



Astaro Command Center **V2.2**

Release Notes

Version: 2.200
Revision: GA
Date: July 2010

Contents

WHAT'S NEW IN ASTARO COMMAND CENTER V2.2	3
HTTP/S PROXY CONFIGURATION	3
PACKET FILTER CONFIGURATION	3
MANAGEMENT AND DISTRIBUTION OF RULES	3
DEFINITIONS	4
AUTO DEPLOYMENT OF DEFINITIONS.....	4
NEW GLOBAL DEFINITION TYPES	4
PRIVILEGE RESTRICTION	4
MISCELLANEOUS	5
LICENSING	5
SOFTWARE & VIRTUAL APPLIANCE:	5
IMPORTANT:	5
HARDWARE APPLIANCES SUNSET	5
SYSTEM REQUIREMENTS	5
HARDWARE REQUIREMENTS	5
VIRTUAL APPLIANCE INSTALLATION	6
SUPPORTED WEB BROWSERS	6
NOTE.....	7
INSTALLATION AND UPGRADE INFORMATION	7
GENERAL INFORMATION	7
KNOWN ISSUES	7

What's new in Astaro Command Center V2.2

Astaro Command Center (ACC) 2.2 remains a free product designed to simplify the operation of even a single ASG installation. No matter if you have one or hundreds of our products, ACC is constantly evolving to support more tasks and central features, which in turn reduces repetitiveness and manual steps for the administrator. Partners are also able to use ACC to manage multiple, independent companies from the same installation across multiple administrators and their staff.

In this version, we are adding new features that are focused mainly around the new central configuration of the Web Security settings (HTTP/S Proxy) and Packet Filter (firewall). In addition, there are almost a dozen new and updated controls and abilities which have been introduced.

HTTP/S Proxy Configuration

One main focus of ACC 2.2 is the centralized configuration of Web Security (HTTP/S Proxy). Using this new ability, it is possible to create and distribute Web Content Filtering actions and settings to ASG installations. This is useful if you often need to make additions or changes company-wide, and currently accomplish this by making manual adjustments within each device. In *Configuration → Web Security* you will see the areas you can manage with ACC. Filter actions can be built much the same as in ASG, comprised of a mix of filtering options like which sites and types of sites to block (or allow if you configure the profile that way) and AntiVirus options.

"*URL Filtering Categories*" lets you build your own category buckets from the list of available classifications a site can have. You use these categories when building filtering actions, and you can deploy/remove them to the ASG's themselves. You can choose to deploy any parts of the supported parameters, such as only the URL categories, or filter actions for later use within a Web Security Profile. For logical reasons, tasks like deploying a filter action which has not already had its Filtering Category deployed will automatically include it during the deployment.

Rounding out the central configuration and distribution of Filter Actions and URL Category buckets are the ability to work with Web Security exceptions in same way. You can easily build and maintain exceptions from ACC. This is very useful for example when a specific site needs to be skipped company-wide, you can define the exception centrally vs. on each device manually. You can also use ACC 2.2 to build and deploy Proxy Auto Configuration Files (PAC) which are parameter files fetched by the users Web Browsers. Installations typically use these to distribute browser proxy settings so they can automate/enforce the use of a proxy and the user does not have to make manual adjustments themselves.

Packet Filter Configuration

Management and distribution of rules

The other major feature of ACC 2.2 is the introduction of control over the packet filter rules. This feature allows you to build rules and deploy them to selected installations. To get started with building rules, go to *Configuration → Network Security* in the ACC Gateway manager. The tab "*Packet Filter Rules*" is modeled after the same screen in Astaro Security Gateway. You can

build rules by specifying factors like source, service, destination, action etc. Note the box for specifying the Organizational unit; this is used to assign the rule to a group of devices assigned to a company, or select Global. Rules built using ACC make use of definitions within ACC itself, not the definitions which might exist locally at the installation(s).

The “*Packet Filter Rulesets*” tab is also new, where you can group rules you have built together, and then define how this set of rules will behave once deployed, such as the position on the rules table they should occupy. Using rulesets can be very handy in management, and you can use another new feature in ACC 2.2 (discussed below) to auto-deploy rules added to sets to their assigned Organizational unit(s). Via the Rulesets tab, you can also enable/disable rules, deploy and remove them from ASG installations, and get overview information such as where they are used and what rules make up the set, along with their status.

Definitions

Auto Deployment of Definitions

During the configuration of Organizational Units and the ASG device(s) which are members, you can select to use auto deployment. This feature will automatically apply global definitions to member ASG devices, saving you from having to keep the devices updated via constant object push operations when you make and use new definitions. Note that this option only affect global definitions, for logical/tech reasons, Packet Filter and Web Security settings cannot be automatically deployed and updated with this feature.

New Global Definition Types

You can now define and distribute definitions for Time-Events and custom IPsec policies. As with other definition types, this lets you centrally work objects which can be deployed, edited and revoked to ASG devices as desired. Time Events can be created in the Gateway Manager at “*Configuration → Definitions → Time Events*” while IPsec policies are built using the new tab located at “*Configuration → VPN → IPsec Policies*”.

Merge Granularity

When you are deploying definition objects to ASG installations from within ACC, if the object already exists you will now be able to choose the outcome of what should happen. You can overwrite it completely with what the ACC is trying to send, skip it and keep the ASG definition, or keep the existing name and just update the object parameters with what the ACC Global Object parameters are. This is handy when making the move to using ACC for installations which already have established configuration, and gives you choices in how you want to proceed when conflicts are found between what ACC is tasked with sending and what already exists on the local ASG(s).

Privilege Restriction

You can choose what area(s) of ASG should be manageable by the Astaro Command Center. Within the ASG installation running version 7.506+ or 8.000+, navigate in WebAdmin to “*Management → Central Management*”. From here, you can select some or all of what ACC should have control over in the areas of Administration, Reporting, Monitoring and Configuration.

Miscellaneous

- IPsec configuration can now re-use global network definitions and global/custom IPsec policies.
- Expired license subscriptions will gradually loose impact on monitoring level. This means that if you choose not to renew a subscription previously licensed, it will decay over time so that the license state is not always in an alert mode.
- Up2Date Cache restricts access to Up2Date Servers only. This prevents erroneous configuration by the administrator creating an open relay and causing unwanted connections and abuse by limiting outbound connections from the Up2Date cache to official Astaro Up2date servers only. It does not affect the intended operation of this feature.
- Beginning with the upcoming ASG 7.507 and 8.002, you will be able to specify a second ACC server within the ASG WebAdmin "*Management* → *Central Management*". This allows for two ACC instances to interact with the ASG(s) as desired, such as having a partner ACC box as well as a customer one. These releases of ASG will also introduce SSO real name pass through.

Licensing

Software & Virtual Appliance:

ACC V2.2 Software and ACC V2.2 Virtual Appliances are exempt from charges. The software itself, including all configuration, capabilities and features are free of charge.

Note: Beginning with the past release of ACC 2.1 near the end of 2009, a framework which supports a personalized ACC licensing key was introduced. The old key which was mass-used by all installations before this expired at the end of 2009.

IMPORTANT: To register and receive a free, new personalized key for the Astaro Command Center, please visit <http://www.astaro.com/download/acc> at any time.

You can also access this page via the ACC WebAdmin by going to Management-→Licensing and clicking the updated link at the bottom of the page in the section 'How to retrieve your free license'.

Hardware Appliances Sunset

Since January 2010, ACC is no longer offered for sale as a dedicated hardware appliance from Astaro. Customers can choose to run ACC on their own x86 hardware or within a VMware virtual environment.

System Requirements

Hardware requirements

The ACC software needs to be installed supported platforms; a dedicated Intel compatible PC or within a VMware Virtualized Environment.

For proven hardware components please check our Hardware Compatibility List (HCL) at: <http://www.astaro.com/lists/HCL-ACC-V2.txt>

Recommended hardware for ACC installations:

The requirements for Astaro Command Center V2.2 depend on the number of managed devices in use, as well as the number of administrators who access the ACC simultaneously. There are numbers for CPU, RAM, Hard Disk and Bandwidth (devices) / Bandwidth for clients respectively in addition.

Note: These figures are general-use estimates and may be different for you based on activity and load of the connected devices.

Gateways	10	25	50	100	300
CPU:	Intel 1.6 GHz	Intel 2.8 GHz	Dual 1.8 GHz	Dual 3 GHz	8 x 2.4 GHz
RAM:	1 GB	1 GB	1 GB	2 GB	8 GB
HDD:	40 GB	40 GB	80 GB	120 GB	250 GB
Internet Link:	512 Kbit	512 Kbit	1 Mbit	2 Mbit	6 Mbit

(*): Required bandwidth from ACC to managed Gateways, excluding Up2Date Cache service.
 Note: An ADSL line is suitable for monitoring purposes as the downstream to the ACC is considerably higher than the upstream to the managed Gateways.

Please note: the above bandwidth estimations do not cover the usage of the Astaro Up2Date Cache. As a rule of thumb, a Firmware Up2Date of 50 MB size will saturate a 6 Mbit xDSL line for roughly two hours when 100 devices pull the Up2Date package via the same dedicated ACC. In such cases, you should consider implementing a traffic shaping strategy for Monitoring and Up2Date traffic, respectively or have the devices retrieve the Up2Date directly from the Astaro Content Distribution Network via the Internet.

Virtual Appliance installation

ACC V2.2 can be installed as a virtual appliance.

The following VMware virtualization platforms are supported:

- VMware Player
- VMware Server
- VMware Workstation
- VMware ESX Server 3.5/4 (including vSphere 4 architecture)

Supported Web Browsers

Astaro Command Center V2.2 WebAdmin and Gateway Manager supports the following browser/platform combinations:

MS Windows 2000/XP/Vista/7

- Internet Explorer 8+
- Mozilla Firefox 3.6+
- Safari 5.0+

Linux:

- Mozilla Firefox 3.5+

Mac OSX:

- Safari 5.0+
- Mozilla Firefox 3.0

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.

Because much of the AJAX GUI processing is done by the management workstation instead of the ACC, we recommend using **Firefox 3.6+** on a management workstation with at least 1024MB RAM and a CPU with 3 GHz. More system performance will increase GUI processing speed significantly; hence a Dual-Core CPU and 2 GB of RAM will be beneficial.

Installation and Upgrade Information

General Information

Due to a new ACC device agent and the new features we have introduced in ACC 2.2, **ASG version 7.506(and higher) and/or ASG Version 8.000+ is required.**

*You cannot benefit from the new features and enhanced capabilities until you update both your Astaro Security Gateway and your ACC installations to our latest offered versions!

Known Issues

The actual ACC V2 Known Issues List (KIL) can be found at http://www.astaro.com/lists/Known_Issues-ACC-V2.txt