Evaluation Guide

EdgeWave™

V7.100

iPrism Web Security

800-782-3762
www.edgewave.com

Evaluation Guide

iPrism Web Security

V7.100

Welcome to EdgeWave Web Security!

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

= Advantage

= Goal

Product Deployment and Network Implementation

iPrism uses either a transparent bridge (and proxy mode) or proxy-only deployment and supports VLAN environments.

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.

iPrism also recognizes and filters VLAN-tagged traffic in networks that use VLAN Trunking, and can participate in any 802.1q trunking environment, eliminating the need for separate appliances for separate VLANs.

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://www.edgewave.com/support/web_security/documentation.asp.

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.

Evaluation Guide

iPrism Web Security

V7.100

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.

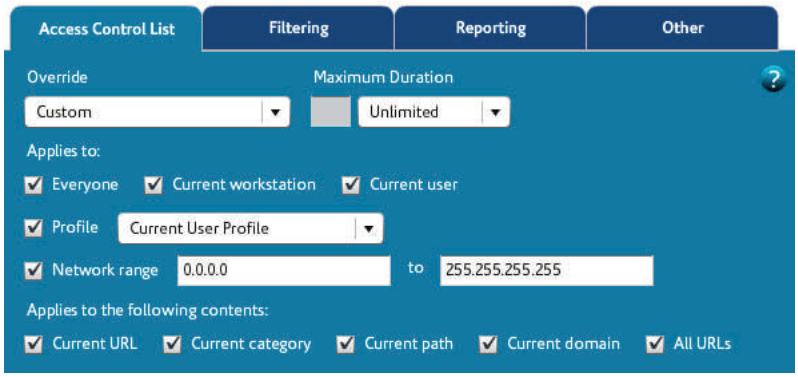
System updates are automatically downloaded and installed on the iPrism appliance requiring no maintenance. Alternatively, administrators can be alerted by email and click one button.

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) reduces the time and effort required 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 either transparent or manual user authentication:

Concepts

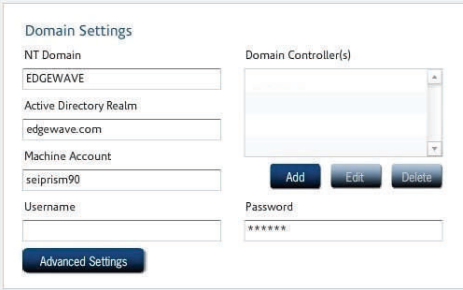
Transparent user authentication does not require any server- or client-based agents, or other network systems to be modified in Windows or Mac environments, by using iPrism's embedded Kerberos, NTLM or LDAP authentication server.

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.

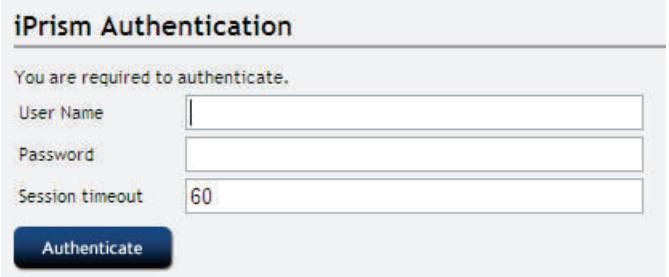
Both transparent and manual user authentication is allowed at the same time in transparent bridge and proxy deployments for the greatest flexibility and ease.

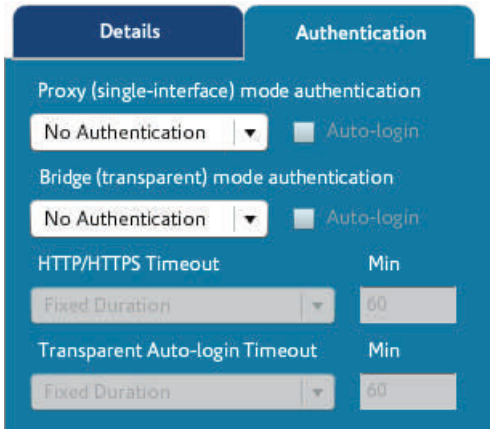
Initial Setup of iPrism for Evaluation



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)

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





Evaluation Guide

iPrism Web Security

V7.100

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, per 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 anges, or anyone who exceeds a granularly defined threshold over specified time spans

- iPrism also includes Quotas and Warnings. Quotas offer administrators the ability to set thresholds for either bandwidth or session duration for each category. Warnings inform end users that they are working outside the regular AUP, and inform them of any quota limits.

Quotas and Warnings help administrators better manage acceptable use policies and control bandwidth. They also serve as a valuable tool to educate end users on your AUP

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 work stations and/or users are participating, or of course, in a permanent deployment

a. Enforce AUP by workstations residing in a particular subnet regardless of which domain or non-domain user is requesting access. [Users & Networks > Networks].

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

b. 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].

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

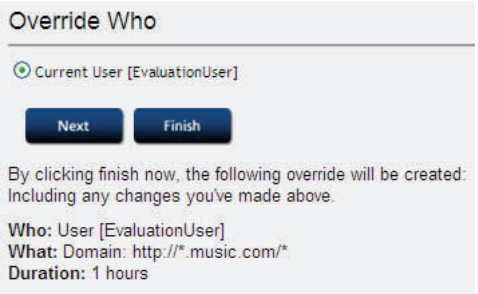
Domain	Group	Privilege
*	Students	Single Override

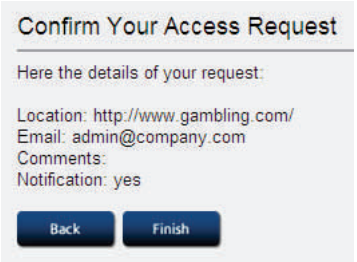
c. Enforce AUP for guests and other non-domain users regardless of which workstation they use on any network. [Users & Networks > Local Users].

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.





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 [Profiles and Filters > Quotas and Warnings].

Alerts can be granularly created to detect and notify administrators of a wide range of suspicious 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.

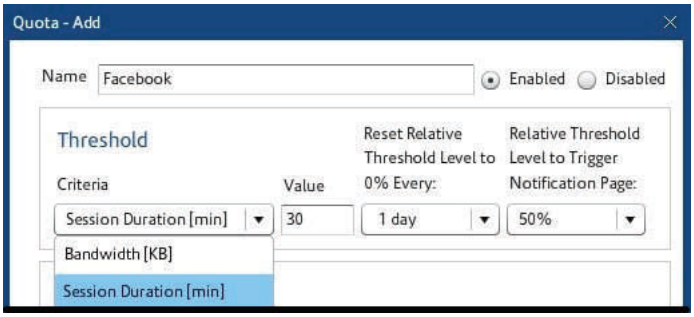
Evaluate iPrism's Quotas and Warnings

Evaluate Quotas and Warning after you set up Web Profiles

Goal: Set up a unique set of filtering rules for each group in the organization.

1. CREATE a Quota to be assigned to a Profile [Profiles and Filters > Quotas and Warnings].
   - Email Alerts, Quotas and Warnings are summarized on one page. Each tab provides details for each setting created.

2. ADD a new Quota based on parameters to suit your needs.



   - Provide a Name for your Quota and determine if you wish to notify for bandwidth usage or time duration usage.
   - Threshold levels may be set to restart after one day or one week.
   - Threshold levels can also trigger a customizable notification page to the end user after a percentage of use has been reached.

3. SELECT the Categories you wish to monitor

   - Selecting an ACL Category brings up a list of the categories seen when building the original Profiles.
   - Sub-categories can further define your selection if needed.

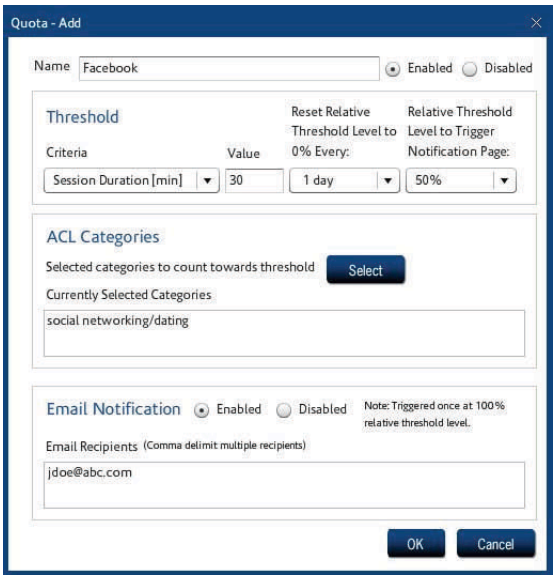
4. ENABLE email notification when threshold is reached.

- This option provides for email notification to one or more individuals once an end-user reaches a Quota at 100% threshold.

5. Click OK to complete.

- The settings shown here names the Quota Facebook, sets the duration to 30 minutes and alerts the user when 15 minutes has elapsed. Further, this setting notifies one user when the full quota is reached.

- In addition to Quotas, Warnings can be set up in a similar fashion under the "Warnings" tab of the same window. Warnings can be used to alert end users that they are being monitored when they are trying to access sites that don't necessarily have a quota associated with them, but are in violation of AUP.



6. ASSIGN the created Quota to a Profile.
   - Assign a Quota to the Profile you wish by going to [Profile and Filters > Web Profiles]. Click on the Profile and Edit the ACL.
   - Click the Assign Quotas and Warnings button in upper right-hand corner
   - Click on the box under "Assign" that corresponds to the Quota or Warning you wish to assign and click Save.

Assign	Name	Criteria	Value	Frequency	Categories	Notify At	Type
☑	Facebook	Bandwidth [KB]	1000	1 day	social networking/dating	50%	Quota
☐	Personal Banking	Session Duration [min]	30	1 day	finance	50%	Quota
☐	Sports	Bandwidth [KB]	1000	1 week	sports	70%	Quota

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	http://172.16.1.152/lic	429 bytes
10:00:22 AM	Web	[Unknown]@192.168.5.52	EvaluationAUP	Passed	other sites	http://172.16.1.152/lic	429 bytes
10:00:22 AM	Web	[Unknown]@192.168.5.52	EvaluationAUP	Passed	other sites	http://172.16.1.152/lic	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: blocked

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	http://www.gambling.co	n/a
09:28:59 AM	Web	evaluationuser@172.27.47.51	EvaluationAUP	Blocked	lingerie/bikini,specialized shopping	http://www.victoriassec	n/a
09:29:14 AM	Web	evaluationuser@172.27.47.51	EvaluationAUP	Blocked	entertainment,Web Log(Blog)	http://cache.gawker.co	n/a

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.

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	☐
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.

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

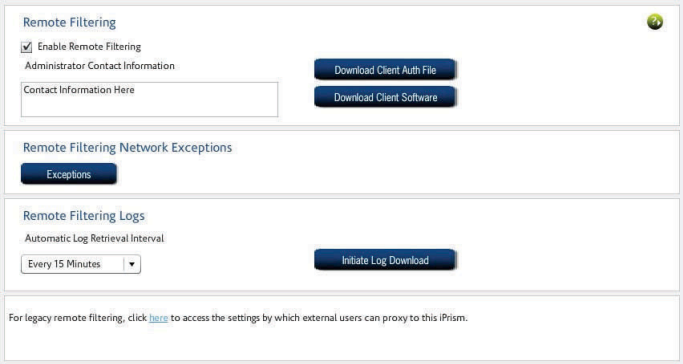
Report ▲	When	Last Run Status	Owner
Security Exploits and Malware (iprism)	Daily	Unknown	iprism

Remote Filtering

Evaluate Remote Filtering after you set up Web Profiles.

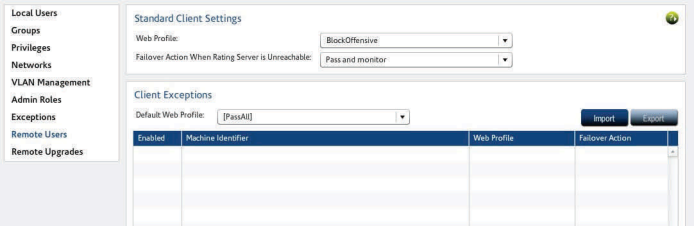
Goal: Set up a Profile to monitor and filter remote desktop and laptop users.

1. ENABLE Remote Filtering and download both the Client Auth File and Client Software once the Remote Filtering License Key has been activated.
   - Download Remote software from [Profiles and Filters > Remote Filtering]. The software, along with the Machine ID of the Remote laptop or desktop is used to enable Remote Filtering.
   - In the "Contact Information Here" section, type in the message you wish to send to the Remote User when a blocked page is accessed.
   - Determine how often you wish to retrieve Remote Reporting data.

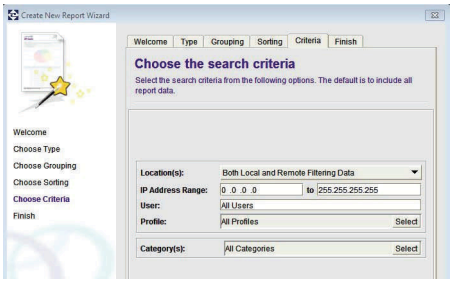


2. CREATE a new Profile [Profiles and Filters > Web Profiles] for use by Remote Mac and PC users.
   - Remote Users are assigned a Profile that may be the same or different from Local Profiles

3. ASSIGN the Profile to your Remote Users.
   - From [Users and Networks > Remote Users], choose the Profile you wish to assign the Remote PC and Mac Users
   - Exceptions to the Remote Profile can also be created.



4. REPORT on Remote User Activity
   - Reports can be generated for Local, Remote or both groups of Users.
   - Reports can also be generated to provide data on software updates for the Remote Clients if needed



Social Media Security

Concepts

Social Media Security offers the ability to seamlessly monitor, filter and report on social media activity through granular, policy-driven controls. Social Media Security enables real-time policy matching and enforcement across your organization.

- Granular Control — *Social Media Security includes standard policy templates that allow you to apply policies governing inappropriate content across your organization. You can define policies for different groups and social media applications as well as implement time-of-day rules to manage productivity.*
- Real-time Alerts and Automated Blocking at the Application Level — *When a policy violation is detected, Social Media Security can take many different actions. They range from blocking an individual post at the application level, to notifying the user or administrator of the violation, all the way to simply monitoring the content in reports.*
- Comprehensive Reporting — *Social Media Security includes real-time visibility into Web 2.0 activity and comprehensive reporting to help insure AUP and regulatory compliance. Reporting is customizable for date and time ranges per your organization's requirements.*

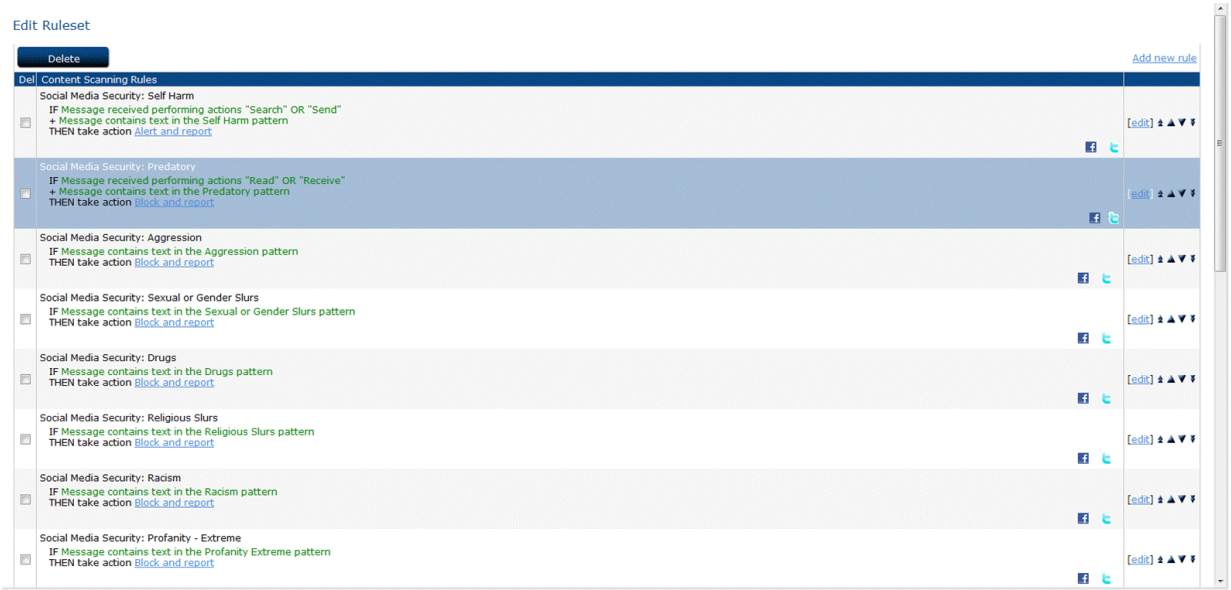
Evaluate iPrism Social Media Security

Goal: Set up Rules and Actions for Social Media Security

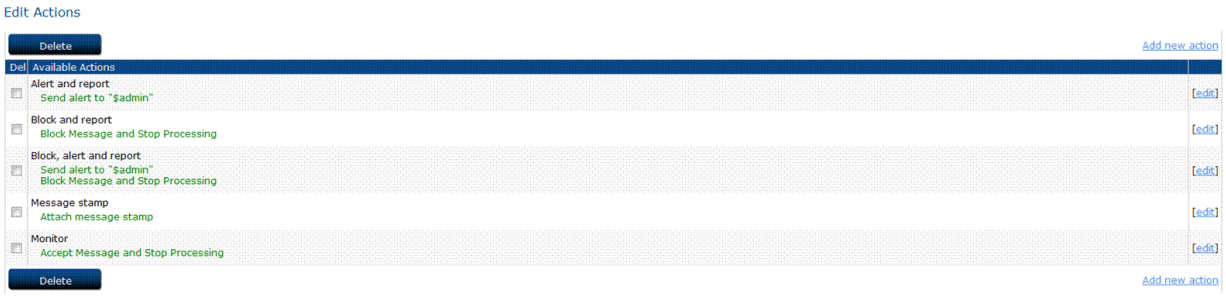
1. ENABLE Social Media Security by downloading and activating the license key
   - Save the activation key contained in your Welcome email to your desktop
   - On the iPrism home menu select System Settings, then License Key.
   - In the Upload License Key section, select Upload License Key and navigate to the Activation Key file.
   - Click on "Enable Social Media Security" and wait for provisioning to finish.
   - Once the provisioning is finished, the Social Networking > Social Media Settings screen will be enabled. You can now begin setting policy for Social Media users.

2. DEFINE General Settings and Organization Type
   - In the Social Networking > General Settings tab set up your general settings as well as your business type from the drop down list (Accounting, Automotive, Education, Healthcare, etc)
   - Click on Add Suggested Set - This will apply a pre-defined ruleset for the selectedorganization type. You can customize the pre-defined ruleset if desired in the next step.

3. REVIEW and EDIT your Ruleset
   - Review the suggested ruleset in Social Networking > Edit Ruleset
   - You can delete any rule in the set by selecting the checkbox in front of the rule. You can edit any rule by clicking on Edit.
   - You can add a new rule by clicking on Add New Rule. Follow the instructions on the next screen.



4. REVIEW and EDIT Actions
   - Each rule is associated with an Action to be taken if the rule is triggered. Review the suggested set of actions by clicking on Social Networking > Edit Actions.
   - You can delete or modify any action in the set by selecting the checkbox in front of the action.
   - You can add a new action by clicking on Add New Action. Follow the instruction on the next screen.
   - To connect Actions with Rules select a rule and connect it with an Action in Edit Rules



Goal: Run Reports for SOcial Media Security

1. To set up and run reports for Social Media activity, select Reporting > Social Media Security.
2. In the Reporting screen for Social Media Security select either a pre-defined report from the list, or create your own customized report from the selection on the screen.
3. Define your date frange for the desired report

Next Steps

The following steps are recommended to evaluate a significantly-sized subnet or for a permanent organization-wide deployment. See the Installation and Administration Guides for details. Also, online knowledgebase articles are regularly written by EdgeWave technical support personnel. You can find them here: http://supportdocs.edgewave.com

1. Convert from manual user authentication to transparent user authentication:
   - Removes the requirement to force users to re-enter their credentials to gain web access.
2. 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.

*Please keep the original box your iPrism evaluation unit arrived in. In the event that you need to return your iPrism after your evaluation, please contact Technical Support at **1-858-676-5050** for a Return Material Authorization (RMA) number. You can return the unit in the original box it was shipped.*

*For further assistance submit a request at http://supportdocs.edgewave.com or contact iPrism Customer Support at **1-858-676-5050***

EdgeWave

15333 Avenue of Science, San Diego, CA 92128.
www.edgewave.com

Toll Free: 800-782-3762
Email: info@edgewave.com

Phone: 858-676-2277
Fax: 858-676-2299