# Customer manual

Esapanel

Esalogica

15 November 2026

# Contents


Getting started....5
Signing in....5
How the panel is laid out....5
Help in the panel....6
A suspended or disabled subscription....6
Your account....7
Profile....7
Second factor....7
Sessions....8
Users and roles....9
The users....9
The roles....10
The company data....10
Subscriptions....11
The list of subscriptions....11
The page of a subscription....11
Usage....12
The state of the subscription....12
Configuration backups....13
The Backup page....13
Making a copy now....13
The encryption....13
The schedule....14
Restoring....14
Downloading and deleting....15
Notifications....16
Who decides who receives them....16
The emails you can receive....16
If an alert does not arrive....17
Sending logs to the panel....18
1. Introduction....18
2. Where to find the values....18
3. The reception ports....19
4. Adding a device....20
5. Windows servers....22
6. Linux servers....23
7. Routers, firewalls and other devices....25
8. Checking that the logs arrive....26

9. Common problems..... 27
Sending logs from MikroTik..... 29
1. What the panel receives..... 29
2. Adding the MikroTik in the panel..... 29
3. Sending the logs..... 29
4. Firewall rules..... 30
5. Checking that the logs arrive..... 30
6. Common problems..... 30
Sending logs from pfSense and OPNsense..... 32
1. What the panel receives..... 32
2. Adding the firewall in the panel..... 32
3. pfSense..... 32
4. OPNsense..... 33
5. Checking that the logs arrive..... 34
6. Common problems..... 34
Devices and quarantine..... 35
The list of devices..... 35
The page of a device..... 35
The quarantine..... 36
The codes of the agents and of the links..... 37
Ports 514 and 6514..... 37
Searching and reading the logs..... 38
Searching..... 38
The fields of the event..... 38
Interruptions of the reception..... 38
The names of the addresses..... 38
Downloading..... 39
Where the older logs are..... 39
Alert me if it repeats..... 39
Event alerts..... 40
Episodes..... 40
The rules..... 40
Your rules..... 41
Exceptions..... 42
Reports and analysis..... 43
The analysis..... 43
The reports..... 43
Importing logs from files..... 45
How it works..... 45
1. Sending the files..... 45

2. What the files hold....46
3. Your choices....46
Good to know....46
Taking an import away....46
Log archives and backups....47
The log archive....47
The backups of the subscription....47
The off-site copy....49
1. Introduction....49
2. The pages of the subscription....49
3. The space and where to connect....50
4. Adding an account....50
5. Connecting the programs....51
6. Encrypting the copies....52
7. Managing an account....52
8. Shared folders....52
9. Checking that the copies arrive....53
10. The reports....53
11. When the space runs out....54
12. Subscription suspended or deleted....54
13. Common problems....54
14. For administrators and resellers....55
Hosts and checks....56
Where to find it....56
Adding a host....56
Adding checks....56
The states....57
The page of a host....57
Problems....58
Alerts....58
Downtimes and availability....59
What happens during a downtime....59
Planning a downtime....59
All the downtimes....59
Availability....59
DMARC reports....61
The domains....61
How the reports arrive....61
Reading the reports....62

How to use the Esapanel panel and the services of your subscription.

# Getting started

The Esapanel panel is where you find the services you bought, your **subscriptions**, and where you manage the users of your company. This page explains how to sign in, how the panel is laid out and where to find help.

## Signing in

Your service provider gives you the address of the panel. It may be a name with the provider's brand, for example `panel.example.com`.

On the **Sign in** page, write your **Username** and **Password** and press **Sign in**. **Remember me** makes the browser remember the sign-in: use it only on a computer of your own.

### *The first sign-in*

When an administrator of your company creates a user for you, they can:

- send you an email with a link to choose your password: open the link, choose the password and confirm it with **Save the password**. Until then your user is **Invited**;
- or set the password themselves and tell it to you.

Your username is the one given to you by whoever created the user.

### *Forgotten password*

On the **Sign in** page, **Forgot your password?** opens **Reset your password**: write the **Email address** of your account and press **Send the reset link**. The email contains a link to choose a new password.

### *The second factor*

If you turned on the second factor (see Your account), after the password the panel asks for the **Code** that the authenticator app on your phone shows at that moment. Without the phone, **You do not have the phone? Use a recovery code** lets you sign in with one of your recovery codes.

### *Too many attempts*

After too many wrong attempts the panel asks you to wait before trying again, and says for how many seconds. If you stay inactive for too long, the panel asks you to sign in again.

### *Signing out*

**Sign out**, at the top right, closes the session. On a shared computer, always sign out at the end of your work.

## How the panel is laid out

### *The menu*

The menu is on the left. On a phone it opens with the **Menu** button at the top. The items a customer can see are:

| Group | Item | What it holds |
|---|---|---|
| | **Home** | The start page |
| **Services** | **Subscriptions** | Your subscriptions, with the services of each (see Subscriptions) |
| **Organization** | **Users** | The people of your company who use the panel (see Users and |

| Group | Item | What it holds |
|---|---|---|
| | | roles) |
| | **Roles** | What each user can do |
| | **Company data** | Company name, tax data, address |
| | **Backup** | The copies of your organization (see Configuration backups) |
| **Modules** | **Hosts**, **Problems**, **Downtimes** | With UCP (Uptime Check): the hosts watched in all your subscriptions, the open problems, the downtimes (see Hosts and checks) |

Everyone sees only the items their **role** allows: a user with the **Auditor** role, for example, sees the pages but cannot change them. If an item you need is missing, ask an administrator of your company.

*The start page*

**Home** opens the **Dashboard**, with a welcome. From here you go to your subscriptions with **Services** › **Subscriptions**.

*Your account*

At the top right is your username: it opens the pages of your account, that is profile, second factor and sessions (see Your account).

## Help in the panel

The panel explains its own pages, in two ways.

- **Help**, at the top, with the question mark: it opens **About this page**, a short explanation of what the page you are looking at does and of its buttons. At the bottom, under **Need help?**, are the support contacts of your provider.
- The **small question mark** next to a field (**What is this?**) explains that field.

This manual describes the same pages more fully, with the way to reach them and the typical cases. For the details of a page, the help of the panel always matches the version installed.

## A suspended or disabled subscription

If a subscription is **Suspended** or **Disabled**, the pages of its services do not open and the panel shows why. A subscription suspended for going over a limit of its plan becomes active again by itself when the usage is back within the limit. In the other cases, ask whoever provides the service. The states are explained in Subscriptions.

# Your account

Everyone who uses the panel has an account of their own. The pages of the account open from your username, at the top right, and are three: **Profile**, **Second factor** and **Sessions**.

What you change here applies only to you. The data of the company, shared by all its users, are in **Organization** › **Company data** (see Users and roles).

## Profile

| Field | What it is for |
|---|---|
| **Username** | The name you sign in with. Only an administrator of your company changes it |
| **Name** | Your name, as the other users see it |
| **Mobile** | Optional. Whoever manages the users of your company and your provider can see it. For now the panel does not send you messages |
| **Timezone** | The times the panel shows you, and the time of the backup schedules you save |
| **Language** | The language of the panel and of the emails you receive |
| **Color palette** | The colors of the panel, for you only |

Press **Save the profile** to save.

Choose the time zone of the place where you work: with a wrong time zone the times of logs and backups look shifted.

### *Email address*

The address that receives the link to reset the password. To change it, write the new address and your **Current password**, then **Change the email**.

### *Password*

Write the **Current password**, the **New password** and **Confirm the new password**, then **Change the password**. Changing the password closes all the other sessions: the devices you had signed in on ask you to sign in again.

An administrator of your company can give a role the right to change the profile data but not the password and the email: in that case, ask them.

## Second factor

With the second factor, signing in asks, besides the password, for a six-digit code made by an app on your phone. Whoever finds out your password cannot sign in without your phone. It is the most useful protection you can give your account.

You need an authenticator app, such as Google Authenticator, Microsoft Authenticator or FreeOTP.

### *Turning it on*

1. In **Second factor**, write your **Current password** and press **Turn on**.
2. Scan the QR code with the app. If you cannot scan it, enter in the app the **Setup key** shown below it.

3. Write the **Code** the app shows at that moment and press **Confirm**.

Until you confirm the code, signing in does not change. If the code is not accepted, check that the time of the phone is right.

### *The recovery codes*

When the second factor is on, the panel shows the **Recovery codes**, only once. Each one lets you in once without the phone. Keep them in a safe place, away from the phone, for example printed or in a password manager.

The page says how many codes you have left. **Generate new codes** makes a new set: the old ones stop working.

### *Turning it off*

**Turn off the second factor**: signing in asks only for the password again. To turn it back on you will scan a new QR code.

### *Lost phone*

If you lost your phone, sign in with a recovery code, turn off the second factor and turn it on again with the new phone.

If you lost the recovery codes too, ask an administrator of your company: they can turn off your second factor from the page of your user. For the main account of the company (**Owner**), ask your provider.

## Sessions

**Open sessions** lists the devices and browsers you signed in on, with the **IP address** and the **Last activity**. The session you are using is marked **This session**.

- **Close** closes a session you do not recognize.
- **Close all other sessions** closes every session except the one you are using, for example after using a shared computer.

If you think someone else knows your password, close the sessions and change the password from **Profile**.

# Users and roles

Several people of the same company can use the panel, each with their own account. Every user has a **role**, which decides what they can see and do. Users, roles and the data of the company are in the **Organization** group of the menu.

To manage users and roles you need a role that allows it, such as **Owner** or **Administrator**.

## The users

**Organization** › **Users** lists the people of your company who use the panel, with **Role**, **Status** and **Last login**.

The **Owner** is the main account of the company. It is not changed from this page: the Owner changes their own data from their profile, and your provider can change the Owner.

### *Adding a user*

**New user** asks for:

| Field | What to write |
|---|---|
| **Username** | The name the person signs in with |
| **Name** | The name of the person |
| **Email** | Their address: it receives the invitation and the links to reset the password |
| **Mobile** | Optional |
| **Role** | What they can do (see below) |
| **Password** | How the person will get the password |

For the password there are two ways:

- **Send a link to choose the password**: the person receives an email and chooses the password at the first sign-in. Until then they are **Invited**. This is the way to prefer: only they know the password.
- **Set the password now**: you write it and tell it to the person.

### *The states of a user*

| State | What it means |
|---|---|
| **Active** | Signs in normally |
| **Invited** | Has not chosen the password yet |
| **Suspended** | Cannot sign in, for example during an absence |
| **Disabled** | Cannot sign in |

A suspended or disabled user is stopped at the next page, even with a session open.

### *Changing a user*

**Edit**, on the row of a user, opens their data, role and state.

- **Send the invitation again**, for an **Invited** user who did not receive the email or lost it.
- **Turn off the second factor**, for a user who lost the phone and the recovery codes: they sign in with the password only and can turn it back on from their account.
- **Delete the user**: the user can no longer sign in. It cannot be undone.

You cannot change the role or the state of your own account: another administrator has to.

When a person leaves the company, delete or disable their user: do not leave active accounts of people who no longer work with you.

## The roles

A role is a set of functions, each **Granted** or **Denied** as a whole: for example **CSP · View logs**, **CSP · Manage the devices and the quarantine** or **Manage users and roles**. **Organization › Roles** shows the roles and how many users have each.

### *The system roles*

They are the same for every customer and cannot be changed:

| Role | What it can do |
|---|---|
| **Owner** | The main account, with every function |
| **Administrator** | Every function |
| **Operator** | Works on the services, but without deletions, exports and restores |
| **Auditor** | Read only, besides managing their own account |

The functions of these roles are updated with the new versions of the panel.

### *Custom roles*

If a system role does not fit, make one of your own:

- **Duplicate**, on a system role, makes a copy to change;
- or **New role**, with a **Name**, a **Description** and the **Access to the functions**.

You can grant only the functions you have yourself. The functions marked as *includes operations that cannot be undone*, such as deletions and restores, should go only to those who really need them. Every role can always see and change its own account.

A change to a role applies at once to every user who has it. A role assigned to some users cannot be deleted: first give those users another role.

### *Example: someone who only reads the logs*

For a consultant who must read the logs but not change anything, the **Auditor** role is enough. If they must also download them, duplicate **Auditor**, grant in the copy the function **CSP · Export logs** and give the consultant the new role.

## The company data

**Organization › Company data** holds the data of your company, shared by all its users: **Company name**, **VAT number**, **Tax code**, **Contact person**, **Contact email**, **Telephone**, **Fax**, **Website** and the address.

Every user sees them. Only the administrators of the account can change them, with **Save the company data**.

- The **VAT number** is written in the international form, with the country code in front, for example `IT01234567890`. If you write it without, the panel adds the code of the country chosen.
- **Telephone** and **Fax** take the international prefix chosen next to the number.
- A **Website** written without `https://` gets it.

# Subscriptions

A **subscription** is a service you bought: for example the collection of the logs of your devices, or the space for off-site copies. A company may have several subscriptions, even of the same service, for example one per site.

Every subscription comes from a **plan**, which your provider chooses with you: the plan sets which services it includes and its **limits**, such as the number of devices or the space. Your provider changes the plan and the limits. You use the services and keep an eye on the usage.

## The list of subscriptions

**Services** › **Subscriptions** lists your subscriptions, with:

| Column | What it shows |
|---|---|
| **Name** | The name of the subscription, useful when you have more than one |
| **Plan** | The plan it comes from, and whether it **Follows the plan** or is **Customized** |
| **Modules** | The services it includes |
| **Since** | Since when it is active |
| **Status** | **Active**, **Suspended** or **Disabled** |

A **Customized** subscription has some values different from its plan, agreed with your provider.

The name of a subscription opens its page.

## The page of a subscription

At the top is the name of the subscription. Below, a **tile** for each thing you can see or do: every tile opens a page.

The tiles depend on the services of the subscription and on your role. A user with a limited role sees fewer tiles.

*The tiles of the services*

| Service | Tiles |
|---|---|
| CSP (Central Syslog), the collection of the logs | **Logs**, **Analysis**, **Reports**, **Event alerts**, **Devices**, **Backup**, **Log archive**, **Quarantine** |
| UCP (Uptime Check), the watch over your servers and services | **Hosts** |
| WFP (Web File), the off-site copy | **Off-site copy**, **Accounts**, **Shared folders**, **Activity**, **Reports** |
| DRP (DMARC Report), the DMARC reports of your domains | **DMARC** |
| LSP (License Server), the license of a product | **License** |

Some tiles show a number when something waits for you. For example, **Quarantine** shows how many senders wait for a decision, and **Hosts** how many problems are open.

Each service has its own pages in this manual. For the collection of the logs, for example, you start from Sending logs to the panel.

For a CSP subscription the page also shows, at the top, the **Reception of the logs** box, with the server and the ports the devices send to.

## Usage

The **Usage** tile shows how much the subscription uses of the resources the panel measures, such as the monthly volume of the logs or the space of the backups.

- For each resource there is a chart, with **Last 30 days** (one point a day) or **Last 12 months** (the value at the end of the month).
- The **red line** is the limit of the plan, the **dotted line** the threshold of the warning.
- The usage is measured every night for the day just closed. A subscription just created has no history yet: the first point comes with the measure of the night.
- **Recalculate the usage** measures at once, for example after deleting old backups to free some space. After a recalculation you have to wait a little before the next one.

### *Near the limit and over the limit*

When a resource reaches the threshold of the warning, the panel sends a warning once. When it goes over the limit, it sends a warning every day while it stays over. Your provider decides who receives these warnings (see Notifications).

What happens over the limit depends on the plan. With some plans the subscription is **suspended** until the usage is back within the limit: the service goes on behind the scenes (for example the logs keep arriving), but its pages stay closed. It becomes active again by itself as soon as the usage is back within the limit, also after a recalculation.

To get back within the limit you can free some space, for example by deleting old backups, or ask your provider for a larger plan or an addition to the plan.

## The state of the subscription

| State | What it means for you |
|---|---|
| **Active** | It works normally |
| **Suspended** | You see the subscription and its state, but not the pages of its services. The service goes on behind the scenes: the logs arrive and are kept, the checks go on. The alerts of the services go to your provider instead of you |
| **Disabled** | The service is stopped: the logs that arrive are discarded, the checks do not run. What was received before stays until the end of its retention, and the ports stay with the subscription: when it is active again, the devices start sending again without being configured again |

Your provider decides suspension, disabling and reactivation, except for the automatic suspension for a limit gone over. For a suspended or disabled subscription, ask whoever provides it.

# Configuration backups

A backup of your organization is a copy of what you set up in the panel: the company data, the users and the roles and, for every subscription, the name, the devices, the plan and the limits. It can also hold the **searchable logs** of the subscriptions. It is there to put things back as they were after a mistake, for example a device or a user deleted by accident.

The backups are in **Organization** › **Backup**. To make and restore them you need a role that allows it.

This page is about the copy of the organization. The copies of the logs of a single CSP (Central Syslog) subscription are in the **Backup** tile of the subscription. For an off-site copy of WFP (Web File), the backup holds its accounts and shared folders, not the files.

## The Backup page

At the top, the page sums up the situation:

- **Last copy**, with its outcome;
- **Next copy**, with the schedule told in one sentence (for example: every day at 02:00, always a full copy, keeps the last 7 copies, on the server), or "No schedule: the copies are made by hand only.";
- **Space**, the one taken by the copies.

The **Make a copy now** and **Schedule** buttons open the pages described below. The **Copies** list shows every copy with **Date**, **Type**, **Content**, **Key** and **Status**, and the **Download**, **Restore** and **Delete** buttons.

## Making a copy now

**Make a copy now** prepares a copy with everything already chosen: you only confirm. The copy is made in the background: the list shows when it is ready (**Queued**, **In progress**, **Completed**) and an email tells the outcome.

In the **Advanced options** you can change the **Encryption** (see below) and the address that receives the email with the outcome (**Send the outcome to**).

## The encryption

| Choice | What it means |
|---|---|
| **With the key of the server** | The panel encrypts and decrypts by itself. The download comes decrypted and the restore is automatic. This is the normal choice |
| **With my personal age key** | Only your private key opens the backup, not even the server can read it. Write the **Public age key** (it starts with `age1`). If you lose the private key, the backup is lost |
| **In plain text** | No encryption: whoever gets the file reads it, logs included |

The personal key is for those who want to keep copies that nobody else can open, not even whoever runs the server. The key is made with the `age` program, on your computer. Keep the private key in a safe place, apart from the copies.

## The schedule

**Schedule** makes the copies by itself.

| Field | What to choose |
|---|---|
| **Make the backups on schedule** | Turns the schedule on |
| **Every** and **At** | **Day**, **Week** or **Month**, and the time. The time is in the time zone of whoever saves the schedule |
| **A full backup, then incremental ones with only the new logs** | After a full copy, the next ones hold only the new logs: smaller and faster. **A new full backup every** week or month |
| **Copies to keep** | How many copies to keep. The oldest are deleted; the copies made by hand are never touched |
| **Where** | **On the server**, **On a remote destination**, or **On the server and on a remote destination** |

With incremental backups a "copy" is a full backup with the incremental ones that follow it. The restore rebuilds the chain from the full backup by itself.

Press **Save the schedule**.

*Remote destinations*

A **remote destination** is a server of yours where the schedule copies the backups: an **SFTP or FTP** server, or an **S3**-compatible storage. So the copies also stay outside the server of the panel. The files arrive as they are on the server, encrypted if they are, and the remote space does not count in your limits.

In **Remote destinations**, **Add a destination** asks for the **Name**, the **Type** and the access data:

- **SFTP or FTP**: **Server**, **Port**, **User**, **Password** or **Private SSH key**, the **Folder**. With FTP, turn on **FTP with TLS (FTPS)** if the server supports it: without TLS the password travels in clear.
- **S3**: **Bucket**, **Region**, **Endpoint** (empty for Amazon S3), **Access key**, **Secret key**; **Path-style addresses** for MinIO and some NAS.

For SFTP, the panel reads the **fingerprint** of the key of the server and asks you to confirm it: check it on the server with `ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub`. From then on the panel connects only to a server with that fingerprint.

The panel tests the destination when you save it. **Test** tests it again whenever you want; the list says whether it works and when it was tested. If a copy does not reach the destination, the panel says so and the file stays on the server.

Deleting a destination does not delete the copies already there, but the panel no longer reaches them.

## Restoring

**Restore**, on the row of a copy, opens a page in steps.

1. **What to restore**: the whole copy or a part of it, for example a single subscription; the logs, the configuration or both. For the logs you can choose the period (**Logs from** … **to**).

2. **The key of the copy**, only for a copy encrypted with your personal key: write the private age key (it starts with `AGE-SECRET-KEY-`). It is used for this restore only and is not stored.
3. **Summary and confirmation**: what happens, and the confirmation.

What comes back:

- **Logs**: the missing ones of the period come back; the ones still in the panel and the ones arrived later stay.
- **Configuration**: company data, users, roles and devices go back to how they were in the copy, and what was added later is removed. That is why the panel asks you to confirm with "I understand that the configuration goes back to the one of …".

The restore runs in the background; the email and the list tell its outcome.

Before restoring the configuration, think about what changed after the copy: a user created later, for example, disappears. If you only need to get some logs back, restore only the logs.

## Downloading and deleting

**Download** saves the copy on your computer. A copy with the key of the server comes decrypted.

**Delete** removes it for good. For a full copy with incremental ones, it also deletes the incremental ones that follow it.

# Notifications

The panel sends an email when something that concerns you happens: a resource near its limit, a backup that failed, a device that stops sending logs, a server that does not answer. This page says which emails you can receive and who receives them.

## Who decides who receives them

Your **provider** decides who receives each alert, for all their customers: they can send it to you, to themselves, or to other addresses, for example the one of their support. The texts of the emails are theirs too. You do not change these settings from the panel: if you want to receive an alert that does not reach you, or stop receiving one, ask your provider.

When an alert is for "the customer", it goes to the main account of your company (**Owner**).

Some emails go to a precise address and do not depend on these settings:

- the link to reset the password goes to the user who asked for it;
- the outcome of a backup or of a restore goes to the address written when you asked for it or scheduled it.

You decide instead **when** some alerts of the services go off: for example **Alert if silent for** on a device of CSP (Central Syslog), or the rules of the **Event alerts**.

The emails arrive in the language chosen in the profile of whoever receives them, with the brand and the signature of your provider.

## The emails you can receive

*The panel*

| Event | When it arrives |
|---|---|
| A resource of a subscription is near its limit | Once, when the usage reaches the threshold of the warning |
| A resource of a subscription is over its limit | Every day, while the usage stays over |
| A subscription is suspended for going over a limit | Once, when it is suspended |
| A subscription suspended for going over a limit is active again | Once, when the usage is back within the limit |
| A backup failed | At every backup that does not succeed |
| Report of a backup or of a restore | To the address given in the request |
| Password reset | To the user who asked for it |

*CSP (Central Syslog)*

| Event | When it arrives |
|---|---|
| An event alert of the logs; still going on; over | Following the rules of the **Event alerts** tile |
| A report of the logs is ready | When a daily, weekly or monthly report is ready |
| A source stopped sending logs; sends logs again | Following **Alert if silent for** of each device |

*UCP (Uptime Check)*

| Event | When it arrives |
|---|---|
| A host is down; is up again | When a host stops answering and when it comes back |
| A check has a problem; is OK again | When a check changes state |
| A problem is still open | As a reminder, while the problem stays open |

*WFP (Web File)*

| Event | When it arrives |
|---|---|
| An account has not uploaded for too long; uploads again | When a device stops sending its copies, and when it starts again |
| A copy is much smaller than usual | When a copy looks incomplete |
| An upload replaced or deleted a large part of the files of an account | It may be the sign of ransomware or of a mistake |
| A report of the off-site copy is ready | Every week and every month |
| The space is over the limit; is within the limit again | Over the limit the accounts become read only |

Each service explains its alerts in its own pages of this manual.

## If an alert does not arrive

1. Check the spam folder.
2. Check the email address of the recipient: for the Owner it is in their **Profile**.
3. Ask your provider: they decide who receives each alert, and can check the list of the notifications sent.

# Sending logs to the panel

## 1. Introduction

*What the service does*

The CSP (Central Syslog) module of Esapanel collects the **logs** of your servers and network devices: successful and failed sign ins, errors, warnings, firewall and VPN events. It keeps them in your **subscription**, lets you search and analyse them and summarizes them in reports, also as support for documenting the security measures required by the NIS2 directive.

The logs arrive with the **syslog** protocol, the standard that almost every network device knows. For Windows and Linux servers there is the **Esapanel agent**, a small program that reads the events of the server and sends them to the panel.

*Who this guide is for*

The IT staff of the company, or the provider that manages its systems. You need to know how to configure a server or a firewall; you do not need to know Esapanel.

The guide covers only **sending the logs**: how to configure servers and devices, and how to check that the logs arrive.

*What you need*

- An active CSP **subscription**.
- A panel user who can open the **Devices** page of the subscription (in the panel: the subscription, then the **Devices** tile).
- Administrative access to the servers and devices to configure.
- Servers and devices that can **go out to the Internet** towards the panel server, on the ports given below. No inbound port has to be opened.

In this guide names and addresses are examples (`example.com`, `192.0.2.10`, `203.0.113.10`, `2001:db8::10`). The real values of your subscription are on the **Devices** page.

---

## 2. Where to find the values

The server and the ports of the subscription are shown at the top of the subscription page, in the **Reception of the logs** box: **Server**, **Port in clear**, **TLS port** and **Port of the agents**.

All the values to enter in the devices are also on the **Devices** page of the subscription, in the **Sending the logs** box at the top:

| Field on the page | What it holds | In this guide |
|---|---|---|
| **Server** | The name of the server to send to. If the subscription receives on a dedicated address, that address is here | `<server>` |
| **Port** | The port of the subscription, in clear | `<port in clear>` |
| **Protocols** | "UDP or TCP, syslog RFC 3164 or RFC 5424" | |
| **Over TLS (encrypted)** | The name of the server and the TLS port, as `name:port` | `<server name>` and `<TLS port>` |
| **Port of the agents** | The name of the server | `<port of the agents>` |

| Field on the page | What it holds | In this guide |
|---|---|---|
| | and the port of the agents, as `name:port` | |

Next to server and port, the **Copy** button copies the value.

The instructions of each device (see chapter 4) repeat these values, already filled in, and add the **Address** field: the IP address of the server, for devices that do not accept a name.

The ports are assigned to each subscription and differ from one subscription to another: **always use those of your Devices page**, never ports taken from other examples.

If the page says "The subscription has no port yet", the reception is not ready yet: contact your service provider.

---

## 3. The reception ports

Each subscription receives logs on **three ports**, all on the same server.

| Port | How the logs arrive | For whom |
|---|---|---|
| **Port in clear** (`<port in clear>`) | UDP or TCP, not encrypted | Devices that do not support TLS; rsyslog and NXLog |
| **TLS port** (`<TLS port>`, row **Over TLS (encrypted)**) | TCP with TLS: the logs travel encrypted. The server proves its name with its certificate; the device does not present a certificate | Routers and firewalls that support syslog over TLS |
| **Port of the agents** (`<port of the agents>`) | TCP with TLS, and the agent presents a **client certificate** of its own | Only the Esapanel agent, which uses it by itself |

The port of the agents is not configured by hand: the agent receives it from the panel when it is installed. It only has to be **allowed outbound** in the firewall of the servers with the agent, before the installation: you find it in the **Reception of the logs** box and on the **Devices** page.

*Which port to use*

| Who sends | How | Port |
|---|---|---|
| Windows server | Esapanel agent (recommended) | Chosen by itself: port of the agents |
| Windows server | NXLog Community Edition, as an alternative | Port in clear, TCP |
| Linux server (Debian, Ubuntu, Red Hat, Rocky, AlmaLinux) | Esapanel agent (recommended) | Chosen by itself: port of the agents |
| Linux server | rsyslog, as an alternative | Port in clear, TCP |
| Router or firewall that supports syslog over TLS | Syslog settings of the device | TLS port, with the server name |
| Router or firewall without TLS | Syslog settings of the device | Port in clear, UDP or TCP |

| Who sends | How | Port |
|---|---|---|
| Switches, access points, NAS, other devices | Syslog settings of the device | TLS port if supported, otherwise port in clear |

*Security in short*

- **In clear:** the logs cross the Internet readable by anyone on the path. Fine for logs that are not sensitive, or when the device offers nothing else.
- **TLS:** the logs travel encrypted and the device checks that it is talking to the right server. The choice to prefer for NIS2, which asks to protect data in transit.
- **Client certificate (agent):** besides encryption, the panel knows for sure which agent is sending: only the agents of your subscription, each with its own certificate, get in on the port of the agents.

*TLS requirements*

- **Use the server name, not the IP address.** The certificate of the server carries its name: if the device connects to the IP address, the certificate check fails.
- **TCP** only: there is no TLS over UDP.
- The device must **trust the authority** that issued the certificate of the server and have the **right clock**, otherwise it rejects the certificate.
- The **Esapanel agent** uses TLS by itself when the certificate of the panel is valid (not self-signed); there is nothing to configure.

*Ports 514 and 6514 on a dedicated address*

Some devices cannot choose the port and send only to the standard port **514** (syslog) or **6514** (syslog over TLS). For them the subscription can receive on a **dedicated IP address**, assigned by the service provider.

With a dedicated address the **Devices** page shows:

- "The devices may send also to `<dedicated address>` on the standard port 514": the **Receive also on the port 514** button turns it on, **Stop the port 514** turns it off;
- the same for **6514**, with **Receive also on the port 6514** and **Stop the port 6514**.

They are extra ports: 514 brings the logs to the port in clear of the subscription, 6514 to the TLS port. The ports of the subscription stay open. Without a dedicated address, ports 514 and 6514 are not available.

With 6514 the device connects to the dedicated address, but the certificate carries the **server name**: the device must be able to check that name. If it cannot, use the server name with the TLS port of the subscription.

---

## 4. Adding a device

The panel accepts only the logs of the **devices** of the subscription. The logs of a sender that is not among the devices are not lost at once: they wait in the **Quarantine** (see chapter 8).

*Adding a device step by step*

On the **Devices** page, the **Add a device** button opens three steps:

1. **Category**: "What do you want to add?" Server; Router and firewall; Switch and access point; Storage (NAS); Other device.
2. **Model**: the models of the category (the list is in chapter 7). If yours is not there, choose **Other**.
3. **Name and instructions**: the **Name of the device**, the one you know it by (for example "Firewall of the office"), and how the panel recognizes it.

For Windows servers and for Linux servers with the agent the third step is different: see chapters 5 and 6.

For the other devices the third step asks:

| Field | What to enter |
|---|---|
| **Name of the device** | A name for you |
| **Recognized by** | How the panel recognizes the logs of the device (see below); the panel proposes the choice suited to the model |
| **Address or name** | The matching value |
| **Timezone** | The timezone of the clock of the device, for example `Europe/Rome` |
| **Alert if silent for** | An email if the device stops sending (see chapter 8) |

Then **Add and show the instructions**: the device is registered and its page shows the instructions of the model, already filled in with the values of the subscription.

*How a device is recognized*

| Recognized by | Example | When to use it |
|---|---|---|
| **IP address** | `203.0.113.10` or `2001:db8::10` | The **fixed** public address the device sends from. The normal choice for routers and firewalls |
| **Network** | `203.0.113.0/28` | Several fixed addresses of the same network |
| **DNS name** | `office.example.com` | An address that changes, with a DNS name (dynamic too) that follows it: the panel resolves it again from time to time |
| **Device name** | `FW-OFFICE` | The name the device writes in every log (the HOSTNAME field of syslog). It is accepted from any address, but only on the ports of your subscription: useful for a line that changes address, such as a backup line |
| **Esapanel agent** | | Enrolls by itself: nothing to enter |

Good to know:

- The address is the one **the panel sees**, that is the public address of the Internet connection the device goes out from. Several devices behind the same connection (for example a switch and a NAS in the office) go out with the same address: a device recognized by that address accepts the logs of all of them. To tell them apart, recognize each one by its **Device name**.

- The **Device name** is the least strict way: whoever knows the name and the port could send logs in its name. Prefer the IP address when it is fixed, or the agent on servers.
- For a Linux server with rsyslog the name in the logs is the one given by the `hostname` command on the server.

If the **Devices** page says "This subscription accepts logs from any source", your plan does not check the senders: all the logs arrive, even with no devices in the list.

### *The limit of devices*

The plan sets how many devices the subscription can have: the **Devices** page shows the count, for example "3 of 10 sources". Every device counts one, an agent too.

When the limit is reached, **Add a device** disappears and the page says "The plan allows N sources: remove one, or ask for a larger plan". To free a place, **Remove** a device no longer used: its next logs will go to the Quarantine.

### *Changing a device*

In the list, the **Instructions** link (or the name of the device) opens its page: there you can change the **Name of the device** and the **Model** and read the instructions again. In the list you can change **Timezone** and **Alert if silent for**, with **Save**.

---

## 5. Windows servers

### *With the Esapanel agent (recommended)*

The agent is a Windows service that reads the event log and sends the events to the panel. It enrolls in the subscription by itself: there are no addresses to authorize, even if the server changes address or sits behind a NAT.

**What it sends:**

- the whole **Security** log (sign ins, failed sign ins, locked accounts, users and groups changed);
- the warnings and errors of **System** and **Application**.

It starts from the new events: the history already in the event log is not sent. If the panel does not answer, the events wait in a queue on the disk of the server and leave when it is back; after a restart of the server the agent goes on from where it stopped.

**Installation:**

1. On the **Devices** page: **Add a device**, category **Server**, model **Windows Server**.
2. Write the **Name of the device** (for example "Mail server") and press **Show the commands**.
3. The panel shows the PowerShell commands, with the enrollment code and the name already in them. **Copy the commands**.
4. On the server, open **PowerShell as administrator** and run the commands. They download the agent from the panel into `C:\Program Files\Esapanel`, install it as a Windows service and enroll it in the subscription.
5. The panel page stays on "Waiting for the agent to enroll" and updates by itself. When the agent has enrolled it shows "The agent has enrolled." with the **Open the device** link.

The device appears in the **Devices** list with the chosen name, recognized by **Esapanel agent**.

The server must be able to reach, outbound:

- the address of the panel written in the command (after `--panel`), in HTTPS: it uses it to enroll and, at start and every 6 hours, to ask for its configuration;
- the server of the subscription on the port of the agents (or, without a certificate, on the TLS port or the port in clear), in TCP.

**The certificate of the agent.** At installation the agent creates a key of its own, which never leaves the server, and gets from the panel a client certificate valid for **one year**. It renews it by itself a month before it expires. The device page shows "The agent sends over TLS with its client certificate, valid until ...".

### Useful commands

In PowerShell as administrator:

| Command | What it does |
|---|---|
| `& "C:\Program Files\Esapanel\esapanel-agent.exe" status` | Shows the name of the agent, where it sends (server, port, TLS, end of the certificate), what it reads and how much data waits in the queue |
| `& "C:\Program Files\Esapanel\esapanel-agent.exe" uninstall` | Stops and removes the service; the data of the agent stay |
| `& "C:\Program Files\Esapanel\esapanel-agent.exe" uninstall --purge` | Removes the service and deletes the data of the agent too (configuration, enrollment, key, queue) |

The data of the agent (configuration, certificate, queue, its log `agent.log`) are in `C:\ProgramData\Esapanel\Agent`, readable only by administrators.

Uninstalling the agent does not remove the device from the panel: remove it with **Remove** on the **Devices** page, so it frees its place in the limit of the plan.

### Updating the agent

Open the page of the device in the panel (**Instructions** link in the list): for an agent already enrolled it shows the commands that **update** the agent and keep its enrollment, so no new device is created. Run them in PowerShell as administrator.

A server **reinstalled from scratch** has lost its enrollment: add it again as a new device and remove the old one.

#### *With NXLog (alternative)*

If you do not want to install the agent, the section **Instead of the agent: NXLog Community Edition** on the same page shows an alternative with a free third-party product:

1. Install **NXLog Community Edition** from nxlog.co (the site asks for a free registration before the download).
2. Run in PowerShell as administrator the commands the page shows: they keep a copy of the previous configuration, download the one of the panel and restart NXLog.

NXLog sends the same events as the agent (all of Security, warnings and errors of System and Application) to the **port in clear**, in TCP, with syslog RFC 5424.

With NXLog the device **does not register by itself**: the first logs arrive in the **Quarantine**. From there authorize the address of the server (**Authorize the address**) or its name (**Authorize the device name**); see chapter 8. Then, on the page of the device, choose the model **Windows Server**.

---

## 6. Linux servers

For servers of the **Debian** family (Debian, Ubuntu) and of the **Red Hat** family (Red Hat, Rocky, AlmaLinux) the panel offers two ways: the Esapanel agent, recommended, and rsyslog.

### *With the Esapanel agent (recommended)*

The agent is a systemd service that reads the **journal** of the server.

**What it sends:**

- all the messages of the journal with severity **warning or worse** (warning, error, critical, ...);
- **all** the sign-in messages (facilities auth and authpriv: sshd, sudo, su, login), at any severity. For SSH sign ins it reports user and address, successful and failed.

As on Windows: it enrolls by itself, no address to authorize, queue on disk if the panel does not answer, nothing lost after a restart; it starts from the new messages.

**Installation:**

1. On the **Devices** page: **Add a device**, category **Server**, model **Linux Debian / Ubuntu** or **Linux Red Hat / Rocky / AlmaLinux**.
2. The page proposes **With the agent of Esapanel (recommended)**. Write the **Name of the device** and press **Show the commands**.
3. **Copy the commands** and run them on the server **as root** (or with sudo). They download the agent for the architecture of the server (amd64 or arm64) into `/usr/local/bin/esapanel-agent`, install it as the systemd service `esapanel-agent` and enroll it in the subscription. `curl` is needed.
4. The page goes from "Waiting for the agent to enroll" to "The agent has enrolled." with the **Open the device** link.

The panel recognizes by itself whether the server belongs to the Debian or the Red Hat family. Outbound connections and the certificate work as for Windows (see chapter 5).

**Useful commands** (as root):

| Command | What it does |
|---|---|
| `esapanel-agent status` | Name, where it sends (server, port, TLS, end of the certificate), queue |
| `esapanel-agent uninstall` | Stops and removes the service; the data stay |
| `esapanel-agent uninstall --purge` | Removes the service and deletes the data of the agent too |
| `systemctl status esapanel-agent` | The state of the service |

The data of the agent are in `/var/lib/esapanel-agent`, with its log `agent.log`.

**Updating:** the page of the device of an agent already enrolled shows the commands that update it and keep its enrollment. A server reinstalled from scratch is added again as a new device, removing the old one.

### *With rsyslog (alternative)*

rsyslog is the syslog service already present in many distributions. It does not require installing the agent.

1. When adding the server choose **Use rsyslog instead**.
2. Fill in the fields (see chapter 4): usually **Recognized by** = **Device name**, with the name given by the `hostname` command on the server; or **IP address**, if the server goes out with a fixed address.
3. **Add and show the instructions**. The page of the device shows the commands to run as root:
    - they install rsyslog, if missing (Debian 12 and later no longer install it);
    - they download from the panel the file `/etc/rsyslog.d/90-esapanel.conf` (with **Show the file** you can read it first);

- on Red Hat, Rocky and AlmaLinux they add the port of the subscription to the ports SELinux allows to rsyslog (where SELinux is off the command gives an error that can be ignored);
- they restart rsyslog and send a test log ("Esapanel test").

The configuration file sends **all the logs** of the server to the **port in clear**, in **TCP**, with syslog RFC 5424, and keeps a queue on disk: if the panel does not answer, the logs wait on the server.

The commands download the file from a link of the subscription. The link holds only name, address and port, no secret. **New code for the links** (at the bottom of the Devices page) stops the commands copied before; the configuration already on the servers keeps working.

*Other servers*

For a server that is neither Windows nor of the Debian or Red Hat family, choose the model **Other** of the **Server** category and use the general settings of chapter 7.

---

## 7. Routers, firewalls and other devices

Routers, firewalls, switches, access points and NAS send their logs with their own syslog settings, from the web interface or the command line. First add the device in the panel (see chapter 4), usually recognized by the public **IP address** it sends from; then configure it.

*General settings*

| Setting of the device | Value |
|---|---|
| Syslog server | `<server>`, or the **Address** if the device wants an IP address |
| Port | `<port in clear>` (or 514 on the dedicated address, if on) |
| Protocol | UDP or TCP |
| Format | syslog RFC 5424 or RFC 3164 (the "classic" one): both are fine |
| Level of the messages | At least informational, warnings and errors; for firewalls and VPNs also traffic and sign-in events, if you need them |

With TLS, if the device supports it:

| Setting of the device | Value |
|---|---|
| Syslog server | `<server name>` of the **Over TLS (encrypted)** row: the name, never the IP address |
| Port | `<TLS port>` (or 6514 on the dedicated address, if on) |
| Protocol | TCP with TLS |
| Client certificate | None: the device does not have to present one |

**UDP or TCP?** For devices UDP is enough. TCP keeps the logs in order and does not lose them on a busy line; with UDP the logs sent while the reception is stopped (for example during a restart of the server) are lost.

**The time of the logs.** Every log has the time the panel receives it, always right, used to search and sort the logs. It also has the time written by the device:

- with **RFC 5424** the device states its timezone, and the time stays as it is;
- with **RFC 3164** the device writes the time of its clock **without a timezone**. Set the **Timezone** of the device in the panel (for example `Europe/Rome`, which includes daylight saving time): the panel turns that time into the right instant. "Time as it arrives" leaves it as it is.

The timezone is set when the device is added (the panel proposes yours) and changed in the **Devices** list; a change applies to the following logs. In any case keep the clock of the device in sync (NTP).

*Models with their own instructions*

For these models the page of the device shows where the settings are in the menus, or the commands to copy, already filled in with the values of the subscription:

| Category | Models |
|---|---|
| Router and firewall | DrayTek Vigor; Zyxel ZyWALL / USG FLEX; Fortinet FortiGate; Cisco ASA; Check Point; MikroTik; pfSense / OPNsense; Sophos Firewall; SonicWall; WatchGuard Firebox |
| Switch and access point | Cisco IOS (Catalyst); HPE Aruba; Ubiquiti UniFi; MikroTik |
| Storage (NAS) | Synology DSM; QNAP QTS |

Some notes from the instructions:

- **pfSense and OPNsense:** step-by-step guide in Sending logs from pfSense and OPNsense.
- **MikroTik:** step-by-step guide in Sending logs from MikroTik. The firewall rules need a log prefix with the action (for example `DROP-WAN`): the RouterOS line does not say whether the packet passed.
- **DrayTek Vigor:** System Maintenance › SysLog / Mail Alert Setup: enable SysLog, enter server and port, choose the kinds of messages to send.
- **Zyxel:** if the model cannot change the port, the dedicated address with port 514 is needed.
- **Cisco ASA:** use **UDP**: with TCP, if the server does not answer, the ASA can stop passing traffic.
- **Synology** and **QNAP:** choose the RFC 5424 format (on Synology "IETF").

Menus change with the firmware version: if the path given does not match, look for the "syslog" or "remote log" settings of the device and use the values of the general settings.

For a model not in the list choose **Other**: the page shows the general values. The same goes for the devices of the **Other device** category (for example a printer or a UPS that sends syslog).

---

## 8. Checking that the logs arrive

*The page of the device*

After adding it, the page of the device shows:

- **Recognized by**: how the panel recognizes it;
- **Last log**: "Last log from `<address>`, `<when>`", or "No log yet";
- until something arrives, "Waiting for the first log of the device: this page updates by itself".

To try, create an event on the device: for example a sign in to its administration interface. The rsyslog commands send a test log by themselves.

For an agent the **Devices** list also shows "Agent `<version>`, last heartbeat `<when>`": the agent sends a heartbeat every 5 minutes, even when the server has no events. Just enrolled it shows "Enrolled: waiting for the first heartbeat of the agent".

The logs received are in the **Logs** tile of the subscription.

### *The Quarantine*

The logs that reach the ports of your subscription from a sender that **is not among the devices** go to the **Quarantine** (**Quarantine** tile). They stay a few days (the page says how many), then they are deleted. They are grouped by **Address** and **Device name**, with the number of logs and the period.

For each sender:

| Button | What it does |
|---|---|
| **Authorize the address** | The sender becomes a device recognized by its address; its logs in quarantine move into the subscription |
| **Authorize the device name** | The same, recognized by the name it writes in the logs, from any address |
| **Discard** | Deletes its logs in quarantine; the next ones go back to the quarantine |
| **Ignore the address** / **Ignore the name** | Its logs in quarantine are deleted and the next ones dropped on arrival, only counted. It does not count among the devices. **Stop ignoring**, in the **Ignored senders** list, undoes it |

An authorized sender counts among the devices of the plan: if the limit is reached, the page asks to remove one from the Devices page. After authorizing it, choose its **Model** on the page of the device.

Ignore only senders you know and do not want, such as a test device: their logs are not kept anywhere.

The Quarantine is the first place to look when a configured device does not show up: often its logs arrive, but from an address different from the one entered.

### *Alert if a device is silent*

The **Alert if silent for** column of the **Devices** list (Never, 15 minutes, 1 hour, 6 hours, 24 hours) sends an **email** when a device has sent no logs for longer than that, for example a firewall switched off or an office without connection, and another when it starts again. In the list the device shows "Silent since …".

- Choose it for the devices that send all the time: many send only when something happens.
- For **agents** it is always useful: the heartbeat every 5 minutes counts as activity, so a quiet server does not look switched off.
- If logs arrived in the Quarantine meanwhile, the email names their senders: often the device has a new address.

---

## 9. Common problems

### *Nothing arrives*

1. **The Quarantine.** If the logs are there, the device sends but is not recognized: authorize it, or correct the address or the name in the **Devices** list. Remember that what counts is the **public** address the device goes out to the Internet with, not the one of the internal network.

2. **Port and protocol.** Check that port and protocol are those of the **Devices** page: the port in clear accepts UDP and TCP; the TLS port only TCP with TLS. A device configured in clear on the TLS port, or with TLS on the port in clear, delivers nothing.
3. **The outbound firewall.** Your firewall must let traffic out towards the panel server on the port used (UDP and/or TCP). For the agent: the address of the panel in the command, in HTTPS, and the **Port of the agents** of the Devices page.
4. **Ports 514 and 6514** work only on the dedicated address and only if turned on on the **Devices** page.
5. **An ignored sender.** Check the **Ignored senders** list in the Quarantine.
6. **An agent.** Run the `status` command and look at the log of the agent (`agent.log` in the data folder): if data wait in the queue, the agent does not reach the server.

*The time of the logs is wrong*

- If the device sends RFC 3164, set its **Timezone** in the **Devices** list and save: it applies to the following logs.
- Check that the clock of the device is right (NTP).
- The time of reception of the panel is always right: searching and sorting the logs use it.

*The enrollment of the agent is refused*

The agent writes "the panel refused the enrollment", followed by the reason.

| Reason | What to do |
|---|---|
| The enrollment code is not valid, or the subscription is not active | Someone gave a **New code** (section **Codes of the agents and of the links**, at the bottom of the Devices page): the commands copied before no longer enroll agents. Copy the commands from the page again. If the subscription is suspended, contact your service provider |
| The subscription already has the maximum number of devices | Remove a device no longer used, or ask for a larger plan |
| Too many requests | Wait a minute and try again |

The enrollment code lets anyone add devices to the subscription: give it only to whoever installs the agent. If it ended up where it should not, give a **New code**: the agents already enrolled keep working.

*The agent sends without a client certificate*

If the page of the device says "The agent sends without a client certificate", the agent was installed before the certificates existed, or the panel could not sign it yet. The agent asks for the certificate by itself at start; if the message stays, reinstall it as a new device:

1. uninstall the agent with `uninstall --purge`;
2. remove the old device with **Remove** (so it does not count in the limit);
3. add the server as a new device and run the commands of the page.

*TLS errors*

- **The name:** the device must connect to the **server name** of the **Over TLS (encrypted)** row, not to the IP address, otherwise the certificate check fails.
- **The authority:** if the device rejects the certificate of the server, it probably does not know the authority that issued it. On some devices the list of authorities is updated with the firmware or imported by hand: ask your service provider which authority the certificate uses.
- **The clock:** a wrong clock makes the certificate look expired or not yet valid.
- **The protocol:** TLS only over TCP.
- If the device cannot use TLS, send to the port in clear.

# Sending logs from MikroTik

This guide completes Sending logs to the panel for **MikroTik** routers and switches with **RouterOS 7**. The values to enter (address and port) are on the page of the device in the panel, already filled in: below they are written as `<Address>` and `<port in clear>`.

## 1. What the panel receives

With the model **MikroTik** the panel reads the logs and shows them in the **Events** section of the **Analysis** page and in the reports:

| In the Events section | Where it comes from |
|---|---|
| **Sign ins** succeeded and failed | The sign ins of every service (Winbox, SSH, web interface, API), with user and address |
| **Administration** | The changes to the configuration, with who made them, from where and the command |
| **Firewall** blocked and **Traffic** allowed | The firewall rules with logging on, with addresses, ports and interface (see chapter 4) |

All the other logs can still be searched in the **Logs** tile.

The MikroTik sends in **UDP** to the **port in clear**.

---

## 2. Adding the MikroTik in the panel

1. On the **Devices** page, **Add a device**.
2. Category **Router and firewall** (or **Switch and access point** for a MikroTik switch), model **MikroTik**.
3. **Name of the device**: a name for you, for example "Office router".
4. **Recognized by**: **IP address**, with the fixed public address the MikroTik goes out to the Internet from. If the address changes, see chapter 6.
5. **Add and show the instructions**.

The page of the device shows the commands below already filled in with your **Address** and your port, with the button to copy them.

---

## 3. Sending the logs

Open the terminal of the MikroTik: in Winbox **New Terminal**, or over SSH. Paste the commands of the page of the device; they look like this:

```
/system logging action add name=esapanel target=remote remote=<Address> remote-port=<port in clear>
remote-log-format=syslog
/system logging add topics=info action=esapanel
/system logging add topics=warning action=esapanel
/system logging add topics=error action=esapanel
/system logging add topics=critical action=esapanel
```

- The first command creates the destination: the server with its **Address** (RouterOS takes only an IP address here, not a name) and the port of the subscription, in syslog format with date and timezone.

- The others send to that destination the informational messages, warnings, errors and critical ones: they include sign ins, changes and the firewall logs.

If RouterOS answers that `remote-log-format` does not exist, your version does not have this option: run the first command again without `remote-log-format=syslog`. The panel reads the default format too.

The same settings are in Winbox under **System › Logging**: **Actions** tab for the destination, **Rules** tab for the topics.

---

## 4. Firewall rules

RouterOS logs a firewall rule only if logging is on for it, and the log line **does not say whether the packet was accepted or dropped**. So:

1. In **IP › Firewall › Filter Rules** open the rule you want to see.
2. **Action** tab: tick **Log** and write a **Log Prefix** that contains the action, for example `DROP-WAN` for a rule that drops, `ACCEPT-VPN` for one that accepts. The panel understands the outcome from these words: **drop**, **reject**, **block**, **deny** (blocked) and **accept**, **allow**, **pass** (allowed), upper or lower case.
3. **General** tab: for a rule that accepts, set **Connection State** to **new**, so only the start of each connection is logged. Without it, every packet becomes a line and the logs grow very fast.
4. **OK**.

A rule with logging but without one of those words in its prefix shows up among the **Firewall** logs, without an outcome.

Turn logging on only for the rules that count: usually those that drop traffic from the Internet and those that let services or VPNs in.

---

## 5. Checking that the logs arrive

1. Create an event: for example a sign in to Winbox or over SSH with a wrong password, then the right one.
2. On the page of the device, **Last log** shows the time of the log just arrived.
3. In the **Logs** tile search the logs of the device: the failed sign in is there.
4. After a few minutes the **Analysis** page shows the failed sign in in the **Events** section, among the failed **Sign ins**.

---

## 6. Common problems

*Nothing arrives*

- Check the **Quarantine**: if the logs arrive from an address different from the one entered (for example a router with two Internet connections), they are there. **Authorize the address** lets them in.
- Check in **System › Logging › Actions** that the `esapanel` destination has the **Address** and the **port in clear** of your subscription.
- The firewall rules in the **output** chain of the MikroTik, or a firewall upstream, must let UDP pass towards `<Address>` on `<port in clear>`.

*The MikroTik has an address that changes*

Recognize the MikroTik by its **Device name** instead of its address. In syslog format the name in the logs is the **identity** of the MikroTik (**System › Identity**), `MikroTik` from the factory: give each device an identity of its own before using it in the panel. In the default format there is no name: then the IP address or a **DNS name** is needed.

*Too many logs*

- Check that the rules that accept have **Connection State new**.
- Remove logging from the rules that see a lot of traffic and that you do not need.

# Sending logs from pfSense and OPNsense

This guide completes Sending logs to the panel for **pfSense** and **OPNsense** firewalls. The values to enter (address and port) are on the page of the device in the panel, already filled in: below they are written as `<Address>` and `<port in clear>`.

## 1. What the panel receives

The firewall sends all its logs. With the model **pfSense / OPNsense** the panel reads them and shows them in the **Events** section of the **Analysis** page and in the reports:

| In the Events section | Where it comes from |
|---|---|
| **Firewall** blocked | The connections blocked by the rules, with source address, destination, port and interface |
| **Traffic** allowed | The connections passed by the rules you turned logging on for |
| **Sign ins** succeeded and failed | The sign ins to the web interface and over SSH, with user and address |
| **Administration** | The changes to the configuration, with who made them and from where |
| **Attacks detected** | The addresses reported and blocked by the protection against repeated sign-in attempts |
| **VPN** | The IPsec tunnels established and those that failed |

All the other logs (services, DHCP, system) can still be searched in the **Logs** tile.

The firewall sends in **UDP** to the **port in clear**: pfSense offers nothing else for remote logging.

---

## 2. Adding the firewall in the panel

1. On the **Devices** page, **Add a device**.
2. Category **Router and firewall**, model **pfSense / OPNsense**.
3. **Name of the device**: a name for you, for example "Office firewall".
4. **Recognized by**: **IP address**, with the fixed public address the firewall goes out to the Internet from. If the address changes, see chapter 6.
5. **Add and show the instructions**.

The page of the device shows the steps below already filled in with your **Address** and your port.

---

## 3. pfSense

The settings are in **Status › System Logs › Settings**.

*Use the address, not the name*

In the remote server field write the **Address** (the IP address of the server, on the page of the device), not the server name: so the sending does not depend on the DNS of the firewall.

*The steps*

1. **General Logging Options › Log Message Format:** choose **syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps)**. With this format every log carries its timezone.
2. Keep **Log packets matched from the default block rules in the ruleset** ticked: these are the blocked connections.
3. **Remote Logging Options:**
    - tick **Enable Remote Logging**;
    - **Source Address:** Default (any);
    - **IP Protocol:** IPv4;
    - **Remote log servers:** `<Address>:<port in clear>`, for example `203.0.113.5:18670`.
4. **Remote Syslog Contents:** tick **Everything**.
5. **Save**.

*Allowed connections (optional)*

To see the allowed traffic in the panel too, turn logging on in the rules that matter: **Firewall › Rules**, edit the rule, **Extra Options**, tick **Log packets that are handled by this rule**, **Save** and **Apply Changes**.

Do it only on the rules that count (for example access from outside to a server, or the VPNs): a rule that passes all the web browsing of the office produces a great many logs.

*IPsec tunnels*

With IPsec tunnels, pfSense writes many service messages (key renewals, checks that the tunnel is alive): they can be most of the logs. If they fill the logs, lower their levels in **VPN › IPsec › Advanced Settings › IPsec Logging Controls**. The tunnels established and those that failed stay visible.

---

## 4. OPNsense

The settings are in **System › Settings › Logging**, **Remote** tab.

1. The **+** button adds a destination.
2. Fill in:

| Field | Value |
|---|---|
| **Enabled** | Ticked |
| **Transport** | UDP(4) |
| **Applications** | Empty: all |
| **Levels** | All except **debug** |
| **Facilities** | Empty: all |
| **Hostname** | `<Address>` |
| **Port** | `<port in clear>` |
| **RFC5424** | Ticked |
| **Description** | Esapanel |

3. **Save**, then **Apply**.

Choose the levels: if the **Levels** field stays empty, OPNsense also sends the debug messages, many and of no use for monitoring.

For blocked and allowed connections, tick **Log** in the rules that matter (**Firewall › Rules**), with the same criterion as pfSense: only the rules that count.

## 5. Checking that the logs arrive

1. Create an event: for example a sign in to the web interface of the firewall with a wrong password, then the right one.
2. On the page of the device, **Last log** shows the time of the log just arrived.
3. In the **Logs** tile search the logs of the device: the failed sign in is there.
4. After a few minutes the **Analysis** page shows the failed sign in in the **Events** section, among the failed **Sign ins**.

## 6. Common problems

*Nothing arrives*

- Check the **Quarantine**: if the logs arrive from an address different from the one entered (for example a firewall with two Internet connections), they are there. **Authorize the address** lets them in.
- Check that you wrote the **Address** and the **port in clear** of your subscription, not port 514.
- A firewall upstream, or the outbound rules of the firewall itself, must let UDP pass towards `<Address>` on `<port in clear>`.

*The firewall has an address that changes*

Recognize the firewall by its **Device name** instead of its address. The name is the one the firewall writes in the logs: on pfSense and OPNsense it is the hostname and domain set in **System › General Setup** (pfSense) or **System › Settings › General** (OPNsense), for example `pfSense.home.arpa`. Give each firewall a name of its own, different from the factory one, before using it in the panel.

*Too many logs*

- Remove logging from the rules that pass a lot of traffic.
- On pfSense lower the IPsec levels (see IPsec tunnels); on OPNsense leave out the debug level.
- Devices of the local network that announce themselves (for example on port 5353, mDNS) can make most of the blocked connections: if you do not need them, do not log the rules that block them.

# Devices and quarantine

In CSP (Central Syslog) a **device** is a server or a network device that sends its logs to the subscription. Only the logs of the devices enter the subscription; those of an unknown sender wait in the **Quarantine**.

How to add a device and configure it is explained in Sending logs to the panel. This page explains how to keep the devices in order over time: the list, the page of each one, the quarantine and the codes.

## The list of devices

The **Devices** tile of the subscription shows at the top the **Sending the logs** box, with the server and the ports, and below it the list of devices. The count at the top, for example "3 of 10 devices", says how many devices the plan allows.

For each device the list shows:

- the name you gave it and the **Model**;
- **Recognized by**: the IP address, the network, the DNS name, the device name or the **Esapanel agent**. For a DNS name the list also says what it resolves to now;
- **Last log**: "Last log from `<address>`, `<when>`", or "No log yet". For an agent, "Agent `<version>`, last heartbeat `<when>`";
- **Time zone** and **Alert if silent for**, which you change right in the row with **Save**.

**Remove** takes a device away: its next logs will go to the quarantine, and its place in the limit of the plan becomes free. The logs it already sent stay.

### *Alert if silent for*

**Alert if silent for** (Never, 15 minutes, 1 hour, 6 hours, 24 hours) sends an email when the device has not sent logs for longer than that time, and another when it starts again. A silent device shows "Silent since ...".

Choose it for the devices that send all the time, such as a firewall or a server with the agent: many devices send only when something happens, and would give false alarms. The time when the server of the panel itself was not receiving does not count.

### *The time zone*

Many devices write in their logs the time of their clock without the time zone (syslog RFC 3164). The **Time zone** of the device, for example `Europe/Rome`, lets the panel turn that time into the right moment, daylight saving included. **Time as it arrives** leaves it as it is. A change applies to the next logs.

## The page of a device

The name of a device in the list opens its page, with the instructions to configure it already filled in. Here you can:

- change the **Name of the device** and the **Model**: the instructions follow the model;
- choose the **Profile of the logs** (see below);
- see when the last log arrived. Until the first arrives, the page says so and refreshes by itself.

A device authorized from the quarantine has no model yet: choose it here to see the instructions.

### *The profile of the logs*

The **Profile of the logs** is how the panel reads the logs of the device to recognize the events: sign ins, configuration changes, blocked traffic, VPN. These events feed the **Events** section of the **Analysis**, part of the reports and the event alerts.

- **Automatic**, the normal choice, uses the profile of the model, or recognizes it from the logs.
- **Generic text (by words)** is for a device that no profile reads: it looks for words such as "login failed" or "denied". Its events do not start alerts.
- **None** reads nothing.

There are profiles for Linux, Windows, DrayTek Vigor, pfSense / OPNsense, MikroTik, Fortinet, Sophos, SonicWall, Zyxel, WatchGuard, Check Point, Cisco ASA and IOS, Aruba switches, UniFi gateways, Synology and QNAP, and generic profiles for the devices that send CEF / LEEF, key=value or iptables.

*Recognize it as ...*

Some devices, such as the DrayTek Vigor, do not write their name where the panel expects it, and show up with the reverse name of their address. In this case the page proposes **Recognize it as** followed by the name the device really writes: from then on the device is accepted with that name from any address, even when a backup line changes the address.

*An agent*

For an agent the page says until when its client certificate is valid: the agent renews it by itself a month before it expires. For an agent already enrolled the page shows the commands that update it without making a new device.

## The quarantine

The **Quarantine** tile collects the logs that reached the ports of the subscription from senders that are not among the devices. The number on the tile says how many senders are waiting. The logs stay a few days, then they are deleted; beyond a daily limit the quarantine only counts them, without keeping them.

The senders are grouped by **Address** and **Device name**, with the number of logs and the period. For each one:

| Button | What it does |
|---|---|
| **Authorize the address** | The sender becomes a device recognized by its address, and its logs in quarantine move into the subscription |
| **Authorize the device name** | The same, recognized by the name it writes in the logs, from any address |
| **Discard** | Deletes its logs in quarantine; the next ones come back here |
| **Ignore the address** / **Ignore the name** | Its logs are discarded on arrival and only counted, and those in quarantine are deleted |

Before authorizing you can choose the **Profile** of the sender: **Recognize by itself** is usually enough. The profile also says where the sender writes its name. If it does not write a name of its own, the panel lets you authorize only the address.

An authorized sender counts among the devices of the plan. If the sender was already a device, for example added meanwhile from the **Devices** page, authorizing only moves the logs left in quarantine.

*Ignored senders*

The **Ignored senders** list shows the ignored senders and how many logs they have sent since. **Stop ignoring** brings their next logs back to the quarantine.

Ignore only senders you know and do not want, such as a test device: their logs are lost. There is no need to ignore the scanners of the Internet, which the firewall of the server blocks anyway.

*When to look at the quarantine*

- A device just configured does not show up: its logs are almost always in the quarantine, with an address different from the one you entered. Authorize it from here, or correct the address in the **Devices** list and remove the wrong one.
- The email of a silent device mentions logs in quarantine: the device has probably changed address.

## The codes of the agents and of the links

At the bottom of the **Devices** page, **Codes of the agents and of the links** holds the two codes that the instructions of the servers use:

- the **code of the agents** enrolls agents in the subscription: whoever has it can add a device, within the limit of the plan. Give it only to whoever installs the agent;
- the **code of the links** is in the links that download the configuration of rsyslog. These links hold no secret, only the name, the address and the port.

Give a **New code** (for the links, **New code for the links**) when a code ended up where it should not. The agents already enrolled and the servers already configured keep working; only the commands copied before stop working.

## Ports 514 and 6514

When the subscription receives on a dedicated IP address, on the **Devices** page you can also turn on the standard port **514** (syslog) and **6514** (syslog over TLS), for the devices that do not let you choose the port. The details are in Sending logs to the panel.

# Searching and reading the logs

The **Logs** tile of a CSP (Central Syslog) subscription shows the logs received, the most recent first, and lets you search and download them. Without filters the page shows the last 24 hours.

## Searching

The filters are at the top of the page:

| Filter | What it does |
|---|---|
| **From** and **To** | The period |
| **Device** | The name or the address of the device |
| **Category** | **Errors**, **Warnings**, **Information**, or **All** |
| **Facility** | The syslog facility, for example auth for the sign ins |
| **Text** | A word or a phrase of the message |

**Search** applies the filters, **Last 24 hours** removes them. **Newer** and **Older** move through the results.

For each log the page shows **Received** (the time the panel received it, in your time zone), the **Device**, the **Severity** and the **Message**. The **Device** column shows first the name the device writes in its logs, then the name you gave it and its address.

The time of reception is the one the logs are searched and sorted by: it is always right, even if the clock of a device is wrong.

## The fields of the event

The Esapanel agents, and the devices that send syslog RFC 5424 with structured data, give each log fields of its own: for example **User**, **Source address**, **Event** (on Windows, 4625 is a failed sign in) and **Outcome**.

- **Details**, under a log, shows its fields.
- A click on a user or an address (**Show only the logs with this value**) shows only the logs with that value.
- In **Fields of the event** you can search by exact value: all the failed sign ins of a user, or everything a source address did. The user is compared without telling upper and lower case apart.

*Example: who tried to get into a Windows server*

1. Filter the **Device** with the name of the server.
2. In **Fields of the event**, write `4625` in **Event**.
3. The result is the failed sign ins. Open **Details** on one of them and click the **Source address** to see everything that address did.

## Interruptions of the reception

A yellow row marks an interruption of the reception of the server of the panel, for example during a restart: the logs your devices sent over UDP in that interval did not arrive. The logs sent over TCP, or by the agent, are usually sent again by the device.

## The names of the addresses

If your plan includes it, the panel looks up in the DNS the names of the public addresses that appear in the logs, for example those of an attacker in the logs of a firewall, and shows them in brackets

after the address. The most recent logs may not have their names yet. The option is off unless asked for, because whoever runs the DNS of an address can see that it was looked up.

## Downloading

**Download** saves the logs found with the current filters, as **CSV** for a spreadsheet or as syslog **text**. A download holds at most a fixed number of logs: for a long period, download in parts, for example one month at a time. The downloads hold the logs as they arrived, without the names of the addresses.

To download you need a role that allows it (**CSP · Export logs**).

## Where the older logs are

The plan sets how long the logs stay searchable on this page. The older logs are not lost: every night they move to the **Log archive** tile, where you download them (see Log archives and backups).

## Alert me if it repeats

On a log, **Alert me if it repeats** opens the form of a new alert rule already filled in with the text of that log: it is the quickest way to be told when a message shows up again (see Event alerts).

# Event alerts

Keeping the logs is not enough: you have to notice when something happens. The **event alerts** of CSP (Central Syslog) read the new logs of the subscription every 3 minutes and write to you when there is something worth a look: attempts to guess a password, a sign in to the administration of a firewall at night, a configuration changed, an attack above the norm. You do not have to write rules: the predefined ones are already on.

It also helps with the NIS2 directive, which asks you to **detect** incidents, not only to keep the logs.

The **Event alerts** tile is there if the plan of the subscription includes the service. To see the page it is enough to be able to see the logs; to change rules and exceptions you need a role that lets you manage the devices.

## Episodes

The events of the same rule about the same thing (an address, a user, a device, an hour) that follow one another make up an **episode**. For example, 34 failed sign ins in 10 minutes from the same address are one episode, not 34 alerts.

- You receive an email when the episode starts, and at most one an hour while it goes on.
- The episode ends when its events stop.
- **Episodes of the last 30 days** lists them, with those **Going on** and a link to their logs.
- The episodes of the period also appear in the reports (see Reports and analysis).

Your provider decides who receives the emails, in the notifications (see Notifications).

## The rules

In **Rules** each rule is turned on or off (**On**). Those with a threshold have a **Sensitivity**: **Low** writes only for many events, **High** already for a few, **Medium** is the default. The numbers of each rule are in its description.

| Rule | When it writes |
|---|---|
| **Repeated failed sign ins** | Many failed sign ins in 10 minutes from the same address or for the same user: someone is trying to guess a password |
| **Sign in after many failed** | A successful sign in right after an episode of failed ones: the attempt may have worked |
| **Access to the administration of a device** | A sign in to a firewall or a router outside working hours (Monday to Friday, 8 to 19) or from an address not seen in the last 30 days. With **Every access**, every sign in |
| **Configuration changed** | A configuration of a device changed, with who and from where |
| **Firmware updated** | An update of the firmware of a network device |
| **Accounts created or changed** | A user created, deleted, locked or added to a group, a password changed |
| **Audit log cleared or audit policy changed** | On Windows, the security log cleared or the audit policy changed |

| Rule | When it writes |
|---|---|
| **Commands with sudo** | A command run with sudo on a Linux server. Usually normal: off by default |
| **Blocked attacks above the norm** | The events blocked by the firewall in an hour, many times more than the same hour in the 14 days before |
| **Attack from the internal network** | Many events blocked from a private address of your network: an infected computer or a compromised device |
| **VPN unstable** | A VPN failing many times in an hour. An email also when it is stable again |

Press **Save** after the changes.

*What they need to work*

The rules rely on the events that the **profiles** recognize in the logs of your devices (see Devices and quarantine).

- A device without a profile, or read by the generic profile by words, gives no alerts.
- Imported logs, or logs arrived more than 15 minutes late, give no alerts.

## Your rules

In **Your rules** you can add rules of your own, as many as the plan allows. Each rule has:

| Field | What to choose |
|---|---|
| **Name** | A name for you |
| **Device** | One device, or **All the devices** |
| **Condition** | **The text of the log contains**, **The kind of event is**, **The user is**, **The source address is** or **The destination port is** |
| **Words or value** | The text or the value to look for |
| **More than (times in 10 minutes)** | Empty: at the first event. With a number, the alert starts when the events go over that number in 10 minutes |

Then **Add the rule**.

The text is searched without upper and lower case, also as part of a word: "admin" finds "Administrator". A threshold counts the events of each device on its own. Unlike the predefined rules, yours also look at the logs that no profile reads.

The quickest way to make a rule is to start from a log: on the **Logs** page, **Alert me if it repeats** opens the form already filled in with the text of that log.

*Examples*

- An alert at every sign in of the user `admin` on a device: condition **The user is**, value `admin`, empty threshold.
- An alert when a NAS reports a failing disk: device the NAS, condition **The text of the log contains**, words as they appear in the log of your NAS.

## Exceptions

An **exception** is an address, a network or a user that the rules leave out, for one rule or for all. It is for the known false alarms: the vulnerability scanner of the office, the user that runs the backups and signs in at night.

From an episode, **Leave out this address** adds the exception for that rule in one click.

An exception hides from the rule the events of that address, network or user for good. The logs are still kept and can be searched. Use them with care: an exception that is too wide hides real attacks too.

# Reports and analysis

CSP (Central Syslog) sums up the logs of the subscription in two ways:

- the **Analysis** is a page always up to date, to see at a glance how the devices behave;
- the **Reports** are documents of a day, a week or a month, made when the period closes and never changed afterwards, to read, print or keep.

## The analysis

The **Analysis** tile counts the logs of the subscription by hour. In **Period** choose **Last 24 hours**, **Last 7 days**, **Last 30 days** or **Last 12 months**.

| Section | What it shows |
|---|---|
| **Logs by severity** | How many logs arrived in each hour, day or week, split into errors (error and worse), warnings and information. An interruption of the reception in the period is written under the chart |
| **Devices** | The devices that sent the most, with their **Errors** and the **Change** compared with the same period before. A click opens the logs of that device in the period |
| **Days and hours** | When the logs arrive, in your time zone |
| **Events** | The events recognized by the profiles of the devices (see below) |

The counts are updated every five minutes and stay for 25 months, even after the logs have been deleted.

### *What to look at*

- A device that suddenly sends **much more or much less** than usual deserves a look: an attack, a fault, a configuration changed.
- In **Days and hours** activity at night or at the weekend stands out.
- A device marked **new** had not sent anything in the period before.

### *The events*

The **profiles** of the devices read the logs and count the events by category: **Sign ins**, **Administration**, **Accounts**, **Firewall**, **VPN**, **Traffic** and others, with their outcome (successful and failed, allowed and blocked). Next to them, the values seen most often: **Addresses of the failed sign ins**, **Users of the failed sign ins**, **Addresses blocked by the firewall**, **Destination ports of the traffic**.

The events are counted with the hourly summaries, so the last minutes arrive a little later. A device without a profile gives no events: the profile is chosen on its page (see Devices and quarantine).

## The reports

The **Reports** tile is there if the plan of the subscription includes the service. It lists the reports made, with **Period**, **Kind** (**Daily**, **Weekly**, **Monthly**), **Coverage** and number of **Logs**.

### *Choosing which reports*

In **Your choices**:

- **A report every day**, **A report every week, on Monday**, **A report every month, on the first**: which periods you want;
- **Keep the reports for (months)**: from 25 months up, to the maximum of the plan. The older reports are deleted.

Then **Save**. A report is made when its period closes in your time zone, and when it is ready an email arrives (your provider decides who receives it, in the notifications).

*What a report holds*

| Section | Content |
|---|---|
| **Coverage of the monitoring** | For how much of the period the reception was active, its interruptions, and the devices that sent nothing |
| **Logs by severity** | The logs of the period by severity, compared with the period before |
| **Devices** | The devices and their logs, compared with the period before |
| **Errors and worse** | The most frequent messages of severity error or worse |
| **Events read by the profiles** | Sign ins, administration, firewall, VPN and traffic with their outcome, and the most frequent addresses, users and ports |
| **Event alerts** | The episodes of the period (see Event alerts) |
| **Senders not authorized** | What arrived in the quarantine |

*Reading, printing, keeping*

Open a report to read it. **Print or save as PDF** prints it or saves it as PDF from the browser.

A report, once made, never changes. At the bottom is the **SHA-256 fingerprint** of its data: a copy saved as PDF can be compared with the one in the panel, to show that it was not changed.

*Reports and NIS2*

The monthly reports are a good basis to document the monitoring: they say that the logs were collected, for how long the reception was active, which devices were silent and which events were detected. Save them as PDF with the rest of your security documentation.

# Importing logs from files

When you start using CSP (Central Syslog), the logs of past years are often on another server: the old syslog server, a NAS, a folder of files. **Import logs** brings them into the subscription: once imported they are searched, analysed and archived like those received by the panel.

The **Import logs** button is on the **Logs** page of the subscription. You need a role that allows importing, and the plan of the subscription must allow it.

## How it works

An import goes through four steps:

1. you send the files;
2. the panel reads them and shows the senders it found;
3. you choose the device of each sender and the clock of its times;
4. the panel writes the lines, in the queue.

The list of imports shows for each one **When**, the **Files**, the **Lines**, the **Period** and the **Status**: **Waiting for the files**, **Reading the files**, **Waiting for your choices**, **In the queue**, **Importing**, **Imported**, **Failed** or **Taken away**.

## 1. Sending the files

**New import** offers three ways:

| Way | When to use it |
|---|---|
| **From this computer** | The files are on your computer. **Send the files** uploads them, showing the progress |
| **From a server (SFTP)** | The files are on a server the panel can reach over SFTP: the panel downloads them from there, without going through your computer. It also needs the right **CSP · Import old logs from a server (SFTP)** |
| **From addresses on the web (HTTPS)** | The files are published on a web server: write the addresses, one per line |

*From a server (SFTP)*

Write **Server**, **Port**, **User** and **Folder of the logs**, and choose the **Access**:

- **With the key of the panel (recommended)**: the page shows the public key of the panel, to add to the user on the server (with **Copy**). No password leaves your hands, the key belongs to your organization only and you can remove it from the server whenever you want;
- **With the password of the user**: it is used for this import only and then not kept.

With **Connect**, the panel shows the fingerprint of the server: check that it is the one of your server and confirm with **Yes, it is my server**. Then choose the files and **Download and read the files chosen**.

*From addresses on the web (HTTPS)*

HTTPS addresses only: the panel checks the certificate of the server and does not download from a server with a certificate that is not valid. If the server publishes the SHA-256 fingerprint of a file, write it after its address: a file that does not match is not imported.

For the **Access** you can choose **None**, **User and password** or **Token**: they are used for this import only and are not kept. **Check the addresses** checks that they answer; then **Download and read the files**.

## 2. What the files hold

The panel reads the files and shows **What the files hold**: how many lines, in how many files, from which day to which day, and **The first lines, as the panel reads them**. The lines in a format the panel does not read are counted and left out.

## 3. Your choices

For each **Sender** found in the files (an address or a name):

- **Device**: the device of the subscription its lines go to, or **Do not import**;
- **Clock of the device**: if the device wrote the local time without a time zone (a router on Italian time, for example), choose its time zone, and the times are read in it. **As written in the file** leaves the times as they are.

Also:

- **Leave out the lines containing**: one text per line, regardless of upper and lower case. It is for leaving out useless debug messages;
- **Leave out the lines before**: a day. It is for lines with a wrong time, such as those of a router just switched on with the clock on 1 January.

**Import** puts the import in the queue. When it is done, the **Outcome** says how many lines were imported and of which period.

## Good to know

- **Each file once only**: a file already imported in the subscription is refused, even with another name.
- **The space**: the imported lines count in the space of the plan, not in the volume of the month.
- **No alerts**: imported logs do not start event alerts.

## Taking an import away

From the page of an import:

- **Take away the lines of this import** removes the imported lines; the logs received by the panel stay;
- **Drop this import** deletes the import and its files.

If an import **Failed**, nothing was written: correct the problem shown and start again with a new import.

# Log archives and backups

CSP (Central Syslog) protects the logs of the subscription in two ways:

- the **Log archive** keeps the logs older than the searchable period, which are no longer on the **Logs** page;
- the **Backups** are safety copies of the subscription, to restore it if something goes wrong.

Archive and copies share the **space of the backups** of the plan. The page shows how much they take, for example "Space of the backups: copies 2 GB and log archive 5 GB, 7 GB of 50 GB".

## The log archive

The plan sets how long the logs stay searchable on the **Logs** page. Every night the days that leave that period move to the archive, one file per day; a month archived in full becomes a single file.

The **Log archive** tile lists the archives, with the **Period** (**Day** or **Month**) and the number of **Logs**. In the archive the logs can no longer be searched from the panel: **Download** an archive to look at it or keep it elsewhere.

### *Opening an archive*

An archive is a tar file compressed with zstd, with a CSV file for each day. It opens:

- on Linux, with `tar --zstd -xf <file>`;
- on Windows, with 7-Zip.

The CSV files open with a spreadsheet.

### *Deleting an archive*

**Delete** removes an archive for good: its logs are no longer in the panel. Do it only after downloading it and keeping it elsewhere, for example to free space when the space of the backups is near its limit.

## The backups of the subscription

The **Backup** tile holds the safety copies of this subscription. It works like the backup of the organization (see Configuration backups), but covers only this subscription:

- at the top, the **Last copy** with its outcome, the **Next copy** of the schedule and the space;
- **Make a copy now** makes one by hand, **Schedule** makes them by itself;
- a copy holds the **Configuration (name, devices, plan and limits)**, the **Searchable logs**, or both;
- encryption, remote destinations, download and deletion are the same as in the backup of the organization.

**Restore** opens a guided page: the missing logs come back and, if you choose so, the configuration goes back to how it was in the copy.

### *Which one to use*

| You need to | Use |
|---|---|
| Get back logs deleted by mistake, or put back a device removed | The backup of the subscription |
| Bring back users, roles and all the subscriptions together | The backup of the organization |
| Look at logs from many months ago | The log archive |
| Keep a copy outside the server of the panel | A remote destination in the schedule, or download the archives |

### *The space*

Copies with logs take a lot of space. To stay within the limit:

- use **incremental** copies: after a full copy, the next ones hold only the new logs;
- keep a reasonable number of **Copies to keep**;
- send the copies to a **remote destination**: the remote space does not count in the limit.

When the space of the backups is near its limit or over it, the usage warnings arrive (see Subscriptions).

# The off-site copy

## 1. Introduction

*What the service does*

WFP (Web File) of Esapanel is a **space outside your premises** where your NAS, your servers and your PCs send their backups and the copies of their files, with the programs you already use: Synology Hyper Backup, QNAP Hybrid Backup Sync, Duplicati, the Backup Manager of Plesk, rsync, FileZilla, WinSCP.

The panel does more than receive the files: it **watches that the copies arrive**. It tells you when each device last uploaded, alerts you when one stops uploading and composes every week and every month a report with the days the copies arrived, also as a support for the documentation of the security measures required by the NIS2 directive.

WFP is a destination for copies, not a network drive: it is not mounted as a drive on the PCs and does not replace the NAS of the office.

*Who this guide is for*

The IT staff of the company, or the supplier that manages its systems. You need to know how a backup job is set up on a NAS or a server; you do not need to know Esapanel.

*What you need*

- An active WFP **subscription**.
- A user of the panel that can open the pages of the subscription.
- Administrative access to the devices and the programs to connect.
- The devices must be able to **go out to the Internet** toward the server of the copies, on the ports listed in chapter 3. No inbound port has to be opened in your network.

In this guide the names are examples (`copies.example.com`, `ab12c-nas`). The real values of your subscription are in the pages of the panel.

---

## 2. The pages of the subscription

Open the subscription in the panel (**Services › Subscriptions**, then your subscription). The off-site copy has five tiles:

| Tile | What it holds |
|---|---|
| **Off-site copy** | The space of the plan, the space used, the server and the ports to connect to |
| **Accounts** | The devices, the programs and the people that send their copies, with the instructions to connect them |
| **Shared folders** | Folders of the subscription that the accounts you choose see together |
| **Activity** | When each account connected and how much it uploaded and downloaded |
| **Reports** | The weekly and monthly reports of the copies arrived |

In every page the **?** at the top right opens the description of the page.

---

## 3. The space and where to connect

The page **Off-site copy** shows:

- **Code**: five letters and digits given by the panel, the same for the whole life of the subscription. The names of the accounts begin with the code: if the code is `ab12c`, the account `nas` signs in as `ab12c-nas`.
- **Space of the plan** and **Space used**: the space used is measured every hour.
- **Accounts of the plan** and **Shared folders of the plan**: how many the plan allows.
- **Where to connect**: the name of the **Server** and the port of each protocol.

| Protocol | Who uses it | Usual port |
|---|---|---|
| **rsync (SSH)** | Synology Hyper Backup, Linux servers | 60022 |
| **SFTP** | Duplicati, WinSCP, FileZilla | 50022 |
| **FTPS** | The Backup Manager of Plesk, FileZilla | 21, with the passive ports 40000–40999 |
| **WebDAV (HTTPS)** | QNAP Hybrid Backup Sync | 443 |

The real ports are those written in the page. If your firewall filters the outgoing traffic, open toward the server only the ports of the protocols you use; FTPS also needs the passive ports.

**Plain FTP is never accepted**: every connection is encrypted.

---

## 4. Adding an account

Every device, program or person that sends copies has an **account**: its folder on the server, its password or its SSH keys, the protocols it may use. An account does not sign in to the panel: it only sends and reads back the files. Give each device its own account, so you always know who uploaded and can stop one without touching the others.

1. Open the tile **Accounts** and press **Add account**.
2. **What sends the copies?** Choose the program: Synology Hyper Backup, QNAP Hybrid Backup Sync, Duplicati, Plesk, rsync on Linux, FileZilla, WinSCP, or **Another program**. The choice sets the kind and the protocols the account starts with and, afterwards, the instructions.
3. **Name**: lowercase letters, digits and dashes, for example `nas`. The programs sign in with the full name, `ab12c-nas`.
4. **Description**: optional, to recognize it ("NAS of the office").
5. **Kind**: **Device or program**, or **Person** for who uploads by hand.
6. **Protocols**: leave on only those the program needs. Each protocol is a door into the folder.
7. **SSH public keys**: optional, for rsync and SFTP, one per line. The account signs in with its password as well.
8. Press **Create the account**.

The panel shows the **password** of the account. **Copy it into the program at once: it is shown only this time.** If it is lost, give the account a new password (chapter 7).

Below the password you find **How to connect**: the steps for the program chosen and **The values to type**, already filled in (server, port, username, folder). With **Instructions for** you can read the instructions of another program.

---

# 5. Connecting the programs

The complete instructions, with the values of your account, are in the page of the account. Here are the essential points.

*Synology Hyper Backup*

1. In Hyper Backup create a new data backup task and choose **rsync** as the destination.
2. Server type: **rsync-compatible server**. Server name, port, username and password: those of the page of the account. Turn on the transfer encryption.
3. **Backup module**: `backup`. **Directory**: a name of your choice, the folder of this task.
4. Both the multi-version and the single-version backup work; with the multi-version one turn on the client-side encryption.

*QNAP Hybrid Backup Sync*

1. In Hybrid Backup Sync open **Storage Spaces**, create a new one and choose **WebDAV**.
2. Server URL: the **Address (WebDAV)** of the page of the account, in HTTPS; username and password of the account.
3. Create a **backup job** toward that storage space, with a folder of your choice.
4. Keep the versions on and turn on the client-side encryption.

Toward an rsync server Hybrid Backup Sync only makes sync jobs, without versions: for a real backup use WebDAV.

*Duplicati*

1. Add a backup; as the destination choose **SFTP (SSH)**.
2. Server, port, username and password of the account. Path on the server: `/` or a subfolder, for example `/office-pc`.
3. Test the connection and accept the key of the server only if it is one of those shown in the page of the account (**Keys of the server**).
4. Keep the AES-256 encryption with a passphrase of your own.

*Plesk*

1. In Plesk open **Tools & Settings** › **Backup Manager** › **Remote Storage Settings** › **FTP** (for the whole server), or the Backup Manager of a subscription.
2. FTP server hostname, username and password of the account. Directory for the backup files: `/`.
3. Turn on the **passive mode** and **FTPS**.
4. Turn on the password protection of the backups.

Plesk leaves a file `.ftpaccess` in the folder: that is normal, and the server ignores it.

*rsync on Linux*

1. Put the public key of the user that runs rsync among the SSH keys of the account, or use the password.
2. Send with rsync over SSH to the port of rsync, into the **Folder (rsync)** of the account, which is an absolute path. For example:

   ```
   rsync -a -e "ssh -p 60022" /path/of/the/backups/
   ab12c-nas@copies.example.com:/srv/wfp/ds1/ab12c/accounts/ab12c-nas/
   ```

3. The options `--inplace` and `--append` are refused: every file arrives as a new file, and an interrupted copy does not spoil the one before.

*FileZilla and WinSCP*

For who uploads by hand. In **SFTP** use the port of SFTP and accept the key of the server only if it is one of those of the page of the account. In FileZilla you can also use **FTP with "Require explicit FTP over TLS"** on the port of FTPS. In SFTP and FTPS the folder is `/`: the account sees only its own.

*Another program*

Any program that sends in SFTP, in FTPS (explicit TLS, passive mode), in rsync over SSH or in WebDAV can use an account, with the values of its page.

---

## 6. Encrypting the copies

Always turn on the **encryption of the program** (Hyper Backup, Hybrid Backup Sync, Duplicati, Plesk), with a password kept **outside** the device and outside the server of the copies.

This way the copies can be read only by you: who runs the server keeps data it cannot read. Mind the other side of it: **without that password nobody, not even us, can restore the copies**.

---

## 7. Managing an account

In the tile **Accounts** the list shows for each account its kind, its protocols, its **Last upload** and its state. Open an account to:

- **Protocols and keys**: change the description, the protocols, the SSH keys and the alerts (chapter 9).
- **New password**: the panel generates a new one and shows it once. The programs that use the old one no longer sign in until you give them the new one.
- **Suspend**: the account no longer signs in with any protocol and its sessions end at once; **the files stay**. **Reactivate** lets it in again.
- **Remove**: the account and **all the files of its folder are removed for good**. There is no way back.

The states of an account: **Active**, **Suspended**, **Being prepared**, **Not ready** (the server did not accept the account: open it and press **Try again**).

If a device is compromised or retired, suspend its account at once: the others go on working.

---

## 8. Shared folders

A **shared folder** belongs to the subscription, not to an account. The accounts you choose find it as a folder inside their own, and a file uploaded by one can be read and changed by the others. It serves, for example, several people who leave documents in the same place.

1. Open the tile **Shared folders** and press **Add a shared folder**.
2. **Name**: the accounts see a folder with this name inside their own.
3. **Accounts that see it**: choose the accounts.

Rules:

- Only accounts with **SFTP or FTPS**, and **without rsync**, see it. An account that uses rsync cannot see a shared folder, and an account that sees one cannot turn rsync on.
- Shared folders are not seen in WebDAV and in rsync.
- An account added sees it at its next connection; an account taken out loses it at once.
- **Remove** deletes the shared folder and all its files, for every account.
- The space of a shared folder counts in the space of the subscription.

---

# 9. Checking that the copies arrive

*Last upload*

In the list of the accounts, **Last upload** is the end of the last session in which the account uploaded at least one file. An account that has not uploaded yet shows **Never**.

*The alerts*

In the page of the account, in **Protocols and keys**:

- **Alert if it does not upload for**: 12 hours, 1, 2, 3 or 7 days. Once that time has passed since the last upload you receive **one** alert by email, and in the list the account is marked **Late**; when it uploads again you receive the notice that it is back. An account of the kind **Device or program** starts with the alert on at **1 day**; one of the kind Person without it. Choose a time a little longer than the interval of your backups: 1 day for a nightly backup, 7 days for a weekly one.
- **Alert if the copy is much smaller than usual**: off by default. It tells you when a session uploads less than half of what the account usually uploads: the case of a backup that arrives, but incomplete.

An account just created does not alert until it has uploaded for the first time. While the subscription is suspended the alerts are suspended.

*The activity*

The tile **Activity** lists the **sessions**: a row is everything an account does in one protocol, until it stays an hour without doing anything. For each session you see the account, the protocol, the address it connected from, the start and the end, the files and the space uploaded and downloaded. The backup of a NAS is usually one session with many files.

- **Under way**: the hour of silence has not passed yet, and the numbers still grow.
- **Refused or failed**: an upload interrupted, a file refused because the space is over the limit, a command not allowed. A session with only this number and nothing uploaded deserves a check on the device.

The single files are not listed. The plan says for how many days the sessions are kept.

---

# 10. The reports

The tile **Reports** holds a report for every **week** (composed on Monday) and one for every **month** (composed on the first). When a report is ready you receive an email with the link.

A report says, for each account:

- the **days with a copy**: how many days of the period, and which ones, saw at least one file arrive;
- the files and the space uploaded;
- the last upload.

The totals and the space used follow. Open a report to read it and press **Print or save as PDF** to keep it.

A report **never changes** once composed: the fingerprint at its end attests that the data are those of the day it was made. The reports are kept as many days as the plan keeps the activity.

In **Your choices** you decide which reports you want (weekly, monthly).

> A report proves that the copies **arrive**, not that they can be **restored**. That is checked only with a restore test from the device or the program: do one periodically.

---

## 11. When the space runs out

When the space used goes over the **Space of the plan**, the accounts become **read only**: they read and delete, but do not upload. You receive an alert by email, and the pages show it in red.

- An upload already started ends; the next ones are refused.
- The backup programs report an error, often a generic one: Hyper Backup only writes "Failed to run backup task". If a backup fails without a clear reason, look at the space first.
- To upload again free some space (reduce the number of versions the program keeps, or delete old copies) or ask for more space. The space is measured again every hour: when it is back within the limit the read only is lifted by itself, and you receive a notice.

Before the limit the panel alerts you when the space passes the warning threshold of the plan.

---

## 12. Subscription suspended or deleted

- **Suspended or disabled**: the accounts are blocked and do not sign in; **the files stay**. When the subscription is active again the accounts work again, with the same passwords.
- **Deleted**: the files are kept **30 days**, then removed for good.

---

## 13. Common problems

| What happens | What to check |
|---|---|
| The program does not connect | Server and port of the page **Off-site copy**; that your firewall lets the traffic out toward that port; for FTPS the passive ports too |
| "Access denied" | The full username, with the code (`ab12c-nas`); the password, shown only at the creation: when in doubt **New password**; that the account is not **Suspended** and has that protocol on |
| The program asks whether to trust the server | Compare the key with the **Keys of the server** in the page of the account, and go on only if it is one of those |
| After many wrong attempts it no longer connects even with the right password | The server blocks for a while the addresses that fail repeatedly: wait, or ask the support to unblock your address |
| The backup fails without a clear reason | The space: over the limit the accounts are read only (chapter 11) |
| An interrupted FTPS upload does not resume | It is meant: a file always arrives whole, and the resume is refused. The program uploads the file again from the start |
| rsync refuses `--inplace` or `--append` | It is meant, for the same reason: take them out |
| The account does not see the shared folder | It needs SFTP or FTPS, without rsync; the folder appears at the next connection |
| The account is marked **Late** but the | Look in **Activity** whether the sessions |

| What happens | What to check |
|---|---|
| backup runs | upload files; if the backup is rarer than the alert, lengthen **Alert if it does not upload for** |
| An upload just made is not in the **Activity** | The sessions are updated every few minutes |

## 14. For administrators and resellers

Who administers the server or resells the service also finds:

- **Verification**, in the page **Off-site copy**: every night the panel compares what the server has for the subscription (folders, owners, permissions, users, groups) with what it knows, and lists the differences. **Verify now** does it at once; **Repair** writes everything again as the panel knows it. No file is ever removed: what the server has and the panel does not know is listed and left as it is.
- **The backup of the configuration**: the backups of the customer and of the server hold the accounts (with their passwords and keys), the shared folders and the reports, **not the files**: those are copies already. After a restore the programs of the customers sign in with the same credentials.
- **The space of the server**: the administrator is alerted when the disk of the copies passes 80% and 90%; at 95% every account becomes read only, until it falls below 90%.
- **The API**: the space, the accounts, the shared folders and the activity are also managed from the API of the panel, for provisioning and for monitoring systems.

# Hosts and checks

UCP (Uptime Check) checks all the time that your servers, firewalls, sites and services answer, and alerts you when something stops working. A **host** is a machine to watch, such as a server, a firewall, a printer or a site. A **check** is a test on that host, such as "the site answers", "port 443 is open" or "the certificate does not expire soon".

## Where to find it

- In the subscription, the **Hosts** tile lists the hosts of that subscription. The number on the tile says how many problems are open.
- In the menu, the **Modules** group has **Hosts**, **Problems** and **Downtimes**, with the hosts of all your subscriptions.

The plan sets how many hosts and checks the subscription may have, and how often they may run: the page shows the count, for example "4 of 10 hosts" and "12 of 50 checks".

## Adding a host

**Add host** asks for:

| Field | What to write |
|---|---|
| **Name** | A name for you, such as "Office firewall" |
| **Address** | An IP address or a DNS name. A name is resolved again at every check |
| **Host check** | The check that says whether the host is **Up** or **Down**: **Ping** for most hosts; **TCP port**, with a port that is always open, for a host that does not answer the ping |
| **Check every** | How often the host check runs. The plan sets the shortest interval |

The first check runs within a minute.

Choose a host check that fails only when the whole host cannot be reached: when the host is down, its other checks do not alert, only the host does.

## Adding checks

Open the host and press **Add check**. Choose the type:

| Type | What it checks |
|---|---|
| **Ping** | The host answers, within the times and the packet loss you set |
| **TCP port** | A port accepts connections, and how fast |
| **HTTP/HTTPS** | A page answers, with the status code and the text you expect |
| **DNS** | A name resolves, to the value you expect |
| **TLS certificate** | The certificate is valid and does not |

| Type | What it checks |
|---|---|
| | expire within the days you set |

*Examples*

- **A site**: an **HTTP/HTTPS** check with **HTTPS** on, the **Name of the site** if the host serves more than one, and perhaps a **Text in the page** that appears only when the site really works. **Also check the certificate (with HTTPS)** adds a **TLS certificate** check together with it, which alerts before the certificate expires (it counts as one more check).
- **A mail server**: a **TCP port** check on port 25, and a **TLS certificate** check with **SMTP with STARTTLS**.
- **The dynamic DNS name of a firewall**: a **DNS** check with the **Expected value**, asking **The authoritative servers of the name**, which show a change at once. In **Addresses of the backup lines** write the addresses of a spare line, such as an LTE line: when the name answers one of them, the check goes to **Warning** instead of **Critical**.

*When a check runs*

In **When it runs**:

- **Check every**: the normal interval;
- **Retry every**: after a failure, the check is repeated more often;
- **Attempts**: how many failures in a row confirm the problem.

With 3 attempts and a retry every minute, a problem is confirmed two minutes after the first failure. So a single lost packet does not wake you up at night. A check that answers again is OK at once.

## The states

| State | What it means |
|---|---|
| **Up** / **Down** | The host answers or does not answer the host check |
| **OK** | The check works |
| **Warning** | The check works badly, for example it is slow or the certificate expires soon |
| **Critical** | The check does not work |
| **Unknown** | The check could not be run, for example because the name of the host does not resolve: read the output |
| **Pending** | Before the first result |
| **Not checked** | The host or the check is disabled |

"to be confirmed" marks a failure that still has attempts left.

## The page of a host

The page of a host shows:

- the **State** and since when;
- the **Checks**, each with its state, the **Last result** and when it ran. Open a check to see its history;
- the **Availability of the host**: the share of time **Up** over 24 hours, 7 days, 30 days and 12 months; the bar of **The last 90 days**, one segment per day (green from 99.9 %, yellow from 99 %, red below, grey without data); the **Response time, last 7 days**. Downtimes do not count. It is updated every hour;
- the **Downtimes** (see Downtimes and availability);

- the **Changes of state**, the most recent first.

**Try now** runs all the checks at once and shows what they answer, without writing anything in the history: it is useful after changing a parameter or fixing a service.

**Edit** changes name, address, note and host check. **Disable** stops the host with all its checks without deleting anything; **Enable** starts it again. **Delete** removes the host, its checks and their history.

## Problems

**Modules** › **Problems** shows what is wrong now:

- **Hosts down**: the hosts whose host check failed all its attempts;
- **Checks**: the checks with a confirmed state **Warning**, **Critical** or **Unknown**. A check of a host that is down is marked "host down": look at the host first.

A problem leaves the page when the check is OK again.

*Acknowledging a problem*

On the page of the check, **Acknowledge** says that someone is dealing with it, with a **Note**: the alerts of that problem are no longer repeated, for anyone. The problem stays on the page marked **Acknowledged**.

The acknowledgement drops by itself when the check is OK again, and a new problem alerts again. **Take back** starts the repetitions again.

## Alerts

An email goes out when a problem is confirmed, after the attempts of the check, and one when it ends. Your provider decides who receives them, in the notifications (see Notifications).

**Send notices**, on the page of the hosts of the subscription, says whether the alerts are repeated while the problem lasts:

| Choice | What happens |
|---|---|
| **Only when the state changes** | An email when the problem starts and one when it ends |
| **When the state changes, then every hour** | Also a reminder every hour, while the problem lasts |
| **At every failed run** | An email every time the check finds the problem: with a check every 5 minutes, 12 emails an hour |

A host can have a choice of its own, on its **Edit** page; **As set for the subscription** follows the one of the subscription.

# Downtimes and availability

A **downtime** is a period in which UCP (Uptime Check) sends no alerts about a host or a check: for example a maintenance you know about, an update of the firewall, or the night window in which your provider runs its backups and the server slows down.

## What happens during a downtime

- The checks keep running and their states change.
- No alert goes out, for any user.
- The time in downtime does not count in the availability.
- A problem still open at the end of the downtime is reported at the first run after it.

The page of a host in downtime says so: "In downtime until …: no notice leaves".

## Planning a downtime

Downtimes are planned from the page of each host, in the **Downtimes** section:

| Field | What to choose |
|---|---|
| **On** | **The whole host**, or a single check |
| **Repeat** | **Once** or **Every week** |
| **From** and **To** | For a one-off downtime, the start and the end |
| **Day**, **At** and **For (minutes)** | For a weekly downtime, the day, the start time and the length |
| **Note** | Optional: why, such as "maintenance of the provider" |

Then **Plan downtime**. The times are in your time zone.

**Remove** takes a downtime away: the alerts start again at the next run. A one-off downtime that is over disappears by itself.

*Examples*

- **Firewall update on Saturday evening**: **The whole host**, **Once**, from 22:00 to 23:30.
- **Night backups of the provider**: an **HTTP/HTTPS** check that slows down every night, **Every week** for each day concerned, at 02:00 for 60 minutes.

## All the downtimes

**Modules › Downtimes** lists the downtimes of all your hosts: first those **Under way**, then the **Next** ones, with the host, on what, when and who planned them (**Planned by**). They are planned and removed from the page of each host.

## Availability

Availability is the share of time in which a host was **Up**, or a check **OK**. It shows on the page of the host (from the host check) and on the page of each check:

- over **24 hours**, **7 days**, **30 days** and **12 months**;
- **The last 90 days**, a bar with one segment per day: green from 99.9 %, yellow from 99 %, red below, grey without data. Point at a day to read its value and the minutes in downtime;
- the **Response time, last 7 days**, hour by hour, with the **Mean** and the **Highest** value.

Downtimes and the wait for the first result do not count. Availability is updated every hour.

It is the number to show to whoever asks how available a service has been, for example to check what a supplier promises you.

# DMARC reports

DMARC is the DNS record that tells mail servers how to treat the messages that use your domain as sender without being authorized. Every day the large mail receivers (Google, Microsoft, Yahoo and the others) send to the address written in the DMARC record an **aggregate report**: from which servers the mail in the name of your domain came, how much of it passed SPF and DKIM, what they did with it.

These reports are XML files that are hard to read. DRP (DMARC Report) collects them and shows them in a readable way, so you can see:

- whether all your legitimate mail passes DMARC, before making the policy stricter (from `p=none` to `p=quarantine` or `p=reject`);
- who sends mail in your name: a forgotten newsletter service, a business application, or someone pretending to be you.

DRP reads the aggregate reports (`rua`). The reports of single failed messages (`ruf`) are not included.

## The domains

The **DMARC** tile of the subscription opens **DMARC domains**: the domains whose reports the subscription follows, with the number of **Reports** and the **Last report**. The plan sets how many domains you can follow.

**Add domain** asks for the **Domain**, as in the DMARC record, for example `example.com`, and an optional **Note**.

- The subdomains without a DMARC record of their own are in the reports of the domain. A subdomain with a record of its own receives reports of its own: add it as a domain to follow it separately.
- A domain can be followed by only one subscription of the panel.
- **Remove** stops following a domain: its summaries go with it, its reports stay until they expire.

## How the reports arrive

The **How the reports arrive** box says how the panel receives the reports of the subscription. There are two ways.

### *A mailbox*

The panel reads a mailbox where the reports arrive: the address written in the `rua` of your DMARC record, for example `rua=mailto:dmarc@example.com`. Every 15 minutes it takes the messages that look like reports and reads them.

In **DMARC mailboxes**, **Add mailbox** asks for:

| Field | What to write |
|---|---|
| **Address** | The address of the mailbox, as in the `rua`. Optional |
| **Protocol** | **IMAP** or **POP3** |
| **Server**, **Port**, **Security** | The mail server; always **TLS** or **STARTTLS** |
| **User** and **Password** | The access to the mailbox. The password is kept encrypted and never shown again |
| **Folder read** | For IMAP, the folder where the reports arrive |

| Field | What to write |
|---|---|
| **Folder of the processed** | For IMAP, where the panel moves the reports taken |

Good to know:

- **Only the reports**: the panel looks at the subject of the messages ("Report Domain: ...") and downloads only those; the others are neither read nor marked as read. A mailbox used only for the reports is better.
- With **IMAP** the reports taken move to the folder of the processed: what stays in the folder read is mail that is not a report. On servers that keep all the folders under INBOX the panel finds them and creates them by itself.
- With **POP3** the reports taken are deleted from the mailbox 7 days later.
- **Microsoft 365** does not accept IMAP and POP3 with the password: for now its mailboxes cannot be used.
- One mailbox serves every domain whose record names it: the panel reads the domain in each report.

**Test the mailbox** signs in and says how many messages there are, without taking anything. **Read now** reads at once. **Turn off** and **Turn on** stop and resume the reading. The **State** says **Read**, **Not read yet**, or **Not read since …** when something is wrong: the reason is written next to it.

### *Uploading reports by hand*

On the page of a domain, **Upload reports** accepts XML files, compressed `.gz` or `.zip`, or messages saved as `.eml`. It is for bringing into the panel the history of a domain whose reports went to another mailbox or service: download them from there, then upload them here.

For each file the page says how it went: **Report written**, **Already received** (a report is never written twice), **Not read**.

## Reading the reports

The page of a domain shows the **Last 30 days**, with the messages the receivers counted and how many passed DMARC, and the list of **Reports received**: **Period**, **Receiver**, **Messages**, **DMARC pass**, **Policy** and how it **Arrived**.

A report shows:

- the **Policy seen by the receiver**: your DMARC record as the receiver read it;
- the **Rows**: for each source address (**Source**), the **Messages**, whether **DKIM** and **SPF** passed aligned with the domain of the sender, and what the receiver **Applied** (**delivered**, **quarantine**, **rejected**). DMARC passes when at least one of DKIM and SPF passes aligned;
- **Signatures and SPF seen**: the DKIM signatures and the SPF check as they were, even when not aligned.

**Download XML** saves the original report.

### *What to look at*

- A **Source** you do not recognize, with many messages that do not pass DMARC, is often someone pretending to be you: with a `p=reject` policy those messages are rejected.
- A source of yours (your mail server, the newsletter service, the business application that sends the invoices) that does not pass DMARC must be fixed, by adding it to the SPF record or setting up DKIM, **before** making the policy stricter: otherwise your own mail would be rejected.