SAS PEREZ

Prioritized remediation plan

Generated on 13/08/2026 09:17 — 63 action(s)

Audited tenant : Test Tenant 1
m365expertise.com
Referentials : Entra ID

P1 : 22 · P2 : 21 · P3 : 20

P1 · ENTRA · L1 · Non-compliant · 7 obj.
ENTRA-WKL-002
Limit application credential lifetimes
Remediation : Reissue the affected credentials with a maximum validity of 12–24 months and enforce rotation with an app management policy.
```
PS> Get-MgApplication -All -Property DisplayName,PasswordCredentials | ForEach-Object { $_.PasswordCredentials | Where-Object { ($_.EndDateTime - $_.StartDateTime).TotalDays -gt 730 } }
```

P1 · ENTRA · L1 · Non-compliant · 2 obj.
ENTRA-WKL-008
Prohibit the OAuth implicit flow on applications
Remediation : Disable implicit access-token issuance on each application (manifest: web.implicitGrantSettings) and migrate clients to the code flow with PKCE.
```
PS> Get-MgApplication -All -Property DisplayName,Web | Where-Object
{ $_.Web.ImplicitGrantSettings.EnableAccessTokenIssuance }
```

P1 · ENTRA · L1 · Non-compliant
ENTRA-ADV-004
Enable Microsoft Authenticator context protections
Remediation : In the Microsoft Authenticator configuration, enable application context and geographic location display for all users.
```
PS> Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId MicrosoftAuthenticator
```

P1 · ENTRA · L1 · Non-compliant
ENTRA-ADV-010
Block the device code flow
Remediation : Create a Conditional Access policy targeting the Device code authentication flow (Conditions > Authentication flows) with Block, excluding only legitimate scenarios.
```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object { $_.Conditions.AuthenticationFlows.TransferMethods -match 'deviceCodeFlow' }
```

P1 · ENTRA · L1 · Non-compliant
ENTRA-ADV-014
Protect Microsoft admin portals with Conditional Access
Remediation : Create a Conditional Access policy on the Microsoft Admin Portals application requiring at least strong MFA, ideally a compliant device.
```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object { $_.Conditions.Applications.IncludeApplications -contains 'MicrosoftAdminPortals' }
```

P1 · ENTRA · L1 · Non-compliant
ENTRA-002
Require MFA for all administrator roles
Remediation : Conditional Access: create a policy targeting directory roles (Global Admin, etc.) with the "Require multi-factor authentication" grant.
```
PS> New-MgIdentityConditionalAccessPolicy -BodyParameter @{ DisplayName='MFA - Administrateurs';
State='enabledForReportingButNotEnforced';
Conditions=@{ Users=@{ IncludeRoles=@('62e90394-69f5-4237-9190-012177145e10') };
Applications=@{ IncludeApplications=@('All') } }; GrantControls=@{ Operator='OR'; BuiltInControls=@('mfa') } }
```

P1 · ENTRA · L1 · Non-compliant
ENTRA-003
Require MFA for all users
Remediation : Conditional Access: a policy targeting all users (with break-glass exclusions) requiring MFA, ideally via a phishing-resistant authentication strength.
```
PS> New-MgIdentityConditionalAccessPolicy -BodyParameter @{ DisplayName='MFA - Tous les utilisateurs';
State='enabledForReportingButNotEnforced'; Conditions=@{ Users=@{ IncludeUsers=@('All'); ExcludeUsers=@('<id-compte-urgence>') }; Applications=@{ IncludeApplications=@('All') } }; GrantControls=@{ Operator='OR';
BuiltInControls=@('mfa') } }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-006

Disable weak authentication methods

Remediation : Protection > Authentication methods: disable SMS and Voice call, and favor Microsoft Authenticator, FIDO2 and Windows Hello.

```
PS> Update-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId
'Sms' -BodyParameter @{ State='disabled' }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-001

Enable security defaults or equivalent Conditional Access policies

Remediation : Enable Security Defaults (Properties > Manage security defaults), or deploy Conditional Access policies covering MFA and blocking legacy authentication.

```
PS> Update-MgPolicyIdentitySecurityDefaultEnforcementPolicy -IsEnabled:$true
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-012

Provide break-glass emergency access accounts

Remediation : Create two cloud-only emergency accounts excluded from Conditional Access policies, with dedicated monitoring and alerts.

P1 · ENTRA · L1 · Non-compliant

ENTRA-014

Prevent non-administrator users from creating tenants

Remediation : Entra portal > Users > User settings > Tenant settings: set "Users can create tenants" to No.

```
PS> Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions @{ AllowedToCreateTenants = $false }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-015

Restrict user consent to applications

Remediation : Enterprise applications > Consent and permissions: set user consent to "Do not allow" or limit it to verified publishers and low-impact permissions.

```
PS> Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions @{ PermissionGrantPoliciesAssigned =
@('managePermissionGrantsForSelf.microsoft-user-default-low') }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-023

Configure Entra protection against weak passwords

Remediation : Protection > Authentication methods > Password protection: enable protection and a custom banned-password list.

P1 · ENTRA · L1 · Non-compliant

ENTRA-024

Extend password protection to on-premises AD

Remediation : Deploy the Entra password protection agents on the domain controllers and set the on-premises mode to "Enforced".

P1 · ENTRA · L1 · Non-compliant

ENTRA-026

Block legacy authentication

Remediation : Conditional Access: create a policy targeting legacy authentication clients (Exchange ActiveSync and others) with the "Block" grant.

```
PS> New-MgIdentityConditionalAccessPolicy -BodyParameter @{ DisplayName='Bloquer authentification héritée';
State='enabledForReportingButNotEnforced'; Conditions=@{ Users=@{ IncludeUsers=@('All') };
Applications=@{ IncludeApplications=@('All') }; ClientAppTypes=@('exchangeActiveSync','other') };
GrantControls=@{ Operator='OR'; BuiltInControls=@('block') } }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-027

Require MFA for access to Microsoft Azure Management

Remediation : Conditional Access: a policy targeting the "Microsoft Azure Management" app requiring MFA.

```
PS> New-MgIdentityConditionalAccessPolicy -BodyParameter @{ DisplayName='MFA - Azure Management';
State='enabledForReportingButNotEnforced'; Conditions=@{ Users=@{ IncludeUsers=@('All') };
Applications=@{ IncludeApplications=@('797f4846-ba00-4fd7-ba43-dac1f8f63013') } }; GrantControls=@{ Operator='OR';
BuiltInControls=@('mfa') } }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-037

Require MFA for device join and registration

Remediation : Conditional Access: create a policy on the "Register or join devices" user action requiring MFA.

P1 · ENTRA · L1 · Non-compliant

ENTRA-042

Restrict default user permissions

Remediation : Users > User settings: harden the default user role (creating apps, groups, tenants, reading other users).

```
PS> Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions @{ AllowedToCreateApps=$false;
AllowedToCreateSecurityGroups=$false; AllowedToCreateTenants=$false; AllowedToReadOtherUsers=$true }
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-051

Require MFA for external and guest users

Remediation : Conditional Access: create a policy targeting guest/external users with the "Require MFA" grant.

P1 · ENTRA · L1 · Non-compliant

ENTRA-052

Cover all cloud applications with Conditional Access

Remediation : Conditional Access: have at least one baseline policy targeting "All cloud apps" (with controlled exclusions).

P1 · ENTRA · L1 · Non-compliant

ENTRA-080

Move conditional access policies out of report-only mode

Remediation : Entra portal > Protection > Conditional Access: switch validated policies from Report-only to On.

```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object State -eq 'enabledForReportingButNotEnforced'
```

P1 · ENTRA · L1 · Non-compliant

ENTRA-082

Block the device code authentication flow

Remediation : Entra portal > Conditional Access: create a policy targeting device code authentication flows with the Block grant.

```
PS> Get-MgIdentityConditionalAccessPolicy | Select-Object DisplayName,Conditions
```

P2 · ENTRA · L2 · Non-compliant · 7 obj.

ENTRA-039

Prefer certificates over secrets for applications and service principals

Remediation : Inventory app registrations using a client secret and migrate them to certificate authentication; then remove the secrets.

```
PS> Get-MgApplication -All | Where-Object { $_.PasswordCredentials.Count -gt 0 } | Select-Object DisplayName, AppId
```

P2 · ENTRA · L2 · Non-compliant · 6 obj.

ENTRA-WKL-004

Identify ownerless applications

Remediation : Assign at least one owner to every application, or delete orphaned applications that are no longer needed.

```
PS> Get-MgApplication -All -ExpandProperty Owners | Where-Object { -not $_.Owners }
```

P2 · ENTRA · L2 · Non-compliant · 6 obj.

ENTRA-056

Ensure applications have an owner

Remediation : App registrations > (application) > Owners: assign at least one owner to orphaned applications.

```
PS> Get-MgApplication -All | Where-Object { (Get-MgApplicationOwner -ApplicationId $_.Id).Count -eq 0 } | Select-
Object DisplayName, AppId
```

P2 · ENTRA · L2 · Non-compliant

ENTRA-ADV-005

Require authentication strengths in Conditional Access

Remediation : Replace 'require MFA' with an authentication strength (at minimum on administrator roles) in your Conditional Access policies.

```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object { $_.GrantControls.AuthenticationStrength }
```

P2 · ENTRA · L2 · Non-compliant

ENTRA-ADV-013

Cover all users with risk-based policies

Remediation : Extend risk-based Conditional Access policies (sign-in and user risk) to all users, with break-glass exclusions only.

```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object { $_.Conditions.SignInRiskLevels -or
$_.Conditions.UserRiskLevels }
```

P2 · ENTRA · L2 · Non-compliant

ENTRA-008

Use authentication strengths for sensitive access

Remediation : Conditional Access: apply an authentication strength (e.g. phishing-resistant) to administrators and critical applications.

P2 · ENTRA · L2 · Non-compliant
ENTRA-009
Protect security method registration
Remediation : Conditional Access: a policy on the "Register security information" user action (trusted location, prior MFA or Identity Protection).

P2 · ENTRA · L2 · Non-compliant
ENTRA-028
Configure sign-in frequency and non-persistent sessions for administrators
Remediation : Conditional Access: for administrator roles, enable the "Sign-in frequency" and "Persistent browser session = never" session controls.

P2 · ENTRA · L2 · Non-compliant
ENTRA-029
Require compliant or hybrid-joined devices
Remediation : Conditional Access: require the "Compliant device" or "Hybrid Entra joined" grant for access to sensitive resources.

P2 · ENTRA · L2 · Non-compliant
ENTRA-031
Require MFA for risky sign-ins
Remediation : Conditional Access + Identity Protection: a sign-in-risk-based policy requiring MFA when risk is medium or high.

P2 · ENTRA · L2 · Non-compliant
ENTRA-032
Require remediation for high-risk users
Remediation : Conditional Access + Identity Protection: a user-risk-based policy requiring MFA and password change.

P2 · ENTRA · L2 · Non-compliant
ENTRA-034
Set up periodic access reviews
Remediation : Identity Governance > Access reviews: create recurring reviews on sensitive groups, roles and applications.

P2 · ENTRA · L2 · Non-compliant
ENTRA-040
Restrict device platforms via Conditional Access
Remediation : Conditional Access: set the "Device platforms" condition to allow only supported platforms.

P2 · ENTRA · L2 · Non-compliant
ENTRA-036
Package access via entitlement management
Remediation : Identity Governance > Entitlement management: create access packages (catalogs, approvals, expiration) for controlled access grants.

P2 · ENTRA · L2 · Non-compliant
ENTRA-045
Restrict Microsoft 365 group creation
Remediation : Groups > General: restrict Microsoft 365 group creation to an authorized security group (EnableGroupCreation setting).

P2 · ENTRA · L2 · Non-compliant
ENTRA-046
Block directory access via MSOnline PowerShell
Remediation : Via Graph (authorizationPolicy): set blockMsolPowerShell to true to prohibit the legacy MSOnline module.
```
PS> Update-MgPolicyAuthorizationPolicy -BlockMsolPowerShell:$true
```

P2 · ENTRA · L2 · Non-compliant
ENTRA-047
Disable email-based self-service subscriptions
Remediation : Disable self-service subscriptions (Set-MsolCompanySettings -AllowAdHocSubscriptions $false).
```
PS> Update-MgPolicyAuthorizationPolicy -AllowedToSignUpEmailBasedSubscriptions:$false
```

P2 · ENTRA · L2 · Non-compliant
ENTRA-053
Restrict access by location via Conditional Access
Remediation : Define named locations (Protection > Named locations) then a location-based Conditional Access policy.

P2 · ENTRA · L2 · Non-compliant
ENTRA-054

Require an approved app or an app protection policy
Remediation : Conditional Access: add the "Require approved client app" or "Require app protection policy" grant for mobile access.

P2 · ENTRA · L2 · Non-compliant
ENTRA-055
Enable app-enforced session restrictions
Remediation : Conditional Access: enable "App enforced restrictions" or the Defender for Cloud Apps integration in session controls.

P2 · ENTRA · L2 · Non-compliant
ENTRA-079
Remove disabled conditional access policies
Remediation : Entra portal > Protection > Conditional Access: delete disabled policies or document them explicitly.
```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object State -eq 'disabled'
```

P3 · ENTRA · L2 · Warning · 489 obj.
ENTRA-WKL-006
Identify service principals with no sign-in activity
Remediation : Review principals inactive for more than 90 days; disable then delete those no longer needed.
```
PS> Get-MgBetaReportServicePrincipalSignInActivity -All | Where-Object LastSignInActivity.LastSignInDateTime -lt
(Get-Date).AddDays(-90)
```

P3 · ENTRA · L1 · Warning · 9 obj.
ENTRA-085
Audit privileged roles assigned to service principals
Remediation : Entra portal > Roles and administrators: inventory service principals holding a role and remove those not justified.
```
PS> Get-MgRoleManagementDirectoryRoleAssignment -ExpandProperty Principal
```

P3 · ENTRA · L2 · Warning · 2 obj.
ENTRA-PIM-013
Enforce separate admin accounts
Remediation : Create dedicated admin accounts without a mail licence.
```
PS> Get-MgUser -Property assignedPlans | Where-Object { $_.AssignedPlans.Service -contains 'exchange' }
```

P3 · ENTRA · L2 · Warning · 1 obj.
ENTRA-WKL-007
Identify service principals carrying their own credentials
Remediation : Move credentials to the app registration, or document and rotate legitimate exceptions.
```
PS> Get-MgServicePrincipal -All -Property DisplayName,ServicePrincipalType,PasswordCredentials,KeyCredentials |
Where-Object { $_.ServicePrincipalType -eq 'Application' -and ($_.PasswordCredentials -or $_.KeyCredentials) }
```

P3 · ENTRA · L2 · Warning · 1 obj.
ENTRA-071
Audit high-permission service principals with active credentials
Remediation : Review service principals with secrets; prefer certificates and remove unnecessary permissions.
```
PS> Get-MgServicePrincipal -All -Property displayName,passwordCredentials | ? { $_.PasswordCredentials }
```

P3 · ENTRA · L2 · Warning
ENTRA-ADV-006
Harden the default cross-tenant access policy
Remediation : In External Identities > Cross-tenant access settings, restrict the defaults and create explicit partner configurations.
```
PS> Get-MgPolicyCrossTenantAccessPolicyDefault | Format-List B2bCollaborationInbound
```

P3 · ENTRA · L2 · Warning
ENTRA-ADV-011
Deploy token protection
Remediation : Add the 'Require token protection' session control to a Conditional Access policy covering supported platforms.
```
PS> Get-MgIdentityConditionalAccessPolicy | Where-Object { $_.SessionControls.SecureSignInSession.IsEnabled }
```

P3 · ENTRA · L1 · Warning
ENTRA-PIM-012
Validate break-glass accounts
Remediation : Create two cloud-only break-glass accounts, monitor their use, and exclude them from blocking CA.
```
PS> # Vérifier l'existence de 2 comptes GA cloud-only dédiés à l'urgence
```

P3 · ENTRA · L2 · Warning
ENTRA-WKL-003
Enforce an application credential management policy
Remediation : Enable the default app management policy and add passwordCredentials restrictions (ban or maximum lifetime).

```
PS> Get-MgPolicyDefaultAppManagementPolicy | Format-List IsEnabled,ApplicationRestrictions
```

P3 · ENTRA · L1 · Warning

ENTRA-020

Restrict guest user permissions

Remediation : Users > User settings > External collaboration settings: set guest access to "most restrictive".

```
PS> Update-MgPolicyAuthorizationPolicy -GuestUserRoleId '2af84b1e-32c8-42b7-82bc-daa82404023b'
```

P3 · ENTRA · L1 · Warning

ENTRA-021

Limit who can invite guest users

Remediation : External collaboration settings: limit sending invitations to administrators and delegated roles (not "everyone").

```
PS> Update-MgPolicyAuthorizationPolicy -AllowInvitesFrom 'adminsAndGuestInviters'
```

P3 · ENTRA · L2 · Warning

ENTRA-030

Enable continuous access evaluation (CAE)

Remediation : Conditional Access: keep continuous access evaluation enabled (default) and avoid disabling it in policies.

P3 · ENTRA · L2 · Warning

ENTRA-064

Prevent users from recovering BitLocker keys

Remediation : Entra > Devices > Settings: 'Restrict users from recovering BitLocker keys' = Yes.

```
PS> Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions @{ AllowedToReadBitlockerKeysForOwnedDevice =
$false }
```

P3 · ENTRA · L1 · Warning

ENTRA-066

Enable report suspicious activity

Remediation : Entra > Protection > Authentication methods > Settings: 'Report suspicious activity' = Enabled.

```
PS> # Entra > Protection > Authentication methods > Settings > Report suspicious activity = Enabled
```

P3 · ENTRA · L1 · Warning

ENTRA-058

Configure named locations

Remediation : Entra > Protection > Conditional Access > Named locations: define trusted IPs and countries.

```
PS> Get-MgIdentityConditionalAccessNamedLocation
```

P3 · ENTRA · L2 · Warning

ENTRA-049

Control self-service sign-up

Remediation : External collaboration settings / user flow: govern or disable self-service sign-up.

P3 · ENTRA · L2 · Warning

ENTRA-068

Restrict access to the Entra admin portal

Remediation : Entra > User settings: restrict access to the admin portal and harden default user permissions.

```
PS> Get-MgPolicyAuthorizationPolicy | Select-Object -ExpandProperty DefaultUserRolePermissions
```

P3 · ENTRA · L1 · Warning

ENTRA-069

Restrict B2B invitations to administrators

Remediation : Entra > External Identities > External collaboration settings: 'Restrict invitations to users with inviter roles'.

```
PS> Get-MgPolicyAuthorizationPolicy | Select-Object AllowInvitesFrom
```

P3 · ENTRA · L2 · Warning

ENTRA-083

Use restricted management administrative units

Remediation : Entra portal > Roles and administrators > Administrative units: create a restricted management unit for sensitive accounts.

```
PS> Get-MgBetaDirectoryAdministrativeUnit | Select-Object DisplayName,IsMemberManagementRestricted
```

P3 · ENTRA · L2 · Warning

ENTRA-084

Deploy certificate-based authentication

Remediation : Entra portal > Protection > Authentication methods: enable certificate-based authentication and target it at administrators.

```
PS> Get-MgBetaPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId
x509Certificate
```