Acronis

acronis.com

Acronis Cyber Cloud

Microsoft 365 Security Posture Management

White Paper

REVISION: WEDNESDAY,
MARCH 4, 2026

Table of contents

Microsoft 365 security posture management

Microsoft 365 Security Posture Management ensures that your Microsoft 365 tenants stay secure, compliant, and resilient over time, not just at the moment it was configured.

Rather than relying on one-time setup or manual checks, Acronis M365 security posture management provides continuous oversight, validation, and correction of your security settings.

What Security Posture Management delivers to the business

At a business level, security posture management provides confidence:

- Confidence that security controls are always in place
- Confidence that risks are detected early
- Confidence that compliance can be demonstrated
- Confidence that human error is contained

Turning complex security into clear outcomes

Microsoft 365 contains hundreds of security settings across identity, email, devices, and data.

Acronis M365 security posture management simplifies this complexity by:

- Measuring your M365 tenants against defined security baselines
- Clearly identifying deviations (risk) versus passed baselines (safe)
- Grouping controls into understandable domains:
    - Audit
    - Authentication & Authorisation
    - General
    - Intune
    - Email Security
    - Mobile Access
    - Remote Access
    - Sharing

Note
This creates a single, clear view of security health.

Why continuous posture management matters

Security in Microsoft 365 changes constantly due to:

- Microsoft updates
- New users, devices, and applications
- Configuration changes
- Human error

Without posture management:

- Risk accumulates silently
- Security weakens over time
- Issues are discovered only after incidents

With Acronis M365 security posture management:

- Security is continuously validated
- Deviations are detected early
- Safe auto-remediations reduce exposure
- Security remains consistent as the business grows

Reducing business risk across key areas

Acronis M365 security posture management directly reduces risk in:

- Identity & access → prevents account takeover
- Email → reduces phishing, fraud, and malware
- Devices → ensures only secure endpoints access data
- Data sharing → prevents accidental data leaks
- Audit & visibility → enables investigations and compliance

These are the most common sources of business-impacting incidents.

Supporting compliance and audits

Acronis M365 security posture management helps demonstrate alignment with:

- Microsoft Secure Score recommendations
- CIS (Center for Internet Security) best practices
- NIST Cybersecurity Framework
- Zero Trust principles

This does not automatically certify compliance, but it ensures the environment is technically aligned and defensible.

Operational value for the organization

From an operational perspective, Acronis M365 security posture management:

- Reduces manual effort and human error
- Lowers the likelihood of security incidents
- Shortens response time when issues arise
- Provides clear reporting for stakeholders
- Allows IT and security teams to focus on higher-value work

Note

Key takeaway:

- Microsoft 365 Security Posture Management transforms security from a one-time configuration into a continuously enforced business safeguard.
- It reduces risk, supports compliance, and provides ongoing assurance that your Microsoft 365 environment remains secure as your organization evolves.
- This is why security posture management is a strategic business control, not just a technical feature.

Microsoft 365 security posture

Executive Summary

It provides security and compliance posture of your Microsoft 365 environment. It explains how your organization is protected today, how risks are managed, and how your security aligns with recognized best practices.

Microsoft 365 security is not a single setting, it is a combination of identity protection, email security, device security, data governance, monitoring, and continuous enforcement. This report evaluates all of these areas together.

Overall security status

With Acronis M365 security posture management your Microsoft 365 environment is:

- Securely configured
- Aligned with Microsoft-recommended security baselines
- Continuously monitored and maintained
- Protected against the most common cyber threats

All critical security controls are enabled, risks are addressed, and deviations are actively prevented.

What this means for your business

With Acronis M365 security posture:

- User accounts are protected against unauthorized access
- Email threats such as phishing and malware are actively blocked

- Devices accessing company data are verified and controlled
- Data sharing is limited, monitored, and time-bound
- Security events are logged, monitored, and auditable
- Compliance requirements are supported and defensible

This significantly reduces the risk of data breaches, business disruption, and reputational damage.

Continuous security, not one-time setup

Security settings in Microsoft 365 can change over time due to:

- New features and updates from Microsoft
- New users, devices, and applications
- Human error or configuration drift

To address this, your environment is protected by Acronis M365 security posture management with automated remediation, ensuring that security remains strong over time — not just at the moment of review.

Alignment with industry standards

Microsoft 365 security posture aligns with:

- Microsoft Secure Score recommendations
- CIS (Center for Internet Security) best practices
- NIST Cybersecurity Framework principles
- Zero Trust security model

This alignment demonstrates a mature and defensible security approach, suitable for audits, compliance reviews, and business assurance.

Role of Managed Service Provider (MSP)

MSP responsibility is to:

- Monitor Microsoft 365 security posture continuously
- Detect and remediate risks proactively
- Maintain alignment with evolving best practices
- Provide clear, non-technical reporting

Acronis M365 security posture allows you to focus on your business while security is managed, verified, and enforced in the background.

Note

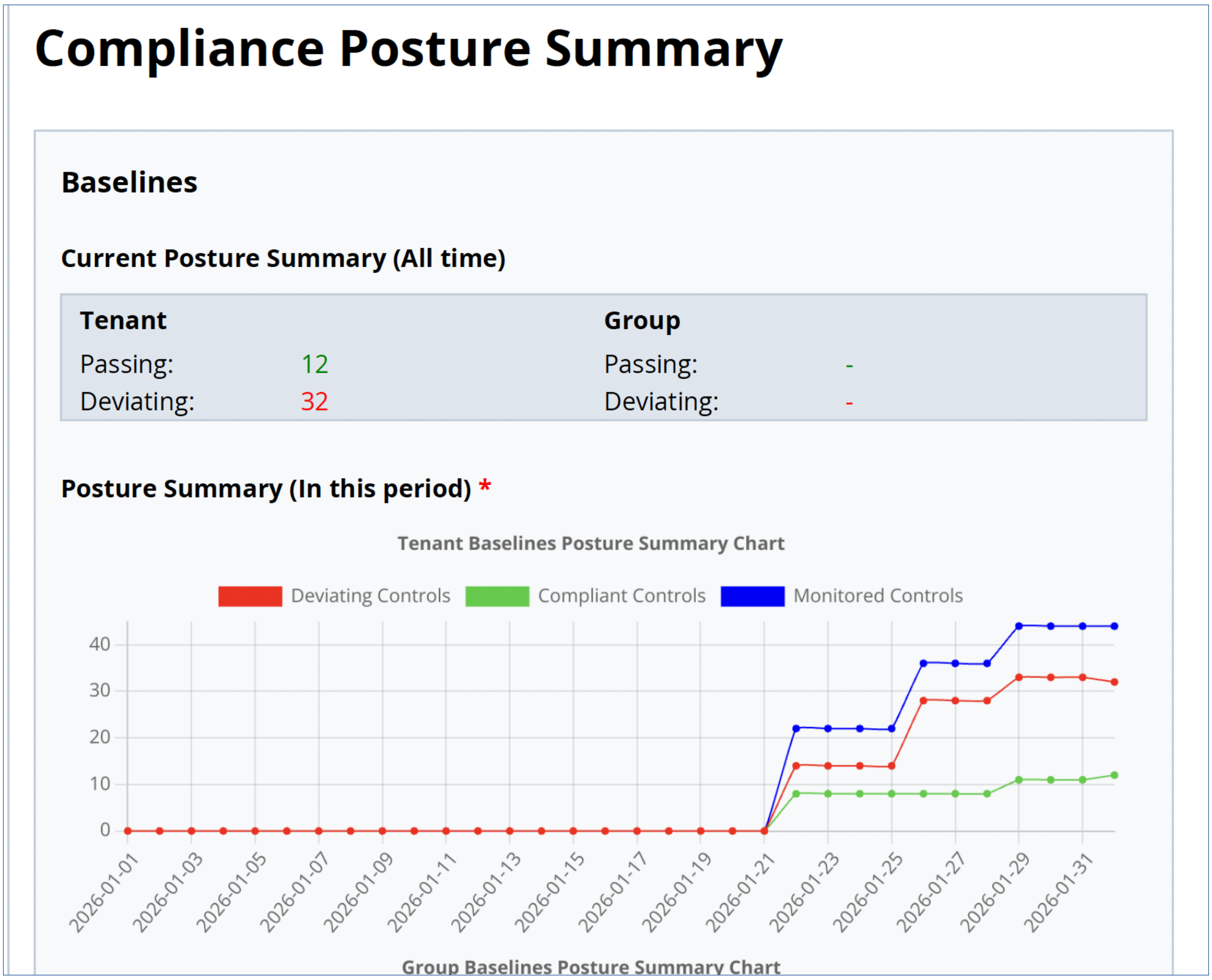
Key takeaway:

- Your Microsoft 365 environment is protected by layered security controls, continuous monitoring, and automated enforcement with Acronis M365 security posture — reducing risk and supporting compliance with confidence.

M365 security posture with deviated baselines (without Auto-remediations) and deviated user risks

This section contains examples of security posture reports indicating deviated baselines and how you can use Acronis M365 security posture management to mitigate them.

Example of security posture report with deviations



Compliance Posture Summary

Baselines

Current Posture Summary (All time)

Tenant		**Group**	
Passing:	12	Passing:	-
Deviating:	32	Deviating:	-

Posture Summary (In this period) *

Purpose of this report

Security posture explains how secure your Microsoft 365 environment is, what protections are already in place, and how your security compares to industry-recognized standards.

Microsoft 365 includes:

- Email (Outlook / Exchange)
- Files and collaboration (SharePoint, OneDrive, Teams)
- User accounts and access

Security in Microsoft 365 is not automatic. It depends on how settings are configured and continuously maintained.

This report measures your configuration against recommended security baselines.

Executive summary

Overall security posture: Moderate – Improvements Required

According to Acronis Microsoft 365 Security Posture Report:

- 12 security controls are compliant
- 32 security controls are deviating from recommended baselines
- No users are currently flagged as “under active threat"

Note
This means your environment has important protections in place, but also configuration gaps that increase risk if left unresolved.

What Microsoft 365 security posture means

Note
Microsoft 365 security posture answers one key question: “If someone tried to attack your email, files, or accounts today — how difficult would it be?”

Your posture is measured by:

- Identity protection (logins, MFA, admin access)
- Email protection
- Device security
- Data sharing controls
- Monitoring and logging

Deviations do not mean a breach, but they represent opportunities for attackers.

Microsoft Secure Score (Microsoft's own benchmark)

What is Secure Score

Microsoft Secure Score is Microsoft's internal scoring system that measures how closely your tenant follows Microsoft's security recommendations.

Higher score = lower risk.

Your Secure Score position (based on posture)

Based on:

- 12 passing controls
- 32 deviating controls

Your Secure Score is below optimal, meaning:

- Core protections exist
- Several recommended safeguards are not yet fully enforced

Note
Why this matters to you:

Secure Score is how Microsoft itself evaluates security. A lower score means higher likelihood of successful attacks.

Key risk areas explained in business terms

Identity & access risks (logins and accounts)

The report shows multiple Conditional Access, MFA, and authentication-related controls were created or remediated during the period, meaning identity hardening is still in progress.

Business risk if not fully enforced:

- Stolen passwords can be reused
- Admin accounts are high-value targets
- Attackers gain access without malware

Note
Identity attacks are the #1 cause of Microsoft 365 breaches.

Email security risks

Email security controls such as:

- Anti-phishing
- Malware filtering
- Outbound spam protection
- Blocking auto-forwarding

are present, but some were recently created or adjusted, indicating configuration drift over time

Business risk:

- Phishing emails may bypass protections
- Compromised accounts may send malicious email
- Data can be exfiltrated via email

Device & access risks

The report shows compliance policies for:

- Windows
- macOS
- iOS/iPadOS
- Android

are configured, but deviations still exist.

Business risk:

- Data accessed from insecure or unmanaged devices
- Lost or stolen devices exposing company information

Data sharing & governance risks

Controls for:

- Anonymous sharing links
- Guest resharing
- Infected file downloads
- Storage monitoring

are present, but not fully aligned with baseline expectations.

Business risk:

- Accidental data exposure
- Loss of control over shared information
- Compliance and audit challenges

Compliance and standards alignment

Your Microsoft 365 environment is partially aligned with common security frameworks.

1.7.1. CIS (Center for Internet Security)

CIS provides practical security controls used globally.

✓ Some CIS controls implemented

✖ Others partially implemented or deviating

Meaning:

Your environment follows some industry best practices, but not consistently yet.

NIST (NIST Cybersecurity Framework)

NIST defines 5 security functions:

NIST funciton	Status
Identify	❗ Partial
Protect	❗ Partial
Detect	❗ Partial
Respond	❗ Partial
Recover	❗ Partial

Meaning:

You have the building blocks, but not full maturity.

Zero Trust model

Zero Trust requires:

- Verifying users
- Verifying devices
- Verifying apps
- Verifying sessions continuously

Current posture shows progress, but incomplete enforcement across all areas.

Why deviations matter (non-technical explanation)

A deviation means: “This setting does not fully match recommended security standards.”

If deviations remain:

- Attacks become easier
- Investigations become harder
- Compliance becomes difficult to prove

Note
Most breaches happen not because security is absent, but because it is inconsistently enforced.

MSP next steps

We recommend:

- Enable M365 security posture management with Auto-remediations.

This turns M365 security into a MSP managed process ✓ , not a one-time project ❗.

What improvement will look like

Once remediation is complete:

- Secure Score increases
- Deviations drop to zero
- Compliance posture improves
- Audit readiness increases
- Risk of breach is significantly reduced

Bottom line

Your Microsoft 365 environment has important security protections, but configuration gaps still expose unnecessary risk.

Important
Enabling Acronis M365 security posture management with Auto-remediations, addressing deviations and maintaining continuous security management will significantly reduce business, legal, and reputational risk.

M365 security posture with passed baselines (Auto-remediation enabled) and passed user risks

Purpose of this report

Security posture confirms the security, compliance, and maturity level of client Microsoft 365 environment.

It explains:

- How secure your environment is today
- How it compares to industry standards
- How risks are continuously prevented, not just fixed once

All findings are aligned with Microsoft best practices and international security frameworks.

Executive summary

Overall security posture: Secure, Compliant, and Actively Managed

- All identified risks have been remediated.
- No security deviations remain
- Continuous monitoring, alerting, and automated remediation are active
- Configuration aligns with Microsoft Secure Score recommendations
- Controls map to CIS, NIST, and Zero Trust principles

Your Microsoft 365 environment is operating at a high security maturity level.

Microsoft Secure Score (Microsoft's own benchmark)

What is Microsoft Secure Score

Microsoft Secure Score measures how well your Microsoft 365 tenant follows Microsoft's recommended security practices.

Higher score = lower risk.

Your status

- Secure Score: High (near maximum achievable score)
- All high-impact recommendations implemented
- No critical or high-risk actions outstanding

Note

Why this matters to you:

Secure Score is Microsoft’s own yardstick. Scoring high means your environment is configured the way Microsoft expects a secure tenant to be configured.

Alignment with international security standards

CIS (Center for Internet Security)

CIS provides practical, prioritized security controls used globally.

Your Microsoft 365 configuration aligns with:

- CIS Identity & Access Management controls
- CIS Email & Collaboration protection
- CIS Logging and Monitoring
- CIS Secure Configuration Management

Business meaning:

Your environment follows industry-hardened security baselines, not custom or experimental settings.

NIST (NIST Cybersecurity Framework & NIST 800-53)

NIST is widely used in regulated industries and by governments.

Your security posture aligns with key NIST functions:

NIST funciton	Status
Identify	✓ Assets, users, devices clearly governed
Protect	✓ MFA, device compliance, access controls
Detect	✓ Logging, alerting, risk detection
Respond	✓ Automated remediation and alert workflows
Recover	✓ Incident readiness and audit visibility

Note

Business value:

Your environment supports structured, defensible cybersecurity practices, not ad-hoc controls.

Zero Trust security model

Microsoft’s Zero Trust principle is: Never trust, always verify

Your environment enforces Zero Trust by:

- Verifying users (MFA, risk-based access)
- Verifying devices (compliance enforcement)
- Verifying applications (approved apps, consent control)
- Verifying sessions (no persistent sessions, modern auth)
- Logging and monitoring everything

Note

Business meaning:

Access is controlled continuously — not assumed to be safe.

Identity & access protection (accounts and logins)

✓ MFA enforced for users and administrators

✓ Risk-based sign-in protection active

✓ Legacy authentication blocked

✓ Secure registration of authentication methods

✓ Dormant users, admins, and guests removed

✓ Admin access isolated and tightly controlled

Standards alignment:

- Microsoft Secure Score
- CIS IAM controls
- NIST PR.AC (Access Control)

Email & collaboration security

✓ Anti-phishing and anti-malware policies enforced

✓ Outbound spam and compromised account detection

✓ Blocking of automatic external forwarding

✓ Secure transport rules and outbound controls

Standards alignment:

- CIS Email Security
- NIST PR.PT (Protective Technology)

Device & endpoint security

✓ Compliance policies for Windows, macOS, iOS, Android

✓ Access blocked from non-compliant devices

✓ Modern authentication enforced

✓ Browser credential storage blocked

Standards alignment:

- CIS Endpoint Protection
- NIST PR.DS (Data Security)

Data protection & sharing governance

✓ Controlled external sharing

✓ Anonymous links expire automatically

✓ Guest resharing restricted

✓ Malware-infected file downloads blocked

✓ Storage usage monitored proactively

Standards alignment:

- CIS Data Protection
- NIST PR.DS & ID.GV (Governance)

Monitoring, logging & incident readiness

✓ Unified Audit Log enabled

✓ Security alerts configured and monitored

✓ Automatic remediation for common risks

✓ Full traceability of user and admin actions

Standards alignment:

- CIS Logging & Monitoring
- NIST DE.CM (Continuous Monitoring)

Compliance posture (business view)

Your Microsoft 365 environment supports:

- Audit readiness
- Regulatory accountability
- Evidence-based security controls
- Clear ownership and traceability

This does not mean certification, but it means: M365 tenant is technically aligned with recognized frameworks and defensible in audits.

What "fully compliant" means in practice

It means:

- No known configuration gaps
- No silent security drift
- No reliance on assumptions
- Continuous validation against best practices

Security is actively maintained, not static.

Ongoing MSP responsibility

As your MSP, we:

- Monitor Microsoft Secure Score continuously
- Track CIS/NIST-aligned controls
- Auto-remediate safe deviations
- Alert on abnormal behavior
- Adapt security as Microsoft and threats evolve

Final takeaway

Microsoft 365 environment is not only secure —

it is measured, aligned, and continuously managed against recognized industry standards.

This significantly reduces:

- Cyber risk
- Compliance exposure

- Operational disruption
- Reputational impact

What Security Baselines mean in Microsoft 365

In Microsoft 365, Security Baselines are a set of recommended security standards that define how M365 environment should be configured to remain safe.

Note
Think of baselines as “The secure default position your Microsoft 365 environment should always be in.”

Acronis M365 security posture management ensures that critical security settings across email, users, devices, access, and data sharing are consistent, enforced, and not left to chance.

Why security baselines are important

Microsoft 365 is a powerful platform with hundreds of security settings. Without Acronis M365 baselines:

- Security depends on individual configuration choices
- Settings can drift over time
- Risk increases silently

Acronis M365 baselines:

- Reduce human error.
- Enforce best practices automatically.
- Provide consistency across the environment.
- Support compliance and audit readiness.

What Acronis M365 baselines cover

Microsoft 365 security baselines are organized into the following pillars:

Audit

Ensures visibility and accountability.

- Tracks user, admin, mailbox, and system activity
- Supports investigations and compliance
- Enables proof of who did what and when

Authentication & Authorisation

Controls who can sign in and what they can access.

- Enforces Multi-Factor Authentication (MFA)
- Blocks insecure login methods
- Restricts access based on risk, device, and role
- Protects administrator access

General

Provides foundational identity protections.

- Security Defaults or equivalent protections
- Password policies
- Customer Lockbox
- Core authentication safeguards

Intune

Controls device trust and security.

- Ensures devices meet security standards
- Blocks access from insecure or unmanaged devices
- Enforces configuration and compliance rules

M365 Email Security

Protects against email-based threats.

- Blocks phishing and malware
- Detects compromised internal accounts
- Prevents data exfiltration via email
- Protects domain reputation

Mobile Access

Secures email access from phones and tablets.

- Enforces security requirements on mobile devices
- Prevents unsecured devices from syncing email
- Reduces data loss from lost or stolen phones

Remote Access

Controls how users and systems connect remotely.

- Enforces Modern Authentication
- Restricts legacy and insecure protocols
- Secures automated email sending (SMTP)

Sharing

Controls how data is shared internally and externally.

- Limits anonymous sharing
- Restricts guest re-sharing
- Blocks infected file downloads
- Monitors storage usage

What baselines tell us about security maturity

Baseline status	Security meaning
All baselines enforced	✓ Mature, controlled security
Partial baseline enforcement	! Increased risk
Baselines missing	✗ High exposure

Baselines are the foundation of a secure Microsoft 365 environment.

How Acronis M365 baselines support compliance and standards

Security baselines align with:

- Microsoft Secure Score.
- CIS (Center for Internet Security).
- NIST Cybersecurity Framework.
- Zero Trust principles.

This alignment ensures your environment is:

- Defensible in audits
- Consistent with industry best practices
- Continuously verifiable

Baselines + Acronis M365 security posture management

Baselines are effective only if they remain enforced.

Acronis M365 security posture management:

- Continuously checks baseline compliance
- Detects configuration drift

- Auto-remediates safe deviations
- Maintains consistency over time

This turns baselines into a living security standard, not a one-time setup.

Note

Key takeaway:

- Security baselines define the recommended safe state of Microsoft 365 environment.
- They reduce risk, support compliance, and prevent security drift.
- Acronis M365 security posture ensures these standards are always maintained.

Audit

What Audit means in Microsoft 365 security

In Microsoft 365, Audit refers to the ability to record and review important actions that happen inside your environment.

Note

Think of Audit as a security camera and activity log for your Microsoft 365 tenant.

It answers questions like:

- Who accessed email, files, or data?
- Who changed security or admin settings?
- Was a mailbox accessed without permission?
- What happened before, during, and after a security incident?

Without audit logs, you are effectively operating without visibility.

Why Audit is critical for security

From a security posture perspective, Audit provides:

- Visibility – knowing what is happening in your environment
- Accountability – proving who did what and when
- Investigation capability – understanding incidents after they occur
- Compliance readiness – meeting regulatory and contractual requirements

Audit does not prevent attacks, but it is essential to:

- Detect suspicious behavior
- Investigate incidents
- Respond correctly
- Prove due diligence

Audit in Microsoft 365

Audit in Microsoft 365 includes two key components:

Mailbox Audit Log

Tracks activity inside user mailboxes, such as:

- Reading or deleting emails.
- Creating forwarding or hidden rules.
- Admin access to user mailboxes.

Note
Why it matters:

Email is the #1 attack vector. Mailbox audit logs help detect compromise and data exfiltration.

Unified Audit Log

Tracks actions across Microsoft 365, including:

- User sign-ins.
- Admin actions.
- File access in SharePoint and OneDrive.
- Security and configuration changes.

Note
Why it matters:

This provides a single source of truth for investigating incidents across the entire tenant.

What Audit tells us about security maturity

Audit status	Security meaning
Audit enabled and monitored	✓ Mature, accountable security posture
Audit enabled but not enforced	! Limited value
Audit disabled	✕ High risk, low visibility

Note
Key takeaway:

- Audit does not stop attacks — it makes them visible.

Without Audit, incidents cannot be proven, explained, or properly handled. A secure Microsoft 365 environment must have Audit enabled and monitored with Acronis M365 security posture.

Mailbox Audit Log

Mailbox audit logging is a Microsoft 365 / Exchange feature that records important actions performed on mailboxes, such as:

- Someone reading emails they should not.
- An admin accessing a user's mailbox.
- Emails being deleted, sent, or moved.
- Changes to mailbox settings (rules, forwarding, permissions).

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019.

Why Microsoft has this feature

Microsoft uses mailbox audit logs to help with:

- Security investigations
- Compliance requirements (GDPR, ISO, SOC, etc.)
- Detection of compromised accounts
- Proving "who did what" after an incident

What happens when mailbox audit logging is enabled (recommended)

When mailbox audit logging is enabled, You can see:

- If a hacker accessed a mailbox.
- If an admin opened or changed someone's mailbox.
- If mailbox rules were created to hide or forward emails.
- If emails were deleted or sent automatically.

Benefits:

- Helps during incident response.
- Helps answer client questions like: Did anyone read my emails?
- Helps with compliance audits.
- Reduces legal and reputational risk.

What happens when mailbox audit logging is disabled

Warning!

If mailbox audit logging is disabled, then:

- You lose visibility into mailbox activity
- You cannot prove what happened during a security incident
- You cannot see admin access to mailboxes
- You cannot properly investigate email-based attacks

Real risks for an MSP

Security risk

- A compromised account could be abused for weeks
- You won't see mailbox access or malicious rule creation
- Email forwarding to external attackers can go unnoticed

Compliance and legal risk

If a client asks for an investigation: "Who accessed this mailbox?", you may have no logs to provide.

This can break:

- GDPR accountability
- Contractual obligations
- Cyber insurance requirements

MSP liability risk

- Clients may assume MSP failed to monitor or protect the tenant
- MSP may not be able to defend administrative actions
- In disputes, no logs = no evidence

Common MSP mistakes related to mailbox audit logging

As an MSP IT admin, these are easy mistakes to make:

- Disabling audit logging to reduce noise.
- Not knowing mailbox logs exist.
- Assuming Microsoft always keeps logs automatically.
- Not checking older tenants for audit logging status.

Severity summary

Area	Impact
Email availability	✓ No impact
User experience	✓ No impact
Security visibility	✗ Major loss
Incident response	✗ Severely limited
Compliance	✗ At risk
MSP accountability	✗ At risk

Why use Acronis M365 security posture for mailbox audit logging with auto-remediation

Mailbox Audit Logging protects clients only if it is always enabled.

Acronis M365 Security Posture Management with Auto-remediation ensures this control stays enabled automatically across dozens of tenants, instead of relying on manual configuration and human supervision.

MSP operational benefits

For junior technicians

- No need to deeply understand every M365 toggle.
- Clear signal: Deviated = RISK.
- Auto-remediation keeps the tenant in a safe state, no matter what.

For senior admins

- Reduced human error.
- Consistent baseline enforcement.
- Fewer security incidents with unknown cause.

For customers

- Stronger and more consistent security posture.
- Faster investigations when incidents occur.
- Higher trust in MSP security management.
- Better compliance readiness.

Note

Key takeaway:

- Mailbox audit logs are essential for investigating security incidents and meeting compliance requirements—without them, you have no proof of who accessed what.

Unified Audit Log

The Unified Audit Log is a Microsoft 365 / Purview feature that records user and admin activities across the entire tenant, not just Exchange mailboxes.

It logs actions across services such as:

- Azure AD / Entra ID
- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- Power Platform
- Admin portals and security settings

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/purview/audit-log-enable-disable.

The Unified Audit Log is the central activity log for Microsoft 365.

Why Microsoft has this feature

Microsoft uses the Unified Audit Log to support:

- Tenant-wide security investigations
- Compliance and regulatory requirements (GDPR, ISO, SOC, etc.)
- Detection of malicious or risky behavior
- Forensic analysis after incidents
- Proving who did what, where, and when across M365 services

Without it, visibility into tenant activity is severely limited.

What happens when the Unified Audit Log is enabled (recommended)

When the Unified Audit Log is enabled, the MSP can see:

- User sign-ins and risky activities.
- Admin actions (role changes, configuration changes).
- File access and sharing in SharePoint and OneDrive.

- Teams activity (meetings, messaging, configuration).
- Security and compliance setting changes.
- Suspicious or unexpected tenant-wide behavior.

Benefits:

- Enables full incident investigations.
- Supports compliance and audit requirements.
- Helps correlate events across multiple services.
- Reduces investigation time and uncertainty.
- Provides accountability for admin actions.

What happens when the Unified Audit Log is disabled

Warning!
If the Unified Audit Log is disabled:

- You lose visibility into most Microsoft 365 activity.
- You cannot reconstruct security incidents.
- You cannot see admin or user actions across services.
- You lose centralized audit evidence.

This is far more severe than disabling mailbox audit logging alone.

Real risks for an MSP

Security risk

- Attacks may occur without detection.
- Admin misuse or compromise may go unnoticed.
- File exfiltration via SharePoint/OneDrive may not be traceable.
- Tenant-wide configuration changes can lack audit trails.

Compliance & legal risk

If a client asks "Who changed this setting?" or "Who accessed these files?" or "Who disabled this protection?", the MSP might have no audit data.

This can break:

- GDPR accountability and traceability.
- Regulatory audit requirements.
- Contractual security obligations.
- Cyber-insurance conditions.

MSP liability risk

- The MSP cannot demonstrate proper oversight.
- Difficult to defend admin actions or access.
- High reputational risk after incidents.
- Increased chance of blame during disputes.

No unified logs = no tenant-level evidence.

Common MSP mistakes related to the Unified Audit Log

As an MSP IT administrator, common mistakes include:

- Assuming the Unified Audit Log is always enabled by default.
- Confusing it with mailbox audit logging.
- Disabling it temporarily and forgetting to re-enable.
- Not validating its status across all tenants.
- Not monitoring log retention or availability.

Severity summary

Area	Impact
Microsoft 365 availability	✓ No impact
User experience	✓ No impact
Tenant-wide visibility	✗ Critical loss
Incident response	✗ Severely impaired
Compliance	✗ High risk
MSP accountability	✗ High risk

Why use Acronis M365 security posture for Unified Audit Log with auto-remediation

The Unified Audit Log protects customers only if it is enabled continuously.

Acronis M365 Security Posture Management with auto-remediations ensures:

- Continuously monitors audit log status
- Flags deviations immediately
- Automatically re-enables the Unified Audit Log when disabled
- Prevents long-term blind spots caused by human error

This is critical because audit data cannot be recreated retroactively(!).

MSP operational benefits

For junior technicians

- No need to understand every Purview or M365 audit setting
- Clear signal: Deviated = Risk
- Auto-remediation ensures safe configuration
- Less chance of missing critical misconfiguration

For senior admins

- Reduced operational overhead
- Fewer unknown cause security events
- Consistent baseline enforcement
- Fewer security incidents with unknown cause

For customers

- Stronger security posture across Microsoft 365
- Faster and more accurate investigations
- Higher confidence in MSP-managed security
- Better compliance readiness

Note

Key takeaway:

- The Unified Audit Log captures all critical M365 activities across your entire tenant.
- If it's disabled, you lose visibility forever because audit data cannot be recreated retroactively.
- Acronis ensures this protection stays enforced automatically.

Authentication & Authorisation

What Authentication & Authorisation means in Microsoft 365 security

In Microsoft 365, Authentication & Authorisation controls who can sign in and what they are allowed to access once signed in.

Note

Think of it as:

- Authentication → Are you really who you claim to be?
- Authorisation → What are you allowed to do once inside?

This area is the front door and access control system for your Microsoft 365 environment.

Why Authentication & Authorisation are critical

Most Microsoft 365 security incidents start with:

- Stolen passwords
- Weak or missing Multi-Factor Authentication (MFA)
- Insecure or outdated login methods
- Over-permissive access

Authentication & Authorisation controls are designed to stop attackers before they get in, even if a password is compromised.

What these controls protect

The attached capabilities work together to protect:

User identities

- Enforce MFA using secure methods (Microsoft Authenticator)
- Control weaker methods (Email OTP)
- Secure how users register authentication details

Administrator access

- Restrict access to Microsoft Admin portals
- Restrict access to Azure portals
- Require stronger conditions for privileged accounts
- Prevent persistent admin sessions

Admins are high-value targets — these controls reduce the blast radius.

Devices and applications

- Block access from unknown or unsupported devices
- Require compliant or managed devices
- Restrict access to approved client apps
- Enforce application-level restrictions

This ensures access is granted only from trusted devices and apps.

Risk-based access decisions

- Require MFA when sign-in risk is detected
- Block legacy (older, insecure) authentication
- Prevent long-lived browser sessions

This allows Microsoft 365 to adapt security based on risk, not just static rules.

Third-party and application access

- Control user consent for apps
- Use Admin Consent Workflow for high-risk permissions
- Ensure only vetted applications gain access

This prevents shadow IT and excessive app permissions.

Microsoft internal access (Customer Lockbox)

- Requires explicit approval before Microsoft engineers can access data
- Ensures transparency and accountability

What means security maturity

Authentication & Authorisation status	Security meaning
Policies enforced consistently	✓ Strong identity security
Policies partially enforced	! Gaps attackers can exploit
Policies missing	✗ High risk of account compromise

Strong authentication controls are the single most effective way to prevent breaches.

Business impact of strong Authentication & Authorisation

With these controls in place:

- Stolen passwords alone are not enough to breach accounts
- Admin access is tightly controlled
- Access is continuously verified
- Risk is reduced without impacting daily productivity

Without them:

- One phished password can lead to full tenant compromise.
- Incidents are harder to contain.
- Compliance and accountability suffer.

How this fits with Acronis M365 security posture management

Authentication & Authorisation settings are:

- Numerous
- Interconnected
- Easy to weaken accidentally

Acronis M365 security posture management:

- Continuously checks these controls
- Detects missing or weakened policies
- Auto-remediates safe configurations
- Ensures identity security does not drift over time

Note

Key takeaway:

- Authentication & Authorisation decide who gets in and what they can do.

Strong controls stop attacks at the door. Continuous Acronis M365 security posture management ensures those controls stay strong over time.

Admin Consent Workflow

What is the Admin Consent Workflow in Microsoft Entra ID

The Admin Consent Workflow controls how applications request admin-level permissions in Microsoft Entra ID (Azure AD).

When a user tries to access an application that requires admin consent:

- The request is not automatically approved
- It is routed to designated reviewers
- Reviewers can approve or deny the request
- All actions are logged with a full audit trail

Note

This control governs which applications are allowed to access tenant data at a high privilege level.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-admin-consent-workflow is official Microsoft Learn documentation.

Why Microsoft provides this control

Microsoft provides the Admin Consent Workflow to:

- Prevent uncontrolled application access
- Reduce the risk of malicious or overly-permissive apps
- Protect sensitive tenant data (mail, files, users)
- Enforce least-privilege and Zero Trust principles
- Provide accountability and traceability for applications approvals

Applications are a major attack vector when granted excessive permissions.

What happens when the Admin Consent Workflow is enabled (recommended)

When the admin consent workflow is enabled:

- Users cannot self-approve high-risk app permissions
- App requests are reviewed by authorized admins
- Only approved applications gain elevated access
- Approval and denial actions are logged
- Shadow IT is reduced at minimum

Benefits:

- Strong control over third-party and internal applications
- Reduced risk of data exfiltration via malicious applications
- Improved governance and compliance
- Clear ownership of app access decisions

This ensures applications are trustable before accessing data.

What happens when the Admin Consent Workflow is Disabled

Warning!
If the workflow is disabled or overly permissive:

- Users may grant apps excessive permissions
- Malicious apps can access mail, files, or directory data
- App access spreads without oversight
- Difficult to identify who approved what and why
- Breaches via OAuth apps become more likely

OAuth-based attacks often bypass MFA and user sign-in protections.

Important clarification (commonly misunderstood)

This control applies to:

Apps requesting admin-level permissions

It does not block:

- All app access.
- User-level consent (unless configured separately).

It complements:

- Conditional Access.
- Audit logging.

Note
The workflow protects against privileged app access, not normal user apps.

Real risks for an MSP

Security risk

- Malicious apps gain persistent access.
- Data can be accessed without user interaction.
- Attacks bypass traditional sign-in defenses.

Compliance & audit risk

- If a client asks: Who approved this app to access our data?

Without the workflow: The answer may be unclear or unavailable.

MSP liability risk

- Uncontrolled app consent is difficult to defend
- OAuth breaches are high-impact incidents
- Lack of approval trail damages trust

Severity summary

Area	Impact
User experience	❗ Minor (approval required)
Applications governance	❌ Weak without workflow
Data protection	❌ High risk

Area	Impact
OAuth attack exposure	❌ High
Compliance posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Managemen for Admin Consent Workflow with Auto-remediation

The Admin Consent Workflow is critical because:

- It is often disabled for convenience
- Changes can go unnoticed
- Manual checks do not scale across tenants
- One malicious app can cause widespread damage

Acronis M365 Security Posture Management:

- Continuously verifies the workflow is enabled
- Detects disabled or misconfigured approval flows
- Flags deviations from security baselines
- Automatically restores secure approval settings
- Ensures consistent app governance across tenants

Note
This ensures only approved applications gain elevated access.

MSP operational benefits

For Junior Technicians

- Clear rule: Apps needing admin consent must be reviewed
- No need to understand OAuth internals
- Workflow enforces safe configurations
- Fewer app-related security incidents

For Senior Administrators

- Strong control over application permissions
- Reduced OAuth-based attack surface
- Clear audit trail for approvals
- Easier compliance and security reviews

For Customers

- Better protection of tenant data
- Reduced risk from malicious or risky apps
- Transparent app approval process
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Applications can be as powerful as users — sometimes more.
- Admin Consent Workflow ensures apps earn trust before accessing data.
- Acronis keeps this control enforced automatically.

Authentication Method Policy - Email OTP

What is Email One-Time Passcode (OTP) in Microsoft 365

Email One-Time Passcode (OTP) is an authentication method where a temporary, single-use code is sent to a user’s email address to verify their identity.

Email OTP is used in two specific scenarios:

- Internal users (employees) → Only for self-service password recovery (SSPR)
- External (guest) users without a managed identity → Can be used as a sign-in method

Note

Email OTP provides a basic verification mechanism when stronger identity options are not available.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode.

Why Microsoft provides Email OTP

Microsoft provides Email OTP to:

- Enable access for external users who don't have Azure AD / Entra ID accounts
- Allow collaboration without forcing guest users to create full identities
- Support password recovery for internal users
- Reduce friction in external collaboration scenarios

Email OTP is designed for convenience and reach, not maximum security.

What happens when Email OTP is Enabled

When Email OTP is enabled correctly:

For internal users

- Used only for password recovery, not normal sign-in
- Provides a fallback recovery option
- Reduces helpdesk tickets for password resets

For external (guest) users

- Enables secure access without unmanaged passwords
- Provides time-limited authentication
- Prevents permanent credentials for temporary collaborators

Benefits:

- Simplifies external collaboration.
- Improves user experience.
- Reduces administrative overhead.
- Supports controlled guest access.

This makes Email OTP useful for low-risk, temporary access scenarios.

What happens when Email OTP is Disabled

If Email OTP is treated as a primary or unrestricted authentication method:

Warning!

- Security strength depends on the security of the user's email
- Compromised external mailboxes can be reused
- Phishing attacks can capture OTP codes
- No device or location trust is enforced
- Lower assurance compared to MFA apps or FIDO keys

Email OTP is not equivalent to strong MFA.

Important clarification (commonly misunderstood)

Email OTP is:

- Acceptable for guest users.
- Acceptable for password recovery.

Email OTP is not recommended as:

- A primary sign-in method for internal users
- A replacement for Microsoft Authenticator or strong MFA

Note

Email OTP should be limited, intentional, and monitored.

Real risks for an MSP

Security risk

- Overuse weakens overall authentication posture.
- External access depends on unknown email security.
- Increased phishing exposure.

MSP liability risk

- Weak authentication choices are hard to justify after incidents.
- External access incidents can impact trust.
- Poor documentation of access methods increases risk.

Severity summary

Area	Impact
User experience	✓ Easy access
External collaboration	✓ Flexible
Authentication strength	✗ Lower
Phishing resistance	✗ Limited
Compliance posture	! Depends on use
MSP accountability	! Requires justification

Why use Acronis M365 Security Posture Management for Email OTP with Auto-remediation

Email OTP is safe only when used in the right context.

Acronis M365 Security Posture Management:

- Detects where Email OTP is enabled
- Ensures it is limited to approved use cases
- Flags risky configurations
- Helps enforce stronger authentication where required
- Maintains visibility over external access paths

Note

This ensures convenience does not quietly override security.

MSP operational benefits

For Junior Technicians

- Clear guidance: Email OTP is not full MFA
- Reduced risk of misconfiguration
- Safe defaults enforced automatically

For Senior Administrators

- Stronger authentication posture
- Clear separation between convenience and security
- Easier justification during audits

For Customers

- Simple access for external users
- Reduced friction in collaboration
- Confidence that security remains appropriate

Note

Key takeaway:

- Email One-Time Passcode is a convenience control, not a strong security control.
- Used correctly, it enables safe collaboration. Used incorrectly, it weakens authentication.
- Acronis M365 security posture management ensures it stays in the right role.

Authentication Method Policy - Microsoft Authenticator

What is the Microsoft Authenticator Authentication Method Policy

The Microsoft Authenticator authentication method policy controls how Microsoft Authenticator is used for:

- Push-based MFA approvals
- Passwordless authentication
- Which users or groups can use Authenticator
- Whether additional context (app name, location, companion app) is shown in approval prompts

Note

This policy defines how secure and informative authentication prompts are.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-authenticator-app.

Why Microsoft provides this control

Microsoft provides this policy to:

- Strengthen MFA against push-based attacks
- Enable secure passwordless authentication
- Reduce MFA fatigue
- Support modern, phishing-resistant authentication methods

Authentication prompts without context are easy to abuse.

What happens when the policy is properly Enabled (recommended)

When the Microsoft Authenticator policy is configured securely:

- Only approved users can use Authenticator
- Passwordless sign-in is supported
- Push notifications include app name and location
- Number matching or contextual prompts reduce abuse
- MFA approvals are more intentional and secure

Benefits:

- Reduced risk of MFA fatigue attacks.
- Stronger defense against credential compromise.
- Better user decision-making during sign-in.
- Improved overall identity security posture.

This turns MFA from a blind approval step into a trusted security signal.

What happens when the policy is Disabled or misconfigured

If the policy is not enforced or lacks context controls:

Warning!

- Users may approve malicious MFA requests
- MFA fatigue and push-bombing attacks succeed
- Passwordless authentication may be unavailable
- Sign-in approvals lack meaningful context
- Account compromise becomes more likely

Attackers commonly rely on user confusion, not technical bypass.

Important clarification (commonly misunderstood)

This policy:

- Does not replace Conditional Access.
- Controls how MFA is presented and approved.

Strong MFA requires:

- Modern authentication.
- Conditional Access.
- Contextual Authenticator prompts.
- MFA without context is significantly weaker.

Real risks for an MSP

Security risk

- MFA fatigue attacks succeed.
- Compromised credentials still lead to account takeover.
- Passwordless benefits are not realized.

Compliance & audit risk

- If a client asks: Why did the user approve this sign-in?
- Without context: They saw a generic prompt and tapped Approve.

MSP liability risk

- Weak MFA configuration is hard to defend post-incident.
- Identity breaches damage trust.
- MSP security maturity may be questioned.

Severity summary

Area	Impact
Sign-in availability	✓ No impact
User experience	! Minor change (more context)
MFA effectiveness	✗ Reduced if misconfigured
Account takeover risk	✗ High
Identity security posture	✗ At risk
MSP accountability	✗ High risk

Why use Acronis M365 Security Posture Management for Authentication Method Policy - Microsoft Authenticator with Auto-remediation

This policy is critical because:

- It evolves as Microsoft improves MFA defenses
- Misconfiguration weakens all MFA protections
- Manual validation across tenants does not scale
- Small gaps lead to high-impact identity breaches

Acronis M365 Security Posture Management:

- Continuously verifies Authenticator policy settings
- Detects missing or weak configurations
- Flags deviations from secure identity baselines
- Automatically restores recommended settings
- Keeps MFA protections aligned across all tenants

Note
This ensures MFA stays strong, contextual, and phishing-resistant.

MSP operational benefits

For Junior Technicians

- Clear rule: Authenticator prompts must show context
- No need to master identity attack techniques
- Auto-remediation enforces safe defaults
- Fewer identity-related incidents

For Senior Administrators

- Stronger, consistent MFA posture
- Reduced account takeover incidents
- Easier audit and compliance explanations
- Improved Zero Trust alignment

For Customers

- Safer sign-in experience
- Reduced risk of accidental MFA approvals
- Better protection of accounts and data
- Higher trust in MSP-managed identity security

Note

Key takeaway:

- MFA is only as strong as the prompt users approve.
- Contextual Microsoft Authenticator policies stop fatigue attacks.
- Acronis ensures these protections stay enforced automatically.

Conditional Access Policy - Application Enforced Restrictions For Unmanaged Devices

What is Conditional Access – App-Enforced Restrictions in Microsoft Entra ID

App-enforced restrictions is a Conditional Access policy that controls how users access SharePoint Online, OneDrive for Business, and Exchange Online when they are using unmanaged or non-compliant devices.

Instead of fully blocking access, the policy can:

- Allow access only through web apps
- Restrict actions such as:
  - Downloading files
  - Syncing content
  - Copying sensitive data
  - Enforce read-only or limited access

Note
This policy protects data based on device trust, not just user identity.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-app-enforced-restrictions.

Why Microsoft provides this control

Microsoft provides app-enforced restrictions to:

- Prevent data leakage from unmanaged devices
- Support Bring-Your-Own-Device (BYOD) scenarios safely
- Enforce Zero Trust principles
- Reduce risk when users access data from personal or unknown devices
- Maintain productivity without sacrificing security

Note
Identity alone is not enough — device trust matters.

What happens when the policy is Enabled (recommended)

When app-enforced restrictions are enabled:

- Users on unmanaged devices have limited access
- Downloads and sync are blocked or restricted
- Sensitive data stays within managed environments
- Risky access is controlled without full denial
- Data exfiltration risk is reduced

Benefits:

- Strong protection against data leakage.
- Secure BYOD access.
- Reduced need for full access blocking.
- Improved overall data governance.

This provides secure access without blind trust.

What happens when the policy is Disabled

If app-enforced restrictions are not in place:

Warning!

- Unmanaged devices may have full data access
- Files can be downloaded to personal devices
- Sensitive information can leave the organization
- Data loss incidents become more likely
- Investigations are harder after leaks

Unmanaged devices are a primary data-exfiltration vector.

Important clarification (commonly misunderstood)

This policy:

- Does not require device enrollment.
- Works at the application access level.

It complements:

- Device compliance policies.
- DLP
- Audit logging.
- It does not replace endpoint management.

Real risks for an MSP

Security risk

- Data copied to personal devices.
- Loss of visibility and control.
- Increased insider and accidental leakage risk.

Compliance & audit risk

- If a client asks: How do you prevent data from leaving via personal devices?

Without this policy: The answer may be incomplete.

MSP liability risk

- Data leaks are high-impact incidents
- Weak device-based controls are hard to justify
- Trust in MSP security posture is reduced

Severity summary

Area	Impact
Service availability	✓ No impact
User experience	❗ Limited access on unmanaged devices
Data leakage risk	✖ High if missing
BYOD security	✖ Weak without policy
Compliance posture	✖ At risk
MSP accountability	✖ High risk

Why use Acronis M365 Security Posture Management for App-Enforced Restrictions with Auto-remediation

This policy is critical because:

- It applies tenant-wide
- Exceptions are easy to introduce
- Manual validation does not scale
- One permissive change can expose large volumes of data

Acronis M365 Security Posture Management:

- Continuously verifies Conditional Access enforcement
- Detects disabled or weakened app-enforced restrictions
- Flags deviations from approved baselines
- Automatically restores protective configurations
- Maintains consistent Zero Trust posture across tenants

Note
This ensures data access always respects device trust.

MSP operational benefits

For Junior Technicians

- Clear rule: Unmanaged device = restricted access
- No need to deeply understand Conditional Access internals

- Auto-remediation prevents accidental exposure
- Fewer data-leak investigations

For Senior Administrators

- Stronger Zero Trust enforcement
- Reduced data-exfiltration incidents
- Easier governance and audits
- Better alignment with security frameworks

For Customers

- Safer access from personal devices
- Reduced risk of sensitive data leakage
- Improved compliance and governance
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Identity alone is not enough — device trust matters.
- App-enforced restrictions keep data inside controlled environments.
- Acronis ensures this protection stays enforced automatically.

Conditional Access Policy - Block Legacy Authentication

What is Conditional Access – MFA Strength / Legacy Authentication Blocking

This Conditional Access policy enforces modern, strong authentication methods and blocks legacy authentication protocols that do not support modern security controls such as MFA, Conditional Access, and risk evaluation.

Legacy authentication includes protocols like:

- IMAP
- POP
- SMTP AUTH (basic)
- Older Exchange and Office clients using username + password only

Note

This policy ensures only secure, modern authentication methods are allowed.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-legacy-authentication.

Why Microsoft provides this control

Microsoft provides this policy to:

- Prevent credential-based attacks
- Eliminate MFA bypass paths
- Enforce Zero Trust identity standards
- Reduce attack surface from outdated protocols
- Align tenants with modern security expectations

Legacy authentication is one of the most abused attack vectors in Microsoft 365 environments.

What happens when the policy is Enabled (recommended)

When legacy authentication is blocked via Conditional Access:

- MFA is consistently enforced
- Conditional Access rules cannot be bypassed
- Password-only authentication is blocked
- Credential-stuffing and password-spray attacks are reduced
- Identity security posture is significantly strengthened

Benefits:

- Strong reduction in account compromise.
- Consistent identity enforcement across services.
- Better alignment with Zero Trust principles.
- Fewer security incidents related to stolen credentials.

This removes entire classes of identity attacks.

What happens when the policy is Disabled

If legacy authentication is still allowed:

Warning!

- MFA can be bypassed
- Password-only logins remain possible
- Attackers exploit old protocols
- Credential-spray attacks succeed
- Compromised accounts go unnoticed longer

Many identity breaches occur even when MFA is enabled, due to legacy auth paths.

Important clarification (commonly misunderstood)

MFA alone is not enough

If legacy authentication is allowed:

- MFA may not be enforced
- Conditional Access may not apply

This policy complements:

- Modern Authentication.
- Authentication policies.
- MFA registration and enforcement.

Note
Blocking legacy authentication is mandatory for effective MFA.

Real risks for an MSP

Security risk

- Attackers exploit legacy protocols to bypass MFA.
- Compromised accounts can persist silently.
- Identity incidents escalate quickly.

Compliance & audit risk

- If a client asks: Why did MFA not stop this breach?

If legacy auth was allowed: The answer is uncomfortable.

MSP liability risk

- Weak identity controls are hard to justify
- Identity breaches carry high reputational damage
- MSP security maturity may be questioned

Why use Acronis M365 Security Posture Management for Block Legacy Authentication with Auto-remediation

This policy is critical because:

- Legacy auth often remains enabled unintentionally
- Exceptions are created and forgotten

- Manual checks across tenants do not scale
- One legacy path can undermine all MFA controls

Acronis M365 Security Posture Management:

- Continuously verifies legacy authentication is blocked
- Detects exceptions and policy drift
- Flags deviations from secure baselines
- Automatically restores enforcement
- Ensures consistent identity protection across tenants

Note

This ensures MFA cannot be bypassed.

MSP operational benefits

For Junior Technicians

- Clear rule: Legacy authentication = risk
- No need to understand protocol-level details
- Auto-remediation prevents accidental exposure
- Fewer identity-related incidents

For Senior Administrators

- Strong, consistent identity security baseline
- Reduced account takeover incidents
- Easier audits and compliance discussions
- Clear Zero Trust alignment

For Customers

- Stronger protection against credential theft
- Fewer account compromises
- Improved security confidence
- Better compliance readiness

Note

Key takeaway:

- If legacy authentication is allowed, MFA can be bypassed.
- Blocking legacy authentication is mandatory for secure identity.
- Acronis ensures this protection stays enforced automatically.

Conditional Access Policy - Block Unknown Or Unsupported Device Access

What is Conditional Access – Block Unknown Or Unsupported Device Access in Microsoft Entra ID

Device type (platform) conditions in Conditional Access control which device platforms are allowed to access company resources.

Using these conditions, admins can:

- Allow access only from approved device types (Windows, macOS, iOS, Android)
- Block access when the device type is unknown or unsupported
- Apply different controls based on device platform

Note
This control ensures only recognized and supported device types can access corporate data.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-device-unknown-unsupported.

Why Microsoft provides this control

Microsoft provides device type conditions to:

- Reduce risk from unknown or untrusted devices
- Enforce predictable access paths
- Support Zero Trust (never trust unknown devices)
- Protect against access from unsupported or risky platforms
- Improve overall identity and device governance

Unknown devices represent unknown risk.

What happens when Block Unknown Or Unsupported Device Access is Enabled (recommended)

When Conditional Access blocks access from unknown or unsupported devices:

- Access is limited to approved platforms
- Shadow IT access paths are reduced
- Data exposure risk from exotic or unsafe devices is lowered

- Security posture becomes more predictable
- Investigation and auditing are simplified

Benefits:

- Reduced attack surface.
- Better alignment with device management strategy.
- Improved Zero Trust enforcement.
- Clear security boundaries.

This ensures resources are accessed only from known environments.

What happens when Block Unknown Or Unsupported Device Access is Disabled

If unknown or unsupported devices are allowed:

Warning!

- Attackers can use untrusted platforms
- Access may occur from insecure environments
- Device-based controls may not apply
- Data exfiltration risk increases
- Incidents become harder to investigate

Unknown devices often bypass expected security assumptions.

Important clarification (commonly misunderstood)

Unknown device does not mean malicious

It means:

- Platform is not recognized.
- Device is unsupported or unmanaged.

Note

Blocking unknown devices enforces predictability, not punishment.

Real risks for an MSP

Security risk

- Access from insecure or unsupported platforms.
- Reduced effectiveness of device-based controls.
- Increased data leakage risk.

Compliance & audit risk

- If a client asks: Which devices are allowed to access our data?

Without this control: The answer may be unclear.

MSP liability risk

- Weak device governance is hard to justify
- Data-leak incidents increase accountability risk
- Trust in MSP security posture is reduced

Severity summary

Area	Impact
Service availability	❗ Some devices blocked
User experience	❗ Limited to supported devices
Device governance	❌ Weak if missing
Data leakage risk	❌ High
Zero Trust posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Block Unknown Or Unsupported Device Access with Auto-remediation

Device type controls are critical because:

- They are easy to overlook
- Exceptions can be added quietly
- Manual review does not scale
- One unknown access path can expose sensitive data

Acronis M365 Security Posture Management:

- Continuously verifies device type conditions
- Detects access from unsupported platforms
- Flags deviations from approved baselines

- Automatically restores blocking rules
- Maintains consistent Zero Trust enforcement

Note

This ensures unknown devices never become trusted access paths.

MSP operational benefits

For Junior Technicians

- Clear rule: Unknown device = no access
- No need to master Conditional Access logic
- Auto-remediation prevents accidental exposure
- Fewer complex investigations

For Senior Administrators

- Stronger device governance
- Reduced data-exfiltration incidents
- Easier audits and reporting
- Better Zero Trust alignment

For Customers

- Better protection of company data
- Reduced risk from unmanaged or unknown devices
- Clear access boundaries
- Higher confidence in MSP-managed security

Note

Key takeaway:

- If the device is unknown, the risk is unknown.
- Blocking unknown device types keeps access predictable and secure.
- Acronis ensures this Zero Trust control stays enforced automatically.

Conditional Access Policy - Enforce MFA

What is Conditional Access – Enforce MFA for All Users

This Conditional Access policy requires Multi-Factor Authentication (MFA) for all users when accessing Microsoft 365 resources.

With this policy:

- Password-only sign-ins are no longer sufficient.
- Users must complete an additional verification step.
- MFA is enforced consistently across applications and locations.

Note

This policy ensures identity security does not rely on passwords alone.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-mfa-strength.

Why Microsoft provides this control

Microsoft provides tenant-wide MFA enforcement to:

- Protect against stolen or guessed passwords
- Reduce successful phishing and credential-stuffing attacks
- Enforce Zero Trust identity principles
- Standardize authentication security across all users
- Dramatically reduce account takeover risk

Passwords are easy to steal. MFA makes them much harder to abuse.

What happens when Enforce MFA is Enabled for all users (recommended)

When MFA is enforced via Conditional Access:

- All users must complete MFA
- Password-only access is blocked
- Account takeover risk drops significantly
- Security posture becomes consistent
- Identity attacks are harder to succeed

Benefits:

- Strong reduction in compromised accounts.
- Consistent protection across users and apps.
- Improved audit and compliance posture.
- Better resilience against phishing attacks.

This removes password-only access as a viable attack path.

What happens when Enforce MFA is Disabled or not Enabled for all users

If MFA is optional, partial, or inconsistent:

Warning!

- Some accounts remain password-only
- Phishing attacks succeed more easily
- Privileged or forgotten accounts are exposed
- Attackers target weaker users
- Incidents escalate quickly

Attackers always look for the weakest account.

Important clarification (commonly misunderstood)

MFA available ≠ MFA enforced

MFA must be enforced through:

Conditional Access

MFA enforcement must be combined with:

- Blocking legacy authentication
- Strong authentication methods

Note

MFA is effective only when it cannot be bypassed.

Real risks for an MSP

Security risk

- Password-only users are easily compromised.
- Attackers move laterally after first access.
- Identity incidents increase.

Compliance & audit risk

- If a client asks: Why was this account accessed without MFA?

Without enforcement: The answer is uncomfortable.

MSP liability risk

- Partial MFA is difficult to defend
- Identity breaches damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
Sign-in availability	❗ Slight user friction
User experience	❗ Additional verification
Account takeover risk	❌ High if missing
Identity posture	❌ At risk
Compliance	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Enforce MFA with Auto-remediation

Tenant-wide MFA enforcement is critical because:

- Exceptions accumulate over time
- Legacy access paths may bypass MFA
- Manual validation across tenants does not scale
- One non-MFA account undermines the entire posture

Acronis M365 Security Posture Management:

- Continuously verifies MFA enforcement
- Detects gaps or disabled policies
- Flags deviations from secure baselines
- Automatically restores MFA enforcement
- Ensures consistent identity protection across all tenants

Note
This ensures MFA is always enforced, not optional.

MSP operational benefits

For Junior Technicians

- Clear rule: All users must use MFA
- No need to manage per-user exceptions manually
- Auto-remediation prevents accidental exposure
- Fewer identity-related incidents

For Senior Administrators

- Strong, uniform identity security baseline
- Reduced account compromise incidents
- Easier audits and compliance discussions
- Clear Zero Trust alignment

For Customers

- Stronger protection against unauthorized access
- Reduced risk of phishing-based compromise
- Improved trust in security controls
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Passwords alone are no longer sufficient.
- Enforcing MFA for all users dramatically reduces account takeover risk.
- Acronis ensures this protection stays enforced automatically.

Conditional Access Policy - No persistent Browser Sessions

What is Conditional Access – No persistent Browser Sessions

This Conditional Access policy controls whether users are allowed to maintain persistent browser sessions when accessing Microsoft 365 resources.

When No persistent Browser Sessions is Enabled:

- Users must re-authenticate more frequently
- Browser sign-in cookies are not trusted indefinitely
- Long-lived sessions on shared or unmanaged devices are prevented

Note

This policy limits how long a browser session remains trusted.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-persistent-browser.

Why Microsoft provides this control

Microsoft provides persistent browser session controls to:

- Reduce risk from stolen or reused browser sessions
- Protect access from shared or public devices
- Limit damage from unattended or unlocked browsers
- Enforce Zero Trust principles (continuous verification)
- Reduce session-hijacking and walk-up access risk

A logged-in browser is often more valuable to attackers than a password.

What happens when No persistent Browser Sessions is Enabled (recommended)

When persistent browser sessions are disabled:

- Users must re-authenticate regularly
- Access from shared devices is safer
- Session hijacking risk is reduced
- Stolen browser cookies become less useful
- Unauthorized long-term access is prevented

Benefits:

- Strong reduction in unauthorized access risk.
- Better protection on unmanaged and public devices.
- Reduced impact of unattended sign-in sessions.
- Improved Zero Trust enforcement.

This ensures access is continuously re-validated.

What happens when No persistent Browser Sessions is Disabled

If persistent browser sessions are allowed:

Warning!

- Sessions can remain active for long periods
- Shared devices may retain authenticated access
- Stolen cookies can be reused by attackers
- Walk-up access becomes possible
- Incident detection is delayed

Persistent sessions are a silent access risk, especially outside managed devices.

Important clarification (commonly misunderstood)

This policy:

- Does not log users out immediately.
- Controls how long browsers stay authenticated.

It complements:

- MFA enforcement.
- Device-based controls.

Note

MFA at sign-in does not protect long-lived sessions.

Real risks for an MSP

Security risk

- Unauthorized access from shared or unattended devices.
- Session hijacking via stolen cookies.
- Reduced effectiveness of identity protections.

Compliance & audit risk

- If a client asks How did someone access data without logging in again?

With persistent sessions allowed: The answer is uncomfortable.

MSP liability risk

- Weak session controls are hard to justify
- Data access incidents damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
Sign-in availability	❗ More frequent sign-ins
User experience	❗ Slight inconvenience
Session hijacking risk	❌ High if allowed
Shared device security	❌ Weak without control
Zero Trust posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Persistent Browser Session Control with Auto-remediation

This policy is critical because:

- It is often left at default settings
- Convenience pressure encourages persistence
- Manual review across tenants does not scale
- One persistent session can expose sensitive data

Acronis M365 Security Posture Management:

- Continuously verifies persistent browser controls
- Detects overly permissive session settings
- Flags deviations from secure baselines
- Automatically restores safe configurations
- Maintains consistent Zero Trust session controls

Note
This ensures sessions expire when trust expires.

MSP operational benefits

For Junior Technicians

- Clear rule: Browsers should not stay logged in forever
- No need to master session-management internals
- Auto-remediation prevents accidental exposure
- Fewer unexplained access incidents

For Senior Administrators

- Stronger control over session lifetime
- Reduced unauthorized access incidents
- Better Zero Trust alignment
- Easier audit explanations

For Customers

- Safer access from shared or personal devices
- Reduced risk of unauthorized data access
- Stronger protection without blocking productivity
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Authentication is not a one-time event.
- Persistent sessions increase risk on shared and unmanaged devices.
- Acronis ensures session trust expires automatically.

Conditional Access Policy - Require Approved Client Apps

What is Conditional Access – Require Approved Client Apps

This Conditional Access policy ensures that users can access Microsoft 365 resources only through approved client applications or through apps that are protected by App Protection Policies (APP).

With this policy enforced:

- Access is limited to trusted, managed apps.
- Data accessed through mobile or unmanaged endpoints is protected.
- Unapproved or risky apps are blocked.

Note

This policy controls which applications are trusted to handle organizational data.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-approved-app-or-app-protection.

Why Microsoft provides this control

Microsoft provides this policy to:

- Prevent data leakage through unmanaged or risky apps
- Enforce secure access on mobile and BYOD devices
- Support Zero Trust principles
- Ensure data is accessed only via apps that can enforce protections
- Reduce risk from third-party or outdated applications

Untrusted apps are a common data-loss vector, especially on mobile devices.

What happens when Require Approved Client Apps is Enabled (recommended)

When access is limited to approved or protected apps:

- Only trusted apps can access company data
- App-level protections (encryption, copy/paste control) apply
- Data leakage risk is reduced
- Mobile access becomes safer
- Security posture is strengthened without blocking productivity

Benefits:

- Strong control over mobile and BYOD data access.
- Reduced reliance on device trust alone.
- Better enforcement of data protection rules.
- Improved Zero Trust alignment.

This ensures data follows security controls, not just users.

What happens when the policy is Disabled

If users can access data through any app:

Warning!

- Unmanaged or insecure apps may access company data
- Data can be copied, saved, or shared outside control
- App-level protections cannot be enforced
- Data leakage incidents increase
- Investigations become harder

Attackers and shadow IT both exploit weak app controls.

Important clarification (commonly misunderstood)

This policy:

- Does not require full device management.
- Works even on personal devices.

It complements:

- App Protection Policies.
- Device-based Conditional Access.
- Audit logging.

Note
App trust can be enforced without full device control.

Real risks for an MSP

Security risk

- Sensitive data accessed through untrusted apps.
- Increased chance of accidental or malicious data leakage.
- Limited visibility into app-level data handling.

Compliance & audit risk

- If a client asks: Which apps are allowed to access our data?

Without this policy: The answer may be unclear.

MSP liability risk

- Weak app governance is hard to justify
- Data leakage incidents damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
Service availability	❗ Some apps blocked
User experience	❗ Restricted to approved apps
Data leakage risk	❌ High if missing

Area	Impact
App governance	❌ Weak without policy
Zero Trust posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Require Approved Client Apps with Auto-remediation

This policy is critical because:

- App exceptions accumulate over time
- Shadow IT grows silently
- Manual app reviews do not scale
- One unprotected app can leak large amounts of data

Acronis M365 Security Posture Management:

- Continuously verifies approved app enforcement
- Detects overly permissive app access
- Flags deviations from secure baselines
- Automatically restores enforcement
- Maintains consistent app-level Zero Trust controls

Note

This ensures only trusted apps can handle company data.

MSP operational benefits

For Junior Technicians

- Clear rule: Only approved or protected apps are allowed
- No need to master mobile security internals
- Auto-remediation prevents accidental exposure
- Fewer data-leak incidents

For Senior Administrators

- Strong app governance across tenants
- Reduced mobile and BYOD risk
- Easier audits and compliance discussions
- Better Zero Trust enforcement

For Customers

- Safer mobile and BYOD access
- Reduced risk of data leakage
- Stronger protection without blocking productivity
- Higher confidence in MSP-managed security

Note

Key takeaway:

- Data security depends on the apps that access it.
- Approved and protected apps keep data under control.
- Acronis ensures this protection stays enforced automatically.

Conditional Access Policy - Require Compliant Or Hybrid Azure AD Joined Device.

What is Conditional Access – Require Compliant Or Hybrid Azure AD Joined Device

This Conditional Access policy requires that administrative (privileged) users sign in only from devices that are compliant or Hybrid Azure AD joined.

With this policy enforced:

- Admins must use managed, trusted devices.
- Access from personal, unmanaged, or unknown devices is blocked.
- High-risk admin actions are limited to controlled environments.

Note

This policy protects privileged access, which represents the highest security risk in a tenant.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-alt-admin-device-compliand-hybrid.

Why Microsoft provides this control

Microsoft provides this control to:

- Protect privileged identities from compromise
- Reduce risk of admin credential theft
- Prevent admin access from unsafe or infected devices

- Enforce Zero Trust for high-impact accounts
- Limit blast radius if an admin account is targeted

Admin accounts have disproportionate power — they must have disproportionate protection.

What happens when the policy is enabled (recommended)

When admins are restricted to compliant or hybrid-joined devices:

- Admin access is limited to managed devices
- Malware-infected or personal devices are blocked
- Privileged actions occur in controlled environments
- Credential theft risk is reduced
- Overall tenant security posture improves

Benefits:

- Strong protection of privileged access.
- Reduced likelihood of tenant-wide compromise.
- Better auditability of admin actions.
- Clear separation between admin and user access.

This enforces secure workstation principles for admins.

What happens when the policy is Disabled

If admins can sign in from unmanaged or unknown devices:

Warning!

- Admin credentials can be stolen via malware
- Personal or shared devices become attack paths
- One compromised admin can impact the entire tenant
- Investigations become harder
- Breaches escalate quickly

Most catastrophic M365 incidents start with admin access from an unsafe device.

Important clarification (commonly misunderstood)

This policy:

- Does not affect standard users.
- Applies only to privileged roles.

It complements:

- MFA enforcement.
- Privileged Identity Management (PIM).
- Audit logging.

Note
MFA alone is not sufficient for admin protection.

Real risks for an MSP

Security risk

- Full tenant compromise from one infected admin device.
- Loss of control over identity, mail, and data.
- Difficult containment once admin access is abused.

Compliance & audit risk

- If a client asks: How do you protect admin access?

Without this policy: The answer is uncomfortable.

MSP liability risk

- Admin compromise is hard to defend
- High reputational damage after incidents
- MSP security maturity may be questioned

Severity summary

Area	Impact
Admin sign-in availability	❗ Restricted to managed devices
User experience (admins)	❗ Controlled access
Privileged access security	❌ High risk if missing
Tenant compromise risk	❌ Critical
Zero Trust posture	❌ At risk
MSP accountability	❌ Very high risk

Why use Acronis M365 Security Posture Management for Require Compliant Or Hybrid Azure AD Joined Device with Auto-remediation

This policy is critical because:

- Admin exceptions are often added temporarily
- Drift happens quietly over time
- Manual checks do not scale across tenants
- One gap can expose the entire environment

Acronis M365 Security Posture Management:

- Continuously verifies admin device restrictions
- Detects missing or weakened enforcement
- Flags deviations from secure baselines
- Automatically restores compliant configurations
- Maintains strong protection for privileged access

Note
This ensures admin access is always device-trusted.

MSP operational benefits

For Junior Technicians

- Clear rule: Admins must use managed devices
- No need to manage per-admin exceptions
- Auto-remediation prevents risky shortcuts
- Fewer catastrophic incidents

For Senior Administrators

- Strong privileged access controls
- Reduced tenant-wide breach risk
- Easier audits and security reviews
- Better alignment with Microsoft best practices

For Customers

- Strong protection of administrative access
- Reduced risk of full tenant compromise
- Higher trust in MSP security controls
- Better compliance and governance posture

Note

Key takeaway:

- Admins are the keys to the kingdom.
- If admin access isn't device-trusted, the tenant isn't secure.
- Acronis ensures privileged access stays protected automatically.

Conditional Access Policy - Restrict Access To Azure Portal

What is Conditional Access – Restrict Access (Require MFA) To Azure Portal Require MFA for Azure Management

This Conditional Access policy requires Multi-Factor Authentication (MFA) whenever users access Azure management services, such as:

- Azure Portal
- Azure CLI
- Azure PowerShell
- Azure Resource Manager APIs

Note

This policy protects management-plane access, which controls cloud resources, subscriptions, and configurations.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-old-require-mfa-azure-mgmt.

Why Microsoft provides this control

Microsoft provides this policy to:

- Protect Azure subscriptions and resources
- Prevent unauthorized changes to cloud infrastructure
- Reduce risk from stolen or reused credentials
- Enforce Zero Trust for management operations
- Prevent privilege abuse and cloud takeover

Azure management access can:

- Create or delete resources.
- Modify security settings.
- Exfiltrate data.
- Disable protections.

Note

This access must never rely on passwords alone.

What happens when MFA is enforced for Azure management(recommended)

When MFA is enforced for Azure management:

- All management access requires MFA
- Password-only admin access is blocked
- Stolen credentials alone are insufficient
- Unauthorized infrastructure changes are prevented
- Cloud security posture is significantly strengthened

Benefits:

- Strong protection of subscriptions and resources.
- Reduced risk of cloud environment takeover.
- Better audit and compliance posture.
- Clear separation between user access and admin access.

This ensures high-impact actions require strong verification.

What happens when MFA is Disabled for Azure management

If Azure management access does not require MFA:

Warning!

- Password-only access to Azure is possible
- Attackers can take over subscriptions
- Security controls can be disabled remotely
- Resources can be deleted or modified
- Breaches escalate rapidly and silently

Many severe cloud breaches start with unprotected management access.

Important clarification (commonly misunderstood)

MFA for user sign-in ≠ MFA for Azure management

This policy applies to:

- Azure Portal.
- Azure APIs.

It complements:

- Admin MFA policies.
- Audit logging.

Note
MFA must be enforced per access type, not assumed globally.

Real risks for an MSP

Security risk

- Full subscription compromise.
- Loss of cloud resources.
- Security controls disabled by attackers.

Compliance & audit risk

- If a client asks How do you protect Azure administrative access?

Without this policy: The answer may be non compliant.

MSP liability risk

- Cloud breaches are high-impact and visible
- Weak admin protections are hard to justify
- MSP credibility and trust are at risk

Severity summary

Area	Impact
Azure management availability	❗ MFA required
Admin user experience	❗ Additional verification
Cloud takeover risk	❌ Critical if missing
Infrastructure integrity	❌ At risk

Area	Impact
Compliance posture	❌ At risk
MSP accountability	❌ Very high risk

Why use Acronis M365 Security Posture Management for Azure Management MFA with Auto-remediation

This policy is critical because:

- It is sometimes overlooked
- Exceptions accumulate over time
- Manual verification across tenants does not scale
- One unprotected admin can compromise everything

Acronis M365 Security Posture Management:

- Continuously verifies MFA enforcement for Azure management
- Detects disabled or weakened policies
- Flags deviations from secure baselines
- Automatically restores MFA enforcement
- Ensures consistent protection of cloud management access

Note

This ensures cloud control planes are always protected.

MSP operational benefits

For Junior Technicians

- Clear rule: Azure management always requires MFA
- No need to understand Azure internals deeply
- Auto-remediation prevents dangerous shortcuts
- Fewer catastrophic incidents

For Senior Administrators

- Strong protection of cloud infrastructure
- Reduced risk of tenant-wide or subscription-wide compromise
- Easier audits and compliance discussions
- Better alignment with Microsoft security best practices

For Customers

- Strong protection of cloud resources
- Reduced risk of infrastructure compromise
- Higher trust in MSP-managed cloud security
- Better governance and compliance readiness

Note
Key takeaway:

- Azure management access controls the entire cloud environment.
- If it's not protected by MFA, everything is at risk.
- Acronis ensures this critical protection stays enforced automatically.

Conditional Access Policy - Restrict Access To Microsoft Admin Portal

What is Conditional Access – Restrict Access (Require MFA) To Microsoft Admin Portal

This Conditional Access policy requires Multi-Factor Authentication (MFA) whenever users access Microsoft administrative portals, including:

- Microsoft 365 Admin Center
- Microsoft Entra Admin Center
- Exchange Admin Center
- SharePoint Admin Center
- Defender & Security portals

Note
This policy protects high-privilege management interfaces used to configure and control Microsoft 365 services.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-old-require-mfa-admin-portals.

Why Microsoft provides this control

Microsoft provides this policy to:

- Protect administrative portals from unauthorized access
- Prevent attackers from modifying tenant-wide settings
- Enforce Zero Trust for management access

- Reduce risk from stolen or reused credentials
- Limit damage from compromised admin accounts

Admin portals are high-impact targets for attackers.

What happens when MFA is enforced for admin portals (recommended)

When MFA is enforced for admin portals:

- Password-only admin access is blocked
- Stolen credentials alone are insufficient
- Unauthorized configuration changes are prevented
- Tenant-wide security controls are protected
- Overall admin security posture improves

Benefits:

- Strong protection of management interfaces.
- Reduced risk of tenant-wide compromise.
- Better audit and compliance posture.
- Clear enforcement of privileged access security.

This ensures admin access requires strong verification.

What happens when MFA is Disabled for admin portals

If admin portals do not require MFA:

Warning!

- Password-only access to admin portals is possible
- Attackers can disable security controls
- Tenant settings can be modified silently
- Full tenant compromise becomes likely
- Incidents escalate rapidly

Many Microsoft 365 breaches start with unprotected admin portal access.

Important clarification (commonly misunderstood)

MFA for user sign-in ≠ MFA for admin portals

Admin portals require separate enforcement

This policy complements:

- Admin MFA enforcement.
- Privileged Identity Management (PIM).
- Audit logging.

Note
Admin access must be protected at every entry point.

Real risks for an MSP

Security risk

- Tenant-wide configuration abuse.
- Disabling of security protections.
- Loss of control over services and data.

Compliance & audit risk

- If a client asks: How do you protect administrative access?

Without this policy: The answer is uncomfortable.

MSP liability risk

- Admin compromise has high reputational impact
- Weak admin protections are hard to justify
- MSP credibility and trust are at risk

Severity summary

Area	Impact
Admin portal availability	❗ MFA required
Admin user experience	❗ Additional verification
Tenant compromise risk	❌ Critical if missing
Security posture	❌ At risk
Compliance posture	❌ At risk
MSP accountability	❌ Very high risk

Why use Acronis M365 Security Posture Management for Restrict Access To Microsoft Admin Portal with Auto-remediation

This policy is critical because:

- It is sometimes assumed but not enforced
- Exceptions accumulate over time
- Manual validation across tenants does not scale
- One unprotected admin can compromise the entire tenant

Acronis M365 Security Posture Management:

- Continuously verifies MFA enforcement for admin portals
- Detects disabled or weakened policies
- Flags deviations from secure baselines
- Automatically restores MFA enforcement
- Ensures consistent protection of management access

Note
This ensures admin portals are never accessible without MFA.

MSP operational benefits

For Junior Technicians

- Clear rule: Admin portals always require MFA
- No need to remember per-portal rules
- Auto-remediation prevents dangerous shortcuts
- Fewer catastrophic incidents

For Senior Administrators

- Strong, consistent admin access protection
- Reduced tenant-wide breach risk
- Easier audits and compliance discussions
- Better alignment with Microsoft security best practices

For Customers

- Strong protection of administrative access
- Reduced risk of tenant compromise
- Higher confidence in MSP-managed security
- Improved governance and compliance readiness

Note

Key takeaway:

- Admin portals control everything.
- If they aren't protected by MFA, the tenant isn't protected.
- Acronis ensures this critical protection stays enforced automatically.

Conditional Access Policy - Securing Security Info Registration

What is Conditional Access – Securing Security Info Registration

This Conditional Access policy controls how users register or update their security information, such as:

- MFA methods
- Phone numbers
- Authenticator apps
- Passwordless credentials

When enforced, the policy ensures that security information registration occurs only under secure conditions, such as:

- From trusted locations
- With MFA already completed
- From managed or compliant devices

Note

This policy protects the foundation of identity security: authentication methods themselves.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-security-info-registration.

Why Microsoft provides this control

Microsoft provides secure registration controls to:

- Prevent attackers from registering their own MFA methods
- Protect accounts after credential compromise
- Ensure authentication methods are set up in trusted conditions
- Reduce account takeover persistence
- Support Zero Trust identity principles

If an attacker controls MFA registration, they control the account.

What happens when secure registration is Enabled (recommended)

When secure registration is enforced:

- Users must register MFA methods in trusted contexts
- Attackers cannot silently add their own authentication methods
- MFA integrity is preserved
- Account recovery processes are safer Identity security posture is significantly strengthened

Benefits:

- Reduced risk of persistent account takeover.
- Stronger protection against post-compromise abuse.
- Better control over authentication lifecycle.
- Improved audit and compliance posture.

This ensures MFA cannot be re-weaponized by attackers.

What happens when secure registration is Disabled

If security information registration is not protected:

Warning!

- Attackers can add their own MFA methods
- Accounts remain compromised even after password resets
- Detection and recovery become harder
- Users may be locked out by attackers
- Incidents become longer and more damaging

Many advanced breaches persist through MFA re-registration abuse.

Important clarification (commonly misunderstood)

MFA enforcement alone is not sufficient

Without secure registration:

MFA can be bypassed after compromise

This policy complements:

- MFA enforcement.
- Legacy authentication blocking.
- Audit logging.

Note
Protecting how MFA is registered is as important as enforcing MFA itself.

Real risks for an MSP

Security risk

- Attackers persist via stolen MFA registration.
- Password resets do not remove attacker access.
- Identity incidents escalate.

Compliance & audit risk

- If a client asks: How did the attacker keep access after MFA was enabled?

Without secure registration: The answer is uncomfortable.

MSP liability risk

- Weak MFA lifecycle controls are hard to defend
- Identity breaches damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
User experience	❗ Slight restrictions during setup
MFA integrity	❌ High risk if missing
Account takeover persistence	❌ High
Identity posture	❌ At risk
Compliance posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Securing Security Info Registration with Auto-remediation

Secure registration is critical because:

- It is often overlooked
- Defaults may be too permissive
- Manual validation does not scale
- One compromised registration undermines MFA entirely

Acronis M365 Security Posture Management:

- Continuously verifies secure registration policies
- Detects disabled or weakened enforcement
- Flags deviations from secure baselines
- Automatically restores protective controls
- Ensures consistent MFA lifecycle protection

Note

This ensures authentication methods cannot be hijacked.

MSP operational benefits

For Junior Technicians

- Clear rule: MFA registration must be protected
- No need to manage per-user exceptions
- Auto-remediation prevents accidental exposure
- Fewer persistent identity incidents

For Senior Administrators

- Strong end-to-end MFA protection
- Reduced account takeover dwell time
- Easier incident recovery
- Better Zero Trust alignment

For Customers

- Stronger account protection
- Faster and cleaner incident recovery
- Reduced risk of repeated compromise
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- MFA is only secure if its registration is secure.
- Protecting how authentication methods are added prevents persistent compromise.
- Acronis ensures this critical control stays enforced automatically.

Conditional Access Policy - Sign-In Risk-Based Multifactor Authentication.

What is Conditional Access – Sign-In Risk-Based Multifactor Authentication in Microsoft Entra ID

Risk-based sign-in is a Conditional Access policy that requires Multi-Factor Authentication (MFA) when Microsoft Entra ID determines that a sign-in attempt is risky.

Risk signals can include:

- Unusual sign-in locations or travel patterns.
- Anonymous IP addresses.
- Malware-linked IPs.
- Suspicious sign-in behavior.
- Known compromised credentials.

This policy is especially important for administrator accounts.

Note
This control applies adaptive security — stronger protection when risk is detected.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-risk-based-sign-in.

Why Microsoft provides this control

Microsoft provides risk-based sign-in policies to:

- Detect and respond to suspicious sign-in behavior
- Stop account takeover attempts in real time
- Add friction only when needed
- Protect high-value accounts (especially admins)
- Leverage Microsoft's global threat intelligence

Not all sign-ins are equal — risky sign-ins require stronger verification.

What happens when MFA is required for risky sign-ins (recommended)

When risk-based MFA is enforced:

- Suspicious sign-ins trigger MFA automatically
- Legitimate users can still sign in after verification
- Stolen credentials alone are insufficient
- Admin accounts receive extra protection
- Identity attacks are stopped earlier

Benefits:

- Reduced account takeover success.
- Adaptive security without constant user friction.
- Strong protection for privileged identities.
- Improved overall identity security posture.

This ensures risk triggers protection automatically.

What happens when Sign-In Risk-Based Multifactor Authentication is Disable

If risky sign-ins are not protected by MFA:

Warning!

- Suspicious logins may succeed silently
- Stolen credentials can be abused
- Admin accounts are exposed during attacks
- Detection happens late or after damage
- Breaches escalate quickly

Risk signals without enforcement are missed opportunities to stop attacks.

Important clarification (commonly misunderstood)

This policy:

- Does not replace baseline MFA enforcement.
- Adds extra protection when risk is elevated.

It works best when combined with:

- MFA for all users
- Legacy authentication blocking
- Secure MFA registration

Note

Risk-based MFA is an adaptive layer, not a standalone control.

Real risks for an MSP

Security risk

- Credential theft leads directly to access.
- Admin accounts become high-value targets.
- Identity attacks bypass basic defenses.

Compliance & audit risk

- If a client asks: Why didn't suspicious sign-ins trigger extra verification?

Without this policy: The answer is uncomfortable.

MSP liability risk

- Missed risk signals are hard to justify
- Identity breaches damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
Sign-in availability	❗ MFA triggered on risky attempts
User experience	❗ Minimal (only when risk detected)
Account takeover risk	❌ High if missing
Admin account protection	❌ At risk
Identity posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Sign-In Risk-Based Multifactor Authentication with Auto-remediation

Risk-based MFA is critical because:

- It relies on correct Conditional Access configuration
- Policies may be disabled or mis-scoped

- Manual validation does not scale across tenants
- One missing rule can expose privileged accounts

Acronis M365 Security Posture Management:

- Continuously verifies risk-based sign-in policies
- Detects disabled or weakened enforcement
- Flags deviations from secure identity baselines
- Automatically restores MFA enforcement
- Ensures consistent adaptive protection across tenants

Note

This ensures risk always triggers protection.

MSP operational benefits

For Junior Technicians

- Clear rule: Risky sign-in = MFA required
- No need to interpret risk signals manually
- Auto-remediation prevents missed protection
- Fewer identity incidents to escalate

For Senior Administrators

- Stronger adaptive identity defense
- Reduced admin account compromise risk
- Better use of Microsoft threat intelligence
- Easier audits and posture reporting

For Customers

- Better protection against suspicious logins
- Reduced account takeover incidents
- Security that adapts to real threats
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Not every sign-in is safe.
- Risk-based MFA adds adaptive protection when threats are detected.
- Acronis ensures this protection stays enforced automatically.

Customer Lockbox

What is Customer Lockbox in Microsoft 365

Customer Lockbox is a security and privacy feature that ensures Microsoft support engineers cannot access your tenant’s content without your explicit approval. It introduces a controlled approval workflow for situations where Microsoft needs to access customer data to resolve support issues.

Customer Lockbox applies to services like Exchange Online, SharePoint Online, OneDrive for Business, Teams, and Windows 365.

Note

This means Microsoft cannot access your content just because they are “support staff” — you must approve it explicitly.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/archive/technet-wiki/35748.office-365-what-is-customer-lockbox-and-how-to-enable-it.

Why Microsoft provides this feature

Microsoft provides Customer Lockbox to:

- Give customers explicit control over Microsoft's access to their data
- Reduce risk of unauthorized or unintended support access
- Support compliance and data-privacy requirements
- Provide audit trails for all support access events
- Support Zero Trust principles for data access

Ordinarily, Microsoft engineers perform most operations without human access to content. Lockbox applies in the rare cases where direct access is necessary.

What happens when Customer Lockbox is enabled (recommended)

When Customer Lockbox is turned on:

- Microsoft engineers must request access before viewing or modifying data
- You receive a notification for each access request
- You can approve or deny the request manually
- Access is time-bound and limited to the need defined in the request
- Every action is logged in the Microsoft 365 audit logs

This gives you control and visibility over support-related access to your content.

What happens when Customer Lockbox is disabled

If Customer Lockbox is turned off:

Warning!

- Microsoft engineers may access data during support operations without explicit approval
- You lose the ability to approve or deny individual access requests
- Audit trails for Microsoft support access may be less granular
- Compliance and data-protection governance may be weakened

Even though Microsoft follows strict internal controls, you have less direct control over when and how human access occurs.

How Customer Lockbox works — key steps

Microsoft determines that an engineer must access your data to resolve an issue.

A Lockbox request is generated and routed to your organization's approved approver(s).

The approver reviews and either approves or denies the request.

If approved, access is granted only for the specified duration.

If denied or not acted on in time, the request expires and no access is granted.

All actions are recorded in the audit logs.

Real risks for an MSP

Security risk

Without Lockbox, support engineers may access data without per-request approval.

This may expose sensitive emails, documents, or collaboration content.

Compliance & audit risk

If a client asks: Who approved Microsoft accessing our data?

Without Lockbox: The answer is uncomfortable or incomplete.

MSP liability risk

Loss of control over data access weakens security posture.

Auditors and customers expect visibility into who accessed sensitive content.

Severity summary

Area	Impact
Service availability	✓ No impact
User productivity	✓ No impact
Data access governance	✗ Exposed without Lockbox
Support transparency	✗ Reduced
Compliance posture	✗ At risk
MSP accountability	✗ High risk

Why use Acronis M365 Security Posture Management for Customer Lockbox with Auto-remediation

Customer Lockbox matters because:

- Human access to customer data is rare but high-impact.
- Default settings may not enforce approval workflows.
- Manual oversight does not scale across many tenants.
- One unapproved access can damage trust or compliance.

Acronis M365 Security Posture Management:

- Continuously verifies that Lockbox is enabled
- Detects if Lockbox is disabled or misconfigured
- Flags deviations from your security baselines
- Automatically restores the approved configuration

Note
This ensures you stay in control of access to your data — always.

MSP operational benefits

For Junior Technicians

- Clear rule: Microsoft support must ask before accessing data
- No need to guess who approved what
- Auto-remediation ensures Lockbox stays on
- Less risk of unexpected data exposure

For Senior Administrators

- Better governance over data access
- Stronger compliance and audit readiness
- Easier justification of data-access decisions
- Clear tracking of support engineer activities

For Customers

- Full control over who can see their data
- Transparent support interactions
- Reduced risk from unauthorized access
- Higher confidence in MSP data governance

Note

Key takeaway:

- Customer Lockbox keeps support access under your control.
- It ensures Microsoft cannot view or fix issues involving your data without your explicit approval, and every access is logged.

Password Policy

What is the Password Policy in Microsoft 365

The Domain Password Policy defines password expiration and complexity requirements for user accounts in Microsoft 365.

It controls:

- How long passwords remain valid.
- When users are notified before password expiration.
- Whether passwords must be changed periodically.
- Baseline password hygiene expectations.

Note

This policy governs how long credentials can be used before renewal.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide.

Why Microsoft provides this control

Microsoft provides password expiration and policy controls to:

- Reduce the risk of long-lived credential compromise
- Limit the usefulness of stolen passwords
- Encourage better password hygiene
- Support compliance and governance requirements
- Provide organizations flexibility based on risk tolerance

Passwords that never change can remain compromised for years without detection.

What happens when the policy is Enabled (recommended)

When password expiration and notifications are configured appropriately:

- Stolen passwords become time-limited
- Users are warned before expiration
- Forgotten credentials are rotated regularly
- Attack windows are reduced
- Baseline account hygiene is enforced

Benefits:

- Reduced impact of credential theft.
- Predictable account lifecycle.
- Better alignment with governance requirements.
- Improved overall identity posture (when combined with MFA).

This limits how long an attacker can reuse a stolen password.

What happens when the policy is disabled or overly permissive

If passwords never expire or policies are weak:

Warning!

- Stolen passwords remain valid indefinitely
- Old credentials are reused for long periods
- Compromised accounts persist silently
- Incident dwell time increases
- Attackers gain long-term access

Password compromise without expiration leads to persistent access.

Important clarification (commonly misunderstood)

Password expiration alone is not sufficient

Modern best practice requires:

- MFA enforcement.
- Blocking legacy authentication.
- Secure MFA registration.
- Password expiration is a supporting control, not a primary defense.

Note
Passwords should not be the only line of defense.

Real risks for an MSP

Security risk

- Long-lived credential compromise.
- Increased blast radius of phishing attacks.
- Silent persistence of attackers.

Compliance & audit risk

- If a client asks: How long could a stolen password remain valid?

Without expiration: The answer is uncomfortable.

MSP liability risk

- Weak credential hygiene is hard to justify
- Identity breaches damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
Sign-in availability	❗ Periodic password changes
User experience	❗ Minor inconvenience
Credential hygiene	❌ Weak if missing
Account compromise risk	❌ High

Area	Impact
Identity posture	✖ At risk
MSP accountability	✖ High risk

Why use Acronis M365 Security Posture Management for Password Policy with Auto-remediation

Password policies matter because:

- Defaults vary by tenant age.
- Exceptions accumulate over time.
- Manual checks do not scale.
- One weak policy undermines identity security.

Acronis M365 Security Posture Management:

- Continuously verifies password policy configuration
- Detects disabled or overly permissive expiration settings
- Flags deviations from approved baselines
- Automatically restores policy enforcement
- Maintains consistent identity hygiene across tenants

Note
This ensures password policy drift does not weaken security.

MSP operational benefits

For Junior Technicians

- Clear rule: Passwords must follow policy
- No need to track tenant-by-tenant differences
- Auto-remediation prevents risky configurations
- Fewer identity-related incidents

For Senior Administrators

- Consistent credential hygiene
- Reduced long-term compromise risk
- Easier audits and security reviews
- Stronger baseline identity posture

For Customers

- Better protection against unauthorized access
- Reduced risk from stolen credentials
- Clear and predictable password lifecycle
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Passwords that never expire can stay compromised forever.
- Expiration limits the lifetime of stolen credentials.
- Acronis ensures password policies stay aligned with security best practices automatically.

SharePoint Modern Auth Enforced

What is Modern Authentication Enforcement for SharePoint Online

This configuration enforces the use of modern authentication protocols for SharePoint Online by disabling legacy authentication methods.

It is typically configured using the Set-SPOTenant PowerShell command (as shown in Example 5 of the documentation).

Note

This setting ensures SharePoint access uses secure, modern authentication flows.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/powershell/module/microsoft.online.sharepoint.powershell/set-spotenant?view=sharepoint-ps#example-5.

Why Microsoft provides this control

Microsoft provides this control to:

- Prevent use of outdated authentication protocols
- Ensure SharePoint supports MFA and Conditional Access
- Reduce attack surface from password-only authentication
- Align SharePoint with Zero Trust identity principles
- Protect organizational data from credential-based attacks

Legacy authentication cannot enforce modern security controls.

What happens when modern authentication is Enabled (recommended)

When legacy authentication is disabled for SharePoint:

- MFA can be enforced consistently
- Conditional Access policies apply
- Password-only access is blocked
- Credential-spray and brute-force attacks are reduced
- SharePoint data is better protected

Benefits:

- Stronger identity protection for SharePoint access.
- Reduced risk of account compromise.
- Better alignment with Microsoft security best practices.
- Improved overall tenant security posture.

This ensures SharePoint does not become an identity weak point.

What happens when modern authentication is Disable

If legacy authentication remains enabled:

Warning!

- MFA may be bypassed
- Conditional Access may not apply
- Password-only sign-ins are possible
- Attackers exploit legacy protocols
- SharePoint becomes a high-risk access path

Many Microsoft 365 breaches occur through legacy authentication paths.

Important clarification (commonly misunderstood)

This setting:

- Applies specifically to SharePoint Online.
- Does not automatically affect Exchange or Entra ID.

Legacy authentication:

- Bypasses MFA.
- Ignores Conditional Access.

This control complements:

- Tenant-wide legacy auth blocking.
- Conditional Access policies.

Note
Blocking legacy auth must be consistent across workloads.

Real risks for an MSP

Security risk

- Attackers bypass MFA using legacy protocols.
- SharePoint data accessed without modern controls.
- Increased likelihood of credential-based compromise.

Compliance & audit risk

- If a client asks: Can SharePoint be accessed without MFA?

If legacy auth is enabled: The answer is non compliant.

MSP liability risk

- Weak authentication controls are hard to defend
- SharePoint data exposure incidents damage trust
- MSP security maturity may be questioned

Severity summary

Area	Impact
SharePoint availability	❗ Legacy clients may be blocked
User experience	❗ Modern clients unaffected
MFA enforcement	❌ Inconsistent if missing
Data protection	❌ High risk
Identity posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for SharePoint Modern Auth Enforced with Auto-remediation

This control is critical because:

- It requires PowerShell to configure
- Older tenants often still allow legacy auth
- Manual validation does not scale
- One legacy access path undermines MFA

Acronis M365 Security Posture Management:

- Doesn't requires PowerShell to configure
- Continuously verifies SharePoint authentication settings
- Detects legacy authentication exposure
- Flags deviations from secure baselines
- Automatically enforces modern authentication
- Prevents configuration drift over time

Note
This ensures SharePoint always enforces modern, secure authentication.

MSP operational benefits

For Junior Technicians

- Clear rule: SharePoint must use modern authentication
- No need to understand legacy protocols
- No need to know PowerShell to configure
- Auto-remediation prevents risky configurations
- Fewer identity-related incidents

For Senior Administrators

- Consistent authentication security across workloads
- Reduced credential-based attack surface
- Easier audits and security reviews
- Better Zero Trust alignment

For Customers

- Stronger protection of SharePoint data
- Reduced risk of unauthorized access

- Support for MFA and modern security features
- Higher confidence in MSP-managed collaboration security

Note

Key takeaway:

- Legacy authentication bypasses modern security controls.
- Enforcing modern authentication protects SharePoint data.
- Acronis ensures this protection stays enforced automatically.

User Consent Settings

What is User Consent Settings for Enterprise Applications in Microsoft Entra ID

User consent controls whether and how end users can grant applications permission to access organizational data in Microsoft Entra ID.

Depending on configuration, users may be able to:

- Grant consent only to apps from verified publishers and low-risk permissions
- Grant consent to any app
- Be blocked from granting consent entirely, forcing admin approval

Note

This control governs how applications gain access to tenant data.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=portal.

Why Microsoft provides this control

Microsoft provides user consent controls to:

- Reduce risk from malicious or overly-permissive apps
- Limit OAuth-based attacks and data exfiltration
- Balance productivity with security
- Enforce governance over third-party application access
- Support Zero Trust and least-privilege principles

Apps can access mail, files, users, and directory data — consent must be controlled.

What happens when user consent is restricted (recommended)

When user consent is limited (for example, verified publishers only or disabled):

- Users cannot approve high-risk app permissions
- Untrusted apps are blocked automatically
- App access decisions are reviewed intentionally
- Shadow IT is reduced
- OAuth attack surface is minimized

Benefits:

- Stronger control over third-party apps.
- Reduced data-exfiltration risk.
- Clear governance over app access.
- Better audit and compliance posture.

This ensures apps cannot self-authorize into the tenant.

What happens when user consent is too permissive

If users can consent to any app:

Warning!

- Malicious apps can gain access easily
- Users may approve permissions they don't understand
- OAuth attacks bypass MFA and Conditional Access
- App access spreads without visibility
- Incident detection is delayed

Many modern breaches rely on over-permissive OAuth consent.

Important clarification (commonly misunderstood)

User consent:

- Is separate from admin consent.
- Applies even when MFA is enabled.

OAuth apps:

Can maintain access without user interaction

This control complements:

- Admin Consent Workflow.
- Audit logging.
- Conditional Access.

Note

MFA does not protect against malicious app consent.

Real risks for an MSP

Security risk

- Malicious apps access mail and files persistently.
- Attacks bypass sign-in protections.
- Difficult cleanup once consent is granted.

Compliance & audit risk

- If a client asks: Who approved this app to access our data?

With open user consent: The answer is uncomfortable.

MSP liability risk

- Weak app governance is hard to justify
- OAuth breaches are high-impact
- MSP security maturity may be questioned

Severity summary

Area	Impact
User productivity	❗ Some apps require approval
User experience	❗ Consent restrictions
App governance	❌ Weak if permissive
Data protection	❌ High risk
Identity posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for User Consent Settings with Auto-remediation

User consent settings are critical because:

- Defaults may be too permissive
- Changes are easy to miss
- Manual reviews do not scale
- One malicious app can expose large volumes of data

Acronis M365 Security Posture Management:

- Continuously verifies user consent configuration
- Detects overly permissive consent settings
- Flags deviations from approved baselines
- Automatically enforces restricted consent models
- Maintains consistent app governance across tenants

Note
This ensures apps cannot gain access without proper trust.

MSP operational benefits

For Junior Technicians

- Clear rule: Users should not approve risky apps
- No need to understand OAuth internals
- Auto-remediation enforces safe defaults
- Fewer app-related security incidents

For Senior Administrators

- Stronger control over application ecosystem
- Reduced OAuth-based attack surface
- Easier audits and compliance discussions
- Better Zero Trust alignment

For Customers

- Better protection of tenant data
- Reduced risk from malicious or unknown apps
- Transparent and controlled app approval process
- Higher confidence in MSP-managed identity security

Note

Key takeaway:

- Apps can be more dangerous than users.
- Controlling user consent prevents silent data access.
- Acronis ensures only trusted applications gain access automatically.

General

What Security Defaults Policy means in Microsoft 365

Security Defaults is Microsoft's built-in set of basic security protections for user and administrator accounts.

Note

Think of Security Defaults as Microsoft's minimum safety standard for protecting identities.

When enabled, Microsoft automatically enforces:

- Multi-Factor Authentication (MFA) for administrators
- MFA for users when risk is detected
- Blocking of legacy (older, insecure) login methods
- Use of modern, more secure authentication

Security Defaults provides immediate protection without complex configuration.

What Security Defaults protect against

Security Defaults help prevent:

- Account takeover via stolen passwords.
- Admin account compromise.
- Attacks using outdated login methods.
- Automated credential-stuffing attacks.

These are the most common causes of Microsoft 365 breaches.

How Security Defaults fit into security maturity

Configuration	Security meaning
Security Defaults enabled	✓ Basic identity protection
Security Defaults disabled, no replacement	✗ High identity risk

Configuration	Security meaning
Security Defaults replaced by advanced policies	✓ Mature security posture

Security Defaults is ideal for baseline protection or as a starting point.

Why Security Defaults matter from a business perspective

Without Security Defaults (or equivalent protections):

- Password-only logins remain possible
- Admin accounts are easier targets
- Identity attacks are more likely

With Security Defaults:

- Identity security is enforced automatically.
- Risk is reduced without daily admin effort.
- Basic compliance expectations are met.

Security Defaults Policy

What are Security Defaults in Microsoft 365

Security Defaults is a set of preconfigured identity security protections provided by Microsoft that, when enabled, automatically enforces basic but impactful security controls across your tenant.

These protections include:

- Requiring Multi-Factor Authentication (MFA) for privileged roles.
- Blocking legacy authentication that doesn’t support MFA.
- Enforcing modern authentication.
- Protecting admin and user accounts from common identity attacks.

Note
Security Defaults acts as an automated baseline security posture for identity protection.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults.

Why Microsoft provides Security Defaults

Microsoft provides Security Defaults to:

- Simplify baseline identity security for all tenants
- Protect against the most common identity-based attacks
- Ensure essential safeguards are in place even without custom Conditional Access
- Help small and mid-size organizations adopt best practices
- Reduce reliance on manual configuration

Security Defaults is a broad, no-touch security baseline recommended for most tenants.

What happens when Security Defaults are enabled (recommended)

When Security Defaults are enabled:

Multi-Factor Authentication is required for:

- All administrator roles
- Risky or unfamiliar sign-ins

- Legacy authentication protocols are automatically blocked
- Modern authentication is enforced
- Basic protection is provided even without Conditional Access
- Users and administrators are better protected from credential-based attacks

Benefits:

- Immediate, broad identity security improvements.
- Reduced risk of account compromise.
- No need to design complex Conditional Access policies.
- Works out-of-the-box with minimal setup.

Security Defaults provides a security safety net for identity protection.

What happens when Security Defaults are disabled

If Security Defaults are turned off:

Warning!

- You must implement identity controls manually
- Legacy authentication may remain enabled
- MFA may not be enforced for all roles or scenarios
- Tenant may be vulnerable to credential-based attacks
- You must design your own Conditional Access policies to achieve similar protections

Without Security Defaults, the tenant relies entirely on custom configuration.

Important clarification (commonly misunderstood)

Security Defaults is not flexible — it's a baseline, not a detailed policy engine

For advanced Conditional Access requirements, you must build custom policies

Note
Think of Security Defaults as a "quick start" safety harness, not a full policy framework.

Real risks for an MSP

Security risk

- Without defaults or equivalent policies, credential attacks are easier.
- Legacy authentication may be abused.
- Less-experienced admins may leave gaps.

Compliance & audit risk

- If a client asks: How are you protecting our user identities out of the box?

Without Security Defaults or equivalent: The answer is uncomfortable.

MSP accountability risk

- Data breaches resulting from weak identity controls carry high reputational impact
- Lack of baseline identity security is hard to justify post-incident

Severity summary

Area	Impact
Identity protection	❌ Weak if disabled
Legacy authentication blocking	❌ May not be applied
MFA enforcement	❌ Limited without policies
Attack surface	❌ Increased
Compliance posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Security Defaults with Auto-remediation

Security Defaults matter because:

- Not all admins enable them manually.
- They can be turned off without replacing key protections.
- Manual setup of equivalent controls is complex.
- Custom Conditional Access requires expertise.

Acronis M365 Security Posture Management:

- Detects whether Security Defaults are enabled
- Flags missing or disabled essential protections
- Helps enforce a secure baseline even when defaults are off
- Suggests or auto-remediates with equivalent security controls

Note
This ensures your tenants maintain baseline identity protections at all times.

MSP operational benefits

For Junior Technicians

- Gives a clear baseline: Security Defaults = safer by default
- No need to design initial policies
- Auto-remediation ensures essential protections stay in place
- Fewer identity-related incidents

For Senior Administrators

- Consistent identity protection across tenants
- Reduced risk surface without a full CA deployment
- Bridge to more advanced Conditional Access as customers mature
- Better audit readiness

For Customers

- Immediate basic identity security
- Reduced likelihood of compromise
- Predictable behavior with minimal admin effort
- Higher confidence in MSP security posture

Note

Key takeaway:

- Security Defaults provides essential identity protection automatically.
- If they are disabled, equivalent protections must be explicitly configured.
- Acronis ensures those protections stay enforced automatically.

Intune

What Intune / Device Management means in Microsoft 365 security

In Microsoft 365, Intune is the service that controls how devices are allowed to access company data.

Note

Think of Intune as the gatekeeper for laptops, phones, and tablets that connect to your email, files, and applications.

It answers questions like:

- Is this device secure enough to access company data?
- Does the device have encryption, a password, and up-to-date software?
- Can a lost or stolen device be blocked or wiped?
- Are personal devices allowed — and under what conditions?

Without Intune, Microsoft 365 cannot tell if a device is safe or risky.

Why Intune is critical for security

From a security posture perspective, Intune provides:

- Device trust – only secure devices are allowed access
- Data protection – data stays protected even on mobile devices
- Access control – risky or non-compliant devices are blocked
- Loss protection – stolen or lost devices can be contained
- Policy enforcement – security rules are applied consistently

Intune does not replace antivirus or firewalls.

It ensures that devices meet minimum security standards before accessing data.

Why Intune is critical for security

From a security posture perspective, Intune provides:

- Device trust – only secure devices are allowed access
- Data protection – data stays protected even on mobile devices

- Access control – risky or non-compliant devices are blocked
- Loss protection – stolen or lost devices can be contained
- Policy enforcement – security rules are applied consistently

Intune does not replace antivirus or firewalls. It ensures that devices meet minimum security standards before accessing data.

Intune security is built on two core pillars

Device Compliance Policies

These check whether a device is secure.

They verify things like:

- Operating system version.
- Encryption enabled.
- Screen lock and password strength.
- Jailbreak / root detection.

Note
Why it matters:

Non-compliant devices are automatically blocked from accessing company data.

Device Configuration Policies

These enforce how devices behave.

They control things like:

- Blocking password saving in browsers.
- Enabling encryption and security settings.
- Restricting risky features.
- Enforcing corporate security standards.

Note
Why it matters:

Even compliant devices can be risky if security settings are not enforced.

What Intune tells us about security maturity

Intune status	Security meaning
Intune configured and enforced	✓ Devices are trusted

Intune status	Security meaning
Intune partially configured	❗ Inconsistent protection
Intune not used	❌ Devices are uncontrolled

Note

Key takeaway:

- Users are only as secure as the devices they use.
- Intune correct configuration ensures that only trusted, compliant devices can access Microsoft 365.
- Acronis ensures this protection stays enforced automatically.

Android Enterprise - Compliance Policy

What is an Intune Compliance Policy for Android for Enterprise

An Intune Compliance Policy defines rules and settings that a device must meet to be considered compliant with your organization’s security requirements.

For Android for Work (Android Enterprise), these policies can enforce things like:

- Required OS versions
- Minimum security patch levels
- Device health attestation
- Restricted access if jailbroken or rooted
- Password/PIN requirements
- Encryption requirements

Note

This policy determines whether a device is trusted and can access corporate resources.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-create-android-for-work.

Why Microsoft provides this control

Microsoft provides compliance policies to:

- Enforce security requirements on managed devices
- Ensure only compliant (secure) devices can access company data
- Support Conditional Access decisions

- Reduce risk from insecure or outdated endpoints
- Improve visibility into device posture

Device compliance is a key pillar of Zero Trust.

What happens when the compliance policy is properly configured

When an Android for Work compliance policy is configured and enforced:

- Devices must meet security criteria to be compliant
- Non-compliant devices trigger Conditional Access restrictions
- Risk of data exposure on insecure devices is reduced
- Enforcement is consistent across Android Enterprise endpoints
- Admins can track compliance status centrally

Benefits:

- Better protection of company data on mobile devices.
- Reduced risk from lost, stolen, or poorly configured devices.
- Consistent enforcement across the fleet.
- Compliance information ties into Conditional Access policies.

This ensures only trusted mobile devices can access corporate resources.

What happens when the compliance policy is not configured or weak

If the compliance policy is missing or too permissive:

Warning!

- Unsecured Android devices may be treated as compliant
- Devices with outdated OS or missing security updates are allowed
- Conditional Access may allow risky access
- Sensitive data can be accessed from insecure endpoints
- Risk of malware, data leakage, or compromise increases

Mobile endpoints become uncontrolled access paths.

Important clarification (commonly misunderstood)

A compliance policy does not replace:

- Device enrollment
- Conditional Access

- App Protection Policies
- Compliance + Conditional Access = blocked access for non-secure devices
- Simply enrolling a device does not make it trusted — it must meet the compliance rules

> **Note**
> Compliance is about desired device state, not just enrollment.

Real risks for an MSP

Security risk

- Access from insecure or compromised devices.
- Increased risk of data leaks or ransomware.
- Harder to enforce security on BYOD or unmanaged devices.

Compliance & audit risk

- If a client asks: Which devices meet our security standards?

Without compliance enforcement: The answer is unclear or unreliable.

MSP liability risk

- Weak device governance is hard to justify
- Data-exposure incidents reduce customer confidence
- MSP security maturity may be questioned

Severity summary

Area	Impact
Device availability	❗ Compliant devices only
User experience	❗ Some devices blocked
Data leakage risk	❌ High if missing
Device posture governance	❌ Weak without policy
Conditional Access effectiveness	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Android Compliance with Auto-remediation

Compliance policies matter because:

- Device security standards drift over time.
- Users bypass settings without policy enforcement.
- Manual checks do not scale across tenants.
- One insecure device can expose data.

Acronis M365 Security Posture Management:

- Continuously verifies compliance policy status
- Detects missing or misconfigured policies
- Flags deviations from secure baselines
- Automatically restores compliant configurations
- Ensures consistent mobile security posture across tenants

Note

This ensures Android endpoints are always evaluated against your policy.

MSP operational benefits

For Junior Technicians

- Clear rule: Android devices must meet security standards
- No need to manually check device states
- Auto-remediation enforces safe defaults
- Fewer mobile security incidents

For Senior Administrators

- Strong mobile device governance
- Reduced risk of insecure access
- Better Conditional Access integration
- Easier audit and posture reporting

For Customers

- Protection of sensitive data on mobile endpoints
- Predictable security behavior across devices
- Compliance standards enforced automatically
- Higher trust in MSP-managed security

Note

Key takeaway:

- Mobile security depends on device posture.
- Compliance policies enforce trusted device states.
- Acronis ensures these protections stay enforced automatically.

iOS/iPadOS - Compliance Policy

What is an Intune Compliance Policy for iOS/iPadOS

An Intune Compliance Policy for iOS/iPadOS defines the security requirements that Apple mobile devices must meet to be considered compliant with your organization's security standards.

These policies can enforce settings such as:

- Minimum OS version
- Passcode requirements
- Jailbreak detection
- Encryption requirements
- Security patch level

Note

This policy helps determine whether an iOS/iPadOS device is trusted before accessing corporate resources.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-create-ios.

Why Microsoft provides this control

Microsoft provides mobile compliance policies to:

- Ensure devices accessing company data meet baseline security requirements
- Reduce risk from insecure or compromised mobile devices
- Support Conditional Access decisions
- Protect corporate data on mobile endpoints
- Improve governance and control over BYOD and corporate devices

Device compliance is a key pillar of Zero Trust — ensuring that only secure devices interact with business data.

What happens when the compliance policy is not configured or weak

If the iOS/iPadOS compliance policy is missing or too permissive:

Warning!

- Insecure mobile devices may be treated as compliant
- Devices with outdated OS versions may access sensitive resources
- Conditional Access may allow risky access
- Sensitive data can be accessed from compromised endpoints
- Risk of malware and data leakage increases

Mobile endpoints then become uncontrolled access paths for attackers.

What happens when the compliance policy is properly configured

When an iOS/iPadOS compliance policy is configured and enforced:

- Devices must meet defined security criteria to be marked compliant
- Non-compliant devices can be blocked via Conditional Access
- Risk of data exposure on insecure mobile devices is reduced
- Admins gain visibility into device posture
- Compliance integrates with access decisions

Benefits:

- Better protection of corporate information on iPhones and iPads.
- Reduced risk from jailbroken or outdated devices.
- Consistent enforcement across mobile fleets.
- Integration with Conditional Access for secure access.

This ensures only trusted iOS/iPadOS devices can access sensitive resources.

Important clarification (commonly misunderstood)

A compliance policy does not replace:

- Device enrollment
- App Protection Policies (MAM)
- Conditional Access

Simply enrolling an iOS device does not guarantee compliance — it must meet the policy rules

Compliance + Conditional Access = trusted access only

Note

Compliance is about device state and security, not enrollment alone.

Real risks for an MSP

Security risk

- Access from insecure, jailbroken, or outdated devices.
- Increased risk of data leakage through mobile endpoints.
- Harder to enforce consistent security on BYOD.

Compliance & audit risk

- If a client asks: Which devices meet our security standards?

Without this policy: The answer may be unclear or incomplete.

MSP liability risk

- Weak device governance is hard to justify
- Mobile security incidents reduce customer confidence
- MSP security maturity may be questioned

Severity summary

Area	Impact
Device availability	❗ Secure devices only
User experience	❗ Some devices blocked
Data leakage risk	❌ High if missing
Mobile posture governance	❌ Weak without policy
Conditional Access effectiveness	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for iOS/iPadOS Compliance with Auto-remediation

Mobile compliance policies matter because:

- Device security standards drift over time
- Users may bypass settings without policy enforcement

- Manual checks do not scale across tenants
- One insecure device can expose sensitive corporate data

Acronis M365 Security Posture Management:

- Continuously verifies compliance policy status
- Detects missing or misconfigured policies
- Flags deviations from secure baselines
- Automatically restores compliant configurations
- Ensures consistent mobile security posture across tenants

Note
This ensures iOS and iPadOS devices are always evaluated against your policy.

MSP operational benefits

For Junior Technicians

- Clear rule: Mobile endpoints must meet security requirements
- No need to manually check device states
- Auto-remediation enforces safe defaults
- Fewer mobile security incidents

For Senior Administrators

- Stronger mobile device governance
- Reduced risk of insecure access
- Better Conditional Access integration
- Easier audits and security reviews

For Customers

- Protection of sensitive data on mobile devices
- Predictable security behavior across iPhones and iPads
- Enforcement of security standards automatically
- Higher confidence in MSP-managed security

Note
Key takeaway:

- Mobile security depends on device posture.
- Compliance policies enforce trusted device states.
- Acronis ensures these protections stay enforced automatically.

MAC OS - Compliance Policy

What is an Intune Compliance Policy for macOS

An Intune Compliance Policy for macOS defines the security requirements that Apple Mac computers must meet to be considered compliant with your organization's security standards.

These policies can enforce things such as:

- Minimum operating system version
- Encryption (FileVault) enabled
- Required password/PIN policies
- Blocked or restricted jailbroken/rooted states
- Security patch levels

Note
This policy helps determine whether a Mac device is trusted and secure before accessing corporate resources.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-create-mac-os.

Why Microsoft provides this control

Microsoft provides compliance policies to:

- Ensure devices accessing corporate data meet baseline security requirements
- Reduce risk from insecure or compromised macOS endpoints
- Support Conditional Access decisions
- Protect corporate data on employee and BYOD computers
- Improve governance over unmanaged and managed devices

Device compliance is a core part of a Zero Trust access model — securing not just the user, but the device they use.

What happens when the compliance policy is not configured or weak

If the macOS compliance policy is missing or overly permissive:

Warning!

- Insecure macOS devices may be treated as compliant
- Devices without encryption or old OS versions can access corporate data
- Conditional Access may allow risky access paths
- Sensitive data can be accessed from compromised endpoints
- Risk of data leakage increases

Unprotected or unmanaged devices become easy infiltration points.

What happens when the compliance policy is properly configured

When a macOS compliance policy is configured and enforced:

- Devices must meet defined security criteria to be marked compliant
- Non-compliant macOS devices can be blocked via Conditional Access
- Risk of data exposure on insecure Macs is reduced
- Admins gain visibility into device posture
- Compliance integrates with access decisions

Benefits:

- Better protection for corporate information accessed from macOS.
- Reduced risk from outdated or unprotected laptops.
- Consistent enforcement across corporate and BYOD Macs.
- Stronger integration with Conditional Access for secure access.

This ensures only trusted macOS endpoints can access sensitive corporate resources.

Important clarification (commonly misunderstood)

A compliance policy does not replace:

- Device enrollment
- Conditional Access
- App Protection Policies

Merely enrolling a macOS device does not guarantee compliance — it must meet all policy rules

Compliance + Conditional Access = trusted access only

Note

Compliance is about desired device state, not enrollment alone.

Real risks for an MSP

Security risk

- Access from insecure or unmanaged macOS laptops.
- Increased opportunity for malware and data theft.
- External actors exploit lax device security.

Compliance & audit risk

- If a client asks: Which macOS devices meet our security standards?

Without enforced compliance: The answer may be unclear or incomplete.

MSP liability risk

- Weak device governance is hard to justify to stakeholders
- Data-exposure incidents reduce customer confidence
- MSP security maturity may be questioned

Severity summary

Area	Impact
Device availability	❗ Secure devices only
User experience	❗ Some devices blocked
Data leakage risk	❌ High if missing
Mac posture governance	❌ Weak without policy
Conditional Access effectiveness	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for macOS Compliance with Auto-remediation

macOS compliance policies matter because:

- Device security standards evolve over time
- Users may bypass settings without policy enforcement
- Manual checks do not scale across many tenants
- One insecure device can expose sensitive corporate data

Acronis M365 Security Posture Management:

- Continuously verifies compliance policy status
- Detects missing or misconfigured policies
- Flags deviations from secure baselines
- Automatically restores compliant configurations
- Ensures consistent macOS security posture across tenants

Note

This ensures macOS endpoints are always evaluated against your policy.

MSP operational benefits

For Junior Technicians

- Clear rule: macOS devices must meet security requirements
- No need to manually check device states
- Auto-remediation enforces safe defaults
- Fewer macOS security incidents

For Senior Administrators

- Stronger governance of macOS endpoints
- Reduced risk of insecure access
- Better alignment with Conditional Access
- Easier audits and security reviews

For Customers

- Protection of sensitive corporate data on Macs
- Predictable security behavior across Apple devices
- Enforcement of security policies automatically
- Higher confidence in MSP-managed security

Note

Key takeaway:

- Device security isn't optional.
- Compliance policies enforce trusted device states for macOS.
- Acronis ensures these protections stay enforced automatically.

Windows 10 Or Later - Compliance Policy

What is an Intune Compliance Policy for Windows

An Intune Compliance Policy for Windows devices defines the security requirements that Windows computers must meet to be considered compliant with your organization's security standards.

These policies can enforce security criteria such as:

- Minimum operating system version
- BitLocker encryption enabled
- Firewall enabled
- Required password/PIN complexity
- Prevention of jailbroken/unsupported configurations
- Antivirus/Defender status

Note

This policy helps determine whether a Windows device is trusted and secure before allowing it to access corporate resources.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-create-windows.

Why Microsoft provides this control

Microsoft provides compliance policies to:

- Ensure Windows devices meet baseline security requirements
- Reduce risk from insecure or compromised endpoints
- Support Conditional Access decisions
- Protect corporate data on laptops and desktops
- Improve governance over managed and unmanaged devices

Device compliance is a core part of Zero Trust — securing not just the user, but the device they use.

What happens when the compliance policy is not configured or weak

If the Windows compliance policy is missing or overly permissive:

Warning!

- Insecure or unmanaged Windows devices may be treated as compliant
- Devices without encryption or security protections could access resources
- Conditional Access may allow risky access paths
- Sensitive data can be accessed from compromised endpoints
- Risk of malware infection and data leakage increases

Windows endpoints then become uncontrolled attack vectors.

What happens when the compliance policy is properly configured

When a Windows compliance policy is configured and enforced:

- Devices must meet defined security criteria to be marked compliant
- Non-compliant Windows devices can be blocked via Conditional Access
- Risk of data exposure on insecure Windows endpoints is reduced
- Admins gain visibility into device posture
- Compliance ties into secure access decisions

Benefits:

- Better protection of corporate data on Windows machines.
- Reduced risk from outdated or insecure devices.
- Consistent enforcement across corporate and BYOD Windows.
- Stronger integration with Conditional Access for secure access.

This ensures only trusted Windows endpoints can access sensitive corporate resources.

Important clarification (commonly misunderstood)

A compliance policy does not replace:

- Device enrollment
- Conditional Access
- Endpoint protection

Merely enrolling a Windows device does not guarantee compliance — it must meet all policy rules

Compliance + Conditional Access = trusted access only

Note
Compliance is about device state and security, not enrollment alone.

Real risks for an MSP

Security risk

- Access from insecure or compromised Windows endpoints.
- Increased risk of malware, ransomware, or credential theft.
- Attackers use unmanaged devices to bypass controls.

Compliance & audit risk

- If a client asks: Which Windows devices meet our security standards?

Without enforced compliance: The answer may be unclear or incomplete.

MSP liability risk

- Weak device governance is hard to justify to stakeholders
- Data-exposure incidents reduce customer confidence
- MSP security maturity may be questioned

Severity summary

Area	Impact
Device availability	❗ Secure devices only
User experience	❗ Some devices blocked
Data leakage risk	❌ High if missing
Windows posture governance	❌ Weak without policy
Conditional Access effectiveness	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Windows Compliance with Auto-remediation

Windows compliance policies matter because:

- Device security standards evolve over time
- Users may bypass settings without policy enforcement
- Manual checks do not scale across multiple tenants
- One insecure device can expose sensitive corporate data

Acronis M365 Security Posture Management:

- Continuously verifies compliance policy status
- Detects missing or misconfigured policies
- Flags deviations from secure baselines
- Automatically restores compliant configurations
- Ensures consistent Windows security posture across tenants

Note

This ensures Windows endpoints are always evaluated against your policy.

MSP operational benefits

For Junior Technicians

- Clear rule: Windows devices must meet security requirements
- No need to manually check device states
- Auto-remediation enforces safe defaults
- Fewer Windows security incidents

For Senior Administrators

- Stronger governance of Windows endpoints
- Reduced risk of insecure access
- Better alignment with Conditional Access
- Easier audits and security reviews

For Customers

- Protection of sensitive data on Windows devices
- Predictable security behavior across desktops and laptops
- Enforcement of security policies automatically
- Higher confidence in MSP-managed security

Note

Key takeaway:

- Device security is fundamental.
- Compliance policies enforce trusted Windows device states.
- Acronis ensures these protections stay enforced automatically.

Windows 10 or later Configuration Policy - Block Password Saving In Google Chrome

What is a Device Restrictions Configuration Policy (Block Password Saving in Google Chrome)

A Device Configuration Policy in Microsoft Intune can be used to block users from saving passwords in the Google Chrome browser on managed devices.

This setting is part of Device Restrictions under Intune configuration profiles and applies to Windows, macOS, Android, and iOS when supported.

Note

This control ensures users cannot store passwords in the Chrome browser, reducing the risk of credential theft from browser-stored passwords.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/intune/intune-service/configuration/device-restrictions-configure.

Why Microsoft provides this control

Microsoft provides this control to:

- Prevent sensitive credentials from being stored insecurely
- Reduce credential theft from stolen or unmanaged devices
- Limit exposure from shared or unmanaged browsers
- Support corporate security policies
- Align browser behavior with Zero Trust principles

Browser-saved passwords are a common attack vector in credential compromise and lateral movement.

What happens when the policy is enabled (recommended)

When the configuration policy blocks password saving in Chrome:

- Users are prevented from storing credentials in the Chrome browser
- Browser-cached passwords cannot be extracted by malware or other processes
- Risk of credential theft from stolen or compromised devices is reduced
- Credential hygiene is improved across the device fleet
- Enforcement is consistent across all managed endpoints

Benefits:

- Stronger protection of user credentials.
- Reduced risk of credential reuse and theft.
- Fewer breaches caused by stored passwords.
- Better compliance with corporate security policies.

This ensures credentials remain dynamic and protected, not cached insecurely in browsers.

What happens when the policy is not enabled

If password saving is allowed in Chrome:

Warning!

- Users may store corporate credentials in the browser
- Saved passwords can be accessed by other processes or malware
- Shared or lost devices expose saved credentials
- Credential theft risk increases
- Account compromise becomes more likely

Browser-stored passwords can be a single point of failure.

Important clarification (commonly misunderstood)

This policy only blocks saving passwords in the browser

It does not:

- Force users to change current passwords.
- Prevent users from using dedicated password managers (unless separately controlled).

It complements other controls such as:

- MFA enforcement
- Legacy authentication blocking
- Device compliance policies

Note

This control protects at the browser level, not just authentication.

Real risks for an MSP

Security risk

Passwords stored in browsers can be extracted by:

- Malware
- Local attackers
- Remote scripts via browser compromise

Compliance & audit risk

If a client asks: Can users store company credentials in Chrome?

Without this policy: The answer may expose credential risk.

MSP liability risk

- Credential theft incidents are high impact
- Hard to justify unmanaged password storage
- Reduces confidence in MSP security posture

Severity summary

Area	Impact
User convenience	❗ Slightly reduced
Password security	❌ Weak if allowed
Credential theft risk	❌ High without block
Device posture governance	❌ At risk
Compliance	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Chrome Password Blocking with Auto-remediation

Blocking browser password saving matters because:

- Users tend to save credentials for convenience
- Defaults may permit caching of passwords
- Manual configuration across many devices does not scale
- One saved password can lead to multiple account compromises

Acronis M365 Security Posture Management:

- Continuously verifies configuration policies are enabled
- Detects overly permissive browser settings
- Flags deviations from secure baselines
- Automatically enforces restrictive controls
- Ensures consistent credential protection across tenants

Note
This ensures browser settings support security, not undermine it.

MSP operational benefits

For Junior Technicians

- Clear rule: Do not allow password saving in Chrome
- No need to inspect browser settings manually

- Auto-remediation prevents accidental exposure
- Fewer credential-related incidents

For Senior Administrators

- Stronger credential hygiene across endpoints
- Reduced risk of password theft
- Easier audits and security reviews
- Better alignment with corporate security policy

For Customers

- Protected corporate credentials
- Reduced risk of unauthorized access
- Browser usage aligns with security expectations
- Higher confidence in MSP-managed endpoint security

Note

Key takeaway:

- Passwords stored in browsers are easy targets.
- Blocking password saving in Chrome protects corporate credentials.
- Acronis ensures this protection remains enforced automatically.

Windows 10 or later Configuration Policy - Block Password Saving In Microsoft Edge

What is a Device Restrictions Configuration Policy (Edge Password Saving Block)

A Device Configuration Policy in Microsoft Intune can be used to block users from saving passwords in Microsoft Edge on managed devices.

This setting is part of Device Restrictions under Intune configuration profiles and applies to Windows, macOS, Android and iOS when supported.

Note

This control ensures users cannot store passwords in the browser, reducing the risk of credential theft from browser-stored credentials.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/intune/intune-service/configuration/device-restrictions-configure.

Why Microsoft provides this control

Microsoft provides this control to:

- Prevent sensitive credentials from being stored insecurely
- Reduce credential theft via stolen laptops or unmanaged devices
- Limit exposure from shared or unmanaged browsers
- Support corporate security policies
- Align browser behavior with Zero Trust principles

Browser-saved passwords are a common attack vector in compromise and lateral movement.

What happens when the policy is Enabled (recommended)

When the configuration policy blocks password saving in Edge:

- Users are prevented from storing passwords in the browser
- Credentials cannot be extracted from saved browser forms
- Risk of credential theft from stolen or compromised devices is reduced
- Credential hygiene is improved
- Enforcement is consistent across managed devices

Benefits:

- Stronger protection of user credentials.
- Reduced risk of credential reuse and theft.
- Fewer breaches caused by browser-stored passwords.
- Better compliance with corporate security policies.

This ensures credentials remain dynamic and protected, not cached in browsers.

What happens when the policy is Disabled

If password saving is allowed in Edge:

Warning!

- Users may store corporate credentials in the browser
- Saved credentials can be extracted by other processes or malware
- Shared or lost devices expose credentials
- Credential theft risk increases
- Account compromise becomes more likely

Browser-stored passwords can be a single point of failure.

Important clarification (commonly misunderstood)

This policy only blocks saving passwords in the browser

It does not:

- Force users to change current passwords.
- Prevent the use of password managers (unless separately controlled).

It complements other controls such as:

- MFA enforcement
- Legacy authentication blocking
- Device compliance policies

Note
This control protects at the browser level, not just authentication.

Real risks for an MSP

Security risk

Passwords stored in browsers are accessible to:

- Malware
- Local attackers
- Sync features across devices

Compliance & audit risk

If a client asks: Can users store company credentials in the browser?

Without this policy: Answer may expose credential risk.

MSP liability risk

- Credential theft incidents are high impact
- Hard to justify unmanaged password storage
- Reduces trust in MSP security posture

Severity summary

Area	Impact
User convenience	❗ Slightly reduced
Password security	❌ Weak if allowed
Credential theft risk	❌ High without block

Area	Impact
Device posture governance	✖ At risk
Compliance	✖ At risk
MSP accountability	✖ High risk

Why use Acronis M365 Security Posture Management for Edge Password Blocking with Auto-remediation

Blocking browser password saving matters because:

- Users tend to save credentials for convenience
- Defaults may permit password caching
- Manual configuration across many devices does not scale
- One browser-stored password can lead to multiple account compromises

Acronis M365 Security Posture Management:

- Continuously verifies configuration policies are enabled
- Detects overly permissive browser settings
- Flags deviations from secure baselines
- Automatically restores restrictive controls
- Ensures consistent credential protection across tenants

Note
This ensures browser settings support security, not undermine it.

MSP operational benefits

For Junior Technicians

- Clear rule: Do not allow password saving in Edge
- No need to inspect browser settings manually
- Auto-remediation prevents accidental exposure
- Fewer credential-related incidents

For Senior Administrators

- Stronger credential hygiene across endpoints
- Reduced risk of password theft
- Easier audits and security reviews
- Better alignment with corporate security policy

For Customers

- Protected corporate credentials
- Reduced risk of unauthorized access
- Browser usage aligns with security expectations
- Higher confidence in MSP-managed endpoint security

Note

Key takeaway:

- Passwords stored in browsers are easy targets.
- Blocking password saving in Edge protects corporate credentials.
- Acronis ensures this protection remains enforced automatically.

M365 Email security

What Email Security means in Microsoft 365

In Microsoft 365, Email Security protects your organization from email-based threats, which are the most common way cyberattacks begin.

Note

Think of Email Security as a multi-layered filter and monitoring system that:

- Blocks malicious emails before users see them
- Detects compromised accounts
- Prevents sensitive data from leaving the organization
- Protects your domain reputation

Email is often the front door for attackers.

Why Email Security is critical

Most cyber incidents start with:

- Phishing emails
- Malicious attachments
- Compromised internal accounts sending spam or malware
- Email forwarding used to silently steal data

Email Security controls are designed to stop attacks early, before they become business incidents.

What the attached Email Security controls protect

Prevent data exfiltration and silent compromise

Automatic Forwarding – Block

Mail Auto Forwarding controls

These prevent attackers from secretly forwarding emails outside your organization after compromising an account.

Detect and block compromised internal accounts

Default Hosted Outbound Spam Filter Policy

Malware Internal Sender Filter Notification Policy

These detect when an internal account starts sending spam or malware and alert administrators immediately.

Protect users from malware

Malware File Types Filter Policy

Preset EOP Policies (Standard / Strict)

These block dangerous attachment types and known malware before delivery.

Prevent phishing and impersonation

Standard Default Anti-Phishing Policy

This detects:

- Fake senders.
- Impersonation attempts.
- Credential harvesting emails.

Protect your domain reputation

DKIM Signing for Default Domain

This proves that emails sent from your domain are legitimate and prevents spoofing and reputation damage.

What this tells us about security maturity

Email Security status	Security meaning
All policies enforced	✓ Strong email protection
Partial enforcement	! Increased phishing risk
Missing policies	✗ High breach likelihood

Strong email security significantly reduces business email compromise (BEC) and ransomware risk.

Business impact of strong Email Security

With these controls in place:

- Phishing attacks are blocked early
- Compromised accounts are detected quickly
- Sensitive data stays inside the organization
- Your domain reputation remains trusted

Without them:

- One phishing email can lead to financial loss.
- Email forwarding can silently leak data.
- Customers and partners may lose trust.

How Email Security fits into Acronis M365 security posture management

Email security settings:

- Change over time.
- Can be weakened unintentionally.
- Differ across tenants and defaults.

Acronis M365 security posture management:

- Continuously monitors email security controls
- Detects deviations from best practices
- Auto-remediates safe configurations
- Ensures consistent protection across tenants

Note

Key takeaway:

- Email is the most common attack vector.

Strong email security stops threats before they reach users. Continuous posture management ensures those protections never drift.

This is why Email Security is a core pillar of Microsoft 365 security posture.

Automatic Forwarding - Block

What is the Automatic Forwarding Email (Transport rule)

Mail Forwarding (Transport) Rule blocks automatic email forwarding from internal mailboxes to external recipients.

It prevents:

- Inbox rules that auto-forward emails externally.
- Hidden or malicious forwarding configurations.
- Silent data exfiltration via email forwarding.

The rule is enforced at the Exchange Online mail flow level, before messages leave the tenant.

This control specifically targets automatic forwarding, not user-initiated manual forwarding.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/exchange/mail-flow-rules-transport-rules-in-exchange-2013-exchange-2013-help#transport-rules-in-exchange-2013.

Why Microsoft provides this control

Microsoft includes this rule to:

- Prevent data exfiltration via email
- Reduce the risk of Business Email Compromise (BEC)
- Stop attackers from silently siphoning emails
- Support compliance and data protection requirements
- Protect organizations from misconfigured or abused mailbox rules

Automatic external forwarding is a well-known attacker persistence technique.

What happens when the rule is Enabled (recommended)

When automatic external forwarding is blocked:

Automatic forwarding to external addresses is prevented Malicious inbox rules cannot exfiltrate email Sensitive information stays inside the organization Silent attacker persistence is disrupted Email security posture is strengthened

Benefits:

- Strong protection against data leakage.
- Reduced impact of compromised accounts.
- Improved compliance with data protection policies.
- Faster detection of malicious activity.

What happens when the rule is Disabled or Missing

If this transport rule is not enabled:

Warning!

- Emails can be automatically forwarded outside the organization
- Attackers can silently receive copies of emails
- Data exfiltration may go unnoticed for long periods
- Users may not realize their mailbox is compromised

This is one of the most common post-compromise techniques.

Important clarification (commonly misunderstood)

- This rule blocks automatic forwarding only
- It operates before messages exit the tenant
- It overrides mailbox-level forwarding rules

This makes it a high-impact.

Real risks for an MSP

Security risk

- Attackers commonly create hidden inbox rules.
- Email content is leaked silently.
- Compromises persist even after password resets.

Compliance & audit risk

If a client asks: How did confidential emails leave the company? Without this rule, there may be no alert and no clear trail.

MSP liability risk

- Missing a baseline control is difficult to justify
- Data leakage incidents carry high reputational impact
- MSP may be blamed for weak email governance

Common MSP mistakes related to this rule

- Assuming mailbox rules are enough.
- Allowing external forwarding temporarily.
- Forgetting to enable the rule after migrations.
- Not monitoring rule presence or changes.
- Not aligning with security posture baselines.

Severity summary

Area	Impact
Email availability	✓ No impact
User experience	✓ No impact
Data protection	✗ High risk if missing
Business Email Compromise exposure	✗ High
Incident detection	✗ Reduced
MSP accountability	✗ High risk

Why use Acronis M365 Security Posture Management for Automatic Forwarding Protection with Auto-remediation

This transport rule is critical because:

- It protects against silent data leakage
- It must remain enabled at all times
- It can be accidentally removed or modified
- Manual checks are unreliable at scale

Acronis M365 Security Posture Management:

- Continuously verifies the rule is present
- Detects removal or modification immediately
- Flags deviations from baseline
- Automatically restores the rule when missing
- Prevents long-term data exfiltration gaps

This ensures data stays inside the organization by default.

MSP operational benefits

For Junior Technicians

- Simple rule: External auto-forwarding = Risk
- No need to inspect mailbox rules manually

- Auto-remediation enforces it by default
- Fewer complex investigations

For Senior Administrators

- Consistent protection across all tenants
- Reduced risk of long-term Business Email Compromise persistence
- Clear governance over mail flow
- Stronger security posture reporting

For Customers

- Reduced risk of sensitive data leakage
- Stronger protection after account compromise
- Better compliance with data protection standards
- Increased trust in MSP-managed email security

Note

Key takeaway:

- Blocking automatic external forwarding stops silent data exfiltration.
- If the rule is missing, attackers will use it.
- Acronis ensures it is always enforced automatically.

Mail Auto Forwarding	Automatic Forwarding - Block
Prevention	Detection & Enforcement
Stops most auto-forwarding outright	Catches edge cases, misconfigurations, or regressions

Mail Auto Forwarding control whether automatic external forwarding is allowed at the tenant mail-flow level, while Automatic Forwarding - Block rule actively blocks forwarding behavior during message processing.

They solve the same risk, but at different layers.

Default Hosted Outbound Spam Filter Policy

What is the Default EOP Outbound Spam Filter Policy

The Default Exchange Online Protection (EOP) outbound spam filter policy monitors outbound email traffic from Microsoft 365 and detects suspicious or abusive sending behavior.

It helps identify:

- Compromised user mailboxes.
- Accounts sending spam or phishing.

- Automated or abnormal outbound email patterns.
- Malicious content sent from inside the tenant.

This policy applies by default to all users unless overridden.

It as automatic abuse detection for outbound email.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/defender-office-365/outbound-spam-policies-configure.

Why Microsoft provides this policy

Microsoft includes the default EOP outbound spam filter policy to:

- Detect compromised accounts early
- Limit the spread of spam and malicious emails
- Protect tenant and domain reputation
- Prevent Microsoft 365 from being used as a spam relay
- Automatically contain incidents before they escalate

Outbound spam is often the first visible indicator of account compromise.

What happens when the policy is enabled and properly configured(recommended)

When the default EOP outbound spam filter policy is active and correctly configured:

Suspicious outbound email patterns are detected Compromised accounts are automatically limited or blocked Spam and malicious emails are prevented from leaving the tenant Alerts are generated for investigation Tenant reputation is protected

Benefits:

- Faster detection of compromised users.
- Reduced damage from internal phishing or spam.
- Lower risk of domain or IP blacklisting.
- Improved incident response and containment.

What happens when the policy is disabled, weakened, or overridden

Warning!
If the default EOP outbound spam filter policy is disabled or misconfigured:

- Compromised accounts can send large volumes of spam
- Phishing emails may reach external recipients
- Tenant reputation can be damaged quickly
- Blacklisting by external mail systems becomes likely
- Incidents may only be detected after complaints

Outbound abuse can escalate within minutes.

Real risks for an MSP

Security risk

- Compromised accounts can be abused silently.
- Attackers use internal trust to spread phishing.
- Malware campaigns may originate from the tenant.
- Reputational & compliance risk.
- A client could hears: Your company sent us spam or phishing emails.

The impact includes:

- Loss of trust
- Brand damage
- Possible contractual or regulatory consequences

MSP liability risk

- Poor outbound controls are hard to justify post-incident
- Late detection increases customer dissatisfaction
- MSP credibility may be questioned

Common MSP mistakes related to the default EOP outbound policy

- Assuming the default policy is always sufficient.
- Creating custom policies that override protections.
- Disabling automatic restrictions.

- Not monitoring alerts or actions taken.
- Treating outbound spam as low priority.

Severity summary

Area	Impact
Email availability	❌ May be restricted during incidents
User experience	❌ Impacted when accounts are limited
Tenant reputation	❌ High risk
Incident containment	❌ Delayed
Compliance	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Managemen for the Default EOP Outbound Spam Filter Policy with Auto-remediation

This policy is critical because:

- It protects tenant reputation
- It detects compromised accounts early
- It can be weakened or overridden unintentionally
- Manual review does not scale across many tenants

Acronis M365 Security Posture Management:

- Continuously verifies the default EOP outbound policy is enabled
- Detects weak or overridden configurations
- Flags deviations from approved baselines
- Automatically remediates risky changes
- Ensures consistent protection across all tenants

This ensures outbound abuse is detected and contained automatically.

MSP operational benefits

For Junior Technicians

- Clear signal: Outbound spam activity = possible compromise
- Less guesswork during incidents
- Automatic containment reduces stress
- Fewer escalations due to delayed response

For Senior Administrators

- Consistent outbound security enforcement
- Reduced reputational incidents
- Faster detection and response
- Stronger posture reporting

For Customers

- Reduced risk of their tenant sending spam or phishing
- Better protection of brand and reputation
- Faster response to compromised accounts
- Higher trust in MSP-managed security

Note

Key takeaway:

- Outbound spam is often the first sign of compromise.
- The default EOP outbound spam filter contains the damage, if it's enforced.
- Acronis ensures this protection stays enforced automatically.

DKIM Signing For Default Domain

What is DKIM (DomainKeys Identified Mail) in Microsoft 365

DKIM is an email authentication method that adds a cryptographic digital signature to outbound emails sent from your domain.

This signature allows receiving mail systems to verify that:

- The email was sent by an authorized server
- The message was not modified in transit
- The sender domain is legitimate

DKIM protects the integrity and trustworthiness of outbound email.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure.

Why Microsoft provides DKIM

Microsoft provides DKIM to:

- Prevent email spoofing and impersonation.
- Improve email deliverability.
- Support Domain-based Message Authentication, Reporting, and Conformance (DMARC) enforcement
- Reduce phishing success rates
- Meet modern email security standards

DKIM is a core requirement for secure email and is expected by most modern mail systems.

What happens when DKIM is enabled (recommended)

When DKIM is enabled for a domain:

- Outbound emails are cryptographically signed
- Receiving servers can verify message authenticity
- Spoofed emails pretending to be your domain are rejected
- DMARC policies can be enforced properly
- Email deliverability improves

Benefits:

- Reduced phishing and domain impersonation.
- Better trust with external recipients.
- Lower chance of emails being marked as spam.
- Stronger overall email security posture.

What happens when DKIM is not enabled

If DKIM is missing or disabled:

Warning!

- Outbound emails are easier to spoof
- Domain impersonation attacks are more likely
- DMARC enforcement is weakened or impossible
- Legitimate emails may be marked as spam
- Brand reputation is at risk

Without DKIM, attackers can more easily:

- Send phishing emails that appear to come from your domain
- Damage your organization's trust and credibility

Real risks for an MSP

Security risk

- Attackers can spoof the customer's domain.
- Phishing campaigns appear more legitimate.
- Users and partners are more likely to trust malicious emails.
- Reputational & compliance risk.
- Your partners could say: We received phishing emails from your domain.

The impact includes:

- Brand damage
- Loss of trust
- Possible regulatory or contractual consequences

MSP liability risk

- Missing DKIM is a baseline security gap
- Difficult to justify in post-incident reviews
- MSP may be blamed for weak email authentication

Common MSP mistakes related to DKIM

- Enabling DKIM for only one domain.
- Forgetting to enable DKIM after domain migration.
- Not validating DNS records.
- Not monitoring DKIM status continuously.
- Not aligning DKIM with DMARC policies.

Severity summary

Area	Impact
Email availability	✓ No impact
User experience	✓ No impact
Domain spoofing risk	✗ High
Email deliverability	✗ Reduced
Phishing exposure	✗ Increased
MSP accountability	✗ High risk

Why use Acronis M365 Security Posture Management for DKIM with Auto-remediation

DKIM is critical because:

- It depends on correct DNS configuration.
- It can break silently after changes.
- It is often forgotten during tenant or domain updates.
- Manual checks do not scale across tenants.

Acronis M365 Security Posture Management:

- Continuously monitors DKIM status
- Detects missing or disabled DKIM
- Flags deviations from security baselines
- Automatically remediates configuration gaps
- Ensures DKIM remains enforced over time

This ensures your customer's domain reputation is always protected.

MSP operational benefits

For Junior Technicians

- No need to deeply understand DNS or cryptography
- Clear signal: DKIM missing = Risk
- Auto-remediation prevents configuration drift
- Fewer tickets

For Senior Administrators

- Consistent email authentication across all tenants
- Reduced phishing and spoofing incidents
- Easier DMARC enforcement
- Stronger security posture reporting

For Customers

- Better protection against impersonation attacks
- Improved email deliverability
- Stronger brand and domain reputation
- Higher trust in MSP-managed email security

Note

Key takeaway:

- DKIM proves your emails are legitimate.
- Without it, attackers can pretend to be you.
- Acronis ensures DKIM stays enabled automatically.

Malware File Types Filter Policy

What is the Malware File Types Filter Policy in Microsoft 365

The Malware File Types Filter Policy blocks emails that contain attachments with file types commonly used to deliver malware.

These file types often include:

- Executable files (e.g. .ace, .bat, .cmd, .reg)
- Script files
- Macro-enabled or archive formats used to bypass detection
- Other high-risk attachment types defined by Microsoft

This policy stops dangerous attachments before users can open them.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure.

Why Microsoft provides this policy

Microsoft includes malware file type filtering to:

- Prevent malware infections at the email gateway
- Reduce reliance on user awareness
- Block known high-risk attachment vectors
- Protect endpoints and identities downstream
- Support a defense-in-depth email security model

Email attachments remain one of the most common malware delivery methods.

What happens when the policy is enabled and properly configured(recommended)

When risky file types are blocked:

Emails with dangerous attachments are stopped automatically Users never receive high-risk files Malware infections are prevented early Security incidents are reduced Endpoint and identity protections are reinforced

Benefits:

- Strong reduction in malware incidents.
- Lower risk of ransomware and credential theft.
- Less reliance on user behavior.
- Improved overall security posture.

What happens when the policy is disabled or weakened

Warning!
If malware file type filtering is disabled or too permissive:

- Users may receive executable or script-based malware
- One click can lead to endpoint compromise
- Malware can spread laterally in the environment
- Ransomware risk increases significantly
- Incidents escalate quickly and widely

Attachment-based malware often causes high-impact, high-cost incidents.

Real risks for an MSP

Security risk

- Malware can reach endpoints directly.
- Attackers bypass users via disguised attachments.
- One infected user can impact the entire tenant.
- Compliance & operational risk.
- A client could asks: Why was this malware allowed through email?

Missing baseline attachment filtering is difficult to justify.

MSP liability risk

- Malware incidents carry high remediation costs
- Downtime and data loss increase
- MSP security maturity may be questioned

Common MSP mistakes related to malware file type filtering

- Relying only on antivirus or endpoint protection.
- Allowing risky file types for convenience.
- Not reviewing custom allow lists.
- Assuming users won't open dangerous attachments.
- Not monitoring policy changes.

Severity summary

Area	Impact
Email availability	❌ Some attachments blocked
User experience	❌ Minor friction
Malware infection risk	❌ High if missing
Ransomware exposure	❌ High
Incident impact	❌ Severe
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Malware File Types Filtering with Auto-remediation

This policy is critical because:

- It is often weakened for convenience
- Changes may go unnoticed
- Manual review doesn't scale
- One exception can reintroduce major risk

Acronis M365 Security Posture Management:

- Continuously monitors malware file type filtering
- Detects disabled or weakened configurations
- Flags deviations from secure baselines
- Automatically restores recommended settings
- Prevents long-term exposure to malware risk

This ensures dangerous attachments stay blocked by default.

MSP operational benefits

For Junior Technicians

- Simple rule: Executable attachments = Dangerous
- No need to understand malware techniques
- Auto-remediation enforces safe defaults
- Fewer malware-related tickets

For Senior Administrators

- Consistent attachment protection across tenants
- Reduced malware and ransomware incidents
- Stronger email security posture
- Easier compliance justification

For Customers

- Lower risk of malware infection
- Fewer disruptions caused by ransomware
- Better protection of business data
- Higher confidence in MSP-managed security

Note

Key takeaway:

- Most malware arrives by email attachment.
- Blocking risky file types stops attacks before they start.
- Acronis ensures this protection stays enforced automatically.

Malware Internal Sender Filter Notification Policy

What is Malware Internal Sender Filter Notification Policy

This setting controls alerting, not blocking.

Microsoft Defender already blocks outbound malware by default

This toggle decides whether Aadmins are notified when that block happens

So the real question this setting answers is: Does MSP want to know immediately when an internal account tries to send malware?

Why this alert matters

When this alert triggers, it usually means one of the following is already true:

- The user account is compromised
- The user's device is infected
- A malicious app is sending email as the user

Note
This is not a false positive scenario

Note
This is a high-confidence security signal

Blocking without alerting = silent compromise.

Impact if Malware Internal Sender Filter Notification Policy is Enabled (recommended)

When enabled:

- Admins are notified immediately
- Compromised accounts are identified early
- Incident response can start right away
- Malware spread and reputation damage are reduced

From an MSP perspective:

This turns Microsoft Defender from a silent blocker into an early-warning system

Impact if Malware Internal Sender Filter Notification Policy is Disabled

If disabled:

Warning!

- Malware sending attempts may be blocked silently.
- Compromised accounts remain active.
- Infected devices stay online.
- Repeated attempts may occur unnoticed.
- Investigation starts late — often after customer complaints.

This creates a false sense of security:

Nothing bad happened

when in reality: Something bad was blocked, but never investigated.

Why this is flagged / reviewed in security posture tools

Security posture tools (like Acronis) care about this setting because:

Blocking alone does not equal security

Alerts are required for:

- Accountability
- Investigation
- Containment
- Missed alerts = missed incidents.

This is why it's treated as a baseline security control, not an optional feature.

Real risks for an MSP

Security risk

- Compromised accounts stay active longer.
- Malware retries may succeed via other channels.

Compliance & audit risk

- If asked When did this compromise start?
- Without alerts: We don't know.

MSP liability risk

- Hard to justify lack of visibility.
- Customers expect notification of active compromise.
- Silent failures damage trust.

Correct MSP configuration (recommended)

Enable this alert

Route alerts to:

- Monitored mailbox.
- SOC / ticketing system.
- Do not rely on blocking only.

Severity summary

Area	Impact
Email availability	❌ May be restricted during containment
User experience	❌ Impacted when account is blocked
Malware detection	❌ Severely reduced if alerting is disabled
Incident response	❌ Delayed or missed
Reputational risk	❌ High
MSP accountability	❌ High risk

MSP operational benefits

For Junior Technicians

- Clear signal: Outbound malware alert = active compromise
- No guesswork on severity
- Faster escalation paths
- Reduced chance of missing critical incidents
- Easier triage and prioritization

For Senior Administrators

- Earlier detection of compromised users and devices
- Reduced dwell time of malware in the environment
- Better correlation with identity, endpoint, and mail signals
- Stronger audit trail and incident documentation
- Improved overall security posture metrics

For Customers

- Faster containment of compromised accounts
- Reduced risk of malware spreading externally
- Better protection of brand and reputation
- Clear communication during incidents
- Higher trust in MSP-managed security operations

Note

Key takeaway:

- Alerts turn blocked attacks into action.
- Without them, protection depends on manual investigations.
- Acronis ensures the baseline stays enforced automatically.

Preset EOP Policy (Standard) & Preset EOP Policy (Strict)

What are Preset EOP (Exchange Online Protection) Policiy in Microsoft Defender for Office 365

Preset EOP Policy are Microsoft-managed, preconfigured security policies that apply recommended best-practice protections across Microsoft 365 email and collaboration workloads.

They cover multiple protection areas, including:

- Anti-phishing
- Anti-malware
- Anti-spam
- Safe Links
- Safe Attachments
- This is preset Microsoft mandatory security baseline, maintained and updated

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies.

Why Microsoft provides Preset Security Policies

Microsoft introduced preset security policies to:

- Simplify security configuration for customers and MSPs
- Reduce misconfiguration risk
- Provide consistent baseline protection
- Keep security aligned with evolving threat intelligence
- Lower the operational burden of managing dozens of individual policies

They are designed especially for:

- Small and mid-size organizations
- MSP-managed tenants
- Teams without deep security expertise

What happens when Preset EOP Policy (Standard) is Enabled (recommended)

When preset security policies are enabled:

- Microsoft-recommended protections are enforced
- Policies are automatically updated as threats evolve
- Email and collaboration workloads receive layered protection
- Misconfiguration risk is reduced
- Security posture is standardized

Benefits:

- Faster security maturity.
- Reduced exposure to common email threats.
- Less manual policy tuning.
- Stronger default protection across the tenant.

Microsoft provides two levels:

- Standard – balanced security with minimal user disruption.
- Strict – stronger protection with higher security enforcement.

What happens when Preset EOP Policy (Standard) is Disabled

Warning!
If preset security policy is disabled:

- Protection depends on manual configuration
- Inconsistent settings may exist across workloads
- Policies may fall behind current threat techniques
- Gaps may appear during tenant changes or growth
- Security posture becomes harder to audit

Custom-only environments often suffer from configuration drift.

Real risks for an MSP

Security risk

- Gaps in email and collaboration protection.
- Inconsistent enforcement across tenants.
- Increased success of phishing and malware attacks.

MSP liability risk

- Harder to defend security posture after incidents.
- Increased reliance on manual expertise.
- More opportunities for misconfiguration.

Severity summary

Area	Impact
Email availability	✓ No impact
User experience	! Depends on policy level
Baseline protection	✗ Inconsistent if disabled
Threat exposure	✗ Increased
Incident likelihood	✗ Higher
MSP accountability	✗ At risk

Why use Acronis M365 Security Posture Management for Preset EOP Policy (Standard) with Auto-remediation

Preset security policies are powerful, but:

- They can be overridden by custom policies
- They can be partially disabled
- Changes may go unnoticed
- Manual reviews do not scale across many tenants

Acronis M365 Security Posture Management:

- Continuously verifies preset policies are enabled
- Flags deviations from baseline
- Automatically remediates missing or disabled presets
- Ensures consistent security posture across all tenants

This keeps Microsoft's recommended baseline continuously enforced.

MSP operational benefits

For Junior Technicians

- No need to design complex security policies
- Clear signal: Preset policies disabled = Risk
- Reduced configuration errors
- Faster onboarding of new tenants

For Senior Administrators

- Consistent baseline across customers
- Reduced policy maintenance overhead
- Fewer gaps caused by human error
- Easier posture reporting and audits

For Customers

- Strong, Microsoft-recommended protection
- Lower risk of phishing and malware incidents
- Faster adoption of new security improvements
- Higher confidence in MSP-managed security

Note

Key takeaway:

- Preset EOP Policy (Standard) provides a secure default.
- Without them, protection depends on manual investigations.
- Acronis ensures the baseline stays enforced automatically.

Standard Default Anti-Phishing Policy

What is the Standard Default Anti-Phishing Policy in Microsoft 365

The Standard Default Anti-Phishing Policy is a Microsoft-managed security policy that provides baseline phishing protection for all Exchange Online mailboxes.

It protects against:

- Phishing emails.
- Spoofed sender domains.
- Impersonation attempts (users, domains, brands).
- Credential-harvesting attacks.

This policy applies automatically to all users and serves as the foundation of phishing protection in Microsoft 365.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about.

Why Microsoft provides this policy

Microsoft includes the Standard Default Anti-Phishing Policy to:

- Protect organizations from the most common email attack type
- Reduce reliance on user awareness
- Detect spoofing and impersonation at scale
- Leverage Microsoft threat intelligence and machine learning
- Provide consistent, tenant-wide phishing protection

Phishing remains the primary entry point for account compromise and ransomware.

What happens when the policy is Enabled (recommended)

When the Standard Default Anti-Phishing Policy is enabled:

- All mailboxes receive baseline phishing protection
- Spoofed sender domains are detected
- Impersonation attempts are identified
- Suspicious emails are blocked or mitigated
- Machine-learning detection adapts to new attacks

Benefits:

- Reduced credential-theft risk.
- Fewer successful phishing campaigns.
- Consistent protection across all users.
- Improved overall email security posture.

This policy ensures no mailbox is left unprotected.

What happens when the policy is Disabled

Warning!
If the Standard Default Anti-Phishing Policy is disabled or weakened:

- Mailboxes may lack baseline phishing protection
- Spoofed emails may reach users
- Impersonation attacks become more successful
- Credential theft risk increases significantly
- Security posture becomes inconsistent

Disabling the default policy often creates unintended protection gaps.

Important clarification (commonly misunderstood)

This policy is Microsoft-managed and updated automatically

The default policy should be treated as the minimum required protection, not optional

Real risks for an MSP

Security risk

- Increased phishing success rates.
- Higher likelihood of credential compromise.
- More downstream incidents (spam, malware, BEC).

Compliance & audit risk

- If a client asks: What phishing protections are enforced for all users?

Without the default policy: The answer may be unclear or inconsistent.

MSP liability risk

- Harder to justify weak phishing defenses post-incident
- Increased customer dissatisfaction after account compromise
- Higher operational workload responding to avoidable incidents

Severity summary

Area	Impact
Email availability	✅ No impact
User experience	❗ Minimal
Phishing protection	❌ Reduced if disabled
Credential theft risk	❌ High
Incident likelihood	❌ Increased
MSP accountability	❌ At risk

Why use Acronis M365 Security Posture Management for the Standard Default Anti-Phishing Policy with Auto-remediation

The Standard Default Anti-Phishing Policy is critical because:

- It is the baseline for all users
- Changes may go unnoticed
- Manual verification across tenants does not scale

Acronis M365 Security Posture Management:

- Continuously verifies the default anti-phishing policy is enabled
- Flags deviations from security baselines
- Automatically remediates missing or disabled protections
- Ensures consistent phishing defense across all tenants

This guarantees every mailbox remains protected by default.

MSP operational benefits

For Junior Technicians

- No need to design phishing policies from scratch
- Clear signal: Default anti-phishing disabled = Risk
- Reduced configuration errors
- Fewer phishing-related tickets

For Senior Administrators

- Consistent phishing protection baseline
- Reduced operational overhead
- Fewer identity-based incidents
- Easier audit and posture reporting

For Customers

- Better protection against impersonation and phishing
- Reduced risk of credential theft
- Fewer disruptive security incidents
- Higher confidence in MSP-managed email security

Note

Key takeaway:

- The Standard Default Anti-Phishing Policy is the foundation of email security.
- Without it, phishing becomes easier and incidents become inevitable.
- Acronis ensures this baseline stays enforced automatically.

Mobile Access

What Mobile Access means in Microsoft 365

In Microsoft 365, Mobile Access controls how smartphones and tablets can access company email and data.

Note

Think of Mobile Access as the security rules applied to phones that connect to your email.

It answers questions like:

- Does the phone have a password or PIN?
- Is the device encrypted?
- Can company email be removed if the phone is lost?
- Are insecure phones blocked from syncing email?

Mobile devices are convenient — but they are also easy to lose or steal.

Why Mobile Access is critical

Mobile devices:

- Frequently contain sensitive email and attachments.
- Are often used outside secure office networks.
- Are more likely to be lost or stolen than laptops.

Without mobile access controls, any phone can become a data leak.

What this tells us about security maturity

Mobile Access status	Security meaning
Policy enforced	✓ Secure mobile email access
Policy weak or missing	✗ High data leakage risk

Mobile access security is especially important in bring-your-own-device (BYOD) environments.

Business impact of strong Mobile Access controls

With Mobile Access protections:

- Lost phones do not automatically mean data loss.
- Email access is limited to secured devices.
- Risk from unmanaged devices is reduced.
- Business data remains protected on the move.

Without them:

- Email can be accessed on insecure phones.
- Stolen devices expose company data.
- Incidents are harder to contain.

How Mobile Access fits into Security Posture Management

Mobile access settings:

- Are often configured once and forgotten.
- May not evolve with new threats.
- Can weaken silently over time.

Acronis M365security posture management:

- Continuously verifies mobile access policies.
- Detects missing or weakened controls.
- Auto-remediates safe configurations.
- Ensures consistent mobile security across tenants.

Note

Key takeaway:

- Email on mobile devices must be protected as carefully as laptops.

Mobile Access policies enforce basic security on phones. Security posture management ensures those protections remain in place over time.

Default Mobile Device Mailbox Policy

What is an Exchange ActiveSync Mobile Device Mailbox Policy

An ActiveSync Mobile Device Mailbox Policy controls the security and behavior of mobile devices that sync email, calendar, contacts, and other mailbox data from Exchange Online using Exchange ActiveSync (EAS).

These policies can enforce settings such as:

- Required device password
- Encryption requirement
- Maximum password attempts
- Password complexity
- Device security features (e.g., screen lock timeout)
- Remote wipe capability

Note
This policy defines security requirements for devices syncing corporate email via ActiveSync.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/mobile-device-mailbox-policies.

Why Microsoft provides this control

Microsoft provides ActiveSync mailbox policies to:

- Protect corporate email and mailbox data on mobile endpoints
- Reduce risk from lost, stolen, or compromised devices
- Ensure devices connecting to Exchange meet security standards
- Support compliance and data-protection requirements
- Prevent unauthorized access to email and related data

Mobile devices with weak or no security settings are a high risk for corporate data exposure.

What happens when the policy is properly configured (recommended)

When an ActiveSync policy is configured and enforced:

- Mobile devices must meet security requirements to sync mail
- Devices without PIN/password, encryption, or timeout are blocked

- Administrators can enforce password complexity
- Remote wipe capability is available for lost/stolen devices
- Exchange data is better protected on mobile endpoints

Benefits:

- Stronger protection of email and mailbox content.
- Reduced risk of unauthorized access via mobile devices.
- Better control over BYOD and corporate devices.
- Easier enforcement of security standards across devices.

This ensures Exchange content remains secure even when accessed from mobile.

What happens when the policy is not configured or weak

If no ActiveSync mailbox policy exists or it is too permissive:

Warning!

- Mobile devices may sync without security controls
- Devices without PIN, encryption, or lock timeout can access email
- Lost/stolen devices expose mailbox content
- Email data leakage risk increases
- Compliance violations may occur

Unprotected mobile access becomes a significant attack vector.

Important clarification (commonly misunderstood)

This policy applies only to ActiveSync email sync

It does not apply to:

- Outlook mobile (which uses modern auth/APIs instead of ActiveSync)
- MDM-enforced controls outside of ActiveSync

It complements:

- Device compliance policies in Intune.
- Conditional Access policies.
- Endpoint management tools.

Note

Even strong mailbox policies cannot replace device-level management and compliance.

Real risks for an MSP

Security risk

- Exchange data accessible from insecure or unmanaged devices.
- Lost phones expose email without protection.
- Attackers can access mailboxes if policies are weak.

Compliance & audit risk

- If a client asks: How do you prevent unsecured phones from accessing email?

Without ActiveSync policies: The answer is uncomfortable.

MSP liability risk

- Mobile access incidents are highly visible
- Data leaks via mobile devices are costly
- MSP security maturity is questioned

Severity summary

Area	Impact
Email availability	❗ Devices may be blocked if non-compliant
User experience	❗ More secure device usage
Data leakage risk	❌ High without policy
Mobile posture governance	❌ Weak if missing
Compliance posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for ActiveSync Device Policies with Auto-remediation

ActiveSync policies matter because:

- Mobile device configurations drift over time.
- Modern authentication and Outlook mobile reduce ActiveSync visibility.
- Manual policy review does not scale across tenants.
- One unprotected device can expose email and credentials.

Acronis M365 Security Posture Management:

- Continuously verifies ActiveSync policy configuration
- Detects missing or weakened security requirements

- Flags deviations from secure baselines
- Automatically restores protective settings
- Ensures consistent mobile email security across all tenants

Note

This ensures mobile devices meet security requirements before syncing email.

MSP operational benefits

For Junior Technicians

- Clear rule: Mobile email sync must meet security controls
- No need to audit each device manually
- Auto-remediation prevents accidental exposure
- Fewer mobile email-related incidents

For Senior Administrators

- Stronger enforcement of mobile security
- Reduced risk of data exposure through email
- Better audit and compliance reporting
- Easier governance across large device fleets

For Customers

- Protected mailbox data on mobile
- Reduced risk from lost or compromised devices
- Predictable secure behavior across devices
- Higher confidence in MSP-managed email security

Note

Key takeaway:

- Mobile email is convenient — but risky without controls.
- ActiveSync mailbox policies enforce core protections.
- Acronis ensures these protections stay enforced automatically.

Remote Access

What Remote Access means in Microsoft 365

In Microsoft 365, Remote Access controls how users and systems connect to your environment from outside the organization.

Note
Think of Remote Access as the rules that govern external connections to your email and services.

It answers questions like:

- Are modern, secure login methods being used?
- Are outdated or insecure connection methods blocked?
- Can automated systems send email safely?

Remote access is essential — but it must be carefully controlled.

Why Remote Access is critical

Most attacks do not come from inside the network. They come from:

- Compromised credentials used remotely
- Old authentication protocols that bypass security controls
- Automated abuse of email sending services

Remote access controls ensure external connections meet modern security standards.

What the attached Remote Access controls protect

Modern Authentication

Modern Authentication enforces:

- Secure, token-based sign-ins.
- Compatibility with Multi-Factor Authentication (MFA).
- Protection against credential replay attacks.

Note
Why it matters:

Modern Authentication is required for advanced security features like MFA and Conditional Access.

SMTP Access (Authenticated SMTP)

SMTP access controls how applications and devices send email remotely.

When tightly controlled:

- Prevents misuse of email for spam or malware.
- Limits abuse from compromised credentials.
- Reduces risk of domain reputation damage.

Note

Why it matters:

SMTP is often abused because it is simple and widely supported.

What this tells us about security maturity

Remote Access status	Security meaning
Modern Auth enforced, SMTP restricted	✓ Secure remote access
Partial enforcement	❗ Increased attack surface
Legacy methods allowed	✗ High risk of compromise

Remote access is a primary entry point for attackers if not controlled.

Business impact of strong Remote Access controls

With proper Remote Access protections:

- Stolen passwords are less useful to attackers
- Automated attacks are blocked
- Email abuse is minimized
- Security policies apply everywhere, not just internally

Without them:

- MFA can be bypassed.
- Automated attacks are easier.
- Email reputation can be damaged.
- Incidents are harder to detect.

How Remote Access fits into Acronis M365 Security Posture Management

Remote access settings:

- Are often legacy-driven.
- Can be re-enabled unintentionally.
- Differ across applications and protocols.

Acronis M365 security posture management:

- Continuously checks Modern Authentication status
- Detects insecure SMTP configurations

- Auto-remediates safe misconfigurations
- Ensures legacy access paths stay closed

Note

Key takeaway:

- Remote access must be secure by design.

Modern Authentication and controlled SMTP access prevent old, insecure entry points. Acronis M365 security posture management ensures these protections remain enforced over time.

Modern Authentication

What is "Modern Authentication" in Microsoft 365

Modern Authentication is Microsoft’s secure authentication framework that replaces legacy, password-only authentication methods.

It uses modern security technologies such as:

- Multifactor Authentication (MFA)
- Conditional Access policies
- Token-based authentication (OAuth 2.0)
- Risk-based and context-aware sign-in controls

Modern Authentication applies across Microsoft 365 services, including:

- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- Azure / Entra ID

Modern Authentication is the foundation of secure identity access in Microsoft 365.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online#configure-the-default-authentication-policy.

Why Microsoft has Modern Authentication

Microsoft introduced Modern Authentication to:

- Protect accounts from credential-based attacks
- Enforce MFA consistently
- Prevent security controls from being bypassed
- Reduce reliance on insecure legacy protocols

- Support Zero Trust security principles
- Meet modern compliance and regulatory requirements

Legacy authentication methods were not designed for today's threat landscape and are actively targeted by attackers.

What happens when Modern Authentication is enabled (recommended)

When Modern Authentication is enabled:

- Authentication uses secure, modern protocols
- MFA and Conditional Access are enforced
- Legacy, password-only authentication is blocked
- Identity risk and sign-in protections apply

Benefits:

- Strong protection against credential-based attacks.
- MFA cannot be bypassed by legacy protocols.
- Reduced attack surface across Microsoft 365.
- Better compliance alignment.
- Improved overall security posture.

What happens when Modern Authentication is NOT enabled

If Modern Authentication is not fully enforced:

Warning!

- Legacy authentication may still be allowed
- MFA and Conditional Access can be bypassed
- Password-only authentication may still work
- Attackers can exploit older protocols

This creates a false sense of security, where MFA is enabled, but not enforced everywhere.

Real risks for an MSP

Security risk

- Legacy protocols are frequently abused
- Password-only authentication is easy to exploit
- MFA bypass remains possible

Compliance and audit risk

- Inability to prove secure authentication compliance
- Weak audit trails during incidents

MSP liability risk

- Partial protection is difficult to defend
- Increased exposure after breaches

Severity summary

Area	Impact
Email availability	✓ No impact
User experience (modern clients)	✓ No impact
MFA enforcement	✗ Inconsistent
Attack surface	✗ Increased
Incident likelihood	✗ High
MSP accountability	✗ At risk

Why use Acronis M365 Security Posture Management to enforce Modern Authentication with Auto-remediation

Modern Authentication protects tenants only when it is enforced everywhere and continuously.

Acronis M365 Security Posture Management:

- Continuously validates Modern Authentication enforcement
- Detects legacy authentication usage
- Flags incomplete configurations
- Automatically remediates deviations
- Prevents accidental re-enablement of legacy auth

This removes reliance on manual checks and human memory.

Note

Modern Authentication is not just a setting — it is a mandatory security baseline. Acronis ensures it stays enforced automatically across all tenants.

MSP operational benefits

For Junior Technicians

- No need to understand legacy authentication protocols in depth.
- Clear security signal: Modern Auth enforced = safe baseline.
- Reduced chance of leaving legacy authentication enabled by mistake.
- Less reliance on manual PowerShell actions.
- Fewer identity-related incidents to troubleshoot.
- Clear posture alerts when enforcement is incomplete.

For Senior Administrators

- Consistent identity security baseline across all customers.
- Reduced operational overhead managing legacy auth exceptions.
- Fewer emergency incidents caused by MFA bypass.
- Stronger audit and forensic posture.
- Easier compliance alignment and reporting.
- Reduced dependency on tribal knowledge and manual checks.

For Customers

- Stronger protection against account compromise
- MFA consistently enforced for all users
- Reduced risk of phishing and credential-based attacks
- Faster and more accurate investigations when incidents occur
- Better compliance readiness
- Increased trust in MSP-managed security

Note

Key takeaway:

- Legacy authentication bypasses modern security controls.
- Enforcing modern authentication protects email access.
- Acronis ensures this protection stays enforced automatically.

SMTP Access

What is Authenticated SMTP (SMTP) in Microsoft 365

Authenticated SMTP (SMTP) is a legacy email submission method that allows devices and applications to send email through Microsoft 365 using:

- A mailbox username
- A password

- The SMTP protocol (port 587)

It is commonly used by:

- Printers and scanners
- Legacy applications
- Monitoring systems
- On-prem or third-party devices

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission.

SMTP is not modern authentication and does not support MFA.

Why Microsoft still has this feature

Microsoft keeps SMTP to:

- Maintain compatibility with legacy devices and applications.
- Support environments that cannot yet use modern authentication.
- Allow controlled exceptions during migration periods.

However, Microsoft strongly discourages its use unless absolutely necessary.

SMTP is considered a high-risk legacy protocol.

What happens when SMTP Access is Disabled (recommended)

When SMTP Access is disabled:

- Legacy password-based email submission is blocked
- MFA bypass paths are removed
- Reduced attack surface
- Stronger alignment with Modern Authentication and Zero Trust

Benefits:

- Major reduction in credential-based attacks.
- Fewer compromised accounts used for spam.
- Improved email security posture.
- Better compliance alignment.

What happens when SMTP Access is Enabled

When SMTP Access is enabled:

Warning!

- Authentication relies on username + password only
- MFA cannot be enforced
- Conditional Access does not apply
- Credentials can be reused or stolen
- Attackers can abuse it to send email

Security implications:

One of the most abused protocols for password-spray attacks

Frequently used for:

- Spam
- Phishing
- Malware distribution.
- Often overlooked because email still works.

Real risks for an MSP

Security risk

- Attackers frequently target SMTP.
- Password-spray attacks succeed even when MFA is enabled.
- Compromised accounts may be used silently for spam.

Compliance & audit risk

If a client asks: How was this account used to send spam? Why was MFA bypassed? SMTP access may be the root cause.

MSP liability risk

- Tenant appears protected but is not
- Security incidents are hard to justify post-incident
- MSP may be blamed for leaving legacy protocols enabled

Common MSP mistakes related to SMTP Access

- Leaving SMTP AUTH enabled just in case.
- Enabling it globally instead of per-device.
- Forgetting to disable it after migrations.
- Not auditing mailbox-level SMTP settings.
- Assuming MFA protects SMTP (it does not).

Severity summary

Area	Impact
Email availability	✓ No impact (if not needed)
User experience	✓ No impact
MFA enforcement	✖ Bypassed
Attack surface	✖ Significantly increased
Spam / abuse risk	✖ High
MSP accountability	✖ High risk

Why use Acronis M365 Security Posture Management for SMTP Access with Auto-remediation

SMTP is risky because:

- It exists in multiple places.
- It's easy to forget.
- It's often enabled for temporary reasons.
- It silently bypasses modern security controls.

Acronis M365 Security Posture Management:

- Continuously monitors SMTP Access status
- Detects tenant-level and mailbox-level exceptions
- Flags deviations immediately
- Automatically disables SMTP Access where not approved
- Prevents accidental re-enablement

This ensures SMTP Access is disabled by default and only allowed when explicitly justified.

MSP operational benefits

For Junior Technicians

- No need to understand SMTP internals
- Clear signal: SMTP enabled = High Risk
- Auto-remediation prevents accidental exposure
- Fewer spam-related incidents to handle

For Senior Administrators

- Consistent enforcement across all tenants
- Reduced spam and abuse incidents
- Lower operational noise
- Stronger identity and email security posture

For Customers

- Reduced risk of account compromise
- Fewer spam and phishing incidents originating from their tenant
- Better compliance alignment
- Higher confidence in MSP security management

Note

Key takeaway:

- SMTP AUTH is a legacy protocol that bypasses modern security.
- If it's enabled, attackers will try to use it.
- Acronis ensures it stays disabled automatically.

Sharing

What Sharing means in Microsoft 365

In Microsoft 365, Sharing controls how files and information can be shared with people outside your organization.

Note

Think of Sharing as the rules that decide who can access your files, for how long, and under what conditions.

It answers questions like:

- Can files be shared anonymously?
- How long do shared links remain valid?
- Can external users re-share content?
- Are infected files blocked?
- Are storage limits monitored?

Sharing enables collaboration — but without limits, it can become a data leakage risk.

Why Sharing controls are critical

Most data leaks are not malicious — they are accidental.

Sharing controls help prevent:

- Sensitive data being accessible indefinitely.
- External users spreading access unintentionally.
- Malware spreading via shared files.
- Loss of visibility over who has access to what.

Sharing controls balance collaboration and protection.

What the attached Sharing controls protect

Anonymous Links Expiry

Limits how long anyone with the link access remains valid.

Note
Why it matters:

Old links should not grant access forever.

External (Guest) Users Resharing

Prevents guests from sharing files with others.

Note
Why it matters:

Only trusted internal users should extend access.

Global Default Sharing Policy

Defines the maximum level of sharing allowed across SharePoint and OneDrive.

Note
Why it matters:

This is the ceiling for all sharing behavior.

SharePoint Block Infected Files Download

Prevents users from downloading files identified as malware.

Note
Why it matters:

Stops malicious files from spreading internally or externally.

SharePoint Storage Warning

Alerts when storage usage approaches limits.

Note
Why it matters:

Prevents operational disruption and supports capacity planning.

What this tells us about security maturity

Sharing configuration	Security meaning
Controlled, time-limited sharing	✓ Secure collaboration
Open or unlimited sharing	✗ High data exposure risk

Strong sharing controls indicate mature data governance.

Business impact of strong Sharing controls

With Sharing protections:

- Data exposure risk is reduced.
- External collaboration is controlled.
- Malware spread is limited.
- Access is time-bound and accountable.

Without them:

- Links can remain active indefinitely.
- External users can re-share data freely.
- Sensitive information can escape control.
- Incidents are harder to trace.

How Sharing fits into Acronis M365 security posture management

Sharing settings:

- Are easy to loosen for convenience.
- Are rarely reviewed after initial setup.
- Can change as new sites and users are added.

Acronis M365 security posture management:

- Continuously monitors sharing configurations
- Detects excessive or risky settings
- Auto-remediates safe misconfigurations
- Ensures sharing stays aligned with policy

Note

Key takeaway:

- Sharing enables collaboration — but must be controlled.

Time-limited, monitored sharing prevents accidental data leaks. Acronis M365 security posture management ensures sharing stays safe as the organization grows.

Anonymous Links Expiry

What is Anonymous Sharing Link Expiry in Microsoft 365

Anonymous sharing links (also called Anyone links) allow external users to access SharePoint or OneDrive content without signing in.

The expiration policy defines a maximum lifetime for these links. After the expiration date, the link automatically stops working.

Note

This control limits how long unauthenticated access to shared content is allowed.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/microsoft-365/solutions/best-practices-anonymous-sharing?view=o365-worldwide#set-an-expiration-date-for-anyone-links.

Why Microsoft provides this control

Microsoft provides anonymous link expiration to:

- Reduce long-term unauthorized access
- Limit exposure from forgotten or overshared links
- Maintain governance over externally shared content
- Reduce risk from leaked or forwarded links
- Support compliance and data-protection best practices

Anonymous links are convenient, but high risk when they never expire.

What happens when expiration is enforced (recommended)

When a maximum expiration period is set:

- Anonymous links automatically expire
- Forgotten or abandoned links stop working
- External access is time-bound

- Exposure window is limited
- Control over shared data is improved

Benefits:

- Reduced risk of data leakage.
- Stronger sharing governance.
- Better compliance posture.
- Less reliance on users to manually clean up access.

This turns anonymous sharing into temporary access instead of permanent exposure.

What happens when expiration is not enforced

If anonymous links do not expire:

Warning!

- Links may remain valid indefinitely
- External access persists beyond business need
- Leaked or forwarded links stay usable
- Access cannot be reliably reviewed or revoked
- Sensitive data may remain exposed long-term

This results in persistent, unaudited external access.

Important clarification (commonly misunderstood)

Anonymous links:

- Do not require authentication.
- Are not tied to a specific user identity.

Audit logs may show:

When a link was created

But often cannot reliably show:

Who accessed the content

Expiration is one of the most effective controls available for anonymous sharing.

Real risks for an MSP

Security risk

- Sensitive data remains accessible indefinitely.
- Links can be shared far beyond intended recipients.
- Data exposure may go unnoticed.

Compliance & audit risk

- If a client asks: Who still has access to this document?
- Without expiration: Anyone who has the link — potentially forever.

MSP liability risk

- Unlimited anonymous access is difficult to justify.
- Data-leak incidents have high impact.
- Weak sharing governance damages trust.

Severity summary

Area	Impact
File availability	✓ No impact
User experience	! Minor (links expire)
Data exposure risk	✖ High if not enforced
Access governance	✖ Weak without expiration
Compliance posture	✖ At risk
MSP accountability	✖ High risk

Overall severity if missing: High

Why use Acronis M365 Security Posture Management for Anonymous Links Expiry with Auto-remediation

Anonymous link expiration is critical because:

- It is often left unset
- Convenience overrides security in user behavior
- Manual reviews do not scale
- A single forgotten link can expose sensitive data

Acronis M365 Security Posture Management:

- Continuously verifies anonymous sharing expiration settings
- Detects unlimited or overly long expiration periods
- Flags deviations from approved baselines

- Automatically enforces expiration limits
- Prevents configuration drift over time

This ensures anonymous access is always temporary by default.

MSP operational benefits

For Junior Technicians

- Clear rule: Anonymous access must expire
- No need to audit individual sharing links
- Auto-remediation enforces expirations
- Fewer data-exposure investigations

For Senior Administrators

- Consistent sharing governance across tenants
- Reduced long-term data-leak risk
- Easier compliance justification
- Stronger posture reporting

For Customers

- Better control over externally shared data
- Reduced risk from leaked or forgotten links
- Improved compliance and governance
- Higher confidence in MSP-managed collaboration security

Note

Key takeaway:

- Anonymous links should never be permanent.
- Expiration limits exposure when links are leaked or forgotten.
- Acronis ensures anonymous sharing always expires automatically.

External (Guest) Users Resharing

What is External (Guest) Users Resharing Control in Microsoft 365

This setting controls whether external (guest) users are allowed to reshare content they have been granted access to in Microsoft 365 (SharePoint and OneDrive).

When resharing is disabled:

- Guests can access content only as originally granted.
- Guests cannot extend access to other users.
- Access expansion is restricted to internal users only.

This control limits who can propagate access to shared content.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-limit-sharing?view=o365-worldwide.

Why Microsoft provides this control

Microsoft provides guest resharing controls to:

- Prevent uncontrolled access expansion
- Maintain ownership of sharing decisions
- Reduce accidental or malicious data exposure
- Support least-privilege and Zero Trust principles
- Improve governance over externally shared content

External users should use granted access, not delegate access.

What happens when configuration is Prevent Users From Resharing (recommended)

When guest users are prevented from resharing:

Only authorized internal users can grant access External access remains limited and predictable Sensitive data is better protected Sharing boundaries are clearly enforced Risk of accidental data leaks is reduced

Benefits:

- Stronger control over shared content.
- Reduced risk of uncontrolled access sprawl.
- Improved compliance posture.
- Easier investigation and access review.

This ensures access does not spread beyond intent.

What happens when configuration is Allow External Users to Reshare or Ignore

If guest users are allowed to reshare:

Warning!

- Access can spread beyond original approval
- Internal visibility into who has access is reduced
- Sensitive data may reach unauthorized parties
- Data exposure may go unnoticed
- Revoking access becomes more complex

This creates chain-sharing risk, especially for sensitive content.

Important clarification (commonly misunderstood)

This setting:

- Does not block guests from accessing content.
- Only restricts their ability to share further.
- Internal users retain full control.

Works best when combined with:

- Anonymous Link Expiry
- Audit logging

The goal is control, not collaboration denial.

Real risks for an MSP

Security risk

- Sensitive data spreads outside visibility.
- Sharing chains are hard to track.
- Data leaks can occur without alerts.

Compliance & audit risk

- If a client asks: Who granted access to this external user?

With Allow External Users to Reshare or Ignore enabled: The answer may be unclear.

MSP liability risk

- Difficult to justify unrestricted resharing
- Data-leak incidents damage trust
- Weak sharing governance increases exposure

Severity summary

Area	Impact
File availability	✅ No impact
User experience	❗ Minimal for guests
Access governance	❌ Weak if resharing allowed
Data exposure risk	❌ High

Area	Impact
Compliance posture	✖ At risk
MSP accountability	✖ High risk

Why use Acronis M365 Security Posture Management for External (Guest) Users Resharing with Auto-remediation

Guest resharing control is critical because:

- It is often overlooked
- Users prioritize convenience over governance
- Manual review does not scale
- One resharing chain can expose sensitive data

Acronis M365 Security Posture Management:

- Continuously verifies guest resharing settings
- Detects permissive configurations
- Flags deviations from security baselines
- Automatically restores restrictive settings
- Prevents configuration drift over time

This ensures only authorized users can extend access.

MSP operational benefits

For Junior Technicians

- Clear rule: Guests should not reshare
- No need to audit sharing chains manually
- Auto-remediation enforces safe defaults
- Fewer data-exposure incidents to investigate

For Senior Administrators

- Consistent sharing governance across tenants
- Reduced long-term data-leak risk
- Easier access review and auditing
- Stronger posture reporting

For Customers

- Better control over sensitive data
- Reduced risk of accidental exposure
- Improved compliance and governance
- Higher trust in MSP-managed collaboration security

Note

Key takeaway:

- Guests should use access, not spread it.
- Blocking guest resharing keeps data under control.
- Acronis ensures this governance stays enforced automatically.

Global Default Sharing Policy

What is the Global Default Sharing Policy for SharePoint and OneDrive

The Global Default Sharing Policy defines the maximum external sharing capability allowed across the Microsoft 365 tenant for SharePoint Online and OneDrive.

It controls:

- Whether content can be shared externally at all.
- Whether sharing is limited to specific guests.
- Whether anonymous (Anyone) links are allowed.
- The upper limit that site and user-level settings cannot exceed.

This setting acts as the top-level guardrail for all external sharing in SharePoint and OneDrive.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off.

Why Microsoft provides this control

Microsoft provides an organization-wide sharing level to:

- Enforce consistent sharing boundaries across the tenant
- Prevent over-permissive sharing at site or user level
- Support data protection and governance requirements
- Reduce accidental or uncontrolled data exposure
- Align sharing behavior with business risk tolerance

This control ensures no site or user can exceed what the organization allows.

What happens when Global Default Sharing Policy is properly restricted ("Only people in your organization" recommended)

When the organization-wide sharing level is set appropriately:

- External sharing is limited to approved methods
- Sites cannot override tenant-wide restrictions
- Data exposure risk is reduced
- Sharing behavior is predictable and governable
- Compliance posture is strengthened

Benefits:

- Strong baseline control over data sharing.
- Reduced accidental oversharing.
- Easier auditing and access reviews.
- Clear alignment with security policy.

This establishes defense-in-depth for collaboration.

What happens when the sharing level is too permissive

If the organization-wide sharing level allows broad or anonymous access:

Warning!

- Sensitive data can be shared externally with few restrictions
- Anonymous links may be created tenant-wide
- Oversharing becomes difficult to control
- Data leaks may go unnoticed
- Downstream controls become harder to enforce

Over-permissive tenant settings amplify human error risk.

Important clarification (commonly misunderstood)

This setting defines the maximum allowed sharing

Site-level and OneDrive settings:

- Can only be more restrictive.
- Cannot exceed the tenant-wide level.

Changing this setting immediately affects:

- All sites
- All OneDrive accounts

This makes it one of the highest-impact sharing controls in Microsoft 365.

Real risks for an MSP

Security risk

- Uncontrolled external sharing increases data-leak likelihood.
- Anonymous access may bypass identity controls.
- Sensitive data can leave the organization silently.

Compliance & audit risk

- If a client asks: What is the maximum external sharing allowed?

With permissive settings: The answer may conflict with data-protection expectations.

MSP liability risk

- Weak tenant-wide sharing controls are hard to justify
- Data-exposure incidents carry high reputational impact
- MSP may be blamed for inadequate governance

Severity summary

Area	Impact
File availability	✅ No impact
User experience	❗ Depends on restrictions
Data exposure risk	❌ High if too permissive
Sharing governance	❌ Weak without guardrails
Compliance posture	❌ At risk
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for Global Default Sharing Policy with Auto-remediation

This control is critical because:

- It affects the entire tenant instantly
- It is often set once and forgotten
- Convenience pressure can lead to over-permissive settings
- Manual reviews do not scale across tenants

Acronis M365 Security Posture Management:

- Continuously verifies tenant-wide sharing configuration
- Detects overly permissive sharing levels
- Flags deviations from approved baselines
- Automatically restores safe sharing limits
- Prevents configuration drift over time

This ensures external sharing never exceeds organizational policy.

MSP operational benefits

For Junior Technicians

- Clear rule: Tenant sharing level defines the maximum risk
- No need to audit individual sites manually
- Auto-remediation enforces safe defaults
- Fewer data-exposure incidents to investigate

For Senior Administrators

- Consistent sharing governance across tenants
- Reduced long-term data-leak risk
- Easier compliance and audit discussions
- Stronger posture reporting and visibility

For Customers

- Better control over externally shared data
- Reduced risk of accidental oversharing
- Clear and enforceable collaboration boundaries
- Higher confidence in MSP-managed data governance

Note

Key takeaway:

- The organization-wide sharing level is the guardrail for collaboration.
- If it's too permissive, every site is at risk.
- Acronis ensures these guardrails stay enforced automatically.

SharePoint Block Infected Files Download

What is SharePoint Block Infected Files Download

Malware protection for SharePoint Online and OneDrive scans files stored in Microsoft 365 collaboration services and blocks users from downloading files that are identified as malware.

This protection applies to:

- Files uploaded to SharePoint sites.
- Files stored in OneDrive.

This control prevents malicious files from spreading through collaboration platforms.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/defender-office-365/anti-malware-protection-for-spo-odfb-teams-about.

Why Microsoft provides this control

Microsoft provides SharePoint Block Infected Files Download protection for collaboration services to:

- Prevent malware propagation through shared files
- Protect users from unknowingly downloading malicious content
- Reduce lateral movement inside organizations
- Complement email and endpoint protection
- Support a defense-in-depth security strategy

Collaboration platforms are increasingly used to distribute malware after initial compromise.

What happens when Disallow download is enabled (recommended)

When malware protection is enabled:

- Downloads of malicious files are blocked
- Malware spread inside the organization is reduced
- Security incidents are contained early

Benefits:

- Strong reduction in internal malware infections.
- Lower ransomware and lateral-movement risk.
- Better protection of users and devices.
- Improved overall security posture.

This ensures shared storage does not become a malware distribution channel.

What happens when Allow download or Ignore is enabled

Warning!
If malware protection for SharePoint, OneDrive, and Teams is disabled:

- Users can download infected files
- Malware can spread laterally through shared storage
- One compromised file can impact many users
- Ransomware and credential theft risk increases
- Incidents escalate faster and wider

This turns collaboration platforms into a malware propagation vector.

Important clarification (commonly misunderstood)

This control:

Blocks downloads, not uploads

It does not replace:

- Endpoint protection.
- Email malware filtering.
- It is a critical containment layer.

Blocking downloads buys time for investigation and remediation.

Real risks for an MSP

Security risk

- Malware spreads internally via shared folders.
- Compromised users infect additional endpoints.
- Increased blast radius of a single compromise.

Compliance & audit risk

- If a client asks: Why did multiple users get infected from the same file?

Disabled download protection may be the cause.

MSP liability risk

- Internal malware outbreaks are costly
- Weak internal containment is difficult to justify
- Customer trust may be damaged

Severity summary

Area	Impact
File availability	❌ Infected files blocked
User experience	❗ Minor (download blocked)
Malware spread risk	❌ High if disabled
Lateral movement	❌ High
Incident impact	❌ Severe
MSP accountability	❌ High risk

Why use Acronis M365 Security Posture Management for SharePoint Block Infected Files Download with Auto-remediation

This control is critical because:

- It is sometimes disabled to reduce friction
- Configuration drift can weaken protection
- Manual verification does not scale across tenants
- One exception can expose the entire organization

Acronis M365 Security Posture Management:

- Continuously verifies SharePoint Block Infected Files Download
- Detects weakened configurations
- Flags deviations from approved baselines
- Automatically restores protective settings
- Ensures consistent internal malware containment

This ensures malware is stopped even after it enters collaboration storage.

MSP operational benefits

For Junior Technicians

- Clear rule: Disallow download is enabled -infected files must not be downloadable
- No need to investigate storage manually

- Auto-remediation enforces safe policy
- Fewer internal malware incidents

For Senior Administrators

- Stronger internal containment controls
- Reduced lateral malware spread
- Easier incident scoping and response
- Improved security posture reporting

For Customers

- Reduced risk of internal malware outbreaks
- Better protection of users and devices
- Lower operational disruption
- Higher confidence in MSP-managed collaboration security

Note

Key takeaway:

- Email isn't the only malware vector.
- Blocking malicious file downloads in SharePoint and OneDrive stops internal spread.
- Acronis ensures this protection stays enforced automatically.

SharePoint Storage Warning

What is SharePoint Storage Warning in Microsoft 365

SharePoint Storage Warning tracks how much storage individual SharePoint site collections are consuming compared to their assigned quota.

By configuring:

- A list of monitored sites.
- Storage quotas.
- A usage threshold (percentage of quota).

Admins can receive alerts when a site approaches or exceeds capacity limits.

This control provides early visibility into storage capacity risks.

See the official Microsoft Learn documentation: https://learn.microsoft.com/en-us/sharepoint/manage-site-collection-storage-limits.

Why Microsoft provides this control

Microsoft provides site storage monitoring to:

- Prevent unexpected storage exhaustion
- Avoid service disruption caused by full sites
- Help plan capacity growth proactively
- Maintain performance and availability
- Support operational governance for SharePoint

Storage issues are rarely sudden, they are predictable when monitored correctly.

What happens when storage monitoring and thresholds are configured(recommended)

When storage usage thresholds are set and monitored:

- Admins are alerted before sites run out of space
- Business impact is avoided
- Capacity planning becomes proactive
- SharePoint performance is preserved
- Emergency remediation is reduced

Benefits:

- Early detection of capacity risks.
- Fewer user-reported outages.
- Better storage forecasting.
- Improved operational stability.

This turns storage management from reactive to preventive.

What happens when storage monitoring is not configured

If site storage usage is not monitored:

Warning!

- Sites can suddenly hit storage limits
- File uploads may fail without warning
- Business workflows can be interrupted
- Emergency cleanup or quota increases are required
- Users often detect the issue before IT does

Storage exhaustion almost always becomes a business-impacting incident.

Important clarification (commonly misunderstood)

When a site reaches quota:

- Uploads can fail
- Sync issues may occur

Increasing quota under pressure:

- Is risky.
- Often bypasses governance.

Note
Monitoring thresholds provide time to act safely.

Real risks for an MSP

Operational risk

- Unplanned service disruption.
- Emergency remediation outside change windows.
- Increased support ticket volume.
- Business & compliance risk.
- If a client asks: Why did users suddenly stop uploading files?
- Without monitoring: We were not alerted before the site hit capacity.

MSP liability risk

- Perceived lack of proactive management.
- Reduced customer confidence.
- SLA and trust impact.

Severity summary

Area	Impact
Service availability	❌ Can be disrupted
User experience	❌ Degraded when limits reached
Business continuity	❌ At risk
Capacity governance	❌ Reactive without alerts
MSP accountability	❌ At risk

Why use Acronis M365 Security Posture Management for SharePoint Storage Warning with Auto-remediation

Storage monitoring is critical because:

- Growth patterns vary by site
- Manual reviews do not scale
- Missed alerts lead to outages
- Reactive fixes damage trust

Acronis M365 Security Posture Management:

- Continuously monitors site storage usage
- Detects threshold breaches early
- Flags deviations from defined baselines
- Provides consistent alerting across tenants
- Helps MSPs stay proactive instead of reactive

This ensures capacity risks are identified before users are impacted.

MSP operational benefits

For Junior Technicians

- Clear signal: Storage threshold exceeded = action required
- No need to manually check site usage
- Alerts guide prioritization
- Fewer emergency tickets

For Senior Administrators

- Predictable capacity management
- Reduced firefighting
- Better planning for growth
- Stronger operational maturity

For Customers

- Fewer service disruptions
- Predictable SharePoint availability
- Better planning for storage growth
- Higher confidence in MSP oversight

Note

Key takeaway:

- Storage issues are predictable if you monitor them.
- Threshold alerts turn capacity problems into planned actions.
- Acronis helps MSPs stay ahead of SharePoint storage risks.

User risks

What are User Security Risks in Microsoft 365

User security risks represent identity-level weaknesses in a Microsoft 365 tenant that attackers commonly exploit to gain or retain access.

These risks are typically related to:

- Weak or missing authentication
- Unused or forgotten accounts
- Over-privileged users
- Improper mailbox usage
- Uncontrolled guest access

Note

These risks often exist silently and are frequently missed in MSP-managed environments.

Why Microsoft highlights these risks

Microsoft highlights user risks to:

- Reduce identity attack surface
- Prevent account takeover
- Limit blast of compromised identities
- Support Zero Trust identity principles
- Improve tenant-wide security hygiene

Most Microsoft 365 breaches start with identity abuse, not malware.

Key user risks and why they matter

Key user risk	What it means	Why this is dangerous	Impact	Remediation
MFA is disabled or user not	The account can authenticate using password only.	• Passwords are phishable • Credential	• High likelihood of account takeover	• Enable MFA for the user immediately

Key user risk	What it means	Why this is dangerous	Impact	Remediation
enrolled		stuffing attacks succeed • MFA-bypass is not required — MFA simply isn't there	• Admin accounts are especially critical	
Dormant accounts	User accounts that have not signed in for a long time but remain active.	• Often forgotten • Passwords may be weak or reused • Rarely monitored	• Silent compromise • Long-term persistence	• Block sign-in • Automatically sign out active sessions
Dormant admin accounts	Privileged accounts that are inactive but still hold admin roles.	• High-value target • Rarely monitored • Often excluded from daily checks	• Full tenant compromise • Security controls can be disabled	• Block sign-in • Force sign-out of all sessions
Admin mailboxes	Administrative privileges are tied to licensed mailboxes.	• Admin credentials exposed via email attacks • Phishing targets admins directly • Violates least-privilege best practices	• Admin compromise via mailbox attacks • Increased blast radius	• Remove admin privileges from mailbox user • Create a separate, unlicensed admin account • Enforce one-time passwords and audit trail
Anonymous admins	Admin accounts without clear ownership or traceability.	• No accountability • Hard to audit • Often legacy or abandoned accounts	• Unauthorized access • Compliance failure	• Delete anonymous administrator accounts
Shared mailboxes used as users	User accounts misused where shared mailboxes should be used.	• Shared credentials • No individual accountability • MFA often bypassed or	• Credential sharing • Investigation difficulty	• Convert user account to shared mailbox • Delegate access properly (Send As / Full Access)

Key user risk	What it means	Why this is dangerous	Impact	Remediation
		impossible		
Dormant guest accounts	External users with access that is no longer required.	• External identities are outside your control • Often forgotten • Rarely monitored	• Data exposure • Compliance risk	• Delete dormant guest accounts

What happens when these risks are not addressed

- Identity attack surface grows
- Compromised accounts remain undetected
- Admin access paths are exposed
- Incident response becomes difficult
- Compliance posture degrades

Note

Most identity breaches succeed because basic hygiene was missing.

Real risks for an MSP

Security risk

- Silent account takeover
- Privilege escalation
- Long-term persistence by attackers

Compliance & audit risk

If a client asks: "Why did this account still exist and have access?"

If risks were ignored: The answer is uncomfortable.

MSP liability risk

- Poor identity hygiene is hard to defend
- Breaches damage trust and reputation
- MSP security maturity may be questioned

Severity summary

Area	Impact
Identity hygiene	Weak if unmanaged
Account takeover risk	High
Privileged access risk	Critical
Incident response	Severely limited
Compliance posture	At risk
MSP accountability	High risk

MSP operational benefits

For Junior Technicians

- Clear actions: Risk detected → Remediation
- No need to decide what to do manually
- Reduced chance of mistakes
- Faster response

For Senior Administrators

- Consistent identity governance
- Reduced attack surface
- Easier audits and reporting
- Stronger Zero Trust alignment

For Customers

- Fewer compromised accounts
- Better protection of identities
- Cleaner tenant environment
- Higher confidence in MSP security operations

Note

Key takeaway:

- Identity risks don’t fix themselves.
- Dormant, weak, or over-privileged accounts are silent threats.
- Acronis ensures identity hygiene is enforced continuously and automatically.