2025

MyWorkDrive Technical Summary

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

my workdrive

Executive Summary

MyWorkDrive is a secure file access platform that eliminates VPN dependencies by providing application-level access to existing enterprise file storage. The solution enables browser, mapped drive, and mobile access to Windows SMB shares, SharePoint, OneDrive, Azure Files, and Azure Blob Storage without data migration or changes to existing permission structures.

Key Value Proposition

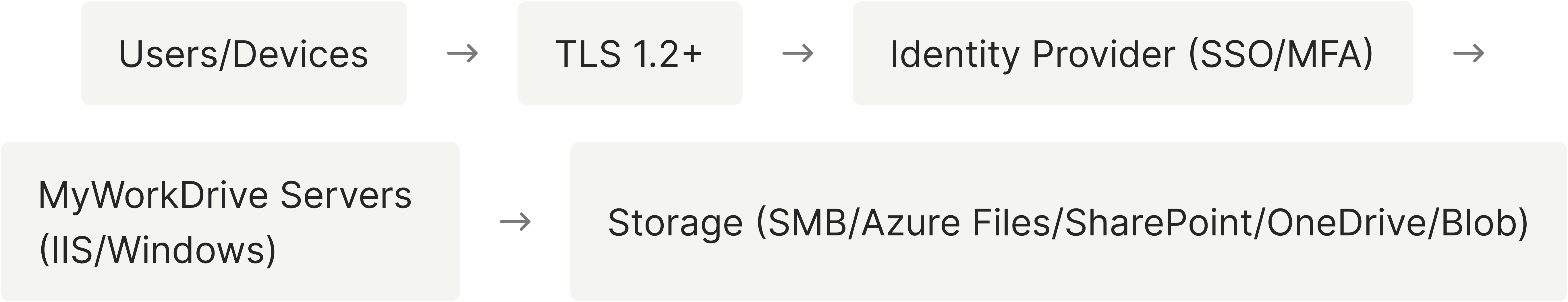
Deploy secure remote file access in days, not months — maintaining complete data sovereignty while eliminating traditional VPN overhead and security exposure.

Architecture & Security Model

Zero Trust Design

- ✓ **Single Port Access** - HTTPS port 443 only — eliminates SMB (445) and NetBIOS (139) exposure
- ✓ **TLS 1.2/1.3 Encryption** - All data transmission encrypted end-to-end
- ✓ **In-Memory Processing** - No customer data persists on application servers
- ✓ **Permission Inheritance** - Cannot elevate rights beyond existing NTFS/ SharePoint/Azure RBAC

Data Flow



Users/Devices → TLS 1.2+ → Identity Provider (SSO/MFA) →

MyWorkDrive Servers (IIS/Windows) → Storage (SMB/Azure Files/SharePoint/OneDrive/Blob)

Core Principle

Authentication and authorization remain with customer's identity provider and storage. MyWorkDrive brokers secure access only — complete data sovereignty maintained.

Deployment Architecture

Platform Requirements

- ✓ **OS** - Windows Server 2019+ (dedicated server)
- ✓ **Sizing** - 2-8 cores, 4-32GB RAM (scales from 50 to 1000+ users), 120GB disk
- ✓ **HA/Scaling** - Multiple servers behind load balancer with shared database (SQL Server, PostgreSQL, Azure SQL)

Identity Integration

Active Directory

Domain-joined server, SSO via SAML 2.0 (ADFS/Entra ID/Okta), Kerberos constrained delegation

Microsoft Entra ID

Native sign-in with OAuth/OIDC, Managed Identity support, Conditional Access enforcement

Publishing Methods

- ✓ **Cloud Web Connector** - Zero inbound firewall changes, outbound port 7844, instant deployment
- ✓ **Direct HTTPS** - Custom domain with SSL, port 443 inbound
- ✓ **Reverse Proxy/WAF** - Compatible with Entra Application Proxy, F5, nginx, NetScaler, Kemp

Storage & Client Access

Supported Storage

Windows SMB, Azure NetApp Files, Amazon FSx, Azure Files (native), Azure Blob/Data Lake Gen2, SharePoint Online, OneDrive for Business, S3-compatible storage, NFS

Access Control

All existing ACLs honored—NTFS permissions, SharePoint permissions, Azure RBAC remain authoritative

Client Options

- ✓ **Web Browser** - Full file manager with Office Online editing
- ✓ **Mapped Drive** - Windows and macOS native integration
- ✓ **Mobile Apps** - iOS and Android with offline support
- ✓ **Editing** - Browser (Office on the web), network (Office Online Server/ONLYOFFICE), or local Office via mapped drives

Deployment Overview

Four-Phase Implementation

01 **Server Installation** - Automated prerequisites, identity mode selection (AD or Entra ID — permanent)

02 **Publishing** - Configure access method (Cloud Web Connector, direct HTTPS, or reverse proxy), SSL and DNS

03 **Storage & Identity** - Add storage connections, configure delegation/app registrations, enable SSO/MFA

04 **Optional Features** - Office Online editing, DLP , device approval, SIEM integration

Required Resources - Windows/Server Admin, AD Admin (AD mode), Network/Security Admin, Azure Global Admin (Entra ID), Storage Admin, Anti-Virus Admin

Enterprise Security & Compliance

Security Features

- ✓ **MFA & SSO** - Enforced at identity provider (DUO, SAML, ADFS, Entra ID Conditional Access)
- ✓ **DLP** - Secure viewer mode with watermarking for sensitive content
- ✓ **Device Approval** - Whitelist devices for mapped drive and mobile access
- ✓ **Guest Access** - Microsoft Entra B2B integration with access reviews
- ✓ **Encryption** - TLS 1.2+ in transit; Windows/Azure encryption at rest
- ✓ **Public Sharing** - Password-protected links with expiration and audit trails

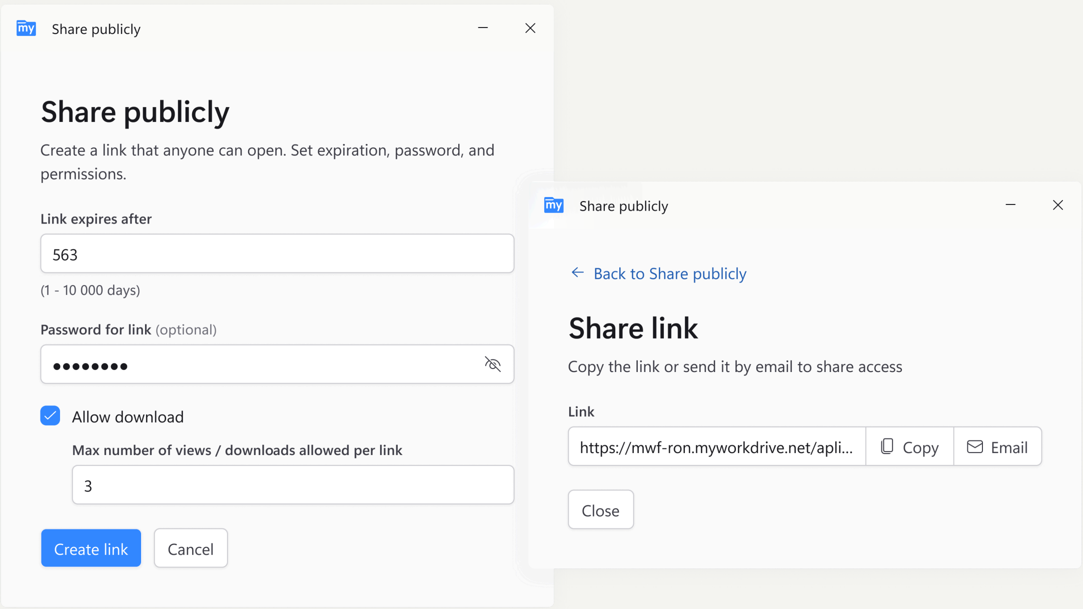
Compliance & Monitoring

01 **Standards** - HIPAA, FINRA, GDPR, FIPS compliance safeguards

02 **SIEM Integration** - Syslog export for audit logging

03 **Complete Audit Trail** - All file access, authentication, and admin actions logged

04 **Privacy by Design** - No customer data stored on MyWorkDrive servers



Share publicly

Share publicly

Create a link that anyone can open. Set expiration, password, and permissions.

Link expires after: 563

(1 - 10 000 days)

Password for link (optional): ••••••••

☑ Allow download

Max number of views / downloads allowed per link: 3

Share publicly

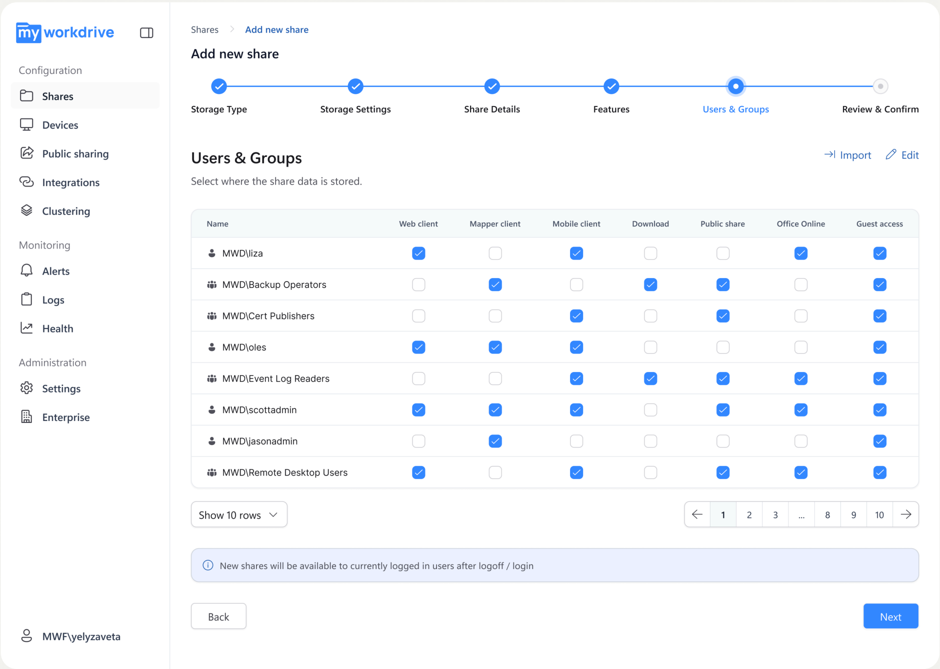
← Back to Share publicly

Share link

Copy the link or send it by email to share access

Link: https://mwf-ron.myworkdrive.net/apli...

Public Link Sharing



Add new share

Users & Groups

Select where the share data is stored.

Name	Web client	Mapper client	Mobile client	Download	Public share	Office Online	Guest access
MWD\liza	☑	□	☑	□	□	☑	☑
MWD\Backup Operators	□	☑	□	☑	☑	□	☑
MWD\Cert Publishers	□	□	☑	□	☑	□	☑
MWD\oles	☑	☑	☑	□	□	□	☑
MWD\Event Log Readers	□	□	☑	☑	☑	☑	☑
MWD\scottadmin	☑	☑	☑	□	☑	☑	☑
MWD\jasonadmin	□	☑	□	□	□	□	☑
MWD\Remote Desktop Users	☑	□	☑	□	☑	☑	☑

New shares will be available to currently logged in users after logoff / login

Guest Access

Technical Differentiators

vs. VPN

- Single port (443) vs. network exposure
- Application-level security vs. broad network access
- Zero Trust alignment

vs. Sync-and-Share

- No data migration required
- Complete data sovereignty
- Real-time access without sync delays

vs. Global File Systems

- Days to deploy vs. months-long migrations
- No migration risk
- Practical file access vs. architectural transformation

Shared Responsibility Model

Customer Owns

IdP configuration, MFA, user lifecycle, NTFS/M365/Azure permissions, network security, SIEM rules, OS patching, certificate management

MyWorkDrive Provides

Authentication integration, session handling, policy enforcement, access brokering, log generation, application updates, secure protocols

Support & Resources

Documentation | Technical Support | Security Contact

For detailed deployment procedures, refer to the Complete Deployment Guide. For comprehensive security documentation, refer to the Security Architecture Whitepaper.