SSO Integration Guide for Main Portal

> **For:** Main Portal Development Team
> **From:** AI Tools Team
> **Purpose:** Enable seamless user login from Main Portal to AI Tools

---

Overview

Users click "Open AI Tools" in Main Portal → redirected to AI Tools already logged in.

We share the same Supabase database. Main Portal inserts a ticket, AI Tools reads it.

Supported Actor Types:

- `child` - Student users (requires `parent_id`)
- `parent` - Parent account owners
- `admin` - System administrators

Step 1: Apply the Migration

Run this SQL in **Supabase Dashboard** → **SQL Editor**:

```
CREATE TABLE IF NOT EXISTS sso_tokens (
  id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
  ticket TEXT UNIQUE NOT NULL,
  actor_type TEXT NOT NULL CHECK (actor_type IN ('child', 'parent', 'admin')),
  actor_id UUID NOT NULL,
  parent_id UUID,
  plan TEXT DEFAULT 'free',
  expires_at TIMESTAMPTZ NOT NULL,
  used_at TIMESTAMPTZ,
  created_at TIMESTAMPTZ DEFAULT NOW()
);

CREATE INDEX IF NOT EXISTS idx_sso_tokens_ticket ON sso_tokens(ticket);
```

Step 2: Generate a Ticket

Example A: Child Login

```sql
INSERT INTO sso_tokens (ticket, actor_type, actor_id, parent_id, expires_at)
VALUES (
  'sso_tk_' || replace(gen_random_uuid()::text, '-', ''),
  'child',
  '{{CHILD_UUID}}',
  '{{PARENT_UUID}}',  -- Required for child
  NOW() + INTERVAL '30 seconds'
)
RETURNING ticket;
```

Example B: Parent Login

```sql
INSERT INTO sso_tokens (ticket, actor_type, actor_id, parent_id, plan,
expires_at)
VALUES (
  'sso_tk_' || replace(gen_random_uuid()::text, '-', ''),
  'parent',
  '{{PARENT_UUID}}',
  NULL,  -- No parent_id needed for parent actors
  'premium',  -- Optional: subscription plan
  NOW() + INTERVAL '30 seconds'
)
RETURNING ticket;
```

Example C: Admin Login

```sql
INSERT INTO sso_tokens (ticket, actor_type, actor_id, parent_id, expires_at)
VALUES (
  'sso_tk_' || replace(gen_random_uuid()::text, '-', ''),
  'admin',
  '{{ADMIN_UUID}}',
  NULL,  -- No parent_id needed for admin
  NOW() + INTERVAL '30 seconds'
)
RETURNING ticket;
```

Step 3: Redirect User

After getting the ticket, redirect the browser to:

```
https://ai-tools.my-ceo.com/auth/callback?ticket={TICKET}
```

JavaScript Examples

Child Login

```javascript
async function openAIToolsAsChild(childId, parentId) {
  const ticket = `sso_tk_${crypto.randomUUID().replace(/-/g, '')}`

  await supabase.from('sso_tokens').insert({
    ticket,
    actor_type: 'child',
    actor_id: childId,
    parent_id: parentId,
    expires_at: new Date(Date.now() + 30000).toISOString()
  })

  window.location.href = `https://ai-tools.my-ceo.com/auth/callback?ticket=${ticket}`
}
```

Parent Login

```javascript
async function openAIToolsAsParent(parentId, plan = 'free') {
  const ticket = `sso_tk_${crypto.randomUUID().replace(/-/g, '')}`

  await supabase.from('sso_tokens').insert({
    ticket,
    actor_type: 'parent',
    actor_id: parentId,
    parent_id: null,
    plan,
    expires_at: new Date(Date.now() + 30000).toISOString()
  })

  window.location.href = `https://ai-tools.my-ceo.com/auth/callback?ticket=${ticket}`
}
```

Admin Login

```javascript
async function openAIToolsAsAdmin(adminId) {
  const ticket = `sso_tk_${crypto.randomUUID().replace(/-/g, '')}`

  await supabase.from('sso_tokens').insert({
    ticket,
    actor_type: 'admin',
    actor_id: adminId,
    parent_id: null,
    expires_at: new Date(Date.now() + 30000).toISOString()
  })

  window.location.href = `https://ai-tools.my-ceo.com/auth/callback?ticket=${ticket}`
}
```

Security Rules

Rule	Details
TTL	Tickets expire in 30 seconds
Single Use	Ticket is marked `used_at` after first exchange
No PII in URL	Only random ticket string in URL

Actor Type Summary

Actor Type	`actor_id`	`parent_id`	Notes
`child`	Child UUID	**Required**	Student accessing tools
`parent`	Parent UUID	`NULL`	Parent viewing dashboard
`admin`	Admin UUID	`NULL`	Admin with elevated permissions

Questions?

Contact the AI Tools team.