote Users](#) for instructions), policies are enforced no matter where the users are physically located. Policies are enforced at the machine level; therefore, if multiple users use a particular laptop, the same policy will be applied to all of them.
- The iPrism Remote Filtering clients are location-aware. So, whether users are on-premises or off-network, their Web activities are filtered and tracked. Location awareness enables flexible policy enforcement based on the laptop's location relative to the corporate network. In addition, there is no added security risk or point of failure.
- iPrism Remote Filtering allows employee Web surfing to be easily managed, regardless of location and time. Administration tasks, policy enforcement, and drill-down reporting are available, as are iPrism policy provisioning and fallback options.
- The client installation is tamper-proof and available for Windows 32- and 64-bit clients, as well as Mac OS X.

- Unlike other remote Web filters, iPrism helps conserve network bandwidth. Because iPrism Remote Filtering doesn't require the use of a DMZ deployment, there is no need for additional hardware. Once mobile laptop and/or remote users are provisioned from the iPrism, there is no need to connect to the iPrism directly, eliminating the need to use your VPN. The EdgeWave Data Center functions as an intermediary for the iPrism and the remote client.
- In reports, the remote filtering system attempts to adjust the time of events on remote clients to the local time zone of the iPrism. This is so that remote events can be viewed side-by-side with local events as they occurred.
- For iLearn video tutorials on Remote Filtering, go to http://edgewave.com/support/web_security/recorded_webinars_ilearn.asp

Using Remote Filtering

To use Remote Filtering:

1. Upload a remote filtering license key (for details, see [License Key](#)).
2. Enable Remote Filtering and download the client software. See [Enabling Remote Filtering](#).
3. Set up users in **Users & Networks > Remote Users** (see [Remote Users](#)):
 - Set up default actions and profiles
 - Import or add remote users
4. Install the remote filtering client software on the remote users' computers (see the *iPrism Remote Filtering Client Guide*).

Enabling Remote Filtering

Once you have uploaded a remote filtering license key, logged out of your iPrism, and logged back in, complete the following steps to enable remote filtering.

1. From the iPrism main window, select **Profiles & Filters**, then **Remote Filtering**.

Remote Filtering

Enable Remote Filtering

Administrator Contact Information

This page has been blocked per school policy.
Pete Peters, IT Administrator, Peterson HS

Download Client Auth File

Download Client Software

Remote Filtering Network Exceptions

Exceptions

Remote Filtering Logs

Automatic Log Retrieval Interval

Every 15 Minutes

Initiate Log Download

For legacy remote filtering, click [here](#) to access the settings by which external users can proxy to this iPrism.

Figure 29. Remote Filtering

2. Check **Enable Remote Filtering**.
3. Remote filtering is centrally administered. When a remote policy is enforced on the client, users of the client will be presented with a Denied page. As the administrator, you have the opportunity to influence the message on that page. In addition to the email addresses of the iPrism administrators, you can type in the **Administrator Contact Information** field, any other information you want to display on a block page. This information will be included in the page presented to the user when they encounter a blocked URL. For example, you might choose to also include something like “The requested page is currently unavailable. Your organization has chosen to limit viewing of this site due to the rating of its content.”
4. If you have already provisioned your iPrism (i.e., uploaded a remote filtering license key and completed step 2), you can click **Download Client Auth File** to create the key file that will be used during the installation of the Remote Filtering client software (see the *iPrism Remote Filtering Client Guide*).
5. Select the location where the code file should be saved. By default, this file is called `iprism_Client_Auth.key`. This file will be used when installing the Remote Filtering client software.
6. Save this key file to a location of your choice.

7. To download the Remote Filtering client software, click **Download Client Software**. This will take you to a website where you can complete the download. For more information about configuring and using `iprism_Client_Auth.key`, refer to the *iPrism Remote Filtering Client Guide*.
8. Click **Exceptions** to define specific network ranges or ports for which filtering on the remote client will not be enforced.
 - Specify the target network ranges (IP address and Netmask) you do not want to monitor for remote users, in **Unmonitored Network Ranges**.
 - Specify the range of target ports you do not want to monitor for remote users, in **Unmonitored Ports**.
 - Click **OK**.

Remote Filtering Exceptions

Specify IP ranges and ports that you want the remote filtering client to ignore.

Unmonitored Network Ranges

IP Address	Netmask
127.0.0.0	255.255.255.0

Unmonitored Ports

From Port	To Port
62	80

Add Edit Delete

Add Edit Delete

OK Cancel

Figure 30. Remote Filtering Exceptions

9. Remote clients that are controlled by a policy in which monitoring is configured periodically send event logs back to iPrism by way of the EdgeWave Data Center. The frequency at which iPrism requests events from the Data Center can be adjusted with the **Remote Filtering Logs** selection. To initiate an immediate log retrieval (i.e., not wait for the next cycle), click **Initiate Log Download**.
10. When you are finished on this page, click **Save**.

11. You will be prompted to select a default web profile for remote users. Select a default profile from the list and click **OK**.

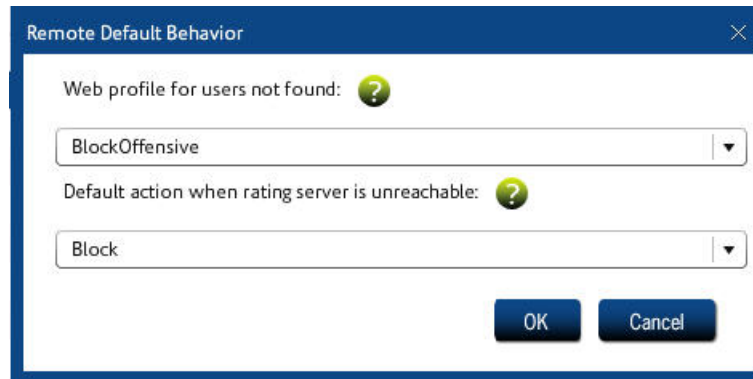


Figure 31. Remote Default Behavior

12. You can now set up remote users (see Remote Users).



Note: The status of log downloads and policy uploads can be viewed in the System Status section's Status.

CHAPTER 4 **Users & Networks**

To access user and network information, click **Users & Networks** from the home page.

Local Users

The Local Users section allows you to view, import, add, delete, or modify locally defined iPrism users. Local users exist in addition to and independent of users defined under Windows or LDAP authentication systems.

To add, change, and delete local users:

1. From the iPrism home page, select **Users & Networks**, then **Local Users**.
2. When you have finished modifying local users, click **Save** to save your changes.
3. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

User Name	Use Network	Web Profile	Admin Privileges
JSmith	No	BlockOffensive	Global Policy Admin
APerson	No	PassAll	Full Access

Figure 32. Local Users

Adding Users

1. In the Local Users window, click **Add**.
2. Type a **Username** and **Password** in the appropriate fields, and type the password again in the **Confirm Password** field.
3. Assign a web profile by selecting it from the dropdown list;

OR

Check **Use network profiles** to assign the web profile based on the IP address of the user's computer.

4. If this user is to have administrator privileges, select a type of Admin Privileges from the dropdown list. Otherwise, select **No access**.

iPrism's administrator levels are:

- **Extended Override:** Allows the user to log in to override management (see [Override Management](#)) and grant access to others.
- **Filter Management:** Allows the user to change the categories associated with a website (e.g., its site rating). Allows access to the Block/Unblock Site interface.

- **Full Access:** Allows the user to reply to administrative requests (overrides, access, etc.). This user can access reports and the Block/Unblock Site interface, but cannot access the Configuration interface or the Real-time Monitor.
- **Global Policy Admin:** This role is a user or login that is in charge of global filtering policies, regardless of existing partitions.
- **No Access:** This basic user account has no administrative privileges.
- **Reports Only:** This user will be allowed access to iPrism's report interface only.
- **Single Override:** Allows a user to grant access to themselves only. They cannot grant access to others.
- **Super Admin:** This allows multiple iPrism administrator/Super Admin accounts. The Super Admin account controls all iPrism access, configuration, and reporting.



Note: Admin Privileges created in Users & Networks > Admin Roles (Admin Roles) are also available and may be selected here.

The screenshot shows a 'Manage User' dialog box with the following fields and controls:

- User Name: [Text Input Field]
- Password: [Text Input Field]
- Confirm password: [Text Input Field]
- Use network profiles [Help Icon]
- Web Profile: [Dropdown Menu (PassAll)]
- Admin Privileges: [Dropdown Menu (Extended Override)]
- Notes: [Text Area]
- OK [Button]
- Cancel [Button]

Figure 33. Adding a User

5. Click **OK**.

Editing a Local User

To edit a local user:

1. In the Local Users window, select a user and click **Edit**.

2. Make changes as needed and click **OK**.

Deleting a Local User

To delete a local user:

1. In the Local Users window, select a user and click **Delete**.
2. Click **Yes** to confirm.

Importing Users

1. In the Local Users window, click **Import**.

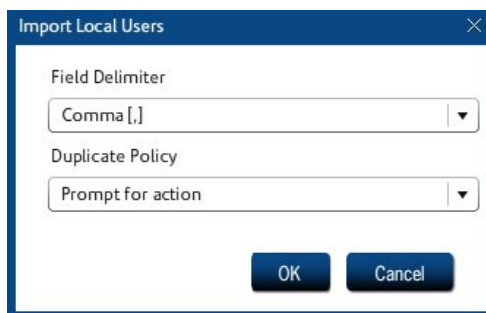


Figure 34. Import Local Users

2. In the Field Delimiter dropdown list, select the desired delimiter (**Comma**, **Pipe**, or **Tab**). This character will be used to delimit individual users in the imported file.
3. In the Duplicate Policy dropdown list, select an option to specify how duplicate policies are handled:
 - **Prompt for action:** When a duplicate policy is encountered, you will be prompted to tell the system how to handle it.
 - **Retain existing:** When a duplicate policy is encountered, the existing policy on the iPrism will be retained.
 - **Overwrite existing:** When a duplicate policy is encountered, the policy being imported will overwrite the policy on the iPrism.
4. Click **OK**.
5. Locate the file containing the users you want to import and click **Open**.

Exporting Users

1. In the Local Users window, click **Export**.



Figure 35. Export Local Users

2. In the Field Delimiter dropdown list, select the desired delimiter (**Comma, Pipe, or Tab**). This character will be used to delimit individual users in the exported file.
3. Click **Save As**.
4. Locate the folder, enter a file name, and click **Save**.

Groups

Once iPrism has successfully joined the domain in **System Settings > Directory Services**, you can map the user groups to iPrism's Web Profiles and administrator privileges (if no mapping is defined, the user will be assigned the Fallback Profile). Users who have been authenticated from a domain controller can be associated with an iPrism profile. All users who are members of a particular user group can be mapped to a particular iPrism access profile or administrator privilege.

To work with groups:

- From the iPrism home page, select **Users & Networks**, then **Groups**.

Allocate iPrism profiles to groups from your Directory Service(s)
Current Authentication Mode: AD 2008 - Joined And Connected

Domain	Group	Web Access Profile	Application Access
*	Students	BlockOffensive	BlockIMP2P
	Teachers	BlockOffensive	BlockP2P
	Administrators	PassAll	PassIMP2P

^ v Group Check Policy Test Fallback Add Edit Delete

Figure 36. Groups

Adding a Group

1. In the **Groups** window, click **Add**.
2. In the **Profile Maps** window, determine the level of access for this group by selecting a Domain, a Web Profile, and an Application Access profile.
3. Type a name for the group in the **Group** field.
4. Click **OK** to save your changes.
5. When you are finished adding all groups, click **Save** at the bottom of the Groups window.

Profile Map

Domain	Group
<input type="text" value="*"/>	<input type="text" value="Students"/>
Web Access Profile	Application Access Profile
<input type="text" value="BlockOffensive"/>	<input type="text" value="BlockP2P"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 37. Profile Map

Editing a Group

1. In the **Groups** window, click **Edit**.
2. Make any changes in the **Profile Maps** window.
3. Click **OK** to save your changes.
4. When you are finished editing all groups, click **Save** at the bottom of the Groups window.

Deleting a Group

1. In the **Groups** window, select a group and click **Delete**.
2. Click **Yes** to confirm the delete.
3. When you are finished modifying all groups, click **Save** at the bottom of the Groups window.

Mapping Groups to Profiles

Before doing any mapping, review the following guidelines.

Notes:

- It is very important to recognize that this particular list editor is ordered.
- LDAP mapping profiles use Attributes and Subquery Attributes, rather than the DOMAIN\groupname notation.

When mapping groups to profiles, keep the following principles in mind:

- As iPrism is determining a user's profile, a top-to-bottom search is performed on the list, with the default assignment applied last (if no match is found).
- For the first group on the list in which the user is a member, the corresponding profile for that map item is associated with the user. iPrism then uses this profile to define this user's access to iPrism.
- If the user is not a member of any group mappings on the list, the user is associated with the Web Fallback and Application Fallback profiles.

- Whatever defines the group (DOMAIN or groupname) can be wildcarded (replaced with a single asterisk (*)). The asterisk wildcard means that all domains or all groups are covered by the mapping entry. An example of this convenience is if you want members of the 'staff' group (in any domain) to be mapped to the MonitorAll profile:

```
( [*\staff > MonitorAll] )
```

Likewise, a wildcard can be used in the group position to cover all groups within a particular domain (e.g., [DOMAIN* > BlockOffensive]).

- The Web Fallback and Application Fallback profiles are checked last and have the implied [** > default profile] map.

The default profile should be carefully assigned, since any user who is not a member of one of the group mappings will be associated with this profile. A common strategy is to plan that most users will obtain the default profile, and use explicit mappings on the list for exceptions.



Note: Since ** is implicitly mapped to the default profile, explicitly mapping ** on the list is not allowed.

In summary, an effective way to view mappings is to set the default profile as what most users will be controlled by. Exceptions to the default profile can be configured via mappings, with the most specific exceptions to be ordered at the top.

Nested Groups

When iPrism is joined to a Windows directory service that supports nested groups, such as Server 2000/2003 or Server 2008 mode, iPrism also supports nested groups.

Nested groups are supported when the iPrism is joined in either Server 2000/2003 or Server 2008 mode and the Windows domain controller is running in Windows 2000 Native mode or higher. (Windows domain controllers running in Windows 2000 mixed mode do not support nested groups.)

When nested groups are in use, groups may be members of other groups. A user who is a member of a group is also a member of any group of which that group is a member; e.g., if there is a group "Color Printer Users", and this group is a member of the group "Printer Users", any user who is a member of the "Color Printer Users" group is also a member of the "Printer Users" group.

iPrism assigns profiles and privileges based on the first group on the Groups page or Privileges page of which the user is a member, whether the user is directly a member of that group or is a member via the nested groups feature. Place direct-membership groups (e.g., “Color Printer Users”) before nested groups (e.g., “Printer Users”) in the list of Groups or Privileges in order to have the profiles or privileges of the direct-membership group (e.g., “Color Printer Users”) take effect.

Allocate iPrism profiles to groups from your Directory Service(s)
Current Authentication Mode: AD 2008 - Joined And Connected

Domain	Group	Web Access Profile	Application Access Profile
	Color Printer Users	PassAll	BlockP2P
	Printer Users	BlockOffensive	BlockP2P

Figure 38. Nested Groups Example

Privileges

Once iPrism has successfully joined the domain in **System Settings > Directory Services** and mapped groups to profiles (see [Groups](#)), you can map the privileges to groups.

To add, edit, and delete privilege mappings:

1. From the iPrism home page, select **Users & Networks**, then **Privileges**.

Allocate iPrism profiles to groups from your Directory Service(s)
Current Authentication Mode: AD 2008 - Joined And Connected

Domain	Group	Privilege
	Domain Admins	Extended Override
	Systems Engineers	Filter management
	Policy Admins	Global Policy Admin

^ v Group Check Fallback ▶ Add Edit Delete

Figure 39. Privileges

2. To add a privilege mapping, click **Add**; to edit an existing privilege mapping, click **Edit**.

3. Select a domain from the Domain dropdown list.
4. Type the group to which you are mapping this privilege; for information about setting up groups, see [Groups](#).

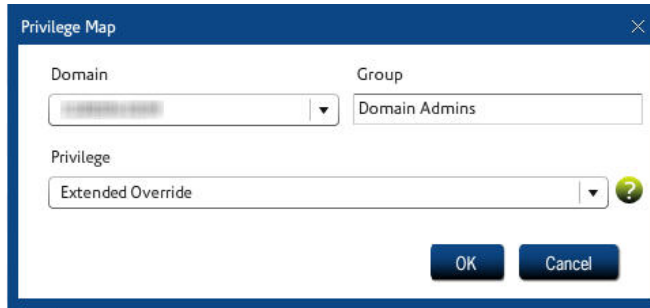


Figure 40. Privilege Map

5. Select a Privilege from the dropdown list:
 - **Extended Override:** Allows the user to log in to override management (see [Override Management](#)) and grant access to others.
 - **Filter Management:** Allows the user to change the categories associated with a website (e.g., its site rating). Allows access to the Block/Unblock Site interface.
 - **Full Access:** Allows the user to reply to administrative requests (overrides, access, etc.). This user can access reports and the Block/Unblock Site interface, but cannot access the Configuration interface or the Real-time Monitor.
 - **Global Policy Admin:** This role is a user or login that is in charge of global filtering policies, regardless of existing partitions.
 - **No Access:** This basic user account has no administrative privileges.
 - **Reports Only:** This user will be allowed access to iPrism's report interface only.
 - **Single Override:** Allows a user to grant their own access. They cannot override a block page for another user.
 - **Super Admin:** This allows multiple iPrism administrator/Super Admin accounts. The Super Admin account controls all iPrism access, configuration, and reporting.



Note: Admin Privileges created in Users & Networks > Admin Roles (Admin Roles) are also available and may be selected here.

6. Click **Save**.

7. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Networks

The Networks section allows you to manage network profiles. A network profile is a profile assigned to a range of IP addresses. Any user whose IP address falls into that specified range will be assigned that profile.

In the example below, we are defining several subnets; one for 192.168.100.1 - 192.168.100.100, as well as one for 192.168.200.1 - 192.168.200.100. All are in proxy mode, but they have varying authentication modes - No Authentication, Manual-Login (Basic, HTTP, or HTTPS), or Disable Web Access. For a list of which options are available for each mode, see [Adding a Network Profile](#).

At the top of the Networks window is a list of IP ranges. When iPrism sees network traffic, it will go down the list looking for a range which matches the IP address associated with the network request. If this address is on the 192.168.x.x network, the first entry in the list is matched, and profiles associated with that entry are used.

If another address is making the request, the system falls through to the second entry which matches everything and uses it. For more information on configuring profiles for your network, see [Profiles](#) and [Application Profiles](#).



Note: If you enter the range 0.0.0.0 - 255.255.255.255, any subnet in this range is included in this profile.

To add, edit, and delete network profiles:

1. From the iPrism home page, select **Users & Networks**, then **Networks**.
2. When you are finished working with network profiles, click **Save** at the bottom of the Networks window.
3. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Current Authentication Mode: AD 2008 - Joined And Connected

Order	IP Range	Web Profile	Application Profile
1	0.0.0.0 - 255.255.255.255	BlockOffensive	BlockIMP2P

^ v Add Edit Delete ?

Figure 41. Networks

Adding a Network Profile

1. In the Networks window, click **Add**.
2. In the Details tab, enter the details of the Network Profile: the **IP Start** and **IP End** range, whether the workstation is proxying to iPrism's external interface (e.g., users are connecting to a firewall VPN when iPrism is in bridge (transparent) mode), and the **Web Profile** and **Application Profile** that will apply to this network profile.

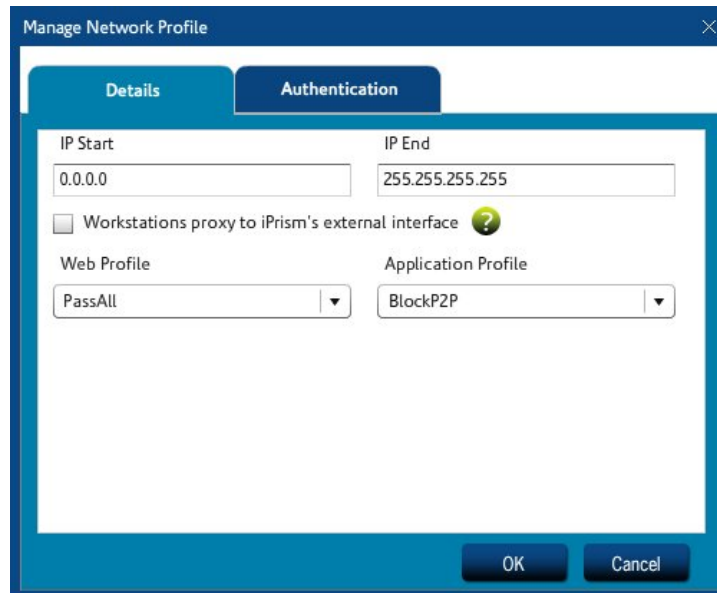


Figure 42. Network Profile Details

3. Click the **Authentication** tab.

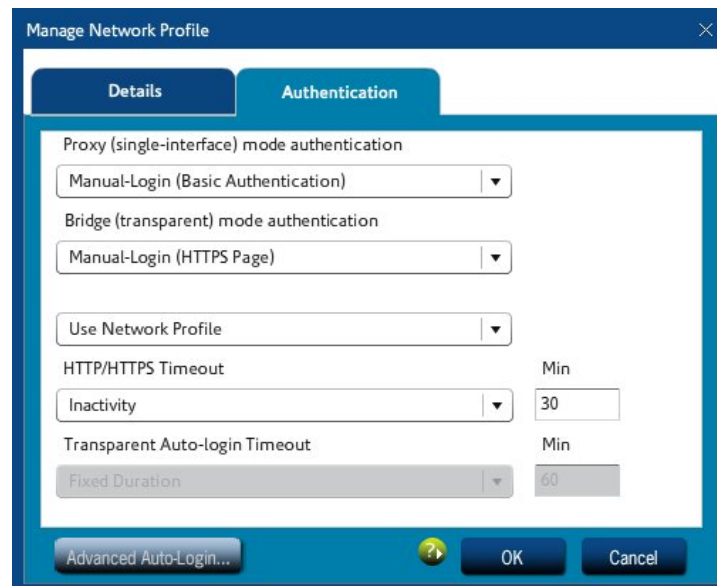


Figure 43. Authentication Tab - Proxy Mode

4. From the appropriate Authentication dropdown list, select which Authentication mode is to be used if **Always attempt manual login** is selected in Advanced Auto-Login settings (see step 8 below). If **Always attempt manual login** is selected, one of the following options must be selected here to specify how to handle the manual login.
5. From the **Failed Option:** dropdown list, select a failover option to specify what happens if authentication fails (**Use Network Profile** or **Disable Web Access**). By default, **Use Network Profile** is selected; the network profile will be applied to web filtering.
6. Configure your authentication mode and settings. For detailed explanations of authentication modes and Auto-login in both proxy and bridge (transparent) modes, see [Choosing an Authentication Mechanism](#).
7. To specify a timeout value, select an option from the **Timeout** dropdown list and type the number of minutes in the **Min** field.
8. Click **Advanced Auto-Login** to specify how to handle failed Auto-Login authentication. Available options are:
 - Always attempt manual login
 - Never attempt manual login

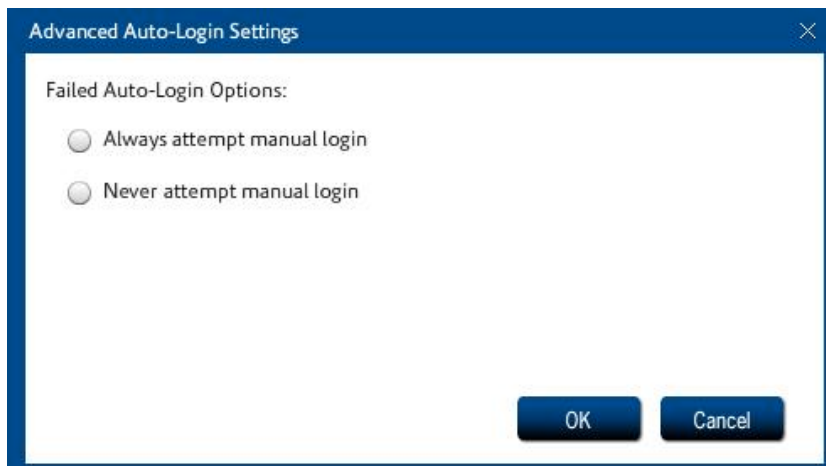


Figure 44. Advanced Auto-Login



Notes:

For iPrism upgrades or a new iPrism setup, select **Always attempt manual login**.

If **Always attempt manual login** is selected, select an option in step 4 above to specify how to handle the manual login.

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

Editing a Network Profile

1. In the Networks window, click **Edit**.
2. Make changes as necessary.
3. Click **OK** to save your changes.

Deleting a Network Profile

1. In the Networks window, select a profile and click **Delete**.
2. Click **Yes** to confirm.

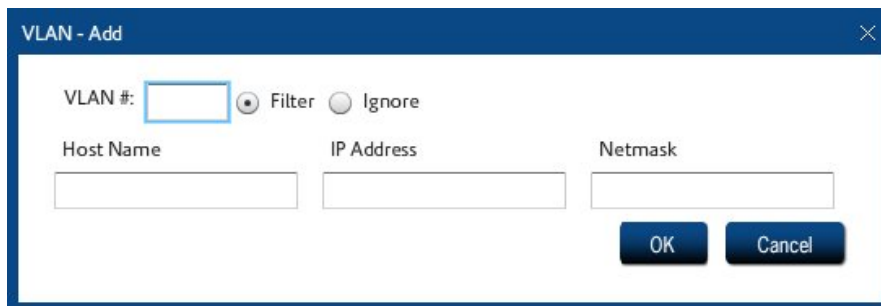
VLAN Management

If your network includes VLANs, you can set up iPrism to filter VLAN tagged traffic on an 802.1Q trunk.

If you want to make unique policy decisions on a per VLAN basis, it is advisable to create a separate network entry for each VLAN on the networks list. This will come into play for non-authenticated traffic as well as administrative privileges such as overrides.

To manage VLANs:

1. From the iPrism home page, select **Users & Networks**, then **VLAN Management**.
2. Add, change and remove VLANs as needed.
3. Click **Save** to save your changes.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.



The screenshot shows a dialog box titled "VLAN - Add". It features a "VLAN #" input field with a blue border. To its right are two radio buttons: "Filter" (which is selected) and "Ignore". Below these are three input fields labeled "Host Name", "IP Address", and "Netmask". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Figure 46. Adding a VLAN

2. Assign a VLAN ID in the range 0-4094.
3. Choose whether to add filtering to this VLAN, or specify that filtering should be ignored for this VLAN.
4. Enter a DNS hostname, IP address, and subnet mask that the iPrism will use for participation on this VLAN. Because user machines will be interacting at a TCP level with this address and name, the IP address and DNS name must be unique.
5. Click **OK**.

Editing a VLAN Description

1. In the VLAN Management window, select a VLAN and click **Edit**.
2. Make changes as needed.
3. Click **OK**.

Deleting a VLAN Description

1. In the VLAN Management window, select a VLAN and click **Delete**.
2. Click **Yes** to confirm.

Adding an Admin Role

1. In the Admin Roles window, click **Add**.
2. Type a name for this Admin Role, and select a Role Type from the dropdown list. The following roles are available:
 - **Global Policy Administrator (GPA)**: The GPA has the right to log in to UI Configuration tools and administer global filtering policies. The GPA can also access reports, filter management, and overrides. Use this role to delegate management policies of the entire iPrism to a user.
 - **iPrism-wide Privileged User**: This role assigns specific rights for the entire iPrism. For example, with this option, you can create a privilege that has full reporting access and overrides for the entire iPrism.
 - **Super User (also referred to as Super Admin)**: The Super User/Super Admin is the built-in account with the username “iprism”, and has all rights. This role is not viewable or configurable, and is the only “mandatory” role. The assignment of other roles and privileges listed below is optional.
3. Select options in the Filtering tab:
 - **Manage profiles**: This Admin role will be able to manage Profiles.
 - **Manage Overrides, Requests and Recent Blocks**: Allow this Admin Role to manage Overrides, Pending Requests, and Recent Blocks.
 - **Manage Antivirus and Remote Filtering settings**: Allow this Admin Role to manage the Antivirus and Remote Filtering settings.
4. Select the **Access Control List** tab.

Figure 48. Admin Roles – Access Control List Tab

5. One or more individual filtering criteria, or Access Control Lists (ACLs), make up a Web profile. A Web ACL tells iPrism what to do for each category of website and specifies which traffic gets blocked or monitored. Admin Roles can be set to allow for specific types of overrides and to have those overrides be valid for custom durations.
6. Select a type of override from the Override dropdown list. The following types of overrides are available:
 - **Cannot Override:** Cannot override blocked pages. If this option is selected, no other ACL options can be selected in this window; click **OK** to finish.
 - **Self Only:** This role can override blocked pages only under its own login, but no others. You can select Durations (step 7) and which contents can be overridden (step 10).
 - **Custom:** Define what kind of overrides you want this role to have. Select Durations (step 7), to whom this applies (step 9), and which contents can be overridden by this role (step 10).
7. Select a duration for this override to be valid by clicking one of the following:

- **Use Predefined Durations:** Select either **Unlimited**, or select **Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, from the dropdown list and type in the number of minute(s), hour(s), day(s), and/or week(s) this override is valid (e.g., 1 hour 30 minutes).
- **Use Customized Durations:** Click **Configure Durations**, click **Add**, then specify the durations you want in week(s), day(s), hour(s), and minute(s).
- **Unlimited Duration:** No duration is set.

If you want the duration you have specified to be used as the default, check **Set this duration as default**.

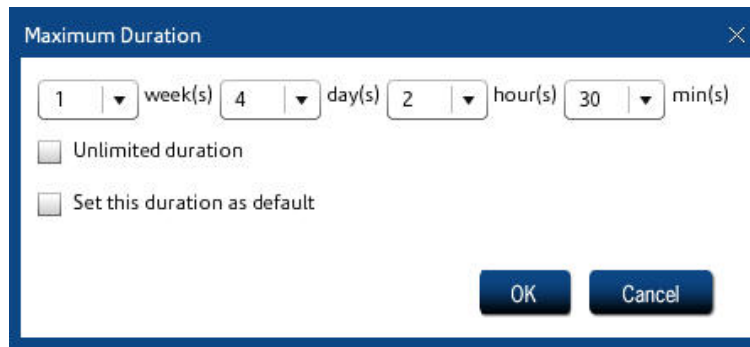
A screenshot of a dialog box titled "Maximum Duration" with a close button (X) in the top right corner. The dialog contains four dropdown menus for specifying duration: "1" for week(s), "4" for day(s), "2" for hour(s), and "30" for min(s). Below these are two checkboxes: "Unlimited duration" and "Set this duration as default", both of which are currently unchecked. At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 49. Maximum Duration for Overrides

8. Click **OK**.
9. Back on the Access Control List tab, check to whom the Admin Role applies:
 - **Everyone**
 - **Only the Current Workstation**
 - **Only the Current User**
 - **A Profile**
 - **Current User profile**
 - **PassAll profile**
 - **BlockOffensive profile**
 - Any defined profile
 - A specified **Network Range** you have typed (0.0.0.0 to 255.255.255.255 covers the entire network).
10. Check which contents can be overridden by this role:
 - **Current URL:** Only the entire URL can be overridden.

- **Current Path:** The path component is the part of the URL which appears after the host name. This allows overriding based on a specific path, regardless of the host name.
 - **Current Domain:** The domain name of the host part of the URL. For example, the domain for `http://www.yahoo.com` is `yahoo.com`. iPrism is aware of country codes, so the domain for `http://www.amazon.co.uk/index.html` is `amazon.co.uk`.
 - **Current Category:** This option allows the administrator to override all users that belong to the category of the URL being requested.
 - **Categories allowed by this user's profile:** This option allows the administrator to apply his/her categories to override the requested URL being requested; i.e., the administrator is overriding the URL request with his/her own profile.
 - **All URLs:** The user can override any URL.
11. Select the Reporting tab to specify Reporting options:
 - None: This role has no reporting rights.
 - Full: Full reporting rights are allowed.
 - Limit Results by Network Range: Enter a start and end IP range. The results will be limited by this range.
 - Limit Results by Profile: Select a profile (Current User Profile, PassAll, or BlockOffensive). The results will be limited to this profile.
 12. Select the **Other** tab.
 13. Check the boxes next to what you want this Admin Role to be able to manage:
 - Manage Users & Networks
 - Manage Access Maintenance
 - Manage System Settings
 - Access System Status
 14. Click **OK** to save your changes.

Editing an Admin Role

1. In the **Admin Roles** window, select a role and click **Edit**.
2. Make changes as needed.
3. Click **OK**.

Deleting an Admin Role

1. In the **Admin Roles** window, select a role and click **Delete**.
2. Click **Yes** to confirm.

Exceptions

iPrism's goal on your network is to act as a web filter for access to the Internet. In fact, this is how it is able to perform its monitoring and blocking tasks. You may want to implement reduced or additional filtering for specific situations.

Exceptions make iPrism ignore traffic coming from or going to a range of hosts (e.g., a corporate web server located in a DMZ or internal servers accessing the Internet without authentication).

Specific examples of the most commonly used types of exceptions are in the iPrism Knowledgebase section on Exceptions.



Note: HTTPS (SSL) traffic on port 443 is now strictly enforced by default. If you do not use SSL but do use port 443, either change the application port or create a filter exception for the client/server addresses.

To work with exceptions:

1. From the iPrism home page, click **Users & Networks**, then **Exceptions**.
2. Add, change, and delete exceptions as needed.
3. When you are finished click **Save** at the bottom of the Exceptions window.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Adding an Exception

1. From the Exceptions window, click **Add**.

Figure 50. Managing Exceptions

2. Type a name for the exception in the **Name** field.
3. Select the type of exception:
 - **No Filter:** Traffic will pass unfiltered through the specified Source and Destination range of IP addresses, or the specified port.
 - **Block:** Traffic destined for the specified IP address range OR the specified port(s) will be blocked.
 - **NAT (Network Address Translation):** NAT replaces the IP address of the sender (i.e., the user) with the IP address of iPrism, for outbound traffic. A reverse translation is done to any responses coming back. The effect of NAT is that requests look like are coming from iPrism only. This setting hides the IP addresses of your internal workstations from the Internet (transparent mode only).
 - **No Authentication:** Traffic destined for the IP address range will not be authenticated.
 - **No Authentication & NAT:** Combines NAT with No Authentication in one option.



Note: Exception types are applied in order of priority based on the type. For example, if a “No Filter” exception has been created for an IP address range, and later a subsequent “Block” exception is created for that same IP address range, the “No Filter” exception wins, as iPrism encounters that type of exception first; thus, traffic will pass unfiltered through that IP address range.

4. Type the IP address range for the sending machine or set of machines in the **Source IP Start** and **End** fields.
5. Type the IP address range for the receiving machine or set of receiving machines in the **Destination IP Start** and **End** fields.
6. If this exception applies to all ports, select **All Ports**. If it applies only to specific ports, select **Specific Ports** and type the ports to which this exception applies. Use commas to separate multiple ports. A range of ports can be specified as well (e.g., 80 - 120, or 1 - 79, 81 - 65535).
7. In Protocols, check either **TCP** or **UDP**. If you select both TCP and UDP, all IP protocols will be blocked, including ICMP and others. At least one must be selected.
8. Click **OK**.

Editing an Exception

1. In the Exceptions window, select an exception and click **Edit**.
2. Make changes as needed.
3. Click **OK** to save your changes.

Deleting an Exception

1. In the Exceptions window, select an exception and click **Delete**.
2. Click **Yes** to confirm.

Remote Users

iPrism provides comprehensive Internet security for off-premises users (see [Remote Filtering](#)). The mobile laptops and/or remote users must be provisioned in order to utilize this capability.

Before setting up remote users:

1. Upload a remote filtering license key (see [License Key](#)). You may be logged out and have to log back into your iPrism.
2. Enable Remote Filtering and download the client software via **Profiles & Filters > Remote Filtering**.



Important: The Machine Identifier identifies a particular remote machine and defines a policy for all users on that machine. It is treated like a username, and by default is the hostname of the machine when the client is installed (to locate the computer's hostname, see *Locating a Hostname in the iPrism Remote Filtering Client Guide*). Thus, the names of the Remote Users you create in the table below must match exactly the names of the mobile laptops to which they are being mapped.

For example, if a mobile laptop's Machine Identifier is "jsmith012-companyA", the corresponding Remote User must also be called "jsmith012-companyA". Conversely, if you set up the Remote User first, you must also make sure that when you provision the Remote Client (see the *iPrism Remote Filtering Client Guide*), you give it the same name ("jsmith012-companyA").

Generally speaking, the first thing to do is designate a default profile that will apply to remote clients. If you want all remote clients to be controlled by that policy, you don't need to do anything else here.

If you want to create exceptions to that default profile, specify those in Client Exceptions. (Exceptions are specifically identified Machine IDs, whereas the default profile applies to all undefined Machine IDs.) If exceptions are specified, iPrism remote filtering will first check if a user is defined that matches the client Machine ID, and apply the specified profile. If there is no (exact) matching Machine ID, then the default profile is applied. It is unlikely you will have more than a few users defined in Client Exceptions.

Even though profile assignment is defined on a per-client machine basis, access events that make their way into iPrism reporting will record the currently logged-on user and iPrism reporting events.



Note: Remote Filtering must be enabled via **Profiles & Filters > Remote Filtering** prior to setting up remote clients.

To work with remote users:

1. From the iPrism home page, select **Users & Networks**, then **Remote Users**.
2. Add, edit, and delete remote users as needed.
3. Click **Save** to save your changes.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Adding a Remote User

1. In the Remote Users window, click **Add**.
2. Enter the username/machine ID. See [Remote Users](#) for details.
3. To enable this machine now, select **Enabled**.
4. Select the Web profile to apply for this machine.
5. Select the Failover action for this machine.
6. Click **OK**.

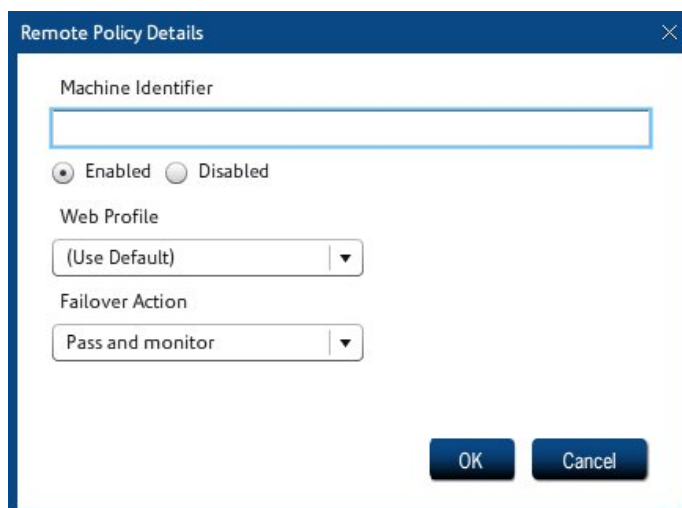
The image shows a dialog box titled "Remote Policy Details" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Machine Identifier". Below it are two radio buttons: "Enabled" (which is selected) and "Disabled". Underneath are two dropdown menus: "Web Profile" with "(Use Default)" selected, and "Failover Action" with "Pass and monitor" selected. At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Figure 51. Add Remote User

When Remote Filtering is ON (see [Remote Filtering](#)), this user will be able to take advantage of iPrism, including having profiles and filtering rules applied to them, downloading filter updates and rules, uploading reports, and having their Internet activities tracked and reported upon.

Editing Remote Users

1. In the Remote Users window, select a user and click **Edit**.
2. Make changes as needed.
3. Click **OK**.

Deleting a Remote User

1. In the Remote Users window, select a user and click **Delete**.
2. Click **Yes** to confirm.

Importing Remote Users

If you already have a list of remote users, you may want to import them to iPrism.

1. In the Remote Users window, click **Import**.

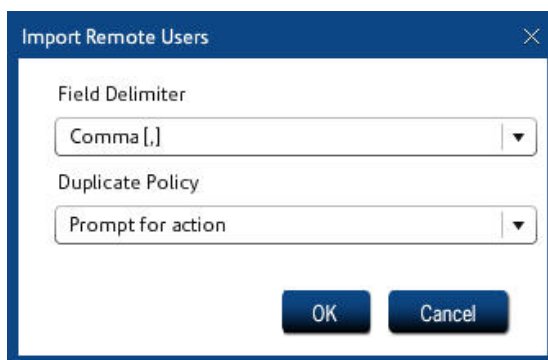


Figure 52. Importing Remote Users

2. Select a field delimiter (comma, pipe, or tab) for the import file.
3. Select an option for handling duplicate policies (usernames):

Prompt for action: The administrator will specify how to handle each duplicate policy (username).

Retain existing: Retain the existing policy (username) on the iPrism; the policy (username) in the import file will be overwritten.

Overwrite existing: Overwrite the existing policy (username) on the iPrism with the policy (username) from the file being imported.

4. Click **OK**.
5. Choose the .CSV file containing the list of users to import. The file might look something like this:

```
name,enabled,default_action,profile_name
```

```
ru_sonia,false,1,BlockOffensive
ru_tony,false,1,PassAll
ru_john,false,1,BlockOffensive
ru_mary,false,1,PassAll
ru_peter,false,1,PassAll
```

Exporting Remote Users



Note: You must **Save & Activate** any unsaved changes prior to exporting users.

1. In the Remote Users window, click **Export**.
2. A check will be performed to verify whether any changes need to be saved and activated. If there are changes, you must click **Save**, then click **Activate Changes** before you can perform an export.
3. If there are no changes, select a field delimiter (comma, pipe, or tab) for the export file:



Figure 53. Exporting Remote Users

4. Click **Save As**.
5. Specify the location of the exported file.

An exported file might look something like this:

```
Name,Enabled,Action Id,Profile
ru_peter,true,2,PassAll
ru_mary,false,2,PassAll
ru_john,true,1,BlockOffensive
ru_tony,true,2,PassAll
ru_sonia,true,1,BlockOffensive
```

Remote Upgrades

System upgrades for remote users can be scheduled during non-peak periods if needed. Set up the defaults that will apply to most systems, and then add exceptions if needed, for specific machines or ranges of machines.

To set up remote upgrades:

1. From the iPrism home page, select **Users & Networks**, then **Remote Upgrades**.



Note: If you have just enabled Remote Filtering, the available Remote Upgrades may not yet be visible on this page. If this occurs, log out then log in again to see the available Remote Upgrades.

2. Set the defaults as they apply to PC and/or Mac systems.
 - Select **Enabled** to turn on remote upgrades, or **Disabled** to turn off remote upgrades. If remote upgrades are disabled for a type of machine (e.g., Mac), you can enable them for specific IDs using the Exceptions settings.
 - Select an upgrade package from the dropdown list. Only available packages for the machine type are listed.
 - Choose the dates and times during which this upgrade will be applied. If a specific machine is unavailable at this time, it will not get the upgrade.
 - Check **Force Reboot** if you want each machine to automatically reboot and complete the upgrade.

Default Upgrade Settings

PC Enabled Disabled

Package: RFC 2.0 Release Candidate 1-C - 2

Start: 11/11/2011 5 AM AM PM

Finish: 11/14/2011 8 AM AM PM

Force Reboot

Mac Enabled Disabled

Package: RFC 2.0 Release Candidate 1-C - 2

Start: 11/11/2011 5 AM AM PM

Finish: 11/14/2011 8 AM AM PM

Force Reboot

Remote Upgrade Exceptions

Enabled	Package	Machine Id	Start	Finish	System	Force Reboot
<input checked="" type="checkbox"/>	RFC 2.0 Release	sales*	2011-11-07 06:00	2011-11-30 17:00	WIN	1
<input checked="" type="checkbox"/>	Do Not Upgrade	qa*	2011-11-01 08:00	2011-11-30 19:00	WIN	0

Select All
Deselect All
Add
Edit
Delete

Figure 54. Remote Upgrade Settings

3. To add exceptions, click **Add**, enter the information, and click **OK**.
 - To enter a range of machine IDs, use the * wildcard (only available at the end of the ID).
 - Select **Enabled** to turn the exception setting on, or **Disabled** to turn off this exception setting.

Remote Upgrade Exception - Add
✕

Machine Id:

Enabled Disabled

System:

Package:

Start: 11/08/2011 11 AM AM PM

Finish: 11/09/2011 11 AM AM PM

Force Reboot

Figure 55. Remote Upgrade Exceptions

4. Click **Save** to save your changes.

5. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

CHAPTER 5 Reporting

The iPrism Report Manager contains predefined, commonly needed reports, such as who was visiting what website and when. You can also create your own custom reports for IM, P2P and URL events. Refer to the *iPrism Reporting Guide* at http://www.edgewave.com/support/web_security/documentation.asp for detailed instructions on how to manage and use the Report Manager.



Note: Email Alerts are now located in the Profiles & Warnings menu, in Quotas & Warnings. See Email Alerts for details.

CHAPTER 6 Maintenance

This section describes how to change iPrism's internal settings and set your preferences for common iPrism activities such as managing updates, backing up, restoring, running tests, and doing self-checks.

Appliance Updates

Also known as the Hotfix Manager, Appliance Updates provide a convenient interface for tracking iPrism updates and patches (called Hotfixes). With Appliance Updates, you can instantly check for new updates, view available updates, see which updates have already been installed, and manually install or uninstall a Hotfix.



Note: Only the iPrism administrator/Super Admin account (iprism) can access Appliance Updates.

To access Appliance Updates:

1. From the iPrism home page, select **Maintenance**, then **Appliance Updates**.
2. Click **Hotfix Manager**.
3. Click **Yes** to confirm.

iPrism automatically checks for updates to its filtering database and system (software) files daily. You can disable this function to allow only manual updates, or specify the time of day when you want iPrism to run its update utility.



Note: Disabling automatic updates is not advised. With automatic updates disabled, your system will not automatically install critical Hotfixes.

By default, iPrism is set up to automatically check for system updates in the early morning hours, when network traffic is likely to be at a minimum. If this is convenient for you, there is no reason to change the default setting.

Installing a New Hotfix

1. If you need to update the Available Hotfixes list, click **Check for New Hotfixes** in the Hotfix Manager.
2. Select the desired Hotfixes from the Available Hotfixes list and click **Install**. The Install Hotfixes web page opens.
3. Click **Install**.

If the Hotfix you selected is dependent upon earlier Hotfixes that are not installed, all required Hotfixes are installed automatically once you authorize the installation of the new Hotfix.



Note: The same dependency principle applies when uninstalling Hotfixes. Uninstalling a Hotfix on which others are dependent results in all dependent Hotfixes being uninstalled.

Rebooting after Installing Hotfixes

To enable Hotfixes, iPrism typically must be rebooted after the Hotfix has been installed. When you are done installing a Hotfix, you normally see a message indicating that a reboot is required, and a button to click to go back to the Hotfix Manager.

1. Click **Back**.
2. Click **Reboot the system**.
3. Confirm the reboot by clicking **Reboot the system**.

Uninstalling a Hotfix

Although it is unlikely you will ever need to do this, you can uninstall a Hotfix if you suspect it is causing issues with your iPrism, or if you are directed to do so by EdgeWave Technical Support.

To uninstall a Hotfix:

1. In the Installed Hotfixes list, select the Hotfix you want to remove and click **Uninstall**. A confirmation message appears.
2. Click **Yes**.



Note: If you uninstall a Hotfix on which others are dependent, all dependent Hotfixes are also uninstalled.

Backup and Restore

You can back up all of your settings to a file on your local hard drive, restore the iPrism configuration to a previously saved version, or reset to factory default settings. In addition, the backup configuration file can be useful to provide configuration data to iPrism Technical Support.

To access the backup and restore options:

- From the iPrism home page, select **Maintenance**, then **Backup & Restore**.

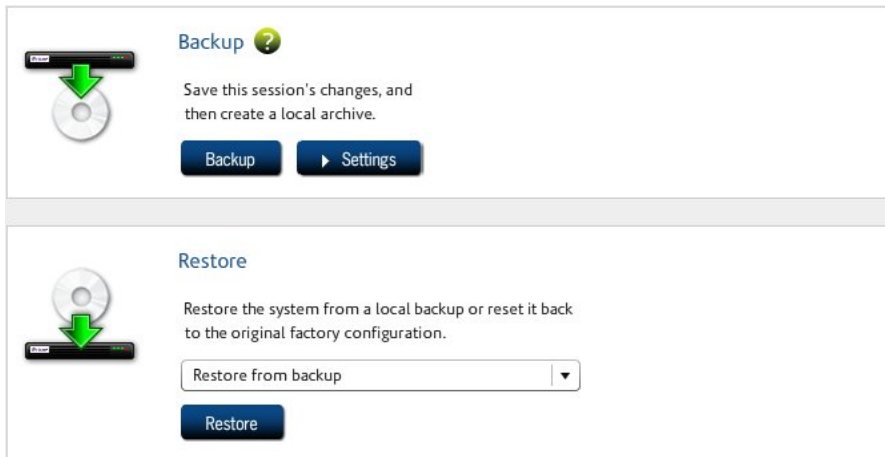


Figure 56. Backup & Restore

Backing Up

Backing up your iPrism configuration stores all of your settings to a file on your local hard drive. If necessary, you can restore your settings from this file. The data in backup files is encrypted for security.

By default, iPrism automatically prompts every 6 days, when you exit, to back up your iPrism System Configuration.

To perform an immediate backup:

- In the Backup & Restore window, click **Backup**.

If you need to change your backup preferences:

- Click **Settings**. See [Backup Settings](#) for details.

Restoring

You can restore your iPrism from a local backup or to its original factory configuration.

Restoring Your System from a Local Backup

1. In the Backup & Restore window, select **Restore from backup** from the dropdown list.
2. Click **Restore**.



Note: iPrism v4.0 introduced a new database format. Backups created prior to version 4.0 are NOT compatible and cannot be restored.

Restoring iPrism to its Default (Factory) Configuration

Restoring the iPrism to its factory settings clears all user-defined configuration information. You should do a backup of your current configuration before performing this procedure. (See [Backing Up](#)).

1. In the Backup & Restore window, select **Restore Factory Configuration** from the dropdown list.



Note: This restores iPrism to its “out of the box” state. All settings, including network settings, are lost or set back to their default values.

2. Click **Restore**.
3. Click **Yes** to confirm.

The iPrism reboots within two minutes, and your iPrism session is ended.

When you log into iPrism again, you will be presented with the installation wizard, as if you were setting up iPrism for the first time. Refer to your *iPrism Installation Guide* for assistance with this wizard.

Event Log

The Event Log provides a status record of Access Events - the number of web and application accesses. Also provided is the date of the oldest record accessed.

The screenshot displays the 'Access Event Status' section with a table of statistics:

Oldest Record	Number of Web Records	Number of Application Records
18 Feb 2011	5965	117

Below the table is the 'Delete Access Event Records' section. It features a date selection field with the value '2 / 23 / 2011' and a 'Delete' button. To the right, there is a 'Delete All' button and a help icon (a question mark in a circle).

Figure 57. Event Log

To view the Event Log:

- From the iPrism home page, select **Maintenance**, then **Event Log**.

Deleting Access Event Records

There are times when you may wish to purge event data from iPrism, such as if an iPrism is transferred from one department to another.

To delete access event records:

1. From the iPrism home page, select **Maintenance**, then **Event Log**.
2. To delete records up to and including a given date, type that date in the date field, or select a date from the calendar. Click **Delete**.

OR

To delete all records in iPrism, click **Delete All**.

3. Click **Yes** to confirm.

Policy Test

You can access additional Directory Service diagnostic information by clicking **Policy Test**. This test allows you to determine what profile will be applied to a user given the current system configuration, and to check whether a user can be authenticated.



Note: To test a policy you must have successfully joined the domain in **System Settings > Directory Services**.

1. From the iPrism home page, select **Maintenance**, then **Policy Test**.
2. Type the **Username**, **Password**, **Domain**, and **IP address** you want to test in their respective fields.
3. Click **Test**.

iPrism validates the user. The results are displayed in the Test Result field.

Current Authentication Mode: Server 2000/2003 - Joined and Connected

Username: iprism Password: *****

User IP Address: [] Domain: []

Test [?]

Test Result

Network authentication settings
Proxy mode: None
Transparent mode: None

WARNING: authentication is not enabled for this IP address and the default network profiles are used. Please review the settings in Users & Networks -> Networks panel.
User mapped to web profile: BlockOffensive
User mapped to imp2p profile: BlockIMP2P

Figure 58. Policy Test

Self Check

iPrism's Self Check allows the administrator to run various diagnostic tasks on the iPrism. Self-check files are often used by iPrism Technical Support to aid in troubleshooting.

To perform a self check:

1. From the iPrism home page, select **Maintenance**, then **Self Check**.
2. Click **Start Check** to start the check.
3. A check will be performed and the results displayed. You can stop the check by clicking **Stop Check**.
4. You can send these results directly to EdgeWave Technical Support by clicking **Send to Tech Support**.
5. To clear the screen and perform a new check, click **Clear**, then **Start Check**.

Send Test Email

This allows the administrator to test designated iPrism email recipients, such as iPrism administrators or users with privileges, as well as the allowable email size (in MB).

1. From the iPrism home page, select **Maintenance**, then **Send Test Email**.
2. Type the email address of the recipient to whom you want to test, and the allowable size you want to test (in MB).
3. Click **Send Test Email**.
4. If the email is sent successfully, a confirmation message appears. Click **OK** to dismiss the message.

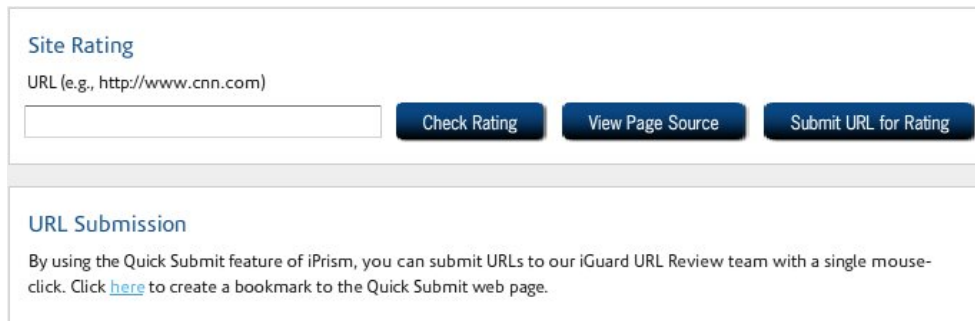
Site Rating & Test

A website's rating determines whether or not it will be blocked by the active filtering profile. All of the websites included in iPrism's URL database have a site rating based on their content. For example, a political website would have a rating that included the category Politics, and potentially other categories as well. If the current profile in iPrism is set to block sites in the Politics category, then this site would be blocked when the Profile member attempts to access it.

To check the category rating of any website:

1. From the iPrism home page, select **Maintenance**, then **Site Rating & Test**.
2. Type the full URL of the website whose ratings you want to check, and click **Check Rating**.

This shows you how the site is rated in iPrism's database, as well as any custom filters you have created for that site.



The screenshot shows a web interface with two main sections. The top section, titled "Site Rating", contains a text input field for a URL (with the example "http://www.cnn.com"), and three buttons: "Check Rating", "View Page Source", and "Submit URL for Rating". The bottom section, titled "URL Submission", contains a paragraph of text explaining the Quick Submit feature and a link labeled "here".

Figure 59. Site Rating & Test

3. If you would like to submit the site to EdgeWave for review, click **Submit URL for Rating**. The URL of the site is sent to the URL Review team and will be reviewed within 24 hours.

Support Tunnel

This allows the administrator to set up a support tunnel to iPrism Technical Support. This is typically done under the direction of Technical Support to aid in troubleshooting.



Note: iPrism supports an Auto-Restart tunnel connection. When the administrator starts a tunnel and iPrism detects the tunnel to be down for any reason, the tunnel restarts automatically. This maintains the tunnel across reboots.

1. From the iPrism home page, select **Maintenance**, then **Support Tunnel**.
2. The **Remote Host** and **Port** are pre-populated with the iPrism Technical Support tunnel server's information.
3. In the **Expires** field, select the amount of time to keep this Support Tunnel active.
4. Click **Start**.
5. If directed, click **Stop** to stop the support tunnel.

Test Directory Services

This allows the administrator to test user credentials on the directory server. A directory service can only be tested if it is enabled and available.

1. From the iPrism home page, select **Maintenance**, then **Test Directory Services**.

2. Enter a username and password.
3. Select the LDAP server or domain to test.
4. Click **Test Credentials**.

CHAPTER 7 System Settings

This section describes how to change iPrism's internal settings and set your preferences for common iPrism activities.

Central Management

See [Central Management](#).

Customizable Pages

iPrism's Customizable Pages allow you to fully customize several of the default pages used by iPrism.

The following pages can be customized:

- Authentication
- Access denied
- Quota notification
- Warning notification
- All other pages (pages the user sees)
- Reporting logo



Note: Only the iPrism administrator/Super Admin account (iprism) can customize these pages.

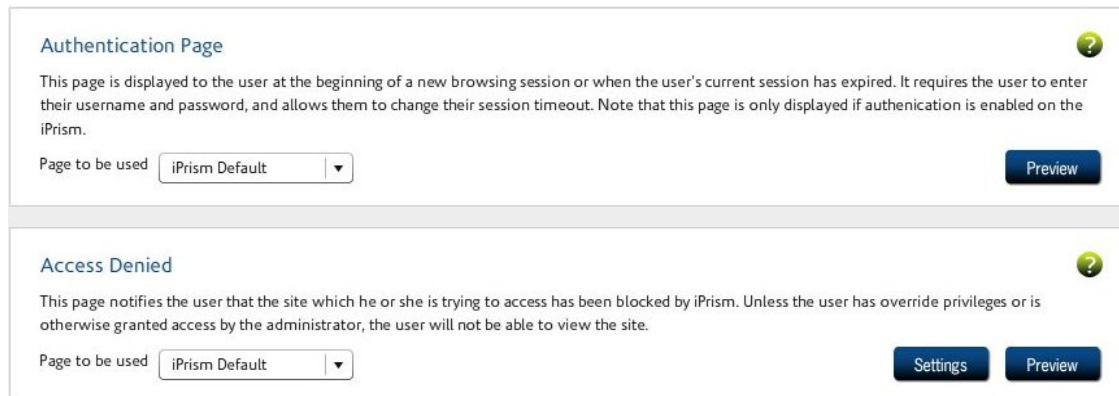


Figure 60. iPrism Customizable Pages

Customizing Pages

1. From the iPrism home page, select **System Settings**, then **Customizable Pages**.
2. If you first want to view the default page, make sure **iPrism default** is selected for that page and click **Preview**.
3. In the frame for the page you want to customize, select the type of customization from the dropdown list and configure the settings (see below).
4. When you are finished customizing pages, click **Save** to save your changes.
5. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Authentication, Access Denied, Quota Notification, and Warning Notification Pages

Customized HTML


To change the contact name:

- Click **Settings**, change the wording, and click **OK**.

This option is available for the access denied, quota notification, and warning notification pages.

To customize the page:

1. Click **Customize**.

2. Use the design window to change the page as needed. For a listing of customizable page tags, see [Customizable Page Tags](#).
3. Click  when you are done editing.
4. Click **Yes** to save the changes.

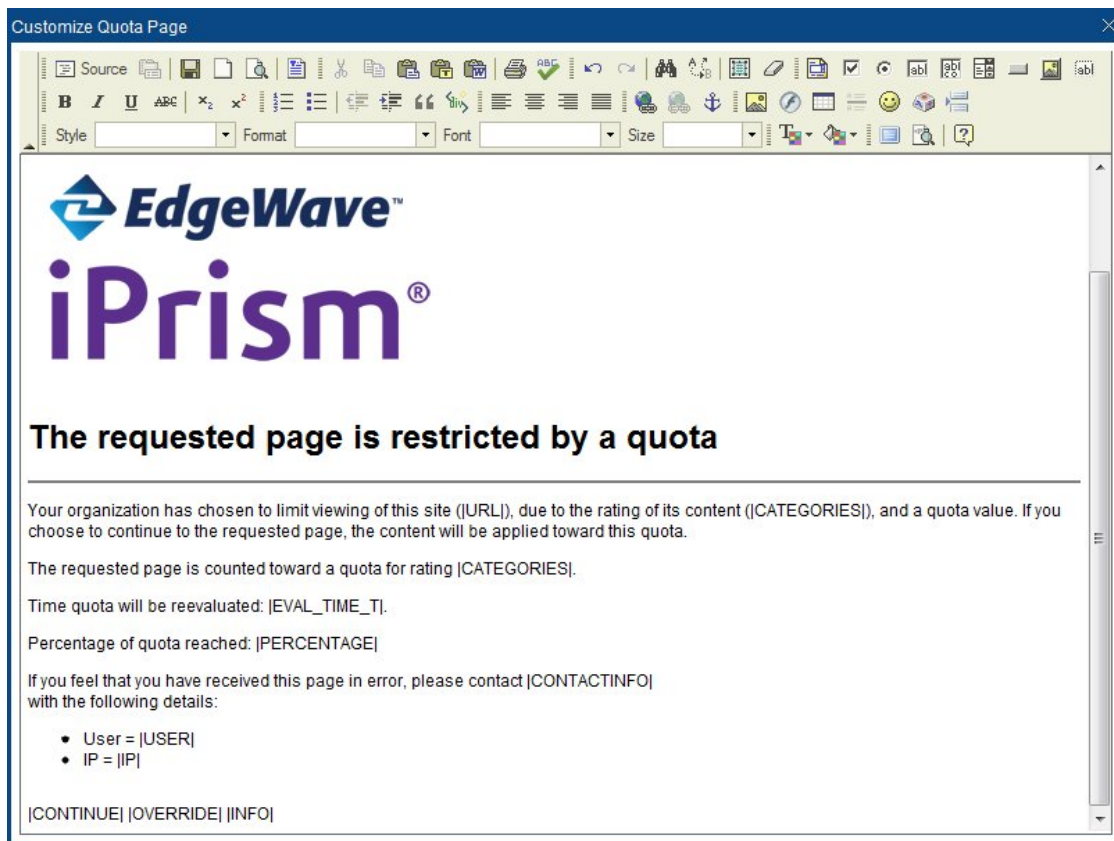


Figure 61. Customizing the Quotas Page

Specified URL

Note that this is not available for the Authentication page.

1. Type the URL to be used in the URL field.
2. Click **Preview** to preview the page the user will see.

All Other Pages

1. Click **Customize**.
2. On the HTML tab, select a theme for the page (**Default** or **Custom**).

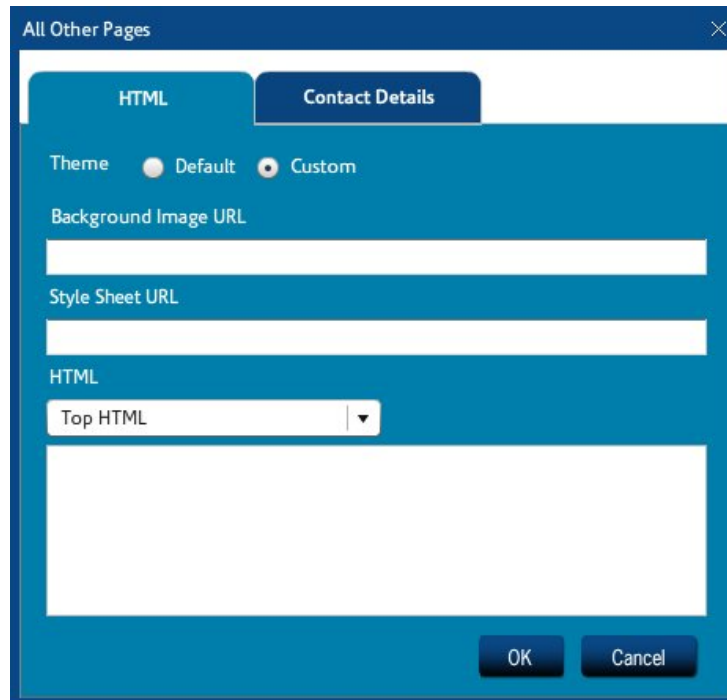
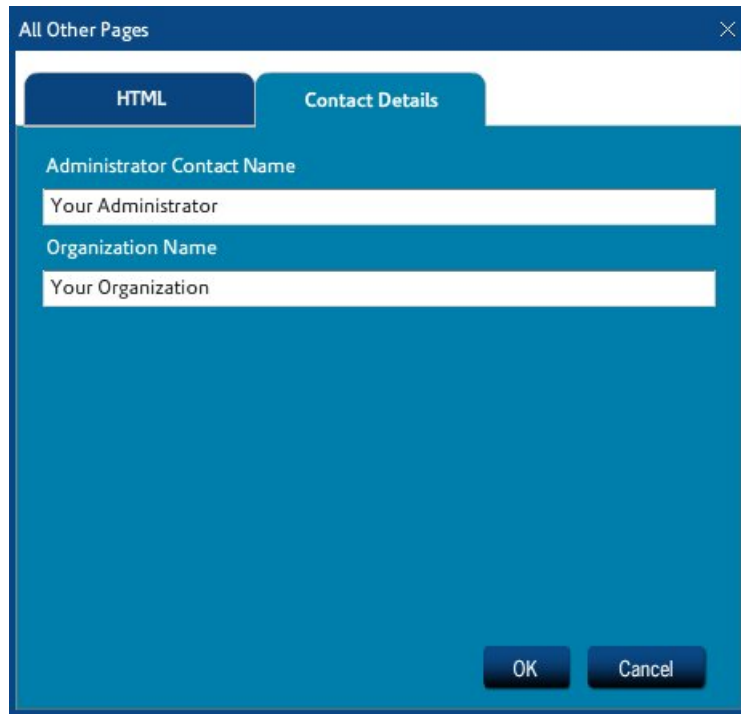


Figure 62. Customizing the Other Pages

3. If you want to use a background image, enter the URL.
4. If you want to use a style sheet, enter the URL.
5. Select where the HTML code will reside (Top, Left, Right, or Bottom).
6. Click the **Contact Details** tab.



The screenshot shows a dialog box titled "All Other Pages" with a close button (X) in the top right corner. It features two tabs: "HTML" and "Contact Details". The "Contact Details" tab is active, showing two text input fields. The first field is labeled "Administrator Contact Name" and contains the placeholder text "Your Administrator". The second field is labeled "Organization Name" and contains the placeholder text "Your Organization". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Figure 63. Customizing the Contact Details

7. Enter the administrator contact name and organization name.
8. Click **OK**.

Reporting Logo

To customize the logo that shows on reports:

1. Select **Customized Logo** from the dropdown list.
2. Click **Yes** to confirm.
3. Navigate to the folder containing the logo file.
4. Select the logo file.
5. Click **Open**.

Customizable Page Tags

Use the following tags to insert relevant iPrism information and tools.

Tag	Description
FORM_START	The starting HTML FORM element. This tag must be placed before any form input elements.
CACHE_USER	The value entered in as the username. Use this when an authentication attempt fails. On the next display of the page, the Username field is populated with the cached value.
SUBMIT	A Submit button to process the user authentication form. This tag must be placed last of all the HTML input elements.
PROTO	iPrism's protocol, either "HTTP" or "HTTPS".
NTLM_DOMAINS	The text label " NTLM Domains " and a dropdown select box of NTLM Domains. This tag will get replaced with an HTML table row containing a text label and a dropdown selection box containing your NTLM Domains. (This tag can only be used when NTLM is enabled and configured.)
PORT	The port on which iPrism's web server is running.
TIMEOUT	The configured default timeout value.
LOGOUTLINK	A hyperlink to the logout page.
HOST	The configured hostname or IP address of iPrism.
ERROR_MESSAGE	An error message (if any).
OVERRIDE	An Override button, which allows for override access.
CONTACTINFO	The Administrator's contact information.
URL	The URL of the site that is trying to be accessed.

Tag	Description
INFO	An Information button, which provides more information about the Access Denied page.
RATING	The rating of the site trying to be accessed.

Directory Services

iPrism can be configured to filter Internet traffic in a variety of ways.

- **By IP address.** Each IP address range is assigned a Web Profile and an Application Profile. If, however, the user moves from one system to another (e.g., a desktop workstation with a very open profile to a lab machine with a very restricted profile), the more restrictive profile applies.
- **By username.** Three different sources are accessed for user information:
 - **Redirect their first web access to an iPrism login page:** Once a user logs in, iPrism knows who they are and can provide filtering based on the profiles assigned to their username.
 - **Local authentication:** For a limited set of users, a local user list resides on the iPrism itself, which does not require contacting an external authentication server (for more information, [Local Authentication](#)).

We recommend that you use **local authentication** only when you initially set up your iPrism. It is the simplest form of authentication and is extremely easy to set up. This will give you a chance to see how the iPrism authentication system works on a limited basis, without having to worry about what may be going on between a Directory Service and iPrism.

- **Protocols to connect to Directory Services:** For a larger user base, iPrism can be configured to use a Windows 2008 (Kerberos), Windows 2000/2003 (NTLM), or LDAP (Unix, Linux, Novell, Mac OS X) directory service.

See [Microsoft Windows Active Directory Authentication \(Active Directory 2008\)](#) for details on Windows authentication, and [LDAP Authentication](#) for information on LDAP authentication.

After you gain experience with the system, you will most likely want to connect to a Directory Service by configuring your iPrism to use Windows 2008 (Kerberos), Windows 2000/2003 (NTLM), or LDAP-based authentication. This will expand your user base to a much wider audience.



Note: iPrism can use only one directory service at a time.

iPrism can also determine a user's identity in a variety of ways, such as several types of login screens, proxy-based authentication, and the Auto-Login feature. For details on Auto-Login, see [Auto-Login Details](#).



Note: iPrism can only authenticate web-based connections. Due to how IM and P2P protocols work, user-based authentication is impossible, so the iPrism uses IP-based profile mapping for these protocols.

If a user cannot be authenticated, they will not be able to use the Internet.

Choosing an Authentication Mechanism

Network-based profiles do not require authentication to be enabled. If authentication is enabled, users **must** authenticate to access the Internet.

iPrism supports the following authentication mechanisms:

- **Local**
- **Kerberos:** this uses a Windows Domain Controller (2003 or 2008) with Active Directory, with the iPrism in Server 2008 mode
- **NTLM** (Windows 2000, Windows 2003): with the iPrism in Server 2003 mode
- **LDAP**
 - Novell NetWare with eDirectory
 - OSX with Open Directory

Active Directory on Windows 2003 is LDAP-compliant by default. For more details about LDAP on Windows. For more information, see the following iPrism Knowledgebase articles:

- Windows 2000/2003 LDAP Authentication
- Windows Active Directory 2008 Authentication
- Migrating from AD2003 to AD2008

For OS X with Open Directory, refer to the iPrism Knowledgebase article: [Integrating iPrism with OS X Open Directory](#).

The knowledgebase articles are available at: , available at www.edgewave.com/support/web_security/knowledgebases.asp.

Local Authentication

The iPrism's local authentication system lets you define a set of users on the iPrism itself. No Directory Service is involved. Even if you have an external authentication server, the local user list allows you to provide a small number of people administrative access rights to iPrism.

To create user accounts on the iPrism:

1. From the iPrism home page, select **Users & Networks**, then **Local Users**.
2. Follow the instructions in [Local Users](#) to add a local user and add/edit administrative privileges.

LDAP Authentication

LDAP centralizes and makes user information available on a network. The iPrism can authenticate users and, optionally, obtain access information (an iPrism Access Profile name) for those users from an LDAP server.

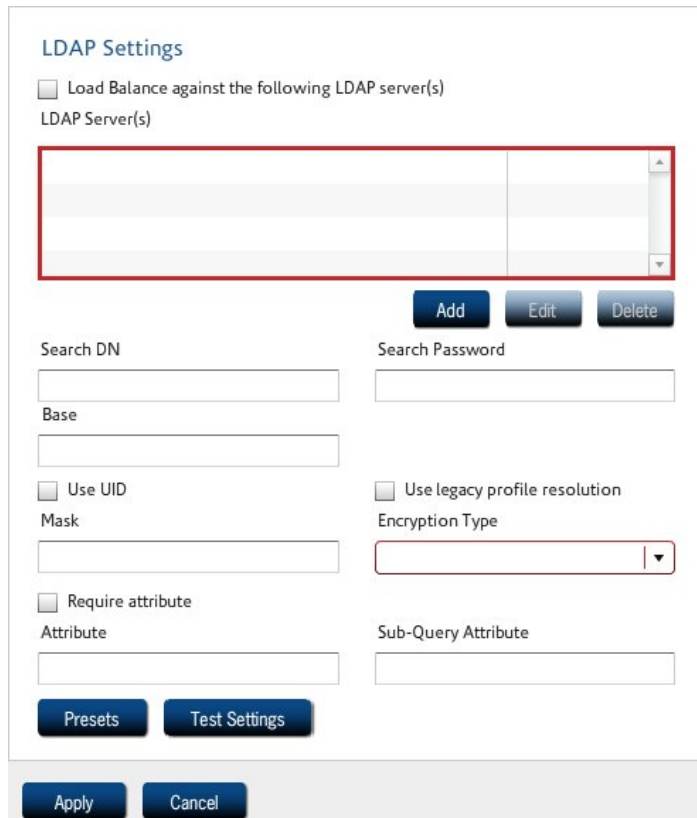
Each user object within the LDAP directory may contain many attributes to associate with the user (such as password, phone number, full name, etc.). For the iPrism to utilize users on a remote LDAP server, that server must perform simple LDAP binds (authentications) to the user's node. When these binds fail (i.e., passwords don't match), then the iPrism considers the authentication to have failed, and the associated service access (Web Proxy) consequently fails.



Note: LDAP authentication does not implement the Simple Authentication and Security Layer (SASL) mechanism.

Setting up the iPrism LDAP Client

1. From the iPrism home page, select **System Settings**, then **Directory Services**.
2. Click **Configure & Join**.
3. From the **Authentication Mode** dropdown list, select **LDAP**.



The image shows a 'LDAP Settings' configuration window. At the top, there is a checkbox labeled 'Load Balance against the following LDAP server(s)'. Below it is a table with the header 'LDAP Server(s)' and an empty table body. To the right of the table are three buttons: 'Add', 'Edit', and 'Delete'. Below the table are several input fields: 'Search DN', 'Search Password', 'Base', 'Mask', 'Attribute', and 'Sub-Query Attribute'. There are also two checkboxes: 'Use UID' and 'Use legacy profile resolution'. A dropdown menu for 'Encryption Type' is also present. At the bottom of the window are two buttons: 'Presets' and 'Test Settings'. At the very bottom of the window are two buttons: 'Apply' and 'Cancel'.

Figure 64. LDAP Authentication

4. Complete the necessary information for the LDAP server to which iPrism will connect.

OR

To use preset information, click **Presets** and select from the following options:

- Active Directory (Multi-Domain)
- Active Directory (Single-Domain)
- NDS
- OSX

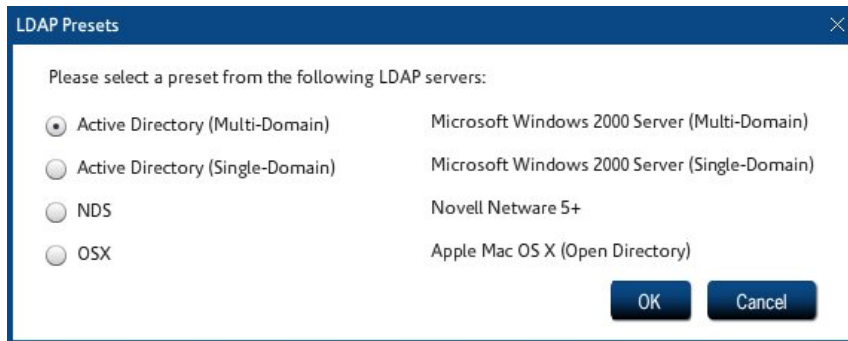


Figure 65. LDAP Presets

5. Click **Test Settings** to test LDAP server connectivity. Once connected, an LDAP bind attempt using administrative credentials is made to configure the base.
 - If either the primary server or backup server test is successful, a notice indicating that the test was successful is displayed.
 - If the server test is successful, the backup server is not tested.
 - If the server fails, then the backup server is tested.
 - If there is an error with the connection or binding, a notice indicating at which point in the test failed is displayed.
6. To test the server and ports, enter incorrect information for both the server and port and click **Test Settings**. When the server test fails due to the incorrect information, the backup server is tested. The connect and bind process described above for the server test is attempted for the backup server, and the appropriate success or error message is displayed.

Authentication from the User's Perspective

When a user first accesses the Internet, they are automatically authenticated if Auto-Login is enabled and functioning. Otherwise, they see an authentication.

1. Type your username and password to be allowed onto the network.
2. If necessary, select a domain from the **Domain** dropdown list.
3. Type a session timeout (in minutes).
4. Click **Authenticate**.

Microsoft Windows Active Directory Authentication (Active Directory 2000/2003)

To implement NTLM authentication in iPrism using a Windows 2003 server network, complete the following steps.

1. From the iPrism home page, select **System Settings**, then **Directory Services**.
2. Click **Configure & Join**.
3. From the Authentication Mode dropdown list, choose **Server 2000/2003**.
4. Type your domain in the **NT Domain** field.
5. Type your fully qualified domain name in the **Active Directory Realm** field.
6. In the Machine Account field, specify a unique machine account name for iPrism. (iPrism must establish a machine account on the NT domain.)



Note: The account will be created with this name and should be defined so as to not conflict with other machine accounts on the domain. This new account must remain, as created by the Join operation, for the duration of iPrism's participation within the domain. If the account is accidentally removed from the NT server, the Join procedure must be repeated again.

7. Type the username and password of the user account that belongs to the Domain Administrator group in the **User name** and **Password** fields, respectively.



Important: The username must be a member of the Domain Admins group for the Active Directory domain.

This account need not be in the same AD domain as the iPrism is joining. However, this account **MUST** have administrative rights in the AD domain that the iPrism is joining. (Permissions may be granted via a trust relationship between domains.)

The only allowable formats are as follows:

Username (e.g., jdoe)

NT Domain\Username (e.g., SALES-ABC\jdoe)

Username@ADDomain (e.g., jdoe@sales.abc.com)

8. Type the IP addresses of the domain controllers you wish to use in the Domain Controllers field. Multiple IP addresses must be separated by commas.
9. Click **Join**.
10. Save your configuration by clicking **Save**.
11. If all settings are correct and the join was successful, under **Authentication Mode & Status**, you will see the authentication mode, the status (e.g., joined) and whether the iPrism is connected.
12. Set up your clients' browsers. For instructions on specific browsers, see:
 - [Configuring Firefox for Proxy Mode](#)
 - [Configuring Safari \(Mac OS X only\) for Proxy Mode](#)
 - [Configuring Internet Explorer for Proxy Mode](#)



Important: Users must proxy to iPrism's fully qualified domain name, not the IP address.

Assigning iPrism Profiles to Windows AD Global Groups

Refer to [Groups](#).

Microsoft Windows Active Directory Authentication (Active Directory 2008)

iPrism now supports authentication using Kerberos against the Windows Active Directory 2008 domain. For a visual representation of how Active Directory 2008 works in the iPrism environment, see below. For a description of how the Active Directory (AD) environment works in general, refer to the iPrism Knowledgebase at www.edgewave.com/support/web_security/knowledgebases.asp.

To set up your iPrism to authenticate against an Active Directory 2008 server, you must have the following prerequisites in place, then complete the steps below .

Prerequisites

- You must know the iPrism's fully qualified domain name and IP address (in our example, `jdoe.sales.abc.com`).
- This name must match the domain of the iPrism (in our example, `jdoe.sales.abc.com`).
- You must know the IP address of your AD2008 server (in our example, `10.1.1.57`).
- You must know the NT domain (NetBIOS name); in our example, `CORPSALES`.

- The client machines must be able to resolve the iPrism fully qualified domain name via DNS.
- You must know an AD username (and password) that is a member of the “Domain Admins” group.
- All clients must be given unique host names, or authentication failures will result.



Important: If you have restored a system configuration, you must explicitly specify the domains and rejoin.



Note: The DNS server used by iPrism should be the AD2008 server. If the AD2008 server is not the organization’s DNS server, the organization’s DNS server must be configured to provide the service records that an Active Directory server provides.

Setting up iPrism to authenticate against a Windows 2008 server

1. From the iPrism home page, select **System Settings**, then **Directory Services**.
2. Click **Configure & Join**.
3. From the **Authentication Mode** dropdown list, choose **Server 2008**

Domain Settings

NT Domain: EDGEWAVE

Active Directory Realm: edgewave.com

Machine Account: ip18477

Domain Controller(s): 172.27.3.41

Buttons: Add, Edit, Delete

Username: [Empty]

Password: [Empty]

Advanced Settings

Auto-login Redirection Settings - only relevant in Bridge (transparent) mode

DNS [Dropdown]

Requires iPrism host entry into all participating network zones.

Buttons: Join, Cancel

Figure 66. Active Directory 2008 Authentication

4. Your NT Domain, Active Directory Realm, Machine Account, and Domain Controllers will be populated. You can change any of these if necessary.
 - If you change the prepopulated Active Directory Realm, you must use a fully qualified domain name.
 - If you change the Machine Account, you must specify a unique machine account name for iPrism. (iPrism must establish a machine account on the NT domain.)




Note: The account will be created with this name and should be defined so as to not conflict with other machine accounts on the domain. This new account must remain, as created by the Join operation, for the duration of iPrism's participation within the domain. If the account is accidentally removed from the NT server, the Join procedure must be repeated.

5. Type the username and password of the user account that belongs to the Domain Administrator group in the **User name** and **Password** fields, respectively.
 - The username must be a member of the "Domain Admins" group for the AD 2008 domain.

- This account need not be in the same AD domain as the iPrism is joining. However, this account **MUST** have administrative rights in the AD domain that the iPrism is joining. (Permissions may be granted via a trust relationship between domains.)

The only allowable formats are as follows:

```
Username (e.g., jdoe)
NT Domain\Username (e.g., SALES-ABC\jdoe)
Username@ADDomain (e.g., jdoe@sales.abc.com)
```

6. **Advanced Settings** is not used in AD2008 mode.
7. Click **OK**.
8. Bridge (transparent) mode only: **Auto-Login Redirection Settings**. When using Server 2008, DNS is the only option available for Auto-Login redirection settings. DNS redirection is required for Auto-Login, because iPrism uses its fully qualified domain name to generate Kerberos keys during Auto-Login. The name iPrism uses for redirection must agree with this name. Setting DNS redirection causes the iPrism to use the same name for both its Kerberos keys and for redirection. For more information about how DNS works with Auto-Login, see the iPrism Knowledgebase article “How do I resolve iPrism’s IP address using DNS?”
9. If your settings are correct, click **Join** in the Join Domain Settings frame.
 -  **Important:** This may take a few minutes. If there is a problem, you will receive an error message. As long as the progress bar is working, do not click **Cancel** or assume there is a problem.
10. Click **Yes** to confirm.
11. Save your configuration by clicking **Save**.
12. If all settings are correct and the join was successful, under **Authentication Mode & Status**, you will see the authentication mode, the status (e.g., joined) and whether the iPrism is connected.
13. Set up your clients’ browsers. For instructions on specific browsers, see:
 - Configuring Firefox for Proxy Mode
 - Configuring Safari (Mac OS X only) for Proxy Mode
 - Configuring Internet Explorer for Proxy Mode



Important: Users must proxy to iPrism’s fully qualified domain name, not the IP address.

Migrating from AD 2003 to AD 2008

If you want to migrate your AD 2003 environment to AD 2008, see the Knowledgebase article “Migrating from AD 2003 to AD 2008” at www.edgewave.com/support/web_security/knowledgebases.asp.

Enterprise Reporting

The Enterprise Reporting Server (ERS) for iPrism provides consolidated reporting for up to thirty (30) iPrism systems. ERS is able to quickly and easily process large amounts of data from iPrism and produce consolidated reports.

For detailed information about ERS and how to use it, go to

<http://edgewave.com/support/ers/help/ers.htm>

Event Logging

Syslog Export

iPrism reporting’s real-time monitor gives you instant access to all monitored Web, IM, and P2P events. This is the preferred tool for viewing these events.

iPrism can export Web, IM, and P2P events using the syslog protocol. To use this feature, you need a system with a syslog client running and configured to accept events from an external source.

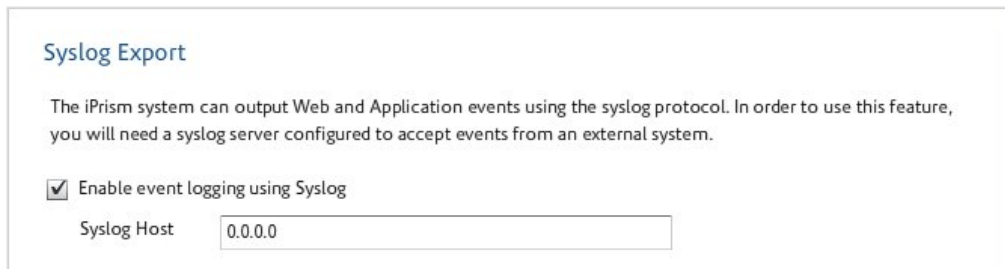


Note: Most UNIX-based systems do not accept external connections by default. This is a security feature.

Syslog is a common UNIX, Linux and FreeBSD communication protocol used for communicating event information. There are also a few Microsoft Windows-based syslog clients available.

To enable event export using syslog:

1. From the iPrism Home Page, select **System Settings**, then **Event Logging**.
2. Check **Enable event logging using Syslog**.



Syslog Export

The iPrism system can output Web and Application events using the syslog protocol. In order to use this feature, you will need a syslog server configured to accept events from an external system.

Enable event logging using Syslog

Syslog Host

Figure 67. Event Logging - Syslog Export

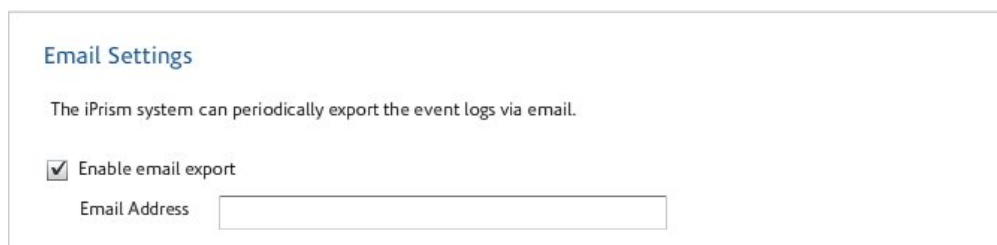
3. Type the IP address of the host which will receive the logging information in the **Syslog Host** field.
4. Click **Save**.
5. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Email Settings

iPrism checks for events on an hourly basis. If there are new events, and you have enabled email exporting as described below, these events will be emailed as a gzipped file to the address specified. Events of the last hour, if there are any, are included.

If you want to export security and application logs via email:

1. From the iPrism home page, select **System Settings**, then **Event Logging**.
2. In the Email Settings frame, check **Enable email export**.



Email Settings

The iPrism system can periodically export the event logs via email.

Enable email export

Email Address

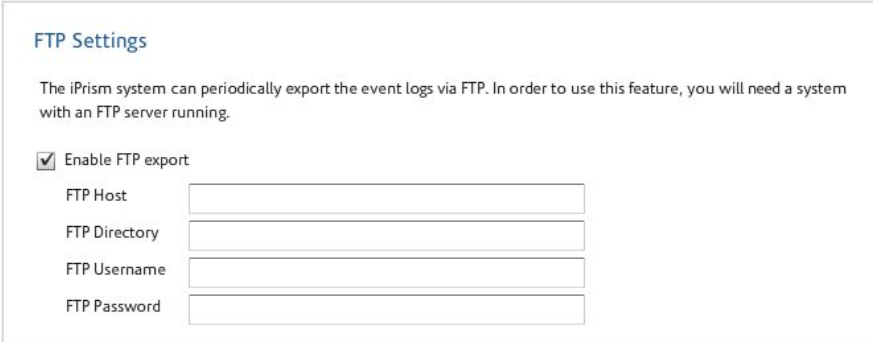
Figure 68. Event Logging - Email Export

3. Type the email address that will receive the logs.
4. Click **Save**.

5. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

FTP Settings

1. From the iPrism Home Page, select **System Settings**, then **Event Logging**.
2. In the FTP Settings frame, check **Enable FTP export**.



FTP Settings

The iPrism system can periodically export the event logs via FTP. In order to use this feature, you will need a system with an FTP server running.

Enable FTP export

FTP Host

FTP Directory

FTP Username

FTP Password

Figure 69. Event Logging - FTP Settings

3. Type the FTP Host, FTP Directory, FTP Username, and FTP Password in their respective fields.
4. Click **Save**.
5. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

High Availability

High Availability (HA) enables two iPrisms to run in parallel on a single network. One iPrism does the filtering while the other remains in standby mode, ready to take over in case the primary iPrism becomes inactive.

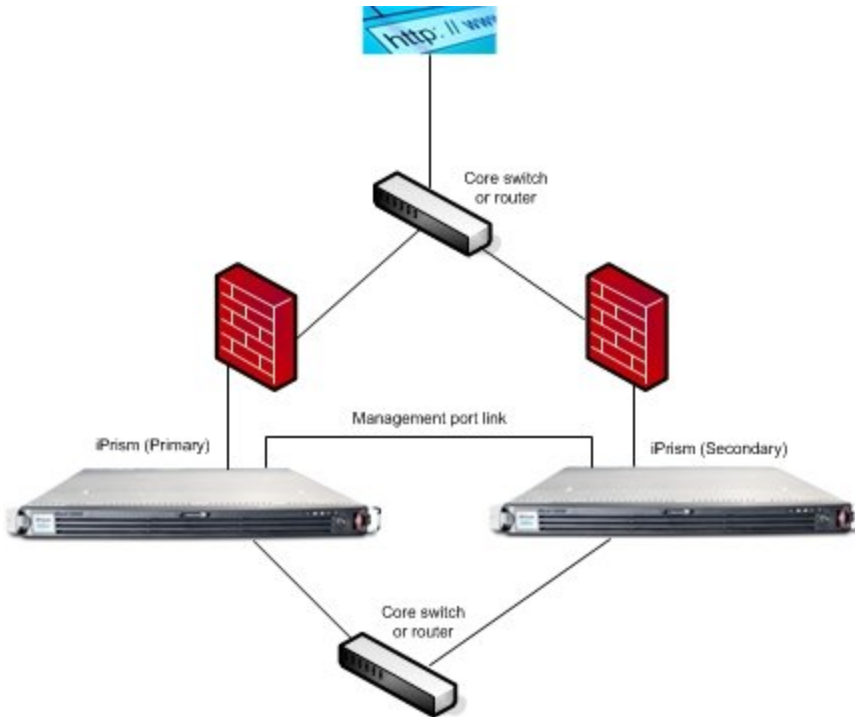


Figure 70. Parallel iPrisms

Setup

Before you can set up high availability:

- The management interface must be enabled on both iPrisms. See [Using the Management Interface](#) for more information.
- The iPrisms must be connected via the management port link. This can be either a crossover cable or a switched network.

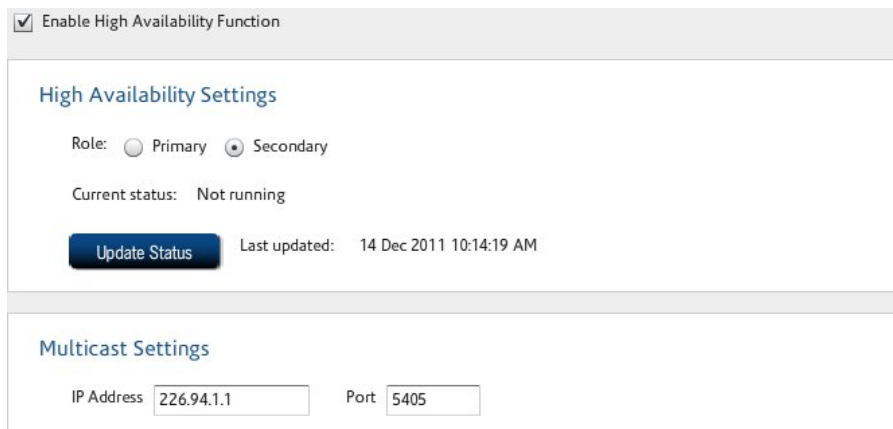


Note: Paired iPrisms use the management interface to keep track of each other's current running status. Interrupting this link results in a situation where both iPrisms believe the other is not working, which results in both becoming active at the same time.

To set up high availability:

1. From the iPrism home page, select **System Settings**, then **High Availability**.

2. Click **Enable High Availability Function**.



Enable High Availability Function

High Availability Settings

Role: Primary Secondary

Current status: Not running

Last updated: 14 Dec 2011 10:14:19 AM

Multicast Settings

IP Address Port

Figure 71. High Availability

3. Select whether this iPrism is **Primary** or **Secondary**. The primary iPrism is the designed active iPrism to filter all traffic. The secondary iPrism remains in standby mode, ready to take over if the primary fails.



Note: For HA to work properly, one iPrism must be designated as the primary and one as the secondary.

4. Leave the default multicast settings (these work for most networks) or change them for your network.
5. Select which interfaces are in use when the iPrism is in standby mode (available if needed, not currently active). These settings combine to determine whether iPrism can pass through traffic in standby mode. Turning any one of these settings OFF, prevents traffic from passing.
 - **Internal Interface On:** Leave the internal interface ON so you can configure your iPrism via a computer on the network.
 - **External Interface Off:** Leave the external interface OFF to prevent network looping.
 - **Bridge On:** Leave the bridge ON.



Note: If these settings are not appropriate for your network configuration, for either state (standby or failed), contact EdgeWave to understand how this will affect your network performance and security.

6. Select which interfaces are in use when the iPrism is in a failed state. The recommendations for these settings are the same as for standby. The internal and external interfaces can be enabled immediately, after a brief time delay, or not at all. If a time delay is chosen, the interface will be shut down for this time period when the iPrism fails, and then iPrism will attempt to turn the interface back on.

The screenshot displays two sections of the configuration interface. The top section, titled "Standby State Settings", contains three rows of radio button controls: "Internal Interface" with "On" selected, "External Interface" with "Off" selected, and "Bridge" with "On" selected. The bottom section, titled "Failed State Settings", contains three rows: "Internal Interface" with a dropdown menu set to "Enable after 1 minute", "External Interface" with a dropdown menu set to "Leave disabled", and "Bridge" with "On" selected.

Figure 72. Standby and Failed State Settings

7. Click **Save** to save your settings.
8. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Recovery

If an iPrism set up for HA fails, a new button, **Recover**, appears in the HA window.

To recover the iPrism:

1. Click **Recover**.

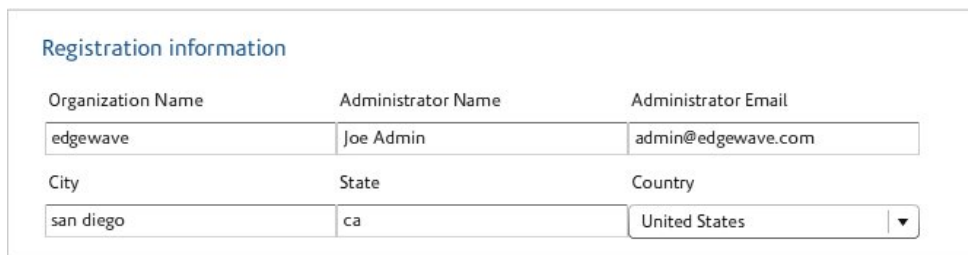
The iPrism comes back up (if the problem has been fixed) in standby mode. Leave it in this mode for several minutes so that it can complete its self checks. If this iPrism is configured as the primary, after the self-check is completed, a new button, **Take Control**, appears.

2. If you want the primary iPrism to become the active iPrism, click **Take Control**. If the iPrism is working properly, it becomes active and the other iPrism goes on standby.

License Key

This window allows you to complete information about the registered license key associated with your iPrism, and create an SSL certificate if necessary.

1. From the iPrism home page, select **System Settings**, then **License Key**.
2. In the Registration information, complete the necessary organizational and administrator information if you have not already done so in the Installation Wizard. If you enter the information here, you will be required to Save and Activate Changes before uploading a license key.
3. Click **Save**.
4. Click **Activate Changes** to activate these changes immediately.



The screenshot shows a form titled "Registration information" with the following fields:

Organization Name	Administrator Name	Administrator Email
edgewave	Joe Admin	admin@edgewave.com
City	State	Country
san diego	ca	United States

Figure 73. Registration Information

iPrism Certificates

You must complete these steps before uploading a license key.



The screenshot shows a form titled "SSL Certificate" with the following elements:

Common Name: Use IP Address (172.27.18.11)

Buttons: Create Certificate, Create/View Request, Upload Certificate, Upload Certificate Chain

Figure 74. SSL Certificate

If you have an external SSL Certificate:

- Click **Upload Certificate**.

**Notes:**

If you upload an external certificate, you will not be required to Activate Changes.

You may now be automatically logged out of iPrism. You must log back in for the keys to take effect.

If you cannot log back in, clear your browser cache and refresh your browser.

If you need to create an iPrism server certificate:

1. Click **Create/View Request** to generate a Certificate Signing Request (CSR), which you can then use to obtain a trusted Server Certificate.
2. To create a self-signed certificate from your registration and license key information, select **Create Certificate**.

You can select the Common Name to be used in the SSL Certificate. Available options are **Use IP Address**, **Use Short Name** or **Use FQDN (Fully Qualified Domain Name)**. This common name will also be used for redirection of pages.

- For Server 2008 mode, **Use FQDN**.
- For Server 2000/2003 mode, **Use Short Name** (for DNS redirection). **Use IP Address** for IP redirection.
- For other modes, use any Common Name option.

Common Name Recommended Values:

Authentication Mode	Redirection Specification	Recommended Common Name Value
No Directory Set		IP Address
NT, AD 2000/2003	IP set as Auto-Login redirection	IP Address
NT, AD 2000/2003	DNS set as Auto-Login redirection	Use Short Name
AD 2008		Fully Qualified Domain Name (FQDN)
LDAP		IP Address

3. When you are finished, click **Create Certificate**. A new SSL certificate will be created and applied immediately. You will be automatically logged out, and returned to the Login page.

For a detailed example of how to request and install a trusted server certificate, see the iPrism Knowledgebase:

www.edgewave.com/support/web_security/knowledgebases.asp

Uploading Your License Key

To upload your iPrism license key and Remote Filtering feature key from a local file:

1. Click **Upload License**.
2. Locate the file containing these keys and click **Open**.

If the key is valid and uploads successfully, you will receive a confirmation message.



Note: If you do not have a local license key file, contact your EdgeWave sales representative for a key.

Upload License Key

Key: Subscription expires: 5 Nov 2014

Feature Key: Subscription expires: 5 Nov 2014 (Remote Filtering)

?

Figure 75. Upload License Key

Local Categories

Local Categories displays a list of the local categories that have been set up. Most of the local categories are named local1, local2, etc. However, there are two special names: **Local Allow** and **Local Deny**. These are intended to be used in a specific way.

Local Allow is reserved for web pages that you want everyone to access. It is automatically cleared (i.e., not blocked or monitored) in any new ACL that is created. iPrism uses this category as part of its Custom Filters feature to grant clearance to blocked URLs. It is recommended that you keep this category cleared in any new or existing ACLs. Local Allow is monitored in both the BlockOffensive and PassAll default profiles.

Local Deny is designed for web pages that no one should see. It is automatically checked (both blocked and monitored) in all new ACLs that are created, and should also be checked in all existing profiles (except the default “PassAll” profile). iPrism uses this category as part of its Custom Filters feature to let users instantly deny access to any URL.



Important: The Local Allow and Local Deny categories are, by default, used internally by iPrism’s Custom Filters and Override features. It is strongly recommended that you keep Local Allow cleared (unchecked) and Local Deny checked in all of your profiles. These settings will automatically default in all new ACLs. If desired, you can change which categories iPrism uses to allow/deny access from within Custom Filters.

The numbered local categories (local1, local2, etc.) can be used for any filtering purpose. For example, if you want to block access to the websites of your competitors, you could do this:

1. Create a custom filter for each website to which you want to block access and assign all of them to the same local category (e.g., local5).
2. In **Filtering > Profiles**, edit the active profile so that the local category (e.g., local5) is blocked (and monitored, if desired).
3. Now, any website that belongs to the local5 rating will be blocked by this profile.



Note: When using local filters, it is up to you to keep track of which sites are assigned to each category. To view local categories, from the iPrism home page, select **System Settings**, then **Local Categories**.

Local Category No	Local Category Name
local1	User defined values
local2	User defined values
local3	User defined values
local4	User defined values
local5	User defined values
local6	User defined values

Figure 76. Local Categories

Network ID

In the Network ID window, you can configure your network settings, including host name, internal, external, and management interfaces, and configuration mode.

To set up iPrism on your network:

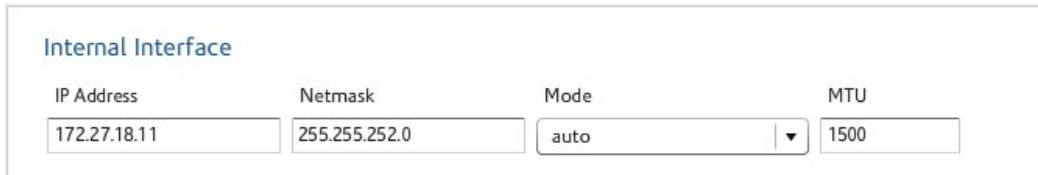
1. From the iPrism home page, select **System Settings**, then **Network ID**.
2. In the **Host Name** field, type the fully qualified domain name of your iPrism host.



The screenshot shows a configuration form titled "Identity". Below the title is the label "Host Name (Fully Qualified Domain Name)". There is a text input field containing the value "ip18477.edgewave.com". To the right of the input field is a small green circular icon with a white question mark and a right-pointing arrow.

Figure 77. Network Identity

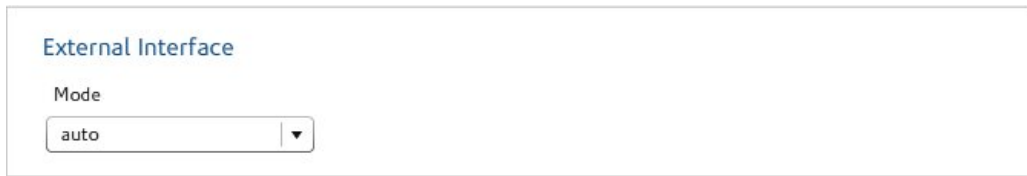
3. Select a mode in which to configure your iPrism (**Bridge (transparent)** or **Proxy (single-interface)**).
4. In the Internal Interface frame, type the IP address of your iPrism's internal interface in the **IP Address** field. To verify which port is the internal interface, refer to the *iPrism Installation Guide*.



The screenshot shows a configuration form titled "Internal Interface". It contains four input fields: "IP Address" with the value "172.27.18.11", "Netmask" with the value "255.255.252.0", "Mode" with a dropdown menu showing "auto", and "MTU" with the value "1500".

Figure 78. Internal Interface

5. In the **Netmask** field, type the netmask you want to use (e.g., 255.255.255.0).
6. Select a mode (**Auto**, **10**, or **100**) from the **Mode** dropdown list.
7. Type a value for the network parameter for Ethernet frame size in the **MTU** (maximum transmission unit) field if necessary (the default is 1500).
8. If you have checked Bridge (transparent) in step 3 above, the External Interface field frame will be enabled (if you have selected Proxy (single-interface), this frame will be disabled). Select a **Mode (Auto, 100, or 1000)**.



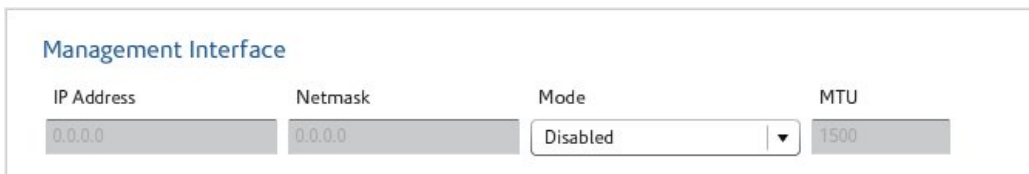
External Interface

Mode

auto

Figure 79. External Interface

9. If you are using a Management Interface, select a **Mode (Auto, 100, or 1000)** from the Mode dropdown list in the Management Interface frame. If you are not using the Management Interface, leave the Mode as **Disabled**.

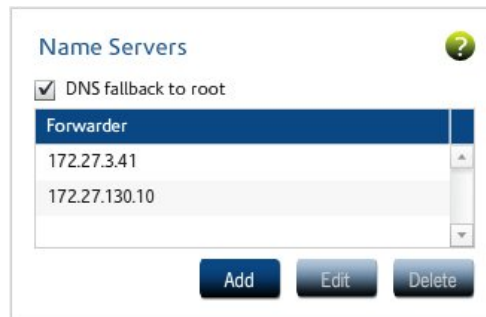


Management Interface

IP Address: 0.0.0.0 Netmask: 0.0.0.0 Mode: Disabled MTU: 1500

Figure 80. Management Interface

10. iPrism constantly resolves Internet host names to their IP address, as well as reverse map IP addresses to their host names. If iPrism's installed environment allows direct Internet access, it will (by default) use its built-in name resolver to perform all DNS tasks. However, some installations require that iPrism defer all DNS lookups to another name server, called the forwarder name server. In these cases, you'll need to designate the IP address of this forwarder name server.



Name Servers

DNS fallback to root

Forwarder

172.27.3.41

172.27.130.10

Add Edit Delete

Figure 81. Name Servers



Note: Although it is possible to run iPrism without specifying a name server, it is not advised. Many of iPrism features such as the anti-spoofing filter depending on being able to contact a name server and will not work if no DNS server is available.

If you want to modify the built-in name server, double-click the existing name server in the list and type a new IP address. Click **OK** when you are done.

If the specified name server is not available, the iPrism will attempt to resolve the name through a root name server if the **DNS fallback to root option** is checked.



Note: When using a forwarder, it is highly desirable to use the same DNS server as used by the workstations. In this way, the DNS information will be cached when iPrism asks for it, reducing the latency of the request.

11. To use iPrism as a standalone DNS server, it must be able to issue DNS queries to the Internet. This requires that iPrism be able to access the Internet for the DNS protocol. In this case, the **Forwarder** field should be left empty.



Note: Although iPrism ships with an internal DNS server, it is always preferable (i.e., faster) to use a name server instead.

It is possible to configure iPrism to use up to three parent servers, to ensure that iPrism will always be able to resolve host names to IP addresses (and vice versa), even if the primary parent server is not available.

To specify multiple parent servers, enter their IP addresses, separated by a comma, in the **Forwarder** field. Enter the IP addresses in the order that you want them to be accessed. For example:

```
192.168.0.1,192.168.0.2,192.168.0.3
```



Note: In forwarding mode, iPrism is at the mercy of its parent name server. If the parent server fails (the first server in this list), iPrism will not be able to resolve names and consequently, not operate effectively. iPrism will not keep hunting for an answer when configured with multiple name servers.

12. iPrism must have a default route set. In more complex situations you may need to set static routes as well. To edit iPrism's default route, enter the desired IP address in the **Default Route** field.



Figure 82. Routing

13. Some routers constantly exchange this type of network information via Routing Information Protocol (RIP) updates. If your routers support RIP, you can have iPrism listen for these updates.



Note: iPrism supports versions 1 and 2 of the RIP protocol.

14. To enable this functionality in iPrism, check the **Listen to RIP updates** box in the Routing frame. When iPrism is listening to RIP updates, changes to local network configurations will automatically propagate to iPrism.

If using RIP is not an option, you will need to create static routes in order for iPrism to “see” workstations that are on a different IP network.

15. iPrism is a network appliance, and as such, must know how to exchange packets with workstations and servers at your organization, as well as servers on the Internet. By default, iPrism monitors workstations and servers that are attached to the same IP network. However, if you want iPrism to communicate with workstations on other IP networks, you must define “static routes” to these networks so iPrism can access them. In other words, if you have a local network that is not reachable via the default route, then you must provide iPrism with information about how to access this network.
16. In the Routing frame, click **Static Routes**.
17. Click **Add**.
18. To change the range of addresses behind the static route, in the IP field, type the base IP address of the subnet that lies behind the route.
19. Type a Netmask in the Netmask field. This defines the series of workstations in the remote location that you want to reach.



Figure 83. Add Static Route

20. In the Gateway Address field, type the IP address of the Internal router/gateway that connects iPrism to the workstations you specified above.
21. Click **OK**. The new route displays in the Static Routes frame.
22. Repeat this procedure as necessary to create additional static routes in iPrism.
23. When you are finished, click **OK**.
24. Click **Save** to save your changes.
25. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Network Services

The Network Services window allows you to configure various aspects of your network topology, including Network Hardening, SNMP, WCCP, SMTP Relay, and Co-Management Network.

To set up iPrism on your network:

- From the iPrism home page, select **System Settings**, then **Network Services**.

Network Hardening (Protecting Against DoS Attacks)

A DoS (Denial of Service) attack occurs when a malicious person tries to shut down a network by flooding it with network traffic. Usually the traffic is designed to use the maximum amount of system resources; e.g., initiating a connection but not finishing the process. (This consumes the memory needed to hold the information on the half-open connection.)

To enable DoS protection:

1. From the iPrism home page, select **System Settings**, then **Network Services**.
2. In the Network Hardening frame, check **Enable Denial of Service Protection**. The iPrism will now detect DoS attacks and limit the resources that a malicious machine can consume on the system.



Figure 84. Enable DoS Protection

Enabling SNMP

The Simple Network Management Protocol (SNMP) is used with iPrism to monitor iPrism appliance(s) for conditions that warrant the iPrism administrator's attention. iPrism SNMP is available on the standard SNMP port of 161.

If you want to monitor iPrism using SNMP, you can use a standard MIB-2 file with any MIB browser. For example, a free MIB browser is available at www.ireasoning.com/mibbrowser.shtml (no endorsement implied); this browser offers a large number of sample MIB files (including a few MIB-2 files). Once in the iPrism, a list of available SNMP Object Identifiers (OIDs) will be displayed.

The SNMP Community String

An SNMP community string consists of four (4) or more alphanumeric characters and functions much like a password, permitting access to the SNMP protocol.

To enable SNMP:

1. From the iPrism home page, select select **System Settings**, then **Network Services**.
2. In the **SNMP** frame, check **SNMP**.

The community string is now available.



Note: The same community string must be used in both the MIB browser and the iPrism.

SNMP
Community

Figure 85. Enabling SNMP

WCCP

iPrism supports the WCCP protocol (versions 1 and 2). WCCP provides fault tolerance by automatic detection and rerouting to eliminate network downtime in the event that iPrism is turned off, disconnected, or a system failure occurs.

For WCCP v2 specifically, iPrism supports the following:

- Specification of up to 32 routers (IP addresses).
- Optional specification of a service group password if desired.



Important: WCCP v2 does not support the use of a multicast IP address for a group of routers. Users must specify each of the router addresses they want to use. Validation exists to prevent users from adding a multicast IP address; i.e., anything within the range of 224.0.0.0 to 239.255.255.255.

The configuration is straightforward, and involves deploying iPrism V3.200 or greater and a router which supports WCCP. When the client workstation generates traffic outbound to web servers on the Internet, the router detects that it is HTTP traffic (TCP port 80) and diverts that traffic to iPrism using a GRE tunnel. iPrism then makes the request to the server on behalf of the client, and responds directly to the client. However, from a client perspective, the response appears to come directly from the origin server, so the client does not even know it is communicating with iPrism.

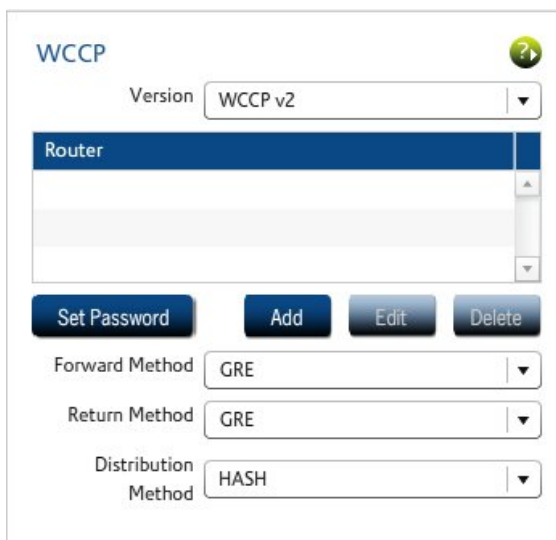


Note: iPrism can be placed on either side of the router.

Configuring WCCP Settings in iPrism

1. From the iPrism home page, select **System Settings**, then **Network Services**.

2. In the **WCCP** frame, select your version (WCCP v1 or WCCP v2) from the **Version** dropdown list.



The screenshot shows the WCCP configuration page. At the top, the title 'WCCP' is displayed with a refresh icon. Below the title, the 'Version' dropdown menu is set to 'WCCP v2'. Underneath is a 'Router' dropdown menu. Below the dropdowns are four buttons: 'Set Password', 'Add', 'Edit', and 'Delete'. Further down, there are three more dropdown menus: 'Forward Method' set to 'GRE', 'Return Method' set to 'GRE', and 'Distribution Method' set to 'HASH'.

Figure 86. WCCP selection

3. In the **Router** dropdown list, select the IP address of your router, or, if you need to add a Router, click **Add**.
4. To set the WCCP password, click **Set Password**.

Refer to the iPrism Knowledgebase for information on configuring various versions of the WCCP router:

www.edgewave.com/support/web_security/knowledgebases.asp

Configuring SMTP Relay Settings

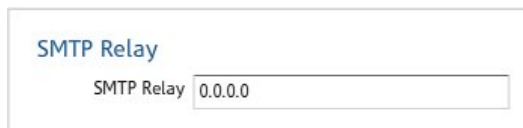
iPrism uses the SMTP protocol to perform the following types of communications:

- reports
- email alerts
- notifications (upgrades, filter list problems, registration)
- access requests

By default, iPrism will perform a DNS (MX record) lookup to deliver these emails. If iPrism is installed in a network where a DNS server is not available and a SMTP Smarthost is used (for efficiency), its IP address can be configured here, in the SMTP Relay field.

If a SMTP relay is specified, iPrism will delegate the delivery of the email to the relay and not attempt to directly contact the recipient's mail server.

1. From the iPrism home page, select **System Settings**, then **Network Services**.
2. Type the IP address of the SMTP Relay in the **SMTP Relay** field.



The image shows a screenshot of a web form. At the top, the text 'SMTP Relay' is displayed in a blue font. Below it, there is a text input field with the label 'SMTP Relay' and the value '0.0.0.0' entered inside it.

Figure 87. SMTP Relay

3. Click **Save**.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Enabling the Co-Management Network

The ability to administer iPrism is normally disabled for addresses located on iPrism's external interface. If iPrism's external interface is enabled (i.e., you are in bridge (transparent) mode), you can define a co-management network, which allows a given range of IP addresses to configure iPrism through the external interface.



Note: Defining a co-management network does not affect the ability to configure iPrism from iPrism's internal interface.

To define an IP range on the co-management network while working in bridge (transparent) mode:

1. From the iPrism home page, select **System Settings**, then **Network Services**.
2. In the **Co-Management Network** frame, click **Set**.



Figure 88. Co-Management Network

3. Check **Enabled**.
4. Type IP addresses in the IP Start and IP End fields to define the range of IP addresses that will be allowed to access iPrism from the external interface. Only workstations in this range of IP addresses will be able to configure iPrism via the external interface.

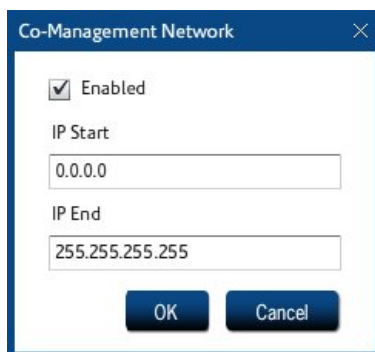


Figure 89. Enabling the Co-Management Network

5. Click **OK**.
6. Click **Save** to save your changes.
7. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Pending Request Options

When a user is surfing the Internet and receives an Access Denied message for a blocked page, they can use click **Request Access** to send a message to the iPrism administrator to explain why they need access to the site. The administrator may review the request and decide whether or not to grant access. No administration privileges are required to submit an access request. (If a request is granted, the requesting user will be allowed to access the site.)

To view a list of pending requests, see [Pending Requests](#).

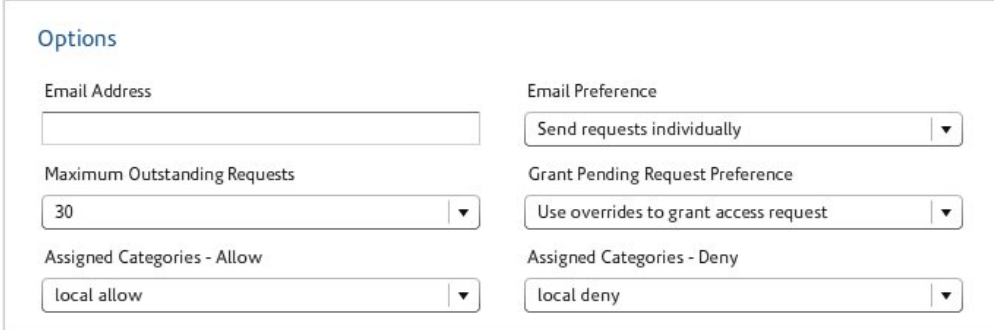
The Pending Request Options window allows you to set options for how to manage these pending requests.

To set the pending request options:

- From the iPrism home page, select **System Settings**, then **Pending Request Options**.

From here, you can set the following:

- The email address to which pending requests are sent
- How you want to receive the requests (e.g., individual emails or in a digest format)
- The maximum number of outstanding requests that may be queued
- The preference pertaining to the pending request grant (e.g., use overrides to grant the access request)
- The assigned categories to which requests are allowed and denied.



The screenshot shows a configuration window titled "Options" with two columns of settings. The left column contains: "Email Address" (text input), "Maximum Outstanding Requests" (dropdown menu with "30" selected), and "Assigned Categories - Allow" (dropdown menu with "local allow" selected). The right column contains: "Email Preference" (dropdown menu with "Send requests individually" selected), "Grant Pending Request Preference" (dropdown menu with "Use overrides to grant access request" selected), and "Assigned Categories - Deny" (dropdown menu with "local deny" selected).

Figure 90. Pending Request Options

Ports

The Ports window allows you to configure or reconfigure default proxy and configuration ports (if needed), specify non-standard ports for filtering in either bridge (transparent) or proxy mode, and add, edit and delete redirect ports (for transparent mode) and HTTPS ports (for proxy mode).

The screenshot shows the 'Ports' configuration page. At the top, there are three input fields: 'Primary Proxy Port' with the value '3128', 'Secondary Proxy Port' which is empty, and 'Configuration Port' with the value '80'. Below these are two main sections. The left section is titled 'Bridge (transparent) mode' and contains a table with the header 'Redirect Ports'. The table has three empty rows. Below the table are three buttons: 'Add', 'Edit', and 'Delete'. The right section is titled 'Proxy (single-interface) mode' and contains a table with the header 'HTTPS Ports'. This table also has three empty rows. Below it are three buttons: 'Add', 'Edit', and 'Delete'.

Figure 91. Ports

Proxy and Configuration Ports

If desired, you can reconfigure the primary client proxy port of 3128, a secondary proxy port, or the standard administration port of 80.



Important: Remote Filtering will not function properly if iPrism's configuration port is not set to the default of port 80.

Primary Proxy Port: 3128 is the default TCP port number used for proxy requests from proxy mode clients (browsers). If you change this port number after client configuration, clients will need to be reconfigured. This port number is meaningful to proxy mode clients, as well as bridge (transparent) mode installations where some of the user community is proxied to iPrism (e.g., Terminal Services users). This port number does not pertain to bridge (transparent) mode traffic.

Secondary Proxy Port: You can set up an additional proxy port. This allows clients that are already set up to use a proxy port other than the primary port. For example, if you have some existing clients that are configured to proxy to port 8080, you would set the secondary proxy port to 8080.

If you do not set the secondary proxy port, only the primary proxy port will be used.

You can test the new port settings by proxying to the new proxy port.

Configuration Port: 80 is the default port used to access iPrism administration tools. The port can be any value between 1 and 65,535, but cannot be the same as either of the proxy ports.

After changing the configuration port, you will need to append the port number to your iPrism URL to access the iPrism configuration tools, for example:

https://[your iPrism]:8080

To add a proxy or configuration port:

1. From the iPrism home page, select **System Settings**, then select **Ports**.
2. To enter a proxy or configuration port, type the port number in the **Proxy Port** or **Configuration Port** field.
3. Click **Save**.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Redirect and HTTPS Ports

Bridge (transparent) mode redirect ports: This setting is no longer used. iPrism does HTTP filtering on all ports by default.

Proxy mode HTTPS ports: By default, iPrism only allows access to secure ports 443 and 563. If using Proxy mode, and you require access to secured sites on other ports, you can define them here as described below.

To add, edit or delete a redirect port (Bridge (transparent) mode only):

1. From the iPrism home page, select **System Settings**, then **Ports**.
2. To add a redirect port (Transparent mode only), click **Add**.
3. Type the port number you want to use and click **OK**.
4. To edit a redirect port (Transparent mode only), select the port in the **Redirect Ports** list and click **Edit**.
5. Make your changes and click **OK**.

6. To delete a redirect port (Transparent mode only), select the port in the **Redirect Ports** list and click **Delete**.
7. Click **Yes** to confirm you want to delete the port.
8. Click **Save** at the bottom of the window.
9. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

To add, edit or delete an HTTPS port (Proxy mode only):

1. To add an HTTPS port (Proxy mode only), click **Add**.
2. Type the port number you want to use and click **OK**.
3. To edit an HTTPS port (Proxy mode only), select the port in the HTTPS Ports list and click **Edit**.
4. Make your changes and click **OK**.
5. To delete an HTTPS port (Proxy mode only), select the port in the HTTPS Ports list and click **Delete**.
6. Click **Yes** to confirm you want to delete the port.
7. Click **Save** at the bottom of the window.
8. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Proxy

The Proxy section allows you to integrate iPrism with an upstream web caching server, typically for performance benefits. This is often referred to as Slaving iPrism to a Parent Proxy or Upstream Proxy.



Note: Slaving iPrism (integrating with an upstream proxy) is not the same as “Slaved iPrisms” (iPrisms that get configuration data from a single “Master” iPrism in a Central Management configuration). If you are interested in managing multiple iPrism units, rather than integrating with an upstream proxy, see Central Management.

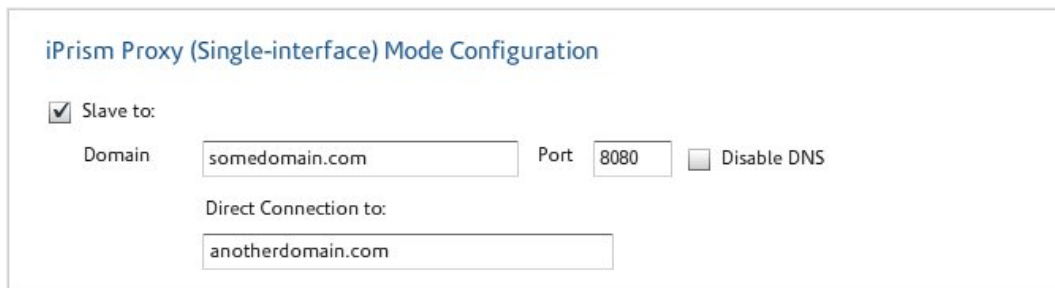
Integration with an Upstream or Parent Proxy can be supported using Bridge (transparent) mode or Proxy mode. However, there are differences in iPrism configuration requirements, client configuration requirements, and session management that must be taken into consideration. These differences, as well as detailed information about and instructions on how to use Parent or Upstream Proxies, are explained in detail in the Knowledgebase article “How do I integrate iPrism with an Upstream or Parent Proxy?” at www.edgewave.com/support/web_security/knowledgebases.asp.

To set up the proxy section:

1. From the iPrism home page, select **System Settings**, then **Proxy**.
2. Define proxy settings as needed. See below for details.
3. Click **Save**.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Slaving iPrism to a Parent Proxy (Proxy Mode)

1. In the Proxy window, in the iPrism Proxy Mode Configuration frame, check **Slave To**.



iPrism Proxy (Single-interface) Mode Configuration

Slave to:

Domain: Port: Disable DNS

Direct Connection to:

Figure 92.

2. In the **Domain** field, type the IP address of the iPrism or web caching server that will serve as a parent proxy.



Note: It is best to use IP address instead of hostname, as hostname will not work if DNS is disabled.

3. Type the port number of this server.
4. Check **Disable DNS** if you want to completely disable iPrism’s DNS functionality.



Note: If iPrism is configured to send administrative alerts, internal logs and/or reports via email, it will need an SMTP server entry for email exchange. iPrism will send all locally generated email to this SMTP server without attempting to contact a DNS server for name resolution.

Enabling an Upstream Proxy in Bridge (transparent) Mode

1. In the Proxy window, in the iPrism Bridge (Transparent) Mode Configuration frame, check **Enable Upstream Proxy**.

Figure 93. Enable Upstream Proxy

2. Type the upstream proxy domain into the field.

HTML Header Handling

When iPrism is used as a proxy, it inserts two headers into HTTP requests: Via and X-Forwarded-For. You can specify whether iPrism inserts these headers, and what values these headers should have.



Note: These headers are important to the correct operation of proxies - use care in altering them.

To modify the HTML header:

1. In the Proxy window, select **Enable x-forwarded-for header**.

Figure 94. HTML Header Handling

2. Select an option for the via header:
 - **Standard:** The standard via header will be used.
 - **Suppress:** No via header will be used.

- **Specify:** The value you enter in the Specified Value field will be used.

Configuring the Filter List/System Update Proxy Server

To specify the proxy server from which filter lists and system updates are downloaded:

1. In the Proxy window, select an option from the Filter List dropdown:
 - **None**
 - **Same as Parent Proxy**
 - **Custom**
2. If you chose Custom:
 - Type the host IP address and port number into their respective fields.
 - An iPrism administrator account username and password are required; type them into their respective fields.

System Preferences

This section allows the administrator to change iPrism's internal settings and set preferences for common iPrism activities.

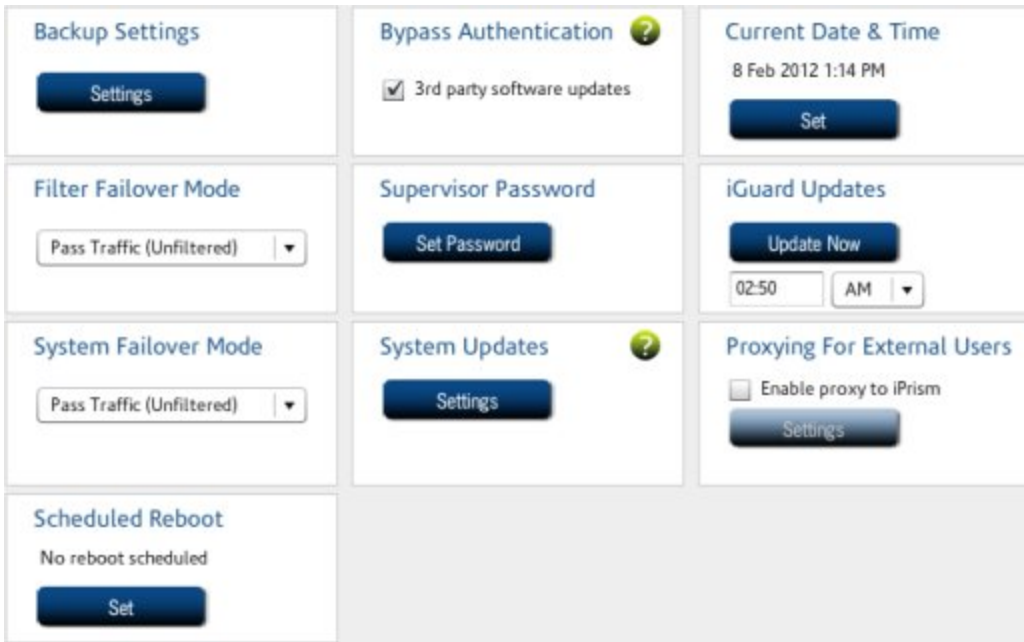


Figure 95. System Preferences

To set system preferences:

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. Select the options as described below.
3. Click **Save** to save your changes.
4. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Backup Settings

Backing up your iPrism configuration stores all of your settings to a file on your local hard drive. If necessary, you can restore your settings from this file.



Note: The data in Backup files is encrypted for security.

- In the System Preferences window, in the Backup Settings frame, select an option:

- **Display backup reminders:** Choose this option to have iPrism prompt you to back up.
 - **Prompt when Exiting:** You will be prompted to back up your iPrism when you exit an iPrism session.
 - **Prompt when Starting:** You will be prompted to back up when you start an iPrism session.
 - Specify the intervals at which you want to be prompted by typing a number between 1 and 30, then selecting **Days** or **Sessions** next to the **Every** field. This is how often you will be prompted to back up. For example, if you want to be prompted once a month, enter **30** and select **Days**. If you want to be prompted every 10th time you open/close the iPrism configuration software, enter **10** and select **Sessions**.



Note: The default setting is to prompt every 6 days when exiting.

- **Email backups to the administrator:** Choose this option to have a backup of the iPrism config file emailed to the administrator at the selected interval.
 - **Time:** The time of day when the config file will be backed up.
 - **Every x days:** The number of days in between backups.

Bypass Authentication

Some tools, such as Microsoft Windows Update, access the Internet without authentication. If your iPrism is configured to require authentication, then these tools may or may not work. If you check **3rd Party Software Updates**, then the iPrism will allow connections to third party software update sites (e.g., <http://update.microsoft.com>) without authentication.

To bypass authentication for 3rd party software updates:

- In the System Preferences window, in the Bypass Authentication frame, check **3rd Party Software Updates**.

Current Date and Time

In iPrism, you can set the date and time manually, or configure iPrism to use the Network Time Protocol (NTP).

1. In the System Preferences window, in the Current Date and Time frame, click **Set**.



Note: If you have any other unsaved changes on this page, you will be prompted to save them prior to setting the current date and time.

2. Select a city that is in your time zone and shares the same local variations, such as Daylight Savings Time, from the **Time Zone** list. This is usually the city that is closest to you geographically.
3. To set the time manually, make sure that **Set time manually** is checked (as it is by default) and type the date and time into their respective fields.
4. If you want to use the Network Time Protocol (NTP) server to set your date and time automatically, in the **NTP Server** field, type the IP address of the server that handles NTP requests. Using an NTP server to maintain an accurate time setting on the iPrism is useful for scheduled events, such as Filter List downloads and System Updates.
5. Click **OK** to save your changes.

Filter Failover Mode

Filter Failover Mode determines how iPrism will respond in the event that a filter list error occurs and iPrism cannot perform its normal filtering duties. Filter failures occur when a filter list fails to download, or when iPrism is unable to download a fresh filter list for an extended period of time (typically 30 days).



Note: iPrism will send an email to the administrator's email address (as defined in the **Registration** tab) if it is unable to download a filter after 3 days.

To configure filter failover mode:

- In the System Preferences window, in the Filter Failover Mode frame, select an option:
 - **Pass Traffic (Unfiltered):** This setting allows all Internet traffic to pass, as though all categories are allowed access. Users will have full access to the web.
 - **Block Traffic:** This setting effectively blocks all HTTP activity, not allowing any web surfing to occur until the problem is resolved and the filter list can be updated. If in bridge (transparent) mode, all other services will work normally.



Note: Regardless of the option you choose, the rest of your network will continue to work normally if iPrism is not operating.

Setting or Changing the Supervisor Password

To set or change the password for the iPrism administrator:

1. In the System Preferences window, in the Supervisor Password frame, click **Set Password**.

2. Type a password in the **Password** field, then type the password again in the **Confirm Password** field.
3. Click **OK** to save the password.
4. Click **Yes** to save your changes.

Filter List (iGuard) Updates

Filter list updates help to keep your iPrism's URL database current with the constantly updated database.

Scheduling Filter List (iGuard) Updates

- In the System Preferences window, in the iGuard Updates frame, click **Update Now** to update immediately; or, to specify a time to download updates, type a time, and select **AM** or **PM**.



Note: It is recommended that automatic updates be done during the late night or early morning hours (e.g., 3:00 a.m.) when the network load is the lightest.

Checking iPrism's Filter List Status

To determine the last time your system received a filter list update:

1. From the iPrism home page, select **System Status**, then **Security Log**.
2. The report window should contain the filter list age and the configuration changes.

If no update was available the last time iPrism checked, the status reads "empty update."

System Failover Mode

System Failover Mode determines how iPrism will respond in the event of a catastrophic system failure (such as either a power failure or hardware failure) and the iPrism is no longer capable of performing its normal filtering duties.



Note: iPrism will send an email to the administrator's email address (as defined in the **Registration** tab) if it is unable to download a filter after 3 days.

To configure filter failover mode:

- In the System Preferences window, in the System Failover Mode frame, select an option:

- **Pass Traffic (Unfiltered):** This setting allows all Internet traffic to pass, as though all categories are allowed access. Users will have full access to the web.
- **Block Traffic:** This setting blocks all Internet traffic that passes through the iPrism. Depending on the nature of the failure, it might be impossible to connect to the iPrism through the user interface. It is possible that a system reset will restore your iPrism to operation.



Note: Regardless of the option you choose, the rest of your network will continue to work normally if iPrism is not operating.

System Updates

System updates keep your iPrism unit up-to-date with the latest software enhancements.

1. In the System Preferences window, in the System Updates frame, click **Settings**.

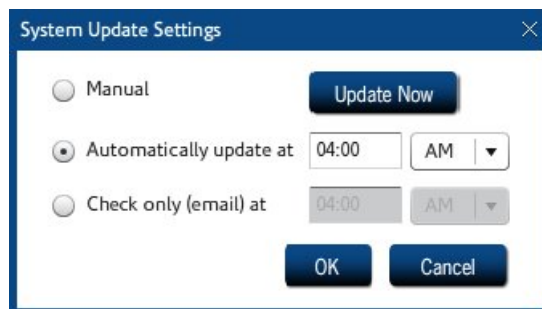


Figure 96. System Update Settings

2. Select an option for how often you want to update your iPrism:
 - Select **Manual**, then click **Update Now** to update immediately.
 - To specify a time to download updates, check **Automatically update at**, type a time, and select **AM** or **PM**.



Note: It is recommended that automatic updates be done during the late night or early morning hours (e.g., 3:00 a.m.) when the network load is the lightest.

- If you only want to check for updates and have the system send you an email, but not perform any updates, select **Check only (email) at**, then type a time and select AM or PM.

Proxying for External Users

This setting is no longer in use.

Scheduled Reboot

If the iPrism needs to be rebooted, but you can't do it immediately, you can schedule the reboot for a later date/time.

To schedule a reboot:

1. In the System Preferences window, in the Scheduled Reboot frame, click **Set**.

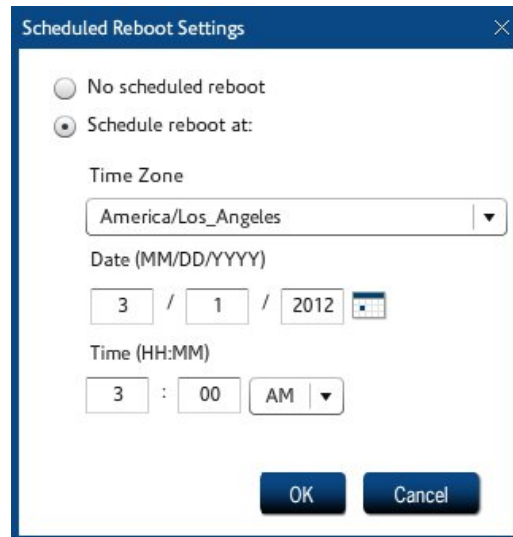


Figure 97. Scheduled Reboot Settings

2. Select **Schedule reboot at**.
3. Select the time zone, date, and time.
4. Click **OK**.

Unrated Pages (iARP)

iPrism can automatically rate unrated, frequently accessed URLs (the iPrism Automatic Rating Protocol, or iARP). After a period of seven (7) days the top 100 currently unrated, frequently accessed URLs for a given iPrism are sent to for rating. You can opt to get an email message when the list of sites is sent and when the rating is complete, which normally occurs within a few days. You can also view those sites that could not be rated automatically and rate them manually. The number of sites listed and the need to manually submit URLs for review or inclusion should decline with the frequent and consistent use of the rating function.

Notes:

- The capability to send unrated sites to iARP can also be enabled during the iPrism installation process. Refer to the *iPrism Installation Guide* for detailed instructions.
- If the total number of unrated sites is less than 100, all of them are sent to iARP.

To set up iGuard notifications:

1. From the iPrism home page, select **System Settings**, then **Unrated Pages**.
2. Check whether you would like to automatically send unrated URLs to iARP.
3. Check whether you would like to receive email notifications.
4. The iPrism administrator's email address is the default recipient if you have checked options in steps 2 or 3. To have notifications sent to a different email, select **Custom E-Mail Address** and type the email address where you want the notifications sent.

A list of URLs automatically sent to for rating is sent, via email, to the iPrism administrator or the custom email address specified. Within a few days the sites are rated and an email is sent indicating the rating response.

5. Click **Save** to save your changes.
6. If you have completed all your administrative changes, click **Activate Changes** to activate the changes immediately. If you do not Activate Changes now, you will be prompted to do so before logging out of iPrism.

Send unrated sites to EdgeWave's iGuard Team

Send unrated URLs to iGuard automatically

Receive request sent notification email

Receive response received notification email

Admin E-mail Address

Custom E-mail Address

Figure 98. Unrated Pages

User Settings

The administrator can reset dialog prompts back to the factory defaults. This affects the dialog prompts that are displayed when certain actions are taken (e.g., confirming delete). If a user checked **Do not ask me about this again** in the following example, resetting dialog prompts results in this setting being cleared, and the user again being asked to confirm delete.

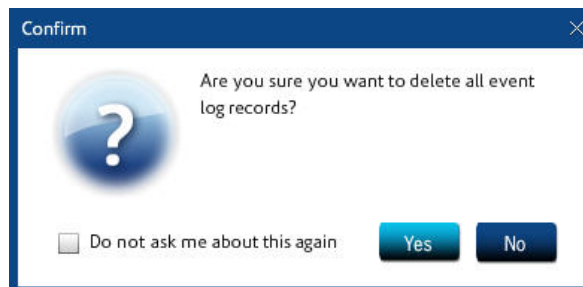


Figure 99. Dialog Prompt Example

To reset dialog prompts:

1. From the iPrism home page, select **System Settings**, then **User Settings**.
2. Click **Reset**.

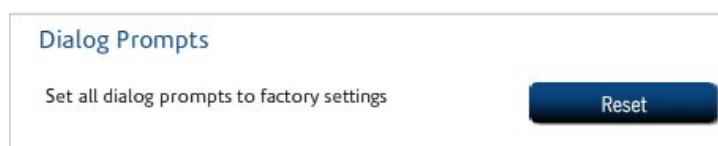


Figure 100. Reset Dialog Prompts

CHAPTER 8 **System Status**

The System status options give you access to event data, as well as build ID, configuration information, connectivity status, and security and other information.

See also

About

The read-only **About** window contains configuration details about your iPrism, such as hardware details, the version of software you are running, the iPrism build number, and how to contact Sales and Technical Support.

- From the iPrism home page, select **System Status**, then **About**.

Administration Log

The Administration Log is a read-only window that displays recorded actions of the iPrism Administrator. You can save this file as a text file, and/or print it. This can be useful to email or FTP to iPrism Technical Support to assist in troubleshooting.

To view the administration log:

- From the iPrism home page, select **System Status**, then **Administration Log**.

The Administration log records actions of iPrism Administrators.

Refresh Clear

Date	Time	Event
2012-01-02	17:49	User 'iprism' Logged in.
2012-01-02	17:49	User 'iprism' Unauthorized.
2011-12-30	13:42	User 'iprism' Logged out.
2011-12-30	13:16	User 'iprism' Logged in.
2011-12-29	18:24	User 'iprism' Logged in.
2011-12-22	14:35	User 'iprism' Logged out.
2011-12-22	13:34	User 'iprism' Activated Configuration.
2011-12-22	13:33	User 'iprism' set 'committed' to '1'
2011-12-22	13:33	User 'iprism' set 'high_availability/standbyInternal' to 'on'
2011-12-22	13:33	User 'iprism' set 'high_availability/standbyExternal' to 'off'
2011-12-22	13:33	User 'iprism' set 'high_availability/standbyBridge' to 'on'
2011-12-22	13:33	User 'iprism' set 'high_availability/mcastPort' to '5405'
2011-12-22	13:33	User 'iprism' set 'high_availability/mcastIP' to '226.94.1.1'
2011-12-22	13:33	User 'iprism' set 'high_availability/failedInternalTimeout' to '1'
2011-12-22	13:33	User 'iprism' set 'high_availability/failedInternal' to 'on'

Select All Deselect All Save As Print

Figure 101. iPrism Administration Log

Configuration Summary

The Configuration Summary is a read-only window that displays information about how your iPrism is configured. You can save this file as a text file, and/or print it. This can be useful to iPrism Technical Support to assist in troubleshooting.

To view the configuration summary:

- From the iPrism home page, select **System Status**, then **Configuration Summary**.

Connectivity

This window provides host tools to ping, trace, and perform DNS Lookups on IP addresses, and displays connectivity status and details on the iPrism update server and routing tables.

To view connectivity information:

- From the iPrism home page, select **System Status**, then **Connectivity**.

To refresh this screen at any time, click **Refresh**.

Pinging a Host

To test whether a particular host is reachable across an IP network, you can ping it.

1. From the iPrism home page, select **System Status**, then **Connectivity**.
2. Type the IP address of the host and click **Ping**.

The results are displayed in the **Results** frame.

Tracing Network Activity

1. From the iPrism home page, select **System Status**, then **Connectivity**.
2. Type the IP address of the host and click **Trace**.

The results will be displayed in the **Results** frame.

Perform a DNS Lookup

1. From the iPrism home page, select **System Status**, then **Connectivity**.
2. Type the IP address of the host and click **DNS Lookup**.

The results are displayed in the **Results** frame.

Refreshing the System Updates Server

System updates keep your iPrism unit up-to-date with the latest software enhancements. For details about and instructions on setting up system updates, see “[System Updates](#)” on page 170.

1. From the iPrism home page, select **System Status**, then **Connectivity**.
2. In the iPrism Update Server frame, click **Refresh**.

Routing Table

The Routing Tables allow you to view and verify routing information for iPrism. A default route should be in place to reach the Internet, but in larger systems, other static routes are needed if internal subnets are reached via a different router. To maximize efficiency, these routes must be set up properly.

To view the routing table:

- From the iPrism home page, select **System Status**, then **Routing Table**.

A list of the network routes is displayed. To refresh the list, click **Refresh**.

Security Log

The security log is a read-only window that displays the last time your system received a filter list update, the last time there were configuration changes, the last time a backup was performed, the last time a remote filtering policy was delivered to the portal, and information about IP accesses, email alerts, overrides, and automatic reports.

You can save this file as a text file, and/or print it. This can be useful to iPrism Technical Support to assist in troubleshooting.

To view the security log:

- From the iPrism home page, select **System Status**, then **Security Log**.

You can clear or refresh the log at any time by clicking **Clear** or **Refresh**, respectively.

If no update was available the last time iPrism checked, the status reads “empty update.”

Status

The Status window displays the status of iPrism(s) on your network, such as amount of uptime, RAID status, System Memory and CPU usage, whether your filtering and proxies are running, the age of your filter list, and network utilization statistics.

You can view information about the status of your iPrism unit, as well as utilization data, in the Access Event Status section (see [Event Log](#)). All of the fields in this area are read-only.

- **Uptime:** The days, hours, and minutes that your iPrism has been continuously running.
- **High Availability:** Whether or not High Availability is enabled (running).
- **System:** The amount of system memory your iPrism is consuming.
- **CPU:** The percentage of CPU that your iPrism is using.
- **RAID:** Status of the RAID disk (if your iPrism model contains RAID).
- **Filtering Status**

- **Web Proxy Requests:** Number of URLs processed and blocked for systems using the iPrism as a proxy.
- **Bridge Sessions:** Number of URLs processed and blocked for systems using the iPrism in bridge (transparent) mode.
- **Number of Clients:** Number of client workstations serviced by iPrism.
- **Network Utilization**
 - **Internal Interface:** Amount of IP traffic (measured in bytes, for all protocols) received by the internal interface.
 - **External Interface:** IP traffic received for the external interface, if one is being used (bridge (transparent) mode only).
 - **Management Interface:** IP traffic received by the management interface, if the management interface is being used. If the management interface is not being used, this shows as Not Available.
- **Filtering:** Displays whether filtering is active, and the size of the filter list database in KB.
- **Proxy:** Displays whether the proxy is being used, and the size.
- **Filter List Age:** Displays the age of the filter list (i.e., when it was last updated), and the revision number.
- **Remote Filtering Status:**
 - **Log Download Status:** The last attempted and last successful downloads of the Remote Filtering activity logs (i.e., the logs of remote user activity).
 - **Policy Upload Status:** The last attempted and last successful Remote Filtering policy uploads.
 - **Custom Filter Upload Status:** The status of the last custom filter upload, including the number of times the custom filter upload was attempted.

CHAPTER 9 Central Management

iPrism's central management features let you manage a large set of iPrism systems using a single configuration manager. The system works by letting you designate a single master system and one or more slave systems. Any configuration changes made to the master system are automatically copied by the slaves.

Before You Begin

Prior to setting the Configuration Sharing properties, each iPrism (master and slaves) should be installed using the Installation Wizard, and the networking parameters and the minimum configurations set. Once that is done, decide which systems should be slaves and which system will be the master. There are no specific criteria for choosing the master; however, you must observe the following guidelines:

- There should be only one master system designated at any given time.
- Other systems need to be set as slaves if they want to participate in the configuration sharing. If you do not want them to participate in the shared arrangement, you must designate them as standalone systems.
- All communications are implemented over the HTTP protocol. This means that master and slave iPrisms should be able to contact themselves with HTTP in both directions. This may be done using direct connections or an HTTP proxy.



Note: This may impact your IP filtering configuration if you have a firewall between the master and the slave systems.

- All communications are encrypted so as not to expose your configuration to network sniffing.



Note: The master iPrism will never try to modify the networking configuration of a slave (IP addresses and mask, routes, interface settings) because these are unique and/or system-dependent.

Setting Up a Master/Slave Configuration

There are two steps to setting up a master/slave configuration, and it is recommended that they be completed in order:

1. Designating Slave Systems.
2. Designating the Master System.

Designating Slave Systems

For each iPrism that will be a slave:

- There must be a valid DNS configured.
- Co-management must be enabled.
- The co-management IP address range must include the IP address of the master

To set up slave:

1. From the iPrism home page, select **System Settings**, then **Central Management**.
2. Select **Slave** from the **iPrism Mode** dropdown list.
3. Click **Yes** to confirm.
4. If the password has not already been set, click **Set Password** and enter the password to be used. This password must be the same for all iPrisms that are included in the Central Management configuration.

If you want to designate another iPrism as a slave, click **Logout**, then log into the iPrism you want to designate as a slave and repeat these steps.

Central Management Mode

Select the mode in which you would like this iPrism to operate.

iPrism Mode

Master iPrism Appliance

IP Address	Hostname	Last Connected
		Indeterminate

Figure 102. Designate Slave

Designating the Master System

1. Log into the iPrism you want to designate as a master.
2. From the iPrism home page, select **System Settings**, then **Central Management**.
3. Select **Master** from the **iPrism Mode** dropdown list.
4. The mode changes to Master, and a notification message appears when this is complete.
5. If the password has not already been set, click **Set Password** and enter the password to be used. This password must be the same for all iPrisms that are included in the Central Management configuration.

Central Management Mode

Select the mode in which you would like this iPrism to operate.

iPrism Mode

Slave iPrism Appliances

IP Address	Hostname	Last Connected

Slave appliances route overrides and access requests back to Master.

Update Slave Appliances

Update slave appliances based on the settings of the Master

Figure 103. Designate Master

- To choose the master settings to be applied to the slaves, click **Manage Policies**.
- Select which set of policies to apply and click **OK**. See [Central Management Policies](#) for descriptions.
- To add slaves, in the Slave iPrism Appliances frame, click **Add**.
- Type the IP address of the slave. Note that you must have already designated this iPrism as a slave. See [Designating Slave Systems](#).
- Click **OK**. The change is applied immediately.
- To add another slave, repeat steps 8-10.

12. If you want the master to handle all overrides and access requests that come to the slaves, check **Slave appliances route overrides and access requests back to Master**.



Note: If this option is selected and the current policy is to synchronize overrides, the initial connection to the slave appliances synchronizes the overrides from the master. This results in the slave appliances losing their current list of overrides. Subsequent overrides created on the slave appliances will be synchronized with the master.

Once you have designated a master system, any slave systems added are automatically slaved to and synchronized with the master. If you want to update and synchronize slaves at any time, click **Update** in the Central Management window.

Changing the Master System

Changing which system is your master may be useful in certain situations, such as if the original master will be unavailable for a long period of time due to network problems, a hardware failure, etc.

Before you change the master, consider the following:

- If you choose an iPrism that was previously a slave to become the new master, **it is imperative to use an iPrism with an up-to-date configuration**. If you choose a previously-slaved iPrism that was not reachable by the master, that iPrism will be outdated. If your iPrism detects that another slave has a more recent configuration, you will be prompted to confirm or cancel your selection.
- Confirming your selection of an outdated iPrism may cause problems, such as changes or settings that are no longer in sync between master and slave.

To change the master system:

1. Log into the iPrism you want to designate as a master.
2. From the iPrism home page, select **System Settings**, then **Central Management**.
3. Select **Master** from the **iPrism Mode** dropdown list.
4. If you want to add slaves, follow the steps (beginning with step 5) in **Designating the Master System**.

Removing a Slave System

1. Log into the master iPrism.
2. From the iPrism home page, select **System Settings**, then **Central Management**.
3. All designated slave systems are listed in the **Slave iPrism Appliances** frame. Select the one you want to remove, and click **Remove**.
4. Click **OK**.
5. Repeat steps 3 - 4 for each iPrism system you want to remove.

Using Standalone Mode

It is possible to configure a system (master or slave) as a standalone system (this is the default configuration when the master/slave configuration is not used).

1. From the iPrism home page, select **System Settings**, then **Central Management**.
2. Select **Standalone** from the **iPrism Mode** dropdown list.

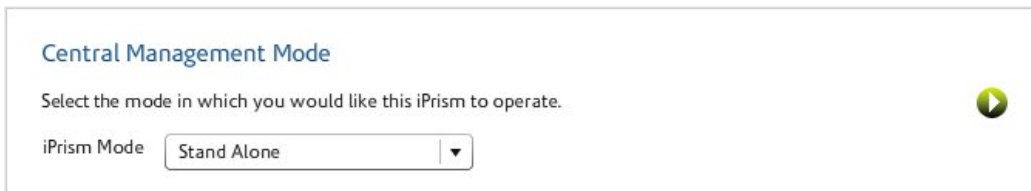


Figure 104. Standalone iPrism

Upgrading iPrisms in a Central Management Configuration

Because Central Management is a collection of units (one master and one or more slave units), a series of steps must be followed to upgrade master and slave units. The first step is to decouple the master and its associated slaves.

To decouple and upgrade the master:

1. Note the IP address of each slave. This makes it easier to set them up later.
2. Log in to the master iPrism.
3. From the iPrism home page, select **System Settings**, then **Central Management**.

4. Select **Stand Alone** from the **iPrism Mode** dropdown list.
5. Click **OK**.
6. Select **System Settings**, then **System Preferences**.
7. In the System Updates frame, click **Update Now**.

You will be prompted to confirm your decision (click **Yes**), and will be notified that the update will commence within 15 minutes. Download time will vary depending on network load.

To upgrade the slaves:

1. Log into a slave iPrism.
2. From the iPrism home page, select **System Settings**, then **Central Management**.
3. Select **Stand Alone** from the **iPrism Mode** dropdown list.
4. Click **OK**.
5. Select **System Settings**, then **System Preferences**.
6. In the System Updates frame, click **Update Now**.

You will be prompted to confirm your decision (click **Yes**), and will be notified that the update will commence within 15 minutes. Download time will vary depending on network load.

7. Repeat these steps for each slave you want to upgrade.
8. After you have upgraded all slaves, add them back to the master iPrism. See [Setting Up a Master/Slave Configuration](#) for details.

CHAPTER 10 **Override Management**

When a browser tries to access a web page that is being blocked by iPrism, an 'Access Denied' page displays. iPrism gives the user and the administrators a variety of options for handling blocked pages. This gives tremendous flexibility for dealing with blocked web pages, yet also allowing a great deal of control over Internet usage.

Access Denied Page Options

If the iPrism administrator has checked **Override Link** and/or **Request Access Link** when setting up the profile that applies to this user (see [Web Profiles](#)), the user sees an Override/Request Access button when they encounter an Access Denied web page. By default, these options are disabled; you must manually enable them if you want to provide Override/Request Access to users on your network. If both options are disabled, the user cannot view or request access to the blocked site.

- **Override:** Override allows the user to bypass the Access Denied page and view the blocked page, assuming s/he has the proper administrative privileges. The override request is recorded and can be viewed by the iPrism administrator by selecting **Profiles & Filters > Current Overrides**. See [Current Overrides](#) for more information.
- **Request Access:** The user can use the Request Access button to send a message to the iPrism administrator to explain why they need access to the site. The administrator can review the request and decide whether or not to grant access. No administration privileges are required to submit an access request. If a request is granted, the requesting user will be allowed to access the site.



Note: A list of pending access requests can be viewed by the iPrism administrator by selecting **Profiles & Filters > Pending Requests**. See [Pending Requests](#) for more information.

Using Override Privileges

If the iPrism administrator has checked **Override Link** when setting up a profile, a user under that profile can bypass the Access Denied page and view the blocked page. The override request is recorded and can be viewed in **Profiles & Filters > Current Overrides**.



Note: When a user has bypassed the Access Denied page and is viewing the blocked page, they are accessing the Internet under the grantor's profile for the specified duration.

You can set up user accounts strictly for the purpose of granting override access. For example, you can use a network-level profile to control web traffic on the network, and if a user encounters a blocked site, s/he can click the Override link, enter their username/password, and (assuming they have override privileges), view the blocked website. While doing so, they are under the network-level profile. If users have *single override* privileges, they can override a block for themselves. If they have *extended override* privileges they can let themselves and other users access a blocked website.

For information on giving local users override privileges, see [Pending Requests](#).

Overriding a Blocked Web Site

To override a blocked site, your user account must be assigned to a profile with override privileges, or be the iPrism administrator account.

1. When the Denied Access page is encountered, click **Override/Request Access**.



Note: If this button is not available, override access is being denied by the active ACL in the current profile. You cannot gain access to the site. You may wish to communicate with your iPrism administrator directly to gain access to the page.

2. In the Select Mode page, select whether you want to **Override** or **Request Access** (in this example, we will use **Override**).
3. Click **Next**.
4. Type your username and password in the Login screen, and click **Login**.
5. On the **Override Request** page, select the user to whom you want to grant access. The options that display here vary depending on your override privileges.
 - **Override applies to:**

- **Current Workstation [IP address]:** Any user on the current workstation will be able to access the blocked URL.
 - **Following Network [network range]:** Any user whose workstation is within the specified network range will be able to access the blocked URL. (This is available if you are using network profiles.)
 - **Current Profile [profilename]:** Any user associated with the specified profile, from any workstation; or any user on a workstation associated with the specified profile will be able to access the blocked URL.
 - **Everyone:** Any user from any workstation will be able to access the blocked URL, if the user has extended override privileges.
 - **Override scope:**
 - **This URL:** Allows access to only the URL that is currently being blocked.
 - **Domain:** Allows access to all web pages in the domain of the URL that is being blocked.
 - **Current Categories:** Allows access to all web pages that would otherwise be blocked by the specified filter categories.
 - **Categories allowed by profile belonging to user:** Allows access to all web pages that are allowed by the profile to which the given user belongs (e.g., if the specified user's profile blocks the category "Sex", URLs belonging to that category will not be overridden and will continue to be blocked).
 - **All URLs:** Allows access to all web pages.
 - **Duration**
 - **45 min(s)** (Default)
 - **1 hr(s) 25 min(s)**
 - **3 day(s) 12 hr(s) 30 min(s)**
 - **1 week(s) 2 day(s) 6 hr(s)**
 - **2 week(s) 3 day(s) 8 hr(s)**
6. Click **Finish**. The blocked site displays in the current browser and should be available to all users to whom you granted access.
7. If the Override Scope is set to **Categories allowed by profile belonging to user:**, and the URL the user is attempting to override belongs to a category blocked by that profile, the blocked page will appear again (i.e., override is rejected). For more information about how categories are blocked by profiles, see [Web Profiles](#).

Using Access Requests

Users that want to get past a blocked page but do not have override privileges have the option to plead their case to the iPrism administrator (or other authorized user with override privileges), who can subsequently grant or deny access to the page. In this scenario, the blocked user would use the **Request Access** button on the Access Denied page to send his request to the iPrism administrator. The request is emailed to the iPrism administrator.

Requesting Access to a Site

1. When the Access Denied page is encountered, click **Override/Request Access**.

If this button is not available, then access is being denied by the active ACL in the current profile. You cannot request access to the site.

2. When the Select Mode page displays, select **Request Access** and click **Next**. The Request Access page displays.

The Location field is prefilled with the URL you are trying to access. Complete the remaining fields by entering your email address in the Email field and describing why you need access in the Comments field.

3. If you want to be notified by email of the administrator's actions, check **Click here if you want notification of the administrator's actions**. You may want to check this if you are not sure your request will be granted.
4. Click **Next**. The Request Access Confirmation page displays.
5. Review your request for accuracy; if you need to make any changes, click **Back**. Otherwise, click **Finish**.
6. The Request Added page confirms that your request has been added, and the request is emailed to the appropriate person.

Your request will be seen the next time the administrator reviews access requests. If you requested notification, you will receive an email after this review is complete. You cannot reply to this email.

For instructions on how to process access requests, see [Pending Requests](#).

Managing Override Access

Override access allows users with the required privileges to be able to “overrule” the active filtering policy and gain access to web pages that would otherwise be blocked. In iPrism, override privileges are determined by a user’s administrator level assignment.

- From the iPrism home page, select **Profiles & Filters > Current Overrides**. The iPrism administrator can review all of the currently active overrides and revoke them, if desired. See [Current Overrides](#) for more information.

APPENDIX A Filtering Categories

This section lists the filtering categories in the database. This is the URL database that iPrism uses to determine a URL's category designation. These are also the categories of content that you can choose to block and/or monitor when configuring an Access Control List in iPrism.



Note: Local categories are not included here. The only categories that are included here are those that are determined by the database.

The database is constantly being updated, and the categories are subject to change as new and different types of content are encountered. To see the most current list of categories, as well as descriptions of each, refer to the online resource at:

http://www.edgewave.com/products/web_security/technology_iGuard.asp

Site Rating Categories

Sex Category

Adult

This category refers to sites that are adult in nature and are not defined in other rating categories. Sites that have adult themes are those that are associated with the following concepts: Adult oriented entertainment not defined as Porn, sale of penis enlargement products, erectile dysfunction products, online pharmacies, and mail order brides. These sites are usually intended for mature persons.

Examples

<http://www.mailorderbrides.com>

<http://www.personals.com>

<http://www.matchmaker.com>

Keywords

mature subjects, mail order brides, penis enlargement, Viagra/Cialis, online pharmacy

Lingerie/Bikini

This category refers to sites displaying or dedicated to bikini or lingerie that could be considered for adults only. Sites about modeling would not be included in this area.

Examples

<http://www.bikinihangout.com>

<http://www.victoriasecret.com>

<http://www.outdoorgirl.net>

Keywords

bikini, swimsuits, garters, underwear (male and female)

Nudity

This category refers to sites that provide images or representations of nudity. They may be in any artistic or non-artistic form like magazines, pictures, paintings, sculptures, etc. This category should be assigned to those sites that display both partial and full nudity but the images are not pornographic in nature.

Examples

<http://www.photo.net/nudes>

<http://www.naturistart.com>

<http://www.naturistworld.com>

Keywords

nudes, body images, nudist colonies, before/after pictures of cosmetic surgery

Pornography

This category covers anything relating to pornography, including mild depiction, soft pornography and hard-core pornography. Pornography pertains to writings, photographs, movies, etc. intended to arouse sexual excitement. Also, any site offering memberships that may provide access to other pornographic sites will fit into this category.

Examples

<http://www.playboy.com>

<http://www.penthouse.com>

<http://www.persiankitty.com>

Keywords

smut, graphic pictures, arousal, sex, escorts, erotica

Sexuality

This category contains sites that provide information, images or implications of body piercing, tattoos and any form of body art. Sites not in this category are those that contain images or information about sexual acts as discussed in the Pornography and Nudity categories.



Note: This category implies adult content in nature; therefore ratings of both Adult and Sexuality are not necessary.

Examples

<http://piercing.org>

<http://www.tattoonow.com>

<http://www.thechateau.com>

Keywords

tattoos, piercing, body art, skin art, henna

Questionable Activities Category

Copyright Infringement

This category refers to sites that offer media, software, MP3, DVD movies or any other copyrighted materials that are bootlegged or illegally available for purchase or download. This category is often blocked to protect iPrism owners from liability caused by the download and installation of bootlegged software. Note that this category does not refer to sites that are specific to computer hacking.

Examples

<http://www.bitoogle.com>

<http://www.mp3search.com>

<http://www.ugpirates.com>

Keywords

bootleg, illegal copy, plagiarize software, descrambler, serialz, warez, ripped and free MP3, patent, exclusive rights

Computer Hacking

This category refers to any site promoting questionable or illegal use of equipment and/or software to crack passwords, create viruses, gain access to other computers, and so on. This includes any site that offers instruction on how to hack as well. This does not include legitimate security information sites that are focused on the prevention of hacking.

Examples

<http://www.2600.com>

<http://www.hackersplayground.com>

<http://www.illegalworld.com>

Keywords

hacking, crack, toolz, warez, cryptanalysis, virus, password, crackz

Intolerance/Extremism

This category refers to any site advocating militant activities or extremism. This includes groups with extreme political views and intolerance to individuals and/or groups based upon discriminating or racial distinction.

Examples

<http://www.kukluxklan.bz>

<http://www.stormfront.org>

<http://www.godhatesamerica.com>

Keywords

KKK, skin heads, nazism, fascism, anti-Semitism, homophobia, hate speech, totalitarianism, absolutism, anti-gay, discrimination, racism, militias, bigotry, prejudice, fanaticism, radicalism

Miscellaneous Questionable

This category refers to sites that are considered questionable in nature and may involve illegal activities, but do not fall under another, more specific "questionable" category. These are sites that could contain information about conspiracy, scams or any other suspected fraudulent behavior or activity.

Examples

<http://www.stopwishing.com>

<http://www.geniuspapers.com>

<http://a4a.mahost.org>

Keywords

anarchy, conspiracy, fraud, illegal, chain letters, pyramid scams, essay/term papers for sale

Profanity

This category refers to any site that contains profanity of any kind that is NOT classified under the SEX category. These are sites that have language that would not be permitted in common social situations. This may include swearing, blasphemy, vulgarity or any dialog with malicious intent. It should be noted that this category should also contain sites with language that implies profanity like some jokes, poems, letters, greeting cards, etc.

Examples

<http://www.tshirthehell.com>
<http://www.eviladam.com>
<http://www.wtfpeople.com>

Keywords

swearing, cursing, vulgarity, strong lyrics, bad language

Tasteless

This category refers to sites that contain information on subjects such as mutilation, torture, horror, grotesque or any behavior that may be considered inappropriate for public audience. This will not include pornography, nudity, or sites dealing with sexuality, which have their own specific classifications.

Examples

<http://www.rotten.com>
<http://www.deathgallery.com>
<http://www.freakhole.com>

Keywords

mutilation, horror, grotesque, torture, scat, gross, in bad taste, in poor taste, garish, vulgar

Weapons/Bombs

This category refers to any site promoting the use of weapons and/or bombs and the making of bombs. This does not include sites related to gun control (social issues).

Examples

<http://www.gunsamerica.com>
<http://www.thefiringline.com>
<http://www.imperialweapons.com>

Keywords

guns, bombs, swords, knives, arms, armaments, artillery, arsenal, weaponry, military hardware

Violence

This category refers to sites that contain visual representations of or invitations to participate in violent acts. This may include war, crime, pranks, hazing, etc. A violent act may be considered any activity that uses physical force designed to injure another living being.

Examples

<http://www.fightworld.com>
<http://www.fightauthority.com>
<http://www.whoopasstv.com>

Keywords

war, crime, pranks, hazing, injury, killing, backyard wrestling, fighting, hostility, brutality, cruelty, sadism, carnage

Security Exploits Category

Phishing

Deceptive websites that trick end-users into revealing personal data such as credit card numbers, account usernames, passwords, social security numbers, etc. These websites pretend to be those of common, well-known sites such as banks and credit card companies.

Examples

<http://www.dotnetssl.com>
<http://www.acctaccess-es.com>
<http://www.paypal.com-cgi.us>

Keywords

phishing, credit card fraud, identity theft

Spyware/Adware

Websites that are known to distribute or contain code that displays unwanted advertisements or gathers information about the user without the users knowledge. This information is oftentimes relayed to advertisers or other 3rd parties.

Examples

<http://www.gamebar.net>
<http://www.esurveiller.com>
<http://www.seeq.com>

Keywords

spyware, adware, browser hijacker, keylogger

Malware

Websites that are known to contain harmful code that may modify a user's system without the user's knowledge.

Examples

<http://www.ivstil.ru>
<http://www.buddylinks.net>
<http://www.1weight.us>

Keywords

malware, virus, trojan, dialer, worm

Society Category

Alt/New Age

This category refers to any site relating to the advocacy and/or information pertaining to the occult (i.e., witchcraft, voodoo, black arts) astrology, ESP or similar forms of telepathy, fortune telling, out-of-body experience, magic, spirituality, and UFOs. Note that common horoscopes found in daily newspapers are not a part of this category. Any site that relates to new age meditation practices or the study of new age principles should be included in this category. Note: Occult will be defined as anything pertaining to any system claiming use or knowledge of secret or supernatural powers or agencies.

Examples

<http://www.crystalhealing.co.nz>
<http://www.pandbox.com>

<http://wicca.net>

Keywords

horoscopes, goddesses, witchcraft, voodoo, Wicca, spells, palm reading, fortune telling

Art/Culture

This category refers to any site relating to the arts or culture. Culture includes the beliefs, customs, practices, and social behavior of a particular nation or people. The arts include the creation of beautiful or thought-provoking works, for example, in paintings, pictures, drawings, or writings. Sites falling into this category include virtual art galleries, museums, architecture, contemporary and fine art.

Examples

<http://www.binggallery.com>

<http://www.ago.net>

<http://www.kamat.com>

Keywords

clip art, museums, galleries, traditions, customs, art gallery, contemporary art, fine art, painting, sculpture

Family Issues

This category refers to any site that deals with issues specific to the family, including divorce, adoption, parenting, marriage, domestic violence, child abuse, father's rights, child custody, incest and fertility. Also included in this category are sites that offer counseling to the above examples.

Examples

<http://www.vifamily.ca>

<http://www.stand.org>

<http://www.voices-unabridged.org/>

Keywords

divorce, adoption, parenting, marriage, domestic violence, child abuse, father's rights, child custody, incest, fertility clinics, counseling on any of these topics.

Government

This category refers to any site that is associated with governments and/or their militaries. This includes federal, state, county, city and local governments as well as any government agency. This does not include general information about a specific geographical location (state, city, etc) - these sites should be classified as Travel. A strong indication is a domain identifier of either .gov or .mil.

Examples

<http://www.whitehouse.gov>

<http://www.dmv.ca.gov>

<http://www.nic.mil>

Keywords

military, white house, senate, congress, FBI, CIA, IRS, federal, state, county, city government, government agencies, regime, fire dept., post office, foreign governments

Politics

This category refers to any site that is associated with political advocacy of any type or the opinions of the government. This includes any site promoting or containing information on any political party, pro or con. This includes registered and officially recognized political parties. Sites that inform or promote an election of any political office receive this rating. It does not include official government sites.

Examples

<http://www.northernviriniagop.com>

<http://www.rnc.org/>

<http://www.declareyourself.com>

Keywords

republican, democrat, grassroots, voting, political affairs, affairs of state and policy, mayoral races, local districts, elections

Social Issues

This category refers to any site that contains information regarding issues that are considered controversial by a society. Examples of these are sites that provide information on abortion, euthanasia, gun control, drug legalization, suicide, immigration, civil/human rights and gay (or anti-gay) sites.

Examples

<http://www.prochoicetalk.com/>

<http://www.guncontrol.org.au>

<http://www.sitins.com/>

Keywords

gay/lesbian marriage, abortion, immigration, civil rights, gun control, feminism

News

This category refers to any site that is associated with online newspapers, headline news sites, news wiring services, personalized news services and mainstream publications. Some online magazines will be given this rating along with another (i.e., www.wired.com will be news and Science & Tech). This does not include Usenet (classified as discussion forums).

Examples

<http://www.cnn.com>

<http://www.suntimes.com>

<http://www.usatoday.com>

Keywords

newspapers, magazines, wire service, publications, headlines

Classifieds

Sites that offer and advertise ads for barter or sale of merchandise or services.

Religion

This category refers to any site that pertains to mainstream religions, religious activities or participation. This includes information relating to any common religious organization. This is a standalone category.

Examples

<http://www.homechurch.com>

<http://www.gospel.com>

<http://www.wop.com>

Keywords

church, synagogue, temple, worship, ministries, atheism, faith, belief, creed, religious conviction, bible study, youth ministry

Cult

This category refers to any site that advocates or discusses information relating to the use of or membership in cults. Cults are defined as a group or movement exhibiting great or excessive devotion or dedication to some person, idea or thing. Cults employ unethical, manipulative or coercive techniques of persuasion and control designed to advance the goals of the group leaders, to the detriment of the members, their families or the community. Sites that relate to the practice or advocacy of common religions do not belong here as well as any site that serves to educate on the perils of cult activity.

Examples

<http://lastdaysministry.com>

<http://www.rael.org>

<http://www.the600club.com>

Keywords

coercion, manipulation, sect, faction, satanic

Alternative Lifestyle

Sites that contain information relating to gay, lesbian or bisexual lifestyles. This excludes sites that are about social issues or contain sexual content. Sites that promote the lifestyle but are of business or professional nature are not included in this category.

Internet (Web) Category

Anonymizer

This category refers to sites that allow the user to surf the net anonymously. It also refers to sites that allow the user to send anonymous emails. This also includes sites providing proxy bypass information or services.

Examples

<http://www.silentsurf.com>

<http://www.proxify.com>

<http://www.anonymizer.com>

Keywords

anonymous surfing, fake email, proxy bypass, web based proxy

Discussion Forums

This category refers to sites dedicated to Usenet, Usenet news, forums, newsgroups, online bulletin board system.

Examples

<http://discussions.apple.com>

<http://www.driverforum.com>

<http://www.smr-archive.com>

Keywords

forums, newsgroups, bulletin boards, Usenet

Online Chat

This category refers to any site that offers access to, software for or participation in any Internet chat forum. The notion of chat should be associated with any online conversation involving at least two people that takes place in real time. If a site offers chat as one of its services, then the exact location where chat is taking place will be rated as 'Chat'.

Examples

<http://chat.yahoo.com>

<http://chat.msn.com>

<http://www.chat.net>

Keywords

chat, post, IRC, ICQ

Translators

This category refers to any site that offers the service of translating a page, URL, or phrase into various different languages.

Examples

<http://world.altavista.com>

<http://www.freetranslation.com>

<http://www.translation2.paralink.com>

Keywords

languages, online translation

Image Host

Sites that provide image hosting, linking and/or sharing. This includes videos and pictures.

File Host

Sites that offer hosting, backup and sharing of files on the internet.

Peer to Peer

Sites that provide client software to enable peer-to-peer file sharing and transfer.

Email Host

Sites that provide email accounts, free or otherwise.

Examples

<http://www.hotmail.com>

<http://mail.yahoo.com>

<http://www.gmail.com>

Keywords

email, POP3, accounts

Safe Search Engine

This category refers to any search site that is specifically targeted toward families and children. Safe search engines will not allow the child or family member to search for pornography.

Examples

<http://www.yahooligans.com>

<http://www.dibdabdo.com>

<http://www.ajkids.com>

Keywords

kids searches, family safe, kid safe

Sharewares Download

This category refers to sites that specialize in the legal downloading of software.

Examples

<http://www.shareware.com>

<http://www.jumbo.com>

<http://www.tucows.com>

Keywords

desktop themes, wallpapers, screen savers, legal software, downloads, shareware, freeware

Web Banners

This category refers to sites that provide service links/ banners/ ads for web sites. This could also include redirect services.

Examples

<http://www.banner-link.com>

<http://www.123banners.com>

<http://www.free-banners.com>

Keywords

links, banners, ads, redirects, spam urls, gibberish urls

Web Host

This category refers to sites that offer web hosting services, free or otherwise. These sites would usually offer domain names and web spaces to host end-user web pages. Sites that offer web hosting as one of their services would get rated as web host only at the location where actual web hosting is taken place.

Examples

<http://www.geocities.com>

<http://www.tripod.com>

<http://www.angelfire.com>

Keywords

hosting, domain names

Web Search

This category refers to sites that specialize or offer a Web search engine. Sites containing links to other search engines or site-specific search functionality do not qualify for this rating.

Examples

<http://www.yahoo.com>
<http://www.google.com>
<http://www.altavista.com>

Keywords

search engines, directories

Portals

Sites that offer multiple web based services to assist a users experience on the Internet.

High Bandwidth

* This category is no longer used in new ratings from EdgeWave and is intended to be removed from future releases of iPrism. The iGuard team is actively recategorizing all sites previously rated under categories that are deprecated. Sites that would have been rated under a category that is going away (e.g., Digital Music) are now generally rated from one or more of several new categories (e.g., Digital Media and Music) to provide more accurate categorization.

Instead use Portals, Image Host, File Host, Peer to Peer, Digital Media, Radio Stations

Previously, this category was used for sites that take up a significant amount of bandwidth (e.g., MP3s, videoconferences, Download sites for software, games, MPEG).

Was often used in conjunction with another category.

Examples

<http://www.dagonbytes.com>
<http://www.sleepingeve.com>
<http://www.fatfile.com>
<http://www.funtra.com>

Dynamically Detected Proxies

Users can turn on or off the option for dynamically trying to match the patterns for anonymizers and only use the statically categorized anonymizers that the iGuard team rates.

Business Category

Specialized Shopping

This category refers to any site that sells a specific item(s) or product(s) that can be purchased using the Internet or telephone with minimal effort using information on the site. This rating is sometimes accompanied by another rating depending on the subject matter of the items sold.

Examples

<http://www.art.com>

<http://www.carparts.com>

<http://www.furniture.com>

Keywords

online ordering, shopping cart, visa/mc accepted, add to cart, purchase

Dining/Restaurant

Sites that list, review, promote, market or advertise food service and eating establishments. Included are catering services, dining guides and recipes.

Real Estate

Information or services related to buying/selling, renting or financing property.

Automotive

Sites that offer repair, maintenance, parts, sale or other services.

Internet Services

Site that offer services to assist in internet communication.

Corporate Marketing

This category refers to any site that offers corporate info and product information, but does not specifically sell their products online.

Examples

<http://www.deltaco.com>

<http://www.honda.com>

<http://www.mcdonalds.com>

Keywords

corporate info, product info, company info, advertising, promotion

Finance

This category refers to any site that provides investment information, stocks, bonds, mutual funds, newsletters, tips, and firms that offers these services (including banks).

Examples

<http://investing.lycos.com>

<http://www.etrade.com>

<http://www.datek.com>

Keywords

loans, futures, options, currency, estate planning, asset planning, retirement planning, taxes, bankruptcy, stocks, bonds, mutual funds, banks, economics, investment, funding

Job/Employment Search

This category refers to sites that provide jobs or employment services. Includes temp agencies, career resources and resume services. Corporate sites containing a Jobs section should have the specific jobs area classified in this category.

Examples

<http://www.monster.com>

<http://www.hotjobs.com>

<http://www.kellyservices.com>

Keywords

jobs, temp agencies, career, resume builder, headhunter

Professional Services

This category refers to business related sites that include technical and professional services. Normally these businesses sell a service such as legal or consulting rather than a product. This excludes professional sites relating to health (doctors, hospitals, etc) that should be classified as 'Health'.

Examples

<http://www.ei.com>

<http://www.c2graphics.com>

<http://www.leveltendesigns.com>

Keywords

firms, consulting, legal services, accounting services, insurance

Online Auctions

This category refers to sites that involve participating in online auctions, where the site visitor can bid on various items.

Examples

<http://www.ebay.com>

<http://auctions.yahoo.com>

<http://www.atozbid.com>

Keywords

eBay, bidding, trading, auction, public sale, Dutch auction

Education Category

Continuing Education/Colleges

This category refers to sites that contain institutions/colleges offering formal course studies for adults. College homepages will fall into this category as well as distance education, degree programs for part time students, vocation and adult education.

Examples

<http://www.grossmont.edu>
<http://www.ucsd.edu>
<http://www.photofieldschool.com>

Keywords

colleges, universities, junior colleges, trade schools, vocational schools, ESL

History

This category refers to sites that offer a systematic, written and methodical record of past events. These events are arranged as to show the connection of causes and effects, to give an analysis of motive and action, etc.

Examples

<http://www.civilwarsite.com>
<http://www.thehistorychannel.com>
<http://www.history.com>

Keywords

past events, historical information, genealogy

K-12

This category refers to sites dealing with the education of children. Also included in this category are sites with the identifier of K12 (Kindergarten through 12th grade) in the URL. Preschools and day care centers also qualify for this rating.

Examples

<http://www.cathedralcatholic.org>
<http://www.goshenschools.org>
<http://www.forestlake.org>

Keywords

high schools, elementary, junior high, child education, school districts, preschools, day care

Reference Sites

This category refers to site specifically dedicated to providing a research method on one or more subject matters.

Examples

<http://www.radnorlibrary.org>

<http://www.mvls.info>

<http://www.libraryspot.com>

Keywords

libraries, databases, yellow pages, people finder

Sci/Tech

This category refers to sites that relate specifically to education in Science and Technology. Also included in this category are sites relating to education with emphasis on computers, astronomy, programming, physics, etc.

Examples

<http://www.pcworld.com>

<http://www.astronomy.com>

<http://www.aip.org>

Keywords

astronomy, computers, programming, physics, NASA

Sex Education

This category refers to sites that are associated with sex education of children. This includes sites that offer information about sex, AIDS, sexually transmitted diseases, human reproduction, contraceptives, medical research or any other sexually oriented material used to educate. Information within these sites may be minimal in nature as in technical journals, dictionaries, encyclopedias or other reference materials. Sites may also display subtle images or graphics showing sexual organs.



Note: If a site is rated as 'K-12 Sex Education', it must not have any other rating.

Examples

<http://www.sxetc.org>

<http://www.siecus.org>

<http://www.teensource.org>

Keywords

reproduction, contraceptives, family planning, safe sex

Health Category

Alcohol/Tobacco

This category refers to sites that support the use of alcohol and tobacco products. They may be commercial sites, such as Philips Morris and Anheuser Busch, or sites that support the use of alcohol and tobacco related products. This category does not refer to sites that contain educational info about the hazards of alcohol and tobacco products.

Examples

<http://www.budweiser.com>

<http://www.richardsliquors.com>

<http://www.cigarettesexpress.com>

Keywords

cigarettes, beer, wine, liquor, smoking, drunk, breweries, bars

Drugs

This category refers to sites associated with the use, legalization or advocacy of illegal drugs and the illegal use of prescription drugs. Exempt from this category are sites that attempt to relay educational information about the dangers of drug use and sites relating to the products of pharmaceutical companies (should be classified as Health).

Examples

<http://www.yahooka.com>

<http://www.homemadedrugs.net>

<http://www.norml.org>

Keywords

bongs, marijuana, cocaine, paraphernalia

Health

This category refers to sites that claim to improve an individual's well being either medically, organically or through support.

Examples

<http://www.webmd.com>

<http://www.deltadental.com>

<http://health.yahoo.com>

Keywords

doctors, hospitals, medications, fitness, nutrition, dentists, weight loss, massage, cosmetic surgery, day spas, diet, clinics, ophthalmology

Adult Sex Education

This category refers to sites that provide sexual education information to anyone who has graduated from high school. Topics would include how to put on a condom, masturbation and other adult topics such as orgasm and ejaculation. Topics that are dealt with in the adult themes category or sexuality category would not be covered here.

Examples

<http://www.sexualcounselling.com>

<http://www.sexhealth.org>

<http://www.sexhealthinplainenglish.com>

Keywords

kama sutra, sex techniques/tips, masturbation, condoms

Recreation Category

Entertainment

This category refers to sites associated with passive activities - meaning visitors are looking for "sit back and entertain me" sites such as those dealing with theatre, online comics, anime, amusement parks, clubs, etc.

Examples

<http://www.theatre.com>

<http://www.playbill.com>

<http://www.comics.com>

Keywords

clubs, anime, comics, e-cards, theatre, plays, musicals

Gambling

This category refers to any site that presents information about gambling for the purpose of advocating its practice. These sites can provide instruction on any gaming activity that involves gambling or provide actual on-line gambling. Sites that attempt to educate the public on the dangers and/or cures for gambling problems do not belong in this category.

Examples

<http://www.betexchange.net>

<http://www.beverlyhillsbookie.com>

<http://www.gambling.com>

Keywords

casinos, betting, bookies, odds, handicap, gaming, poker

Games

This category refers to any site that is associated with traditional board games, role-playing games and pursuits. This includes sites that promote game makers (Mattel), electronic games, video games, computer games or online games. This category includes both game hardware & software. Also included are tips, advice and cheat codes on playing computer/Internet based games and web sites hosting games and contests.

Examples

<http://www.solitaire.com>

<http://games.yahoo.com>

<http://www.gamespot.com>

Keywords

cheats, codes, clans, video games, contests, fantasy sports, lotteries, bingo

Hobbies/Leisure

This category refers to any site associated with the non-competitive active pursuits or interests outside one's regular occupation or an activity engaged in for pleasure and relaxation during spare time. This would include pet lover sites, sewing, model building/making, woodcarving, stamp/coin collecting, mountain biking, hiking, etc. Note that sites dealing with competitive pursuits should be considered as sports.

Examples

<http://www.nmra.com>

<http://www.stamps.org>

<http://www.boat-show.com>

Keywords

collecting, pastime, leisure pursuit, diversion, sideline, model trains, personal home pages (non-offensive)

Mature Humor

This category refers to any site that contains mature themes and humor that may not be suitable for children, but do not contain pornography or strong profanity. These sites may contain a limited amount of PG-13 profanity without a profanity rating.

Examples

<http://www.theonion.com>

<http://www.laughgallery.com>

<http://www.fark.com>

Keywords

jokes, humor, anecdotes

Television/Movies

Sites that promote or provide content relating to television programming or movies. Note: Sites that contain streaming media or downloadable files such as previews or trailers should include the rating of digital media.

Music

Sites that promote music for entertainment purposes relating to bands, concerts, festivals, orchestras, symphonies and disc jockeys. Note: Sites that provide mp3, streaming or other downloadable media will also be rated digital media.

Digital Media

Digital audio, video and other technologies that can be accessible to stream, download or share.

Radio Stations

Sites whose purpose is to provide and/or promote music, talk or sports radio. These sites have live streams and/or archived listening available.

Examples

<http://www.kioz.com>

<http://www.wrko.com>

<http://www.wfan.com>

Keywords

streaming audio, listen now, on air, live feed

Social Networking/Dating

Sites that offer free or paid services that promote interaction, dating or other networking through forums, chat, email or other methods.

Examples

<http://www.match.com>

<http://www.myspace.com>

<http://friendfinder.com>

<http://eharmony.com>

<http://okcupid.com>

<http://www.friendster.com>

Keywords

singles, online dating, personals, connections, find/make friends, matchmakers

Special Interests

Interest groups/clubs that include environmental, worker, social, and philanthropic organizations. These include alumni associations and all non-profit organizations.

Examples

<http://www.amexp.org>

<http://charity.org>

<http://surfrider.org>

<http://www.ncna.org>

<http://www.teamsters.com>

Keywords

associations, foundations, charities, chapters, non-profits, donations, alumni

Sports

This category refers to any site that contains information about sports or sports related activities. This includes sites that provide sports scores or games. These sites may also contain information about sporting events, camps, teams or outings. Sports are defined as organized and competitive athletics.

Examples

<http://www.espn.com>

<http://www.mlb.com>

<http://www.nba.com>

Keywords

baseball, football, tennis, basketball, golf, teams, motor sports, NCAA, high school sports, little league

Travel

This category refers to sites specializing in travel and travel-related information or activities. This includes travel destinations, reservation services, discount travel listings, leisure travel package listings, and special events in various cities. Also included are sightseeing guides, airlines and online flight booking agencies, accommodations and rental cars. Additional items such as chamber of commerce or non-government information pertaining to a given city or region can also be assigned this category.

Examples

<http://www.lasvegastours.com>

<http://www.visit.hawaii.org>

<http://www.travelocity.com>

Keywords

bed & breakfast, reservations, flights, trips, airlines, travel agent, cruise, vacation, site seeing, tourist, tour, voyage, timeshare, rental cars

Web Log (Blog)

Journals, diaries or newsletters that can be updated daily usually involving personal thoughts/opinions on internet, social or political issues. Other categories can be added to further classify.

APPENDIX B Configuring Browsers for Proxy Mode

To enable browser-based authentication through iPrism, you must configure each browser to use iPrism as a proxy server.



Important: Do **not** do this if you are using bridge (transparent) mode.)

Configuring Firefox for Proxy Mode

1. Start up Firefox Version 3.x.
2. From within Firefox, click **Tools**, then select **Options**.
3. Select **Advanced**.
4. Select the **Network** tab and click **Settings**.
5. Select **Manual proxy configuration**.
6. Type the IP address or hostname of the iPrism and default port 3128.



Note: If you changed the iPrism's default proxy port, type that port number instead.

7. Confirm the changes by clicking **OK** until you are returned to the main Firefox window.

Configuring Safari (Mac OS X only) for Proxy Mode

1. Open Safari.
2. Click **Safari** at the top of the screen.
3. Click **Preferences**.

4. In the menu bar at the top of the window, click **Advanced**.
5. Click **Change Settings** (next to the Proxies label).
6. Check **Web Proxy (HTTP)** .
7. In their respective fields next to that check box, type the IP address or hostname of the iPrism and default port 3128.



Note: If you changed the iPrism's default proxy port, type that port number instead.

8. Click **Apply Now**.

Configuring Internet Explorer for Proxy Mode

1. From within Internet Explorer, select the **Tools** menu, then select **Internet Options**.
2. Select the **Connections** tab.
3. Click **LAN Settings** to open the Local Area Network (LAN) Settings dialog box.
4. In the **Proxy Server** frame, check **Use a proxy server**.
5. In the **Address** field, enter the IP address that you assigned to your iPrism server. (You do not need to include the http://.)
6. In the **Port** field, enter 3128.



Note: If you want to manually specify the proxy address and port settings for each protocol (FTP, HTTP, etc.), click **Advanced** and type the information in the Proxy Settings dialog box. Uncheck the Use the same proxy server for all protocols checkbox, and type the iPrism IP address in the HTTP, Secure, FTP, and Gopher fields. Assign each line the Port value "3128".

7. Click **OK**.
8. If you do not want iPrism to filter local (e.g., Intranet) traffic, check **Bypass proxy server for local addresses**.
9. Click **OK**. This browser is now configured to authenticate through iPrism.

APPENDIX C iPrism Error Messages

This section describes the more common error messages that you may encounter while using iPrism.

The error conditions are listed by error name/type in no particular order. A description of the conditions that cause each error is provided as well as a screen shot showing the typical error page that is generated. Beneath each screen shot is a description of how to correct the condition.



Note: This section covers only the more common error messages; errors that occur only rarely are not included.

iPrism Rating Error

If you have created a custom filter and have Filter Failover set to **Block** ([Filter Failover Mode](#)), you may see this error.

If Filter Failover is set to **Pass**, the error will not occur, but traffic may pass unfiltered for a few seconds.

iPrism List Update

By default, iPrism downloads its filter list once per day. During the actual download, web traffic is not impacted. However, once the download is complete, iPrism needs to reload its filter list. (This also occurs when custom filters are added or edited in the system.) The reload process typically lasts 2 - 5 seconds. During this time, iPrism displays the iPrism List Update message.

This message is not an error message and should only last for a few seconds. If the message does not disappear contact Technical Support:

http://edgewave.com/support/web_security/default.asp

iPrism List Error

iPrism needs a filter list to operate correctly. If a system is missing its filter list, it is possible to configure iPrism to 'pass all' or 'block all' HTTP traffic using the settings in the **System Settings > System Preferences > Filter Failover mode** frame ([Filter Failover Mode](#)).

If iPrism is set to block all traffic (i.e., Filter Failover Mode is set to "Block Traffic") it shows this error when the filter list is missing. Otherwise, if Filter Failover Mode is set to "Pass Traffic (Unfiltered)", all traffic will be passed unfiltered.

If the filter list cannot update for 3 days, an email will be sent to the iPrism administrator.

If you receive this error, contact Technical Support at:

http://edgewave.com/forms/support/web_security.asp

iPrism Filter Service Expired

This error indicates that iPrism's subscription to the filter list update has expired.

iPrism's registration key must be updated before access is possible. Contact Technical Support for assistance:

http://edgewave.com/forms/support/web_security.asp

Access Denied

The Access Denied error appears if any of the following conditions occur:

- The IP address of the workstation trying to access iPrism is not allowed to access iPrism. If needed, the configuration can be updated by the system administrator from the **System Settings > Network ID** section.
- The mode used by the workstation is not allowed. Workstations can access iPrism in proxy (direct mode), where the browser or application is configured to use iPrism as a proxy, or in bridge (transparent) mode (no browser configuration needed). Each mode can be independently disabled from the **System Settings > Network ID** section.

- iPrism detected a routing loop. A routing loop occurs when the traffic that iPrism is sending to reach a website is being routed via iPrism again, causing iPrism to filter its own traffic. This is typically the result of configuring iPrism's default gateway as a machine located on the internal interface of the appliance.

Check iPrism's configuration (access and authentication) for the client workstation's IP address; if looping occurs, check the routing setup in **System Settings > Network Services**.

Authentication is Required

The Authentication is Required error displays when a workstation operating in proxy mode does not authenticate or provide valid credentials (username and password). This may occur if the profile associated with the username is invalid (typically, an LDAP configuration error).

Reload the page and provide your user credentials when prompted.

Connection Failed

If you get the Connection Failed message, iPrism is not able to connect to the desired web server. This is typically the result of one of the following conditions:

- The remote server is temporarily unavailable.
- You entered a URL with an incorrect port number.
- The connection is being denied by upstream equipment, such as a firewall.

To correct the error:

- Check the URL to verify it is correct.
- Try accessing the site again later.
- Check your network environment for s that may prohibit the connection.

Unable to Determine IP Address

The error "Unable to determine IP address from host name for <URL>" indicates that iPrism is not able to resolve the hostname of the desired URL.

If this happens only for a small number of websites, it is probably a transient network error with the web server's DNS service, in which case you can try again later.

If multiple (or all) web servers are showing the same symptoms, iPrism's DNS service is unable to operate because its DNS master (if one is used) may be unreachable, or because it can not perform direct DNS requests. This would occur if a firewall were blocking ports UDP/53 and/or TCP/53.

Wait awhile and check the URL again; if the error occurs across multiple web servers, check iPrism's DNS configuration and status.

Invalid Request

The "Invalid Request" error occurs when the syntax of the HTTP request submitted to iPrism is not valid and does not follow the HTTP protocol. A possible reason is that the request did not include the HTTP/1.x information on the HTTP request line. This error is infrequent in web browsers and more often occurs with other HTTP applications.

Check the request syntax as displayed by iPrism and fix the client software.

Invalid URL

The "Invalid URL" error occurs if iPrism detects that the request does not respect the HTTP RFC. In short, the syntax of the URL is incorrect. The usual reason this occurs has to do with invalid characters in the URL, and may happen if the web page contains such an invalid URL as a link.

Check the request's syntax. If the URL is a link on a web page, you can also inform the remote website's administrator.

iPrism is in the Process of Reconfiguring Itself

iPrism displays this message while a reconfiguration is in progress.

If the administrator made a change to the configuration, iPrism reloads its configuration. This is a short-lived condition and the message should go away within 10 seconds.

Retry after a few seconds. If the error message does not go away contact Technical Support at:

http://edgewave.com/forms/support/web_security.asp

Zero Sized Reply

The "Zero Sized Reply" error occurs when no data is returned in the HTTP connection. This may happen under the following conditions:

- The remote web server did not send actual data and closed the connection too early (typically a script error).
- The remote web server is unable to reply.

This is a problem on the web server you are trying to reach. Try again later or contact the web server's administrator.

Write Error / Broken Pipe

This message is shown when iPrism is not able to establish a connection to a web server. A common reason is that an upstream firewall is closing connections (TCP resets), usually because it has reached a threshold in the maximum number of connections it will allow from iPrism (such as CISCO's PIX).

This can be addressed by managing the maximum number of connections on the firewall.

Check the network environment (firewall logs, routing).

Corporate Office

15333 Avenue of Science, San Diego, CA 92128

Phone: 858-676-2277

Toll Free: 800-782-3762

Fax: 858-676-2299

Email: info@edgewave.com