iPrism 8.0 induces new capabilities, including powerful secure web gateway functionality previously only available on our most powerful platform – to the entire fleet of iPrism G-series appliances.

NEW FOR ALL G-SERIES APPLIANCES IN 8.0:

• iPrism is now based on a high performance 64-bit Linux architecture.
• Real-time malware and AV scanning is available for all web content.
• Inspection of HTTPS/SSL sessions for policy enforcement and malware protection.
• Built-in Enterprise Reporting Server allows any 8.0 iPrism to be designated as an Enterprise Reporting Server to collect, consolidate and report on activity from multiple iPrism appliances.
• Reporting interface now supports integrated single-sign-on.
• ICAP integration allows iPrism to direct traffic to an external ICAP service for additional scanning, including DLP.
• WCCP support now allows HTTP and HTTPS processing in either SSL Inspection (interception) or Enforcement (pass-through) modes.
• Authentication timeouts are now profile based.
• Custom filter URL rewriting has been added.
• Additional notes fields are now available in many of the policy areas to assist with documenting the configuration.
• A console configuration menu has been added.
• Enhanced self-monitoring and health reporting capabilities for improved reliability.
• SNMP subsystem has been re-written and provides significantly more capability.
• Configuration history is optionally stored in EdgeCloud to facilitate restore of configuration.

IN SUPPORT OF EXISTING CUSTOMERS:

• Configuration backups from 7.111 H-series devices are supported for restoring on to 8.000 devices.

KNOWN HIGH-LEVEL LIMITATIONS:

• iPrism Social Media Security (iSMS) is not currently supported in 8.0, but is targeted for a future release. If you were using iSMS in an earlier version, iPrism 8.0 will not support this granular enforcement.
• VLAN support is not available in 8.0, but is targeted for a future release.
• High Availability active-passive failover is not supported in 8.0, but is targeted for a future release. If you’re restoring a backup file from a previous iPrism version in which HA was enabled, HA will be disabled in 8.0 during the restore process. NOTE: WCCP can be utilized as an alternative for active-active failover of HTTP/HTTPS network traffic.

OTHER KNOWN ISSUES:

• The status page does not show CPU nor internal or external interface statistics correctly.
• For system alerts to be delivered via email, a SMTP relay must be configured in system preferences.
• Fallback to basic mode authentication is not well supported.
• Under heavy load, Ethernet RX overruns can be observed but they are typically not problematic.

FUNCTIONAL RELEASE NOTES:

• The iPrism directory service join behaves in an unexpected manner when the iPrism has:
  1. Been joined to a Windows directory service and then backed up while the join was valid.
  2. Later disjoined or rejoined, even to the same directory service under the same machine account name.
  3. Been restored from the previously made backup.

The problem is due to operation of Windows Active Directory, in a manner that is correct and intentional, but counterintuitive to many.

  1. When a computer is joined to a Windows domain, a machine account is created in Active Directory. This machine account has a name corresponding to the hostname of the joined computer, and a Security ID and cryptographic secrets unique to this machine account instance.
  2. When a computer is disjoined from the domain, the machine account is destroyed. The security ID and crypto are also destroyed and not reused.
  3. When a computer is rejoined, it receives a machine account that is (again) named according to the hostname, but is no longer the same machine account as was when the computer was previously joined, and therefore it has a different security ID and crypto bits.

If the computer (e.g. iPrism) tries to reuse the security ID or crypto secrets that were backed up when it was previously joined and later restored, they will be invalid and the iPrism will be unable to authenticate to the domain controller. This is intended and is working as designed.

The correct action when this condition is encountered is to disjoin the iPrism from the domain, then rejoin (using the same machine account name and administrator credentials, if these are still valid).

• Dropbox configured to use proxy will attempt to use plaintext passwords and these are not supported by iPrism for security reasons.
• In soft failover:
  1. If failover is set to pass all traffic, authentication that would otherwise be performed will not be performed, and traffic that would otherwise be blocked will be passed.
  2. If failover is set to block all traffic, all direct proxy requests will be blocked immediately. The administrative UI will remain usable.

In soft failover, events for direct proxy requests will not be logged.

• An iPrism that is upgraded or restored from an earlier backup will support “Via headers”. If it is necessary to suppress Via headers (For example, to access Yahoo services with SSL Inspection enabled), the administrator must go to the System Settings - Proxy page and uncheck the Via headers box.

• After enabling Malware and AV scanning, the scanning process will not be active until the system has downloaded an updated malware definitions file. This can take up to 15 minutes before malware and AV scanning is fully functional.

• There are known incompatibilities with iPrism NICs negotiating a connection with Netgear switches. The recommendation is to use higher quality switches for networking with iPrism.

• Off-box syslog is the only supported method of sending events. FTP and Email are not supported in 8.0, and have been removed from the admin interface. Certain issues may arise in off-box syslog use so please contact tech support if this functionality is required.