

Salesforce メールインテグレーションセキュリティガイド

Salesforce, Winter '24



本書の英語版と翻訳版で相違がある場合は英語版を優先するものとします。

© Copyright 2000–2023 Salesforce, Inc. All rights reserved. Salesforce およびその他の名称や商標は、Salesforce, Inc. の登録商標です。本ドキュメントに記載されたその他の商標は、各社に所有権があります。

目次

セキュリティガイドの概要	1
Outlook Integration	2
初回ユーザ認証ログインフロー	4
公開 EWS エンドポイントを使用する Outlook インテグレーション	6
設定要件	6
Web 版の Outlook の設定要件	7
添付ファイル付きメールの Salesforce フローへの記録	7
使用される API	9
Exchange Web サービス (EWS)	9
使用される EWS API	9
Gmail インテグレーション	10
設定要件	10
認証	10
Inbox ライセンスを使用する Outlook および Gmail インテグレーション	11
組織プロビジョニング	11
ネットワーク接続	12
Salesforce および Amazon Web Services (AWS) サーバストレージ	13
AWS データ保持	16
暗号化鍵管理	16
Inbox モバイルアプリケーションのデータストレージ	16
Inbox ライセンスを持つユーザの後続のログイン	17
Gmail ガイドライン	18
Exchange Online (Office 365) ガイドライン	18
Microsoft Exchange 社内ガイドライン	20
OAuth プロトコルについての詳細	21
Salesforce AWS サーバ操作	22
モバイルデバイス管理とモバイルアプリケーション管理および Inbox	22
モバイルアプリケーションデータの削除	23

セキュリティガイドの概要

Salesforce と Outlook および Gmail のインテグレーションにより、営業担当は作業を行う場所に関係なく、より効率的に販売を管理できます。Sales Cloud では、Outlook および Gmail とのインテグレーションを無料で利用できます。

このドキュメントでは、以下の技術およびセキュリティガイドラインについて説明します。

- Outlook および Gmail インテグレーション。
- Inbox ライセンスがあり、ユーザに Inbox 権限が割り当てられている場合のデスクトップおよびモバイルソリューション。Inbox ライセンスは Sales Cloud Einstein とセールスエンゲージメントでスタンドアロンライセンスとして使用できます。

Inbox ライセンスを追加すると、次の内容を実現できます。

- Outlook および Gmail インテグレーションでより多くの機能を使用できるようになり、Outlook や Gmail で作業しているときの営業担当の生産性が向上する。
- Lightning Experience のメールで厳選された Inbox 機能にアクセスできる。
- Inbox モバイルアプリケーションにアクセスできる。

設定手順、考慮事項、機能の詳細などの完全な情報は Salesforce ヘルプにあります。

Salesforce には、メールアカウントと Salesforce を統合する他の機能やソリューションが用意されており、Outlook および Gmail インテグレーションと Inbox 機能が補完されます。たとえば、Einstein 活動キャプチャや Lightning Sync を設定して、連絡先 (取引先責任者) とカレンダーのイベント (行動) を Salesforce 間で同期します。Einstein 活動キャプチャで自動メールおよびイベント (行動) の記録を設定します。セキュリティに関する考慮事項については、『[Einstein 活動キャプチャセキュリティガイド](#)』および『[Lightning Sync Design and Security Guide \(Lightning Sync の設計とセキュリティガイド\)](#)』を参照してください。

❗ 重要: Inbox ライセンスには、Einstein 活動キャプチャが含まれます。ただし、Einstein 活動キャプチャ機能を使用するかどうかに関係なく Inbox を有効にできます。また、Inbox を使用しなくても Einstein 活動キャプチャ機能を有効にできます。

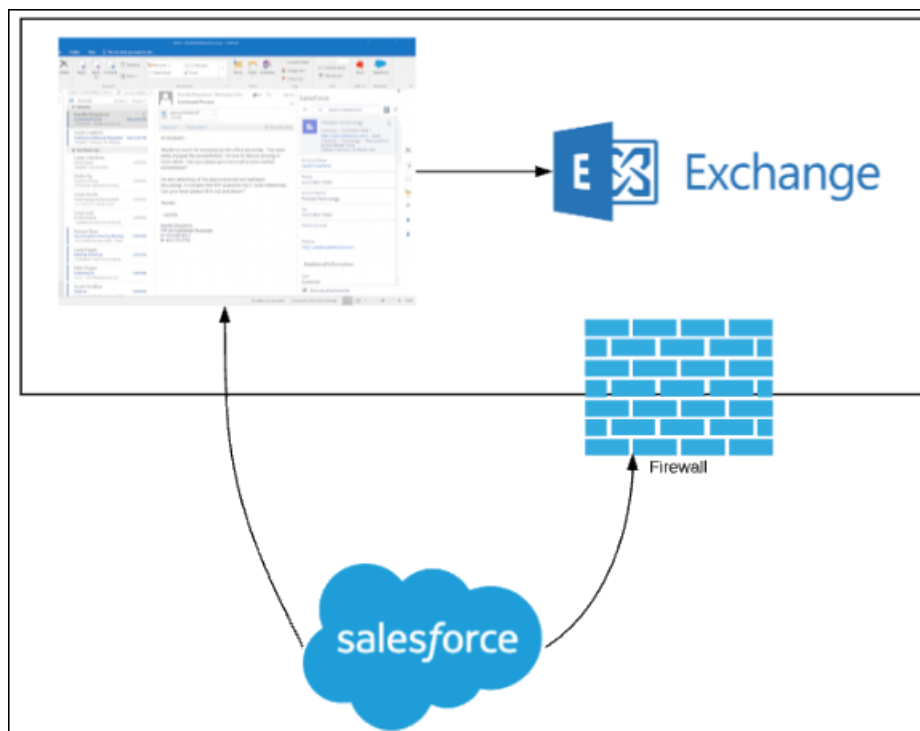
Outlook Integration

Outlook インテグレーションに向けて適切に Exchange サーバへのアクセス権を付与します。

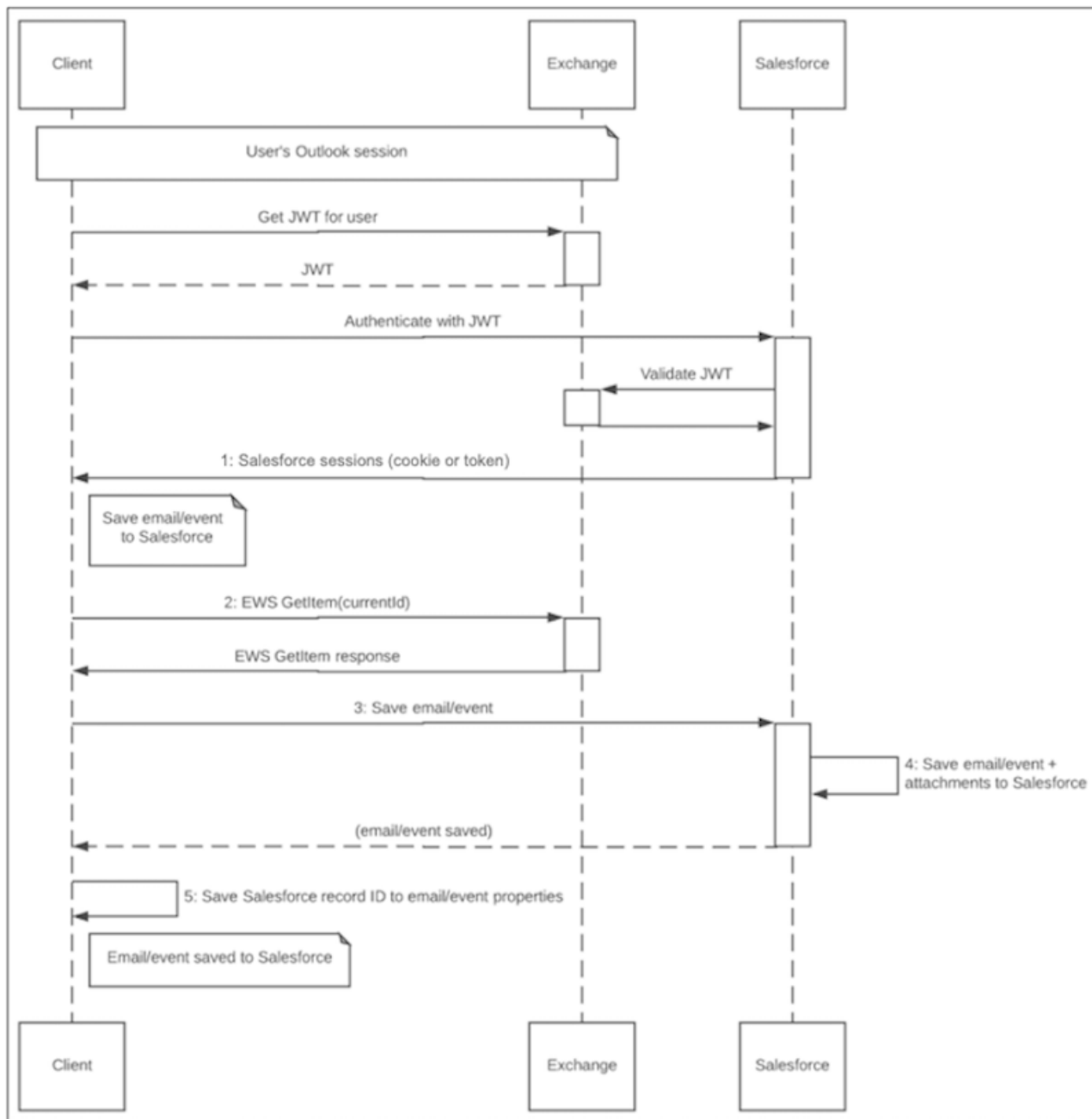
Outlook インテグレーションを設定するには、Exchange サーバへのアクセス権が必要です。そのアクセス権を設定するための選択方法は、使用する Outlook のバージョン、社内のセキュリティポリシー、インテグレーション内で営業担当に必要な機能によって異なります。

Outlook インテグレーションアドインは、[Microsoft Office](#) アドインフレームワークに基づいて構築されています。そのフレームワーク内で特に Outlook から Salesforce へのメールを記録するというエンドユーザアクションでは、Salesforce は Exchange サーバに対してコールを実行する必要があります。

一般的な社内の Exchange 設定では、ファイアウォールでインターネットからのアクセスをブロックします。



Outlook インテグレーションでは Exchange API を利用して、Salesforce アプリケーションサーバから Exchange Web サービス (EWS) コールを実行します。これまで、アドインコールは Exchange 自体で提供される URL と JSON Web トークン (JWT) を使用して EWS を介して実行されてきました。JWT コールでは、EWS エンドポイントを公開する必要がありました (古いバージョンの Exchange および Outlook では引き続き必要)。



最新バージョンの Outlook および Exchange の最近の機能強化により、歴史的な EWS サーバコールを Outlook で提供される Office.js API のクライアントコールにすることができるようになりました。適切なバージョンの Outlook および Exchange では、EWS エンドポイントを公開することなく、Outlook インテグレーションのほぼすべての機能を使用できます。ただし、Outlook と Exchange 間のローカル EWS 接続や Exchange メタデータ URL は引き続き公開する必要があります。

Exchange および Outlook で JavaScript API v1.8 以降が実行されている場合は、EWS エンドポイントを公開することなく、標準の Outlook インテグレーション機能を使用できます。ただし、Outlook と Exchange 間のローカル EWS 接続や Exchange メタデータ URL は引き続き公開する必要があります。設定のこの変更は、Summer '21 からローリ

ング方式で既存のユーザに適用されます。タイミングと対象資格についての詳細は、Salesforce アカウント担当者にお問い合わせください。

Exchange Online の最新のビルドでは、JavaScript API v1.8 以降が実行されます。Outlook クライアントで JavaScript API v1.8 以降が使用されているかどうかを確認するには、Microsoft ドキュメントの「[Outlook JavaScript API の要件セット](#)」を参照してください。

重要: Inbox ライセンスで利用できる機能 ([対応可能時間を挿入] や [後で送信] など) では、Outlook または Exchange API のバージョンに関係なく、Exchange サーバへのアクセス権が必要になります。Inbox ライセンスがある場合は、「[公開 EWS エンドポイントを使用する Outlook インテグレーション](#)」(ページ 6)および「[Inbox ライセンスを使用する Outlook および Gmail インテグレーション](#)」(ページ 11)を参照してください。

Exchange サーバまたは Outlook バージョンで JavaScript AP バージョン 1.4 ~ 1.7 がサポートされている場合でも、公開 EWS を使用せずに Exchange を設定することはできます。ただし、ユーザは次の機能にアクセスできなくなります。

- Outlook から直接添付ファイルを記録する。ユーザは、Salesforce で記録済みのメールに添付ファイルを追加できます。Salesforce に記録されたメールやイベント (行動) の場合、[Salesforce に記録済み] と表示されます。
- Inbox 生産性機能。

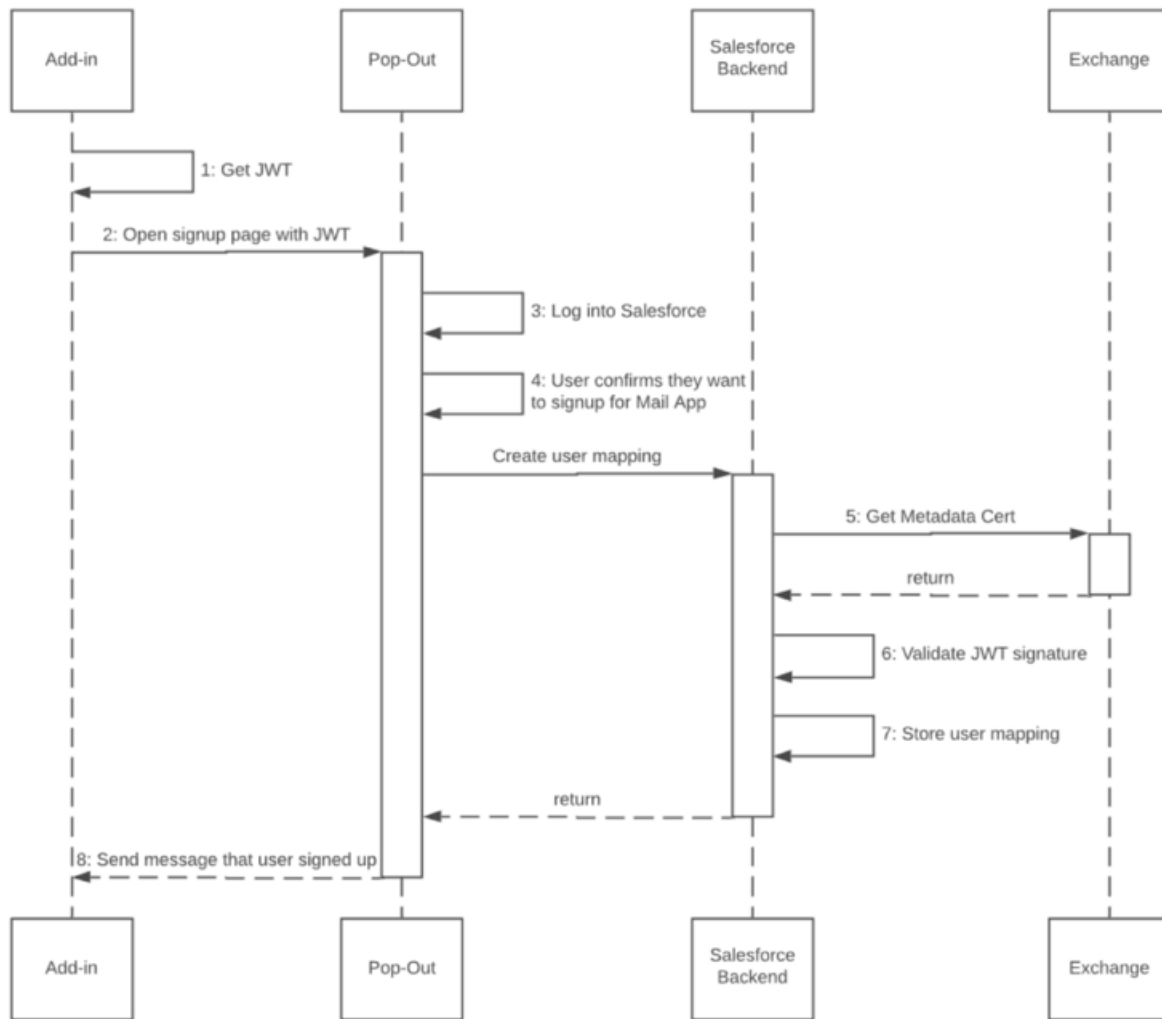
初回ユーザ認証ログインフロー

公開 EWS エンドポイントを使用する Outlook インテグレーション

初回ユーザ認証ログインフロー

Salesforce は Exchange に接続して、メタデータ URL でユーザを認証します。これは、EWS とは異なる考慮事項です。次の図は、ユーザが初めて Outlook インテグレーションアドインを読み込んだときに Exchange が対応する Salesforce ユーザにどのように対応付けられるのかについての詳細なフローを示しています。

次の図は、ユーザが初めて Outlook インテグレーションアドインを読み込んだときに Exchange メールが対応する Salesforce ユーザにどのように対応付けられるのかについての詳細なフローを示しています。このフローは、JavaScript API のバージョンに関係なく、すべてのバージョンの Outlook および Exchange に適用されます。



1. Outlook アドインは、簡単な JavaScript メソッドを使用して ID トークンを取得します。

```
Office.context.mailbox.getUserIdentityTokenAsync(callback, userContext);
```

JavaScript メソッドは、Exchange サーバに対して Exchange ユーザ ID トークン (JSON Web トークンまたは JWT) を要求します。アドインは、Salesforce でホストされるウィンドウでサインアップページを開きます。

2. ユーザは、Salesforce ログイン情報を使用して認証を行います。
3. Salesforce は、(ID トークンで指定された) ユーザの Exchange アカウントを認証済み Salesforce ユーザに接続するように求めます。
4. ユーザはプロンプトをクリックし、サインインすることを確認します。
5. Salesforce サーバは、Exchange トークンコンテンツを検証して、メタデータ URL の公開証明書を取得します。Salesforce では、EWS エンドポイントに有効な証明書が含まれていることが想定されています。サポートされている SSL 証明書については、[Salesforce ヘルプ](#)を参照してください。
6. Salesforce は、Exchange サーバの認証メタデータドキュメントの公開署名鍵にアクセスして、ID トークン署名を検証します。

Exchange サーバは、初めて JSON トークンをアドインに提供するときに以下を指定します。

- トークン自体のペイロード部分の Exchange メタデータエンドポイント URL
- Salesforce アドイン

アドインは、定義されたメタデータ URL に要求を送信して、署名を検証します。Exchange メタデータ URL は、ユーザの ID トークンを検証できるように公開されている必要があります。

トークンの検証についての詳細は、[Microsoft ドキュメント](#)を参照してください。

7. その後、Exchange から Salesforce ユーザへの対応付けは、ユーザの Salesforce 組織データ内に保存されます。

公開 EWS エンドポイントを使用する Outlook インテグレーション

このセクションでは、次のシナリオの Outlook インテグレーションアドインで使用する認証されたコールについて説明します。

- Outlook バージョンで JavaScript API 1.7 以前が実行されている。「[Outlook JavaScript API の要件セット](#)」で、Outlook アプリケーションで実行される API のバージョンを確認します。
- [対応可能時間を挿入]、[後で送信]、[テキストショートカット]、[メール追跡]などの機能を有効にする Inbox ライセンスを追加している。これらの機能を使用するには、Exchange サーバへのアクセス権が必要です。このガイドの「[Inbox ライセンスを使用する Outlook および Gmail インテグレーション](#)」(ページ 11)も確認してください。上記のセクションには、このセクションで説明されていないセキュリティと実装の考慮事項が記載されています。

❗ 重要: これらのシナリオで公開 EWS エンドポイントがない場合、インテグレーションユーザはインテグレーションから添付ファイルを記録したり、Inbox 生産性機能を使用したりできません。

設定要件

[Web 版の Outlook の設定要件](#)

[添付ファイル付きメールの Salesforce フローへの記録](#)

[使用される API](#)

[Exchange Web サービス \(EWS\)](#)

[使用される EWS API](#)

設定要件

Outlook インテグレーションを設定するには、URL を公開する必要があります。

- 認証されていない HTTP アクセスを許可する Exchange メタデータ URL。「[初回ユーザ認証ログインフロー](#)」(ページ 4)を参照してください。
- Exchange Web サービス URL

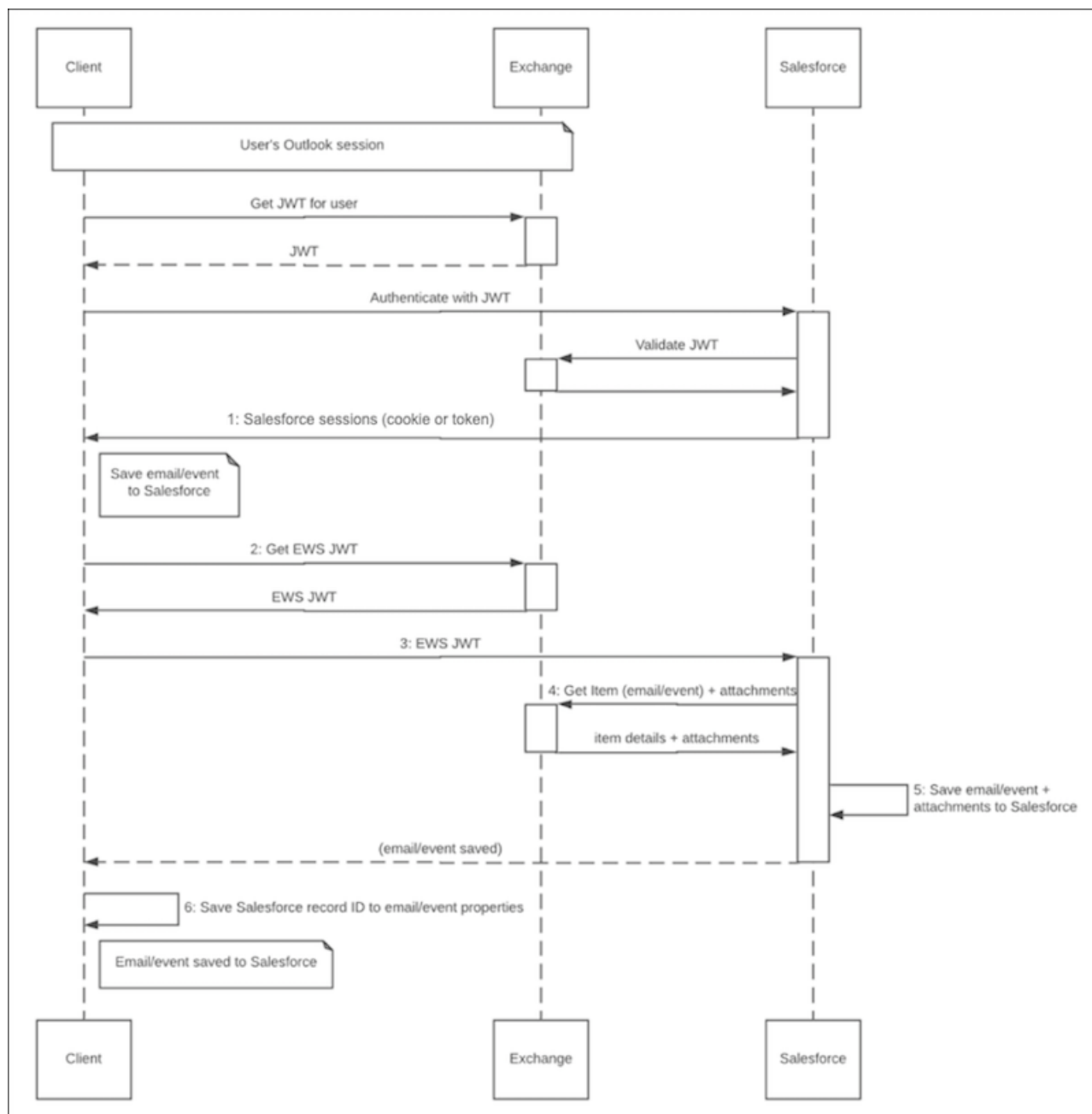
Web 版の Outlook の設定要件

Salesforce は、Exchange エンドポイントに対して送信コールを実行するため、各エンドポイント URL には、有効な [Salesforce でサポートされている SSL 証明書](#)が必要です。

営業担当が Web 版の Outlook (Outlook Web App (OWA) と呼ばれる) を使用する場合、Salesforce の [設定] の [Outlook インテグレーション] 設定でカスタム OWA URL (Office 365 以外の URL など) を指定します。Web 版の Outlook にアクセスする必要があるのはクライアントブラウザのみであるため、カスタム URL を公開する必要はありません。これらの設定は、営業担当が Web 版の Outlook でインテグレーションを使用する場合にのみ適用されます。

添付ファイル付きメールの Salesforce フローへの記録

Outlook インテグレーションから、ユーザは選択した Outlook メールメッセージとその添付ファイルを手動で Salesforce に記録できます。アドインでは、次のフローを使用して記録を実行します。



1. Salesforce で認証します (詳細は、「ログインフロー」を参照)。
2. Outlook アドインに提供される API を介して、認証されたコールを Exchange Web サービス (EWS) に対して実行します。 [Microsoft Office API ドキュメント](#) を参照してください。これで、記録する現在のメールまたはイベント (行動) を Salesforce サーバで取得できます。
3. 現在のメールまたはイベント (行動) とその添付ファイルに対して EWS 操作 EWS GetItem + GetAttachment(s) を実行します。
4. メールまたはイベント (行動) および添付ファイルを Salesforce に保存し、選択した Salesforce レコードに両方を関連付けます。

5. Exchange オブジェクトの拡張プロパティに Salesforce レコード ID が含まれるように、Exchange のメールまたはイベントを変更します。

使用される API

クライアント側 API コールは、Office.js およびサーバ EWS コールを介して実行されますが、GetItem 操作と GetAttachment 操作に制限されます。実行される EWS コールは、クライアント側と Salesforce アプリケーションサーバから開始されます。これらのコールは、特定のメールまたはイベント(行動)のコンテキストで、ユーザーアクションによってトリガされます。Salesforce アプリケーションサーバから EWS URL へのコールは、公開された [IP アドレス範囲](#)から取得されます。

Outlook インテグレーションでは、メールまたはイベント(行動)とその添付ファイルを読み取ることができるように ReadWriteMailbox が指定されます。更新アクセスは、Office.js API で実行される EWS コールを介して Salesforce の ToDoID または行動ID を Exchange レコードに書き戻すためのものです。EWS コールを実行するための設定要件についての詳細は、[Office.js ドキュメント](#)を参照してください。

Exchange Web サービス (EWS)

EWS 要求には、次の要素が含まれます。

- HTTP ヘッダー
 - 認証: (Office.js getCallbackTokenAsync からの) ベアラートークン
 - ユーザエージェント: ExchangeServicesClient/0.0.0.0
- SOAP リクエストボディの XML

使用される EWS API

EWS を介して次のコールが実行されて、メールまたはイベント(行動)および添付ファイルが取得されます。また、Salesforce レコード ID が Exchange 項目のプロパティに書き込まれます。特定のコールについては、Microsoft ドキュメントのリンクをクリックしてください。

- [GetItem](#) (クライアント側とサーバ側): Salesforce レコードを保存するときに [AdditionalProperties](#) と現在のメールメッセージのコンテンツを取得および設定します。
- [GetAttachment](#) (サーバ側): Exchange から添付ファイルを取得し、(Salesforce メールメッセージ表現に関連付けられた) Salesforce レコードに追加します。
- [UpdateItem](#) (クライアント側)
- [GetFolder](#) (クライアント側): ドラフトフォルダを取得します。
- [CreateItem](#) (クライアント側): ドラフトメッセージを作成するために使用します。

「クライアント側」は、Office.js API makeEwsRequestAsync を介して実行されるコールです。「サーバ側」は、Salesforce アプリケーションサーバから EWS エンドポイントに対して実行されるコールです。これらのサーバ側コールでは、[getCallbackTokenAsync](#) の 5 分間のトークンが使用されます。

Gmail インテグレーション

このセクションでは、Gmail インテグレーション Chrome 拡張機能で使用するログイン認証と認証されたコールについて説明します。メールインテグレーションに Inbox が含まれる場合は、このガイドの「[Inbox ライセンスを使用する Outlook および Gmail インテグレーション](#)」セクションも参照してください。

設定要件

認証

設定要件

[Salesforce ヘルプ](#)を確認して、Gmail とのインテグレーションを設定します。Salesforce ヘルプのそのセクションには、Gmail インテグレーションのシステム要件も記載されています。

認証

Salesforce では、OAuth 2.0 プロトコルを使用して、ユーザの Google アカウントに接続します。Salesforce サーバは、Google に対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。このトークンは、そのユーザの Gmail アカウントへのアクセス権を提供するシングルユーザトークンです。このトークンは、Chrome 拡張機能で直接使用されません。これは、接続された Salesforce 組織内に保存され、顧客データとして処理されます。

Gmail インテグレーションでは、Salesforce プラットフォーム機能の認証プロバイダを使用して、Google アクセストークンを保存および管理します。認証プロバイダを使用すると、Apex でアクセストークンを取得して更新できます。詳細は、Salesforce ヘルプの「[認証プロバイダ](#)」を参照してください

Google を使用したログインを維持するには、Salesforce の [設定] の [Gmail インテグレーションおよび同期] ページにある [Gmail と Salesforce の接続を維持] 設定を有効にします。この設定により、ユーザは Google ID に基づいて Salesforce セッションを取得できます。Salesforce セッションは、Salesforce 内で設定された有効期限や他のルール (使用できる IP 範囲など) に従います。Salesforce セッションの有効期限が切れた場合、ユーザは Google ID に基づいて新しいセッションを確立できます。この設定では、ユーザのブラウザで Google アカウントにログインする必要があります。[Gmail と Salesforce の接続を維持] 設定が無効になっている場合、ユーザは Salesforce Desktop と同じ方法でログインします。システム管理者によって制御されるセッションと同じルールが適用されます。Salesforce セッションの有効期限が切れた場合、ユーザは再度ログインする必要があります。

Inbox ライセンスを使用する Outlook および Gmail インテグレーション

重要: この章の内容は、Salesforce Inbox がある場合にのみ適用されます。Inbox ライセンスがない場合や、Inbox 権限が割り当てられているユーザがいない場合、この章をスキップできます。

Inbox ライセンスを追加すると、Outlook および Gmail インテグレーション内で営業担当の生産性を向上させる機能を使用できるようになります。また、営業担当は Lightning Experience のメールでより多くの機能にアクセスしたり、Inbox モバイルアプリケーションにアクセスしたりできます。

この章では、Inbox ライセンスがあり、ユーザに Inbox 権限が割り当てられている場合の接続、データストレージ、データ保持の詳細について説明します。

組織プロビジョニング

ネットワーク接続

[Salesforce および Amazon Web Services \(AWS\) サーバストレージ](#)

[AWS データ保持](#)

暗号化鍵管理

[Inbox モバイルアプリケーションのデータストレージ](#)

[Inbox ライセンスを持つユーザの後続のログイン](#)

[Gmail ガイドライン](#)

[Exchange Online \(Office 365\) ガイドライン](#)

[Microsoft Exchange 社内ガイドライン](#)

[OAuth プロトコルについての詳細](#)

[Salesforce AWS サーバ操作](#)

[モバイルデバイス管理とモバイルアプリケーション管理および Inbox](#)

[モバイルアプリケーションデータの削除](#)

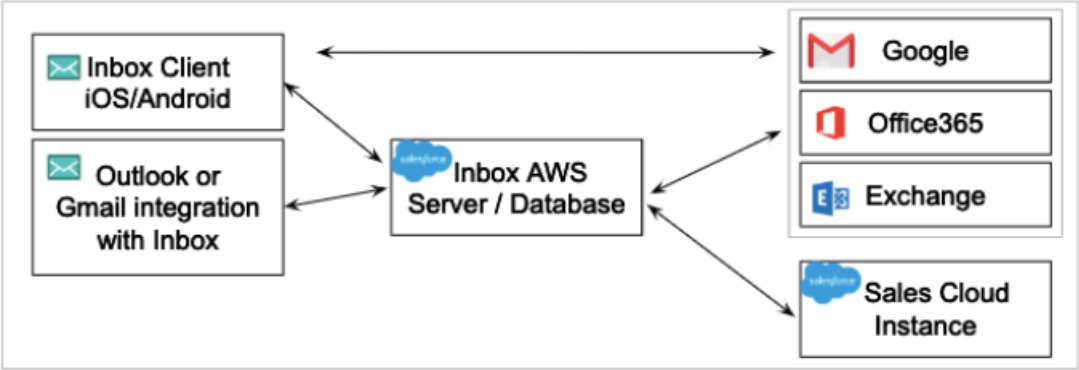
組織プロビジョニング

Salesforce 組織で Inbox が有効になると、Salesforce の Amazon Web Service (AWS) サーバ上に対応する組織が作成されます。ユーザに Inbox を使用してメールボックスを Salesforce に接続する権限がある場合、メールボックスは AWS に接続されます。この接続により、Salesforce AWS サーバは、Google、Microsoft Exchange、または Office 365 に対してネットワークコールを実行するように求められます。AWS データセンター内でアプリケーションは、関連するデータを関連するユーザに提供するために鍵と ID を使用します。

Inbox で使用する Einstein プラットフォームのセキュリティとアーキテクチャについての詳細は、[Einstein プラットフォームの信頼とコンプライアンスに関するドキュメント](#)を参照してください。

ネットワーク接続

Inbox モバイルアプリケーションおよびデスクトップクライアントは、Salesforce AWS サーバに対してネットワークコールを実行します。その後、サーバが Microsoft Exchange、Office 365、Google に対して直接ネットワークコー



ルを実行します。

Inbox ライセンスを使用する Outlook および Gmail インテグレーションから Salesforce AWS サーバ
AES-128 暗号化を使用する HTTPS TLS 1.2 接続。この接続は、ログインと Inbox 固有のタスクの実行で使用されます。

Salesforce AWS サーバから Google
AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、Gmail API プロトコルと OAuth 2.0 認証が使用されます。

Salesforce AWS サーバから Office 365 (Exchange Online)
AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、EWS プロトコルと OAuth 2.0 認証が使用されます。

Salesforce AWS サーバから社内の Exchange (2019、2016、2013)
HTTPS TLS 1.2 接続 (Exchange サーバが TLS バージョンおよび暗号化を決定)。この接続では、EWS プロトコルと、ユーザ名およびパスワードによる基本認証が使用されます。IP または VPN によって EWS エンドポイントが制限されている場合、アドレスの許可リストに次のアドレスを追加します。

Salesforce インスタンスがヨーロッパ以外にある場合	Salesforce インスタンスがヨーロッパにある場合
54.200.130.205 54.218.59.121 34.210.91.105 34.210.91.103 44.224.62.36 52.35.129.120 54.71.145.62 35.166.120.106 44.224.71.98 52.35.232.62 54.68.117.123	52.59.28.245 52.28.30.206 52.57.191.228 18.194.116.65 52.57.191.229 18.184.19.133 52.57.191.226 52.57.191.224 52.57.191.227 18.197.233.154 18.196.51.181

Salesforce インスタンスがヨーロッ パ以外にある場合	Salesforce インスタンスがヨーロッパにある場合
• 52.26.6.102 • 35.163.187.73 • 52.36.92.175 • 34.210.91.106 • 34.210.91.104 • 35.166.17.212 • 34.216.184.173 • 34.210.91.108 • 34.210.91.107	• 3.124.138.13 • 3.124.208.146 • 3.124.224.62 • 3.124.238.55

EWS または Inbox に固有でない Salesforce IP アドレスについては、[こちらのナレッジ記事](#)を参照してください。

Exchange の発信接続が制限されている場合、`ews-webhook-us1-prod.salesforceiq.com` (Salesforce インスタンスがヨーロッパ以外にある場合) または `ews-webhook-eu1-prod.salesforceiq.com` (Salesforce インスタンスがヨーロッパにある場合) への発信アクセスを許可します。その後、Exchange に新しいメールとイベント (行動) が届くと、プッシュ通知が Salesforce に送信されます。

iOS および Android Inbox アプリケーションから Google

AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、Gmail API プロトコルと OAuth 2.0 認証が使用されます。

iOS および Android Inbox アプリケーションから Office 365 (Exchange Online)

AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、Exchange ActiveSync (EAS) または Office 365 API プロトコルが使用されます (それぞれで OAuth 2.0 認証が使用される)。

iOS および Android Inbox アプリケーションから社内の Exchange (2019、2016、2013)

HTTPS TLS 1.2 接続。Exchange サーバが TLS バージョンおよび暗号化を決定します。この接続では、Exchange ActiveSync (EAS) プロトコルと、ユーザ名およびパスワードによる基本認証が使用されます。

Inbox で OAuth がどのように使用されるのかについての詳細は、[「OAuth プロトコルについての詳細」](#)を参照してください。

Salesforce および Amazon Web Services (AWS) サーバストレージ

Inbox ライセンスが有効になっていると、サーバおよびデータベースは、AWS 仮想プライベートクラウド (VPC) の背後にある AWS でホストされます。

重要: Inbox ライセンスには、Einstein 活動キャプチャが付属しています。ただし、Einstein 活動キャプチャ機能を有効にするかどうかに関係なく Inbox を有効にできます。両方の機能で同じデータが使用されるため、Einstein 活動キャプチャが有効になっているかどうかに関係なく、データは AWS に保存されます。

AWS によって取得、保存される データ	追加の詳細	データの使用方法
カレンダーのイベント (行動)	ユーザの接続済み Microsoft アカウ ントまたは Google アカウントから取 得されたすべてのイベント (行動) データが含まれます。イベント (行 動) の添付ファイルは含まれませ ん。	Einstein 活動キャプチャではこのデー タを使用して Salesforce カレンダー の活動タイムラインに行動が表示 されます。 Inbox では [対応可能時間を挿入] 機 能と [推奨コネクション] 機能にこの データが使用されます。
取引先責任者の詳細	連絡先(取引先責任者)のプロファイ ル画面 (Gmail、Exchange、Sales Cloud) に表示されるデータから取得され た取引先責任者データが含まれま す。	取引先責任者データは他の Salesforce 機能 (Einstein メールインサイトなど) で使用されます。
メールアカウント	メールアドレス、サーバ、ドメイ ンなど、ユーザの接続済み Microsoft アカウントまたは Google アカウ ントに関する詳細が含まれます。	Einstein 活動キャプチャと Inbox で は、このデータを使用してユーザ のメールアカウントが Salesforce に 接続されます。
メールの添付ファイル	メールの添付ファイルのメタデー タが含まれます。Einstein 活動キャ プチャの場合、添付ファイル自体 は保存されず、活動タイムライン にも表示されません。 Inbox の場合、[後で送信] 機能を使 用するとメールが送信されるまで 添付ファイルが保存されます。 Inbox のメール送信アクション中、 Google サーバまたは Exchange サーバ にメールメッセージ ID を渡して添 付ファイルをメールの添付ファイ ルとして動的に取得できます。	現在、Einstein 活動キャプチャでは 添付ファイルメタデータは使用さ れていません。 Inbox では添付ファイルとメタデー タは [後で送信] 機能に使用されま す。
メールヘッダーとメタデータ	ユーザの接続済み Microsoft アカウ ントまたは Google アカウントから取 得されたメールメッセージが含ま れます。保存されるメール要素に は、件名、送信者、宛先、CC、送 信日が含まれます。	Einstein 活動キャプチャではこのデー タを使用して Salesforce の関連レコ ードの活動タイムラインにメールが 追加されます。 Inbox と Einstein 活動キャプチャで使 用可能なメールインサイトでは、 このデータを使用して分類が作成 されます。

AWS によって取得、保存される データ	追加の詳細	データの使用方法
		Inbox と Einstein 活動キャプチャで使用可能な推奨コネクションでは、このデータを使用して提案が生成されます。
メール HTML 本文		Einstein 活動キャプチャではこのデータを使用して Salesforce にメールが表示されます。また、このデータはメールインサイトの生成にも使用されます。
パスワードと OAuth トークン	ユーザの Google アカウントまたは Microsoft アカウントを Salesforce に接続するために使用される OAuth の更新トークンとアクセストークンが含まれます。 ユーザが OAuth 2.0 を使用してアカウントを Salesforce に接続すると、ユーザのパスワードは保存されません。そのため、アカウントを Salesforce に接続した後にユーザがメールのパスワードを変更しても Google または Microsoft に対して再認証する必要はありません。 ユーザがオンプレミスの Exchange メールアカウントを使用していて、パスワード認証が使用されている場合は、ユーザのパスワードが保存されます。	
Salesforce レコード	取引先責任者、リード、商談などのレコードのメタデータ (権限、項目、ページレイアウトなど) が含まれます。 Inbox では、レコードのメタデータが最大 24 時間保存されます。Einstein 活動キャプチャでは、Salesforce のデータを削除するまで、レコードのメタデータが保存されます。 Salesforce のレコードデータを削除すると、そのデータは AWS サーバからも削除されます。	Inbox モバイルアプリケーションでは、このデータを使用して、メールや行動に関連するレコードを参照するときのパフォーマンスが改善されます。 メールに関連する Salesforce レコードに関連付けるため、Einstein 活動キャプチャでは、取引先責任者レコードやリードレコードからメールアドレスがコピーされて AWS サーバに保存されます。

AWS によって取得、保存される データ	追加の詳細	データの使用方法
ユーザの設定	Inbox または Einstein 活動キャプチャ ユーザの個人設定が含まれます。	

AWS データ保持

新しいメールアカウントが接続されると、Salesforce AWS サーバは過去 6 か月または 180 日分のメールメッセージをダウンロードします。それ以降、サーバは Gmail、Exchange、または Office 365 の通知登録を使用して、新しいメールメッセージのダウンロードをトリガします。デフォルトでは、メールメッセージは 2 年間保持されてから削除されます。保持期間は、30 日～5 年に設定できます。

暗号化鍵管理

Salesforce AWS インスタンスでは、ユーザ固有の鍵でデータを暗号化することはできません。暗号化には、AWS で管理される鍵が使用されます。

データベースのメールメタデータとカレンダーデータは、ディスクレベルの暗号化を使用して暗号化されます。

Inbox モバイルアプリケーションのデータストレージ

Inbox モバイルアプリケーションは、次の情報を保存します。

対象	詳細
Inbox ユーザ設定	個人ユーザ設定は、デバイスの SQLite データベースとアプリケーション設定に保存されます。 • iOS の NSUserDefaults • Android の SharedPreferences 次のようなユーザ設定が保存されます。 • Salesforce 設定 (応答画面でメール記録を要求) • ユーザが設定した作業時間 • メール設定 (スワイプ方向、メッセージに表示される行数、スレッドによる整理、バッジ数種別など) • カレンダー設定 (不参加や表示される日数など)
メールメッセージ	Inbox モバイルアプリケーションは、最近のメールメッセージ (メール本文を含む) を保存します。メールメッセージは、SQLite データベースに保存されます。iOS の場合、デー

対象	詳細
	データベースは AES-256 暗号化を使用する SQLCipher で暗号化されます。Android の場合、データベースは暗号化されません。
行動	Inbox モバイルアプリケーションは、カレンダーのイベント (行動) を SQLite データベースに保存します。iOS の場合、データベースは AES-256 暗号化を使用する SQLCipher で暗号化されます。Android の場合、カレンダーのイベント (行動) はデフォルトの共有カレンダープロバイダストレージに保存されます。カレンダーについての詳細は、 Android 開発者向けドキュメント を参照してください。
パスワードと OAuth トークン	メールやカレンダーのイベント (行動) を Google、Office 365、Exchange から直接取得するために、Inbox モバイルアプリケーションは Google および Office 365 の OAuth アクセストークンを保存します。また、Exchange のパスワードも保存します。これらのトークンやパスワードは、iOS キーチェーンまたは Android アカウントマネージャ (それぞれのデバイスのデフォルトの暗号化領域) に保存されます。
iOS キーチェーン	キーチェーンサービスの概念 については、Apple 開発者向けガイドを参照してください。
Android アカウントマネージャ	アカウントマネージャプロバイダ については、Android 開発者向けガイドを参照してください。

Inbox ライセンスを持つユーザの後続のログイン

初回ログイン後、Inbox ライセンスを持つユーザは、引き続き認証を行って、メールボックスを Salesforce AWS サーバに接続します。この認証により、Salesforce に対して要求を実行するための OAuth 更新トークンとアクセストークンが取得および保存されます。このトークンは、ユーザの Salesforce アカウントに関連付けられます。

OAuth 更新トークンおよびアクセストークンは、Salesforce AWS サーバに保存されます。接続されると、API コールが実行されて、OAuth アクセストークンが取得されます。デフォルトでは、アクセストークンの有効期限は 1 時間で切れます。Salesforce システム管理者は、有効期限を設定できます。たとえば、システム管理者は 7 日ごとに有効期限が切れるように OAuth 更新トークンを設定できます。デフォルトのトークンの有効期限を変更する手順は、次のとおりです。

1. Salesforce の [設定] から、[クイック検索] ボックスに「[接続アプリケーション](#)」と入力し、[接続アプリケーションを管理する] を選択します。
2. [Salesforce IQ] > [編集] > [更新トークンポリシー] を選択します。

ユーザの Salesforce パスワードは、Outlook インテグレーション、Gmail インテグレーション、または Salesforce AWS サーバに保存されません。Salesforce AWS サーバで認証するための個別のトークンが取得されます。このトークンは、認証 HTTPS ヘッダーに渡される個別のベアラートークンです。

Salesforce AWS サーバに対するネットワークコールは、すべて TLS 1.2 を介して実行されます。

Salesforce システム管理者は、いつでも OAuth アクセスをブロックできます。Salesforce の [設定] から、[クイック検索] ボックスに「[接続アプリケーション](#)」と入力し、[接続アプリケーションの OAuth の利用状況] を選択します。

個人ユーザは、各自の Salesforce OAuth トークンを取り消すことができます。Salesforce システム管理者も、任意のユーザの OAuth トークンを取り消すことができます。OAuth トークンは、個人設定の[接続]に表示されます。

Gmail ガイドライン

ユーザに Inbox ライセンスがある場合、Inbox インテグレーションでは、OAuth 2.0 プロトコルを使用して Gmail アカウントを接続します。Chrome 拡張機能およびモバイルアプリケーションは、Salesforce アカウントにログインするためのページを開きます。この初回ログインが完了すると、Salesforce AWS サーバは、Google に対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。このトークンは、そのユーザの Gmail アカウントへのアクセス権を提供するシングルユーザトークンです。Chrome 拡張機能および Salesforce AWS サーバは、ユーザの Google パスワードを使用したり保存したりしません。

Inbox モバイルアプリケーションは、メールアプリケーションとカレンダーアプリケーションで構成されるため、Google メールとカレンダーに対する参照および更新のフルアクセス権が必要です。また、Google ドライブからメールへのファイル添付をサポートするには、Google ドライブに対する参照のみのアクセス権も必要になります。Inbox モバイルアプリケーションでは、次の Google OAuth 権限が必要です。

- <https://mail.google.com/>
- <https://www.google.com/m8/feeds/>
- <https://www.googleapis.com/auth/userinfo.profile>
- <https://www.googleapis.com/auth/userinfo.email>
- <https://www.googleapis.com/auth/calendar>
- <https://www.googleapis.com/auth/drive.readonly>

ユーザは、Google アカウントユーザ設定でサードパーティアプリケーションに移動して、いつでも Google OAuth トークンを取り消すことができます。サードパーティアプリケーションの削除についての詳細は、[Google ヘルプ](#)を参照してください。

Google に対するネットワークコールは、すべて TLS 1.2 AES-256 暗号化を使用して実行されます。Inbox では、Google の 2 つのプロトコルが使用されます。

- Gmail API - [Gmail API リファレンス](#)を参照してください。
- Google カレンダー API - [Google カレンダー API リファレンス](#)を参照してください。

Exchange Online (Office 365) ガイドライン

ユーザに Inbox ライセンスがある場合、Outlook インテグレーションでは、このガイドに記載されている [OAuth 2.0 プロトコル](#)を使用して Office 365 アカウントを接続します。Outlook アドインおよびモバイルアプリケーションは、Salesforce アカウントにログインするためのページを開きます。この初回ログインが完了すると、Salesforce AWS サーバは Office 365 に対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。このトークンは、そのユーザの Office 365 アカウントへのアクセス権を提供するシングルユーザトークンです。Salesforce は、ユーザの Office 365 パスワードを使用または保存しません。

Inbox モバイルアプリケーションは、メールアプリケーションとカレンダーアプリケーションであるため、Office 365 メールとカレンダーに対する参照および更新のフルアクセス権が必要です。Inbox モバイルアプリケーションでは、次の Office 365 権限が必要です。

- 特定のユーザとしてメールを送信する
- ユーザのカレンダーを参照および更新する
- ユーザの連絡先を参照および更新する
- ユーザのプロファイルを参照する
- EWS を介してサインイン済みユーザとしてメールボックスにアクセスする
- ユーザのメールを参照および更新する

ユーザは、いつでも Office 365 OAuth トークンを取り消すことができます。Office 365 に移動し、[マイアカウント] と [アプリの権限] を選択します。

Microsoft Azure システム管理者は、[Microsoft Azure Active Directory](#) で、Office 365 OAuth 更新トークンの有効期限を MaxAgeSingleFactor および MaxAgeMultiFactor に設定して変更できます。

Outlook アドインまたは Inbox モバイルアプリケーションと Office 365 間のネットワークコールは、すべて TLS1.2 を介して実行されます。

Salesforce は、次のプロトコルを使用して、Office 365 のメールおよびカレンダーにアクセスします。

対象	プロトコル	認証	メモ
Salesforce AWS サーバ	EWS	OAuth 2.0 認証	EWS は、Windows および Mac の Microsoft Outlook デスクトップで使用する SOAP ベースのプロトコルです。Salesforce AWS サーバは、定期的ではなく通知に基づいてデータをポーリングします。詳細は、 Office 開発センターの「Exchange の通知サブスクリプション、メールボックスイベント、および EWS」 を参照してください。
Inbox モバイルアプリケーション	Exchange ActiveSync (EAS) または Office 365 REST API	EAS では、ユーザ名、ドメイン、パスワードを使用した認証がサポートされます。 Office 365 REST API では、OAuth 2.0 アクセストークンが使用されます。	Exchange ActiveSync (EAS) は、モバイルアプリケーションを対象とした XML ベースのバイナリプロトコルです。ネイティブ iOS メールアプリケーションおよび Android Exchange メールアプリケーションでは、EAS プロトコルが使用されます。iOS 用 Exchange ActiveSync についての詳細は、 Apple サポートトピック を参照してください。 Microsoft には、 Microsoft Graph API や Office 365 REST API と呼ばれる新しい API があります。iOS および Android 用 Microsoft Outlook アプリケーションで Microsoft Graph API を使用して、メールやカレンダーのイベント (行動) を読み取りおよび書き込みできるようになりました。 Inbox モバイルアプリケーションでは、IMAP プロトコルは使用されません。

Microsoft Exchange 社内ガイドライン

社内の Exchange インスタンス (2013、2016、2019) との接続では、ユーザ名、パスワード、ドメインに基づく従来の認証が使用されます。この場合、Salesforce AWS サーバと Inbox モバイルアプリケーションが Exchange パスワードを保存します。パスワードは、AES-256 暗号化を使用して保存時に暗号化されます。

Exchange でのネットワークコールは、TLS 1.1 または TLS 1.2 を使用して実行されます。TLS プロトコルは、Exchange サーバでサポートされている最上位の TLS プロトコルで決定されます。

Salesforce は、次の 2 つのプロトコルを使用して、Exchange のメールおよびカレンダーにアクセスします。

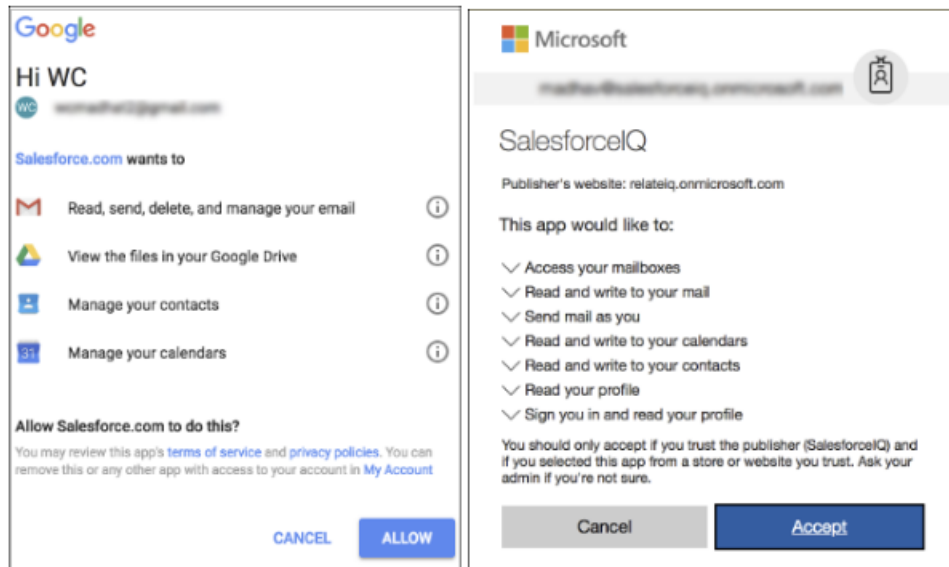
対象	プロトコル	メモ
Salesforce AWS サーバ	EWS	EWS は、Microsoft Outlook デスクトップで使用される SOAP ベースのプロトコルです。
Inbox モバイル アプリケー ション	Exchange ActiveSync (EAS) ま たは Office 365 REST API	Exchange ActiveSync (EAS) は、モバイルアプリケーションを対象とした XML ベースのバイナリプロトコルです。ネイティブ iOS メールアプリケーションおよび AndroidExchange メールアプリケーションでは、EAS プロトコルが使用されます。

社内サーバでは、OAuth 2.0 プロトコルはサポートされません。この接続では、代わりに NT LAN Manager (NTLMv2) および基本認証がサポートされます。これらの認証では、Office 365 の OAuth 2.0 とは異なり、ユーザ名、ドメイン、パスワードが必要になります。

Microsoft で [Microsoft Graph API](#) や Office 365 REST API と呼ばれる新しい API が最近導入されました。Office 365 上にない Exchange サーバでは、新しい Office 365 REST API や Microsoft Graph API はサポートされません。

Office 365 API については、[Microsoft ドキュメント](#)を参照してください。

OAuth プロトコルについての詳細



Inbox ライセンスでプロビジョニングされる場合、ユーザは Salesforce プラットフォームと各自のメールプロバイダに接続されます。Gmail または Office 365 メールアカウントを持つモバイルユーザは、OAuth 2.0 プロトコルを使用して接続されます。この初回ログインが完了すると、Salesforce AWS サーバは、サーバに対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。

OAuth 2.0 を使用すると、Gmail や Office 365 などのサービスにログインプロセスを委任している間、Salesforce などのサードパーティアプリケーションでそのようなサービスにアクセスできます。

ユーザがサービスに接続すると、Salesforce はサービスのログインページにアクセスするための新しいページを開きます。このページは、次のようなサービスの独自のログイン Web ページになります。

- <https://login.salesforce.com/>
- <https://accounts.google.com>
- <https://login.microsoftonline.com>

ユーザがログインすると、サードパーティアプリケーション (このケースでは Salesforce) に権限を付与するように求められます。次のような権限を付与します。

- メールに対する参照および更新のフルアクセス権。
- カレンダーに対する参照および更新のフルアクセス権。

ユーザが権限を付与すると、サービスは Salesforce AWS サーバにリダイレクトされます。Salesforce AWS サーバは、サービスに接続して、以下を取得します。

- OAuth 更新トークン
- OAuth アクセストークン

OAuth アクセストークンは、サービスに対して認証済み要求 (メールやカレンダーのイベント (行動) の取得など) を実行するために使用されます。これらのトークンの有効期限は1時間後に切れます。別のアクセストークンを取得するには、OAuth 更新トークンが使用されます。通常、更新トークンの有効期限は長い、期限がありません。

Salesforce AWS サーバ操作

Salesforce AWS サーバは、次のメールおよびカレンダー操作を実行します。

- メールボックスからメールヘッダーおよび HTML 本文を取得して保存する。
- 送信済みメールからメールヘッダーおよび HTML 本文を取得する。
- カレンダーのイベント (行動) を取得して保存する。
- [後で送信] 機能を使用してメールメッセージを送信する。
- [対応可能時間を挿入] を使用して被招集者が含まれるイベント (行動) を作成する。

Inbox モバイルアプリケーションには、メールとカレンダーに対する参照および更新のフルアクセス権があり、メールとカレンダーに対して次の操作を実行します。

- 添付ファイルが含まれるメールの読み取り、作成、送信を行う
- 既読としてマークしたり、フラグを付けたり、メールをフォルダ、アーカイブ、ごみ箱に移動したりする
- イベント (行動) を表示、作成、編集する
- イベント (行動) に RSVPing する

モバイルデバイス管理とモバイルアプリケーション管理および Inbox

Inbox モバイルアプリケーションでは、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) が制限付きでサポートされます。

Inbox モバイルでは、以下で MDM クライアント証明書がサポートされます。

- ユーザの Salesforce ログイン。
- Office 365 メールアカウントへの接続。
- Google メールアカウントへの接続。

Inbox モバイルでは、Exchange 2013 または 2016 メールアカウントの MDM クライアント証明書はサポートされません。

特定のベンダーについては、次のようになります。

- Inbox モバイルでは、iOS デバイスで Inbox を使用する場合に Office 365 メールアカウントの Microsoft Intune MAM および MDM がサポートされます。
- Inbox モバイルでは、MobileIron や VMWare Airwatch などの MDM ソリューションはサポートされません。

iOS 用 Inbox モバイルの Microsoft Intune サポート

iOS 用 Inbox モバイルバージョン 8.6.0 以降、モバイルアプリケーション管理 (MAM) およびモバイルデータ管理 (MDM) のために iOS 用 Inbox モバイルを Microsoft Intune に追加できます。Inbox モバイルアプリケーションを Intune に追加して、Salesforce 組織が正しく設定されていることを確認するには、次のアクションを実行します。

アクション	詳細	リソース
Salesforce Inbox モバイルアプリケーションを Intune の管理アプリケーションとして追加する。	iOS アプリケーションを Intune に追加 する詳細な手順については、Microsoft ドキュメントを参照してください。	アプリケーションを Intune に追加するには、App Store リンクとバンドル ID が必要です。 App Store リンク: https://apps.apple.com/us/app/salesforce-inbox/id1208232122 iOS バンドル ID: com.salesforce.inbox
Intune の Inbox モバイルアプリケーションエントリ のアプリケーション保護 ポリシーを作成する。	アプリケーション保護ポリシーの作成 については、Microsoft ドキュメントを参照してください。	
Azure Active Directory で、 Office 365 の管理者の同意 設定を定義する。	合理化された認証フローを実現するには、管理者の同意を Intune に提供します。 1. この URL に移動します。 2. Office365 アカウントにログインします。同意を付与するウィンドウが表示されます。 3. 組織の代わりに管理者の同意権限を Salesforce Inbox 用 Intune に付与するには、[同意する]をクリックします。	管理者の同意についての詳細
Salesforce で Intune のサ ポートを有効化する。	Inbox モバイルアプリケーション用 Intune を使用するように Salesforce を設定します。 1. Salesforce の [設定] の [クイック検索] ボックスに「Inbox」と入力し、[設定アシスタント]を選択します。 2. Microsoft Intune を有効化します。	

モバイルアプリケーションデータの削除

Salesforce システム管理者は、いつでも特定のユーザの Salesforce または Salesforce Inbox ライセンスを削除できます。ライセンスが削除されてから、ユーザがアプリケーションを開くと、ユーザはアプリケーションからログアウトされ、ローカルに保存されているそのユーザのすべてのデータが削除されます。

Exchange システム管理者は、Exchange ActiveSync リモートワイプを開始することもできます。Exchange システム管理者は、Exchange Active Sync リモートワイプを呼び出すこともできます。

- Office 365 の場合、Office 365 設定に移動してデータをワイプします。
- 社内の Exchange サーバの場合、Exchange 管理センターに移動してデータをワイプします。

データをワイプした後に、アプリケーションを開くと、アプリケーションはExchangeに接続されて、リモートワイプ応答を受信します。メールアカウントは無効としてマークされます。ユーザはアプリケーションからログアウトされ、ローカルに保存されているそのユーザのすべてのデータが削除されます。