iPrism 8.001 provides the new functionality of the 8.0 release to certain h-series appliances. For g-series appliances, iPrism 8.001 provides numerous bug fixes to the 8.0 release.

**Note:** Please apply service packs SP1, SP2, and SP3 after installing v8.001 for additional bug fixes.

**APPLICABLE APPLIANCES:**

This release is supported on the following platforms:

- h-series appliances: 35h, 55h, 105h, 500h
- g-series (1st generation): 1000gR1 (released 2013)
- g-series (2nd generation) appliances: 35g, 75g, 150g, 500g, 1000gR2 (released April 2015)

Please note: The 15h and 25h appliances are NOT supported in this release, but will be supported in the v8.1 release.

**Important h-series appliance notes: (Please read before upgrading)**

1. All h-series systems must have a BIOS adjustment made to remap memory and support VT-X instructions. For instructions on making these changes, please see the appliance upgrade guide for your model on the iPrism documentation website

2. Certain h-series hardware requires memory upgrades in able to run v8.001 software. Please see knowledge base article: iPrism 8.001 Memory Upgrade Requirements – h series to order the proper memory. For instructions on installing memory, please see the appliance upgrade guide for your model on the iPrism documentation website

3. Do not upgrade from iPrism v7.x if you require the following functionality, which is not yet available and is targeted for a future release.
   - Prism Social Medial Security (iSMS)
   - VLAN support
   - High-Availability active-passive failover - NOTE: WCCP can be utilized as an alternative to provide active-active failover of HTTP/HTTPS network traffic.

4. 8.001 introduced a new SSL inspection capability for applicable h-series appliances. This allows SSL encrypted web pages to be inspected for policy enforcement and malware protection. If enabled, SSL inspection is processor intensive and can result in up to a 40% performance impact on h-series appliances. Without SSL inspection enabled, performance is similar to v7.x software. There is no performance impact when upgrading g-series appliances to 8.001.

5. Please reference the iPrism documentation website for information on how to perform an h-series software upgrade which requires steps to backup your configuration, save your event file, and boot from a USB drive image.
6. If you have a 1st generation 1000gR1, please contact support for assistance with your upgrade to 8.001.

CHANGES SINCE THE V7.11X RELEASE (H-SERIES APPLIANCES):

- 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 8.001 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.
- The console configuration menu has been updated
- A new front-end apache server is running on iPrism.
- 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.
- Configuration backups from 7.111 h-series devices are supported for restoring on to 8.001 devices.
- The admin can now enable serial port console via the console menu. When this is enabled all console output is vectored to the serial port
- New commands in the console menu under backup/restore provide for importing events from USB media or FTP services (see corresponding hotfix for 7.111 systems and the existing 7.11x ftp export functionality)
- SSL signing requests now support SHA2
- Malware and URL datafeeds are now pulled from Amazon S3
- OpenSSL libraries have been updated to 1.01k
- Event export is no longer supported. Please use scheduled reports instead.
- Network Health Status has been removed. An improved version of this will be available in a future release.
• DHCP during initial installation has been turned off. Use the console menu to assign an address to the system.
• WCCP V1 support has been removed from iPrism. All customers should migrate to WCCP V2.

Functional Considerations:

• Routing changes: iPrism 8.001 is a secure web gateway, meaning it transparently proxies traffic and performs full inspection on the content. To do this, iPrism needs to understand routes for any IP address it connects to. It is important that the default gateway configured on iPrism is the actual gateway that services all external networks and that specific gateways for internal networks are properly configured. Previous versions of iPrism bridged traffic and did not need to establish direct connections and could therefore function with less routing information.

• 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.

- Upon a restore from a 7.x version of iPrism, malware and AV scanning will be disabled by default. You will need to enable this in the user-interface if you want this functionality.

- 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.

- Co-management support is no longer supported in 8.001.

- The bypass local nameserver functionality is no longer supported since iPrism 8.001 now supports an integral high performance nameserver, which is required for its proper operation.

- Quotas and warnings in 8.001 will only function with authentication enabled.

- The Report Manager is not accessible from the Management port.

- Manual time adjustments are no longer allowed. iPrism time must be synchronized with a NTP server.

- In iPrism 8.001, any network that does not have a configuration defined for it will be blocked by policy. Create filter exceptions to allow these networks to pass through iPrism unfiltered, which is the default behavior of 7.x systems.

- After the Web server certificate is updated, iPrism admin sessions may not be logged out but will become invalid and cause errors when admin users attempt to save configuration. If this happens, log out of iPrism and then log back in.

- Certain Novell Auto-Login processing may fail. Workarounds for this include:
  - In Directory Service, always select “Legacy Profile Support”.
  - In Groups, always provide a mapping from group to Web profile and Application profile for each significant group.
  - When using secure LDAP (port 636, or TLS on port 389), set “TLS_REQCERT allow” in /etc/ldap/ldap.conf

- Implicit group to profile mapping is no longer supported. Create a direct mapping of groups to profiles in the user interface instead.

- When using Internet Explorer with iPrism, configure the iPrism to be in the “Local intranet” zone. Not doing so will cause Internet Explorer to fail to notify Hotfix Manager of the iPrism session, and Hotfix Manager will have to do an explicit authentication. To make iPrism be in the “Local intranet” zone, use the “Internet options” dialog and select Security -> Local intranet -> Sites -> Advanced. Enter the IP address or the fully-qualified name (FQDN) of the iPrism. (Don’t set “Require HTTPS”.) Alternatively, a domain administrator can propagate this setting to clients using group policy.

- Certain Sandisk based USB flash drives may not be used for imaging iPrism because they are not recognized as ‘removable’ by the operating system. Purchase another brand for use in imaging iPrism.
• Under conditions where network access to resources needed for iPrism operation is actively denied (for example, by a firewall that does not send ICMP “unreachable” messages), boot can take 4 to 5 minutes longer than expected.

• A filter exception that excludes authentication for an IP address (range) will not work in explicit proxy mode. In order to create an exception that excludes authentication create a custom filter with the NO_AUTH property set.

• 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.

**CHANGES SINCE THE V8.0 RELEASE (G-SERIES APPLIANCES):**

• Platform updates including new apache server front-end, Linux kernel and system software updates, and upgrades to the Postgres database.

• Syslog export is no longer supported for event logging. The rate of event logging now exceeds what is practical to perform via syslog.

• Network Health Status has been removed. An improved version of this will be available in a future release.

• DHCP during initial installation has been turned off. Use the console menu to assign an address to the system.

• The admin can now enable serial port console via the console menu. When this is enabled all console output is vectored to the serial port

• A warning is now displayed when an administrator enables SSL inspection. This warning references to our KB article on this topic

• General improvements to the system boot configuration have been implemented to make it more robust

• SSL Signing requests now support SHA2

• Various user interface improvements and documentation updates have been made.

• New commands in the console menu under backup/restore provide for importing events from USB media or FTP services (see corresponding hotfix for 7.111 systems and the existing 7.11x ftp export functionality)

• Certain cases where logfiles can fill up partitions in heavy operation have been fixed and log-file rotation has been improved.

• A bug in login script processing has been corrected

• A bug in certain HTTPS categorization has been corrected.

• WCCP V1 support has been removed from iPrism. All customers should migrate to WCCP V2.

• Improvements in the System Status page have been made

• IARP processing once again connects to the Edgewave back-end service correctly.

• Several reporting bugs have been corrected.
• Several authentication bugs have been corrected.
• The status page now shows CPU and internal/external interface statistics correctly.

Functional Considerations:
• After the Web server certificate is updated, iPrism admin sessions may not be logged out but will become invalid and cause errors when admin users attempt to save configuration. If this happens, log out of iPrism and then log back in.
• Certain Novell Auto-Login processing may fail. Workarounds for this include:
  • In Directory Service, always select “Legacy Profile Support”.
  • In Groups, always provide a mapping from group to Web profile and Application profile for each significant group.
  • When using secure LDAP (port 636, or TLS on port 389), set “TLS_REQCERT allow” in /etc/ldap/ldap.conf
• Implicit group to profile mapping is no longer supported. Create a direct mapping of groups to profiles in the user interface instead.
• When using Internet Explorer with iPrism, configure the iPrism to be in the “Local intranet” zone. Not doing so will cause Internet Explorer to fail to notify Hotfix Manager of the iPrism session, and Hotfix Manager will have to do an explicit authentication. To make iPrism be in the “Local intranet” zone, use the “Internet options” dialog and select Security -> Local intranet -> Sites -> Advanced. Enter the IP address or the fully-qualified name (FQDN) of the iPrism. (Don’t set “Require HTTPS”.) Alternatively, a domain administrator can propagate this setting to clients using group policy.
• Certain Sandisk based USB flash drives may not be used for iPrism imaging because they are not recognized as ‘removable’ by the operating system. Purchase another brand for use with iPrism imaging.
• Under conditions where network access to resources needed for iPrism operation is actively denied (for example, by a firewall that does not send ICMP "unreachable" messages), boot can take 4 to 5 minutes longer than expected.
• A filter exception that excludes authentication for an IP address (range) will not work in explicit proxy mode. In order to create an exception that excludes authentication create a custom filter with the NO_AUTH property set.