REVIEW BEFORE YOU ACT

M365 Admin Quick-Check Pack

10 read-only checks every Microsoft 365 admin should review before making tenant changes.

SecureOps Playbooks
secureopsplaybooks.com

Version 1.0 | Example content — validate in your own environment before production use

How to use this pack

This pack is a repeatable first review for a Microsoft 365 tenant: the checks worth running before bigger changes, policy work, cleanup projects, or a security review. It is a starting point for visibility and documentation, not a compliance framework and not a substitute for judgment.

THE WORKFLOW

- Run the checks. Every check in this pack is read-only: connect, collect, export. Nothing here changes the tenant.
- Save the exports. CSV output attaches cleanly to a ticket, change record, or handoff document.
- Write down what looks expected — and what needs an owner to explain it.
- Only then plan the change. Walk into the change window with notes instead of assumptions.

WHO IT IS FOR

Microsoft 365 admins, MSP engineers, cloud engineers, help desk techs growing into tenant work, and consultants who need a repeatable first review of an unfamiliar or inherited tenant.

IMPORTANT LABELS

- Example content. The checks and scripts are starter examples. Review permissions, output, and limitations before using them in any production tenant.
- Validate first. Test in a lab or test tenant before adding anything to a production change process.
- Administrator responsibility. You remain responsible for permissions, scope, change control, and interpretation of results.
- Not compliance proof. Completing these checks does not prove compliance with any framework or standard.

CONVENTIONS

Each check lists what it tells you, why it belongs in a first review, where to look (admin portal path and a PowerShell starting point), and what the check does not prove. Portal paths reflect the Microsoft admin centers as of mid-2026 and may shift as Microsoft updates its portals — the underlying checks stay the same.

The 10-check list

Use this page as the running checklist. Date and initial each check as you complete it, and keep the exports together with these notes.

- [ ] **1. Tenant summary** Date: _____ By: _____
- [ ] **2. Licensed users** Date: _____ By: _____
- [ ] **3. MFA / authentication method registration** Date: _____ By: _____
- [ ] **4. Privileged role assignments** Date: _____ By: _____
- [ ] **5. Guest users** Date: _____ By: _____
- [ ] **6. External mailbox forwarding** Date: _____ By: _____
- [ ] **7. Conditional Access policy inventory** Date: _____ By: _____
- [ ] **8. Expiring Entra app credentials** Date: _____ By: _____
- [ ] **9. Accepted domains / verification status** Date: _____ By: _____
- [ ] **10. SharePoint external sharing settings** Date: _____ By: _____

Reminder: an export is the start of a review, not the end of one. Every finding needs context from the people who own the environment.

CHECK 1 OF 10

Check 1: Tenant summary

WHAT IT TELLS YOU

The basics of the tenant you are about to work in: organization details, verified domains, technical contacts, and high-level directory counts. It anchors every other check to the right tenant.

WHY IT BELONGS IN A FIRST REVIEW

Working from memory — or worse, from the wrong tenant — is how avoidable mistakes happen. A two-minute summary confirms you are where you think you are and gives your notes a header.

WHERE TO LOOK — PORTAL

Microsoft 365 admin center > Settings > Org settings, and Microsoft Entra admin center > Overview.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
Connect-MgGraph -Scopes "Organization.Read.All"
Get-MgOrganization | Select-Object DisplayName, Id, VerifiedDomains
```

WHAT IT DOES NOT PROVE

A summary does not tell you how the tenant is configured or protected. It is orientation, not assessment.

NOTES

CHECK 2 OF 10

Check 2: Licensed users

WHAT IT TELLS YOU

Which licenses the tenant owns, how many are assigned, and which accounts hold them. Useful for cleanup planning, cost questions, and spotting accounts that should not be licensed.

WHY IT BELONGS IN A FIRST REVIEW

License assignments accumulate: departed users, test accounts, duplicate assignments. Before a licensing change or renewal conversation, a current export beats the last spreadsheet someone made.

WHERE TO LOOK — PORTAL

Microsoft 365 admin center > Billing > Licenses, and Users > Active users (filter by license).

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
Connect-MgGraph -Scopes "User.Read.All","Organization.Read.All"
Get-MgSubscribedSku | Select-Object SkuPartNumber, ConsumedUnits, `
  @{n='Total';e={$_.PrepaidUnits.Enabled}}
```

WHAT IT DOES NOT PROVE

License presence does not prove the license is used, needed, or correctly scoped. Usage review is a separate step.

NOTES

CHECK 3 OF 10

Check 3: MFA / authentication method…

WHAT IT TELLS YOU

Which users have authentication methods registered — a registration inventory that shows who appears prepared to satisfy stronger sign-in requirements before policy work begins.

WHY IT BELONGS IN A FIRST REVIEW

MFA policy and MFA registration are related but not the same. Registration coverage can be uneven even in tenants where MFA is 'handled.' A reviewable list beats assumptions.

WHERE TO LOOK — PORTAL

Microsoft Entra admin center > Protection > Authentication methods > User registration details.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

Full starter script in the appendix (Script A).

WHAT IT DOES NOT PROVE

Registration does not prove MFA is enforced, required, or successfully used. It does not replace Conditional Access review, sign-in log review, or per-user MFA review. Full playbook: secureopsplaybooks.com/guides/audit-mfa-registration

NOTES

CHECK 4 OF 10

Check 4: Privileged role assignments

WHAT IT TELLS YOU

Which users, groups, and service principals hold active Entra directory roles. Privileged access changes how you read every other finding in the tenant.

WHY IT BELONGS IN A FIRST REVIEW

Roles grow over time and are rarely documented. Before Conditional Access, authentication, or admin workflow changes, you need to know who could be affected — and who should not have access at all.

WHERE TO LOOK — PORTAL

Microsoft Entra admin center > Identity > Roles & administrators.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

Full starter script in the appendix (Script B).

WHAT IT DOES NOT PROVE

An active-role export may not show PIM eligible assignments, activation schedules, or access packages. It is a first visibility check, not a complete privileged access review. Full playbook: secureopsplaybooks.com/guides/privileged-role-assignments

NOTES

CHECK 5 OF 10

Check 5: Guest users

WHAT IT TELLS YOU

Every external (guest) identity in the directory: who they are, when they were created, and which still look active or expected.

WHY IT BELONGS IN A FIRST REVIEW

Guests accumulate through Teams shares, project invitations, and one-off collaborations. Stale or unrecognized guests are common in inherited tenants and belong in any access review.

WHERE TO LOOK — PORTAL

Microsoft Entra admin center > Identity > Users > All users, filtered to User type: Guest.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
Connect-MgGraph -Scopes "User.Read.All"
Get-MgUser -All -Filter "userType eq 'Guest'" `
  -Property displayName,mail,createdDateTime,accountEnabled |
  Select-Object DisplayName, Mail, CreatedDateTime, AccountEnabled |
  Export-Csv .\guest-user-review.csv -NoTypeInformation
```

WHAT IT DOES NOT PROVE

A guest list does not show what each guest can access. Sharing links, group membership, and app assignments need separate review.

NOTES

CHECK 6 OF 10

Check 6: External mailbox forwarding

WHAT IT TELLS YOU

Mailboxes with forwarding configured at the mailbox level — including forwarding that may send business mail outside the organization.

WHY IT BELONGS IN A FIRST REVIEW

Forwarding can support a real workflow, reflect an old process, or point to something that needs a deeper look. It affects where business mail goes and who can see it.

WHERE TO LOOK — PORTAL

Exchange admin center > Recipients > Mailboxes (check Mail flow settings per mailbox).

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

Full starter script in the appendix (Script C).

WHAT IT DOES NOT PROVE

This checks mailbox-level forwarding only. Inbox rules, mail flow rules, connectors, and OAuth app access are separate follow-up checks. Finding forwarding does not prove it is malicious — it proves it needs an owner and a reason. Full playbook: secureopsplaybooks.com/guides/external-mailbox-forwarding

NOTES

CHECK 7 OF 10

Check 7: Conditional Access policy inventory

WHAT IT TELLS YOU

Every Conditional Access policy in the tenant: name, state (on, off, report-only), and when each was created and last modified.

WHY IT BELONGS IN A FIRST REVIEW

CA policies interact. Before touching authentication, device, or location requirements, capture the current policy set so you can reason about — and roll back to — a known state.

WHERE TO LOOK — PORTAL

Microsoft Entra admin center > Protection > Conditional Access > Policies.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
Connect-MgGraph -Scopes "Policy.Read.All"
Get-MgIdentityConditionalAccessPolicy |
  Select-Object DisplayName, State, CreatedDateTime, ModifiedDateTime |
  Export-Csv .\ca-policy-inventory.csv -NoTypeInformation
```

WHAT IT DOES NOT PROVE

A policy list does not prove the policies work as intended, cover everyone, or have safe exclusions. Policy-by-policy review and sign-in log validation are separate steps.

NOTES

CHECK 8 OF 10

Check 8: Expiring Entra app credentials

WHAT IT TELLS YOU

App registrations whose client secrets or certificates are expiring or already expired. These are the credentials that break integrations at the worst possible time.

WHY IT BELONGS IN A FIRST REVIEW

Expired app secrets cause sudden, hard-to-diagnose outages in automation and third-party integrations. Knowing what expires in the next 60-90 days turns an outage into a calendar entry.

WHERE TO LOOK — PORTAL

Microsoft Entra admin center > Identity > Applications > App registrations (Certificates & secrets per app).

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
Connect-MgGraph -Scopes "Application.Read.All"
Get-MgApplication -All -Property displayName,passwordCredentials,keyCredentials |
  ForEach-Object { $app = $_
    foreach ($cred in @($_.PasswordCredentials) + @($_.KeyCredentials)) {
      [pscustomobject]@{ App = $app.DisplayName; EndDate = $cred.EndDateTime }
    }
  } |
  Sort-Object EndDate |
  Export-Csv .\app-credential-review.csv -NoTypeInformation
```

WHAT IT DOES NOT PROVE

Credential dates do not tell you whether an app is still needed, who owns it, or what permissions it holds. Ownership and consent review are separate checks.

NOTES

CHECK 9 OF 10

Check 9: Accepted domains / verification…

WHAT IT TELLS YOU

Which domains the tenant accepts mail for, how each is configured (authoritative or relay), and which domain is the default.

WHY IT BELONGS IN A FIRST REVIEW

Domain configuration mistakes affect mail flow for everyone. Before mail routing, migration, or DNS work, confirm the domain list matches what the business actually uses.

WHERE TO LOOK — PORTAL

Microsoft 365 admin center > Settings > Domains, and Exchange admin center > Mail flow > Accepted domains.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
Connect-ExchangeOnline
Get-AcceptedDomain |
  Select-Object DomainName, DomainType, Default |
  Export-Csv .\accepted-domains.csv -NoTypeInformation
```

WHAT IT DOES NOT PROVE

Domain presence does not prove SPF, DKIM, and DMARC are correct. Email authentication review is a separate (and important) check.

NOTES

CHECK 10 OF 10

Check 10: SharePoint external sharing…

WHAT IT TELLS YOU

The tenant-level external sharing posture for SharePoint and OneDrive: who can share what with people outside the organization.

WHY IT BELONGS IN A FIRST REVIEW

Sharing settings are often set once and forgotten. Before collaboration, governance, or DLP work, know the current posture — it frames every conversation about external access.

WHERE TO LOOK — PORTAL

SharePoint admin center > Policies > Sharing.

WHERE TO LOOK — POWERSHELL (READ-ONLY STARTING POINT)

```
# Requires the SharePoint Online Management Shell module
Connect-SPOService -Url https://YOURTENANT-admin.sharepoint.com
Get-SPOTenant |
  Select-Object SharingCapability, DefaultSharingLinkType,
    RequireAnonymousLinksExpireInDays
```

WHAT IT DOES NOT PROVE

Tenant settings do not show per-site overrides or what has already been shared. Site-level review and sharing reports are separate steps.

NOTES

STARTER SCRIPTS APPENDIX

Script A — MFA registration review

Review the scopes, permissions, and output in a test or lab environment before using this in a production change process. The full playbook — expected output, false positives, troubleshooting, and limitations — is at:

secureopsplaybooks.com/guides/audit-mfa-registration

```
# SecureOps Playbooks | secureopsplaybooks.com
# Read-only example: MFA registration review. Validate in a lab first.

Connect-MgGraph -Scopes "User.Read.All","UserAuthenticationMethod.Read.All"

$users = Get-MgUser -All -Property "id,displayName,userPrincipalName,accountEnabled"
$rows = foreach ($user in $users) {
  $methods = Get-MgUserAuthenticationMethod -UserId $user.Id
  $methodTypes = @($methods | ForEach-Object { $_.AdditionalProperties["@odata.type"] })
  $reviewNote = if ($methodTypes.Count -eq 0) {
    "No registered authentication methods returned by this Graph check."
  } else {
    "Registered methods found; this does not prove MFA enforcement or coverage."
  }

  [pscustomobject]@{
    DisplayName = $user.DisplayName
    UserPrincipalName = $user.UserPrincipalName
    AccountEnabled = $user.AccountEnabled
    RegisteredMethodCount = $methodTypes.Count
    RegisteredMethodTypes = ($methodTypes -join ";")
    ReviewNote = $reviewNote
  }
}

$rows |
  Sort-Object UserPrincipalName |
  Export-Csv ".\mfa-registration-review.csv" -NoTypeInformation
```

STARTER SCRIPTS APPENDIX

Script B — Privileged role assignment review

Review the scopes, permissions, and output in a test or lab environment before using this in a production change process. The full playbook — expected output, false positives, troubleshooting, and limitations — is at:

secureopsplaybooks.com/guides/privileged-role-assignments

```
# SecureOps Playbooks | secureopsplaybooks.com
# Read-only example: privileged role review. Validate in a lab first.

Connect-MgGraph -Scopes "RoleManagement.Read.Directory","Directory.Read.All"

$roles = Get-MgDirectoryRole -All
$rows = foreach ($role in $roles) {
  $members = Get-MgDirectoryRoleMember -DirectoryRoleId $role.Id -All

  foreach ($member in $members) {
    [pscustomobject]@{
      RoleName = $role.DisplayName
      RoleId = $role.Id
      MemberId = $member.Id
      MemberType = $member.AdditionalProperties["@odata.type"]
      DisplayName = $member.AdditionalProperties["displayName"]
      UserPrincipalName = $member.AdditionalProperties["userPrincipalName"]
      AppId = $member.AdditionalProperties["appId"]
      ReviewNote = "Active role member; confirm whether PIM needs separate review."
    }
  }
}

$rows |
  Sort-Object RoleName, DisplayName |
  Export-Csv ".\entra-privileged-role-review.csv" -NoTypeInformation
```

Script C — External mailbox forwarding…

Review the scopes, permissions, and output in a test or lab environment before using this in a production change process. The full playbook — expected output, false positives, troubleshooting, and limitations — is at:

secureopsplaybooks.com/guides/external-mailbox-forwarding

```
# SecureOps Playbooks | secureopsplaybooks.com
# Read-only example: forwarding review. Validate in a lab first.

Connect-ExchangeOnline

$forwardingProperties = @(
  "DisplayName",
  "UserPrincipalName",
  "PrimarySmtpAddress",
  "ForwardingSmtpAddress",
  "ForwardingAddress",
  "DeliverToMailboxAndForward"
)

$mailboxes = Get-EXOMailbox -ResultSize Unlimited -Properties $forwardingProperties

$forwardingReview = $mailboxes |
  Where-Object {
    $_.ForwardingSmtpAddress -or
    $_.ForwardingAddress -or
    $_.DeliverToMailboxAndForward
  } |
  Select-Object DisplayName,
    UserPrincipalName,
    PrimarySmtpAddress,
    ForwardingSmtpAddress,
    ForwardingAddress,
    DeliverToMailboxAndForward

$forwardingReview |
  Sort-Object UserPrincipalName |
  Export-Csv ".\mailbox-forwarding-review.csv" -NoTypeInformation
```

After the review

TURN THE EXPORTS INTO DECISIONS

- Group findings into: expected and documented, expected but undocumented, and needs an owner to explain.
- Attach the exports and this checklist to the ticket or change record that prompted the review.
- Schedule follow-ups for anything that needs a deeper check (PIM review, sign-in logs, sharing reports, email authentication).
- Re-run the pack after major changes, before audits, and when inheriting a tenant.

GO DEEPER

- Full playbooks with expected output, false positives, and limitations: secureopsplaybooks.com/guides
- Field notes on admin workflows: secureopsplaybooks.com/notes
- New playbooks and updates by email: secureopsplaybooks.com/dispatch
- RSS: secureopsplaybooks.com/feed.xml

FREE COMPANION TOOL: SECUREOPS SCRIPT LIBRARY LITE

Prefer these checks in a desktop app? SecureOps Script Library LITE is a free Windows app with 15 read-only reporting scripts — tenant summary, MFA status, admin roles, guest users, external forwarding, mailbox sizes, and more — with tenant profiles, quick-fill variables, and a preflight module checker. It is the free edition of the full 117-script SecureOps Script Library. Download it at secureopsplaybooks.com/script-library.

FEEDBACK AND CORRECTIONS

If a check, permission note, or explanation in this pack looks wrong, email hello@secureopsplaybooks.com with the page and what you observed. Corrections are welcome and taken seriously.