



# Astaro Security Gateway **V7.1**

## Release Notes

**Version:** 7.103

**Revision:** Rev. A

**Date:** 19. February 2008

## CONTENTS

<b>WHAT'S NEW IN ASTARO SECURITY GATEWAY V7.1 .....</b>	<b>3</b>
WEB FILTERING.....	3
OTHER NEW FEATURES .....	4
MANAGEMENT AND ADMINISTRATION .....	5
PERFORMANCE IMPROVEMENTS .....	5
<b>CHANGES .....</b>	<b>6</b>
FEATURE AND BEHAVIOR CHANGES.....	6
DROPPED FEATURES .....	6
<b>ASTARO SECURITY GATEWAY V7.101 .....</b>	<b>7</b>
FIXES .....	7
<b>ASTARO SECURITY GATEWAY V7.102 .....</b>	<b>7</b>
NEW FEATURES AND ENHANCEMENTS .....	7
FIXES .....	7
<b>ASTARO SECURITY GATEWAY V7.103 .....</b>	<b>8</b>
FIXES .....	8
<b>SYSTEM REQUIREMENTS .....</b>	<b>9</b>
HW REQUIREMENTS .....	9
SUPPORTED WEB BROWSER .....	9
<b>INSTALLATION AND UPGRADE INFORMATION .....</b>	<b>10</b>
UPGRADING ASG V7.0 TO V7.1 .....	10
UPGRADING ASG V6 HARDWARE APPLIANCES TO V7.1 .....	10
UPGRADING ASG V6 SOFTWARE INSTALLATIONS TO V7.1 .....	11
BACKUP CONVERTER LIMITATIONS.....	11
SOFTWARE DOWNLOAD .....	12
<b>SUPPORTING MANAGEMENT APPLICATIONS .....</b>	<b>12</b>
ASTARO COMMAND CENTER SUPPORT .....	12
ASTARO REPORT MANAGER SUPPORT .....	12
<b>KNOWN ISSUES.....</b>	<b>12</b>

## What's new in Astaro Security Gateway V7.1

The new version provides a completely re-designed HTTP proxy, replacing the squid proxy which has been used up until now. The new proxy significantly improves Web Filtering functionality & performance.

The new version also offers many usability enhancements as well as bug fixes.

### Web Filtering

The new HTTP proxy provides the following major enhancements:

#### **Active Directory native mode (NTLMv2/Kerberos)**

NTLMv2 and Kerberos authentication has been added to the Active Directory Single-Sign-On (SSO) capabilities during complete rewrite of the SSO facility. Support of these protocols is required in order to authenticate against a Windows Domain Controller running in Native Mode. Kerberos is supported by Internet Explorer 7 and Firefox browsers (IE6 only support NTLMv2). Kerberos is used as default if available. SSO Support for pure Broadcast/NetBIOS domains running with NT4 as Domain Controller is not supported any longer. Clients running Windows Vista joined to a domain using Windows 2003 R2 server as domain controllers can only use Kerberos Authentication (so they need to put the firewall hostname in the browser proxy settings).

#### **Concurrent usage of black and white lists per profile**

Within HTTP profiles you can now define filter actions that block and allow access to dedicated URLs/sites at the same time.

#### **Streaming media bypass**

Scanning of video and audio streams can be selectively disabled in order to avoid delays caused by downloading and scanning the entire stream through the HTTP proxy prior to playing.

#### **Block content before download**

File extension filter rules are now applied before downloading a file. This avoids unnecessary waste of bandwidth.

#### **Dynamic configuration changes without restart**

Configuration changes of the HTTP proxy no longer require a restart, which has often lead to a termination of existing connections.

#### **Profile/Filter action logging**

To help troubleshooting wrong profile/filter assignment matching, the used profile and filter action is now logged in the http logfile.

#### **HTTP Proxy scans POST request bodies**

The proxy now employs virus scanning for bodies sent with POST requests to foreign servers as well. If the body contains a Virus, the content is blocked with '403 Forbidden'

## Other new features

Besides HTTP proxy enhancements the new release also includes the following new features:

### **Packet filter based on interface**

Packet filter rules can now be based on network definitions that are bound to specific network interfaces. This significantly improves the flexibility of packet filter rules in many environments.

### **Auto-Packet filter rule generation for NAT traffic**

Packet filter rules can now be generated automatically from DNAT/SNAT configurations by selecting the new checkbox within the NAT-rule.

### **SPAM Scanner with X-SPAM Flag**

If the spam score of an email exceeds the configured SPAM warn threshold (but doesn't exceed the quarantine threshold) the SMTP SPAM engine now adds an 'X-SPAM-Flag: Yes' header to the forwarded email. This allows the user to configure a filter rule within his email client for moving suspected SPAM mails into a dedicated folder.

### **Network Accounting/Usage**

Additional pre-defined reports have been added offering information similar to the Web Security reporting. Data displayed can be selected by timeframe, sorted by various orders or drilled down by clients, servers and service.

### **Content filter double byte support**

The download manager now supports file names using double byte characters. The double byte default character set can be selected via WebAdmin.

### **Virtual HA MAC-Addresses (MAC address takeover)**

When activating active/active HA (cluster) or active/passive HA (stand-by) configurations, MAC addresses of all interfaces (except for the HA interface) are changed to virtual MAC addresses taken from the range 00-1A-8C-F0-XX-XX, which is part of the official MAC address range owned by Astaro.

### **Multiple-IP-Check Uplink Failover**

In order to avoid occurrences of unnecessary fail-over you can now define multiple IP addresses (*Check IPs*) – in a comma-separated list – when configuring the primary network interface for uplink fail-over. Fail-Over will only be initiated if all of the specified IPs fail to reply to a *ping* message. The same (set of) IPs can be specified multiple times. The default *Check IP* 0.0.0.0 is a symbolic IP address that represents the interface's default gateway.

### **DynDNS enhancements**

DynDNS can now be used on more than one interface and also on static interfaces like "Ethernet Standard"

### **Automatic user creation for eDirectory Single-Sign-On**

You can now trigger the automatic creation of user objects for users authenticated via Novell eDirectory in Single-Sign-On mode.

## Management and Administration

The V7 WebAdmin interface contains the following usability improvements:

### **Disabling of proxy and IPS-exceptions**

You can now (temporarily) disable exception rules within proxies and IPS without deleting them.

### **Disabling of aliases on network interfaces**

You can now (temporarily) disable additional addresses (aliases) for network interfaces without deleting them.

### **Global NAT Traversal option**

NAT-Traversal can now be deactivated/activated via a global option under Site-to-Site VPN >> Advanced.

## Performance Improvements

The performance of the HTTP proxy has been significantly improved through the following enhancements:

### **Intelligent caching**

All content cached within the HTTP proxy cache will only be scanned once. Re-scanning will only be done if the Virus scanner configuration changes. This helps increasing throughput of the HTTP Proxy.

### **New IO model**

The new proxy uses an IO model that allows for increased network performance of up to 80% depending on hardware and content scanning configuration.

### **Full support for HTTP 1.1 connection keepalive**

The new proxy fully supports HTTP 1.1 keepalive on client and server connections, improving network performance.

## Changes

### Feature and behavior changes

#### **Virtual MAC Addresses for HA configurations**

As interface MAC addresses are now dynamically changed to virtual MAC addresses when activating a high availability configuration, it might happen that client PCs and other network components can't communicate with the ASG as they still use the old MAC addresses they might have in their ARP cache.

#### **Domain joining for Active Directory (Windows) domains**

In order to join the AD domain, the firewall must find a DC (Domain Controller) machine. In previous versions, this was done with a NetBIOS broadcast. Starting with ASG 7.100, pure AD (native) mode is used, which in turn requires finding the DC with a DNS lookup. There are also more strict requirements on DNS resolution and time differences. The following conditions must be met:

- The time zone on the firewall and the DC must be the same.
- There **MUST NOT** be a time difference of more than five minutes between the firewall clock and the DC clock.
- The ASG hostname must exist in the AD DNS system.
- The ASG must use the AD DNS as forwarder, or must have a DNS request route for the AD domain which points to the AD DNS server.

#### **Domain re-join needed on upgrade**

Customers upgrading from versions prior to 7.100 **MUST** re-join the Firewall to the AD domain if they use SSO. See above for more information.

#### **Kerberos support requires proper network setup**

In order for opportunistic SSO Kerberos support to work, the clients **MUST** use the FQDN hostname of the ASG in their proxy settings - using the IP address will not work. NTLMv2 mode is not affected by this requirement, and will automatically be used if it is not met, or if the browser does not support Kerberos authentication.

#### **Changed behaviour with transparent proxy profiles that have users/groups assigned**

When transparent mode is enabled in a proxy profile, user authentication is not supported. Consequently, having users or groups in a filter assignment does not make sense. Up to 7.011, the proxy would silently match the assignment based on time events only. In 7.100, the proxy will completely ignore filter assignments with users/groups in transparent mode.

#### **Download manager window appears only on slow downloads**

When a download is triggered in 7.100, the proxy will start to retrieve the content without initially displaying the download manager. It will only start to show the download manager if it was not able to transfer half of the advertised content size within five seconds.

## Dropped features

#### **SSO support for NT4 domains**

SSO Support for pure Broadcast/NetBIOS domains running with NT4 as Domain Controller is not supported any longer.

## Astaro Security Gateway V7.101

### Fixes

The following issues have been fixed with the current release, among others:

#### **High system load after remote access login**

Frequent connect/disconnect activities of many remote access users could cause high system load due to a backend service using CPU resources for user and system management.

#### **Customization Texts for HTTP Proxy not working**

The customizable end-user messages defined for the HTTP Proxy (i.e. download manager) have been ignored and replaced with the default text.

#### **Kaspersky Antivirus client blocks HTTPS through proxy**

When using Kaspersky antivirus on a client, surfing the web via HTTP Proxy did not work in all cases.

#### **Adobe Download Manager may fail to download pdf files**

Downloading pdfs using HTTP Proxy and Adobe Download Manager did fail in certain cases

#### **SNAT rule for network groups not set**

Using network definitions that had been bound to a specific interface within a group and then using this group in a SNAT rule did not cause the correct creation of rules within the backend.

## Astaro Security Gateway V7.102

### New Features and Enhancements

#### **WebAdmin Auditor role**

Users with Auditor role will be able to login to WebAdmin with restricted (read-only) access, so they only can only view reports and logfiles without permission to change system settings.

#### **Web Filter Reporting for Blocked Pages**

New Web Security Reports list all websites that have been blocked by the Astaro Web Filter due to viruses found, blocked file extensions or blocked URL categories. Different views are available sorted by categories, users, domains, and more.

### Fixes

The following issues have been fixed with the current release, among others:

#### **High Availability**

Several fixes have been made for High Availability configurations, including proper start-up of IPsec services, synchronization of authentication state when using external authentication like eDirectory, synchronization of configuration data and logfiles as well as the Up2Date process.

### **HTTP Proxy**

Several minor issues with the new HTTP Proxy have been fixed, i.e. with time based profiles, misbehaviour when parent proxy is not resolvable and with sites not working correctly.

### **Authentication**

Auto-usercreation now only creates lowercase usernames in order to avoid duplicate, case-sensitive usernames with remote authentication back-ends. Furthermore Single Sign-On within clustered eDirectory environments has been improved.

### **Tunnel Reference within live log**

When using the IPsec live log viewer, the tunnel references will now be resolved to the tunnel names. That should help while debugging/viewing the IPsec status.

### **MMS connection tracking helper**

The connection tracking helper for MMS has been removed as the protocol is only rarely used and also causes unstable behaviour in some cases.

## **Astaro Security Gateway V7.103**

### **Fixes**

The following issues have been fixed with the current release:

#### **Middleware may slow down on some systems**

On systems with heavy road warrior traffic the Middleware may slow down and allocate large amounts of memory.

#### **High availability log file filling up with stats**

When using ASG in High availability or Cluster mode, the log file will fill up with statistics data. Hence over time, log files might allocate too much of local disk space.

We also revised the installation procedure for Version 7.102 in order to allow multiple installation tries. Therefore if an installation of 7.102 (or 7.103) fails it can be repeated via WebAdmin without the need for contacting support.

## System Requirements

### HW requirements

Astaro minimum recommendation for V7.1 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 V7.1 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 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 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 V7.0 to V7.1

Please note: please contact support for installations with less than 512MB RAM if *automatic firmware download* (Management>>Up2Date>>Configuration) can not be used.

When upgrading from version 7.0x to V7.1 please carefully read the following notes if AD SSO is used:

#### **Domains re-join for Active Directory SSO**

Customers upgrading from versions prior to 7.100 MUST re-join the Firewall to the AD domain if they use SSO. In order to join the AD domain, the firewall must find a DC (Domain Controller) machine. In previous versions, this was done with a NetBIOS broadcast. Starting with ASG 7.100, pure AD (native) mode is used, which in turn requires finding the DC with a DNS lookup. There are also more strict requirements on DNS resolution and time differences. The following conditions must be met:

- The time zone on the firewall and the DC must be the same.
- There MUST NOT be a time difference of more than five minutes between the firewall clock and the DC clock
- The ASG hostname must exist in the AD DNS system.
- The ASG must use the AD DNS as forwarder, or must have a DNS request route for the AD domain which points to the AD DNS server.

### Upgrading ASG V6 hardware appliances to V7.1

ASG V7.1 runs on all currently sold Astaro Security Gateway (ASG) appliance models.

For upgrading ASG V6 appliances to ASG V7.1 Astaro offers the following three alternatives:

#### **1. Install with new configuration**

- Ask your certified Astaro partner to install ASG V7.1 firmware on your appliance
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.1
- import your existing V6 license

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

- Ask your certified Astaro partner to install ASG V7.1 software on your appliance and convert existing V6 configuration into new release.

#### **3. Automatic V6 to V7.1 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 7.1 in a second step

## Upgrading ASG V6 software installations to V7.1

For upgrading existing ASG V6 software installations to ASG V7.1 Astaro offers the following two alternatives:

### 1. Install with new configuration

- Download and install new ASG V7.1 ISO image on gateway
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.1
- 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 V7.1 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 V7.1

## Backup Converter Limitations

Due to the different system architectures an exhaustive conversion of V6 into V7.1 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 V7.1)
- DHCP Relay
- Eth-alias instances with status=0 (status fields will not be supported in V7.1)
- 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.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 V7.1 will be supported by Astaro Command Center (ACC) V1.4.

### Astaro Report Manager support

Astaro Security Gateway V7.1 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)