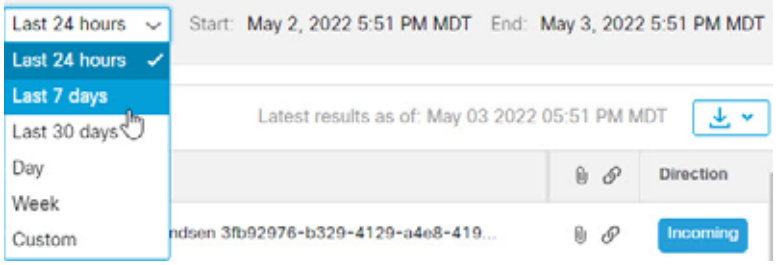
メッセージ

[メッセージ(Messages)] ページにはメッセージと検索結果が表示され、侵害の可能性を調べることができます。1 ページあたり最大 100 件のメッセージを表示できます。

ドロップダウンメニューを使用して、既定の期間(過去 24 時間、過去 7 日間、過去 30 日間)のデータを表示するか、過去 90 日間の特定の日、週、またはカスタム時間枠を設定します。

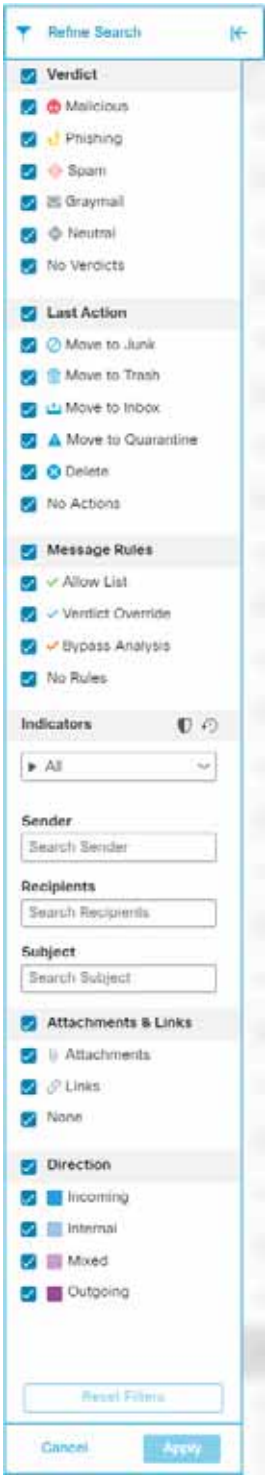


検索フィールドを使用して、文字列を検索したり、ハッシュや URL などの注目する指標を検索します。

[検索の絞り込み(Refine Search)] フィルタパネルを使用して検索を絞り込みます。たとえば、特定の送信者から送信されたすべてのメール、特定の判定のメール、添付ファイルやリンクがあるメール、または迷惑メールに移動されたメールを表示できます。

1. 矢印をクリックして、フィルタパネルを展開します。

2. 選択を行い、[Apply] をクリックします。少なくとも 1 つの判定を選択する必要があることに注意してください。



フィルタをデフォルトにリセットには、[フィルタのリセット（Reset Filters）] ボタンを使用します。

Messages ページのアイコン

次の表に、[Messages] ページで使用されるアイコンとその意味を示します。

表 1　Messages ページのアイコン

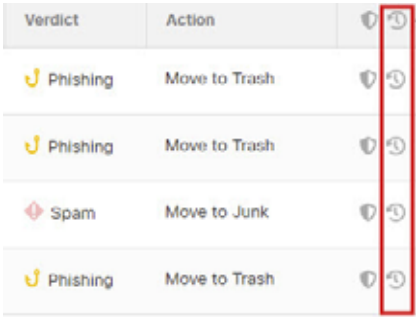
アイコン	名前	説明
	リンク	メッセージにリンクが含まれています。
	添付ファイル	メッセージに添付ファイルが含まれています
	自動修復	メッセージは クラウドメールボックス によって自動修復されました。
	レトロスペクティブな判定	レトロスペクティブな判定が適用されました。レトロスペクティブな判定は、メッセージが クラウドメールボックス によって最初にスキャンされた後に適用されたものです。
	許可	メッセージが、指定された項目（許可リスト、MS 許可リスト、または安全な送信者）に基づいて許可されました。
	判定のオーバーライド	判定が、判定のオーバーライド メッセージ ルールに基づいてオーバーライドされました。
	バイパス分析	バイパス分析メッセージルールにより、メッセージが分析されませんでした。ルールのタイプ（安全な送信者またはフィッシングテスト）が指定されています。
	ニュートラル	メッセージがニュートラルとしてマークされています。
	Spam	メッセージが手動または自動修復によってスパムとしてマークされました。
	フィッシング	メッセージは、手動または自動修復によってフィッシングとしてマークされています。
	悪意あり	メッセージは、手動または自動修復によって悪意のあるものとしてマークされています。
	Graymail	メッセージがグレイメールとしてマークされています。グレイメールは、マーケティング、ソーシャル、またはジャンクと判断されたメールです。

レトロスペクティブな判定

レトロスペクティブな判定は、メッセージが クラウドメールボックス によって最初にスキャンされた後のある時点でメッセージに適用されたものです。

クラウドメールボックス のレトロスペクティブな判定は、他のシスコのセキュリティ製品とは若干異なります。クラウドメールボックス はインラインメールプロセッサではありませんが、メッセージの初期分析を完了するための固定の時間範囲があります。Talos のディープ URL 分析など、分析時間が長い新しいコンテンツエンジンは、レトロスペクティブな判定として扱われます。判定が遅れると、修復も遅れます。したがって、クラウドメールボックス はこれらの判定を明確にタグ付けします。

レトロスペクティブな判定は、次のように [メール(Messages)] ページに示されます。



レトロスペクティブな判定の電子メール通知

レトロスペクティブな判定の電子メール通知をオンまたはオフにするには、次の手順を実行します。

1. [Settings](歯車アイコン)> [Administration] > [Business] を選択します。
2. [Notification Email Address] で、[Send Notifications for Retrospect Verdicts] を選択または選択解除します。

このチェックボックスがオンの場合、レトロスペクティブンな判定の電子メール通知が通知用に指定された電子メールアドレスに送信されます。これらの通知はデフォルトでオンになっています。

メッセージの調査

[Messages] ページの検索結果内のメッセージを調査するには、[>] アイコンを選択してメッセージを展開し、送信者 IP、Microsoft メッセージ ID、添付ファイル、リンクなどの詳細を確認します。

Timeline

特定のメッセージのイベントタイムラインを表示するには、[More](縦の 3 つのドット)> [Timeline] を選択します。

イベントタイムラインには次の情報が表示されます。

- [Received]:メッセージが受信された時刻、およびメッセージの詳細
- [Verdict]:示された判定に関する情報
- [アクション(Action)]:メッセージに対して実行されたアクションに関する情報
- [メッセージルール(Message Rule)]:適用されたルールに関する情報

- [ルール(Rule)]:適用されたメッセージルールに関する情報

Conversation(ベータ)

注: この機能は現在ベータ版です。改善への取り組み中であるため、いくつか問題が発生する可能性があります。既知の問題は次のとおりです。

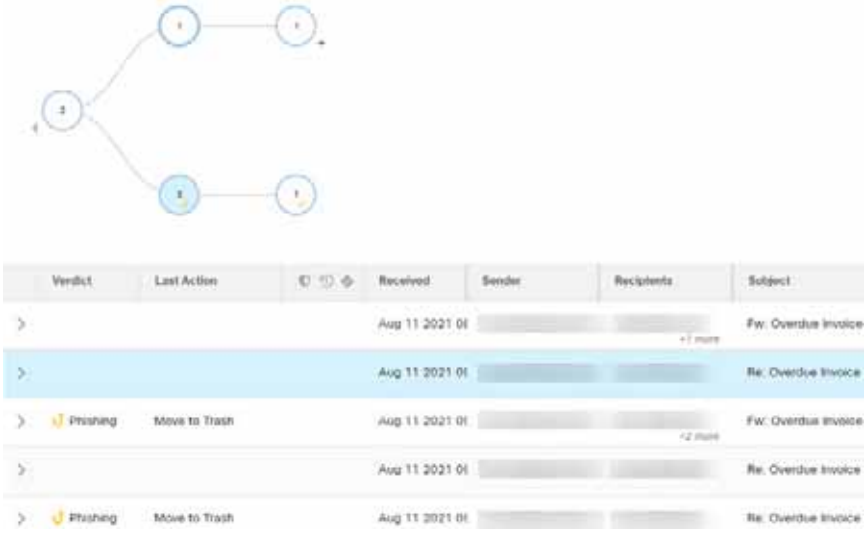
- 追加のメッセージがない場合でも、**[+]** 記号はクリックするまで表示されたままです。
- 水平ノードは 9 個に制限されています。

カンバセーションビューでは、カンバセーションの全体ビューが表示されます。カンバセーションビューを使用して、カンバセーション内のメッセージを追跡し、メールフローを完全に把握します。これは、脅威の発生源と組織内で拡散する方法を判断するのに役立ちます。

[More](縦の 3 つのドット)> **[Conversation]** を選択すると、特定の電子メールと繋がりがあるメッセージが表示されます。

ノード(青色で塗りつぶし)は、開始したメッセージを表します。**[+]** アイコンをクリックしてカンバセーションのノードを展開すると、カンバセーションの前後のメッセージを確認できます。展開されたノードは、ノードの下に表示されるメッセージグリッドに追加されます。ノードとメッセージは、着信、発信、混合、または内部を示すために色分けされています。

ノード円内の数字は、メッセージの送信先アドレス数を示します。ノード内のアイコンは、脅威が検出されたかどうかを示します。ノードを選択すると、対応するメッセージがグリッド内で強調表示されます。



メッセージの移動と再分類

誤って分類されたと思われるメッセージを移動または再分類するには、[Messages] ページを使用します。1 ページに表示されるメッセージ数を変更することで、一度に最大 100 件のメッセージを移動または再分類できます。

注:再分類は、選択したメッセージの判定にのみ影響します。選択した送信者からの今後のメッセージ、またはメッセージの内容に基づいた今後のメッセージへの変更は示すものではありません。メッセージは、Cisco Talos による確認のためにキューに入れられます。Talos は、今後の分類に影響を与えるためにこのフィードバックを使用する場合があります。スパムまたはグレイメールメッセージの誤検出については、判定のオーバーライドルール(44 ページ)をビジネスに追加することを検討してください。

Audit モード

[Audit] モードでは、メッセージの再分類(異なる判定の適用)が可能です。

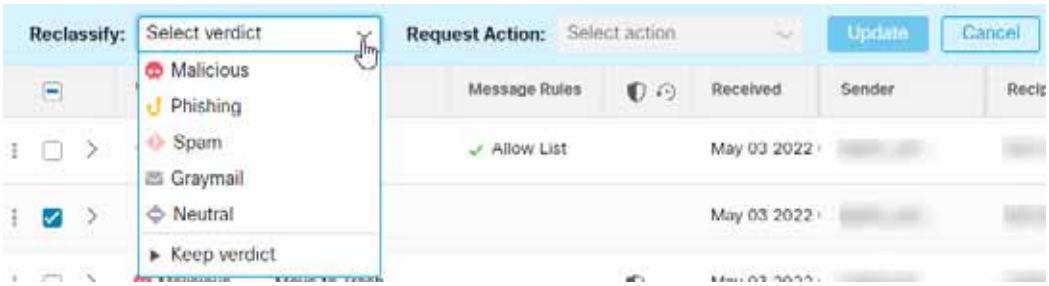
1. 再分類するメッセージを選択します。
2. ドロップダウンメニューから判定を選択します。メッセージは、[悪意のある(Malicious)]、[フィッシング(Phishing)]、[スパム(Spam)]、[グレイメール(Graymail)]、または [ニュートラル(Neutral)] に再分類できます。

3. 新しい分類を適用するには、[更新(Update)] をクリックします。

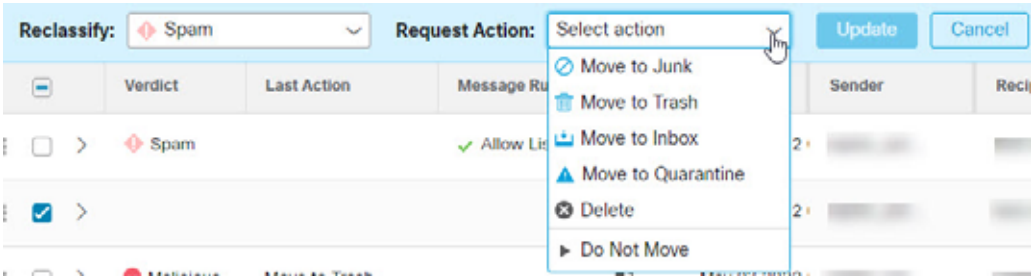
Audit with Enforcement モード

[Audit with Enforcement] モードでは、疑わしいメッセージをユーザの受信トレイから迷惑メール(Junk)またはゴミ箱(Trash)に移動できます。同様に、迷惑メールまたはごみ箱に移動されたメッセージが疑わしくないと判断した場合は、そのメッセージをユーザの受信トレイに戻すことができます。メッセージを完全に削除することもできます。このプロセスでは、メッセージを再分類(異なる判定を適用)することもできます。

1. 移動または再分類するメッセージを選択します。
2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[悪意のある(Malicious)]、[フィッシング(Phishing)]、[スパム(Spam)]、[グレイメール(Graymail)]、または [ニュートラル(Neutral)] に再分類するか、または判定を保持することができます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューからアクションを選択します。[迷惑メールに移動(Move to Junk)]、[ゴミ箱に移動(Move to Trash)]、[受信トレイに移動(Move to Inbox)]、[隔離に移動(Move to Quarantine)]、[削除(Delete)]、または [移動しない(Do Not Move)] を選択できます。



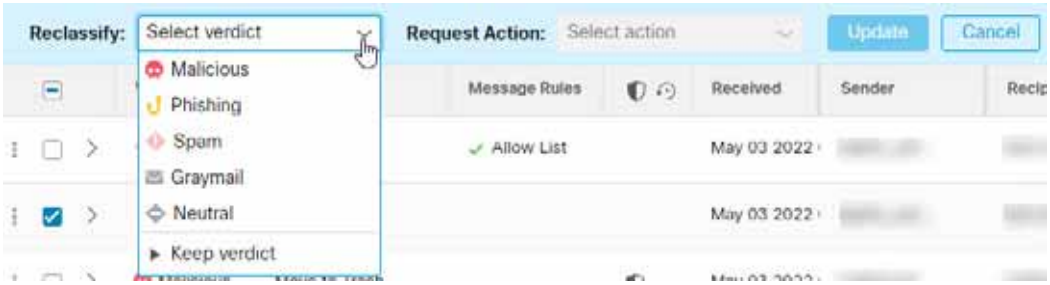
4. [更新(Refresh)] をクリックして新しい分類を適用し、メッセージに対してアクションを実行します。

メッセージが移動された場合は、[最後のアクション(Last Action)] 列に示されます。

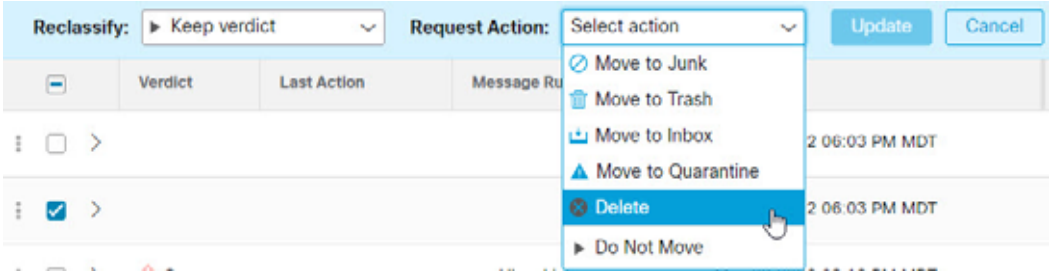
メッセージを削除する

スーパー管理者および管理ユーザーは、再分類/修正ワークフローの削除アクションを使用して、メールボックスからメッセージを完全に削除できます。削除されたメッセージは、**recoverableitemspurges** フォルダに移動されます。ユーザーはこのフォルダにアクセスできず、Cloud Mailbox では削除されたメッセージを受信トレイに復元できません。

1. 削除するメッセージを選択します。
2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[悪意のある(Malicious)]、[フィッシング(Phishing)]、[スパム(Spam)]、[グレイメール(Graymail)]、または [ニュートラル(Neutral)] に再分類するか、または判定を保持することができます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューから [削除(Delete)] を選択します。



4. [更新(Update)] をクリックしてメッセージを削除します。
5. [削除の確認(Confirm Deletion)] ダイアログに、メッセージは復元できないことが表示され、続行するかどうか確認されます。続行するには、[削除(Delete)] をクリックします。

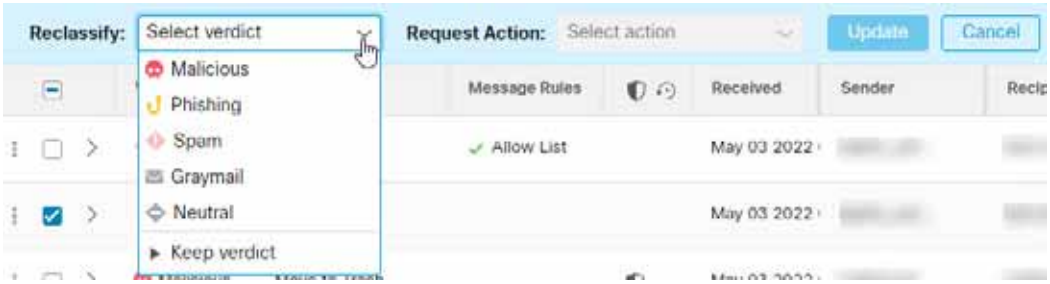
[最後のアクション(Last Action)] 列に削除が表示されます。この項目を選択または操作することはできません。

メッセージの隔離

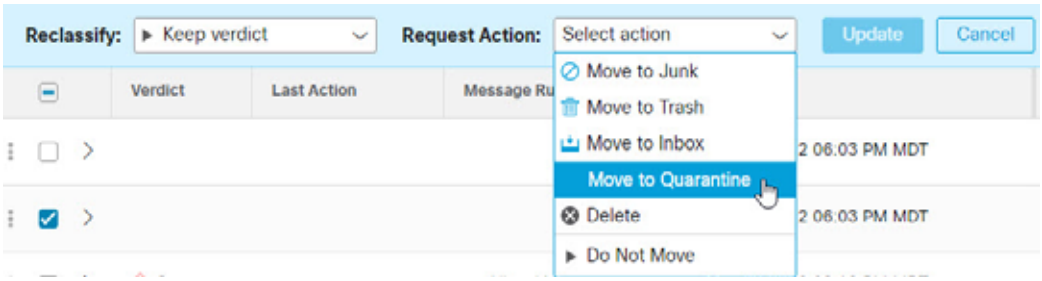
検疫フォルダはメールボックスごとに自動的に作成され、Outlook ユーザーには表示されません。シークレットフォルダ名は、[管理(Administration)] > [ビジネス(Administration)] ページで、スーパー管理者および管理者ユーザーに表示されます。Outlook では、検疫フォルダ内のメッセージは、削除済み項目の消去設定に従って自動的に消去されます。Cloud Mailbox では、検疫フォルダから消去されたメッセージをユーザーの受信トレイに復元することはできません。

メッセージを手動で隔離に移動するには、次の手順を実行します。

1. 隔離に移動するメッセージを選択します。
2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[悪意のある(Malicious)]、[フィッシング(Phishing)]、[スパム(Spam)]、[グレイメール(Graymail)]、または [ニュートラル(Neutral)] に再分類するか、または**判定を保持**することができます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューから [隔離に移動(Move to Quarantine)] を選択します。



4. [更新(Update)] をクリックして、メッセージを隔離します。

[隔離に移動(Move to Quarantine)] は、[最後のアクション(Last Action)] 列に表示されます。

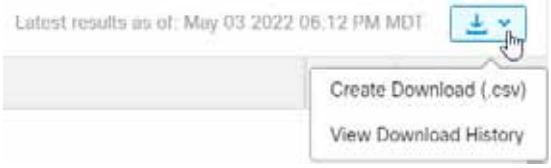
ハイブリッドアカウントについて

Cloud Mailbox は、Exchange Online(O365)に存在するメールボックス上でのみ動作します。メールボックスをオンプレミスの Exchange から Exchange Online(O365)に移行中の場合、修復(移動または削除)は、Exchange Online(O365)にあるメールボックスに対してのみ機能します。オンプレミスの Exchange メールボックスの修復が失敗したことは通知されません。

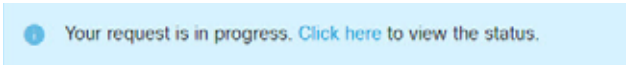
検索結果のダウンロード

検索結果のメッセージに関するデータの CSV ファイルをダウンロードできます。ダウンロードは 10,000 メッセージに制限されています。データをダウンロードするには、次の手順を実行します。

1. [ダウンロード(Download)] ボタンをクリックし、[ダウンロードの作成(.csv)(Create Download (.csv))] を選択します。



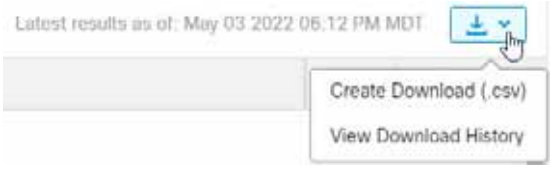
2. 要求が進行中であることを示すバナーが表示されます。テキストをクリックして、[ダウンロード履歴:メッセージ(Download History: Messages)] ページに移動します。



3. ダウンロードの準備ができたら、[アクション(Actions)] 列の [ダウンロード(Download)] アイコンをクリックしてファイルをダウンロードします。

ダウンロード履歴

ダウンロード履歴は 90 日間保持されます。[ダウンロード(Download)] ボタンをクリックし、[ダウンロード履歴の表示(View Download History)] を選択して [ダウンロード:メッセージ(Download: Messages)] ページに移動します。



このページには、日付範囲、ダウンロードを要求したユーザ、ダウンロードが開始された日付、およびステータスが表示されます。[アクション(Actions)] 列の [ダウンロード(Download)] アイコンを選択して、ファイルをダウンロードします。