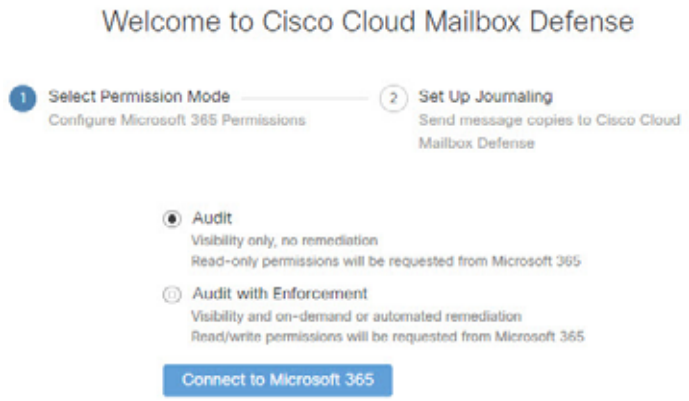
ビジネスの設定

クラウドメールボックス ビジネスを設定するには、次の手順を実行します。次の手順は、**要件（9 ページ）**を満たしていることを前提としています。

1. シスコからのウェルカムメールの指示に従って、アカウントを設定します。

   クラウドメールボックス Cisco SecureX サインオンを使用してユーザ認証を管理します。SecureX サインオンの詳細については、https://cisco.com/go/securesignon を参照してください。既存の SecureX Threat Response、Cisco Secure Malware Analytics（旧 Threat Grid）、または Cisco Secure Endpoint（旧 AMP）のお客様は、必ず既存のクレデンシャルでサインインしてください。既存のユーザでない場合は、新しい SecureX サインオンアカウントを作成するように求められます。

   これで、[Welcome to Cisco Cloud Mailbox Defense] ページにアクセスできます。

2. [Permission Mode] を選択します。

   [Permission Mode] は、適用できる修復ポリシーのタイプを定義します。[Permission Mode] には次の 2 つのオプションがあります。

   - [Audit]：可視性のみを許可し、修復は許可しません。読み取り専用権限が Microsoft 365 から要求されます。
   - [Audit with Enforcement]：可視性、およびオンデマンドまたは自動の修復（疑わしいメッセージの移動または削除）が可能です。読み取り/書き込み権限が Microsoft 365 から要求されます。

     注：[Audit with Enforcement] を選択した場合は、**ポリシー設定（15 ページ）**で [Automated Remediation] をオンにする必要があります。すべての内部電子メールに自動修復を適用するには、[Apply auto-remediation to domains not in the domain list] トグルを [On] に設定します。

3. Microsoft 365 に接続します。

   a. [Connect to Microsoft 365] をクリックします。

   b. 指示に従って、Microsoft 365 アカウントにログインします。Microsoft 365 でジャーナリングを設定するには、このアカウントにグローバル管理者権限が必要です。このアカウントは クラウドメールボックス で保存または使用されません。これらの権限が必要な理由については、Cisco Secure Email Cloud Mailbox の FAQ「Cloud Mailbox を設定するために Microsoft 365 グローバル管理者権限が必要なのはなぜですか。(Why are Microsoft 365 Global Admin rights required to set up Cloud Mailbox?)」を参照してください。

   c. [承認(Accept)] をクリックして、Cloud Mailbox アプリケーションの権限を承認します。クラウドメールボックス の設定ページにリダイレクトされます。

4. **Cisco Secure Email Gateway(SEG)を使用しているユーザーの場合**:Microsoft 365 にコネクタを追加します。

   ジャーナルが Cisco Secure Email Gateway を経由することなく、Microsoft 365 から Cloud Mailbox に直接送信されるようにするには、Microsoft 365 に送信コネクタを追加することをお勧めします。コネクタはジャーナルを設定する前に追加する必要があります。

   Microsoft 365 Exchange 管理センターから、[コネクタの追加(Add a connctor)] ウィザードの次の設定を使用して新しいコネクタを作成します。

   - [接続元(Connection from)]:Office 365
   - [接続先(Connection to)]:パートナー組織
   - [コネクタ名(Connector name)]:Cisco Secure Email Cloud Mailbox へのアウトバウンド([オンにする(Turn it on)] チェックボックスを選択)
   - [コネクタの使用(Use of connector)]:電子メールメッセージがこれらのドメインに送信される場合のみ(mail.cmd.cisco.com を追加)
   - [ルーティング(Routing)]:パートナーのドメインに関連付けられた MX レコードを使用
   - [セキュリティの制限(Security restrictions)]:接続を保護するために、常に信頼できる認証局(CA)によって発行されたトランスポート層セキュリティ(TLS)を使用します(推奨)。
   - [検証用の電子メール(Validation email)]:クラウドメールボックス の設定ページのジャーナルアドレス。

   注:設定が完了したら、[Cloud Mailbox ポリシー(Cloud Mailbox Policy)] ページで Cisco Secure Email Gateway(SEG)の存在を示す必要があります。詳細については、ゲートウェイを使用している場合のポリシー設定(17 ページ)を参照してください。

5. Microsoft 365 でジャーナリングを設定します。

   クラウドメールボックス にジャーナルを送信するように Microsoft 365 を設定する必要があります。これを行うには、ジャーナルルールを追加します。

   注:ジャーナルルールを設定すると、すぐにクラウドメールボックス バックエンドへのデータフローが始まります。デフォルトの クラウドメールボックス ポリシー設定が適用されます。ジャーナルルールを有効にしてから 10 ~ 60 分以内に、コンソールにデータが表示されます。

   注:最小限の Cisco Secure Malware Analytics(旧 Threat Grid)アカウントが作成され、ウェルカムメールが届きます。新しいアカウントは、既存のマルウェア分析/Threat Grid アカウントにリンクされていません。クラウドメールボックス を設定するためにマルウェア分析/Threat Grid アカウントで必要なアクションはありません。

   a. クラウドメールボックス の設定ページから、ジャーナルアドレスをコピーします。後でこのプロセスを繰り返す必要がある場合は、[管理(Administration)] ページでジャーナルアドレスを確認することもできます。

   b. Microsoft 365 管理センター(https://admin.microsoft.com/AdminPortal/Home#/homepage)に移動します。

      注:これらの手順は、従来の Exchange 管理センターを使用していることを前提としています。

c. [管理センター] > [Exchange] > [コンプライアンス管理] > [ジャーナルルール] の順に移動します。

d. [Send undeliverable journal reports to] フィールドに Exchange の受信者を追加します。使用される電子メールアドレスはジャーナリングされません。クラウドメールボックス の分析対象とするアドレスを使用しないでください。この目的で使用する受信者がいない場合は、受信者を作成する必要があります。

e. [+] ボタンをクリックして、新しいジャーナルルールを作成します。

f. クラウドメールボックス 設定ページからコピーしたジャーナルアドレスを [ジャーナルレポートの送信先(Send journal reports to)] フィールドに貼り付けます。

g. [Name] フィールドに **Cisco クラウドメールボックス** と入力します。

h. [If the message is sent to or received from] ドロップダウンから [Apply to All Messages] を選択します。

i. [Journal the following messages] ドロップダウンから適切なオプションを選択します。

– クラウドメールボックス のお客様の場合は、[すべてのメッセージ(All messages)] を選択してください。

– CES Internal Mailbox Defense(IMD)のお客様の場合は、[Internal messages only] を選択してください。

j. [保存(Save)] をクリックします。

6. クラウドメールボックス の設定ページに戻ります。[enable policy enforcement] をクリックします。

注: ジャーナルルールを有効にしてから 10 ~ 60 分以内にコンソールにデータが表示されます。テナント統合時からジャーナリングが完全に有効になるまでのこのキャッシングの遅延中に、Microsoft 365 から配信不能メッセージレポートを受信する場合があります。これらのメッセージは、システム統合が完了すると停止します。

ポリシー設定の確認または変更については、**ポリシー設定(15 ページ)**を参照してください。[監査と施行(Audit with Enforcement)] モードを選択した場合は、[自動修復(Automated Remediation)] 設定を確認する必要があります。すべての内部電子メールに自動修復を適用するには、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domain not in domain list)] がオンに設定されていることを確認します。

ドメインのインポート

ドメインをインポートして、特定のドメインに自動修復を適用できるようにします。Cloud Mailbox は、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] ボックスがオンかオフかによって、新しくインポートされたドメインを異なる方法で処理します。

- [ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] がオンになっている場合、インポートされるすべての新しいドメインに自動修復が適用されます。
- [ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] がオフになっている場合、インポートされる新しいドメインに自動修復は適用されません。

デフォルトでは、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] はオフになっています。

手動インポート

ドメインを手動でインポートするには、次の手順を実行します(ビジネスをセットアップするときに推奨):

1. [Settings](歯車アイコン)> [Policy] に移動します。
2. [インンポートされたドメインの更新(Update Imported Domains)] ボタンをクリックし、ドメインを クラウドメールボックス にインポートします。
3. 各ドメインの横にあるチェックボックスを使用して、そのドメインの自動修復設定を調整します。

4. また、[ドメインリストにないドメインに自動修復を適用する（Apply auto-remediation to domains not in the domain list）] をオンにして、自動修復がすべての内部メールと後で自動的にインポートされるドメインに適用されるようにすることもお勧めします。
5. [Save and Apply] をクリックします。

自動インポート

リストを最新にするために、ドメインは 24 時間ごとに自動的にインポートされます。