Web Filter 5.0.10

Trustwave is pleased to announce the release of Web Filter software version 5.0.10, available for downloading to a virtual machine in an environment supporting Virtualization Technology. For Web Filter appliances, this software release requires one of the following models running Web Filter software version 4.2.00 or later: Web Filter 300, 500 or 700, R3000 HL or SL, or MSA or IR MSA sold after January 2008.

WARNING: By applying this upgrade, the legacy M86 Mobile Client and AD Agent will no longer be operable in your environment. If using the new Mobile Security Client (MSC) application, note that an IR or WFR cannot be used as a mobile server.

NOTE: If upgrading from software version 4.2.00, after applying this update, Web Filter 500 and 700 models with Cavium SSL accelerator cards will automatically reboot.

FREQUENTLY ASKED QUESTIONS

Q. What is MSC?

A. Introduced in the Web Filter 5.0 LA release, Mobile Security Client (MSC) performs Internet filtering and blocking on mobile workstations physically located outside your organization. This product uses a Web Filter configured in the mobile mode, certificates for authentication purposes, and the client installed on each mobile workstation. MSC replaces the legacy Mobile Client product.

Q. What are the advantages of using MSC instead of the legacy Mobile Client?

A. With MSC deployed, the following Web Filter features are no longer restricted for end users with mobile workstations:

- Minimum Filtering Level
- Time Profile
- Exception URL
- LDAP Authentication
- Warn and Quota filter settings
- Pattern filtering
- HTTPS filtering
- Extended URL Keyword filtering
- Safe search for Bing, AOL, Youtube, and Ask.com
- Custom block page redirect URL
- Always Allow feature for set categories

Q. Which versions of Macintosh OS are supported in MSC?

A. Using Macintosh with MSC, OS X versions 10.6 (Snow leopard) and 10.7 (Lion) are supported.

continued

NEW FEATURES AND ENHANCEMENTS

Web Filter Virtual and Mobile Security Client introduced in 5.0

See **What's New in Web Filter 5.0.00** for information about the Web Filter Virtual product and the Mobile Security Client (MSC) feature introduced in the 5.0 Limited Availability (LA) release.

NOTE: Override accounts cannot be used with MSC in this release.

Enhancements to existing Mobile Security Client features

The following enhancements were made to Mobile Security Client (MSC) since its introductory 5.0 release:

- When selecting "Mobile" in the Operation Mode screen (System: > Mode > Operation Mode), the new Block/Warn Page Settings frame displays with the LAN1 IP address of the server pre-populated in the Hostname or IP address to serve block/warn pages field. This entry should be modified if a server other than this mobile Filter will be serving block pages to mobile users.
- Using MSC in a synchronization environment:
  - All MSC settings can now be synchronized.
  - An IR or WFR can function as a source or target server, but cannot be used as a mobile server.
  - Only the source server will see Mobile and Certificate Management menus. When setting up a server as the source, these menus now automatically display.
- In the Certificate Management screen (System: Mobile > Certificate Management):
  - Certificate Management tab: "Internal Certificate Management" option is now available and is selected by default, instead of "Enterprise PKI"—the latter which requires an external server to sign, issue, and manage MSC-related certificates.
  - Certificate Authority tab: Field names have changed from State or Province to State or Province Name, City or Locality to Locality Name, Organization to Organization Name, and Organization Unit to Organizational Unit Name.

continued

Q. Can MSC be used in a synchronization environment?

A. Yes. A Web Filter set in mobile mode can be a source or target server. An IR or WFR Web Filter can function as a source or target server, but cannot be used as a mobile server. Only the source server will see the Mobile and Certificate Management menus.

Q. When upgrading to this software release, can a Web Filter still be set to use two modes, e.g. invisible and mobile modes, as in 4.2.00?

A. Since the 5.0 software release, the Web Filter can be set to use only one mode. If the Web Filter is set in the mobile mode, it will only function as a mobile server. An IR or WFR does not have the mobile mode option available.

Q. What are the differences between MSC's internal mode and external (PKI) mode?

A. The internal mode, new in this software release, lets you use the mobile Web Filter for issuing and managing all MSC-related certificates. Using the PKI mode, an external server (such as an LDAP server on your network) must be used for issuing and storing MSC-related certificates. In the internal mode, certificates can be issued to users with IP group profiles and/or LDAP user profiles. In the PKI mode, only users with profiles on the LDAP server can be issued MSC certificates.

Q. Can the MSC client be used in an environment with a Web Filter and a Secure Web Gateway (SWG)?

A. The client is designed to be used with either a Web Filter 5.0 (and higher) or an SWG 10.2 (and higher), but not in the same environment running both applications.

Q. Can the Web Filter Virtual application be used as a mobile server in a synchronization environment?

A. Web Filter Virtual functions the same as 64-bit Web Filter Appliance models—minus the appliance—for use in an environment supporting Virtualization Technology. In this environment, the Web Filter can be configured to be used as a mobile server and function in a synchronization environment with other Web Filters, Virtual or Appliance.

New internal mode uses mobile Filter to manage certificates

The internal mode option for certificate management lets the mobile Web Filter—instead of an external device, such as an LDAP server—sign, issue, and manage all MSC-related certificates. In this mode, mobile user certificates can be assigned to IP group/LDAP domain users—instead of solely LDAP domain users, as in the PKI mode.

In the internal mode:

- Mobile end users are authenticated by a designated server containing their IP group/user or LDAP domain group/user profiles.
- A generic user certificate is bundled in the client installer and can be issued to all mobile end users instead of unique certificates. Using the generic certificate, the administrator does not need to set up mobile end users in the Policy section's Certificate Management screen in order to manage their certificates.
- Using the generic certificate with an LDAP server for user authentication, the DNS Domain Name field in the Address tab of the Domain Details screen must be populated with the fully qualified domain name.

System section Certificate Management screen

When configuring the mobile Web Filter in the internal mode, in the Certificate Management screen (System: Mobile > Certificate Management):

- Certificate Management tab: "Internal Certificate Management" option is pre-selected.
- Certificate Authority tab: The only populated fields include Common Name ("Certificate Authority"), Country Name, and Expiration Date (defaulted to five years from this point in time). Filling out the rest of the fields is optional. Click Generate Certificate to populate the CA Certificate box to the right.
- Server Certificate tab: The Common Name (host name) field is pre-populated, along with fields populated in the Certificate Authority tab, and Expiration Date (defaulted to five years from this point in time). Click Apply to complete the wizard.

System section Configuration screen

In the internal mode's System: Mobile > Configuration screen:

- Connection Settings tab: The fields are named the same as the ones used in the PKI mode, except the Client Certificate Identification field is pre-populated with a modifiable EKU to use for all client certificates.
- Client Options tab: In addition to the Client Enforcement options found in the PKI mode, this tab includes the Password and Confirm Password fields that require a Global Certificate Private Key Password for all end users without individual passwords to use when installing unique, non-generic client certificates.
- The Bypass and Download Options tabs contain the same fields as the ones used in the PKI mode.

Policy section Certificate Management screen

The new Certificate Management screen—accessible by navigating to Policy: IP/LDAP > group/domain > Certificate Management—lets you add/remove mobile users to/from the certificate management table, and issue, email, export, or revoke mobile user certificates.

- For IP group members to be issued unique, non-generic user certificates, add users to the certificate management table as follows:
  - Click Add User(s) to add a row for each user to be included in this table. By default, the added row displays a Certificate Expiration date five years from this point in time, and a "Not Issued" certificate Status. The Profile column contains a pull-down menu list of all IP group members currently included in the Policy tree node for that group.
  - Select the user from the list of IP group members in the Profile column pull-down menu, and enter information in any non-populated column, such as Name, and/or Email Address.

continued

Policy section Certificate Management screen, continued

- For LDAP domain group members to be issued unique, non-generic user certificates, add users to the certificate management table in the Certificate Management screen as follows:
  - Click Add User(s); this action routes you to the LDAP Browser screen where you perform a User search.
  - Select the user(s) returned by the query, and then click the Add to Certificate Management button beneath the profile table. Certificates are managed by navigating to the Certificate Management screen in that domain.

- Certificate Management screen conventions and functionality:
  - Entries/modifications made in the table are saved automatically.
  - To remove any row from the certificate management table, click the checkbox(es) to the right of the Status column, and then Delete User(s).
  - To filter users in the table, click the radio button corresponding to available selections (Name, Email Address, Profile, Certificate Expiration, status) and use the field/menu above to refine your query. Any character input in the text field is used as a wildcard. Query results automatically display in the table below.
    - Selecting: “Name” displays the Name field; “Email Address” displays the Email Address field; “Profile” displays the pull-down menu with “All Profiles” and a list of individual profiles in the table; “Certificate Expiration” displays a range of valid certificate dates, five years prior to the current date and time (From), and five years from the current date and time (To); “Status” displays a pull-down menu of all certificate status selections: “All Status”, “Not Issued”, “Valid”, “Expired”, “Revoked”.

  - Users in the table can be sorted by Name, Email Address, Profile (for IP groups) or DN (Distinguished Name for LDAP domains), Certificate Expiration, or certificate Status. This feature is particularly useful when needing to issue or revoke certificates.
  - The certificate expiration cannot be set to less than 24 hours from the current point in time, even when modifying a non-issued certificate.
  - Once a certificate is issued, the displayed expiration date cannot be modified; the certificate must be revoked and re-issued if the expiration date needs to be changed.
  - Unless a unique password is entered in the password column, the user will use the global certificate password set up in System: Mobile > Configuration > Client Options tab to install the certificate.

General Modifications

New SNI Extension feature enabled for HTTPS filtering

In System: Control > Filter, the HTTPS/SSL Filtering frame now includes the “Hostname Identification Based on SNI Extension” option, enabled by default. Server Name Indication (SNI) identifies the hostname for secure client connections, allowing multiple HTTPS sites to be served from one IP address and port number, without requiring those sites to use the same certificate.

- This feature can be disabled if filtering performance is impacted.
- With this feature enabled, an option is available to block access to sites over HTTPS, with *youtube.com included in the list box by default.

YouTube for Schools Enforcement option provided

In System: Control > Filter, the new YouTube for Schools frame includes the YouTube for Schools Enforcement option, disabled by default. Clicking “On” displays the Unique School ID for YouTube Access field, in which the YouTube school ID should be entered, so that the school’s network can access the approved YouTube videos. When using this feature, youtube.com and ytimg.com must not be blocked.

NOTE: If using this feature, the Approved Content feature (which includes VuSafe) must be disabled, since YouTube for Schools Enforcement requires YouTube to be ***un***blocked, while Approved Content (incl. VuSafe) settings requires YouTube to ***be*** blocked.

continued

Web Filter 5.0.10

ABOUT TRUSTWAVE

Trustwave is the leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organisations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions. Trustwave has helped thousands of organisations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, Central and South America, Europe, the Middle East, Africa, and Asia-Pacific. For more information, visit https://www.trustwave.com.

General Modifications, continued

AD Agent removed from Enable/Disable Authentication screen

In System: Authentication > Enable/Disable Authentication, the AD Agent frame has been removed from this screen since the application is no longer being supported.

Hardware Failure Detection reference to spare drive removed

In System: Hardware Failure Detection, the instructions for replacing a failed hard drive have been updated to remove the reference to a spare hard drive, since spare hard drives are no longer included in appliance shipping cartons.

Resolved Known Issues

- Go to http://www.m86security.com/software/8e6/ts/r3000-rki.html and click the Web Filter 5.0.10 accordion to open it and view the resolved known issues for this software release.

Version 08.06.12