BEACON HELP · GUIDE

Administration

Users, roles, the audit log and connected AI apps



BEACON VERSION
2026.11

PUBLISHED
25 November 2026

FOR
Beacon administrators

ONLINE
help.beacon.earlytree.co.uk

© 2026 Early Tree Ltd

Screenshots show a fictional nursery group and people.

Contents

Administration: users, roles, the audit log and connected ai apps. These steps match Beacon 2026.11; for another version, see help.beacon.earlytree.co.uk. Beacon runs at your organisation's own address.

Administering Beacon 4
- Setting up a new Beacon 4

Approving new users 5
- Purpose 5
- Before you start 5
- Approve someone who has signed in 5
- Turn someone away 6
- Import colleagues from Microsoft 6
- Common problems 6
- Related guides 7

Changing someone's role or nurseries 8
- Purpose 8
- Before you start 8
- Open someone's access 8
- Add a role, or more nurseries 8
- Remove a role 9
- Suspend or reactivate someone 9
- Common problems 9
- Related guides 10

Administrators 11
- Purpose 11
- Before you start 11
- Make someone an administrator 11
- Take administrator access away 11
- Common problems 12
- Related guides 12

The audit log 13
- Purpose 13

Before you start 13
Look something up 13
Some actions you'll see 14
Common problems 14
Related guides 14

Connecting an AI app to Beacon 15
Purpose 15
Before you start 15
Connect an app 15
Check and disconnect apps 16
What a connected app can never do 16
Common problems 16
Related guides 17

Managing connected AI apps for everyone 18
Purpose 18
Before you start 18
Review apps and access 18
Revoke access 18
Common problems 19
Related guides 19

Reading the screenshots. The orange numbers 1 on a picture match the numbers in the step text, and an orange box marks the part of the screen a step is about. Every guide is also online, with search, at help.beacon.earlytree.co.uk.

ADMINISTRATION

Administering Beacon

Administrators look after who can use your organisation's Beacon and what each person can see. In Beacon an administrator is anyone marked **Admin** in the users list. Being an administrator is separate from your role: most administrators are also area support managers, but they don't have to be.

Administrators see an extra **Admin** section at the bottom of the menu, with:

Menu item	What it's for	Guide
Users & Roles	Approving people who've signed in, giving them roles and nurseries, suspending them	Approving new users, Changing someone's role or nurseries
MCP tokens	Every AI app connected to Beacon, for everyone	Managing connected AI apps for everyone
Audit Log	A record of who did what, and when	The audit log

Everyone, administrator or not, has **Connected apps** at the bottom of the menu for the AI apps they've connected themselves. See Connecting an AI app to Beacon.

> NO SCREENSHOTS IN THIS AREA
>
> These pages are switched off in the public Beacon demo, which the guides' screenshots come from, so this area describes them in words only.

Setting up a new Beacon

When Early Tree sets up your Beacon, it names your first administrators. When they first sign in with Microsoft, they go straight in as administrators and area support managers with full maintenance access, without waiting for approval. (If no administrators were named, the first person to sign in becomes the first administrator.) Early Tree also sets which Microsoft organisations can sign in: usually just yours. The first administrators then:

1. Add the nurseries and their rooms (see Nurseries).
2. Import colleagues from Microsoft, or approve them as they sign in (see Approving new users).
3. Make sure there are always at least two administrators (see Administrators).

ADMINISTRATION

Approving new users

WHO IT'S FOR	WHERE TO FIND IT	TIME	YOU NEED
Administrator	**Admin** › **Users & Roles**	1 minute per person	Administrator (Admin)

Purpose

When someone signs in to Beacon for the first time, their account is created as **Pending Approval** and they wait on the **Awaiting access approval** page until an administrator lets them in. Approving them gives them a role, the nurseries they can see and their maintenance access, all in one go. Alternatively, you can import colleagues from your organisation's Microsoft directory before they sign in, so they go straight in.

Before you start

- You're an administrator: you can see **Admin** in the menu.
- You know the person's role, which nurseries they work with, and what they need to do in Maintenance. See Roles and what each can do.
- When someone is waiting, administrators see a count next to **Users & Roles** in the menu and a banner on the dashboard. Where your organisation has email switched on, every administrator is also emailed once about each person.

Approve someone who has signed in

1. In the menu, select **Admin**, then **Users & Roles**. The top line shows how many users there are and how many are pending approval.
2. People waiting are listed first, under **N users awaiting approval**, each with their email address and when they first signed in.
3. Under **Role**, choose their role, for example **Nursery Manager**.
4. Under 🔧 **Maintenance**, choose their maintenance access: **No maintenance access**, **Read-only**, **Contributor** or **Manager (full access)**.
5. Under **Access Scope**, choose 🏢 **Specific nurseries** and tick each nursery they work at (or **Select all**), or choose 🌐 **Group-wide** for every nursery.
6. Select **Approve & Grant Access** (with several nurseries ticked, the button reads **Approve · N nurseries**). Everyone needs at least one role: Beacon won't approve someone without one, because they'd see an empty Beacon.

What you should see

> A message confirms the approval, and the person moves to **Active Users** with their role, nursery and maintenance access shown as labels. They can now sign in and see their dashboard.

Turn someone away

If you don't recognise the person, or they shouldn't have access, select **Deny** on their card, then **Deny access** to confirm. Their account is suspended, so they see **Account suspended** if they sign in. You can reactivate them later from **Manage** (see Changing someone's role or nurseries).

Import colleagues from Microsoft

You can bring people in from your organisation's Microsoft directory (Microsoft Entra ID) before they sign in. They're approved as they're imported.

1. On **Users & Roles**, select **Import from Microsoft** at the top right.
2. In **Import from Microsoft Entra ID**, Beacon lists the people in your Microsoft directory who aren't in Beacon yet. Use **Search by name or email...** to find someone.
3. Tick each person to import.
4. Under **Assign role to N selected users**, choose the **Role**, the **Scope** (**Group-wide** or **Specific nurseries**, then tick the nurseries) and their **Maintenance access**. Everyone you import together gets the same role and access.
5. Select **Import N users**.

If anyone can't be imported, the window stays open and a message names them and gives the reason.

Common problems

"Select at least one nursery, or switch to Group-wide".
You chose Specific nurseries without ticking one. Tick a nursery, or choose Group-wide.

"Permission missing" in the import window.
Beacon isn't allowed to read your Microsoft directory. Your Microsoft 365 administrator needs to add the **User.Read.All** application permission to Beacon's app registration and grant admin consent. Until then, approve people as they sign in.

"Give this person at least one role first".
You selected Approve on someone with no role. Give them a role with Approve & Grant Access instead.

"No new users to import".
Everyone in your Microsoft directory is already in Beacon. Find them under Active Users or Suspended instead.

The person still sees Awaiting access approval.
Ask them to refresh the page or sign in again.

Related guides

- Changing someone's role or nurseries
- Roles and what each can do
- Signing in and out

ADMINISTRATION

Changing someone's role or nurseries

WHO IT'S FOR	WHERE TO FIND IT	TIME	YOU NEED
Administrator	**Admin** › **Users & Roles** › **Manage**	1 to 2 minutes	Administrator (Admin)

Purpose

People change jobs, move nurseries and leave. Keep their access in Beacon up to date so everyone sees exactly the nurseries and work they're responsible for, and nobody who has left can still sign in.

Each person can hold several roles. Each role has its own scope (group-wide or specific nurseries) and its own maintenance access, and the person gets the combination of all of them.

Before you start

- You're an administrator.
- You know which role, nurseries and maintenance access the person needs. See Roles and what each can do.

Open someone's access

1. In the menu, select **Admin**, then **Users & Roles**.
2. Find the person under **Active Users** (or **Suspended**). Their card shows their roles as labels, for example **Nursery Manager · Bramble Hill** with 🔧 **Contributor** if they have maintenance access.
3. Select **Manage** on their card. **Manage User Access** opens, with their **Status**, their **Current Roles** and **Add Role**.

Add a role, or more nurseries

1. In **Manage User Access**, under **Add Role**, choose the **Role**.
2. Under **Access Scope**, choose 🏢 **Specific nurseries** and tick the nurseries, or 🌐 **Group-wide**.
3. Under 🔧 **Maintenance Access** (independent of role), choose **None**, **Read-only**, **Contributor** or **Manager (full)**.
4. Select **Assign Role** (or **Assign to N nurseries**).

Choosing a role and nursery the person already has updates its maintenance access instead of adding a second copy. To move someone to another nursery, add the new nursery first, then remove the old one.

Remove a role

1. In **Manage User Access**, find the role under **Current Roles**.
2. Select the bin button at the end of that row. The role is removed straight away.

Removing a role doesn't remove anything the person did: their inspections, comments and actions stay, with their name.

Suspend or reactivate someone

1. In **Manage User Access**, next to **Status**:
   - for an active person, select **Suspend**: they can no longer use Beacon, and see **Account suspended** if they try;
   - for a suspended person, select **Re-activate**;
   - for someone still pending, select **Approve**. Give them a role first: Beacon won't approve someone with none.
2. Select **Close**.

Suspend people who leave your organisation, as well as removing them in Microsoft. Suspending takes effect on their next page, even if they're signed in.

What you should see

> A message confirms each change (**Role assigned to N nurseries**, **Group-wide role assigned** or **User updated**), and the person's card shows their new roles. The change is recorded in the audit log.

Common problems

"Select at least one nursery".
You chose Specific nurseries without ticking one.

The person still sees a nursery after I removed it.
Check they don't have another role covering it, including a group-wide one. Each role is listed separately.

A maintenance manager or area support manager has full maintenance access even though I chose less.
Those two roles always have full (Manager) maintenance access.

"Give this person at least one role first".
They have no role. Add one under Add Role, then approve them.

"You can't suspend your own account" or "This is the last active admin".
Beacon won't let an administrator suspend themselves, or suspend the last active administrator, so nobody is locked out. Ask another administrator, or make someone else an administrator first.

I can't give someone access to just one room.
Beacon doesn't support room-level access yet. Give them their nursery.

Be careful with your own roles.
Beacon lets you remove your own roles. Make sure there's always at least one other area support manager before changing your own access.

Related guides

- Approving new users
- Administrators
- Roles and what each can do
- The audit log

ADMINISTRATION

Administrators

WHO IT'S FOR	WHERE TO FIND IT	TIME	YOU NEED
Administrator	**Admin** › **Users & Roles**	Under a minute	Administrator (Admin)

Purpose

An administrator can manage every user account and role, see the full audit log, and see and revoke every connected AI app. It's a separate switch from a person's role, so you can, for example, make an office manager an administrator without giving them area support powers.

Keep the number of administrators small, but always have at least two, so one person being away never locks you out.

Before you start

- You're an administrator yourself. Only an administrator can make someone else one.
- The person already has an account in Beacon (they've signed in, or you've imported them).

Make someone an administrator

1. In the menu, select **Admin**, then **Users & Roles**.
2. Find the person under **Active Users**.
3. Select **Make Admin** on their card.
4. Read **Grant admin access?** ("This user will be able to manage all user accounts, roles, and view the full audit log.") and select **Grant admin access**.

What you should see

Admin access granted, and the person's card shows a 🛡️ **Admin** label. The button now reads **Admin**. Next time they open a page, they see the **Admin** section in their menu.

Take administrator access away

1. On their card, select **Admin**.
2. Read **Revoke admin access?** and select **Revoke admin access**.

They keep their role and nurseries; they just lose user management, the audit log and the other Admin pages.

You can't take away your own administrator access, or the last active administrator's, so there's always someone who can manage users. People named as first administrators when Beacon was installed get it back each time they sign in, so Beacon won't take it away from them here; ask Early Tree to change the install's settings instead.

Common problems

I can't see Make Admin.
You're not an administrator. Ask one of your administrators.

"You can't remove your own admin access".
Ask another administrator to do it.

"This is the last active admin".
Make someone else an administrator first.

"This person is named in the install's BOOTSTRAP_ADMIN_EMAILS".
They were set up as a first administrator when Beacon was installed. Ask Early Tree to remove them from that setting.

Related guides

- Changing someone's role or nurseries
- The audit log
- Managing connected AI apps for everyone

ADMINISTRATION

The audit log

WHO IT'S FOR	WHERE TO FIND IT	TIME	YOU NEED
Administrator	**Admin** › **Audit Log**	A few minutes	Administrator (Admin)

Purpose

Beacon records important events in an audit log: who did it, what they did, to what, when, from where, and whether it was done on the web, by a connected AI app, by a scheduled job or by Beacon itself. Use it to answer questions such as "who signed this report off?", "when was this person's access changed?" or "what has this AI app been doing?". Maintenance changes are logged too, with the record type **MaintenanceItem**: jobs logged and edited, comments, quotes, merges and undone merges, contractor sign-offs and inspection links.

The log can't be edited from Beacon. Every entry is kept.

Before you start

- You're an administrator.
- It helps to know roughly what you're looking for: the kind of action (for example a sign-off), the kind of record (for example an inspection) or the source.

Look something up

1. In the menu, select **Admin**, then **Audit Log**. The newest events are at the top, 50 to a page, with the total number of events.
2. Narrow the list with the filters:
   - **All origins**: choose **Web session**, **MCP tool call** (a connected AI app), **Cron job** (a scheduled job) or **System**.
   - **All actions**: choose one kind of action, such as `USER_APPROVED` or `ROLE_ASSIGNED`. The list holds every action that has happened in your Beacon.
   - **Entity type (e.g. Inspection)**: type the kind of record, such as `Inspection`, `User` or `RoleAssignment`.
3. Select **Filter**.
4. Use ← **Prev** and **Next** → at the bottom to page through.

Each entry shows:

- the action, in capitals (for example `ROLE_ASSIGNED`), and a coloured label for where it came from (**Web**, **MCP**, **Cron** or **System**);
- the kind of record and the start of its reference;
- who did it, the date and time to the second, and their network address;
- the first part of what changed, as recorded.

What you should see

> Only the events that match your filters, newest first, with **Page N of M** at the bottom if there's more than one page.

Some actions you'll see

Action	What happened
`USER_SIGN_IN`, `USER_SIGN_OUT`	Someone signed in or out
`USER_APPROVED`, `USER_SUSPENDED`, `USER_REACTIVATED`	An administrator changed someone's status
`ROLE_ASSIGNED`, `ROLE_REVOKED`	An administrator gave or removed a role
`ADMIN_GRANTED`, `ADMIN_REVOKED`	Someone was made, or stopped being, an administrator
`FIRST_USER_AUTO_PROMOTED`	The first person to sign in became the first administrator
Starting with `MCP_TOOL_`	A connected AI app read or changed something for someone

Common problems

I can't see Audit Log.
Only administrators can. Ask one of your administrators.

I can't search by person or date.
The filters are origin, action and record type only. Filter as tightly as you can, then page through by date.

The entity type filter finds nothing.
It matches the record type's name (for example Inspection, not "inspections at Bramble Hill"). Clear it and try a shorter word.

Related guides

- Administrators
- Changing someone's role or nurseries
- Managing connected AI apps for everyone

ADMINISTRATION

Connecting an AI app to Beacon

WHO IT'S FOR	WHERE TO FIND IT	TIME	YOU NEED
Everyone	**Connected apps**	5 minutes	Your organisation allows AI apps to connect

Purpose

Beacon can be connected to AI apps that support MCP (the Model Context Protocol), such as Claude. Once connected, you can ask the app questions like "which actions at Bramble Hill are overdue?" or ask it to add a comment, and it works in Beacon **as you**: it sees only what you can see, and can only do what you could do.

Connected apps, at the bottom of the menu, lists the apps you've allowed and what they've been doing, and lets you disconnect them.

Before you start

- Check your organisation's policy on AI apps first. Your administrator may ask you not to connect them.
- You need an AI app that can add an MCP server (often called a connector).
- You need your Beacon address. The address to give the app is your Beacon address followed by `/api/mcp`, for example `yourgroup.beacon.earlytree.co.uk/api/mcp`, starting with `https://`.

Connect an app

1. In the AI app, add a new connector (MCP server) and give it your Beacon address followed by `/api/mcp`.
2. The app opens Beacon in your browser. Sign in with Microsoft if you're asked.
3. Beacon shows **Authorise application**: "**[app name]** wants to connect", **Signed in as** your name, and what it will be able to do:
   - **Read data on your behalf**: view inspections, action items, maintenance tickets and reports you already have access to.
   - **Update data on your behalf**: change action item status, add comments, update inspection narratives and grades, create inspections and maintenance items. It **cannot sign off inspections**.
4. Check the app name and where Beacon will send access (**After approving, tokens will be sent to …**). If Beacon warns that the app registered less than five minutes ago, only carry on if you started the connection yourself.
5. Select **Approve**, or **Deny** if anything looks wrong.

What you should see

> You're returned to the AI app, which can now use Beacon. In Beacon, **Connected apps** lists the app with **Connected** and the date, **Last used**, its permissions (`mcp:read`, `mcp:write`) and how many active tokens it has.

Check and disconnect apps

1. Select **Connected apps** at the bottom of the menu.
2. Check the list. **Recent activity** shows the last 20 things your apps did in Beacon, with the app and the time. Anything shown in red failed.
3. To remove an app, select **Disconnect**, then **Confirm**.

Disconnecting takes effect immediately. If the app tries again later, you'll have to approve it again.

What a connected app can never do

- See more than you can. It has your nurseries, your role and your permissions, nothing more.
- Sign off an inspection. That's only ever done by an area support manager, in Beacon itself.
- Act after you're suspended or after you disconnect it.

Everything a connected app does is recorded in the audit log as an **MCP** entry. Treat what it tells you like a colleague's summary: check before acting, especially for anything about safeguarding.

Common problems

There's no Connected apps link.
It's not available in the public demo. In your organisation's Beacon it's at the bottom of the menu.

"No apps connected."
You haven't approved any yet, or they've all been disconnected or expired.

The app stopped working after a while.
Access lasts an hour at a time and the app renews it itself. If it hasn't been used for 30 days, connect it again.

I don't recognise an app in the list.
Select Disconnect straight away and tell your administrator.

Related guides

- Managing connected AI apps for everyone
- The audit log
- Nina, the AI assistant

ADMINISTRATION

Managing connected AI apps for everyone

WHO IT'S FOR	WHERE TO FIND IT	TIME	YOU NEED
Administrator	**Admin** › **MCP tokens**	A few minutes	Administrator (Admin)

Purpose

Anyone can connect an AI app to Beacon for themselves (see Connecting an AI app to Beacon). **MCP tokens** shows administrators every app that has registered with your Beacon and every person's active access, so you can spot anything unexpected and switch it off.

Before you start

- You're an administrator.

Review apps and access

1. In the menu, select **Admin**, then **MCP tokens**.
2. **Registered clients** lists every app that has registered: its **Name**, **Client ID**, when it was **Registered**, when it was **Last used**, how many **Tokens** it has, and its **Status** (**Revoked** if it has been switched off).
3. **Active access tokens** lists each person's current access: the **User**, the **Client** (app), its **Scopes** (`mcp:read`, `mcp:write`), when it was **Issued**, when it **Expires** and when it was **Last used**.

Revoke access

1. To switch an app off for everyone, select **Revoke client** on its row in **Registered clients**, then **Confirm**. All its access ends at once and it can't be used again.
2. To end one person's access through one app, select **Revoke** on that row in **Active access tokens**, then **Confirm**. They can connect again later, and will be asked to approve it.

What you should see

A revoked app shows **Revoked** in **Registered clients**, and its tokens disappear from **Active access tokens**. The person's **Connected apps** page no longer lists it.

Common problems

An app I don't recognise has registered.

Any app can register, but it can't do anything until a signed-in person approves it. If no one recognises it, select Revoke client.

Someone has left but their app access is listed.

Suspend them in Users & Roles (that stops their access too), and revoke their tokens here.

I want to see what an app has done.

Open the audit log and choose **MCP tool call** under All origins.

Related guides

- Connecting an AI app to Beacon
- The audit log
- Changing someone's role or nurseries