Astaro Gateway Software **V7.5**

Release Notes

Table of Contents

Introduction

The Astaro Gateway Software V7.5 release provides extended capabilities and enhancements. Many of the new things for this release were gathered or validated by our new approach to feature requests; a public forum for everyone to participate in, located at http://feature.astaro.com. Continuing forward, we will further build on this process with more capabilities and improvements to making as much detail as possible to participants of this system, so that you can easily track and gain insight into various feature requests. Please visit the feature portal for a better look into what is being talked about and considered for future versions of Astaro!

NOTE - Astaro Gateway Software runs on all Astaro Gateway products, including Astaro Security Gateway (ASG), Astaro Web Gateway (AWG) and Astaro Mail Gateway (AMG). Hence these will be sometimes referred to as "AxG" throughout this document and other areas of publication, both here, and in other documents from Astaro.

New & Evolved Features

Intrusion Protection Engine Upgrade

With this release, the IPS engine gets a significant upgrade to a new version. Multi-Core/CPU installations will instantly gain a large performance boost, as IPS has been redesigned and tuned to take full advantage of this type of architecture. In addition to this redesign, more rules have been added which extend the detection capabilities of the system, so that it is now possible to detect the newest exploits targeted at Microsoft Systems. As this has been delivered with transparency, there is no need to re-configure your IPS parameters in order to enjoy these new benefits. As a reminder, a complete, specific list of IPS patterns is located at http://www.astaro.com/lists

Real-Time Bandwidth Monitor

A common problem faced by many administrators with increasing frequency is the need to know at a certain point "how my Internet connection bandwidth is currently being utilized". During times where users are complaining about slow browsing or file copying for example, it is very useful to be able to gain insight as to who is using what traffic right now. To address this need for information, we have implemented a new Real-Time Bandwidth Monitor.

The monitor is accessible from the WebAdmin Dashboard, by clicking the bandwidth bar/statistics for the Interface you wish to examine in real-time. From there a popup window will open (be sure your allowing pop-ups for your AxG) and you will get a per-connection output which shows Source/Destination IP, port, bandwidth in and out, along with other details. Using this type of instant monitoring, it is possible to quickly ascertain where traffic is coming and going from so that action (if needed) can be taken. If you do not see the new bar-style interface usage graphs, navigate to WebAdmin→Network→Interfaces and edit the Interfaces you wish to have utilization bar graphs for. The values placed in the "Displayed Max" field, are only for visual representation purposes only, and do not limit, shape, or control bandwidth. For interfaces that have differing amounts of upload and download bandwidth (such as a cable connection with 10Mbits/down, 2Mbits up) you can specify them separately.

Ability to Import/Export Lists

Astaro frequently replaces existing products in a Network. Whether it is a new customer that is replacing their current device with an Astaro solution, or an existing Astaro customer who is adding more areas of responsibility to their product (consolidation, such as moving Mail Security onto their existing ASG), Astaro is making it easier to quickly upgrade to one of our products. 7.500 now offers a redesigned widget for most entry areas that in the past only supported single-line entry per submission. This could add layers of difficulty and time for administrators who wanted to import/migrate large existing black or white lists.
In order to streamline this process, we have now added an Import and Export controls (represented by green Up or Down arrows) to most areas which are compatible with this new feature. Using these buttons, you can import large amounts of text file lists or entries directly into AxG, and if needed, export the data on those lists for backup or upgrade at a later date. Simply click the Up / Down arrow to open the configuration prompt for this option, then perform your task, such as importing a large whitelist of allowed sites to the URL filter.

Cloning of Objects

WebAdmin now allows you to duplicate many existing configuration in WebAdmin easily, which saves time when having to make many entries, objects, or profiles which share a common base. When this function is available, a "clone" button will appear, usually near buttons like "edit" and "delete". Pressing the new cloning button will instantly create a duplicate object that shares all the same parameters as the item being cloned; however you will need to specify a new title. The cloning operation also allows you to edit and otherwise change parameters of the newly cloned object before completing the process.

Transparent Proxy with Authentication

This new operational mode for the HTTP/S filter allows authenticated access to the proxy without changing browser settings. When this mode is set via the HTTP/S proxy operational mode dropdown box, users will be presented with a login "portal" where they can authenticate against local and other databases (such as eDirectory or Active Directory). Once connected, a configurable countdown timer will begin, after which they will need to authenticate again. This is useful for businesses that provide a managed web access (such as Sports Stadiums, Hotels, Convention Centres etc...) which wish to have a degree of control and reporting without having to provide documentation on how to configure a browser. It is possible to customize the logo displayed on the authentication portal popup, along with the text and a "Terms of Use" agreement. Future versions will see additional flexibility and opportunities to support more customizable designs of this new login portal. In the Management→Customization section you can define the logo and text to be used.

Extended Network Security Reporting

In most areas of threat management, the amount of data which is correlated into reports has a direct impact on the value of the solution, especially during forensic periods or other times when situations warrant a closer look at an event. We have increased the amount of Network Security Reporting detail that is preserved and made available for historical viewing and searching, by adding new tabs under Reporting→Network Security. The new tabs here will display Source Hosts, Destinations, and other information for the Intrusion Protection, Instant Message, Peer to Peer, and Packet Filter system of the installations when they are being used Much of this data was available in the past only as a daily In-line report.

Reputation Support for Web Security

The URL filtering engine used by Astaro performs a metric which determines a websites "reputation" as being one of 5 levels, from Trusted to Malicious. This metric by itself is widely reliant on the type of email messages that the site generates, and as well what other sites have it whitelisted, blacklisted, and other measurements, which all add up to the URL's final reputation according to www.trustedsource.org.
Astaro has now implemented the ability to filter sites based on this reputation, which can further solidify your security policy. As a good rule, dropping sites with a reputation below Neutral (which will deny Suspicious-rated and Malicious-rated) can prevent sites that have been positively identified as a source of malicious or damaging content. This feature can be configured from the HTTP/S→URL Filtering as a checkbox to enable, then by selecting the threshold for denial. Note that there are only 4 configurable levels here, since you cannot block things below the lowest level, which is Malicious. The block message will communicate the appropriate messaging to the user if their site is blocked due to the reputation check. You can visit http://www.trustedsource.org/en/about/faq for more information on their ratings.

SSL VPN

The SSL VPN client has been upgraded to the latest version, which allows for compatibility with 64-bit operating systems. In the past, users that wished to use this type of OS with the VPN client needed to download it separately from OpenVPN and use it in combination with the configuration file generated by the Astaro UserPortal. This extra step is no longer required, and the included client now work for the Windows 7 32-bit and 64-bit Release Candidates 71xx and 72xx (tested so far).
This new version also allows for the use of OpenVPN configuration files, which can enable many powerful features such as auto-starting a tunnel with the computer, auto-entering the name and password, and other "operator" switches. We will have detailed knowledgebase articles for common tasks using these configuration files soon, or you can directly visit the www.openvpn.net site for their own documentation on various switches and configuration file variables.

Dashboard RSS Feed

There is a new object on the WebAdmin dashboard which will display certain notifications or updates posted by Astaro which may be of interest to you. As we are aware not all our customers frequent our http://up2date.astaro.com blog or take delivery of the Astaro Newsletter but would like to know about key Astaro elements, we've integrated a small RSS window into WebAdmin. You can use the navigation to page through the posts to this feed, roll it up via the "X" button, or disable it completely from the WebAdmin Settings page. Posts to this feed will be limited and mostly of a technical or informative nature.

Web Security Cache Improved

The caching intelligence of Web Security has been redesigned and improved to make the cache more capable. To start, note that the size of the Web Security Cache is 25% of the installed Hard Drive size, and the maximum size of any object in the Cache is this number divided by 256. Hence for an 80GB HDD, the cache will be 20GB and the maximum size of any object will be approximately 74Megabytes. These values are non-configurable.

The biggest new change is how object expiry is handled. In pre-7.500, the cache expired objects if either the server time-to-live was reached, or if there was no TTL set on the object by the issuing server, 30 minutes was used as a default. Now, objects in the cache will no longer auto-expire and will remain present in the cache until such time as the space is needed to make room for newer/updated objects. Further, the server TTL, while noticed, will no longer be used as an expiry mechanism, and the object will only be refetched, (even if past its server-issued expiry time), if the server indicates a change has been made to it. These changes alone will have a significant improvement on cache hit percentages, and introduce new flags to the logs for caching results:

- **Cached=0**: Object is new and not currently cached, and its nature cannot be handled by the cache for this hit, so it was served directly from the target server.
- **Cached=1**: Object is known and cached and has been served to the user via the cache directly.
- **Cached=2**: Object is known to the cache but was past its server-configured expiry time. Object was revalidated (but not re-downloaded), and since no change was made to the object, it was issued to the user via the cache directly.
- **Cached=4**: Object was not present in the cache but it cacheable. As such, the object was downloaded and inserted in the cache while being served to the user.

Lastly, it is now possible in the exceptions tab to completely remove URLS, users, or networks from the cache to aid in support of situations where caching is not playing nice with certain sources or targets due to various technical factors.

DHCP Improvements

The DHCP server has received some excellent convenience and time-saving features. You can now visit the list of currently assigned DHCP leases, and select to create a static mapping out of the lease. For those looking to preserve the DHCP-style of their network, but have statically assigned leases to the MAC addresses of their machines, this dramatically shortens the process, as well as removes many places where a margin for typing errors is present (such as entering MAC addresses manually). This feature also allows you to create a network definition for the object being mapped directly from the mapping feature-box, so that then making configuration regarding the object is even further simplified.

As an additional security bonus, the server can now be configured to only hand out DHCP assignments to the list of statically-mapped machines, which provides a measure of security against unwanted "new" objects entering the network via DHCP.

The DHCP server now also has a lease time which can be configured by the admin directly in WebAdmin, and DHCP server object itself has been reworked so that if a server is disabled, and then re-enabled at a later time, the configuration is not cleared to default values, and retains the past information.

Multicast Routing Daemon

Astaro now sports a PIM-Sparse Mode Multicast Routing Daemon. Multicast allows network administrators to conserve bandwidth. By using multicast protocols to deliver a single data stream (video, audio, or other) to multiple recipients in a routed environment, bandwidth use is far less than delivering one data stream to each recipient. Astaro's support for sparse mode multicast traffic taking advantage of multicast bandwidth savings when it is applicable. While

most administrators will know if they require this feature or not, it might be educational to investigate how this might improve your network topology and efficiency.

To configure the Multicast Routing, navigate to the new section for this feature at Network→PIM-SM to configure the interfaces and rendezvous points.

For further reading/education on Multicast Routing, Rendezvous Points, and PIM Sparse Mode, you may find these links useful:
1) http://technet.microsoft.com/en-us/library/bb742462.aspx
2) http://en.wikipedia.org/wiki/Multicast
3) http://www.dataconnection.com/multicast/pimprotocol.htm

Scheduled Install of Up2date

On a per-Up2Date basis, administrators can now set an available Up2Date package to install at a specific time in the future. This is useful for networks where possible downtimes (even mere seconds/minutes) during the day would cause a negative impact. No longer do Administrators have to wait around after-hours simply to click the install button. When an Up2Date for Firmware is available, you can schedule it to auto-install at a certain time. This setting is not recurring, so you retain full control over when to install available Firmware Up2dates on your Astaro.

Authentication Redesigned

The authentication section of WebAdmin (in Users→Authentication) has been redesigned with a new layout and feel, in order to support the new ability for the configuration and use of multiple authentication servers and to make this area more user-friendly. At first glance you will notice the tabs list has been shortened and replaced with an updated navigation.

The global tab contains the automatic user creation section with the area(s) for which to enable this functionality, along with the cache-flush and live-log controls. The new "servers" tab contains all the necessary controls to define and add a server that can be worked with to the configuration, of any supported type. The SSO tab lets you specify which server to use as the single-sign on resources. Only 1 single-sign on server is currently supported, however the ability to create and utilize groups and users from multiple servers allows for some powerful functionality such as for UserPortal logins across different directory servers such as for MSP's which offer mail filtering services and wish to provide the UserPortal to separate customers via their directory resource(s). The advanced tab has been redone to include the mechanisms for passwords, prefetching, and backend synchronization.

New as well is the support of the Apple OpenDirectory authentication method for the HTTP proxy, which is basically LDAP combined with Kerberos. Configuration options are the same as for Active and Edirectory, however please note that Apple's own browser (Safari) currently does not support SSO with proxies, so you will have to use Camino or Firefox as your browser to make use of this functionality.

Other Features and Additions

WebAdmin & UserPortal Usability

WebAdmin and the UserPortal have received numerous upgrades and usability enhancements designed to make working within these tools sleeker, faster, and simply more convenient:

- **UserPortal configuration** - you can now visit the a new UserPortal configuration page in Management→UserPortal→Advanced
- **Customized items** - Administrators can now disable sections of the UserPortal via the above section
- **New Quarantine/UserPortal polish**:
  - ➢ navigation controls have been added to the bottom of pages (supplementing the existing controls at the top),
  - ➢ it is possible to select large amounts (250-1000) of displayed items per page
  - ➢ you can now sort items in by subject line
- **Customizable shortcuts** - Remap the default Ctrl+Hotkey assignments
- **Improved Definition/Services sidebar** – Mouse over now instantly shows full name and extended info to aid identifying desired object for drag 'n drop
- **User List display for IP's** - if a user is assigned a static IP address, this will be shown via the Users list without having to edit the object to view
- **Console/SSH login notifiers** - provides the needed insight when the installation is accessed via these methods
- **Instant email backup** – A new button is present for every created backup file which allows it to be sent immediately via email as a manual, on-demand event
- **Custom text for notifications** – You can now attach a text-label to all notifications sent from an installation, which allows easier identification of what location/unit is sending the message. This is especially useful if managing multiple sites with notifications that pool to a central address/repository
- **Test NTP sync** – A new button which immediately polls the configured NTP server and displays the result
- **Configurable default for lists** - Allows for the amount of items per page (Packet Filter Rules, or any place where a drop down exists in WebAdmin for the number of items to be displayed) to have a larger default view without having to constantly change them upon each visit/load
- **WebAdmin Network section split** – There are now two sections; "Network" and "Network Services"
- **Search boxes retain data** – There is now no need to re-enter your search query after returning from a drill down search result click.
- **System restart reason** - Allows logging of "why was system restarted" in the notification for various events (such as Up2Date required it). "Unknown" will be used for events that have either no configured reason, or if the unit was restarted forceably
- **Group tooltips for members** - Easily discern Network/Service Group members without having to edit in order to view
- **Deletion confirmation for most objects** – now presents a platform-wide confirmation dialog box to avoid accidental deletion of various WebAdmin objects

Up2Date Improvements

Astaro now uses a new, cloud-based Up2Date distribution network. This should drastically increase the speed at which newly-released Up2Dates can propagate to Astaro installations, as this new distribution system has several-hundred-percent more bandwidth capacity.

Other changes:
- **Up2date status reworked** – New status texts will clarify the current status of a Firmware Up2date to avoid confusion regarding the availability, download progress, or readiness of an issued Up2Date
- **Configurable download intervals** for Patterns and Firmware are now possible
- **Before each Up2Date firmware installation**, a backup file will be created automatically

Networking
- **Masquerading for additional IP addresses** – This allows the use of Masquerading (vs. just SNAT) for additional IP's bound to an interface
- **New definition for "Internet"** – The default configuration template has been updated to included an "Internet" object which will exclude internal network(s) to aid policy creation (0.0.0.0/0 on Gateway interface). Especially useful for allowing traffic from an Internal zone access to the "Internet" without automatically granting them access to other zones behind the ASG (such as what happens when you do Internal Network—>To Any Destination in the packet filter)
- **DNS cache flush** – there is now a button which will manually flush the DNS cache to aid in troubleshooting, DNS maintenance, or changes in the network
- **DHCP Interfaces** - an optional hostname can be entered to send along with the DHCP request which is needed in some countries to successfully pull an address from the ISP depending on their requirements
- **QoS** – This feature now has automatic performance rules for QoS to optimize traffic flows and provide some magic prioritization of packets if QoS is simply enabled and no rules are created/set.

Mail Security
- **Global POP3 Sender Blacklist** – Items caught for this new option will be quarantined as "other" in the Quarantine Manager or UserPortal
- **Configurable SMTP Variables** – Administrators can now configure some advanced operational parameters of the SMTP proxy (such as maximum threads) under SMTP→Advanced. Note that these parameters can cause your network significant evil if used in combination with a mis-configured SMTP permissions list (open relay).

Clustering & High Availability
- **Cluster/HA serial number view** – Now displayed on the dashboard as part of the information arrayed, removing the need to physically examine connected units to obtain the serial number(s) when needed
- **New imaging** – New icon arrangements which represent connected units of an HA or Cluster configuration to clearly show the amount and type of connected nodes
- **Dead node removal –** Dead nodes in a cluster can be removed via WebAdmin, which will cause the Master to takeover various node-specific data such as the (mail quarantine and spool)
- **Configurable primary –** You can now set a node to be the "desired primary" which will cause the cluster/HA setup to automatically pass the Master role to this device whenever technically possible

- **Link Aggregation support** – Astaro's proprietary clustering functionality now supports Link Aggregation on the community interface, allowing for more redundancy and throughput of the cluster link. For example you can "bond" together eth3 and eth4 to act as the single, combined cluster interface. Up to 4 physical interfaces are supported in a single aggregation group.
- **New State "Synching"** – When nodes of a cluster system are currently receiving core data essential to allow it access to and operation in a cluster, the state will show as "Synching" to inform the administrator that currently the node is not performing work, but rather entering the cluster properly. Once synched, the operational mode will change accordingly.

Logging/Reporting
- **NAT logging** – A new log flag for connections that matched against the first instance where a hit is seen vs. A NAT rule.
- **Live log negation** – use "-" to negate the log from showing data following this symbol, which filters the live log entries. For example, if you do –test jdoe, the log will show only lines which include the term "jdoe" but also do not include any mention of "test"
- **Reporting exclusions** – You can now configure reports to exclude unwanted/irrelevant data. This is useful to remove entries which tend to over-represent due to their nature, such as Google-analytics, Mediaclick, Doubleclick, or "error"
- **SNMP MIB** – There is now an official, downloadable MIB via the SNMP section of WebAdmin
- **Inline/Snap Report Links** – You can now move directly to the relevant details report when browsing the embedded daily reports located throughout WebAdmin, providing for a more integrated approach when reviewing logs and wanting to "drill-down" for more information

Monitoring
- **ASG 110/120 Watchdog -** There is now an additional feature called a Watchdog on our ASG 110/120 models. These models are mostly used in smaller offices or in environments without power conditioning or temperature controls or alternatively in a server room which is not easily accessible. This feature enables the device to recognize a failure (for example due to a voltage swing) and to reboot itself without any interaction of the administrator thereby increasing the robustness of the solution and reducing the need for manual intervention in the unlikely case of such a failure.
This feature has been extensively field tested - we have hundreds of units in production with the feature enabled - and there have been no "false positives" or other negative effects of enabling this watchdog so we have decided to enable the watchdog by default on all ASG 110/120 appliances with version 7.500 and above.

System Requirements

Updated Hardware Requirements

Astaro minimum recommendation for V7.5 installations:

- Intel^{TM} Pentium 4 @1.8 GHz, 1 GB RAM, 12 GB hard disk drive and above.
- Best performance results are experienced when using hardware specifications at or beyond: Intel Dual/Quad-Core CPUs >2GHz, 2GB RAM.

For proven hardware components please check our Hardware Compatibility List (HCL) at:
http://www.astaro.com/lists/HCL-ASG-V7.txt

AxG V7.5 can also be installed within virtual environments, such as VMWare Server 1 & 2, VMWare ESX Server, VMWare Workstation or VMWare Player, by using a pre-configured/pre-installed AXG ISO called VMWare Virtual Appliance. This ISO provides the same functionality as the standard AXG. Other Virtualization platforms may work flawlessly with AxG, and are not inhibited by Astaro. However as they are not officially supported, compatibility issues may arise in various areas of use, such as networking.

Supported Browsers

Astaro Gateway V7.5 WebAdmin officially supports the following browser/platform combinations:

MS Windows 2000/XP/Vista

- Internet Explorer 7 or higher**
- Mozilla Firefox 3.0 or higher
- Safari 3.0 or higher

Linux:

- Mozilla Firefox 3.0 or higher

Mac OSX:

- Safari 3.0 or higher*
- Mozilla Firefox 3.0 or higher

Note:
*The iPhone Safari browser has certain limitations – hence it is not officially supported
Other browsers and versions also commonly work without issues, but are untested and may have rendering or JavaScript issues. They are thus officially not support. Java or Flash support is not needed.

**IE8 is expected to work fine in most situations, however it is not yet officially supported, and may require compatibility view to operate correctly in some conditions. Combined with Windows 7 may increase areas of incompatibility, however again, the current Win7 RC should be usable with WebAdmin.

***With the V7 GUI, much of the GUI processing has been moved from the appliance to the management workstation. Astaro officially recommends using Firefox 3.x on a system with at least 512 MB RAM and a CPU with 1.5 GHz. More workstation system performance will increase GUI processing speed significantly.

Installation and Upgrade Information

Upgrading ASG V6 hardware appliances to V7.5

AxG V7.5 runs on all currently sold Astaro Gateway (ASG) appliance models.
For upgrading ASG V6 appliances to ASG V7.4 Astaro offers the following three alternatives:

1) Install with new configuration
- Ask your certified Astaro partner to install ASG V7.5 firmware on your appliance.
- Use the Setup Wizard (recommended) to create your configuration for ASG V7.5
- Import your existing V6 license.

2) Install with import of V6 configuration
- Ask your certified Astaro partner to install ASG V7.5 software on your appliance and convert existing V6 configuration into new release.

3) Automatic V6 to V7.5 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 7.5 using Up2Date.

Upgrading ASG V6 software installations to V7.5

For upgrading existing ASG V6 software installations to ASG V7.5 Astaro offers the following two alternatives:

1) Install with new configuration
- Download and install new ASG V7.5 ISO image on gateway.
- Use the Setup Wizard (recommended) to create your configuration for AXG V7.5.
- 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 V7.5 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!). The V6 license files can also be used with the V7.5 framework, and can be officially upgraded to V7 style licenses via the MyAstaro Portal (https://my.astaro.com).

Backup Converter Limitations

Due to the different system architectures an exhaustive conversion of V6 into V7.5 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 V7.4)
- DHCP Relay
- Eth-alias instances with status=0 (status fields will not be supported in V7.4)
- 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, past releases, Up2Dates, and other software is available at Astaro's official download servers:
ftp://ftp.astaro.com/pub/
ftp://ftp.astaro.de/pub/
http://download.astaro.com

Supporting Applications

Astaro Command Center Support
Astaro Gateway V7.5 will be supported by Astaro Command Center (ACC) V2.0+.

Astaro Report Manager Support
Astaro Gateway V7.5 will be supported by Astaro Report Manager (ARM) V4.6.

Known Issues

The actual AxG V7 Known Issues List (KIL) can be found at
http://www.astaro.com/lists/Known_Issues-ASG-V7.txt