



# Astaro Security Gateway **V7.3**

## Release Notes

**Version:** 7.300  
**Revision:** Rev. A  
**Date:** 18 August 2008

## Contents

<b>WHAT'S NEW IN ASTARO SECURITY GATEWAY V7.3.....</b>	<b>3</b>
IMPROVED MAIL SECURITY .....	3
ENHANCED ANTI-SPAM IMPLEMENTATION .....	3
SENDER/DOMAIN AND IP/NETWORKS BLACKLIST (SMTP).....	3
SPAM AND MALWARE REJECTION DURING SMTP TRANSACTION .....	3
EMAIL RECIPIENT VERIFICATION BASED ON ACTIVE DIRECTORY .....	3
MIME TYPE BLOCKING WITH FILE-TYPE LOOKUP .....	4
QUARANTINE FOR UNSCANNABLE ATTACHMENTS.....	4
UPLOAD/CHANGE SMTP TLS/SSL CERTIFICATE .....	4
UPSTREAM HOST-ONLY OPTION .....	4
RDNS AND HELO ANTI-SPAM CHECKS.....	4
QUARANTINE REPORT SCHEDULER .....	4
DOMAIN KEYS IDENTIFIED MAIL (DKIM) .....	4
SMTP PARENT-PROXY SUPPORT FOR SPAM SCANNING .....	5
ENHANCED PROFILE MODE .....	5
IMPROVED POP3 HANDLING .....	5
POP3 MESSAGE QUARANTINE DELETION .....	5
REDESIGNED USERPORTAL .....	5
USERPORTAL LAYOUT .....	5
MULTI-LANGUAGE SUPPORT.....	5
USERPORTAL LOGIN COOKIE.....	6
CUSTOMIZABLE LOGIN MESSAGE .....	6
POP3/SMTP/VPN DISPLAY IMPROVEMENTS.....	6
ENHANCED MESSAGE SEARCH, FILTERING, AND MANAGEMENT OPTIONS .....	6
NEW MAIL LOG VISIBILITY .....	6
EMAIL ENCRYPTION REWORKED .....	6
ENGINE REBUILT .....	6
PGP KEY SERVER QUERY.....	7
CLUSTERING SUPPORT .....	7
EMAIL ENCRYPTION INCLUDED IN MAIL SECURITY SUBSCRIPTION.....	7
DIRECTORY AUTHENTICATION FEATURES.....	7
NEW ACTIVE DIRECTORY BROWSER .....	7
ACTIVE DIRECTORY AND E-DIRECTORY TEST TOOLS .....	7
SUPPORT FOR BACKEND GROUPS.....	7
PREFETCH DIRECTORY USERS.....	7
<b>SYSTEM REQUIREMENTS .....</b>	<b>8</b>
HW REQUIREMENTS .....	8
SUPPORTED WEB BROWSER.....	8
<b>INSTALLATION AND UPGRADE INFORMATION .....</b>	<b>9</b>
UPGRADING ASG V6 HARDWARE APPLIANCES TO V7.3.....	9
UPGRADING ASG V6 SOFTWARE INSTALLATIONS TO V7.3.....	9
BACKUP CONVERTER LIMITATIONS .....	10
SOFTWARE DOWNLOAD .....	10
<b>SUPPORTING MANAGEMENT APPLICATIONS .....</b>	<b>10</b>
ASTARO COMMAND CENTER SUPPORT.....	10
ASTARO REPORT MANAGER SUPPORT .....	10
<b>KNOWN ISSUES.....</b>	<b>10</b>

## What's new in Astaro Security Gateway V7.3

ASG V7.3 focuses on numerous updates to the Mail Security area, a Reworked Email encryption engine, a redesigned UserPortal, Active Directory graphical browser, directory integration test tools, and a new database backend and framework. The following paragraphs provide information on in the major new and changed features in V7.3.

### Improved Mail Security

Administrators can now take advantage of many changes to the Mail Security area of Astaro. This new offering adds new tools and checks, streamlines the WebAdmin implementation and management, and dramatically improves performance.

#### Enhanced Anti-Spam Implementation

The points system leftover from the Spam Assassin implementation previously used by Astaro has been removed. The new spam engine previously had its categories mapped to various point spreads, which has been replaced by allowing administrators to specify actions for the new "Spam" and "Confirmed Spam" results of the scanner. It is also possible to activate spam rejection during the SMTP transaction for better performance and throughput at configurable levels of "Spam" or "Confirmed Spam".

The new thresholds should be considered such as messages marked as spam are most-likely so, however cautious installations that have less room for error will want to quarantine/pass messages of this result to avoid any possible false positives. Messages marked as confirmed spam can be rejected/deleted/discarded with a great level of confidence. Note that no matter the action chosen, a detailed log remains of every message and its particulars, along with what action was taken on it, all fully searchable and accountable by users/administrators.

#### Sender/domain and IP/networks blacklist (SMTP)

It is now possible to completely blacklist and deny mail that originates from a specified sender, domain, IP address, or entire network block.

#### Spam and malware rejection during SMTP transaction

With this change, a message can be filtered during the SMTP dialog from the remote host, as the mail is being received by the Astaro gateway. This way, if the mail turns out to be undesirable, you can issue a SMTP *reject* response. As a result, it is possible to stop the delivery of most junk mail early in the SMTP transaction, before the actual message data has been received, thus saving you both network bandwidth and CPU processing.

#### Email recipient verification based on Active Directory

This feature is now configurable and checks if an email address specified with a RCPT command is actually present in the backend system(s). There are two methods, using callouts and using an LDAP lookup in Active Directory. Callouts work by trying to "route" the destination address, and perform an SMTP session to the target host up to the RCPT stage. If that succeeds or fails with a temporary error, the callout is successful. If there is a permanent error (RCPT not accepted by the target server), the message is rejected.

The new Active Directory LDAP lookup searches for the target email address in the "proxyAddresses" field of LDAP objects. If a matching object is found, the message is accepted, otherwise this check will fail. Temporary errors in the LDAP lookup cause incoming mail to be temporarily deferred. The lookups are made with the Base DN specified in global

active directory settings. It is possible to override the Base DN used per profile. It is not possible to use a different LDAP/AD server for different domains. LDAP referrals are NOT followed.

#### **MIME type blocking with file-type lookup**

Using this feature allows messages that contain a certain MIME type to be quarantined for such a reason. For ease of adoption, we have included selection boxes for 3 commonly requested types: audio, video, and executable. Further extending this functionality is the ability for administrators to specify MIME types manually to add to the check list.

#### **Quarantine for unscannable attachments**

Messages can now be moved to the quarantine if they cannot be scanned for certain reasons. Conditions such as if the archive is encrypted, overly large and too big to be scanned, or if the scanner fails for a period due to a technical issue, can trigger this failsafe. It is possible to filter the mail manager of the UserPortal for reason "unscannable".

#### **Upload/Change SMTP TLS/SSL Certificate**

You can also select the certificate that will be used to identify this system when performing a TLS handshake. You can manage available certificates under IPsec VPN -> Certificate Management.

#### **Upstream Host-Only Option**

If you exclusively get inbound mail forwarded by upstream hosts (such as an ISP or outside filtering services), it is now possible to limit access to SMTP to specified upstream and relay hosts (including authenticated relays) only.

#### **RDNS and HELO Anti-Spam Checks**

Of significant impact is a new check which can greatly reduce spam at a very low resource cost. This feature does basic checks on a host's "identity" by evaluating its IPv4 address and HELO string via DNS and syntactic checks. It is implemented as a simple per-profile on/off switch and exceptions can skip it. Various conditions that are part of the check can trigger it, such as a requirement that the HELO/EHLO string contains at least one dot ".", thus indicating a qualified hostname. Note that the effectiveness of this feature is high and can be evaluated in the new Mail Manager global overview.

#### **Quarantine Report Scheduler**

The Quarantine Report (previously referred to as the Daily Spam Digest) is now available to be sent out twice per day at times configured by the administrator. It is also possible to select which types of messages that have been quarantined are able to be released by end-users.

#### **Domain Keys Identified Mail (DKIM)**

Newly added is the support for cryptographically signing OUTGOING mail with DKIM. In this context, OUTGOING means "all mail which isn't routed inbound", which in turn means "mail sent to domains that don't appear in the SMTP configuration". Sender domains for which ASG signs all outgoing mail have to be explicitly specified and setup. The DKIM settings are global, meaning that ASG uses the same private key and selector string for all sender domains it signs mail for. For setup, it is required that a private RSA key and a "selector" string is specified. Also, you need to publish the public portion of the RSA key along with the selector in the DNS for the domains that you want to sign mails for. See [www.dkim.org](http://www.dkim.org) for more information.

### **SMTP Parent-Proxy Support for Spam Scanning**

It is now possible to support upstream proxies in the event that the Astaro installation does not have direct HTTP access to the Internet. This is required for the spam scanning engine, as such support for specifying an upstream proxy, (including one that requires authentication) for the Spam Scanner has been added.

### **Enhanced Profile Mode**

With some installations filtering mail for only a single domain, while others filter dozens or hundreds of them, support for multiple domains has been improved by the addition of a Simple or Profile configuration mode. Profile mode allows fine granularity in being able to override or extend various settings for domains, and use base settings as the default for new domains that are added. It is also possible to copy, override, or extend the defaults.

### **Improved POP3 Handling**

In addition to various improvements already covered under SMTP, the POP3 prefetch has been redesigned to allow for better global support with less possibility for error. By default, the prefetch is disabled and must be enabled by the administrator. Prefetching allows for less messages to be downloaded by the client, whereas with the prefetch off spam and other messages will be replaced by an action placeholder to ensure the actual message downloaded count matches the clients expectation for a certain number of messages in the inbox. With the prefetch mode enabled, end-users must login to the UserPortal and add their POP3 account information under the POP3 Accounts section. This allows for accurate operation of the POP3 proxy. Note that POP3 server selection is limited to servers added by the administrator, as noted below.

A new feature of the prefetch mode is the administrator being able to set the servers that will use per-user tracking and thusly support quarantine operations and other features of the UserPortal. This is especially useful for controlling which servers can be accessed via the POP3 proxy, such as if you wish to prevent POP3 to anything but the company mail server host.

### **POP3 Message Quarantine Deletion**

This new feature deletes quarantined messages from the POP3 server automatically. If your organization is laptop/roadwarrior heavy and faced with users re-downloading messages once they leave the shroud of the Astaro device, they can avoid this scenario by having Astaro delete any messages from the server so they are not re-downloaded again when they connect from outside the Astaro's protection.

## **Redesigned UserPortal**

### **UserPortal Layout**

Immediately apparent is the new UserPortal design. Featuring a better layout that scales with browser and screen size and more prominent handling options, users gain many new tools without feeling lost or overwhelmed.

### **Multi-Language Support**

The UserPortal can now be displayed in more than a dozen languages, either by having a user specify one during the login screen or having it auto-detect the language set in the browser.

### **UserPortal Login Cookie**

The UserPortal can now use a cookie to keep an end-user logged in without having to re-authenticate each time they visit. This feature can be disabled by the administrator in Managementà User Portal under the “Advanced” tab.

### **Customizable Login Message**

Administrators can create their own, customized welcome message that will be displayed to the users upon login to the portal. It is possible to utilize simple HTML in this message as well, (including hyperlinks) so as to craft the most functional message that conveys the intended information.

### **POP3/SMTP/VPN Display Improvements**

The UserPortal now has separate sections for POP3 and SMTP mail management that feature protocol specific handling options. Also new is the filtering of VPN technologies, so that users are not displayed VPN options for which they have not been configured for by the administrator.

### **Enhanced Message Search, Filtering, and Management Options**

There have been many improvements to the UserPortal in how messages can be found and dealt with by both the administrator and end-user. It is possible to select some or all displayed messages, adjust how many messages are displayed, and take action on what has been selected. Messages can be viewed, downloaded, deleted, marked as false positives, white listed, or released.

There is also a new global cleanup which can be used to delete messages that have entered the quarantine for a certain reason, or by the age they have been present, including a “delete all content” option. Messages can also be sorted by various factors and displayed by some or all of the email addresses for the user account.

### **New Mail Log Visibility**

The UserPortal now includes the customized log output on a per user basis that indicates every message that was received by the system, regardless of the action taken. In the past, if a message was denied for a check such as RBL, the message never made it to the inbox or the quarantine, being rejected before this takes place. As such only the administrator could find the outcome of certain messages. Now with this new display in the UserPortal, it is possible to search and identify each message that was handled, if it was delivered, quarantined, or rejected, and what action (if any) was taken on it. It is also possible to search and sort this list with the same powerful system as the Quarantine.

## **Email Encryption Reworked**

### **Engine Rebuilt**

The Email Encryption engine has been significantly redesigned over the past months, leading to a better performing solution that is smaller in size and resource demands. This engine is completely new and offers an excellent platform for Astaro to begin development of even more features for this area.

### **PGP Key Server Query**

Newly added is the ability to specify the address and port of a Key server for OpenPGP. This allows even easier acquisition, loading and support of PGP keys.

### **Clustering Support**

With the new changes to the encryption engine, support has been added for clustered installations. This leads to dramatic performance improvements of the encryption system.

### **Email Encryption Included in Mail Security Subscription**

As of 7.300, the Mail Security subscription has had the Email Encryption functionality made part of this package. Users that currently subscribe to either Email Encryption or Email Filtering will be automatically given the functionality of the newly named "Mail Security" subscription. Note that it is no longer possible to purchase Email Encryption separately on its own. If any issues are encountered with the licensing of this, please contact your support resource.

## **Directory Authentication Features**

### **New Active Directory Browser**

You have spoken, and in direct response to the popularity of the fully interactive, drag-and-drop style browser that Astaro has long had for E-Directory environments, we have built and added this functionality for Active Directory environments. By offering a full browser-style tool that allows selection of users and groups with the mouse, administrators no longer need to manually type out strings when setting up AD integration, massively reducing the time and expertise needed to take full advantage of user-based reporting, policy assignment, VPN access, and any area of that supports authentication, while reducing the chance of syntax or typographical error.

### **Active Directory and E-Directory Test Tools**

New tools have been added to the WebAdmin to assist administrators in configuring their Astaro product to connect and work with Active and E-Directory resources. It is now possible to test the connection to the server for errors during setup, along with being able to validate a test-user directly from WebAdmin against the backend server without the need for command line troubleshooting.

### **Support for Backend Groups**

Of significant note is the ability to specify a backend group for features such as SSL VPN and the UserPortal, which are then extrapolated and have their users created automatically. This decreases the time needed to deploy features to a user group which previously required the users to be created manually or via automatic user creation over time, and then specified individually. Now, simply drag the user group you wish to use into the Users and Groups box, and the rest is automated by Astaro.

### **Prefetch Directory Users**

For Active/E-Directory setups, administrators now have a powerful prefetch which can be scheduled to synchronize users with the Astaro device at a certain time. This has a large impact where many users sign on in a short time interval (such as the start of the school or workday) by reducing potentially long authentication times (and corresponding timeouts). This feature has seen a considerable positive effect in large environments where authentication is extensively relied upon.

## System Requirements

### HW requirements

Astaro minimum recommendation for V7.3 installations:

Intel Pentium III 800 MHz, 512MB RAM, 10 GB hard disk drive and above.

Best performance results running on:

Intel™ Dual/Quad-Core CPUs, 2GB RAM, 74 GB SATA/SAS 7200RPM hard disk drive and above.

For proved hardware components please check our Hardware Compatibility List (HCL) at:

<http://www.astaro.com/lists/HCL-ASG-V7.txt>

ASG V7.3 might also be installed within VMWare virtual environments, such as VMWare Server, VMWare ESX Server, VMWare Workstation or VMWare Player, by using a pre-configured/pre-installed ASG ISO called VMWare Virtual Appliance. This ISO provides the same functionality as the standard ASG.

### Supported web browser

Astaro Security Gateway V7 WebAdmin will support the following browser/platform combinations:

#### MS Windows 2000/XP/Vista

- IE6 or higher (including IE7)  
**note:** parallel installations of IE6 and IE7 are not supported!
- Mozilla Firefox 1.5 or higher
- Safari 3.0 or higher

#### Linux:

- Mozilla Firefox 1.5 or higher

#### Mac OSX:

- Safari 2.0.3 or higher
- Mozilla Firefox 1.5 or higher

**Note:** the iPhone Safari browser has certain limitations – hence it is not officially supported. Other browsers could also work, but might be subject to rendering or JavaScript issues. They are unsupported. Java or Flash support is not needed.

As with the new V7 GUI technology much of the GUI processing has been moved from the appliance to the management workstation we recommend using [Firefox](#) on a system with at least 512 MB RAM and a CPU with 1,5 GHz. More system performance will increase GUI processing speed significantly.

## Installation and Upgrade Information

### Upgrading ASG V6 hardware appliances to V7.3

ASG V7.3 runs on all currently sold Astaro Security Gateway (ASG) appliance models. For upgrading ASG V6 appliances to ASG V7.3 Astaro offers the following three alternatives:

#### 1. Install with new configuration

- Ask your certified Astaro partner to install ASG V7.3 firmware on your appliance
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.3
- import your existing V6 license

#### 2. Install with import of V6 configuration

- Ask your certified Astaro partner to install ASG V7.3 software on your appliance and convert existing V6 configuration into new release.

#### 3. Automatic V6 to V7.3 upgrade

- Beginning with ASG V6.310 you are able to automatically upgrade V6 firmware and configuration files to V7.0 (suggested for remote installations)
- You can then upgrade 7.0 to 7.3 in a second step

### Upgrading ASG V6 software installations to V7.3

For upgrading existing ASG V6 software installations to ASG V7.3 Astaro offers the following two alternatives:

#### 1. Install with new configuration

- Download and install new ASG V7.3 ISO image on gateway
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.3
- import your existing V6 license

#### 2. Install with import of V6 configuration

- Store the V6 system configuration into a backup file
- Download and install new ASG V7.3 ISO image on gateway
- Click on "Restore existing backup File" on the Setup Wizard screen

#### Note:

- All log files and reports of your V6 installation will be deleted during migration (make a backup first)
- V6 license files can also be used within V7.3

## Backup Converter Limitations

Due to the different system architectures an exhaustive conversion of V6 into V7.3 configuration files is not possible.

Thus the conversion covers all settings, aside from the following:

- HA configuration
- Remote syslog
- IPS
- Site to site/remote access IPsec VPN (conversion for PPTP only)
- Certificates (will not be carried over)
- QoS rules
- dynamic (DHCP) IP-Addresses on Eth-VLAN Interfaces (will not be supported in V7.3)
- DHCP Relay
- Eth-alias instances with status=0 (status fields will not be supported in V7.3)
- Email address fields (e.g. settings -> adminmail)
- eDirectory user authentication (conversion for SSO mode only)
- Active Directory/NTLM
- WebAdmin authentication via external sources
- HTTP proxy
- SMTP proxy
- Group definitions (network and service groups), which contain further groups will be expanded.

It should be noted however, that with the simplification of the administration interface, as well as new self configuring features (such as HA), all of the settings listed above can be adjusted with minimal effort.

## Software Download

The new version is available at Astaro's official download servers:

<ftp://ftp.astaro.com/pub/ASG/v7/>  
<http://download.astaro.com/ASG/v7/>

## Supporting management applications

### Astaro Command Center Support

Astaro Security Gateway V7.3 will be supported by Astaro Command Center (ACC) V1.4 and above. Usage of ACC V1.9 requires at least ASG V7.3.

### Astaro Report Manager Support

Astaro Security Gateway V7.3 will be supported by Astaro Report Manager (ARM) V4.6.

## Known Issues

The actual ASG V7 Known Issues List (KIL) can be found at

[http://www.astaro.com/lists/Known\\_Issues-ASG-V7.txt](http://www.astaro.com/lists/Known_Issues-ASG-V7.txt)