ST BERNARD

iPrism® Release Notes

Contact Us 1-800-782-3762
www.stbernard.com

iPrism v.6.500

February 2011

iPrism v6.500 adds new, expanded or enhanced features, rolls up hotfixes added since iPrism v6.410, and resolves bugs from previous releases. Also, information is provided in regards to restoring configuration backups, upgrading iPrism code, and known issues.

New Features for 6.5

Outbound Anti-Botnet Protection

- **WHAT?** Adds a simple "set and forget" checkbox in Profiles & Filters > Application Profiles > Profile Details > Access Control List for Security Exploits > Botnet
  - Near-zero false positives and without constantly tweaking reputation score threshold or signature/pattern rules like many other solutions
- **HOW?** iPrism Web Security leverages the ThreatSTOP Botnet Threat List to bring an additional layer of defense to your gateway security by protecting your organization from dangerous botnet attacks. By enforcing the ThreatSTOP Botnet List, which is continuously updated, iPrism Web Security is able to block any attempt at an outbound connection and instantly mitigate botnet damage.
  - Improved time to detection by blocking emerging botnet threats at their source, which is estimated to provide an additional 5-10% catch rate on top of existing AV/IPS-based endpoint, network or gateway solutions
  - Adds no network latency and reduces potential bandwidth loss & peak loads
- **WHY?** Bot-related malware is much more evasive and costly to remediate than other viruses, malware or spyware, which might slow down machines and interfere with productivity, but not cause significant financial losses. And the real damage is done by the botnet hosts, not the bot-related malware. Bots are, for the most part, harmless until they "call home", via any protocol and port, to their command and control botnet hosts outside your network. If its activation or other follow-up instructions are successful, it is highly probable that the bot will breach your network, download or propagate additional malware, and steal sensitive data or identities.
  - Mitigates damaging data leakage and other non-compliance events with preservation and non-repudiation of logged event

Circumvention Defense Network (CDN)

- **WHAT?** Adds simple "set and forget" checkboxes in Profiles & Filters > Application Profiles > Profile Details > Access Control List for Anti-Circumvention
  - Circumvention tools including UltraSurf, Tor and JAP are fully monitored and/or blocked
  - Later without waiting for a new product release, FreeGate and Other Client Anonymizers will be added, or protection enhanced for any newly updated application versions
- **HOW?** Virtually runs applications using 100s of frequently-reset virtual machine instances covering multiple versions and OS/config permutations in a scalable cloud data center, with the dynamic ability to add new software when released. Dynamically captures IP addresses associated with the 1,000s of proxy/re-routing servers that the circumvention tool attempts to connect to in real-time. Correlates and filters the IPs from all virtual machines, comparing to legitimate websites hosted on shared servers via the 100% human-reviewed iGuard analysts, and continuously purge old entries for certain applications with rapidly changing networks. Inspects and enforces communication attempts over any port per user- and/or network-based policy by combining threat list and behavioral enforcement techniques.
  - Current solutions relying only on protocol pattern or other behavioral on-box rules often either over-block Web access or under-block the application
- **WHY?** Circumvention tools not only bypass acceptable use and security policies, but they create huge network security holes that are hacker portals for data theft, malware, spyware and viruses. End users unknowingly trust strangers hosting proxy/re-routing servers used by circumvention tools, which can log their activity off your network and/or hijack the content they transmit and receive.

ST BERNARD

iPrism® Release Notes

Contact Us 1-800-782-3762
www.stbernard.com

Enhanced User Authentication

- Failed Login Options: If an on-box or external failure prevents iPrism from successfully authenticating a user (auto-login or page-login), the user may optionally be transparently filtered by the profiles mapped to the network range and Internet activity logged by IP address. Additional selections available in Users & Networks > Networks > Profiles > Authentication.
- Increased Performance: In maintaining the latest Microsoft best practices, we will achieve two to three times more efficient domain controller queries. No GUI changes.
- 1-Way Outgoing Trusts Supported: iPrism previously required Active Directory domain controller 2-way trust to access users in domains on a different controller than the primary controller specified in the directory service integration setup. No GUI changes.
- Nested Groups Supported: When detecting users within Active Directory Domain groups, membership within a sub-group nested in a parent group is recognized. No GUI changes..

Expanded Application Control

- Filter Skype Communications: iPrism now detects and applies policy by user or network to Skype's encrypted proprietary Instant Messenger protocol over any port. Adds a simple "set and forget" checkbox in Profiles & Filters > Application Profiles > Profile Details > Access Control List.
- Filter FTP Communications: iPrism now detects and applies policy by user or network to the File Transfer Protocol (FTP) over any port. Adds a simple "set and forget" checkbox in Profiles & Filters > Application Profiles > Profile Details > Access Control List.

Other

- Enhanced Remote Filtering Service: As custom filters are added, edited or deleted via the on-premises appliance they are frequently synced with the policy uploaded to the off-premises Cloud Data Center operating the Remote Filtering Service (requires subscription and activation of service). No GUI changes.
- Enhanced WCCP L2 Redirection Support: iPrism now supports both Layer 2 and GRE redirect, return and assignment methods. Please contact Technical Support for setup of this configuration.
- Enhanced SSL Certificate Management: Improved uploading of certificates and provides a cleaner user interface for creating and viewing certificate requests. New options available in System Settings > License Key.
- Enhanced LDAP Server Load Balancing: Supports newer Novell eDirectory versions that use IP and/or TCP formats. No GUI changes.
- New Health Monitor: Alerts a 3rd-party device, such as a load balancer, that user authentication or other sub-systems are failing. New options available in System Settings > Network Services.
- More Granular Anonymous Browsing Control: iPrism blocks web-based anonymizers using the hourly-updated, 100% human-reviewed iGuard database ratings, as well as advanced real-time rules to dynamically detect web proxies. Now network admins can monitor and/or block both techniques via separate categories. Two sets of checkboxes in Profiles & Filters > Web Profiles > Profile Details > Access Control List for Internet > Anonymizer or Dynamically Detected Proxies.
- New iLearn Tutorial: To step through and explain authentication settings and options. Video is linked in Users & Networks > Networks > Profiles > Authentication.

Restoring Configuration Backups

Restore from an iPrism version prior to v6.500 will not automatically set policy dispositions for the new Anti-Circumvention (UltraSurf, Tor, JAP, etc) or Security Exploit (Botnet) application categories, nor the Skype or FTP protocols. Please be sure that you select your desired policy upon completion of a restore.

Supported Upgrade Paths

Upgrade from an iPrism version no earlier than v6.221.

Important Notes and Known Issues

We have qualified* iPrism monitoring with these application versions:

- UltraSurf v10.06 US/Europe/Asia
- JAP / JonDo v00.13.006
- Tor exit nodes
- Skype v5.1.0.112

* Note: Additional application versions can be rapidly qualified as needed

- **Application Profiles > Skype & UltraSurf:**
  - Clients that have active Skype sessions, or Skype sessions that have terminated within the last several hours, may initially continue to function after configuring a profile to block Skype. This is due to Skype client caching. Rebooting the workstation should resolve this.
  - If using Skype is part of your daily business and you choose to monitor Skype, this can add significant reporting data.
  - If UltraSurf is being actively blocked, occasionally Skype will make successful connections even if the profile is set to Block.
- **Authentication:**
  - Failed Options
    - Selecting "Use Network Profile" or either of the Advanced Auto-Login settings in a Network Profile is only fully functional in bridge mode and transparent proxy (WCCP) mode. It is not implemented for direct proxy mode (i.e. for Citrix or Terminal Services).
  - Proxy mode, basic manual login:
    - For users who have a single override privilege, in order to execute that single override, the user must have authenticated as domain\user as noted above. (Bug 9344)
- **Custom Filters:** Customers with Remote Filtering are advised to limit the number of categories for a single custom filter to 5, and limit the total number of custom filter entries to 2000. Any additional will be ignored by the Remote Filtering clients
- **Health Status:** The new feature of checking the Health Status of an iPrism requires that the Health Status field be enabled in System Settings/Network Services. If disabled, the URL path will return a 404 error.
- **ERS:** Our Enterprise Reporting System has not yet been updated with the features and functions present in 6.5. This means that new Application protocols will not be represented. (Bugs 9310, 9311)