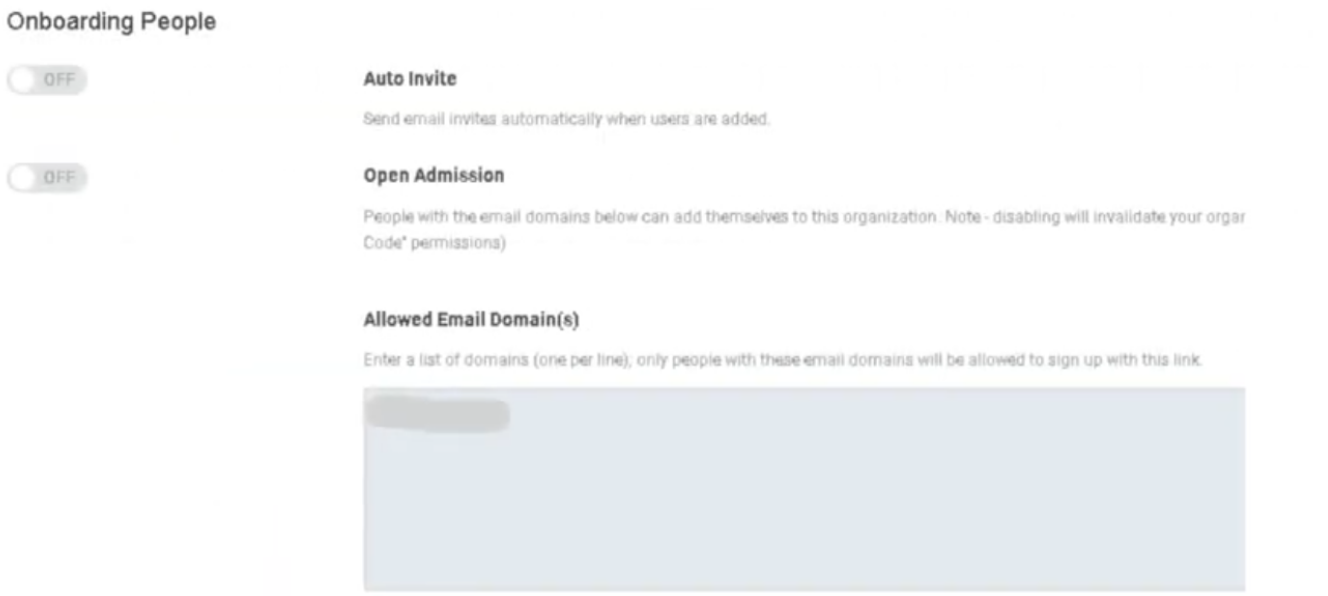
Onboarding & Access

> These settings control how new users are introduced to the platform, what email domains are permitted to join the organization, and how sessions are managed for security and compliance. Configured under **Admin → Account Settings → Organization Settings → Settings → Onboarding People and Telephony Settings**.

Navigation Path

Step	Path
1	Click **Admin**
2	Under **Account Settings**, click **Organization Settings**
3	Click the **Settings** tab
4	Locate the **Onboarding People and Telephony Settings** section

> □□ Authentication settings (Password Policy, SSO, MFA) are on the **Authentication tab**, not the Settings tab. See the **Security & Compliance** page.



---

1. Invitation Settings

Auto Invite (Automatically Send Welcome Email)

State	Behavior
Enabled	When a new user is created (manually or via bulk import), Genesys Cloud immediately sends a Welcome email containing a link to set their password.
Disabled	Users are created silently with no email sent. Admins must manually trigger invitations later from the People list.

When to disable Auto Invite:

Useful when pre-loading a large batch of users (e.g., 100 agents before a go-live) and you don't want them logging in until a specific training date. Create all users, then bulk-send invitations when ready.

> ⚠ Do not send manual email invitations to users who already received an automatic invite — they will receive duplicate emails.

Invitation Link Expiration

Item	Detail
Expiry period	**30 days** from the date the invitation is sent
What happens after expiry	The password-set link in the email becomes invalid
How to recover	Admin must go to **Admin → People & Permissions → People**, find the user, and click **Resend Invite**
Status check	Use the **Welcome Sent** column on the Manage People page to verify whether an invite has been sent to a user

> ⚠ **Note:** The invitation link expires after **30 days**, not 48 hours.

Open Admission (Self-Service Invite Link)

Setting	Description
Open Admission / Invite Link	Generates a shareable link that allows people to add themselves to the organization. Anyone with the link can create an account (subject to Allowed Domains restrictions).
Disable to invalidate	Toggling this off immediately invalidates any previously shared link. Useful for closing off self-registration after an onboarding event.

> □□ Post the invite link on an internal SharePoint or intranet during structured onboarding, then disable it once all expected users have joined.

2. Allowed Email Domains

Setting	Description
Allowed Email Domain(s)	A whitelist of email domains permitted to create accounts in the organization. Only users with a matching domain can be added or self-register.

Example:

Configured Domain	Result
`@telecom-corp.com`	✅ Users with `@telecom-corp.com` can be added
`@gmail.com`	❌ Blocked — cannot create an account
`@outlook.com`	❌ Blocked — cannot create an account

> ⚠ **Important distinction:** This setting controls who can **join the org**. It is not the same as the **Contact Center Email Domain Allowlist**, which controls outbound email routing. These are two different settings in two different locations.

---

3. Free Seating

Setting	Description
Free Seating	When enabled, a station (WebRTC or physical phone) is released once an agent goes offline, making it available for the next user who logs in to that workstation.

> ☐☐ Free Seating must be enabled here at the org level **and** configured on compatible phone base settings before it applies to individual users. See **Technical & Routing Behaviours** for how this interacts with station assignment logic.

---

4. Inactivity Timeout

Setting	Description
Inactivity Timeout	Automatically logs a user out of Genesys Cloud after a set period of idle time with no user input detected.

Configuration range:

Limit	Value

Minimum	5 minutes
Maximum	8 hours
HIPAA orgs	**Mandatory maximum of 15 minutes** — enforced even if the toggle is off

Behavior notes:

Scenario	Behavior
User is actively clicking/typing	Timer resets — no logout
Browser tab is open but no interaction	Timer counts down
Mobile app users	Not recommended — mobile apps handle session state differently and unexpected logouts may occur
Specific API calls	Certain API calls can be excluded from resetting the timer (configured separately)

> **License management tip:** If agents leave browsers open overnight, an open session may still consume a license seat depending on your billing model. Inactivity Timeout closes those sessions automatically.

Onboarding Checklist

Step	Setting	Recommended Action
1	Allowed Email Domains	Set to your corporate domain(s) before any users are added
2	Auto Invite	Decide enabled vs. disabled based on your go-live timeline
3	Open Admission Link	Enable during structured onboarding, disable afterward
4	Inactivity Timeout	Align with corporate security policy (typically 30–60 min); mandatory 15 min for HIPAA
5	Free Seating	Enable if shift workers share workstations
6	SSO / MFA	See **Security & Compliance** page

Last verified against Genesys Cloud Resource Center – March 2026

Revision #2
Created 12 March 2026 22:14:18 by Cesar Gzz
Updated 13 March 2026 00:20:17 by Cesar Gzz