B2B CONNECTIONS

About B2B Connections

Why B2B is the preferred way to access GDOTS resources.

What Is B2B?

A B2B (business-to-business) connection is a trust relationship between your organization's Microsoft tenant and the GDOTS tenant. Once established, your users can access GDOTS resources using their own work credentials, the same username and password they already use every day.

No more separate GDOTS guest accounts. No more extra passwords. No more separate MFA setup.

Benefits

No separate passwords: Your users sign in with their existing organizational credentials. No need to create, remember, or manage a separate GDOTS guest password.

MFA handled by your organization: Multi-factor authentication is managed through your own organization's existing MFA setup. Users don't need to configure a separate MFA method for GDOTS.

Easier onboarding: When new people in your organization need GDOTS access, they don't need to go through the guest account setup process. They can be granted access and sign in immediately with their work credentials.

More secure: Identity management stays centralized under your organization's control. When someone leaves your organization, their access to GDOTS is automatically revoked when you disable their account. No separate GDOTS account to track.

Seamless experience: One fewer account to manage. Your users access GDOTS resources the same way they access everything else, with their normal work login.

BEFORE YOU START

B2B partners must enforce MFA for their users and, for ITAR-controlled sites, verify that users meet U.S. person requirements. See the requirements section below.

Guest Account vs. B2B: Comparison

Sign-in credentials	Separate @guest.gdots.com account	Your own work credentials
Password management	Managed separately from your org	Managed by your org (no extra password)
MFA	Separate MFA setup with GDOTS	Your org's existing MFA
New user onboarding	Each user sets up a guest account	Grant access, and they sign in immediately
Offboarding	Must notify GDOTS to disable account	Disable their org account, and GDOTS access is revoked automatically
SharePoint access	Same	Same (permissions are preserved)

What It Takes

Setting up a B2B connection is a one-time configuration by your organization's IT administrator:

- Your IT admin configures a cross-tenant trust in Microsoft Entra ID (15-30 minutes of technical work)
- Your IT admin contacts GDOTS to request conversion of existing guest accounts to B2B
- GDOTS converts the accounts. All existing permissions and access are preserved
- Your users start signing in with their own work credentials

What Changes for Your Users

When the switch happens, your users will:

- Stop using their `@guest.gdots.com` username and password
- Start signing in with their normal organizational credentials
- Use their organization's existing MFA method (not the GDOTS Authenticator setup)
- Keep all the same SharePoint site access. Nothing is lost or disrupted

For details on the conversion process, see Converting from Guest to B2B.

> **READY TO GET STARTED?**
>
> Share the B2B Setup Guide with your IT team.

Requirements

> **DISCLAIMER**
>
> This section provides informational guidance about requirements for B2B connections with GDOTS. It is not legal advice. Consult your organization's compliance and legal teams for definitive guidance on your specific obligations.

HOW GDOTS PROTECTS YOUR DATA

GDOTS operates in Microsoft Azure Government GCC High, an environment built for workloads requiring the highest levels of federal security compliance. Regardless of your organization's own compliance posture, GDOTS maintains these protections on all data in its tenant:

- FedRAMP High and DoD IL4/IL5 environment — the GCC High infrastructure meets stringent federal security baselines
- Conditional Access policies enforced on all external users accessing GDOTS resources, including MFA requirements and session controls
- Data Loss Prevention (DLP) policies and sensitivity labels protect controlled content within GDOTS SharePoint
- Audit logging and eDiscovery capabilities track all access to GDOTS resources
- SharePoint permissions and sharing controls limit access to authorized users on a per-site basis

With B2B, your organization provides the identity — GDOTS controls the data and enforces security on its side.

WHAT GDOTS REQUIRES FROM YOUR ORGANIZATION

To establish a B2B connection, your organization must meet these requirements:

1. MFA enforced for all users who will access GDOTS resources. Your Entra ID tenant must require multi-factor authentication — GDOTS trusts your tenant's MFA claims instead of managing MFA separately.
2. Account lifecycle management — disable or remove user accounts promptly when people leave your organization. With B2B, revoking a user's account in your tenant automatically revokes their GDOTS access.
3. U.S. persons verification — for users who will access ITAR-controlled SharePoint sites, verify they are U.S. persons (U.S. citizens, permanent residents, or protected individuals as defined by 22 CFR 120.62). See ITAR requirements below.

4. Export control awareness training — for users who will access ITAR-controlled sites, provide basic training on recognizing and handling controlled data.
5. Cross-tenant access settings configured — your IT administrator configures outbound cross-tenant access in Microsoft Entra ID. See the B2B Setup Guide for step-by-step instructions.

ITAR-SPECIFIC REQUIREMENTS

Some GDOTS SharePoint sites contain data controlled under the International Traffic in Arms Regulations (ITAR). If your users will access these sites, the following apply:

- U.S. persons only: Access to ITAR-controlled data is restricted to U.S. persons — U.S. citizens, permanent residents, or protected individuals as defined by 22 CFR 120.62
- Your organization verifies status: With B2B, your organization is responsible for confirming that users who access ITAR-controlled sites meet the U.S. persons requirement
- Awareness training: Provide export control awareness training to users who will access ITAR-controlled SharePoint sites so they understand handling expectations
- Report suspected violations: Any suspected unauthorized access to ITAR-controlled data should be reported through your organization's established procedures and to your GDOTS point of contact

NOT SURE WHICH SITES ARE ITAR-CONTROLLED?

Your GDOTS point of contact can clarify which SharePoint sites contain ITAR data and which do not.

FOR DOD CONTRACTORS: ADDITIONAL CONSIDERATIONS

If your organization is a DoD contractor or subcontractor that independently processes, stores, or transmits CUI (Controlled Unclassified Information), you may have compliance obligations under your own contracts that go beyond what GDOTS requires for B2B. These are obligations between your organization and your contracting authority — not requirements imposed by GDOTS.

Common frameworks that may apply to your organization independently:

DFARS 252.204-7012	Adequate security for CUI per NIST SP 800-171; 72-hour cyber incident reporting to DoD
DFARS 252.204-7021	CMMC certification at the level specified in your contract
NIST SP 800-171	Security requirements for protecting CUI in nonfederal systems and organizations
ITAR (22 CFR 120-130)	Controls on export and access to defense articles and technical data; U.S. persons requirement

If you are unsure whether these apply to your organization, consult your compliance or legal team.

READY TO PROCEED?

Follow the B2B Setup Guide to configure the technical connection. Contact your GDOTS point of contact with any questions.