## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>iPrism Overview</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>iPrism Installation</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Installation Instructions</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Before you Begin</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Gathering Information</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Hardware Setup</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Setting up iPrism and your workstation</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Powering Up</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Setting up IP addresses</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>iPrism Testing</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Test #1: Accessing the iPrism Main Menu</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Test #2: Using the iPrism as a Proxy Server</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>Familiarizing Yourself with iPrism</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>Deploying iPrism in Production</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Bridge (Transparent) Mode</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Proxy Mode</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>Information Sheet</td>
<td>38</td>
</tr>
<tr>
<td>7</td>
<td>Support Information</td>
<td>39</td>
</tr>
<tr>
<td>8</td>
<td>Configuring Your Browser for Proxy Mode</td>
<td>40</td>
</tr>
<tr>
<td>9</td>
<td>Upgrading your iPrism</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Upgrade Process Overview</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Upgrade Process Example</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>What do I do if ...?</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>How to Upgrade iPrisms in a Central Management Configuration</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Upgrading Decoupled Master and Slave(s)</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>To Upgrade the Slave(s):</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Upgrading Master &amp; Slave(s) without Decoupling</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>55</td>
</tr>
</tbody>
</table>
iPrism is the award-winning Internet filtering appliance that secures your organization from Internet-based threats such as malware, spyware, IM/P2P, and inappropriate content at the perimeter, while it helps enforce your acceptable use and security policies.

This guide will help you understand the basic functions of your iPrism as well as get you started using it. Let’s begin with the basic functionality of your iPrism.
The iPrism is designed to operate in either **proxy mode** or **bridge (transparent) mode**:

In **proxy mode**, iPrism uses a single internal interface to connect to the Internet. Proxy mode uses 1 network (NIC) connection, as only the internal interface is connected to the local network. The iPrism acts as a filtering web proxy; web and IM network traffic explicitly directed to the iPrism is filtered. This is the preferred mode in which to operate an iPrism when *testing* (see Figure 1).

**FIGURE 1. Proxy Mode**
**Bridge (transparent) mode** is an “in-line installation” which has 2 network (NIC) connections. 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. iPrism filters web and IM/P2P traffic only. It is best to position iPrism between the outbound Internet connection and an internal switch to limit traffic handling to outbound Internet traffic. This is the preferred mode in which to deploy and operate an iPrism (see Figure 2).

**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 IM/P2P traffic will be filtered for these users.
FIGURE 2. Bridge (Transparent) Mode
The following steps must be completed to successfully install your iPrism. All will be covered in greater detail in this guide.

1. Set up the iPrism for testing, evaluation, and initial configuration.

2. Configure the iPrism for use with your system. Define the web and IM/P2P profiles and filters you want to use, and ensure the iPrism works with your authentication system. During this time, your user community can test the iPrism’s ability to filter web traffic by configuring their browser to use the iPrism as a proxy (see Appendix B: “Configuring Your Browser for Proxy Mode” on page 40).

3. After the iPrism is up and running, it can be deployed in one of the following modes:

   **Bridge (Transparent) Mode** (the preferred operating mode): Connect the iPrism between your internal network and the Internet, inside the firewall if you have one. Enable the external interface in bridge (transparent) mode.

   **Proxy Mode**: Inform your user community that they must use the iPrism as a proxy or create a domain policy that makes the iPrism the proxy for everyone. Change the firewall rules to block any http traffic that does not come from the iPrism.
Installation Instructions

This section provides detailed step-by-step instructions for installing your iPrism. After completing the installation, your iPrism will be ready for configuration and testing. When testing is complete and you are satisfied with the configuration, you can deploy your iPrism into a production environment.

To quickly set up your iPrism in proxy mode, refer to the Quick Setup Guide at www.stbernard.com/docs/guide/iPrism_quickSetup_6-0.pdf

Before you Begin

**Important:** Make sure your browser is not configured to use a proxy while you are running the iPrism Installation Wizard.

Gathering Information

The first step in the installation process is ensuring you have all of the necessary information.

Completing the Information Sheet

Begin by photocopying the information sheet on page 38, and completing it. Follow the instructions below to help you locate the information you need.

**iPrism Information**

You will need certain information to install and configure your iPrism. The following information is lettered to correspond with the information sheet.

Note: If you already know this information and can complete the information sheet, you can skip to Hardware Setup on page 7.

(A) **iPrism Serial Number:** Your iPrism serial number can be found on your iPrism appliance.

(B) **License Key** and (C) **Expiration Date:** Your license key is emailed to you as well as included on a separate sheet with your iPrism appliance. This key will expire with the termination of your license agreement or subscription.

The email you are sent with your registration key also has an attachment containing this registration key. It is recommended that you save this file in a secure location.

(D) **IP Address** and (E) **Netmask:** The iPrism appliance requires a unique IP address on the subnet to which it is installed. Locate the available IP address and its netmask on your network and enter it in the blanks for (D) and (E) on your information sheet. The computer you are using for configuration and the iPrism **must** be connected to the same hub or switch, and **must** be on the same subnet. In addition,
when configuring the iPrism, you must choose network settings matching the network on which your computer is located.

To locate your current IP address, do the following from your computer:

1. Open a command prompt (from the Start Menu, select **Run**, then type **cmd** (Windows® NT4, 2000, XP, and 2003) or **command** (Windows 9x, ME)).

2. At the c:/> prompt, type **ipconfig /all**

3. Look for the Ethernet adapter Local Area Connection, e.g.:

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : .example.com
IP Address......................... : 192.168.1.10
Subnet Mask....................... : 255.255.255.0
Default Gateway................... : 192.168.1.1
```

Select an IP address for the iPrism on the same IP network. Using the example above, you can choose any available IP address in the 192.168.1.1 – 192.168.1.254 range.

**Important:** Verify that the IP address you choose is not in use by another system.

**(F) iPrism Host Name:** During the setup procedures, you will be asked to assign a host name to the iPrism appliance. The name you choose should reflect your DNS domain, such as **iprism.example.com**. You can then create an entry for iPrism in your domain DNS configuration (some email filters will not deliver email from a system with no DNS entry.)

**(G) Default Route (Gateway) Address:** The default route refers to the IP address of the device, usually a firewall’s internal interface, that lies between the local network (subnet) and the Internet. This address should be on the same physical network as the iPrism.

**(H) Name Server (DNS):** Since the iPrism and its clients tend to look up many of the same host names, you can improve efficiency and your cache hit rate by using the same DNS server for the iPrism and the computers that use it. Enter the IP address of this DNS server here.

**Hardware Setup**

This section describes the iPrism’s LED lights and connectors, as well as how to physically install and connect the iPrism appliance to your network in **proxy mode** (for a description of proxy mode, see page 2). This is done in the least obtrusive way possible, allowing your network to operate normally until you are ready to make the final connection.
Mounting the Hardware Appliance

If you have not already done so, now is a good time to unpack the iPrism appliance and physically mount it in its final location (e.g., a 19” rack). If you need help installing the iPrism in a rack or installing rails, see the Knowledgebase article “Installing iPrism on a Rack” at www.stbernard.com/products/support/iprism/help/iprism.htm

Note: On the model 3000, make sure the power isolation switch on the back of the unit is turned off (0).

Connect the power cord to the back of the iPrism and plug it in.

Overview of LED Lights and Connectors

The following section describes the LEDs and lights on the iPrism control panels, and the console and internal/external Ethernet interfaces (ports) on the back panels. Note the following:

• iPrism models 10h and 20h have the same front panel, but different back panels.
• iPrism models 30h, 50h, and 100h have the same front and back panels.

Refer to the iPrism h-Series Appliance Specifications at www.stbernard.com/products/support/iprism/help/iprism.htm for detailed information about each model’s hardware configuration.
**LEDs and Lights**

The LEDs and lights on the iPrism control panel keep you informed of the system status. The following LEDs and lights are available on the h-Series:

- **UID**: Unit identifier. Depressing the UID button illuminates an LED on both the front and rear of the appliance to allow you to easily locate the appliance in large stack configurations. The LED will remain on until the button is pushed a second time. Another UID button on the rear of the appliance serves the same function.

- **NIC2**: Indicates network activity on LAN2 when flashing.

- **NIC1**: Indicates network activity on LAN1 when flashing.

- **HDD**: Indicates IDE channel activity or SATA and/or DVD-ROM drive activity when flashing.

- **Power**: Indicates power is being supplied to the system’s power supply units. This LED should normally be illuminated when the system is operating.

- **Temperature**: Indicates CPU temperature (model 500h only).

- **Reset**: Reboots the system. **Important**: Do not press this button until you have shut down the iPrism from the Exit > Shutdown menu option. This cleanly terminates the current iPrism services and network connections and prepares iPrism to be powered down using this button.

- **Power Button**: Used to apply or remove power from the power supply to the server system. Turning off system power with this button removes the main power but keeps standby power supplied to the system. **Important**: Do not press this button until you have shut down the iPrism from the Exit > Shutdown menu option. This cleanly terminates the current iPrism services and network connections and prepares iPrism to be powered down using this button.
iPrism Installation

Front Panels

10h

20h

30h

50h

100h

500h
### Rear Panels

**10h**

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power connector</td>
</tr>
<tr>
<td>2</td>
<td>Mouse port</td>
</tr>
<tr>
<td>3</td>
<td>Keyboard port</td>
</tr>
<tr>
<td>4</td>
<td>USB ports</td>
</tr>
<tr>
<td>5</td>
<td>Console port</td>
</tr>
<tr>
<td>6</td>
<td>Video port</td>
</tr>
<tr>
<td>7</td>
<td>Internal interface (LAN1)</td>
</tr>
<tr>
<td>8</td>
<td>External interface (LAN2)</td>
</tr>
</tbody>
</table>
iPrism Installation

20h

<table>
<thead>
<tr>
<th></th>
<th>Power connector</th>
<th>This connects power to iPrism (115 – 230 VAC auto-sensing).</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Mouse port</td>
<td>Unused</td>
</tr>
<tr>
<td>3</td>
<td>Keyboard port</td>
<td>Unused</td>
</tr>
<tr>
<td>4</td>
<td>USB ports</td>
<td>Unused</td>
</tr>
<tr>
<td>5</td>
<td>Console port</td>
<td>Access to this port is only under the direction of St. Bernard Technical Support for a specific reason.</td>
</tr>
<tr>
<td>6</td>
<td>Video port</td>
<td>Unused</td>
</tr>
</tbody>
</table>
| 7 | Management interface (LAN1) | This port provides a third auto-sensing 10/100/1000 Mbps Ethernet port that can be used for out-of-band management of the iPrism.  
**Note:** This is used for advanced configurations only. See the *iPrism Administration Guide* for more information. |
| 8 | Interface       | Unused                                                      |
| 9 | External interface | This port provides auto-sensing Ethernet connectivity to the external network (Internet). |
|10 | Internal interface | This port provides auto-sensing Ethernet connectivity to your internal network (the network to which iPrism will apply filtering). |
### 30h, 50h and 100h

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power connectors&lt;br&gt;These connect power to iPrism (100 – 240 VAC auto-sensing).</td>
</tr>
<tr>
<td>2</td>
<td>Mouse port&lt;br&gt;Unused</td>
</tr>
<tr>
<td>3</td>
<td>Keyboard port&lt;br&gt;Unused</td>
</tr>
<tr>
<td>4</td>
<td>USB ports&lt;br&gt;Unused</td>
</tr>
<tr>
<td>5</td>
<td>Console port&lt;br&gt;Access to this port is only under the direction of St. Bernard Technical Support for a specific reason.</td>
</tr>
<tr>
<td>6</td>
<td>Video port&lt;br&gt;Unused</td>
</tr>
<tr>
<td>7</td>
<td>Management interface&lt;br&gt;(LAN1)&lt;br&gt;This port provides a third auto-sensing 10/100/1000 Mbps Ethernet port that can be used for out-of-band management of the iPrism.&lt;br&gt;&lt;b&gt;Note:&lt;/b&gt; This is used for advanced configurations only. See the &lt;i&gt;iPrism Administration Guide&lt;/i&gt; for more information.</td>
</tr>
<tr>
<td>8</td>
<td>Interface&lt;br&gt;Unused</td>
</tr>
<tr>
<td>9</td>
<td>External interface&lt;br&gt;This port provides auto-sensing Ethernet connectivity to the external network (Internet).</td>
</tr>
<tr>
<td>10</td>
<td>Internal interface&lt;br&gt;This port provides auto-sensing Ethernet connectivity to your internal network (the network to which iPrism will apply filtering).</td>
</tr>
</tbody>
</table>
### 500h

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power connectors</td>
</tr>
<tr>
<td>2</td>
<td>Mouse port</td>
</tr>
<tr>
<td>3</td>
<td>Keyboard port</td>
</tr>
<tr>
<td>4</td>
<td>USB ports</td>
</tr>
<tr>
<td>5</td>
<td>Console port</td>
</tr>
<tr>
<td>6</td>
<td>Video port</td>
</tr>
<tr>
<td>7</td>
<td>Interface</td>
</tr>
<tr>
<td>8</td>
<td>Interface</td>
</tr>
<tr>
<td>9</td>
<td>Management interface (LAN1)</td>
</tr>
</tbody>
</table>

1. **Power connectors**: These connect power to iPrism (100 – 240 VAC auto-sensing).
2. **Mouse port**: Unused
3. **Keyboard port**: Unused
4. **USB ports**: Unused
5. **Console port**: Access to this port is only under the direction of St. Bernard Technical Support for a specific reason.
6. **Video port**: Unused
7. **Interface**: Unused
8. **Interface**: Unused
9. **Management interface (LAN1)**: This port provides a third auto-sensing 10/100/1000 Mbps Ethernet port that can be used for out-of-band management of the iPrism. **Note**: This is used for advanced configurations only. See the *iPrism Administration Guide* for more information.
Setting up iPrism and your workstation

There are two ways you can set up iPrism and your workstation for the initial configuration.

1. Connect iPrism and your workstation to the same network switch.

2. Connect iPrism and your workstation using the crossover cable shipped with your iPrism.

Cable Identification

The cables shipped with your iPrism can be distinguished by holding one of the cables at each end so the connectors are oriented the same way. Now, look at the color-coding of the wires in each connector. If the colors are in the exact same order, it is a standard Ethernet patch cable. If the colors are in a different order, it is a crossover cable.

The crossover cable’s package will be marked with “crossover”.

Connecting iPrism to your network

1. Take the white Ethernet cable (provided) from the box and connect one end to the iPrism’s Internal interface.

2. Connect the other end of the cable into the hub/switch that serves the local subnet.

Important: Do not connect the external side of the iPrism at this point. This configuration is used for initial setup and testing so as not to interrupt network traffic. The configuration may be changed later, during the actual deployment of the iPrism in bridge (transparent) mode (see “Deploying iPrism in Production” on page 33).
Connecting iPrism and your workstation using the crossover cable

1. Take the crossover cable (provided) from the box and connect one end to the iPrism’s Internal interface.

2. Connect the other end of the cable into your workstation’s Ethernet port.

Powering Up

Unlock the front panel of the iPrism. Press and hold the power button ( ) to turn on the appliance.

Note: If you are using an iPrism model 500h, the front panel (bezel) is not attached when shipping. Attach the front panel after powering up.

Setting up IP addresses

1. Locate your iPrism’s IP address and subnet from the worksheet you completed on page 6.

   Note: Your iPrism is automatically configured with the IP address 199.248.230.1.

2. Make note of your workstation’s IP address. You will be temporarily assigning your workstation a new IP address on the same subnet as the iPrism, and once the initial configuration of your iPrism is complete, you will need to assign your original IP address back to your workstation.

3. Assign your workstation an IP address on the same subnet as iPrism; e.g., 199.248.230.2.
   • Macintosh: This is done in Network Preferences on the Mac.
   • Windows:
     a. Click Start > Control Panel > Network Connections > Network Tasks > Change Settings of this connection.
     b. Click the Networking tab. Under This connection uses the following items, click Internet Protocol (TCP/IP).
     c. Click Properties.
     d. Click Use the following IP address, and in IP address, type the IP address you want to use (e.g., 199.248.230.2).

4. Use the subnet 255.255.255.0.
5. You may get a certificate error dialogue. If so, click **Continue** to bypass this message.

6. At the iPrism login screen, type the default username `iprism` and password `setup`. 

![iPrism Login](image)

**FIGURE 3. iPrism Login**
7. You will be prompted to accept or decline the license agreement by clicking **Agree** or **Disagree**.
8. Click **Agree** to accept the license agreement and proceed. The following screen will appear:

![Installation Wizard](image)

**FIGURE 5. Configuration**

9. If this is not your first installation of an iPrism and you have a backup of a previous configuration you wish to use, select **Restore from archive**, then click **Browse** to locate the backup file. The iPrism will use that archived configuration as the base for configuring the new iPrism. Otherwise, if this is a new configuration, select **Start a new configuration**.

10. Click **Next**.

11. Your license key was included on a separate sheet and shipped with your iPrism appliance. This key will expire with the termination of your license agreement or subscription. The license key was also emailed to you and included an attachment also containing the license key. It is recommended that you save this file in a secure location.

   Click **Browse** to locate your license key file, then when your license key file has been uploaded, click **Next**. Your subscription information will be retrieved.
FIGURE 6. Upload license key
12. Complete all required fields (in red).

**FIGURE 7. Registration**

13. Click **Set Password** and type a new password for the iPrism administrator account.

14. Click **Next**.
Network Settings

Refer to the worksheet you completed in your iPrism Quick Start Guide for the information needed to complete the fields on this screen. Click here to open the Quiz.

**FIGURE 8. Network Settings**

15. In the Network Settings window, complete the required fields (in red) based on the information you entered on the information sheet you completed in “Completing the Information Sheet” on page 6:

- Host Name
- Interface Negotiate Mode
- DNS Servers (click Settings to enter a Name Server)
- Network Mode
- IP Address (this is the IP address that will ultimately be used for your iPrism, not the IP address it was shipped with)
- Netmask
- Default Gateway
- Enable Management Interface
  - IP Address (for Management Interface if used)
  - Netmask (for Management Interface if used)
Note: The iPrism is initially set up in proxy mode for testing. Only the internal interface is connected to the Internet and the iPrism acts as a filtering web proxy. The iPrism may later be set to a dual-interface configuration using bridge (transparent) mode when it is ready for production. For descriptions of each mode, see page 2.

16. Click Next.
17. In the Filter Settings window, define which each set of filtering rules (Profiles) applies to Web and IM/P2P traffic.

**Installation Wizard**

**Filter Settings**

Define the range of IP addresses to which each set of filtering rules (Profiles) applies.

| Do NOT block any traffic but monitor everything | Block ONLY offensive traffic and monitor everything |
| Web | ![Checkbox](on.png) | ![Checkbox](off.png) |
| IMP/2P | ![Checkbox](off.png) | ![Checkbox](on.png) |

Select the iPrism's local time zone.

Time Zone *

America/Los_Angeles

**FIGURE 9. Filter Settings**

18. You can also select the Time Zone for your iPrism (this is usually the city that is closest to you geographically).

19. Click **Next** when you are done.

20. Review your settings, and if everything is correct, click **Finish**. If you need to make any corrections, click **Back**. If everything is correct, click **Finish**.

You can also print this screen for later reference by clicking **Print**.
21. Click Next.

22. Review your settings and click Back to make any changes. If everything is correct, click Finish to save your settings.

23. iPrism will now halt the operating system. This process takes approximately 2 minutes. Once this is complete, power off iPrism using the power button ( ), and relocate iPrism as needed (e.g., if you will be installing it on a rack).

24. Power iPrism back up using the power button ( ) and wait approximately 2 minutes before logging in at https://[your iPrism IP address]/ (it is recommended you bookmark this link for future access). You may also need to restore this computer’s network settings to their former values if they were changed during the installation process. Please note that upon reboot, iPrism will attempt to
refresh the iGuard filter list; this may take several minutes, depending on network speed. During this process, iPrism will filter using the default filter list, which may not be up-to-date.

FIGURE 11. Shutdown Notification

25. Once your iPrism has restarted, log in:
26. The iPrism home page will appear after you log in. You can now begin working with your iPrism. Refer to the iPrism Administration Guide for detailed information about working with and administering your iPrism.
FIGURE 13. iPrism Home Page
It is now time to run tests to verify that your iPrism has been installed successfully. If any of the tests fail, do not proceed to the next test until the problem is resolved and the test passes.

**Test #1: Accessing the iPrism Main Menu**

In this test, you will use a web browser to access the iPrism configuration utility. This ensures that the iPrism is being recognized on your network with the new network settings you entered in the setup wizard in Chapter 2.

Before performing this test, verify that the iPrism is properly connected and has completely booted up (this takes approximately 2 minutes).

1. Open a web browser on one of the computers monitored by the iPrism (it does not have to be the same workstation you used for the installation and setup).

You must use a web browser to access the iPrism’s configuration utility. The following browsers are supported:

- Internet Explorer version 5.0 or greater
- Netscape Navigator version 4.5 or greater
- Firefox (all versions).

**Note:** The iPrism supports all browsers for filtering.
2. In the Address bar at the top of the browser window, type http://[IP address you assigned to the iPrism]. This is the value you entered on line D of the information sheet in Chapter 2; e.g.: http://123.456.7.8.

3. Press Enter. The iPrism home page should appear in the browser window.

Congratulations! If you see the iPrism home page, iPrism is recognized on your network. You may proceed to Test #2.

If you do not see the iPrism home page, try the following to resolve the issue:

• Use the ping command to check if you can access the iPrism over the network, and verify that you are using the correct IP address.
• Verify that the IP address you typed into the browser’s address bar is correct.
• Check all of the cable connections to and from the iPrism.
• Wait two minutes, then try again.

**Test #2: Using the iPrism as a Proxy Server**

This test verifies that the iPrism can be used as a proxy server.

1. Configure your web browser to use the iPrism as the proxy server. For detailed instructions on how to do this, see “Configuring Your Browser for Proxy Mode” on page 40.

2. Use your browser to surf to a site that should be blocked – www.stbernard.com/test2 is rated specifically for this purpose. You should see an “Access Denied” page.
3. Use your browser to surf to a site that should not be blocked, such as www.yahoo.com. You should be able to access this site.

If both tests are successful, you can deploy your iPrism to your user community for testing. Each user must configure his or her browser to use iPrism as the proxy server; for detailed instructions on how to do this, see “Configuring Your Browser for Proxy Mode” on page 40.

If the test in Step 2 (blocked site) fails (i.e., you are able to access a site that should be blocked), try the following to resolve the issue:

- Type a different URL, refresh the page, or clear your cache. If the test page you are trying to access is stored in your cache, the iPrism will not be able to block it.
- Verify the proxy settings. Ensure that you entered the iPrism’s IP address properly and specified a port value of 3128.

If you are unable to load a web page that is not blocked:

- Verify the existence and/or validity of your Default Gateway (also known as the Default Route) within the iPrism Configuration Manager (located in the System section’s Network section).

If you experience a filtering error:

- If you experience a filtering error, the iPrism iGuard™ database may need to be updated; iPrism will do so automatically within 20 minutes, after which you can try the test again. Alternately, you can update the iGuard database immediately by doing the following (you must have a working Internet connection):
  - From the iPrism home page, select System Settings, then System Preferences.
  - In Filter List Updates, click Update Now to download an updated filter list. Note: This can take up to 20 minutes.
- If you continue to experience a filtering error after updating the iGuard database, contact St. Bernard Software technical support.
Your iPrism is now installed and set up so that you may configure it, test the results, run reports, and generally experiment with your system before deploying it in a production environment. iPrism has an extensive list of features for you to explore; details can be found in the *iPrism Administration Guide*.

Advanced configuration options include:
- Various filters for different types of users
- Using your existing LDAP or NTLM authentication service for user management
- Defining time-dependent filters
- Creating reports and using drill-down reporting
- Using the “Management Port” to manage the iPrism on a secure subnet
- Configuring static routes (this may be necessary if you have a complex internal network with many subnets)
Deploying iPrism in Production

It is recommended that installation, setup and testing be done in proxy mode, and the iPrism be switched to bridge (transparent) mode in production. For additional descriptions of these modes, see Chapter 1.

**Bridge (Transparent) Mode**

To convert your iPrism system from proxy mode to bridge (transparent) mode, complete the following steps:

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

2. In the Host Name field, type the fully qualified domain name of your iPrism host.

3. Select **Bridge (transparent)** mode.

4. The External interface will be enabled. Select a **Mode** (Auto, 100, or 1000).

5. 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 a Management Interface, leave the **Mode** as **Disabled**.

6. Click **Save** to save your changes.
7. 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).

8. Shut down your iPrism.

   **Note:** Do not change any of the routing tables on your network. Previous releases of the iPrism required router changes for deployment in bridge (transparent) mode; this is no longer necessary.

9. Connect the internal interface of the iPrism to your internal network (see Figure 15).

10. Remove the connection between your switch and the Internet, and connect it to the External interface (see “Rear Panels” on page 11) using the crossover cable.

    To identify the crossover cable, look at the color-coding of the wires in each connector that came with your iPrism. If the colors are in the exact same order, it is a standard Ethernet patch cable. If the colors are in a different order, it is a crossover cable. In addition, the crossover cable’s package will be marked with “crossover”.

11. Turn on the iPrism.

    **Note:** If you are using a VLAN or other intelligent switch, the default route for your iPrism must be set to an address outside your local network; i.e., the firewall or a location past the firewall.
Proxy Mode

To convert your iPrism system from testing to production in proxy mode, complete the following steps:

1. Configure all workstations to use the iPrism as the proxy, or define a domain policy/configuration which requires all users to use the iPrism as the proxy.

2. Configure your firewall to disallow all traffic on port 80 for all systems except the iPrism (see Figure 16 on page 37).

3. The iPrism is now configured for deployment in proxy mode (see Figure 16).
Figure 16 shows the iPrism configured in single-interface proxy mode. Note that only the internal interface is used; traffic comes into the iPrism via the internal interface, and the iPrism proxies to the Internet using the internal interface. The first two workstations in Figure 16 have been configured to use the iPrism as their proxy, so all of their web traffic goes through the iPrism. The iPrism then filters the traffic and sends it to the Internet through the firewall. Your firewall must be configured properly, or the iPrism will not be able to access the Internet.

The third workstation in Figure 16 has not been configured to use the iPrism as its proxy. Since the firewall only allows traffic from the iPrism, this workstation is unable to access the Internet.
FIGURE 16. Deployment in Proxy Mode
The information listed on this page is needed to configure your iPrism. Refer to section “Completing the Information Sheet” on page 6.

A. iPrism Serial Number: ________________________________
B. Permanent Registration Key: _______ - _______ - _______ - _______
C. Permanent Registration Key Expiration Date: ___ / ___ / ______
D. iPrism IP Address: ________________________________
E. Subnet mask (netmask): ________________________________
F. iPrism Host Name: ________________________________
G. Default Gateway IP Address: ________________________________
H. Name Server (DNS) IP Address: ________________________________
APPENDIX 7

Support Information

There are some special considerations to be aware of, such as network conditions, for which additional documentation is available. Go to the St. Bernard Software support website at www.stbernard.com/products/support/iprism/support_iprism.asp

Topics include:

• If other proxy servers are configured on the network.
• If you have a wide area network serviced by a router that is also the Internet router.
• If you have concerns about your network’s ability to interact with the iPrism.

If you are unable to resolve your issue using the provided documentation, please contact St. Bernard Software’s technical support team. Contact information is available on the St. Bernard Software website: http://www.stbernard.com/products/support/iprism/support_iprism.asp

When contacting tech support, have the following information ready:

• All relevant information about how iPrism is configured on your network (topology, other hardware, networking software, etc.).
• Your iPrism serial number and registration key.
• In order to help our support staff resolve your issue, it is helpful to send us a network diagram showing the basic hardware used on your network.
To configure your browser for proxy mode, follow the instructions below for your specific Internet browser.
Internet Explorer

1. Select Tools -> Internet Options.

2. Select the Connections tab.

3. Click LAN Settings.
4. Check “Use a proxy server ...“ and type the IP address of your iPrism in the **Address:** field. Type 3128 in the **Port:** field. Click **OK**, then **OK** again.

*Note*: Port 3128 is the default. The iPrism administrator can change this setting.
Firefox

1. Select **Tools -> Options -> Advanced**.

2. Click **Settings**.

3. In the Connection Settings window, select “Manual proxy configuration” and type the IP address of your iPrism in the **HTTP Proxy** field. Type 3128 in the **Port** field. Click **OK**.

   **Note**: Port 3128 is the default. The iPrism administrator can change this setting.
FIGURE 20. Connection Settings
APPENDIX 9

Upgrading your iPrism

Note: iPrism units running v4.1 or earlier must upgrade to v4.2 before upgrading to v5.x/6.x via field upgrade. iPrism units running either 5.x or 6.0 can upgrade directly to 6.x.

Upgrade enhancements include improved diagnostics, scheduling, and progress updates. There have also been improvements to the upgrade process for the Central Management environment.
Upgrade Process Overview

Once your iPrism serial number is enabled, if iPrism is configured for *automatic* system updates (as most iPrism units are) a *system health check* diagnostic will download (approximately 100K; the actual upgrade package downloaded later is approximately 200MB). This download occurs on iPrism at *automatic system update time*, or optionally by using **Update Now**, and will evaluate conditions known to cause upgrade issues.

To check or change how your system is configured to receive updates, from the iPrism home page, select **System Settings -> System Preferences -> System Updates**. Click **Settings** as shown below:

The *system health check* runs and looks for HotFix, disk or other upgrade issues. An email is sent to the iPrism administrator indicating an issue to resolve, or indicating your scheduled upgrade time (shown below). A link to an **iPrism Upgrade Manager** web page will display issues that must be resolved before proceeding, or will present a default upgrade time (3 days out).

Assuming there are no issues to resolve, you may change the upgrade scheduling as you want (in the example below, to 12:00 a.m.):

At update time (e.g., 12:00 a.m.), iPrism upgrades itself, reboots, then rebuilds the reporting database using a new database schema.
Upgrade Process Overview

Note: The upgrade process (notifications and iPrism Upgrade Manager) will be the same as you move from one iPrism build to another, although of course the upgrade may vary in terms of what is being updated.

Upgrade Process Example

When the serial number was enabled for the unit below, the upgrade process was started on 6/28 using the **Update Now** option, rather than waiting for the automatic system update time. In either case, the email below indicates that the **system health check** was successful, and shows an upgrade time of 7/1/2007 at 10:00 AM as the automatic system update time.

The **iPrism Upgrade Manager** link shown in the sample email above provides additional status detail. If your email does not contain the link above, or you need flexible access, you may access the system health check page with the following URL to your iPrism:

http://iPrism-ip-address/cgi-bin/upgradeinfo.pl

The following page is displayed after entering this URL.

Note: **Upgrade data download = Pending** means the upgrade package has not yet been downloaded. This is normal at this point.
Rather than wait for 3 days, we have elected to change the upgrade to ASAP and clicked **Apply new setting**.

*Note:* You must consider how this will affect your users. Using an automatic system update time as the default is specifically provided for performing updates at a time when users are unlikely to be accessing the Internet.
The sample email below confirms the upgrade process has begun. In this example, it arrived about 15 minutes after the scheduling was changed to ASAP.

The sample email below confirms the upgrade process is complete.
Note: HotFixes are currently needed for several features such as partitioning an iPrism for delegation, or using ERS.

What do I do if ... ?

If there is a HotFix, Disk or Central Management issue, it will be noted in the initial upgrade email and the iPrism Upgrade Manager page (see below).

HotFix issues can typically be resolved through uninstalling the HotFix.
Important: Currently, if an incompatible HotFix issue is reported in the email and iPrism Upgrade Manager page, you must **wait 5 minutes** before using HotFix Manager to uninstall the incompatible HotFix, or you may receive an error.
• If Disk Issues are reported, contact iPrism Technical Support for assistance. Cleanup may be required to create enough free space for the upgrade. The following sample demonstrates the kind of email that may be generated to report disk issues:

Subject: *** iPrism Upgrade Notification ***

Your iPrism system [ your-iPrism] has received the iPrism 5.0 Upgrade, however, the upgrade has determined that your system has an incompatibility or resource issue that needs to be resolved before the upgrade can be applied successfully.

Problem(s) detected are categorized as:

Disk: Disk problem has been detected. Can't proceed with upgrade at this time!

Please use your browser to visit the following URL for details about why your iPrism is currently not suited for upgrade, and what can be done to resolve any remaining issues:

http://your-iPrism/cgi-bin/upgradeinfo.pl

Thank you for using the St. Bernard iPrism product.

• Central Management is only an “issue” in regard to the fact that there is an optimal way to upgrade the iPrism units and keep the Master/Slave relationship in sync. Refer to the How to Upgrade iPrisms in a Central Management Configuration below for details.

After resolving upgrade issues, the system health check will run again at the next automatic update time, or by using the ASAP System Updates option. When you click ASAP and there are no issues that arise during the health check, the iPrism will automatically upgrade and reboot with no further user intervention.
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 21).
5. Click **OK**.
6. Click **Save**, then click **Activate Changes** to activate these changes immediately.
7. Select **System Settings**, then **System Preferences**.
8. 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.
9. 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 21).

4. Click OK.

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

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 slave will have been upgraded. Repeat steps 1 – 7 for each slave you want to upgrade.

9. After you have upgraded each slave, add them back to the master iPrism by completing the steps in “Setting up a Master/Slave Configuration” in the Central Management chapter of the iPrism Administration Guide.

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.
Index

Numerics
100h 10, 13
10h 10, 11
20h 10, 12
30h 10, 13
500h 10, 14
50h 10, 13

B
bridge mode 4
installing in 5
buttons 8

C
Central Management 50
decoupling master and slaves in 53
upgrading iPrisms in 53
upgrading without decoupling 54
configuring
  browser for proxy mode
    Firefox 43
    Internet Explorer 41
connection settings
  Firefox 43
    Internet Explorer 41
connectors 8

D
decoupling master and slave iPrisms 53
disk issue 50
fixing 52

F
Firefox
  configuring for proxy mode 43
front panels 10

H
HotFix 50
fixing issues 50

I
Internet Explorer
  configuring for proxy mode 41
IP address, locating 7
iPism
cable identification 15
connecting to internal LAN 15
date and time settings 25
default route (gateway) 7
filter settings 24
front panels 10
host name 7
iGuard updates 31
information sheet 38
in-line installation 3
LEDs and lights 9
login 26
name server (DNS) 7
network settings 22
preferred operating mode 3
rear panels 11
support 39
testing 2
  blocked site 30
  filtering error 31
  unblocked site 31
  using iPrism as proxy server 30
  using web browser 29
turning on 16
Upgrade Manager 46
upgrading 45
web and IM/P2P filtering 3

L
LEDs 8
lights 8
log in 26

P
proxy mode
  configuring
    Firefox 43
    Internet Explorer 41
installing in 5

R
rear panels 11

T
transparent mode 4

U
updates
  receiving
    ASAP 46
    scheduled 46
upgrading 45, 54