iPrism 7.150 introduces Gigabit throughput support to iPrism along with new features and improvements

iPrism 7.150 runs ONLY with the new EdgeWave 1000g hardware. Previous iPrism versions cannot be upgraded to iPrism 7.150.

7.150 New Features

Gigabit throughput

- Using the new EdgeWave 1000g hardware platform, iPrism 7.150 provides Gigabit throughput.

Antivirus

- iPrism 7.150 introduces a completely redesigned Antivirus solution that uses a Kaspersky SafeStream II implementation.

SSL Inspection, Man in the Middle

- iPrism can now detect, inspect and scan for AV HTTPS traffic. SSL traffic is rated based on the decoded URL and headers, and scanned for AV, as normal HTTP traffic is.

Reporting

- iPrism 7.150 reporting implements the most recent ERS reporting features and enhancements in addition to current iPrism reports.
- Reporting now implements single sign on.

WCCP

- Support SSL inspection.

Bug Fixes from previous iPrism releases

The following problems reported in previous iPrism releases were fixed in iPrism 7.150:

Overriding

- Corrections and improved stability in the overrides subsystem

User Interface

- Small cosmetic changes as well an update to the Technical Support contact information

Usage Notes

Installation

- New EdgeWave 1000g hardware is required for this installation.
- This version of iPrism 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

- **Antivirus**
  - Antivirus is Off by default. To enable Antivirus, go to the Profiles & Filters menu, select Antivirus, slide the switch to On. Note: AV needs to be re-enabled after restore.
- **Exporting Event Logs**
  - We recommend exporting of Event logs to a dedicated destination with at least 1TB of free space; data will be mirrored to this destination removing all other content. We recommend you contact Technical Support for assistance in using this feature.
- **System Configuration**
  - It is recommended to make policy and network changes during low usage time or after hours maintenance windows. The iPrism's filtering can be unresponsive when saving and activating these changes.

Known Issues

- **Antivirus**
  - Overrides for antivirus are not functional. Filter Exceptions should be used instead.
- **Authentication**
  - "No Authentication" Exceptions on destination IP addresses may not function properly. Administrators should create Custom Filters using the No Authentication property as a workaround.
- **Custom Filters**
  - Import of local filters from previous versions may fail. Contact Technical Support for assistance.
  - If a user adds two NO_AUTH custom filter properties that have similar domains (i.e. one is *.domain.com and the other is domain.com) it may cause the filtering system to abort and not process requests. Should this occur, either remove the duplicated custom filters, or change their order in the list.
- **Filtering**
  - Websockets traffic is not supported.
  - The "Recent Blocks" page does not populate with data.
- **Quotas and Warnings**
  - Quotas and warnings are not enforced for authenticated users.
  - 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.
  - The user column in the Remote Session Report displays 0.0.0.0 instead of 'remote'
  - Pages with detected viruses may show as passed initially in Real Time Monitor.
- **SSL Inspection**
  - To support the SSL inspection feature, the system administrator will need to install the iPrism root certificate as an authority on all browsers on filtered devices.
  - Users will need to install the iPrism root certificate in order to use windows activation services.
  - When visiting the SSL inspection panel in the configuration UI, the value for the SSL Inspection Enabled checkbox will always be 'off' regardless of the configured setting. User may need to re-enable this checkbox in order to allow editing of the SSL exceptions. To turn off SSL inspection, the user can reenable and save the change, then disabled and save / activate the change.
  - In SSL Inspection, to Revert unsaved changes, user will need to logout of the UI and login again in.
  - The Enable SSL Inspection checkbox in the Web Profile Details window will always show as Enabled.

- **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 initiating a purge of user events (reporting data) from the user interface, the events may not be correctly purged. Please contact technical support for assistance.
- **User Interface**
  - Under System Status, the Routing Table and Status pages will show in accurate data.
  - VLANs are not supported in this release.
  - If using Internet Explorer to manage the iPrism, only IE versions 9 and above are supported.
  - Users may be prompted for credentials when launching the Hotfix Manager.
- **WCCP**
  - The only form of forwarding and return traffic supported is GRE.

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