Microsoft Azure Active Directory

M365 Minimum Viable Secure Configuration Baseline

Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

V0.1	17 October 2022	Entire document	A	Initial Draft

Table of Contents

1. Introduction 1

1.1 Key Terminology 1

1.2 Assumptions 1

1.3 Common guidance 1

1.4 Resources 2

2. Baseline 2

2.1 Legacy Authentication SHALL Be Blocked 2

2.2 High Risk Users SHALL Be Blocked 3

2.3 High Risk Sign-ins SHALL Be Blocked 3

2.4 Phishing-Resistant Multifactor Authentication SHALL Be Required for All Users 4

2.5 Azure AD logs SHALL Be Collected 8

2.6 Only Administrators SHALL Be Allowed to Register Third-Party Applications 8

2.7 Non-admin Users SHALL Be Prevented from Providing Consent to Third-Party Applications 9

2.8 Passwords SHALL NOT Expire 10

2.9 Session Length SHALL Be Limited 10

2.10 Browser Sessions SHALL NOT Be Persistent 11

2.11 The Number of Users with the Highest Privilege Roles SHALL Be Limited 11

2.12 Highly Privileged User Accounts SHALL Be Cloud-Only 12

2.13 Multifactor Authentication SHALL Be Required for Highly Privileged Roles 13

2.14 Users Assigned to Highly Privileged Roles SHALL NOT Have Permanent Permissions 14

2.15 Activation of Highly Privileged Roles SHOULD Require Approval 15

2.16 Highly Privileged Role Assignment and Activation SHALL Be Monitored 16

2.17 Managed Devices SHOULD Be Required for Authentication 18

2.18 Guest User Access SHOULD Be Restricted 19

3. Acknowledgements 20

Appendix A. Hybrid Azure AD Guidance A-1

This page is intentionally blank.

1. Introduction

1.1 Key Terminology

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

Hybrid Azure Active Directory (AD) – This term denotes the scenario when an organization has an on-premises AD domain that contains the master user directory but federates access to the cloud Microsoft 365 (M365) Azure AD tenant.

Resource Tenant – In scenarios where external users are involved (e.g., guest users), the resource tenant hosts the M365 resources being used.

Home Tenant – In scenarios where external users are involved, the home tenant is the one that owns the external user's (e.g., guest) account.

1.2 Assumptions

The agency has created emergency access accounts in Azure AD and implemented strong security measures to protect the credentials of those accounts. Once created, those accounts should be placed into a group named "Emergency Users" or a similar name. Throughout Microsoft's instructions, this entity is referred to as "emergency access or break-glass accounts." Use the following Microsoft guidance to create and manage emergency access accounts.

Manage emergency access accounts in Azure AD

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

1.3 Common Guidance

1.3.1 Conditional Access Policies

This section provides common guidance that should be applied when implementing baseline instructions related to Azure AD Conditional Access policies.

As described in Microsoft's instructions and examples related to conditional access policies, Cybersecurity and Infrastructure Security Agency (CISA) recommends setting a policy to **Report-only** when it is created and then performing thorough hands-on testing to ensure that there are no unintended consequences before toggling the policy from **Report-only** to **On**. One tool that can assist with running test simulations is the What If tool. Microsoft also describes Conditional Access insights and reporting features that can assist with testing.

1.3.2 Azure AD Privileged Identity Management

Some of the guidance in this baseline document leverages specific features of the Azure AD Privileged Identity Management (PIM) service to demonstrate how to improve the security of highly privileged Azure AD roles. The PIM service provides what is referred to as "Privileged Access Management (PAM)" capabilities in industry. As an alternative to Azure AD PIM, there are third-party vendors that provide products or services with privileged access management capabilities that can be leveraged if an agency chooses to do so.

1.4 Resources

License Compliance and Copyright

Portions of this document are adapted from documents in Microsoft's Microsoft 365 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. Source documents 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.

2. Baseline

2.1 Legacy Authentication SHALL Be Blocked

Block legacy authentication protocols using a conditional access policy. Legacy authentication does not support multifactor authentication (MFA), which is required to minimize the impact of user credential theft.

2.1.1 Policy

- Legacy authentication SHALL be blocked.

2.1.2 Resources

- Conditional Access: Block Legacy Authentication
- Five steps to securing your identity infrastructure

2.1.3 License Requirements

- N/A

2.1.4 Implementation

1. Before blocking legacy authentication across the entire application base, follow these instructions to determine if any of the agency's existing applications are presently using legacy authentication. This helps develop a plan to address policy impacts.
2. Follow the instructions on this page to block legacy authentication. **Note:** The instructions suggest using Report-only mode which will not block legacy authentication.

2.2 High Risk Users SHALL Be Blocked

Azure AD Identity Protection uses various signals to detect the risk level for each user and determine if an account has likely been compromised. Users who are determined to be high risk are to be blocked from accessing the system via Conditional Access until an administrator remediates their account. Once a respective conditional access policy with a block is implemented, if a high-risk user attempts to login, the user will receive an error message with instructions to contact the administrator to re-enable their access.

2.2.1 Policy

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

2.2.2 Resources

- Conditional Access: User risk-based Conditional Access
- User-linked detections
- Simulating risk detections in Identity Protection
- User experiences with Azure AD Identity Protection (Examples of how these policies are applied in practice)
- Five steps to securing your identity infrastructure

2.2.3 License Requirements

- Requires an AAD P2 [Azure Active Directory] license.

2.2.4 Implementation

Policy #1:

1. To create the conditional access policy that implements the block for users at the risk level of High, follow the instructions in the Enable with Conditional Access policy section, but set the policy to block access as follows:
2. Under **Access Controls** -> **Grant**, select **Block access**.

Policy #2:

1. Follow the instructions in the Configure users at risk detected alerts section to configure Azure AD Identity Protection to email the security operations team/administrator when a user account is determined to be high risk so that they can review and respond to threats.

2.3 High Risk Sign-ins SHALL Be Blocked

Azure AD Identity Protection uses various signals to detect the risk level for each user sign-in. Sign-ins detected as high risk are to be blocked via Conditional Access.

2.3.1 Policy

Sign-ins detected as high risk SHALL be blocked.

2.3.2 Resources

- Conditional Access: Sign-in risk-based Conditional Access

- Sign-in risk
- Simulating risk detections in Identity Protection
- User experiences with Azure AD Identity Protection (Examples of how these policies are applied in practice)

2.3.3 License Requirements

- Requires an AAD P2 license.

2.3.4 Implementation

To create the conditional access policy that implements the block for sign-ins at the risk level of **High**, follow the instructions in the Enable with Conditional Access policy section, but set the risk level to **High** and block access.

1. Under **Select the sign-in risk level this policy will apply to**, select **High.**
2. Under **Access Controls** -> **Grant**, select **Block access.**

Note: If after implementing this, it is observed that numerous legitimate user sign-ins are consistently being blocked due to their location being interpreted as suspicious and this creates an operational burden on the agency, then a Trusted Location can be configured in the Conditional Access blade for each of the legitimate sign-in locations. Azure AD Identity Protection considers the Trusted Location data when it calculates sign-in risk, and this may help to prevent users signing in from legitimate locations from being flagged as high risk.

2.4 Phishing-Resistant Multifactor Authentication SHALL Be Required for All Users

Phishing-resistant multifactor authentication protects against sophisticated phishing attacks. Recognizing the significant risk these attack present, the Office of Management and Budget (OMB), requires federal agencies to implement phishing-resistant authentication.

However, phishing-resistant MFA may not always be immediately available, especially on mobile devices. Where phishing-resistant MFA is not yet available, organization should adopt an MFA method from the list below. Organizations must upgrade to a phishing-resistant MFA method as soon as possible to become compliant with this policy and address the critical security threat posed by modern phishing attacks.

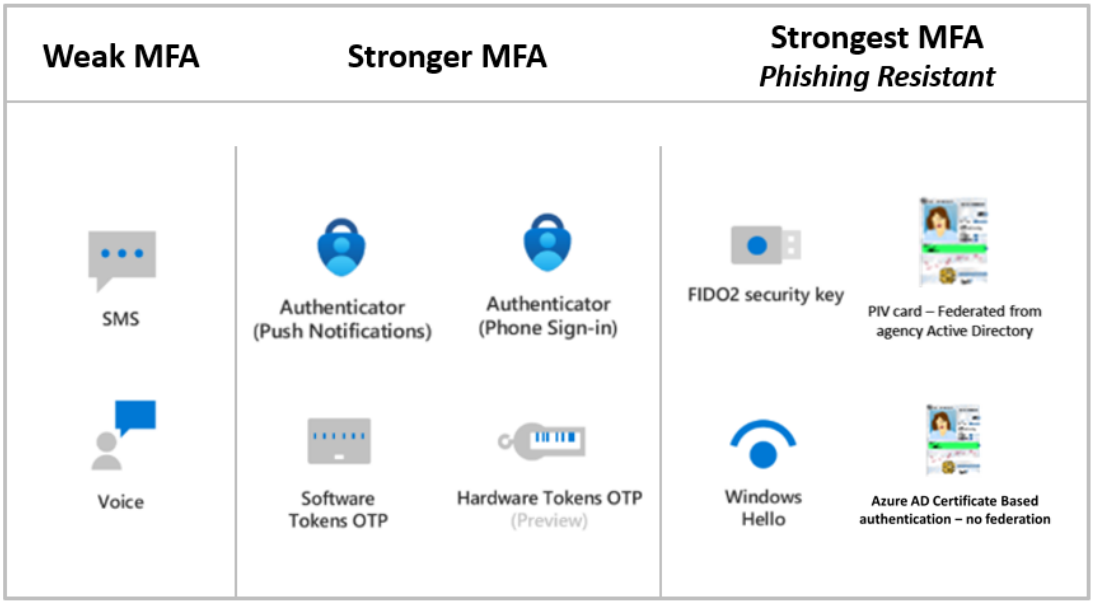
Weak MFA
Stronger MFA
Strongest MFA
Phishing Resistant
SMS
Voice
Authenticator (Push Notifications)
Authenticator (Phone Sign-in)
Software Tokens OTP
Hardware Tokens OTP (Preview)
FIDO2 security key
PIV card – Federated from agency Active Directory
Windows Hello
Azure AD Certificate Based authentication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

Figure 1: Options for Weak MFA, Stronger MFA Options, and Strongest MFA

Note: Figure adapted from MS Build Page article (12/29/2021).

2.4.1 Policy

- MFA SHALL be required for all users.
- Phishing-resistant MFA SHALL be used for all users.
    - Phishing-resistant methods:
        - Federal Personal Identity Verification (PIV) card (Azure AD Certificate-Based authentication [CBA]).
        - FIDO2 Security Key.
        - Windows Hello for Business.
        - Federal PIV card (Federated from agency Active Directory or other identity provider).
- If phishing-resistant MFA cannot be used, an MFA method from the list below SHALL be used in the interim:
    - Microsoft Authenticator (Push Notifications).
    - Microsoft Authenticator (Phone Sign-in) (Also referred to as Passwordless Sign-in).
        - When using Microsoft Authenticator:
            - Number Matching SHALL be enabled.
            - Additional Context SHALL be enabled.
    - Software Tokens One-Time Password (OTP) – This option is commonly implemented using mobile phone authenticator apps.
    - Hardware tokens OTP.
- SMS or Voice as the MFA method SHALL NOT be used.

2.4.2 Resources

- What authentication and verification methods are available in Azure Active Directory?
- Use number matching in multifactor authentication (MFA) notifications (Preview) - Azure Active Directory - Microsoft Entra | Microsoft Docs
- Use additional context in Microsoft Authenticator notifications (Preview) - Azure Active Directory - Microsoft Entra | Microsoft Docs
- M-22-09 Federal Zero Trust Strategy

2.4.3 License Requirements

- N/A

2.4.4 Implementation

Policy #1:

1. Follow these instructions to create a conditional access policy that requires all users to authenticate with MFA.

Policy #2:

Use the following instructions to configure a phishing-resistant MFA method for users with highly privileged roles. If the agency is configuring a phishing-resistant MFA method for all users, then the instructions in this section also apply, but set the **Target** to **All Users** instead of a specific group in the respective configuration screens.

CISA recommends placing highly privileged users into an Azure AD group named “Highly Privileged Admins” or an equivalent and then referencing the group in the MFA configuration. Newly created, highly privileged users should be added to the group so they can register a phishing-resistant method. CISA does not recommend assigning MFA methods directly to individual users.

Select one of the following phishing-resistant MFA methods to configure:

FIDO2 Security Key

1. Follow the instructions at this link to configure FIDO2.
2. For **Enable**, select **Yes.**
3. For **Target**, select the **Highly Privileged Admins** group or an equivalent.

Certificate Based Authentication (CBA)

1. Follow the instructions at this link to configure CBA.
2. On the tenant, in the instructions section named **Enable CBA on the tenant** , under **Target**, select the **Highly Privileged Admins** group or an equivalent.

Windows Hello for Business

1. Follow the instructions at this link to configure Windows Hello for Business.

Policy #3:

If the agency is implementing a phishing-resistant MFA method for all users, follow the instructions in the previous section. Otherwise, use the following instructions to configure a non-phishing resistant MFA method for users that are not in highly privileged roles.

Microsoft Authenticator (Phone Sign-in) (Also referred to as Passwordless Sign-in) or Microsoft Authenticator (Push Notifications)

1. In the Azure Portal navigate to **Azure Active Directory.**
2. Select **Security.**
3. Select **Manage** -> **MFA.**
4. Under **Configure,** select **Additional cloud-based MFA settings.**
5. Under **verification options**, select **Notification through mobile app.**
6. If desired, to enforce Microsoft Authenticator app usage and disable third party authenticator apps usage, make sure that **Verification code from mobile app** or **hardware token** is not selected.
7. Click **Save.**
8. Go back to the **Azure Active Directory** home tab and select **Security**.
9. Select **Authentication Methods**.
10. In the **Policies** window, select **Microsoft Authenticator**.
11. For **Enable**, select **Yes**.
12. For **Target**, select **All users**.
13. In the row for the **All users**, click the … -> **Configure.**
14. If configuring Phone Sign-in (aka Passwordless Sign-in), for **Authentication mode**, select **Passwordless**. If configuring Push Notifications, for **Authentication mode**, select **Push**. If configuring the usage of both, for **Authentication mode**, select **Any**.
    a. For **Require number matchin**g, select **Enabled**.
    b. For **Show additional context in notifications**, select **Enabled**.
15. Select **Done**.
16. Click **Save**.

Software Tokens OTP or Hardware Tokens OTP

1. In the **Azure Portal**, navigate to **Azure Active Directory**.
2. Select **Security**.
3. Select **Manage** -> **MFA**.
4. Under **Configure**, select **Additional cloud-based MFA setting**s.
5. Under **verification options**, select **Verification code from mobile app** or **hardware token**.
6. If configuring Hardware Tokens OTP, follow the additional steps at this link when provisioning a user.

Policy #4:

1. In the **Azure Portal,** navigate to **Azure Active Directory**.
2. Select **Security**.
3. Select **Manage** -> **MFA**.
4. Under **Configure**, select **Additional cloud-based MFA settings**.

5. Under **verification options**, make sure that **Text message to phone** and **Call to phone** are **disabled**.

2.5 Azure AD Logs SHALL Be Collected

Configure Azure AD to send critical logs to the agency's centralized SIEM [security information and event management] and to CISA's central analysis system so that they can be audited and queried. Configure Azure AD to send logs to a storage account and retain them for when incident response is needed.

2.5.1 Policy

- The following critical logs SHALL be sent at a minimum: AuditLogs, SignInLogs, RiskyUsers, UserRiskEvents, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, ADFSSignInLogs, RiskyServicePrincipals, and ServicePrincipalRiskEvents.
  - If managed identities are used for Azure resources, also include the ManagedIdentitySignInLogs log type.
  - If the Azure AD Provisioning Service is used to provision users to software-as-a-service apps or other systems, also include the ProvisioningLogs log type.
- The logs SHALL be sent to the agency's security operations center [SOC] for monitoring.

2.5.2 Resources

- Everything you wanted to know about Security and Audit Logging in Office 365
- Sign-in logs in Azure Active Directory - preview
- National Cybersecurity Protection System-Cloud Interface Reference Architecture Volume 1
- National Cybersecurity Protection System - Cloud Interface Reference Architecture Volume 2

2.5.3 License Requirements

- N/A

2.5.4 Implementation

Follow these instructions to configure sending the logs to a storage account:

1. From the **Diagnostic settings** page, click **Add diagnostic** setting.
2. Select the specific logs mentioned in the previous policy section.
3. Under **Destination Details,** select the **Archive to a storage account** check box and select the storage account that was specifically created to host security logs.
4. In the **Retention** field enter "365" days.

2.6 Only Administrators SHALL Be Allowed to Register Third-Party Applications

Ensure that only administrators can register third-party applications that can access the tenant.

2.6.1 Policy

- Only administrators SHALL be allowed to register third-party applications.

2.6.2 Resources

- Restrict Application Registration for Non-Privileged Users.

2.6.3 License Requirements

- N/A

2.6.4 Implementation

1. In the **Azure Portal**, navigate to **Azure Active Directory.**
2. Under **Manage**, select **Users**.
3. Select **User settings**.
4. Under **App Registrations** -> **Users can register applications**, select **No.**
5. Click **Save**.

2.7 Non-admin Users SHALL Be Prevented from Providing Consent to Third-Party Applications

Ensure that only administrators can consent to third-party applications and only administrators can control which permissions are granted. An admin consent workflow can be configured in Azure AD; otherwise, users will be blocked when they try to access an application that requires permissions to access organizational data. Develop a process for approving and managing third-party applications.

2.7.1 Policy

- Only administrators SHALL be allowed to consent to third-party applications.
- An admin consent workflow SHALL be configured.
- Group owners SHALL NOT be allowed to consent to third-party applications.

2.7.2 Resources

- Enforce administrators to provide consent for apps before use.
- Configure the admin consent workflow.

2.7.3 License Requirements

- N/A

2.7.4 Implementation

1. In the **Azure Portal**, navigate to **Azure Active Directory.**
2. Create a new Azure AD Group that contains admin users responsible for reviewing and adjudicating app requests.
3. Under **Manage**, select **Enterprise Applications.**
4. Under **Security**, select **Consent and permissions.**

5. Under **User consent for applications**, select **Do not allow user consent.**
6. Under **Group owner consent for apps accessing data**, select **Do not allow group owner consent.**
7. In the menu, navigate back to **Enterprise Applications**.
8. Under **Manage**, select **User Settings**.
9. Under **Admin consent requests** -> **Users can request admin consent to apps they are unable to consent to**, select **Yes.**
10. Under **Who can review admin consent requests**, select the group created in step two that is responsible for reviewing and adjudicating app requests.
11. Click **Save.**

2.8 Passwords SHALL NOT Expire

Ensure that user passwords do not expire. Both the National Institute of Standards and Technology (NIST) and Microsoft emphasize MFA because they indicate that mandated password changes make user accounts less secure.

2.8.1 Policy

- User passwords SHALL NOT expire.

2.8.2 Resources

- Password policy recommendations - Microsoft 365 admin | Microsoft Docs.
- Eliminate bad passwords using Azure Active Directory Password Protection.
- NIST Special Publication 800-63B - Digital Identity Guidelines.

2.8.3 License Requirements

- N/A

2.8.4 Implementation

Follow the instructions at this link to configure the password expiration policy.

2.9 Session Length SHALL Be Limited

To reduce the risk of credential theft during user sessions, configure the sign-in frequency to a limited period of time.

2.9.1 Policy

- Sign-in frequency SHALL be configured to 12 hours.

2.9.2 Resources

- Configure authentication session management with Conditional Access.
- NIST Special Publication 800-63B - Digital Identity Guidelines.

2.9.3 License Requirements

- N/A

2.9.4 Implementation

Follow the instructions at this link to implement the conditional access policy that configures the sign-in frequency,

1. Set the **Users** or **workload identities** to include **All users.**
2. Set the **Cloud apps or actions** to include **All cloud apps.**
3. Set the **Access Controls** -> **Session** -> **Sign-in frequency** to a value of “12 hours.”

2.10 Browser Sessions SHALL NOT Be Persistent

To reduce the risk of credential theft during user sessions, disallow persistent browser sessions.

2.10.1 Policy

- Browser sessions SHALL not be persistent.

2.10.2 Resources

- Configure authentication session management with Conditional Access.
- NIST Special Publication 800-63B - Digital Identity Guidelines.

2.10.3 License Requirements

- N/A

2.10.4 Implementation

Follow the instructions at this link to implement the conditional access policy that prevents persistent browser sessions.

1. Set the **Users or workload identities** to **include All users.**
2. Set the **Cloud apps or actions** to include **All cloud apps.**
3. Set the **Access Controls** -> **Session** -> **Persistent browser session** to **Never persistent.**

2.11 The Number of Users with the Highest Privilege Roles SHALL Be Limited

Global Administrator is the highest privileged role in Azure AD because it provides unfettered access to the tenant. Therefore, if a user’s credential with these permissions were to be compromised, it would present grave risks to the security of the tenant. Limit the number of users that are assigned the role of Global Administrator. Assign users to finer-grained administrative roles that they need to perform their duties instead of being assigned the Global Administrator role.

2.11.1 Policy

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

2.11.2 Resources

- Best practices for Azure AD roles (Limit number of Global Administrators to less than 5)

- About admin roles

2.11.3 License Requirements

- N/A

2.11.4 Implementation

Policy bullet #1:

1. In the **Azure Portal**, navigate to **Azure Active Directory.**
2. Select **Roles and administrators.**
3. Select the **Global administrator role.**
4. Under **Manage**, select **Assignments.**
5. Validate that between two to four users are listed.
    a. For those who have Azure AD PIM, they will need to check both the **Eligible assignments** and **Active assignments** tabs. There should be a total of two to four users across both of these tabs (not individually).
    b. If any groups are listed, need to check how many users are members of each group and include that in the total count.

Policy bullet #2:

1. In the **Azure Portal**, navigate to **Azure Active Directory.**
2. Select **Security.**
3. Under **Manage**, select **Identity Secure Score.**
4. Click the **Columns** button and ensure that all the available columns are selected to display and click A**pply.**
5. Review the score for the action named **Use limited administrative roles.**
6. Ensure that the maximum score was achieved, and that the status is **Completed.**
7. If the maximum score was not achieved, click the **Improvement action** and Microsoft provides a pop-up page with detailed instructions on how to address the weakness. In short, to address the weakness, assign users to finer grained roles (e.g., SharePoint Administrator, Exchange Administrator) instead of Global Administrator. Only the minimum number of users necessary should be assigned to Global Administrator. Once the roles are reassigned according to the guidance, check the score again after 48 hours to ensure compliance.

2.12 Highly Privileged User Accounts SHALL Be Cloud-Only

Assign users that need to perform highly privileged tasks to cloud-only Azure AD accounts to minimize the collateral damage of an on-premises identity compromise.[1]

[1] "Cloud-only" user accounts have no ties to the on-premises AD and are not federated—they are local to Azure AD only.

2.12.1 Policy

- Users that need to be assigned to highly privileged Azure AD roles SHALL be provisioned cloud-only accounts that are separate from the on-premises directory or other federated identity providers.
- The following built-in Azure AD roles are considered highly privileged at a minimum. Additional built-in roles that are considered highly privileged in the agency's environment can be added to this list:
  - Global Administrator
  - Privileged Role Administrator
  - User Administrator
  - SharePoint Administrator
  - Exchange Administrator
  - Hybrid Identity Administrator
  - Application Administrator
  - Cloud Application Administrator

2.12.2 Resources

- Securing privileged access for hybrid and cloud deployments in Azure AD

2.12.3 License Requirements

- N/A

2.12.4 Implementation

Review these instructions to identify users assigned to highly privileged roles and verify the account does not exist outside Azure AD.

2.13 Multifactor Authentication SHALL Be Required for Highly Privileged Roles

Require users to perform MFA to access highly privileged roles. This configuration provides a backup policy to enforce MFA for highly privileged users in case the main conditional access policy—which requires MFA for all users—is disabled or misconfigured.

2.13.1 Policy

- MFA SHALL be required for user access to highly privileged roles.
  - Refer to the baseline statement Highly Privileged User Accounts SHALL be Cloud-Only for a recommended minimum list of Azure AD built-in roles that are considered highly privileged. It is also possible to designate additional built-in roles that are considered highly privileged in the agency's environment based on its risk tolerance.

2.13.2 Resources

- Five steps to securing your identity infrastructure
- M-22-09 Federal Zero Trust Strategy

2.13.3 License Requirements

- N/A

2.13.4 Implementation

Follow these instructions to create a conditional access policy requiring MFA for access, but under **Assignments,** use the following tailored steps to scope the policy to privileged roles.

1. Under **Assignments**, select **Users and groups.**

   a. Under **Include**, choose **Select users and groups**, then click the **Directory roles** checkbox. Select each of the roles listed in the baseline statement, Highly Privileged User Accounts SHALL be Cloud-Only.

      Under **Exclude**, follow Microsoft's guidance from the previously provided instructions link.

2.14 Users Assigned to Highly Privileged Roles SHALL NOT Have Permanent Permissions

Do not assign users to highly privileged roles using permanent active role assignments. Instead, assign users to eligible role assignments in a PAM system and provide an expiration period for active assignments requiring privileged users to reactivate their highly privileged roles upon expiration.

Note: Although Azure AD PIM is referenced in the implementation instructions, an equivalent third-party PAM service may be used instead.

2.14.1 Policy

- Permanent active role assignments SHALL NOT be allowed for highly privileged roles. Active assignments SHALL have an expiration period.
  - Refer to the baseline statement, Highly Privileged User Accounts SHALL be Cloud-Only, for a recommended minimum list of Azure AD built-in roles that are considered highly privileged. It is also possible to designate additional built-in roles that are considered highly privileged in the agency's environment based on its risk tolerance.
- Provisioning of users to highly privileged roles SHALL NOT occur outside of a PAM system, such as the Azure AD PIM service, because this bypasses the controls the PAM system provides.

2.14.2 Resources

- Assign Azure AD roles in Privileged Identity Management

2.14.3 License Requirements

- Use of an Azure AD PIM or an equivalent third-party PAM service.
- Azure AD PIM requires an AAD P2 license.

2.14.4 Implementation

Note: Any parts of the following implementation instructions that reference the Azure AD PIM service will vary if using a third-party PAM system.

1. In the **Azure Portal**, navigate to **Azure AD Privileged Identity Management (PIM).**
2. Under **Manage**, select **Azure AD roles.**
3. Under **Manage**, select **Roles.** This should bring up a list of all the Azure AD roles managed by the PIM service.

4. **Note**: This step is specific to the first policy bullet. Repeat this step and step 5 for each highly privileged role referenced in the policy section. The role "Global Administrator" is used as an example in these instructions.
   a. Click the **Global Administrator** role in the list.
   b. Click **Settings**.
   c. Click **Edit.**
   d. Select the **Assignment** tab.
   e. De-select the option named **Allow permanent active assignment.**
   f. Under **Expire active assignments after**, select **15 days**.
   g. Click **Update.**
5. Note: This step is specific to the second policy bullet.
   a. While on the **Assignments** page for the role, select the **Active Assignments** tab.
   b. Review the assignments list. If any of the assignments show a **Start time** of "-" (i.e., empty start time) and of **End time** of **Permanent**, then those role assignments were made outside of the PIM service and therefore are out of compliance with the policy.
   c. Delete the non-compliant role assignments and then recreate them using the PIM service.
6. In addition to checking for permanent assignments using the PIM Assignments page in step #5, PIM also provides a report that lists all role assignments that were performed outside of PIM so that those assignments can be deleted and properly recreated using PIM.
   a. From the **PIM landing page**, under **Manage**, select **Azure AD roles.**
   b. Under **Manage**, select **Alerts.**
   c. Click the **Scan** button and wait for the scan to complete.
   d. If there were any roles assigned outside of PIM, the report will display an alert named, **Roles are being assigned outside of Privileged Identity Management**; Click that alert.
   e. PIM displays a list of users, their associated roles, and the date/time that they were assigned a role outside of PIM: Delete the non-compliant role assignments and then recreate them using the PIM service.

2.15 Activation of Highly Privileged Roles SHOULD Require Approval

Require approval for a user to activate a highly privileged role, such as Global Administrator. This makes it more challenging for an attacker to leverage the stolen credentials of highly privileged users and ensures that privileged access is monitored closely.

Note: Although Azure AD PIM is referenced in the implementation instructions, an equivalent third-party PAM service may be used instead.

2.15.1 Policy

- Activation of highly privileged roles SHOULD require approval.

  - Refer to the baseline statement Highly Privileged User Accounts SHALL be Cloud-Only for a list of Azure AD built-in roles that are considered highly privileged. It is also possible to configure additional built-in roles that are considered highly privileged in the agency's environment based on its risk tolerance.

2.15.2 Resources

- Approve or deny requests for Azure AD roles in Privileged Identity Management

2.15.3 License Requirements

- Use an Azure AD PIM or an equivalent third-party PAM service.
- Azure AD PIM requires an AAD P2 license.

2.15.4 Implementation

Note: Any parts of the following implementation instructions that reference the Azure AD PIM service will vary if using a third-party PAM system.

1. In the **Azure Portal**, navigate to **Azure AD** and 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. Users in this group must, at least, have the permissions provided to the Privileged Role Administrators role to adjudicate requests.
2. In the **Azure Portal**, navigate to **Azure AD Privileged Identity Management (PIM).**
3. Under **Manage**, select **Azure AD roles**.
4. Under **Manage**, select **Roles**. This should bring up a list of all the Azure AD roles managed by the PIM service.
5. Repeat this step for the Privileged Role Administrator role, User Administrator role, and other roles that the agency has designated as highly privileged.

   a. Click the **Global Administrator** role in the list.

   b. Click **Settings.**

   c. Click **Edit.**

   d. Select the **Require approval to activate** option.

   e. Click **Select approvers**, select the group **Privileged Escalation Approvers**, and then click **Select.**

   f. Click **Update.**

2.16 Highly Privileged Role Assignment and Activation SHALL Be Monitored

Since many cyberattacks leverage privileged access, it is imperative to closely monitor the assignment and activation of the highest privileged roles for signs of compromise. Create alerts to trigger when a highly privileged role is assigned to a user and when a user activates a highly privileged role.

Note: Although Azure AD PIM is referenced in the implementation instructions, an equivalent third-party PAM service may be used instead.

2.16.1 Policy

- Eligible and Active highly privileged role assignments SHALL trigger an alert.
  - Refer to the baseline statement Highly Privileged User Accounts SHALL be Cloud-Only for a recommended minimum list of Azure AD built-in roles that are considered highly privileged. It is also possible to designate additional built-in roles that are considered highly privileged in the agency's environment based on its risk tolerance.
- User activation of the Global Administrator role SHALL trigger an alert.
- User activation of other highly privileged roles SHOULD trigger an alert.
  - Note: Alerts can be configured for user activation of other highly privileged roles as well but note that if users activate these other roles frequently, it can prompt a significant number of alerts. Therefore, for those other roles, it might be prudent to set up a separate monitoring mailbox from the one configured for the alerts associated with the Global Administrator role. This separate mailbox would be designed to store alerts for "review as necessary" purposes versus the mailbox configured for the Global Administrator role, which should be monitored closely since that role is sensitive.

2.16.2 Resources

- Assign Azure AD roles in Privileged Identity Management

2.16.3 License Requirements

- Use an Azure AD PIM or an equivalent third-party PAM service.
- Azure AD PIM requires an AAD P2 license

2.16.4 Implementation

Note: Any parts of the following implementation instructions that reference the Azure AD PIM service will vary if using a third-party PAM system.

1. In the **Azure Portal**, navigate to **Azure AD Privileged Identity Management (PIM).**
2. Under **Manage**, select A**zure AD roles.**
3. Under **Manage**, select **Roles**. This should bring up a list of all the Azure AD roles managed by the PIM service.
4. Click the **Global Administrator** role.
5. Click **Settings** and then click **Edit.**
6. Click the **Notification** tab.
7. 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 mailbox configured to receive the alerts for this role.
8. Under S**end notifications when members are assigned as active to this role**, in the **Role assignment alert** -> **Additional recipients** textbox, enter the email address of the mailbox configured to receive the alerts for this role.

9. Under **Send notifications when eligible members activate this role**, in the **Role activation alert** -> **Additional recipients** textbox, enter the email address of the mailbox configured to receive the alerts for this role.
10. Click **Update**.
11. Repeat steps 4 through 10 for each of the other highly privileged roles referenced in the policy section above, with one modification:
    a. When configuring the **Send notifications when eligible members activate this role** for these other roles, enter an email address of a mailbox that is different from the one used to monitor Global Administrator activations.

2.17 Managed Devices SHOULD Be Required for Authentication

Require that users connect to M365 from a device that is managed using conditional access. Agencies that are implementing a hybrid Azure AD environment will likely use the conditional access control option named **Hybrid Azure AD joined**, whereas agencies that are using devices that connect directly to the cloud and do not join an on-premises AD will use the conditional access control option named, **Require device to be marked as compliant**.

Guest user access note: This conditional access policy will impact guest access to the tenant because guest users will be required to authenticate from a managed device similar to regular Azure AD users. For guest users, the organization that manages their home tenant is responsible for managing their devices and the resource tenant must be configured to trust the device claims from the home tenant, otherwise guest users will be blocked by the policy. This link describes the detailed authentication flow for guest users and how conditional access related to devices is applied. The implementation section describes the cross-tenant settings that must be configured in both the home and the resource tenants to facilitate guest access with managed devices.

2.17.1 Policy

- Managed devices SHOULD be required for authentication.

2.17.2 Resources

- Configure hybrid Azure AD join
- Azure AD joined devices
- Set up enrollment for Windows devices (for Intune)

2.17.3 License Requirements

- Use Microsoft Intune (if implementing the requirement for the device to be compliant).

2.17.4 Implementation

Follow these instructions to create a conditional access policy that requires the device to be either hybrid Azure AD joined or compliant during authentication.

Use the following instructions to facilitate guest access with managed devices. Although the agency implementing this baseline only controls the resource tenant and does not have control over the home tenant, CISA provides our recommended security configuration for the home tenant in this section.

1. Reference this link for a general description of cross-tenant access settings to become familiar with the terminology and configurations.
2. For the resource tenant, use the following steps (for demonstration purposes, the home tenant domain is named “home.onmicrosoft.com” — replace this name with the actual name of the tenant):
   a. Navigate to **Azure AD** -> **External Identities** -> **Cross-tenant access settings.**
      i. In **Organizational Settings**, add a new organization – “home.onmicrosoft.com”.
      ii. Open the **Inbound access** settings for the newly added organization.
      iii. Click the **B2B collaboration** tab. Under **External users and Groups** -> **Access status**, select **Allow access.**
      iv. Under **External users and Groups** -> **Applies to**, select **All external users and groups.**
      v. Click the **Trust settings** tab. Under **Customize settings** -> select **Trust multi-factor authentication from Azure AD tenants**, **Trust compliant devices,** and **Trust hybrid Azure AD joined devices**
3. For the home tenant, use the following steps (for demonstration purposes the resource tenant domain is named “resource.onmicrosoft.com” — replace this name with the actual name of the tenant):
   a. Navigate to **Azure AD** -> **External Identities** -> **Cross-tenant access settings.**
      i. In **Organizational Settings**, Add a new organization – “resource.onmicrosoft.com”.
      ii. Open the **Outbound access** settings for the newly added organization.
      iii. Click the **B2B collaboration** tab. Under **Users and Groups** -> **Access status**, select **Allow access.**
      iv. Under **Users and Groups** -> **Applies to**, select **All users.**

2.18 Guest User Access SHOULD Be Restricted

Ensure that only users with specific privileges can invite guest users to the tenant and that invites can only be sent to specific external domains. Ensure that guest users have limited access to Azure AD directory objects.

2.18.1 Policy

- Only users with the Guest Inviter role SHOULD be able to invite guest users.
- Guest invites SHOULD only be allowed to specific external domains that have been authorized by the agency for legitimate business purposes.
- Guest users SHOULD have limited access to Azure AD directory objects.

2.18.2 Resources

- Configure external collaboration settings

2.18.3 License Requirements

- N/A

2.18.4 Implementation

Follow these instructions to configure the Azure AD **External collaboration settings.**

1. Under **Guest user access**, select **Guest users have limited access to properties and memberships of directory objects.**
2. Under **Guest invite settings**, select **Only users assigned to specific admin roles can invite guest users.**
3. Under **Collaboration restrictions**, select **Allow invitations only to the specified domains (most restrictive).**

   b. Select **Target domains** and enter the names of the external domains that have been authorized by the agency for guest user access.

3. Acknowledgements

In addition to acknowledging the important contributions of a diverse team of CISA experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership
Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors
Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors
Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).

Appendix A. Hybrid Azure AD Guidance

Most of this document does not focus on securing hybrid Azure AD environments. CISA is working on a separate document that addresses the unique implementation requirements of hybrid Azure AD infrastructure, including the on-premises components. Meanwhile, the following limited set of hybrid Azure AD policies that include on-premises components are provided:

- Azure AD Password Protection SHOULD be implemented for the on-premises directory.
  - Enforce on-premises Azure AD Password Protection for Active Directory Domain Services
  - Plan and deploy on-premises Azure Active Directory Password Protection
- Password hash synchronization with the on-premises directory SHOULD be implemented.
  - Implement password hash synchronization with Azure AD Connect sync
- Service accounts created in Azure AD to support the integration of Azure AD Connect SHOULD be restricted to originate from the IP address space of the network hosting the on-premises AD. This can be implemented via a conditional access policy that is applied to the Azure AD Connect service accounts and blocks access except from a specific Azure AD Named Location that is configured with respective on-premises IP address range.
  - Using the location condition in a Conditional Access policy
  - Azure AD Connect: Accounts and permissions