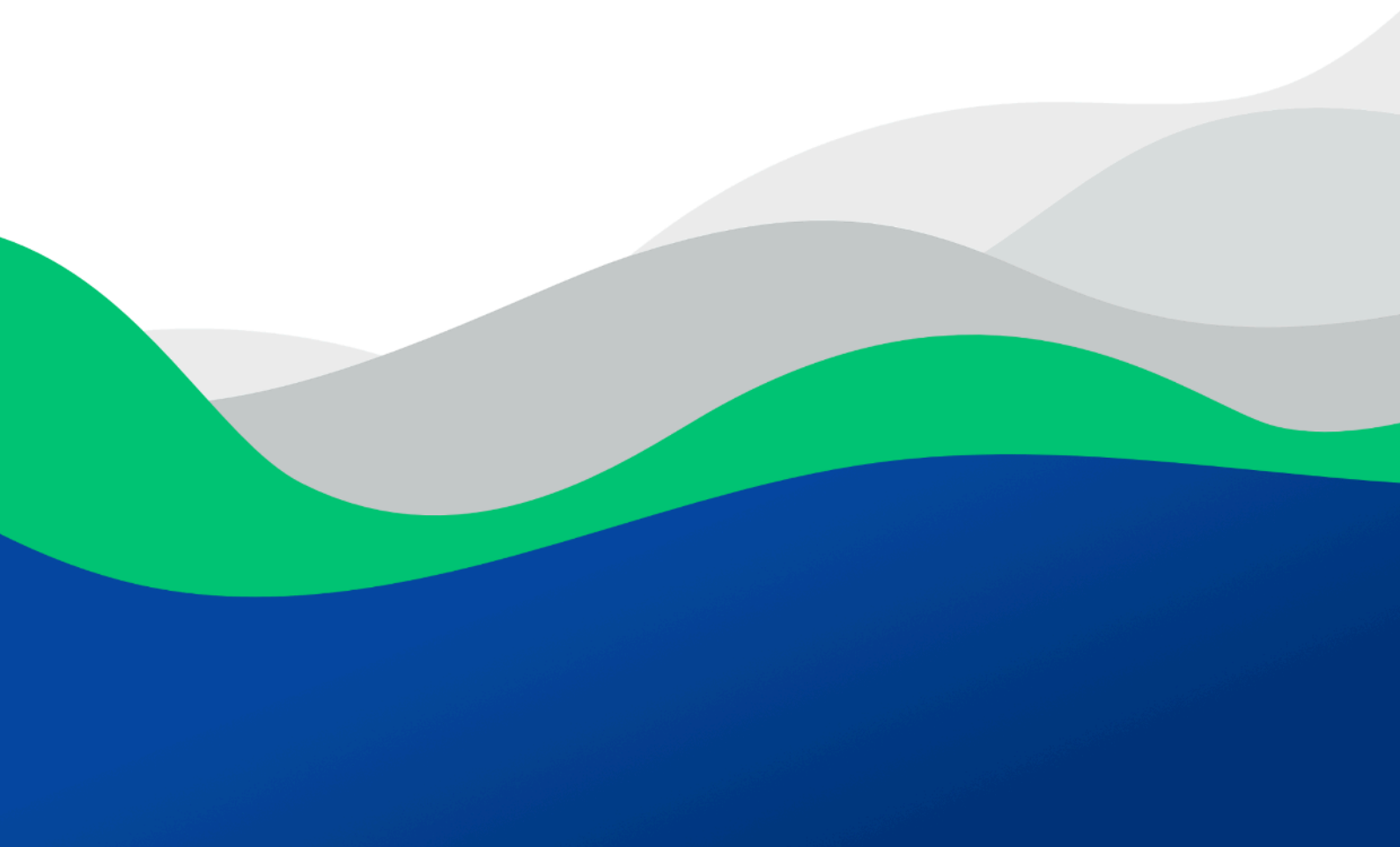
Rublon

Rublon Deployment Best Practices



Inhaltsverzeichnis

1. Übersicht

Rublon MFA ist eine Multi-Faktor-Authentifizierungsplattform, die die Anwendungen, Server und Netzwerke Ihrer Organisation vor Datenlecks schützt, indem sie bei Benutzeranmeldungen einen zweiten Faktor zur Verifizierung erfordert. Da kompromittierte Passwörter eine der Hauptursachen für Sicherheitsvorfälle sind, stellt die Implementierung von Rublon MFA eine entscheidende Verteidigungsschicht dar, die das Risiko einer Kontoübernahme und unbefugten Zugriffe erheblich reduziert.

Dieser Leitfaden erklärt, wie Sie Rublon MFA in Ihrer Umgebung planen, implementieren und bereitstellen, wobei die bewährten Vorgehensweisen (Best Practices) auf jedem Schritt berücksichtigt werden.

(Hinweis: Dies ist ein Best Practices Guide und kein Ersatz für die Rublon-Dokumentation. Für detaillierte Schritt-für-Schritt-Anleitungen siehe Rublons offizielle Dokumentation.)

Warum Sie diesen Guide benötigen:

Zweck dieses Guides ist es, IT-Administratoren und Projektteams mit einem klaren Fahrplan für die Implementierung von Rublon MFA auszustatten.

Was abgedeckt wird:

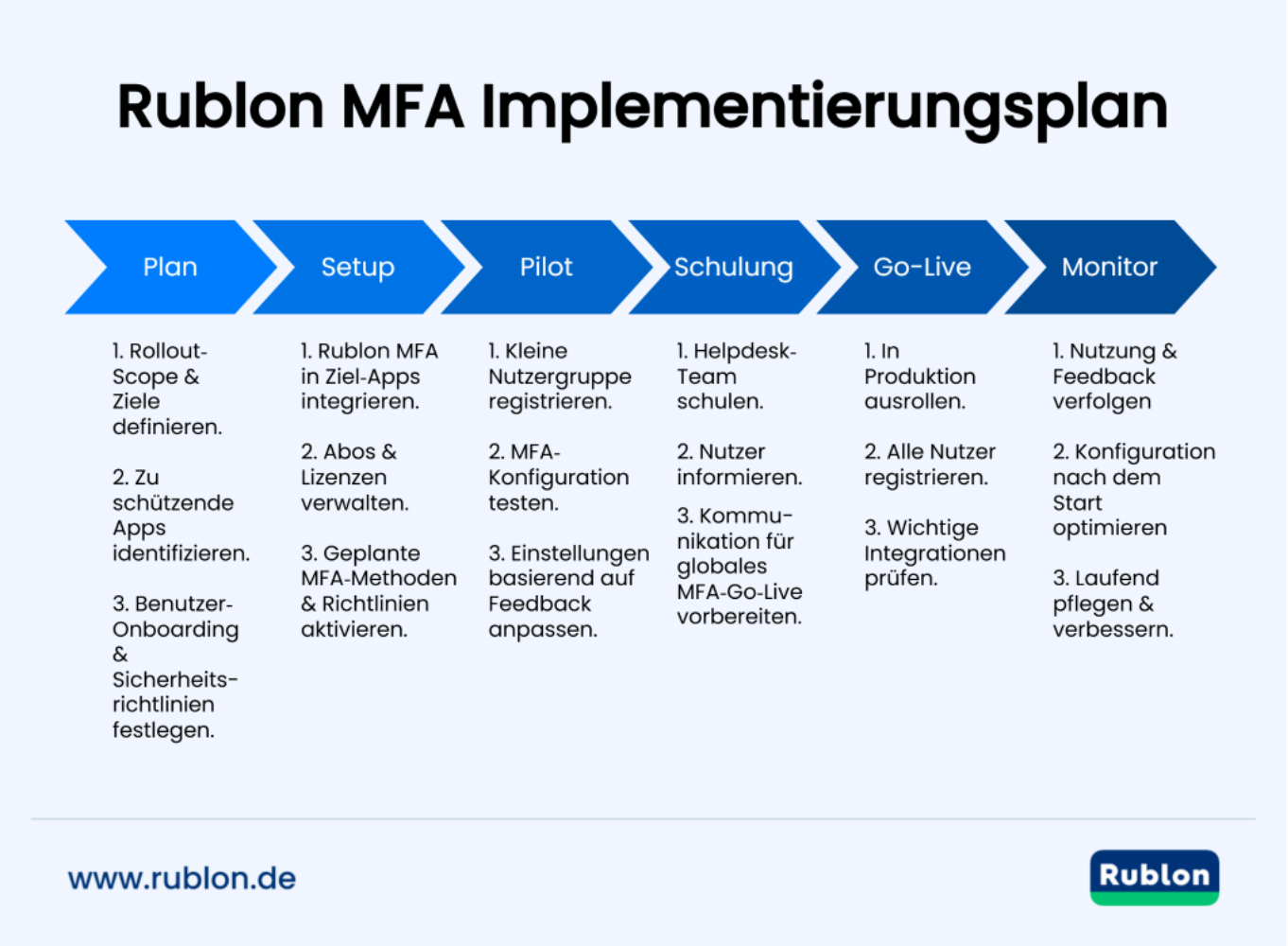
Wir behandeln alle Schritte von der frühen Planungsphase (Vorbereitung Ihrer Admin-Umgebung und Registrierungsstrategie) über die Konfiguration von Anwendungen, das Festlegen von Richtlinien, die Kommunikation mit Endanwendern, das Training Ihres Helpdesks bis hin zum Go-Live. Unser Ziel ist es, Ihre Implementierung so einfach und erfolgreich wie möglich zu gestalten.

Für wen dieser Guide gedacht ist:

Dieser Guide richtet sich an alle, die für die Bereitstellung von Rublon in einer Organisation verantwortlich sind. Unabhängig davon, ob Sie Security Manager, IT-Admin oder Projektleiter sind, der für die Einführung von Rublon verantwortlich ist, dieser Guide ist für Sie gedacht.

2. Planen Sie Ihr Deployment

Erfolgreiche MFA-Deployments beginnen mit einer guten Planung. In dieser Phase entwickeln Sie Ihre Rollout-Strategie für Rublon und bereiten das administrative Fundament für Ihre Organisation vor. Zu den wichtigsten Aktivitäten gehören das Einrichten Ihres Rublon Admin Console Accounts, das Zuweisen von Administratorrollen, die Verwaltung Ihres Rublon-Abonnements und die Entscheidung, wie sich Benutzer für MFA registrieren werden. Eine gründliche Planung an dieser Stelle spart später Zeit und verhindert Störungen. Entscheidend ist, diese Punkte im Voraus zu klären und Ihre Entscheidungen zu dokumentieren.



2.1. Richten Sie Ihre Organisation in der Rublon Admin Console ein

- Beginnen Sie mit der Registrierung Ihrer Organisation in der Rublon Admin Console. Dies umfasst die Registrierung für ein Rublon-Konto, um die Instanz Ihrer Organisation in

unserer Cloud-Konsole zu erstellen. Stellen Sie sicher, dass Sie Ihre E-Mail-Adresse bestätigen und alle erforderlichen Registrierungsschritte abschließen.

- Nach der Registrierung wird in der Rublon Admin Console eine neue Organisation mit einem Administrator-Account des Typs **Owner** erstellt.
- Sobald Sie sich in der Admin Console befinden, machen Sie sich mit dem Aufbau vertraut und lernen Sie, wie Sie Anwendungen, Benutzer und Richtlinien verwalten. Werfen Sie dazu einen Blick in die Dokumentation zur Rublon Admin Console, die eine umfassende Beschreibung aller Tabs und Funktionen der Konsole bietet.

2.2. Administrative Rollen zuweisen

- Rublon unterstützt rollenbasierten administrativen Zugriff in der Admin Console, sodass Sie administrative Aufgaben an andere delegieren können, während die Sicherheit gewahrt bleibt.
- Legen Sie fest, wer für verschiedene Aspekte des Deployments verantwortlich ist (z. B. Gesamtverantwortung, Benutzerverwaltung, Helpdesk-Support usw.), und weisen Sie die entsprechenden Administratorrollen in der Rublon Admin Console zu.
- Das erste Konto, das Sie bei der Registrierung für die Admin Console erstellt haben, ist der **Owner** (Super-Admin).
- Als Best Practice sollten Sie mindestens einen weiteren Administrator mit Owner-Berechtigung zuweisen, um Redundanz sicherzustellen, falls ein Administrator nicht verfügbar ist. Owner-Admins können Rollen vergeben und andere Administratoren verwalten. Stellen Sie daher sicher, dass Sie die richtigen Personen für diese Top-Level-Berechtigungen auswählen.
- Sie können weitere Administratorkonten mit Rollen wie **Administrator**, **User Manager** oder **Help Desk** erstellen, um Verantwortlichkeiten aufzuteilen. Ein Help-Desk-Administrator kann beispielsweise bei alltäglichen Benutzeranfragen unterstützen (z. B. erneutes Versenden von Registrierungsmails), ohne vollen Zugriff auf alle Einstellungen zu haben.
- Verwenden Sie Administrative Units, um den Zugriff auf bestimmte Benutzergruppen für ausgewählte Administratoren zu steuern.
- Das frühzeitige Einrichten von Administratorrollen stellt sicher, dass Verantwortlichkeiten während des Rollouts und bei der späteren Wartung klar definiert sind und Engpässe vermieden werden.

2.3. Abonnement und Lizenzen verwalten

- Erfassen Sie die Anzahl der zu schützenden Benutzerkonten und stellen Sie sicher, dass Ihr Rublon-Abonnement diese abdeckt.
- Während der kostenlosen Testphase können Sie alle Rublon-Funktionen mit allen Benutzern testen. Vor dem Go-Live müssen Sie jedoch den passenden Abonnementplan auswählen (Anzahl der geschützten Benutzer und Laufzeit). Wenn Sie die Lizenzierung vorab klären, vermeiden Sie Begrenzungen der Benutzeranzahl oder unerwartete Kosten während des Deployments.
- Dies ist auch ein guter Zeitpunkt, um das Rublon-Preismodell zu prüfen. Beachten Sie, dass SMS-Nachrichten und Telefonanrufe zusätzliche Kosten verursachen, sodass Sie entscheiden können, ob Sie diese Authentifizierungsmethoden benötigen. Falls ja, berücksichtigen Sie die zusätzlichen Kosten für Phone Credits bei der Bewertung der Gesamtkosten für Deployment und Wartung.
- Wenn alles vorbereitet ist, starten Sie Ihr Rublon Business-Abonnement (siehe: Wie starte ich ein Rublon Business-Abonnement?).

2.4. Definieren Sie die Anwendungen, die Sie schützen möchten

Nehmen Sie sich Zeit, eine Liste aller Anwendungen und Systeme zu erstellen, die Sie mit Rublon MFA absichern möchten. Dieser Schritt ist entscheidend für die Planung des Umfangs Ihres Deployments, die Zuweisung von Verantwortlichkeiten und dafür, den Integrationsprozess schneller und strukturierter zu gestalten.

Beginnen Sie damit, Ihre IT-Infrastruktur zu analysieren und Systeme zu identifizieren, die sensible Daten verarbeiten oder Zugriff auf geschäftskritische Prozesse bieten. Dazu gehören beispielsweise Cloud-Services, VPNs, E-Mail-Plattformen, Identity Provider, Remote-Access-Lösungen, On-Premises-Anwendungen, Entwickler-Tools und interne Portale.

Listen Sie alle Systeme, Anwendungen und Anmeldepunkte auf, die Sie absichern möchten. Für jede Anwendung, die Sie mit Rublon MFA schützen wollen, dokumentieren Sie Folgendes:

- **Anwendungsname** – z. B. „Outlook Web App (OWA)“, „Fortinet FortiGate SSL VPN“, „Remote Desktop Gateway“.
- **Integrationstyp** – z. B. Entscheidung, ob Sie die Integration mit Fortinet FortiGate SSL VPN über RADIUS oder LDAP durchführen.

- **Rublon MFA-Integrationsmethode** – z. B. Rublon Authentication Proxy, dedizierter Connector, dediziertes Plugin.
- **Link zur Integrationsdokumentation** – Link zur passenden Rublon-Integrationsdokumentation (z. B. „https://rublon.com/doc/fortinet-ldap/“).

Durch das Zusammenfassen dieser Informationen in einer einfachen Tabelle erhalten Sie eine klare Übersicht darüber, welche Systeme geschützt werden sollen und wie jede Integration umgesetzt wird.

Tipps:

- Es ist nicht zwingend erforderlich, sofort jedes einzelne System mit MFA zu schützen. Sie können mit den kritischsten oder am häufigsten genutzten Systemen beginnen und die Abdeckung im Laufe der Zeit erweitern.
- Identifizieren Sie alle Systeme, die aufgrund von Sicherheitsrichtlinien und Compliance-Anforderungen unbedingt im initialen Rollout enthalten sein müssen (zum Beispiel kann die Absicherung eines VPNs durch eine Vorschrift vorgeschrieben sein).
- Ermitteln Sie Randfälle, bei denen MFA nicht ohne Weiteres unterstützt wird (z. B. Legacy-Systeme). Für diese Systeme benötigen Sie möglicherweise einen speziellen Ansatz oder Sie akzeptieren zunächst, dass diese außen vor bleiben, planen jedoch ihre spätere Einbindung.
- Verwenden Sie die von Ihnen erstellte Anwendungsliste als Arbeitsdokument während des gesamten Deployment-Projekts. Aktualisieren Sie diese in den Integrations- und Testphasen mit Deployment-Notizen, zugewiesenen Technikern und Links zu interner Konfigurationsdokumentation.
- Pflegen Sie die Dokumentation auch nach dem Deployment und aktualisieren Sie sie, um neue Anwendungen aufzunehmen, sobald Sie entscheiden, weitere Systeme mit Rublon MFA zu schützen.

2.5. Zu aktivierende Authentifizierungsmethoden auswählen

Dokumentieren Sie die zugelassenen Authentifizierungsmethoden sowie alle ausgeschlossenen Methoden. Falls zutreffend, unterscheiden Sie dabei nach Anwendungen oder Benutzergruppen. Während des Deployments konfigurieren Sie Rublon Policies, um diese Entscheidungen abzubilden (z. B. Deaktivierung von SMS für eine bestimmte Benutzergruppe oder Erzwingen von FIDO-Sicherheitsschlüsseln nur für eine bestimmte kritische Anwendung).
Berücksichtigen Sie auch die Benutzerfreundlichkeit: Mehr Optionen ermöglichen eine größere

Flexibilität und decken mehr Szenarien ab. Kritische Infrastrukturen sollten jedoch ausschließlich mit den sichersten Methoden geschützt werden, wie etwa von FIDO-Sicherheitsschlüsseln.

Rublon MFA unterstützt eine Vielzahl von Authentifizierungsmethoden. Sie können entscheiden, welche Methoden Sie aktivieren, basierend auf Ihren Sicherheitsanforderungen und dem Benutzerkomfort. In der Rublon Admin Console können Sie Richtlinien (Policies) erstellen, in denen Sie konfigurieren, welche Authentifizierungsmethoden in jeder Richtlinie verfügbar sind. Diese Richtlinien können anschließend bestimmten Anwendungen oder Benutzergruppen zugewiesen werden.

Während der Planung entscheiden Sie, welche Optionen für Ihre Umgebung sinnvoll sind:

- **Push vs. OTP:** Push-Benachrichtigungen über die Rublon Authenticator App sind benutzerfreundlich und sicher. TOTP-Codes (die rotierenden 6-stelligen Codes) sind eine gute Backup-Option, sollten Benutzer offline sein. Für mehr Flexibilität können sowohl Push (Mobile Push) als auch TOTP (Passcode) aktiviert werden.
- **SMS und Telefon:**
  - SMS Link ist eine praktische Methode, erfordert jedoch eine aktive Internetverbindung.
  - SMS Passcode erreicht Benutzer auch ohne Smartphone oder aktive Internetverbindung, ist jedoch weniger sicher als Push oder FIDO-Sicherheitsschlüssel.
  - Telefonanruf ist eine gute Alternative für Festnetztelefone.
  - Alle diese Methoden verursachen Phone Credits-Kosten. Aktivieren Sie sie daher nur für Benutzer, die sie tatsächlich benötigen.
- **FIDO-Authentifizierung:** Wenn Benutzer über Hardware- oder Software-Passkeys oder FIDO2-Sicherheitsschlüssel wie YubiKey verfügen, unterstützt Rublon diese. Die FIDO-Methode bietet dank Phishing-Resistenz das höchste Sicherheitsniveau. Der Kauf von FIDO-Keys für alle Mitarbeiter kann jedoch kostenintensiv sein. Eine praktikable Alternative sind phishingsichere Software-Passkeys, die auf dem Computer oder Telefon des Benutzers gespeichert werden.
- **Weitere Methoden:** Ziehen Sie auch andere Authentifizierungsmethoden wie QR-Code und E-Mail-Link in Betracht.

2.6. Benutzerregistrierungsstrategie festlegen

Eine der wichtigsten Planungsentscheidungen ist, wie Benutzer in Rublon MFA registriert werden. Rublon bietet verschiedene Methoden zur Benutzerregistrierung. Wählen Sie die Methode (oder eine Kombination von Methoden), die am besten zur Größe und Benutzerbasis Ihrer Organisation passt. Die Methoden zur Benutzerregistrierung in Rublon umfassen:

- **Automatische Registrierung:** Wenn sich ein Benutzer erstmals bei einer durch Rublon geschützten Anwendung anmeldet, wird er automatisch zu Ihrer Organisation hinzugefügt. Diese Methode ist besonders praktisch, da sie kein vorheriges Laden aller Benutzer in die Rublon Admin Console erfordert. Benutzer registrieren sich bei der ersten Nutzung selbst. Diese Methode eignet sich gut für schrittweise Rollouts und technikaffine Benutzergruppen.
- **Registrierung mit Genehmigung:** Bei kleineren Deployments oder speziellen Anwendungsfällen können Anmeldeversuche von Benutzern eine E-Mail-Anfrage an Administratoren auslösen, die dann genehmigt werden muss. Benutzer werden erst hinzugefügt, wenn einer der Administratoren die Mitgliedschaft in der Organisation bestätigt.
- **Manuelle Registrierung (Einzelne Benutzer hinzufügen):** Sie können Benutzer manuell über add users zu Rublon MFA hinzufügen. Diese Option eignet sich für Pilotprojekte, ist jedoch für die Registrierung einer großen Anzahl von Benutzern meist zu aufwendig.
- **Manuelle Registrierung (Import aus CSV):** Sie können Benutzer über import users from a CSV file hinzufügen. Diese Option ermöglicht eine schnellere und effizientere Benutzeranlage, spart Zeit und reduziert die Fehlerwahrscheinlichkeit.
- **Manuelles Bypass-„Silent"-Enrollment:** Sie können den Enrollment Type auf Manual Bypass setzen. Dadurch bleibt der Authentifizierungsprozess aus Sicht des Benutzers unverändert (keine MFA-Abfrage), die Benutzer erscheinen jedoch in der Registerkarte „Users" der Admin Console. Dies ist eine gute „stille" Enrollment-Option für den produktiven Einsatz, wenn keine einmalige Massenregistrierung gewünscht ist.
- **Directory Synchronization:** In größeren Organisationen kann das manuelle Hinzufügen von Benutzern unpraktikabel sein. Rublon bietet die Möglichkeit, Benutzer automatisch über vorhandene Verzeichnisse zu importieren und zu aktualisieren (Entra ID Sync, Active Directory Sync). So bleibt Ihre Benutzerbasis in Rublon MFA stets mit Ihrer primären Identitätsquelle synchronisiert.

Tipps:

- Dokumentieren Sie die von Ihnen verwendeten Methoden zur Benutzerregistrierung sowie deren Reihenfolge.
- Planen Sie, wie mit Benutzern umgegangen wird, die später hinzukommen (z. B. neue Mitarbeiter oder solche, die den initialen Onboarding-Prozess verpasst haben).
- Die Flexibilität von Rublon erlaubt es, jederzeit Benutzer hinzuzufügen. Empfehlenswert ist jedoch ein klarer Prozess, bei dem die MFA-Registrierung fest in die IT-Einrichtung neuer Mitarbeiter integriert ist.

2.7. Benutzergruppen definieren

Benutzergruppen spielen eine zentrale Rolle bei der Strukturierung Ihres Rublon-Deployments, da sie es ermöglichen, Benutzer in überschaubare Einheiten zu gliedern, den Zugriff auf Anwendungen zu steuern und Zugriffsrichtlinien zuzuweisen.

Nehmen Sie sich vor dem Rollout Zeit, um festzulegen, welche Benutzergruppen in Rublon existieren sollen und wie diese verwaltet werden.

- **Manuelle Gruppenerstellung:**
  - Sie können Benutzergruppen manuell hinzufügen in der Rublon Admin Console. Diese Methode bietet Ihnen die volle Kontrolle und eignet sich für kleinere Umgebungen oder Pilot-Deployments.
  - **Wann diese Methode sinnvoll ist:** Wenn Sie schnell kleine, benutzerdefinierte Gruppen für Tests anlegen möchten oder keine Synchronisierung von Benutzern aus einem externen Verzeichnis planen.

- **Verzeichnis-synchronisierte Gruppen:**
  - Wenn Sie Directory Sync verwenden, kann Rublon Benutzer und deren Gruppenzugehörigkeiten aus Ihrem externen Verzeichnisdienst (z. B. Microsoft Entra ID oder Active Directory) importieren. Diese synchronisierten Gruppen lassen sich direkt in Richtlinienkonfigurationen und Anwendungszuweisungen nutzen.
  - **Wann diese Methode sinnvoll ist:** Wenn Sie die Verwaltung von Gruppenmitgliedschaften zentral in Ihrem Identity Provider belassen und manuelle Gruppenverwaltung in Rublon vermeiden möchten.

2.8. Strategie zur Registrierung von Authenticatoren festlegen

Nachdem Sie entschieden haben, wie Benutzer in Rublon MFA registriert werden, empfiehlt es sich, festzulegen, wie diese ihre Authenticatoren registrieren.

Ein Authenticator dient dazu, die Identität eines Benutzers während des zweiten Authentifizierungsschritts zu verifizieren (typischerweise nach Eingabe des Passworts). Authenticatoren können Telefonnummern (Festnetz oder Mobilfunk), E-Mail-Adressen, die Rublon Authenticator Mobile App, Drittanbieter-Apps sowie WebAuthn/U2F-Sicherheitsschlüssel umfassen. Jeder Authenticator muss registriert sein, bevor er genutzt werden kann.

Wählen Sie eine Strategie, die sicherstellt, dass jeder Benutzer spätestens zu dem Zeitpunkt, an dem MFA für sein Konto erzwungen wird, mindestens einen Authenticator registriert hat. Rublon bietet eine Reihe flexibler Optionen zur Registrierung von Authenticatoren, abhängig von der Integrationsmethode der Anwendung und den Richtlinien Ihrer Organisation. Beachten Sie, dass sich beide Optionen auch kombinieren lassen, z. B. indem die Mehrheit der Benutzer Self-Enrollment nutzt und nur technisch weniger versierte Benutzer Registrierungs-E-Mails erhalten.

- **Self-Enrollment über „Authentikatoren verwalten“:**
  Wenn Ihre Rublon-geschützte Anwendung den Rublon Prompt unterstützt, können sich Benutzer über die Ansicht **Authentikatoren verwalten** selbst registrieren.
  - Dieses Self-Service-Verfahren ist intuitiv und funktioniert in den meisten Umgebungen zuverlässig. Benutzer können die Rublon Authenticator Mobile App hinzufügen, Sicherheitsschlüssel registrieren und weitere Authentifizierungsmethoden eigenständig verwalten.
    (Siehe: Rublon User Guide – Registrierung)
  - Die Ansicht **Authentikatoren verwalten** kann pro Anwendung aktiviert oder deaktiviert werden, indem die Option **Let Users Manage Authenticators** in den Anwendungseinstellungen ein- oder ausgeschaltet wird.
  - Die wichtigste Einschränkung dieser Methode ist, dass Benutzer Zugriff auf mindestens eine Anwendung benötigen, die den Rublon Prompt unterstützt. Soll die Registrierung der Authenticatoren bereits vor der Integration Ihrer Anwendungen mit Rublon erfolgen, empfiehlt sich der Versand von Registrierungs-E-Mails.

- **Authenticator-Registrierung über von Administratoren versendete Registrierungs-E-Mails:**
    - In Umgebungen, in denen Self-Enrollment eingeschränkt ist oder der Rublon Prompt nicht zur Verfügung steht, können Administratoren aus der Admin Console eine Registrierungs-E-Mail versenden. Diese enthält einen Link, über den der Benutzer Schritt für Schritt durch den Registrierungsprozess geführt wird.
    - Diese Option ist sinnvoll, wenn der Rublon Prompt aus Sicherheits- oder Compliance-Gründen deaktiviert ist, die Integration den Rublon Prompt nicht unterstützt (z. B. Deployments mit dem Rublon Authentication Proxy) oder wenn Sie eine strengere Kontrolle darüber wünschen, wer sich registriert und zu welchem Zeitpunkt.

2.9. Sicherheitsrichtlinien definieren

Rublon bietet die Möglichkeit festzulegen, wann und wie MFA angewendet wird, Regeln für Remembered Devices (gemerkte Geräte) zu definieren und autorisierte Netzwerke zu verwalten. Legen Sie idealerweise bereits vor der Konfiguration in der Admin Console fest, welche Richtlinien für unterschiedliche Anwendungen und Benutzergruppen gelten. Eine saubere Dokumentation im Vorfeld unterstützt Sie dabei, eine umfassende Zugriffskontrollstrategie zu entwickeln, die sich einfach implementieren und dauerhaft pflegen lässt.

Ressourcen zum Thema Richtlinien:

- Rublon Admin Console - Policies
- Group Policies
- Authentication Methods Policy
- Authorized Networks Policy
- Remembered Devices Policy

Best Practices für Rublon-Richtlinien:

- Stellen Sie sicher, dass die Global Policy Ihre grundlegenden Zugriffskontrollanforderungen erfüllt, sodass keine Anpassung für jede einzelne Anwendung und Benutzergruppe notwendig ist.

- Jede Custom Policy sollte einen eindeutigen und leicht verständlichen Namen haben, damit es keine Verwechslungen bei der Zuweisung zu einer Anwendung oder Benutzergruppe gibt.
- Achten Sie auf mögliche False Negatives, z. B. wenn ein Benutzer MFA erwartet, aber keine Abfrage erfolgt. Überprüfen Sie, ob Ihre Richtlinien alle Szenarien abdecken.
- **Best Practices für Authentication Methods Policy**
    - Entscheiden Sie, ob eine Standard-Authentifizierungsmethode aktiviert werden soll.
- **Best Practices für Authorized Networks Policy**
    - Definieren Sie ausschließlich wirklich sichere Netzwerke.
    - Viele Organisationen gehen von standortbasierter Vertrauenswürdigkeit weg, dennoch kann es in Ihrer Umgebung sinnvoll sein.
    - Wenn Sie diese Policy aktivieren, halten Sie die IP-Liste aktuell. Testen Sie immer: Ein Login von einer nicht autorisierten IP sollte MFA auslösen, während ein Login von einer autorisierten IP keine Abfrage erzeugt.
- Best Practices für Remembered Devices Policy
    - Konfigurieren Sie die Dauer entsprechend Ihrer Sicherheitsanforderungen. Gängige Werte sind 2 Tage, 7 Tage und 14 Tage.
    - Deaktivieren Sie die Remembered Devices Policy vollständig bei Anwendungen mit besonders hohen Sicherheitsanforderungen.
    - Weisen Sie Administratoren und den Helpdesk an, wie sie die Remembered Devices der Benutzer verwalten.

2.10. Anwendungsspezifische Einstellungen definieren

- Legen Sie den Fail Mode (Fehlermodus) für jede Anwendung fest. (Weitere Informationen: Rublon Business Continuity – Vorbereitungsleitfaden)

- Erfahren Sie mehr über die Best Practices für das Testen von Rublon MFA in einer Produktionsumgebung (die dort genannten Empfehlungen gelten ebenso für Test- und Staging-Umgebungen während der ersten Bereitstellung).

2.10.1. Rublon Authentication Proxy

Best Practices:

- Best Practices für die Installation und Konfiguration des Rublon Authentication Proxy

Wichtige Ressourcen:

- Rublon Authentication Proxy - Documentation
- Rublon Help - Rublon Authentication Proxy
- Configuring the Rublon Authentication Proxy as a RADIUS Proxy Server
- Configuring the Rublon Authentication Proxy as an LDAP Proxy Server
- Rublon Authentication Proxy RADIUS Modes Explained

2.10.2. Rublon for Windows

Best Practices:

- Bevor Sie die erste Installation durchführen, lassen Sie mindestens eine aktive Sitzung eines angemeldeten Benutzers geöffnet (vorzugsweise eine lokale Sitzung), um eine Situation zu vermeiden, in der eine fehlerhafte Konfiguration, fehlende erforderliche Bibliotheken im System oder zusätzliche Software, die mit dem Rublon for Windows Connector interferiert, zum Verlust des Zugriffs auf die Maschine führt.
- Aktivieren Sie bei der ersten Installation MFA nur für RDP-Verbindungen, damit der lokale Zugriff ohne MFA im Falle von Installationsproblemen weiterhin möglich ist.
- Die Installation des Connectors endet mit einem Systemneustart, der bestehende Remote Desktop Protocol (RDP)-Sitzungen unterbrechen kann. Planen Sie die Installation daher außerhalb der Stoßzeiten, um Störungen zu minimieren.

- Wenn Sie mehrere Endpunkte haben und Rublon for Windows auf allen bereitstellen müssen, verwenden Sie PDQ Deploy, Microsoft System Center Configuration Manager (SCCM) oder Intune, um die Bereitstellung zu automatisieren.
- Stellen Sie sicher, dass die Firewall auf dem Server, auf dem Sie Rublon for Windows installiert haben, die Rublon-Kommunikation über TCP-Port 443 nicht blockiert.
- Aktivieren Sie den Offline-Modus, um den Benutzerzugriff mit Rublon MFA auch dann zu schützen, wenn keine Internetverbindung besteht.

Wichtige Ressourcen:

- Rublon MFA for Windows - Documentation
- Rublon MFA for Windows - FAQ
- Deploy Rublon MFA for Windows using PDQ Deploy
- Deploy Rublon MFA for Windows using SCCM
- Deploy Rublon MFA for Windows using Intune

2.11. Definieren Sie einen Bereitstellungszeitplan und Meilensteine

Ein klar definierter Zeitplan hilft dabei, Kommunikation und Aufgaben zu koordinieren. Er stellt außerdem sicher, dass genügend Zeit für Tests und Anpassungen eingeplant wird. Für größere Unternehmen wird ein gestuftes Vorgehen (Pilot → breitere Einführung → Erzwingung) empfohlen, anstatt alles auf einmal umzusetzen. Wenn möglich, verwenden Sie eine „stufenweise Registrierung“ (staged enrollment): Beginnen Sie mit einer Kernbenutzergruppe, die sich zunächst mit Rublon vertraut macht, nehmen Sie deren Feedback auf und erweitern Sie anschließend auf größere Gruppen.

Das folgende Beispiel zeigt einen Rublon-Bereitstellungsplan für ein großes Unternehmen (mehr als 20.000 Mitarbeitende). Kleinere Unternehmen können diese Schritte in kürzerer Zeit durchführen. Dieses Beispiel dient lediglich als Orientierung.

- **Pilotstart:** z. B. „Woche 1: Rublon im Testmodus für IT-Administratoren oder eine Pilotgruppe bereitstellen.“

- **Registrierungsphase (Enrollment period):** z. B. „Woche 2–3: Ankündigung an alle Mitarbeitenden, Registrierung in der Admin Console und Hinzufügen ihrer Authenticatoren.“
- **Phase der Anwendungsintegration:** z. B. „Woche 2: Schützen Sie ein VPN und eine kritische Anwendung mit Rublon (für Pilotbenutzer). Woche 4: Erweiterung auf alle wichtigen Anwendungen.“
- **Verfeinerungen:** z. B. „Woche 3: Erste Ergebnisse der Pilotphase überprüfen und bei Bedarf Anpassungen vornehmen.“
- **Go-Live (Erzwingungsdatum):** z. B. „Woche 5, Montag: MFA-Erzwingung für alle Benutzer in den relevanten Systemen aktivieren.“
- **Nachbereitungsprüfung (Post go-live review):** z. B. „Woche 5: Überprüfung der Nutzungsmetriken, Unterstützung von Benutzern, die sich noch nicht registriert haben, und Anpassung der Einstellungen bei Bedarf.“

3. Rublon MFA im Testmodus bereitstellen

Nach Abschluss der Planungsphase ist es an der Zeit, Rublon in Ihre Anwendungen zu integrieren und gründliche Tests durchzuführen. Ziel ist es, dass Rublon MFA nahtlos mit der IT-Umgebung Ihrer Organisation funktioniert, ohne den Geschäftsbetrieb zu unterbrechen.

Am Ende der Testphase sollten Sie Folgendes erreicht haben:

- Alle Ihre Schlüsselanwendungen sind in Rublon MFA integriert.
- Ein bewährter Anmeldeablauf für jede mit Rublon integrierte Anwendung ist vorhanden.
- Die Gewissheit, dass sich Benutzer erfolgreich registrieren und anmelden können.
- Ein Verständnis dafür, welche Richtlinien (Policies) und Einstellungen basierend auf dem Feedback aus der Pilotphase angewendet werden sollen.

Während der gesamten Testphase sollten Sie die Rublon-Dokumentation griffbereit halten. Wenn komplexe Probleme auftreten, konsultieren Sie die entsprechende Dokumentation:

- Rublon Integration Dokumentation
- Rublon Downloads
- Rublon Admin Console - Documentation
- Rublon User Guide
- Rublon Help Desk Guide
- Rublon Business Continuity – Vorbereitungsleitfaden

3.1. Test in einer Staging-Umgebung

Bevor Sie die Lösung in der Produktionsumgebung bereitstellen, können Sie Rublon-Integrationen in einer kontrollierten Staging-Umgebung testen. Wenn Sie keine Staging- oder Testinstanzen Ihrer Anwendungen haben, können Sie in der Produktionsumgebung einen „Soft Launch“ für eine begrenzte Benutzergruppe in Betracht ziehen (siehe nächsten Abschnitt).

- Integrieren Sie Rublon zunächst in die Testinstanz. Verwenden Sie Testbenutzerkonten, um den Anmeldeablauf (Login Flow) zu prüfen.
- Simulieren Sie sowohl erfolgreiche MFA- als auch Fehlerszenarien. Testen Sie beispielsweise, was passiert, wenn ein Benutzer die Push-Benachrichtigung ablehnt oder einen falschen Code eingibt.
- Wenn ein Rublon Connector den Fail Mode unterstützt, testen Sie diesen ebenfalls.
- Überprüfen Sie, ob die Benutzerbereitstellung (User Account Provisioning) funktioniert – z. B. ob ein neuer Testbenutzer mit den korrekten Informationen in der Rublon Admin Console hinzugefügt wird. Wenn Sie Directory Sync verwenden, stellen Sie sicher, dass der Benutzer vorhanden ist und der richtigen Gruppe zugeordnet ist.
- Überprüfen Sie, ob der Rublon Prompt angezeigt wird und die erwarteten Authentifizierungsmethoden anbietet. Wenn bestimmte Methoden in einer Policy deaktiviert wurden, stellen Sie sicher, dass sie im Prompt nicht auswählbar sind. Wenn Sie benutzerdefinierte Branding- oder Hilfenachrichten konfiguriert haben, prüfen Sie diese ebenfalls.

3.2. Pilotphase mit einer kleinen Benutzergruppe

Eine bewährte Vorgehensweise für die Einführung von MFA (Multi-Factor Authentication) besteht darin, zunächst mit einer Teilmenge realer Benutzer zu starten, bevor die Lösung organisationsweit erzwungen wird. Wählen Sie technikaffine Benutzer (z. B. Mitarbeitende der IT-Abteilung oder des Helpdesk) aus. EAktivieren Sie Rublon MFA nur für diese Benutzer in einigen wenigen Anwendungen:

- Erstellen Sie in der Rublon Admin Console eine Group Policy, die gezielt diese Pilotbenutzer für MFA in einer bestimmten Anwendung erfasst. Beispiel: Die Gruppe „IT Department“ muss MFA für Windows Logons und RDP-Verbindungen verwenden, während alle anderen Benutzer den Status Bypass erhalten.
- Lassen Sie die Pilotbenutzer den Registrierungsprozess (Enrollment) durchlaufen und Rublon in ihrem Arbeitsalltag verwenden. Sammeln Sie ihr Feedback: War die Registrierung einfach? Gab es Systeme, bei denen Rublon nicht funktionierte? Gab es Beschwerden über Prompts (z. B. zu langsam)? Dieses Feedback ist von unschätzbarem Wert, um Ihre Einstellungen vor der unternehmensweiten Einführung zu optimieren.

- Simulieren Sie während der Pilotphase häufige Support-Szenarien mit der Pilotgruppe, z. B. wenn ein Benutzer sein Telefon verliert. Lassen Sie ihn den Wiederherstellungsprozess durchlaufen (z. B. die Verwendung einer Backup-Authentifizierungsmethode oder die Ausstellung eines Bypass Code). Auf diese Weise können Sie auch die Support-Bereitschaft prüfen.

4. Kommunikation mit Endbenutzern

Selbst die beste MFA-Bereitstellung (Multi-Factor Authentication) kann scheitern, wenn die Benutzerkommunikation nicht richtig umgesetzt wird. Eine klare und rechtzeitige Kommunikation stellt sicher, dass die Benutzer verstehen, was passiert, warum es wichtig ist und was sie tun müssen.

Wichtige Ressourcen:

- Rublon User Guide
- Rublon Help Desk Guide

Kommunikationsvorlagen:

- Rublon Kommunikationsvorlagen für Endbenutzer

Best Practices für die Kommunikation mit Endbenutzern:

- Halten Sie es einfach. Verwenden Sie kurze, leicht verständliche Anweisungen.
- Beginnen Sie frühzeitig. Kündigen Sie die Änderung mindestens zwei Wochen vor dem Go-Live an.
- Nutzen Sie mehrere Kanäle: E-Mail, Intranet-Banner, Login-Meldungen oder Chat-Nachrichten.
- Erklären Sie das „Warum“. Betonen Sie, dass MFA sowohl das Unternehmen als auch den Benutzer schützt.
- Verwenden Sie visuelle Elemente. Screenshots helfen, Unsicherheiten zu reduzieren und Supportanfragen zu vermeiden.
- Weisen Sie auf verfügbare Supportressourcen hin. Lassen Sie Benutzer wissen, an wen sie sich wenden können, wenn sie Unterstützung benötigen.
- Fördern Sie die Gerätebereitschaft. Bitten Sie Benutzer, den Rublon Authenticator im Voraus zu installieren.

- Heben Sie den Komfort hervor. Erwähnen Sie die Funktion „Remember this device“ (Dieses Gerät merken), wo sie relevant ist.

5. Helpdesk schulen

Ihr Helpdesk ist die erste Supportinstanz während der Einführung von Rublon MFA. Bereiten Sie das Team frühzeitig vor, um Verwirrung zu vermeiden und Benutzerprobleme schnell zu lösen.

Wichtige Ressourcen:

- Rublon Help Desk Guide
- Rublon Help Wissensdatenbank
- Rublon Admin Console
- Contact Rublon Support

Zentrale Schulungsthemen:

- **Praktische Übungen:** Registrieren Sie das Supportpersonal frühzeitig, damit es Rublon MFA aus Sicht der Endbenutzer erleben kann. Lassen Sie es jede Authentifizierungsmethode testen, die Ihre Organisation unterstützen möchte (Push, TOTP, SMS usw.).
- **Fertigkeiten in der Admin Console:** Stellen Sie sicher, dass die Supportmitarbeitenden wissen, wie man:
    - Benutzer sucht und deren Registrierungsstatus einsehen kann
    - Registrierungs-E-Mails sendet und erneut versendet
    - Benutzergeräte hinzufügt und entfernt
    - Bypass Codes generiert
    - Authentifizierungsprotokolle (Authentication Logs) analysiert
- **Fehlerdiagnose:** Schulen Sie die Mitarbeitenden im Umgang mit häufigen Supportfällen, z. B.:
    - Registrierungs-E-Mail wurde nicht empfangen
    - Gerät wurde verloren oder ersetzt

    - Push-Benachrichtigungen funktionieren nicht
    - Der Benutzer hat Schwierigkeiten mit dem QR-Code oder dem Einrichtungsprozess.

- **Entsprechende Administratorrollen verwenden:** Der Support der Stufe 1 (Level 1 Support) kann eingeschränkten Zugriff haben (z. B. Help Desk-Rolle), während Administratoren oder der Support der Stufe 2 (2nd Level Support) eskalierte Aufgaben mit der Rolle Application Manager oder User Manager bearbeiten.

Best Practices:

- Schulen Sie das Supportpersonal, bevor Rublon MFA in der Produktionsumgebung aktiviert wird.
- Gehen Sie davon aus, dass das Helpdesk-Team Rublon MFA ebenso neu kennenlernt wie Endbenutzer.
- Informieren Sie Rublon-Administratoren über die Unterschiede zwischen Administrator Account und User Account. Stellen Sie klar, dass Administratoren beide Konten benötigen.
- Stellen Sie einfache Schritte zur Verfügung, um häufige Probleme mithilfe von Skripten und Checklisten zu lösen.
- Schulen Sie die Mitarbeitenden darin, die Benutzeridentität zu bestätigen, bevor Bypass Codes ausgegeben werden.
- Weisen Sie darauf hin, wann ein Problem an den Rublon Support weitergeleitet werden soll, falls es intern nicht zeitnah gelöst werden kann.
- Rechnen Sie zum Go-Live mit einem erhöhten Ticketaufkommen. Weisen Sie zusätzliche Supportressourcen zu und richten Sie bei Bedarf spezielle Supportkanäle ein (z. B. „Rublon MFA Help Desk“).

6. Rublon MFA in der Produktionsumgebung bereitstellen

Der Go-Live-Tag ist der Höhepunkt aller Planungs- und Vorbereitungsschritte. In diesem Abschnitt finden Sie eine abschließende Checkliste zur Einsatzbereitschaft, Hinweise zur Durchführung des Rollouts sowie empfohlene Schritte nach der Bereitstellung.

6.1. Go-Live-Readiness-Checkliste

1. **Anwendungen getestet und integriert:** Stellen Sie sicher, dass alle Anwendungen ordnungsgemäß mit Rublon verbunden sind und MFA wie erwartet funktioniert.
2. **Benutzerregistrierung nahezu abgeschlossen:** Streben Sie eine Registrierungsquote von über 90 % an. Identifizieren Sie nicht registrierte Benutzer und erinnern Sie diese zur Registrierung.
3. **Richtlinien überprüft und angewendet:** Stellen Sie sicher, dass alle Policies korrekt zugewiesen sind.
4. **Helpdesk bereit:** Vergewissern Sie sich, dass das Supportpersonal informiert, erreichbar und für den Go-Live vorbereitet ist.
5. **Notfallplan definiert:** Stellen Sie sicher, dass Sie die Empfehlungen aus dem Rublon Business Continuity – Vorbereitungsleitfaden geprüft und umgesetzt haben.
6. **Stakeholder und Benutzer informiert:** Kommunizieren Sie den Zeitpunkt des Go-Live und die Eskalationsprotokolle an die Leitungsebene. Senden Sie eine unternehmensweite Erinnerung.
7. **Rublon-Supportkontakt und wichtige Ressourcen verfügbar:** Stellen Sie sicher, dass alle relevanten Informationen, wie der Rublon-Supportkontakt und die Rublon-Dokumentation, leicht zugänglich sind und bei Bedarf schnell genutzt werden können.

6.2. Go-Live-Durchführung

1. **MFA-Erzwingung aktivieren:** Schalten Sie Ihre Anwendungen so um, dass MFA erforderlich ist (z. B. um 7:00 Uhr).

2. **Aktivität überwachen:** Beobachten Sie die Protokolle (Logs) auf vermehrte Fehler oder fehlgeschlagene Anmeldungen und analysieren Sie Auffälligkeiten umgehend.
3. **In Verbindung bleiben:** Halten Sie während des Go-Live einen Live-Chat oder Telefonkontakt zwischen den Supportverantwortlichen offen, um Informationen in Echtzeit auszutauschen.
4. **Unterstützung bei Bedarf leisten:** Seien Sie bereit, Benutzer zu unterstützen, die sich verspätet registrieren. Geben Sie bei Bedarf Bypass Codes aus und stellen Sie sicher, dass eine Nachverfolgung erfolgt.
5. **Status kommunizieren:** Informieren Sie Stakeholder zur Mittagszeit über den Fortschritt und eventuelle bekannte Probleme.

6.3. Nachbereitung nach dem Go-Live

1. **Nachzügler verwalten:** Erfassen und registrieren Sie Benutzer, die die Anmeldung (Enrollment) verpasst haben (z. B. aufgrund von Urlaub oder Abwesenheit).
2. **Feedback einholen:** Befragen Sie Benutzer und Teamleiter, um Rückmeldungen zum Rollout und zu möglichen Problemen zu sammeln.
3. **Richtlinien anpassen (falls erforderlich):** Optimieren Sie Einstellungen und den Umfang der MFA-Erzwingung basierend auf dem erhaltenen Feedback.
4. **Interne Dokumentation aktualisieren:** Überarbeiten Sie Ihre internen Handbücher und verbessern Sie gegebenenfalls die Benutzerkommunikation.
5. **Team anerkennen:** Teilen Sie Erfolge, bedanken Sie sich bei Mitarbeitenden und Benutzerinnen bzw. Benutzern für ihre Zusammenarbeit.

6.4. Beispielhafter Go-Live-Zeitplan

- **Eine Woche vor der Bereitstellung:** Letzte Registrierungsphase, Helpdesk geschult.
- **Go-Live-Tag (Vormittag):** MFA-Erzwingung aktivieren, Supportkanäle öffnen.
- **Mittags:** Überwachung fortsetzen, auftretende Probleme priorisieren, Leitungsebene informieren.

- **Ende des Tages:** Teambesprechung und Dokumentation der gewonnenen Erkenntnisse.
- **Tag 1 nach dem Go-Live:** Fortgesetzter Support, Nachbearbeitung und Nachverfolgung offener Punkte.

Rublon sp. z o.o.
ul. Stanislawa Wyspianskiego 11
65-036 Zielona Gora
Polen

www.rublon.de