



## What's New in the R3000 '2.1.00' Version

*This newest release of software for the R3000 Enterprise Filter requires an R3000 unit running software version 2.0.12 or later. In order to use this software, a minimum of 2GB memory is required on a standalone R3000 unit, and a minimum of 3GB is required for an R3000IR 1U unit. This software version cannot be applied to an R3000IR mini tower unit.*

**NOTE:** 8e6 recommends applying this software update during periods of low network usage, as it will have a severe impact on the server resulting in a decreased filtering performance for approximately five minutes.

### New Features and Enhancements

- **Real time authentication means no logout, login for profile updates** – This feature resolves the need for end users to log out and back into the network again to obtain a different filtering profile, such as when a time profile or exception URLs should apply to the user's Internet accessibility. The R3000 now maps the authenticated user's IP address to the login name or distinguished name, or vice versa, so whenever a user needs to be using a different authentication profile, that profile is effective for the user in real time.
- **Time based profiles provide greater flexibility, also now available for NT / LDAP users** – This enhanced feature lets administrators create, maintain, and use time profiles that can be configured to run at a specific time each day, week, month, or year. A pop-up calendar makes it easier to configure these settings. Time profiles can now be set up for all NT and LDAP profiles.
- **Quota feature lets users visit specified sites for a defined time period** – This new filtering profile component (accessible via the Category Profile page) lets the administrator specify a set number of minutes/hits in which an end user can access a library category or category group before receiving a warning message or quota block page. If a specified number of minutes is defined for the Overall Quota, the end user can only spend that maximum amount of time at all quota-marked libraries/categories before being blocked from accessing URLs in any quota-marked library/category. If the end user is blocked from Internet access via the quota feature, he/she will need to wait until the quota is reset before accessing any Internet content.

This feature affects the following areas of the interface:

- The new **Quota Settings** window (System > Quota Settings) lets a global administrator specify the number of seconds that constitute a hit. This setting, along with the minutes specified in the quota, determine when the quota time has maxed-out and the user will be blocked from further access to URLs in that category, until the quota is reset. This window also lets the global administrator reset all quotas on demand, or set up a schedule for automatically resetting all quotas.

- The **Category Profile** tab in the Rules window (Group > Global Group > Rules window) and in any filtering profile in the Group tree now includes the Quota column where the number of minutes that constitute a quota is specified. The new Overall Quota field lets the administrator cap the time limit for all quotas included in a rule/profile.
- In the **Upload/Download IP Profile** window (Group > IP > group > Upload/Download IP Profile), quotas can now be included in IP/MAC address profiles. Enter quotas after the filter options using this format: A semicolon ( ; ), Overall Quota minutes, a comma ( , ), the first library category code, a colon ( : ), the number of quota minutes, and a comma between each quota. For example: ;10, EMPL:30, FINAN:30, GENBUS:30, TRADING:30, ESTATE:30
- In the **Upload User/Group Profile** window (Group > NT/LDAP > domain > Upload User/Group Profile), quotas can now be included in a quota.conf profile file and uploaded to the server. When creating the quota.conf file, enter the username, press the Tab key, and then enter quotas using this format: Overall Quota minutes, a comma ( , ), the first library category code, a colon ( : ), the number of quota minutes, and a comma between each quota. For example: 10, EMPL:30, FINAN:30, GENBUS:30, TRADING:30, ESTATE:30
- The new **Quota Block Page Customization** window (System > Customization > Quota Block Page) lets a global administrator customize the quota block page.
- The new **Quota Notice Page Customization** window (System > Customization > Quota Notice Page) lets a global administrator customize the quota notice page.
- In the **Real Time Probe Information** window (Reporting > Real Time Probe > Real Time Probe window > Go to Real Time Probe Reports GUI link > Real Time Probe Reports window > View tab > View button > Real Time Information window) the Filter Action column displays “Quota” if the user was blocked by quota time.

NOTE: The Real Time Probe email report also includes this information.

- **Upload/Download Global Profile feature removed** – The Upload/Download IP Profile global group window (Group > Global Group > Upload/Download IP Profile) has been removed due to enhancements made to group profiles management, and the similarities in functionality between this window and the Upload/Download IP Profile window for IP groups (Group > IP > group > Upload/Download IP Profile).
- **NT / LDAP entities are now assigned Sub Admin group administrators** – The group administrator for an NT or LDAP entity is now also known as a Sub Admin, and is set up in the interface by selecting “Sub Admin” from the new Type drop-down menu in the System > Administrator section of the administrator console.

A Sub Admin is assigned to an NT/LDAP entity in the Group tree via the new Assign to menu option. In the Assign Access pop-up window, choose from the available Sub Admin selections. The navigational panels for the selected Sub Admin can be viewed in the Assign Access View pop-up window. The Group panel shows the current entities (if any) already assigned to that Sub Admin.

NOTE: Group administrators for IP groups are still set up in the Group section of the interface, in the IP group branch of the Group tree.

- **Exception URL feature now accessible from all NT / LDAP branches of group tree** – This feature that has long been used by IP group members is now available to NT/LDAP entities. Using this feature, specific URLs can be set up to be blocked or bypassed in the end user's profile.
- **Exception URL included in NT / LDAP profile string** – Due to the inclusion of Exception URLs in NT/LDAP profiles, the structure of NT/LDAP profile strings have changed. When entering profile strings in an NT/LDAP file to be uploaded to the R3000 (Upload User/Group Profile), to specify that all filter options are disabled, "0x1" should be entered at the end of the profile string instead of a "0" (zero).
- **Safe Search Filter Option now includes Ask.com and AOL search** – The Google/Yahoo! Safe Search Enforcement option (Filter Options tab in the filtering profile) has been expanded to include Ask.com and AOL.
- **Existing rules can be used as templates when creating new rules** – When creating a new rule (Group > Global Group > Rules), if you wish to use an existing rule as a basis for the rule, select that rule, click New Rule, modify the existing rule as necessary, and then save that rule with a different name. NOTE: The Modify Rule button has been removed due to these functional enhancements.
- **Active Profile Lookup lets you see which profile the end user is now using** – This feature (System > Diagnostics > Active Profile Lookup) has been enhanced to include the Login Summary tab. This tab shows the IP group Domain name, end user's Profile name, Rule name (if one of the numbered Rules is used in that profile), and Profile Type (Regular, Global, Override, Lock, Time, TAR, or Radius profile). For time profiles, the Time profile name assigned to that profile also displays.
- **ICAP Operation Mode lets you set up an R3000 with a proxy server** – The new ICAP option (System > Mode > Operation Mode) is used only if this R3000 will function with an ICAP server to off-load content from the source R3000 server, such as Internet filtering. The ICAP Server Settings frame is used for configuring options response settings for the ICAP R3000 server. When an end user makes a request for Internet content, this request is routed to the proxy server, which then submits the request to the ICAP server. The ICAP server sends back a response to the proxy server—which may send the request to the original R3000 server in some network setups, and then return a response to the proxy server. Based on the end user's filtering profile, the proxy server either fulfills the request or returns a block page.

NOTE: When using the ICAP mode, the following items must be taken into consideration:

- In order for Tier 3 authentication to work correctly with the ICAP mode, the virtual IP used for authentication has to be a real and available IP address.
- The proxy server must be configured to not forward any traffic to the R3000's virtual IP (used for authentication) via ICAP, or else the Tier 3 applet will be blocked if the R3000 is configured to block uncategorized sites.
- To display block pages correctly and to prevent "looping," the proxy server must be configured to not forward any traffic to the R3000 via the ICAP server. Looping occurs in environments in which an R3000 is filtering traffic from end users to an internal proxy.
- Also to prevent "looping," if a custom URL is being used for the X Strikes block page, the proxy must be configured to not forward any traffic to that custom URL.

- In order for the authentication form to display correctly, the proxy server must be configured to accept the certificate coming from port 8081 of the R3000 as being valid.
- Since the authentication form is only accessible via HTTPS, the proxy server must be configured to give workstations access to HTTPS sites from the R3000.
- **Centralized Management Console (CMC) features available for synchronization** – This new feature lets a global administrator apply software updates on target servers using a Centralized Management Console (CMC) on a source R3000 server. If a target server fails, the source server can be set up to detect the failed server, notify the administrator about the failed "node" in the Range to Detect Settings window, and perform filtering for that server.

NOTE: If using the failover detection feature in which the source server performs filtering for a failed target server, Local Filtering on the source R3000 must be enabled, Troubleshooting must be disabled, there can be no mixed Operation Mode between the source and target servers (all servers must be using the same mode), and the Mobile mode cannot be used.

The 2.0.00 software release of the 8e6 Appliance Watchdog is required in order to use the failover detection feature.

These features affect the following windows and menus:

- The **Setup window** (System > Synchronization > Setup) now includes the "Upstream Failover Detect" checkbox in the Mode frame if the R3000 is set up in the Source or Target mode. If this checkbox is populated, the source server functions as the "upstream" R3000, and all target servers function as "downstream" R3000s. In the event that an R3000 "node" fails to filter, the source server will detect the failed node and filter that R3000.  
  
NOTE: If the "Library" Selective Synchronization option is used, the Global Group Profile might be used instead of the active profile.
- If a node fails, the new Node tab in the **Range to Detect Settings window** (Group > Global Group > Range to Detect) will display range to detect information from the failed server, if that server was set up in the range to be detected on the source server.
- If the R3000 is set up in the Source mode, the new **CMC Management menu topic** displays in the System navigational panel. This menu includes the Patch Management and Status options:
  - The **Patch Management window** includes the Patches frame that shows the software update statuses of the source and target R3000s.
  - When using the failover detection feature, the new **Status window** available from the CMC Management menu displays the filtering status of the source and target servers.
  - Due to the addition of the Patch Management window, the menu selection and former Patch window (System > Patch) have been renamed **Local Patch**. This new name implies the software update information pertains only to the current R3000.
- **Secure Log transfers to the ER** – This feature enhancement (Reporting > Report Configuration > 8e6 Enterprise Reporter) lets shadow log files be transferred to an ER through an HTTPS channel. The ER must be using software version 5.0.00 or higher in order for the R3000 to use this feature.

- **Library updates transfer now uses HTTPS** – The transfer protocol for libraries (Library > Updates > Configuration) is now set to use HTTPS instead of FTP for greater efficiency in transferring updates to the R3000.
- **Library Lookup now includes administrator email link** – The **Library Lookup window** (Library > Library Lookup) now includes the Email Result link at the bottom of the Lookup Result frame. If using a non-Web based email client such as Outlook, you can send an email to the administrator at your organization regarding a URL or search engine keyword that appears to be incorrectly categorized.
- **Block page variables now included in end user emails** – Emails received by end users for block pages can now include variables for customization.
- **New System Commands** – The following System Commands are now available (System > Diagnostics > System Command) for troubleshooting the R3000: “uptime(system uptime),” “df(disk usage),” and “dmesg(print kernel ring buffer).”