2025

MyWorkDrive Complete Deployment Guide

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

Administrator's Reference for Setup and Configuration

Transform your file storage (Windows file servers, SharePoint, OneDrive, Azure Files, and Blob Storage) into a secure, modern remote access solution - we'll guide you through every step.

Welcome - Here's What We'll Accomplish Together

This guide will walk you through deploying MyWorkDrive from start to finish. My team and I have helped hundreds of organizations through this process, and we've refined it to be as smooth as possible.

The entire process takes 60-90 minutes (with the right resources available: DNS access, firewall rules, SSL certificates, Azure app creation capabilities, Anti-Virus configuration access, and either Azure Global Administrator or Domain Administrator credentials). It's common to break this into 2-3 calls with different team members to complete each step sequentially.

By the end, you'll have:

- Eliminated VPN dependency for file access
- Enabled secure access to on-premises file servers, SharePoint Online, OneDrive for Business, Azure File Shares, and Blob Storage
- Accessed files from browsers, mapped drives, and mobile devices
- Preserved all your existing permissions (NTFS, SharePoint, Azure)
- Set up Office editing both locally and through the web
- Implemented enterprise security (SSO, MFA, DLP)
- Connected audit logs to your SIEM

Important
Many features are available, but not all are relevant for every deployment. This guide focuses on what most organizations need for a successful start.

Before We Begin: Let's Get Everything Ready

Who Should Be Available

Based on typical deployments, you'll want these team members:

- **Windows/Server Admin** - To create VMs, join domains, handle IIS
- **Active Directory Admin** - For delegation rules and domain operations (if using AD mode)
- **Network/Security Admin** - DNS entries, firewall rules, SSL certificates
- **Azure Global Admin or Domain Administrator** - For app registrations and directory configuration
- **Storage Admin (if applicable)** - For Azure File Shares, Blob Storage, or file server access permissions
- **Anti-Virus Admin** - To configure exclusions
- **Project Owner** - Someone who knows which shares/users need access

Your MyWorkDrive Server

VM Sizing (we can always adjust later):

- **Start with** - 4 cores, 8GB RAM (handles ~250 concurrent users)
- **Minimum** - 2 cores, 4GB RAM
- **Maximum recommended** - 8 cores, 32GB RAM (1000+ active users)
- **Disk** - 120GB for Windows, updates, MyWorkDrive, logs, and temp files

Operating System:

- Windows Server 2019, or higher
- Must be dedicated to MyWorkDrive (no Exchange, no other IIS sites)
- Domain-joined if using Active Directory mode

Before We Begin: Let's Get Everything Ready

Network Requirements

Internet Outbound:

- Port 443 to licensing.myworkdrive.net and Microsoft cloud APIs (Firewall Settings Reference)
- Port 7844 if using Cloud Web Connector (Cloudflare)

LAN (Internal Only):

- DNS (53), LDAP/LDAPS (389/636), SMB (445) to domain controllers, file servers, and DFS
- **Important** - Clients connect only on port 443. SMB, LDAP, and DNS remain internal between MyWorkDrive server and your infrastructure

Inbound (Depends on publishing method):

- Port 443 if direct publishing or behind your proxy
- Nothing if using Cloud Web Connector (outbound only)

Critical Decision: User Directory Mode

You will choose one user directory for this server during install (cannot be changed later):

- **Active Directory** (recommended when users and groups live in on-prem AD)
  - Authenticate users with SSO via any SAML 2.0 provider (Entra ID, Okta, OneLogin, ADFS, etc.)
  - **Required** - Kerberos constrained delegation from the MyWorkDrive server to CIFS on each file server
  - If you use DFS, add both the DFS namespace servers and all back-end file servers to CIFS delegation
  - **Best for** - On-premises Windows file servers with AD-managed permissions

Before We Begin: Let's Get Everything Ready

- **Microsoft Entra ID** (recommended when either: a) storage is primarily located in Azure (Azure File Shares/Blob Storage) or b) no local AD environment exists)
  - Users sign in exclusively with Microsoft Entra ID credentials (MFA and Conditional Access supported)
  - **Native support for Azure File Shares and Azure Blob Storage** with delegated permissions
  - **For on-prem SMB shares** - Configure an SMB service account in MyWorkDrive for file access on behalf of users. No AD CIFS delegation is required
  - **Best for** - Cloud-first organizations or those using Azure storage

Have These Ready

- MyWorkDrive license key from portal.myworkdrive.com
- DNS name for your server (e.g., files.company.com)
- Service account credentials (if using Entra ID with on-prem SMB shares)
- List of initial shares to test with
  - **On-prem** - UNC paths (\\server\share)
  - **Azure** - Storage account names and container/share names
  - **SharePoint** - Site URLs and document library names
  - **OneDrive** - User accounts to test
- 2-3 test users with different permission levels

Phase 1: Installation & Initial Setup (15-30 minutes)

Step 1.1 - Prepare Your Windows Server

1. Create your VM and apply all Windows Updates
2. Join to domain (if using Active Directory mode)
3. Configure antivirus exclusions for real-time and on-access scanning (Reference: Antivirus Settings)
    - C:\Program Files\MyWorkDrive*
    - C:\ProgramData\MyWorkDrive*
    - C:\Windows\Temp\MyWorkDrive*
    - C:\inetpub\wwwroot\MyWorkDrive* (if AV inspects web directories)
4. Verify network connectivity to your file servers and domain controllers (if applicable)

Step 1.2 - Install MyWorkDrive

1. Download the latest MyWorkDrive-Setup.exe from your portal account
2. Run as Administrator - The installer will handle all prerequisites
    - Required .NET versions
    - C++ redistributables
    - IIS with necessary features
3. Choose your user directory mode when prompted (Remember: this choice is permanent for this installation)
    - Active Directory (for on-premises AD and Windows file servers)
    - Entra ID (for Azure AD/cloud-first or Azure storage)

Phase 1: Installation & Initial Setup (15-30 minutes)

Step 1.3 - Access the Admin Console

The MyWorkDrive Console is designed to be accessed from the server desktop, typically via RDP.

1. Launch MyWorkDrive shortcut from desktop
2. Open Admin Panel
3. Login with (Reference: Admin Portal Login)
    - Domain Admin account (automatically authorized)
    - Or a local administrator

Step 1.4 - Initial Configuration Wizard

The setup wizard launches on first login. Don't worry about getting everything perfect - all settings can be changed later.

2. Initial recommendations
    - Choose "Direct Connection" for publishing method (we'll configure properly in Phase 2)
    - Skip Office Online setup for now (we'll configure in Phase 4)
    - Skip file size/type limits for now
    - Skip home folder setup initially

Note: We'll add file shares in the next phase after publishing is configured.

Phase 2: Publishing Your Server - Choose Your Method (30-45 minutes)

Before adding file shares, we need to make the server accessible. This is required for SSO and Office Online editing.

Option A - Cloud Web Connector (CWC) - Easiest Start

Perfect for: Quick deployment, maximum security, no firewall changes
This is our built-in reverse proxy using Cloudflare. While you might not use it long-term, it's great for getting started quickly.

1. Settings → Cloud Web Connector → Enable
2. Note your URL: https://yourcompany.myworkdrive.net
3. That's it! No firewall rules, no certificates needed
4. Only requires outbound port 7844

Note: Cloud Web Connector (CWC) uses a MyWorkDrive-hosted domain for the public URL. Choose direct or proxy publishing if you require your own hostname branding or custom file size controls.

Reference: Cloudflare Integration

Option B - Direct HTTPS Connection

Perfect for: Full control, custom domain, traditional deployment

1. Obtain SSL certificate for your domain
2. Configure IIS:
    - Bind certificate to port 443 on the wanpath.webclient site in IIS
    - Set up your hostname
3. Create DNS record pointing to server
4. Open firewall port 443 inbound
5. Configure: TLS 1.2 minimum, TLS 1.3 preferred

Reference: SSL Certificate Setup

Phase 2: Publishing Your Server - Choose Your Method (30-45 minutes)

Option C: Behind Your Proxy/Load Balancer

Perfect for: Enterprise environments with F5, Kemp, NetScaler, nginx

Configuration requirements:

- Disable HTTP compression for the MyWorkDrive site
- Enable WebSockets end to end
- Preserve X-Forwarded-For or X-Real-IP
- TLS 1.2 minimum, TLS 1.3 preferred
- Optional but helpful: short session stickines

Note: For clustered environments (covered in Optional: Production Enhancements section), you'll want a load balancer. For POC/POV, test with direct connection first for simplicity.

Reference: Load Balancing Guide

Verify Access

From an external network:

1. Confirm the login page loads over HTTPS without warnings
2. Sign in with a test account
3. You should see an empty share list (we'll add shares next)

Phase 3: Adding Your File Shares (20-30 minutes)

Now that your server is accessible, it's time to add your storage locations. The process differs based on your user directory mode and storage type. MyWorkDrive supports:

- **On-premises Windows file servers** (SMB/CIFS shares)
- **SharePoint Online** (document libraries and sites)
- **OneDrive for Business** (individual and shared storage)
- **Azure File Shares** (cloud-native SMB)
- **Azure Blob Storage** (object storage)

For Active Directory Mode: On-Premises SMB Shares

1. Navigate to **Shares → Add Share**
2. Enter the UNC path: \\server\share
3. MyWorkDrive will automatically:
    - Import existing NTFS permissions
    - Preserve your security model
    - Map AD users/groups to access rights
4. Test the share:
    - Click "**Test Share**" in the Admin Console
    - Use "Effective Access" to verify a test user can see expected folders
5. If SSO or public sharing is enabled, the Admin Panel will check delegation:
    - Look for the "**Fix Delegation**" button if delegation is missing
    - Click to automatically configure CIFS delegation
    - Or configure manually (see Phase 4 SSO section)

I**mportant:** For DFS namespaces, add both the DFS namespace servers and all back-end file servers.

Reference: Share Configuration

Phase 3: Adding Your File Shares (20-30 minutes)

For Entra ID Mode: Azure File Shares

Perfect for: Native Azure storage with identity-based access

1. Navigate to **Integrations → Azure File Shares**
2. Configure Azure app registration:
   - Create an app registration in Azure
   - Grant appropriate permissions for Azure Files
   - Add client ID and secret to MyWorkDrive
3. Add your storage accounts:
   - Select your Azure subscription
   - Choose storage account
   - Select specific file shares to publish
4. Test the connection:
   - Verify green check in Integrations panel
   - Login as a test user and browse the share

Reference: Azure File Shares Setup

For Entra ID Mode: Azure Blob Storage

Perfect for: Object storage, unstructured data, cost-effective cloud storage

1. Navigate to **Integrations → Azure Blob Storage**
2. Configure Azure app registration (similar to File Shares)
3. Add your storage accounts:
   - Select your Azure subscription
   - Choose storage account
   - Select specific containers to publish

Phase 3: Adding Your File Shares (20-30 minutes)

4. Test the connection:
    - Verify green check in Integrations panel
    - Login as a test user and browse the share

Reference: Azure Blob Storage Setup

SharePoint Online (Works with Both AD and Entra ID Modes)

Perfect for: Document libraries, team sites, modern collaboration

1. Navigate to **Integrations → SharePoint Online**
2. Configure Azure app registration:
    - Create an app registration in Azure
    - Grant Sites.Read.All or Sites.Selected permissions
    - Add client ID and secret to MyWorkDrive
3. Add your SharePoint sites:
    - Select your tenant
    - Choose specific sites or document libraries
    - Configure permissions
4. Test the connection:
    - Verify green check in Integrations panel
    - Login as a test user and browse the share

Reference: SharePoint Online Integration

Phase 3: Adding Your File Shares (20-30 minutes)

OneDrive for Business (Works with Both AD and Entra ID Modes)

Perfect for: Individual user storage, personal files

1. Navigate to **Integrations → OneDrive for Business**
2. Configure Azure app registration:
   - Create an app registration in Azure
   - Uses Files.Read.All or delegated user permissions
   - Add client ID and secret to MyWorkDrive
3. Configure access
   - Users automatically see their own OneDrive
   - Or map specific users' OneDrive as admin
4. Test the connection:
   - Verify green check in Integrations panel
   - Login as a test user and access their OneDrive

Reference: OneDrive for Business Integration

For Entra ID Mode: On-Premises SMB Shares (via Service Account)

Perfect for: Hybrid environments with on-prem file servers

1. Create a service account:
   - Create a domain or local account on your file servers
   - Grant NTFS and share permissions for all shares users need access to
   - This account acts on behalf of all MyWorkDrive users
2. Configure in MyWorkDrive:
   - Navigate to **Settings → SMB Service Account**
   - Enter domain\username and password
   - Test connection

Phase 3: Adding Your File Shares (20-30 minutes)

3. Add shares:
   - Navigate to **Shares → Add Share**
   - Enter UNC path: \\server\share
   - MyWorkDrive will use the service account for access
4. **Important:** All users will have access based on the service account permissions. Fine-grained access control happens at the MyWorkDrive share level, not NTFS level.

Reference: SMB Service Account Configuration

Testing Your Shares

After adding shares:

1. Login as 2-3 different test users
2. Verify each user sees only their authorized content
3. Test file operations: open, edit, save
4. Use the **File Share Test Tool** in Admin Console
5. Check the **Health Dashboard** for any warnings

Phase 4: Setting Up SSO - For Active Directory User Directory (45-60 minutes)

Step 4.1: Configure SSO with Your Identity Provider

MyWorkDrive supports any SAML 2.0 compliant identity provider. Most organizations use one of these:

1. Microsoft Entra ID (Azure AD) - most common
2. Okta
3. OneLogin
4. ADFS
5. Other SAML 2.0 providers

For detailed setup instructions for your specific provider: SSO Setup Overview

Quick Setup for Entra ID (Azure AD):

In Entra ID:

1. Entra ID → Enterprise Applications → New Application
2. Search for "MyWorkDrive" (we're in the gallery!)
3. Follow the detailed configuration: SAML Single Sign-On Configuration

In MyWorkDrive Admin:

1. Enterprise tab → Enable SAML/ADFS SSO
2. Choose your identity provider type
3. Paste the App Federation Metadata URL
4. Optional: Enable "Require SSO Login" to force SSO for all users
5. Save - certificates download automatically!

Reference: Entra ID SAML Setup

Phase 4: Setting Up SSO - For Active Directory User Directory (45-60 minutes)

Step 4.2: Configure Delegation (CRITICAL for AD Mode!)

Important: Delegation is critical for Active Directory deployments with SSO. Without delegation, users see empty shares after SSO login.

Recommended Approach: Use the Admin Panel

When you add a share to MyWorkDrive with SSO or public sharing enabled, the Admin Panel will detect if delegation is missing and provide a "Fix Delegation" button directly in the share configuration window. This automated approach is recommended for most deployments.

For Complex Configurations: Manual Delegation

If you need manual control or have complex requirements:

1. Open Active Directory Users and Computers
2. Find your MyWorkDrive server's computer account
3. Properties → Delegation tab
4. Select "Trust this computer for delegation to specified services only"
5. Add your file servers:
    - Service Type: CIFS
    - Computers: Each file server
6. If using DFS: Add both the DFS namespace servers and all back-end file servers to the CIFS delegation list
7. **Important:** Allow 15-60 minutes for AD replication and Kerberos ticket renewal before testing

Phase 4: Setting Up SSO - For Active Directory User Directory (45-60 minutes)

Troubleshooting Tip: If shares are blank after SSO, delegation is not configured or not fully replicated. Check the Admin Panel for delegation warnings and use the "Fix Delegation" feature, or verify CIFS entries for all file and DFS servers manually, then wait 15-60 minutes.

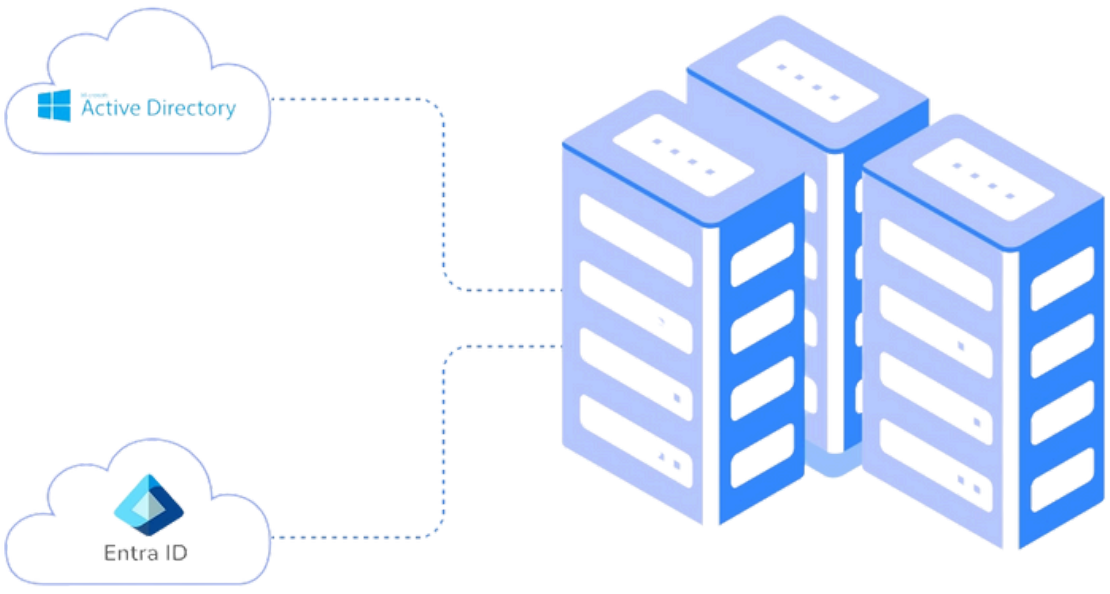
References:

- Delegation Setup
- Troubleshooting Empty Shares

For Entra ID User Directory

- In Entra ID user directory mode, no SAML configuration is required. Users authenticate with Microsoft directly and your Conditional Access policies apply automatically.

You're done with SSO setup! - Authentication happens directly through Microsoft



Phase 5: Office Online Editing Setup - Understanding Your Options (30-45 minutes)

OneDrive Mode (Recommended for Initial Deployment)

Perfect for: Quick setup, individual user workflows, POC/POV
Uses individual users' OneDrive for staging. We offer a hosted app option for quick setup with minimal configuration.

Setup:

1. Navigate to **Integrations → Office Online (OneDrive)**
2. Follow the OneDrive integration wizard in the Admin Panel
3. Users can now edit Office files directly in their browser

SharePoint Service Mode (Advanced - Contact Support)

Perfect for: Enterprise deployments requiring advanced control and team co-authoring
This is the most complex configuration we offer.

For production deployments requiring SharePoint Service Mode, we **strongly recommend working with our support team to ensure proper setup.**

The Process:

1. User clicks "Edit" on an Office file from your SMB share
2. File is locked on the SMB share
3. Copy temporarily moves to SharePoint for editing
4. Changes sync back periodically
5. When done, file returns to SMB and unlocks
6. If user abandons edit, file unlocks after 15 minutes

Co-authoring: Multiple users can edit simultaneously using Office 365 share links. File stays locked on SMB until all editors finish. Co-authoring requires all editors to use Office Online. Mixed desktop and online co-editing is not supported in this mode.

Phase 5: Office Online Editing Setup - Understanding Your Options (30-45 minutes)

Reference: SharePoint Service Mode Setup (Contact support for implementation assistance)

Testing Office Workflows

1. Open an Office document in browser
2. Make edits and save changes
3. Verify changes persist
4. Test co-authoring with two users (if using SharePoint mode)
5. Verify file locking on source storage (SMB/Azure)

Phase 6: Security & Advanced Features (30 minutes)

Data Leak Prevention (DLP) - Control how users interact with sensitive files

Global Settings (Settings → Advanced → DLP):

- Block downloads while allowing viewing
- Add watermarks (username, timestamp, custom text)
- Disable clipboard operations
- Prevent printing

Per-Share Controls (Shares → Edit → DLP):

- Marketing: View with watermarks
- HR: View only, no downloads
- Finance: Full audit trail

I**mportant:** DLP-enabled shares require the Secure Driver for desktop client access. The secure driver is not installed by default. If a share has DLP enabled and the secure driver is not installed, the share will not load correctly in the desktop client. Plan to deploy the secure driver when enabling DLP for mapped drive users.

Reference: DLP Configuration

Device Approval

Control which devices can access via mapped drive and mobile:

1. Start in **Monitor Mode** - logs devices without blocking
2. Review after a week - see all devices that connected
3. Switch to **Enforce** - only approved devices allowed

Reference: Device Approval

Syslog Integration

Send logs to your SIEM for compliance and monitoring:

- Settings → Syslog Integration → Configure your SIEM endpoint

Reference: Syslog Setup

Phase 7: Client Deployment (15-30 minutes)

Windows Mapped Drive Client

For POC/POV: Simply download the EXE installer, install, and share the URL with users.

For Production Deployment: The standard client installer is an EXE. For silent deployment:

batch
MyWorkDrive-Windows-Client.exe /S /SERVERURL=https://files.company.com /MAPATSTARTUP=1 /REMEMBERME=1 /OFFICEONLINE=1

Note: If you specifically need an MSI installer for your deployment tools, contact support for extraction instructions. Verify property names in the Desktop Clients Admin guide for your exact client build.

Mac Client

Deploy config.xml to users' Documents folder for zero-touch setup:

xml
<?xml version="1.0" encoding="UTF-8"?>
<loginConfig>
<url>https://files.company.com</url>
 <rememberMe>1</rememberMe>
 <mapAtStartup>1</mapAtStartup>
</loginConfig>

You may also set the server URL via configuration profile if preferred.

Mobile Apps

Deploy via MDM or app stores. Remember to approve devices if enforcement is enabled.

Phase 8: Validation & Go-Live

At This Point, You Have a Functional MyWorkDrive Server!

For POC/POV: Simply download the EXE installer, install, and share the URL with users.

Users can now:

- Log in via browser with SSO (or Microsoft credentials in Entra ID mode)
- Access their authorized shares across all storage types (on-prem, SharePoint, OneDrive, Azure Files, Blob Storage)
- Edit Office documents online via OneDrive or SharePoint Service Mode
- Use mapped drives and mobile apps
- Access files securely without VPN

Testing Checklist

Core Functions:

- SSO login works without password (or Microsoft login for Entra ID mode)
- Users see only their authorized shares
- Files open in Office (web and local)
- Mapped drive appears correctly
- Open the **Health Dashboard** in the Admin Console and confirm all checks are green
- Use the **File Share Test Tool** and **Effective Access** to validate pilot users

Phase 8: Validation & Go-Live

Security:

Core Functions:

- DLP watermarks display properly (if enabled)
- Download blocking works on restricted shares (if enabled)
- Audit logs capture events
- TLS 1.2 minimum, TLS 1.3 preferred
- No inbound SMB, LDAP, or DNS from the internet
- Files are not synced to endpoints by the mapped drive client (files open in memory, not stored locally)

Performance Baseline:

- Upload/download speeds
- Office online open times
- Page load performance

Optional: Production Enhancements

High Availability / Clustering

Not required for POC/POV, but consider for production

Three components to clustering:

1. **Load Balancing** - Use your existing solution (F5, Kemp, NetScaler, nginx)
   - Session persistence recommended to reduce reconnect churn, especially for WebSockets and large uploads
   - If all nodes share the same locks and sessions database and your proxy fully supports WebSockets, affinity is optional
2. **Shared Configuration** - Optional, has pros/cons depending on your environment
2. **SQL Database** - Provides multiple benefits:
   - Office co-editing across nodes
   - Public sharing links stored centrally
   - Improved performance
   - Supported: SQL Express, PostgreSQL, Azure SQL

Reference: Clustering Guide

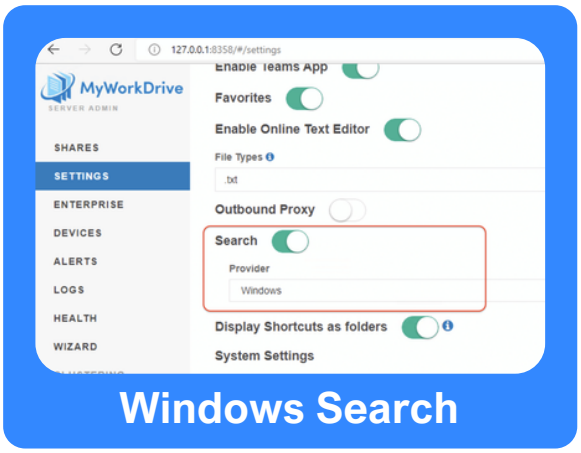
Production Hardening Checklist

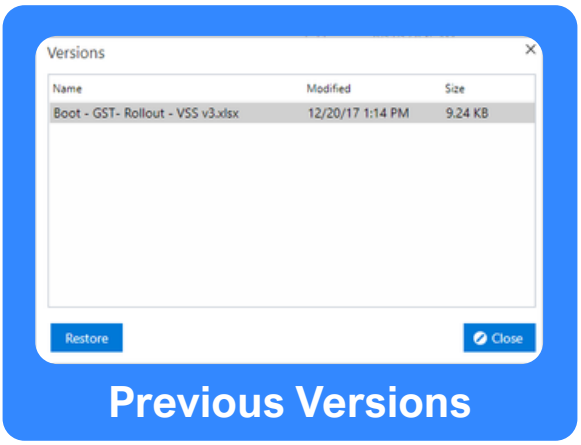
- TLS settings configured (1.2 minimum, 1.3 preferred)
- Cipher suites hardened per your security policy
- HTTP compression disabled on reverse proxy/WAF
- Log retention configured
- SIEM forwarding active
- MyWorkDrive configuration backed up
- Second node deployment planned (if using HA)
- Certificate renewal scheduled

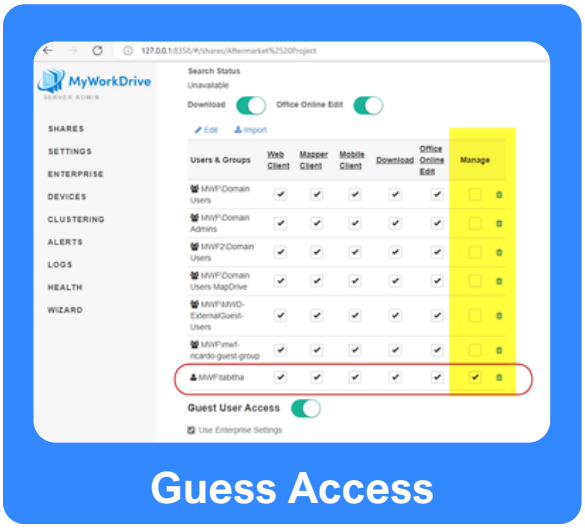
Optional: Production Enhancements

Additional Features to Explore

- **Public Link Sharing** - Secure external file sharing with passwords and expiration
- **Azure B2B Guest Access** - External collaboration through Entra ID
- **Previous Versions** - Shadow copy integration
- **Windows Search** - Full-text search integration







How We Support You

During Deployment

We're happy to guide you through this process on a call or series of calls. The entire setup typically takes 60-90 minutes when you have the necessary resources available. It's common to break this into 2-3 calls with different team members.

Resources Available

- **Support Email:** support@myworkdrive.com
- **Help Desk:** MyWorkDrive Support Portal
- **Hours:** Monday-Friday, 6 AM - 6 PM PST
- **KB Articles: Full documentation at www.myworkdrive.com/support**

Common Questions We Get

Q: What ports do clients connect on?
A: Only port 443 (HTTPS). No SMB ports (445, 139) are exposed to the internet - all SMB communication happens server-side on your LAN.

Q: How is this different from sync and share?
A: Your files stay exactly where they are - on-prem servers, SharePoint, OneDrive, Azure Files, or Blob Storage. We don't sync or copy files to client devices - everything is accessed real-time and files open in memory, not stored locally. You maintain complete control.

Q: What about compliance (HIPAA, GDPR, etc.)?
A: Since data stays in your chosen storage location under your control (your servers, SharePoint, OneDrive, Azure), you maintain compliance.

We support:

- **Public sector:** Deployed successfully in FedRAMP-authorized environments
- **Healthcare:** HIPAA compliance
- **Cryptography:** Supports FIPS-aligned operation when Windows is configured for FIPS mode

How We Support You

Q: Can I use multiple storage types?
A: Yes! You can mix and match storage types. Many customers use MyWorkDrive to access legacy on-prem file servers alongside SharePoint Online, OneDrive for Business, and Azure storage - all from a single unified interface.

What Makes MyWorkDrive Unique

- **No VPN needed** - Access files over HTTPS only
- **No data migration** - Files stay where they are (on-prem, SharePoint, OneDrive, or Azure)
- **No sync to endpoints** - Files open in memory, not stored locally
- **No commonly exploited ports** - Only 443 or outbound 7844
- **No vendor lock-in** - Your files, your storage, your control
- **Unified access -** Single interface for Windows file servers, SharePoint, OneDrive, Azure Files, and Blob Storage

15-Minute Smoke Test Script

After initial setup, run through this quick validation:

1. **External Access (2 min)**
   - Browse to public URL from external network
   - Verify HTTPS with no certificate warnings
   - Confirm login page loads
2. **Authentication (3 min)**
   - Test SSO login (or Microsoft login for Entra ID mode)
   - Verify MFA triggers (if configured)
   - Confirm user lands on share list
3. **File Operations (5 min)**
   - Browse into test share
   - Open a document in browser
   - Edit and save changes
   - Verify changes persist on source storage
4. **Client Access (3 min)**
   - Install mapped drive client
   - Connect with test user
   - Open file from mapped drive
5. **Security Check (2 min)**
   - Test DLP share (if configured)
   - Verify watermarks appear
   - Confirm download is blocked

Expected Result: All steps complete without errors

Ready to Start?

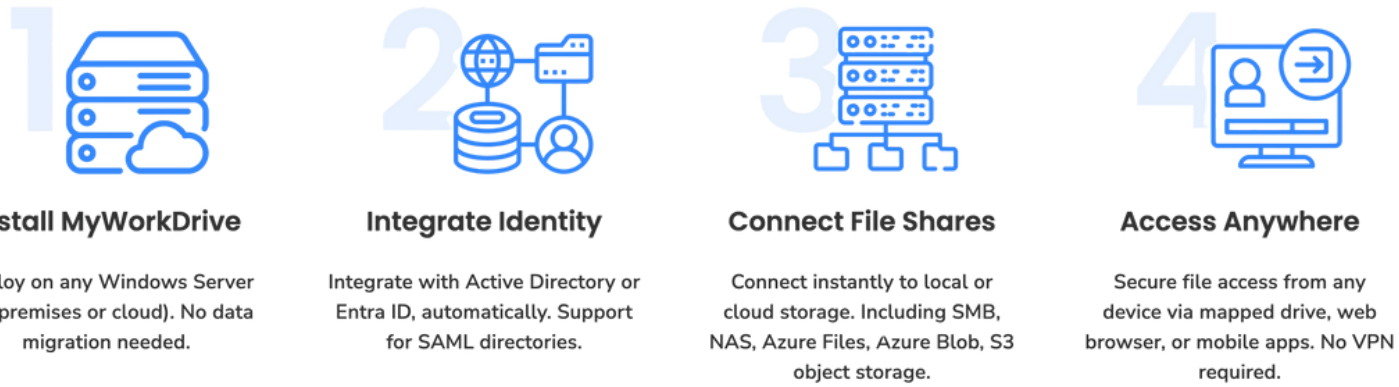
You now have everything needed to deploy MyWorkDrive successfully. Remember:

1. **Start simple** - Get basic access working first
2. **Add features gradually** - Publishing, then shares, then SSO, then Office, then DLP
3. **Test with small groups** - IT first, then pilot users
4. **We're here to help** - Don't hesitate to reach out

Next Steps:

1. Schedule your deployment call with our team
2. Ensure your team members are available
3. Have your resources ready:
   - DNS, certificates, Azure access
   - List of shares to publish (UNC paths, SharePoint sites, OneDrive users, or Azure storage details)
   - Test user accounts
4. Plan for 60-90 minutes of focused setup time

Let us know when you're ready to begin or if you have any questions after reviewing this guide!



Appendix: Roles and Responsibilities

PHASE	REQUIRED TEAM MEMBER	TASKS
SERVER PREP	Windows Admin	Create VM, join domain, configure AV exclusions
INSTALLATION	Windows Admin	Run installer, complete wizard
PUBLISHING	Network Admin	DNS, SSL certificates, firewall rules
SHARE SETUP	Storage Admin + AD Admin (if AD mode)	Add file shares, Azure storage, or configure service account
SSO SETUP	AD Admin + Azure Admin	Configure SSO provider, delegation (if AD mode)
OFFICE INTEGRATION	Azure Admin	Configure OneDrive or SharePoint (with support)
SECURITY	Security Admin	Configure DLP, device approval, SIEM
CLIENT DEPLOYMENT	Desktop Admin	Deploy via GPO/MDM
TESTING	Project Owner	Validate workflows, user acceptance

Appendix: Storage Options Quick Reference

STORAGE TYPE	BEST FOR	USER DIRECTORY MODE	KEY REQUIERMENTS
ON-PREM SMB (WITH DELEGATION)	Traditional Windows file servers	Active Directory	CIFS delegation to file servers
ON-PREM SMB (SERVICE ACCOUNT)	Hybrid environments without AD	Entra ID	Service account with file permissions
SHAREPOINT ONLINE	Document libraries, team collaboration	Both (AD or Entra ID)	Azure app registration with Sites permissions
ONEDRIVE FOR BUSINESS	Individual user storage	Both (AD or Entra ID)	Azure app registration with Files permissions
AZURE FILE SHARES	Cloud-native file storage	Entra ID (recommended)	Azure app registration
AZURE BLOB STORAGE	Object storage, unstructured data	Entra ID (recommended)	Azure app registration

This guide reflects MyWorkDrive best practices and is regularly updated. For the latest features and updates, always check www.myworkdrive.com/support