🔍 Что учитывать перед включением MFA

- MFA значительно повышает безопасность — без неё злоумышленники могут получить доступ к учётке через взлом пароля. (CRN)
- Есть два основных подхода: **per-user MFA** (включение для отдельных пользователей) и использование правил доступа (например, политик условного доступа).
- У вас должны быть права администратора (например, глобальный администратор или администратор безопасности).
- Пользователи должны быть готовы настроить дополнительный метод аутентификации (телефон, приложение-аутентификатор и т.д.).

✅ Шаги включения MFA

Ниже приведены основные методы — вы можете выбрать наиболее подходящий для вашей организации.

Метод 1: Включение MFA для отдельных пользователей (per-user)

1. Войдите в портал администратора Microsoft 365: https://admin.microsoft.com
2. Перейдите в раздел **Пользователи → Активные пользователи**. (NinjaOne)
3. Выберите пользователя(ей), для которого хотите включить MFA.
4. Нажмите на ссылку или кнопку **Многофакторная аутентификация** (Multi-factor authentication). (ManageEngine)
5. В открывшейся панели выберите для пользователя статус **Включено** или **Обязательно** (Enabled / Enforced). (NinjaOne)
6. При следующем входе пользователь будет перенаправлен на экран настройки MFA: выбор метода (приложение, SMS, звонок и др.) и активация.

Метод 2: Использование настроек MFA через портал Microsoft Entra ID (ранее Azure AD)

1. Войдите в Microsoft Entra админ-центр.
2. Перейдите: **Entra ID → Аутентификационные методы** или **Entra ID → Многофакторная аутентификация**. (Microsoft Learn)
3. На странице настроек можно:
    - Установить методы проверки (SMS, звонок, приложение) (Microsoft Learn)
    - Настроить исключения (доверенные IP-адреса) — например, если из офиса вход осуществляется из конкретного диапазона IP. (Microsoft Learn)
    - Установить правило «Запомнить устройство/браузер» (то есть не запрашивать MFA снова в течение X дней) для удобства. (Microsoft Learn)

Метод 3: Включение через политики условного доступа (Conditional Access)

- В Microsoft Entra можно создать политику условного доступа, которая требует MFA при определённых условиях (например, при входе из неизвестного устройства или из другого гео-локации). Это более гибкий подход для компаний. (Microsoft Learn)
- Рекомендуется комбинировать с блокировкой устаревшей аутентификации (legacy authentication) для повышения безопасности. (NinjaOne)

📋 **После включения: проверка и обслуживание**

- Проверьте статус MFA для всех пользователей — кто настроил, кто нет.
- Убедитесь, что пользователи получили инструкции: как настроить приложение-аутентификатор, как использовать резервный метод.
- Держите список пользователей, кто может сбросить или помочь с проблемами MFA.
- Включите мониторинг: следите за попытками входа, которые требуют MFA и фиксируйте исключения.
- Регулярно проверяйте настройки: возможно, потребуется обновление политик или методов (например, убрать SMS-код, если придумана более безопасная альтернатива).