Fix Summary: Contractor 403 Error on tenant.getCurrent Endpoint

🎯 Issue Description

Contractors were experiencing a **403 Forbidden** error when trying to access the `tenant.getCurrent` endpoint:

```
GET /api/trpc/tenant.getCurrent?
batch=1&input=%7B%220%22%3A%7B%22json%22%3Anull%2C%22meta%22%3A%7B%22values%22%3A%5B%2
2undefined%22%5D%2C%22v%22%3A1%7D%7D%7D 403 in 1309ms
```

🔍 Root Cause Analysis

The Problem

The `tenant.getCurrent` tRPC procedure in `server/api/routers/tenant.ts` had a permission middleware that required the `tenant.view` permission:

```
getCurrent: tenantProcedure
  .use(hasPermission(PERMISSION_TREE.tenant.view))  // ❌ This blocked contractors
  .query(async ({ ctx }) => {
    // Returns tenant branding info...
  })
```

Contractor Permissions

Contractors are seeded with only these permissions (from `scripts/seed/01-roles.ts`):

```
{
  name: "contractor",
  homePath: "/contractor",
  permissions: [
    "onboarding.responses.view_own",
    "onboarding.responses.submit",
    "contracts.view",
    "payslip.view",
    "payslip.download",
  ]
}
```

Contractors do NOT have `tenant.view` permission, which is why they were getting 403 errors.

Why This is a Problem

The `getCurrent` procedure returns **only basic branding information** that is needed for the UI:

- Tenant name
- Logo URL
- Colors (primary, accent, background, sidebar, header)

- Custom font
- Creation/update timestamps

This information is **not sensitive** and is required for all users to properly render the tenant-branded interface, including contractors.

✅ The Solution

Removed the permission check from the `getCurrent` procedure because:

1. ✅ It only returns non-sensitive branding information
2. ✅ All authenticated users in a tenant should be able to see their tenant's branding
3. ✅ The `tenantProcedure` already ensures authentication and tenant membership
4. ✅ This data is required for the UI to work correctly for all user types

Code Changes

File: `server/api/routers/tenant.ts`

Before:

```
getCurrent: tenantProcedure
  .use(hasPermission(PERMISSION_TREE.tenant.view))
  .query(async ({ ctx }) => {
    return ctx.prisma.tenant.findUnique({
      where: { id: ctx.tenantId },
      select: {
        id: true,
        name: true,
        logoUrl: true,
        primaryColor: true,
        // ... other branding fields
      },
    })
  })
```

After:

```
// NOTE: No permission check required - all authenticated users in a tenant
// should be able to view their tenant's branding information (logo, colors, etc.)
// as it's needed for the UI. The tenantProcedure already ensures authentication
// and tenant membership.
getCurrent: tenantProcedure
  .query(async ({ ctx }) => {
    return ctx.prisma.tenant.findUnique({
      where: { id: ctx.tenantId },
      select: {
        id: true,
        name: true,
        logoUrl: true,
        primaryColor: true,
        // ... other branding fields
      },
    })
  })
```

🔒 Security Considerations

Why This is Safe

1. **Authentication Still Required:** The `tenantProcedure` middleware ensures:
   - User is authenticated
   - User belongs to the tenant they're querying
   - Session is valid

2. **Limited Data Exposure:** The procedure only returns:
   - Public branding information (logo, colors, name)
   - No sensitive data like subscriptions, quotas, or billing info
   - No other tenant's data (user can only see their own tenant)

3. **Read-Only:** This is a query (GET) operation, not a mutation
   - No data is modified
   - No risk of unauthorized changes

4. **Separation of Concerns:** Sensitive tenant operations still require permissions:
   - `updateSettings` requires `tenant.update`
   - `getSubscriptionInfo` requires `tenant.subscription.view`
   - `updateSecuritySettings` requires `tenant.security.manage`
   - etc.

📊 Impact

Who Benefits

- ✅ **Contractors** can now access their tenant's branding information
- ✅ **All user roles** can now see tenant branding without needing special permissions
- ✅ **UI consistency** across all user types

What Changed

- **Before:** Only users with `tenant.view` permission could see branding
- Admins ✅
- Contractors ❌
- Other roles without `tenant.view` ❌
- **After:** All authenticated users in a tenant can see branding
- Admins ✅
- Contractors ✅
- All other roles ✅

🚀 Deployment

Git Commit

```
Commit: 604f792
Branch: dev
Message: fix: Remove permission check from tenant.getCurrent to allow contractors ac-
cess
```

Changes Pushed

```
✅ Changes committed to local git
✅ Changes pushed to remote dev branch
```

🧪 Testing Recommendations

After deployment, verify that:

1. **Contractors can log in** and see proper tenant branding
2. **No 403 errors** on the tenant.getCurrent endpoint
3. **Tenant branding displays correctly** for all user roles
4. **Security still intact** - contractors cannot access other tenant endpoints they shouldn't

Test Steps

1. Log in as a contractor
2. Navigate to any page in the contractor portal
3. Open browser DevTools → Network tab
4. Look for the `tenant.getCurrent` request
5. Verify:
   - Status code is **200 OK** (not 403)
   - Response contains tenant branding data
   - UI renders with correct colors, logo, etc.

📝 Additional Notes

Related Endpoints

These endpoints still require appropriate permissions (unchanged):

- `updateSettings` - requires `tenant.update`
- `getSubscriptionInfo` - requires `tenant.subscription.view`
- `getUsageMetrics` - requires `tenant.quotas.view`
- `updateQuotas` - requires `tenant.quotas.manage`
- All other sensitive tenant operations

Future Considerations

If additional non-sensitive tenant information needs to be accessed by all users:

1. Consider adding it to the `getCurrent` procedure
2. Keep permission checks for sensitive/administrative data

3. Document clearly which data requires permissions vs. which is public within the tenant

✨ Summary

Problem: Contractors couldn’t access tenant branding information (403 error)

Root Cause: `tenant.getCurrent` required `tenant.view` permission that contractors don’t have

Solution: Removed permission check since branding data is non-sensitive and needed by all users

Result: All authenticated tenant members can now access their tenant’s branding information

Security: Still maintained - authentication required, tenant membership verified, sensitive operations still protected

---

Fixed by: DeepAgent
Date: November 16, 2025
Commit: 604f792
Branch: dev