

iPrism v6.2xx

Release Date: January 2009



Supported Upgrade Paths

- M-Series hardware with iPrism version 5.0 to 6.2 can upgrade to v6.2xx on the same appliance (applies to M500, M1200, M3100 and M11000).
- h-Series hardware with iPrism version 5.1 to 6.2 can upgrade to 6.2xx on the same appliance (applies to all h-Series appliances).
- If you have iPrism version 4.2, you will have to first upgrade to iPrism version 5.x. Then, you can upgrade to version 6.2xx.
- For all customers using version 4.2 and above, your configurations files will be applied after the upgrade(s) are installed. If you buy a new h Series appliance, you can restore the configuration file after activating the new appliance.

STBERNARD 
iPrism[®]

New iPrism 6.2xx Features

Authentication

- iPrism version 6.2xx allows you to have multiple Super Admin accounts. This is important for customers who need to secure user names and passwords by not sharing. Now, if you require more than one local administrator, you can give multiple administrators' unique names and passwords, simplifying iPrism management across your enterprise.
- Block Page Re-Authentication allows you to designate an additional threshold for authenticating users at the block page. By enabling this feature, you can allow all traffic without authentication until a threshold is reached (usually very restrictive). At that time, a user can authenticate and receive a less restrictive policy. This is used for implementations when management does not want to track/block Web traffic by user until a certain threshold is reached. To read more about this new feature, please go to <http://www.stbernard.com/products/support/iprism/help/IP0480.htm>.

Reporting

- Added: A new report template for "Web Top Domain (Grouped)." This feature allows you to run a top domains report by user, IP address or Profile.
- Added: A predefined report that automatically selects all malware-related ACLs as criteria and generates a detailed report of this activity. Because this report includes both pre-categorized (URL) and dynamically detected malware, you receive a comprehensive view of all the malware being blocked from your network.

Utilities/Tools

- Standard Network Management Protocol (SNMP) support is now available. Using the standard port 161, you can use any MIB browser to locate and view a variety of Object Identifiers (OID) to help monitor the health of your iPrism appliance in real time. There is a community string available and iPrism uses standard MIB-2 with SNMPD for FreeBSD.
 - Note: OID ".1.3.6.1.2.1.1.3.0" for sysUpTime will provide the time since last boot or policy apply (which ever is of shorter duration).
 - Note: The SNMP device PEN = 12325. In later releases, we will modify this value to a unique St. Bernard Software iPrism identifier.
 - Note: OID ".1.3.6.1.2.1.1.6.0" for sysLocation will provide the time zone selected for that iPrism.

Bug Fixes

Anti-Circumvention	
Bug Various	Some SSL sites would not load in a timely manner or were blocked as potential anonymizer sites. These SSL implementations have been identified and now load properly. In addition, HF 2-510 was included in this release. This fixed some examples of these false positive, anonymizer sites.

Authentication	
Bug 4622	Designate OU when joining AD domain instead of only default OU.
Bug 5137	Increased username + domain allowance from 31 to 127 characters
Bug 6537	NT LAN Manager (NTLM). For NTLM authentication, we now support escape and non-standard characters (e.g., " , ' and \).
Bug 6812	Code added to prevent hanging during authentication processes.

Configuration/System Management	
Bug 6964	Central Management Slave email upgrade to connect to correct Master IP address.
Bug 6999	Inclusion of HF 2-444. Changes Central Management default so that the domain controller for each Slave is set using local configuration manager.
Bug 7067	Slave configurations now checked by Master every 15 minutes and updates can be manually pushed to Slaves.
Bug 7052	Central Management change to synchronize all Slaves whenever a Slave is promoted to Master.
Bug 7050/7053/7083	Various Central Management changes that repair/improve Master/Slave synchronization.
Bug 7048	In Central Management, the password field will no longer be pre-populated after changing the role from Stand-Alone to Master or Slave. The field is blank to prevent setting a password without knowing its value.

Database	
Bug 6968	Inclusion of HF 2-509. Fixes disk partitioning problems for larger appliances where excessive reporting data was backed up beyond the partition's specification. iPrism now monitors and prevents this issue.

Documentation/Help	
Bug 6929 / 6935	Added Central Management to Administrator and Installation Guides. Documentation enhanced and accuracy improved.

Filter Manager/Custom Filter	
Bug 7093	Timestamp added to pending filter manager requests.

Malware Detection	
Bug 6924	Fixes delays in loading pages with non-standard items when malware detection is turned on (for example: digg.com).
Bug 7279	Upgraded the Authentium malware detection library. In addition to better catch rate, solves a bug in Authentium causing crashes for some proxy-mode deployments.

Bug Fixes (cont.)

Policy Management/Enforcement

Bug 6690	Fixes Web profile manager to provide accurate results after unchecking an ACL to unlock and unmonitor in successive profiles
----------	--

Reporting

Bug 5903	All reports now sort accurately
----------	---------------------------------

Security

Bug 7110	Fixes Java Console transmission by encrypting all passwords when transmitted via Java UI.
----------	---

Traffic Classification (HTTP, IM, P2P, etc.)

Bug 6947	When configured for upstream proxy, traffic no longer receives an additional classification of "anonymizer."
----------	--