



STBERNARD 

iPrism®

Evaluation Guide

Version 6.4

This conceptual guide is intended to help administrators set up and test the iPrism Web Filtering appliance for evaluation purposes. A more prescriptive step-by-step guide is also available upon request. You will find the following icons throughout the guide, indicating an area of special interest:

 ADVANTAGE

 GOAL



TIP/IDEA


## PRODUCT DEPLOYMENT AND NETWORK IMPLEMENTATION




*iPrism* uses either a transparent bridge (and proxy mode) or proxy-only deployment:

### CONCEPTS

**Transparent bridge** deployment places the iPrism appliance in-line with all traffic behind the Internet gateway. No third-party network systems are required, and requests or traffic are dropped to block access.

 *A built-in fail-open/close bypass prevents network disruption and kernel-level filtering prevents loss of network and browser session integrity in the unlikely event of a hardware failure or software malfunction.*

**Proxy mode** can optionally be used at the same time in transparent bridge deployment. No third-party network systems are required, and requests are terminated to block access.

 *This deployment is useful for mixed-machine environments with both Citrix/Terminal Service clients and Windows OS or Mac OSX clients.*

**Proxy-only** deployment places the iPrism appliance out-of-band with only web traffic, which is re-routed through a third-party switch/router behind the Internet gateway. Recommended for evaluation purposes as it will not interrupt network traffic.

### Initial Installation of iPrism for Evaluation

Follow the steps listed in the Quick Start Guide included with your iPrism or the Installation Guide, which can be found at <http://supportdocs.stbernard.com>.

1. **Connect** one end of the Ethernet **patch** cable to iPrism's **Internal** interface. **Connect** the other end to a **non-mirrored port** on a switch connected to a test network.



## USER INTERFACE AND ADMINISTRATION



*iPrism* uses a web-based UI with a single integrated console and multiple admin roles:

### CONCEPTS

**Web-Based UI** is hosted on the iPrism appliance and enables all administrative tasks from system settings and maintenance to users and networks to profiles and filters

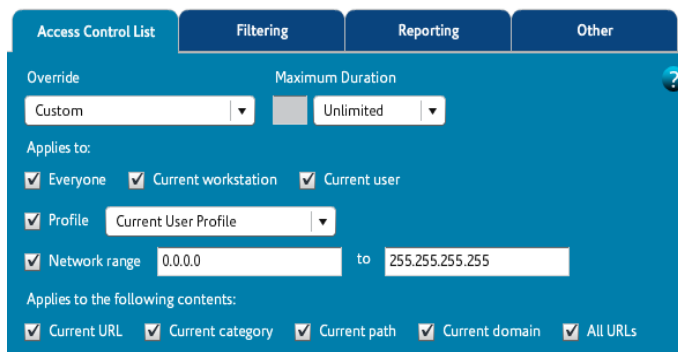
- ✔ System updates are automatically downloaded and installed on the iPrism appliance requiring no maintenance. Alternatively, administrators can be alerted by email and click one button.

**Admin Roles** enable multiple local or domain users with administrative privileges to granularly filter and report on different users, as well as granularly administer the UI

- ✔ Creating delegated administrators (i.e. business manager) reduce the time and effort for a system administrator to learn the particular needs of each business unit and support on-going maintenance requests, such as filter exceptions.

1. Topical, task-oriented video tutorials and contextual help windows are available throughout the interface. To view the help windows and tutorials, select the green help icon 

2. View the pre-defined admin roles and granular customizable privileges by selecting each role listed on the [\[Users & Networks > Admin Roles\]](#) page.



3. View the iPrism dynamic malware scanning engine [\[Profiles & Filters > Antivirus\]](#) 

4. View the new remote filtering feature [\[Profiles & Filters > Remote Filtering\]](#) 


5. View the system status dashboard [\[System Status > Status\]](#) 

## USER AUTHENTICATION AND IDENTIFICATION


*iPrism* uses transparent or manual user authentication:

### CONCEPTS

**Transparent user authentication** does not require any server- or client-based agents, or other network systems to be modified in Windows or Mac environments, by using iPrism’s embedded Kerberos, NTLM or LDAP authentication server.

 *In mixed Citrix or Terminal Service environments, client browsers are configured to forward traffic to a Citrix-ready™ certified iPrism appliance using proxy mode.*

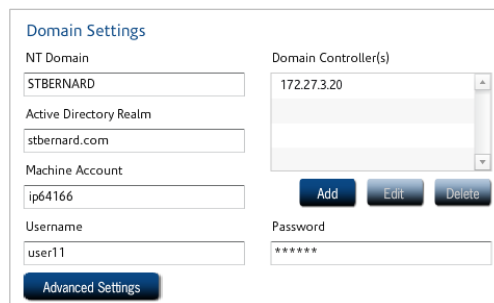
**Manual user authentication** requires users to enter local or domain credentials via a page sent by the iPrism appliance to access the web and report activity by username.

 *Both transparent and manual user authentication is allowed at the same time in transparent bridge and proxy deployments for the greatest flexibility and ease.*

### Initial Setup of iPrism for Evaluation

1. Integrate your directory services using the **Configure and Join** option on the [[System Settings > Directory Services](#)] page. Select your Authentication mode and apply settings. The following directory services are currently supported:

- Microsoft Active Directory (Windows 2000, 2003 or 2008 supported)
- Novell eDirectory v8.7.3 or v8.8 (Novell Netware servers supported)
- Apple Open Directory (Mac OS X v10.4 “Tiger”, v10.5 “Leopard” or v10.6 “Snow Leopard” supported)



Domain Settings

NT Domain: STBERNARD

Active Directory Realm: stbernard.com

Machine Account: ip64166

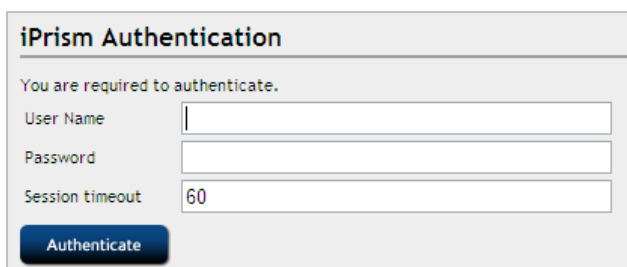
Username: user11

Domain Controller(s): 172.27.3.20

Password: \*\*\*\*\*

Buttons: Add, Edit, Delete, Advanced Settings

2. Setup and test manual user authentication [[Users & Networks > Networks](#)]



**iPrism Authentication**

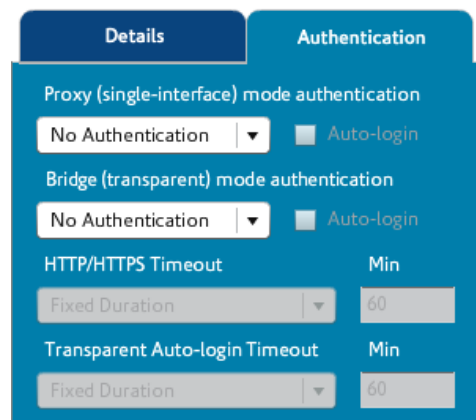
You are required to authenticate.

User Name:

Password:

Session timeout: 60

Authenticate



Details | Authentication

Proxy (single-interface) mode authentication

No Authentication | Auto-login

Bridge (transparent) mode authentication

No Authentication | Auto-login

HTTP/HTTPS Timeout: Fixed Duration | 60 Min

Transparent Auto-login Timeout: Fixed Duration | 60 Min

## ACCEPTABLE USE POLICY (AUP) FILTERING AND MANAGEMENT



*iPrism* uses a profile and exception-based framework with independently defined alerts:

### CONCEPTS

The **Web Profile** is used to filter web requests and the **IM/P2P Profile** is used to filter application traffic. Each profile applies **Access Control Lists** (ACLs), which specify web categories or application protocols to monitor (log) and/or block, to daily time periods in a weekly schedule. One Web Profile and one IM/P2P Profile is allocated to:

- **Groups** (sets of domain users defined in the integrated directory service) or **Local Users** (individuals with credentials defined in the iPrism configuration), which are identified by user authentication and processed top-down.
- **Networks** (sets of client or server machines defined in the network IP range), which are identified by requests' source IP address and processed top-down.

*For granular AUP frameworks, administrators create and assign a small number of relevant profiles to groups or networks. Next, the master or delegated administrator manages a smaller number of traffic, filter or override exceptions.*

- **Exceptions** ignore traffic coming from or going to a range of hosts (i.e. internal server).
- **Custom Filters** adapt ACLs to each customer's specific needs (i.e. URL categorization).
- **Current Overrides** adapt AUPs to each user's specific needs (i.e. time-limited access).

*For greater AUP control, the administrator has the ability to lock settings of web categories and application protocols within all ACLs that no one will be able to modify. This can or cannot be extended to applicable filter or override exceptions.*

- **Alerts** send administrators an email if specific web activity for specific users, profiles, IP ranges, or anyone exceeds a granularly defined threshold over specified time spans.

## Evaluate iPrism's Web Filtering

### 1. Create a Web profile [[Profiles & Filters](#) > [Web Profiles](#)]



Goal: Flexibly block recreation categories during work

Profile Name	ACLs
PassAll	ACL 1
BlockOffensive	ACL 1
EvaluationAUP	ACL 1,ProductivityLoss

### 2. Allocate this web profile:



Goal: Identify users and/or workstations requesting web access. For basic evaluation, choose either **option a** or **option c**. For full evaluation, choose **option b**. More than one option can be used in evaluation deployment if multiple workstations and/or users are participating, or of course, in a permanent deployment.

- Enforce AUP by workstations residing in a particular subnet regardless of which domain or non-domain user is requesting access. [[Users & Networks](#) > [Networks](#)]
- Enforce AUP for domain users defined in this directory service group regardless of which workstation they use on any network. [[Users & Networks](#) > [Groups](#) and [Privileges](#)]
- Enforce AUP for guests and other non-domain users regardless of which workstation they use on any network. [[Users & Networks](#) > [Local Users](#)]

Order	IP Range	Web Profile	IM/P2P Profile
1	192.168.5.1 - 192.168.5.52	EvaluationAUP	BlockIMP2P
2	0.0.0.0 - 255.255.255.255	BlockOffensive	BlockIMP2P

Domain	Group	Web Access Profile	IM/P2P Access Profile
*	Students	EvaluationAUP	BlockIMP2P

Domain	Group	Privilege
*	Students	Single Override

User Name	Use Network	Web Profile	Admin Privileges
EvaluationUser	No	EvaluationAUP	Single Override

### 3. Request access to and override a blocked page.



Goal: View the end user experience.

Override Who

Current User [EvaluationUser]

By clicking finish now, the following override will be created:  
Including any changes you've made above.

Who: User [EvaluationUser]  
What: Domain: http://\*.music.com/\*  
Duration: 1 hours

Confirm Your Access Request

Here the details of your request:

Location: http://www.gambling.com/  
Email: admin@company.com  
Comments:  
Notification: yes

### 4. Grant the request [[Profiles & Filters](#) > [Pending Requests](#)] and revoke the override [[Profiles & Filters](#) > [Current Overrides](#)]



Goal: View the master administrator or delegated administrator experience.

Date/Time	URL/Domain	Category	User(s)/Workstation	Locked
10/09/2009 1:39 PM	http://www.gambling.com/	gambling	EvaluationUser (172.27.47.51)	No

Expires	Administrator	Profile	Rating Category	User(s)/Workstation	URL/Domain
9 Oct 2009 3:05 PM	EvaluationUser	EvaluationAUP	*	EvaluationUser (0.0.0.0-255.255.255.255)	http://*.music.com/*
9 Oct 2009 3:41 PM	EvaluationUser	EvaluationAUP	*	EvaluationUser (0.0.0.0-255.255.255.255)	http://*.gambling.com/*

### 5. Create a new alert [[Reports](#) > [Email Alerts](#)]


Alerts can be granularly created to detect and notify administrators of a wide range of suspicious or web activity that may prompt fine-tuning the AUP. For example, spikes in traffic bandwidth consumed by less productive web categories may disrupt mission-critical processes. Perhaps self-override permissions will need to be revoked or privileges removed entirely to resolve the situation.

## MONITORING AND REPORTING



**iPrism** uses a Real-Time Monitor (for real-time data) and uses Report Manager (for logged data) for pre-defined, saved and scheduled reports with integrated drill-down functionality:

**Real-Time Monitor**—allows administrators to observe all web requests and application traffic as it passed by destination, user, rating (category) or protocol, profile and various other attributes.

 **Advantage:** The requests may be filtered by any attribute either in advance or on-the-fly and the scrolling display can be paused to review the previous 25,000 entries.

**Report Manager**—allows administrators to review up to the last 65,000 logged requests by run and view now, run in the background to view later, or schedule many pre-filtered and sorted reports, some with embedded drill-down data. New reports can be created, run, saved and scheduled using a report wizard from scratch or based on existing reports.

**Schedules**—allow administrators to manage already scheduled reports.



**Tip:** Having more pre-defined reports may seem to save time, but having fewer pre-defined reports may reduce irrelevant clutter. Customer surveys have indicated it is a personal administrator preference; therefore, the decisive factors are the ability quickly create, save and run the reports most important to each administrator

## Evaluate iPrism Real Time Monitor and Reports Manger

### 1. Monitor all web activity in real-time [[Report Manager](#) > [Real-Time Monitor](#)]

Time	Type	User & IP Address	Profile	Action	Rating/Protocol	URL	Bandwidth
10:00:22 AM	Web	[Unknown]@192.168.5.52	EvaluationAUP	Passed	other sites	<a href="http://172.16.1.152/lc">http://172.16.1.152/lc</a>	429 bytes
10:00:22 AM	Web	[Unknown]@192.168.5.52	EvaluationAUP	Passed	other sites	<a href="http://172.16.1.152/lc">http://172.16.1.152/lc</a>	429 bytes
10:00:22 AM	Web	[Unknown]@192.168.5.52	EvaluationAUP	Passed	other sites	<a href="http://172.16.1.152/lc">http://172.16.1.152/lc</a>	429 bytes



**Goal:** Learn general web or application usage trends in the network environment and users or IP addresses with suspicious web requests or application activity. Help determine initial AUP and/or fine-tune AUP by creating custom filters and perhaps filter exceptions.

Filter:

### 2. Monitor filtered web activity in real-time

Time	Type	User & IP Address	Profile	Action	Rating/Protocol	URL	Bandwidth
09:28:47 AM	Web	evaluationuser@172.27.47.51	EvaluationAUP	Blocked	gambling	<a href="http://www.gambling.co">http://www.gambling.co</a>	n/a
09:28:59 AM	Web	evaluationuser@172.27.47.51	EvaluationAUP	Blocked	lingerie/bikini,specialized shopping	<a href="http://www.victoriassec">http://www.victoriassec</a>	n/a
09:29:14 AM	Web	evaluationuser@172.27.47.51	EvaluationAUP	Blocked	entertainment,Web Log(Blog)	<a href="http://cache.gawker.co">http://cache.gawker.co</a>	n/a



**Goal:** In some cases, there will be internal servers with automatic update services that create many hits (i.e. 192.168.5.52), which may make it difficult to view the most relevant web activity. The administrator will want to filter out these irrelevant web hits.

Web Monitor Settings	
Starting IP Address	0.0.0.0
Ending IP Address	255.255.255.255
User	All Users
Profile	All Profiles
Action	Blocked
Include Media	<input type="checkbox"/>
Category(s)	All Categories

### 3. Create an exception [[Users & Networks](#) > [Exceptions](#)]



**Goal:** Based on the real-time monitor observations, an IP address may need to be unfiltered.

4. Create a custom filter [[Profiles & Filters > Custom Filters](#)]

Based on the real-time monitor observations, a URL may need to be categorized.

Status	Location	File Types	Apply to sub-URLs	Action
Enabled	*://172.16.1.152	*	Yes	Local Allow

5. Report on and drill-down into web activity [[Report Manager > Reports](#)]

Based on the real-time monitor observations, the administrator may want to report on certain usage over a longer time period for a particular user or IP address.

"4pm" by User Name
"4pm" by IP Address
"4pm" by Profile
"4pm" details

6. Create and schedule a report

Schedule periodic reports to provide management with evidence of the product's ROI and effectiveness, to remediate AUP violations or infected clients, and for on-going compliance with regulations or corporate policies. For example, send a daily security-focused report.

Name ▲	Type	Owner
IM/P2P Detailed Report	IM/P2P Detailed	Predefined
IM/P2P Statistics Report	IM/P2P Statistics	Predefined
Web Detailed Report	Web Detailed	Predefined
Web Hourly Statistics	Web Hourly Statistics	Predefined

Report ▲	When	Last Run Status	Owner
Security Exploits and Malware (iprism)	Daily	Unknown	iprism

## NEXT STEPS



The following steps are recommended to evaluate a significantly-sized subnet or for a permanent organization-wide deployment. See the [Installation or Administration Guides](#) for details. Also, online [knowledgebase](#) articles are regularly written by St Bernard technical support personnel.

- Convert from manual user authentication to transparent user authentication:
  - Removes the requirement to force users to re-enter their credentials to gain web access.
- Convert from a proxy-only deployment to a transparent bridge (w/proxy mode) deployment:
  - Removes the requirement to configure clients to forward traffic to the iPrism proxy, enforces AUP for application traffic (i.e. IM, P2P), eliminates a potential point of failure, maintains 100% network and browser session integrity, and increases the system performance.
- Create and allocate an IM/P2P profile, then test that the AUP is enforced on a client machine.



# Evaluation Guide

## Version 6.4

©2001-2010 St. Bernard Software, Inc. All rights reserved.  
The St. Bernard Software logo, iPrism and iGuard are trademarks of St. Bernard Software Inc.  
All other trademarks and registered trademarks are hereby acknowledged.

### Corporate Office

15015 Avenue of Science  
San Diego, CA 92128, USA

**Main Phone:** 858-676-2277  
**Toll Free:** 800-782-3762  
**Fax:** 858-676-2299  
**Email:** [info@stbernard.com](mailto:info@stbernard.com)  
**Web:** [www.stbernard.com](http://www.stbernard.com)

