Exchange Online での基本認証の廃止

[アーティクル] • 2022/08/12 • 2 人の共同作成者

この記事の内容

長年にわたり、アプリケーションは基本認証を使用してサーバー、サービス、API エンドポイントに接続してきました。 基本認証とは、アプリケーションが要求ごとにユーザー名とパスワードを送信し、それらの資格情報も多くの場合、デバイスに保存または保存されていることを意味します。 従来、基本認証はほとんどのサーバーまたはサービスで既定で有効になっており、簡単に設定できます。

単純さはまったく悪くありませんが、基本認証を使用すると、攻撃者がユーザーの資格情報を簡単にキャプチャできるようになります (特に、資格情報が TLS によって保護されていない場合)。これにより、盗まれた資格情報が他のエンドポイントやサービスに再利用されるリスクが高まります。 さらに、基本認証が有効なままであれば、多要素認証 (MFA) の適用は単純ではなく、場合によっては可能です。

基本認証は古い業界標準です。この脅威によってもたらされる脅威は、最初にこの機能を無効にすることを発表してから増加の一途をたどっています （「セキュリティの向上 - 共に 」 参照）。より優れた、より効果的なユーザー認証の代替手段があります。

ユーザーとデバイスが企業情報にアクセスするときに、ゼロ トラスト (信用せず、常に検証する) などのセキュリティ戦略を採用するか、リアルタイムの評価ポリシーを適用することを積極的に推奨します。 これらの代替手段を使用すると、ユーザーを偽装する悪いアクターである可能性のある認証資格情報を信頼するのではなく、どのデバイスから何にアクセスしようとしているのかをインテリジェントに判断できます。

これらの脅威とリスクを念頭に置いて、Exchange Online のデータ セキュリティを向上させるための対策を講じます。

> ⓘ **注意**
>
> 基本認証の廃止により、2 段階認証をサポートしていないアプリでアプリ パスワードを使用することもできなくなります。

変更する内容

Exchange Online for Exchange ActiveSync (EAS)、POP、IMAP、リモート PowerShell、Exchange Web サービス (EWS)、オフライン アドレス帳 (OAB)、Outlook for Windows、Mac で基本認証を使用する機能を削除します。

また、使用されていないすべてのテナントで SMTP AUTH を無効にしています。

この決定では、顧客は基本認証を使用するアプリから最新の認証を使用するアプリに移行する必要があります。 最新の認証 (OAuth 2.0 トークン ベースの承認) には、基本認証の問題を軽減するするのに役立つ多くの利点と改善点があります。 たとえば、OAuth アクセス トークンの使用可能期間は限られており、発行先のアプリケーションとリソースに固有であるため、再利用することはできません。 最新の認証では、多要素認証 (MFA) の有効化と設定も簡単に行えます。

この変更はいつ行われますか?

この変更は既に開始されています。新しい Microsoft 365 テナントは セキュリティの既定値 が有効になっているため、基本認証が既にオフになっている状態で作成されます。

2021 年の初めから、既存のテナントの基本認証を無効にし、使用状況が報告されなくなりました。 テナントで基本認証が完全に無効になる前に、常に顧客にメッセージ センター通知を提供します。

2021 年 9 月に、**2022 年 10 月 1 日** より、Exchange Online の Outlook、EWS、RPS、POP、IMAP、EAS プロトコルの基本認証の無効化が開始されることを発表しました。 SMTP 認証が使用されていない場合も無効になります。 以下のアナウンス全文を参照してください: 「基本認証と Exchange Online – 2021 年 9 月の更新プログラム 」。

> ⓘ **注意**

Office 365 Operated by 21Vianet では、2023 年 3 月 31 日に基本認証の無効化を開始します。 その他のすべてのクラウド環境は、2022 年 10 月 1 日の日付が適用されます。

メッセージング プロトコルと既存のアプリケーションへの影響

この変更は、さまざまな方法で使用する可能性があるアプリケーションとスクリプトに影響します。

POP、IMAP、および SMTP AUTH

2020 年に、POP、IMAP、および SMTP AUTH の OAuth 2.0 サポートをリリースしました。 一部のクライアント アプリの更新プログラムは、これらの認証の種類 (Thunderbird など) をサポートするように更新されているため、最新バージョンのユーザーは OAuth を使用するように構成を変更できます。 Outlook クライアントが POP と IMAP の OAuth をサポートする予定はありませんが、Outlook は MAPI/HTTP （Windows クライアント）とEWS （Mac 版 Outlook）を使用して接続することができます。

これらのプロトコルを使用して電子メールを送信、読み取り、またはその他の方法で処理するアプリを構築したアプリケーション開発者は、同じプロトコルを維持できますが、ユーザーに対してセキュリティで保護された先進認証エクスペリエンスを実装する必要があります。 この機能は、Microsoft Identity platform v2.0 上に構築されており、Microsoft 365 メール アカウントへのアクセスをサポートします。

社内アプリケーションが Exchange Online の IMAP、POP、SMTP AUTH プロトコルにアクセスする必要がある場合は、次の手順に従って OAuth 2.0 認証を実装します。 「OAuth を使用して IMAP、POP、および SMTP 接続を認証する」。 さらに、この PowerShell スクリプト Get-IMAPAccesstoken.ps1 を使用して、共有メールボックスのユース ケースを含む簡単な方法で OAuth の有効化後に IMAP アクセスをテストします。 これが成功した場合は、ベンダーまたは内部ビジネス パートナーのアプリケーション所有者と自信を持って次の手順に進んでください。

ベンダーと協力して、影響を受ける可能性のあるアプリまたはクライアントを更新します。

基本認証が 2022 年 10 月 1 日に完全に無効になった場合でも、SMTP AUTH は引き続き使用できます。 SMTP が引き続き利用可能になる理由は、プリンターやスキャナーなどの多くの多機能デバイスを先進認証を使用するように更新できないためです。 た

だし、可能な場合は、SMTP AUTH で基本認証を使用しないようにすることを強くお勧めします。 認証されたメールを送信するためのその他のオプションには、Microsoft Graph API などの代替プロトコルの使用があります。

Exchange ActiveSync (EAS)

多くのユーザーは、EAS を使用するように設定されたモバイル デバイスを持っています。 基本認証を使用している場合、この変更の影響を受けます。

Exchange Online に接続するときは、iOS および Android 版 Outlook を使用することをお勧めします。 iOS および Android 版 Outlook は、条件付きアクセスとアプリ保護 (MAM) 機能を有効にする Microsoft Enterprise Mobility + Security (EMS) を完全に統合します。 iOS および Android 版の Outlook は、ユーザーと会社のデータをセキュリティで保護するのに役立ち、先進認証をネイティブにサポートします。

先進認証をサポートする他のモバイル デバイス メール アプリがあります。 すべての一般的なプラットフォーム用の組み込みメール アプリは、通常、先進認証をサポートするため、場合によっては、デバイスが最新バージョンのアプリを実行していることを確認することが解決策です。 電子メール アプリが最新であっても、基本認証を使用している場合は、デバイスからアカウントを削除してから、もう一度追加することが必要な場合があります。

Microsoft Intune を使用している場合は、デバイスにプッシュまたは展開するメール プロファイルを使用して認証の種類を変更できる可能性があります。 iOS デバイス (iPhone および iPad) を使用している場合は、「Microsoft Intune で iOS および iPadOS デバイスの電子メール設定を追加する」 をご覧ください。

> **注意**
>
> 証明書ベースの認証を使用しているデバイスは、Exchange Online が今年の後半に Exchange Online の基本認証をオフにしても影響を受けません。 基本認証を使用して直接認証するデバイスのみが影響を受ける。
>
> 証明書ベースの認証はまだレガシ認証であるため、レガシ認証をブロックする Azure AD 条件付きアクセス ポリシーによってブロックされます。 詳細については、「Block **レガシ認証** - Azure Active Directory」 を参照してください。

Exchange Online PowerShell

Exchange Online V2 PowerShell モジュール (EXO V2 モジュールと略す) のリリース以降、先進認証を使用して、コマンド ラインから Exchange Online の設定と保護設定を

簡単に管理できます。 Exchange Online PowerShell V2 モジュールは、先進認証を使用し、Microsoft 365 のすべての Exchange 関連 PowerShell 環境への接続において多要素認証 (MFA) と連携します。Exchange Online PowerShell、Security & Compliance PowerShell、スタンドアロンの Exchange Online Protection (EOP) PowerShellなど、Exchange 関連のすべての PowerShell 環境に接続し、多要素認証 (MFA) を使用します。

EXO V2 モジュールは非対話型で使用することもできます。これにより、無人スクリプトを実行できます。 証明書ベースの認証を使用すると、管理者は、サービス アカウントを作成したり、資格情報をローカルに保存したりする必要なくスクリプトを実行できます。 詳細については、「EXO V2 モジュールの無人スクリプトのアプリ専用の認証」 を参照してください。

古いリモート PowerShell 接続方法または古い Exchange Online リモート PowerShell モジュール (V1) を引き続き使用している管理者は、できるだけ早く EXO V2 モジュールの使用を開始することをお勧めします。 これらの古い接続方法は、基本認証の無効化またはサポートの終了を通じて、最終的に廃止されます。

> ⓘ **重要**
>
> PowerShell で WinRM に対して基本認証が有効になっている必要があること (セッションの実行元のローカル コンピューター) を混同しないでください。「**EXO V2 モジュールの前提条件**」 を参照してください。
>
> ユーザー名/パスワードは Basic を使用してサービスに送信されませんが、WinRM クライアントが OAuth をサポートしていないため、セッションの OAuth トークンを送信するには Basic Auth ヘッダーが必要です。 この問題に取り組んでおり、今後発表する予定です。 WinRM で Basic を有効にしても、Basic を使用してサービスに対する認証を 行いません。
>
> 詳細については、こちらをご覧ください: 「**Exchange Online PowerShell モジュールと基本認証のさまざまなバージョンについて理解する** 」

Exchange Web サービス (EWS)

多くのアプリケーションは、メールボックスと予定表のデータにアクセスするために EWS を使用して作成されています。

2018 年に、Exchange Web サービスは機能更新プログラムを受け取らなくなることを発表しました。アプリケーション開発者は、Microsoft Graph の使用に切り替えることが推奨されました。 「Office 365 向け Exchange Web サービス (EWS) API の今後の変更 」 を参照してください。

多くのアプリケーションが Graph に正常に移行されましたが、まだ移行していないアプリケーションでは、EWS が既に先進認証を完全にサポートしていることは注目に値します。 そのため、まだ Graph に移行できない場合は、EWS で先進認証を使用するように切り替えることができます。EWS は最終的に非推奨になります。

詳細については、次を参照してください。

- Exchange Online 用 Exchange Web サービスでの今後の API 非推奨について - Microsoft Tech Community
- OAuth を使用して EWS アプリケーションを認証する
- 基本認証を使用する EWS マネージド API PowerShell スクリプトの操作

Outlook、MAPI、RPC、オフライン アドレス帳 (OAB)

2016 以降のすべてのバージョンの Outlook for Windows では、既定で先進認証が有効になっているため、既に先進認証を使用している可能性があります。 Outlook Anywhere (以前は RPC over HTTP と呼ばれていました) は、MAPI over HTTP を優先して Exchange Online で非推奨になりました。 Outlook for Windows では、MAPI over HTTP、EWS、OAB を使用してメールにアクセスし、空き時間情報と不在を設定し、オフライン アドレス帳をダウンロードします。 これらのプロトコルはすべて先進認証をサポートしています。

Outlook 2007 または Outlook 2010 は先進認証を使用できず、最終的に接続できなくなります。 Outlook 2013 では先進認証を有効にする設定が必要ですが、設定を構成すると、Outlook 2013 は問題なく先進認証を使用できます。 ここで既に発表したように、Outlook 2013 では、Exchange Online に接続するための最小更新レベルが必要です。 「Microsoft 365 の新しい Outlook for Windows 最小バージョン要件 」 参照してください。

Mac 版 Outlook では、先進認証がサポートされています。

Office での先進認証のサポートの詳細については、「Office クライアント アプリの先進認証のしくみ」 を参照してください。

パブリック フォルダーを Exchange Online に移行する必要がある場合は、「先進認証サポートを使用したパブリック フォルダー移行スクリプト 」を参照してください。

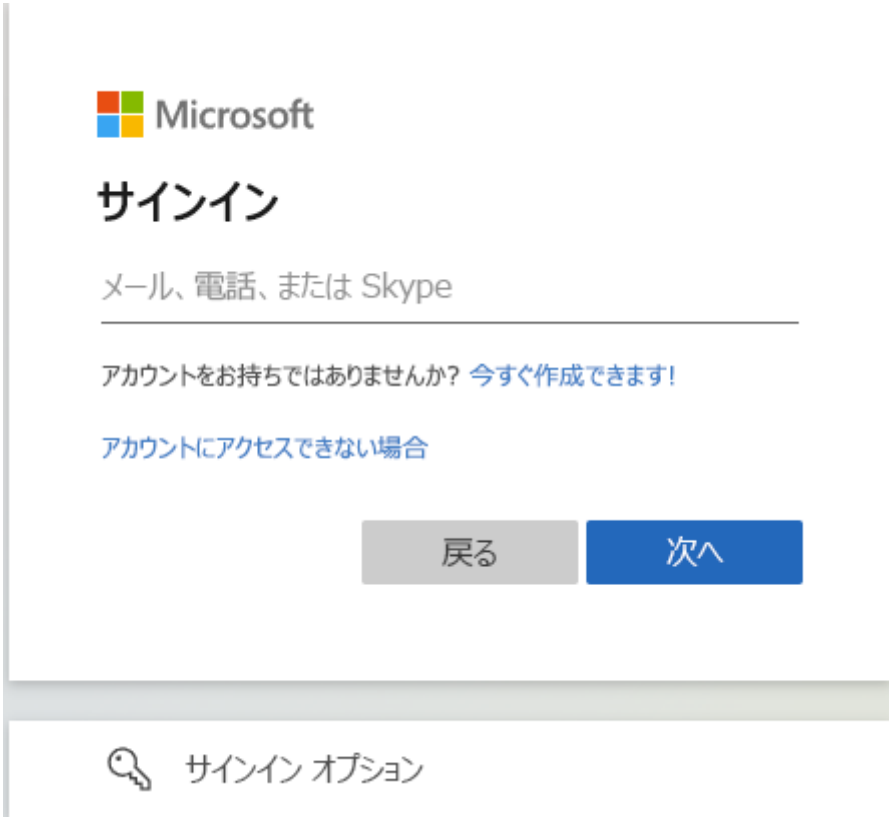
ユーザーが影響を受けるかどうかを確認するにはどうすればよいですか?

基本認証と先進認証のどちらを使用しているかを判断するには、いくつかの方法があります。 基本認証を使用している場合は、認証の送信元と対処方法を決定できます。

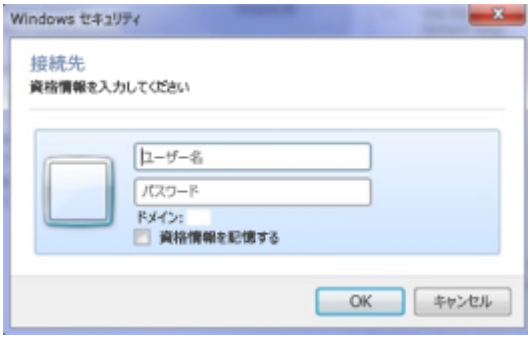
[認証] ダイアログ

クライアント アプリ (Outlook など) が基本認証または先進認証を使用しているかどうかを確認する簡単な方法は、ユーザーがログインしたときに表示されるダイアログを確認することです。

先進認証では、Web ベースのログイン ページが表示されます。



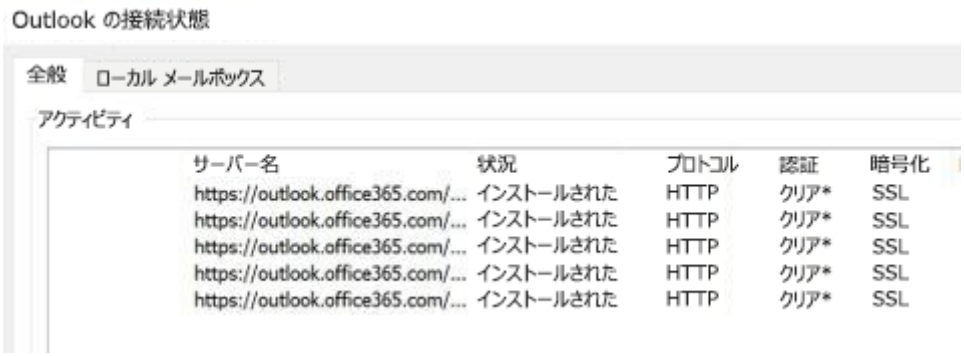
基本認証では、ダイアログ資格情報モーダル ボックスが表示されます。



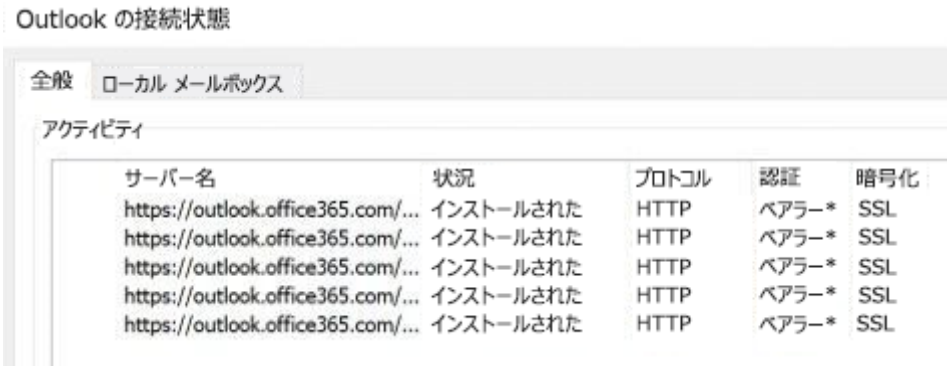
モバイル デバイスで先進認証を使用して接続しようとすると、認証時に同様の Web ベースのページが表示されます。

Ctrl キーを押しながらシステム トレイの Outlook アイコンを右クリックし、[接続状態] を選択して、[接続状態] ダイアログ ボックスを確認することもできます。

基本認証を使用している場合、**Outlook接続状態** ダイアログの **［認証］** 列には、**［クリア］** の値が表示されます。



先進認証に切り替えると、[Outlook の接続状態] ダイアログの **［認証］** 列に、**［ベアラー］** の値が表示されます。



メッセージ センターを確認する

2021 年末から、基本認証の使用状況を要約したメッセージ センター投稿をテナントに送信し始めました。 基本認証を使用しない場合は、基本認証が既にオフになっている可能性があります (また、そう言うメッセージ センターの投稿を受け取っている) ので – 使用を開始しない限り、影響を受けることはありません。

使用状況の概要を取得した場合は、前月に基本認証を使用した一意のユーザーの数と、使用したプロトコルがわかります。 これらの数値は示すものであり、メールボックスまたはデータへの正常なアクセスを必ずしも反映しているわけではありません。 たとえば、ユーザーは IMAP を使用して認証できますが、構成またはポリシーによりメールボックスへのアクセスが拒否されます。 ただし、使用状況の概要は、何らかのユーザーが基本認証を使用してテナントに対して正常に認証されていることを示しています。 この使用状況をさらに調査するには、Azure Active Directory サインイン イベント レポート – を使用することをお勧めします。これらの認証試行の詳細なユーザー、IP、およびクライアントの詳細を提供できるレポート (詳細については以下を参照してください)。

管理センターを確認

2022 年の初めに、Microsoft 管理センターを更新して、使用状況の概要とプロトコルの有効化/無効化を容易にする予定です。 これらの変更が利用可能になった時点で、さらに詳しい情報を公開します。

Azure Active Directory サインイン レポートを確認する

テナントによる基本認証の使用状況を最新の状態に保つ最適な場所は、Azure AD サインイン レポートを使用することです。 詳細については、「組織のレガシ認証をブロックする新しいツール - Microsoft Tech Community 」 を参照してください。

分析のためにログをエクスポートするには、Azure AD テナントの Premium ライセンスが必要です。 Premium ライセンスをお持ちの場合は、次の方法を使用してログをエクスポートできます。

- **Azure Event Hubs、Azure Storage、またはAzure Monitor (最適な方法)**: これらのエクスポート経路はすべて、数十万人のユーザーを持つ大規模な顧客からの負荷を処理できます。詳細については、「Stream Azure Active Directory ログを Azure Monitor へ」 を参照してください。
- **Graph API**: MS Graph ページング ロジックを使用して、すべてのログをプルできるようにすることをお勧めします。 詳細については、「Microsoft Graph API で Azure AD のログにアクセスする」 を参照してください。
- **Web ブラウザーからのダイレクト ダウンロード**: 大規模な顧客の場合、データ量が原因でブラウザーのタイムアウトが発生する可能性があります。

プロアクティブ保護の再有効化とオプトアウト

次の環境では、基本認証の無効化が既に開始されています。

- どのプロトコルにも基本認証を使用しない組織。
- まだ基本認証を使用している組織では、使用量が記録されていない個々のプロトコルで基本認証を無効にします。

組織に変更を加える前に、メッセージ センターの投稿で変更についてお知らせします。 メッセージ センター投稿で指定された日付より前に操作する場合は、変更をオプトアウトできます。 これは 2022 年 10 月まで実行できます。それ以降、変更をオプトアウトすることはできません。

オプトアウト プロセスの詳細については、「基本認証および Exchange オンライン – 2021 年 9 月の更新プログラム 」 を参照してください。

メッセージ センターの投稿が表示される前に既に無効になっている場合は、2022 年 10 月より前であればいつでも再び有効にすることができます。 プロトコルを一時的に

無効にした場合、無効になっている間はいつでも再度有効にすることができます。また、このプログラムをオプトアウトしたい場合は、それを行うこともできます。

再有効化プロセスの詳細については、「基本認証および Exchange Online – 2021 年 6 月の更新プログラム 」 を参照してください。

クライアント オプション

影響を受けた各プロトコルで使用できるオプションの一部を以下に示します。

プロトコルの推奨事項

Exchange Web サービス (EWS)、リモート PowerShell (RPS)、POP と IMAP、Exchange ActiveSync (EAS) の場合:

- **これらのプロトコルを使用して独自のコードを記述した場合** は、基本認証ではなく **OAuth 2.0** を使用するようにコードを更新するか、新しいプロトコル (Graph API) に移行します。
- **これらのプロトコルを使用するサード パーティ製アプリケーションを使用している場合**・は、このアプリケーションを提供したサード パーティ製アプリ開発者に連絡して、OAuth 2.0 認証をサポートするように更新するか、OAuth 2.0 を使用して構築されたアプリケーションにユーザーを切り替えるのを支援します。

キー プロトコル サービス	影響を受けたクライアント	クライアント特定の推奨事項	プロトコル情報/メモ
Outlook	Windows および Mac 用のすべてのバージョンの Outlook	• Windows 版Outlook 2013 以降、Mac 版 Outlook 2016 以降にアップグレードする • Windows 版 Outlook 2013 を使用している場合は、レジストリ キーを使用して先進認証を有効にします	Outlook の先進認証を有効にする – どのくらい難しいのでしょうか?

キー プロトコル サービス	影響を受けたクライアント	クライアント特定の推奨事項	プロトコル情報/メモ
Exchange Web サービス (EWS)	OAuth をサポートしていないサード パーティ製アプリケーション	• 最新の認証を使用するようにアプリを変更します。 • Graph API と先進認証を使用するようにアプリを移行します。 人気のアプリ: • Microsoft Teams Rooms: Authentication in Microsoft Teams Rooms の手順に従って先進認証を有効にします • Dynamics 365 / PowerApps: Exchange Online での基本認証の使用 • Cisco Unity: Microsoft Office 365 Product Bulletin を使用した Unified Messaging の Cisco Unity Connection Service Bulletin	• 基本認証を使用する EWS マネージド API PowerShell スクリプトの操作 • 2018 年 7 月以降の EWS 機能の更新はありません
リモート PowerShell (RPS)	• Exchange 管理者 • 委任された管理者権限 • 自動管理ツール	どちらかを使用します。 • Exchange Online PowerShell V2。 • PowerShell within Azure Cloud Shell 。	EXO V2 モジュールの Automation と証明書ベースの認証のサポートと、Exchange Online PowerShell モジュールと Basic 認証のさまざまなバージョン について説明します。

キー プロトコル サービス	影響を受けたクライアント	クライアント特定の推奨事項	プロトコル情報/メモ
POP と IMAP	POP または IMAP を使用するように構成された Thunderbird ファースト パーティ クライアントなどのサード パーティ製モバイル クライアント	推奨事項: • 完全な機能を有効にしないため、これらのプロトコルから離れる。 • クライアント アプリでサポートされている場合は、POP/IMAP の OAuth 2.0 に移動します。	IMAP は、Linux および教育機関のお客様に人気があります。 OAuth 2.0 のサポートは、2020 年 4 月にロールアウトを開始しました。

キー プロトコル サービス	影響を受けたクライアント	クライアント特定の推奨事項	プロトコル情報/メモ
Exchange ActiveSync (EAS)	Apple、Samsung などのモバイル メール クライアント	• iOS または Android 版 Outlook、および Modern Auth をサポートする別のモバイル メール アプリに移行する • OAuth を実行できるがデバイスが引き続き Basic を使用している場合は、アプリの設定を更新してください • Outlook on the web または最新の認証をサポートする別のモバイル ブラウザー アプリに切り替えます。 人気のアプリ: • Apple iPhone/iPad/macOS: 最新の iOS/macOS デバイスはすべて、最新の認証を使用できます。アカウントを削除して追加し直すだけです。 • Microsoft Windows 10 メール クライアント: アカウントの種類として Office 365 を選択して、アカウントを削除して追加し直します	ネイティブ アプリを使用して Exchange Online に接続するモバイル デバイスは、通常、このプロトコルを使用します。

基本認証を今すぐブロックする場合はどうすればよいですか?

基本認証を事前に無効にするためのオプションをまとめた表を次に示します。

Method	利点	欠点
セキュリティの既定値	- すべてのプロトコルについて、テナント レベルですべてのレガシ認証をブロックします - 追加のライセンスは必要ありません	- Azure AD 条件付きアクセス ポリシーと一緒に使用することはできません - すべてのユーザーに MFA の登録と要求を要求するなど、その他の影響が生じる可能性があります
Exchange Online 認証ポリシー	- プロトコルごとの無効化オプションを使用した段階的なアプローチを可能にする - 追加のライセンスは必要ありません - 基本認証の事前認証をブロックします	管理者 UI を使用して組織レベルで基本認証を無効にできますが、例外は PowerShell が必要です
Azure AD 条件付きアクセス	- すべてのプロトコルのすべての基本認証をブロックするために使用できます - ユーザー、グループ、アプリなどにスコープを設定できます。 - 追加のレポート用にレポート専用モードで実行するように構成できます	- 追加のライセンスが必要です (Azure AD P1) - 認証後の基本認証をブロックします

リソース

基本認証をブロックする方法の詳細については、次の記事を参照してください。

セキュリティの既定値:

- セキュリティの既定値群とは?
- セキュリティの既定値群を有効にする

Exchange Online **認証ポリシー**:

- Microsoft 365 管理センターでの基本認証の管理 (簡易)
- Exchange Online の認証ポリシープロシージャ (詳細設定)

Azure AD **条件付きアクセス**:

- 条件付きアクセス: レガシ認証をブロックする (簡易)
- 条件付きアクセスを使用して Azure AD への従来の認証をブロックする方法 (詳細)

詳細概要と次の手順