Admin Documentation

Internal Employee Portal Setup Guide

Everything needed to set up a private, login-protected chatbot for employees — including access code management, domain restrictions, and the full employee login experience.

~20 min setup
Admin access required
9 Steps

Prerequisite A tenant must already exist with Deployment Mode set to Internal. If you haven't created the tenant yet, complete the *Tenant Setup & Configuration Guide* first, then return here.

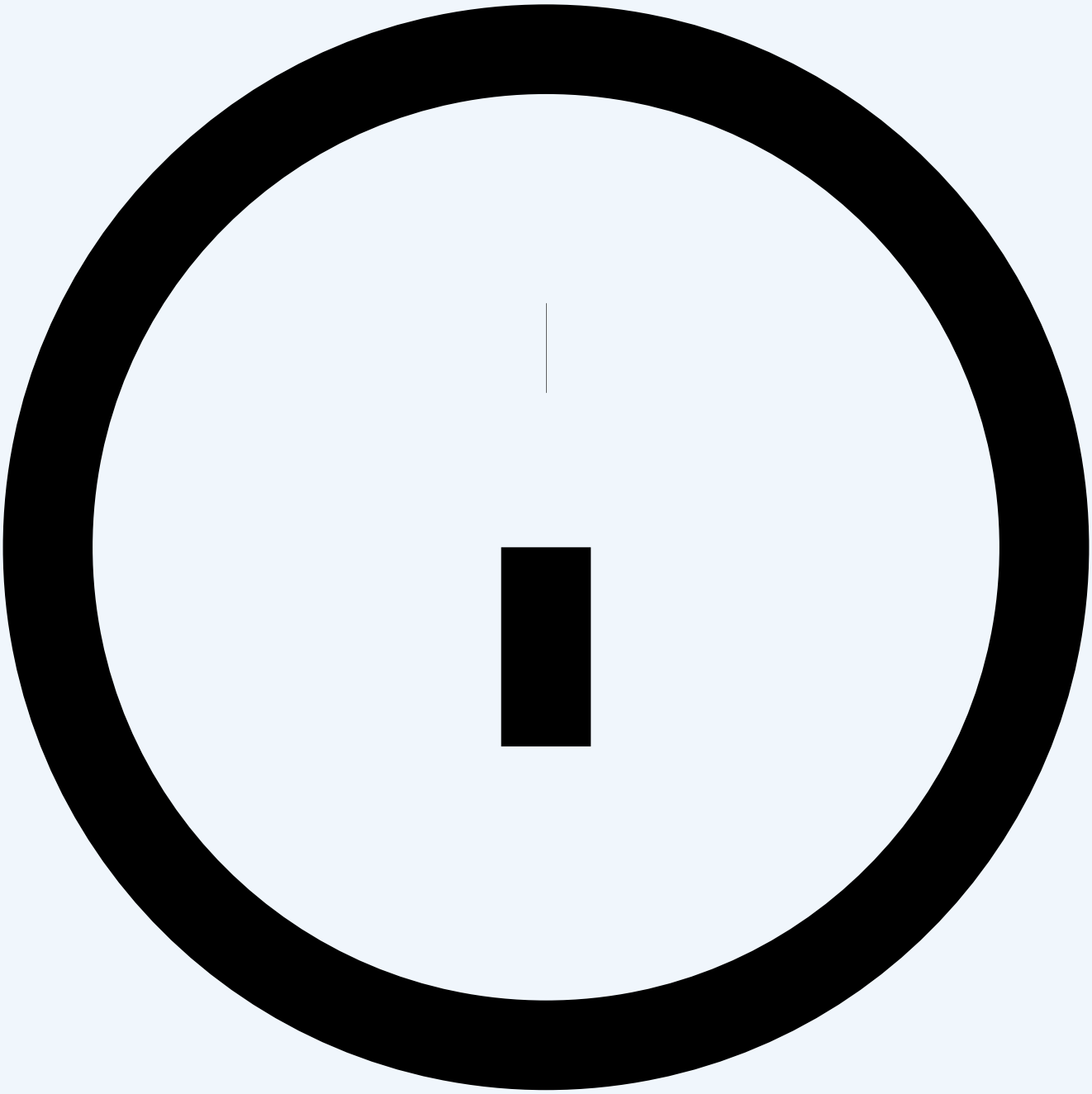
When to Use Internal Portal vs. External Widget

Use Case	Recommended Mode
Customer support on a public website	External Widget
Employee HR & policy questions	Internal Portal
Internal IT helpdesk for staff	Internal Portal
Internal onboarding assistant	Internal Portal
Sales chat on a marketing site	External Widget

STEP 01

Enable Internal Deployment Mode

1. Log in as an **Admin**.
2. Go to **Tenants** and open the tenant you want to configure.
3. Scroll to the **Advanced Settings** section and expand it.
4. Find the **Deployment Mode** dropdown.
5. Select **"Internal"**.



Once you select Internal, a new **"Internal Deployment"** configuration section will appear below with additional fields. Do not save yet — complete the configuration in the following steps first.

IPG-01

Screenshot

The Deployment Mode dropdown open with "Internal" highlighted, and the Internal Deployment configuration section appearing below it

STEP 02

Configure Portal Branding

These fields control what employees see on the login screen when they visit the portal URL.

Internal Portal Title

The main heading on the employee login page. Defaults to the tenant's company name if left empty.

Examples:
`Employee Knowledge Assistant`
`HR Help Desk`

Internal Portal Subtitle

A short description or tagline shown below the title on the login page.

Examples:
`Ask about policies, benefits, IT support`
`Your 24/7 HR assistant`

IPG-02
Screenshot
The Portal Title and Portal Subtitle fields filled in, alongside a preview of how they appear on the employee login screen

STEP 03

Configure Access Control

Allowed Email Domains

Restrict login access to employees with a company email address. Enter one or more domain names separated by commas.

Setting	Example	Effect
Single domain	`acmecorp.com`	Only `@acmecorp.com` addresses allowed
Multiple domains	`acmecorp.com, acme-sub.com`	Both domains permitted
Empty (not recommended)	—	Any email address can attempt login

When an employee enters an email that does not match an allowed domain, they see: "*Only emails from acmecorp.com are allowed.*"

IPG-03
Screenshot
The Allowed Email Domains field with "acmecorp.com" entered and saved

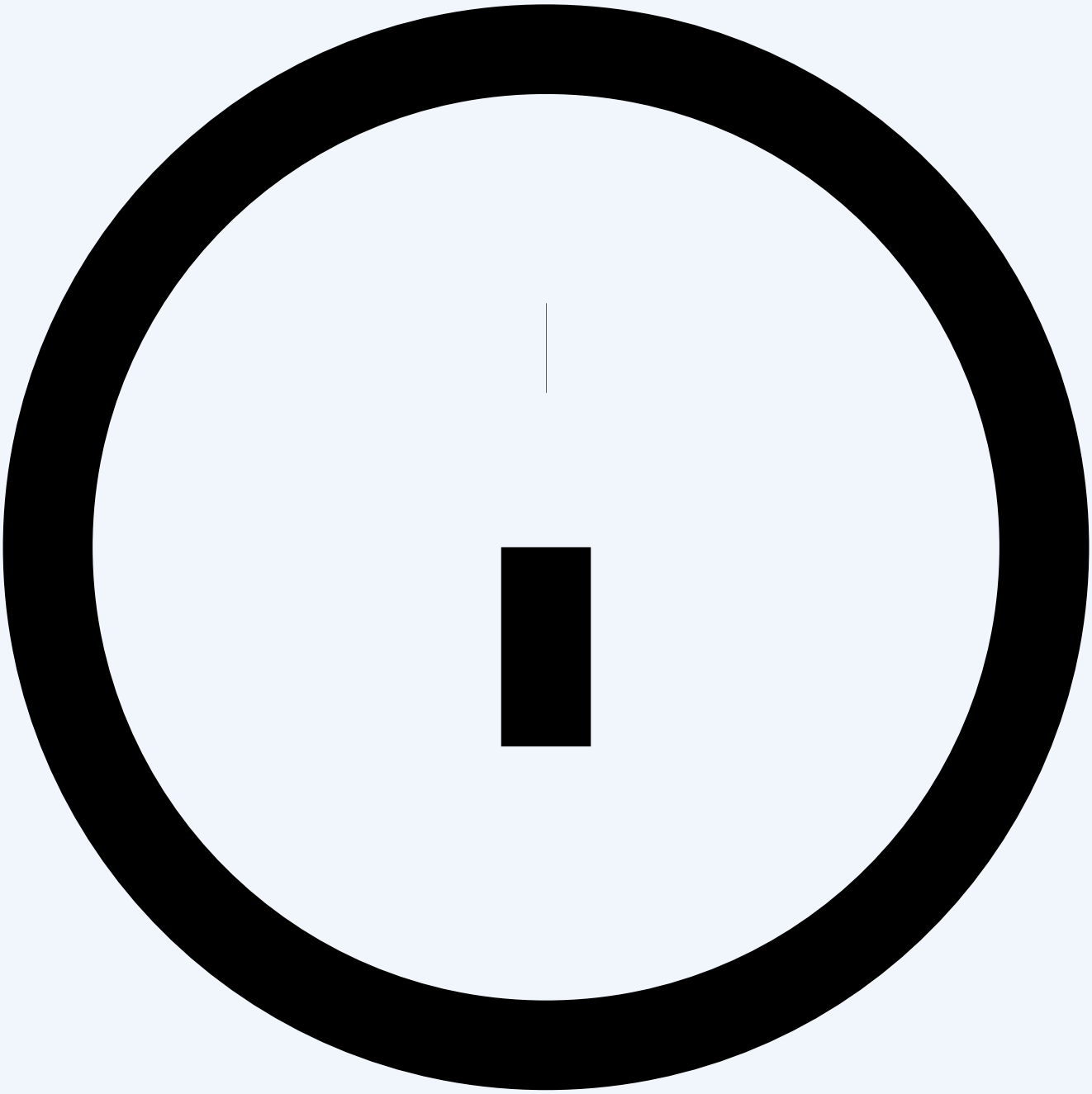
Employee Self-Registration

Enabled

Employees can initiate sign-in with their email and access code. An access code must still be generated by an admin first.

Disabled

Only admins can provision access. Employees cannot initiate the process on their own.



In both cases, an admin must generate an access code for each employee. Self-registration controls whether employees can use the portal before an admin has explicitly provisioned them.

IPG-04

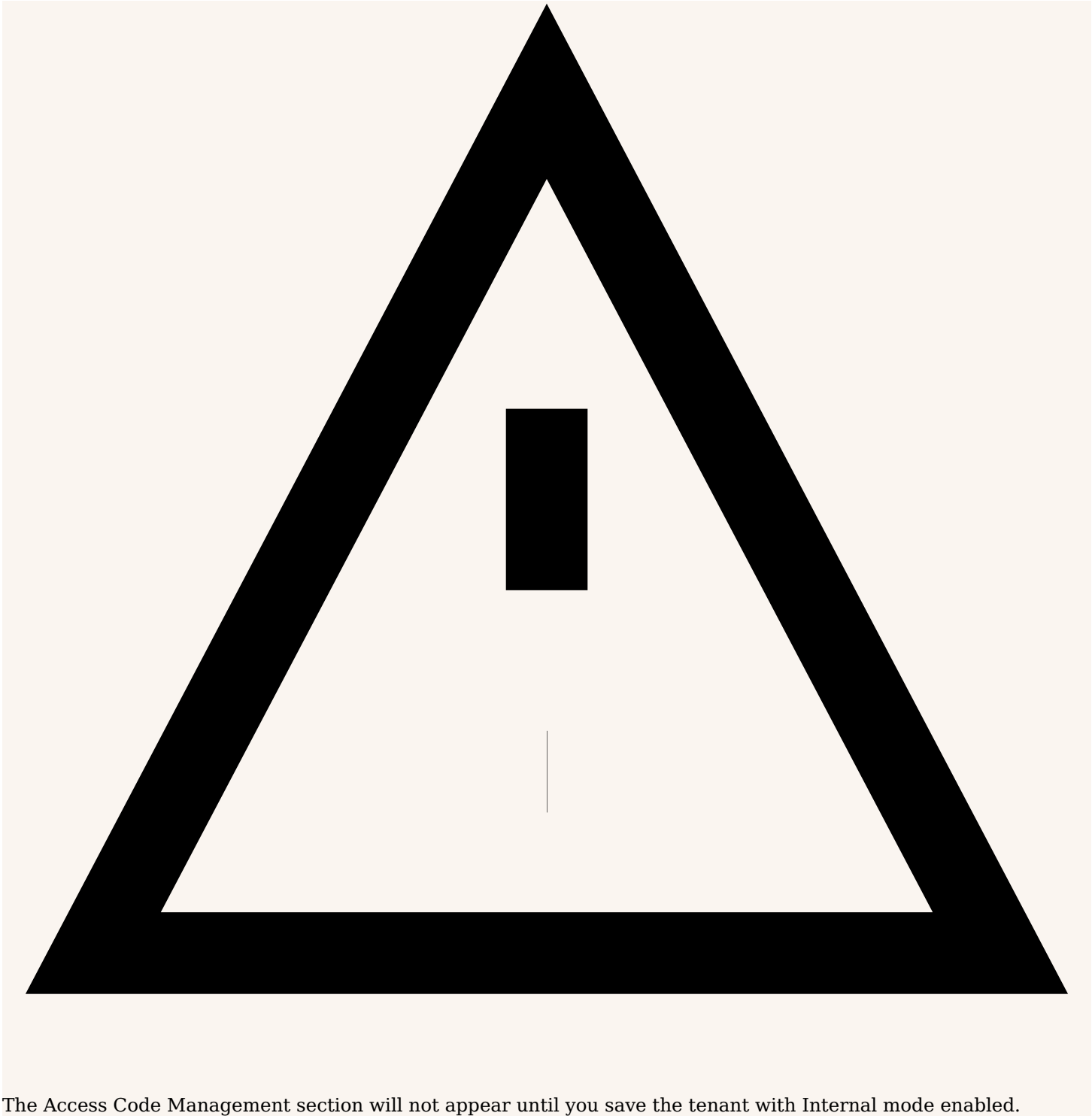
Screenshot

The "Allow employee self-registration" toggle shown in both its enabled and disabled states

STEP 04

Save the Tenant Configuration

Click **"Update Tenant"** to save all Internal Deployment settings before continuing. You must save before Access Code Management becomes available.



The Access Code Management section will not appear until you save the tenant with Internal mode enabled.

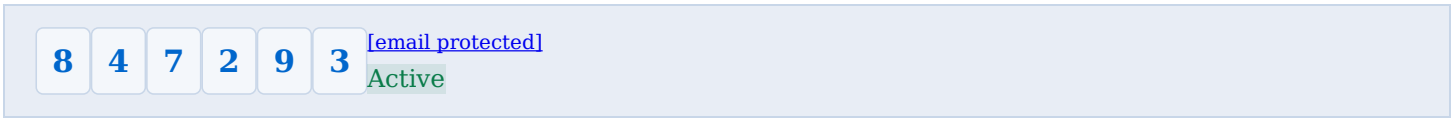
STEP 05

Create Employee Access Codes

Every employee needs a unique 6-digit access code to log in. Access codes are managed in the **Access Code Management** section inside the tenant settings.

1. In **Tenants**, open the tenant and scroll to the **"Internal Deployment"** section.
2. Click **"Manage Access Codes"** — the Access Code Management panel opens.
3. Click **"Add Access Code"**.
4. Enter the employee's **email address**. It must match the allowed domain if one is configured.
5. Click **"Create Access Code"**.

The system automatically generates a random 6-digit numeric code for that email address.



One Code Per Email Each email address can only have one active access code at a time. If you attempt to create a second code for the same email, you will see: "*An access code already exists for this email. Delete the existing code first.*"

IPG-05
Screenshot
The Access Code Management section showing an empty code list and the "Add Access Code" button

IPG-06
Screenshot
The "Add Access Code" form with an employee email entered and the Create Access Code submit button

Sharing the Code with the Employee

1. Click the **copy icon** next to the code — the icon turns green briefly to confirm it was copied.

2. Send the code to the employee via email, Slack, or any internal communication tool.
3. Also send the **Internal Portal URL** (see Step 6).

IPG-07
Screenshot
The access code table showing a code in the Code column with the copy icon turning green after clicking

STEP 06

Share the Portal URL with Employees

The Internal Portal has a unique URL tied to each tenant. Send this URL to your employees along with their access code.

```
https://yourdomain.com/internal-portal?tenant=YOUR_TENANT_ID
```

The Tenant ID is visible in the Internal Deployment section of the tenant settings, or in the browser URL when you are viewing the tenant in the admin panel.

IPG-08
Screenshot
The Internal Portal URL displayed in a code block inside the tenant settings, with a Copy button beside it

Instructions to Send to Employees

1. Go to the portal URL provided by your administrator
2. Enter your company email address
3. Enter the 6-digit access code provided by your administrator
4. Click **Sign In**
5. You will be taken directly to the chat interface

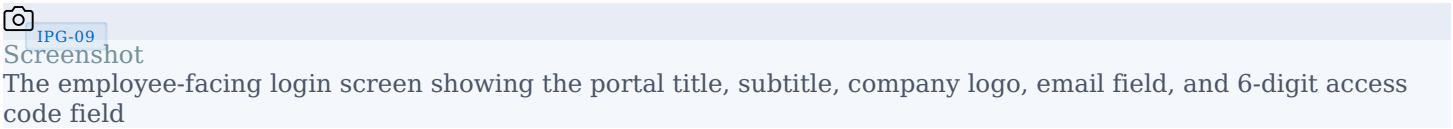
STEP 07

What Employees See

The Login Screen

When an employee visits the portal URL, they see:

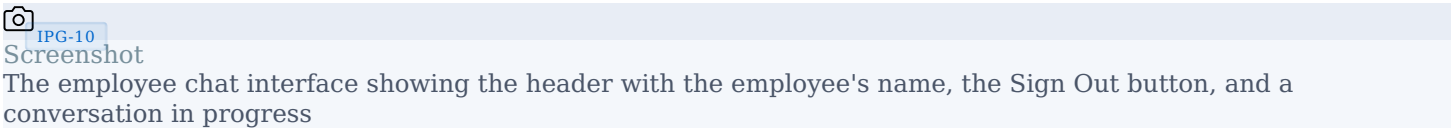
- The company logo (if configured in the tenant)
- The **Portal Title** and **Portal Subtitle** you configured
- A login form with two fields: **Email Address** and **Access Code** (6 digits)
- If the email domain is not in the allowed list, an error appears immediately after entry
- If the email or code is incorrect: "*Invalid email or access code.*"


IPG-09
Screenshot
The employee-facing login screen showing the portal title, subtitle, company logo, email field, and 6-digit access code field

The Chat Interface

After signing in successfully:

- The employee is taken to the chat page for that tenant
- The header shows the company logo, portal name, and their name (derived from their email)
- A **Sign Out** button is available in the header
- The chat experience is identical to the external widget
- Sessions last **24 hours** — after that, the employee must sign in again


IPG-10
Screenshot
The employee chat interface showing the header with the employee's name, the Sign Out button, and a conversation in progress

STEP 08

Managing Access Codes

All access codes for a tenant are visible in the Access Code Management table.

Column	Description
Email	The employee's email address
Access Code	The 6-digit code — click the copy icon to copy to clipboard
Status	Active or Inactive
Last Used	Date and time of the last successful login, or "Never"
Actions	Regenerate (refresh icon) and Delete (trash icon) buttons


IPG-11
Screenshot
The full access code management table showing multiple employees with different statuses and last-used dates

Code Actions

Disable / Enable

Click the Active badge to toggle to Inactive. The employee cannot log in while disabled. Existing sessions expire within 24 hours. Use for employees on leave or during investigations.

Regenerate

Click the refresh icon. After confirmation, a new 6-digit code replaces the old one immediately — the old code stops working right away. Use if a code may have been compromised, or for periodic rotation.

Delete

Click the trash icon. After confirmation, the employee can no longer log in. **This action is permanent.** A new code would need to be created for that email. Use when an employee leaves the organization.


IPG-12
Screenshot
Close-up of the Actions column showing the Regenerate (refresh) and Delete (trash) icons, with a confirmation dialog visible

STEP 09

Monitoring Employee Activity

Employee chat sessions are tracked in the platform analytics. Navigate to **Chat Analytics** or **Chat History** in the main dashboard to view data filtered by tenant.

Chat Volume

Total sessions and messages per time period, filterable by tenant

Questions Asked

Content and topics employees are asking about most frequently

Handoff Requests

Instances where an employee requested a human agent

Session Timestamps

When employees are accessing the portal and session durations

HELP

Troubleshooting

?
An employee sees "Invalid email or access code" but I know the code is correct.

- Check that the access code is Active — not Inactive — in the management table
- Confirm the employee is entering exactly 6 digits with no spaces
- Confirm the email matches exactly what was entered when the code was created (case-insensitive)
- If Allowed Email Domains are set, confirm the employee's email domain matches

?
An employee can log in but gets redirected back to the login page immediately.

- Their 24-hour session has expired — they need to log in again
- Their access code may have been deactivated since they last logged in
- Ask them to clear their browser's local storage or try an incognito/private window

?
I do not see the "Internal Deployment" section in the tenant settings.

- Confirm you have set Deployment Mode to **"Internal"** and saved the tenant
- The section only appears after selecting Internal mode and saving

?
I need to give an employee access to multiple portals (multiple tenants).

- Each tenant is independent — create a separate access code for that employee in each tenant they need access to
- Each tenant has its own portal URL; the employee will need both the URL and code for each one

?
I want to update the allowed email domains after codes are already created.

- You can update the Allowed Email Domains field at any time — changes take effect immediately on the next login attempt
- Existing active sessions are not affected until they expire (24 hours)