



Web Filter 4.1.00

M86 Security is pleased to announce the release of Web Filter software version 4.1.00. This software release requires a Web Filter (HL, SL, MSA) or IR (MSA) appliance running Web Filter software version 4.0.10 or later.

WARNING: M86 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. This update cannot be uninstalled.

NOTE: If using the synchronization feature in your environment, please note this software update cannot be installed on older hardware platforms: R3000 G, S and H models, and MSA and IR models sold until January 2008. Please contact your M86 account representative if you wish to upgrade your hardware in order to apply this software update.

FREQUENTLY ASKED QUESTIONS

Q. Which versions of Java are supported in this release?

A. This release supports Java 1.6.0_17 through 1.6.0_21. Versions 1.6.0_22 and higher are incompatible with this software upgrade.

Q. Can non-educational enterprises use the Approved Content feature?

A. Though the Approved Content feature is primarily designed for the educational sector, Web Filter users in other industries may find it useful to block all YouTube videos except those they wish their employees and/or visitors to access.

Q. What is VuSafe, and how does it apply to the Approved Content feature?

A. VuSafe is an online content library to which educators post approved videos for students to watch in a secure environment. This free Web-based service requires no additional software or hardware setup and supports the Approved Content feature.

Q. Does this Web Filter software release use a different port number than the one used in the previous software release?

A. No, the same port number (1443) for a secure "https" network connection is also used in this software release.

(continued)

NEW FEATURES

Approved Content gives users access to acceptable videos

The Policy section of the user interface now includes menu options for "Approved Content (incl. VuSafe)" under Global Group, IP, and LDAP branches of the tree for all profile types, including Time Profiles.

The Approved Content feature is primarily used by the education sector, giving instructors the ability to grant students access only to online videos they want them to view. Educators can choose from videos posted to YouTube or SchoolTube, or from VuSafe—an online content library to which they can post approved educational videos for students to watch in a secure environment. VuSafe removes all outside content on sites such as YouTube.com, eliminating access to inappropriate material. This free Web-based service requires no additional software or hardware setup.

To accommodate this feature, Approved Content Settings windows have been added to all node menus in the Policy tree. Approved Content Settings screens include the following objects that are used as follows:

- For the Global Group:
 - Checking the "Enable Approved Content (incl. VuSafe)" checkbox enables all profiles in the Policy tree to inherit passkeys entered in the Passkey list box.
- For all other profiles:
 - Radio buttons correspond to the following options: "Inherit Global Passkeys", "Disable approved content for this profile", and "Use specific passkey(s)". Choosing the latter option lets you add/remove passkeys in/from the Passkey list box, and not inherit any passkeys set up for the Global Group Profile.
 - The default option is "Inherit Global Passkeys".
 - If the Global Group Profile has the Approved Content feature disabled:
 - Any passkeys set up for the Global Group Profile will not be inherited. However, a profile can still use specific passkeys if "Use specific passkey(s)" is selected and the passkey(s) are entered in the Passkey list box.
 - If the Global Group profile has the Approved Content feature enabled:
 - Choosing the "Disable approved content for this profile" option in a profile indicates the profile will not use the Approved Content feature. Any passkeys that might previously have been entered and saved in the Passkey list box are retained but become greyed-out.
 - Choosing the "Use specific passkey(s)" option indicates the current profile will only use the passkeys set up in that profile and not any passkeys entered for the Global Group Profile.

(continued)

Web Filter 4.1.00

FAQs, continued

Q. If the synchronization feature is used in our environment, can one of the Web Filters be running a different software version than 4.1.00?

A. In a synchronization environment, all Web Filters must use the same software version. If this 4.1.00 software release is installed on the source Web Filter, all target Web Filters must be upgraded to 4.1.00. For a WFR in a synchronization environment, the compatible software version is 3.0.00. Due to hardware limitations in older Web Filter and IR models, if the 4.1.00 software upgrade is downloaded to the server, it cannot be applied. The server must be upgraded to a later model in order to apply the software update.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and 16 million users worldwide. As one of the largest independent Internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information, and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

Approved Content, continued

For Real Time Probes, the new "Approved Content" selection is available when choosing the Category selection for running a probe. Real Time Probe reports display Approved Content information in the Category column of Real Time reports.

New HTTPS filtering setting for proxy environments

If using one or more proxy servers, the new HTTPS Proxy Setting frame lets you specify the IP address of each proxy server, and allow HTTPS traffic to pass without being overblocked.

Access Authenticator and AD Agent via links to Web pages

Labels and links for downloading the M86 Authenticator and M86 AD Agent have changed in the System > Authentication > Enable/Disable Authentication window:

- Links for "Download M86 Authenticator for Windows" and "Download M86 Authenticator for Apple" have been consolidated to a single link now named "Download M86 Authenticator Deployment Kit." Clicking this link opens a Web page giving you access to links for downloading Authenticator installer files.
- The "Download M86 AD Agent Installer" link now points to a Web page giving you access to links for downloading AD Agent Installer files.

Security Reporter label added in Report Configuration UI

"M86 Security Reporter" labels have been added in the Reporting > Report Configuration window to indicate that an M86 Security Reporter can be used for receiving Web Filter logs, if a standalone Web Filter is used in your environment.

Security vulnerability issues resolved

Apache Tomcat has been upgraded to resolve security vulnerability issues.

Resolved Known Issues

- Go to <http://www.m86security.com/software/8e6/ts/r3000-rki.html> to view the resolved known issues for this software release.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 4.21.11

© Copyright 2010. M86 Security. All rights reserved

All text and figures included in this publication are the exclusive property of M86 Security. This document may not, in whole or in part, be copied, published or reproduced without prior written consent from M86 Security. Every effort has been made to ensure the accuracy of the content contained in this document. Such content is provided "as is" without warranty of any kind. M86 Security disclaims all warranties and conditions with regard to this content, including all expressed or implied warranties and conditions of merchantability, and fitness for a particular purpose. The company shall not under any circumstance be liable for any errors or damages of any kind (including but not limited to compensatory, special, indirect or consequential damages) in connection with the document's contents. Any information in this document is subject to change without notice.

M86 Security, the M86 Security logo and M86-branded products are registered trademarks under license by M86 Security. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies. All rights reserved.