CIS Microsoft Entra ID STIG Benchmark

v1.0.0 - 08-13-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Microsoft Entra ID Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 28 Feb 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Entra ID and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Microsoft Entra ID

Recommendations

1 STIG RULES

Microsoft Entra ID

Microsoft Entra ID Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 28 Feb 2025

CLASSIFICATION unclassified

1.1 ENTR-ID-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must initiate a session lock after a 15-minute period of inactivity.

```
GROUP ID: V-270200
RULE ID: SV-270200r1085610
```

Rationale:

Session locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Session locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the session lock (e.g., via a Bluetooth-enabled session or dongle). User-initiated session locking is behavior or policy-based and, as such, requires users to take physical action to initiate the session lock. Session locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Satisfies: SRG-APP-000295

Audit:

To verify the inactivity timeout is configured for 15 minutes or less, follow the steps outlined below:

1. Sign in to entra.microsoft.us.
2. Navigate to the Gear icon (right) and select Settings >> Signing out + notifications.
3. Check that the "Enable directory level idle timeout" is selected.
4. Verify the Signing out value is 15 minutes or less.

If the directory level idle timeout is not set to 15 minutes or less, this is a finding.

Remediation:

1. Sign into entra.microsoft.us.
2. Navigate to the Gear icon (right) and select Settings >> Signing out + notifications.
3. Check the "Enable directory level idle timeout" box.
4. Populate the "Hours" field to "0" and the "Minutes" field to "15".
5. Click "Apply".

1.2 ENTR-ID-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must automatically disable accounts after a 35-day period of account inactivity.

```
GROUP ID: V-270204
RULE ID: SV-270204r1085660
```

Rationale:

Attackers that are able to exploit an inactive account can potentially obtain and maintain undetected access to an application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained. Applications need to track periods of user inactivity and disable accounts after 35 days of inactivity. Such a process greatly reduces the risk that accounts will be hijacked, leading to a data compromise.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to offload those access control functions and focus on core application features and functionality.

This policy does not apply to either emergency accounts or infrequently used accounts. Infrequently used accounts are local login administrator accounts used by system administrators when network or normal logon/access is not available. Emergency accounts are administrator accounts created in response to crisis situations.

References:

- https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/get-mguser?view=graph-powershell-1.0
- https://learn.microsoft.com/en-us/graph/api/user-list?view=graph-rest-1.0&tabs=http
- https://learn.microsoft.com/en-us/graph/api/resources/user?view=graph-rest-1.0#properties
- https://learn.microsoft.com/en-us/graph/api/resources/signinactivity?view=graph-rest-1.0#properties

For any PowerShell scripts that are Graph, note that Graph endpoints differ depending on where the tenant is located.

- For commercial tenants, graph endpoints are graph.microsoft.com.
- For GCC High tenants (IL4), graph endpoints are graph.microsoft.us.
- For DOD tenants (IL5), graph endpoints are dod-graph.microsoft.us.

Satisfies: SRG-APP-000025, SRG-APP-000163

Audit:

Verify Entra ID disables accounts after 35 days of inactivity.

Use the following procedure to discover inactive user accounts in Entra ID (35+ days) via the use of the Graph PowerShell SDK.

Installation instructions:

https://learn.microsoft.com/en-us/powershell/microsoftgraph/installation?view=graph-powershell-1.0

Required roles:

At least Global Reader

Required tenant license:

Entra ID Premium P1

Example PowerShell commands:

```
Connect-MgGraph -Scopes AuditLog.Read.All,User.Read.All -Environment USGov

$inactiveDate = (Get-Date).AddDays(-35)

$users = Get-MgUser -All:$true -Property Id, DisplayName, UserPrincipalName,
UserType, createdDateTime, SignInActivity, AccountEnabled | Where-Object {
$_.AccountEnabled -eq $true }

$inactiveUsers =
$users | Where-Object {
    ($_.SignInActivity.LastSignInDateTime -lt $inactiveDate) -or
($_.SignInActivity.LastSignInDateTime -eq $null -and $_.CreatedDateTime -lt
$inactiveDate)
} | Select-Object DisplayName, UserPrincipalName, UserType, createdDateTime,
@{Name = 'LastSignInDateTime'; Expression =
{($_.SignInActivity).LastSignInDateTime}}, Id | Sort-Object
LastSignInDateTime

$inactiveUsers | Format-Table -AutoSize
```

If accounts are not disabled after a 35-day period of account inactivity, this is a finding.

Remediation:

1. Sign in to the Microsoft Entra admin center as at least a Reports Reader.
2. Browse to Identity >> Users >> All users.
3. Select a user from the list.
4. Use the following procedure to disable inactive user accounts in Entra ID via the use of the Graph PowerShell SDK.

Installation instructions:

https://learn.microsoft.com/en-us/powershell/microsoftgraph/installation?view=graph-powershell-1.0
Required roles:
Global Administrator
Install the Microsoft Graph PowerShell SDK.
Install-Module Microsoft.Graph -Scope CurrentUser

```
Connect-MgGraph -Scopes "User.ReadWrite.All", "Directory.ReadWrite.All",
"SignInActivity.Read.All"
```

Set the inactivity threshold (in days)

```
$inactivityThreshold = 35
```

Get the current date

```
$currentDate = Get-Date
```

Get all users and their last sign-in activity

```
$users = Get-MgUser -All -Property "DisplayName", "SignInActivity"
```

Filter for inactive users

```
$inactiveUsers = $users | Where-Object {
    $_.SignInActivity.LastSignInDateTime -lt ($currentDate.AddDays(-
$inactivityThreshold))
}
```

Disable inactive users

```
foreach ($user in $inactiveUsers) {
    Set-MgUser -UserId $user.Id -AccountEnabled $false
    Write-Host "Disabled user: $($user.DisplayName)"
}
```

1.3 ENTR-ID-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period.

```
GROUP ID: V-270208
RULE ID: SV-270208r1085616
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-APP-000345

Audit:

Verify Entra ID is configured to enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period.

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Browse to Identity >> Protection >> Authentication methods >> Password protection.
3. Verify the Lockout Threshold has been set to "3" and Lockout duration is set to "900" or more.

If Entra ID is not configured to enforce the limit of three consecutive invalid logon attempts with a lockout period of 15 minutes, this is a finding.

Remediation:

To configure account lockout settings, complete these steps:

1. Sign in to the Microsoft Entra admin center as at least an Authentication Administrator.
2. Browse to Identity >> Protection >> Authentication methods >> Password protection.
3. Set the Lockout threshold to "3".
4. Set the Lockout duration to "900" (15 minutes).

1.4 ENTR-ID-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the application.

```
GROUP ID: V-270209
RULE ID: SV-270209r1085618
```

Rationale:

Display of the DOD-approved use notification before granting access to the application ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for applications that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Satisfies: SRG-APP-000068, SRG-APP-000069, SRG-APP-000070

Audit:

Verify Entra ID has been configured to display the DOD logon banner when a user logs on.

1. Sign in to the Microsoft Entra admin center as a Global Administrator.
2. Browse to or search "Company Branding".
3. Browse to the "Sign-in form" tab and review the required DOD banner text in the "Sign-in page text". Note: This field is limited to 1024 characters.

If the DOD logon banner text is not present in the "Sign-in page text" field, this is a finding.

Remediation:

To create the standard DOD banner in Entra ID:

1. Sign in to the Microsoft Entra admin center as a Global Administrator.
2. Browse to or search "Company Branding".
3. Select "Customize" under "Default sign-in experience".
4. Browse to the "Sign-in form" tab and place the required DOD banner text in the "Sign-in page text". Note: This field is limited to 1024 characters.
5. Populate all required fields.
6. Click "Review + Create".

1.5 ENTR-ID-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must be configured to transfer logs to another server for storage, analysis, and reporting.

```
GROUP ID: V-270227
RULE ID: SV-270227r1085728
```

Rationale:

Protection of log data includes ensuring log data is not accidentally lost or deleted. Backing up audit records to a different system or onto separate media than the system being audited on an organizationally defined frequency helps to ensure the audit records will be retained in the event of a catastrophic system failure.

This also ensures a compromise of the information system being audited does not result in a compromise of the audit records.

This requirement only applies to applications that have a native backup capability for audit records. Operating system backup requirements cover applications that do not provide native backup functions.

Satisfies: SRG-APP-000358

Audit:

Verify Microsoft Entra ID sign-in logs are updated in Microsoft Sentinel or equivalent SIEM. Verify the Connected Status is "green" with Last Log Received within the past hour.

1. Sign in to the Microsoft Entra admin center as a Global Administrator.
2. Browse to Identity >> Monitoring & health >> Diagnostic settings.
3. Select "Edit settings" for the entry that has an established log analytics workspace.
4. Review the selected log categories. The minimum required categories are:

- SigninLogs.
- AuditLogs.
- ServicePrincipalSignInLogs.
- ManagedIdentitySignInLogs.
- UserRiskEvents.
- RiskyUsers.
- RiskyServicePrincipals.
- ServicePrincipalRiskEvents.

If there is not an entry established to offload logs to a log analytic workspace and the minimum log categories are not selected, this is a finding.

Remediation:

Configure the Microsoft Entra to transfer Microsoft Entra server logs to another server for storage, analysis, and reporting at least every seven days.

1. Sign in to the Microsoft Entra admin center as a Global Administrator.
2. Browse to Identity >> Monitoring & health >> Diagnostic settings.
3. Select "+ Add diagnostic settings".
4. Select at least these required categories:

- SigninLogs.
- AuditLogs.
- ServicePrincipalSignInLogs.
- ManagedIdentitySignInLogs.
- UserRiskEvents.
- RiskyUsers.
- RiskyServicePrincipals.
- ServicePrincipalRiskEvents.

5. Select "Send to Log Analytics workspace". For details on establishing a log analytics workspace, reference the DOD365 TCG.

1.6 ENTR-ID-000440 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Microsoft Entra ID must be configured to use multifactor authentication (MFA).

```
GROUP ID: V-270233
RULE ID: SV-270233r1085634
```

Rationale:

Without the use of MFA, the ease of access to privileged functions is greatly increased.

MFA requires the use of two or more factors to achieve authentication.

Factors include: (i) Something a user knows (e.g., password/PIN); (ii) Something a user has (e.g., cryptographic identification device, token); or (iii) Something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

Satisfies: SRG-APP-000149, SRG-APP-000150, SRG-APP-000154, SRG-APP-000155

Audit:

Verify user accounts require MFA.

1. Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.
2. Browse to Identity >> Protection >> Conditional Access.
3. Select "Policies" and find the MFA policy.
4. Confirm the policy state is set to "On".
5. Select the policy and confirm "All users included" is specified under the Users option of the policy.
6. Confirm any exclusions listed under the "Exclude" section of the Users option are documented with the authorizing official (AO).

If the MFA policy is not set to "On" with "All users included" selected and any exclusions are not documented with the AO, this is a finding.

Remediation:

Account authentication is managed by Entra ID. The following steps will create a Conditional Access policy to require all users to use MFA:

1. Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.
2. In the search bar, search for "Conditional Access".
3. Select "Create new policy".
4. Give the policy a name. It is recommended that organizations create a meaningful standard for the names of policies.
5. Under "Assignments", select "Users" or "workload identities".
6. a. Under "Include", select "All users".
7. b. Under "Exclude", select "Users" and "groups", and then choose the organization's emergency access or break-glass accounts.
8. Navigate to Target resources >> Cloud apps >> Include. Select "All cloud apps".
9. a. Under "Exclude", select any applications that do not require MFA.
10. Navigate to Access controls >> Grant. Select "Grant access, Require multifactor authentication", and then click "Select".
11. Confirm the settings and set "Enable policy" to "Report-only".
12. Select "Create" to enable the policy.
13. After confirming the policy, deploy the policy by either moving the "Enable" policy toggle from "Report-only" to "On" or alternately, deploying the policy using a Conditional Access template.

1.7 ENTR-ID-000610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must enforce a 60-day maximum password lifetime restriction.

```
GROUP ID: V-270239
RULE ID: SV-270239r1085663
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed at specific intervals.

One method of minimizing this risk is to use complex passwords and periodically change them. If the application does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the system and/or application passwords could be compromised.

This requirement does not include emergency administration accounts, which are meant for access to the application in case of failure. These accounts are not required to have maximum password lifetime restrictions.

Audit:

Verify the Entra ID password expiration time period has been changed to 60 days.

Interview the site Entra ID system administrator and verify the script shown in the Fix has been run.

If the Entra ID password expiration time period is not 60 days or less, this is a finding.

Note: It is not possible to view the current value for the password expiration time (the Entra ID default is 90). An administrator can check the maximum password age of their Entra ID tenant by using the Graph PowerShell SDK module and the "Get-MgDomain" command by using the script located here:

https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.directorymanagement/get-mgdomain?view=graph-powershell-1.0

Note: For any PowerShell scripts that are Graph, note that Graph endpoints differ depending on where the tenant is located.

- For commercial tenants, graph endpoints are graph.microsoft.com.
- For GCC High tenants (IL4), graph endpoints are graph.microsoft.us.
- For DOD tenants (IL5), graph endpoints are dod-graph.microsoft.us.

Remediation:

Change the default Entra ID password expiration time period to 60 days by using the Graph script located here:

https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguser

Use the "Get-MgDomain" command, and update it to 60 days using the "Update-MgDomain -DomainId <DomainName>

-PasswordValidityPeriodInDays 60" command.

Note: For any PowerShell scripts that are Graph, note that Graph endpoints differ depending on where the tenant is located.

- For commercial tenants, graph endpoints are graph.microsoft.com.
- For GCC High tenants (IL4), graph endpoints are graph.microsoft.us.
- For DOD tenants (IL5), graph endpoints are dod-graph.microsoft.us.

1.8 ENTR-ID-000835 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must notify system administrators (SAs) and the information system security officer (ISSO) when privileges are being requested.

```
GROUP ID: V-270255
RULE ID: SV-270255r1085626
```

Rationale:

When application accounts are modified, user accessibility is affected. Accounts are used for identifying individual users or for identifying the application processes themselves. Sending notification of account modification events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

Verify PIM is in use with email notifications going to the SA and ISSO when privileges are requested.

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Search for "Microsoft Entra Privileged Identity Management".
3. Navigate to "Management" and select "Microsoft Entra roles".
4. Expand the "Manage" menu and select roles.
5. For each role that is either active or eligible perform the following:
6. a. Select the role.
7. b. Navigate to role settings.
8. c. Under "Send notifications when eligible members activate this role:" Verify the SA and ISSO email addresses are listed under "Additional recipients" for the type "Role activation alert".

If the SA and ISSO are not set up to receive email notification when privileges are requested through PIM, this is a finding.

Remediation:

Configure PIM to email notifications to the SA and ISSO when privileges are requested.

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Search for "Microsoft Entra Privileged Identity Management".
3. Navigate to "Management" and select "Microsoft Entra roles".
4. Expand the "Manage" menu and select roles.
5. For each role that is either active or eligible perform the following:
6. a. Select the role.
7. b. Navigate to role settings.
8. c. Select "Edit".
9. d. Navigate to the "Notification" tab.
10. e. Under "Send notifications when eligible members activate this role:" add the SA and ISSO email addresses under "Additional recipients".
11. f. Select "Update".

1.9 ENTR-ID-001900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must use Privileged Identity Management (PIM).

```
GROUP ID: V-270335
RULE ID: SV-270335r1085641
```

Rationale:

Emergency accounts are administrator accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon/access is not available). Infrequently used accounts also remain available and are not subject to automatic termination dates. However, an emergency account is normally a different account created for use by vendors or system maintainers.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to offload those access control functions and focus on core application features and functionality.

Audit:

Verify PIM is in use with just-in-time (JIT) access and employing the principle of least privilege access.

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Search for "Microsoft Entra Privileged Identity Management".
3. Navigate to "Management" and select "Microsoft Entra roles".
4. Expand the "Manage" menu and select "Assignments".
5. Select the "Active assignments" tab and for each privileged role, verify there are no roles with an end time of "Permanent".

If any privileged roles are present with an end time of "Permanent", this is a finding.

Remediation:

Configure PIM to just-in-time (JIT) access and employ the principle of least privilege access.

When assigning privileged roles to accounts, select the assignment type of "Eligible".

1.10 ENTR-ID-003350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Entra ID must, for password-based authentication, verify when users create or update passwords that the passwords are not found on the list of commonly used, expected, or compromised passwords.

```
GROUP ID: V-270475
RULE ID: SV-270475r1085680
```

Rationale:

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multifactor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Audit:

As an authorized administrator, browse to https://portal.azure.us/#view/Microsoft_AAD_ConditionalAccess/PasswordProtectionBlade.

Check the "Custom banned passwords" section. If "Enforce custom list" has not be configured to "Yes" and a custom banned password list has not been populated, this is a finding.

Remediation:

As an authorized administrator, browse to https://portal.azure.us/#view/Microsoft_AAD_ConditionalAccess/PasswordProtectionBlade.

Enable the Custom banned password list by selecting "Yes" next to the "Enforce custom list" option.

Populate the "Custom banned password list".

The list must be one word per line, with a maximum of 1000 words. The words are case insensitive, and common character substitutions (o for 0, etc) are automatically considered.

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	ENTR-ID-000030 (Manual)	☐	☐
1.2	ENTR-ID-000090 (Manual)	☐	☐
1.3	ENTR-ID-000140 (Manual)	☐	☐
1.4	ENTR-ID-000150 (Manual)	☐	☐
1.5	ENTR-ID-000370 (Manual)	☐	☐
1.6	ENTR-ID-000440 (Manual)	☐	☐
1.7	ENTR-ID-000610 (Manual)	☐	☐
1.8	ENTR-ID-000835 (Manual)	☐	☐
1.9	ENTR-ID-001900 (Manual)	☐	☐
1.10	ENTR-ID-003350 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08/13/2025	1.0.0	Initial CIS Release