MSP360

MANAGE. SUPPORT. PROTECT.

Guide

How to Protect Your MSP360 Backups for Future Recoveries

1-866-4-MSP360
1-415-301-7773

sales@msp360.com

6425 Living Place Suite 200
Pittsburgh, PA 15206

msp360.com

This guide covers four protection layers — confidentiality, integrity, immutability, and access controls — and maps each to specific MSP360 features. For every control: what to configure, how to verify it works, what typically breaks, and how often to check it.

Why Backup Protection Needs Multiple Layers

Ransomware operators routinely target not just production data, but the organisation's ability to recover data. This means hunting for access to backup storage, attempting to delete or encrypt accessible backup copies, and compromising management consoles. A backup strategy that only tracks "successful backup" is not enough.

The four controls that matter — and why

Control layer	Risks addressed	Threats
A. Encryption	Impact of storage exposure or data interception	Anyone with storage or backup software access can potentially read backup contents
B. Retention + immutability	Loss of known-good restore points	Attacker deletes or corrupts backup data, leaving no known-clean copy for recovery
C. Consistency checks + restore verification	Risk of discovering corruption during an outage	Backup reports success but data cannot actually restore
D. RBAC / MFA / IP allowlisting	Backup storage or management tools compromised	Single compromised credential = full control over backup infrastructure

Looking for a quick-start checklist? Jump to the Recoverability Checklist at the end of this guide — it maps every control to a maintenance frequency so you can turn this guide into a recurring IT calendar item.

A Confidentiality Controls

SSL/TLS in transit · AES client-side encryption · Server-side encryption

A1 — Encrypt data in transit (SSL/TLS)

Prevents credential theft and data interception during transfers to backup storage and the management console.

Configure

In the Add Storage Account wizard, enable Use SSL in Advanced Settings. For CLI: use -ssl yes when creating storage accounts.

Verify

Run a small backup/restore and confirm no network interception rules are needed. Validate that required MSP360 endpoints and ports are reachable from your network.

Common failure

TLS broken indirectly by proxy rules, SSL inspection, or blocked domains. Treat the official MSP360 port/IP/domain list as your baseline allowlist.

Cadence

Configure once. Re-validate after any network, proxy, or storage account changes.

> Read more:
> Security Features of MSP360

A2 — Client-side AES encryption for backup contents

Ensures backup data remains confidential even if someone gains access to the destination bucket. MSP360 supports AES with 128, 192, or 256-bit keys.

Configure

In the backup plan wizard, go to Compression and Encryption Options. Enable encryption and set a password. Applies to file, image, SQL, and VM backup plans.

> IMPORTANT: The encryption password is not stored in the plan configuration file. You must store it securely — without it, restores will fail completely. MSP360 also offers a Password Recovery Service that stores an emergency decrypt hash — consider enabling it as an additional safety net.

Verify

You can easily verify your encryption password by drilling down the backup data in the Backup Storage interface. Restore verification for image-based backup also requires an encryption password. Lastly you can run a test restore that requires the password.

Common failure

Lost encryption password = unrecoverable backup. Treat password management like a credential vault requirement, not an afterthought.

Cadence

Configure once per plan. Spot-check quarterly with a small restore.

> Read more:
> Backup Encryption Options Explained
> New Backup Format

Image-Based Backup: Encryption (New Backup Format)
File-Level Backup. Compression and Encryption | Help Center

A3 — Server-side encryption (SSE / KMS)

For most customers, client-side AES encryption combined with immutability provides sufficient protection. SSE/KMS is recommended for organisations with specific compliance or regulatory requirements — confirm with your security or solutions team before enabling.

Configure

For Amazon S3 plans: server-side encryption is on by default. Additional KMS options appear in the Compression and Encryption step of the backup wizard. Ensure your IAM policy grants the necessary KMS permissions.

Verify

Confirm that uploaded objects show SSE enabled at the provider level. Run a backup and restore to confirm encryption did not break availability.

Common failure

Misconfigured KMS permissions show up as upload or restore failures. Always run a backup+restore test immediately after enabling KMS — do not treat it as set-and-forget.

Cadence

Review annually and after IAM/KMS policy changes. Validate quarterly via restore tests.

Read more:
Image-Based Backup: Encryption (SSE/KMS)

B Immutability and Retention Controls

GFS retention · Object Lock (Governance / Compliance)

B1 — Retention policy and GFS

A retention policy defines how long backup data is kept before it is automatically deleted. Without a deliberate retention policy, you may find that all available restore points fall within the ransomware's attack window — meaning every backup you can access is already compromised.

In the new backup format, retention works by generation: each generation is one full backup plus its subsequent incrementals. The retention period applies to previous generations only — the current generation is always kept. Configure how long previous generations are retained at the Retention Policy step of the backup plan wizard.

GFS (Grandfather-Father-Son) is an additional layer on top of the regular retention policy. It marks selected full backups as weekly, monthly, or yearly restore points and keeps them for a longer defined period — regardless of the regular retention window. This gives you a structured long-term history without keeping every backup indefinitely.

Configure

Set your base retention period first: at the Retention Policy step, choose Keep backup for and specify the period. Then enable GFS to extend selected restore points. Your full-backup frequency must match your GFS periods — monthly GFS requires at least monthly full backups.

Verify

Confirm that older restore points (not just the latest) are visible and restorable. Test restoring from a monthly or yearly GFS point.

Common failure

Setting GFS keeping periods longer than the base retention without understanding the interaction — GFS-marked backups override regular retention, so they will be kept even after the regular window expires. Also: if you only run full backups monthly, GFS can only be set at monthly and yearly level.

Cadence

Review quarterly and after any change to RPO/RTO requirements or storage costs.

Read more:
About GFS Retention Policy
File Backup Plan (new format)

Note: if you use the Simple (Forever Forward Incremental) schedule instead of Advanced, you cannot enable GFS or Object Lock — meaning immutability protection described in B2 will be unavailable. Choose your schedule deliberately.

B2 — Object Lock (Immutability)

Prevents deletion or modification of selected backup datasets for a defined period, even if an attacker gains endpoint or admin access. Supported for Amazon S3, Wasabi, and Backblaze B2.

Governance vs. Compliance — what leadership will ask

Mode	Who can delete objects	How to enable
Governance (default)	Cannot delete via Backup Agent, but can delete via storage provider console	Enabled by default when Object Lock = is turned on
Compliance	No one — including the storage root account — until the retention period expires	Configured in the storage provider console. MSP360 support can advise on configuration to ensure it does not interfere with the retention process.

Configure

Step 1: Edit the storage account, select a bucket with Object Lock enabled (or create a new one — Object Lock can only be enabled on new buckets). Enable Allow Object Lock. Step 2: In the backup plan, go to Retention Policy, enable GFS, then enable Object Lock and confirm the warning.

Verify

Confirm the plan uses Advanced (GFS, Object Lock) scheduling. Attempt a controlled agent-side deletion — Governance mode should block it. Validate that recent immutable restore points exist.

Common failure

Unexpectedly high storage costs: immutable objects cannot be deleted until the GFS keeping period expires, even if you change the plan. Use with caution and set retention windows deliberately.

Cadence

Monthly: confirm immutable restore points still exist. Quarterly: review retention windows vs. storage costs.

> Object Lock must be configured through MSP360 workflows — not directly in the storage provider console. Object Lock settings applied outside MSP360 are not supported and may cause unexpected behaviour.

Read more:
Object Lock (Immutability) — Standalone
Object Lock (Immutability) — Managed Backup
Immutable Backups Explained
Backblaze B2 Object Lock Announcement

C Integrity and Recoverability Controls

Consistency checks · Repository hygiene · Restore Verification

C1 — Consistency checks (New Backup Format)

Detects missing or corrupted objects early — before a restore window — by checking that all required backup components exist in storage and match expected sizes and modification dates.

MSP360 runs two types of consistency checks in the New Backup Format:

- Mandatory check: runs automatically at the start of every backup plan. Verifies the current generation is intact. If discrepancies are found, a full backup runs automatically.
- Full check: covers previous generations as well. Optional. Configure in the Consistency Check and Restore Verification step of the backup plan wizard.

Verify

Confirm consistency check results appear in backup history. Treat any discrepancy warning as a stop-the-line event for that dataset.

Common failure

In the New Backup Format, consistency checks complete quickly — even full checks take seconds. If you have a mix of old and new format backups, use the skip legacy option at the storage account level to reduce overhead on older data.

Cadence

Mandatory checks run automatically with each backup plan. Enable full checks for plans where data integrity is critical. Always run after storage migrations or suspected incidents.

Read more:
Mandatory and Full Consistency Checks

C2 — Repository hygiene and sync

The MSP360 repository is a local SQLite database that tracks backup metadata. When it falls out of sync with storage, restore point browsing may show incomplete or missing data — even when backups are intact.

Right approach

Run a consistency check first. Use repository sync only if browsing is demonstrably wrong after the consistency check passes. Sync does not affect cloud data — it only updates the local database.

Configure

Tools → Options → Repository → Synchronize Repository. Select the storage account and click Synchronize Now.

Common failure

Treating sync as a routine step. Sync can take a significant amount of time to complete, blocks the Backup Storage view during operation, and cannot be scheduled.

Cadence

On-demand only. Review repository size and health quarterly.

Read more:
Repository Sync and Consistency Check

C3 — Restore Verification for image-based backups

Proves that image-based backups are bootable and can reach system logon — without downloading the full dataset. MSP360 mounts a Hyper-V VM on the fly using only the backup parts needed to boot. For a 160 GB system disk, typically only ~8 GB is downloaded.

Prerequisites

Hyper-V must be available on the machine running the verification. As of Backup for Windows 7.5, the required environment installs automatically. If installation fails (code 2042), run: cloudberry backup.exe /installdiskdriver

Run manually

In the Backup Storage tab, expand a plan generation, right-click a restore point, and select Restore Verification. Available in Backup Agent only — not available from the MBS Management Console.

Run on schedule

In the image-based backup plan wizard, go to Consistency Check and Restore Verification. Options: Full only, Incremental only, or Full and Incremental. Automation supports Full/Incremental/Both — not time/date-based frequency.

Verify

VM reaches system logon within the configured timeout. Review screenshots and failure-timeout thresholds in advanced settings.

Common failure

Missing Hyper-V support (e.g., Windows Home editions), driver install failures, or timeout misconfiguration.

Cadence

Enable Restore Verification for Full and/or Incremental backups. For less critical systems, enable for Full backups only.

Pass: VM reaches system logon within configured timeout, screenshot captured in report.

Fail: Repeated failures due to missing Hyper-V, driver issues, or timeout. Investigate before relying on these backups for recovery.

Read more:
Restore Verification — Standalone
Restore Verification — Managed Backup
Add Boot Critical Drivers (installdiskdriver)

D Access and Administration Controls (MBS only)

Master password · 2FA · RBAC · IP allowlisting · IAM roles · Key rotation

D1 — Master password and local agent hardening

Prevents a local attacker or malware with user-level access from changing backup settings, stealing stored credentials, or running CLI commands that alter backup posture.

Configure

In Backup Agent: Tools → Options → General. Enable Protect console with master password. Also enable Protect CLI with master password — required to prevent CLI-based bypass. In MBS: can also be configured via Backup Template under Global Agent Options.

Verify

Restart the agent and confirm it prompts for the master password. Run a CLI command without -mp and confirm it is blocked.

Cadence

Configure once. Validate quarterly. Review immediately after staffing changes or suspected credential compromise.

> If the master password is reset, access to the Backup Agent console and CLI is restored but you will need to re-enter the master password where required. Document the master password securely and ensure at least two authorised admins can access it.

> Read more:
> Master Password Protection
> Master Password — Options
> Master Password Feature 6.1.1

D2 — Management Console 2FA and forced enforcement

Prevents single-factor compromise of the control plane. Console access can alter plans, retention settings, and storage configuration — making it a high-value target.

Configure

Settings → General → Enable Two-Factor Authentication. Follow the authenticator setup flow. Save recovery codes — they are required for break-glass access if the primary device is unavailable.

Force for all admins

Select Force 2FA for all administrators. Admins without 2FA will be prompted to configure it on next login.

Break-glass recovery

The main administrator can disable 2FA for a sub-admin who has lost their recovery codes. The admin will be prompted to reconfigure 2FA on next login.

Verify

Test a login from a clean browser session — password-only must not be sufficient. Confirm recovery codes exist and are stored in a documented break-glass process.

Cadence

Monthly audit of admin account 2FA status. Quarterly: confirm recovery codes are securely stored and accessible to break-glass admins. Test the admin-disable reset workflow rather than the codes themselves — recovery codes are single-use and should not be consumed during drills.

Read more:
Best Practices for Management Console
MSP360 Security Best Practices PDF

D3 — RBAC / Granular administrator permissions

Limits blast radius if an admin account is compromised. Restricts what a routine operator can modify — particularly storage accounts, Object Lock settings, and retention policy.

Configure

Organization → Administrators → select admin → Permissions tab. Global access is standard for MSP operators who manage multiple companies. Use Administrator (Specific Companies) only when a customer's internal IT team should be restricted to their own company's data. Note: limiting all admins to specific companies requires multiple logins and multiple 2FA registrations per operator — this will significantly impact day-to-day workflow.

Key restriction

Permissions required to manage storage accounts should be granted only to explicitly authorised admins. Object Lock at the bucket level can only be enabled at bucket creation. Object Lock at the plan level can be enabled or edited at any time when creating or modifying a plan.

Verify

Log in as a limited admin and confirm they cannot access storage accounts or immutability controls outside their scope.

Cadence

Quarterly review. Immediately after any staffing or offboarding event.

Read more:
Best Practices for Management Console
MSP360 Security Best Practices PDF
Managing Administrators with MSP360 Managed Backup
Managing Sub-Administrators

D4 — IP allowlisting for the Management Console

Reduces exposed attack surface of the control plane by restricting which IP addresses can log in. Effective for organisations with known office or VPN egress IPs.

Configure

Settings → IP AllowListing → enable the toggle. Your current IP is allowlisted automatically to prevent accidental lockout. Add required IP ranges or individual addresses. Changes are logged in the Audit Log under Security operations

Precondition

If you have remote staff or dynamic ISP ranges, use a VPN or static NAT before enforcing allowlisting — otherwise you will lock out legitimate admins.

Verify

Test console access from an allowlisted network (must succeed) and a non-allowlisted network (must fail). Confirm the Audit Log records the allowlist change.

Cadence

Quarterly review. Update immediately after office moves, VPN changes, or new admin onboarding.

Read more:
IP Address Allowlist

D5 — Storage IAM roles and credential management

Reduces long-lived credential exposure. Where possible, use IAM roles with temporary credentials rather than long-term access keys — stolen temporary credentials have a limited useful lifetime.

IAM roles (preferred)
MSP360 Managed Backup supports S3 authentication via IAM roles. Use the Add an S3 Account Using IAM Role workflow with Provider ID and Role ARN. MSP360 also supports AWS STS temporary credentials and cross-account Assume Role patterns.

Key rotation (if keys required)
If long-term access keys must be used, rotate them at least every 90 days. After updating keys in MSP360, run a small backup and restore, then disable the old key. Confirm no remaining workloads depend on the old key before deleting it.

Verify
Confirm backups and restores succeed using the IAM role path. Review IAM policies for least privilege — only the buckets and actions required for backup/restore.

Cadence
Review IAM policies quarterly. Rotate keys at most every 90 days, or immediately after any staffing change or suspected key exposure.

Read more:
Add S3 Account Using IAM Role
How to Create IAM Role for MBS
STS / Temporary Credentials

E Combined Test Block

Run this routinely to produce auditable pass/fail evidence

Each test below is structured to give a clear outcome. Run the full block quarterly; run the marked tests more frequently.

Integrity tests

E1 — Storage-account consistency check

Steps: Run Now on the primary storage account consistency check. If legacy encrypted data exists, supply the encryption password. Review results.

Pass: Results are green, or warnings have documented remediation actions.

Fail: Repeated warnings with no remediation path, or checks cannot complete within operational windows.

E2 — Full consistency check

Steps: Enable full consistency check. Run the plan and confirm checks complete.

Pass: Full consistency check completes successfully. No persistent discrepancies.

Fail: Recurring discrepancies or forced full backups with no identified root cause.

Access tests

E3 — 2FA enforcement and recovery codes drill

Steps: Confirm 2FA is enabled for all admins. Confirm recovery codes are stored and accessible under break-glass conditions. Test a login requiring 2FA from a clean session.

Pass: Password-only login is blocked. Recovery codes exist and are usable under documented controls.

Fail: Any admin account without 2FA. Any admin with no accessible recovery codes and no documented reset path.

E4 — RBAC sanity check

Steps: Log in as a limited admin. Confirm they cannot access storage accounts, Object Lock controls, or retention settings outside their assigned scope.

Pass: Least privilege holds in practice.

Fail: Any role drift where operators have unintended access to storage or immutability controls.

E5 — IP allowlisting negative test

Steps: Confirm your IP is allowlisted. Attempt console access from a non-allowlisted network. Review Audit Log for the change record.

Pass: Non-allowlisted access is blocked. Audit Log entry exists for allowlist change.

Fail: Non-allowlisted access succeeds, or allowlist changes are not logged.

Recovery tests

E6 — Restore Verification for image-based backups

Steps: Run Restore Verification for a current restore point. Confirm Hyper-V prerequisites are met. Review screenshot and failure timeout configuration.

Pass: VM reaches system logon within configured timeout.

Fail: Repeated failures — missing Hyper-V, driver issues, or timeout. Do not rely on these backups until resolved.

E7 — Encrypted restore spot-check (quarterly)

Steps: Restore a small encrypted dataset. Confirm the process requires the encryption password. Confirm the team can locate and use the password under simulated pressure.

Pass: Restore succeeds with password. Password retrieval took under 5 minutes.

Fail: Password not retrievable, or restore cannot proceed without escalation.

F Control Reference Table

Executive summary for audits and leadership reviews

Control	Layer	Key MSP360 feature	Verification method	Cadence
SSL/TLS in transit	Confidentiality	Use SSL in storage account settings	Backup/restore succeeds, endpoints reachable	After network/storage changes
AES client-side encryption	Confidentiality	Backup plan encryption step, 128/192/256-bit	Restore requires password, fails safely without it	Quarterly spot-check
Server-side encryption (SSE/ KMS)	Confidentiality	SSE on by default, KMS option in wizard	Object encryption visible at storage level	Annual review; quarterly validation
GFS retention	Immutability	Advanced (GFS, Object Lock) schedule	Older restore points exist and are restorable	Quarterly
Object Lock (Immutability)	Immutability	Object Lock on GFS-enabled plans, S3/Wasabi/B2	Agent-side deletion blocked, retention enforced	Monthly validation
Mandatory consistency check	Integrity	Runs automatically in New Backup Format	Discrepancies trigger automatic full backup	Automatic — monitor alerts
Full consistency check	Integrity	Optional, per-plan setting	Full check completes; no persistent discrepancy	Monthly (T1), quarterly (T2)
Repository sync discipline	Integrity	Tools → Options → Repository	Browse matches storage; sync not routinely needed	On-demand only
Restore Verification	Integrity	Image-based backup plan / Backup Storage tab	VM boots and logs on within timeout	Weekly (T1), monthly (T2)
Master password (agent)	Access	Tools → Options → General	Agent prompts, CLI requires -mp	Quarterly verification
2FA + force enforcement	Access	Settings → General → 2FA	Password-only login blocked; recovery codes work	Monthly audit; quarterly drill
RBAC / permissions	Access	Organization → Administrators → Permissions	Limited admin cannot access forbidden controls	Quarterly + offboarding
IP allowlisting	Access	Settings → IP Allow List	Non-allowlisted access blocked; logged in Audit Log	Quarterly + office/VPN changes
IAM roles / temp credentials	Access	S3 IAM Role workflow in storage setup	Backups succeed; IAM policy least-privilege	Quarterly review
Access key rotation	Access	Storage account rotation (GUI/CLI)	Old key disabled with no service impact	Max 90 days, whenever ops staff change

Recoverability Checklist

Before diving into each control, here is the maintenance schedule this guide recommends. Use it as your planning baseline.

Frequency	Task
Every plan execution	Mandatory consistency check runs with each backup plan → See section C1
For Full / Incremental backups	Restore Verification for image-based backups → See section C3
Monthly	Storage-account consistency check (primary storage) → See section C1
Monthly	Object Lock validation — immutable restore points still present → See section B2
Monthly	Audit administrator accounts + 2FA status → See section D2
Quarterly	RBAC permissions review — confirm least privilege → See section D3
Quarterly	Encrypted restore spot-check — confirm password retrieval + restore success → See section A2
Quarterly	IP allowlist review — new admins, new office locations → See section D4
Quarterly	Access key rotation (if long-term keys are in use, max 90 days) → See section D5
Semi-annual / annual	Retention + immutability policy review — costs vs. compliance window → See section B1
After any staffing change	Revoke or update credentials, RBAC, IP allowlist entries → See section D3
After any network/storage change	Re-validate SSL/TLS connectivity and storage account settings → See section A1

What to Do Next

Treat this guide as a hardening backlog, not a one-time read.

If you already use MSP360:

- Identify which controls from Section F are not yet configured — those are your gaps.
- Prioritise Object Lock + GFS, Restore Verification, and 2FA enforcement — these have the highest impact on ransomware resilience.
- Add the cadence timeline from Section B to your quarterly IT calendar.
- Run the Combined Test Block from Section E once now as a baseline, then quarterly.

If you are evaluating MSP360:

- Run a proof-of-value that includes Object Lock with GFS, Restore Verification for image-based backups, and Management Console hardening (2FA, RBAC, IP allowlisting).
- These are the controls that most directly reduce ransomware's ability to hold your recovery capability hostage.

> The goal is not just to have backups — it is to know, continuously, that recovery will work when the pressure is real.

About MSP360

Established in 2011 by a group of IT professionals, MSP360™ provides simple and reliable cutting-edge Backup and IT management solutions for MSPs and IT departments worldwide.

MSP360™ platform combines the number one easy-to-use backup solution to deliver best-in-class data protection, secure remote access software to provide support to customers or team members, and painless RMM to handle all aspects of IT infrastructures, all under a single pane of glass.