



iPrism®

Administration Guide

Version 6.500

© 2001 – 2011 St. Bernard Software Inc. All rights reserved. The St. Bernard Software logo, iPrism and are trademarks of St. Bernard Software 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, or translated into another language without prior permission of St. Bernard Software, Inc.

ADM0001.6.5.000REL

Contents

Chapter 1	Introduction	1
	About iPrism	1
	About this Guide	1
	Who Should Use this Guide?	2
	Overview	2
	Knowledgebase, Tutorials and Technical Support.....	4
	Installation Notes	4
Chapter 2	Overview	5
	How iPrism Works	5
	The Filtering Database	5
	<i>Deciding What Gets Blocked</i>	6
	<i>Assigning Profiles</i>	9
	Getting Past Blocked Sites.....	9
	How iPrism Filters Internet Activity	11
	Introduction to Profiles	12
	Proxy Mode	12
	Bridge (Transparent) Mode	13
	Using the Management Interface	15
	Logging into and out of iPrism.....	15
	Restarting and Shutting Down iPrism.....	16
	The iPrism Home Page	17
	Using the iPrism Home Page	17
Chapter 3	Profiles & Filters	19
	Custom Filters	20
	To edit a custom filter	23
	To delete a custom filter	23
	To search for a custom filter	23
	Profiles	24
	How iPrism Uses Profiles.....	24
	iPrism's Default Profiles	25
	Web Profiles.....	25
	<i>Adding a Profile</i>	26

<i>Copying a Profile</i>	27
<i>Deleting a Profile</i>	28
Application Profiles.....	29
<i>Adding a Profile</i>	29
<i>Copying a Profile</i>	30
<i>Deleting a Profile</i>	31
Authentication and Assigning Profiles to Users	31
Assigning Profiles to a Set of IP Addresses (Workstations)...	31
Access Control Lists (ACLs).....	32
Creating a New ACL	32
Editing ACL Settings	34
Deleting an ACL	34
Lock ACL.....	34
Current Overrides	36
Revoking Overrides.....	37
Pending Requests	38
Granting Requests	38
Denying Requests.....	39
Recent Blocks	40
Antivirus.....	40
Remote Filtering	41
Using Remote Filtering.....	41
Enabling Remote Filtering.....	42
Chapter 4	
Users and Networks	47
Local Users	48
To Add a User	48
To Import a User.....	49
Groups.....	51
Mapping Groups to Profiles.....	51
<i>Rules and Guidelines for Group Mapping</i>	51
<i>Nested Groups</i>	52
To Add, Edit, or Delete Groups	53

	<i>To Add a Group</i>	53
	<i>To Edit a Group</i>	54
	<i>To Delete a Group</i>	54
	Privileges	54
	Mapping Privileges to Groups	54
	Networks	57
	To Add a Network Profile.....	59
	To Edit a Network Profile.....	64
	To Delete a Network Profile.....	64
	Admin Roles	65
	To Add or Edit an Admin Role	65
	To Delete an Admin Role	69
	Exceptions	70
	To Add an Exception	70
	To Edit an Exception	72
	To Delete an Exception	73
	Remote Users	73
	To Add a Client Exception.....	76
	To Edit a Client Exception	77
	To Delete a Client Exception	78
	To Import Remote Users	78
	To Export Remote Users	80
Chapter 5	Reporting	81
	Email Alerts	82
	To Add an Email Alert.....	83
	To Edit an Email Alert.....	84
	To Delete an Email Alert.....	85
	Report Manager	86
Chapter 6	Maintenance	87
	Appliance Updates	88
	Checking for Hotfixes	88
	Installing a New Hotfix.....	88

Rebooting after Installing Hotfix(es)	90
Uninstalling a Hotfix	91
Searching for a Hotfix.....	91
Backup & Restore	93
Backing Up.....	93
<i>Setting Backup Preferences</i>	93
<i>Setting Backup Reminders</i>	94
Restoring.....	94
<i>Restoring Your System from a Local Backup</i>	94
<i>Restoring iPrism to its Default (Factory) Configuration</i>	95
Event Log	96
To Delete Access Event Records.....	97
Policy Test	98
Self Check	99
Send Test Email	100
Site Rating & Test.....	102
Support Tunnel.....	103
Test Directory Services.....	104
Chapter 7	
System Settings	107
Central Management.....	108
Customizable Pages	108
To Customize the Authentication, Access Denied, or Other Pages.....	109
<i>Customizable Page Tags</i>	112
Directory Services	113
Choosing an Authentication Mechanism.....	114
Local Authentication.....	115
<i>Creating User Accounts on the iPrism</i>	115
LDAP Authentication	115
<i>Setting up the iPrism LDAP Client</i>	115
Microsoft Windows Authentication (NTLM)	121
<i>Maintaining iPrism's Machine Account</i>	125
<i>Debugging Windows Authentication Problems</i>	126

<i>Assigning an Authentication Mechanism to an IP Address Range</i>	126
<i>Auto-Login Details</i>	126
Authentication from the User's Perspective	131
Microsoft Windows Active Directory Authentication (Active Directory 2000/2003).....	132
<i>Assigning iPrism Profiles to Windows AD Global Groups</i>	136
Microsoft Windows Active Directory Authentication (Active Directory 2008).....	136
Migrating from AD 2003 to AD 2008	140
Enterprise Reporting	141
Event Logging	141
Syslog Export.....	141
Email Settings	142
FTP Settings	143
License Key.....	144
Creating the iPrism server certificate and installing a trusted server certificate.....	144
Uploading your license key	146
Local Categories	147
Using Local Categories	147
Network ID.....	149
Network Services	154
Network Hardening (Protecting Against DoS Attacks).....	155
Enabling SNMP	155
<i>The SNMP Community String</i>	156
WCCP	156
<i>Configuring WCCP Settings in iPrism</i>	157
Configuring SMTP Relay Settings.....	158
Enabling the Co-Management Network	158
Checking iPrism Status	160
Pending Request Options	161
Ports	162

Proxy and Configuration Ports	162
Redirect and HTTPS Ports.....	162
To Add a Proxy or Configuration Port.....	163
To Add, Edit or Delete a Redirect port (Bridge (transparent) mode only)	164
To Add, Edit or Delete an HTTPS port (Proxy mode only)	164
Proxy	166
To Slave iPrism to a Parent Proxy (Proxy Mode)	166
To Enable an Upstream Proxy (Bridge (transparent) Mode) ..	168
To Configure the Filter List/System Update Proxy Server	168
System Preferences	169
Backup Settings	169
Bypass Authentication.....	170
Current Date and Time.....	170
Filter Failover Mode	171
Setting or Changing the Supervisor Password	172
Filter List (iGuard) Updates	172
<i>Scheduling Filter List (iGuard) Updates</i>	172
<i>Checking iPrism's Filter List Status</i>	173
System Updates.....	173
Proxying for External Users	174
Unrated Pages (iARP)	175
User Settings.....	177
Chapter 8	
System Status	179
About	180
Administration Log.....	181
Configuration Summary.....	182
Connectivity.....	184
To ping a host.....	184
To trace network activity	185
To perform a DNS lookup.....	185
To refresh the System Updates server.....	186

	Routing Table	187
	Security Log	188
	Status	190
	Status	190
Chapter 9	Central Management	193
	Before You Begin	193
	Setting up a Master/Slave Configuration	194
	<i>Designating Slave Systems</i>	194
	Designating the Master System	195
	Changing the Master System	198
	Removing Slave System(s)	198
	Using Standalone Mode	199
	How to Upgrade iPrisms in a Central Management Configuration.....	199
	Upgrading Decoupled Master and Slave(s)	199
	<i>To Upgrade the Slave(s):</i>	200
	Upgrading Master & Slave(s) without Decoupling.....	201
Chapter 10	Override Management	203
	Access Denied Page Options.....	203
	Using Override Privileges.....	205
	Overriding a Blocked Web Site	205
	Using Access Requests.....	210
	<i>Requesting Access to a Site</i>	210
	Managing Override Access	214
APPENDIX A	Filtering Categories	215
	Site Rating Categories	216
	Sex Category	216
	<i>Adult</i>	216
	<i>Lingerie/Bikini</i>	216
	<i>Nudity</i>	217
	<i>Pornography</i>	217
	<i>Sexuality</i>	218

Questionable Activities Category	218
<i>Copyright Infringement</i>	218
<i>Computer Hacking</i>	219
<i>Intolerance/Extremism</i>	219
<i>Miscellaneous Questionable</i>	220
<i>Profanity</i>	220
<i>Tasteless</i>	221
<i>Weapons/Bombs</i>	221
<i>Violence</i>	222
Security Exploits Category	222
<i>Phishing</i>	222
<i>Spyware/Adware</i>	223
<i>Malware</i>	223
Society Category.....	224
<i>Alt/New Age</i>	224
<i>Art/Culture</i>	224
<i>Family Issues</i>	225
<i>Government</i>	225
<i>Politics</i>	225
<i>Social Issues</i>	227
<i>News</i>	227
<i>Classifieds</i>	227
<i>Religion</i>	228
<i>Cult</i>	228
<i>Alternative Lifestyle</i>	229
Internet (Web) Category.....	229
<i>Anonymizer</i>	229
<i>Discussion Forums</i>	229
<i>Online Chat</i>	230
<i>Translators</i>	230
<i>Image Host</i>	230
<i>File Host</i>	231
<i>Peer to Peer</i>	231

<i>Email Host</i>	231
<i>Safe Search Engine</i>	231
<i>Sharewares Download</i>	232
<i>Web Banners</i>	232
<i>Web Host</i>	233
<i>Web Search</i>	233
<i>Portals</i>	233
<i>High Bandwidth</i>	234
<i>Dynamically Detected Proxies</i>	234
Business Category	235
<i>Specialized Shopping</i>	235
<i>Dining/Restaurant</i>	235
<i>Real Estate</i>	235
<i>Automotive</i>	235
<i>Internet Services</i>	235
<i>Corporate Marketing</i>	236
<i>Finance</i>	236
<i>Job/Employment Search</i>	237
<i>Professional Services</i>	237
<i>Online Auctions</i>	238
Education Category.....	238
<i>Continuing Education/Colleges</i>	238
<i>History</i>	239
<i>K-12</i>	239
<i>Reference Sites</i>	240
<i>Sci/Tech</i>	240
<i>Sex Education</i>	241
Health Category	241
<i>Alcohol/Tobacco</i>	241
<i>Drugs</i>	242
<i>Health</i>	242
<i>Adult Sex Education</i>	243
Recreation Category	243

	<i>Entertainment</i>	243
	<i>Gambling</i>	244
	<i>Games</i>	244
	<i>Hobbies/Leisure</i>	245
	<i>Mature Humor</i>	245
	<i>Television/Movies</i>	246
	<i>Music</i>	246
	<i>Digital Media</i>	246
	<i>Radio Stations</i>	246
	<i>Social Networking/Dating</i>	247
	<i>Special Interests</i>	247
	<i>Sports</i>	248
	<i>Travel</i>	248
	<i>Web Log (Blog)</i>	248
APPENDIX B	Configuring Browsers for Authentication	249
	Configuring Firefox for Authentication	250
	Configuring Safari for Authentication (Mac OS X only)	252
	Configuring Netscape Navigator for Authentication.....	254
	Configuring Internet Explorer for Authentication	255
APPENDIX C	iPrism Error Messages	259
	iPrism Rating Error.....	260
	iPrism List Update Error	261
	iPrism List Error.....	262
	iPrism Filter Service Expired Error	263
	Access Denied Error	264
	Authentication is Required Error	265
	Connection Failed Error	266
	Unable to Determine IP Address Error.....	267
	Invalid Request Error	267
	Invalid URL (Error)	269
	iPrism is in the Process of Reconfiguring Itself (Error).....	270
	Zero Sized Reply (Error)	271

Write Error / Broken Pipe	272
Index	285

Figures

FIGURE 1. Blocking setup in an ACL.....	7
FIGURE 2. Profiles and Scheduling	8
FIGURE 3. Blocked Page.....	10
FIGURE 4. Deploying iPrism in Proxy Mode	13
FIGURE 5. Deploying iPrism in Bridge (Transparent) Mode.....	14
FIGURE 6. Logging in	16
FIGURE 7. Logging out	16
FIGURE 8. Custom Filters.....	21
FIGURE 9. Filter Details.....	22
FIGURE 10. Web Profiles.....	26
FIGURE 11. Web Access Control List (ACL)	27
FIGURE 12. Deleting a Profile.....	28
FIGURE 13. Application Profiles	29
FIGURE 14. Application ACL	30
FIGURE 15. ACL	33
FIGURE 16. Lock ACL	35
FIGURE 17. Current Overrides	36
FIGURE 18. Pending Requests.....	38
FIGURE 19. Antivirus	40
FIGURE 20. Remote Filtering.....	42
FIGURE 21. Setting up Remote Filtering Exceptions.....	44
FIGURE 22. Select a default web profile for remote users.....	45
FIGURE 23. Import Local Users.....	50
FIGURE 24. Groups	52
FIGURE 25. Nested Groups Example.....	53
FIGURE 26. Profile Map.....	54
FIGURE 27. Privileges	55
FIGURE 28. Privilege mapping	56
FIGURE 29. Networks section.....	58
FIGURE 30. Network Profile Details.....	59
FIGURE 31. Authentication Tab – Proxy Mode.....	60
FIGURE 32. Advanced Auto-Login settings	63
FIGURE 33. Admin Roles.....	65
FIGURE 34. Admin Roles – Access Control List Tab.....	67
FIGURE 35. Maximum Duration for Overrides.....	68

FIGURE 36. Managing Exceptions.....	71
FIGURE 37. Remote Users	75
FIGURE 38. Adding or Editing a Remote User	77
FIGURE 39. Importing Remote Users	78
FIGURE 40. Exporting Remote Users.....	80
FIGURE 41. Email Alerts.....	82
FIGURE 42. Hotfix Manager/Appliance Updates	89
FIGURE 43. Completion of Hotfix Installation	90
FIGURE 44. Reboot iPrism	91
FIGURE 45. Confirm Reboot.....	91
FIGURE 46. Backup & Restore	93
FIGURE 47. Event Log.....	96
FIGURE 48. Policy Test	98
FIGURE 49. Self Check.....	100
FIGURE 50. Send Test Email.....	101
FIGURE 51. Confirmation of Test Email Sent	101
FIGURE 52. Site Rating & Test.....	102
FIGURE 53. Support Tunnel	103
FIGURE 54. Test Directory Services.....	105
FIGURE 55. iPrism Customizable Pages	108
FIGURE 56. Customizing the 'Access Denied' Page	109
FIGURE 57. LDAP Authentication.....	116
FIGURE 58. LDAP Presets	117
FIGURE 59. Joining iPrism to an Microsoft Windows Domain	122
FIGURE 60. Advanced Settings	124
FIGURE 61. Auto-Login in Bridge (Transparent) Mode.....	128
FIGURE 62. Proxy Mode authentication	130
FIGURE 63. Transparent Authentication Login	131
FIGURE 64. Enabling Active Directory 2000/2003 Authentication	133
FIGURE 65. Advanced Settings	134
FIGURE 66. Authentication Mode & Status.....	135
FIGURE 67. Active Directory 2008 authentication	137
FIGURE 68. Enabling Active Directory 2008 Authentication	138
FIGURE 69. Authentication Mode & Status.....	140
FIGURE 70. Event Logging – Syslog Export.....	142

FIGURE 71. Event Logging – Email Export.....	142
FIGURE 72. Event Logging – FTP Settings	143
FIGURE 73. Registration, License Key and SSL Certificate information	144
FIGURE 74. SSL Certificate options	146
FIGURE 75. Local Categories	148
FIGURE 76. Network ID	150
FIGURE 77. Add Static Route	153
FIGURE 78. Network Services	154
FIGURE 79. Enable DoS protection	155
FIGURE 80. Enabling SNMP	156
FIGURE 81. WCCP selection.....	157
FIGURE 82. Set Service Group Password.....	157
FIGURE 83. Co-Management Network.....	159
FIGURE 84. Network Health Status	160
FIGURE 85. Pending Request Options.....	161
FIGURE 86. Ports window.....	163
FIGURE 87. Proxy.....	167
FIGURE 88. System Preferences.....	169
FIGURE 89. Date and Time Settings	171
FIGURE 90. System Update Settings	173
FIGURE 91. Proxying for External Users	174
FIGURE 92. External Connection Settings.....	174
FIGURE 93. Unrated Pages	176
FIGURE 94. Dialog prompt example	177
FIGURE 95. Reset dialog prompts	177
FIGURE 96. About iPrism.....	180
FIGURE 97. iPrism Administration Log	181
FIGURE 98. Configuration Summary	183
FIGURE 99. Connectivity Window.....	184
FIGURE 100. Ping.....	185
FIGURE 101. DNS Lookup Results.....	186
FIGURE 102. Default Routes	187
FIGURE 103. Security Log	189
FIGURE 104. System Status window.....	191
FIGURE 105. System Status window	192

FIGURE 106. Designate Slave.....	195
FIGURE 107. Designate Master.....	196
FIGURE 108. Standalone iPrism.....	199
FIGURE 109. Access Denied Page.....	204
FIGURE 110. Override.....	206
FIGURE 111. Login.....	206
FIGURE 112. Override Request.....	208
FIGURE 113. Override Request rejected.....	210
FIGURE 114. Request Access page.....	211
FIGURE 115. Request Access page, part II.....	212
FIGURE 116. Request Access Confirmation.....	213
FIGURE 117. Configuring Firefox for authentication.....	250
FIGURE 118. Configuring Firefox for authentication – Connection Settings.....	251
FIGURE 119. Configuring Safari for authentication.....	253
FIGURE 120. Proxy Settings in Netscape Navigator.....	254
FIGURE 121. LAN Settings.....	256
FIGURE 122. Manually Configuring Proxy Settings in IE.....	257
FIGURE 123. iPrism Rating Error.....	260
FIGURE 124. iPrism List Update Error.....	261
FIGURE 125. iPrism List Update Error.....	262
FIGURE 126. iPrism Filter Service Expired Error.....	263
FIGURE 127. Access Denied Error.....	264
FIGURE 128. Authentication is Required Error.....	265
FIGURE 129. Connection Failed Error.....	266
FIGURE 130. Unable to Determine IP Address from Host Name Error.....	267
FIGURE 131. Invalid Request Error.....	268
FIGURE 132. Invalid URL Error.....	269
FIGURE 133. iPrism is in the Process of Reconfiguring Error.....	270
FIGURE 134. Zero Sized Reply Error.....	271
FIGURE 135. Write Error.....	272

Introduction

About iPrism

The iPrism Web Filter from St. Bernard 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, in order to get the best performance possible from your appliance.

This chapter introduces you to how information is arranged and presented in this guide. This chapter also provides information about how to access the iPrism tutorials and Knowledgebase, and contact information for St. Bernard Software Technical Support.

This manual does not include installation instructions. Please refer to the *iPrism Installation 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

Overview

The following chapters are included in this manual:

Chapter 1: Introduction shows you how iPrism fits into your network, as well as giving you an overview of the capabilities of this system.

Chapter 2: Overview describes the major software components that iPrism uses, including Antivirus (AV) Scanning and Filtering, and how they fit together.

Chapter 3: Profiles & Filters provides detailed instructions on how to use iPrism's extensive filtering capabilities, including Remote Filtering.

Chapter 4: Users and Networks shows you how to create local iPrism users, how to create remote users, how to configure the iPrism's network interface, and other network-related settings.

Chapter 5: Reporting describes how to use the various iPrism Reporting tools, such as how to set up reports, schedules, the Real-Time Monitor, and Email Alerts.

Chapter 6: Maintenance covers the iPrism maintenance operations and tools, such as how to update your appliance, how to back it up or restore it, how to view events and test policies, how to run a self check and send a test email, how to open a support tunnel to iPrism Technical Support, how to test directory services, and how to manage and test site ratings.

Chapter 7: System Settings explains how to customize iPrism's HTML templates, how to set up and configure Directory Services such as Windows Active Directory 2008, the Enterprise Reporting System (ERS), event logging, your iPrism license and remote filtering keys, local filtering categories, network management, ports, proxies, system preferences such as how often to download updated filter lists, and unrated pages.

Chapter 8: System Status contains information about how to use the various system monitoring and status tools, such as the Security Log and the Administration Log, a summary of your iPrism configuration, connectivity status, default routes, and the status of your iPrism system.

Chapter 9: Central Management describes how to set up and manage large set of iPrisms in a central management (master/slave) configuration.

Chapter 10: Override Management describes the user and administrator options for handling blocked pages, and how iPrism gives tremendous flexibility for dealing with blocked web pages, while at the same time allowing a great deal of control over Internet usage.

Appendix A describes the filtering categories.

Appendix B describes how to configure your Web browsers for authentication.

Appendix C describes the error messages you may encounter, and what causes them.

Knowledgebase, Tutorials and Technical Support

If you are unable to resolve your issue using the manual, please check our Knowledgebase at <http://www.stbernard.com/products/support/iprism/knowledgebases.asp>, and our iLearn embedded video tutorials at <http://ilearn.stbernard.com/>. iLearn consists of a series of short task-oriented videos to help guide you through specific iPrism configuration scenarios.

For iLearn tutorials specific to Remote Filtering, go to http://ilearn.stbernard.com/profiles_filtering/remote_filtering/tutorial.asp.

You may also contact the St. Bernard Software iPrism support team at <http://www.stbernard.com/products/support/iprism/default.asp>. When contacting tech support, please be sure to 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, in order 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 manual 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 **St. Bernard Software website**. This site contains the very latest support information for iPrism.

http://www.stbernard.com/products/support/iprism/support_iprism.asp

If you are still unable to find a solution, you may request assistance with your installation from St. Bernard Software's 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.

This chapter describes how iPrism works and provides an overview of its features and capabilities. The following topics are contained in this chapter:

How iPrism Works: page 5

How iPrism Filters Internet Activity: page 11

The iPrism Home Page: page 17

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.

There are two independent type of blocking rules. The Web Profiles control web traffic, and the Application Profiles controls IM and P2P traffic. For detailed information on profiles, refer to the *Profiles* section of Chapter 3, Profiles & Filters.

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.). In order to ensure that each iPrism unit is always operating with the very latest filtering database, the iPrism appliance automatically connects to St. Bernard’s server daily and downloads the most recent filtering database files. The URL database now contains more than 80 categories with millions of websites. See Appendix A on page 215 for detailed information about categories.

Deciding What Gets Blocked

The first step in setting up your filter is to create a Access Control List (ACL). This is a list which 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
<i>everything else</i>	No	No

To create a ACL, from the iPrism home page, select Profiles & Filters, then **Profiles**. When you create a new profile, you will be prompted to create a new ACL.

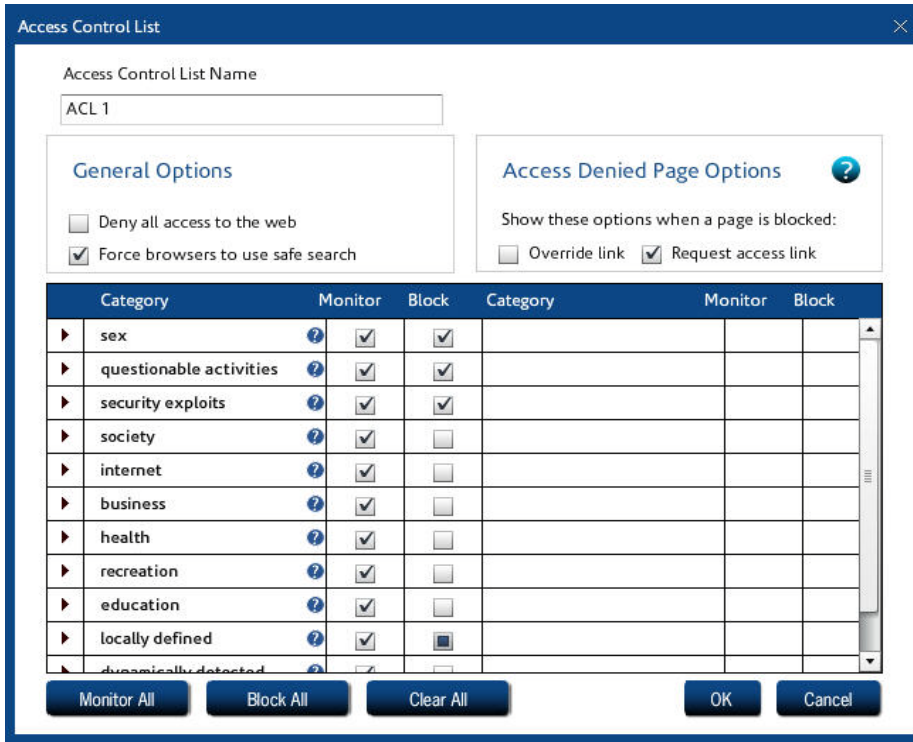


FIGURE 1. Blocking setup in an ACL

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 our two ACLs, as shown in Figure 2.

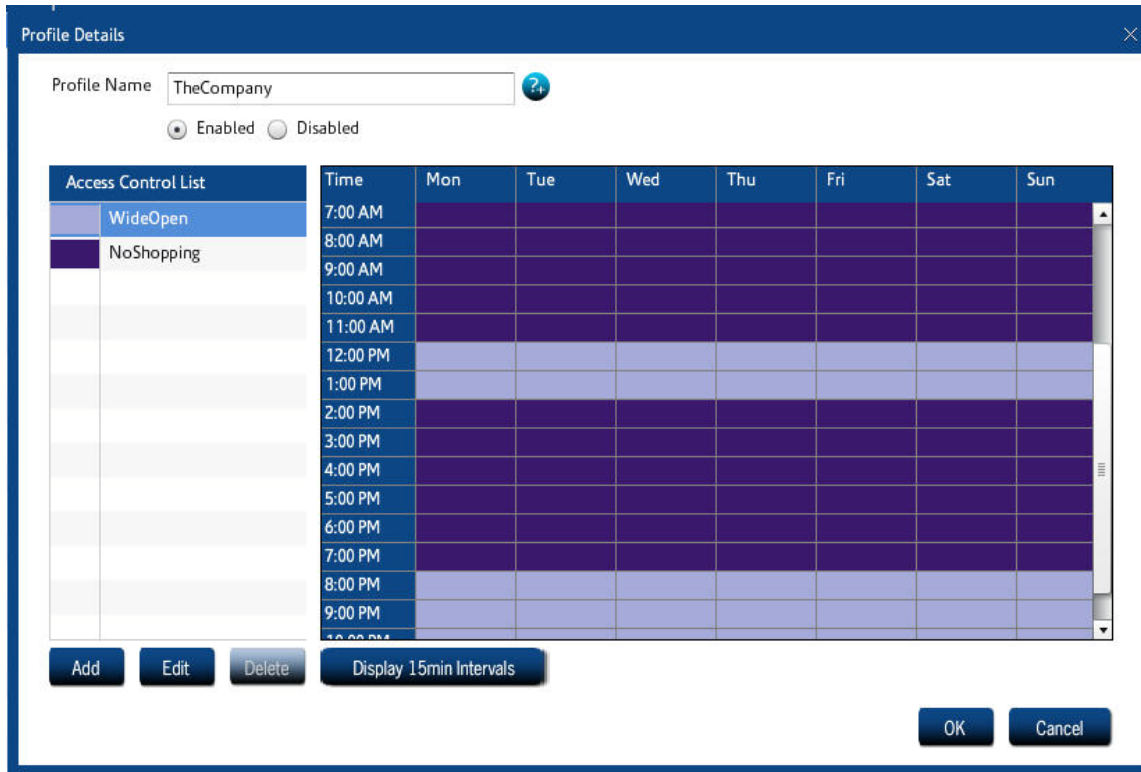


FIGURE 2. Profiles and Scheduling

In our example, we’ve created a schedule that applies to the entire company (Profile name = TheCompany). 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.¹

iPrism interfaces with Windows NTLM authentication as well as LDAP, which is used UNIX, Linux, Novell. If you want to use "user level" authentication, *Chapter 4: Users and Networks* contains simple, step-by-step instructions which will help you get your iPrism working with your existing authentication system. Please refer to that section for further information.

Assigning a Profile to a set of IP addresses

The network to profile mapping dialog can be found in Users & Networks > Groups, explained in detail beginning on page 51.

For more information on configuring profiles for your network, see "Profiles" on page 24 and "Application Profiles" on page 29.



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

Getting Past Blocked Sites

Users that have been granted the proper administrative privileges in iPrism have options when they encounter a blocked site. The **Override/Request Access** button when the user encounters an Access Denied page provides two different options for getting to a page that is being blocked by iPrism.

1. 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 *Chapter 4: Users and Networks*.

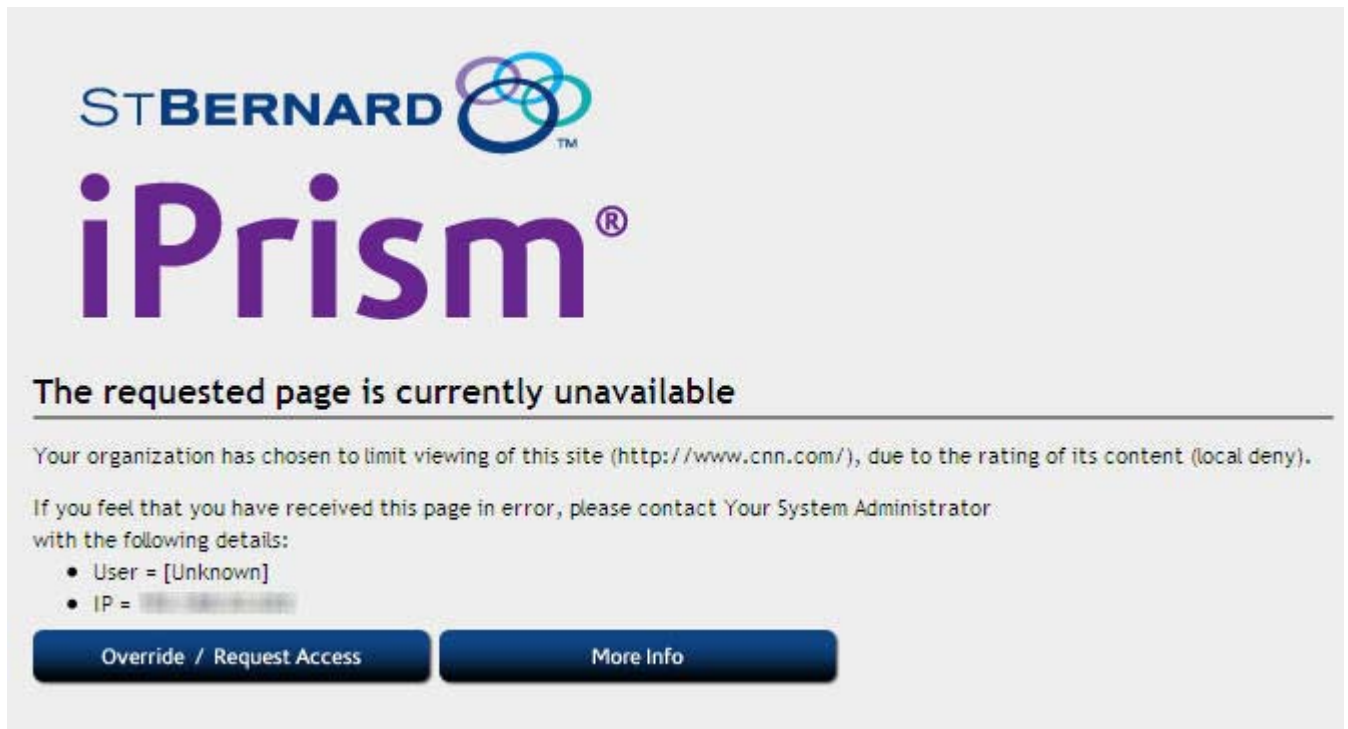


FIGURE 3. Blocked Page

The first option, **Override**, prompts you to login with your administrative password. Users 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, if a user has been granted override privileges (see “Managing Override Access” on page 214), s/he can override the blocked page. Whether or not user(s) can override blocked pages is configured and managed by the iPrism administrator(s).

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 *Chapter 10: Override Management* for detailed instructions on managing overrides and requests.

The second option, **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” on page 38).



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 instead² (what the user sees is determined by how the iPrism administrator has chosen to handle requests to blocked categories; for specifics, see **Access Denied Page Options** under “Access Control Lists (ACLs)” on page 32). An Access Denied page notifies the client that the web page they tried to access belongs to a category which is currently being blocked.

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 www.stbernard.com/products/support/iprism/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 Chapter 3, **Profiles & Filters**, beginning on page 19.

2. 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.

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*, which determine which websites are filtered, and *Application Profiles*, which 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.

Prism can be configured in either **proxy mode** or **bridge (transparent) mode**.

Proxy Mode

Proxy mode (Figure 4) 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.

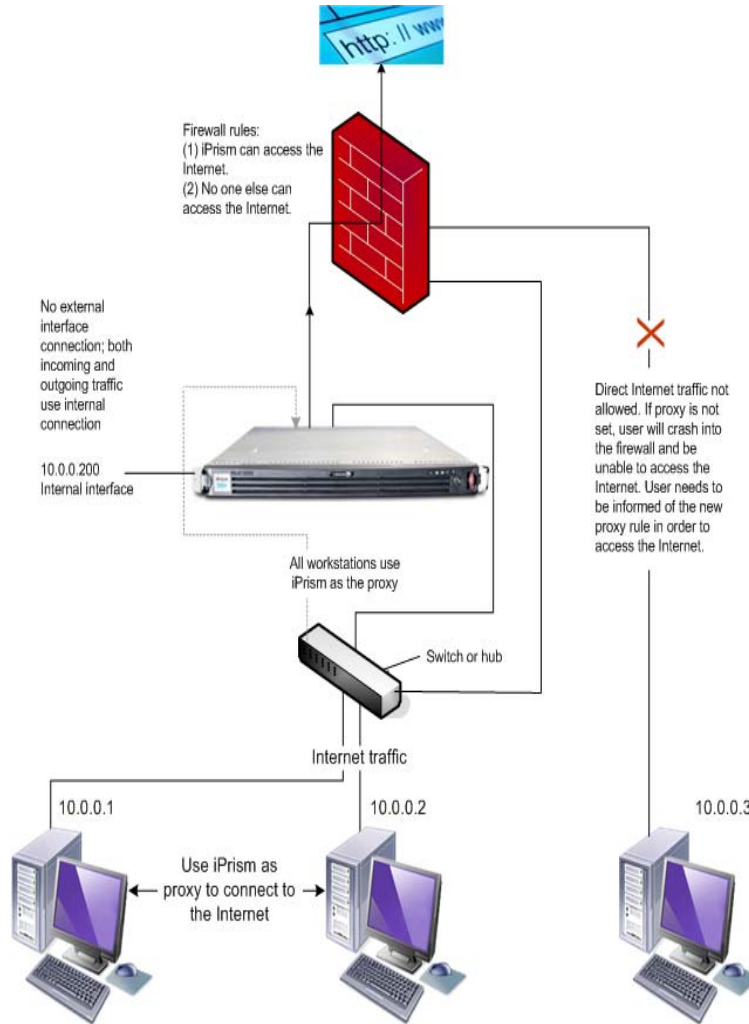


FIGURE 4. Deploying iPrism in Proxy Mode

Refer 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.

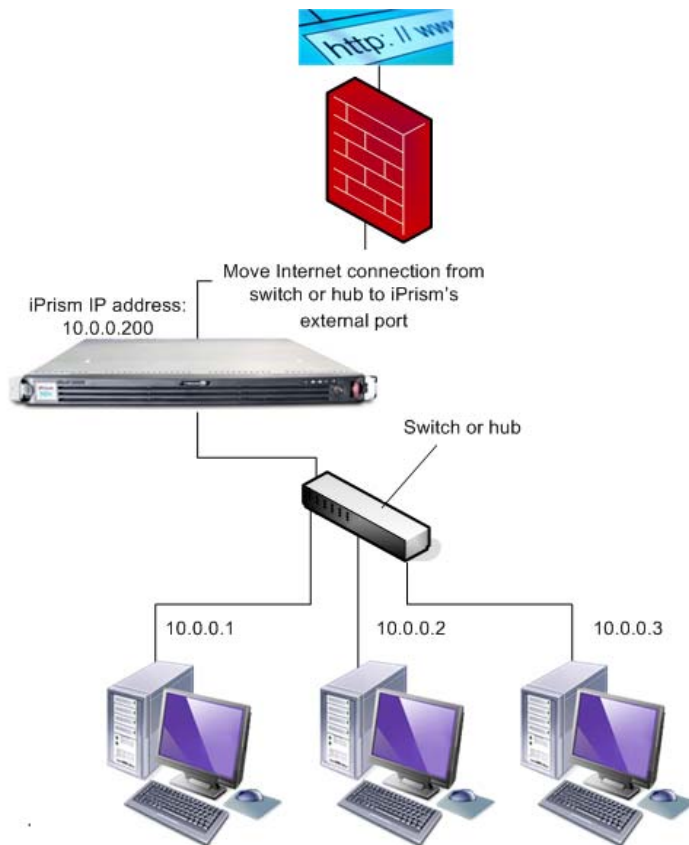




FIGURE 5. Deploying iPrism in Bridge (Transparent) Mode

 **Note:** 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*.

 **Note:** 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.

It also provides you with 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.

The management interface is only needed if you require a high level of security. For more information on its configuration and use, refer to the Knowledgebase article “How do I enable the Management Interface?” at www.stbernard.com/products/support/iprism/help/iprism.htm

Logging into and out of iPrism

Logging into iPrism is done via the login page (Figure 6). It is recommended that you bookmark this page.

When in an iPrism session, you can log out via the **Logout** menu in the top right corner of the page (Figure 7). Select **Logout** from the dropdown menu.

If the user is on a shared computer, s/he should logout when s/he is finished. If s/he does not, the next person who uses the machine will be able to access the Internet using his/her profile.



FIGURE 6. Logging in

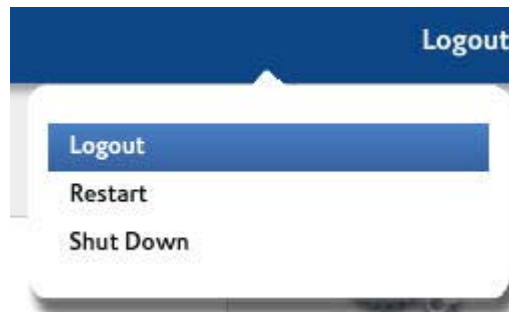


FIGURE 7. Logging out

Restarting and Shutting Down iPrism

- To restart iPrism, select **Restart** from the **Logout** menu in the top right corner of the page (Figure 7).
- To shut down iPrism, select **Shut Down** from the **Logout** menu in the top right corner of the page (Figure 7).

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.

Using the iPrism Home Page

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 chapter in this book, as referenced below:

- Chapter 3, **Profiles & Filters**, beginning on page 19
- Chapter 4, **Users and Networks**, beginning on page 47
- Chapter 5, **Reporting**, beginning on page 81
- Chapter 6, **Maintenance**, beginning on page 87
- Chapter 7, **System Settings**, beginning on page 107
- Chapter 8, **System Status**, beginning on page 179
- Chapter 9, **Central Management**, beginning on page 193
- Chapter 10, **Override Management**, beginning on page 203

For detailed information about and instructions how to use each tool, refer to the associated chapter in this book.

This chapter 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 appears with the following Filtering features, which are covered in this chapter on the pages listed:

Custom Filters: page 20

Profiles: page 24

Access Control Lists (ACLs): page 32

Current Overrides: page 36

Pending Requests: page 38

Recent Blocks: page 40

Antivirus: page 40

Remote Filtering: page 41

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 (see Figure 9 on page 22). 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 will treat the URL as a member of that category and either allow or deny access to the site based on the active filtering profile.

In the Custom Filters section, you can import, add, edit, and delete custom filters on your iPrism. 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	Action
Enabled	*://www.jibjab.com	*.mpg, *.mpeg, *.mov, *.avi, *.ram	Yes	Local Deny
Disabled	*://www.tgifridays.com	*	Yes	Local Deny
Enabled	*://www.prosecurityservice.com	*	Yes	corporate marketing

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

FIGURE 8. Custom Filters

2. To import custom filters from a file, click **Import**. Click **Browse** to locate the file, then click **OK**.
3. To add a custom filter, click **Add**.

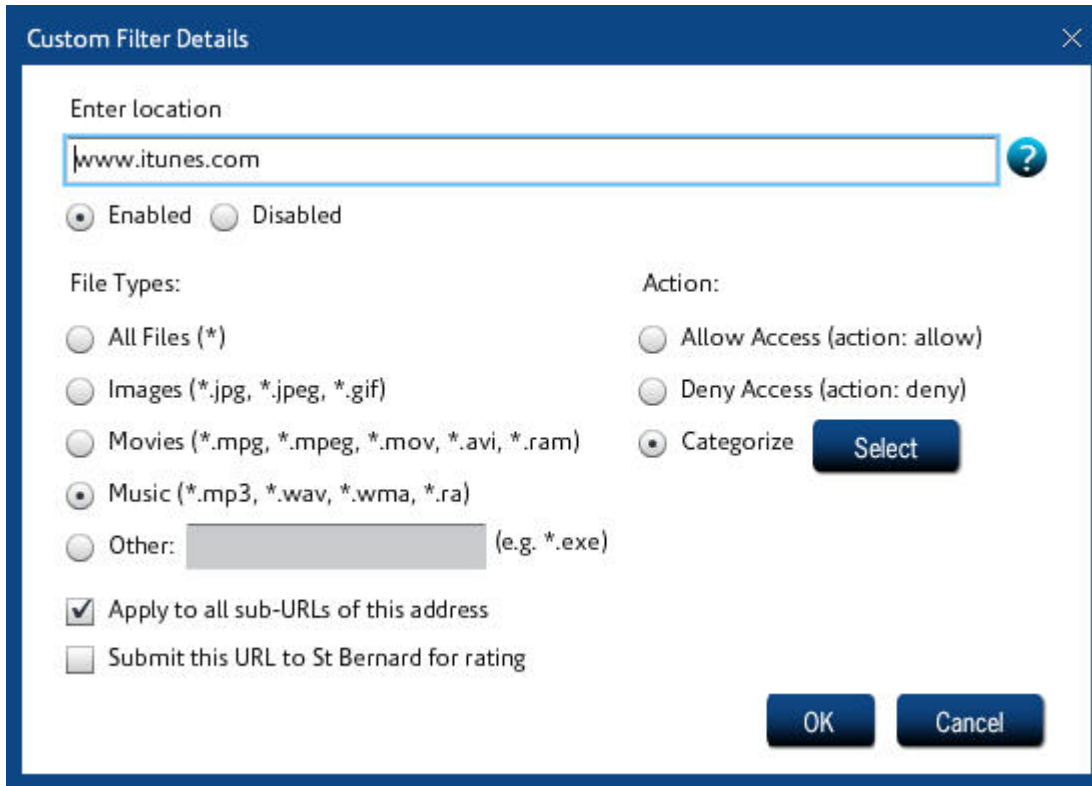


FIGURE 9. Filter Details

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

To edit a custom filter

1. From the iPrism home page, select **Profiles & Filters**, then **Custom Filters**.
2. Select the filter you want to edit and click **Edit**.
3. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To delete a custom filter

1. From the iPrism home page, select **Profiles & Filters**, then **Custom Filters**.
2. Select the filter you want to delete and click **Delete**.
3. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To search for a custom filter

1. From the iPrism home page, select **Profiles & Filters**, then **Custom Filters**.
2. Type all or part of the filter name and click **Search**.

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) and *Application profiles* (for filtering IM/P2P traffic).

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’ 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)” on page 32.

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:

1. **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 *Chapter 7: System Settings*, “Directory Services” on page 113 for more information on authentication.

2. **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.

3. **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” on page 73.

iPrism’s Default Profiles

iPrism ships with five (5) preconfigured (default) profiles, two (2) for web filtering and three (3) for IM/P2P. 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.

1. To work with Web Profiles, from the iPrism home page, select **Profiles & Filters**, then **Web Profiles**. The Web Profiles window appears (Figure 10).

Profile Name	ACLs
PassAll	ACL 1
BlockOffensive	ACL 1

Select All Deselect All  Add Copy Edit Delete

FIGURE 10. Web Profiles

Adding a Profile

To add a profile, complete the following steps:

1. Click **Add** in the main Web Profiles window (Figure 10).
2. Create your profile, then click **Add** (Figure 11) to create or modify an Access Control List (ACL), as shown in Figure 11.
3. Click **OK** to add the ACL.
4. Click **OK** again to add the Web Profile.
5. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

For more information on ACLs, see “Access Control Lists (ACLs)” on page 32.

Access Control List

Access Control List Name
ACL 1

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 checked="" type="checkbox"/>			
▶ questionable activities	? <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
▶ security exploits	? <input checked="" type="checkbox"/>	<input checked="" 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"/>			
▶ locally defined	? <input checked="" type="checkbox"/>	<input type="checkbox"/>			
▶ dynamically detected	? <input checked="" type="checkbox"/>	<input type="checkbox"/>			

Monitor All Block All Clear All OK Cancel

FIGURE 11. Web Access Control List (ACL)

Copying a Profile

To copy a profile, complete the following steps:

1. Select a profile in the main Web Profiles window (Figure 10), and click **Copy**.
2. Make any changes, then select Add or **Edit** (Figure 3) to create or modify an Access Control List (ACL).
3. Click **OK** to add or update the ACL.
4. Click **OK** again to add the Web Profile.

5. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Deleting a Profile

If you want to delete a profile, you must replace it with an existing profile.

1. Select a profile in the main Web Profiles window and click **Delete**.

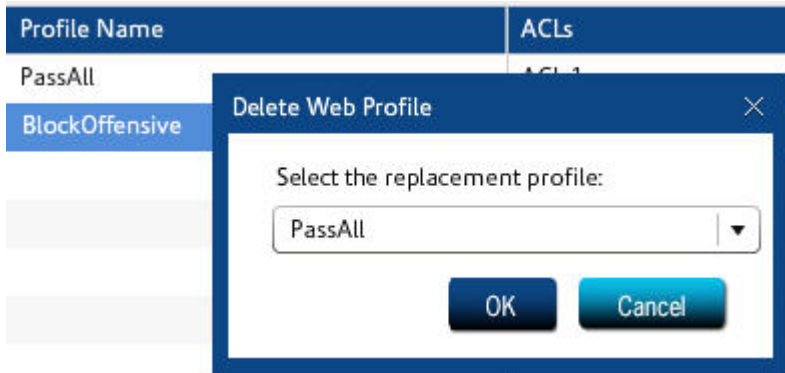


FIGURE 12. Deleting a Profile

2. Select a replacement profile from the dropdown list as shown in Figure 12, and click **OK**.



Important: Assigning a different profile may dramatically change what the user(s) see(s); for specific information about the default profiles (e.g., PassAll, BlockOffensive) and what they allow and do not allow, see “iPrism’s Default Profiles” on page 25.

3. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Application Profiles

Application Profiles filter IM and P2P usage.

1. To work with Application Profiles, from the iPrism home page, select Profiles & Filters, then **Application Profiles**. The Application Profiles window appears (Figure 13).

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

FIGURE 13. Application Profiles

Adding a Profile

To add a profile, complete the following steps:

1. Click **Add** in the main Application Profiles window (Figure 13).
2. Create your profile, then click **Add** (Figure 13) to create or modify an Access Control List (ACL), as shown in Figure 14.

In the example in Figure 14, we are blocking IM/P2P traffic from 6:00 AM – 7:00 PM, with the exception of 12 PM – 1 PM, when IM/P2P traffic is allowed to pass through.

3. Click **OK** to add the ACL.

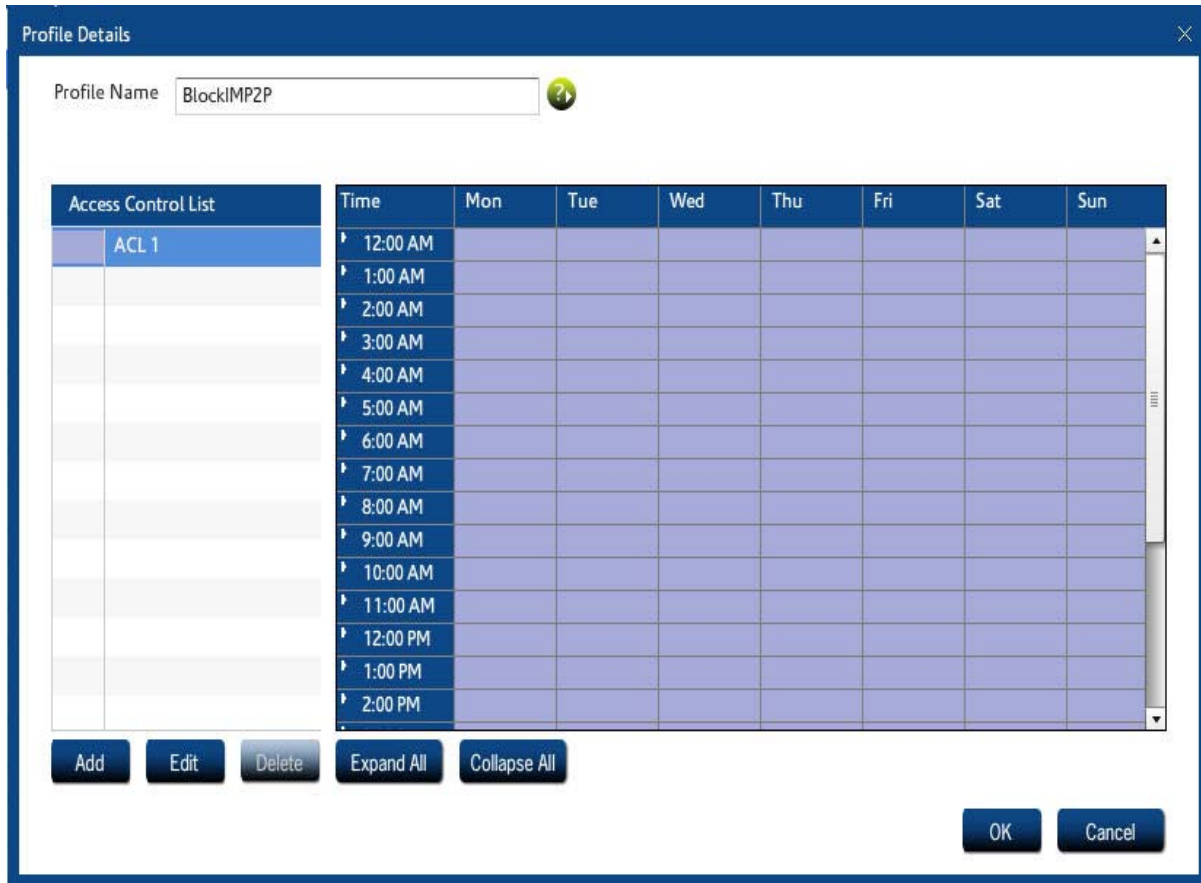


FIGURE 14. Application ACL

4. Click **OK** again to add the Application Profile.
5. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Copying a Profile

To copy a profile, complete the following steps:

1. Select a profile in the main Application Profiles window (Figure 13), and click **Copy**.
2. Make any changes, then select Add or **Edit** (Figure 3) to create or modify an Access Control List (ACL).
3. Click **OK** to add or update the ACL.

4. Click **OK** again to add the Application Profile.
5. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Deleting a Profile

If you want to delete a profile, you must replace it with an existing profile.

1. Select a profile in the main Web Profiles window and click **Delete**.
2. Select a replacement profile from the dropdown list (an example of this is shown for a Web Profile in Figure 12; the procedure for an Application Profile is the same), and click **OK**.



Important: Assigning a different profile may dramatically change what the user(s) see(s); for specific information about the default profiles (e.g., PassIMP2P, BlockP2P, BlockIMP2P) and what they allow and do not allow, see “iPrism’s Default Profiles” on page 25.

3. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Authentication and Assigning Profiles to Users

Users can be authenticated on iPrism in a number of ways. See Chapter 7: System Settings, “Directory Services” on page 113 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 Chapter 4: Users and Networks, “Networks” on page 57.

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 squares on the time grid. You may create new ACLs and schedule them by applying them to the time grid.

Creating a New ACL

1. From the iPrism home page, select **Profiles & Filters**, then **Web Profiles** (if you are adding an ACL to a Web Profile) or **Application Profiles** (if you are adding an ACL to an Application Profile). For the remainder of this example, we will use a Web Profile.
2. If you want to add a new ACL to an existing profile, select that profile in the main Web Profiles window (Figure 10), click **Edit**, then click **Add**.
- or -
If you want to edit an existing ACL within an existing profile, select that profile in the main Web Profiles window (Figure 10), click **Edit**, select the ACL (for example, ACL2), then click **Edit**.
3. Type a name for the ACL and select a color to use (Figure 15).
4. Select General Options:
 - **Deny all access to the web:** If this is selected, no web traffic is allowed for this ACL. This is a quick way of setting all categories (even **local allowed**) to **Blocked**. (This is the equivalent of setting everything to **Blocked/Monitored**.) Note that 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 the safe search for Google, Yahoo, Alltheweb, Hotbot, Lycos, Dogpile, and Excite. “Safe Search” will be turned on even if the user attempts to do a search with this feature turned off.
5. Select **Access Denied Page Options**. This determines what will be shown when a user encounters a blocked page:
 - **Override link:** When selected, the Access Denied page will include an Override button, so users with override privileges can gain access to the page.
 - **Request access link:** When selected, the Access Denied page will include a Request Access button, which allows users to petition the administrator for access whenever they are blocked from a site.

6. Check the categories you want to monitor and/or block. If you want to monitor all categories, click Monitor All. If you want to block all categories, click Block All.
 - **Monitor All:** Web pages are supplied to the user; each access is recorded and can be viewed using the reporting system or the Real-Time Monitor.
 - **Block All:** If this selected, all web traffic is blocked for this ACL.
7. Click **OK** to finish modifying the ACL.
8. Select the times you want this ACL to be active by clicking a square next to a time (e.g., 7:00 AM) and dragging your mouse across the calendar while holding down the left mouse button. In the example in Figure , ACL1 is active at all times except for the period of 7:00 AM – 7:00 PM Monday – Friday, when ACL2 is active.

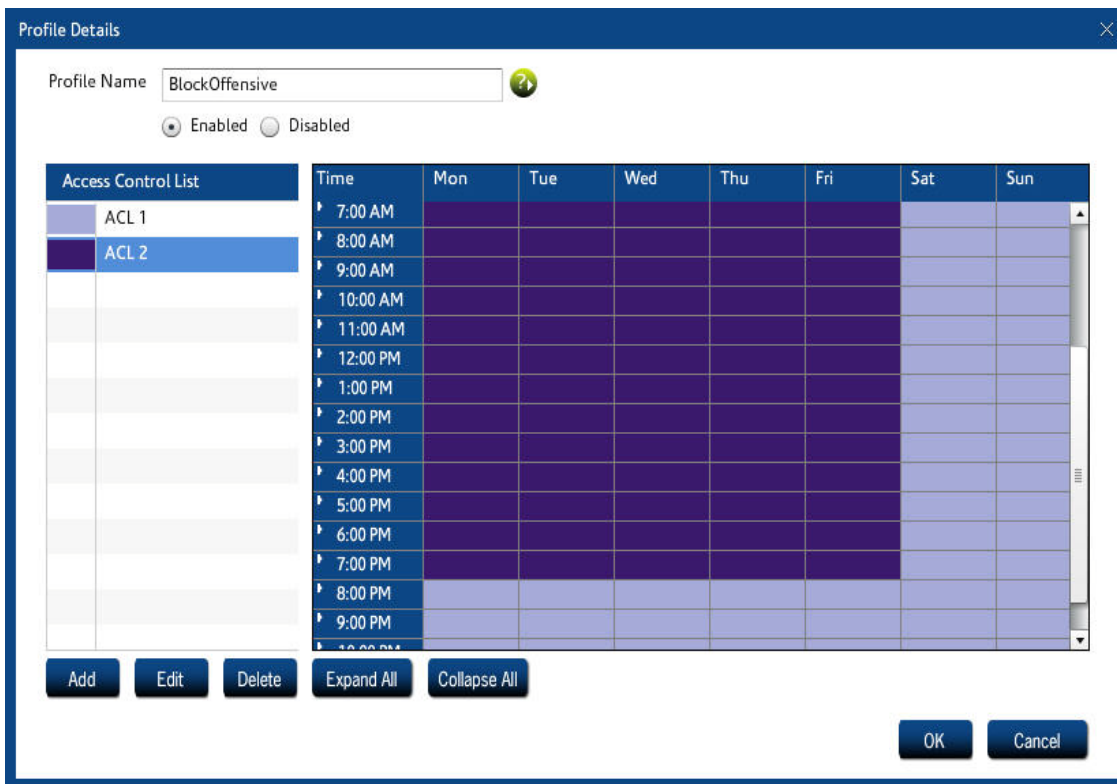


FIGURE 15. ACL

Along the left side, you can see the different-colored blocks; each of these represents an ACL that has been “attached” to this profile. After creating an ACL, you need to drag it to the profile grid to schedule the times for which you want it to be active.

9. Click **OK** to add or save the changes to the associated Web Profile.
10. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Editing ACL Settings

1. From the iPrism home page, select **Profiles & Filters**, then **Web Profiles** (or **Application Profiles** if you are editing an ACL in an Application Profile). In this example, we will use a Web Profile.
2. Select the profile associated with this ACL in the main Web Profiles window (Figure 10), then click **Edit**.
3. Select the ACL and click **Edit**.
4. Make your changes, then click **OK** to save the changes to this ACL.
5. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Deleting an ACL

1. From the iPrism home page, select **Profiles & Filters**, then **Web Profiles**.
2. Select the profile associated with this ACL in the main Web Profiles window (Figure 10), then click **Edit**.
3. Select the ACL and click **Delete**.
4. Click **Yes** to delete the ACL, or **No** to cancel.
5. Click **OK** to save these changes.

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” and “nudity”. Once a category is blocked and/or monitored in **Lock ACL**, all the existing and newly created profiles (including those created by the SuperUser and Global Policy Administrator) are updated and the category is blocked and/or monitored. However, if you unblock a category from **Lock ACL**, it does not automatically update all profiles, so the category will remain blocked in those profiles. You must manually unblock them in each profile.

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” on page 38). **Lock ACL** will have to be turned off for that category before the Pending Request can be granted.



Note: The **Lock ACL** tab is only available to the SuperUser or the Global Policy Administrator.

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.

Web Lock ACL **Edit** Application Lock ACL **Edit**

Advanced

Categories locked in the Web and Application Lock ACLs cannot be overridden by anyone. To allow any administrator the ability to override any category, select option(s) from the following list:

- Lock ACLs in each profile
 - but allow users to request access
- Lock ACLs are not overridable
 - except by administrators

FIGURE 16. Lock ACL

1. From the iPrism home page, select **Profiles & Filters**, then **Lock ACL** (Figure). The Lock ACL window appears (Figure 16).
2. Click **Edit** next to the type of ACL you want to lock (**Web Lock ACL** or **Application Lock ACL**).
3. Make any changes, and click **Save** to save your changes, or **Revert** to cancel and revert to the previous state.
4. If you want to give any Administrator the ability to override any categories, check *both* **Lock ACLs cannot be overridden** and **except by administrators** in the Lock ACL window.
5. Click **Save**, then click **Activate Changes** to activate these 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.

From the iPrism home page, select **Profiles & Filters**, then **Current Overrides** (Figure 17). 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 17. Current Overrides

The following columns are available in the **Current Overrides** page:

- **Expires:** The date and time at which the override will expire by itself.
- **Administrator:** The user who created the override. This is only relevant when using user authentication. The override will only be valid for the indicated user. When user authentication is not used, or when the override is valid for all users, this column will indicate **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** in Figure 17). 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 will show its IP address. If several workstations are affected, this column will show 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 will be displayed.

Revoking Overrides

1. To revoke one or more overrides, select the override(s) from the Current Overrides window and click **Revoke**.
2. Click **Revoke** to revoke the override(s), or **Cancel** to cancel.

Pending Requests

When a user is surfing the Internet and receives an Access Denied message for a blocked page (which s/he will only see if the administrator has checked Request Access link when setting up the ACL, as explained in “Creating a New ACL” on page 32), s/he can use click **Request Access** to send a message to the iPrism administrator to explain why they need access to the site (for more information on this, see “Overriding a Blocked Web Site” on page 205). 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, from the iPrism home page, select **Profiles & Filters**, then **Pending Requests** (Figure 18).



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)	

FIGURE 18. Pending Requests

Granting Requests

1. To grant pending request(s), select the request(s) from the Pending Requests window 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” on page 34), 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), or **Cancel** to cancel.
4. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Denying Requests

1. To deny pending request(s), select the request(s) from the Pending Requests window and click **Deny**.
2. Click **Deny** to deny the request, or **Cancel** to cancel.
3. Click **Save**, then click **Activate Changes** to activate these 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 item and click **Allow Access**.

Antivirus

iPrism provides virus detection and prevention via Antivirus (AV) scanning and reporting for HTTP traffic. AV is enabled by default for new installations (newly shipped appliances).

When users try to access a web page which attempts to download a malicious file or script via HTTP, they will be notified that the page is blocked.

This prevents the introduction of viruses, and identifies virus sources using the following AV categories: Virus, Worm, or Other Malware.

1. To enable Antivirus protection, from the iPrism home page, select **Profiles & Filters**, then **Antivirus**.
2. Make sure Antivirus slider is set to **ON**.
3. If the slider was set to **OFF** and you changed it to **ON**, click **Save**, then click **Activate Changes** to save these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

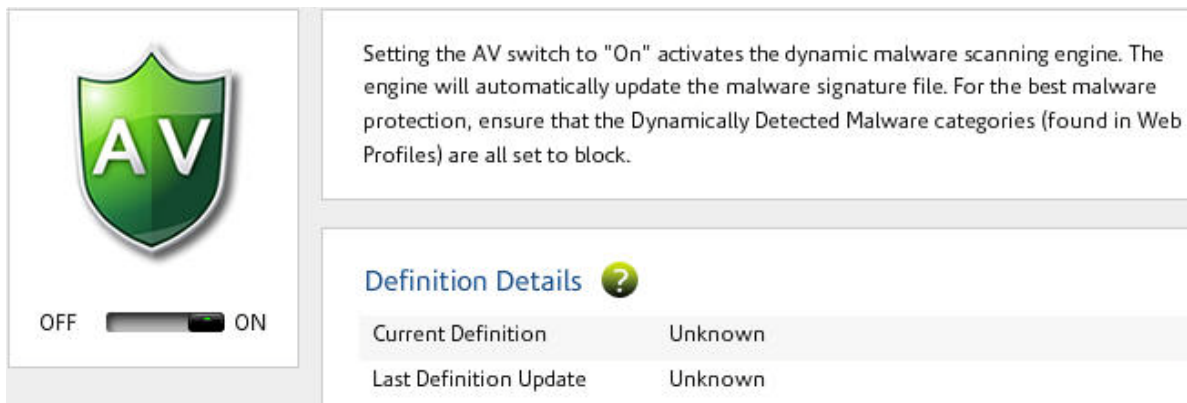


FIGURE 19. Antivirus

Antivirus details, such as Current Definition and the last time the AV definition was updated, are displayed in this window.

Remote Filtering

Using the Windows and/or Macintosh® Remote Filtering Client, and St. Bernard (SBS) Data Center cloud service, 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/or 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 (refer to “Remote Users” on page 73 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 SBS Data Center functions as an intermediary for the iPrism and the remote client.
- **Important:** Remote Filtering will not function properly if iPrism's configuration port is not set to the default of port 80. To learn how to check or change the configuration port, see “Proxy and Configuration Ports” on page 162.
- For iLearn video tutorials on Remote Filtering, go to <http://ilearn.stbernard.com/>

Using Remote Filtering

To utilize Remote Filtering, complete the following steps:

1. Upload a remote filtering license key (see page 144 for instructions on how to do this).
2. Enable Remote Filtering and download the client software as described in the next section.
3. Set up users in **Users & Networks > Remote Users** (see “Remote Users” on page 73) :
 - 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 as described on page 144, complete the following steps to enable Remote Filtering.

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

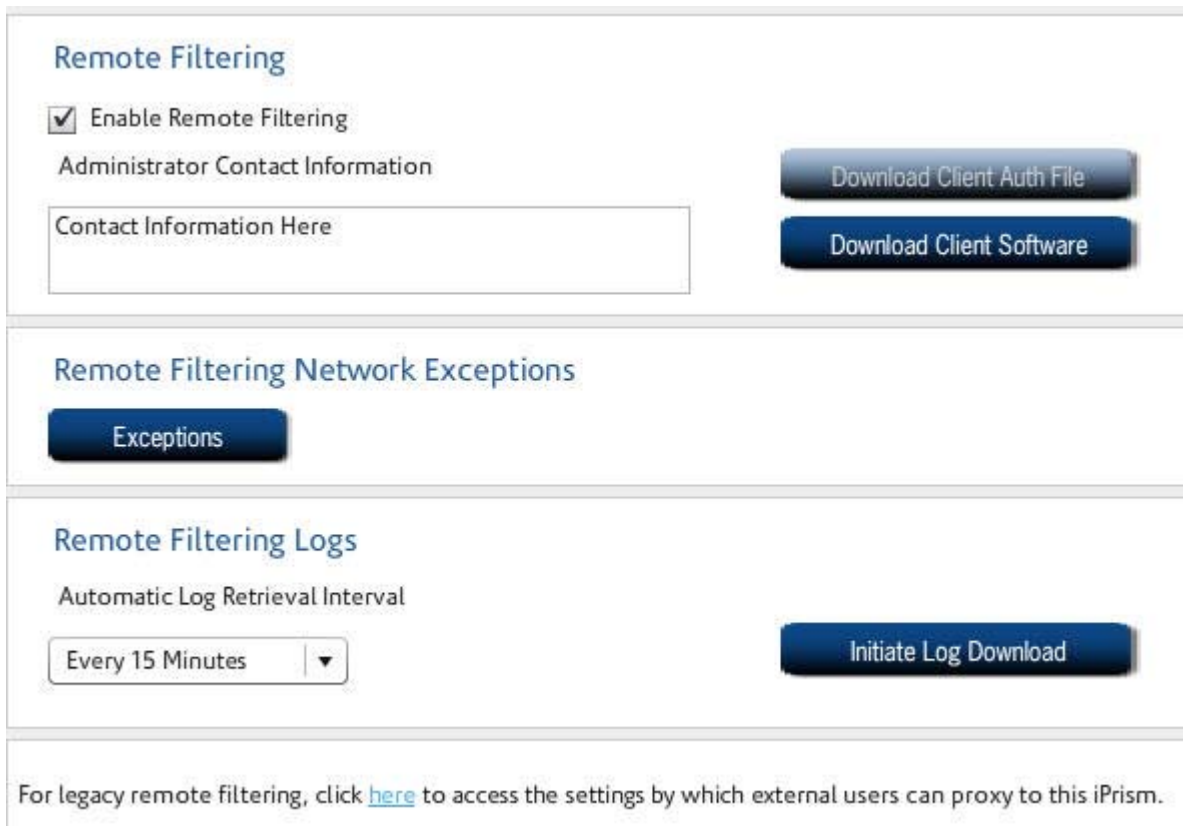


FIGURE 20. Remote Filtering

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 address(es) of the iPrism administrator(s), 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 software³.
6. Save this key file to a location of your choice.



Important: Do not change the name of this file, as the Remote Filtering client software installer looks for the file with this specific name.

7. To download the Remote Filtering client software, click **Download Client Software**. This will take you to a website where you can complete the download⁴.
8. Specific network ranges or ports for which filtering on the remote client will not be enforced are called *Remote Filtering Network Exceptions*. Under Remote Filtering Network Exceptions, click **Exceptions**.
9. Specify the target network ranges (IP address and Netmask) you do not want to monitor for remote users, in **Unmonitored Network Ranges**.

3. For more information about configuring and using `iprism_Client_Auth.key`, refer to the *iPrism Remote Filtering Client Guide*.

4. For detailed instructions on how to set up and configure the Remote Filtering Client, refer to the *iPrism Remote Filtering Client Guide*.

- Specify the range of target ports you do not want to monitor for remote users, in **Unmonitored Ports**.

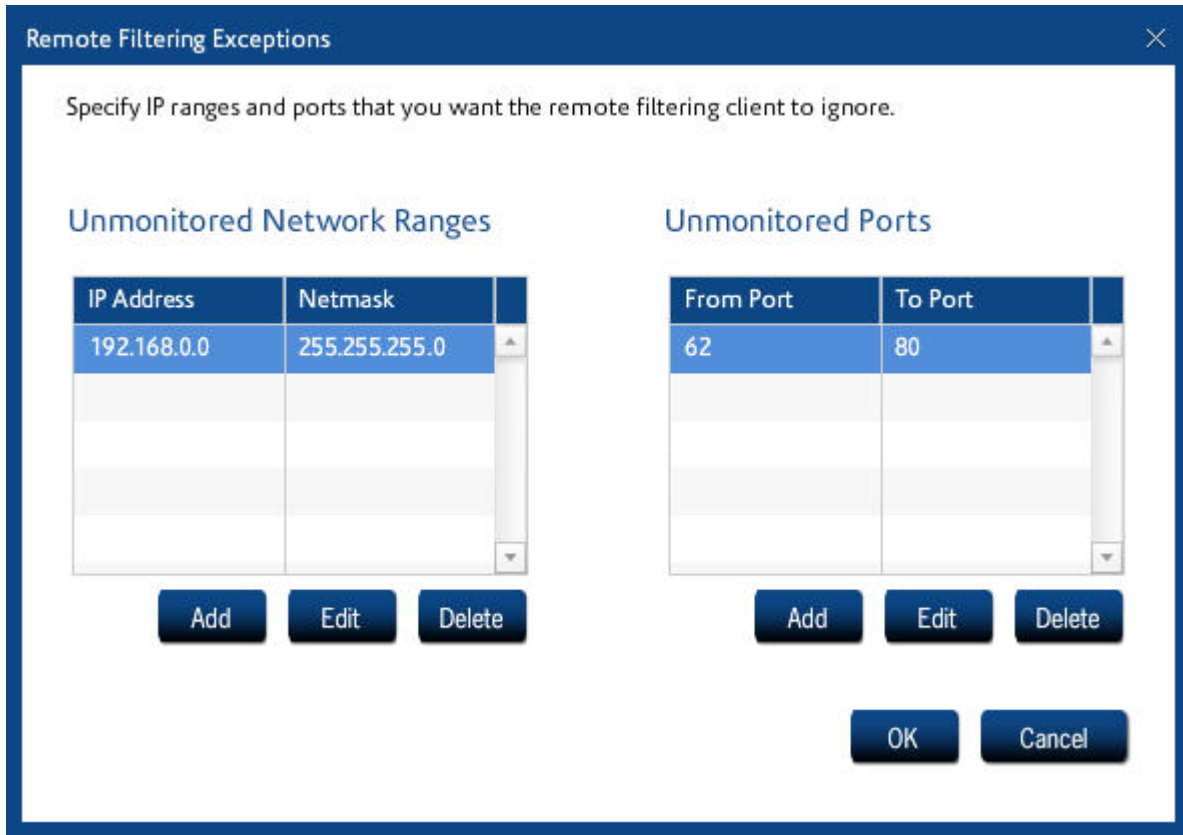


FIGURE 21. Setting up Remote Filtering Exceptions

- Remote clients that are controlled by a policy in which monitoring is configured will periodically send event logs back to iPrism by way of St. Bernard’s Data Center. The frequency at which iPrism will request events from the Data Center may 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** (see Figure 20 on page 42).
- When you are finished on this page, click **Save**.
- You will be prompted to select a default web profile for remote users. Select a default profile from the list (**PassAll** or **BlockOffensive**) and click **OK**.

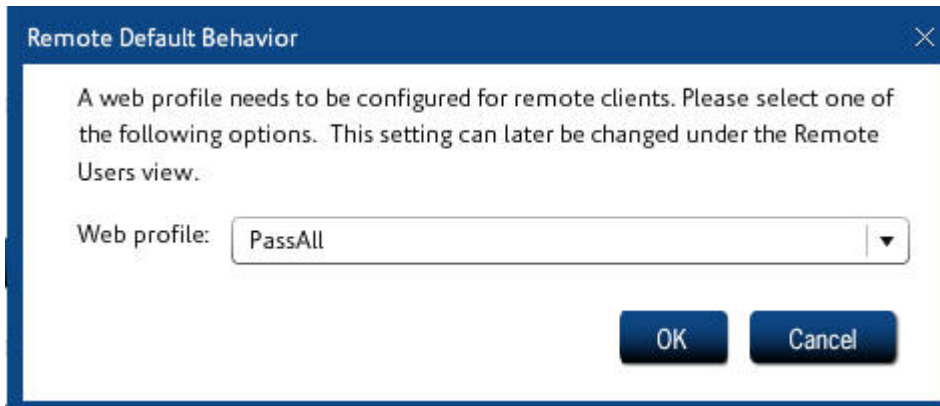


FIGURE 22. Select a default web profile for remote users

14. You can now set up remote users (see “Remote Users” on page 73).



Note: The status of log downloads and policy uploads can be viewed in the System Status section’s “Status” on page 190.

This chapter contains the following:

Local Users: page 48

Groups: page 51

Privileges: page 54

Networks: page 57

Admin Roles: page 65

Exceptions: page 70

Remote Users: page 73

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 a User

1. From the iPrism home page, select **Users & Networks**, then **Local Users**.
2. In the **Local Users** window, click **Add**.
3. Type a **Username** and **Password** in the appropriate fields, and type the password again in the **Confirm Password** field.
4. Assign a Web Profile by selecting one from the dropdown list;
- or -
Check **Use network profiles** to assign the web profile based on the IP address of the user's computer. To assign a user a profile from the network list, click the **Use Network** checkbox. This user will then be governed by a network profile.
5. 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" on page 203) 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 (see “Admin Roles” on page 65) are also available and may be selected here.

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

- User Name:** A text input field.
- Password:** A text input field.
- Confirm password:** A text input field.
- Use network profiles:** A checkbox with a blue question mark icon.
- Web Profile:** A dropdown menu currently set to 'PassAll'.
- Admin Privileges:** A dropdown menu currently set to 'Extended Override'.
- Notes:** A large text area for additional information.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

6. Click **OK** to save your changes, or **Cancel** to cancel.
7. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Import a User

1. From the iPrism home page, select **Users & Networks**, then **Local Users**.
2. Click **Import**.

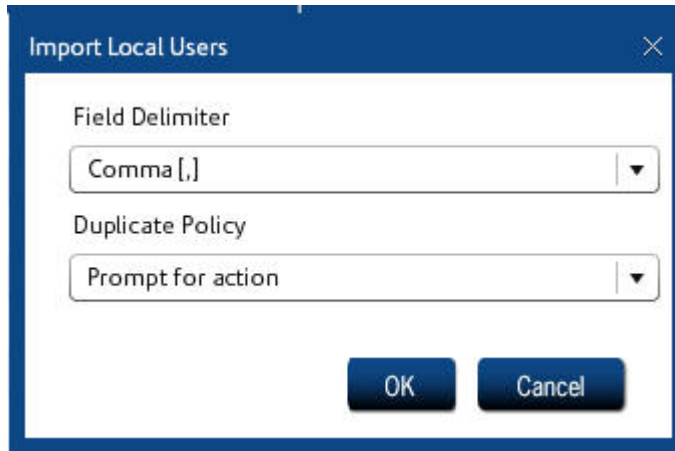


FIGURE 23. Import Local Users

3. In the **Import Local Users** window, click **Browse** to locate the file containing the users you want to import.
4. 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.
5. In the **Duplicate Policy** dropdown list, select an option specifying what you want the system to do when a duplicate policy is encountered:
 - Prompt for action:** Each time a duplicate policy is encountered, you will be prompted to tell the system how to handle it.
 - Retain existing:** Each time a duplicate policy is encountered, the existing policy on the iPrism will be retained.
 - Overwrite existing:** Each time a duplicate policy is encountered, the policy being imported will overwrite the policy on the iPrism.
6. Click **OK**.
7. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not **Activate Changes** now, you will be prompted to do so before logging out of iPrism).

Groups

Mapping Groups to Profiles

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. Before doing any mapping, you should review the following guidelines.

Rules and Guidelines for Group Mapping

Users on iPrism can be controlled based on their group memberships. This is accomplished by mapping a group to an iPrism resource; **groups** (fully qualified with the DOMAIN\groupname notation) are mapped to iPrism **profiles**.

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, the following principles should be kept 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.

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

Navigation: ^ v Group Check Policy Test Fallback Add Edit Delete

FIGURE 24. Groups

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 25. Nested Groups Example

To Add, Edit, or Delete Groups

To add, edit, and delete groups, select **Users & Networks**, then **Groups** (Figure 24).

To Add a Group

1. In the **Groups** window, click **Add**.
2. In the **Profile Maps** window (Figure 26), 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, or **Cancel** to cancel.
5. When you are finished adding all groups, click **Save** at the bottom of the Groups window.

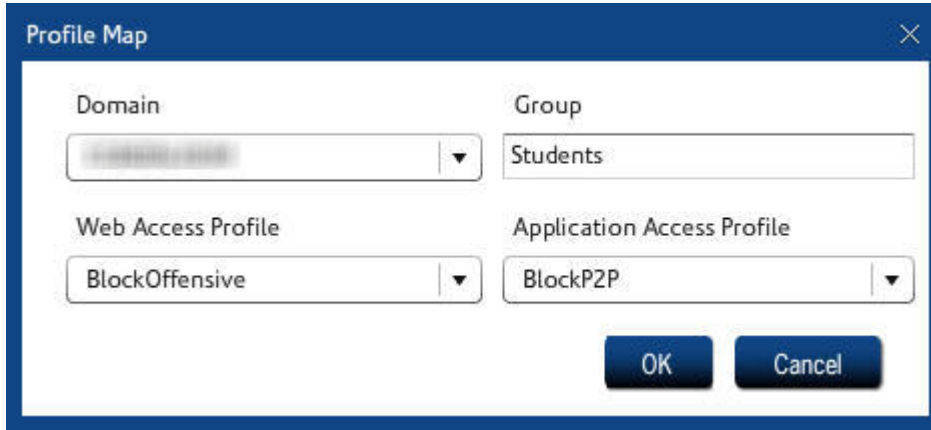


FIGURE 26. Profile Map

To Edit a Group

1. In the **Groups** window (Figure 24), click **Edit**.
2. Make any changes in the **Profile Maps** window (Figure 26).
3. Click **OK** to save your changes, or **Cancel** to cancel.
4. When you are finished editing all groups, click **Save** at the bottom of the Groups window.

To Delete a Group


1. In the **Groups** window, select a group to delete and click **Delete**.
2. Click **Yes** to confirm the delete, or **No** to cancel.
3. When you are finished modifying all groups, click **Save** at the bottom of the Groups window.

Privileges

Mapping Privileges to Groups

Once iPrism has successfully joined the domain in **System Settings > Directory Services** (see page 113) and mapped groups to profiles (see “Mapping Groups to Profiles” on page 51), you can map the privileges to groups.

To add, edit, and delete privilege mappings, 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





       

FIGURE 27. Privileges

1. To add a privilege mapping, click **Add**; to edit an existing privilege mapping, click **Edit**.
2. Select a domain from the Domain dropdown list.
3. Type the group to which you are mapping this privilege; for information about setting up groups, see “Groups” on page 51.

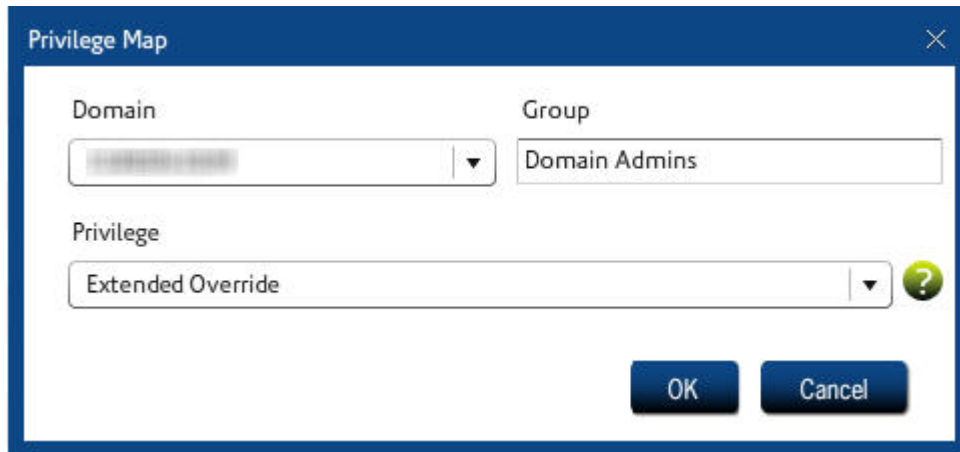


FIGURE 28. Privilege mapping

4. Select a Privilege from the dropdown list:
 - **Extended Override:** Allows the user to log in to override management (see “Override Management” on page 203) 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 (see “Admin Roles” on page 65) are also available and may be selected here.

5. Click **Save**.
6. Your changes will not be applied to the iPrism until you click **Activate Changes**. 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 page 60.

For detailed explanations of authentication modes and Auto-login in both proxy and bridge (transparent) modes, see “Recommended Authentication Settings” on page 126.

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” on page 24 and “Application Profiles” on page 29.



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, select **Users & Networks**, then **Networks** (Figure 29).

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 29. Networks section

To Add a Network Profile

1. To add a network profile, 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.



The screenshot shows a dialog box titled "Manage Network Profile" with a close button (X) in the top right corner. The dialog has two tabs: "Details" (selected) and "Authentication". Under the "Details" tab, there are four input fields: "IP Start" with the value "0.0.0.0", "IP End" with the value "255.255.255.255", "Web Profile" with a dropdown menu showing "PassAll", and "Application Profile" with a dropdown menu showing "BlockP2P". Below these fields is a checkbox labeled "Workstations proxy to iPrism's external interface" with a question mark icon to its right. At the bottom of the dialog are "OK" and "Cancel" buttons.

FIGURE 30. Network Profile Details

3. Click the Authentication tab (Figure 31).

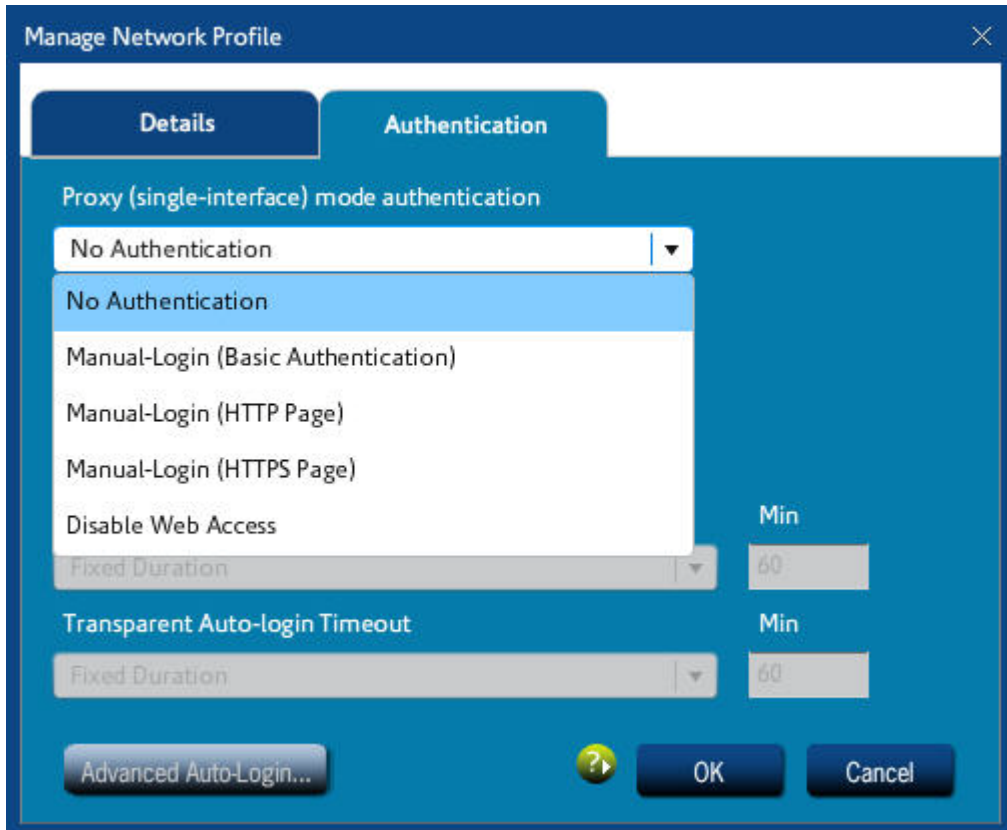


FIGURE 31. Authentication Tab – Proxy Mode

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 in step 8 below, one of the following options must be selected here to specify how to handle the manual login.

See the **Authentication Combinations** table below for the various options available for different modes and authentication methods.

Authentication Combinations

Directory Service	Proxy mode options	Bridge (transparent) mode options
NTLM (NT, AD 2000/2003, AD 2008) Authentication Options	No Authentication Auto-Login (Basic Authentication) Manual-Login (Basic Authentication) Manual-Login (HTTP Page) Manual-Login (HTTPS Page) Disable Web Access	No Authentication Auto-Login (HTTP Authentication) Manual-Login (HTTP Page) Auto-Login (HTTPS Authentication) Manual-Login (HTTPS Page) Disable Web Access
Failed Options	Use Network Profile Disable Web Access	Use Network Profile Disable Web Access
LDAP Authentication Options	No Authentication Manual-Login (Basic Authentication) Auto-Login (HTTP Authentication) Manual-Login (HTTP Page) Auto-Login (HTTPS Authentication) Manual-Login (HTTPS Page) Disable Web Access	No Authentication Auto-Login (HTTP Authentication) Manual-Login (HTTP Page) Auto-Login (HTTPS Authentication) Manual-Login (HTTPS Page) Disable Web Access
Failed Options	Use Network Profile Disable Web Access	Use Network Profile Disable Web Access

Authentication Mode Combination Descriptions

Proxy Mode:

- **No Authentication:** No attempt will be made to identify specific users, and reporting is done by IP address only.
- **Auto-Login (Basic Authentication):** This option is only available for NTLM (NT, AD 2000/2003, or AD 2008). Auto-Login uses Windows NTLM v2, which encrypts credentials. This is the same protocol Windows clients use to authenticate on a domain. Therefore, the authentication directory must be Windows Active Directory. If Auto-Login is enabled, user authentication occurs with NTLM v2 but fails over to the selected mode of authentication (Basic, HTTP or HTTPS) if needed. Authentication in this mode is based on Browser/Proxy Server protocols. The username is sent in plain text, but the password is encrypted.

- **Manual-Login (Basic Authentication):** authentication is based on Browser/Proxy Server protocols. The username is sent in plain text, but the password is encrypted.
- **Manual-Login (HTTP Page):** authentication is based on iPrism. Logins are not strongly encrypted. Credentials are cached on iPrism and expired using configurable timeout values. If you select HTTP, be sure to set the timeout value in step 7.
- **Manual-Login (HTTPS Page):** authentication is based on iPrism; useful where internal logins must be strongly encrypted. Credentials are cached on iPrism and expired using configurable timeout values. If you select HTTPS, be sure to set the timeout value in step 7.
- **Disable Web Access:** all traffic is blocked for the selected network.

Bridge (transparent) mode:

- **No Authentication:** No attempt will be made to identify specific users, and reporting is done by IP address only.
 - **Auto-Login (HTTP Authentication):** This option is only available for NTLM (NT, AD 2000/2003, or AD 2008). Auto-Login uses Windows NTLM v2, which encrypts credentials. This is the same protocol Windows clients use to authenticate on a domain. Therefore, the authentication directory must be Windows Active Directory. If Auto-Login is enabled, user authentication occurs with NTLM v2 but fails over to the selected mode of authentication (Basic, HTTP or HTTPS) if needed.
 - **Manual-Login (HTTP Page):** authentication is based on iPrism. Logins are not strongly encrypted. Credentials are cached on iPrism and expired using configurable timeout values. If you select HTTP, be sure to set the timeout value in step 7.
 - **Auto-Login (HTTPS Authentication):** This option is only available for NTLM (NT, AD 2000/2003, or AD 2008). This option encrypts credentials and is useful where internal logins must be strongly encrypted. Credentials are cached on iPrism and expired using configurable timeout values. If you select HTTPS, be sure to set the timeout value in step 7.
 - **Manual-Login (HTTPS Page):** authentication is based on iPrism; useful where internal logins must be strongly encrypted. Credentials are cached on iPrism and expired using configurable timeout values. If you select HTTPS, be sure to set the timeout value in step 7.
 - **Disable Web Access:** all traffic is blocked for the selected network.
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 “Recommended Authentication Settings” on page 126.
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 as follows:
 - **Always attempt manual login**
 - **Never attempt manual login**

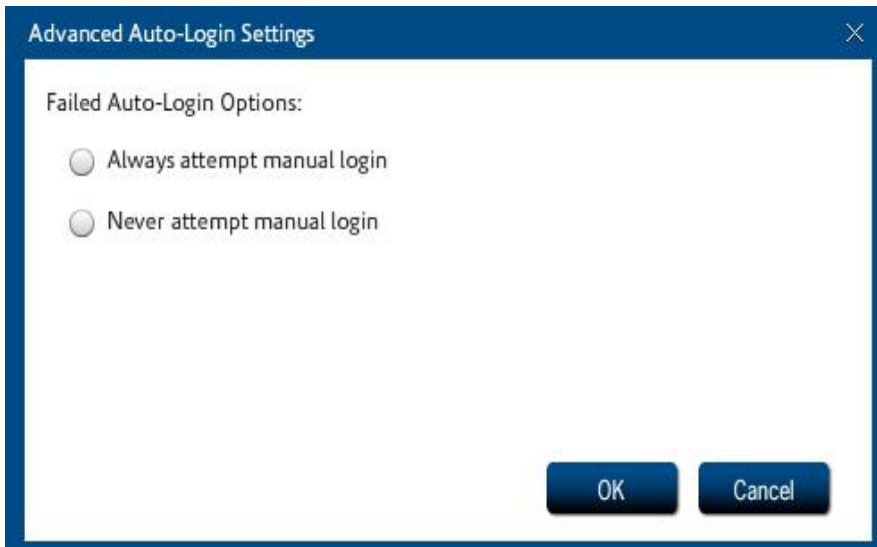


FIGURE 32. Advanced Auto-Login settings



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, or **Cancel** to cancel.
 10. When you are finished adding network profiles, click **Save** at the bottom of the Networks window.
 11. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Edit a Network Profile

1. In the **Networks** window (Figure 29), click **Edit**.
2. Make changes as necessary.
3. Click **OK** to save your changes, or **Cancel** to cancel.
4. When you are finished editing network profiles, click **Save** at the bottom of the Networks window.
5. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Delete a Network Profile

1. In the **Networks** window (Figure 29), select a profile to delete and click **Delete**.
2. Click **Yes** to confirm the delete, or **No** to cancel.
3. When you are finished modifying network profiles, click **Save** at the bottom of the Networks window.
4. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Admin Roles

Administrator Roles (Admin Roles) define the type of access an iPrism administrator has. Detailed descriptions of each role are on page 65.

To access administrator roles, click **Users & Networks** from the home page, then select **Admin Roles** (Figure 33).

Role Name	Filtering Privileges	Report Privileges	Other Privileges
Extended Override	Limited	None	None
Filter management	Limited	None	None
Full Access	Full	Full	Limited
Global Policy Admin	Full	Full	Limited
No access	None	None	None
Reports Only	None	Full	None
Single Override	Limited	None	None
Super Admin	Full	Full	Full

FIGURE 33. Admin Roles

To Add or Edit an Admin Role

1. In the Admin Roles window, click **Add**; or, if you are editing an existing Admin Role, select it in the list and click **Edit**.
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.

The screenshot shows the 'Admin Role Details' dialog box with the 'Access Control List' tab selected. The 'Name' field contains 'Super Admin' and the 'Role Type' dropdown is set to 'Super User'. Below the tabs, the 'Override' dropdown is set to 'Custom'. The 'Maximum Duration' section has 'Use Predefined Durations' selected, with 'Unlimited' chosen from the dropdown. A 'Configure Durations' button is visible. The 'Applies to' section includes checked boxes for 'Everyone', 'Current workstation', 'Current user', 'Profile' (with 'Current User Profile' selected), and 'Network range' (with '0.0.0.0' to '255.255.255.255'). The 'Applies to the following contents' section has checked boxes for 'Current URL', 'Current path', 'Current domain', 'Current category', 'Categories allowed by the grantor's profile', and 'All URLs'. 'OK' and 'Cancel' buttons are at the bottom right.

FIGURE 34. 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. 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 (step10).

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).

Or, click **Unlimited Duration**.

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

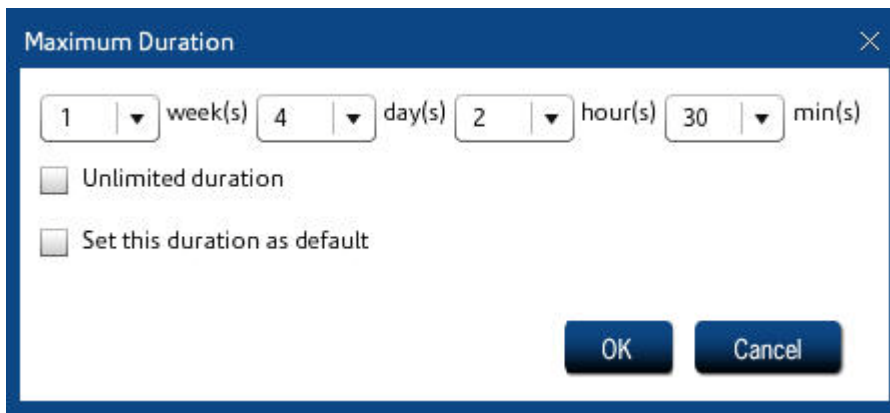


FIGURE 35. Maximum Duration for Overrides

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, or **Cancel** to cancel.

15. When you are finished adding Admin Roles, click **Save** at the bottom of the Admin Roles window.

16. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Delete an Admin Role

1. In the **Admin Roles** window (Figure 33), select a role to delete and click **Delete**.

2. Click **Yes** to confirm the delete, or **No** to cancel.
3. When you are finished modifying admin roles, click **Save** at the bottom of the Admin Roles window.
4. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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 Add an Exception

1. From the iPrism home page, click **Users & Networks**, then select **Exceptions**.
2. Click **Add**.

The image shows a dialog box titled "Exception Details" with a close button (X) in the top right corner. The dialog contains several input fields and controls:

- Name:** A text box containing "Unfiltered Access to Specific IP".
- Exception Type:** A dropdown menu currently showing "No Filter" with a question mark icon to its right.
- Source IP Start:** A text box containing "10.1.2.3".
- Source IP End:** A text box containing "10.1.2.3".
- Destination IP Start:** A text box containing "63.112.169.1".
- Destination IP End:** A text box containing "63.112.169.1", which is highlighted with a blue border.
- Ports:** Two radio buttons: "All Ports" (selected) and "Specific Ports". Below "Specific Ports" is a greyed-out text box.
- Protocols:** Two checkboxes: "TCP" and "UDP", both of which are checked.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

FIGURE 36. Managing Exceptions

3. Type a name for the Exception in the **Name** field.

4. 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.

5. Type the IP address range for the sending machine or set of machines in the **Source IP Start** and **End** fields.
6. Type the IP address range for the receiving machine or set of receiving machines in the **Destination IP Start** and **End** fields.
7. 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. Multiple ports must be separated by commas. A range of ports can be specified as well (e.g., 80 – 120, or 1 – 79, 81 – 65535).
8. 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.)
9. Click **OK**.
10. Click **Save** at the bottom of the Exceptions window, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Edit an Exception

1. In the **Exceptions** window, select the desired Exception and click **Edit**.
2. Make any changes to the exception.
3. Click **OK** to save your changes.

4. Click **Save** at the bottom of the Exceptions window, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Delete an Exception

1. In the **Exceptions** window, select the exception to delete and click **Delete**.
2. Click **Yes** to confirm the delete, or **No** to cancel.
3. When you are finished modifying exceptions, click **Save** at the bottom of the Exceptions window.
4. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Remote Users

iPrism now provides comprehensive Internet security for off-premises users (see “Remote Filtering” on page 41). The mobile laptops and/or remote users must be provisioned in order to utilize this capability. Before setting up remote users, you must have completed the following steps:

1. Upload a remote filtering license key (see page 144). 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** (see page 42).

Once you have completed these steps, you can set up users by following the steps below.



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 will 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 you create in the steps below 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* (in Figure 37, **Web Profile** in **Standard Client Settings**) 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 set up remote clients:

1. Select **Users & Networks**, then **Remote Users**.

Standard Client Settings

Web Profile:

Failover Action When Rating Server is Unreachable:

Client Exceptions

Default Web Profile:

Enabled	Machine Identifier	Web Profile	Failover Action
Enabled	test6	BlockOffensive	Pass (and do not monitor)
Enabled	test5	PassAll	Pass and monitor
Enabled	test4	[PassAll]	Pass (and do not monitor)

FIGURE 37. Remote Users

2. You will see the default Web Profile you selected for remote users before saving your changes in **Profiles & Filters > Remote Filtering**. You can change this profile here if you wish. This profile will be applied to all remote clients' web browsing, unless they are specified in a Client Exception:
Pass All (default)
BlockOffensive

3. From the **Failover Action When Rating Server is Unreachable** list, select what action will occur by default if they attempt to connect to a site and the rating server (the St. Bernard Data Center) is unreachable:
Pass and monitor (default): Pass and monitor activity for eventual delivery to iPrism reports
Block and monitor: Block and monitor web traffic
Pass (and do not monitor): Pass and do not monitor web traffic
Block (and do not monitor): Block and do not monitor (default) web traffic
4. If you want to create exceptions to the default profile specified in Step 2, specify those in Client Exceptions. If exceptions are specified, iPrism remote filtering will first check if a user is defined that matches the client machine, and apply that profile. If there is no (exact) matching Machine ID, then the default profile is applied.
5. Select a profile for the Client Exceptions in the **Default Web Profile** list (**PassAll** or **BlockOffensive**, or any other profile you may have created in iPrism). This profile will be applied to any remote user defined as an exception in the list. To add exceptions, continue to the next section.
6. If you have client exceptions, the next step is getting them into the system; to import them, see “To Import Remote Users” on page 78. To add them individually, continue to the next section.

To Add a Client Exception

1. To add remote users, select **Users & Networks**, then **Remote Users**.
2. Click **Add**. (If you already have a list of remote users and want to simply import it, see “To Import Remote Users” on page 78).
3. In the Remote User Details screen, enter the necessary information about the remote user:
Machine Identifier: 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*).
Domain: (e.g., companyname.com)
4. Check **Enabled** to enable this remote user.
5. Select a Web Profile from the list (**Use Default** to use the default profile, **BlockOffensive**, or **PassAll**). For details about each of these profiles, see “iPrism’s Default Profiles” on page 25.

6. Select which Failover Action will apply when a user encounters a URL that cannot be rated (i.e., the St. Bernard Data Center cannot be reached):

Pass and monitor (default): Pass and monitor activity for eventual delivery to iPrism reports

Block and monitor: Block and monitor web traffic

Pass (and do not monitor): Pass and do not monitor web traffic

Block (and do not monitor): Block and do not monitor (default) web traffic

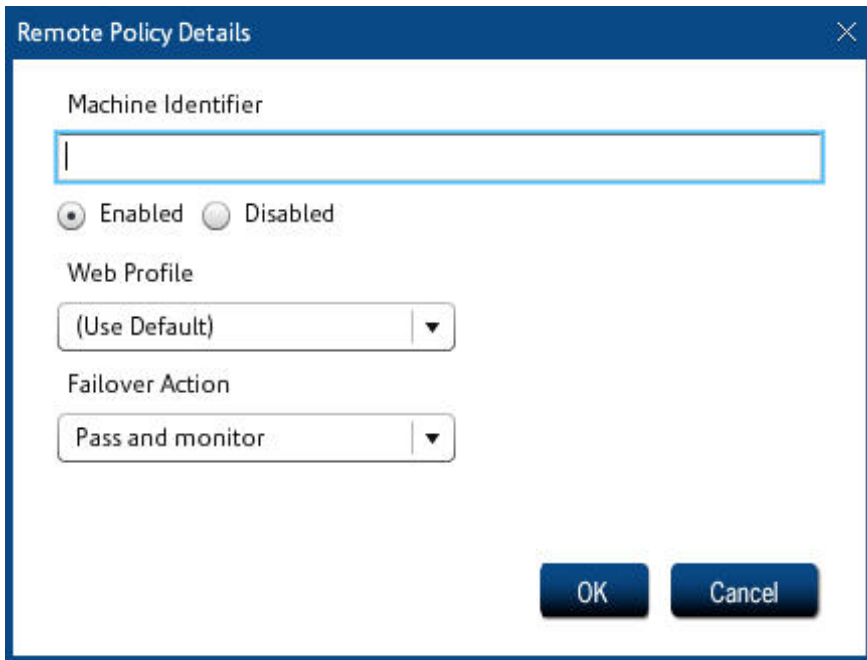


FIGURE 38. Adding or Editing a Remote User

7. When you are finished, click **OK**.
8. Click **Save**, then **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Edit a Client Exception

1. To edit a remote user, select **Users & Networks**, then **Remote Users**.
2. Select the user from the list and click **Edit**.
3. In the Remote User Details screen, make the necessary modifications.

4. If this user is currently enabled for remote filtering and you wish to disable him/her, check **Disabled**.
5. If you want to change this user's web profile, select one from the list. For details about web profiles, see "iPrism's Default Profiles" on page 25.
6. If you want to change a Default Action, select it from the list (**Permit** remote filtering for this user; **Deny** remote filtering for this user).
7. When you are finished, click **OK**.

To Delete a Client Exception

1. To delete remote users, select **Users & Networks**, then **Remote Users**.
2. Select the user from the list, and click **Delete**.
3. Click **Yes** to confirm, or **No** to cancel.

To Import Remote Users

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

1. Select **Users & Networks**, then **Remote Users**.
2. Click **Import**.

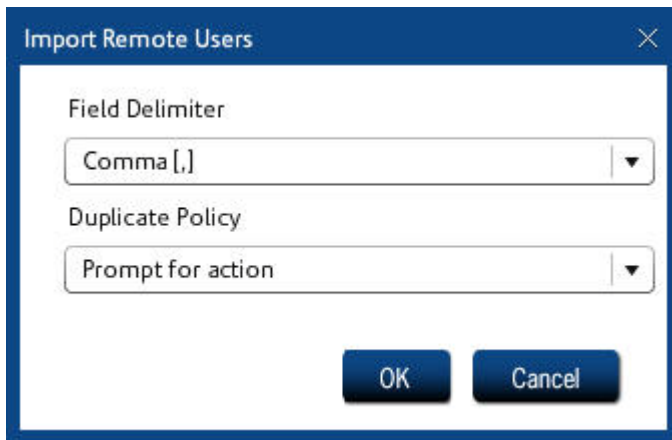


FIGURE 39. Importing Remote Users

3. Select a field delimiter (comma, pipe, or tab) for the import file.
4. 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.

5. Click **OK**.

6. 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
```

To Export Remote Users



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

1. Select **Users & Networks**, then **Remote Users**.
2. Click **Export**.
3. 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.
4. If there are no changes, select a field delimiter (comma, pipe, or tab) for the export file:

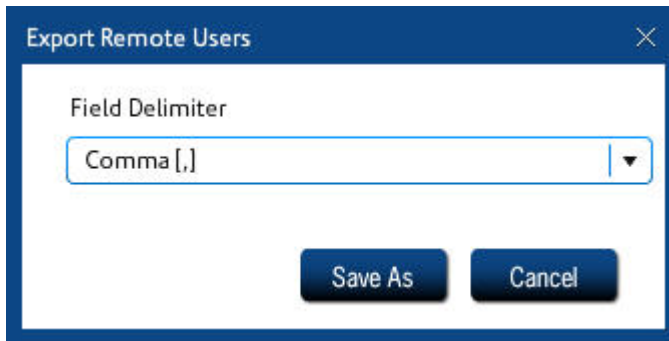


FIGURE 40. Exporting Remote Users

5. Click **Save As**.
6. Specify the location of the exported file.
7. 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
```

This chapter contains the following:

- **Email Alerts:** page 82
- **Report Manager:** page 86

Email Alerts

iPrism’s Email Alerts keep you aware of specific Internet-related events. Email Alerts work by sending an email notification to one or more defined email addresses each time a certain type of event occurs, or a certain threshold of activity is exceeded. Email Alerts are useful when the ACLs are configured to *monitor* activity, rather than blocking it, such as the following activities:

- You want to be immediately notified every time a particular employee surfs for more than 2MB of material from the job/employment search category in any 1-hour timeframe.
- You want to be immediately notified whenever any workstation whose profile monitors pornographic material attempts to surf to more than 10 web pages with pornographic content within 10 minutes.
- You want to receive an email when the combined bandwidth from all workstations within a low-priority Internet lab exceeds 100MB during any 30-minute period.

Once created, email alerts can be turned on and off as desired, so you can control when you are notified of events.

To configure email alerts, from the iPrism home page, click **Reporting**, then select **Email Alerts** (Figure 41).




Status	Name	Send Alert To	Content Monitored
 Enabled	Large Bandwidth Alert	admin@abc.com	adult,lingerie/bikini,nudity,pornography,
 Enabled	Large Number of Pages	admin@abc.com	adult,lingerie/bikini,nudity,pornography,
 Enabled	Large Number of Hits	admin@abc.com	adult,lingerie/bikini,nudity,pornography,

FIGURE 41. Email Alerts

To Add an Email Alert

1. From the Email Alerts window, click **Add**.
2. Type a name for the email alert in the **Name** field.

The screenshot shows the 'Email Alert' dialog box with the following details:

- Name:** Large Number of Hits
- Send Alert To:** admin@abc.com
- Status:** Enabled (radio button selected)
- Monitoring:** Any (dropdown menu)
- Threshold for Alert:**
 - Data:** Hits (dropdown menu)
 - Threshold:** 1000 (text box)
 - Time span:** 5 mins (dropdown menu)
 - Grouped:**
- Content:** Selected content to monitor (text) and a Select button
- Buttons:** OK and Cancel

3. Type the email address(es) of those who will receive the email alert. (Multiple email addresses must be separated by commas.)
4. Select **Status (Enabled or Disabled)**.
5. 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.
6. In the **Threshold for Alert** frame, select the parameters that should be watched and specify the threshold of activity that will cause an email alert to be sent.
- Under **Data**, select an option from the dropdown list:
 - **Bandwidth (KB):** An email alert will be sent every time 10 kilobytes of data is accessed by those defined in the **Type** frame within the time range specified in the **Time span** field.
 - **Pages:** An email alert will be sent every time 10 pages are accessed by those defined in the **Type** frame within any 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 every time 10 web accesses of any content type are accessed by those defined in the **Type** frame within any 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 after the user(s) specified in the **Type** frame have spent more than 10 minutes within any 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.
 - **Threshold:** Type an integer value. This will represent either kilobytes, pages, hits, or time spent, depending on what you selected from the **Data** dropdown list.
 - **Time span:** This is the duration over which the email alert tracker counts access information. Anytime the number of counts exceeds the threshold value within this time span, an email alert is sent.
7. In the **Content** frame, select the categories that will trigger the alert.
8. Click **OK** to save this email alert, or **Cancel** to cancel.
9. When you are finished modifying email alerts, click **Save** at the bottom of the Email Alerts window.
10. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Edit an Email Alert

1. In the **Email Alerts** window (Figure 41), click **Edit**.

2. Make any changes to the email alert.
3. Click **OK** to save your changes, or **Cancel** to cancel.
4. When you are finished editing email alerts, click **Save** at the bottom of the Email Alerts window.
5. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Delete an Email Alert

1. In the **Email Alerts** window (Figure 41), select an alert to delete and click **Delete**.
2. Click **Yes** to confirm the delete, or **No** to cancel.
3. When you are finished modifying email alerts, click **Save** at the bottom of the Email Alerts window.
4. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Report Manager

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 www.stbernard.com/products/support/iprism/documentation.asp for detailed instructions on how to manage and use the Report Manager.

This chapter shows you how to change iPrism's internal settings and set your preferences for common iPrism activities, such as managing updates, how to backup and restore, tests, self-checks, etc. The following maintenance tools are covered in this chapter:

Appliance Updates: page 88

Backup & Restore: page 93

Event Log: page 96

Policy Test: page 98

Self Check: page 99

Send Test Email: page 100

Support Tunnel: page 103

Test Directory Services: page 104

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, view which ones have already been installed, and manually install/uninstall a Hotfix.



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

To access Appliance Updates, from the iPrism home page, select **Maintenance**, then **Appliance Updates**. A list of available appliance updates (Hotfixes) is displayed (Figure 42).


Checking for Hotfixes

iPrism automatically checks for updates to its filtering database and system (software) files once each day. 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.⁵ 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. From the iPrism home page, select **Maintenance**, then **Appliance Updates**. Select the desired Hotfix(es) from the list and click **Install** (Figure 42). The Install Hotfixes web page opens.

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

ST BERNARD  **iPrism**[®]

Hotfix Manager

[Logout](#) - [Help](#)

Keep up-to-date:

Check for new Hotfixes or Reboot the system to activate recently (un)installed Hotfixes.

Available Hotfixes:

The below list contains the Hotfixes available for installation. Select the Hotfix you want to install and press the "Install" button.

2-520 Windows 2008 R2 Support (optional, inactive)
2-523 Windows with large numbers of groups (optional, inactive)

Installed Hotfixes:

The below list contains the Hotfixes currently installed on the the system. To uninstall a Hotfix, select it and press the "Uninstall" button.

2-521 SP1 (critical, inactive)

Manually Install Hotfix:

Manual installation of a Hotfix should only be used when instructed by Technical Support.

Hotfix ID:

Extra Arguments:

FIGURE 42. Hotfix Manager/Appliance Updates

2. Enter any optional parameters here.
3. Click **Install**, or click **Cancel** to return to the main Appliance Updates page.

If the Hotfix you selected is dependent upon earlier Hotfix(es) that you have not installed, then all required Hotfixes will be 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 will result in all dependent Hotfixes being uninstalled.

Rebooting after Installing Hotfix(es)

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 (Figure 43).

1. Click **Back**.

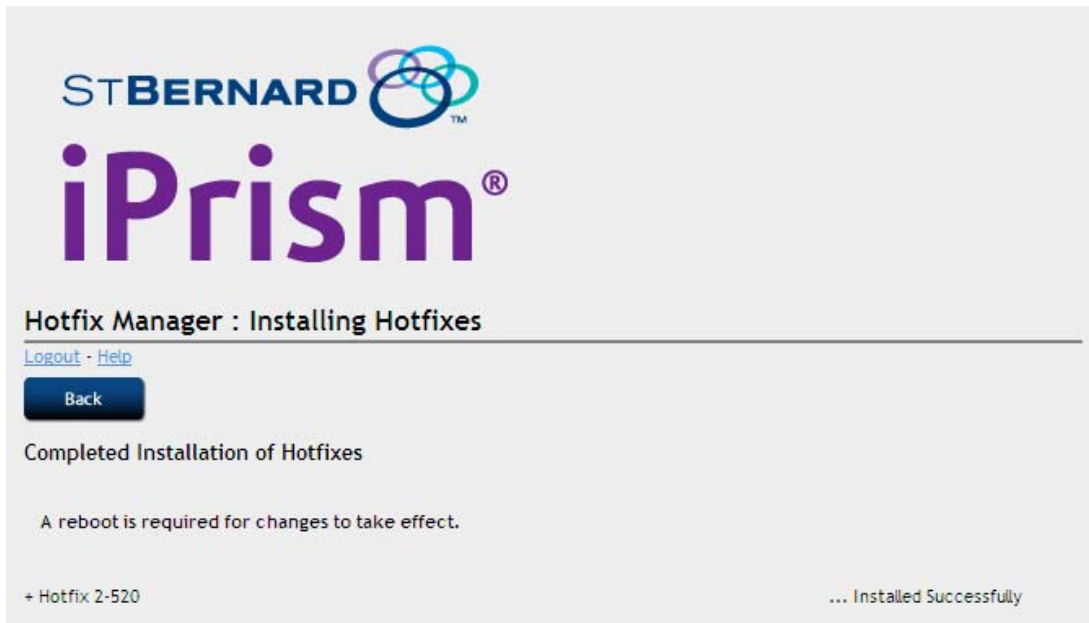


FIGURE 43. Completion of Hotfix Installation

2. Click **Reboot the system**.

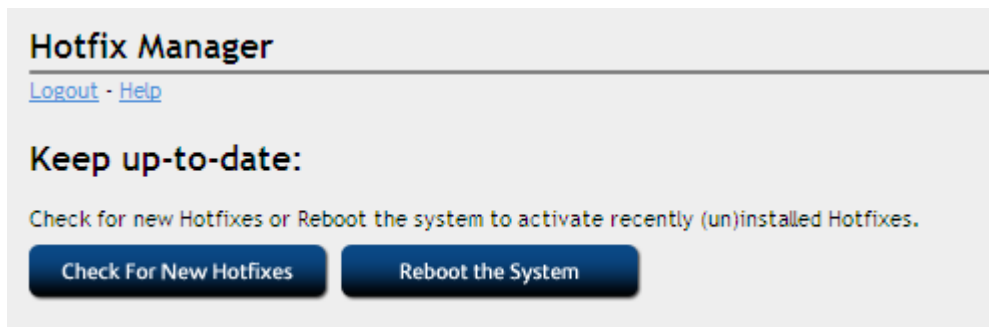


FIGURE 44. Reboot iPrism

3. Confirm the reboot by clicking **Reboot the system**.

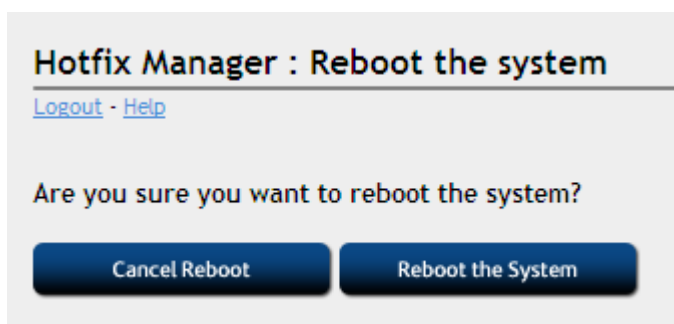


FIGURE 45. Confirm Reboot

Uninstalling a Hotfix

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

1. To uninstall a Hotfix, select the Hotfix you want to remove from the list and click **Uninstall**. A confirmation message will appear.
2. Click **Yes** to uninstall this Hotfix, or **No** to cancel and return to the main Appliance Updates page.



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

Searching for a Hotfix

To search for a specific Hotfix, type the Hotfix ID in the **Search for a Hotfix ID** field.

Installing a Private Hotfix

Private hotfixes are installed only under the direction of iPrism Technical Support. If you have received a Hotfix ID from iPrism Technical Support, follow the instructions below to install the Hotfix.

1. From the iPrism home page, select **Maintenance**, then **Appliance Updates**.
2. In the **Manually Install Hotfix:** frame, type the Hotfix ID and any extra arguments, if appropriate.
3. Click **Manual Install**.
4. Click **Install**.
5. When the hotfix has finished installing, follow the instructions in “Rebooting after Installing Hotfix(es)” on page 90 to reboot your iPrism.



Note: After you’ve rebooted your iPrism, log back into Hotfix Manager to verify that the new Hotfix appears in the Installed Hotfixes list.

Backup & 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. **Note:** the backup configuration file can be useful to provide configuration data to iPrism Technical Support.

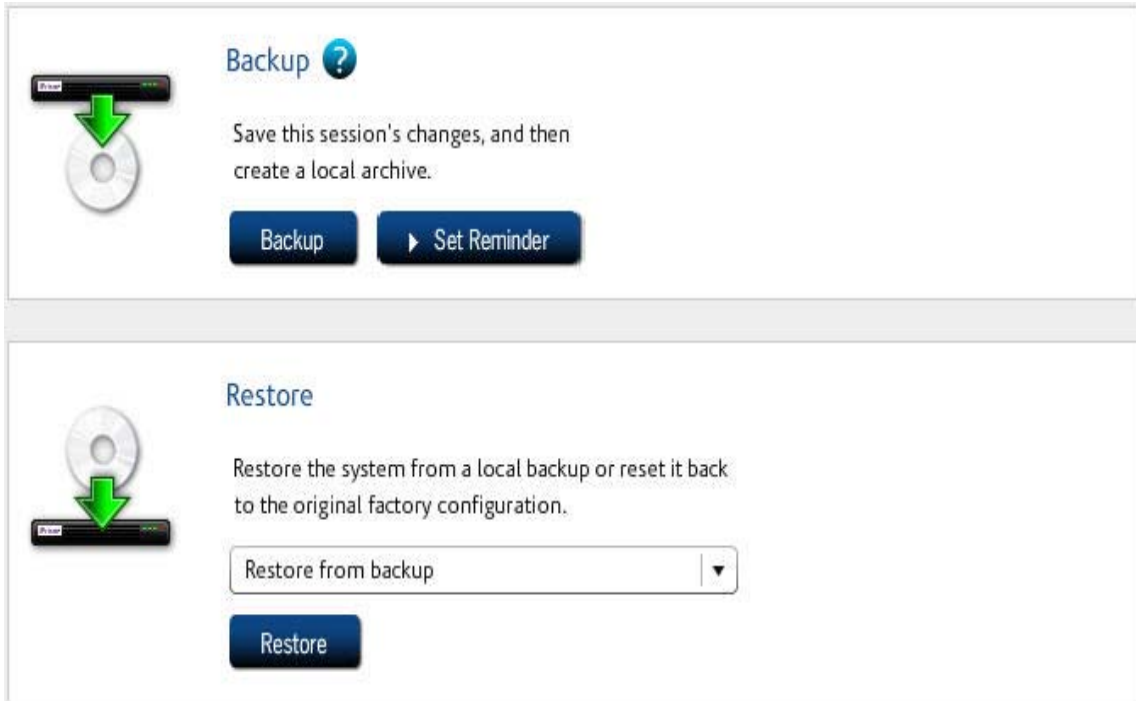


FIGURE 46. Backup & Restore

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.



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

Setting Backup Preferences

By default, iPrism automatically prompts you when you exit to back up your iPrism System Configuration. You can change the frequency of the prompts by doing the following:

1. From the iPrism home page, select **Maintenance**.

2. Select **Backup & Restore** (Figure 46).
3. To perform an immediate backup, click **Backup**.

Setting Backup Reminders

1. To set your backup reminder preferences, click Set Reminder and select your desired options in the **System Settings > System Preferences** page (for more information about this page, see page 169):
 - **Prompt when Exiting:** You will be prompted to back up your configuration when you exit an iPrism session.
 - **Prompt when Starting:** You will be prompted to back up your system 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 (1-30)** 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.

2. Save your iPrism configuration by selecting **Save** at the bottom of the window.
3. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Restoring

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

Restoring Your System from a Local Backup

1. From the iPrism home page, select **Maintenance**.
2. Select **Backup & Restore Settings** (Figure 46).
3. In the **Restore** frame, select **Restore from backup** and 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 will clear all user-defined configuration information. You should do a backup of your current configuration before performing this procedure. (See “Backing Up” on page 93).

1. From the iPrism home page, select **Maintenance**.
2. Select **Backup & Restore Settings** (Figure 46).
3. In the **Restore** frame, select **Restore Factory Configuration**.



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

4. Click **Restore**.

A dialog box appears to inform you about the ramifications of the choice you have made.

5. Click **OK** to proceed with the restoration that you selected. If you want to cancel this process now, click **Cancel**.

If you clicked **OK**, the iPrism unit will reboot within two minutes, and your iPrism session will end. 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 IM/P2P accesses. Also provided is the date of the oldest record accessed.

Access Event Status

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

Delete Access Event Records

Delete up to and including date

/ /  

Delete all access event records in the system.

FIGURE 47. Event Log

To Delete 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 data from iPrism:

1. From the iPrism home page, select **Maintenance**, then **Event Log** (Figure 47).
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 delete, or **No** to cancel.

Policy Test

You can access additional NTLM 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: You must have successfully joined the domain in **System Settings > Directory Services** (see page 113) in order to test a policy. Once you have done so, complete the following steps:

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 will attempt to validate the user. The results will be displayed in the Test Result field.

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

Username	Password
<input type="text" value="iprism"/>	<input type="password" value="*****"/>
User IP Address	Domain
<input type="text" value="192.168.1.100"/>	<input type="text" value="iprism.local"/>



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 user mapped to web profile: BlockOffensive

FIGURE 48. 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 check on all mapped groups to determine whether they exist in your directory:

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 (see Figure 49 for an example). You can stop the check by clicking **Stop Check**.
4. You can send these results directly to St. Bernard Software Technical Support by clicking **Send to Tech Support**.
5. To clear the screen and perform a new check, click **Clear**, then **Start Check**.

The screenshot displays a 'Self Check' interface with a light gray header containing 'Print' and 'Send to Tech Support' buttons. The main content area lists several checks, each with a status in brackets: 'Name Server... [PASSED]' with the note 'You have 1 nameserver(s) listed.'; 'Results for [REDACTED]: OK'; 'RateD... [PASSED]' with 'Service is running'; 'Default Gateway... [PASSED]' with 'No Comments'; 'System Information... [COMPLETED]' showing 'Uptime 6 hrs', 'System Memory 989724 KB', 'Free Memory 527972 KB', and 'CPU Utilization 0.0 %'; 'Disk space check... [PASSED]' with 'iPrism disk space test passed (0% used)'; 'NTP Server... [COMPLETED]' with 'Use NTP Server is not enabled on the appliance.'; and 'Routing Tables... [COMPLETED]' with 'Routing tables'. Below these is an 'Internet:' section with a table header: 'Destination Gateway Flags Refs Use Netif Expire'. The footer contains 'Start Check', a help icon, 'Stop Check', and 'Clear' buttons.

FIGURE 49. Self 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).

Send Test Email

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**.

The Test email facility allows iPrism administrators to ensure that iPrism emails are being sent to specifiable recipients and are an allowable size (in Megabytes).

Email Address	Email Size MB	
<input type="text" value="test@domain.com"/>	<input type="text" value="5"/>	<input type="button" value="Test Email"/>

FIGURE 50. Send Test Email

4. If the email is sent successfully, a confirmation message similar to the one in Figure 51 will appear. Click **OK** to dismiss the message.

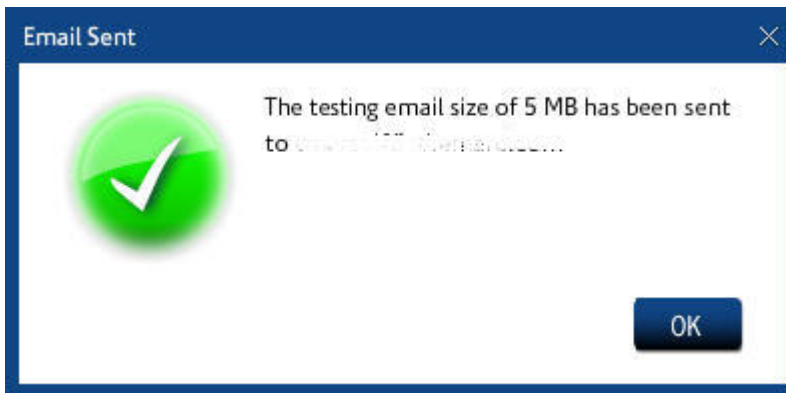


FIGURE 51. Confirmation of Test Email Sent

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. A simple way to check the category rating of any website is to do the following:

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



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

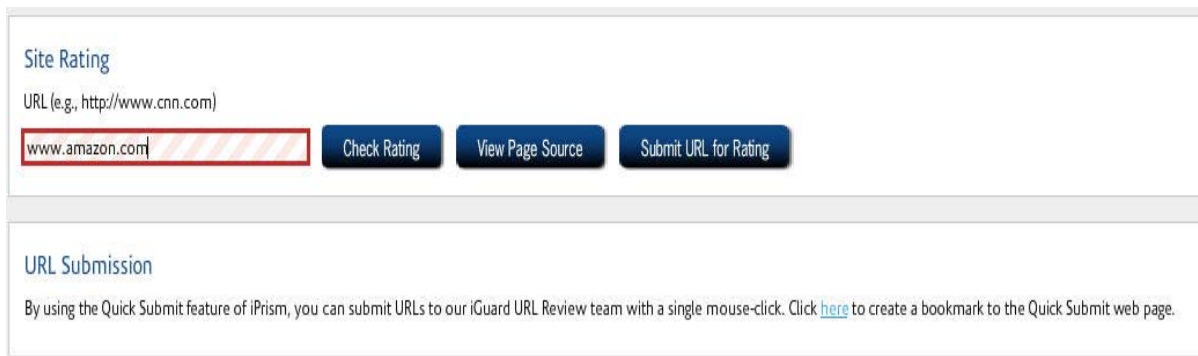


FIGURE 52. Site Rating & Test

3. If you would like to submit the site to St. Bernard Software’s team for review, click **Submit URL for Rating**. The URL of the site will be 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 will restart automatically. This maintains the tunnel across reboots.

Status **Tunnel is not enabled.**

Username: iprism

Password: *****

Remote Host: 199.245.188.22

Port: 25

Expires: 1 days

Start Stop

FIGURE 53. Support Tunnel

1. From the iPrism home page, select **Maintenance**, then **Support Tunnel**.
2. As directed by Technical Support, type your username and password.
3. The **Remote Host** and **Port** are pre-populated with the iPrism Technical Support tunnel server’s IP address (199.245.188.22) and accepts port 25, 80, or 8000.
4. In the **Expires** field, select from the dropdown list the number of days to keep this Support Tunnel active (between 1 – 7 days).
5. Click **Start**.

If directed, stop the support tunnel by clicking **Stop**.

Test Directory Services

This allows the administrator to test iPrism directory services (authentication modes).

1. From the iPrism home page, select **Maintenance**, then **Test Directory Services**.
2. Select a directory service (LDAP, AD 2000, AD 2003, or AD 2008) from the **Select Directory Service** dropdown list.



Note: A directory service can only be tested if it is enabled and available.

3. Type a **Username** and **Password** in their respective fields.
4. Click **Test Credentials** to test the credentials you have entered and directory service you have selected.

Authentication Mode & Status

Mode: Server 2000/2003
Status: Joined to M13DOMAIN
Connected: Connected to M13DOMAIN

Credentials to Test

Username

Password

Domain

Results

FIGURE 54. Test Directory Services

This chapter shows you how to change iPrism's internal settings and set your preferences for common iPrism activities. The following features are covered in this chapter:

Central Management: page 108

Customizable Pages: page 108

Directory Services: page 113

Enterprise Reporting: page 141

Event Logging: page 141

License Key: page 144

Setting up iPrism on your Network (**Network ID:** page 149)

Network Services: page 154

Pending Request Options: page 161

Ports: page 162

Proxy: page 166

System Preferences: page 169

Unrated Pages (iARP): page 175

User Settings: page 177

Central Management


See “Central Management” on page 193.

Customizable Pages



Formerly referred to as the *HTML Template Manager*, iPrism’s Customizable Pages allow you to fully customize the default Authentication, Access Denied and other pages used by iPrism.




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




Authentication Page 

This page is displayed to the user at the beginning of a new browsing session or when the user’s current session has expired. It requires the user to enter their username and password, and allows them to change their session timeout. Note that this page is only displayed if authentication is enabled on the iPrism.

Page to be used  

Access Denied 

This page notifies the user that the site which he or she is trying to access has been blocked by iPrism. Unless the user has override privileges or is otherwise granted access by the administrator, the user will not be able to view the site.

Page to be used   

All Other Pages

Customize all other end-user visible pages, for example, the Override Request page. This is independent of customizing the Authentication and Access Denied pages. You can specify organization information, contact information, a background image, a style sheet, and HTML code for the top, left, right, and bottom regions of the page.



 

FIGURE 55. iPrism Customizable Pages

To Customize the Authentication, Access Denied, or Other Pages

1. From the iPrism home page, select **System Settings**, then **Customizable Pages**.

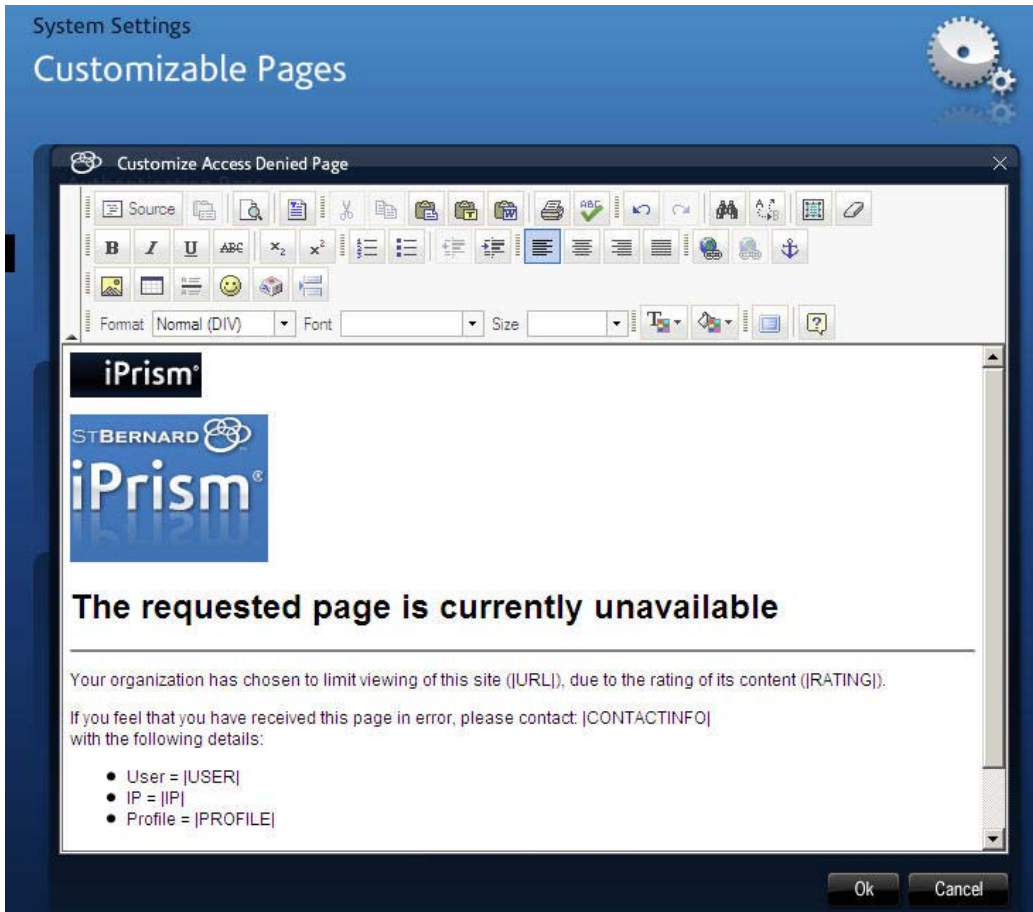
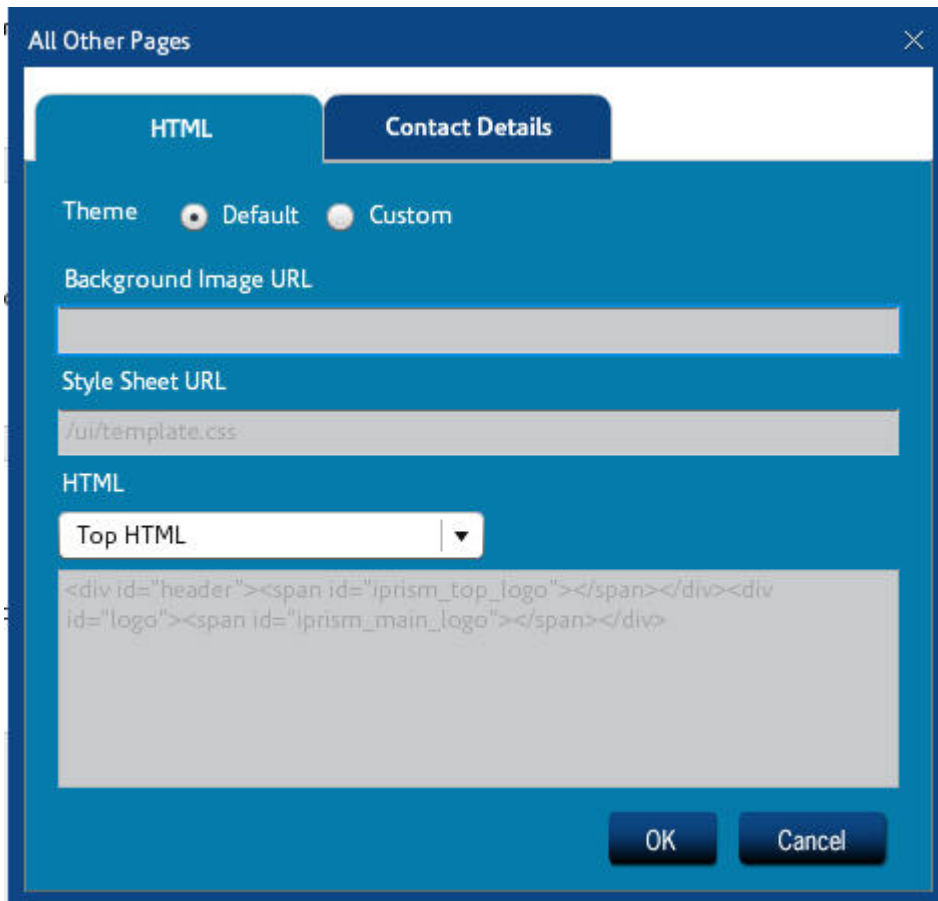


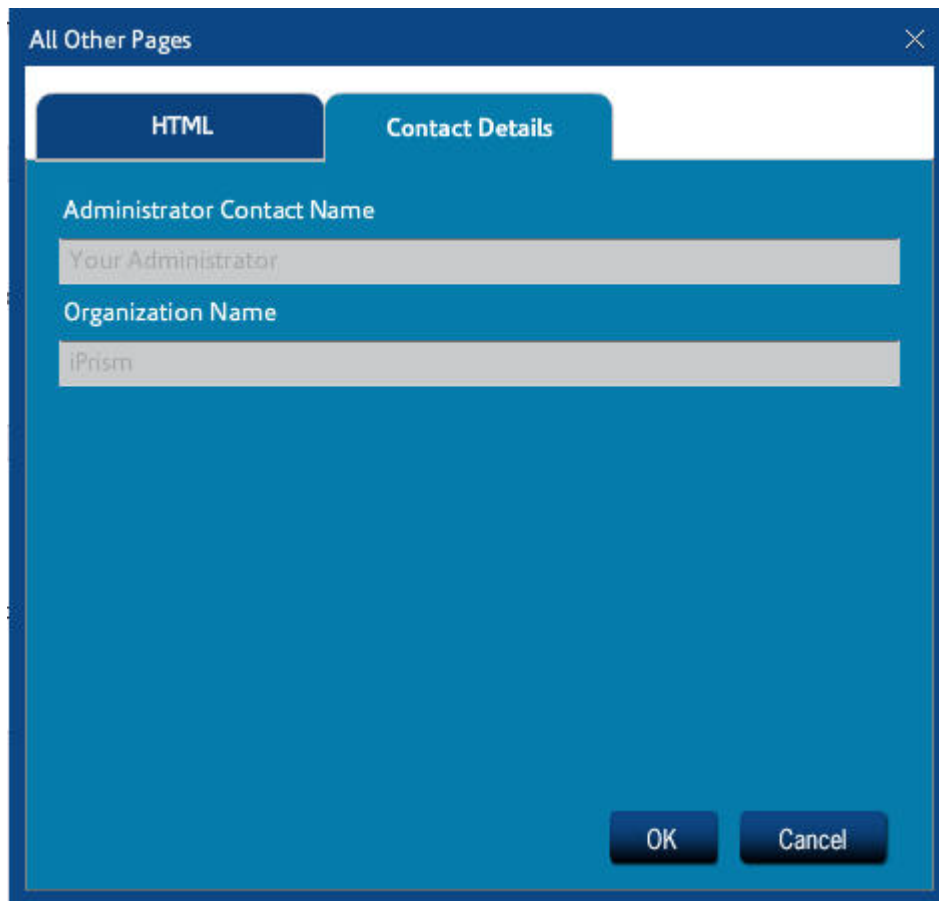
FIGURE 56. Customizing the 'Access Denied' Page

2. If you want to change the Authentication page that is displayed to users, in the Authentication page frame, select either **iPrism Default** or **Customized HTML** from the **Page to be used** dropdown list.
 - If you select **iPrism Default**, click **Preview** to look at a preview (you cannot edit this page).
 - If you select **Customized HTML**, the **Customize** button will become available. Click it to edit the HTML content of the page. For a listing of customizable page tags, see **Customizable Page Tags** on page 112. Click **X** in the top right corner of the window when you are done editing.

3. If you want to change the Access Denied page that is displayed to users, in the Access Denied frame, select from the dropdown list the page to be used (**iPrism Default**, **Customized HTML**, or **Specified URL**).
 - If you select **iPrism Default**, click **Settings** to view the page settings, or **Preview** to preview the page.
 - If you select **Customized HTML**, click **Customize** to edit the HTML content of the page. For a listing of customizable page tags, see **Customizable Page Tags** on page 112. Click **X** in the top right corner of the window when you are done editing.
 - If you select **Specified URL**, type the URL to be used in the URL field. Click **Preview** to preview the page the user will see.
4. If you want to change what the user sees in other pages (e.g., the Override Request page), in the All Other Pages frame, click **Customize**.
5. In the HTML tab, select a theme for the page (**Default** or **Custom**).



6. Type a Background Image URL if you want to use a background image, and a Style Sheet URL if you want to use a style sheet.
7. Select where the HTML code will reside (Top, Left, Right, or Bottom).
8. Click the Contact Details tab. Type the contact information for your administrator, and your organization name, if you want them to display on the page.



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 and contains two text input fields. The first field is labeled "Administrator Contact Name" and contains the text "Your Administrator". The second field is labeled "Organization Name" and contains the text "iPrism". At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

9. When you are done, click **OK** to save, or **Cancel** to cancel.
10. When you are finished customizing pages, click **Save** to save your changes, or **Revert** to cancel.
11. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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).

Tag	Description
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.
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:
 1. **Redirect their first web access to an iPrism login page** (see Figure 1 and Figure 63): Once s/he logs in, iPrism knows who they are and can provide filtering based on the profiles assigned to their username.
 2. **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, see "Local Authentication" on page 115).

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.
 3. **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 page 136 for details on Windows authentication, and page 115 for information on LDAP authentication.

After you gain experience with the system, you'll 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" on page 126.



Notes:

- 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, s/he 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



Note: Active Directory on Windows 2003 is LDAP-compliant by default. Windows NT supports LDAP only through Exchange server. For more details about LDAP on Windows, refer to 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".

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.

Creating User Accounts on the iPrism

1. From the iPrism home page, select **Users & Networks**, then **Local Users**.
2. Follow the instructions in Chapter 4: Users and Networks, "Local Users" on page 48, 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.

Refer to the "Configuration example (using NT Active Directory)" on page 120 to understand how iPrism performs lookups.

Setting up the iPrism LDAP Client

1. From the iPrism home page, select **System Settings**, then **Directory Services** (see Figure 57).
2. Click **Configure & Join**.
3. From the **Authentication Mode** dropdown list, select **LDAP**.

Authentication Mode and Status

Authentication Mode

LDAP

LDAP Settings

LDAP Server(s)

--	--

Add Edit Delete

Search DN

Base

Use UID

Mask

Require attribute

Attribute

Search Password

Use legacy profile resolution

Encryption Type

Sub-Query Attribute

Presets Test Settings

FIGURE 57. 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**

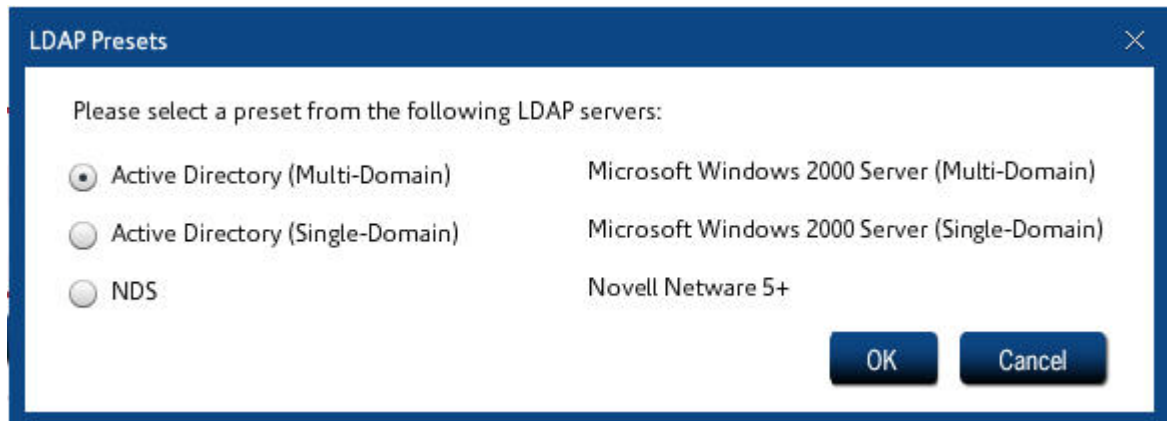


FIGURE 58. LDAP Presets

If you are filling in your own LDAP server information:

- **LDAP Server(s):** Click **Add** to add an LDAP server. Enter the DNS name or IP address of your LDAP Server from which user authentication and profile information will be retrieved.



Note: iPrism requires plain-text authentication to be enabled on the server.

- **Port:** Enter the TCP port number used by LDAP. The default LDAP port is 389. For NT/Win2k Active Directory, the global catalog port is 3268.
- The **Search DN** needs to be a domain user account with privileges to query the LDAP server. The DN can be in Windows 2003/2008 LDAP format or Windows 2003/2008 UPN format (e.g., admin@iprism.stbernard.com); however, note that non-Windows LDAP servers may accept only LDAP distinguished name (DN) format: CN=domain_user_account, DC=your_domain_name, DC=com.
- Windows 2000 and above servers accept DNs, but also accept RFC 822 User Principal Name (UPN) format: domain_user_account@stbernard.com, where stbernard.com is a domain name.



Note: If left empty, an anonymous bind is performed. Note that anonymous binds lack administrative rights to perform a sufficient search of the LDAP tree.

- **Search Password:** The password associated with the Search DN or UPN username on the LDAP server. It can be left empty if the LDAP server does not require a password.

- **Base:** This parameter indicates the common root of all information that will be considered when iPrism queries the LDAP server for user data. Base DN will typically be some representation of your organization. LDAP data is stored conceptually in a tree, containing nodes, or branches of information. This describes how the LDAP information is organized in the source server. Changing the Base DN can restrict to searching a given group on the LDAP server. The setting depends on your LDAP vendor:

Novell NDS: o=organization
Windows Active Directory: dc=domain, dc=com
MacOSX

- It can also be left empty for servers that accept an empty Base DN, such as NDS, and iPrism will default to the root of the LDAP server. Base DN's can use domain components (DC) to search as subdomain, as in: "DC=mySubdomain, DC=mydomain, DC=com."
- **Use UID:** Selecting the checkbox automatically activates the simple Mask value of **uid=%1**.



Note: Since the pound sign (#) is used as the attribute value separator, it must be considered an illegal character in any attribute value (uid, name, organization, etc.)

- **Use Legacy Profile Resolution:** When un-checked, it enables LDAP group-to-profile mapping via the Profile Mapping tab. When checked, it disables access to the Profile Mapping tab, implying you wish to use an pre-existing LDAP configuration as is.



Note: This method is no longer recommended, but is supported for users with iPrism prior to version 5.0.

- **Mask:** The mask is a way to designate the attribute(s) that will cause the LDAP access to result in a unique user node. The syntax for the **Mask** field uses a combination of attribute (**attrNUM**) and value (**%NUM**) separated by the equals sign (=). Multiple attribute/value pairs must be separated by the # character. **attrNUM** is the actual name of the attribute, and **%NUM** indicates the position in which a user would enter the information in the name field of an authentication prompt. So the syntax is as follows **attr1=%1[#attr2=%2[...]]**.

Mask	User login example
uid=%1	bill
name=%1#organization=%2	sally#accounting

In the first row, the LDAP server is going to search for the unique node that has the uid attribute equal to `bill`. In the second row, the matching node will have the name attribute equal to `sally` and the organization attribute equal to `accounting`. This flexibility allows the organization to have the same username (`sally`) in two different departments.

- **Encryption Type:** This dropdown menu supports secure connectivity and contains the values of **none** (default), **SSL**, and **TLS**. **SSL** (Secure Sockets Layer) and **TLS** (Transport Layer Services) enable encrypted traffic between iPrism and eDirectory for improved security. When selecting SSL, change the port to **636**.
- **Require Attribute:** Check this box if you want to force the LDAP server to supply the profile name attribute. As a consequence, fallback profiles are not used. If this box is checked and a profile name attribute is not obtained, authentication will fail.



Note: This method is no longer recommended, but is supported for users with iPrism prior to version 5.0. Instead, use Profile Mapping to map LDAP user profile results with iPrism profiles; See “Assigning an Authentication Mechanism to an IP Address Range” on page 126.

- **Attribute / SubQuery Attribute:** Each LDAP node will usually have many attributes of information about the user. iPrism can run up to two LDAP queries to determine a user’s profile. If the value in the **Attribute** field is a distinguished name, iPrism will perform a second query, searching for the SubQuery attribute. This allows the ability to use groups to define profiles, so you will not have to reconfigure individual users. For example:

```
Query for user <CN=joe, DC=stbernard, DC=com> returns the values  
memberOf = <CN=group1, DC=stbernard, DC=com>  
memberOf = <CN=group2, DC=stbernard, DC=com>
```

The iPrism LDAP client will then query each ‘memberOf’ group until it finds a valid attribute. Since there is no mapping yet, the first valid attribute is used.

iPrism can also just retrieve a single attribute to use as the name of an access profile on iPrism. This will then be associated with the user for access privileges. If you want to use this feature, configure your LDAP server to provide such information under a specific attribute name, and list that name in the **Attribute** field.

If a **SubQuery Attribute** is defined, iPrism will proceed as follows:

1. Authenticate the user using provided credentials
2. Look up the value of the (primary) attribute for the user
3. If the attribute is a DN, look up this DN
4. Search for the secondary (SubQuery) attribute of this DN
5. Use the value of the secondary attribute as the iPrism filtering profile name



Note: For multi-valued attributes, the first valid match (i.e., the value maps to an existing iPrism profile) will be used.

6. When you have finished configuring the LDAP server, 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.
7. 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.

Configuration example (using NT Active Directory)

User John:

```
DN = samaccountname=John, dc=company, dc=com
email = John@company.com
location = San Diego
memberOf = cn=group1, dc=company, dc=com
memberOf = cn=group2, dc=company, dc=com
Group1
DN = cn=group1, dc=company, dc=com
attr1 = value1.1
attr2 = value2.1
```

Group2

```
DN = cn=group2, dc=company, dc=com
attr1 = value1.2
attr2 = value2.2
iprism = BlockOffensive
```

Group3

```
DN = cn=group3, dc=company, dc=com
attr1 = value1.3
attr2 = value2.3
iprism = undefined_value
```

iPrism configuration :

```
Attribute = memberOf
SubQuery attribute = iprism
Profiles = BlockOffensive, Pass All, MonitorOffensive
```

Notes:

When John tries to authenticate, iPrism will lookup the group's 'memberOf' attribute attached to John's user settings.

John is a member of group1 and group2. iPrism will first look up group1 and search for the 'iprism' attribute; there is no such attribute in group1 so iPrism will move on to group2 and find the value BlockOffensive, which is used as John's profile.

Group3's 'iprism' attribute is not valid because the value does not correspond to a profile on iPrism; it would be skipped.

Troubleshooting LDAP Authentication

For instructions on how to test and troubleshoot authentication, see “Maintenance” on page 87 and “Test Directory Services” on page 104.

How Profiles are Assigned

When users on your network authenticate through a LDAP authentication server, you can configure iPrism to access user information directly from the LDAP domain controllers. After authenticating, iPrism can obtain group assignments, and each of these groups can be mapped directly to an iPrism profile. The group mapping for profiles is done in the Groups section (see “Mapping Privileges to Groups” on page 54), and the mapping for assigning iPrism administrator privileges is done in the **Privileges** section (see “Privileges” on page 54).

Microsoft Windows Authentication (NTLM)

The Microsoft Windows authentication feature lets iPrism access Microsoft Windows users information directly from one or more Microsoft Windows domain controllers. This allows iPrism to seamlessly authenticate Microsoft users and obtain Microsoft group assignments. With this information, iPrism can control and/or monitor user access to the Internet. iPrism provides a simple mapping scheme in which Microsoft Windows groups are associated with iPrism access profiles and administrative privileges. This allows for extremely detailed control of externally authenticated users.

Configuring Microsoft Windows authentication on iPrism requires only a few steps. In fact, depending on the complexity of your Microsoft Windows environment, and the granularity with which you want to control/monitor users, it can be extremely easy. The next few sections will show you how to join iPrism to your Microsoft Windows Domain and map Microsoft groups to iPrism’s profiles and administrator privileges.

Joining iPrism to a Microsoft Windows domain requires configuring a small number of Microsoft Windows parameters, such as the domain name and the WINS server addresses, if needed. After you have supplied sufficient Microsoft Windows administration credentials, clicking **Join** will create a Microsoft Windows account for iPrism. It is under this account that iPrism will securely communicate with the domain controllers.

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** (Figure 59).

Authentication Mode and Status

Authentication Mode

Domain Settings

NT Domain

Active Directory Realm

Machine Account

Username

Advanced Settings

Domain Controller(s)

Add Edit Delete

Password

FIGURE 59. Joining iPrism to an Microsoft Windows Domain

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 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 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 AD 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. Click **Advanced Settings** (Figure 60).
9. Type the IP address of the domain controller you want to use in the **Domain Controllers** field.



Notes:

- Each domain controller must be entered separately. When you have finished entering your first domain controller, click **OK** to save it, then click **Add** on the main Authentication window (Figure 59) to add another domain controller.
- Multiple domain controllers must be for the same domain.
- Each domain controller must be a domain controller for the Active Directory Realm specified to the left of the Domain Controllers (Figure 59).
- Multiple domain controllers must implement Active Directory Sites and Services and must replicate the group, user account, and computer account information between them.

10. **Enable NetBIOS** is checked by default, in order to use the NetBIOS protocol.
11. The LMHosts file provides a mapping between IP address and NETBIOS computer names for networks without WINS Servers (or networks with broken WINS Servers). If you have a LMHosts file on your workstation, you can transfer it to the iPrism by checking **Enable LMHosts**, then clicking **Import** and selecting the LMHosts file from the window that appears. You can also edit this file manually by clicking **Edit**, which brings up an editing window.

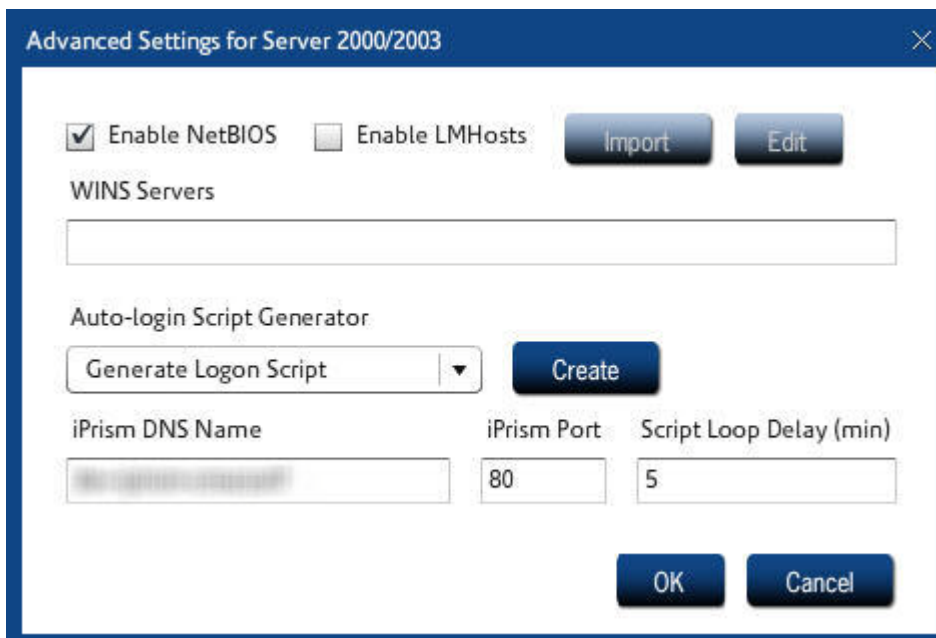


FIGURE 60. Advanced Settings

12. If you are using WINS servers, type their IP addresses in the **WINS Servers** field. Multiple IP addresses must be separated by commas.

The **Auto-Login Script Generator** allows the generation of the logon/logoff scripts for deployment to users. Bridge (transparent) mode filtering configurations can benefit from client-side logon/logoff scripts. They support immediate Windows authentication to iPrism when users log on to their workstations. This provides up-front user identification without requiring web browsing to establish the authenticated session with iPrism, providing timelier authentication for bridge (transparent) mode users.

For example, a user can be profiled/reported-on by username for an IM/P2P application without the user browsing the Internet first to establish an authenticated iPrism session. Another benefit is that the first browsed website may now be an HTTPS (secure) website, which will be profiled by username, instead of IP address. Basic requirements for successfully using these scripts are as follows:

- Windows Authentication and Transparent-Mode Auto-Login are working.
- Transparent Auto-Login Timeout compatibility check.
- Script generation using iPrism.

For more information, refer to the Auto-Login tech-note on the iPrism support web page:
http://www.stbernard.com/products/support/iprism/support_iprism-tnotes.asp

13. Select whether to **Generate Login Script** or **Generate Logoff Script**.
14. To create a script, click **Create**.
15. If the Auto-Login redirection setting is configured to resolve iPrism's IP address using DNS, the iPrism's hostname will be used to redirect traffic to the iPrism's authentication scripts. The reason that the hostname is used, rather than the fully qualified domain name of the iPrism, is so that Internet Explorer will recognize the iPrism as a suitable host for Auto-Login.
 - The **iPrism Port** defaults to 80. If you are using a different port number for HTTP, you may change this value.
 - The **Script Loop Delay** (minutes) determines the frequency of user authentication by the iPrism logon script. The default is 5 minutes.
16. Click **OK**.
17. To add another domain controller, click **Add** on the main Authentication window (Figure 59).
18. Click **Join**.
19. Save your configuration by clicking **Save**.
20. If all settings are correct and the join was successful, you can now set up your clients' browsers. For instructions on specific browsers, refer to the following articles in the Knowledgebase:
 - “Configuring IE for proxy mode Auto-Login”
 - “Configuring IE for transparent mode Auto-Login”
 - “Configuring Firefox”



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

Maintaining iPrism's Machine Account

The process of joining a domain (establishing the machine account and defining the encryption key by which all communications will be encoded) is a one-time event. Once a client has “joined” the domain, it is not necessary to rejoin, unless some event occurs on either the domain or the iPrism that causes the shared encryption key to be lost, such as the following:

- The machine account is deleted from the domain.
- The domain controller encounters a failure in which all machines must rejoin the domain.
- A replacement iPrism is deployed and is configured from scratch.

Debugging Windows Authentication Problems

See “Policy Test” on page 98 for detailed information about troubleshooting NTLM.

Assigning an Authentication Mechanism to an IP Address Range

See “Users and Networks” on page 47 for instructions on how to assign an authentication mechanism to a range of IP addresses.

Recommended Authentication Settings

Proxy Mode: If you are using NTLM or LDAP, the recommended authentication settings is **Auto-Login** with **Basic** enabled. If you are not using NTLM or LDAP, the recommended authentication setting is **HTTPS**.

Bridge (Transparent) Mode: The recommended authentication setting is **Auto-Login** with **HTTP** enabled.

iPrism and External Certificate Authorities

The iPrism can use a trusted server certificate if one is obtained by an administrator. For more information, refer to the iPrism Knowledgebase article “Windows SSL Certificate Management for iPrism” at http://www.stbernard.com/products/support/iprism/help_6-4/iPrism/Networking/Sessions-Clients/Https/Authentication/IP0325.htm

Auto-Login Details

Auto-Login automatically obtains user credentials from the workstation using a secure Microsoft authentication method. This means users do not have to manually provide credentials to iPrism. iPrism is able to authenticate Windows users when they are logged into a domain trusted by iPrism’s configured domain controller and client browsers can respond to Windows authentication requests from iPrism.

The mechanism is different if you are using Windows or LDAP. Auto-Login is also different depending on whether your iPrism is configured in Proxy mode or Bridge (Transparent) mode.

For more information, see the following iPrism Knowledgebase articles, available at www.stbernard.com/products/support/iprism/help/iprism.htm:

- “How do I enable Bridge (Transparent) mode Auto-Login?”
- “How do I enable Proxy mode Auto-Login?”

Active Directory (Windows Server 2000/2003 or 2008) Authentication

When using Windows, rather than requiring a user to manually enter their account information, it is automatically obtained from the browser.⁶ The details vary somewhat depending on which mode (proxy or bridge (transparent)) is in effect.

When using Windows, iPrism is able to authenticate any workstation as long as the user is logged in to a domain trusted by iPrism's domain controller and the browser is configured to allow automatic authentication. If the Auto-Login fails, iPrism will revert to its regular authentication interface and prompt the user for his/her account credentials.

1. Windows Directory Services must be enabled on the iPrism, and the iPrism must be joined to the Active Directory domain.
2. Users must log in to domain user accounts, on client machines joined to the domain.
3. Client machines must provide a browser that is Internet Explorer 6 or later (on PC), Safari (on Mac), or Firefox (on any platform). For more information on configuring browsers for authentication, see Appendix B: "Configuring Browsers for Authentication" on page 249.
4. If the client machine is to be proxied, it must proxy to the iPrism.
5. Citrix, Terminal Server, or shared IP address configurations are supported only in proxy mode.

LDAP (Novell eDirectory) authentication:

1. LDAP directory service must be enabled on the iPrism.
2. Users must log in using the Novell Client.
3. Shared IP address configurations are not supported.

When using LDAP, rather than requiring a user to manually enter their account information, iPrism queries the Novell eDirectory **networkaddress** attribute that keeps track of the IP address of the user's workstation. When the user logs on, the attribute is populated with the IP address and the appropriate profile is applied. When the user logs off, the attribute is cleared.

Using Auto-Login in Bridge (Transparent) Mode

For Auto-Login to work in bridge (transparent) mode, the following network/system requirements must be met:

Windows

- Windows authentication must be configured, enabled, and operational on iPrism (see "Authentication from the User's Perspective" on page 131).
- The primary web browser is either Internet Explorer or Firefox.

-
6. Some web accesses do not involve a browser (e.g., Windows Update). In this case the application may not honor the protocol used for automatic authentication. When this happens, the iPrism is unable to select a profile based on the username, so it falls back to IP address-based profiles.
-

- In Internet Explorer, one of the following modes must be in place to verify that the user is logged in to a domain trusted by iPrism’s domain controller.
 - **IP-based mode:** Under this configuration, the IP address of iPrism (i.e., not the DNS name or WINS name) must be in the local Intranet zone of the browser. (This can be done network-wide by configuring the domain controller, or each workstation can be configured manually using the procedure below.)
 - or -
 - **DNS-based mode:** This approach requires that the browser be able to resolve iPrism’s non-fully qualified host name to an IP address. This can be done network-wide by configuring your local DNS forward lookup zone[s] to contain an A record for iPrism.
 - **Firefox** must be configured to use **NTLM** authentication through the *about:config* page. The parameter *network.automatic-ntlm-auth.trusted-uris* must include *http:<iPrism-ip>*, where *<iPrism-ip>* is the IP address of the iPrism.
- In the **Networks** section of Users & Networks (see “Networks” on page 57), the **Auto login** checkbox must be checked in **Bridge (Transparent) mode authentication** (see Figure 61).

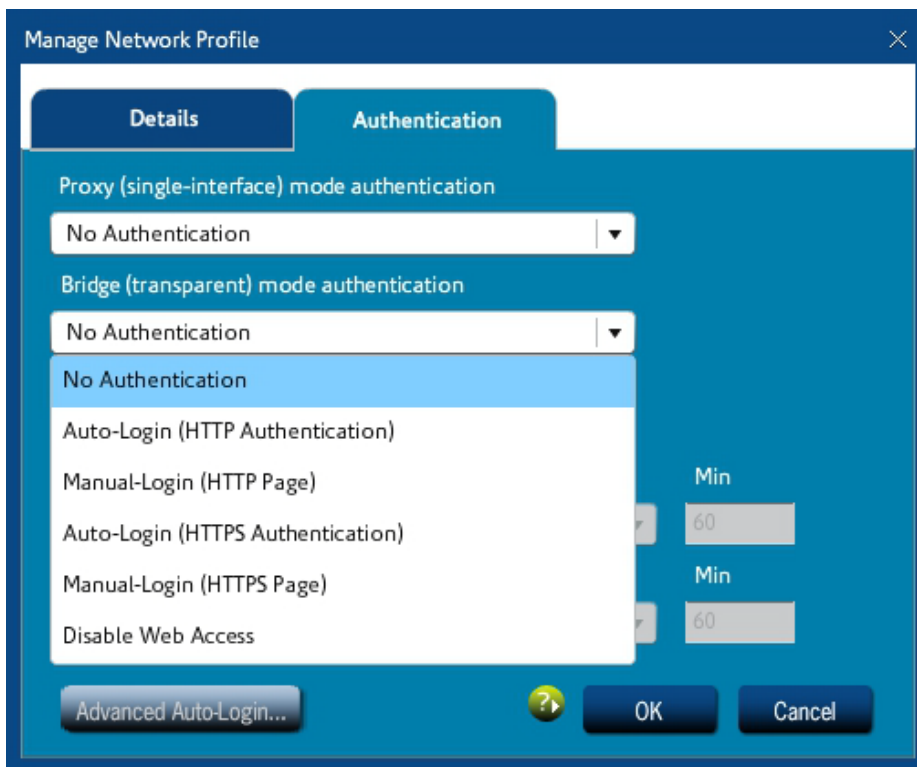


FIGURE 61. Auto-Login in Bridge (Transparent) Mode

For LDAP

- LDAP authentication must be configured, enabled, and operational on the iPrism (see “LDAP Authentication” on page 115).
- Internet Explorer is the primary web browser.
- LDAP Auto-Login Server requirements:
 - Novell eDirectory 8.7.3 or 8.8, on Novell NetWare
 - LDAP Auto-Login is supported for Windows/Linux users running a Novell “NMAAS capable” (Novell Modular Authentication Service) login client, meaning a Novell login client version 4.90 and higher.
- End users must login to the Novell eDirectory using a Novell client.
- In the **Networks** section of Users & Networks (see “Networks” on page 57), the **Auto login** checkbox must be checked in **Bridge (Transparent) mode authentication** (see Figure 61).



Note: Auto-Login requires precise configuration in order to work properly. Please check the iPrism Knowledgebase for up-to-date information.

http://www.stbernard.com/products/support/iprism/help_6-4/iprism.htm

Using Auto-Login in Proxy Mode

Auto-Login capability is implemented differently in proxy mode than in bridge (transparent) mode. Here, it is not an extension of the IP-mapped authentication, but rather a session-based authentication system which authenticates on a per-connection basis. By using the same credentials that were used to log in to the workstation and authenticating against the same domain controller, Auto-Login can uniquely identify users and securely apply the correct profile to their browsing session. To make this work, Internet Explorer and Firefox open a number of socket connections to iPrism, each of which must succeed the authentication process. These connections can then transfer any number of URL requests without re-authenticating.

Not using a connection for more than a minute will usually cause the browser to close the connection, but it will automatically open and authenticate more connections as necessary. Most browsers use one to four active connections, depending on the amount of URL traffic being transferred.

For Auto-Login to work in proxy mode, the following network/system requirements must be met:

- Internet Explorer v5.0 (or later), and iPrism v3.4 (or later).
- Firefox (all versions).
- The browser must be configured to use iPrism as a proxy. See “Configuring Browsers for Authentication” on page 249.
- Workstations must participate in and log into a Windows domain. iPrism must have a shared trust in this same domain.

- NTLM authentication must be enabled, configured, and operational on iPrism. See “Configuring Browsers for Authentication” on page 249.
- In the **Networks** section of Users & Networks (see “Networks” on page 57), authentication must be set to **Manual-Login (Basic Authentication)** in **Proxy (single-interface) mode authentication** (see Figure 62) . This is necessary to support software that does not, or cannot, support NTLM authentication.

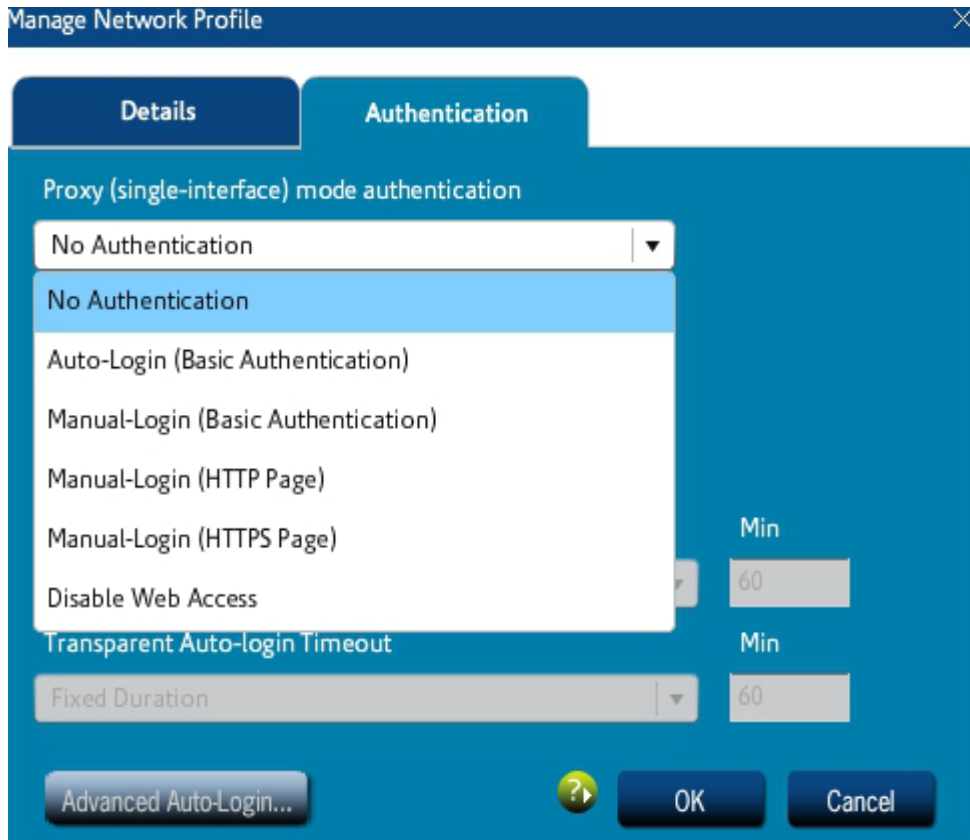


FIGURE 62. Proxy Mode authentication

Auto-Login can be enabled simultaneously for both proxy mode and bridge (transparent) mode operation, as long as the network/system requirements for each configuration are met.

Authentication from the User's Perspective

When a user first accesses the Internet, s/he will be automatically authenticated if Auto-Login is enabled and functioning. Otherwise, s/he will see an authentication page (Figure 63).

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**.

STBERNARD ™

iPrism®

iPrism Authentication

You are required to authenticate.

User Name

Password

Session timeout

Authenticate

You can bookmark this link and select it to end your session before it times out.
[iPrism Logout](#)

FIGURE 63. Transparent Authentication Login

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** (Figure 64).
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.)
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.



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.



Important: 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)

Authentication Mode and Status

Authentication Mode
Server 2000/2003

Domain Settings

NT Domain
IPDEV

Active Directory Realm
[Empty field]

Machine Account
[Red box around field]

Username
[Empty field]

Advanced Settings

Domain Controller(s)
[List with one entry]

Add Edit Delete

Password
[Empty field]

FIGURE 64. Enabling Active Directory 2000/2003 Authentication

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 **Advanced Settings** (Figure 65).
10. If your network is configured to use NetBIOS protocol, check **Enable NetBIOS**.
11. The LMHosts file provides a mapping between IP address and NETBIOS computer names for networks without WINS Servers (or networks with broken WINS Servers). If you have a LMHosts file on your workstation, you can transfer it to the iPrism by checking **Enable LMHosts**, then clicking **Import** and selecting the LMHosts file from the window that appears. You can also edit this file manually by clicking **Edit**, which brings up an editing window.

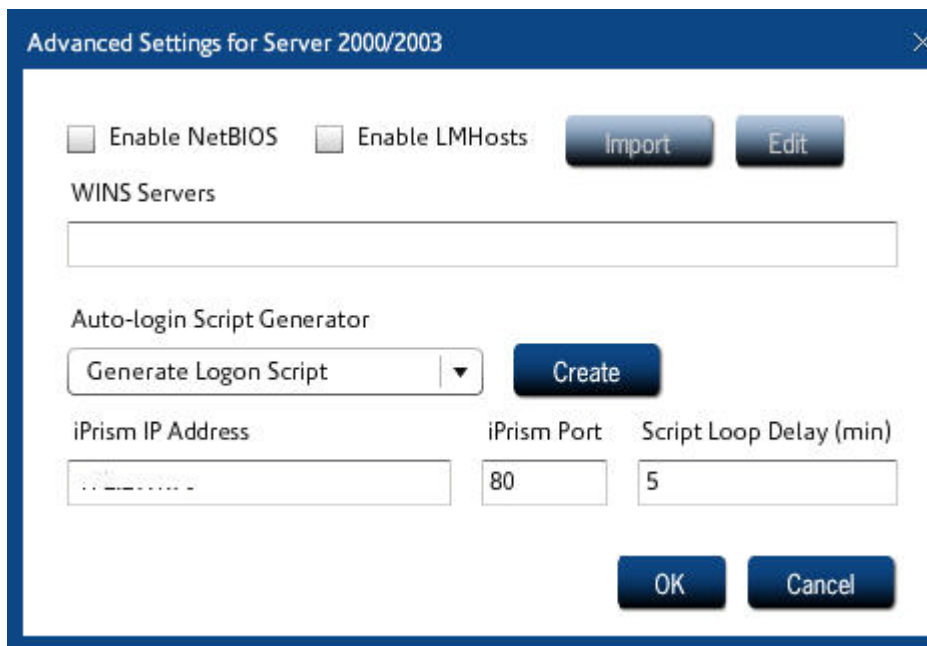


FIGURE 65. Advanced Settings

12. If you are using WINS servers, type their IP addresses in the **WINS Servers** field. Multiple IP addresses must be separated by commas.

The **Auto-Login Script Generator** allows the generation of the logon/logoff scripts for deployment to users. Bridge (transparent) mode filtering configurations can benefit from client-side logon/logoff scripts. They support immediate Windows authentication to iPrism when users log on to their workstations. This provides up-front user identification without requiring web browsing to establish the authenticated session with iPrism, providing timelier authentication for bridge (transparent) mode users.

For example, a user can be profiled/reported-on by username for an application without the user browsing the Internet first to establish an authenticated iPrism session. Another benefit is that the first browsed website may now be an HTTPS (secure) website, which will be profiled by username, instead of IP address. Basic requirements for successfully using these scripts are as follows:

- Windows Authentication and Transparent-Mode Auto-Login are working.
- Transparent Auto-Login Timeout compatibility check.
- Script generation using iPrism.

For more information, refer to the Auto-Login tech-note on the iPrism support web page:
[http://www.stbernard.com/products/support/iprism/
support_iprism-tnotes.asp](http://www.stbernard.com/products/support/iprism/support_iprism-tnotes.asp)

13. Select whether to **Generate Login Script** or **Generate Logoff Script**.
14. To create a script, click **Create**.
15. If the Auto-Login redirection setting is configured to resolve iPrism's IP address using DNS, an **iPrism DNS Name** should be displayed.
 - The **iPrism Port** defaults to 80. If you are using a different port number for HTTP, you may change this value.
 - The **Script Loop Delay** (minutes) determines the frequency of user authentication by the iPrism logon script. The default is 5 minutes.
16. Click **OK**.
17. Click **Join**.
18. Save your configuration by clicking **Save**.
19. 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 .



FIGURE 66. Authentication Mode & Status

20. Set up your clients' browsers. For instructions on specific browsers, refer to the following articles in Appendix B:

“Configuring Firefox for Authentication” on page 250

“Configuring Safari for Authentication (Mac OS X only)” on page 252

“Configuring Netscape Navigator for Authentication” on page 254

“Configuring Internet Explorer for Authentication” on page 255



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” on page 51.

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 Figure 67. For a description of how the Active Directory (AD) environment works in general, refer to the iPrism Knowledgebase at www.stbernard.com/products/support/iprism/help/iprism.htm

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 beginning on page 137.

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.

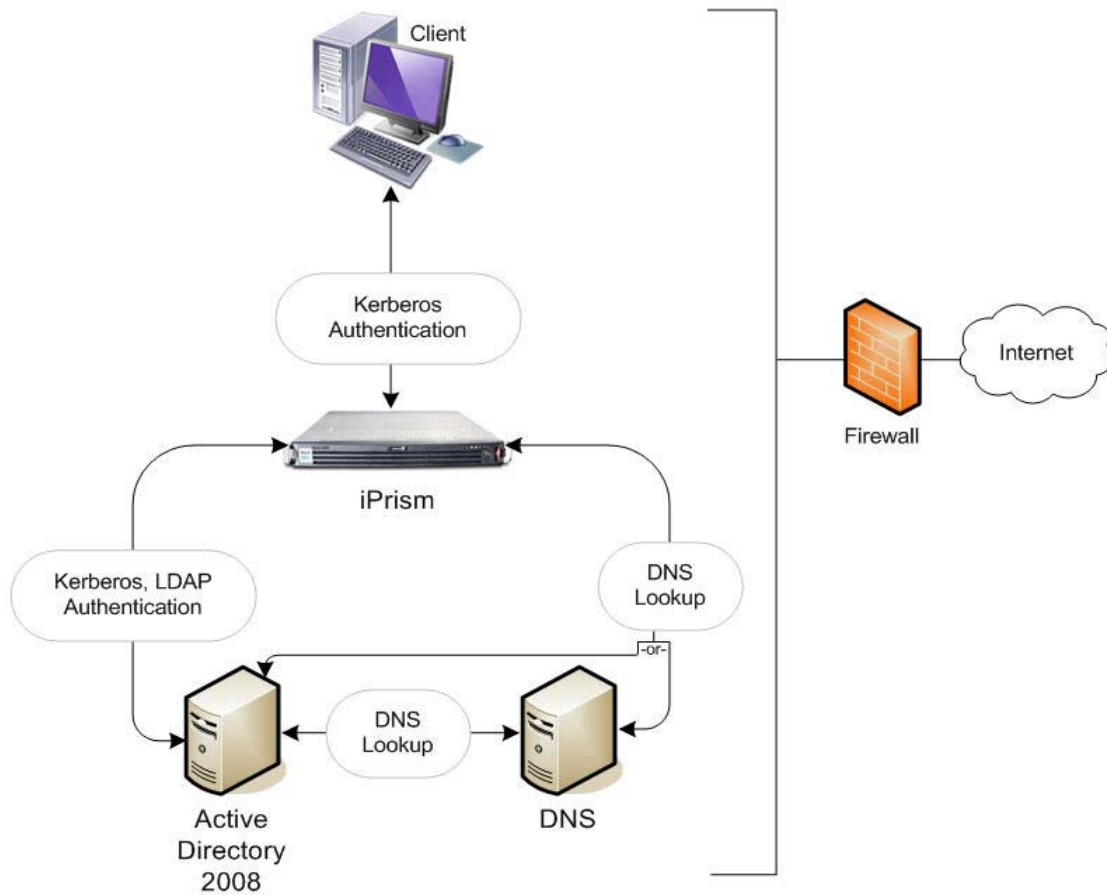


FIGURE 67. Active Directory 2008 authentication



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**.

The screenshot displays a configuration window with three main sections:

- Authentication Mode and Status:** A dropdown menu is set to "Server 2008".
- Domain Settings:** Fields for "NT Domain" (IPDEV), "Active Directory Realm", and "Machine Account" (highlighted with a red border). A list of "Domain Controller(s)" is shown with "Add", "Edit", and "Delete" buttons. A "Password" field is also present. An "Advanced Settings" button is at the bottom left of this section.
- Auto-login Redirection Settings - only relevant in Bridge (transparent) mode:** A dropdown menu is set to "DNS". A note states: "Requires iPrism host entry into all participating network zones."

At the bottom of the window are "Join" and "Cancel" buttons.

FIGURE 68. Enabling Active Directory 2008 Authentication

3. From the **Authentication Mode** dropdown list, choose **Server 2008** (Figure 68).
4. Your NT Domain, Active Directory Realm, Machine Account, and Domain Controllers will be populated. You can change any of these if necessary.



Note: 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 again.

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.



Important: 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 .



FIGURE 69. Authentication Mode & Status

13. Set up your clients' browsers. For instructions on specific browsers, refer to the following articles in the Knowledgebase:
 - “Configuring IE for proxy mode Auto-Login”
 - “Configuring IE for transparent mode Auto-Login”
 - “Configuring Firefox”



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” on www.stbernard.com/products/support/iprism/help/iprism.htm

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://www.stbernard.com/products/support/iprism/ers.asp>

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. In order to use this feature, you will need a system with a syslog client running and configured to accept events from an external source.⁷

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, do the following:

1. From the iPrism Home Page, select **System Settings**, then **Event Logging**.
2. Check **Enable event logging using Syslog** (see Figure 70).

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

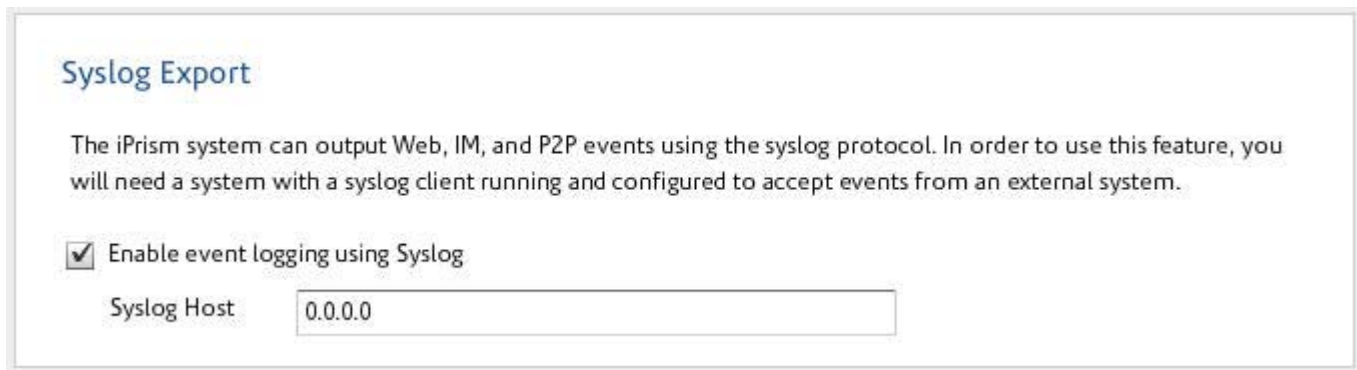


FIGURE 70. Event Logging – Syslog Export

3. Type the IP address of the host which will receive the logging information in the **Syslog Host** field.
4. Click **Save**, then click **Activate Changes** to activate these 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, do the following:

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

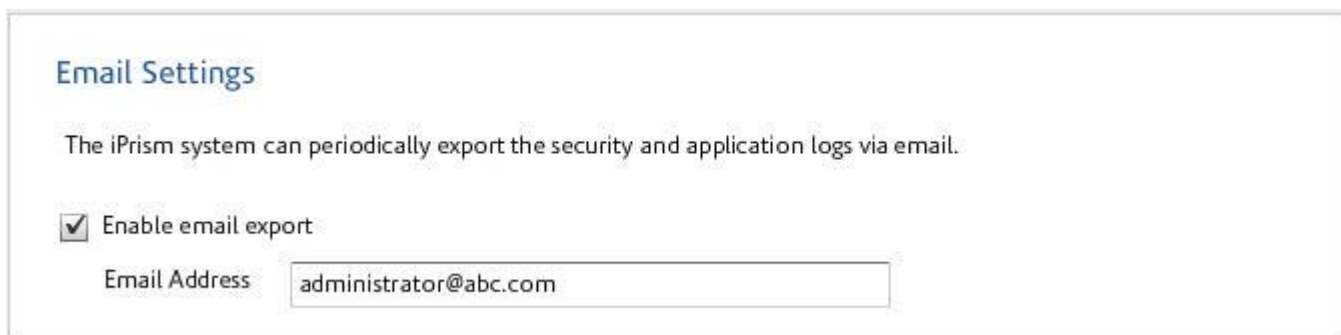


FIGURE 71. Event Logging – Email Export

3. Type the email address that will receive the logs.

4. Click **Save**, then click **Activate Changes** to activate these 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 security and application log 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 72. Event Logging – FTP Settings

3. Type the FTP Host, FTP Directory, FTP Username, and FTP Password in their respective fields.
4. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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**.

Registration information

Organization Name	Administrator Name	Administrator Email
<input type="text"/>	<input type="text"/>	<input type="text"/>
City	State	Country
<input type="text"/>	<input type="text"/>	<input type="text"/>

Upload License Key

Key: Subscription expires: 13 Jul 2011
Feature Key: Subscription expires: 13 Jul 2011 (Remote Filtering)



SSL Certificate

Common Name:

The self-signed certificate installed is valid.

FIGURE 73. Registration, License Key and SSL Certificate information

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. Click **Save**, then click **Activate Changes** to activate these changes immediately.

Creating the iPrism server certificate and installing a trusted server certificate

You must complete these steps before uploading a license key.

1. 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, complete the following steps:

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.

See “Common Name Recommended Values” on page 146.

SSL Certificate

Common Name:

A Certificate was successfully uploaded.

SSL Certificate

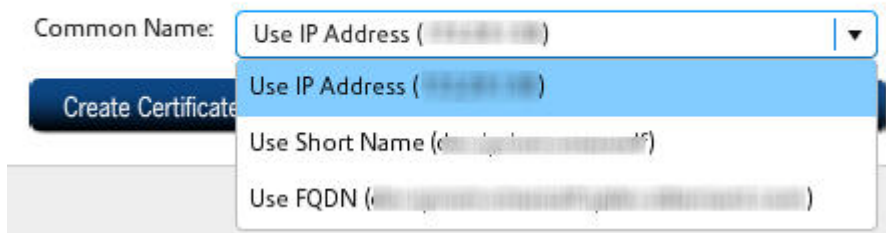


FIGURE 74. SSL Certificate options

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

- 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 to log in again.
- For a detailed example of how to request and install a trusted server certificate, refer to *Requesting and installing a trusted server certificate* section in the following iPrism Knowledgebase article:
http://www.stbernard.com/products/support/iprism/help_6-4/iPrism/Networking/Sessions-Clients/Https/Authentication/IP0325.htm
- You may also want to review the *Avoiding browser warnings when using a self-signed certificate* section in the above Knowledgebase article.

Uploading your license key

- To upload your iPrism license key and Remote Filtering feature key from a local file, click **Upload License** and locate the file containing these keys. If it is valid and uploads successfully, you will receive a confirmation message.



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

Using Local Categories

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** (see page 24), 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
local7	User defined values
local8	User defined values
local9	User defined values
local10	User defined values
local11	User defined values
local12	User defined values
local13	User defined values
local14	User defined values
local15	User defined values
local16	User defined values

FIGURE 75. Local Categories

Network ID

In the Network ID window (Figure 76), 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** (Figure 76).

The screenshot displays the Network ID configuration interface, organized into several sections:

- Identity:** Features a text field for "Host Name (Fully Qualified Domain Name)" containing "10.10.10.10" and a "Mode" dropdown menu set to "Proxy (single-interface)".
- Internal Interface:** Includes fields for "IP Address" (192.168.1.1), "Netmask" (255.255.255.0), a "Mode" dropdown set to "auto", and an "MTU" field set to 1500.
- External Interface:** Shows a "Mode" dropdown menu set to "Disabled".
- Management Interface:** Includes fields for "IP Address" (0.0.0.0), "Netmask" (0.0.0.0), a "Mode" dropdown set to "Disabled", and an "MTU" field set to 1500.
- Name Servers:** Contains a checked checkbox for "DNS fallback to root", a table with one entry for "Forwarder" (192.168.1.1), and "Add", "Edit", and "Delete" buttons.
- Routing:** Features a "Default Route" field (192.168.1.1), a "Static Routes" button, and a checkbox for "Listen to RIP updates" which is currently unchecked.

FIGURE 76. Network ID

2. In the **Host Name** field, type the fully qualified domain name of your iPrism host.
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 "Rear Panels" section of the *iPrism Installation Guide*.
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**).
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**.
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.



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.

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.

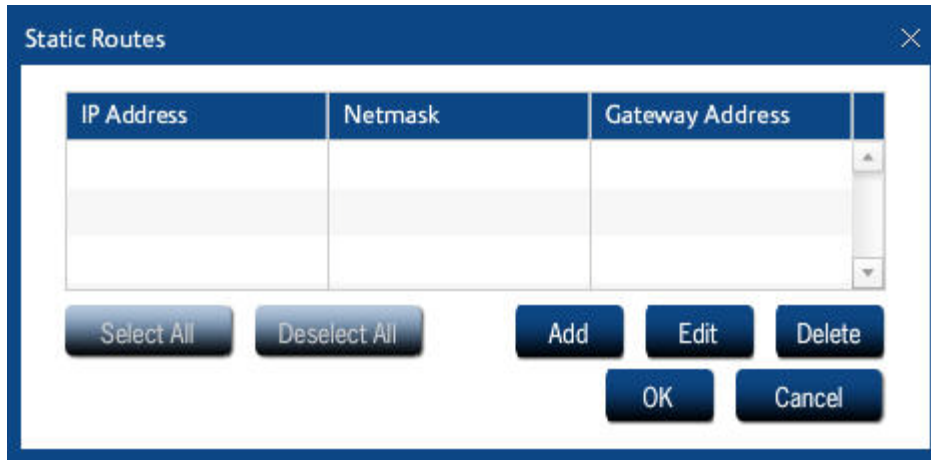


FIGURE 77. Add Static Route

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, or **Revert** to cancel.
25. Click **Activate Changes** to activate these 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:

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

Network Hardening
 Enable Denial of Service protection

SMTP Relay
SMTP Relay

SNMP
Community

Co-Management Network
Only available when iPrism is in Bridge (transparent) mode.

WCCP
Version
WCCP Router

Network Health Status
Username Password
User IP Address Domain

NOTE: When enabling this feature, use this URL address with your load balancer or other 3rd-party system to check the network status of your iPrism: <http://.../nethealthcheck>.
If the connection succeeds then OK will be reported, conversely, if the connection fails then ERROR will be reported.

FIGURE 78. 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, do the following:

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 79. 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 **System Settings**, then **Network Services**.
2. In the **SNMP** frame, check **Enable**.

The community string is now available.



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

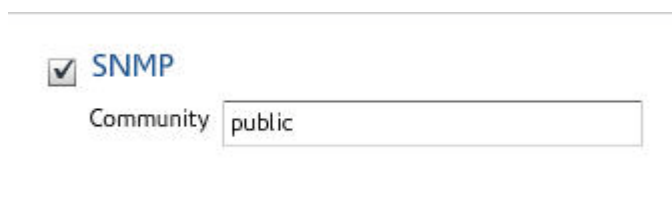


FIGURE 80. Enabling SNMP

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.
3. In the **Router** dropdown list, select the IP address of your router, or, if you need to add a Router, click **Add**.
4. Set the WCCP password by clicking **Set Password**, as shown in Figure 82.

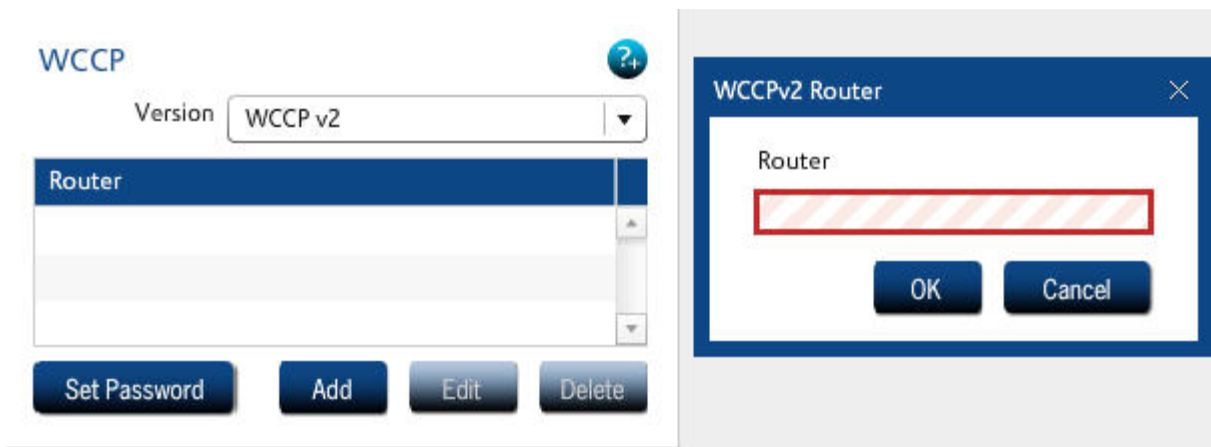


FIGURE 81. WCCP selection

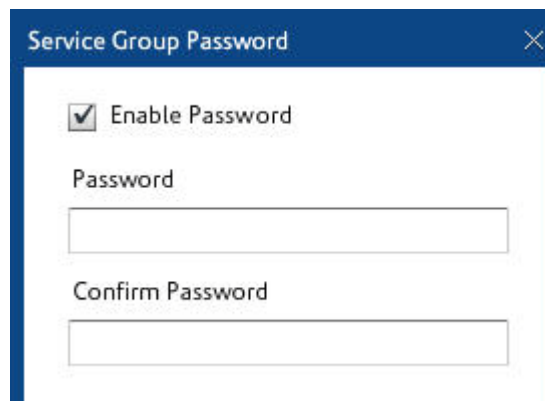


FIGURE 82. Set Service Group Password



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

http://www.stbernard.com/products/support/iprism/help_6-4/iprism.htm

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.
3. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

SMTP Relay

SMTP Relay

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**.
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.

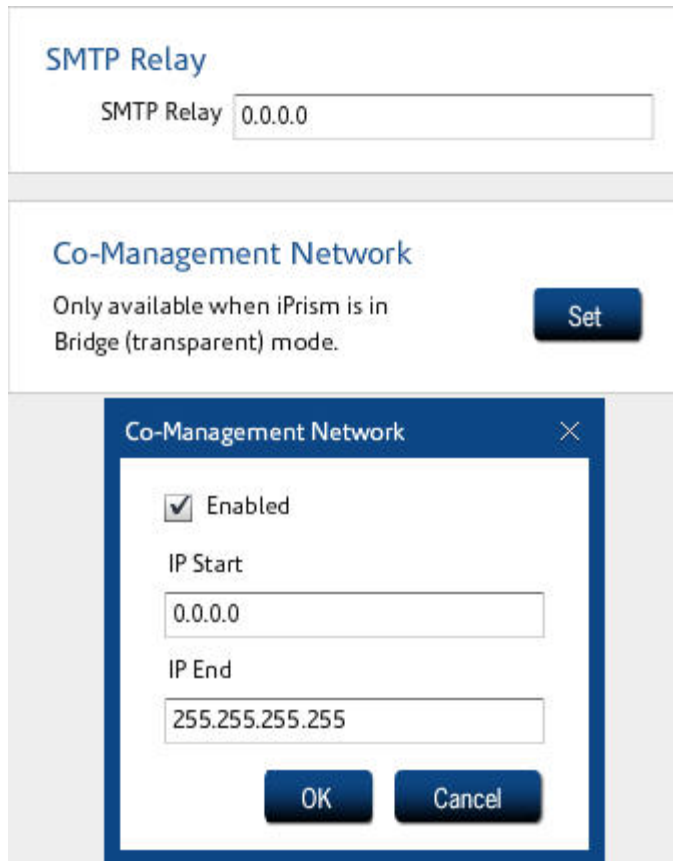


FIGURE 83. Co-Management Network

5. Click **OK** to save your changes, or **Cancel** to cancel.
6. Click **Save** to save your changes, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

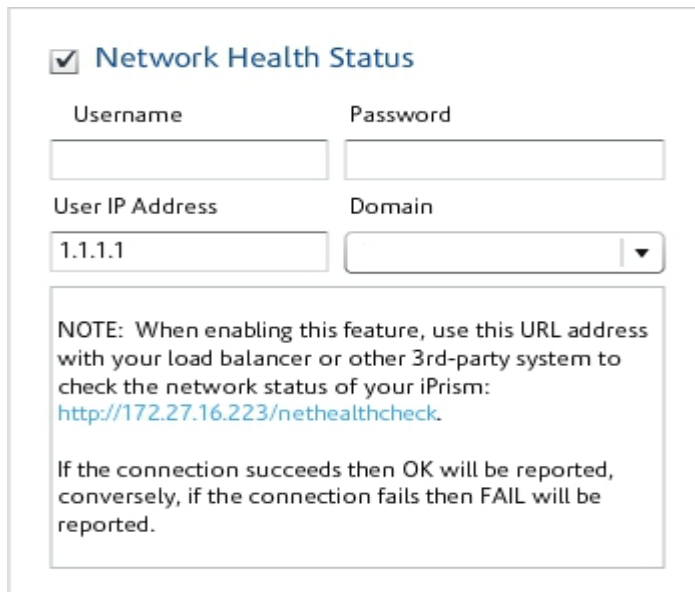


Note: You must click **Save** at the bottom of the Network Services window to apply your changes to iPrism.

Checking iPrism Status

You can check the connection status to and load balancing of an iPrism by doing the following:

1. To check the status and load balancing of your iPrism, check **Network Health Status**.
2. Enter the username, password, and IP address of the iPrism whose status you want to check.
3. If necessary, select a domain from the Domain dropdown list.
4. When you are done with the Network Services window, click **Save**.



The screenshot shows a configuration window titled "Network Health Status" with a checked checkbox. It contains four input fields: "Username" and "Password" (text boxes), "User IP Address" (text box with "1.1.1.1" entered), and "Domain" (dropdown menu). Below the fields is a note box with the following text: "NOTE: When enabling this feature, use this URL address with your load balancer or other 3rd-party system to check the network status of your iPrism: <http://172.27.16.223/nethealthcheck>. If the connection succeeds then OK will be reported, conversely, if the connection fails then FAIL will be reported."

FIGURE 84. Network Health Status

5. In your load balancer or other third-party system, type the URL noted in the Network Health Status window as shown above ([http://\[your iPrism IP address\]/nethealthcheck](http://[your iPrism IP address]/nethealthcheck))

Pending Request Options

When a user is surfing the Internet and receives an Access Denied message for a blocked page, s/he 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” on page 38.

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

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 three dropdown menus: "Email Address" (empty), "Maximum Outstanding Requests" (set to 30), and "Assigned Categories - Allow" (set to local allow). The right column contains three dropdown menus: "Email Preference" (set to Send requests individual), "Grant Pending Request Pri" (set to Use overrides to grant a), and "Assigned Categories - Den" (set to local deny).

FIGURE 85. 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).

Proxy and Configuration Ports

If desired, you may reconfigure the standard client proxy port of 3128, 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.

Standard Client 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.

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

Administration/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 the Proxy Port.

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`

Redirect and HTTPS Ports

Bridge (transparent) mode redirect ports: Redirect ports are ports that iPrism will filter in transparent proxy mode. By default, iPrism will only filter port 80 traffic, but more ports can be added here. Traffic on the ports configured here should be HTTP only.

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.

Ports

Proxy Port Configuration Port

Bridge (transparent) mode

Redirect Ports

Add Edit Delete

Proxy (single-interface) mode

HTTPS Ports

Add Edit Delete

FIGURE 86. Ports window

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**, then click **Activate Changes** to activate these 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 a Redirect port (Bridge (transparent) mode only)

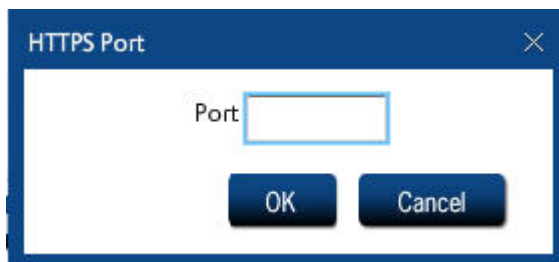
1. From the iPrism home page, select **System Settings**, then select **Ports**.
2. To add a redirect port (Transparent mode only), click **Add**.



3. Type the port number you want to use and click **OK** to save, or **Cancel** to cancel.
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** to save, or **Cancel** to cancel.
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, or **No** to cancel.
8. Click **Save**, then click **Activate Changes** to activate these 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** to save, or **Cancel** to cancel.
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** to save, or **Cancel** to cancel.
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, or **No** to cancel.



Note: You must click **Save** at the bottom of the Ports window to apply your changes to iPrism.

7. After you click **Save**, click **Activate Changes** to activate these 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 "Chapter 9: Central Management" on page 193.

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.stbernard.com/products/support/iprism/help/iprism.htm.

To Slave iPrism to a Parent Proxy (Proxy Mode)

1. From the iPrism home page, select **System Settings**, then **Network Services**.
2. In the **iPrism Proxy Mode Configuration** frame, check **Slave To**.
3. 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.

4. Type the port number of this server.
5. 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.

6. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

iPrism Proxy (Single-interface) Mode Configuration

Slave to:

Domain: Port: Disable DNS

iPrism Bridge (Transparent) Mode Configuration

Enable upstream proxy

Filter List / System Update Proxy

Filter List	Host	Port
<input type="text" value="None"/>	<input type="text"/>	<input type="text"/>
	Username	Password
	<input type="text"/>	<input type="text"/>

FIGURE 87. Proxy

To Enable an Upstream Proxy (Bridge (transparent) Mode)

1. From the iPrism home page, select **System Settings**, then **Network Services**.
2. In the **iPrism Bridge (Transparent) Mode Configuration** frame, check **Enable Upstream Proxy**.
3. Type the upstream proxy domain into the field.
4. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

To Configure the Filter List/System Update Proxy Server

1. To specify the proxy server from which filter lists and system updates are downloaded, select an option from the Filter List dropdown:
 - None**
 - Same as Parent Proxy**
 - Custom**
2. Type the host IP address and port number into their respective fields.
3. An iPrism administrator account username and password is required; type them into their respective fields.
4. When you are finished, click **Save** to save your changes, or **Revert** to cancel.
5. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

System Preferences

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



FIGURE 88. System Preferences

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 are encrypted for security.

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. In the Backup Settings frame, select an option:
 - **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.

3. Click **Save** to save your changes, or **Revert** to cancel.
4. Click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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.

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. Check **3rd Party Software Updates**.
3. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. In the Current Date and Time frame, click **Set**. (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.)
3. 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.)
4. 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.

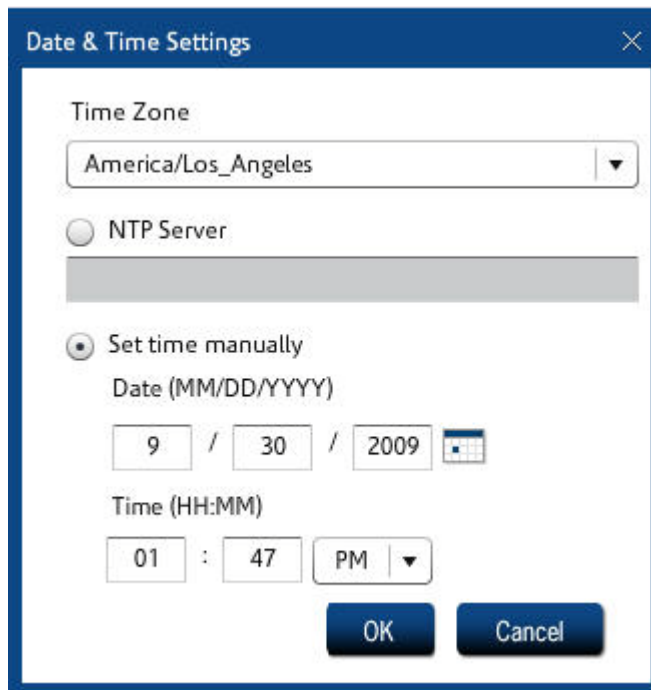


FIGURE 89. Date and Time Settings

5. 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.
6. Click **OK** to save your changes, or **Cancel** to cancel.
7. Click **Save**, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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 three days.

To configure filter failover mode, do the following:

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. 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.

3. Click **Save** to save your changes, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Setting or Changing the Supervisor Password

To set or change the password for the iPrism administrator, complete the following steps:

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. In the **Supervisor Password** frame, click **Set Password**.
3. Type a password in the **Password** field, then type the password again in the **Confirm Password** field.
4. Click **OK** to save the password.
5. 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

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. In the iGuard Updates frame, click **Update Now** to update immediately; or, 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.

3. Click **Save** to save your changes, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

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 will read “empty update”.

System Updates

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

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. In the System Updates frame, click **Settings**.

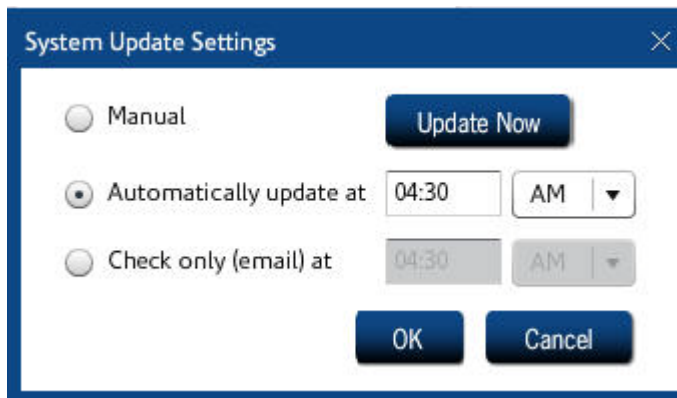


FIGURE 90. System Update Settings

3. 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., 1:30 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.
4. Click **Save** to save your changes, then click **Activate Changes** to activate these changes immediately (if you do not Activate Changes now, you will be prompted to do so before logging out of iPrism).

Proxying for External Users

To allow external (e.g., remote) users to connect to iPrism as a proxy server, complete the following:

1. Check **Enable proxy to iPrism**.



FIGURE 91. Proxying for External Users

2. Click **Settings**.

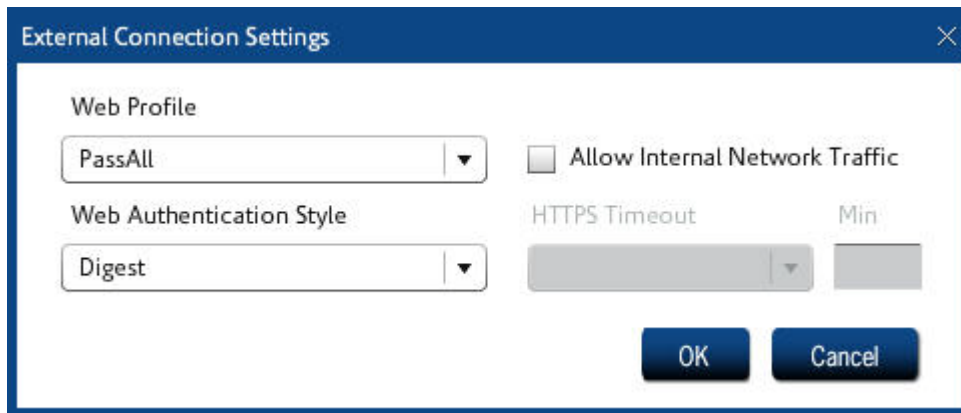


FIGURE 92. External Connection Settings

3. To set the web profile that will apply to all external users who proxy to iPrism, select either **PassAll** or **BlockOffensive** from the Web Profile list.

4. To select the type of authentication style that will apply to all external users who proxy to iPrism, select a Web Authentication Style from the list.



Note: Currently, the only available option is **Digest**.

5. If you also want to allow these external users to proxy to iPrism for internal network traffic, check **Allow Internal Network Traffic**.
6. When you are finished, click **OK**.
7. When you are finished with all System Preferences, click **Save** to save your changes.

Unrated Pages (iARP)

allows iPrism to 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 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 .
1. From the iPrism home page, select **System Settings**, then **Unrated Pages** (Figure 93).
 2. Check whether you would like to automatically send unrated URLs to .
 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, or **Revert** to cancel.
6. Click **Activate Changes** to activate these 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 St Bernard'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 93. Unrated Pages

User Settings

In **System Settings > User Settings**, the administrator can adjust the settings for dialog prompts that are displayed when certain actions are taken (e.g., a dialog prompt that asks the user if they are sure they want to delete an item, such as the example shown below).

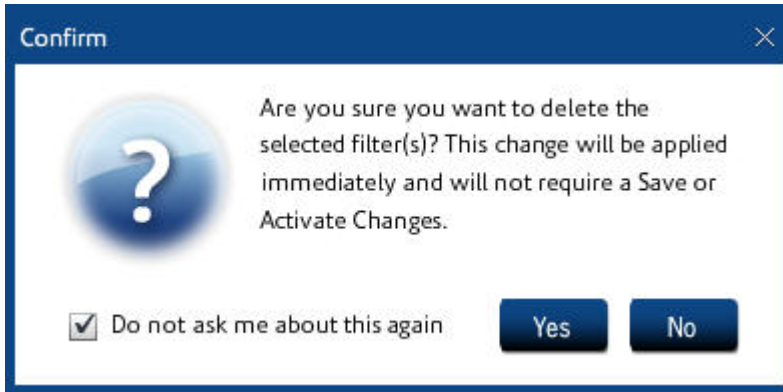


FIGURE 94. Dialog prompt example

If the administrator clicks **Reset** in **System Settings > User Settings** (shown below), all dialog prompts are reset to factory settings; e.g., in the example shown above, if the user has checked **Do not ask me about this again**, that setting will now be cleared and all dialog prompts will again be shown.



FIGURE 95. Reset dialog prompts

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

About: page 180

Administration Log: page 181

Configuration Summary: page 182

Connectivity: page 184

Routing Table: page 187

Security Log: page 188

Status: page 190

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 St. Bernard Software Sales and Technical Support.

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

System Information

Hardware Model	10
Serial Number	██████
Version	6.401
System Build	WHITNEY3-1042
Protocol Version	49

St. Bernard Software Contact Information

Sales Information

Phone	1-800-782-3762
Fax	858-676-2299
Email	sales@stbernard.com

Support Information

Phone	858-676-5050
Fax	858-676-5055
Email	jprism-support@stbernard.com

© 2000-2009 St. Bernard Software, Inc. All rights reserved.

FIGURE 96. About iPrism

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.

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

The Administration log records actions of iPrism Administrators.

Date	Time	Event
2009-10-02	11:58	User 'iprism' Activated Configuration.
2009-10-02	11:57	User 'iprism' set 'committed' to '1'
2009-10-02	11:52	User 'iprism' Logged in.
2009-10-02	11:51	User 'iprism' Logged out.
2009-10-02	11:26	User 'iprism' Logged in.
2009-10-01	18:06	User 'iprism' Logged out.
2009-10-01	16:58	User 'iprism' Joined domain.
2009-10-01	16:56	User 'iprism' Discarded changes.
2009-10-01	15:44	User 'iprism' Logged in.
2009-10-01	11:43	User 'iprism' Activated Configuration.
2009-10-01	11:43	User 'iprism' set 'committed' to '1'
2009-10-01	11:43	User 'iprism' set 'vendor/updates/update_action' to '0'
2009-10-01	11:43	User 'iprism' set 'vendor/updates/system_update_time' to '01:30 AM'
2009-10-01	11:43	User 'iprism' set 'vendor/updates/filter_update_time' to '02:00 AM'

FIGURE 97. 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.

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

Provisioning	
License registration key	[REDACTED]
Serial number	[REDACTED]
License expiration date	2009-12-02
iPrism version	6.400
Third party software updates	no
Enable global policy viewer	no
Organization name	St. Bernard Software
Organization city	San Diego
Organization state	CA
Organization country	US
Administrator name	[REDACTED]
Administrator email	[REDACTED]
Date/time	
Timezone	America/Los_Angeles
Timezone Offset	-25200
NTP server	0.0.0.0
Hostname	[REDACTED]
DNS	
DNS server(s)	[REDACTED]
DNS server(s)	[REDACTED]
Resolver	[REDACTED]
Forward to root	no
Disabled	no
Default gateway	[REDACTED]
Listen to RIP updates	no
Enable bridging/transparent mode	bridge
Software failover action	disabled
SMTP relay host	0.0.0.0
Enable DOS prevention	enabled
Internal interface	
IP address	[REDACTED]
Netmask	255.255.255.0
Speed	auto
MTU	1500
External interface	
IP address	0.0.0.0

[Save As](#) [Print](#)

FIGURE 98. 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.

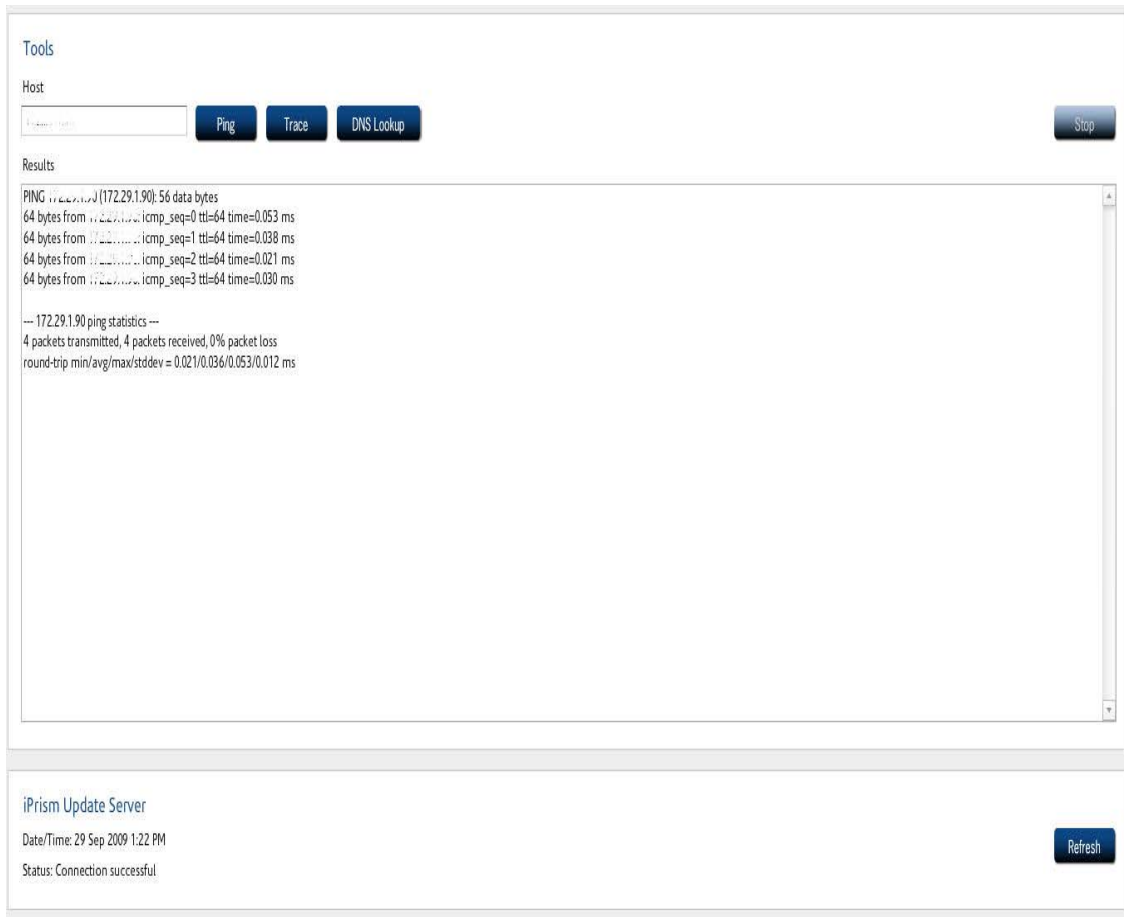


FIGURE 99. Connectivity Window

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

To ping 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 will be displayed in the **Results** frame.

Tools

Host

Ping

Trace

DNS Lookup

Results

```
PING 192.168.1.1: 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=0.063 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.043 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.043/0.049/0.063/0.008 ms
```

FIGURE 100. Ping

To trace 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.

To 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**.
3. A DNS lookup will be performed and the results will display in the **Results** frame (see Figure 101).

Tools

Host

Ping

Trace

DNS Lookup

Results

```
; <<> DiG 9.3.0 <<>
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 12868
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;                IN  A

;; AUTHORITY SECTION:
.                10800  IN  SOA A.ROOT-SERVERS.NET. NSTLD.VERISIGN-GRS.COM. 2009102600 1800 900 604800 86400

;; Query time: 26 msec
;; SERVER:
;; WHEN: Mon Oct 26 10:11:48 2009
;; MSG SIZE rcvd: 104
```

FIGURE 101. DNS Lookup Results

To refresh 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 173.

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.

1. From the iPrism home page, select **System Status**, then **Routing Table**.
2. A list of the network routes is displayed. To refresh the list, click **Refresh**.

Network Routes

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	192.168.1.1	UGS	0	145206	em0	
192.168.1.0	192.168.1.1	UH	0	59515	lo0	
192.168.1.1	link#1	UC	0	0	em0	
192.168.1.2	00:10:db:ff:20:00	UHLW	1	1	em0	1039
192.168.1.3	00:1b:c0:51:94:80	UHLW	0	0	em0	1091
192.168.1.4	00:07:e8:20:8d:5a	UHLW	0	10	lo0	

FIGURE 102. Default Routes

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.

1. From the iPrism home page, select **System Status**, then **Security Log**.
2. 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 will read “empty update”.

The security log records and lists iPrism Status, Configuration and Relevant User Activity. Refresh Clear

iPrism Security log

[1] Filter List Age
Incremental filter list is 8 hours old [lifr.update.091022-091025.igz]
Base filter list is 3 days old [stafr.091022.gz]

[2] Last configuration changes
Last configuration saved : 72 hours ago
Last system upgrade : Thu Oct 22 08:58:12 2009

[3] Last Backup
No backup performed yet

[4] Last successful remote filtering policy delivery to portal
Remote Filtering Status: Disabled
Policy Last Delivered: [never]

[5] Unauthorized IP accesses, Email Alerts, Overrides and Automatic Reports

2009-10-25 04:51:05 1256471465	Authorized attempt to access configuration services from 172.27.3.90:60536
2009-10-25 04:51:56 1256471516	Authorized attempt to access configuration services from 172.27.3.90:60536
2009-10-25 04:56:55 1256471815	Authorized attempt to access configuration services from 172.27.3.90:34406
2009-10-25 04:57:06 1256471826	last message repeated 5 times
2009-10-25 04:57:06 1256471826	Authorized attempt to access configuration services from 172.27.3.90:34429
2009-10-25 04:57:06 1256471826	last message repeated 2 times
2009-10-25 04:57:06 1256471826	Authorized attempt to access configuration services from 172.27.3.90:34406
2009-10-25 04:57:07 1256471827	Authorized attempt to access configuration services from 172.27.3.90:34429
2009-10-25 04:57:07 1256471827	last message repeated 2 times
2009-10-25 04:57:07 1256471827	Authorized attempt to access configuration services from 172.27.3.90:34432
2009-10-25 04:57:08 1256471828	last message repeated 5 times
2009-10-25 04:57:08 1256471828	Authorized attempt to access configuration services from 172.27.3.90:34436
2009-10-25 04:57:08 1256471828	last message repeated 5 times
2009-10-25 04:57:08 1256471828	Authorized attempt to access configuration services from 172.27.3.90:34438
2009-10-25 04:57:09 1256471829	last message repeated 5 times
2009-10-25 04:57:09 1256471829	Authorized attempt to access configuration services from 172.27.3.90:34440
2009-10-25 04:57:14 1256471834	last message repeated 5 times
2009-10-25 04:57:14 1256471834	Authorized attempt to access configuration services from 172.27.3.90:34452
2009-10-25 04:57:14 1256471834	last message repeated 2 times
2009-10-25 04:57:14 1256471834	Authorized attempt to access configuration services from 172.27.3.90:34440
2009-10-25 04:57:15 1256471835	Authorized attempt to access configuration services from 172.27.3.90:34452
2009-10-25 04:57:19 1256471839	last message repeated 2 times
2009-10-25 04:57:19 1256471839	Authorized attempt to access configuration services from 172.27.3.90:34459

Save As Print

FIGURE 103. Security Log

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.

Status

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” on page 96). All of the fields in this area are read-only. Figures 104 and 105 display the Status window; for ease of viewing, the Status window is shown in two separate screen shots.

- **Uptime:** The days, hours, and minutes that your iPrism has been continuously running.
- **System:** The amount of system memory your iPrism is consuming while running.
- **CPU:** The percentage of CPU that your iPrism is utilizing while running.
- **RAID:** Status of the RAID disk if your iPrism model contains RAID (available on iPrism models 30h, 50h, and 100h).
- **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:**
 - **Traffic received (internal interface):** Amount of IP traffic (measured in bytes, for all protocols) received by the internal interface.
 - **Traffic Received (external interface):** IP traffic received for the external interface, if one is being used (bridge (transparent) mode only).
 - **Traffic Received (management interface):** IP traffic received by the management interface, if the management interface is being used. If the management interface is not being used, Not Available will be displayed.
 - **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.

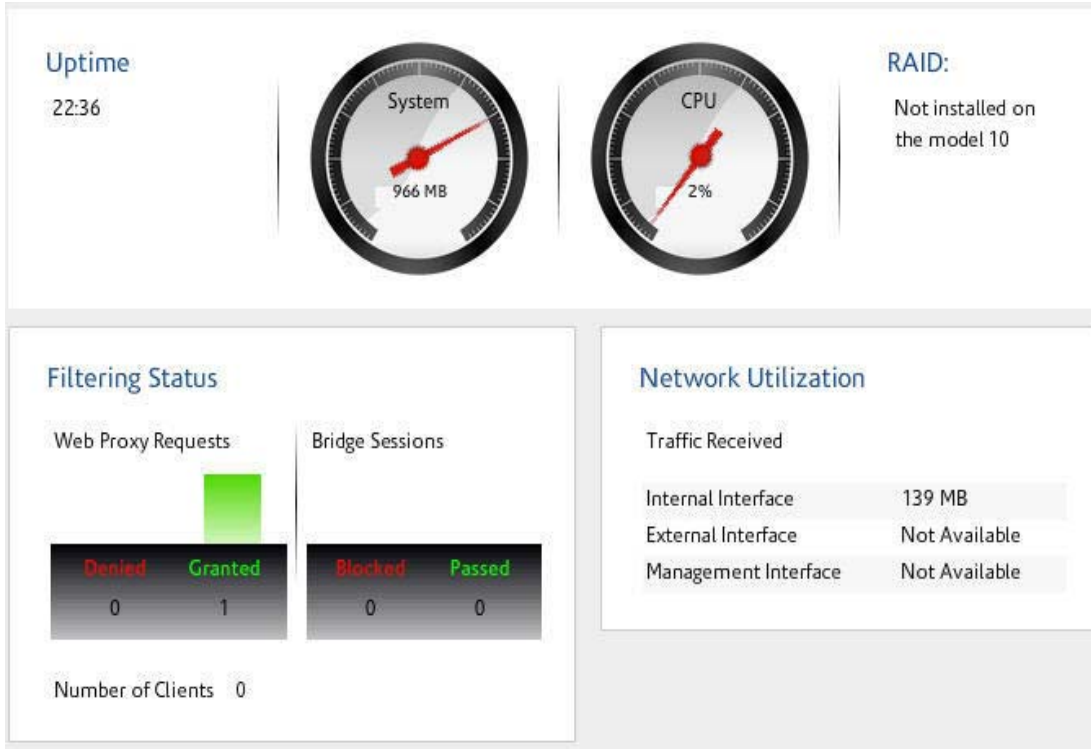


FIGURE 104. System Status window

The screenshot displays the 'System Status' window. On the left is a vertical navigation menu with the following items: About, Administration Log, Configuration Summary, Connectivity, Routing Table, Security Log, and Status (which is highlighted). The main content area is divided into three top-level status boxes: 'Filtering' (Status - Running, Size of service is 61228kb), 'Proxy' (Status - Running, Size of service is 14344kb), and 'Filter List Age' (Age: unknown, Revision: unknown). Below these is a large section titled 'Remote Filtering Server - iPrism Status'. This section contains three sub-sections: 'Log Download Status', 'Policy Upload Status', and 'Custom Filter Upload Status'. Each sub-section provides details on the last attempt and last success, including time, duration, and result codes.

Section	Item	Value
Filtering	Status	Running
	Size of service	61228kb
Proxy	Status	Running
	Size of service	14344kb
Filter List Age	Age	unknown
	Revision	unknown
Remote Filtering Server - iPrism Status	Log Download Status	
	Last Attempt:	
	Time:	9 Nov 2010 2:47 PM
	Duration:	1
	Result Code:	Success
	Last Success:	
Time:	9 Nov 2010 2:47 PM	
Duration:	1	
Event Count:	0	
Policy Upload Status		
Last Attempt:		
Time:	Indeterminate	
Duration:	-	
Result Code:	Success	
Last Success:		
Time:	Indeterminate	
Duration:	-	
Client exception count:	-	
Custom Filter Upload Status		
Last Success Time:	9 Nov 2010 10:40 AM	
Number of Attempts:	0	
Result Code:	Success	
Next Time to Try:	-	

FIGURE 105. System Status window

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 will be 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 only two steps to setting up a master/slave configuration, and it is recommended that they be completed in the following order:

1. Designate the slave system(s).
2. Configure the master system.

Designating Slave Systems

1. From the iPrism home page, select **System Settings**, then **Central Management**.
2. Select **Slave** from the **iPrism Mode** dropdown list (Figure 106).

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 steps 1 – 2.

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

iPrism Mode


Master iPrism Appliance

IP Address	Hostname	Last Connected
		Indeterminate

FIGURE 106. 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 (Figure 107).

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

iPrism Mode

Slave iPrism Appliances

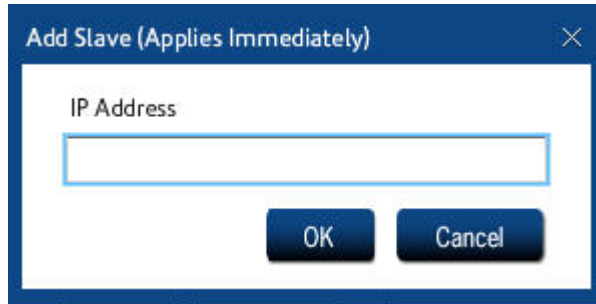
IP Address	Hostname	Last Connected

Update Slave Appliances

Update slave appliances based on the settings of the Master

FIGURE 107. Designate Master

4. The mode will be changed to Master, and you will receive a notification message when this is complete.
5. To add slaves, in the Slave iPrism Appliances frame, click **Add**.
6. Type the IP address of the slave (you must have already designated this iPrism as a slave in “Designating Slave Systems” on page 194).



7. Click **OK**. This change will apply immediately.

8. To add another slave, repeat steps 5 – 7.

Once you have designated a master system, any slave systems you added in “Designating Slave Systems” on page 194 will automatically be slaved to and synchronized with this master. If you want to update and synchronize slaves at any time, click **Update**.

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.

Notes:

- 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 chose 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.
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 (Figure 107).
 4. If you want to add slaves, follow the steps (beginning with step 5) in “Designating the Master System” on page 195.

Removing Slave System(s)

1. Log into the master iPrism.
2. From the iPrism home page, select **System Settings**, then **Central Management**.
3. All designated slave systems will be listed here 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 108).

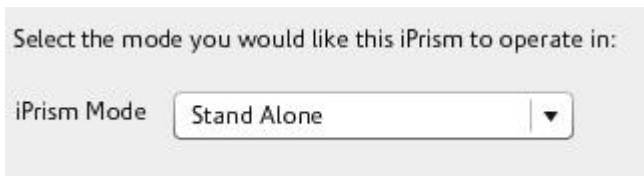


FIGURE 108. Standalone iPrism

How to Upgrade 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. It is recommended that the master and its associated slave(s) be decoupled prior to upgrading by completing the following steps.

Upgrading Decoupled Master and Slave(s)

To decouple and upgrade the master:

1. Note the IP addresses of each slave, to make 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 (Figure 108).
 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.

8. After it is complete, the master will have been upgraded.

To Upgrade the Slave(s):

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 (Figure 108).
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. After it is complete, the slave will have been upgraded. Repeat steps 1 – 7 for each slave you want to upgrade.
8. After you have upgraded each slave, add them back to the master iPrism by completing the steps in “Setting up a Master/Slave Configuration” on page 194.

Upgrading Master & Slave(s) without Decoupling

If you do not want to decouple master and slave iPrisms before upgrading, follow the steps in the KnowledgeBase article “Upgrading your iPrism”, available at www.stbernard.com/products/support/iprism/help/iprism.htm

Once you have upgraded your master iPrism, all slave(s) will be automatically synchronized and updated.

Override Management

When a browser tries to access a web page that is being blocked by iPrism, an ‘Access Denied’ page displays (see Figure 109). 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 Chapter 3: Profiles & Filters, “Web Profiles” on page 25), the user will see 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, then 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” on page 36 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 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.)



Note: A list of pending access requests can be viewed by the iPrism administrator by selecting **Profiles & Filters > Pending Requests**. See “Pending Requests” on page 38 for more information.

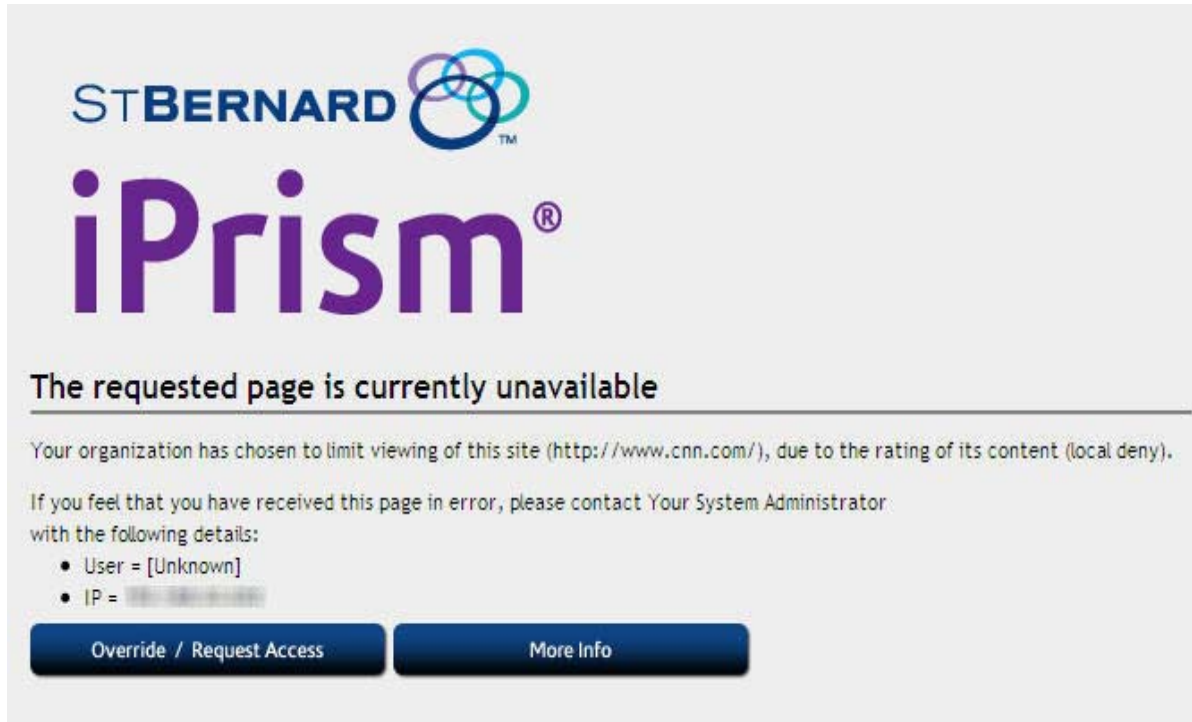


FIGURE 109. Access Denied Page

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” on page 38.

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** (Figure 109).



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 (Figure 110), select whether you want to **Override** or **Request Access** (in this example, we will use **Override**).
3. Click **Next**.

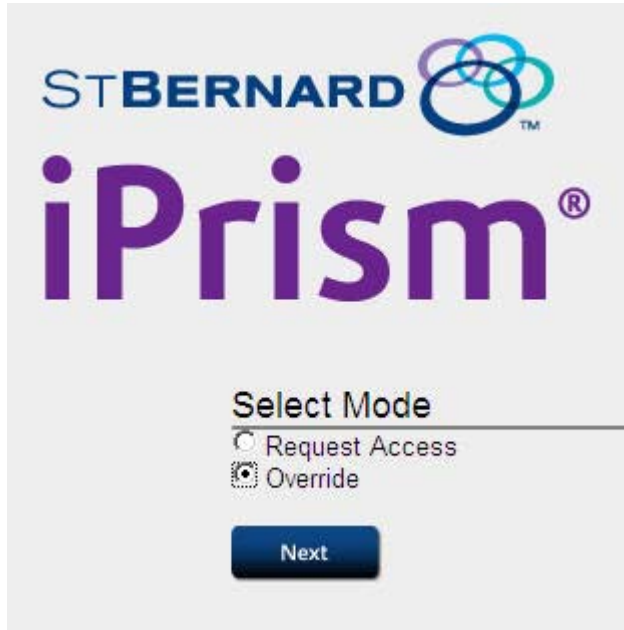


FIGURE 110. Override

4. Type your username and password in the Login screen, and click **Login**.



FIGURE 111. Login

5. On the **Override Request** page (Figure 112), select the user to whom you want to grant access so they can view the blocked site. The options that display here will 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.



FIGURE 112. Override Request

- **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” on page 25.



FIGURE 113. Override Request rejected

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 (Figure 114) 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 the **Override/Request Access** button.
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.

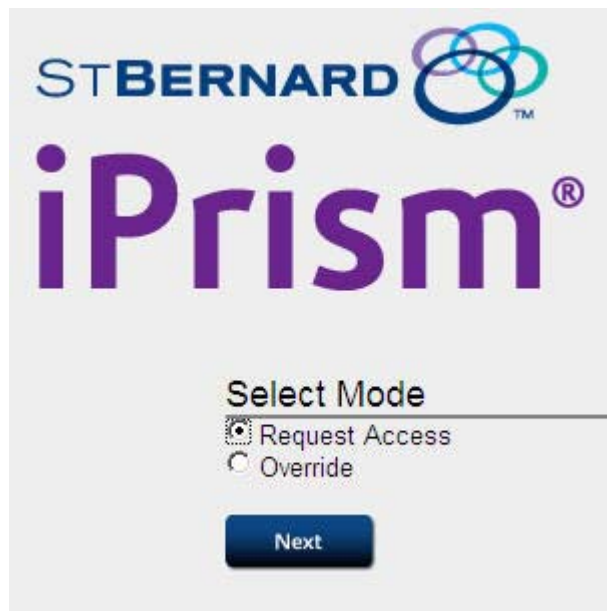


FIGURE 114. Request Access page

2. When the **Select Mode** page displays (Figure 114), select **Request Access** and click **Next**. The **Request Access** page displays (Figure 115).

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.

Request Access

Location

Your Email

Comments

Click here if you want notification of the administrator's actions.

FIGURE 115. Request Access page, part II

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 (Figure 116).

5. Review your request for accuracy; if you need to make any changes, click **Back**. Otherwise, click **Finish**.

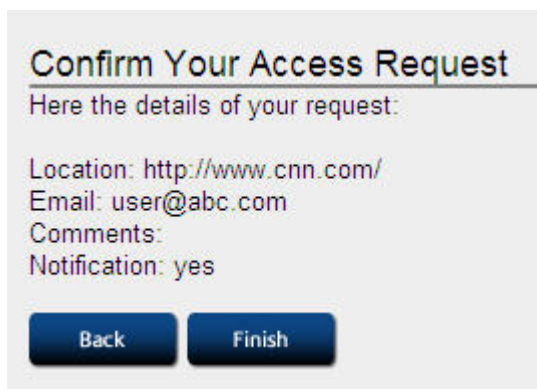


FIGURE 116. Request Access Confirmation

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” on page 38.

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” on page 36 for more information.

Filtering Categories

This appendix 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 very latest list of categories, as well as descriptions of each, you should refer to the online resource at http://www.stbernard.com/products/iprism/iguard/filtering_categories.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.victoriassecret.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 a rating of 'Adult' and 'Sexuality' is 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.tshirthell.com>

<http://www.evildam.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.dotnetsql.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.northernvirginiagop.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.dibdabdoo.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.

Note: 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 St. Bernard Software 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 "r;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 'r;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 “relax 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 "r;PG-13" profanity without a profanity rating.

Examples:

<http://www.theonion.com>

<http://www.laughgallery.com>

<http://www.fark.com>

Keywords:

jokes, humor, anecdotes

Televison/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.

Configuring Browsers for Authentication

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.)** The following procedures describe how to make the necessary proxy settings in web browsers.

Configuring Firefox for Authentication: page 250

Configuring Safari for Authentication (Mac OS X only): page 252

Configuring Netscape Navigator for Authentication: page 254

Configuring Internet Explorer for Authentication: page 255

Configuring Firefox for Authentication

1. Start up Firefox Version 3.x.
2. From within Firefox, click **Tools**, then select **Options**.

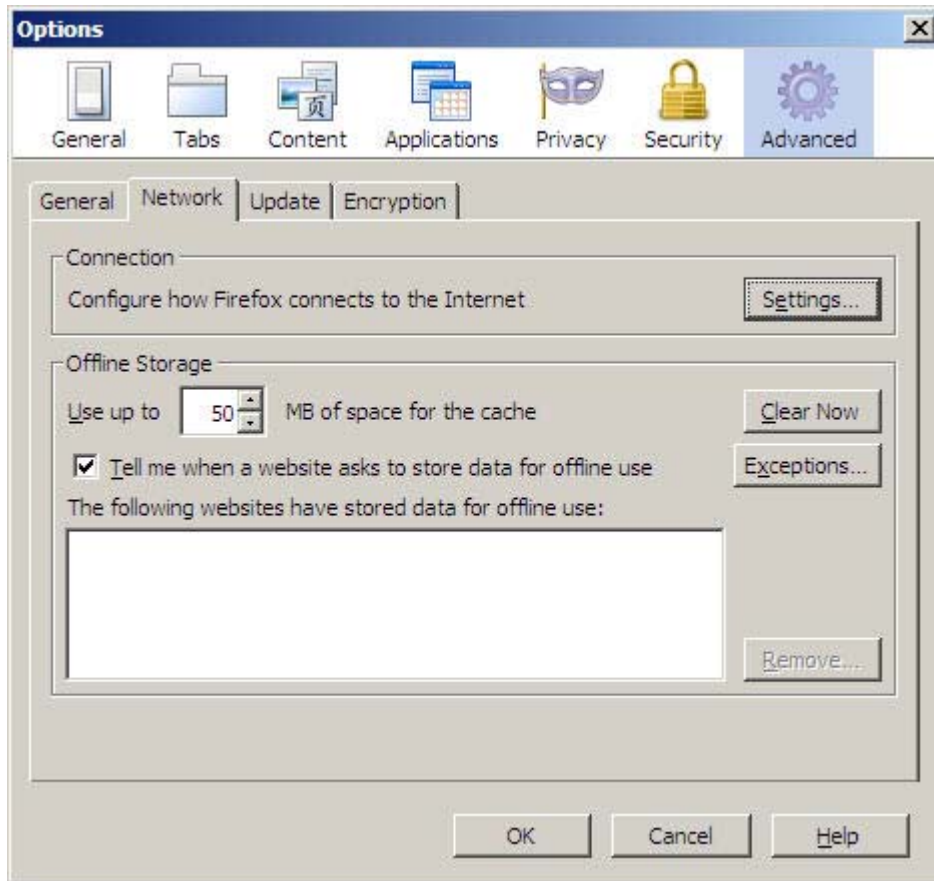


FIGURE 117. Configuring Firefox for authentication

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.

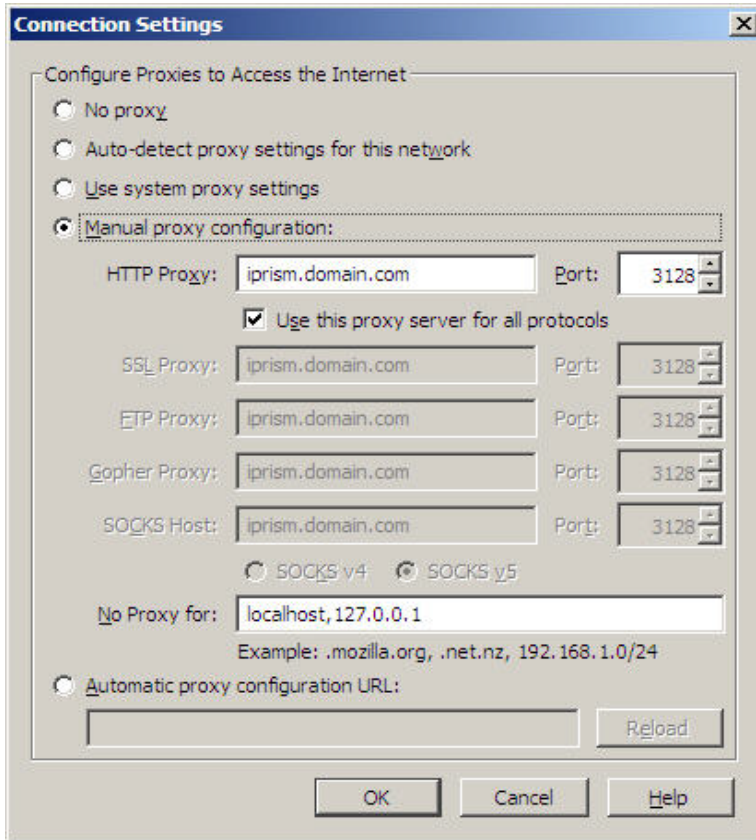


FIGURE 118. Configuring Firefox for authentication – Connection Settings

Configuring Safari for Authentication (Mac OS X only)

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**.

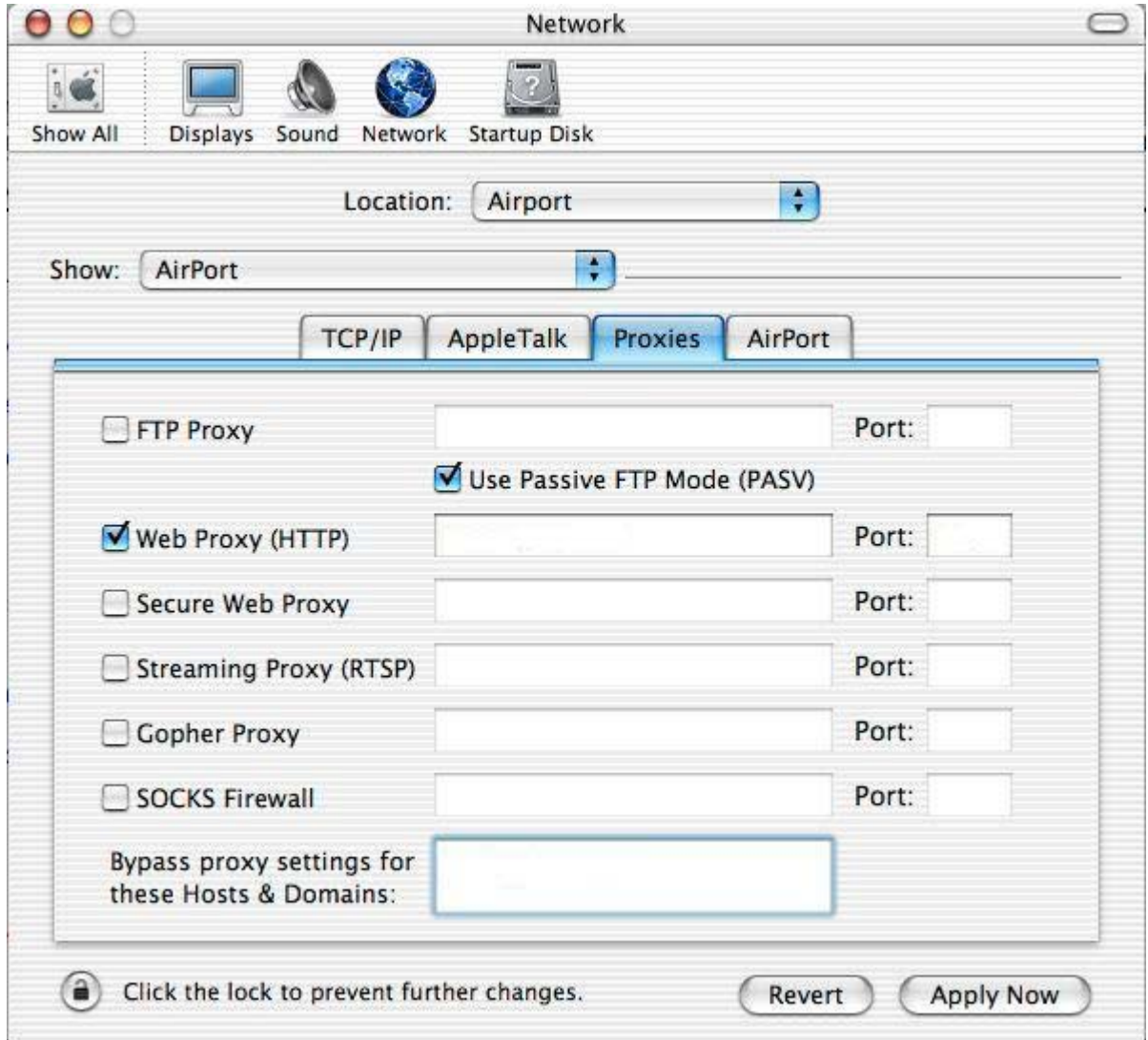
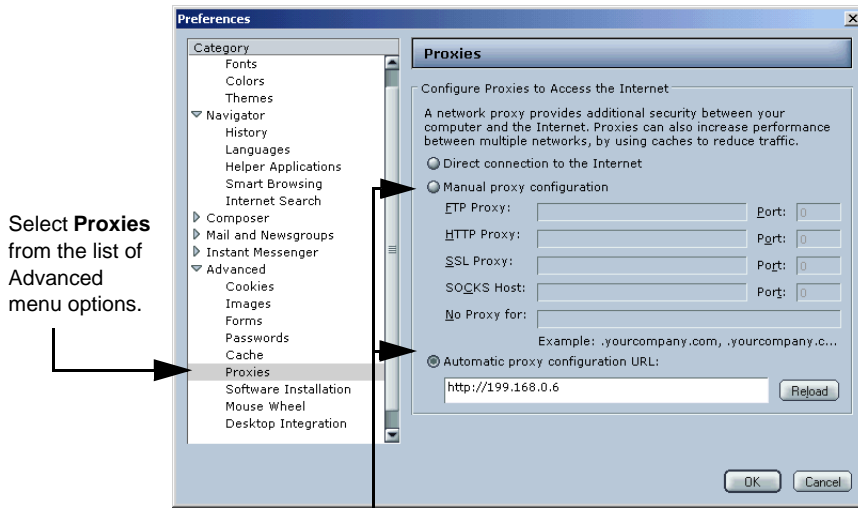


FIGURE 119. Configuring Safari for authentication

Configuring Netscape Navigator for Authentication

1. In Netscape Navigator, open the **Edit** menu and select **Preferences** to display the Preferences window.
2. In the **Category** list, double-click the word **Advanced**. This opens the **Advanced** menu so you can view the various menu options.
3. Select **Proxies** from the **Advanced** menu to display the Proxies page (see Figure 120).



Select either **Manual proxy configuration** or **Automatic proxy configuration**, then enter the IP address that you assigned to the iPrism unit in the appropriate field(s). When using the manual configuration, enter the IP address in the **FTP Proxy**, **HTTP Proxy**, and **SSL Proxy** fields.

FIGURE 120. Proxy Settings in Netscape Navigator

4. Since you will be assigning the same IP address to each protocol, you must select the **Manual proxy configuration** option.

Enter the IP address that you assigned to your iPrism server in the **FTP Proxy** field, the **HTTP Proxy** field, and the **SSL Proxy** field. In the adjacent **Port** fields, enter the value “3128” next to each proxy field. The following example shows the proxy settings for iPrism unit that has an IP address of 192.168.0.6 and is using the default iPrism port (3128).

<input checked="" type="radio"/> Manual proxy configuration			
F T P Proxy:	<input type="text" value="192.168.0.6"/>	Port:	<input type="text" value="3128"/>
H T T P Proxy:	<input type="text" value="192.168.0.6"/>	Port:	<input type="text" value="3128"/>
S S L Proxy:	<input type="text" value="192.168.0.6"/>	Port:	<input type="text" value="3128"/>
S O C K S Host:	<input type="text"/>	Port:	<input type="text" value="0"/>



Note: iPrism is not a SOCKS proxy. Leave the **SOCKS Host** field empty.

5. After entering the settings, click **OK**. Your Netscape browser is now configured to use the new proxy settings.

Configuring Internet Explorer for Authentication

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 (see Figure).

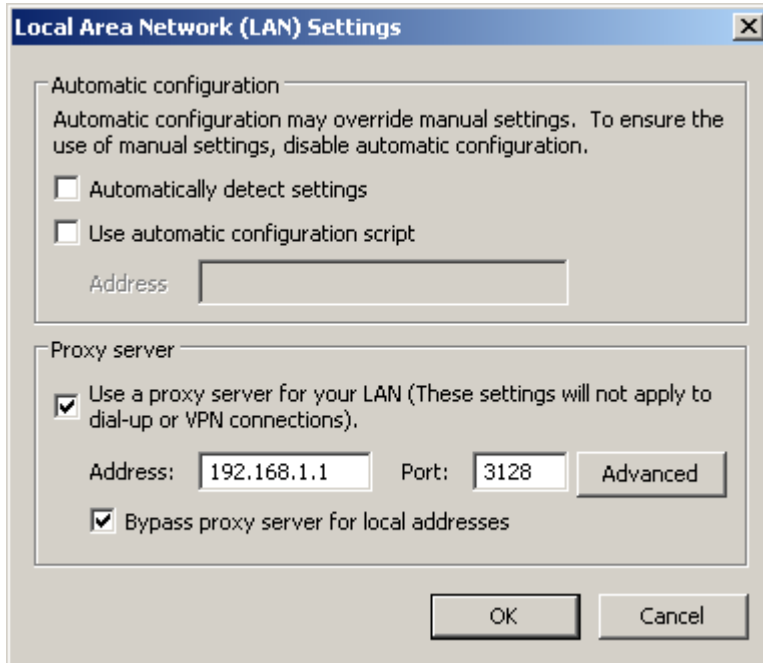



FIGURE 121. LAN Settings

4. In the **Proxy Server** frame, check the **Use a proxy server** checkbox.
5. In the **Address** field, enter the IP address that you assigned to your iPrism server. (You do not have to put “http://” in front of it.) The example in Figure shows the settings for an iPrism unit with the IP address 192.168.1.1.
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” (see Figure 122).
7. Click **OK**.

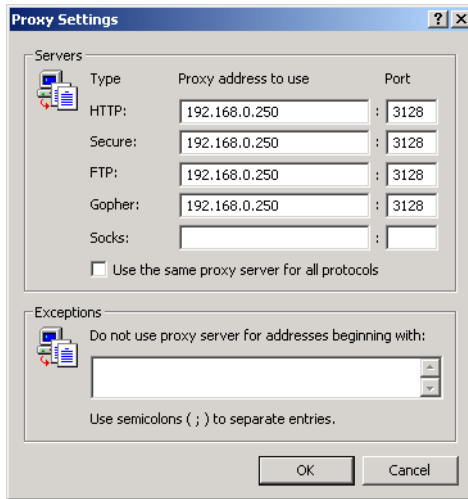


FIGURE 122. Manually Configuring Proxy Settings in IE

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.

This section describes the more common error messages that you may encounter while using iPrism.

The error conditions are listed by error name/type, one per page, and 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 “What to Do” section that suggests how to correct the condition.




Note: This appendix 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** (see “Filter Failover Mode” on page 171), you may see the following error.

If Filter Failover is set to **Pass**, the error will not occur, but traffic may pass unfiltered for a few seconds.



ST BERNARD 

iPrism®

iPrism Rating Error

The Rating service could not rate the page being accessed.

Contact your local system administrator for assistance.

Details	
Service Name	/usr/rapid/bin/rated
Additional Data	The attempted access was blocked, because the Filter Failover Mode is set to 'Block Traffic'.

FIGURE 123. iPrism Rating Error

iPrism List Update Error

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 will need 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 will display the “iPrism List Update” message as shown in Figure 124.

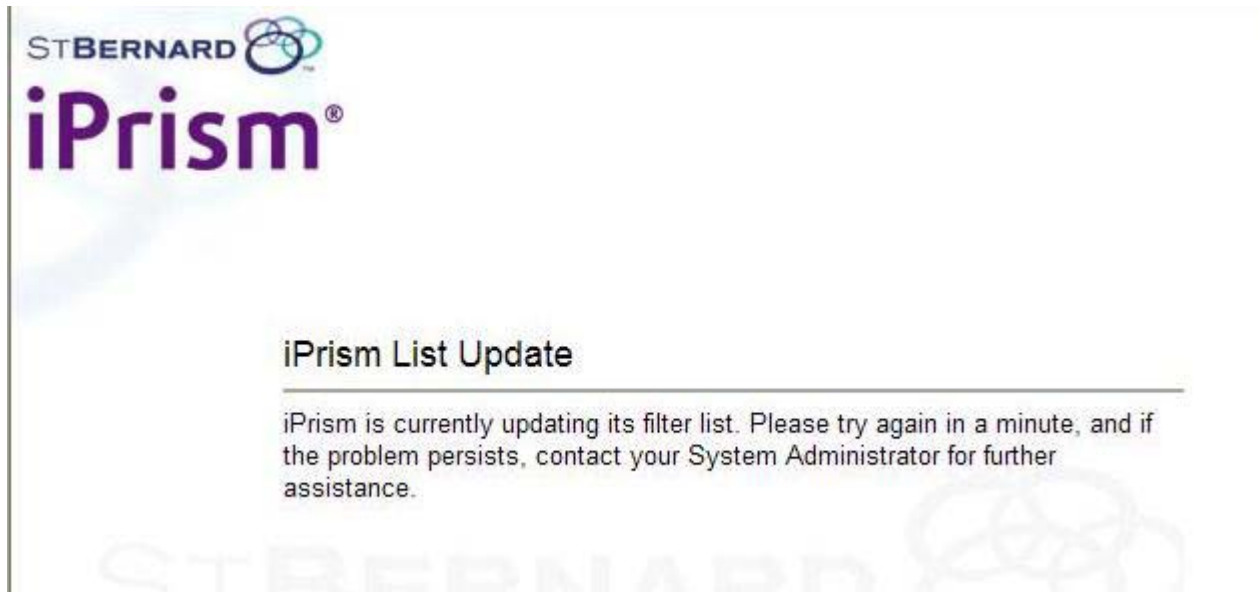


FIGURE 124. iPrism List Update Error

What to Do:

This message is not an error message and should only last for a few seconds. Contact St. Bernard Technical Support (www.stbernard.com/products/support/support.asp) if the message does not disappear.

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 (see “Filter Failover Mode” on page 171).

If iPrism is set to block all traffic when the filter list is missing (i.e., Filter Failover Mode is set to “Block Traffic”), it will display the error shown below. 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.



FIGURE 125. iPrism List Update Error

What to Do:

This is an error condition. Contact St. Bernard Technical Support (www.stbernard.com/products/support/support.asp) to resolve this issue.

iPrism Filter Service Expired Error

If iPrism's subscription to the filter list update expires, the error message shown in Figure 126 will be displayed:

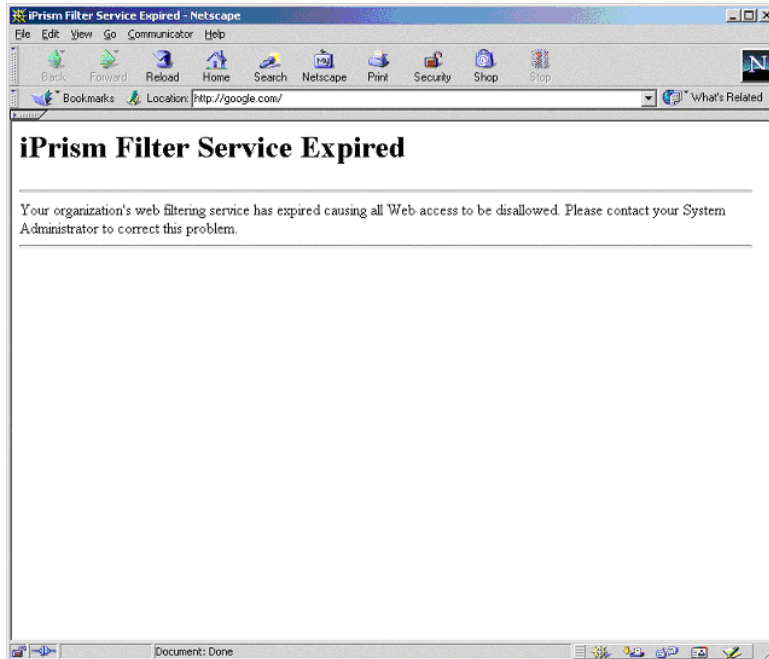


FIGURE 126. iPrism Filter Service Expired Error

What to Do:

iPrism's registration key must be updated before access is possible. Contact St. Bernard Technical Support (www.stbernard.com/products/support/support.asp).

Access Denied Error

The error shown in Figure 127 will display 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 (see page 149).
- 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 (see page 149).
- 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.

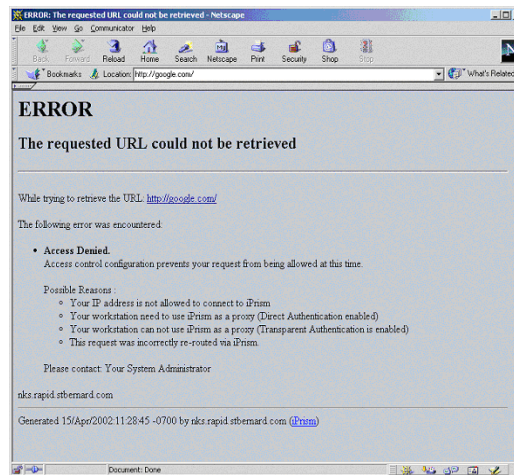


FIGURE 127. Access Denied Error

What to Do:

Check iPrism's configuration (access and authentication) for the client workstation's IP address; if looping occurs, check the routing setup (see *Routing* in **System Settings > Network Services** on page 154).

Authentication is Required Error

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).

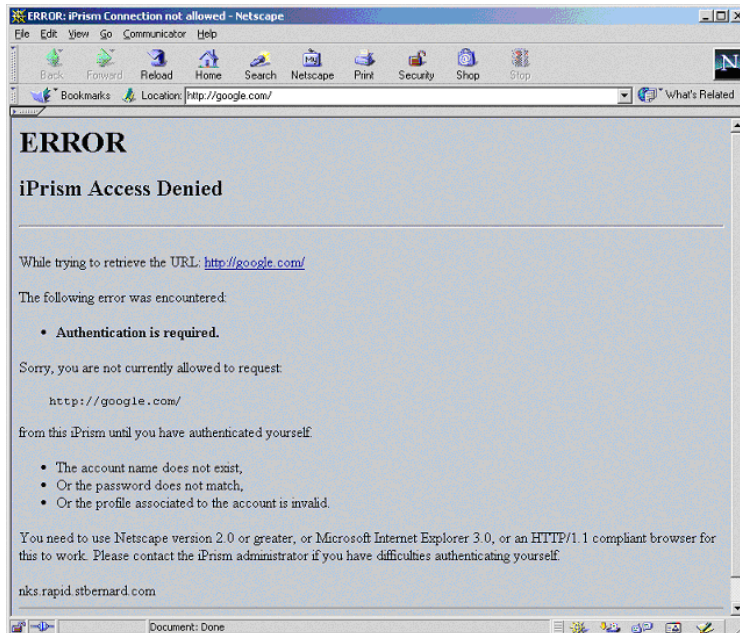


FIGURE 128. Authentication is Required Error

What to Do:

Reload the page and provide your user credentials when prompted.

Connection Failed Error

If you get the “Connection Failed” message (see Figure 129), 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.

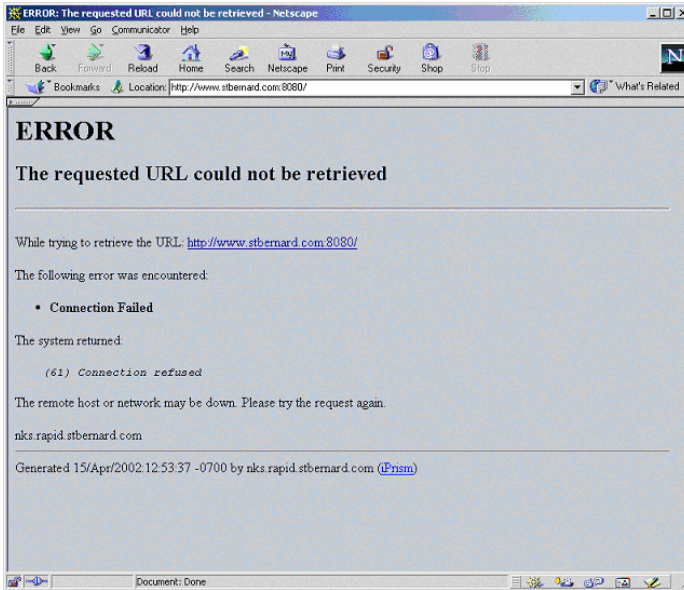


FIGURE 129. Connection Failed Error

What to Do:

- 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 Error

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.

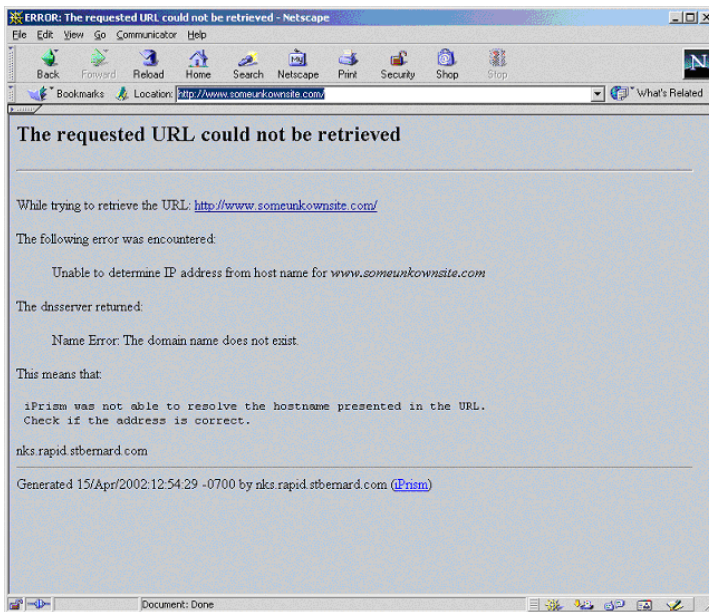


FIGURE 130. Unable to Determine IP Address from Host Name Error

What to Do:

Wait awhile and check the URL again; if the error occurs across multiple web servers, check iPrism’s DNS configuration and status.

Invalid Request Error

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.

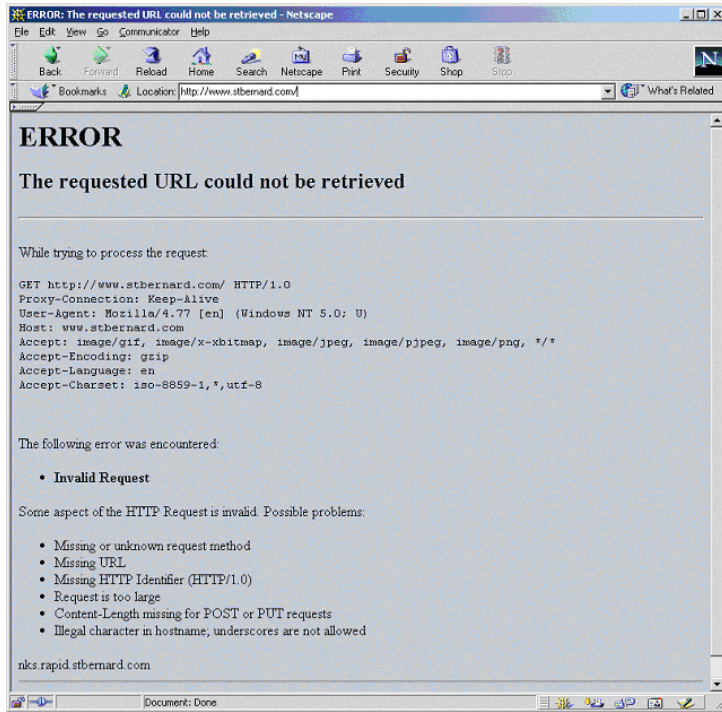


FIGURE 131. Invalid Request Error

What to Do:

Check the request syntax as displayed by iPrism and fix the client software.

Invalid URL (Error)

Much like the “Invalid Request” error on the previous page, 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.

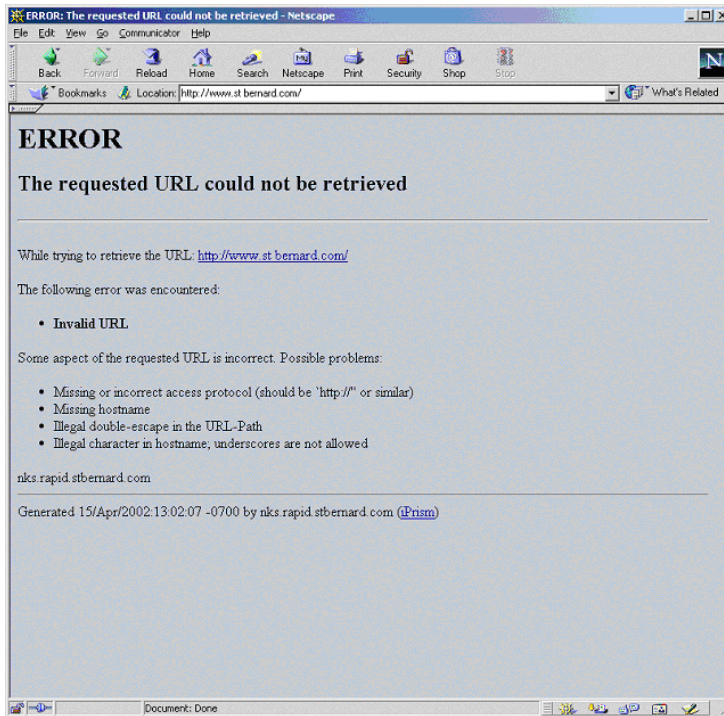


FIGURE 132. Invalid URL Error

What to Do:

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 (Error)

iPrism will display the message shown in Figure 133 while a reconfiguration is in progress.

If the administrator made a change to the configuration, iPrism will reload its configuration. This is short-lived condition and the message should go away within 10 seconds.

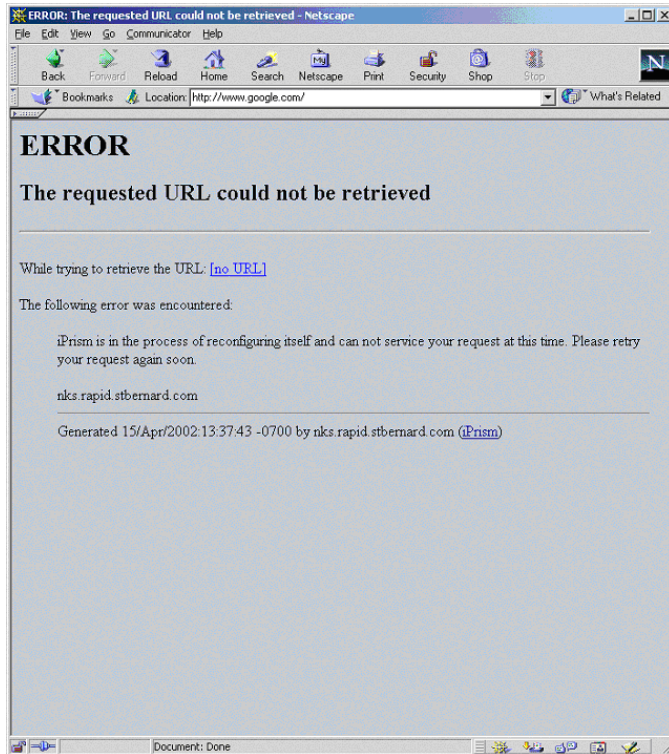


FIGURE 133. iPrism is in the Process of Reconfiguring Error

What to Do:

Retry after a few seconds. If the error message does not go away, Contact St. Bernard Technical Support (www.stbernard.com/products/support/support.asp).

Zero Sized Reply (Error)

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.

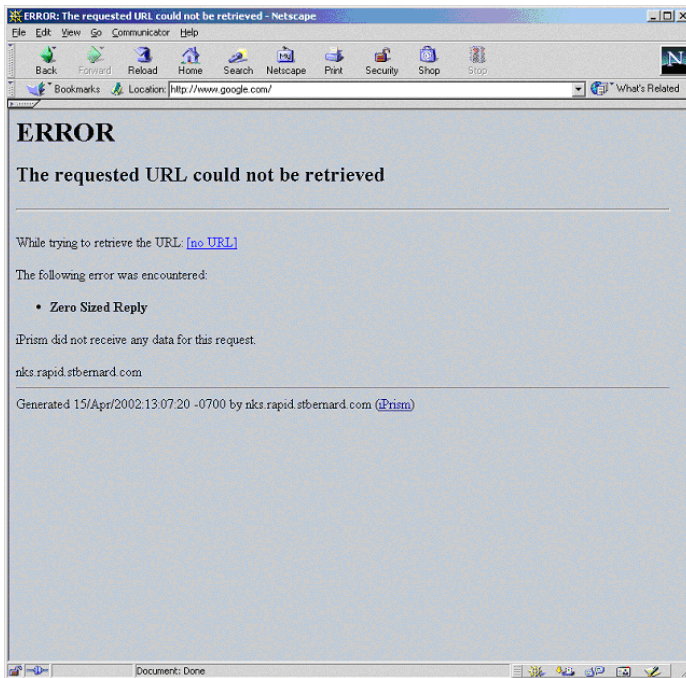


FIGURE 134. Zero Sized Reply Error

What to Do:

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.

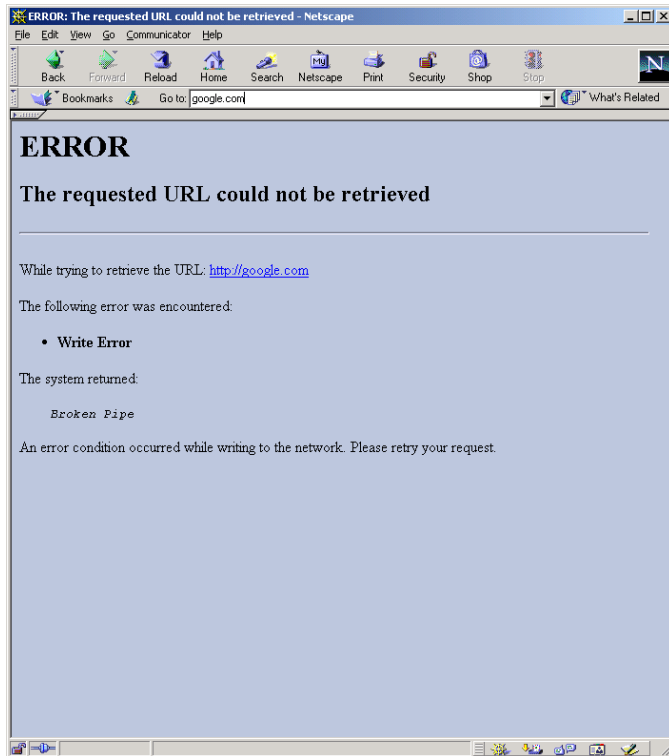


FIGURE 135. Write Error

What to Do:

Check the network environment (firewall logs, routing).



St. Bernard Software, Inc.

Terms and Conditions

(for the "iPrism Web Filter" System)

These Terms and Conditions ("Conditions") apply to an entities access and/or use of the iPrism Internet Filtering System (the "SBS System"). As used in these Conditions, "**SBS**" means St. Bernard Software, Inc., and "**Subscriber**" or "**you**" means the client who is purchasing services and appliances from SBS. THIS IS A LEGAL AND BINDING AGREEMENT BETWEEN YOU AND SBS.

READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SBS. BY CLICKING YOUR ACCEPTANCE OF THESE CONDITIONS, OR BY USING THE SBS SYSTEM, OR WHEN THE SBS SYSTEM IS "IN USE", OR IF YOU AUTHORIZE ANY OTHER PERSON TO DO SO, YOU ACKNOWLEDGE THAT YOU ARE AUTHORIZED TO ENTER INTO THIS AGREEMENT, HAVE READ ALL OF THE TERMS AND CONDITIONS OF THESE CONDITIONS, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. The SBS System is "in use" when the system's Firmware is loaded into temporary memory (i.e. RAM) on the Appliance. If you do not agree to these Conditions, you may not use or access the SBS System.

These Conditions, together with any quotation issued to you by us ("**Quotation**"), constitute the entire contract between us ("**Agreement**"), and supersede all prior agreements and understandings between us, whether written or oral, relating to the subject matter hereof. In the event of a conflict, a Quotation takes precedence over these Conditions, and a written contract signed by you and an authorized officer of SBS takes precedence over both. The effective date of this Agreement is the earlier of the date which you sign a Quotation or click below to accept these Conditions. Any purchase orders issued by you or any entity other than SBS shall be valid only for the purpose of identifying this Agreement for reference purposes only, and any terms included in such purchase orders are void and shall be of no effect. SBS's failure to object to

provisions contained in any communication from Subscriber shall not be deemed a waiver of the provisions herein.

1. **Services**

1.1 **Activation Key.** - During the Term of this Agreement, SBS will provide Subscriber with an Activation Key allowing Subscriber to activate the SBS System. Activation Keys also serve as an enforcement tool and all Activation Keys are setup for the Term or Rollover Term (as defined below) and will expire at the end of the relevant Term or Rollover Term. New Activation Keys will be sent for each Rollover Term.

1.2 **Updates** - Periodically throughout the Term, SBS may update the Firmware or URL Database used by the SBS System to filter Internet use. However, SBS retains the right, at its discretion, to create any modifications to, enhancements and updates of the Firmware without notice.

1.3 **Support Service** - SBS shall provide, via telephone, email or the Internet, technical support to Subscriber in connection with the use of the SBS System. This support shall be available from 8 a.m. to 5:30 p.m. Pacific Time, Monday through Friday, excluding SBS's holidays.

1.4 **Maintenance Service** - SBS shall provide appliance maintenance for appliances with an active maintenance subscription. Appliance maintenance includes the processing of a replacement System within 24 hours from the determination that the active System or Firmware has failed. There will be no cost for the replacement System as long as the failed System is returned, as detailed within section 10.2 of this Agreement.

1.5 **No Consulting or Advisory Services** - Subscriber acknowledges and agrees that SBS is not providing any consulting or advisory services to Subscriber, legal or otherwise.

2. **SBS System.** The SBS System is an Internet filtering system comprised of SBS's proprietary Firmware and Appliance. "**Appliance**" refers only to the hardware device or server provided by SBS to Subscriber that will be installed within Subscriber's network for purpose of running the Firmware and open source software. "**Firmware**" refers to all software embedded in the Appliance, including, but not limited to, the iPrism Web Filter software (but not including any open source software, which is described below), the URL Database, as well as any accompanying documentation and any updates and enhancements to the software and documentation. "**URL Database**" refers to the list of Internet URL's and their associated content

categorization ratings and provided from time to time by SBS. The SBS System may contain software modules, referred to as "open source software" that are licensed under the GNU General Public License, Version 2 June 1991 (the "GPL") and/or the GNU Lesser General Public License, Version 2.1 February 1999 (the "LGPL"). The SBS System may contain software modules licensed under the GPL and/or LGPL: Openssl, bash2, bonie++, libbf, libgmp, libiconv, libsha1, samba, vtun, kunststoff, glazedlists, jasperreports, jcalendar, jfreechart, metouia, bison-1.875_2.tbz, squid2 and FreeBSD.

3. **Fees and Payment.** Subscriber agrees to pay the fees in the manner as set forth in the Quotation. For Rollover Terms, renewal fees shall be paid no later than thirty (30) business days after the commencement of the Rollover Term. A one and a half percent (1.5%) monthly service charge is payable on all overdue balances that are outstanding more than thirty (30) days after the date of the invoice. All fees are exclusive of, and Subscriber is responsible for, applicable foreign, federal, state, or local sales, use, excise, value added, export or other applicable taxes other than taxes on the net income of SBS and all customs, duties and other governmental fees or levies. Subscriber shall pay or reimburse SBS for any such taxes and SBS may add any such taxes to invoices submitted to Subscriber by SBS. SBS shall be entitled to any costs of collecting any amount past due hereunder, including reasonable attorneys' fees. Unless otherwise agreed in writing, all payments are to be in United States dollars. Subscriber will notify SBS in advance of having actual Seats that exceeds the maximum number of Seats permitted in the Quotation and SBS will charge Subscriber for the additional Seats.

4. **License.** Subject to Subscriber's payment of all applicable fees to SBS and Subscriber's acceptance of all the terms and conditions of the Agreement, SBS hereby grants to you, during the Term and during any Rollover Term, and for your internal business purposes only, the non-exclusive, non-sub-licensable, non-transferable, non-assignable and non-exclusive license (the "License") to use the SBS System as specifically permitted hereunder in connection with the number of licensed workstation ("Seats" or "Users") as reflected in the Quotation. SBS also retains the right to publish, copy, modify or otherwise make use of the SBS System in any manner, shape or form.

5. **License Restrictions.** Other than the rights expressly granted in this Agreement, each party retains all of its rights to its trademarks, logos, trade names, and service marks, web site(s), technologies, patents, copyrights, trade secrets, know-how, and other intellectual property and

proprietary rights. Without limiting the generality of the foregoing, SBS shall at all times solely and exclusively own all rights, title, and interest in and to the SBS System, and all intellectual property rights therein. No implied licenses are granted herein. Subscriber may not (i) use any reverse compilation, reverse engineering, decompilation or disassembly techniques or similar methods to determine any design structure, concepts and construction method of the SBS System or replicate the functionality of the SBS System for any purpose; (ii) remove, modify, or obscure any SBS or other copyright, trademark, and other proprietary notices affixed to or displayed on or in the SBS System or Firmware, and shall not allow any third party to take any such action (iii) transfer, distribute, sublicense, rent, lease and/or assign or otherwise make available the SBS System to a third party; (iv) transfer the Firmware from an Appliance through a network or other data transmission channels to another hardware appliance or computer; or (v) use the SBS System in connection with more Seats or User than the number of Seats or Users approved in the Quotation.

6. **Term.** The term of this Agreement is for the duration set forth in the Quotation (the “**Term**”). The Agreement may be terminated in the manner provided in Section 7. Absent termination in accordance with Section 7, this Agreement shall automatically renew for successive rollover terms (each a “Rollover Term”) for the same duration as the original Term, with each such Rollover Term commencing on the applicable anniversary date of the commencement of the previous Term or Rollover Term. By way of example, if the original Term was for three years and had an effective on June 1, 2008, then unless the Agreement is terminated in the manner provided in Section 7, the first Rollover Term shall commence on June 1, 2011 for a three-year term and Subscriber shall be required to pay the then current fees. SBS shall endeavor to provide Subscriber with written notice at least 60 days prior to the expiration of the Term and each Rollover Term.

7. **Termination.** Either party may terminate this Agreement:

(a) Without Cause at any time with written notice. Such termination shall be effective at the conclusion of the Term or Rollover Term during which such termination occurred; or

(b) At any time upon written notice in the event the other party has committed a material breach of this Agreement which remains uncured forty-five (45) days after written notice of such

breach, except that SBS may terminate this Agreement immediately upon written notice for a breach by Subscriber of Section 3,4, 5 or 9.

8. **Effect of Termination.** Upon termination for any reason, (a) Subscriber shall cease all use of the SBS System, (b) the Activation Key will be cancelled; and (c) in the event the Agreement is terminated by SBS for breach by Subscriber, Subscriber will be required to pay all fees detailed in the Quotation.

9. **Confidential Information.**

9.1 **Definition of Confidential Information.** SBS and Subscriber understand and agree that in the performance of this Agreement, each party may have access to or may be exposed to, directly or indirectly, proprietary or confidential information of the other party, including, but not limited to, trade secrets, Web site usage statistics, and technical information (“Confidential Information”).

9.2 **Protection of Confidential Information.** Each party agrees that it shall not, during the Term of this Agreement and after its termination, use (except as expressly authorized by this Agreement or by SBS in order to improve its service or the SBS System) or disclose Confidential Information of the other party without the prior written consent of the other party, unless the receiving party can prove such Confidential Information (i) was known to the receiving party prior to the Effective Date of this Agreement, or (ii) becomes publicly available without breach of this Agreement, or (iii) becomes known to the receiving party after rightful disclosure from a third party not under an obligation of confidentiality; or (iv) was disclosed to the minimum extent necessary to comply with a lawful court order or government regulation, provided that the party making such disclosure provide the other party with advance written notice thereof, and reasonably cooperates with the other party to seek confidential or protective treatment of such information. In addition, each party agrees to take all reasonable measures to protect and maintain in confidence the Confidential Information received from the other party. With respect to information disclosed by a party under this Agreement, this Section 9.2 shall supersede any existing agreement relating to confidential treatment and/or non-disclosure of Confidential Information.

9.3 **Collection of Anonymous Information.** Subscriber acknowledges that in order for SBS to improve the SBS System, SBS may collect and analyze anonymous internet usage across all

customer sites for the purpose of rating websites, detection of malware, diagnostic monitoring, and anonymous aggregation of internet usage for benchmarking and industry data. In all such cases, there will be no personally identifying information related to Subscriber or our Subscriber's internet users stored within this aggregated or analyzed data.

9.4 **Security of Data.** SBS represents that it shall use commercially reasonable efforts to protect against the loss, misuse and alteration of the Subscriber information under SBS's control, including SBS's standard encryption protocols and digital certificate to protect the security of such information.

10. Warranties

10.1 **Warranties by Both Parties.** Each party represents and warrants to the other party that it has the right to enter into this Agreement and perform its obligations hereunder in the manner contemplated by this Agreement.

10.2 **Warranties By Subscriber.** Subscriber represents, warrants, and covenants that it shall comply with all applicable United States of America, any State thereof, all applicable foreign jurisdictions, and any other applicable rules, ordinances, and regulations in connection with the performance of Subscriber's obligations under this Agreement and any use of the SBS System, including, but not limited to, the U.S. Export Administration Regulations, as well as enduser, enduse, and destination restrictions issued by U.S. and other governments (for additional information on U.S. export controls see <http://www.bis.doc.gov>).

10.2 **SBS Warranties.** SBS hereby stresses and Subscriber acknowledge that on the basis of today's technologies it is not possible to manufacture computer software or hardware that performs its functionality error-free in all applications and combinations. Subject to (i) Subscriber's compliance with all the terms of the Agreement, and (ii) the proper installation and use of the SBS System, SBS warrants that during the Term the Firmware will substantially conform with SBS's then current functional specifications as set forth in the applicable documentation ("Warranty"). SBS's sole obligation, during the Term, shall be to repair or replace the defective SBS System or Firmware at no charge to you. In the event Subscriber fails to return a defective SBS System within 30 days of receiving a replacement SBS System, Subscriber will be required to pay for the then current price of replacing the Appliance with no right to receive a credit in the event the defective SBS System is received by SBS later than the 30 day grace period.

If SBS replaces the SBS System or Firmware, and if at a time of such replacement SBS has launched a new version of the SBS System or Firmware, then SBS retains the right to replace the SBS System or Firmware with the new version, at SBS sole discretion. An Appliance that is replaced by SBS shall become the property of SBS upon replacement.

10.3 **Limitation of Liability.**

(a) The above limited warranty does not apply and is voidable by SBS, at its discretion, if the SBS System (i) has been altered, except by SBS or its authorized representative, (ii) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by SBS, (iii) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (iv) is licensed, for beta, evaluation, testing or demonstration purposes for which SBS does not charge a purchase price or license fee. This Warranty is also voidable by SBS, at its discretion, if the SBS System is used for any other purpose other than for its intended purpose or if Subscriber has in any way violated the terms of the Agreement.

(b) SBS EXPLICITLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, CONDITIONS OR REPRESENTATIONS, EXPRESSED OR IMPLIED INCLUDING, BUT NOT LIMITED TO, THE ABSENCE OF DEFECTS, FLAWS OR MALFUNCTIONS OF THE SBS SYSTEM. IN PARTICULAR, SUBSCRIBER ACKNOWLEDGES THAT EXCEPT AS PROVIDED ABOVE, THE SBS SYSTEM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. SBS DOES NOT WARRANT THAT THE SBS SYSTEM WILL MEET SUBSCRIBER'S REQUIREMENTS OR THAT THE OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE FULLEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW, SBS DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS, IMPLIED, AND STATUTORY, CONCERNING THE SBS SYSTEM, OR OTHERWISE RELATED TO THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY STATUTORY WARRANTIES OF NON-INFRINGEMENT. THE ENTIRE RESPONSIBILITY IN CONNECTION WITH THE APPROPRIATE ELECTION AND THE CONSEQUENCES RESULTING FROM THE USE OF THE SBS SYSTEM AS WELL AS THE INTENDED OR ACHIEVED RESULTS RESULTING FROM THE USE OF THE FIRMWARE LIES ENTIRELY WITH SUBSCRIBER. IF SUBSCRIBER HAS ACQUIRED THE SBS SYSTEM THROUGH AN AUTHORIZED DISTRIBUTOR OR RESELLER OF SBS, SBS SHALL NOT BE HELD RESPONSIBLE FOR ANY ADDITIONAL PROMISES OR WARRANTIES MADE BY SUCH DISTRIBUTOR OR RESELLER.

(C) TO THE MAXIMUM EXTENT PERMITTED BY LAW, SBS IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE SBS SYTEM, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA) RESULTING FROM THE USE OF THE SBS SYSTEM, RELATING TO THE WARRANTY, OR ARISING OUT OF ANY BREACH OF THIS WARRANTY, EVEN IF SBS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING SBS SYSTEM AS SPECIFICALLY STATED IN THE SECTION ABOVE. THE FOREGOING IS YOUR SOLE AND EXCLUSIVE REMEDY AND STATES SBS' ENTIRE LIABILITY.

11. **Indemnity**

11.1 **Indemnity by Subscriber**. Subscriber agrees to indemnify, defend and hold SBS harmless from all expenses, losses, damages or liabilities (including reasonable legal fees) arising out of or relating to any third party claims, demands, or suits, in connection with (i) a breach of Subscriber's warranties, representations, covenants, or obligations set forth herein; and (ii) a violation by Subscriber of any laws, rules or regulations or third party patent, copyright, trademark, trade secret or privacy rights; or (iii) any data or content included in or used in conjunction with the SBS System by Subscriber.

11.2 **Indemnification by SBS**. SBS agrees to indemnify, defend and hold Subscriber harmless from all expenses, losses, damages or liabilities (including reasonable legal fees) arising out of or relating to any third party claims, demands, or suits in connection with (i) a breach of its obligations set forth in Section 9 herein; and (ii) a violation by the SBS System of any third party United States copyright or trademark rights. The foregoing indemnification obligation in Section 11.2 (ii) shall not apply to the extent the alleged infringement is caused by: (a) changes or modifications to the SBS System by Subscriber or any third party; or (b) combinations of the SBS System with any product not supplied or specified by SBS under this Agreement. If a claim contemplated under this Section 11.2 (ii) is brought, SBS shall, at its sole option and expense, and within a reasonable period, (1) procure for Subscriber the right to continue using the

allegedly infringing item; (2) replace the same with a non-infringing item providing equivalent functions and efficiency; (3) modify the same to be non-infringing without loss of functionality; or (4) if none of the foregoing is reasonably available to SBS, SBS shall require Subscriber to discontinue use of the infringing item and SBS shall provide a refund of the pro-rated amounts paid by Subscriber to SBS under this Agreement. This Section 9.2 sets forth SBS's sole liability, and Subscriber's sole and exclusive remedy, in lieu of all others, with respect to infringement.

11.3 **Procedures.** The obligations under this Section 11 are conditioned upon the party seeking indemnification (i) giving the indemnifying party prompt written notice of any claim, action, suit or proceeding; (ii) granting complete control of the defense and settlement to the indemnifying party; and (iii) reasonably cooperating with the indemnifying party at the indemnifying party's expense.

12. **Force Majeure.** SBS shall not be liable to Subscriber or any other person or entity for any delay or failure in the performance of this Agreement or for loss or damage of any nature whatsoever suffered by such party due to disruption or unavailability of communication facilities, utility or Internet service provider failure, acts of war, acts of vandalism, terrorism, lightning, fire, strike or any other causes beyond SBS's reasonable control.

13. **Verification.** SBS may, at its expense, automatically audit Subscriber's use of the SBS System, provided that any such audit shall not interfere with Subscriber's business activities. SBS shall be permitted to conduct automated audits at its discretion, provided that such automated audits take place without accessing Subscriber's internal information technology networks and do not materially interfere with Subscriber's use of the SBS System. If an audit reveals that Subscriber has underpaid fees to SBS, Subscriber shall pay SBS such underpaid fees based upon the charging methodology set forth on the Quotation. Subscriber shall cooperate with SBS to provide passwords and other information necessary for SBS to conduct such audits.

14. **Independent Contractor.** The relationship of SBS and Subscriber is solely that of independent contractors. Nothing contained in this Agreement shall be construed to give either party the power to direct or control the activities of the other or constitute either party as the other's partner, joint venturer, co-owner, agent, franchisee or employee. Neither party is authorized or empowered to transact business, incur obligations, or make representations on behalf of the other party.

15. **Miscellaneous.** This Agreement shall be binding and shall inure to the benefit of the parties hereto and their respective successors and permitted assigns. This Agreement may not be assigned by Subscriber without SBS's prior written consent, such consent not to be unreasonably withheld. SBS may assign, delegate and/or subcontract any or all of its rights or obligations hereunder. Any attempted assignment in violation of the foregoing shall be null and void. All notices and consents required or permitted to be given under this Agreement shall be in writing to the parties at the addresses designated herein or to such other address as either party may designate to the other by written notice, and shall be effective upon receipt. Written notice shall be made in the form of a certified letter, confirmed facsimile transmission or acknowledged receipt of electronic mail. Receipt shall be deemed to have occurred: four days following mailing of a certified letter; upon receipt of confirmation of fax; and upon receipt of confirmation of receipt of e-mail. Sections 3,8,9,10,11,13,15 and 16 will survive the termination of this Agreement.

16. **Governing Law, Dispute Resolution and Exclusive Jurisdiction**

(a) This Agreement shall be governed by and interpreted exclusively in accordance with the laws of the State of California, U.S.A., without reference to conflict of laws principles, and to the maximum extent permitted under applicable law, you expressly waives any rights to the application of any other law or regulation on the effect thereof. Exclusive venue for any disputes will be in San Diego County, California.

(b) Except as otherwise provided below, any controversy or claim arising out of or relating to this Agreement shall be submitted to final and binding arbitration before, and in accordance with, the rules of the American Arbitration Association ("AAA") as modified herein, decided by a single independent arbitrator who shall have expertise in the subject matter of the dispute. The arbitration process, including exchanges of requests for information and the arbitration hearing, shall be completed within sixty (60) days following the initiation of the arbitration by either party, shall be held exclusively in San Diego County, and the actual arbitration hearing shall be limited to one (1) day. The arbitrator shall issue a written judgment within ten (10) days following the arbitration hearing. Judgment upon any arbitration award may be entered in any court having jurisdiction thereof. This provision is self executing, and in the event that either party fails to appear at any properly noticed arbitration proceeding, an award may be entered

against such party notwithstanding said failure to appear. This clause shall survive the termination of this Agreement.

(c) Notwithstanding the foregoing: (1) any claim between the parties relating to the validity of the SBS System or Firmware, SBS' trademarks, or other proprietary technology or intellectual property shall not be determined by arbitration, but only by a court located in San Diego County, California, to whose sole jurisdiction you hereby consent or such other court in the United States which SBS, in its sole discretion as owner of the licensed intellectual property, shall select; and you expressly waive any right you may have to any other forum; and (2) Subscriber acknowledges that any breach of your obligations under this Agreement which relates to the proprietary rights, or which is otherwise not subject to remedy by monetary damages, will cause SBS irreparable harm, and that SBS accordingly will be entitled to injunctive and other equitable relief in addition to all other remedies provided by this Agreement or available at law, in any court of competent jurisdiction.

Client: _____ St. Bernard Software, Inc.

Signature: _____

Title: _____

Date: _____

Index

- A**
- About iPrism 180
 - Access Control List
 - Adding to a Profile 31
 - Creating 32
 - Deleting 34
 - Editing Settings 34
 - locking 34
 - Profiles and ACLs 12
 - tab 66
 - Access Denied
 - Error message 264
 - Access Denied page
 - customizing 109
 - default 204
 - options 203
 - Access Event Records 96
 - Access Requests 203, 210
 - How to Request Access to a Site 210
 - ACL
 - definition of 12, 24
 - Active Directory
 - 2003 132
 - 2008 136
 - AD 2003 132
 - AD 2008 136
 - Domain Admins group 136
 - joining 139
 - Admin Roles 65
 - adding 65
 - deleting 69
 - Administration Log 181
 - Administrative Profiles
 - Extended Override 48, 56
 - Filter Management 48, 56
 - Full Access 48, 56
 - Global Policy Admin 48, 56
 - No Access 48, 56
 - Reports Only 48, 56
 - Single Override 48, 56
 - Antivirus
 - scanning 40
 - Appliance Updates 88
 - Authentication 131
 - Auto-Login 61, 126
 - failover options 63
 - Basic 61
 - bypass 170
 - Choosing an Authentication Mechanism 114
 - combinations 61
 - Configuring Browsers for Authentication 249
 - Creating User Accounts in iPrism 115
 - Error 265
 - failed Auto-Login and 63
 - Failed Options 61
 - HTTP 61
 - HTTPS 61
 - LDAP 115
 - local 115
 - manual login 60, 61
 - page
 - customizing 109
 - remote client 43
 - Testing 131
 - testing 104
 - using Kerberos 136
 - Windows
 - 2000/2003 LDAP 132
 - AD 2003 132
 - AD 2008 136
 - Windows (NTLM) 121
 - Auto-Login 126
 - Configuration Requirements 127
 - failover options 63
 - using in proxy mode 129
 - automatically rating URLs 175
 - AV Scanning 40
- B**
- backup 93
 - Block Offensive (profile) 25
 - blocked sites
 - recent 40
 - Requesting Access to 210
 - bridge (transparent) mode 13, 14
 - and authentication 57
 - deploying in 14
 - bypass authentication 170
- C**
- categories 215
 - local 147
 - Central Management
 - decoupling master and slaves in 199
 - setting up 193
 - upgrading iPrisms in 199
 - upgrading without decoupling 201
 - using standalone mode 199
 - Certificate Signing Request (CSR) 145
 - certificates
 - external SSL 144
 - common name usage 145
 - self-signed 145
 - server 144, 145
 - trusted 144, 145
 - changing password 172
 - Co-Management Network 158
 - Common Name 145
 - recommended values 145, 146
 - Use FQDN 145
 - Use IP Address 145
-

- Use Short Name 145
- community string 155
- configuration port 162
- Configuration Summary 182
- Connection Failed (Error) 266
- Connectivity
 - IUS 184
- CSR 145
- current overrides 36
- Customizable Pages 108

- D**
- dashboard, system status 190
- date and time, current 170
- decoupling master and slave
- iPrisms 199
- Default Profiles 25
- Directory Services 113
 - testing 104
- DNS
 - lookup 185
 - redirection 139
- DNS redirection, and certificates 145
- Documentation
 - iPrism Installation Guide 4
- Domain Admins group 136
- DoS attacks
 - detecting 155
 - preventing 155
- download
 - remote user logs 44
- download Client Auth File 43

- E**
- email
 - alerts 82
 - sending test 100
- Error Messages 259
- Event Log 96
- event logging 141
 - syslog export 141

- exceptions 70
 - adding 70
 - deleting 73
 - editing 72
- export 80
- Extended Override 48, 56
 - administrative profile 48, 56
- external interface, configuring
- iPrism from 158

- F**
- failed options, in authentication 61
- Failover action 76
- failover action, in remote filtering 76
- fails 62
- fallback profile 76
- Filter
 - Failover Mode 171
 - List Updates 172
- Filter Management 48, 56
 - administrative profile 48, 56
- Filtering
 - ACLs 32
 - Antivirus 40
 - categories 215
 - Current Overrides 36
 - custom filters 20
 - database 5
 - deciding what gets blocked 6
 - filtering database 5
 - IM/P2P Profiles 29
 - introduction to filtering
 - profiles 12
 - Lock ACL 34
 - network-level 25
 - pending requests 38
 - profiles 24
 - recent blocks 40
 - remote 41
 - enabling 42

- exceptions 43
 - log files 44
 - user-level 24
 - web profiles 25
- Full Access 48, 56
 - administrative profile 48, 56

- G**
- Global Policy Admin 48, 56
 - administrative profile 48, 56
- Group Mapping 51, 126
- groups 51
 - adding 53
 - deleting 54
 - editing 54

- H**
- Help
 - Technical Support 4

- host
 - pinging 184
- hostname 73
- HotFix Manager 88
- HotFixes 88
- HTML Template Manager (see Customizable Pages) 108
- HTTP port 162

- I**
- iARP 175
- iArp (see Unrated Pages) 175
- iGuard 5
 - rating 175
 - Site Rating Categories 216
- IM/P2P Profiles 29
- import
 - remote users 78
- Installing iPrism
 - Pre-installation Notes 4
- Internet Explorer
 - Configuring for Authentication 255

Invalid Request (Error) 267
Invalid URL (Error) 269
IP redirection, and certificates 145
iPrism
 About 180
 backing up 93
 date and time 170
 external interface,
 configuring from 158
 Filter Service Expired (Error)
 263
 How iPrism Works 5
 in-line installation 13
 integrating with existing web
 caching server 166
 is in the Process of
 Reconfiguring Itself (Error)
 270
 List Error 262
 List Update (Error) 261
 logging into 15
 logging out of 15
 machine account 125
 preferred operating mode 14
 privileged user 65
 restarting 16
 restoring 93
 self-check 99
 server certificate 144
 shutting down 16
 slaving to upstream proxy 166
 technical support tunnel 103
 testing 12
iPrism Automatic Rating Protocol
175
iprism_Client_Auth.key 43
IUS connectivity 184

J
join
 AD 2008 domain 139

K
Kerberos 114, 136

L
LDAP authentication 115
 troubleshooting 121
LDAP Server
 Example using NT Active
 Directory 120
 Query Attributes 119
 Setting Up the iPrism LDAP
 Client 115
license key 144
 uploading 146
local authentication 115
local categories 147
local users 48
Lock ACL 34
logging into iPrism 15
logging out of iPrism 15

M
Machine Account 122, 132
 Maintaining 125
Machine ID 73
machine identifier 73
Maintenance
 Appliance Updates 88
 Backup & Restore 93
 Event Log 96
 Policy Test 98
 Self Check 99
 send test email 100
 Site Rating & Test 102
 support tunnel 103
 Test Directory Services 104
management interface 15
mapping
 groups to profiles 51
 profiles to groups 51
mapping mobile laptops 73
master system

 changing 198
 designating 195
master/slave configuration (see
also Central Management)
 changing the master 198
 designating slave(s) 194
 designating the master 195
 removing a slave 198
 setup order 194
 using standalone mode 199

N
Netscape Navigator
 Configuring for
 Authentication 254
network 57
 activity
 tracing 185
 configuring your topology
 154
 hardening 155
 ID 149
 profile 57
 deleting 64
 editing 64
 services 154
Network-level filtering 25
No Access 48, 56
 access level 48
 administrative profile 48, 56
NT Domain
 Maintaining iPrism's
 Machine Account 125
NT machine account
 Maintaining 125
NTLM
 authentication 121
NTLM
 authentication 131
NTLM diagnostic information 98

-
- O**
- Overrides 203
 - current 36
 - How to Override a Blocked Site 205
 - Managing Override Access 214
 - Override Who screen 207
 - Override/Request Access button 205
 - Privileges 205
 - revoking 37
- P**
- pages, customizing 108
 - parent proxy 166
 - Pass All (profile) 25
 - password
 - changing 172
 - setting 172
 - supervisor 172
 - pending requests 38
 - options 161
 - ping 184
 - policy test 98
 - ports 162
 - configuration 162
 - proxy 162
 - preferences, system 169
 - privileges 51
 - Product Support 4
 - Profiles 12
 - adding 26
 - and ACLs 12
 - and authentication 31
 - assigning 9
 - Assigning Profiles to Networks (Workstations) 31
 - Assigning Profiles to Users 31
 - copying 27
 - default 25
 - deleting 28
 - IM/P2P 29
 - introduction to filtering profiles 12
 - mapping 51
 - mapping groups to 51
 - Scheduling ACLs 31
 - web 25
 - proxy
 - Configuring Proxy Settings in Netscape 254
 - for external users 174
 - mode 12
 - ports 162
 - Proxy Settings in IE 257
 - upstream 166
- R**
- recent blocks 40
 - redirect port 162
 - remote client 43
 - remote filtering 41
 - adding users
 - assigning profiles to 76
 - default failover action for users 76
 - defining policy 73
 - enabling 42
 - exceptions 43
 - Failover Action When Rating Server is Unreachable 76
 - log files 44
 - tutorials 4, 41
 - users
 - exporting 80
 - importing 78
 - web profile for defined users 76
 - remote machines, identifying 73
 - remote users 73, 80
 - adding 73
 - exporting 80
 - importing 78
 - unmonitored network ranges 43
 - unmonitored ports 43
 - Report Manager 86
 - Reporting
 - email alerts 82
 - Report Manager 86
 - Reports Only 48, 56
 - administrative profile 48, 56
 - Request Access 203
 - How to Request Access to a Site 210
 - Requesting Access to a Blocked Page 210
 - screen 212
 - Requests
 - denying 39
 - granting 38
 - pending 38
 - resources
 - limiting consumption of 155
 - restarting iPrism 16
 - restore 93
 - restoring iPrism
 - from local backup 94
 - to its original factory settings 95
 - revoking overrides 37
 - roles, admin 65
- S**
- SASL 115
 - scanning
 - Antivirus 40
 - Scheduling ACLs within a Profile 31
 - Security Log 188
 - server certificate 144, 145
 - setting password 172
-

-
- Shared Configurations
 - Configuring the Master iPrism Server 195
 - Removing a Slave from a Shared Configuration 198
 - Stand Alone Mode with Configuration Sharing 199
 - shutting down iPrism 16
 - Single Override 48, 56
 - administrative profile 48, 56
 - site rating 102
 - slave
 - designating 194
 - removing 198
 - slaving iPrism 166
 - SMTP Relay Settings 158
 - SNMP 156
 - community string 155, 156
 - enabling 155
 - St. Bernard Software Technical Support 4
 - Stand Alone Mode 199
 - status 190
 - Super Admin 66
 - Super User 66
 - supervisor password 172
 - support tunnel 94, 103
 - support, technical 4
 - syslog export 141
 - system
 - preferences 169
 - date and time 170
 - updates 173
 - refreshing server 186
 - System Settings
 - Bypass Authentication 170
 - Central Management 193
 - Customizable Pages 108
 - Directory Services 113
 - Event Logging 141
 - Filter Failover Mode 171
 - Filter List Updates 172
 - license key 144
 - Local Categories 147
 - Network ID 149
 - Network Services 154
 - Pending Request Options 161
 - Ports 162
 - Proxy 166
 - SMTP Relay Settings 158
 - System Preferences 169
 - System Updates 173
 - Unrated Pages 175
 - WCCP 156
 - System Status
 - About 180
 - Administration Log 181
 - Configuration Summary 182
 - Connectivity 184
 - DNS lookup 185
 - Security Log 188
 - Status 190
 - tracing network activity 185
 - T**
 - Technical Support 4
 - test
 - email, sending 100
 - site rating 102
 - testing
 - directory services 104
 - transparent mode (see Bridge (transparent) mode) 13
 - U**
 - Unable to Determine IP Address (Error) 267
 - unmonitored network ranges, for remote users 43
 - unmonitored ports, for remote users 43
 - Unrated Pages 175
 - updates
 - system 173
 - refreshing server 186
 - upgrading 201
 - upstream proxy 166
 - Uptime 190
 - URL Database 5
 - URLs
 - frequently accessed 175
 - rating 175
 - Use FQDN 145
 - Use IP Address 145
 - Use Short Name 145
 - User Accounts
 - About 114
 - Creating in iPrism 115
 - users
 - adding 48
 - local 48
 - remote 73
 - exporting 80
 - importing 78
 - Users & Networks
 - Admin Roles 65
 - Exceptions 70
 - groups 51
 - local users 48
 - network profiles 57
 - networks 57
 - privileges 51
 - W**
 - WCCP 156
 - WCCP2 156
 - Web
 - Browsers
 - Configuring for Authentication 249
 - profiles 25
 - for defined remote users 76
 - for remote users 76
-

Write Error / Broken Pipe 272

Z

Zero Sized Reply (Error) 271

iPrism[®]

Administration Guide

Version 6.500

©2011 St. Bernard Software, Inc. All rights reserved.

The St. Bernard and iPrism logos are trademarks of St. Bernard Software, Inc.
All other trademarks and registered trademarks are hereby acknowledged.

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@stbernard.com

