Administrator manual

Esapanel

Esalogica

15 November 2026

Contents

Installation....4
Before you start....4
Installing....4
After the installation....5
Running esapanel-setup again....5
Security from the start....5
The license....6
Activating the license....6
The daily check....6
Expiry....6
Another machine....6
Updates, reboot and shutdown....7
Updates of Esapanel....7
Reboot and shutdown....7
Network and security....9
IP addresses....9
The security overview....9
The firewall....9
IP bans....10
Internet scanners....10
Certificates, mail and DNS....11
The certificate of the panel....11
Mail....11
DNS....12
Resellers....13
Creating a reseller....13
Reseller plans....13
The resources of the reseller....13
The rest....13
Statistics and notifications....14
The statistics of the server....14
Notifications....14
Disaster recovery....16
What it holds....16
Making the backups....16
The key of the server....16
Restoring on this server....16
Rebuilding the server on a new server....16

A test now and then....17
CSP: the reception of the logs....18
The state of the reception....18
Logs that do not reach the database....18
Ports without an answer....18
The ports in the firewall....18
The certificate....18
UCP: the settings of the checks....19
All the hosts....19
Checks towards private addresses....19
The resolver....19
The outbound firewall....19
WFP: datastores and relocation....20
Datastores....20
Relocation....20
The remote copy....20
Verification and repair....21
LSP: the license server....22
A license is a subscription....22
Licenses....22
The page of a license....22
Transfers....22
A delicate server....23

How to install Esapanel and run the server: the license, the updates, network and security, the resellers, the backup of the server and the settings of the modules. For the pages resellers and customers see too, see their manuals.

Installation

Esapanel is installed on a freshly installed Debian 13 server, physical or virtual (VMware, Hyper-V, Proxmox and the other KVM environments), a VPS too. A script adds the package repository, installs the `esapanel` package and runs `esapanel-setup`, which configures the server and the panel.

Before you start

- **Debian 13** freshly installed, **amd64** or **arm64** architecture, with **root** access.
- The **final full name** of the server, such as `log.example.com`, and its **final address**: the panel uses them for its certificate and for the license. The name must resolve to the address.
- **Internet access** outbound: the package repository over HTTPS (port 443) and the license server (`license.esalogica.com`, port 9444). A server without Internet can neither activate nor check the license.
- The **activation code** of the license, if you already have it: it can also be entered later, in the panel.
- For the modules that keep a lot of data (the logs of CSP, the off-site copies of WFP), a separate disk or partition, mounted before the installation.

Installing

As root:

```
wget -qO install.sh https://repo.esalogica.com/install.sh && bash install.sh --modules=csp
```

On a minimal Debian without `wget`, first: `apt-get install -y wget ca-certificates`.

The script checks the system, the name and the architecture, adds the key and the package repository, installs `esapanel` and runs `esapanel-setup`. If the administrator data are missing, it asks for them.

The options

The options of `install.sh` go to `esapanel-setup`:

Option	What it does
`--channel=stable`	The package channel: `stable` (default) or `testing`, for test servers. Of `install.sh` only
`--modules=csp,ucp`	The modules to install: `csp`, `ucp`, `drp`, `wfp`, `lsp`, also together
`--license=ESAP-XXXX-XXXX-XXXX-XXXX`	The activation code
`--company=`, `--name=`, `--username=`, `--email=`	The company and the administrator of the panel
`--sender=panel@example.com`	The sender of the mail of the panel; without it, `panel@` followed by the name of the server
`--ssh-port=22`	The SSH port the firewall leaves open
`--backups-path=/var/lib/esapanel/backups`	The folder of the backups, best on a separate disk
`--wfp-datastore=/srv/wfp/ds1`	The first datastore of WFP (Web File), best the mount of a disk of its own

The password of the administrator is asked, or read from the environment variable `ESAPANEL_ADMIN_PASSWORD`: never on the command line.

The modules

Module	What it installs
`csp`	CSP (Central Syslog): the reception of the logs
`ucp`	UCP (Uptime Check): the plugins of the checks and the database of the results
`drp`	DRP (DMARC Report): the database of the DMARC reports
`wfp`	WFP (Web File): FTPS and SFTP, rsync on port 60022, WebDAV on 443, the datastore of the copies
`lsp`	LSP (License Server): the license server, on port 9444. Only for whoever sells the licenses

A module can be added later: run `esapanel-setup` again with all the modules, the previous ones and the new one. The module must also be in the license.

After the installation

At the end `esapanel-setup` shows the address of the panel:

```
https://log.example.com:9943
```

1. Open the address. The panel starts with a **self-signed certificate**: the browser warns about it, and that is normal. Replace it right away with a Let's Encrypt one (see Certificates, mail and DNS).
2. Sign in with the administrator created by the installation.
3. If you did not give it with `--license`, enter the **activation code** (see The license).
4. Confirm the **sender** of the mail in **Server › Mail**: until you do, every page reminds you.
5. Turn on the **second factor** on your account.
6. Check the **firewall**: for example open SSH only from your office (see Network and security).
7. Set up the **backup of the server** to a remote destination (see Disaster recovery).

Running esapanel-setup again

`esapanel-setup` can be run again whenever you want: what is already configured stays (the database password, the application key, the certificate), the rest is written again, and the panel is installed only once. It is for adding a module, adding a WFP datastore or writing again the IP addresses added by the panel.

Do not edit by hand the files that `esapanel-setup` writes: run it again.

Security from the start

- The **firewall** of the panel is on from the installation: the panel, SSH and the ports of the modules are open.
- **fail2ban** protects SSH, the sign-in of the panel and the web server.
- The **security updates of Debian** are automatic.

The license

The panel works with a license issued by Esalogica for your server. The license says which modules you can use and with which limits, for example how many subscriptions.

The page is **Server › License**.

Activating the license

Write the **Activation code** you received, in the form `ESAP-XXXX-XXXX-XXXX-XXXX`. The panel sends it to the license server of Esalogica, which binds the license to this server.

A new code replaces the current license. To add a module to the license you do not need a new code: **Check now** brings it. If the module is not installed on the server yet, the page says so: install it with `esapanel-setup` (see Installation).

Without a valid license only the administrator can sign in to the panel, on this page. The services already configured, such as the reception of the logs, keep working.

The daily check

Every day the panel checks the license with Esalogica, and receives renewals and changes by itself. **Check now** does it at once, for example after a renewal.

If the check fails, for example without Internet, nothing stops: the license stays valid until it expires, and after 7 days you receive a warning. Check that the server reaches `license.esalogica.com` on port 9444.

Expiry

- The administrators receive an email 7, 3 and 1 days before the expiry, on the day itself, 5 and 10 days after, and when the panel has stopped. After signing in they see it from 7 days before.
- After the expiry the panel works for another **10 days**, with a warning to everyone. A **Trial** license stops at once.
- A renewal reaches the panel by itself and stops the emails.

Another machine

The license is bound to this server by a **fingerprint**, which changes when the server is restored on another machine or copied. After a restore on another server, or on a copy of the server, the license belongs to the previous machine: the panel works for 10 days.

Transfer the license to this server with the button on the page. A license moves by itself up to 2 times in 30 days; beyond that, the transfer waits for the approval of Esalogica.

The page shows the fingerprint: Esalogica may ask you for it to issue a license by hand or to follow a transfer.

Updates, reboot and shutdown

Updates of Esapanel

New versions come from the package repository, which the panel checks every hour. The page is **Server › Updates**: it shows the version installed, the latest of the channel and the list of the updates made with their outcome.

The channel

- **Stable**: the versions tested. It is the choice for production servers.
- **Testing**: the new versions before the others, for test servers.

Going from Testing to Stable does not bring back an older version: the server stays on the version it has until Stable reaches it.

Updating by itself or by hand

With **Update Esapanel by itself** on, the panel installs a new version in the time window and on the days you choose, after the days of **Wait (days)** (counted from when this panel first saw the version). Off, the panel only tells you that there is a new version, and you install it from the page.

During the update the panel does not answer for a minute or two while it restarts.

For a server many others depend on, such as the license server, wait a few days and choose the mornings of working days: a version arrives after other servers have tried it, and an error shows up when someone can step in.

What an update does

1. It keeps a copy of the database of the panel and the package of the version installed.
2. It updates the `esapanel` package only, not the whole system.
3. It checks that the panel answers and that its services are running.

The outcome arrives by email. A failed update says how to go back to the previous version.

The security updates of Debian

With **Security updates of Debian by themselves** on, the security fixes of the system are installed every day by themselves. Esapanel is not among them: it follows the settings above. Turning them off leaves the system without its security fixes until someone updates it by hand.

The server never reboots by itself: the page says when a reboot is needed, for example after a kernel update.

Reboot and shutdown

Server › Reboot and shutdown reboots or shuts down the server from the panel, without a terminal.

When: in one minute, or at a time of day in your time zone (today if it has not passed yet, otherwise tomorrow). For example at night, after the security updates, when the updates page says the server needs a reboot. Until then the plan can be cancelled, from the page or from the notice at the top of every page.

While the server is down nothing works: the panel, the reception of the logs, the checks of the hosts. The devices that send their logs over UDP lose those of the minutes of the reboot; the agents keep them and send them afterwards. The reception of the logs records the interruption, and the customers see it in their logs.

Shut down: the panel cannot switch the server on again. After a shutdown it is switched on from the console of the provider or by hand. That is why the page asks you to write the name of the server: a check against shutting down the wrong server.

Choose for reboots a time when the customers feel it little, and tell them if they have devices that send over UDP only.

Network and security

This page is about the IP addresses of the server and its protections: the firewall, the bans of fail2ban, the blocking of the Internet scanners and the security overview.

IP addresses

Server › IP addresses lists the addresses of the server.

- **Detect the addresses** reads those configured on the server, which stay read only. The first time you open the page it does it by itself.
- **Add an address** puts a secondary address on an interface: the panel configures it at once and at every boot. It stays **In progress** until the server confirms it.
- **Public address** is needed only when the server is behind NAT: it is the address the server has as seen from the Internet.

An address is **Shared**, if it serves all the customers, or **Dedicated**, if it belongs to a reseller or a customer, within the limits of their subscriptions. A dedicated address is needed, for example, for a CSP (Central Syslog) subscription to receive logs on the standard ports 514 and 6514. The shared addresses a reseller gives to their customers come from their pool.

An added address is written in the network configuration of the server, so it comes back at every boot. At every boot the panel checks it: if it is missing it becomes **Failed**. Run `esapanel-setup` again to write the addresses again; if it stays failed, its interface no longer exists or the network of the server was changed by hand.

The security overview

Security › Overview shows the protections of the server at a glance:

- **Firewall**: whether the rules of the panel are active, and whether there are changes waiting to be applied;
- **IP bans**: the addresses fail2ban blocks now, and those blocked in the last day;
- **Internet scanners**: how many networks and addresses the firewall stops;
- **Failed sign-ins**: wrong passwords and second factor codes in the last day;
- **Certificate of the panel**: how long it still lasts;
- **Second factor**: how many active people have turned it on.

Each box leads to its page.

The firewall

Security › Firewall: inbound traffic is closed, except what the rules open.

- **Rules of Esapanel**: they protect the server and serve the modules, for example the reception ports of CSP and port 514 of the dedicated addresses. The panel writes them and they are read only.
- **Your rules**: checked in their order, the first that matches decides. They come after the connections already established and before the openings of the modules: a rule that drops a network blocks it on the ports of the modules too. The **SSH** and **Panel** rules were created by the installation and you can change them.
- **SSH access**: from any address, or only from the addresses and networks you list, such as the office and the home of the administrator. The page warns you when the address you are using now is not in the list. The panel stays reachable: only SSH is closed.

Applying changes without locking yourself out

Changes are a **draft**: the server keeps its firewall until you review and apply them.

1. Make the changes and open the preview: it shows the whole firewall that will be loaded, with the lines added and removed.

2. **Apply the firewall**: the server loads it at once.
3. Go back to the **Firewall** page and **confirm** within 60 seconds. The confirmation reaches the server only if you still reach the panel.

If a rule locked you out, you cannot confirm, and the server goes back to the previous firewall by itself.

Even when SSH is closed to your address, the console of the provider still works.

IP bans

Security › **IP bans** shows the bans applied by fail2ban.

- **Active bans**: the addresses blocked now, by fail2ban after their failed attempts or by hand, with the expiry. **Unban** removes a ban at once.
- **Ban an address**: blocks an address for a while or for ever, for example one that scans the server. A ban by hand ends by itself at its expiry.
- **Jails**: for SSH, for the sign-in of the panel and for the web server (bad bots, searches for weak applications, failed logins), how many failed attempts within how many minutes ban an address, and for how long. With WFP (Web File) installed, a row also watches FTPS, SFTP, rsync and WebDAV; an attempt there bans the address on all ports.
- **Never banned**: addresses and networks fail2ban never bans. Put the network of your office here, so a wrong password does not lock you out. The system entries keep the server from banning itself.

The register of the bans is updated every minute.

Internet scanners

Services such as Censys, Modat or Shodan probe every address of the Internet and catalogue the services that answer. By themselves they do no harm, but they fill the quarantine of CSP and tell whoever reads their catalogues what the server exposes.

Security › **Scanners**: the firewall stops them before they reach anything on the server, panel and SSH included:

- the **networks** the scanners publish, listed in **Scanners known**;
- the **addresses found**: every few minutes the panel looks up the reverse name of the unauthorized senders of CSP, and those with the name of a scanner are blocked for 30 days. An authorized source, an address of the server and an address that is never banned are never blocked.

Unblock removes an address; if it comes back with the name of a scanner, it is blocked again.

Research scanners, such as Shadowserver, warn the national CERTs and the owners of the networks about services exposed by mistake or vulnerable. Blocking them, those warnings about this server no longer arrive: think about it before doing it.

Certificates, mail and DNS

The certificate of the panel

Server › SSL certificates manages the certificate the panel uses for HTTPS on the name of the server. The same certificate also serves the TLS port of CSP (Central Syslog): a valid certificate lets devices and agents verify the server.

Kind	When to use it
Let's Encrypt	The normal choice: free, accepted by browsers, renewed by the panel 30 days before it expires
Upload a certificate	A certificate from another authority, for example the company one
Self-signed certificate	Made by the server, valid 10 years. It encrypts the connection, but every browser warns about it. The installation starts with one of these

Let's Encrypt

Let's Encrypt checks the name over HTTP on **port 80**:

- the name of the server must point to the server in the DNS;
- port 80 must be reachable from the Internet. The firewall of the panel opens it; a router or a provider in front of the server must also let it through.

The request takes a minute; the panel keeps its certificate until the new one is installed. If the request fails, the page shows why: fix it and request again. When a renewal fails, the administrators receive a single message and the panel tries again every day.

Uploading a certificate

Paste, in PEM format:

- the **certificate** of the server;
- the **intermediate certificates** of the authority: without them, some clients refuse the certificate;
- the **private key**, without a password. It is stored encrypted and never shown again.

The panel checks that the key belongs to the certificate, that it covers the name of the server, that it has not expired and that it leads to a trusted authority. An uploaded certificate is not renewed: the panel warns 30 and 7 days before it expires and on the day it expires.

Mail

Server › Mail: the mail the panel sends (notifications, invitations, outcomes of the backups) goes through postfix on this server. postfix only sends: it does not accept mail from outside.

Setting	What it holds
Sender	The address and the name the mail comes from; empty, `panel@` followed by the name of the server. Saving the page confirms it: until then every page reminds you
Receiver of the mail of the system	Where the mail of the server for root and postmaster goes, and the mail

Setting	What it holds
	that could not be delivered. Set an address you read
Delivery	**Direct: postfix delivers to the servers of the recipients**, or **Through a relay: postfix hands everything to another SMTP server**, such as the one of your company, Microsoft 365 or a sending service

The mail to the customers of a reseller keeps the sender of the server, but carries the name of the brand of the reseller, and the replies go to the support address of their brand.

Use a **relay** when the provider of the server blocks port 25, or when the mail ends up in spam.

Making the mail arrive

For direct delivery, the servers of the recipients trust the mail when:

- the **reverse name** of each address the server sends from, IPv4 and IPv6, is the name of the server. The provider of the address sets it;
- the **SPF record** of the domain of the sender authorizes the server. With the default sender, the record `v=spf1 a -all` on the name of the server is enough.

If the SPF does not authorize the server, the page shows the record to publish and the DMARC policy of the domain, which says what happens to the mail meanwhile; every page reminds you until it is fixed. With a relay, the SPF concerns the provider of the relay.

The **Queue** shows the mail postfix could not deliver yet: it tries again by itself for a few days. The **Test message** checks that a message leaves and arrives.

DNS

Server › DNS sets, in **How it finds the names**, the resolver of the server, which finds the addresses of the names for the panel, the mail, the certificates and the modules. It keeps the answers in its cache and answers only the server itself.

Mode	When to use it
By itself, from the root servers, checking the DNSSEC signatures	The normal choice: the resolver asks the servers of each domain directly and checks the DNSSEC signatures. It does not depend on the DNS of the provider, and the antispam lists, which refuse the questions of public resolvers, answer it
By asking other resolvers, such as those of the provider	When the provider blocks DNS towards the Internet: the resolver asks the resolvers you give, usually those of the provider. The signatures are not checked

Private domains: the domains that exist only in your network, such as `company.lan`, are not known on the Internet: give the DNS of the network that knows them. They are needed, for example, by the UCP (Uptime Check) checks towards internal machines.

Changing the mode empties the cache: for a moment the names are looked up again. If the resolver does not answer, the installation keeps the resolver the server had.

Resellers

A **reseller** is a customer who resells the services to customers of their own, with their own brand, within the limits of their **reseller plan**. What a reseller does in the panel is described in the reseller manual.

Services › Resellers lists the resellers. You, as administrator, also manage the direct customers, those without a reseller: in **Services › Customers** the **Belongs to** filter shows the customers of a reseller or the **Direct** ones.

Creating a reseller

New reseller asks, as for a customer, for the company data, the main account and, if you want, a first subscription of a **reseller plan**.

The reseller plan decides how many customers and subscriptions the reseller can have and which services they can resell. A reseller without a reseller plan cannot have customers: you can assign it later, from their page.

An existing customer can become a reseller: on their page, **Convert into reseller**. They keep their subscriptions.

Reseller plans

Reseller plans are created in **Services › Service plans**, like the other plans, choosing **For**: **Reseller**. Besides the services to resell, they include the reselling service, with its limits: how many customers, how many subscriptions, and how many resources the reseller can hand out in total. There are also **Reseller add-ons**.

The resources of the reseller

The page of a reseller shows **Resources of the reseller**: for each resource, how much they have **Assigned to the clients** (the sum of the limits of their subscriptions that are not disabled), the **Measured usage** and how much the **Reseller plan** allows. A red row goes beyond the plan.

With **Overselling** the limits assigned can go beyond the plan in total: the reseller sells more than they have, counting on the fact that not all customers use everything. The measured usage says how prudent that is.

Clients and subscriptions lists the customers of the reseller, with **Open the client**.

The rest

The other sections of the page of a reseller work as for a customer: company data, main account, status, backup, IP addresses and deletion (see the reseller manual, "Customers").

- **Suspending** or **disabling** a reseller applies to their subscriptions.
- A reseller can be **deleted** only when they no longer have customers: move or delete them first.
- The **Dedicated** addresses of a reseller or a customer are assigned by you (see Network and security).

Statistics and notifications

The statistics of the server

Server › Statistics shows how the server is doing: the panel measures CPU, RAM, network and disks every minute.

Chart	What it shows
CPU	The share in use, with the mean and the highest minute of each point, and the load of the last minute
RAM	The share in use, without the cache the system frees by itself when a program needs it
Network	The traffic received and sent by the main network card, in bytes per second
Disks	How full the disk of the system is, and those of the databases and of the data of the panel when they are separate

Choose the period at the top: the last 24 hours show a point every 10 minutes, the last 7 days one an hour, the last 30 days one every 6 hours, the last 12 months one a day. Minutes stay 2 days, hours 3 months, days 2 years. Hover over a point to read its time and value.

The start page shows the last 24 hours, with **All the statistics**.

Look at the disks above all: a disk of the logs or of the off-site copies that fills up must be enlarged, or the data moved, before it is full.

Notifications

Server › Notifications chooses who receives the emails the panel sends when something happens, and with which text. It works as for the resellers (see the reseller manual, "Notifications"), with these differences:

- there is also the **Administrator** column;
- your choices apply to the whole installation; a reseller can change them for their own customers, and where they change nothing yours apply;
- only you set the events of the installation.

The events of the installation

They are about the server and reach you:

Group	Events
Certificate	The uploaded certificate expires soon, has expired; the Let's Encrypt renewal failed; the renewal of the certificate of the panel name of a reseller failed
License	The license expires soon, today, has expired; the panel has stopped; the license cannot be checked
Updates	A new version is available; the panel was updated; the update failed

Group	Events
Reception of the logs (CSP)	The reception has stopped, started again; the logs do not reach the database, reach it again; the reception service does not listen on some ports, listens again
Off-site copy (WFP)	The datastore is filling up, has space again; the verification found differences; a relocation is over, has failed
License Server (LSP)	A license transfer waits for approval

Make sure these alerts reach an address that is read: in **Email addresses** you can add the one of the team that looks after the servers.

The notifications sent

Notifications sent in the last 90 days lists every notification sent, with the addresses reached and those it could not be sent to. An address shown as sent was handed to the mail of the server; if it did not arrive, look at the queue in **Server › Mail**. The list comes from the activity log.

Disaster recovery

The backup of the whole server is there to rebuild it if it is lost: a failed disk, a deleted server, a provider that closes. It is different from the backups customers and resellers make of their organizations and subscriptions.

The page is **Server › Disaster recovery**.

What it holds

- Always the **configuration**: the database of the panel, the configuration of the server, the data of each customer.
- For each module what you choose: for CSP (Central Syslog) the **searchable logs** and the **log archives**.

The backups customers and resellers keep on the server are not included.

Making the backups

Make a copy now makes one by hand, in the background; the email tells the outcome.

Above all, set a **Schedule** with a **remote destination** (an SFTP or FTP server, or an S3 storage): a backup kept only on this server is lost with it. The schedule works like the one of the backups of the customers: frequency, time, copies to keep, incremental backups. With incremental backups only the logs are incremental; the rest is full in every backup.

Download (single file) gives a file with everything inside, encrypted as you chose.

The key of the server

The backups are encrypted with the **key of the server**, or with your personal age key. In **Key of the server**, **Download the key** (with your password) and keep it away from the server, for example in a password manager: without it, or without your personal key, the backups cannot be opened if the server is lost.

Restoring on this server

Restore brings back, on this server, a part of the backup:

- the customers you choose (a reseller with their customers; none chosen means all);
- their configuration, their searchable logs, the archives no longer present;
- within a period.

The restore runs in the background; the email and the list tell its outcome. For a single customer or a single subscription, the backup of the customer or of the subscription is usually enough.

Rebuilding the server on a new server

1. Prepare a new server as for the installation (see Installation), with the same name and address if you can.
2. Install the `esapanel` package, of the version of the backup or newer.
3. Copy the files of the backup into a folder of the server.
4. As root:

```
esapanel-setup --restore=/root/backup --key=<key of the server>
```

or, with your personal key, `--identity=<private key>`.

The configuration comes back complete and the panel starts again with its customers, users, certificates and keys. The logs are then restored from **Server › Disaster recovery**, all of them or a choice.

If the new server has another name or address

`esapanel-setup` asks you:

- if the name or the main address will be changed to those of before, it stops: change them and run it again;
- with `--host=adapt` the panel takes the name and the address of the new server.

For the addresses added by the panel that the new server does not have: `--addresses=apply` moves them here, `--addresses=skip` leaves them **Failed**.

Remember that the devices and agents of the customers send to the name and ports of before: if the name changes, they must be configured again.

The license

After a restore on another machine, the license belongs to the previous machine: the panel works for 10 days, and you transfer it from the **Server › License** page (see The license).

A test now and then

A backup that has never been restored is not a safe backup. Now and then, try rebuilding the server on a test machine, with the key you kept: it is the only way to know that it works when it is needed.

CSP: the reception of the logs

CSP (Central Syslog) receives the logs of the devices of the customers on the ports of their subscriptions. If the reception stops, the logs sent over UDP at that moment are lost. **Modules › Log reception** is the page you keep an eye on it with.

The state of the reception

At the top the page says how the reception is now: "The server is receiving the logs (checked at …)", or the problem under way. The check runs every minute.

Below, the list of the **interruptions**, with **From**, **To**, **Duration** and **Cause**:

- **Reception stopped (restart or shutdown)**: a restart of the reception service or a shutdown of the server; start and end are accurate to the second;
- **Server stopped without warning**: a fault or a power cut. The start is the last check before, approximate to the minute.

The customers see each interruption among their logs, where it falls, and in the reports. When the reception stays stopped for a few minutes you receive a notification, and another when it starts again.

Logs that do not reach the database

The reception service (rsyslog) can be running and still not write the logs, for example when the database refuses a message and rsyslog retries it for ever. Every minute the panel sends a test message along the path of the logs: when it does not arrive for a few minutes, the page shows it and you receive a notification.

Meanwhile the logs wait in the queue of rsyslog, up to 1 GB, and reach the customers when the problem is solved; the alerts of silent devices are suspended.

Look at the log of rsyslog on the server, for example with `journalctl -u rsyslog`.

Ports without an answer

rsyslog can also be running and not listen on some reception ports, when it could not start them. Every minute the panel compares the ports rsyslog listens on with all the reception ports: when some are missing for a few minutes, the page says how many and you receive a notification with the first ones.

The devices that send to those ports lose their logs until rsyslog is restarted: look at its log and restart it with `systemctl restart rsyslog`.

The ports in the firewall

The reception ports of the subscriptions, and 514 and 6514 of the dedicated addresses, are opened by the panel among the **Rules of Esapanel** of the firewall: you do not need to open them by hand (see Network and security). If the server is behind an external firewall or NAT, the ports must be opened there by hand.

The certificate

The TLS port and the port of the agents use the certificate of the panel: with a self-signed certificate the devices cannot verify it, and the agents do not send over TLS. Use a valid certificate, from Let's Encrypt or uploaded (see Certificates, mail and DNS).

UCP: the settings of the checks

UCP (Uptime Check) runs the checks of the customers from this server: the pings, the connections, the HTTP and DNS requests leave from here and reach the addresses the customers write. How hosts and checks are used is described in the customer manual.

All the hosts

Modules › Hosts lists the hosts of all the subscriptions, with the **State**, the **Checks** in each state and since when (**Since**). At the top, the **Hosts down** and the **Checks with a problem**: both open **Modules › Problems**. You can search by name or address and filter by state and by customer.

Checks towards private addresses

Modules › Check settings has a single choice, an important one: **Allow checks towards private addresses**.

Choice	When
On	The panel is installed in the network of the company that uses it: the customers can check the machines of the internal network, such as `192.168.x.x` and `10.x.x.x`
Off	The panel hosts customers who do not know each other: only public addresses are accepted, and not those of this server

On a panel that hosts several customers leave it off: on, a customer could use their checks to probe the internal network of the server.

The panel itself (`127.0.0.1`) is never a destination. Turning the choice off, the hosts already saved are not deleted: their checks answer **Unknown** with the reason.

The resolver

The DNS checks "to the resolver of the panel", and the names of the hosts, use the resolver of the server. To let the customers check names that exist only in the internal network, add the **Private domains** in **Server › DNS** (see Certificates, mail and DNS).

The outbound firewall

The checks leave from the server: if the server is behind a firewall that limits outbound traffic, the checks towards the blocked ports fail. Check the outbound rules before giving UCP to the customers.

WFP: datastores and relocation

WFP (Web File) keeps the off-site copies of the customers in one or more **datastores**: folders of the server, best each on a disk of its own, which hold the files of the subscriptions. The page is **Modules › Off-site datastores**.

Datastores

The first datastore is born with the module, in the folder given with `--wfp-datastore` at the installation (see Installation).

To add one, mount the new disk and run on the server, as root:

```
esapanel-setup --modules=csp,wfp --wfp-add-datastore=/mnt/disk2/wfp
```

with all the installed modules in `--modules`. The datastore appears on the page within five minutes. The folder cannot be under `/home`, `/root` or `/run`. The panel never chooses a folder of the server by itself.

For each datastore the page shows the **Folder**, how much of its disk is **In use** and **Free**, and how many **Subscriptions** it holds.

- At 80% and 90% you receive a warning.
- At 95% its accounts become read only, until it goes below 90%.
- "Not found on the server: is its disk mounted?" means the folder is no longer there: check the mount.

New subscriptions: the datastore where the subscriptions created from now on are born (**Make them here**). The existing ones stay where they are: move them with **Relocate**.

Relocation

Relocate moves the files to another datastore, for example to empty a disk to replace or to balance the space. In **What to relocate** choose **A subscription**, **A customer, or a reseller with its customers** or **Every subscription of a datastore**, and **To the datastore**.

The subscriptions move one at a time, in three steps:

1. **Copying, accounts working**: the files are copied while the accounts keep working, for as long as it takes;
2. **Last copy, accounts stopped**: the last copy is made with the accounts stopped, so it finds the files still. It lasts the time to read the list of the files again, usually a few minutes; a backup that starts in those minutes fails and is made again at the next round;
3. the subscription moves to the new datastore and is verified. Accounts, passwords, keys and addresses do not change: there is nothing to change on the devices of the customers.

You receive a warning when a relocation is over and when it fails. A relocation that fails leaves the subscription where it was, working. **Cancel** stops a relocation under way and removes its copy.

The old folder

After a relocation the old folder stays in the datastore it left, and takes its space. **Remove the old folder** when you have seen that the copies arrive in the new datastore: it cannot be undone. Until then the same subscription cannot be relocated again.

The remote copy

The off-site copies of the subscriptions with the **Remote copy** service can be sent every night to a second Esapanel server in another place, also with WFP.

This server can only add. On the other server each subscription has an account of its own, which keeps what is replaced or deleted for the days chosen there. Whoever took control of this server could not destroy the remote copies.

To set it up:

1. On the other server create an off-site copy subscription and, inside it, **one account for each subscription to send**, with rsync only. On the page of the account paste the **Public key of this server** and choose for how many days it keeps what is replaced or deleted.
2. Here, in **Remote copies**, write the **Server of the remote copies** and save. Compare the **Fingerprints of the server** shown with those on the page of the account on the other server: if they differ, something else answers at that address.
3. Give the **Remote copy** service to a subscription, in its plan or as an add-on, and write here its **Account on the other server**.

The transfers start at the chosen time, one subscription at a time, and send only what changed; you can limit the **Bandwidth, in KB per second**. **Send now** starts one without waiting for the night. When a transfer fails you receive a warning; the next one is tried the night after.

Verification and repair

Every night the panel compares what the server has for each subscription with what it knows. The differences, and the **Repair** that fixes them, are on the **Off-site copy** page of each subscription (see the reseller manual, "Modules for the reseller"). When the verification finds differences you receive a warning.

LSP: the license server

LSP (License Server) is the module that issues the licenses of Esapanel: it is only for whoever sells the licenses of the panel, such as Esalogica. On a panel that does not sell licenses it is not installed, and this page does not concern you.

With LSP installed, the server answers the panels of the customers on port **9444**, where they activate and check their license every day.

A license is a subscription

Every license sold is a **subscription** of a plan with the **License** service:

- the **plan** sets the module, the tier, whether it is a Trial and the limits;
- the **subscription** sets the validity and the state.

To sell a license, then, you create a subscription of the right plan for the customer, as for any service.

Licenses

Modules › Licenses sold lists the licenses, with:

- **Code**: the activation code the customer enters on the **License** page of their panel;
- **Status**: active, suspended or ended, like the state of the subscription. The panel of the customer receives it at the daily check;
- **Server**: the server the license is bound to, or "Not activated";
- a possible **transfer waiting**.

You can search by code, server name or customer.

The page of a license

In the subscription, the **License** tile shows:

- the **Activation code**: the license binds to the first server that activates it, and the panel of the customer receives the signed license;
- the **Status**: suspend, reactivate or end the license with the state of the subscription. A suspended or ended license stops the panel of the customer at the next daily check; the services already configured keep working;
- the **Server** bound to the license, with its last daily check;
- **Renewal and terms**: the last day of validity, the module, the tier and the limits. The empty limits of customers and resellers are those of the tier. The server of the customer receives every change at the next daily check;
- **Activations and transfers**: when the license was activated and moved to other servers, by itself or with approval.

Transfers

A customer moves the license to another server, for example after a restore on new hardware, from the **License** page of their panel.

- A license moves by itself up to **2 times in 30 days**: the panel of the customer receives it at once.
- Beyond that, the transfer waits in **Modules › License transfers**. **Approve** moves the license: the new server receives it at the next daily check, and the previous server stops at its own. **Reject** leaves the license where it is.
- A new request from the customer replaces the one waiting.

You receive a notification for each transfer waiting.

A delicate server

The panels of all the customers depend on this server. Keep it updated with care: automatic updates with a few days of waiting, on the mornings of working days (see Updates, reboot and shutdown). A panel that cannot check its license keeps working until it expires, but its administrators receive a warning after 7 days.