

Staff Wi-Fi Administration

Running Staff Wi-Fi from the panel — settings, connector, setup link and certificate management

- [Staff Wi-Fi Administration](#)
- [Settings and Status](#)
- [Useroam Connector](#)
- [Inviting Staff](#)
- [Certificates and Staff](#)
- [Portal Texts](#)

Staff Wi-Fi Administration

Staff WiFi lets employees join the company network **without typing a password**, using a certificate installed once on their device. It is entirely separate from the guest network: the guest portal ties the 5651 record to a phone number, while Staff WiFi ties network traffic to a **person**.

“ **Where is this screen? Staff WiFi** in the left menu, between Analytics and Reports and Settings. Only users with **administrator rights** see the menu.

“ **Pilot stage:** the feature is currently enabled on a limited number of devices. If you cannot see the **Staff WiFi** menu in your panel, it has not been enabled for your device yet — talk to your reseller.

1. What a shared password breaks

When a single WPA2 password is shared across the staff network, the only thing left in the records is the device MAC address. You cannot tell who connected, and cutting off a departing employee means **changing the password and redistributing it to everyone** — which in most organisations means it never changes at all.

Certificate sign-in reverses this: every device gets a certificate issued to one person, it cannot be shared, it is revoked one device at a time, and the company password is no longer stored in the device's Wi-Fi settings.

2. How the flow works

1. The **administrator** turns the feature on and sets the staff network name (SSID).
2. The **Useroam Connector** is installed; it is what verifies the staff password during setup.
3. A **staff member** opens the setup link on their phone and enters their company username and password **once**.
4. The portal produces the right file for the device: a signed profile for iPhone and iPad, a `.p12` certificate file for Android and Windows.
5. The device joins the staff network. It is never asked for a password again.

3. What you need

- **A separate wireless network (SSID) for staff.** It cannot be the same as the guest network.
 - **A Windows machine inside the company network** — the connector app is installed there.
 - **Staff records.** There are two routes: synced from Active Directory / LDAP, or local users created by hand in the panel. Organisations without AD use the second route.
 - **Administrator rights.** Restricted users cannot open this screen.
-

4. What is in this book

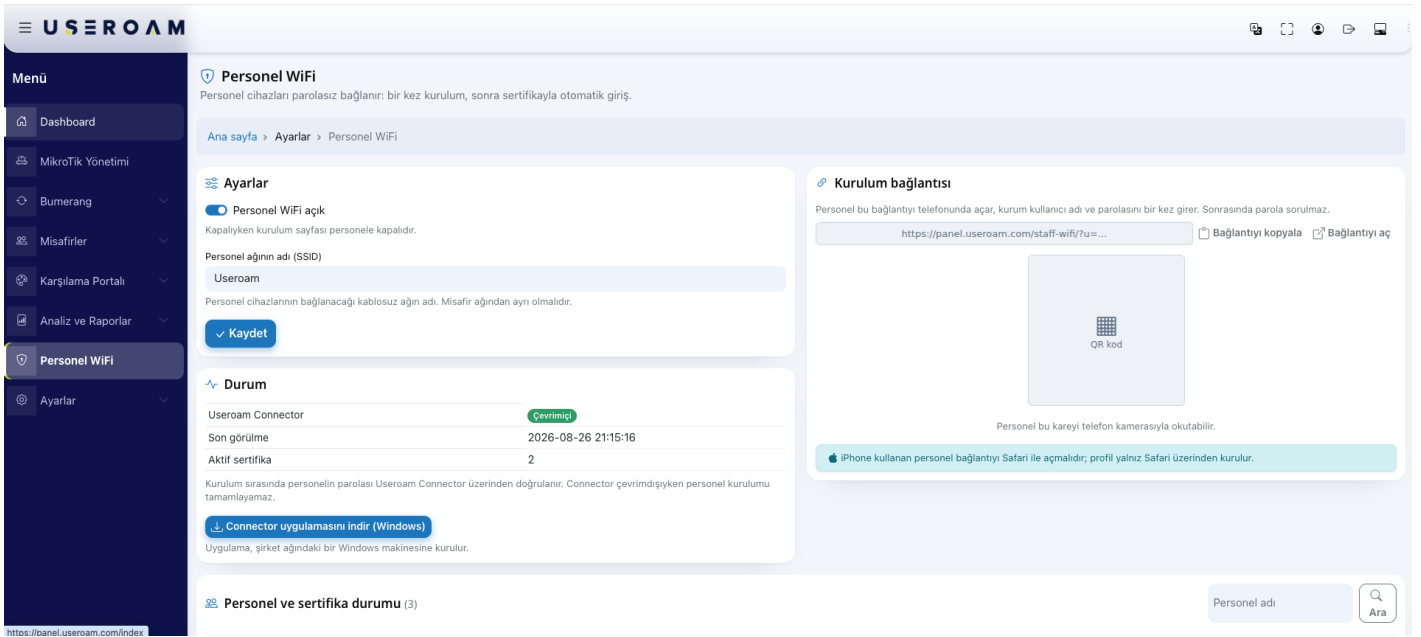
- **Settings and status** — turning the feature on, the network name, connector status.
 - **Useroam Connector** — download, what it does, what happens when it is offline.
 - **Inviting staff** — the setup link, QR code, sending by SMS, user type.
 - **Certificates and staff** — status badges, revocation, expiry, orphaned certificates.
 - **Portal texts** — editing what staff read, language by language.
-

“ **For staff:** the setup guides you send to employees live in a separate book — **Staff Wi-Fi** (iPhone, Android, Windows).

Settings and Status

The **Staff WiFi** screen is made of four cards: **Settings**, **Status**, **Setup link** and **Staff and certificate status**. This page covers the first two.

“ **Where is this screen? Staff WiFi** in the left menu. Settings are per device — you are always editing whichever device is selected in the top menu.



1. The Settings card

- **Staff WiFi is on** — while it is off, the setup page is closed to staff. If you leave it off you will see a warning on the setup link card.
- **Staff network name (SSID)** — the name of the wireless network staff devices will join. It **must be separate from the guest network**. Up to 64 characters, and it cannot be left empty.

Press **Save** and you get *Settings saved*.

The network name you enter is written verbatim into the configuration profile installed on iPhone and iPad. If you change it later, **those profiles keep looking for the old name** and staff on iPhone have to run the setup again. On Android and Windows the certificate is installed independently of the network profile, so those staff simply pick the new network by hand and connect with the same certificate.

2. The Status card

It shows three rows:

- **Useroam Connector** — *Online, Offline or Not installed.*
- **Last seen** — when the connector last reached the panel. Shown only if there is a record.
- **Active certificates** — how many certificates on this device have not been revoked.

Below the card sits the **Download the Connector app (Windows)** button. See **Useroam Connector** for details.

3. Two warnings and what they mean

- **“Staff WiFi is off. The setup link will not work until you turn it on.”** — the switch on the Settings card is off. Staff can open the link but cannot complete setup.
- **“The network name is empty. Staff will not know which network to join.”** — no SSID entered. Even if a certificate is issued, the device has no network to join.

Both appear above the setup link card, because both make that link useless.

4. The verification server name

A staff device verifies the server's identity when it connects. This value is **not managed from the panel**; the setup portal shows it to the staff member on screen, and on Android and Windows it goes into the *Domain* field. Do not look for it on the Settings card.

“ **Related pages: Staff Wi-Fi Administration → Useroam Connector; Inviting staff.**

Useroam Connector

Useroam Connector is a small Windows application installed inside the organisation's own network. When a staff member enters their username and password on the setup page, **the password is verified through this connector**. It is never sent to the panel and never stored there.

“ **Where do I get it?** The **Download the Connector app (Windows)** button on the **Staff WiFi → Status** card. Direct address:

`https://panel.useroam.com/api/connector-download.php`

1. Where it is installed

On a **Windows machine inside the company network**. That machine must be able to reach the directory server (Active Directory / LDAP) used for authentication. The connector's public IP address does **not** have to match the device's IP registered in the panel — the connector proves its identity with a key issued to it, not with its address.

2. What it does

- **Password verification.** When a staff member types their password on the setup page, the request goes to the connector, the connector asks the directory, and the answer comes back.
- **User sync.** Active Directory / LDAP users are copied into the panel and appear in the **Staff and certificate status** list. Groups are copied too. **Passwords are not.**
- **Status reporting.** The connector checks in with the panel regularly; that is where **Last seen** comes from.

3. The three states

- **Online** — the connector is reaching the panel. Staff can run the setup.
- **Offline** — the connector is registered but has not checked in recently. **Staff cannot finish setup**; there is nothing to verify the password against. Check that the machine is

switched on and has internet access.

- **Not installed** — no connector has ever been registered for this device.

While the connector is offline **no new setup can be completed**; there is no password to check against. Devices that already hold a certificate are authenticated by **that certificate**, and this check does not go through the connector. Even so, do not leave the connector down for long: user sync stops as well.

4. Organisations without Active Directory

Neither the connector nor a directory is mandatory. **Local users** created by hand in the panel can also receive certificates; in that case the password is checked against the panel's own user records. When you create the user, set the type to **Staff WiFi (certificate)** — see **Inviting staff**.

“ **Related pages: Staff Wi-Fi Administration → Settings and status; Guests → New User.**

Inviting Staff

Staff setup starts with the **setup link**. You can hand it over directly, let people scan it as a QR code, or have it sent to their mobile number when you create the user.

“ **Where is this card? Staff WiFi → Setup link**. It only appears when a device is selected.

1. The Setup link card

- **Copy link** — puts the address on the clipboard so you can paste it into an email or a message.
- **Open link** — opens the portal in a new tab; useful for seeing it yourself.
- **QR code** — staff scan it with the phone camera. For rolling out to a group, this is the fastest route.

The link does not expire. It belongs to the device, not to a person — every staff member uses the same link. Who may receive a certificate is decided by the **staff record**, not by the link.

“ **iPhone note:** the link must be opened in **Safari**. The profile installs only through Safari; Chrome or an in-app browser cannot install it. This note also appears on the card.

2. User type: hotspot or certificate

When you create a local user (**Guests → New User**) there is a **User type** field:

- **Hotspot user (connects with a password)** — the default. Classic username and password sign-in.
- **Staff WiFi (certificate)** — the user may receive a certificate, and the setup link is **sent to their mobile number**: SMS for local numbers, WhatsApp for international ones.

Choosing the certificate type makes the **phone field required**; leaving it blank stops the record from being saved.

For staff synced from Active Directory you do not have to choose anything.

3. What happens when staff open the link

1. They enter their company username and password. The password is verified through the **Useroam Connector**.
 2. The portal recognises the device and produces the right file: a signed configuration profile for iPhone and iPad, a password-protected `.p12` certificate file for Android and Windows.
 3. On Android and Windows the portal shows the **Identity** and **Domain** values that have to be typed into the Wi-Fi form. Staff must enter them exactly as shown.
 4. The download step must be completed **within 15 minutes**. If it lapses, the staff member fills in the form again — no new link is needed.
-

4. Common situations

- **A staff member says it will not connect** — first check on the **Status** card that the connector is online.
 - **The setup page does not open** — the **Staff WiFi is on** switch may be off.
 - **Someone shows as “Not permitted” in the list** — that user's type is hotspot; they cannot receive a certificate.
-

“ **Related pages: Staff Wi-Fi Administration → Certificates and staff**; the **Staff Wi-Fi** book (guides to send to employees).

Certificates and Staff

The **Staff and certificate status** card lists every staff member on this device and shows where each one stands. The list is staff-centred: people without a certificate appear too.

“ **Where is this card?** The lower half of the **Staff WiFi** screen. The number next to the heading is the total staff count for the device.

1. Status badges

- **Set up** — has a valid certificate; the device can join the network.
- **Not set up yet** — the staff record exists, the setup has not been run.
- **Not permitted** — the user type is not certificate. This person can open the setup link and still receive nothing. Do not confuse it with “Not set up yet”: this person **cannot** set up at all.
- **Expires soon (%d days)** — fewer than 60 days left on the certificate.
- **Expired** — the certificate is no longer valid and the device has dropped off the network.
- **Revoked** — an administrator revoked the certificate.

Certificates are valid for **825 days** and are **not renewed automatically**. When one expires the staff member drops off the network silently — and everyone who was set up in the same period drops **together**. When you see “Expires soon” badges, have those people run the setup again.

2. Search and the list limit

The list shows at most **100 staff** at a time. If there are more, you get “Showing %d of %d staff. Use the search box.” underneath. Type a name into the box at the top right and press **Search**.

3. Revoking a certificate

To cut off a departing employee, use **Revoke** on their row. A confirmation appears: “Revoke this certificate? The device will not be able to connect again and the staff member must run the setup once more.”

Revoking closes **every valid certificate that person holds on this device**. The same person may have set up as both `ahmet` and `ahmet@company.local`; those are separate records, and leaving one behind would keep that device on the network.

“ **When does revocation take effect?** At the device's next network authentication. **A device that is already connected may stay connected until its session ends.** If you need it off immediately, drop the device from the network side as well.

4. Issued certificates

A separate table lists the certificates produced on this device, with **User**, **Issued**, **Valid until**, **Status** and **Action** columns. The newest record is at the top.

If nobody has run the setup yet: *“No certificates issued yet. They appear here once a staff member opens the setup link and completes it.”*

5. Orphaned certificates

Below the staff list you may find a collapsible section headed **“Certificates with no matching staff record”**. These were issued before the staff list check was added and cannot be tied to any staff record.

Revoke them if they are not in use. A valid certificate with no known owner means a device that can join the network and cannot be tracked in the list.

“ **Related pages:** [Staff Wi-Fi Administration](#) → [Inviting staff](#); [Analytics and Reports](#) → [5651 Logs](#).

Portal Texts

You can edit what staff read on the setup portal. The texts are stored **per language and per device**: you edit the texts of whichever language row you opened.

“ **Where is this section?** **Captive Portal → Portal Language Settings**, then click a language in the list. On the language page you get a collapsible section headed **Staff Wi-Fi Texts**.

The badge next to the heading shows **how many texts are customised for this device** in that language. No badge means the language is running entirely on the ready-made texts.

1. Text groups

- **Login form** — the welcome text, username and password labels, the sign-in and back buttons.
- **Status and error messages** — “please wait”, “installing”, empty or wrong username, timeout, user type not eligible, no staff record.
- **Setup result** — the screen after the file is produced: download button, certificate password and the time note.
- **Android steps** — six steps plus the *Identity* and *Domain* field labels.
- **Windows steps** — six steps.

2. What leaving a field empty means

The grey hint inside each field **is the ready-made text for that language**. Leave the field empty and staff see that text. You do not have to fill in everything — write only what you want to say differently. Clear a field later and it returns to the ready-made text.

Field labels are shown **in the panel's own language**, so you can tell what you are filling in even when the language you are editing is another one.

3. Saving

The section has its own **Save** button, **separate from the captive portal form**. Saving staff texts does not touch the captive settings, and the other way round. You get *Texts saved.* when it succeeds.

Each field holds up to **1000 characters**.

4. Things to watch

- **Do not hard-code a server name.** The portal already produces the *Identity* and *Domain* values and shows them on screen; a value typed into the text by hand may be wrong.
- **Keep the step numbering intact.** The Android and Windows steps are read in order.
- **Follow your organisation's language.** Edit the row for whichever language most of your staff use first; the rest keep running on the ready-made texts.
- **If the section is not there**, either you do not have administrator rights, or the feature is not enabled on your device, or the language row you opened belongs to a different device.

“ **Related pages: Staff Wi-Fi Administration → Inviting Staff; Captive Portal → Portal Language Settings.**