

2025

MyWorkDrive Security Architecture



Executive Context

Enterprises are transitioning from network-level to application-level access models. Traditional VPN architectures for file access create unnecessary lateral movement exposure, increase operational overhead, and conflict with zero trust principles. Application-level access reduces the attack surface while preserving data sovereignty and existing identity controls.

MyWorkDrive follows that path. The application brokers VPN-free access to existing repositories while identity, policy, and audit remain with your identity provider. Organizations gain faster rollout, lower change risk, and alignment with least privileged access and data-minimization principles without large-scale migrations.

Executive Summary

What MyWorkDrive provides

Users get secure access to files where they already live: Windows SMB shares, cloud-managed SMB such as Azure NetApp Files and Amazon FSx for NetApp ONTAP, Azure Files, SharePoint and OneDrive, and Azure Blob with Data Lake Gen2. No data migration into a proprietary repository. Customer files never leave their environment, maintaining complete data sovereignty.

What remains under your control

Authentication flows through Active Directory with optional SAML SSO or through Microsoft Entra ID using native sign-in. MFA and Conditional Access continue to enforce at your identity provider. Authorization honors your NTFS and share permissions and your Microsoft 365 site and library ACLs. MyWorkDrive cannot elevate rights and can only restrict further by policy.

Executive Summary

How the security model works

All client connections use only port 443 (HTTPS), eliminating exposure of commonly compromised ports such as 445 (SMB), 139 (NetBIOS), and 53 (DNS) to external clients. All client and API paths use TLS 1.2 or higher, with TLS 1.3 preferred where supported. Browser editing with Office on the web uses temporary staging in your OneDrive or SharePoint tenant, then writes back on save with cleanup. File contents are processed in memory only and never written to disk on MyWorkDrive application servers. Temporary artifacts and session state remain in memory or short-lived tenant staging with automated cleanup. No customer file content persists on application servers. Optional controls include DLP with watermarking, device approval for mapped drive and mobile clients, Microsoft Entra B2B guest access, and comprehensive logging for SIEM ingestion. Managed Identity is supported for eligible Azure services.

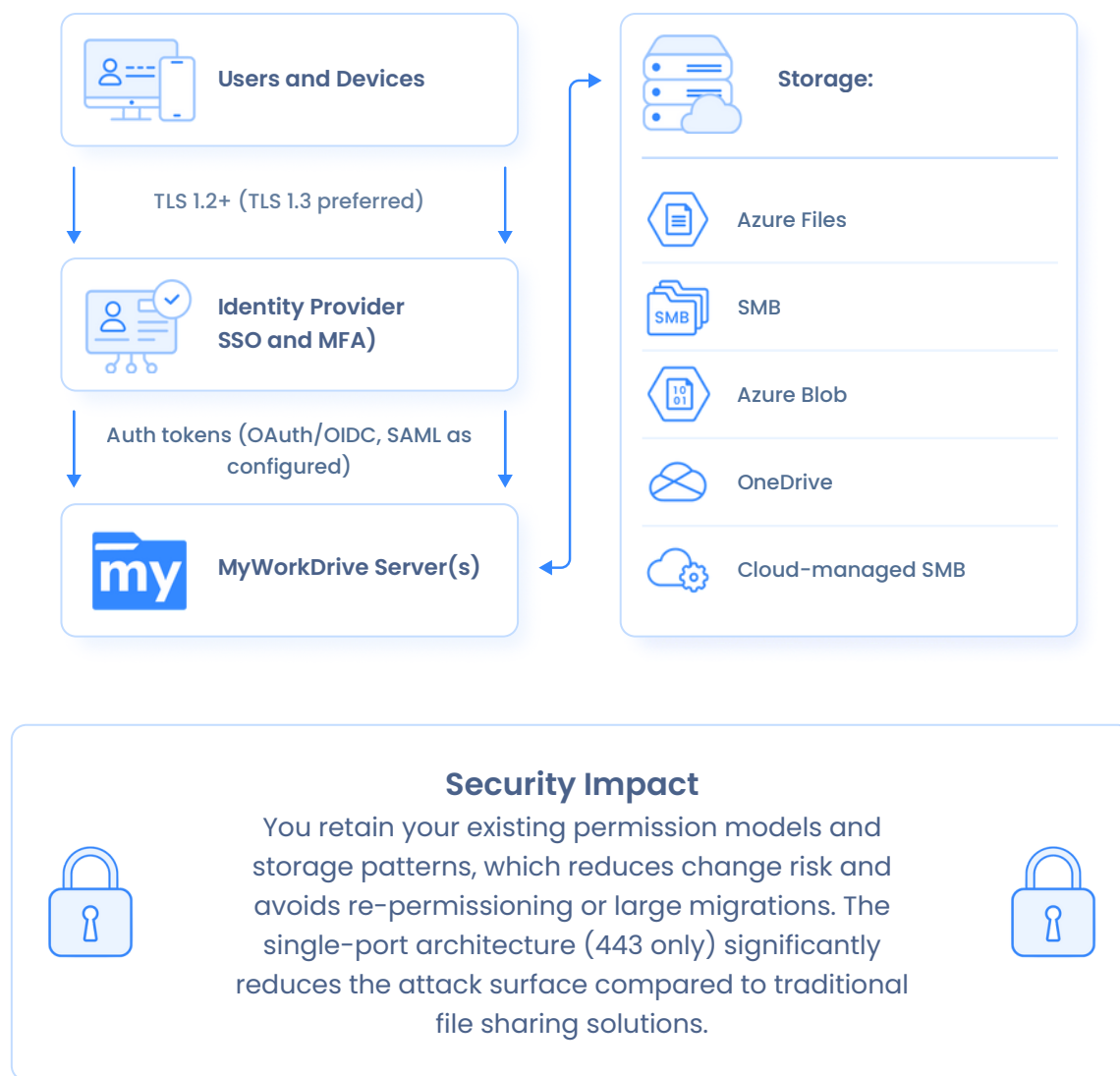
Where it fits

Clients connect over HTTPS to Windows Server hosts running IIS. For production environments requiring scalability or redundancy, you can optionally deploy multiple servers behind a load balancer with a shared database (SQL Server or PostgreSQL) for session coordination and file locks. You can publish directly on 443, through a reverse proxy or WAF, through Microsoft Entra Application Proxy, or via an outbound-only Cloud Web Connector using Cloudflare tunnels on port 7844 with no inbound firewall changes required.

Architecture and Trust Boundaries

Security begins with clear boundaries. Identity stays with your provider. Authorization stays with your storage. MyWorkDrive sits between them as a secure translator that enforces your policies without moving your files.

The application tier can scale horizontally when needed. File contents do not persist on MyWorkDrive servers and are processed in memory only as a TLS-proxied pass-through between client and storage; no file contents are written to disk. Session details remain in server memory. For multi-server deployments, an optional shared database stores what is needed to coordinate across nodes, such as compact session references and file locks.



Identity, Authentication, and MFA

Authentication belongs to your identity provider. MyWorkDrive does not store passwords and is not a second identity system.

Active Directory

Domain controllers continue to authenticate users. For browser SSO, add SAML through ADFS or a compatible provider. Enforce MFA at the IdP. Use Kerberos constrained delegation to validate access without broad privileges, scoped to required SPNs only. Avoid unconstrained delegation.

Critical Requirements for Active Directory Integration:

- ✓ Users must be able to read their own attributes on the domain (username/UPN lookup, account status, group membership)
- ✓ Domain-joined MyWorkDrive servers must have appropriate delegation rights configured
- ✓ Allow 15-60 minutes for delegation changes to propagate throughout the domain

Microsoft Entra ID

Users sign in with Microsoft credentials using the native flow. Conditional Access and MFA policies apply automatically because the IdP owns them. Clients use modern OAuth 2.0 flows with PKCE.

Private and isolated networks

Air-gapped designs are possible depending on the IdP and editor choice. Active Directory mode offers the broadest flexibility for isolated environments. Note that MyWorkDrive servers may require periodic communication with licensing.myworkdrive.net for license validation.



Security Impact

Keeping identity centralized preserves audit trails, avoids duplicated policy, and simplifies reviews.



Authorization and Least Privileged Access

Existing permissions remain authoritative. MyWorkDrive can only restrict further through policy.

SMB repositories

NTFS and share permissions control access. Access-Based Enumeration hides folders users cannot access. MyWorkDrive honors these rules without modification.

Microsoft 365 repositories

Tenant, site, and library ACLs govern access. Microsoft Graph calls request the least privilege needed, including the Sites.Selected scope where available with per-site consent.

Additional restrictions you can apply

Per share, user, or group you can allow or block client types, control public link creation, block downloads, and enable or disable Office on the web. Administrative policy can only subtract capabilities.

Entra ID with SMB

When Entra ID users reach SMB shares, a service account may perform SMB operations. Discovery and access still follow per-share configuration and Access-Based Enumeration.



Security Impact

Auditors expect least privileged access by design. You keep your ACLs and group models, and MyWorkDrive adds policy controls without creating a second permissions universe.




Storage Connectivity and Hybrid Visibility

One access layer, multiple repositories. Users work the same way whether data is on premises or in the cloud.


STORAGE TYPE	HOW IT CONNECTS	WHAT CONTROLS ACCESS	WHEN IT FITS BEST
WINDOWS SMB SHARES	UNC paths over LAN or through gateways	NTFS and share permissions with ABE	Departmental shares, home drives
CLOUD-MANAGED SMB (ANF, FSX FOR NETAPP ONTAP)	SMB endpoints	NTFS and share permissions with ABE	Lift-and-shift, performance SMB
AZURE FILES	SMB or REST	Connection strings or Managed Identity	Cloud-native file shares
SHAREPOINT AND ONEDRIVE	Microsoft Graph APIs	Tenant policy and site ACLs	Collaboration and content
AZURE BLOB (DATA LAKE GEN2)	REST with hierarchical namespace	RBAC and POSIX-style ACLs	Archives and analytic datasets

DFS Namespaces are supported for SMB routing. Windows Search and Previous Versions require direct Windows share connections. For disaster recovery, deploy a MyWorkDrive instance in each site rather than stretching one cluster across distance.



Security Impact

You standardize access without refactoring storage, which keeps cost, performance, and residency choices in your hands.



Publication and Network Patterns

Choose a publication pattern that aligns with your enterprise standards. Each option uses TLS 1.2 or higher, with TLS 1.3 preferred where supported.

- ① **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.
- ② **Reverse proxy or WAF** - MyWorkDrive sits behind your proxy which applies filters and monitoring. Maintain session persistence for multi-server deployments so a user returns to the same node. Disable HTTP compression for MyWorkDrive paths to reduce exposure to compression-based attacks. Important: TLS should terminate on the MyWorkDrive server, not on the proxy. Pass-through TLS or re-encryption is recommended to maintain end-to-end security.
- ③ **Microsoft Entra Application Proxy** - If inbound ports are not allowed, publish through the service. Pre-authentication and Conditional Access evaluate before requests reach MyWorkDrive.
- ④ **Cloud Web Connector** - Uses outbound-only Cloudflare Tunnels on port 7844. No inbound firewall changes required. This option provides maximum firewall simplicity while maintaining enterprise-grade security through Cloudflare's global network.

Publication and Network Patterns

Ports at a glance

Client connections: Inbound 443 ONLY for direct publication or your proxy listener.

MyWorkDrive clients never connect to commonly compromised ports like 445, 139, or 53.

Outbound 7844 for Cloud Web Connector, standard AD or LDAP for AD mode, and 443 to Microsoft Graph for Entra ID integrations. Outbound 443 to licensing.myworkdrive.net for license validation.

Multi-server deployments

For organizations requiring additional capacity or redundancy, multiple servers can be deployed behind a load balancer. Session persistence is required to ensure users return to the same node during active sessions. A shared database (SQL Server or PostgreSQL) coordinates sessions and file locks across nodes. Note that if a server becomes unavailable, users connected to that server will need to reconnect and establish a new session on another node.

Security Impact



Security teams can adopt the pattern that best aligns with enterprise controls without sacrificing usability. The single-port client architecture significantly reduces firewall complexity and attack surface.



Data Flows and Editing Modes



A typical request sequence: the user authenticates at the IdP, establishes an HTTPS session to MyWorkDrive, per-share policies are evaluated, repository ACLs are checked, and the service brokers access to the storage that already contains the files. Editing options balance collaboration and residency:

- ✓ **Office on the web** - Edits run in Microsoft's cloud. Files stage temporarily in OneDrive or SharePoint within your tenant and write back on save. Coauthoring is available.
Note: Office on the web does not support strict no-download/no-print enforcement through MyWorkDrive controls. For strictly view-only enforcement, consider enabling Data Leak Prevention
- ✓ **Desktop Office via mapped drive** - Edits run on the workstation against SMB. File locking prevents conflicts.
- ✓ **Open in Local Office from the web** - Opens locally from a web view. When DLP view-only is enabled, supported file types open in secure viewers rather than native apps.
- ✓ **Office Online Server (OOS)** - Edits run on infrastructure you host. Content stays on your network. Coauthoring is available.
- ✓ **ONLYOFFICE** - Edits run on infrastructure you host. Open source preference. Coauthoring is available.

SharePoint Service Mode for Office Online Editing

When a user requests to edit a file from an SMB share, the file is locked on SMB, a copy is placed on the configured SharePoint site, and an Office 365 edit session is opened. The file is periodically written back to the original share. When editing completes, the file is removed from SharePoint and unlocked on SMB. For abandoned sessions, files are locked for 15 minutes to facilitate user rejoining, then automatically cleaned up.

Locking is handled by SMB on SMB shares. For non-SMB repositories such as SharePoint or Azure Blob, MyWorkDrive coordinates locks internally. Administrators can view active locks and sessions in the console.

**Security Impact**

You can meet strict residency controls or collaboration needs without introducing a second document system.

Data Protection Controls

Controls should fit how people work.

- ✓ **DLP view-only** - Users can view files without downloading, copying, or printing. Dynamic watermarking adds user details and optional text. Clipboard blocking applies in secure viewers, including mapped drive secure view for supported file types.
- ✓ **Public links** - Apply passwords, expirations, and separate view versus download permissions. Administrative approval is available. Disable for sensitive shares by default. All activity is logged.
- ✓ **Device approval** - Control which devices can access via mapped drive and mobile. Start in monitor mode to build an allowlist, then enforce approvals. Apply different rules to web, mapped drive, and mobile.
- ✓ **Microsoft Entra B2B guests** - Bring guests in through Entra ID so Conditional Access and access reviews apply. Guest activity appears in your central logs.



Security Impact

Effective controls reduce exceptions and shadow IT while preserving productivity.



Keys, Secrets, & Managed Identity

SSL certificates are customer-owned and stored in the Windows Certificate Store. Rotate certificates under your enterprise lifecycle.

For Microsoft 365, request only the scopes required. Where supported, use Sites.Selected for SharePoint with per-site consent. In Azure, Managed Identity can be used for eligible services so secrets do not need to be stored on disk. Store any remaining secrets in your enterprise vault and rotate per policy.

Browser editing creates temporary items in a staging location. These are removed on commit or when the session ends. File contents do not persist on application servers. Security Impact: Minimizing secrets and keeping certificates under your control reduces operational and compliance risk.



Security Impact

Minimizing secrets and keeping certificates under your control reduces operational and compliance risk.



Logging, Alerting, and SIEM

MyWorkDrive records events needed for investigations and audits: authentication and authorization decisions, file operations, public link lifecycle, administrative changes, and device approvals.

Export structured logs to your SIEM over Syslog. Choose verbosity from high-level errors to detailed debug. Email notifications use your SMTP service with consolidation to avoid alert floods. Include fields such as user, source IP, device identifier where available, share, path, operation, result, and bytes transferred.

Suggested thresholds include mass downloads, sudden public link creation on sensitive shares, unexpected policy changes, repeated authentication failures, and unusual device requests.



Security Impact

Good visibility shortens incident timelines and simplifies audits.



Cryptography and TLS Posture

Require TLS 1.2 or higher and prefer TLS 1.3 where supported. Prefer ECDHE key exchange with AES-GCM encryption. Redirect HTTP to HTTPS. Disable SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1.

Set security headers: HSTS, X-Content-Type-Options, Referrer-Policy, a restrictive Content-Security-Policy with frame-ancestors denying framing, and secure cookies.

For regulated environments, FIPS-validated cryptographic components are available. MyWorkDrive has been issued FIPS 186-4 RSA validation certificate #3018 from NIST. Windows FIPS mode is supported.



Security Impact

Clear and current transport standards reduce audit time and eliminate legacy protocol risk.



Availability, Performance, & Scale

For organizations requiring additional capacity, multiple nodes can be deployed behind a load balancer with session persistence. A shared database coordinates sessions and file locks across nodes. Keep that database available if you enable coauthoring or public links in a multi-server environment.

Important: In multi-server deployments, if a server becomes unavailable, users connected to that server will be disconnected and will need to reconnect. Their session will automatically establish on an available server.

Performance depends on storage latency between app servers and repositories, network paths and bandwidth, TLS termination capacity, file size and type, and the frequency of secure viewer use with DLP. Place application servers network-close to SMB storage. Latency, more than raw bandwidth, is the primary driver of perceived performance.

A practical pilot starts with a single server at 4 vCPU and 16 GB RAM, SSD for the OS and temporary paths. Maximum recommended sizing is 8 cores and 32GB RAM supporting up to 1000 active users. For multi-server deployments, a highly available SQL Server or PostgreSQL instance is required.

Scale by adding nodes when CPU becomes TLS-bound or connection queues rise. Monitor CPU utilization, TLS handshakes, active sessions, request queues, and SMB round-trip time. If you use cloud editing, account for Microsoft egress charges.



Security Impact

Sizing and placement have more effect on user experience than any single setting.



Threat Model and Mitigations

- ✓ **Credential compromise or token replay** - : Enforce MFA and Conditional Access at the IdP, require strong TLS, and set appropriate session timeouts.
- ✓ **Insider exfiltration with valid access** - Apply DLP view-only with watermarking, require device approval, alert on mass downloads, and govern public links with expiration and passwords.
- ✓ **Lateral movement over SMB** - Enforce NTFS least privileged access and Access-Based Enumeration, configure constrained delegation where needed, and segment networks.
- ✓ **Stale guests or unmanaged sharing** - Use Microsoft Entra B2B access reviews, require link expirations, and optionally gate external sharing with administrative approval.
- ✓ **Data residency constraints** - Keep edits on network with OOS or ONLYOFFICE. If using Office on the web, rely on automated cleanup of staging artifacts after save.
- ✓ **Supply chain and platform hygiene** - Run servers on supported Windows versions, apply cumulative updates, and review IIS module inventories quarterly. Configure antivirus exclusions as recommended by your security vendor to prevent interference with MyWorkDrive operations.



Security Impact

Mitigations map cleanly to the most common file access risks.



Shared Responsibility Model

AREA	YOU OWN	MYWORKDRIVE PROVIDES
IDENTITY & ACCESS	IdP configuration, MFA, Conditional Access, user lifecycle	Authentication integration and session handling
AUTHORIZATION	NTFS and share permissions, Microsoft 365 ACLs, groups	Policy enforcement and access brokering
STORAGE SECURITY	File system ACLs, SharePoint permissions, Azure RBAC	Permission evaluation and API security
DATA CLASSIFICATION	Policies and labels	Enforcement of configured controls
NETWORK SECURITY	Firewalls, segmentation, private connectivity	TLS and secure protocols

Shared Responsibility Model

AREA	YOU OWN	MYWORKDRIVE PROVIDES
MONITORING AND SIEM	SIEM rules and response	Log generation and Syslog export
COMPLIANCE	Program, evidence, and audits	Complete audit logs and compliance features
INFRASTRUCTURE	OS patching, certificate management, database care, patching cadence	Application updates and configuration integrity
DLP POLICY	Business rules and handling standards	Technical enforcement and secure viewers
DEVICE GOVERNANCE	Approval policies and device standards	Fingerprinting and enforcement workflow

Compliance and Attestations

How MyWorkDrive supports HIPAA

PHI remains in customer storage or tenant. TLS 1.2+ on all communications, least privileged access, and comprehensive audit logs. A Business Associate Agreement can be executed on request.

How MyWorkDrive supports CMMC

Alignment with relevant control families such as AC, AU, IA, and SC through IdP-owned MFA, role-based access, detailed audit trails, and encrypted communications. Detailed mappings are available on request.

How MyWorkDrive supports GDPR

Data minimization since file content does not reside on application servers, portability since files remain in your repositories, complete audit trails, privacy by design, and policy controls for cross-border transfer.

How MyWorkDrive supports FedRAMP

MyWorkDrive's architecture supports FedRAMP requirements through data sovereignty, strong encryption, comprehensive audit logging, and ability to deploy in government-approved environments. The self-hosted model ensures government data never leaves approved infrastructure.

Data Privacy Framework

Privacy controls and residency preserved by architecture. For detailed mappings and evidence, refer to the separate compliance documentation.

Operational Hardening Checklist

Transport and TLS

- ✓ Require TLS 1.2 or higher; prefer TLS 1.3 where supported
- ✓ Disable SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1
- ✓ Prefer ECDHE with AES-GCM
- ✓ Configure HSTS and secure cookies; set Referrer-Policy, X-Content-Type-Options, and a restrictive CSP with frame-ancestors
- ✓ Redirect HTTP to HTTPS

Operational Hardening Checklist

Identity

- ✓ Validate MFA and Conditional Access for MyWorkDrive
- ✓ Configure constrained delegation for AD mode where required
- ✓ Test SSO across web, mapped drive, and mobile
- ✓ Set session timeouts aligned to policy
- ✓ Validate de-provisioning removes access promptly
- ✓ Terminate TLS on MyWorkDrive servers, not on proxies

SMB and permissions

- ✓ Enable Access-Based Enumeration
- ✓ Verify inheritance and nested group resolution
- ✓ Confirm users only see authorized content

Editors and DLP

- ✓ Choose editors to match residency and collaboration needs
- ✓ Verify Office on the web staging cleanup in your tenant
- ✓ Test view-only, watermarking, and clipboard blocking with DLP

External sharing and devices

- ✓ Set link expirations and passwords
- ✓ Consider administrative gating for sensitive areas
- ✓ Start device approval in monitor mode, then enforce
- ✓ Enforce minimum client versions

Operational Hardening Checklist

Infrastructure and Environment

- ✓ Configure antivirus exclusions as per recommendations
- ✓ Ensure outbound connectivity to licensing.myworkdrive.net
- ✓ Verify firewall rules permit only required ports (443 inbound, or 7844 outbound for Cloud Web Connector)
- ✓ Domain-join MyWorkDrive servers for AD integration

Observability

- ✓ Export Syslog to your SIEM
- ✓ Test alert thresholds for mass downloads and policy changes
- ✓ Confirm retention and archive settings

Continuity

- ✓ Back up configuration and sessions/locks database (if applicable)
- ✓ Test restoration procedures and document RTO and RPO
- ✓ For multi-server deployments, validate session persistence
- ✓ Keep application servers network-close to SMB storage

Appendices

Appendix A. Port and publication reference

METHOD	INBOUND PORTS	OUTBOUND REQUIREMENTS	SESSION PERSISTENCE	BEST FOR
DIRECT HTTPS	443	AD or LDAP, Microsoft Graph as applicable	Not required for single server	Simple deployments
REVERSE PROXY OR WAF	Proxy listener ports	Same as above	Required for multi-server	Security-focused environments
MICROSOFT ENTRA APPLICATION PROXY	None	443 to Entra endpoints	Handled by service	Entra SSO environments without inbound ports
CLOUD WEB CONNECTOR	None	7844 to Cloudflare	Handled by connector	Maximum firewall simplicity

Appendices

Appendix B. Configuration examples

IIS Web.config secure cookies, verb filtering, and security headers

```
xml
<system.web>
  <httpCookies requireSSL="true" />
</system.web>
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <add name="Referrer-Policy" value="no-referrer" />
      <add name="X-Content-Type-Options" value="nosniff" />
      <add name="Strict-Transport-Security" value="max-age=31536000;
includeSubDomains; preload" />
      <add name="Content-Security-Policy" value="default-src 'self'; frame-
ancestors 'none'; object-src 'none'" />
    </customHeaders>
  </httpProtocol>
  <security>
    <requestFiltering>
      <verbs allowUnlisted="false">
        <add verb="GET" allowed="true" />
        <add verb="POST" allowed="true" />
      </verbs>
    </requestFiltering>
  </security>
</system.webServer>
```

Appendices

Appendix B. Configuration examples

SQL Server connection for sessions and locks

```
Server=sqlserver.domain.local;  
Database=MyWorkDriveLocks;  
User Id=mwd_service;  
Password=<store_in_vault>;  
Encrypt=true;  
TrustServerCertificate=false;
```

Appendix C. Architecture quick reference

Users ←TLS→ **Identity Provider** ←Auth→ **MyWorkDrive** ←APIs→ **Storage**

For multi-server deployments:

Users ←TLS→ **Identity Provider** ←Auth→ **Load Balancer** ↔ **MyWorkDrive**

Servers ←APIs→ **Storage**

↓ ↓ ↓ ↓ ↓ ↓

Shared Sessions/Locks Database

Key Points: files stay in your storage, strong TLS on every path, no privilege escalation, session context in memory, single-port client architecture (443 only).

Appendices

Appendix D. Glossary

Access-Based Enumeration (ABE): Windows feature that hides folders a user cannot access

DLP: Data Loss Prevention controls that prevent unauthorized extraction

FIPS: Federal Information Processing Standards for cryptographic modules

IdP: Identity Provider that authenticates users and applies MFA

NTFS: Windows file system with granular permissions

OOS: Office Online Server for customer-hosted web editing

SAML: Standard for federated authentication

SMB: Windows network file sharing protocol

TLS: Transport Layer Security for encrypted communications

Cloud Web Connector: MyWorkDrive's built-in reverse proxy using Cloudflare tunnels for outbound-only connectivity