Product Overview

2025

Secure File Access Without Migration

+1 (415) 692-1843
support@myworkdrive.com
101 Europa Dr, Suite 150
Chapel Hill, NC 27517

myworkdrive

Executive Summary

Organizations have invested millions in file infrastructure, yet users struggle with VPN connections and cannot collaborate effectively across all their devices. MyWorkDrive solves this without migrations. The platform delivers secure, VPN-free access to files where they already reside.

Whether data sits in Windows SMB shares, cloud-managed storage like Azure NetApp Files, or across Azure Blob, Azure Files, OneDrive, and SharePoint repositories, users get one consistent experience through web browsers, mapped drives, and mobile apps.

The solution preserves existing identity providers, whether traditional Active Directory with SAML SSO or Microsoft Entra ID. NTFS and share permissions, Microsoft 365 site and library permissions, and Data Lake ACLs remain. Organizations can layer on modern controls like DLP and device approval without disrupting current workflows.

What MyWorkDrive Is

MyWorkDrive functions as a secure translation layer between existing file infrastructure and modern access requirements. The platform takes any storage repository and makes it accessible through HTTPS, no VPN required, no data migration needed.

Supported Storage Systems

- Traditional Windows file servers with SMB shares, including legacy departmental servers
- Cloud-managed SMB platforms including Azure NetApp Files and Amazon FSx for NetApp ONTAP
- Azure Files, whether connected via SMB or REST API
- SharePoint document libraries and OneDrive for Business
- Azure Blob Storage configured with Data Lake Gen2 for hierarchical namespaces

The platform does not elevate permissions, bypass existing security policies, or store files on the server. Users cannot gain access through MyWorkDrive beyond what existing NTFS or tenant permissions allow. The identity provider remains the single source of truth.

Three Key Prinicples

Original files stay on the user’s storage and are never copied out

All transit uses TLS encryption ensuring data security

Privileges are never escalated beyond existing granted permissions

Architecture Overview

Many solutions require disruptive rip-and-replace migrations. MyWorkDrive does not. The platform sits between users and storage, operating as a secure broker rather than another storage tier. The architecture follows a three-layer model: users authenticate to the identity provider (keeping all MFA and conditional access policies intact), establish encrypted HTTPS connections to MyWorkDrive servers, then access is brokered to backend storage, with TLS encryption in transit across all hops.

How It Works

Clients

Windows mapped drive;
MacOS Finder;
iOS/Android;
Browser

MyWorkDrive

Windows Web Server;
Physical, Virtual or Azure

Your Storage

Your Files, Your Servers;
Windows Shares, SMB, Azure File Shares, Azure Blob,OneDrive, SharePoint

Your institution’s existing file shares, whether on Windows Servers, Azure, OneDrive, or On-Prem, are instantly available through secure access points.

Publishing Options

01 Direct HTTPS with IIS

Publish IIS over 443 with an enterprise or public CA certificate. Full feature support across web, mapped drive, and mobile. Requires an inbound firewall rule.

02 Reverse proxy or WAF

Terminate TLS on a proxy that applies filters and monitoring. Maintain session persistence for clusters so a user returns to the same node. Disable HTTP compression for MyWorkDrive paths to reduce exposure to compression-based attacks.

03 Microsoft Entra Application Proxy

If inbound ports are not allowed, publish through the service. Pre-authentication and Conditional Access evaluate before requests reach MyWorkDrive.

04 Cloud Web Connector

Uses outbound-only Cloudflare Tunnels on port 7844. No inbound firewall changes required. Version 6.4+ removed the previous 200MB file size limit.

MyWorkDrive does not store file contents at rest on the server. File data is proxied over TLS between storage and client. When Office on the Web is used (co-authoring requires a temporary copy in OneDrive or SharePoint; changes are written back on save), edits are performed on a temporary staging path with cleanup per tenant policy.

Identity, Authentication, And Authorization

Identity remains under organizational control. Choose Active Directory or Entra ID during setup. There is no in-place conversion. To switch, deploy a new server in the target mode and republish shares and policies.

Identity Mode Decision Flow

Active Directory

SAML 2.0 providers supported

Entra ID

Native sign-in, no SAML configuration

The platform follows least-privilege principles. When a user attempts to access a file, the system checks with storage using his credentials. If NTFS permissions deny access, access is denied. If SharePoint restricts that document library, it stays restricted. The security model remains unchanged.

Active Directory

Most enterprises start here. Existing domain controllers handle authentication as always. Organizations can add SSO through SAML 2.0 with providers such as Okta, Duo, ADFS, Ping, and OneLogin. Security teams keep using the same tools, policies, and audit trails they trust.

Entra ID

Cloud-first organizations skip on-premises complexity. Users sign in with Microsoft credentials, Entra ID conditional access policies apply automatically, and MFA works exactly as configured in the tenant. No SAML configuration required.

Storage And Hybrid Visibility	One interface, multiple repositories. Each storage type maintains its native behavior and security model. Modern access is delivered without re-permissioning. NTFS, SharePoint, OneDrive, and Data Lake ACLs remain authoritative.
SMB Network Shares	Traditional file servers connect exactly as configured. Shared drives maintain their existing folder structure. The platform preserves NTFS permissions down to the most granular level, honors Access-Based Enumeration, and maintains DFS namespaces.
Cloud-Managed SMB	Azure NetApp Files and Amazon FSx maintain their promise of lift-and-shift simplicity. Full NTFS fidelity, all existing security groups, even complex permission inheritance chains work as designed. Remote users access these shares without VPN bandwidth consumption.
Azure Files	Organizations connect via SMB for familiar Windows experience or REST API for cloud performance optimization. Both approaches are supported, and organizations can mix approaches for different shares. Manufacturing clients often use SMB for CAD files (where latency matters) and REST API for document archives (where cloud economics prevail).
SharePoint And OneDrive	Integration through Microsoft Graph API means tenant policies stay in control. External sharing restrictions remain enforced. The retention policies that Legal requires remain applied. The platform provides another access path that respects all Microsoft 365 governance.

Azure Blob With Data Lake	Organizations using analytics can surface Azure Blob containers with Data Lake Gen2. POSIX ACLs work exactly as configured. Data scientists retain familiar tools while business users get simple file access.
End-User Experience	Security solutions must be usable to be effective. Access feels natural across every interface.
Web Client	The browser interface provides single sign-on, familiar folder structure, and standard operations. Drag and drop works as expected. Search finds content where the repository supports it. Public links are not available for every storage type and are governed by policy. The interface can display organizational branding for consistency.
Mapped Drive Clients	Windows and macOS clients present repositories as traditional drive letters. Legacy line-of-business applications that depend on mapped drives are supported. Command-line and scripted workflows remain supported. Performance depends on storage latency, network path quality, and file characteristics. Device approval applies to mapped drive and mobile clients.
Mobile Applications	iOS and Android apps address modern work requirements. Users can view and edit where supported, and upload from the device. Local caching can be disabled or limited by policy. Field users can upload site photos directly to project folders, reducing delays between capture and availability.

Office Integration Options

INTEGRATION METHOD	DATA LOCATION	ADMINISTRATIVE CONTROL
LOCAL DESKTOP OFFICE	Customer storage	Maximum, zero cloud exposure
OFFICE ON THE WEB	Temporary OneDrive/SharePoint staging	Managed, automatic cleanup
CUSTOMER-HOSTED EDITORS (office online server or only office)	On-premises only	Complete, no external dependencies

Organizations typically deploy multiple approaches. A pharmaceutical company uses desktop Office for research teams needing full functionality, Office on the Web for sales teams reviewing documents, and on-premises ONLYOFFICE for clinical trial data requiring air-gap protection.

Security And Governance Controls

Security forms the foundation, not an add-on feature. Every connection uses TLS 1.2 or higher. Authentication occurs at the identity provider. Passwords are not stored on the server. Sessions are short-lived and encrypted. Multi-factor authentication and conditional access policies remain enforced at the identity provider level.

Core Security Posture

01 Transport Encryption

TLS 1.2 or higher for all client connections and API communications.

02 Identity Integration

Authentication and multi-factor requirements enforced at customer identity provider.

03 Authorization Model

Least-privilege access with no capability for permission elevation.

04 Zero Trust Architecture

No VPN requirement, no inbound firewall ports when using Cloud Web Connector.

Policy Controls

DLP provides granular control. Marketing might download files with watermarks containing username and timestamp. Contractors might view but not copy to clipboard. HR shares might block downloads entirely while allowing browser viewing. Rules are configured per share, per group, or per user based on organizational requirements.

Public link sharing is governed by policy. Organizations set expiration, require passwords, limit downloads, disable editing, or disallow links entirely for sensitive shares. Search behavior and public link availability depend on the connected repository and configuration. Financial services clients often allow sharing with 24-hour expiration and mandatory password protection.

Unapproved or unknown devices are blocked from access through device approval controls.

Optional Security Controls

Data Loss Prevention

Per-share controls for download blocking, dynamic watermarking, and clipboard restrictions.

Public Link Sharing

Granular controls for external file and folder sharing (availability depends on storage type)

Device Approval

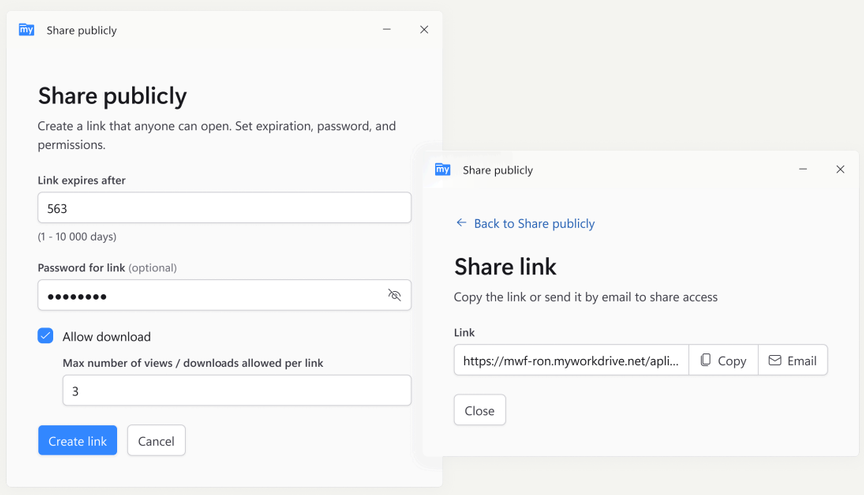
Administrative oversight for mapped drive and mobile client device registration

Guest Access Integration

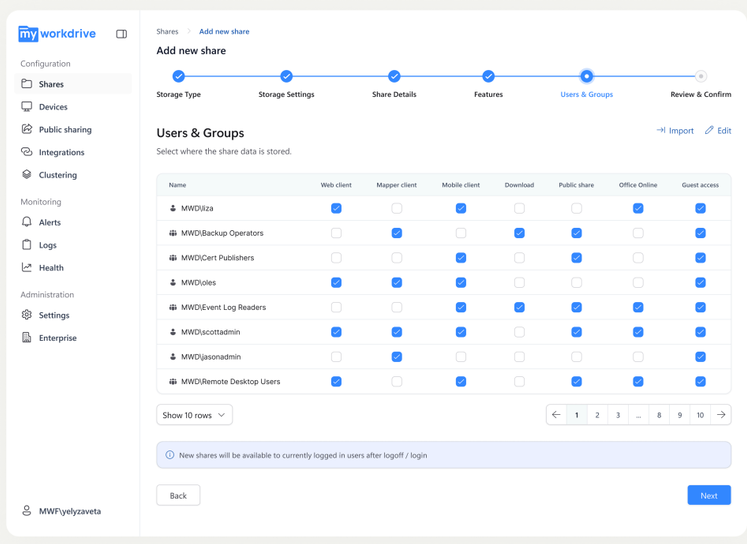
Microsoft Entra B2B external user collaboration with policy inheritance

Audit and Logging

Centralized activity logging with Syslog export for SIEM (Security Information and Event Management) integration and compliance reporting. Logged events include authentication success or failure with IdP claims, and file actions such as open, download, and share-link create or revoke.



Public Link Sharing



Guest Access

Shared Responsibility Model

AREA	USER OWNS	MYWORKDRIVE HANDELS
IDENTITY & AUTHENTICATION	IdP , MFA policies, access rules	Integration plumbing, session management
STORAGE PERMISSIONS	NTFS ACLs, SharePoint permissions, all authorization	Enforcement, brokering, honoring decisions
DATA CLASSIFICATION	Labels, sensitivity markings, confidentiality	DLP controls, watermarking, applying classifications
COMPLIANCE MONITORING	SIEM configuration, alert thresholds, incident response	Generating logs, audit trails, thresholds, incident response shipping to SIEM
DEVICE MANAGEMENT	MDM policies, endpoint security, device compliance	Approval workflow, client access controls

Performance, Scale, And Reliability

Performance depends on four primary factors:

01

Storage system latency

Existing SAN performance characteristics remain unchanged

02

Network path quality

Latency is distance-bound; size and path matter

03

File characteristics

Thousands of tiny files behave differently than one massive CAD drawing

04

Concurrent load

50 users and 5,000 users require different architectures

Deployments range from 50-person firms to enterprise-scale implementations. Smaller organizations often run a single server. No database is required unless Office on the Web coauthoring or public links are needed. Larger deployments use full clusters behind load balancers with database-backed session state. The shared sessions-and-locks database (SQL Server or PostgreSQL) is required for clustering, Office on the Web coauthoring, and public links. Single-server deployments can run without it.

High Availability Architecture: Production deployments utilize multi-node clusters behind load balancers with session persistence requirements. Database options include SQL Server or PostgreSQL with standard high availability configurations.

Pilot Validation Checklist

- ✓ Test actual workflows, not just file copies
- ✓ Include largest commonly-used files
- ✓ Validate from worst network location
- ✓ Test Office save operations during peak hours
- ✓ Verify SIEM log delivery and parsing
- ✓ Check performance from mobile devices on cellular networks

Publishing Options

01

Direct HTTPS

Simple deployment, requires firewall rules

02

Reverse Proxy/WAF

Enhanced security, existing infrastructure

03

Microsoft Entra Application Proxy

AD + SAML only, no inbound ports

04

Cloud Web Connector

Outbound only, maximum security

Typical Use Cases And Real Outcomes

VPN Elimination

A healthcare organization spending significant helpdesk time on VPN issues deployed MyWorkDrive. VPN-related tickets dropped substantially. Remote clinicians gained iPad access to patient documents. ROI calculations proved straightforward.

License Optimization

A manufacturing company had thousands of users but only a subset needed full Microsoft 365 capabilities. Light users needed to view and occasionally edit documents. Organizations can enable browser editing for appropriate users through Office on the Web. All licensing requirements are governed by Microsoft tenant licensing and policy. Result: measurable licensing savings.

Multi-Repository Unification

Mergers create storage chaos. One organization had files across three Active Directory forests, two SharePoint tenants, and numerous departmental file servers. Instead of massive migration, MyWorkDrive presented everything through one interface. Users got immediate relief while IT planned methodical consolidation.

Partner Collaboration

A biotech firm needed to share research data with partners without VPN access. Public link sharing with enforced expiration and download restrictions provided the solution. For longer-term collaborations, Microsoft Entra B2B through the platform provides controlled external access.

Implementation Snapshot

Prerequisites

- Windows Server (2016 or newer) or Azure VM
- Identity source (AD or Entra ID)
- Network routes to storage
- SSL certificate from recognized CA

Week One Deployment

1. **Monday** - Install MyWorkDrive, run setup wizard, connect identity source
2. **Tuesday** - Add first SMB share, test with IT team accounts
3. **Wednesday** - Add cloud repository, validate permissions
4. **Thursday** - Test clients (web, mapped drive, mobile), document issues
5. **Friday** - Resolve issues, configure initial DLP policies

Week Two and Beyond

- Expand to pilot users, gather feedback, adjust policies, test disaster recovery, prepare documentation for change board review.

Publication Options

- **Private Network** - Reverse proxy or WAF with internal load balancing
- **Public Internet** - Direct HTTPS with firewall rules and optional CDN
- **Hybrid Cloud** - Microsoft Entra Application Proxy (for AD plus SAML SSO) or Cloud Web Connector
- **Air-Gap Environment** - Internal deployment with customer-hosted editing solutions

Frequently Asked Questions

- **What Happens To Existing NTFS Permissions?**

  Nothing. They stay exactly as configured. The platform reads, honors, and enforces them.

- **Is Office Editing Seamless With On-Premises Files?**

  Desktop Office through mapped drives works like traditional network drives with standard file locking. Browser editing stages files temporarily to OneDrive or SharePoint for coauthoring, then writes changes back automatically.

- **Can Downloads Be Restricted While Allowing Viewing?**

  Yes. Configure per share, user, or group. Marketing might download everything while contractors only view in browser.

- **How Are Acquisitions And Mergers Handled?**

  Both environments can be presented through MyWorkDrive while maintaining separate identity providers and permissions. This provides time for proper integration planning.

- **How Is Public Link Sharing Secured?**

  Organizations control expiration (hours to days), password complexity, download permissions, edit rights, and which users can create links. Some clients require manager approval through ServiceNow for link creation.

- **Does This Work With DFS Namespaces?**

  Yes. DFS redirects to actual file servers. Connection can be to namespace or directly to underlying servers based on architecture.

Frequently Asked Questions

- **How Does Office File Locking Work?**

  Traditional locking for desktop Office (first person gets write, others get read-only). For browser editing with Office on the Web, real-time co-authoring works as Microsoft designed.

- **What About GDPR/HIPAA/CMMC Compliance?**

  MyWorkDrive supports customer compliance efforts for programs such as CMMC, HIPAA, and GDPR by preserving customer control of identity, data location, and audit. The product uses FIPS-validated cryptographic components where available and supports Windows FIPS mode. Program certifications are achieved and maintained in the customer's environment.

- **How Does Performance Compare Over High-Latency Links?**

  Over high-latency links, HTTPS often performs more consistently than legacy VPN overlays. For web client traffic, a reverse proxy or Azure Front Door can help with global entry and TLS termination. Mapped drive traffic should be sized and tested from representative locations.

- **What Happens During AD Migrations Or Domain Consolidations?**

  If user SIDs change, permissions on file shares need updating. This is standard Windows behavior. MyWorkDrive works with whatever identity emerges from migration.

Next Steps

Ready to Evaluate MyWorkDrive?

Technical Demonstration

Review your files accessed through MyWorkDrive. Bring representative edge cases and complex shares.

Security Review

Receive architecture diagrams, pen test reports, and compliance documentation for security team evaluation.

Pilot Design

Define success criteria relevant to your organization, focusing on user satisfaction and operational efficiency metrics.

Glossary

ABE (Access-Based Enumeration) - Windows Server feature that hides files and folders from users who lack read permissions.

Microsoft Entra Application Proxy - Microsoft service for publishing on-premises apps through Microsoft Entra ID (formerly Azure AD). Works with MyWorkDrive in Active Directory plus SAML SSO mode.

Data Lake Gen2 - Azure Blob storage configuration providing hierarchical namespace and POSIX-style access control lists.

Managed Identity - Azure feature providing automatically managed credentials for applications to authenticate to Azure services.

Zero Trust Network Access - Security model requiring strict identity verification regardless of user location, with no implicit trust assumptions.

About MyWorkDrive

MyWorkDrive bridges the gap between functional file storage and modern access requirements without massive migrations or security compromises.

The platform makes existing investments work the way users expect in 2025, securely, reliably, and without the complexity that creates operational burden.

Founded on the principle that IT should enable work rather than constrain it, MyWorkDrive serves organizations that value data sovereignty, appreciate existing infrastructure investments, and need to modernize access without modernizing everything.

Let's Discuss Your Environment

Book Demo