

Astaro Technical Support Requirements

1. Introduction

Astaro support provides you with assistance to solve your problem as soon as possible. To guarantee a quick processing time, we need as much information as possible about the problem. The following document gives you helpful hints as to which information we require from you. At the end of this document, you will find an overview with all this information. The log-files should be compressed as .zip or .tar archive.

2. General Information

Generally, we need the following basic information of your Astaro Security Gateway System. This will allow us to get an idea of the environment Astaro is implemented in. *Cursive written information is optional.*

2.1 Basics

Software version:

Initial installation version:

License ID:

Hardware platform:

Version of the first installation (commandline output from `cat /tmp/.build`)

2.2 Definitions

Please attach screenshots from the necessary definitions set in WebAdmin >> Definitions >> Networks

2.3 Network diagram

Please attach a detailed network diagram (in JPEG, BMP, Visio file or PDF formats) showing how the ASG is implemented and how it interacts with other devices.

2.4 Log-files

Please attach the following log-files of the date when the problem occurred:

- mdw.log
- confd.log
- selfmon.log
- kernel.log

2.5 Network Interfaces

The screenshots from the following WebAdmin sections are needed:

- Network >> Interfaces
- Reporting >> Advanced >> Interface Information

2.6 NAT Configuration

- WebAdmin >> Paket Filter >> Advanced >> Current System NAT rules

3. Problem Description

Describe your problem as accurately as possible. In the table below, you will find a summary which compiles together what information we need (Screenshots from WebAdmin, command line output and log-files).

3.1 Networking

Please describe exactly your problem.

- Do you have problems to reach any host in the network?
- Is it possible to access the Internet by IP address and by name?

Mark the related IPs in your network diagram and attach the packet-filter log-file.

3.2 High Availability

The following debug information is needed:

- High Availability Log-file from Master *and* Slave
- Screenshot of WebAdmin >> System >> High Availability
- Command Line Output of ifplugstatus.pl

3.3 VPN

Please send us a detailed description of the error or misdemeanor.

In the case of a VPN problem, we will need the following information:

- PPTP, L2TP or IPSec VPN
- Roadwarrior or Net-to-Net connection
- Tunnel endpoint vendor, Astaro (which version) or which other vendor
- Authentication Type (PSK, RSA, x.509)

The following debug information is needed:

- Screenshot of WebAdmin >> IPSec VPN >> Connections
- IPSec log-file
- Command Line Output of vpnstatus.pl ROUTES

3.4 Intrusion Protection

The following debug information is needed:

- Email you have received from the Intrusion Detection System.
- How often did you get this mail?
- What kind of host (internal/external) provoked the alert?
- Screenshots of WebAdmin >> Intrusion Protection >> Settings
- IPS log-file

3.5 Proxies

Please send us a detailed description of the error or misdemeanor of the according proxy. Please send us the debug information- you find a summary in the table below.

3.6 Up2Date/Pattern Download

The following debug information is needed:

- The PopUp Window of the Up2Date process
- Screenshot of Proxies >> DNS
- Up2date log-file

4. Other products

4.1 ASC

The following debug information is needed:

- The ASC configuration file (WebAdmin >> IPsec >> Remote Keys >> Download (config.ini) and if applicable the remote certificate.
- ASC Log-file
- According IPsec log-file of ASG

4.2 ARM

Please send us a detailed description of the error or misdemeanor.

The following debug information is needed:

- The report showing the error
- Files of the following folder where ARM is installed (e.g. C:\Programms\AstaroReportManager\Fwa\fwadiaglogs)

Information	Webadmin (Screenshot)	Console	Logfile
Networking			
Problems with DSL connect			pppoe.log
Other	Network->Interfaces		
	Network->Routing (static)	route -nn (Version<6)	
	Network->Routing (policy based routing)	ip route show table all	
		cat /etc/wfe/conf/itf.conf	packetfilter.log
	Network->NAT/Masquerading		
VPN			
PPTP	Network->pptp VPN Access		pptpd.log
L2TP over IPsec	VPN->L2TP over IPsec		
IPsec	VPN-> Connections		ipsec.log
	VPN-> Connections->Status		
	VPN-> Connections->Routes	vpnstatus.pl ROUTES	
HTTP Proxy			
Error message from browser	Proxies >> HTTP		http_access.log
URL causing the problem			http_block.log
			contentfilter.log
			aua.log
SMTP Proxy			
Complete mail (with all header information).	Proxies- >> SMTP		smtp.log
			contentfilter.log
POP3 Proxy			
Complete mail (with all header information).	Proxies >> POP3	tcpdump -i INTERNAL_INTERFACE port 110 -s0 -nv -w /opt/tmpfs/int.pcap	pop3.log
		tcpdump -i EXTERNAL_INTERFACE port 110 -s0 -nv -w /opt/tmpfs/ext.pcap	contentfilter.log
Intrusion Protection			
Alert eMail	Intrusion Protection >> Settings		ips.log
Up2Date			
Error message of popup window		pattern_aus --debug	up2date.log
		pattern_aus --install	
		aus --debug (system update)	
High Availability			
	System >> High Availability	cat /etc/ha/ha.cf ifplugstatus.pl	high-availability.log (Master and Slave)