



What's New in the R3000 '2.0.10' Version

This newest release of software for the R3000 Enterprise Filter requires an R3000 unit running software version 2.0.07 or later.

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.*

WARNING 1: *If this R3000 has a custom category using the short name "PASSED", after applying this software update, that category will be renamed "RNPASSD". Any profile using the "PASSED" category will be modified internally to use the "RNPASSD" category. There will be no change in the way your profiles are applied to your end users, or in the end user's experience.*

WARNING 2: *After applying this software update, both the cache of your browser window and Java Control Panel on your workstation must be cleared in order to access the R3000 Administrator console. This may take up to 20 minutes. Please wait until both caches are cleared before proceeding.*

To clear the Java cache:

- **Windows Vista:** *Start icon in taskbar > Control Panel > Advanced Options > Java Plug-In*
- **Windows XP Pro:** *Control Panel > Java Plug-Ins > Cache > Clear*
- **Windows 2000:** *Control Panel > Java > General tab > Settings > Delete Files > Ok*

New Features, Enhancements and Fixes

- **Enhanced Password Format:** The enhanced password format improves security by requiring a more complex password with a minimum length of eight characters, one alpha character, one number, and one special character. This feature affects login dialog boxes used for accessing: the R3000 Administrator console, X Strikes Blocking Unlock Workstation window, or Real Time Probes View and Create windows.

Passwords for accessing these login dialog boxes are set up in the following windows: Administrator (System > Administrator), X Strikes Blocking (System > X Strikes Blocking > Logon Accounts tab), and Real Time Probe (Report > Real Time Probe > Logon Accounts tab). In these windows/tab, the "Name" or "User ID" fields have been renamed "Username". Passwords used when creating new IP groups (these passwords are later entered by group administrators in the login dialog box) are set up in the Create New Group (Group > IP > Add Group > Create New Group) dialog box.

- **New Account Expiration and Lockout Feature:** This new feature lets a global administrator specify settings for R3000 user passwords. Passwords can be set to expire after a specified number of days, prompting the user to enter a new password when attempting to access the interface. Users who enter an incorrect password to access windows in the R3000 after a designated number of attempts within a specified interval can be locked out of the R3000.

The following new windows are accessible via the new Secure Logon option available from the System menu:

- **Logon Settings** – This new window (System > Secure Logon > Logon Settings) lets global administrators set R3000 user passwords to expire after a specified number of days, and/or lock out the user from accessing the R3000 after a specified number of failed password entry attempts within a defined interval of time.
- **Logon Management** – This new window (System > Secure Logon > Logon Management) is comprised of frames used for viewing any usernames or IP addresses of users currently locked out of the R3000 due to an incorrect password entry attempt or an expired password. Only a global administrator can unlock a locked user account.
- **Unidentified Category Handling:** The Warn option is now available for specifying how the R3000 should handle Uncategorized Sites in a filtering profile (Global Group, group, sub group, individual, etc.). Selecting the "Warn" radio button at the Uncategorized Sites field indicates a warn message will display for an end user who attempts to access a URL for a site that has not yet been categorized by the R3000.
- **Expanded Pattern Blocking:** Pattern blocking on the R3000 has been expanded to include IM and P2P logging in addition to proxy pattern blocking. In the interface, this enhancement affects the Filter window (System > Control > Filter). The Service Control frame has been modified so that the option formerly named "Proxy Pattern Blocking" has been renamed "Pattern Blocking" to accommodate Instant Message and P2P logging. The Service Blocking frame that contained the "Instant Messaging" and "P2P" options has been removed.
- **New Method for Medium and High HTTPS Filtering:** The methods for HTTPS filtering with a medium or high setting have been enhanced to provide additional filtering options. In the interface, this enhancement affects the HTTPS Filtering frame in the Filter window (System > Control > Filter). If "Medium" is selected, by default the option is enabled for forwarding the DNS lookup in order to validate the hostname in the certificate. To disable this option, deselect the checkbox corresponding to "Forward lookup to validate qualified DNS". If "High"

is selected, by default the option is enabled for a library lookup to overrule the DNS validation of the hostname in the certificate. To disable this option, deselect the checkbox corresponding to "Library lookup to overturn DNS decision".

- **New Shadow Log Format for 2.0.10:** A new shadow log option has been added to the Shadow Log Format window (Report > Shadow Log Format). If this R3000 currently has the 2.0.10 or higher software version applied, the Post 2.0.10 log format option should be selected, since the ER 4.1.20 software version uses different logging methods for Medium and High HTTPS filtering.
- **Real Time Probe Report Recurrence:** The new Recurrence field in the Create tab of the Real Time Probe Reports window (Report > Real Time Probe > Real Time Probe Reports window > Create tab) lets you specify if the report should run "Daily". If the report runs daily, the View tab in this window displays "Daily" in the new Recurrence column.
- **Expanded Operating System and Browser Compatibility:** The R3000 interface can now be accessed using Internet Explorer 7 on a Windows Vista operating system, or Firefox 2.0 or Safari 2.0 on a Macintosh OS X 10.5 operating system.
- **AD Agent Download Link Re-instated:** The "Download 8e6 AD Agent Installer" link has been added back into the AD Agent frame in the Enable/Disable Authentication window (System > Authentication > Enable/Disable Authentication > AD Agent frame). Clicking this link opens a dialog box that lets you download the installer file.

NOTE: This version of the Active Directory agent does not support Team Mode (multiple satellites coupled to a primary agent). It is intended for single-agent installations only.

- **MAC Address User Limit Removed:** The number of MAC Addresses used for group profiles of R3000 Mobile Client users was previously capped at 200. This limit has been removed.
- **New Block All Rule:** The new "Block All" rule is now available in the Rules window (Group > Global Group > Rules). If this rule is applied to a profile, all categories and uncategorized sites will be blocked for the end user.