
Release Notes for iPrism v. 6.0/6.010

Release Date: May 2008

Supported Upgrade Paths

- M-Series hardware with iPrism version 5.x can upgrade to v. 6.010 on the same appliance (applies to M500, M1200, M3100, M11000).
- h-Series hardware with iPrism version 5.1 can upgrade to 6.010 on the same appliance (applies to all h-Series appliances).
- For customers using iPrism version 4.2, an upgrade to 5.x is necessary. Then, upgrading to version 6.010 is performed.
- For all customers using version 4.2, 5.x and 6.010, your configurations will be applied to 6.010 after the upgrade is installed. If you buy a new h-Series appliance, you can restore the configuration file after activating the new appliance.

New Features

Filtering

- New Feature: Virus and Malware scanning. HTTP traffic is subjected to AV scanning. All HTTP responses are scanned 128 KB at a time.
- The following malware types are detected and blocked when the AV function is turned on.
 - Virus: File-based, boot sector, corrupted virus, backdoor proxy
 - Worm: Net worm, P2P worm
 - Other Malware: Adware, backdoor Trojan, bomb, denial of service, dialer, downloader, exploit, password stealer, spyware, virus generation tool, Trojan

Anonymizer

- Now available: Various anonymizer blocking hotfixes are rolled into this release. By default, all customers who choose to block sites that are categorized as anonymizers will automatically utilize the following features.
 - HTTPS (Non-standard or non-SSL) traffic on Port 443 is now strictly enforced by default.
 - HTTPS traffic is reported using domain names, instead of IP addresses where possible.
 - Anonymizer traffic is reported:
 - Some anonymizers are detected by inspecting traffic behavior; others are detected by using the iGuard database.
 - Proxy URLs are collected and message groups are monitored daily for new anonymizers. These results are distributed via iGuard updates as prequalified websites.
 - The http-proxy domain is reported when non-standard http-proxy traffic is detected.

Reporting

- Reporting of AV detection through new “Dynamically Detected Malware” category.

Configuration

- New “AV Scanning” configuration tab under “GLOBAL” menu to enable/disable AV scanning.
- Dynamic categories must be set to “block.”

Authentication

- No new features to the Authentication subsystem in this release.

System

- Transparent update of AV signatures through IUS so that new AV function for HTTP traffic is always up to date.
- Performance improvements, tuned for the h-Series appliances.
 - Various performance and stability improvements for all appliances.

Rating and Categories

- New Category: “Dynamically Detected Malware” with the following sub-categories.
 - Virus
 - Worm
 - Other Malware
- Category Change: The social networking/dating category is moved from under “sex” to “recreation.”
- Rating fix:
 - Some sites were wrongly categorized as “anonymous.”

Known Issues

- M-Series customers who upgrade and turn on the malware defense (AV) will experience slower throughput. Depending on the M-Series model and your throughput requirements, you may want to upgrade to the faster h-Series appliances. Contact your sales representative or reseller if you have questions. With malware defense (AV) turned off, you will not notice any changes in throughput performance.
- MSN doesn't always show the “Conversation being monitored” message when using the IM Filtering service.

Bug Fixes

Configuration

Bug 1764	Filter Manager displays stale request entries.
Bug 4700	Empty parentheses in iPrism Central Management Status Message.

Filtering

Bug 4922	<i>liburlrating</i> may stick in waiting for response from the rating engine.
Bug 6619	5.0 mobile filtering change caused no web access in proxy mode.
Bug 6679	Filter Update code in IUS server needs to check Filter list version.
Bug 6720	iPrism Policy handles profile type incorrectly.
Bug 6655	Advanced filter settings in the Filter Manager do not always work as expected when allowing or denying access.
Bug 6777	Some URLs are misclassified by the rating engine.

Authentication

Bug 2538	NTLM domain name validation now allows >15 characters.
--------------------------	--

Reporting

Bug 6611	In some instances, when upgrading, ERS does not behave as expected.
Bug 6614	5.0 Reports Guide discrepancy for Daily Scheduled Reports
Bug 6676	Social Networking/Dating category is now visible when creating a report.

System

Bug 6604	Memory statistics are now accurate.
Bug 6045	When user must authenticate, Adobe programs will not update without authenticating via a browser session first.
Bug 6261	Google updater gets blocked.
Bug 6629	One of the subsystems table does not get updated.
Bug 6680	Reduce file deletion time in iARP/Surfguard staging to 2 weeks.
Bug 6689	RDS hangs and takes up to 80% of CPU.
Bug 6695	BID version mismatch between what App Mgr sees and real version.
Bug 6718	Performance enhancements for all appliances
Bug 6723	Multiple rating engine instances running.
Bug 6860	Temp directory overflow of EOF is fixed now.