

Authorized Organizations (Pairing)

Navigation: Admin → People & Permissions → Authorized Organizations

What Are Authorized Organizations?

Authorized Organizations (also called **Pairing**) allows users from one Genesys Cloud org to log into and administer a second org — without needing a separate license seat in the target org.

Common use cases:

- A support vendor or MSP managing a customer's org
- A Genesys partner administering a client environment
- A parent company accessing a subsidiary org
- Genesys Product Support pairing with your org to troubleshoot

“ **Telecom analogy:** Think of this like a Federated Trust between two PBX systems — a technician from System A uses their own credentials to manage System B without needing a local extension or station created for them in System B.

Hard Constraints (Exam Critical)

Constraint	Detail
Same AWS region required	Pairing is only possible between orgs in the same AWS region — cross-region pairing is not supported

Constraint	Detail
Max 25 users	A maximum of 25 users from the requesting org can be authorized to access the target org
No license consumption	Authorized users do not consume a license seat in the target org — they are billed to their home org
Admin tasks only	Authorized users cannot receive ACD interactions (calls, chats, emails), use internal chat, or access the agent dashboard
Division access	Authorized users are automatically granted access to all divisions assigned to the roles they receive in the target org

How Pairing Works — Two Sides

Pairing involves two org administrators: one who **requests** access and one who **grants** it.

Side 1: Creating a Pairing Request (Requesting Org)

The org that wants access initiates the request:

1. Admin → People & Permissions → **Authorized Organizations**
2. Click **Create Pair**
3. In the selection box, type and select the **users or groups** from your org who need access
4. Click **Create Pairing Link**
5. Click the **copy icon** to copy the unique URL
6. **Manually send the link** to an administrator of the target org (via email, chat, etc. — Genesys does not send it automatically)

“ ⚠ The pairing link must be sent out-of-band. Genesys does not email it to the target org.

Side 2: Accepting a Pairing Request (Target Org)

The org being accessed approves and assigns permissions:

1. Open the pairing link received from the requesting org
2. Review the prompt and click **Yes, I authorize access**
3. You are taken to the paired organization management page
4. Click on the users or groups included in the request
5. **Assign the specific roles** they need (e.g., Admin, Architect, Telephony Admin)
6. Click **Save**

“ ⚠ **Until roles are assigned, authorized users have zero permissions** in the target org. Accepting the pairing alone grants no access.

Role Assignment in the Target Org

Roles assigned to authorized users work the same as regular role assignments with one important note:

- The roles assigned determine what the authorized user can **do** in the target org
- Division access is **automatically scoped** to all divisions attached to those roles
- Roles should follow least-privilege — only assign what the partner/vendor actually needs

Common role assignments for external access:

Scenario	Suggested Roles
Genesys support troubleshooting	Admin (temporary, revoke after session)
Partner building Architect flows	Architect access, flow designer permissions
Vendor monitoring dashboards	Read-only supervisor / analytics roles
MSP full management	Admin or Master Admin (use with caution)

Managing the Pairing

Revoking Access

- Go to Admin → People & Permissions → **Authorized Organizations**
- Delete the pairing
- This **immediately terminates all active sessions** for the authorized users in your org

Cloned Users

- Authorized users sometimes appear as "**Cloned Users**" in the org directory
- This is expected behaviour — most commonly seen when Genesys Product Support pairs with your org
- Cloned users are read-only representations; they do not consume license seats

Pairing vs. Regular User Creation

Factor	Authorized Org (Pairing)	Creating a User in Target Org
License in target org	Not consumed	Consumed
Identity / credentials	Home org credentials	Target org credentials (separate account)
ACD interactions	Not allowed	Allowed (if role permits)
Internal chat	Not available	Available
Max users	25	No pairing limit
Region requirement	Must match	No restriction
Best for	Temporary admin / vendor access	Permanent staff

Permissions Required

Action	Permission
Create pairing request	People & Permissions admin access
Accept pairing request	Admin in the target org
Assign roles to authorized users	Authorization > Grant > Add in the target org
Delete/revoke pairing	Admin in the target org

See Also

- **Roles & Permissions** — role assignment principles that apply to authorized users
- **Divisions & Access Control** — how division scoping affects authorized user access
- **Organization Settings → Security & Compliance** — IP allowlists and auth controls that also apply to authorized users

Revision #1

Created 12 March 2026 22:38:20 by Cesar Gzz

Updated 13 March 2026 00:20:17 by Cesar Gzz