AZURE ACTIVE DIRECTORY

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.0

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see [https://www.cisa.gov/tlp.](https://www.cisa.gov/tlp)

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
1.0	• Creation	CISA	08/13/2023

CONTENTS

1. CISA Security Configuration Baseline for Azure Active Directory 7
  1.1 License Compliance And Copyright 7
  1.2 Assumptions 7
  1.3 Key Terminology 7
2. Baseline Policies 8
  2.1 Legacy Authentication 8
  2.2 Policies 8
    2.2.1 MS.AAD.1.1v1 8
  2.3 Resources 9
  2.4 License Requirements 9
  2.5 Implementation 9
    2.5.1 MS.AAD.1.1v1 Instructions 9
3. Risk-Based Policies 9
  3.1 Policies 9
    3.1.1 MS.AAD.2.1v1 9
    3.1.2 MS.AAD.2.2v1 9
    3.1.3 MS.AAD.2.3v1 10
  3.2 Resources 10
  3.3 License Requirements 10
  3.4 Implementation 10
    3.4.1 MS.AAD.2.1v1 Instructions 10
    3.4.2 MS.AAD.2.2v1 Instructions 10
    3.4.3 MS.AAD.2.3v1 Instructions 10
4. Strong Authentication and a Secure Registration Process 11
      Figure 1: Depiction of MFA methods from weakest to strongest (adapted from Microsoft page) 11
  4.1 Policies 11
    4.1.1 MS.AAD.3.1v1 11
    4.1.2 MS.AAD.3.2v1 11

4.1.3 MS.AAD.3.3v1 12
4.1.4 MS.AAD.3.4v1 12
4.1.5 MS.AAD.3.5v1 12
4.1.6 MS.AAD.3.6v1 12
4.1.7 MS.AAD.3.7v1 12
4.1.8 MS.AAD.3.8v1 13
4.2 Resources 13
4.3 License Requirements 13
4.4 Implementation 13
4.4.1 MS.AAD.3.1v1 Instructions 13
4.4.2 MS.AAD.3.2v1 Instructions 13
4.4.3 MS.AAD.3.3v1 Instructions 14
4.4.4 MS.AAD.3.4v1 Instructions 14
4.4.5 MS.AAD.3.5v1 Instructions 14
4.4.6 MS.AAD.3.6v1 Instructions 14
4.4.7 MS.AAD.3.7v1 Instructions 14
4.4.8 MS.AAD.3.8v1 Instructions 15
5. Centralized Log Collection 15
5.1 Policies 15
5.1.1 MS.AAD.4.1v1 15
5.2 Resources 15
5.3 License Requirements 16
5.4 Implementation 16
5.4.1 MS.AAD.4.1v1 Instructions 16
6. Application Registration and Consent 16
6.1 Policies 16
6.1.1 MS.AAD.5.1v1 16
6.1.2 MS.AAD.5.2v1 16
6.1.3 MS.AAD.5.3v1 16
6.1.4 MS.AAD.5.4v1 16
6.2 Resources 17
6.3 License Requirements 17

6.4 Implementation 17
    6.4.1 MS.AAD.5.1v1 Instructions 17
    6.4.2 MS.AAD.5.2v1 Instructions 17
    6.4.3 MS.AAD.5.3v1 Instructions 17
    6.4.4 MS.AAD.5.4v1 Instructions 17
7. Passwords 17
  7.1 Policies 18
    7.1.1 MS.AAD.6.1v1 18
  7.2 Resources 18
  7.3 License Requirements 18
  7.4 Implementation 18
    7.4.1 MS.AAD.6.1v1 Instructions 18
8. Highly Privileged User Access 18
  8.1 Policies 18
    8.1.1 MS.AAD.7.1v1 18
    8.1.2 MS.AAD.7.2v1 19
    8.1.3 MS.AAD.7.3v1 19
    8.1.4 MS.AAD.7.4v1 19
    8.1.5 MS.AAD.7.5v1 19
    8.1.6 MS.AAD.7.6v1 19
    8.1.7 MS.AAD.7.7v1 19
    8.1.8 MS.AAD.7.8v1 20
    8.1.9 MS.AAD.7.9v1 20
  8.2 Resources 20
  8.3 License Requirements 20
  8.4 Implementation 20
    8.4.1 MS.AAD.7.1v1 Instructions 20
    8.4.2 MS.AAD.7.2v1 Instructions 20
    8.4.3 MS.AAD.7.3v1 Instructions 21
    8.4.4 MS.AAD.7.4v1 Instructions 21
    8.4.5 MS.AAD.7.5v1 Instructions 21
    8.4.6 MS.AAD.7.6v1 Instructions 22

8.4.7 MS.AAD.7.7v1 Instructions 22
8.4.8 MS.AAD.7.8v1 Instructions 22
8.4.9 MS.AAD.7.9v1 Instructions 22
9. Guest User Access 23
9.1 Policies 23
9.1.1 MS.AAD.8.1v1 23
9.1.2 MS.AAD.8.2v1 23
9.1.3 MS.AAD.8.3v1 23
9.2 Resources 23
9.3 License Requirements 23
9.4 Implementation 23
9.4.1 MS.AAD.8.1v1 Instructions 23
9.4.2 MS.AAD.8.2v1 Instructions 24
9.4.3 MS.AAD.8.3v1 Instructions 24

1. CISA SECURITY CONFIGURATION BASELINE FOR AZURE ACTIVE DIRECTORY

Microsoft 365 (M365) Azure Active Directory (Azure AD) is a cloud-based identity and access control service that provides security and functional capabilities. This Secure Configuration Baseline (SCB) provides specific policies to help secure Azure AD.

The Secure Cloud Business Applications (SCuBA) project run by the Cybersecurity and Infrastructure Security Agency (CISA) provides guidance and capabilities to secure federal civilian executive branch (FCEB) agencies' cloud business application environments and protect federal information that is created, accessed, shared, and stored in those environments.

The CISA SCuBA SCBs for M365 help secure federal information assets stored within M365 cloud business application environments through consistent, effective, and manageable security configurations. CISA created baselines tailored to the federal government's threats and risk tolerance with the knowledge that every organization has different threat models and risk tolerance. Non-governmental organizations may also find value in applying these baselines to reduce risks.

The information in this document is being provided "as is" for INFORMATIONAL PURPOSES ONLY. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA. This document does not address, ensure compliance with, or supersede any law, regulation, or other authority. Entities are responsible for complying with any recordkeeping, privacy, and other laws that may apply to the use of technology. This document is not intended to, and does not, create any right or benefit for anyone against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

1.1 LICENSE COMPLIANCE AND COPYRIGHT

Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Sources are linked throughout this document. The United States government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

1.2 ASSUMPTIONS

The License Requirements sections of this document assume the organization is using an M365 E3 or G3 license level, at a minimum. Therefore, only licenses not included in E3/G3 are listed.

Some of the policies in this baseline may link to Microsoft instruction pages. This is done with the presumption that an agency has created emergency access accounts in Azure AD and implemented strong security measures to protect the credentials of those accounts.

1.3 KEY TERMINOLOGY

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

The following are key terms and descriptions used in this document.

Hybrid Azure AD – This term denotes the scenario where an organization has an on-premises AD domain that contains the master user directory but federates access to the cloud M365 Azure AD tenant.

Resource Tenant and Home Tenant – In scenarios where guest users are involved, the resource tenant hosts the M365 target resources that the guest user accesses. The home tenant hosts the guest user's identity.

Highly Privileged Roles – This section provides a list of what CISA considers highly privileged built-in roles in Azure AD.

- Global Administrator
- Privileged Role Administrator
- User Administrator
- SharePoint Administrator
- Exchange Administrator
- Hybrid Identity Administrator
- Application Administrator
- Cloud Application Administrator

Throughout this document, this list of highly privileged roles is referenced in numerous baseline policies. Agencies should consider this list a foundational reference and apply respective baseline policies to additional Azure AD roles as necessary.

Conditional Access Policies – Numerous policies in this baseline rely on Azure AD Conditional Access. Conditional Access is a feature that allows administrators to limit access to resources using conditions such as user or group membership, device, IP location, and real-time risk detection. This section provides guidance and tools to support implementation of baseline policies that rely on Azure AD Conditional Access.

As described in Microsoft's literature related to conditional access policies, CISA recommends initially setting a policy to Report-only when it is created and then performing thorough hands-on testing to help prevent unintended consequences before toggling the policy from Report-only to On. The policy will only be enforced when it is set to On. The What If tool runs test simulations. Refer to Microsoft's Conditional Access insights and reporting for further assistance with testing.

2. BASELINE POLICIES

2.1 LEGACY AUTHENTICATION

This section provides policies that reduce security risks related to legacy authentication protocols that do not support multifactor authentication (MFA).

2.2 POLICIES

2.2.1 MS.AAD.1.1v1

Legacy authentication SHALL be blocked.

Rationale: The security risk of allowing legacy authentication protocols is they do not support MFA. Blocking legacy protocols reduces the impact of user credential theft.

Last modified: June 2023

2.3 RESOURCES

- Common Conditional Access policy: Block legacy authentication
- Five steps to securing your identity infrastructure

2.4 LICENSE REQUIREMENTS

- N/A

2.5 IMPLEMENTATION

2.5.1 MS.AAD.1.1v1 Instructions

- Determine if an agency's existing applications use legacy authentication before blocking legacy authentication across the entire application base.
- Create a Conditional Access policy to block legacy authentication.

3. RISK-BASED POLICIES

This section provides policies that reduce security risks related to potentially compromised user accounts. These policies combine Azure AD Identity Protection and Azure AD Conditional Access. Azure AD Identity Protection uses numerous signals to detect the risk level for each user or sign-in and determine if an account may have been compromised.

Additional mitigations to reduce risks associated with the authentication of workload identities: Although not covered in this baseline due to the need for an additional non-standard license, Microsoft provides support for mitigating risks related to workload identities (Azure AD applications or service principals). Agencies should strongly consider implementing this feature because workload identities present many of the same risks as interactive user access and are commonly used in modern systems. CISA urges organizations to apply Conditional Access policies to workload identities.

Note: In this section, the term "high risk" denotes the risk level applied by the Azure AD Identity Protection service to a user account or sign-in event.

3.1 POLICIES

3.1.1 MS.AAD.2.1v1

Users detected as high risk SHALL be blocked.

- *Rationale:* Blocking high-risk users may prevent compromised accounts from accessing the tenant.
- *Last modified:* June 2023
- *Note:* Users identified as high risk by Azure AD Identity Protection can be blocked from accessing the system via an Azure AD Conditional Access policy. A high-risk user will be blocked until an administrator remediates their account.

3.1.2 MS.AAD.2.2v1

A notification SHOULD be sent to the administrator when high-risk users are detected.

- *Rationale:* Notification enables the admin to monitor the event and remediate the risk. This helps the organization proactively respond to cyber intrusions as they occur.

- *Last modified:* June 2023

3.1.3 MS.AAD.2.3v1

Sign-ins detected as high risk SHALL be blocked.

- *Rationale:* This prevents compromised accounts from accessing the tenant.
- *Last modified:* June 2023

3.2 RESOURCES

- What are risk detections?
- Simulating risk detections in Identity Protection
- User experiences with Microsoft Entra Identity Protection

3.3 LICENSE REQUIREMENTS

- Requires a Microsoft Entra ID P2 license.

3.4 IMPLEMENTATION

3.4.1 MS.AAD.2.1v1 Instructions

- Create a conditional access policy blocking users categorized as high risk by the Identity Protection service. Configure the following policy settings in the new conditional access policy as per the values below:

```
Users > Include > All users

Target resources > Cloud apps > All cloud apps

Conditions > User risk > High

Access controls > Grant > Block Access
```

3.4.2 MS.AAD.2.2v1 Instructions

- Configure Azure AD Identity Protection to send a regularly monitored security mailbox email notification when user accounts are determined to be high risk.

3.4.3 MS.AAD.2.3v1 Instructions

- Create a Conditional Access policy blocking sign-ins determined high risk by the Identity Protection service. Configure the following policy settings in the new Conditional Access policy as per the values below:

```
Users > Include > All users

Target resources > Cloud apps > All cloud apps

Conditions > Sign-in risk > High
```

```
Access controls > Grant > Block Access
```

4. STRONG AUTHENTICATION AND A SECURE REGISTRATION PROCESS

This section provides policies that help reduce security risks related to user authentication and registration.

Phishing-resistant MFA is required per Office of Management and Budget Memorandum 22-09, but for a variety of reasons, implementing it for all users may be challenging. This section provides additional backup security policies to mitigate risk associated with lesser forms of MFA. For example, Policy MS.AAD.3.2v1 below enforces MFA without stipulating the specific MFA method.

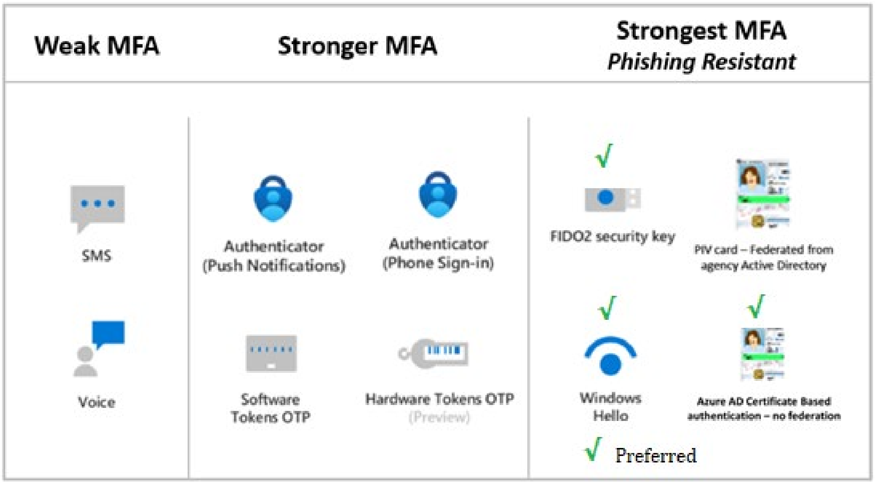
Weak MFA
Stronger MFA
Strongest MFA
Phishing Resistant
SMS
Voice
Authenticator (Push Notifications)
Authenticator (Phone Sign-in)
Software Tokens OTP
Hardware Tokens OTP (Preview)
√
FIDO2 security key
PIV card – Federated from agency Active Directory
√
Windows Hello
√
Azure AD Certificate Based authentication – no federation
√ Preferred

Figure 1: Depiction of MFA methods from weakest to strongest (adapted from Microsoft page).

4.1 POLICIES

4.1.1 MS.AAD.3.1v1

Phishing-resistant MFA SHALL be enforced for all users.

The phishing-resistant methods Azure AD Certificate-Based Authentication (CBA), FIDO2 Security Key, and Windows Hello for Business are the recommended authentication options since they offer forms of MFA with the least weaknesses. For federal agencies, Azure AD CBA supports federal PIV card authentication directly to Azure AD.

If on-premises PIV authentication and federation to Azure AD is used, enforce PIV logon via AD group policy.

- *Rationale:* Weaker forms of MFA do not protect against sophisticated phishing attacks. By enforcing methods resistant to phishing, those risks are minimized.
- *Last modified:* June 2023

4.1.2 MS.AAD.3.2v1

If phishing-resistant MFA has not been enforced, an alternative MFA method SHALL be enforced for all users.

- *Rationale:* This is a stopgap security policy to help protect the tenant if phishing-resistant MFA has not been enforced. This policy requires MFA enforcement, thus reducing single-form authentication risk.

- *Last modified:* June 2023
- *Note:* If a conditional access policy has been created enforcing phishing-resistant MFA, then this policy is not necessary. This policy does not dictate the specific MFA method.

4.1.3 MS.AAD.3.3v1

If phishing-resistant MFA has not been enforced and Microsoft Authenticator is enabled, it SHALL be configured to show login context information.

- *Rationale:* This stopgap security policy helps protect the tenant when phishing-resistant MFA has not been enforced and Microsoft Authenticator is used. This policy helps improve the security of Microsoft Authenticator by showing user context information, which helps reduce MFA phishing compromises.
- *Last modified:* June 2023

4.1.4 MS.AAD.3.4v1

The Authentication Methods Manage Migration feature SHALL be set to Migration Complete.

- *Rationale:* To disable the legacy authentication methods screen for the tenant, configure the Manage Migration feature to Migration Complete. The MFA and Self-Service Password Reset (SSPR) authentication methods are both managed from a central admin page, thereby reducing administrative complexity and potential security misconfigurations.
- *Last modified:* June 2023

4.1.5 MS.AAD.3.5v1

The authentication methods SMS, voice call, and email one-time password (OTP) SHALL be disabled.

- *Rationale:* SMS, voice call, and email OTP are the weakest authenticators. This policy forces users to use stronger MFA methods.
- *Last modified:* June 2023
- *Note:* This policy is only applicable if the tenant has their Manage Migration feature set to Migration Complete.

4.1.6 MS.AAD.3.6v1

Phishing-resistant MFA SHALL be required for highly privileged roles.

- *Rationale:* This is a backup security policy to help protect privileged access to the tenant if the conditional access policy, which requires MFA for all users, is disabled or misconfigured.
- *Last modified:* June 2023
- *Note:* Refer to the Highly Privileged Roles section at the top of this document for a reference list of roles considered highly privileged.

4.1.7 MS.AAD.3.7v1

Managed devices SHOULD be required for authentication.

- *Rationale:* The security risk of an adversary authenticating to the tenant from their own device is reduced by requiring a managed device to authenticate. Managed devices are under the provisioning and control of the agency. OMB M-22-09 states, "When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user."

- *Last modified:* June 2023

4.1.8 MS.AAD.3.8v1

Managed devices SHOULD be required to register MFA.

- *Rationale:* Reduce risk of an adversary using stolen user credentials and then registering their own MFA device to access the tenant by requiring a managed device provisioned and controlled by the agency to perform registration actions. This prevents the adversary from using their own unmanaged device to perform the registration.
- *Last modified:* June 2023

4.2 RESOURCES

- What authentication and verification methods are available in Microsoft Entra ID?
- How to use additional context in Microsoft Authenticator notifications - Authentication methods policy
- M-22-09 Federal Zero Trust Architecture Strategy
- Configure Microsoft Entra hybrid join
- Microsoft Entra joined devices
- Set up automatic enrollment for Windows devices (for Intune)

4.3 LICENSE REQUIREMENTS

- Policies related to managed devices require Microsoft Intune.

4.4 IMPLEMENTATION

4.4.1 MS.AAD.3.1v1 Instructions

Create a conditional access policy enforcing phishing-resistant MFA for all users. Configure the following policy settings in the new conditional access policy, per the values below:

```
  Users > Include > All users

  Target resources > Cloud apps > All cloud apps

  Access controls > Grant > Grant Access > Require authentication strength >
Phishing-resistant MFA
```

4.4.2 MS.AAD.3.2v1 Instructions

If phishing-resistant MFA has not been enforced for all users yet, create a conditional access policy that enforces MFA but does not dictate MFA method. Configure the following policy settings in the new conditional access policy, per the values below:

```
  Users > Include > All users

  Target resources > Cloud apps > All cloud apps

  Access controls > Grant > Grant Access > Require multifactor authentication
```

4.4.3 MS.AAD.3.3v1 Instructions

If phishing-resistant MFA has not been deployed yet and Microsoft Authenticator is in use, configure Authenticator to display context information to users when they log in.

1. In Azure Active Directory, click Security > Authentication methods > Microsoft Authenticator.
2. Click the Configure tab.
3. For Allow use of Microsoft Authenticator OTP, select No.
4. Under Show application name in push and passwordless notifications, select Status > Enabled and Target > Include > All users.
5. Under Show geographic location in push and passwordless notifications, select Status > Enabled and Target > Include > All users.
6. Select Save.

4.4.4 MS.AAD.3.4v1 Instructions

1. Go through the process of [migrating from the legacy Azure AD MFA and Self-Service Password Reset (SSPR) administration pages to the new unified Authentication Methods policy page]().
2. Once ready to finish the migration, set the [Manage Migration option to Migration Complete]().

4.4.5 MS.AAD.3.5v1 Instructions

1. In Azure Active Directory, click Security > Authentication methods.
2. Click on the SMS, Voice Call, and Email OTP authentication methods and disable each of them. Their statuses should be Enabled > No on the Authentication methods > Policies page.

4.4.6 MS.AAD.3.6v1 Instructions

Create a conditional access policy enforcing phishing-resistant MFA for highly privileged roles. Configure the following policy settings in the new conditional access policy per the values below:

```
Users > Include > Select users and groups > Directory roles > select each of
the roles listed in the Highly Privileged Roles section at the top of this
document

Target resources > Cloud apps > All cloud apps

Access controls > Grant > Grant Access > Require authentication strength >
Phishing-resistant MFA
```

4.4.7 MS.AAD.3.7v1 Instructions

Create a conditional access policy requiring a user's device to be either Microsoft Entra hybrid joined or compliant during authentication. Configure the following policy settings in the new conditional access policy per the values below:

```
Users > Include > All users

Target resources > Cloud apps > All cloud apps

Access controls > Grant > Grant Access > Require device to be marked as
compliant and Require  Microsoft Entra hybrid joined device > For multiple
controls > Require one of the selected controls
```

4.4.8 MS.AAD.3.8v1 Instructions

Create a conditional access policy requiring a user to be on a managed device when registering for MFA. Configure the following policy settings in the new conditional access policy per the values below:

```
  Users > Include > All users

  Target resources > User actions > Register security information

  Access controls > Grant > Grant Access > Require device to be marked as
  compliant and Require Microsoft Entra hybrid joined device > For multiple
  controls > Require one of the selected controls
```

5. CENTRALIZED LOG COLLECTION

This section provides policies to reduce security risks related to the lack of security logs, which hampers security visibility.

5.1 POLICIES

5.1.1 MS.AAD.4.1v1

Security logs SHALL be sent to the agency's security operations center for monitoring.

- *Rationale:* The security risk of not having visibility into cyber attacks is reduced by collecting logs in the agency's centralized security detection infrastructure. This makes security events available for auditing, query, and incident response.
- *Last modified:* June 2023
- *Note:* The following logs (configured in Azure AD diagnostic settings) are required: AuditLogs, SignInLogs, RiskyUsers, UserRiskEvents, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, ADFSSignInLogs, RiskyServicePrincipals, ServicePrincipalRiskEvents, EnrichedOffice365AuditLogs, and MicrosoftGraphActivityLogs. If managed identities are used for Azure resources, also send the ManagedIdentitySignInLogs log type. If the Azure AD Provisioning Service is used to provision users to software-as-a-service (SaaS) apps or other systems, also send the ProvisioningLogs log type.
- *Note:* Agencies can benefit from security detection capabilities offered by the CISA Cloud Log Aggregation Warehouse (CLAW) system. Agencies are urged to send the logs to CLAW. Contact CISA at cyberliason@cisa.dhs.gov to request integration instructions.

5.2 RESOURCES

- [Everything you wanted to know about Security and Audit Logging in Office 365]
- [What are Microsoft Entra sign-in logs?]
- [National Cybersecurity Protection System-Cloud Interface Reference Architecture Volume One: General Guidance]

5.3 LICENSE REQUIREMENTS

- An Azure subscription may be required to send logs to an external system, such as the agency's security information and event management (SIEM).

5.4 IMPLEMENTATION

5.4.1 MS.AAD.4.1v1 Instructions

- Follow the configuration instructions unique to the products and integration patterns at your organization to send the security logs to the security operations center for monitoring.

6. APPLICATION REGISTRATION AND CONSENT

This section provides policies that help reduce security risk of malicious applications or service principals added to the tenant by non-privileged users. Malicious applications can perform many of the same operations as interactive users and can access data on behalf of compromised users. These policies apply to custom-developed applications and applications published by third-party vendors.

6.1 POLICIES

6.1.1 MS.AAD.5.1v1

Only administrators SHALL be allowed to register applications.

- *Rationale:* Application access for the tenant presents a heightened security risk compared to interactive user access because applications are typically not subject to critical security protections, such as MFA policies. Reduce risk of unauthorized users installing malicious applications into the tenant by ensuring that only specific privileged users can register applications.
- *Last modified:* June 2023

6.1.2 MS.AAD.5.2v1

Only administrators SHALL be allowed to consent to applications.

- *Rationale:* Limiting applications consent to only specific privileged users reduces risk of users giving insecure applications access to their data via consent grant attacks.
- *Last modified:* June 2023

6.1.3 MS.AAD.5.3v1

An admin consent workflow SHALL be configured for applications.

- *Rationale:* Configuring an admin consent workflow reduces the risk of the previous policy by setting up a process for users to securely request access to applications necessary for business purposes. Administrators have the opportunity to review the permissions requested by new applications and approve or deny access based on a risk assessment.
- *Last modified:* June 2023

6.1.4 MS.AAD.5.4v1

Group owners SHALL NOT be allowed to consent to applications.

- *Rationale:* In M365, group owners and team owners can consent to applications accessing data in the tenant. By requiring consent requests to go through an approval workflow, risk of exposure to malicious applications is reduced.
- *Last modified:* June 2023

6.2 RESOURCES

- Restrict Application Registration for Non-Privileged Users
- Enforce Administrators to Provide Consent for Apps Before Use
- Configure the admin consent workflow

6.3 LICENSE REQUIREMENTS

- N/A

6.4 IMPLEMENTATION

6.4.1 MS.AAD.5.1v1 Instructions

1. In Azure Active Directory, under Manage, select Users.
2. Select User settings.
3. For Users can register applications, select No.
4. Click Save.

6.4.2 MS.AAD.5.2v1 Instructions

1. In Azure Active Directory, under Manage, select Enterprise Applications.
2. Under Security, select Consent and permissions. Then select User Consent Settings.
3. Under User consent for applications, select Do not allow user consent.
4. Click Save.

6.4.3 MS.AAD.5.3v1 Instructions

1. In Azure Active Directory, create a new Azure AD Group that contains admin users responsible for reviewing and adjudicating application consent requests. Group members will be notified when users request consent for new applications.
2. Then in Azure Active Directory, under Manage, select Enterprise Applications.
3. Select Admin consent settings.
4. Under Admin consent requests > Users can request admin consent to apps they are unable to consent to, select Yes.
5. Under Who can review admin consent requests, select the group responsible for reviewing and adjudicating app requests (created in step one above).
6. Click Save.

6.4.4 MS.AAD.5.4v1 Instructions

1. In Azure Active Directory, under Manage, select Enterprise Applications.
2. Under Security, select Consent and permissions. Then select User Consent Settings.
3. Under Group owner consent for apps accessing data, select Do not allow group owner consent.
4. Click Save.

7. PASSWORDS

This section provides policies that reduce security risks associated with legacy password practices.

7.1 POLICIES

7.1.1 MS.AAD.6.1v1

User passwords SHALL NOT expire.

- *Rationale:* The National Institute of Standards and Technology (NIST), OMB, and Microsoft have published guidance indicating mandated periodic password changes make user accounts less secure. For example, OMB M-22-09 states, "Password policies must not require use of special characters or regular rotation."
- *Last modified:* June 2023

7.2 RESOURCES

- Password expiration requirements for users
- Eliminate bad passwords using Microsoft Entra Password Protection
- NIST Special Publication 800-63B - Digital Identity Guidelines

7.3 LICENSE REQUIREMENTS

- N/A

7.4 IMPLEMENTATION

7.4.1 MS.AAD.6.1v1 Instructions

1. Configure the Password expiration policy to Set passwords to never expire.

8. HIGHLY PRIVILEGED USER ACCESS

This section provides policies that help reduce security risks related to the usage of highly privileged Azure AD built-in roles. Privileged administrative users have access to operations that can undermine the security of the tenant by changing configurations and security policies. Special protections are necessary to secure this level of access.

Some of the policy implementations in this section reference specific features of the Azure AD Privileged Identity Management (PIM) service that provides Privileged Access Management (PAM) capabilities. As an alternative to Azure AD PIM, third-party products and services with equivalent PAM capabilities can be leveraged.

8.1 POLICIES

8.1.1 MS.AAD.7.1v1

A minimum of two users and a maximum of eight users SHALL be provisioned with the Global Administrator role.

- *Rationale:* The Global Administrator role provides unfettered access to the tenant. Limiting the number of users with this level of access makes tenant compromise more challenging. Microsoft recommends fewer than five users in the Global Administrator role. However, additional user accounts, up to eight, may be necessary to support emergency access and some operational scenarios.
- *Last modified:* June 2023

8.1.2 MS.AAD.7.2v1

Privileged users SHALL be provisioned with finer grained roles instead of Global Administrator.

- *Rationale:* Many privileged administrative users do not need unfettered access to the tenant to perform their duties. By assigning them to roles based on least privilege, the risks associated with having their accounts compromised are reduced.
- *Last modified:* June 2023

8.1.3 MS.AAD.7.3v1

Privileged users SHALL be provisioned cloud-only accounts separate from an on-premises directory or other federated identity providers.

- *Rationale:* By provisioning cloud-only Azure AD user accounts to privileged users, the risks associated with a compromise of on-premises federation infrastructure are reduced. It is more challenging for the adversary to pivot from the compromised environment to the cloud with privileged access.
- *Last modified:* June 2023

8.1.4 MS.AAD.7.4v1

Permanent active role assignments SHALL NOT be allowed for highly privileged roles.

- *Rationale:* Instead of giving users permanent assignments to privileged roles, provisioning access just in time lessens exposure if those accounts become compromised. In Azure AD PIM or an alternative PAM system, just in time access can be provisioned by assigning users to roles as eligible instead of perpetually active.
- *Last modified:* June 2023
- Note: Exceptions to this policy are:
  - Emergency access accounts that need perpetual access to the tenant in the rare event of system degradation or other scenarios.
  - Some types of service accounts that require a user account with privileged roles; since these accounts are used by software programs, they cannot perform role activation.

8.1.5 MS.AAD.7.5v1

Provisioning users to highly privileged roles SHALL NOT occur outside of a PAM system.

- *Rationale:* Provisioning users to privileged roles within a PAM system enables enforcement of numerous privileged access policies and monitoring. If privileged users are assigned directly to roles in the M365 admin center or via PowerShell outside of the context of a PAM system, a significant set of critical security capabilities are bypassed.
- *Last modified:* June 2023

8.1.6 MS.AAD.7.6v1

Activation of the Global Administrator role SHALL require approval.

- *Rationale:* Requiring approval for a user to activate Global Administrator, which provides unfettered access, makes it more challenging for an attacker to compromise the tenant with stolen credentials and it provides visibility of activities indicating a compromise is taking place.
- *Last modified:* June 2023

8.1.7 MS.AAD.7.7v1

Eligible and Active highly privileged role assignments SHALL trigger an alert.

- *Rationale:* Closely monitor assignment of the highest privileged roles for signs of compromise. Send assignment alerts to enable the security monitoring team to detect compromise attempts.

- *Last modified:* June 2023

8.1.8 MS.AAD.7.8v1

User activation of the Global Administrator role SHALL trigger an alert.

- *Rationale:* Closely monitor activation of the Global Administrator role for signs of compromise. Send activation alerts to enable the security monitoring team to detect compromise attempts.
- *Last modified:* June 2023
- *Note:* Prioritize user activation of Global Administrator as one of the most important events for monitoring and response.

8.1.9 MS.AAD.7.9v1

User activation of other highly privileged roles SHOULD trigger an alert.

- *Rationale:* Closely monitor activation of high-risk roles for signs of compromise. Send activation alerts to enable the security monitoring team to detect compromise attempts. In some environments, activating privileged roles can generate a significant number of alerts.
- *Last modified:* June 2023

8.2 RESOURCES

- Limit the number of Global Administrators to less than 5
- Implement Privilege Access Management
- Assign Microsoft Entra roles in Privileged Identity Management
- Approve or deny requests for Microsoft Entra roles in Privileged Identity Management
- Configure security alerts for Microsoft Entra roles in Privileged Identity Management

8.3 LICENSE REQUIREMENTS

- Azure AD PIM requires a Microsoft Entra ID P2 license.

8.4 IMPLEMENTATION

The following implementation instructions that reference the Azure AD PIM service will vary if using a third-party PAM system instead. Additionally, the implementation instructions associated with assigning roles to users will be revised in an upcoming release to incorporate functionality provided by the Azure AD PIM for Groups feature.

8.4.1 MS.AAD.7.1v1 Instructions

1. In Azure Active Directory, select Roles and administrators.
2. Select the Global Administrator role.
3. Under Manage, select Assignments.
4. Validate that between two to eight users are listed.
5. If you have Azure AD PIM, count the number of users in both the Eligible assignments and Active assignments tabs. There should be a total of two to eight users across both tabs (not individually). Do not count the same username twice. If any groups are listed, count the number of users who are members of the group and include it in the total count.

8.4.2 MS.AAD.7.2v1 Instructions

1. In Azure Active Directory, select Security.
2. Under Manage, select Identity Secure Score.
3. Click the Columns button, select all available columns and click Apply.

4. Review the score for the action named Use least privileged administrative roles.
5. Review the current score value and compare it to the max score. If the current score is not the maximum value and the status is not Completed, you must perform the improvement actions. In this case, follow the detailed action steps and check the score again after 48 hours to ensure compliance.

8.4.3 MS.AAD.7.3v1 Instructions

Performing a manual review of highly privileged users per the instructions below to determine which ones are not cloud-only is labor intensive; we recommend running the ScubaGear tool instead. ScubaGear will provide a list of the highly privileged users that are not cloud only.

1. Perform the steps below for each highly privileged role. We reference the Global Administrator role as an example.
2. In Azure Active Directory, select Roles and administrators.
3. Select the Global Administrator role.
4. Under Manage, select Assignments. If you have Azure AD PIM, repeat the steps below for both the Eligible and the Active assignments. If a group is listed, you will need to determine the members of the group and perform the steps for each group member.
5. For each highly privileged user, execute the PowerShell code below but replace the username@somedomain.com with the principal name of the user who is specific to your environment. You can get the data value from the Principal name field displayed in the Azure AD portal.

```
Connect-MgGraph
Select-Mgprofile beta
Get-MgUser -Filter "userPrincipalName eq 'username@somedomain.com'" | FL
```

6. Review the output field named OnPremisesImmutableId. If this field has a data value, it means that this specific user is not cloud only. If the user is not cloud only, create a cloud-only account for that user, assign the user to their respective roles, and then remove the account that is not cloud only from Azure AD.

8.4.4 MS.AAD.7.4v1 Instructions

1. In Azure Active Directory, select Roles and administrators. Perform the steps below for each highly privileged role. We reference the Global Administrator role as an example.
2. Select the Global Administrator role.
3. Under Manage, select Assignments, and click the Active assignments tab.
4. Verify there are no users or groups with a value of Permanent in the End time column. If there are any, recreate those assignments to have an expiration date using Azure AD PIM or an alternative PAM system. The only exception to this policy is emergency access accounts and service accounts that require perpetual active assignments. See policy MS.AAD.7.4v1 note section for details.

8.4.5 MS.AAD.7.5v1 Instructions

1. Perform the steps below for each highly privileged role. We reference the Global Administrator role as an example.
2. In Azure Active Directory, select Roles and administrators.
3. Select the Global Administrator role.
4. Under Manage, select Assignments. Repeat the steps below for both the Eligible and the Active Azure AD PIM assignments.
5. For each user or group listed, examine the value in the Start time column. If it contains a value of -, this indicates the respective user/group was assigned to that role outside of Azure AD PIM. If the role was assigned outside of Azure AD PIM, delete the assignment and recreate it using Azure AD PIM.

8.4.6 MS.AAD.7.6v1 Instructions

1. In Azure Active Directory, create a new group named Privileged Escalation Approvers. This group will contain users that will receive role activation approval requests and approve or deny them.
2. Assign this new group to the Azure AD role Privileged Role Administrators. This permission allows users in this group to adjudicate role activation approval requests.
3. Assign the users responsible for reviewing approval requests to the new Privileged Escalation Approvers group via the PIM for Groups feature.
4. In Azure AD Privileged Identity Management (PIM), under Manage, select Azure AD roles.
5. Under Manage, select Roles.
6. Select the Global Administrator role in the list.
7. Click Settings.
8. Click Edit.
9. Select the Require approval to activate option.
10. Click Select approvers and select the Privileged Escalation Approvers group; then click Select.
11. Click Update.

8.4.7 MS.AAD.7.7v1 Instructions

1. In Azure AD Privileged Identity Management (PIM), under Manage, select Azure AD roles.
2. Under Manage, select Roles. Perform the steps below for each highly privileged role. We reference the Global Administrator role as an example.
3. Click the Global Administrator role.
4. Click Settings and then click Edit.
5. Click the Notification tab.
6. Under Send notifications when members are assigned as eligible to this role, in the Role assignment alert > Additional recipients textbox, enter the email address of the security monitoring mailbox configured to receive privileged role assignment alerts.
7. Under Send notifications when members are assigned as active to this role, in the Role assignment alert > Additional recipients textbox, enter the email address of the security monitoring mailbox configured to receive privileged role assignment alerts.
8. Click Update.

8.4.8 MS.AAD.7.8v1 Instructions

1. In Azure AD Privileged Identity Management (PIM), under Manage, select Azure AD roles.
2. Under Manage, select Roles.
3. Click the Global Administrator role.
4. Click Settings and then click Edit.
5. Click the Notification tab.
6. Under Send notifications when eligible members activate this role, in the Role activation alert > Additional recipients textbox, enter the email address of the security monitoring mailbox configured to receive Global Administrator activation alerts.
7. Click Update.

8.4.9 MS.AAD.7.9v1 Instructions

Follow the same instructions as MS.AAD.7.8v1 above for each of the highly privileged roles (other than Global Administrator) but enter a security monitoring mailbox different from the one used to monitor Global Administrator activations.

9. GUEST USER ACCESS

This section provides policies that help reduce security risks related to integrating M365 guest users. A guest user is a specific type of external user who belongs to a separate organization but can access files, meetings, Teams, and other data in the target tenant. It is common to invite guest users to a tenant for cross-agency collaboration purposes.

9.1 POLICIES

9.1.1 MS.AAD.8.1v1

Guest users SHOULD have limited or restricted access to Azure AD objects.

- *Rationale:* Limiting the amount of object information available to guest users in the tenant, reduces malicious reconnaissance exposure, should a guest account become compromised or be created by an adversary.
- *Last modified:* June 2023

9.1.2 MS.AAD.8.2v1

Only users with the Guest Inviter role SHOULD be able to invite guest users.

- *Rationale:* By only allowing an authorized group of individuals to invite external users to create accounts in the tenant, an agency can enforce a guest user account approval process, reducing the risk of unauthorized account creation.
- *Last modified:* June 2023

9.1.3 MS.AAD.8.3v1

Guest invites SHOULD only be allowed to specific external domains that have been authorized by the agency for legitimate business purposes.

- *Rationale:* Limiting which domains can be invited to create guest accounts in the tenant helps reduce the risk of users from unauthorized external organizations getting access.
- *Last modified:* June 2023

9.2 RESOURCES

- Configure external collaboration settings
- Compare member and guest default permissions

9.3 LICENSE REQUIREMENTS

- N/A

9.4 IMPLEMENTATION

9.4.1 MS.AAD.8.1v1 Instructions

1. In Azure Active Directory, select External Identities > External collaboration settings.
2. Under Guest user access, select either Guest users have limited access to properties and memberships of directory objects or Guest user access is restricted to properties and memberships of their own directory objects (most restrictive).
3. Click Save.

9.4.2 MS.AAD.8.2v1 Instructions

1. In Azure Active Directory, select External Identities > External collaboration settings.
2. Under Guest invite settings, select Only users assigned to specific admin roles can invite guest users.
3. Click Save.

9.4.3 MS.AAD.8.3v1 Instructions

1. In Azure Active Directory, select External Identities > External collaboration settings.
2. Under Collaboration restrictions, select Allow invitations only to the specified domains (most restrictive).
3. Select Target domains and enter the names of the external domains authorized by the agency for guest user access.
4. Click Save.

APPENDIX A: HYBRID AZURE AD GUIDANCE

Most of this document does not focus on securing hybrid Azure AD environments. CISA released a separate Hybrid Identity Solutions Architecture document addressing the unique implementation requirements of hybrid Azure AD infrastructure.

APPENDIX B: CROSS-TENANT ACCESS GUIDANCE

Some of the conditional access policies contained in this security baseline, if implemented as described, will impact guest user access to a tenant. For example, the policies require users to perform MFA and originate from a managed device to gain access. These requirements are also enforced for guest users. For these policies to work effectively with guest users, both the home tenant (the one the guest user belongs to) and the resource tenant (the target tenant) may need to configure their Azure AD cross-tenant access settings.

Microsoft's Authentication and Conditional Access for External ID provides an understanding of how MFA and device claims are passed from the home tenant to the resource tenant. To configure the inbound and outbound cross-tenant access settings in Azure AD, refer to Microsoft's Overview: Cross-tenant access with Microsoft Entra External ID.