



# Astaro Security Gateway **V7**

## Release Notes

**Version:** 7.000

**Revision:** Rev. A

**Date:** 22 January 2007

## CONTENTS

<b>WHAT'S NEW IN ASTARO SECURITY GATEWAY V7 .....</b>	<b>3</b>
MANAGEMENT AND ADMINISTRATION .....	3
PERFORMANCE AND BANDWIDTH MANAGEMENT .....	3
NETWORK SECURITY.....	4
EMAIL FILTERING.....	5
EMAIL ENCRYPTION .....	5
WEB FILTERING .....	6
<b>CHANGES .....</b>	<b>7</b>
LICENSING .....	7
HA LICENSING .....	7
TEST LICENSES .....	7
HOME-USE LICENSES .....	7
EMAIL ENCRYPTION LICENSING .....	8
SUBSCRIPTIONS.....	8
MAINTENANCE .....	8
PRICING .....	8
WEBADMIN MENU CHANGES.....	9
DROPPED FEATURES .....	11
<b>SYSTEM REQUIREMENTS .....</b>	<b>12</b>
HW REQUIREMENTS .....	12
SUPPORTED WEB BROWSER .....	12
<b>INSTALLATION AND UPGRADE INFORMATION .....</b>	<b>13</b>
UPGRADING ASG V6 HARDWARE APPLIANCES TO V7.....	13
UPGRADING ASG V6 SOFTWARE INSTALLATIONS TO V7 .....	13
SOFTWARE DOWNLOAD .....	14
<b>SUPPORTING MANAGEMENT APPLICATIONS .....</b>	<b>14</b>
ASTARO COMMAND CENTER SUPPORT .....	14
ASTARO REPORT MANAGER SUPPORT.....	14
<b>KNOWN ISSUES .....</b>	<b>14</b>

## What's new in Astaro Security Gateway V7

### Management and Administration

#### Enhanced GUI & Usability Improvements

The V7 WebAdmin interface provides a new look & feel, a lot of usability improvements and works much faster than previous WebAdmin versions. It now allows creating new network objects from any point within WebAdmin and offers new features like a dashboard, setup wizards, and multi-admin support.

#### End User Portal

Allows each end user to delete, release or white list his personal emails that have been blocked by any protection mechanism and hold in quarantine. Furthermore from here he can download his individual VPN client package including software, configuration file and certificates for all remote access clients (SSL, IPSec, L2TP and PPTP). These self servicing capabilities significantly reduce the administrators work load.

#### Customizable end user messages

Administrators can now individually customize and localize all notifications, HTTP-Status/Error pages, messages and mails that are viewed by end user (not admin). All end user messages also support multiple languages (utf8/unicode compatible).

#### Configurable Alerting

A new GUI allows the administrator to configure which important notifications he wants to receive and which less important (informational) ones should be silently dropped.

#### Improved Reporting

The Executive Report can now be sent at three different intervals (daily, weekly, monthly) to different recipients. In addition most of the reports have been reviewed in terms of usefulness and content.

Enhanced Packet Filter Reports provide extended real-time information about number of transferred and filtered packets by various criteria.

#### Improved Packet Filter Logging

Within the packet filter log you will now see the matching packet filter rule that triggered a log event allowing for much easier troubleshooting. Each entry within the packet filter log file now also has a unique consecutive ID allowing to detect if certain events in a log file got lost (e.g. due to communication errors).

### Performance and Bandwidth Management

#### Active/Active High Availability (Cluster)

This new patent pending technology, developed by Astaro, enables the load distribution of cost-intensive tasks like content scanning (of SMTP, POP3, HTTP, and FTP traffic), IPsec and intrusion protection to multiple nodes without the need for additional load balancers. L4- or L7-switches. A cluster can consist of up to 10 units while operating in high availability mode. New nodes can be added dynamically to the cluster without interrupting operation.

### **VoIP optimized QoS support**

Allows for granular definition of policies for bandwidth usage (guaranteed bandwidth and upper bandwidth limit) while fully supporting the Diffserv standard. Provides better support for applications that need specific quality of service levels for delay and throughput (such as real-time applications).

### **Zero Latency HA**

The active/passive HA concept ("hot standby") has also been improved with V7 in many ways. I.e. the takeover time after a failure has been reduced to less than 2 seconds and IPSec tunnels as well as all quarantined objects will now be synchronized between master and slave, in addition to packet filter connections (which were already synchronized in ASGV6)

### **Auto Configuration HA**

The V7 HA concept now also includes an „automatic setup“ (auto configuration) mode which configures the unit automatically for High Availability mode depending on whether it finds a master or slave unit on a specific interface (the HA-port).

### **Ethernet Link Aggregation**

Allows the aggregation of up to four (physical) Ethernet connections into one (logical). This can be used to increase network throughput as well as reliability e.g. by connecting the ASG Ethernet interfaces to different redundant switches. The implementation is based on the IEEE 802.3ad recommendation.

## **Network Security**

### **SSL VPN**

Adds SSL VPN gateway capabilities to the already existing IPsec, L2TP and PPTP VPN options. By using the Astaro SSL VPN client (OpenVPN compatible) most applications can be used remotely via the VPNs including native MS Office and file sharing. Installation of the client is a one-click-task via the new end-user portal.

### **Dynamic OSPF Routing**

ASG V7 now includes dynamic routing by implementing OSPFv2 according to RFC 2328 including MD5 and password authentication. This makes the integration of ASG into larger networks with redundant paths much easier.

### **Improved VoIP security**

A new stateful packet filter tracking module for SIP and H323 now enables full stateful SIP support in both directions, outbound and inbound and supports all combinations of signaling and data channels when using H.323 protocols. It also allows you to easily configure a certain amount of bandwidth always available for your VoIP connections.

### **DNS Enhancements**

Provides more fine grained configuration options for the DNS proxy (e.g. Split DNS, host configuration, additional DynDNS settings).

### **TACACS+ authentication support**

Allows authentication of ASG users against servers using the Cisco TACACS+ authentication protocol.

### **VPN configuration for network groups**

Allows creation of VPN tunnels between groups of local and remote sub-networks thus making VPN configuration much easier by avoiding separate tunnel creation for each single combination of local/remote subnets.

### **Configurable DSL reconnect**

You can now specify a time at which a DSL connection (PPPoE, PPPoA) should be dis-/re-connected to prevent a (provider initiated) network interruption during working hours. If a DSL connection fails you can now also force an immediate reconnection without any idle period.

## **Email Filtering**

### **End User Spam Report**

The daily spam digest has been improved to not only include information about quarantined (SMTP) spam messages but about all messages (SMTP and POP3) that have been blocked or quarantined via any protection mechanism. A user can click on any entry to release a message or to put the sender on his individual spam white list.

If a message was sent to a mailing list each recipient can release it individually. Furthermore users will only get one single digest for all email addresses they use. The layout/content of the digest is customizable.

### **POP3 pre-fetching**

If this new mode is turned on the proxy polls periodically the POP3 server for new messages. If a new message has arrived it will be scanned and stored into a local database on the ASG. Email clients only communicate with the proxy and receive new messages only if they were already scanned and stored in the database. Hence emails are received much faster and timeout problems through the introduced scanning process are eliminated. This concept allows quarantining of POP3 spam messages and creating a single Daily Spam Report.

### **Foreign Charsets support for SMTP and POP3**

Email subject lines encoded with foreign charsets are now properly decoded with correct charset when shown in replacement messages.

### **Customizable Email Footer**

Allows administrators to add a "virus checked" footer to every e-mail that goes through the system and which is successfully scanned for viruses. Furthermore a customizable disclaimer footer can be added to each email in order to outline that the content of this email is only intended for the recipient of the email.

## **Email Encryption**

### **OpenPGP & S/MIME Email encryption / decryption**

Provides world's first transparent encryption, decryption, and digital signatures of e-mails within an UTM gateway. Supports OpenPGP & S/MIME including certificate/key handling and content scanning for incoming (SMTP) e-mails. Outgoing e-mails from defined users will be automatically encrypted and/or signed. All incoming e-mails will be automatically decrypted, verified and checked via the internal virus and content scanner. As these procedures occur centrally on the Astaro Security Gateway with complete transparency for the end user, no additional encryption software will be required on the client itself.

## Web Filtering

### **Transparent FTP Proxy**

A new transparent FTP proxy is now able to handle “native” FTP connections (e.g. from FTP clients like WS-FTP or CuteFTP) in addition to FTP sessions initiated through a web browser (FTP over HTTP). This allows transparent scanning and filtering of malicious content (viruses, expression lists, extension filter) within all FTP traffic.

### **Instant Messaging and Peer-to-Peer Management**

Administrators can now easily monitor and restrict the usage of IM clients such as ICQ, AOL, MSN and Skype as well as Peer-to-Peer tools such as BitTorrent and Kazaa.

### **Improved HTTP Proxy Performance**

The throughput of the HTTP proxy has been improved by up to 100% depending on application used.

### **Mixed HTTP proxy mode configuration**

You can now use transparent mode, standard mode, and authentication mode simultaneously on different networks with each instance using different filtering actions.

## Changes

### Licensing

The following licensing changes have been made within ASG Version 7:

- A 1000 user license has been added for ASG software
- Base Proxy functionality has been moved from the base license to the subscriptions.
- Within ASG software the limits for maximum IPs / users are now enforced in the following way:
  - The administrator will get an email notification if the IP limit is reached.
  - At that time new IPs / users will still be accepted up to a maximum of 110% of the licensed number of IPs (grace limit)
  - If the grace limit is reached no more IPs / users will be accepted
- At the time a subscription expires, the features included within the subscription package will be disabled
  - To remind the administrator about the approaching expiration date he will get a first email notification 21 days before that date and additional reminders as the date comes closer.
- Existing V6 OEM licenses can still be used with version 7. As with standard ASG software there is no difference between V6 OEM and V7 OEM licenses.

### HA Licensing

Active/passive HA (stand-by mode) is licensed similar as within older versions, i.e. for the stand-by unit you only have to buy an additional base license. All subscriptions and maintenance is only needed once for both units.

For the new Active/Active HA clustering solution you have to buy similar licenses and maintenance contracts for each unit within a cluster, either being master, slave or worker node. The number of IPs supported by the cluster will be similar to the number of IPs supported by each single license.

### Test Licenses

At first installation of ASG V7 the base license as well as all subscriptions will be enabled for a 30 day trial period. Before this period ends customers need to upload a valid license to be able to continue using and managing the product. The customer will get notifications 1 week and 1 day before any trial period expires.

### Home-Use Licenses

We will continue offering a Home-Use package. The new V7 package will be free of charge and will now include the base license, all subscriptions and Astaro Up2Date. But it will be limited to 10 IPs/10 Users, and 1000 concurrent connections.

**Note:** Astaro will provide no support to home users and they need to agree to participate in Astaro's Threat Research Network.

## Email Encryption Licensing

Email encryption is licensed similar to all existing subscriptions, i.e. the same user limitations apply:

- when running within Astaro Security Gateway Software you can use the same maximum number of users as licensed with the base license.
- For Astaro Security Gateway appliances only the ASG110 is limited to 10 email encryption users. Licenses on all other appliances are unrestricted.

**Note:** The initial email encryption functionality does not support the import of user data from external databases. Hence each user has to be manually created within WebAdmin.

If email encryption is enabled within an Active/Active HA solution, email encryption and all other SMTP applications (like AntiVirus and AntiSpam) will be restricted to the master mode. Hence no SMTP load balancing will be done.

## Subscriptions

The following subscription changes have been made within ASG Version 7:

- Email and Web Security have been renamed to Email and Web Filtering
- A new Email Encryption subscription has been added to offer transparent encryption, decryption and digital signatures for SMTP mails based on OpenPGP and S/MIME technology. This subscription does not require an Email Filtering subscription as a prerequisite.

## Maintenance

in order to offer everyone the same high level of service, only gold and platinum support will be offered, which includes email, web and phone support. Also, a new offering was added called Platinum Plus. Platinum Plus is an extended offering of Astaro's Platinum support program and is catered to large enterprises which house mission-critical infrastructures and would like a personalized support partnership with Astaro. Platinum Plus will provide customers with a single point of contact, in-depth resources, remote consulting, and onsite support to receive the most personalized and comprehensive services available from Astaro. This service will be priced on a project basis.

Please refer to the "Astaro Customer Support Services" document for detailed information.

**Note:** All of these changes also apply to Astaro Security Gateway V6 and OEM licenses.

## Pricing

Due to the enormous number of new features included we increased the pricing for the email filtering subscription (former email security) by 10%. Furthermore we introduced a new 1000 user license for ASG software which is priced similar to the former unlimited license. In turn the pricing for unlimited licenses and subscriptions have been increased by 25%.

We also removed prices for 2-year subscriptions and maintenance contracts and added 5-year prices instead.

The price for ASG 525F has been reduced to the price of the ASG 525.

**Note:** All of these changes also apply to Astaro Security Gateway V6 and OEM licenses.

## WebAdmin Menu changes

The following table provides an overview about changes within the ASG V7 menu structure against ASG V6.

ASG V6 WebAdmin Menu	To be found in ASG V7 WebAdmin at:
System >> Settings	Management >> System Settings
System >> Licensing	Management >> Licensing
System >> Up2Date Service	Management >> Up2Date
System >> Backup	Management >> Backup/Restore
System >> AV Engines	Web Security >> HTTP >> Anti-Virus Email Security >> SMTP >> Anti-Virus Email Security >> POP3 >> Anti-Virus
System >> SNMP	Management >> SNMP
System >> Remote Syslog	Logging >> Settings >> Remote Syslog Server
System >> User Authentication	Users >> Authentication
System >> WebAdmin Settings	Management >> WebAdmin Settings
System >> WebAdmin Site Certificate	Management >> WebAdmin Settings >> HTTPS Certificate
System >> High-Availability	Management >> High-Availability
System >> Certifications	none
System >> Shut Down/Restart	Management >> Shutdown/Restart
<b>Definitions</b>	
Definitions >> Networks	Definitions >> Networks
Definitions >> Services	Definitions >> Services
Definitions >> Users	Users >> Users Users >> Groups
Definitions >> Time events	Definitions >> Time Events
<b>Network</b>	
Network >> Hostname/DynDNS	Management >> System Settings >> Hostname Network >> DNS >> DynDNS
Network >> Interfaces	Network >> Interfaces
Network >> Bridging	Network >> Bridging
Network >> Routing	Network >> Routing
Network >> NAT/Masquerading	Network Security >> NAT
Network >> DHCP Service	Network >> DHCP
Network >> PPTP VPN Access	Remote Access >> PPTP
Network >> Accounting	none
Network >> Ping Check	Support >> Tools >> Ping Check
<b>Intrusion Protection</b>	
Intrusion Protection >> Settings	Network Security >> Intrusion Protection >> Global
Intrusion Protection >> Rules	Network Security >> Intrusion Protection >> Attack Patterns
Intrusion Protection >> Portscan Detection	Network Security >> Intrusion Protection >> Anti-Portscan
Intrusion Protection >> DoS/Flood Protection	Network Security >> Intrusion Protection >>

	Anti-DoS/Flooding
Intrusion Protection >> Advanced	Network Security >> Intrusion Protection >> Advanced
Packet Filter >> Rules	Network Security >> Packet Filter >> Rules
Packet Filter >> ICMP	Network Security >> Packet Filter >> ICMP
Packet Filter >> Advanced	Network Security >> Packet Filter >> Advanced
Proxies >> HTTP	Web Security >> HTTP
Proxies >> SMTP	Email Security >> SMTP
Proxies >> POP3	Email Security >> POP3
Proxies >> DNS	Network >> DNS
Proxies >> Generic	Network Security >> Advanced >> Generic Proxy
Proxies >> SIP	VoIP Security
Proxies >> SOCKS	Network Security >> Advanced >> SOCKS Proxy
Proxies >> Ident	Network Security >> Advanced >> IDENT Reverse Proxy
Proxies >> Proxy Content Manager	Email Security >> Quarantine Manager
IPSec VPN >> Connections	Site-to-site VPN >> IPSec >> Connections
IPSec VPN >> Policies	Site-to-site VPN >> IPSec >> Policies
IPSec VPN >> Local Keys	Site-to-site VPN >> IPSec >> Local RSA Key
IPSec VPN >> Remote Keys	Site-to-site VPN >> IPSec >> Remote Gateways
IPSec VPN >> L2TP over IPSec	Remote Access >> L2TP over IPSec
IPSec VPN >> CA Management	Site-to-site VPN >> Certificate Management
IPSec VPN >> Advanced	Site-to-site VPN >> IPSec >> Advanced
Reporting >> Administration	Included in Executive Report
Reporting >> Virus Protection	Included in Executive Report
Reporting >> Hardware	Reporting >> Hardware
Reporting >> Network	Reporting >> Network Network
Reporting >> Packet Filter	Reporting >> Network Security Network Security
Reporting >> Content Filter	Web Security Email Security
Reporting >> IPSec/PPTP	Included in Executive Report
Reporting >> Intrusion Protection	Reporting >> Network Security Network Security
Reporting >> DNS	none
Reporting >> SIP	VoIP Security
Reporting >> HTTP Proxy Usage	Reporting >> Web Security
Reporting >> Executive Report	Reporting >> Executive Report
Reporting >> Accounting	Network
Reporting >> Advanced	none
Remote Management >> ACC	Management >> Central Management

Remote Management >> ARM	none
Local Logs >> Settings	Logging >> Settings
Local Logs >> Query	none
Local Logs >> Browse	Logging >> View Log files
Help / Manual >> Online Help >> Search	none
Help / Manual >> Online Help >> Glossary	none
Help / Manual >> Online Help >> Manual	Support >> Manual
Exit	Logoff

## Dropped features

The following Astaro Security Gateway V6 features have been dropped with ASG V7.000

- Configuration: Group as a member of a Group
- DNS proxy on/off (in V7 always on)
- SMTP anti spam: sender address verification (caused to many issues with mailing lists, spammers today use valid email addresses)
- Custom content removal in HTTP proxy

**Note:** Some features have only been removed temporarily (e.g. ICSA and CC mode), which will be included again within a future V7 release.

## System Requirements

### HW requirements

Astaro minimum recommendation for V7 installations:

Intel Pentium III 667 MHz, 256MB RAM, 10 GB hard disk drive and above.

Best performance results running on:

Dual Xeon or Athlon, 2GB RAM, 36 GB SCSI 15krpm 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 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)
- Mozilla Firefox 1.5 or higher

#### Linux:

- Mozilla Firefox 1.5 or higher

#### Mac OSX:

- Safari 2.0.3 or higher
- Mozilla Firefox 1.5 or higher

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 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

The following sections describe how to upgrade existing ASG V6 gateways to the new version and how to use existing V6 configurations within new V7 installations.

### Upgrading ASG V6 hardware appliances to V7

ASG V7 runs on all currently sold Astaro Security Gateway (ASG) appliance models.

For upgrading ASG V6 appliances to ASG V7 Astaro offers the following three alternatives:

#### 1. Install with new configuration

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

-> **available now**

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

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

-> **available by mid march 2007**

#### 3. Automatic V6 to V7 upgrade

- Beginning with ASG V6.310 you will be able to automatically upgrade V6 firmware and configuration files to V7 (suggested for remote installations)

-> **available by end march 2007:**

### Upgrading ASG V6 software installations to V7

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

#### 1. Install with new configuration

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

-> **available now**

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

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

-> **available by mid march 2007**

**Note:**

- The migration of V6 into V7 configuration files will not convert IPsec VPN and Intrusion Protection configuration.
- 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

## Software Download

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

[ftp://ftp.astaro.de/pub/ASL/v7.0/iso\\_i386/](ftp://ftp.astaro.de/pub/ASL/v7.0/iso_i386/)  
[http://download.astaro.de/ASL/v7.0/iso\\_i386/](http://download.astaro.de/ASL/v7.0/iso_i386/)

## Supporting management applications

### Astaro Command Center support

Astaro Security Gateway will be supported by Astaro Command Center (ACC) V1.3xx.

### Astaro Report Manager support

Astaro Security Gateway 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)