FIRST UNDERWRITERS INSURANCE BROKERS

MFA Implementation Guide

Protecting Your Business with Multi-Factor Authentication

A practical, step-by-step resource for small and mid-sized businesses to deploy multi-factor authentication across their organization.

Covers implementation planning, platform-specific instructions, employee training strategies, and compliance considerations.

Part of: Cyber Security Essentials for Small Business

Free resource series from First Underwriters Insurance Brokers

www.firstunderwriters.com

© First Underwriters Insurance Brokers | All Rights Reserved

What Is Multi-Factor Authentication?

Multi-factor authentication (MFA) is a security method that requires users to verify their identity using two or more distinct factors before gaining access to an account, system, or application. Instead of relying solely on a password, MFA combines something you know (password), something you have (phone or security key), and/or something you are (fingerprint or facial recognition).

MFA is widely recognized as one of the single most effective cybersecurity controls available. According to industry research, enabling MFA blocks over 99% of automated credential-based attacks, making it a critical first line of defense for businesses of any size.

Why MFA Is Essential for Small Businesses

80% of data breaches involve compromised credentials, and small businesses are disproportionately targeted.
Cyber insurance carriers increasingly require MFA as a condition of coverage or premium reduction.
Regulatory frameworks including HIPAA, PCI-DSS, and CMMC mandate or strongly recommend MFA.
The average cost of a data breach for small businesses exceeds $150,000 — often enough to force closure.

The Three Authentication Factors

1

Something You Know

Password, PIN, or security question. This is the traditional first factor but is vulnerable to phishing, brute force, and social engineering attacks.

2

Something You Have

Smartphone, hardware token, or security key. This physical factor ensures that even if a password is stolen, an attacker cannot log in without the device.

3

Something You Are

Biometric data such as fingerprint, facial recognition, or iris scan. Biometrics provide strong verification but require compatible hardware.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

MFA Methods Compared

Not all MFA methods provide equal security. Understanding the strengths and weaknesses of each option helps you choose the right approach for your business needs and risk profile.

SMS / Text Codes

Security: Moderate | Ease: Very Easy | Cost: Low

Convenient but vulnerable to SIM-swapping attacks. Acceptable as a starting point.

Authenticator App

Security: High | Ease: Easy | Cost: Free

Google Authenticator, Microsoft Authenticator, Authy. Recommended minimum standard.

Push Notification

Security: High | Ease: Very Easy | Cost: Low

Duo, Microsoft Authenticator push. Simple tap to approve. Watch for MFA fatigue attacks.

Hardware Security Key

Security: Very High | Ease: Moderate | Cost: $$

YubiKey, Google Titan. Phishing-resistant. Best for high-value accounts and admins.

Biometric

Security: High | Ease: Very Easy | Cost: Varies

Fingerprint, Face ID. Built into modern devices. Often used as second layer with another factor.

Email Codes

Security: Low | Ease: Easy | Cost: Free

One-time codes via email. NOT recommended — if email is compromised, MFA is bypassed.

Our Recommendation

For most small businesses, authenticator apps provide the best balance of security and usability. Require hardware security keys for administrator accounts and any employees with access to financial systems or sensitive customer data. Avoid relying solely on SMS codes for critical systems.

© First Underwriters Insurance Brokers | www.firstunderwriters.com

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Implementation Roadmap

A phased approach ensures smooth MFA deployment with minimal business disruption. Most small businesses can complete the full rollout in 30 to 60 days.

Week 1

1 Assess & Inventory

Catalog all business applications, cloud services, and systems that support MFA. Identify which accounts have admin or elevated privileges. Document current authentication methods for each system and prioritize based on data sensitivity.

Week 1-2

2 Select MFA Methods

Choose your primary MFA method (authenticator app recommended for most). Select a secondary method for backup. Determine if hardware keys are needed for admin accounts. Evaluate vendor compatibility with your existing platforms.

Week 2

3 Configure Admin Accounts First

Enable MFA on all administrator and privileged accounts before the general rollout. This protects your highest-risk accounts immediately and lets your IT team build experience with the enrollment process before supporting other employees.

Week 2-3

4 Pilot with Early Adopters

Roll out MFA to a small group of tech-comfortable employees across different departments. Gather feedback on the enrollment process, daily experience, and any issues. Refine your support documentation and FAQ based on pilot feedback.

Week 3-5

5 Company-Wide Rollout

Deploy MFA to all remaining employees in manageable batches (10-20 users per day). Provide scheduled enrollment sessions with IT support available. Communicate deadlines clearly and follow up with any employees who haven't enrolled.

Week 5-6

6 Verify & Enforce

Audit all accounts to confirm MFA enrollment is complete. Enable policies that block sign-in without MFA. Configure conditional access rules where available. Disable legacy authentication protocols that bypass MFA.

Ongoing

7 Monitor & Maintain

Review MFA logs for anomalies and failed attempts. Update recovery methods regularly. Include MFA enrollment in your onboarding process. Re-evaluate methods annually as threats evolve and new options become available.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Platform-Specific Setup Guides

Below are concise instructions for enabling MFA on the platforms most commonly used by small businesses. For detailed walkthroughs, refer to each vendor's documentation.

Microsoft 365 / Azure AD

1. Navigate to admin.microsoft.com > Settings > Org settings > Multi-factor authentication
2. Select 'Security defaults' to enable MFA for all users (recommended for most small businesses)
3. For granular control, use Conditional Access policies in Azure AD (requires P1 license)
4. Users will be prompted to register MFA on next sign-in — direct them to aka.ms/mfasetup
5. Disable legacy authentication protocols under Authentication Methods to prevent bypass

Google Workspace

1. Open admin.google.com > Security > Authentication > 2-Step Verification
2. Set enforcement to 'On' and choose an enforcement date (recommend 7-14 day grace period)
3. Select allowed methods — enable Google Prompts, Security Keys; consider disabling SMS
4. Admin accounts should enroll first, then enforce for all organizational units
5. Users enroll at myaccount.google.com/signinoptions/two-step-verification

QuickBooks Online

1. Each user signs into their Intuit account at accounts.intuit.com
2. Go to Account > Sign in & security > Two-step verification > Turn on
3. Choose verification method: Authenticator app (recommended) or phone number
4. Company admin cannot force MFA for all users — distribute enrollment instructions
5. Emphasize this step for anyone with accountant or company admin access levels

VPN & Remote Access

1. Check your VPN vendor documentation for MFA integration options (RADIUS, SAML, LDAP)
2. Most enterprise VPNs support integration with Azure MFA, Duo Security, or Okta
3. For basic VPN setups, consider Duo Security's free tier (up to 10 users)
4. Require MFA on every VPN connection — do not allow 'remember this device' for remote access
5. Test thoroughly before enforcement; VPN lockouts can halt remote work entirely

© First Underwriters Insurance Brokers | www.firstunderwriters.com

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Common Challenges & Solutions

Anticipating common obstacles helps ensure a smoother rollout. Below are the issues most frequently encountered during MFA implementation and proven strategies to address them.

Employee Resistance

Some employees view MFA as an inconvenience. Frame it as protecting their own data and the jobs of everyone in the organization. Emphasize that modern MFA adds only seconds to the login process. Share real examples of businesses harmed by credential theft. Involve department managers as champions to encourage adoption within their teams.

Lost or Replaced Devices

Establish a clear process for employees who lose their phone or get a new device. Require backup authentication methods during enrollment — such as backup codes, a secondary phone number, or a recovery email. Keep a secure record of backup codes for critical accounts. Consider hardware security keys as backup for essential personnel.

Shared or Service Accounts

MFA is difficult for accounts shared among multiple employees. Migrate shared accounts to individual accounts where possible. For service accounts that must remain shared, use hardware security keys stored in a secure location, or use a privileged access management tool. Document who has access and rotate credentials on a schedule.

Legacy Applications

Older applications may not support MFA natively. Use a single sign-on (SSO) solution as a wrapper to add MFA to legacy apps. Consider application-specific passwords as a temporary workaround (with compensating controls). Prioritize replacing or upgrading legacy systems that handle sensitive data but cannot support MFA.

MFA Fatigue Attacks

Attackers who have stolen credentials repeatedly trigger MFA push prompts, hoping the user will approve out of frustration. Counter this by using number-matching push notifications (available in Microsoft Authenticator and Duo). Train employees to never approve unexpected MFA prompts and to report repeated prompts immediately.

Account Lockouts During Rollout

Employees may lock themselves out during initial setup. Schedule enrollment during business hours with IT support available. Provide a dedicated help channel (Teams, Slack, phone). Set a grace period before enforcement so employees have time to enroll. Have a documented escalation procedure for locked accounts.

© First Underwriters Insurance Brokers | www.firstunderwriters.com

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Employee Communication & Training

Successful MFA deployment depends on clear communication and accessible training. Employees who understand why MFA matters and how easy it is are far more likely to adopt it without resistance.

Communication Timeline

2 Weeks Before

Send company-wide email announcing MFA rollout. Explain the why: protecting the business and employee personal data. Include FAQ document and enrollment date.

1 Week Before

Send reminder with step-by-step enrollment guide and screenshots. Share a short video demonstration if possible. Open a Q&A channel for questions.

Enrollment Day

Provide live or virtual IT support sessions. Send final reminder with direct links to enrollment pages. Acknowledge early adopters to build positive momentum.

1 Week After

Follow up with any employees who haven't enrolled. Address common issues. Send a thank-you message acknowledging the team's effort in strengthening security.

Monthly Ongoing

Include MFA reminders in security awareness communications. Share relevant news stories about breaches prevented by MFA. Reinforce reporting of suspicious MFA prompts.

Key Training Points to Cover

- How to install and set up the chosen authenticator app on their personal or company phone
- What to do if they get an unexpected MFA prompt they didn't initiate (deny and report it)
- How to use backup codes and where to store them securely
- How to transfer their MFA to a new phone or device
- Who to contact for help with enrollment or if they get locked out
- Why MFA matters — use specific, relatable examples relevant to their role

Sample Announcement Email — Opening Paragraph

"Starting [date], we are strengthening our cybersecurity by enabling multi-factor authentication (MFA) across all company accounts. This means that in addition to your password, you will verify your identity with a quick tap on your phone when signing in. This simple step blocks over 99% of automated attacks and is now required by our cyber insurance carrier."

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

MFA Policy Template

Adapt this template for your organization's MFA policy. A formal policy creates accountability and provides documentation for compliance audits and insurance applications.

1. Purpose

This policy establishes requirements for multi-factor authentication to protect [Company Name]'s information systems, data, and accounts from unauthorized access.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who access company systems, applications, email, cloud services, or networks.

3. Requirements

MFA must be enabled on: all email accounts, cloud storage and collaboration tools, VPN and remote access connections, financial and accounting systems, systems containing customer PII or PHI, administrative and privileged accounts, and any system designated as business-critical by management.

4. Approved Methods

Primary: Authenticator application (Microsoft Authenticator, Google Authenticator, or Authy). Privileged accounts: Hardware security key (YubiKey or equivalent) required. Backup: Printed backup codes stored in a secure location. Not approved: SMS-only authentication for systems containing sensitive data.

5. Enrollment & Compliance

New employees must enroll in MFA during onboarding, before receiving system access. Existing employees must complete enrollment by [deadline]. Non-compliance after the enforcement date will result in account suspension until MFA is configured.

6. Lost Device Procedures

Employees must report a lost MFA device to IT within 24 hours. IT will verify identity through an alternate channel and issue temporary backup access. Replacement MFA enrollment must be completed within one business day of receiving a new device.

7. Exceptions

Exceptions require written approval from [IT Director/CISO] and must include compensating controls, a risk assessment, and a remediation timeline. Exceptions are reviewed quarterly.

8. Review

This policy will be reviewed and updated annually or following any security incident involving credential compromise. Policy owner: [IT Director/CISO].

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

MFA, Insurance & Compliance

MFA has moved from a best practice to a hard requirement across the cyber insurance and regulatory landscape. Implementing MFA directly impacts your ability to secure coverage, reduce premiums, and maintain compliance with industry standards.

Cyber Insurance Requirements

Virtually every cyber insurance carrier now asks about MFA during the application process. Carriers increasingly deny coverage or charge significant premium surcharges for organizations without MFA on email, VPN, and administrative accounts. Having documented MFA policies and enrollment records strengthens your application and may qualify you for premium discounts.

- ✓ MFA enabled on all email accounts (most frequently asked question on applications)
- ✓ MFA enabled on remote access / VPN connections
- ✓ MFA enabled on all administrative and privileged accounts
- ✓ MFA enabled on cloud-hosted services and backup systems
- ✓ Written MFA policy on file and enforced across the organization
- ✓ MFA enrollment records maintained for audit and compliance documentation

Regulatory & Framework Alignment

HIPAA Requires access controls and audit controls; MFA is a recognized addressable implementation specification.

PCI-DSS Requires MFA for all remote network access and administrative access to cardholder data environments.

CMMC / NIST 800-171 MFA is explicitly required for remote and privileged access under CMMC Level 2 and NIST 800-171.

SOC 2 MFA is a common control cited in SOC 2 Type II reports for the Security trust service criteria.

State Privacy Laws Many state data protection laws reference reasonable security measures; MFA is considered a baseline.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Quick-Reference Checklist

- [ ] Inventory all systems and accounts that need MFA
- [ ] Select primary MFA method (authenticator app recommended)
- [ ] Select backup MFA method (hardware key or backup codes)
- [ ] Enable MFA on all admin / privileged accounts first
- [ ] Pilot with a small group and gather feedback
- [ ] Prepare employee communication and training materials
- [ ] Roll out to all employees in scheduled batches
- [ ] Disable legacy authentication protocols
- [ ] Enforce MFA — block sign-ins without MFA
- [ ] Document MFA policy and maintain enrollment records
- [ ] Include MFA enrollment in new-hire onboarding process
- [ ] Schedule annual MFA method review and policy update

Need Help Implementing MFA?

First Underwriters specializes in helping small businesses strengthen their cybersecurity posture and secure the right cyber liability coverage. MFA implementation directly impacts your insurability, premiums, and risk profile.

www.firstunderwriters.com

© First Underwriters Insurance Brokers | www.firstunderwriters.com

This guide is for informational purposes only and does not constitute professional cybersecurity advice.