



Astaro Command Center **V2.0**

Release Notes
ACC Hardware, Software, & Virtual
Appliances

Version: 2.000
Revision: GA
Date: March, 2009

CONTENTS

WHAT'S NEW IN ASTARO COMMAND CENTER V2.0	3
CONFIGURATION: SITE-TO-SITE VPN.....	3
GENERAL	4
WEBADMIN IMPROVEMENTS.....	4
GATEWAY MANAGER	5
LICENSING.....	6
SYSTEM REQUIREMENTS	6
HARDWARE REQUIREMENTS	6
VIRTUAL APPLIANCE INSTALLATION	7
SUPPORTED WEB BROWSERS	7
INSTALLATION AND UPGRADE INFORMATION	8
SUPPORTED ASTARO GATEWAY RELEASES.....	8
KNOWN ISSUES.....	8

What's new in Astaro Command Center V2.0

The Astaro Command Center V2.0 has been significantly redesigned and now offers a new user-experience via an Updated interface and dual-portal style of management, along with the major new feature of being able to centrally configure and management Site-to-Site VPN tunnels for connected devices in various configurations.

Astaro Command Center is now based on the proven and established ASG V7 framework, which provides dramatically increased performance and stability, many new management and reporting features and the base for fast development of new features for upcoming releases. By using the same platform as all other Astaro gateway products, ACC offers the same WebAdmin GUI for managing the ACC device and offers an additional "Gateway Manager" GUI for managing all connected devices. The Gateway Manager now offers enhanced monitoring, sorting and filtering capabilities.

Configuration: Site-to-Site VPN

With this release, it is now possible to setup site-to-site VPN tunnels directly from within ACC itself. Simply indicate the devices to be joined together via VPN, select a few options, and the rest is automated. The new configuration functionality is enhanced by an efficient wizard, which also allows for differing VPN topologies to be constructed (such as "star" or "full-mesh") in a semi-automatic fashion.

IPSec VPN Configuration Wizard

There are new configuration capabilities for VPN of ACC V2.0 which can be easily created with a wizard dedicated to this task, and/or adjusted later. It allows set-up of site-to-site connectivity with only a few clicks. The tunnel configuration supports RSA based authentication for high security environments and offers the same proven and efficient IPSec policy definitions from the Astaro Security Gateway. Using the VPN configuration of ACC, you can create static and dynamic IPSec connections (initiate, respond-only), and the Command Center will automatically import locally accessible interface networks from selected devices in order to assist the creation process. Further, already-deployed VPNs can later be modified with the same wizard.

IPSec VPN Monitoring Overview

This overview area will display the VPN tunnels that are currently managed by ACC, and as the administrator you can re-configure, enable/disable, and delete tunnels. Further, the overview page is an excellent resource with which to instantly get tunnel information such as the current status, and specifics of the VPN such as policy, auth-method, number of tunnels and devices.

IPSec VPN Monitoring Details

Administrators can get more details by drilling-down into a specific tunnel shows extended data, much in the same way as the rest of the Astaro Command Center operates. More details can be obtained about tunnel status, deployment, and which devices are interconnected for the selected VPN. By having more information available directly from within ACC, the need to login to the individual Astaro devices simply to get status and overview details is all but eliminated.

User Access Control

ACC offers the ability to configure individual users, and further have sub-users under them. This allows for the master ACC administrator to specify various areas of user management, and also have those users work with and manage more individuals themselves. This is particularly useful for setting up individual companies which are to be managed on the same ACC appliance, and then allowing the local admin for such companies to manage their own employee's and their access to devices of responsibility within their organization. ACC V2.0 further introduces a "Configuration" role which can be assigned for different devices and defines which users can change current settings related to device configuration, such as VPN.

General

Bandwidth Economy & Data Actuality

The Change to JSON (JavaScript Object Notation), which is a lightweight data-interchange format now saves more than 80% bandwidth compared to the previous ACC version. At the same time, the shown data actuality has been improved with a delay of only some seconds.

Administrative GUI Split

Administrators can now take advantage of two administrative GUIs. The customer-based view to connected gateways is convenient especially for service providers and Astaro partners offering device management as a service. The GUI's are as follows:

- 1.) The **WebAdmin (Port 4444)** is responsible for the ACC system settings of the installation itself (IP Address, Master Admin, ACC Up2Dates etc...)
- 2.) The **Gateway Manager (Port 4422)** for monitoring, managing, and configuring connected Astaro Gateways.

Multipoint Appliance Support

ACC is now supporting Astaro Multipoint Appliances (Astaro Web Gateway, Astaro Mail Gateway). The required base firmware version for all appliances is V7.300 or higher, with 7.400+ being recommended for the best experience.

WebAdmin Improvements

Directory Service integration

Administrators and Users of the ACC are now able to authenticate against existing Directory Services (eDirectory, Active Directory, RADIUS, TACACS+, LDAP).

Monitoring / Reporting / Alerting

The ACC illustrates reports about network traffic, concurrent connections, CPU-, Memory / Swap-, Partition usage and creates the "executive report", familiar from Astaro Security and Web Gateways. This Report can be sent at three different intervals (daily, weekly, monthly) to different recipients. Notifications / Alerts (e.g. in case of system restarts, UPS device problems, etc.) can also be configured.

Network restrictions & Shared Secret

It is now possible to restrict access to the ACC by using network access definitions for Clients and Gateways. You can also activate a Shared Secret authentication scheme requiring both Gateway Manager and connecting devices to exchange a shared common password before communication starts. Enabling or changing this kind of access control requires the same

password to be specified in the Central Management configuration of each device requesting access to the ACC.

By using the **Auto Update** functionality, already connected (online) devices will automatically adjust to changes of the password given here, so there is no need for manual reconfiguration if you have many devices.

Support for Policy Routes

You can now create policy routes in the WebAdmin of ACC to better aid in fitting the ACC installation with your network environment.

Gateway Manager

The new implemented GUI "Gateway Manager" is responsible for managing connected devices.

Trend indicators

In addition to the actual monitoring data, the ACC now augments certain information with trend indicators to show deviations to previously established baselines and historical averages. Depending on the type of data monitored, those baselines are either short-lived (CPU load average) or worth several days of data collection (Threat Monitoring).

Re-sorting

A newly integrated automatic **sorting / re-sorting functionality** improves situational awareness by ensuring that Gateways with the highest threat status are put on top within the various views. The interval of the resorting can be set from 10 to 60 seconds.

Filter Bar

A newly integrated filter bar on the top of the monitoring views, allows focusing to specific gateways, which are above a specified threshold value.

New Worldmap

The integration of "Yahoo Maps" allows having a much more exact zoom-in functionality within the "Worldmap view". The exact editable known longitude / latitude declaration can now be displayed much more exact on the new map.

Service Monitoring

ACC V2.0 monitors up to now the running services on the connected gateways. The services are consolidated into 4 groups:

- Misc (NTP-, DNS-, DHCP Server)
- Network Security (SOCKS Proxy, Intrusion Protection)
- Web Security (FTP Proxy, HTTP Proxy)
- Mail Security (SMTP Proxy, POP3 Proxy)

Enhanced "Mouseover" Details

The "Mouseover functionality" show in different views more exact details, even by pointing with the mouse pointer beyond of the section.

Scheduled operations

The enhanced scheduled operations allow now to set specific weekdays for executing the selected action. It is further on possible to execute these actions once, on a specific day.

Visual Product Types

The cardview on the dashboard will now visually indicate the type of product represented, so that users can easily see the type of the product, such as AWG, ASG, AMG.

Serial Number Info

The inventory and monitoring details pages will now display the serial number of any AxG Hardware appliances, making it easy to obtain for tracking, support, license tasks, and other situations which require the serial number.

Licensing

Software & Virtual Appliance:

ACC V2.0 Software and ACC V2.0 Virtual Appliance is exempt from charges. However due to the new framework you now need to install a free license which you can retrieve from http://www.astaro.com/lists/Free_License-ACC-V2.txt and upload it at the menu: Management >> Licensing >> Installation.

Hardware Appliances

As with all other Astaro products, special basic licenses (for each model) are required. For more information on the official Astaro Command Center Hardware Appliances, please check our web site at

http://www.astaro.com/our_products/management_tools/astaro_command_center/hardware_appliances.

System Requirements

Hardware requirements

The software needs to be installed on a dedicated Intel compatible PC.

For proved 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 V2.0 depends 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.

Gateways	10	25	50	100	250
CPU:	Intel 2.4GHz	Intel 2.8 GHz	Dual 1.8 GHz	Dual 3 GHz	Quad 2,4 GHz
RAM:	1024MB	1 GB	1 GB	2 GB	3-4 GB
HDD:	30 GB	40 GB	60 GB	80 GB	160 GB
WAN Down/Up Kbit:(*)	128 / 32	256 / 64	512 / 128	1 Mbit / 256	2 Mbit / 512

(*): 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.

In addition, you have to calculate **extra upstream bandwidth** from ACC to the number of Clients using the Gateway Manager WebGUI; the demand is **5 Kbit** for each monitored gateway. For instance, if a client is monitoring 50 devices, you have to multiply this value with 50 (250 Kbit). If 5 clients are monitoring simultaneous each 250 devices, you have to multiply this value with 1250 (6,2 Mbit).

A high amount of simultaneous connections can cause the requirement of higher bandwidth for upstream then for downstream!

Please note: the above bandwidth estimations do not cover the usage of the Astaro Up2Date Cache but only encompass standard monitoring operations of the managed devices. 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.

Virtual Appliance installation

ACC V2.0 can be installed as a virtual appliance.

The following VMware virtualization platforms are supported:

- VMware Player
- VMware Server
- VMware Workstation
- VMware ESX Server

Supported Web Browsers

Astaro Command Center V2.0 WebAdmin and Gateway Manager will support 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 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** 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 major system architecture changes in the new Astaro Command Center V2.0 and the focus on future extensibility and scalability, only Versions 7.300 and higher will be supported, with configuration requiring ASG 7.400+. You can continue using older products with the previous ACC V1.4 which offers backward compatibility, but you cannot benefit from the new features and enhanced capabilities until you update both your Astaro Security Gateway and your ACC installations to the latest versions.

Supported Astaro Gateway releases

The following versions of Astaro Gateway product are supported by ACC V2.0*:

- Astaro Security Gateway / Astaro Web Gateway / Astaro Mail Gateway V7.400 and higher
(*To use the new IPSec Site-2-Site Configuration feature Astaro Security Gateway 7.400 is required.)

Known Issues

The actual ACC V1 Known Issues List (KIL) can be found at
http://www.astaro.com/lists/Known_Issues-ACC-V2.txt