Maester Test Results

Contoso (########-####-####-####-############)

6/26/20##, 7:00:16 AM

Test summary

Total tests

129

Passed

51

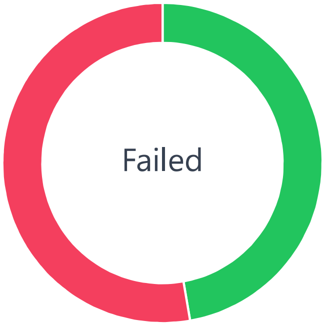
Failed

57

Not tested

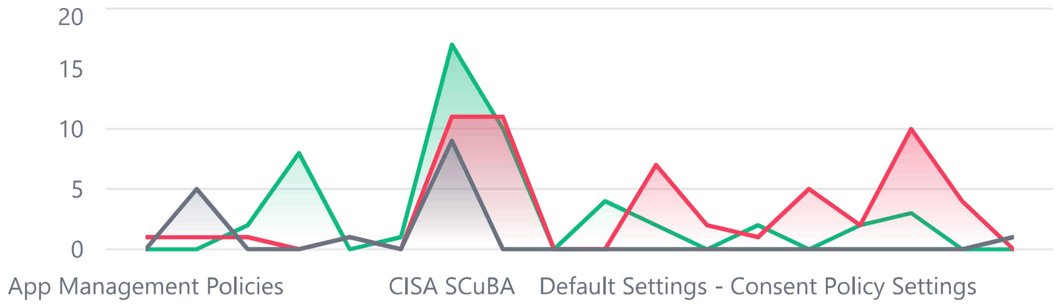
21

Test status



Passed	47%
Failed	53%

By category



Test details

Select category...

✓ Passe(× ⚠ Failed × Skipp(×

Test	Status	Info
EIDSCA.AF01: Authentication Method - FIDO2 security key - State.	⚠ Failed	
EIDSCA.AF02: Authentication Method - FIDO2 security key - Allow self-service set up.	Skipped	
EIDSCA.AF03: Authentication Method - FIDO2 security key - Enforce attestation.	Skipped	
EIDSCA.AF04: Authentication Method - FIDO2 security key - Enforce key restrictions.	Skipped	
EIDSCA.AF05: Authentication Method - FIDO2 security key - Restricted.	Skipped	
EIDSCA.AF06: Authentication Method - FIDO2 security key - Restrict specific keys.	Skipped	
EIDSCA.AG01: Authentication Method - General Settings - Manage migration.	✓ Passed	

Test	Status	Info
EIDSCA.AG02: Authentication Method - General Settings - Report suspicious activity - State.	⚠ Failed	□
EIDSCA.AG03: Authentication Method - General Settings - Report suspicious activity - Included users/groups.	✓ Passed	□
EIDSCA.AM01: Authentication Method - Microsoft Authenticator - State.	✓ Passed	□
EIDSCA.AM02: Authentication Method - Microsoft Authenticator - Allow use of Microsoft Authenticator OTP.	✓ Passed	□
EIDSCA.AM03: Authentication Method - Microsoft Authenticator - Require number matching for push notifications.	✓ Passed	□
EIDSCA.AM04: Authentication Method - Microsoft Authenticator - Included users/groups of number matching for push notifications.	✓ Passed	□
EIDSCA.AM06: Authentication Method - Microsoft Authenticator - Show application name in push and passwordless notifications.	✓ Passed	□
EIDSCA.AM07: Authentication Method - Microsoft Authenticator - Included users/groups to show application name in push and passwordless notifications.	✓ Passed	□
EIDSCA.AM09: Authentication Method - Microsoft Authenticator - Show geographic location in push and passwordless notifications.	✓ Passed	□
EIDSCA.AM10: Authentication Method - Microsoft Authenticator - Included users/groups to show geographic location in push and passwordless notifications.	✓ Passed	□
EIDSCA.AP01: Default Authorization Settings - Enabled Self service password reset for administrators.	⚠ Failed	□

Test	Status	Info
EIDSCA.AP04: Default Authorization Settings - Guest invite restrictions.	Failed	□
EIDSCA.AP05: Default Authorization Settings - Sign-up for email based subscription.	Failed	□
EIDSCA.AP06: Default Authorization Settings - User can join the tenant by email validation.	Failed	□
EIDSCA.AP07: Default Authorization Settings - Guest user access.	Failed	□
EIDSCA.AP08: Default Authorization Settings - User consent policy assigned for applications.	Failed	□
EIDSCA.AP09: Default Authorization Settings - Risk-based step-up consent.	Passed	□
EIDSCA.AP10: Default Authorization Settings - Default User Role Permissions - Allowed to create Apps.	Failed	□
EIDSCA.AP14: Default Authorization Settings - Default User Role Permissions - Allowed to read other users.	Passed	□
EIDSCA.AT01: Authentication Method - Temporary Access Pass - State.	Failed	□
EIDSCA.AT02: Authentication Method - Temporary Access Pass - One-time.	Skipped	□
EIDSCA.AV01: Authentication Method - Voice call - State.	Passed	□
EIDSCA.CP01: Default Settings - Consent Policy Settings - Group owner consent for apps accessing data.	Failed	□
EIDSCA.CP03: Default Settings - Consent Policy Settings - Block user consent for risky apps.	Passed	□

Test	Status	Info
EIDSCA.CP04: Default Settings - Consent Policy Settings - Users can request admin consent to apps they are unable to consent to.	✓ Passed	
EIDSCA.CR01: Consent Framework - Admin Consent Request - Policy to enable or disable admin consent request feature.	✓ Passed	
EIDSCA.CR02: Consent Framework - Admin Consent Request - Reviewers will receive email notifications for requests.	✓ Passed	
EIDSCA.CR03: Consent Framework - Admin Consent Request - Reviewers will receive email notifications when admin consent requests are about to expire.	✓ Passed	
EIDSCA.CR04: Consent Framework - Admin Consent Request - Consent request duration (days).	✓ Passed	
EIDSCA.PR01: Default Settings - Password Rule Settings - Password Protection - Mode.	⚠ Failed	
EIDSCA.PR02: Default Settings - Password Rule Settings - Password Protection - Enable password protection on Windows Server Active Directory.	⚠ Failed	
EIDSCA.PR03: Default Settings - Password Rule Settings - Enforce custom list.	⚠ Failed	
EIDSCA.PR05: Default Settings - Password Rule Settings - Smart Lockout - Lockout duration in seconds.	⚠ Failed	
EIDSCA.PR06: Default Settings - Password Rule Settings - Smart Lockout - Lockout threshold.	⚠ Failed	
EIDSCA.ST08: Default Settings - Classification and M365 Groups - M365 groups - Allow Guests to become Group Owner.	⚠ Failed	

Test	Status	Info
EIDSCA.ST09: Default Settings - Classification and M365 Groups - M365 groups - Allow Guests to have access to groups content.	⚠ Failed	□
MS.AAD.1.1: Legacy authentication SHALL be blocked.	✓ Passed	□
MS.AAD.2.1: Users detected as high risk SHALL be blocked.	✓ Passed	□
MS.AAD.2.2: A notification SHOULD be sent to the administrator when high-risk users are detected.	✓ Passed	□
MS.AAD.2.3: Sign-ins detected as high risk SHALL be blocked.	✓ Passed	□
MS.AAD.3.1: Phishing-resistant MFA SHALL be enforced for all users.	⚠ Failed	□
MS.AAD.3.2: If phishing-resistant MFA has not been enforced, an alternative MFA method SHALL be enforced for all users.	✓ Passed	□
MS.AAD.3.3: If phishing-resistant MFA has not been enforced and Microsoft Authenticator is enabled, it SHALL be configured to show login context information.	✓ Passed	□
MS.AAD.3.4: The Authentication Methods Manage Migration feature SHALL be set to Migration Complete.	✓ Passed	□
MS.AAD.3.5: The authentication methods SMS, Voice Call, and Email One-Time Passcode (OTP) SHALL be disabled.	⚠ Failed	□
MS.AAD.3.6: Phishing-resistant MFA SHALL be required for highly privileged roles.	⚠ Failed	□
MS.AAD.3.7: Managed devices SHOULD be required for authentication.	✓ Passed	□

Test	Status	Info
MS.AAD.3.8: Managed Devices SHOULD be required to register MFA.	⚠ Failed	□
MS.AAD.4.1: Security logs SHALL be sent to the agency's security operations center for monitoring.	Skipped	□
MS.AAD.5.1: Only administrators SHALL be allowed to register applications.	⚠ Failed	□
MS.AAD.5.2: Only administrators SHALL be allowed to consent to applications.	✓ Passed	□
MS.AAD.5.3: An admin consent workflow SHALL be configured for applications.	✓ Passed	□
MS.AAD.5.4: Group owners SHALL NOT be allowed to consent to applications.	⚠ Failed	□
MS.AAD.6.1: User passwords SHALL NOT expire.	✓ Passed	□
MS.AAD.7.1: A minimum of two users and a maximum of eight users SHALL be provisioned with the Global Administrator role.	✓ Passed	□
MS.AAD.7.2: Privileged users SHALL be provisioned with finer-grained roles instead of Global Administrator.	⚠ Failed	□
MS.AAD.7.3: Privileged users SHALL be provisioned cloud-only accounts separate from an on-premises directory or other federated identity providers.	✓ Passed	□
MS.AAD.7.4: Permanent active role assignments SHALL NOT be allowed for highly privileged roles.	⚠ Failed	□
MS.AAD.7.5: Provisioning users to highly privileged roles SHALL NOT occur outside of a PAM system.	✓ Passed	□

Test	Status	Info
MS.AAD.7.6: Activation of the Global Administrator role SHALL require approval.	Failed	□
MS.AAD.7.7: Eligible and Active highly privileged role assignments SHALL trigger an alert.	Failed	□
MS.AAD.7.8: User activation of the Global Administrator role SHALL trigger an alert.	Passed	□
MS.AAD.7.9: User activation of other highly privileged roles SHOULD trigger an alert.	Passed	□
MS.AAD.8.1: Guest users SHOULD have limited or restricted access to Azure AD directory objects.	Passed	□
MS.AAD.8.2: Only users with the Guest Inviter role SHOULD be able to invite guest users.	Failed	□
MS.EXO.1.1: Automatic forwarding to external domains SHALL be disabled.	Skipped	□
MS.EXO.12.1: IP allow lists SHOULD NOT be created.	Skipped	□
MS.EXO.12.2: Safe lists SHOULD NOT be enabled.	Skipped	□
MS.EXO.13.1: Mailbox auditing SHALL be enabled.	Skipped	□
MS.EXO.5.1: SMTP AUTH SHALL be disabled.	Skipped	□
MS.EXO.6.1: Contact folders SHALL NOT be shared with all domains.	Skipped	□
MS.EXO.6.2: Calendar details SHALL NOT be shared with all domains.	Skipped	□

Test	Status	Info
MS.EXO.7.1: External sender warnings SHALL be implemented.	Skipped	▭
MT.1001: At least one Conditional Access policy is configured with device compliance.	✓ Passed	▭
MT.1002: App management restrictions on applications and service principals is configured and enabled.	⚠ Failed	▭
MT.1003: At least one Conditional Access policy is configured with All Apps.	✓ Passed	▭
MT.1004: At least one Conditional Access policy is configured with All Apps and All Users.	✓ Passed	▭
MT.1005: All Conditional Access policies are configured to exclude at least one emergency/break glass account or group.	⚠ Failed	▭
MT.1006: At least one Conditional Access policy is configured to require MFA for admins.	✓ Passed	▭
MT.1007: At least one Conditional Access policy is configured to require MFA for all users.	✓ Passed	▭
MT.1008: At least one Conditional Access policy is configured to require MFA for Azure management.	⚠ Failed	▭
MT.1009: At least one Conditional Access policy is configured to block other legacy authentication.	✓ Passed	▭
MT.1010: At least one Conditional Access policy is configured to block legacy authentication for Exchange ActiveSync.	✓ Passed	▭
MT.1011: At least one Conditional Access policy is configured to secure security info registration only from a trusted location.	⚠ Failed	▭

Test	Status	Info
MT.1012: At least one Conditional Access policy is configured to require MFA for risky sign-ins.	⚠ Failed	□
MT.1013: At least one Conditional Access policy is configured to require new password when user risk is high.	⚠ Failed	□
MT.1014: At least one Conditional Access policy is configured to require compliant or Entra hybrid joined devices for admins.	⚠ Failed	□
MT.1015: At least one Conditional Access policy is configured to block access for unknown or unsupported device platforms.	⚠ Failed	□
MT.1016: At least one Conditional Access policy is configured to require MFA for guest access.	⚠ Failed	□
MT.1017: At least one Conditional Access policy is configured to enforce non persistent browser session for non-corporate devices.	⚠ Failed	□
MT.1018: At least one Conditional Access policy is configured to enforce sign-in frequency for non-corporate devices.	⚠ Failed	□
MT.1019: At least one Conditional Access policy is configured to enable application enforced restrictions.	⚠ Failed	□
MT.1020: All Conditional Access policies are configured to exclude directory synchronization accounts or do not scope them.	✓ Passed	□
MT.1021: Security Defaults are enabled.	Skipped	□
MT.1022: All users utilizing a P1 license should be licensed.	✓ Passed	□
MT.1023: All users utilizing a P2 license should be licensed.	✓ Passed	□

Test	Status	Info
MT.1024: Entra Recommendation - Applications with no owners.	✓ Passed	□
MT.1024: Entra Recommendation - Designate more than one global admin.	✓ Passed	□
MT.1024: Entra Recommendation - Do not allow users to grant consent to unreliable applications.	✓ Passed	□
MT.1024: Entra Recommendation - Enable password hash sync if hybrid.	⚠ Failed	□
MT.1024: Entra Recommendation - Enable self-service password reset.	⚠ Failed	□
MT.1024: Entra Recommendation - Ensure all users can complete multifactor authentication.	⚠ Failed	□
MT.1024: Entra Recommendation - Protect all users with a sign-in risk policy.	⚠ Failed	□
MT.1024: Entra Recommendation - Protect all users with a user risk policy .	⚠ Failed	□
MT.1024: Entra Recommendation - Protect your tenant with Insider Risk condition in Conditional Access policy.	⚠ Failed	□
MT.1024: Entra Recommendation - Remove unused applications.	⚠ Failed	□
MT.1024: Entra Recommendation - Remove unused credentials from applications.	⚠ Failed	□
MT.1024: Entra Recommendation - Require multifactor authentication for administrative roles.	⚠ Failed	□
MT.1024: Entra Recommendation - Use least privileged administrative roles .	⚠ Failed	□

Test	Status	Info
MT.1025: No external user with permanent role assignment on Control Plane.	✓ Passed	□
MT.1026: No hybrid user with permanent role assignment on Control Plane.	⚠ Failed	□
MT.1027: No Service Principal with Client Secret and permanent role assignment on Control Plane.	✓ Passed	□
MT.1028: No user with mailbox and permanent role assignment on Control Plane.	⚠ Failed	□
MT.1029: Stale accounts are not assigned to privileged roles.	⚠ Failed	□
MT.1030: Eligible role assignments on Control Plane are in use by administrators.	⚠ Failed	□
MT.1031: Privileged role on Control Plane are managed by PIM only.	⚠ Failed	□
MT.1032: Limited number of Global Admins are assigned.	⚠ Failed	□

Maester.dev