B2B CONNECTIONS

Setting Up B2B

Steps your IT team takes to enable B2B with GDOTS.

What Is B2B Cross-Tenant Access?

Microsoft Entra ID B2B (business-to-business) collaboration enables organizations to securely share applications and resources with users from other organizations. Cross-tenant access settings control how your organization collaborates with external Entra ID tenants.

To establish a B2B connection with GDOTS, you need to configure outbound cross-tenant access settings in your organization's Entra ID tenant. This allows your users to access resources in the GDOTS tenant when invited.

GDOTS operates in the Microsoft Azure Government (GCC High) environment. This has specific implications for cross-tenant configuration that are noted throughout this guide.

NOT SURE ABOUT B2B?

See About B2B Connections for a non-technical overview of the benefits.

Prerequisites

Entra ID License	Microsoft Entra ID P1 or P2 (included with Microsoft 365 E3/E5, EMS E3/E5)
Admin Role	Global Administrator or Security Administrator in your Entra ID tenant
GDOTS Tenant ID	Will be provided by your GDOTS point of contact
Azure Portal Access	Access to the Microsoft Entra admin center (entra.microsoft.com) or Azure portal

GCC HIGH NOTE

GDOTS uses the Azure Government (GCC High) cloud environment. Cross-cloud B2B collaboration between commercial Azure and Azure Government is supported through cross-tenant access settings. Your commercial tenant can establish trust with the GDOTS GCC High tenant.

BEFORE YOU BEGIN

Review the B2B Requirements to understand what your organization needs before configuring cross-tenant access.

Step-by-Step: Configuring Outbound Cross-Tenant Access

STEP 1: SIGN IN TO THE MICROSOFT ENTRA ADMIN CENTER

Navigate to https://entra.microsoft.com and sign in with an account that has Global Administrator or Security Administrator privileges.

STEP 2: NAVIGATE TO CROSS-TENANT ACCESS SETTINGS

1. In the left navigation, select Identity → External Identities
2. Select Cross-tenant access settings

This page shows your organization's default cross-tenant access policies and any organization-specific configurations.

STEP 3: ADD THE GDOTS ORGANIZATION

1. Click + Add organization
2. In the "Tenant ID or domain name" field, enter the GDOTS tenant ID provided by your GDOTS point of contact
3. Click Add

The GDOTS organization will appear in your list of configured organizations.

> **IMPORTANT**
>
> Since GDOTS operates in GCC High, you must use the tenant ID (a GUID), not a domain name. Cross-cloud lookups by domain name are not supported.

STEP 4: CONFIGURE OUTBOUND ACCESS SETTINGS

Click on the GDOTS organization entry, then select the Outbound access tab. Configure the following:

B2B Collaboration > Users and groups:

- Select Allow access
- Choose either "All users" or specify particular users/groups from your organization that should be able to access GDOTS resources

B2B Collaboration > External applications:

- Select Allow access
- Choose either "All external applications" or select specific applications (e.g., SharePoint Online, Office 365) that your users should be able to access in the GDOTS tenant

Click Save when finished.

STEP 5: CONFIGURE TRUST SETTINGS

Select the Trust settings tab for the GDOTS organization. These settings determine whether the GDOTS tenant will trust MFA and device compliance claims from your organization's tenant.

Trust multi-factor authentication from Microsoft Entra tenants	Enable	Your users' MFA completion is recognized by the GDOTS tenant, so they won't be prompted for MFA again when accessing GDOTS resources
Trust compliant devices	Optional	Allows GDOTS to recognize device compliance claims from your tenant
Trust Microsoft Entra hybrid joined devices	Optional	Allows GDOTS to recognize hybrid join claims from your tenant

Click Save when finished.

STEP 6: VERIFY THE CONFIGURATION

1. Return to the Cross-tenant access settings overview
2. Confirm the GDOTS organization appears with the correct outbound access and trust settings
3. Allow up to 2 hours for the policy to propagate across Microsoft services

Testing the Connection

After configuration is complete and propagation time has elapsed:

1. Have a test user from your organization attempt to access a GDOTS-shared resource (your GDOTS point of contact can provide a test link)
2. The user should be able to sign in with their own organizational credentials
3. If MFA trust is configured, the user should not be prompted for MFA again by GDOTS (assuming they already completed MFA with your tenant)
4. Verify the user can access the intended resources without "Access Denied" errors

Security Considerations

- Principle of least privilege: Only allow access to the specific users, groups, and applications required. Avoid "All users" and "All applications" unless your organization's policy permits it.
- Conditional Access: Review your existing Conditional Access policies to ensure they account for cross-tenant B2B scenarios. Policies that block all external access will override cross-tenant settings.
- Monitoring: Enable sign-in log monitoring for B2B collaboration activity. Audit logs in Entra ID → Monitoring → Sign-in logs can be filtered by cross-tenant access type.
- Regular review: Periodically review your cross-tenant access settings to ensure they remain appropriate. Remove organizations that no longer require access.
- Data Loss Prevention: Consider whether your DLP policies need updates to account for data shared through B2B collaboration with GDOTS.

Common Issues

POLICY CONFLICT WITH DEFAULT SETTINGS

If your tenant's default cross-tenant access policy blocks outbound access, the organization-specific policy for GDOTS should override it. However, Conditional Access policies are evaluated separately and can still block access. Review your Conditional Access policies if users are denied.

PROPAGATION DELAY

Changes to cross-tenant access settings can take up to 2 hours to propagate. If the connection doesn't work immediately after configuration, wait and try again.

CROSS-CLOUD CONSIDERATIONS (GCC HIGH)

Since GDOTS is in Azure Government (GCC High) and your organization may be in commercial Azure:

- Always use the tenant ID (GUID) when adding the GDOTS organization. Domain name lookup is not supported across clouds
- Some features available in commercial Azure may not be available in cross-cloud B2B scenarios. Consult Microsoft's documentation for current cross-cloud feature support
- Token lifetimes and session policies may differ between cloud environments

USERS PROMPTED FOR MFA TWICE

If users are being asked to complete MFA for both their home tenant and GDOTS, verify that MFA trust is enabled in the Trust settings (Step 5 above). Also confirm that the MFA trust policy has had time to propagate.

After Setup: Request Account Conversion

Once you have configured your cross-tenant access settings and verified the connection:

1. Confirm your tenant has MFA enforced and, if your users will access ITAR-controlled sites, that you've verified U.S. person status (see B2B Requirements)
2. Contact your GDOTS point of contact to request conversion of existing guest accounts to B2B collaboration accounts
3. GDOTS will convert the accounts on their side. All existing permissions and SharePoint access are preserved

4. Your users will then sign in with their own organizational credentials instead of their @guest.gdots.com guest accounts

For details on what happens during conversion and what your users need to know, see the conversion section below.

Converting from Guest to B2B

OVERVIEW

When your organization completes the cross-tenant setup above and requests account conversion, GDOTS converts your internal guest accounts to B2B collaboration users using Microsoft Entra ID. This changes where you authenticate, but preserves all your existing access.

WHAT GDOTS DOES

GDOTS uses the Entra ID "Convert to B2B user" feature to change the authentication source for your accounts. Instead of authenticating against the GDOTS tenant (with your @guest.gdots.com credentials), your accounts are linked to your home organization's tenant. GDOTS handles this process. No action is required from end users during conversion.

WHAT CHANGES FOR END USERS

Sign-in credentials	@guest.gdots.com username + password	Your own organization's username + password
Password management	Managed separately by GDOTS	Managed by your organization (no extra password)
MFA	GDOTS-specific Authenticator setup	Your organization's existing MFA
SharePoint access	All granted sites	Same (all permissions preserved)
Bookmarks/saved links	Work	Still work (same URLs)

KEY POINT

All your SharePoint site access and permissions stay exactly the same. The only thing that changes is how you sign in.

WHAT TO DO AFTER CONVERSION

- Navigate to the same SharePoint links from your welcome or notification emails
- When prompted to sign in, use your own organization's credentials (your normal work email and password)
- If prompted for MFA, use your organization's MFA method, not the GDOTS Authenticator setup from before
- Your old @guest.gdots.com credentials will no longer work. This is expected

TIP

If your browser auto-fills your old @guest.gdots.com credentials, clear the saved password or use a private/incognito window for your first sign-in after conversion.

TROUBLESHOOTING POST-CONVERSION ISSUES

I'm still being asked for my old guest credentials

Your browser may have cached your old sign-in. Try these steps:

- Clear your browser's cache and cookies for Microsoft sites
- Open the SharePoint link in a private/incognito window
- Sign in with your organization's credentials when prompted

I see the wrong account or "pick an account" shows my old guest account

Sign out of all Microsoft accounts in your browser:

- Go to https://login.microsoftonline.us/logout
- Close all browser windows
- Open a fresh browser window and navigate to your SharePoint link
- Sign in with your organization's credentials

Access Denied after conversion

- Allow up to 2 hours for the conversion to fully propagate across Microsoft services
- Make sure you are signing in with your organizational credentials, not your old guest account
- If the issue persists after 2 hours, contact your GDOTS point of contact

MFA prompt from both my organization and GDOTS

This usually means the MFA trust setting hasn't propagated yet, or wasn't enabled during the B2B setup. Your organization's IT admin should verify that MFA trust is enabled in the cross-tenant access settings for GDOTS. See Step 5 of the configuration above.

STILL HAVING TROUBLE?

Contact your GDOTS point of contact for assistance with tenant ID, test resources, or troubleshooting the B2B connection.