iPrism Release Notes

V 7.160 November 2013

iPrism 7.160 introduces hotfix and upgrade capability to iPrism along with several bug fixes and improvements

iPrism 7.160 runs ONLY with the new EdgeWave 1000g hardware. Upgrade to iPrism version 7.160 can only be applied to iPrism 7.150.

New Features

Software Upgrades

- Upgrades from previous 1000g versions are now supported.

LDAP Authentication

- LDAP authentication is now supported.

High Availability

- "High Availability" support has been bolstered in the UI and backend.

Appliance Update

- Reworked the Hotfix Manager

Bug Fixes from previous iPrism releases

The following problems/known issues reported in previous iPrism releases were fixed in iPrism 7.160:

Filtering Subsystem:

- Numerous filtering subsystem improvements for robustness have been made.
- Issues with policy identification have been fixed

Recent Blocks:

- Recent blocks in the UI are now properly populated

Authentication:

- Authentication timeouts after reconfiguration have been fixed.
- NTLM auto login robustness has been improved for the Chrome browser.
- Quotas and warnings are now enforced for authenticated users.
- Active Directory integration has had multiple issues fixed.

Failover:

- Improvements have been made to correct the occurrence of iPrism incorrectly moving to the "failover" state.

Reporting:

- Incorrect reporting of "unknown" users has been fixed.

Usage Notes

Installation

- New EdgeWave 1000g hardware is required for this installation.
- Similar to iPrism 7.150, this version of iPrism also requires 3 IP addresses to be defined. These addresses must be on the same subnet.
- 1000g hardware will accept your existing iPrism backups. Network configuration needs to be edited post restore to assign other IP addresses.

Best Practices

- Software Upgrades
  - Upgrades will default to "manual" application. It is advised to keep it in "manual" mode.
- Custom Filters
  - Duplicate "no authentication" custom filters can cause problems with the filtering subsystem and should be avoided.
- Antivirus
  - Antivirus is Off by default. It needs to be re-enabled after a restore.
- Reporting
  - The UI routes report may show values for the 198.51.100.* network. These routes are for internal use, local within iPrism and should be ignored.
- SMS in WCCP
  - In order to get SMS filtering to work in WCCP mode, user must enable SSL inspection at the global level. Then, if user desires to disable SSL inspection for users, user must disable it for each profile. This will ensure that SSL traffic makes it to the WCCP service, but it will not actually be decrypted there. Note that reported events will contain the IP address of the SSL hosts in this case, and not hostnames.

Known Issues

- Antivirus
  - Overrides for antivirus are not functional. Filter Exceptions should be used instead.
- Hotfix Manager
  - Rebooting from the hotfix manager is no longer supported. A note is provided indicating to use the main UI reboot area.
- Import Local Filters
  - Import of local filters may fail due to incorrect formatting of the previously exported data. If this occurs please contact technical support for assistance.
- Network Health
  - The Network Heath page reports an HTTP error rather than "fail" when invalid credentials are supplied.
  - The Network Health page reports a fail with valid credentials.
- Quotas and Warnings
  - Quotas and Warnings will not display their respective block pages for sites rated as 'other'
  - If a quota is reached on the 'other' category, quota e-mail notifications will be sent for each subsequent visit to a site rated as 'other'.
- Reporting
  - For Remote Filtering traffic, only Remote Session reports are available in this release.
  - Pages with detected viruses may show as passed initially in Real Time Monitor.
- Restoring Backup
  - When restoring backup to a cluster of HA paired systems, they may, after the mandatory reboot, come up in a failed state. Should this occur visit the HA configuration section and manually recover the systems.

- System Configuration
  - Changing the iPrism's configuration GUI IP address can result in the loss of connectivity to the configuration GUI from clients outside the iPrism's subnet mask. Any client within the iPrism's subnet mask will be able to connect to the GUI on the new IP address. Such a client should issue a reboot from the GUI to allow external clients' connectivity to the GUI.
- User Events Purge
  - When initializing a purge of user events (reporting data) from the UI, the events may not be correctly purged. If this issue persists please contact technical support for assistance.
- User Interface
  - If using Internet Explorer to manage the iPrism, only IE versions 9 and above are supported.

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