

Celebal Technologies

Summer Internship – Final Assignment Submission

Department: Cloud Infrastructure & Security

Internship Duration: 19th May 2025 – 20th July 2025

Assignment Title

Azure Multifactor Authentication

Submitted by: Sanchit Mathur

Course: 5-Year Integrated M.Tech (CSE – Cyber Security)

Current Week: 8/12

Assignment: Week 8 Final Project

Submitted to:

Celebal Technologies – CSI Team

Submission Date: 10th July 2025

Portal: [CSI Dashboard – Cloud Infra & Security]

Project Reminder: Submitted before deadline (as per notice board)

Table of Contents

1. Configure & Manage Azure Multifactor Authentication (MFA).....	3
2. Two Factor Authentication.....	5
3. Different Methods of Two Factor Authentication	7
4. Setup Self-Service Password Reset.....	11
5. Configure MFA.....	14
6. Configure and Deploy Self-Service Password Reset	16
7. Implement and Manage Azure MFA Settings	19
8. Account Lockout.....	22
9. Manage MFA Settings for Users	25
10. Extend Azure AD MFA to Third Party and On-Premises Devices	28
11. Monitor Azure AD MFA Activity.....	32
12. OAuth Tokens	36
13 Conclusion	42
14 Screenshots	43

1. Configure & Manage Azure Multifactor Authentication (MFA)

Overview

Azure Multifactor Authentication (MFA) provides an additional layer of security by requiring users to provide two or more verification methods during sign-in. This significantly reduces the risk of account compromise even if passwords are stolen.

Prerequisites

- Azure AD Premium P1 or P2 license
- Global Administrator or Security Administrator role
- Azure portal access

Initial Setup Steps

Step 1: Access Azure Portal

1. Navigate to [Azure Portal](#)
2. Sign in with administrative credentials
3. Go to **Azure Active Directory > Security > MFA**

Step 2: Configure MFA Service Settings

1. In the Azure AD portal, navigate to **Security > Multifactor authentication**
2. Click on **Getting started**
3. Select **Configure MFA settings**
4. Configure the following settings:

- **App passwords:** Enable/disable based on organizational needs
- **Trusted IPs:** Define IP ranges that bypass MFA
- **Verification options:** Select available authentication methods
- **Remember MFA on trusted devices:** Configure duration (1-365 days)

Step 3: Enable MFA for Users

1. Navigate to **Users > All users**
2. Select **Per-user MFA** from the top menu
3. Select users and click **Enable** or **Enforce**
4. Configure bulk operations using CSV import if needed

Management Best Practices

- Start with a pilot group before organization-wide deployment
 - Use Conditional Access policies for more granular control
 - Regular review and update of MFA settings
 - Monitor MFA usage and user adoption rates
-

2. Two Factor Authentication

Concept and Implementation

Two-factor authentication (2FA) requires users to provide two different authentication factors:

1. **Something you know** (password, PIN)
2. **Something you have** (mobile device, hardware token)
3. **Something you are** (biometric data)

Azure AD Implementation

Azure AD implements 2FA through:

Primary Authentication Methods

- **Password + Secondary factor**
- **Windows Hello for Business**
- **FIDO2 security keys**
- **Certificate-based authentication**

Secondary Authentication Methods

- **Microsoft Authenticator app**
- **SMS text message**
- **Voice call**
- **Hardware tokens (OATH)**
- **Software tokens**

Configuration Process

1. **Enable MFA service in Azure AD**

2. **Configure authentication methods** available to users
3. **Set up Conditional Access policies** for targeted enforcement
4. **Configure user settings** and registration requirements
5. **Test authentication flow** with pilot users

Security Benefits

- Reduces password-based attacks by 99.9%
 - Protects against credential stuffing
 - Prevents unauthorized access even with compromised passwords
 - Meets compliance requirements for many industries
-

3. Different Methods of Two Factor Authentication

3.1 Microsoft Authenticator App

Type: Push notification or time-based one-time password (TOTP)

Setup Process:

1. User downloads Microsoft Authenticator app
2. Admin enables app-based authentication in MFA settings
3. User adds work account to the app
4. App generates 6-digit codes or receives push notifications

Advantages:

- Most secure method available
- Works offline for TOTP codes
- Supports biometric verification
- No carrier dependency

Use Cases: Recommended for all users as primary method

3.2 SMS Text Message

Type: SMS-based one-time password

Setup Process:

1. Enable SMS authentication in MFA settings
2. User registers mobile phone number
3. System sends 6-digit code via SMS during authentication

4. User enters code within time limit

Advantages:

- Familiar to most users
- No additional app installation required
- Works on basic mobile phones

Limitations:

- Vulnerable to SIM swapping attacks
- Depends on cellular coverage
- May incur SMS charges

3.3 Voice Call

Type: Automated voice verification

Setup Process:

1. Enable voice call authentication
2. User registers phone number (mobile or landline)
3. System places automated call during authentication
4. User presses # to confirm or follows voice prompts

Advantages:

- Works with landlines and mobile phones
- Accessible for users with disabilities
- No smartphone requirement

Use Cases: Backup method or for users without smartphones

3.4 Hardware Tokens (OATH)

Type: Hardware-based TOTP tokens

Setup Process:

1. Purchase OATH-compatible hardware tokens
2. Import token seed values into Azure AD
3. Assign tokens to users
4. Configure token settings and policies

Advantages:

- Highest security level
- No battery dependency for some models
- Cannot be compromised remotely
- Suitable for high-security environments

Use Cases: Privileged accounts, compliance requirements

3.5 FIDO2 Security Keys

Type: Hardware-based passwordless authentication

Setup Process:

1. Enable FIDO2 security keys in Azure AD
2. Configure authentication policy
3. Users register their security keys
4. Test passwordless sign-in process

Advantages:

- Passwordless authentication
- Phishing-resistant

- Fast and convenient
- Industry standard

3.6 Certificate-Based Authentication

Type: Digital certificate on smart card or device

Setup Process:

1. Configure certificate authority trust
2. Set up certificate mapping
3. Deploy certificates to users
4. Configure authentication policies

Advantages:

- Very high security
 - Integrates with PKI infrastructure
 - Supports smart cards
 - Non-repudiation
-

4. Setup Self-Service Password Reset

Overview

Self-Service Password Reset (SSPR) allows users to reset their passwords without administrator intervention, reducing helpdesk burden and improving user experience.

Prerequisites

- Azure AD Premium P1 or P2 license (for on-premises writeback)
- Global Administrator permissions
- Azure AD Connect (for hybrid environments)

Initial Configuration Steps

Step 1: Enable SSPR

1. Navigate to **Azure Active Directory > Password reset**
2. Under **Properties**, select user scope:
 - **None**: SSPR disabled
 - **Selected**: Enable for specific groups
 - **All**: Enable for all users
3. Click **Save**

Step 2: Configure Authentication Methods

1. In **Authentication methods**, configure:
 - **Number of methods required to reset**: 1 or 2
 - **Methods available to users**:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

2. Set up security questions if enabled:

- **Number of questions required to register: 3-5**
- **Number of questions required to reset: 3-5**
- Select predefined or custom questions

Step 3: Registration Settings

1. Configure **Registration** options:

- **Require users to register when signing in: Yes/No**
- **Number of days before users are asked to reconfirm: 180 days (recommended)**

2. Set up **Notifications**:

- **Notify users on password resets: Yes**
- **Notify all admins when other admins reset passwords: Yes**

Step 4: On-Premises Integration

1. Configure **On-premises integration**:

- **Write back passwords to on-premises directory:**
Yes
- **Allow users to unlock accounts without resetting password:** Yes

2. Ensure Azure AD Connect is configured for password writeback

5. Configure MFA

Conditional Access Policy Configuration

Step 1: Create Conditional Access Policy

1. Navigate to **Azure Active Directory > Security > Conditional Access**
2. Click **New policy**
3. Configure policy settings:
 - **Name:** Descriptive policy name
 - **Users and groups:** Select target users/groups
 - **Cloud apps:** Select applications requiring MFA
 - **Conditions:** Configure location, device, risk conditions
 - **Access controls:** Require MFA

Step 2: Configure Authentication Strengths

1. In **Azure AD**, go to **Security > Authentication methods > Authentication strengths**
2. Create custom authentication strength policies
3. Define required authentication methods combinations
4. Apply to Conditional Access policies

Step 3: Set Up Registration Policies

1. Navigate to **Identity Protection > MFA registration policy**
2. Configure:

- **Assignments:** Select users and groups
- **Controls:** Require MFA registration
- **Enforce policy:** On/Off

3. Set grace period for user registration

Method-Specific Configuration

Microsoft Authenticator Configuration

1. Go to **Authentication methods > Microsoft Authenticator**
2. Enable the method
3. Configure settings:
 - **Show application name in notification:** Yes
 - **Show geographic location in notification:** Yes
 - **Number matching:** Required
 - **Show additional context in notification:** Yes

SMS and Voice Configuration

1. Navigate to **Authentication methods > SMS or Voice**
 2. Enable the method
 3. Configure target groups
 4. Set up authentication phone settings
-

6. Configure and Deploy Self-Service Password Reset

Deployment Planning

Phase 1: Planning and Preparation

1. **Stakeholder identification:** IT administrators, helpdesk, security team
2. **Scope definition:** User groups, authentication methods, policies
3. **Communication plan:** User training, documentation, support processes
4. **Testing environment:** Pilot group selection and testing procedures

Phase 2: Technical Configuration

1. **Azure AD SSPR configuration** (as outlined in section 4)
2. **On-premises integration setup:**
 - Install Azure AD Connect
 - Configure password writeback
 - Set up hybrid authentication
3. **Conditional Access policies** for registration enforcement
4. **Monitoring and reporting** setup

Phase 3: Pilot Deployment

1. **Select pilot group:** 5-10% of users from different departments

2. **Enable SSPR** for pilot group
3. **Conduct user training** sessions
4. **Monitor usage** and gather feedback
5. **Resolve issues** and refine configuration

Phase 4: Full Deployment

1. **Gradual rollout** to all users
2. **Monitor adoption** rates and user experience
3. **Provide ongoing support** and training
4. **Regular review** and optimization

User Registration Process

Mandatory Registration Flow

1. User signs in to Azure AD
2. System prompts for SSPR registration
3. User provides required authentication methods:
 - Mobile phone number
 - Alternate email address
 - Security questions (if enabled)
4. System validates provided information
5. Registration completion confirmation

Self-Service Registration

1. User visits <https://aka.ms/ssprsetup>
2. Enters work credentials

3. Follows guided setup process
 4. Confirms registration details
-

7. Implement and Manage Azure MFA Settings

Global MFA Settings Configuration

Service Settings Management

1. Navigate to **Azure Active Directory > Security > MFA > Getting started**
2. Configure **fraud alert** settings:
 - **Allow users to submit fraud alerts:** Yes
 - **Automatically block users who report fraud:** Yes
 - **Code to report fraud during initial greeting:** 0
3. Set up **notifications**:
 - **Notify admins when users report fraud:** Yes
 - **Notify users when their passwords are changed:** Yes
4. Configure **OATH** tokens:
 - **Upload OATH token CSV file**
 - **Assign tokens to users**
 - **Set token refresh intervals**

Account Lockout Configuration

1. In **MFA settings**, configure:
 - **Account lockout threshold:** 3-5 failed attempts
 - **Minutes to reset account lockout counter:** 10 minutes

- **Minutes until account is automatically unlocked:**
30 minutes

2. Set up **IP restrictions**:

- **Trusted IP ranges:** Define corporate networks
- **Skip MFA for requests from trusted IPs:**
Configure based on policy

User-Specific MFA Management

Bulk User Management

1. Navigate to **Users > All users > Multi-Factor Authentication**
2. Use bulk operations:
 - **Bulk enable:** CSV upload for multiple users
 - **Bulk disable:** Remove MFA requirement
 - **Bulk reset:** Clear user MFA settings
3. Monitor user status:
 - **Disabled:** MFA not required
 - **Enabled:** MFA required but not enforced
 - **Enforced:** MFA mandatory for all sign-ins

Individual User Settings

1. Select specific user from MFA portal
2. Configure user settings:
 - **Authentication methods:** Enable/disable specific methods

- **Trusted devices:** Manage remembered devices
 - **App passwords:** Generate for legacy applications
 - **Fraud alerts:** User-specific fraud alert settings
-

8. Account Lockout

Account Lockout Policies

Azure AD Smart Lockout

Azure AD includes intelligent lockout features that distinguish between legitimate users and attackers:

1. **Lockout threshold:** Default 10 failed attempts
2. **Lockout duration:** Starts at 1 minute, increases with repeated failures
3. **Familiar location detection:** Different thresholds for known vs. unknown locations
4. **Password spray protection:** Automatic detection and blocking

Configuration Steps

1. Navigate to **Azure Active Directory > Security > Authentication methods > Password protection**
2. Configure **Smart lockout** settings:
 - **Lockout threshold:** 3-10 failed attempts
 - **Lockout duration in seconds:** 60-600 seconds
 - **Custom banned password list:** Organization-specific weak passwords
3. Set up **Global banned password list:** Microsoft-maintained list of common passwords

MFA-Specific Lockout

MFA Lockout Configuration

1. In **MFA service settings**, configure:
 - **Lockout threshold:** 3-5 failed MFA attempts
 - **Lockout duration:** 10-60 minutes
 - **Auto-unlock:** Enable automatic unlock after duration
2. Set up **fraud alert lockout**:
 - **Immediate lockout:** When fraud is reported
 - **Admin notification:** Alert administrators
 - **Investigation process:** Define response procedures

Lockout Monitoring and Management

1. **Monitor lockout events:**
 - Sign-in logs in Azure AD
 - MFA activity reports
 - Security alerts and notifications
2. **Unlock procedures:**
 - Administrative unlock through Azure portal
 - Automatic unlock after timeout
 - Self-service unlock options
3. **Incident response:**
 - Investigate lockout patterns

- Identify potential security threats
 - Adjust lockout policies as needed
-

9. Manage MFA Settings for Users

User MFA Status Management

User States and Transitions

1. **Disabled:** User not enrolled in MFA
2. **Enabled:** User enrolled but not enforced
3. **Enforced:** MFA required for all sign-ins

State Management Process

1. Navigate to **Users > All users > Multi-Factor Authentication**
2. Select users for state changes
3. Use **Quick steps** for bulk operations:
 - **Enable MFA:** Move from disabled to enabled
 - **Enforce MFA:** Move from enabled to enforced
 - **Disable MFA:** Remove MFA requirement
4. Monitor state changes and user adoption

User Registration Management

Registration Enforcement

1. **Conditional Access policy** for registration:
 - Target all users or specific groups
 - Require MFA registration
 - Set compliance deadline
2. **Registration experience:**

- Guided setup process
- Multiple authentication method options
- Validation and confirmation steps

3. Registration monitoring:

- Track registration completion rates
- Identify non-compliant users
- Send reminders and notifications

User Support and Training

1. Documentation and guides:

- Step-by-step setup instructions
- Troubleshooting common issues
- Best practices for security

2. Training programs:

- Interactive workshops
- Online training modules
- Video tutorials and demos

3. Help desk support:

- MFA-specific support procedures
- Common issue resolution
- Escalation processes

Authentication Method Management

Method Configuration per User

1. Microsoft Authenticator:

- Push notification settings
- Number matching requirements
- Biometric authentication options

2. SMS and Voice:

- Phone number validation
- International number support
- Backup number configuration

3. Hardware tokens:

- Token assignment and activation
- Replacement procedures
- Bulk token management

Method Policies and Controls

1. Authentication strength policies:

- Define required method combinations
- Set security levels for different applications
- Configure method preferences

2. Conditional requirements:

- Location-based method requirements
 - Device-based authentication policies
 - Risk-based authentication adjustments
-

10. Extend Azure AD MFA to Third Party and On-Premises Devices

On-Premises Integration

Azure AD Connect Configuration

1. Install Azure AD Connect:

- Download from Microsoft Download Center
- Run installation wizard
- Configure sync settings

2. Enable password writeback:

- Select password writeback option
- Configure write permissions
- Test writeback functionality

3. Configure hybrid authentication:

- Set up Pass-through Authentication or Federation
- Configure seamless SSO
- Test hybrid authentication flow

Active Directory Federation Services (ADFS) Integration

1. Configure ADFS for MFA:

- Install ADFS MFA adapter
- Configure authentication policies
- Set up claims rules

2. Primary and additional authentication:

- Configure primary authentication methods
- Set up MFA as additional authentication
- Define authentication flow rules

3. Certificate-based authentication:

- Configure certificate trust
- Set up certificate mapping
- Test certificate authentication

Third-Party Application Integration

SAML-Based Applications

1. Configure SAML SSO:

- Add application from Azure AD gallery
- Configure SAML settings
- Set up attribute mapping

2. MFA enforcement:

- Configure Conditional Access policies
- Set authentication requirements
- Test MFA flow with SAML apps

3. Supported applications:

- Salesforce, ServiceNow, Workday
- Custom SAML applications
- On-premises SAML applications

OAuth and OpenID Connect Applications

1. Register applications in Azure AD

2. Configure authentication flows:

- Authorization code flow
- Implicit flow
- Client credentials flow

3. MFA integration:

- Configure authentication context
- Set up conditional access
- Test OAuth MFA flow

VPN and Network Device Integration

RADIUS Integration

1. Network Policy Server (NPS) configuration:

- Install NPS role on Windows Server
- Configure RADIUS clients
- Set up authentication policies

2. Azure MFA NPS extension:

- Install MFA NPS extension
- Configure extension settings
- Test RADIUS authentication with MFA

3. VPN integration:

- Configure VPN server for RADIUS
- Set up authentication policies

- Test VPN connection with MFA

API Integration

1. Azure MFA REST API:

- Obtain API credentials
- Configure API calls
- Implement MFA verification

2. Custom application integration:

- Use Microsoft Graph API
 - Configure authentication flows
 - Implement MFA challenges
-

11. Monitor Azure AD MFA Activity

Monitoring Tools and Reports

Azure AD Reporting

1. Sign-in logs:

- Navigate to **Azure Active Directory > Monitoring > Sign-ins**
- Filter by MFA activity
- Analyze authentication patterns
- Export data for analysis

2. Audit logs:

- Track MFA configuration changes
- Monitor user registration events
- Review administrative actions

3. Usage and insights:

- Authentication methods usage
- User adoption rates
- Failure analysis

MFA Activity Reports

1. MFA activity report:

- Access through Azure AD portal
- View user MFA usage
- Analyze authentication methods

- Track blocked users

2. Fraud alert reports:

- Monitor fraud reports
- Track false positive rates
- Analyze fraud patterns

3. Registration reports:

- Track user registration progress
- Identify non-compliant users
- Monitor registration methods

Advanced Monitoring Solutions

Azure Monitor Integration

1. Log Analytics workspace:

- Create workspace for MFA logs
- Configure data retention
- Set up log queries

2. Diagnostic settings:

- Enable diagnostic logging
- Select log categories
- Configure destination settings

3. Custom queries:

- KQL queries for MFA analysis
- Create custom dashboards

- Set up automated alerts

Security Information and Event Management (SIEM) Integration

1. Azure Sentinel:

- Connect Azure AD data connector
- Configure MFA-specific workbooks
- Set up threat detection rules

2. Third-party SIEM:

- Configure API connections
- Set up log forwarding
- Create correlation rules

3. Automated response:

- Configure alert actions
- Set up automated investigations
- Implement response playbooks

Key Metrics and KPIs

Security Metrics

- 1. MFA success rate:** Percentage of successful MFA authentications
- 2. Fraud alert rate:** Number of fraud alerts per authentication attempts
- 3. Account lockout rate:** Frequency of account lockouts

4. **Authentication method distribution:** Usage patterns across different methods

User Experience Metrics

1. **User adoption rate:** Percentage of users enrolled in MFA
2. **Registration completion time:** Average time to complete registration
3. **Support ticket volume:** MFA-related help desk requests
4. **User satisfaction:** Survey results and feedback

Operational Metrics

1. **System availability:** MFA service uptime
 2. **Response time:** Authentication response times
 3. **Error rates:** Failed authentication attempts
 4. **Configuration changes:** Frequency of policy updates
-

12. OAuth Tokens

OAuth 2.0 and MFA Integration

OAuth Token Flow with MFA

1. Authorization Code Flow:

- Client redirects user to Azure AD
- User authenticates with primary factor
- MFA challenge presented based on Conditional Access
- User completes MFA verification
- Authorization code returned to client
- Client exchanges code for access token

2. Device Code Flow:

- Device requests device code
- User authenticates on separate device
- MFA challenge during authentication
- Device receives access token after verification

Token Claims and MFA

1. MFA claims in tokens:

- amr (Authentication Method Reference): Lists authentication methods used
- auth_time: Time of authentication

- acr (Authentication Context Class Reference):
Authentication strength

2. Conditional Access claims:

- cc: Conditional Access policy applied
- xms_cc: Cross-tenant access claims
- acrs: Authentication requirements satisfied

Access Token Management

Token Lifetime Configuration

1. Configure token lifetimes:

- Navigate to **Azure Active Directory > Security > Token lifetime policies**
- Set access token lifetime
- Configure refresh token policies
- Set session token settings

2. MFA-specific token policies:

- Shorter token lifetimes for high-risk applications
- Refresh token revocation on MFA failure
- Persistent browser sessions with MFA

Token Validation and MFA

1. Server-side validation:

- Validate token signature
- Check MFA claims in token

- Verify authentication strength
- Validate token expiration

2. Application integration:

- Check amr claim for MFA completion
- Validate authentication context
- Implement step-up authentication
- Handle token refresh with MFA

Refresh Token Behavior

MFA and Refresh Tokens

1. Refresh token requirements:

- MFA may be required for refresh
- Conditional Access evaluation during refresh
- Token binding to MFA session

2. Configuration options:

- **Require MFA for refresh:** Force MFA on each refresh
- **Session persistence:** Remember MFA for defined period
- **Risk-based refresh:** Require MFA based on risk assessment

Token Revocation

1. Revocation scenarios:

- MFA method compromise
- Suspicious authentication activity
- Administrative revocation
- User-initiated revocation

2. Revocation methods:

- User revocation through MyApps portal
- Administrative revocation through Azure AD
- Automated revocation through Conditional Access
- API-based revocation

API Authentication with MFA

Microsoft Graph API

1. Application registration:

- Register application in Azure AD
- Configure API permissions
- Set up authentication certificates

2. MFA enforcement:

- Configure Conditional Access for APIs
- Set authentication requirements
- Implement client assertion authentication

3. Token acquisition:

- Use client credentials flow
- Implement certificate-based authentication

- Handle MFA challenges in application flow

Custom API Integration

1. API protection:

- Validate access tokens
- Check MFA claims
- Implement scope-based authorization

2. Client implementation:

- Handle interactive authentication
- Implement token caching
- Manage token refresh with MFA

3. Security considerations:

- Validate authentication context
 - Implement defense in depth
 - Monitor API access patterns
-

Troubleshooting Common Issues

- 1. Authentication failures:** Check method availability and user registration
- 2. Lockout issues:** Review lockout policies and user behavior

3. **Token problems:** Validate token configuration and lifetime settings
 4. **Integration issues:** Test API connections and authentication flows
 5. **User experience:** Gather feedback and optimize authentication processes
-

13 Conclusion

Implementing Azure Multifactor Authentication and Self-Service Password Reset requires careful planning, configuration, and ongoing management. This comprehensive guide provides the foundation for securing your organization's identity infrastructure while maintaining user productivity and satisfaction. Regular review and updates of these configurations ensure continued security effectiveness and compliance with evolving security requirements.

For additional support and updates, refer to the official Microsoft documentation and Azure AD security best practices guides.

14 Screenshots

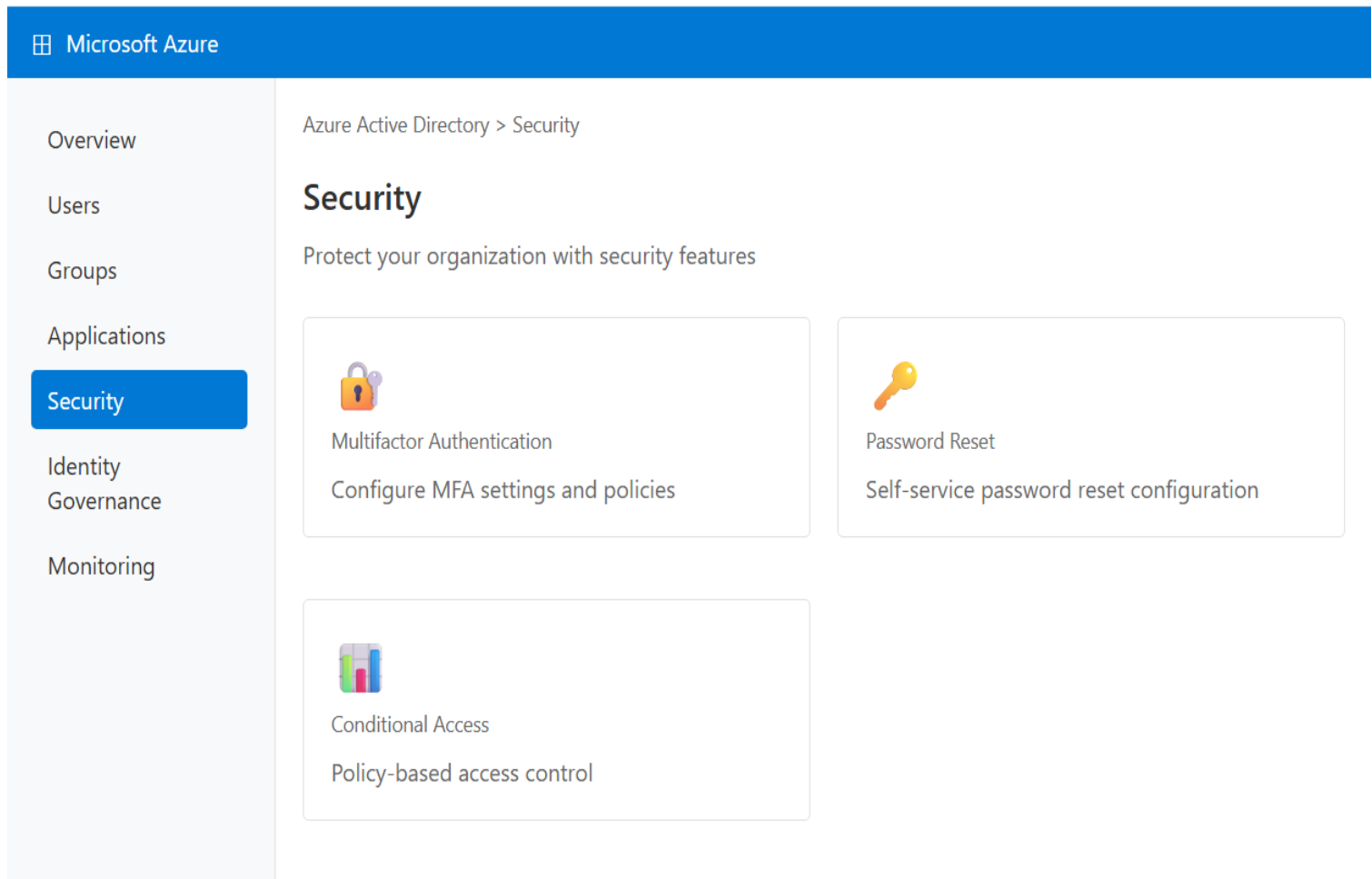



Figure 1 - Azure Active Directory Portal

 Microsoft Azure

Azure Active Directory > Security > Multifactor Authentication

Multifactor Authentication

Configure multi-factor authentication settings

[Getting started](#) [Service settings](#) [Fraud alert](#) [Notifications](#)

Enable MFA for Users

Select users to enable MFA


☐ Enable for all users


☒ Enable for selected groups


Selected Groups

Finance Team

Authentication Methods

 **Microsoft Authenticator**
Push notifications and verification codes

 **SMS Text Message**
6-digit code sent via SMS

 **Voice Call**
Automated voice verification


Save Configuration

Cancel

Figure 2 - Multifactor Authentication Configuration

Multi-Factor Authentication

Manage MFA settings for individual users

 **Tip:** Use bulk operations to enable MFA for multiple users at once.

Bulk Enable
Bulk Disable
Export Users

<input type="checkbox"/>	Display Name	User Principal Name	MFA Status	Authentication Methods	Actions
<input type="checkbox"/>	John Smith	john.smith@contoso.com	Enabled	Authenticator App, SMS	Manage
<input type="checkbox"/>	Sarah Johnson	sarah.johnson@contoso.com	Enforced	Authenticator App	Manage
<input type="checkbox"/>	Mike Wilson	mike.wilson@contoso.com	Disabled	-	Enable

Figure 3 - User MFA Management Interface

Password reset

Configure self-service password reset settings

[Properties](#)
[Authentication methods](#)
[Registration](#)
[Notifications](#)

Self service password reset enabled

☐ None
☒ Selected
☐ All

Select group

All Users

Authentication Methods

Number of methods required to reset

2

Methods available to users

☒ Mobile app notification
☒ Mobile app code
☒ Email
☐ Mobile phone

Save
Discard

Figure 4 - Self-Service Password Reset Configuration

Azure Active Directory > Security > Conditional Access

New Conditional Access Policy

Create a policy to require MFA for specific conditions

Policy Name

Require MFA for All Users

Assignments

Users and groups

- ☒ All users
☐ Select users and groups

Cloud apps or actions

All cloud apps

Access Controls

Grant

- ☐ Block access
☒ Grant access
☒ Require multifactor authentication
☐ Require device to be marked as compliant

Enable Policy

- ☐ Off
☒ Report-only
☐ On

Create

Cancel

Figure 5 - Conditional Access Policy for MFA

Azure Active Directory > Monitoring > Sign-ins

Sign-ins

Monitor authentication activity and MFA usage

1,247

Total Sign-ins Today

892

MFA Challenges

98.5%

MFA Success Rate

3

Fraud Alerts

Filter by:

All

Last 24 hours

Date	User	Application	Status	MFA Method	Location
2024-01-15 09:30	john.smith@contoso.com	Office 365	Success	Authenticator App	New York, US
2024-01-15 09:28	sarah.johnson@contoso.com	Azure Portal	Success	SMS	London, UK
2024-01-15 09:25	mike.wilson@contoso.com	SharePoint	Failed	SMS	Seattle, US

Figure 6 - MFA Activity Reports and Monitoring

Azure Active Directory > Security > Authentication methods

Authentication methods

Configure available authentication methods for your organization

Microsoft Authenticator



Enable Microsoft Authenticator

Target

All users



Show application name in notification



Show geographic location in notification

Figure 7 - Authentication Methods Configuration

Configure Lockout Policy

Export Settings

Search locked accounts...

Account Lockout Settings

Lockout Threshold

5 failed attempts

Lockout Duration

30 minutes

User	Email	Status	Lockout Time	Failed Attempts	Actions
John Smith	john.smith@company.com	Locked	2024-07-10 14:30:00	5	Unlock
Sarah Johnson	sarah.johnson@company.com	Active	-	0	Lock
Mike Wilson	mike.wilson@company.com	Locked	2024-07-10 15:45:00	7	Unlock

Figure 8 - Account Lockout Management

Enable MFA for Selected

Bulk Operations

Export Report

Search users...

1,247
Total Users

892
MFA Enabled

355
MFA Disabled

<input type="checkbox"/>	User	Email	MFA Status	Primary Method	Backup Methods	Last Sign-in	Actions
<input type="checkbox"/>	Alice Brown	alice.brown@company.com	Enabled	Microsoft Authenticator	SMS, Email	2024-07-10 09:15:00	Edit Disable
<input type="checkbox"/>	Bob Davis	bob.davis@company.com	Disabled	-	-	2024-07-09 16:30:00	Enable Configure
<input type="checkbox"/>	Carol White	carol.white@company.com	Enabled	Hardware Token	Phone Call	2024-07-10 11:45:00	Edit Disable

Figure 9 - Manage MFA Settings for Users

Home > Azure Active Directory > Hybrid > MFA Extension

NPS Extension

RADIUS Integration

ADFS Integration

Third Party Apps

Info: Configure Network Policy Server (NPS) extension to enable MFA for VPN, Remote Desktop, and other RADIUS-based authentication.

NPS Extension Configuration

Tenant ID

12345678-1234-1234-1234-123456789012

Authentication Endpoint

https://login.microsoftonline.com/

☒ Enable NPS Extension

☐ Allow fallback to local authentication

PowerShell script to install NPS Extension Install-Module -Name AzureAD -Connect-AzureAD -.\AzureMfaNpsExtnConfigSetup.ps1

Integration Type	Status	Connected Services	Last Sync	Actions
NPS Extension	Active	VPN Gateway, RD Gateway	2024-07-10 10:30:00	<div>Configure</div>
ADFS	Active	SharePoint, Exchange	2024-07-10 09:15:00	<div>Manage</div>
RADIUS	Inactive	-	-	<div>Setup</div>

Figure 10 - Extend Azure AD MFA to Third Party and On-Premises

Home > Azure Active Directory > Monitoring > MFA Activity

Last 7 days

Export Report

Set Alerts

Search activity...

15,428

MFA Attempts

14,892

Successful

536

Failed

96.5%

Success Rate

Sign-in Activity

Authentication Methods

Risk Events

Audit Logs

Date/Time	User	Application	Method	Result	IP Address	Location	Device
2024-07-10 15:30:22	alice.brown@company.com	Office 365	Microsoft Authenticator	Success	192.168.1.100	New York, US	Windows 11
2024-07-10 15:28:15	bob.davis@company.com	SharePoint	SMS	Failed	203.0.113.45	London, UK	Chrome/MacOS
2024-07-10 15:25:03	carol.white@company.com	Azure Portal	Hardware Token	Success	10.0.0.50	Chicago, US	Edge/Windows

Figure 11 - Monitor Azure AD MFA Activity

[Home](#) > [Azure Active Directory](#) > [Security](#) > [OAuth Tokens](#)

[Create New Token](#) [Bulk Revoke](#) [Token Analytics](#)

Warning: Regularly review and rotate OAuth tokens to maintain security. Tokens with excessive permissions should be audited.

[Active Tokens](#) [Expired Tokens](#) [Revoked Tokens](#) [Token Policies](#)

1,847
Active Tokens

23
Expiring Soon

456
This Month

Token ID	Application	User/Service	Scopes	Created	Expires	Status	Actions
tok_abc123...def456	Microsoft Graph API	alice.brown@company.com	User.Read, Mail.Read	2024-07-01 09:00:00	2024-08-01 09:00:00	Active	View Revoke
tok_xyz789...uvw012	Custom Web App	service-account@company.com	Directory.Read.All	2024-06-15 14:30:00	2024-07-15 14:30:00	Expiring	Renew Revoke
tok_mno345...pqr678	Power BI	bob.davis@company.com	Dataset.Read.All	2024-07-05 11:15:00	2024-08-05 11:15:00	Active	View Revoke

Token Configuration
Default Token Lifetime

1 hour

☒ Require MFA for token creation
☐ Auto-revoke on suspicious activity

Figure 12 - OAuth Tokens Management