Cisco Secure Access(SA)およびCisco Email Threat Defense(ETD)での電子メールDLPポリシーの設定方法

内容

はじめに

Eメールは、意図的でないデータ漏洩や不正なデータ漏洩の原因となる最も一般的なチャネルの1つです。組織が電子メールで共有する機密情報を保護できるように、シスコはCisco Secure Access(SA)とCisco Email Threat Defense(ETD)の統合を通じて、電子メールデータ損失防止(DLP)機能を提供しています。

このアーキテクチャでは、電子メールDLPポリシーの作成、設定、および適用アクションはすべてCisco Secure Accessで実行されます。Cisco Eメール脅威に対する防御は、Eメールの可視性とメッセージトラッキングを提供します。また、Cisco Secure Accessは、DLPルールを定義し、適用の動作を行うためのポリシーエンジンとして機能します。

この記事では、事前定義されたDLPテンプレートまたはカスタムのDLPテンプレートのいずれかを使用して、Cisco Secure Accessで電子メールDLPポリシーを作成する方法について説明します。

前提条件

設定プロセスを開始する前に、次の要件が満たされていることを確認してください。

- 管理アクセス：Cisco Email Threat Defense(ESA)インラインコンソールとCisco Secure Accessコンソールの両方に対して「完全な管理者」権限が必要です。
- アクティブサブスクリプション：Eメール脅威に対する防御テナントとセキュアアクセステナントの両方がアクティブで、プロビジョニングされていることを確認します。
- 接続：Email Threat Defense(ESA)とセキュアアクセス間のAPI統合が正常に確立されている必要があります。
- メールフロー設定：Email Threat Defenseが電子メールトラフィックをアクティブに検査していることを確認するために、Inlineモードで正しく展開されている必要があります。

重要：このソリューションではCisco Secure AccessとCisco Email Threat Defenseの両方を使用しますが、この記事で説明するEメールDLPルール設定手順はすべてCisco Secure Accessでのみ実行します。

使用する要件とコンポーネント

電子メールDLPポリシーを正常に実装するには、次のコンポーネントを使用します。

- Cisco Email Threat Defense(ETD):Eメールインスペクションポイントとして機能します。このツールは、送信Eメールトラフィックをキャプチャし、DLPエンジンが分析を実行するた

めに必要な通信フローを容易にします。
- Cisco Secure Access(SA):DLPエンジン：すべてのDLP設定が存在する主要コンポーネントです。Secure Accessコンソールを使用して、次の項目を定義します。
  - データ識別子：システムが監視する必要がある特定のパターンまたは機密データのタイプ（PII、クレジットカード番号、内部プロジェクトコードなど）。
  - DLPポリシー：機密データが検出された場合のシステムの対応を指定するルール（ブロック、暗号化、通知など）。
  - ポリシーアクション：DLPエンジンによってトリガーされる自動応答（電子メールの送信を阻止したり、必須の暗号化を適用するなど）。
- 統合フレームワーク：ETDがSecure Access DLPエンジンに電子メールメタデータを渡して、ポリシーの評価とその後の適用を実現できるようにするバックエンド接続。

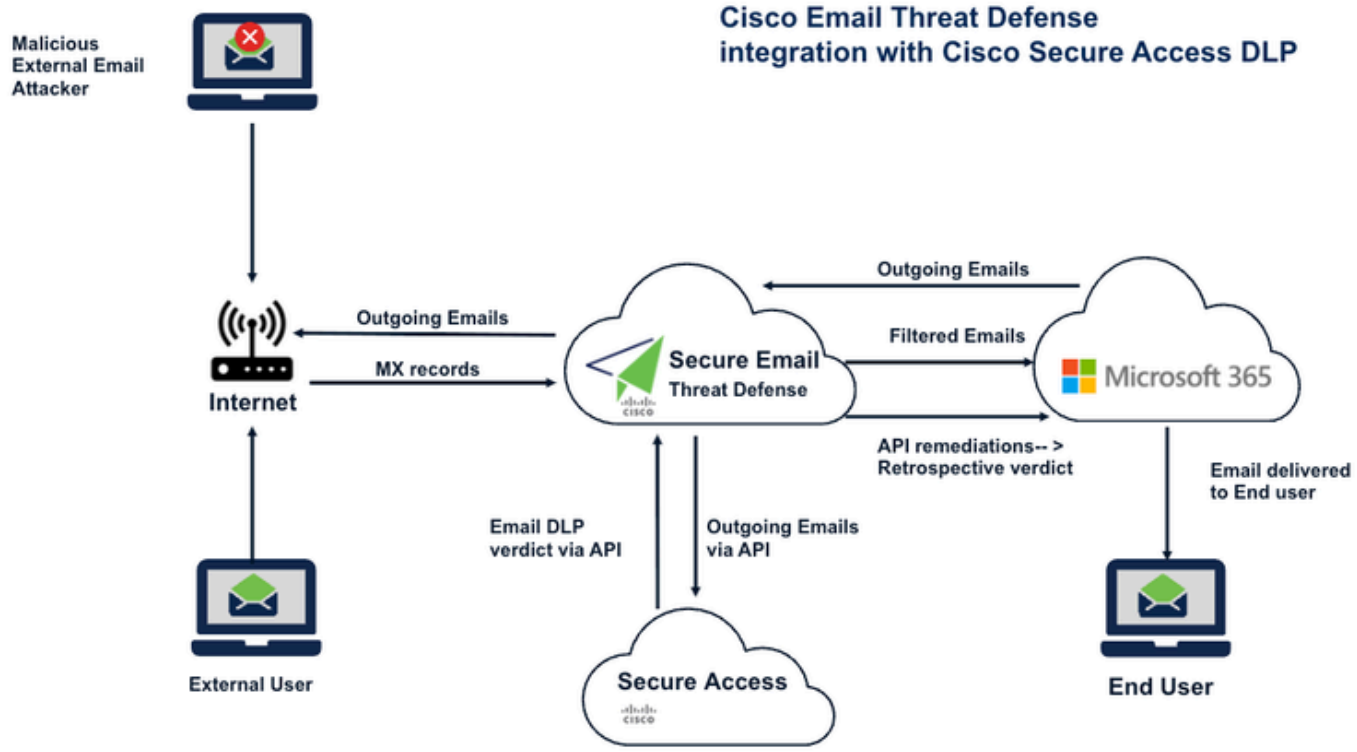
電子メールDLPポリシー機能

Cisco Secure Accessで電子メールDLPポリシーを作成する場合は、次の項目を設定できます。

- ルールの名前と説明
- 重大度
- データ分類
- 以下を含む検査範囲：
  - 電子メールの件名
  - メッセージ本文
  - 添付ファイル名
  - 添付ファイルの内容
- 次のようなファイルコントロール：
  - MIPラベル
  - Titusラベル
- 送信者の条件
- 受信者の条件
- ポリシーアクション：
  - モニタ
  - Block
- オプションのユーザ通知

ネットワーク図

Cisco Secure Email Threat DefenseとCisco Secure Accessの統合、およびトラフィックフローチャートを示すネットワークダイアグラムを以下に示します。



注：上の図では、ExchangeサーバはO365ですが、このDLP設定はSMTPをサポートする任意のExchangeサーバで実行できます。

注：APIを介してCisco Eメール脅威に対する防御とCisco Secure Accessを統合するには、「Steps to integrate Cisco Email Threat Defense(ETD) with Cisco Secure Access:」の記事を参照してください。

設定

Cisco Secure Accessでの電子メールDLPポリシーの設定

ステップ1:Cisco Secure Accessにログインします。

必要な権限を持つ管理者アカウントを使用して、Cisco Secure Access(SA)コンソールにログインします。

ステップ2：電子メールDLPルールの作成に移動します。

セキュアアクセスダッシュボードから、次の場所に移動します。

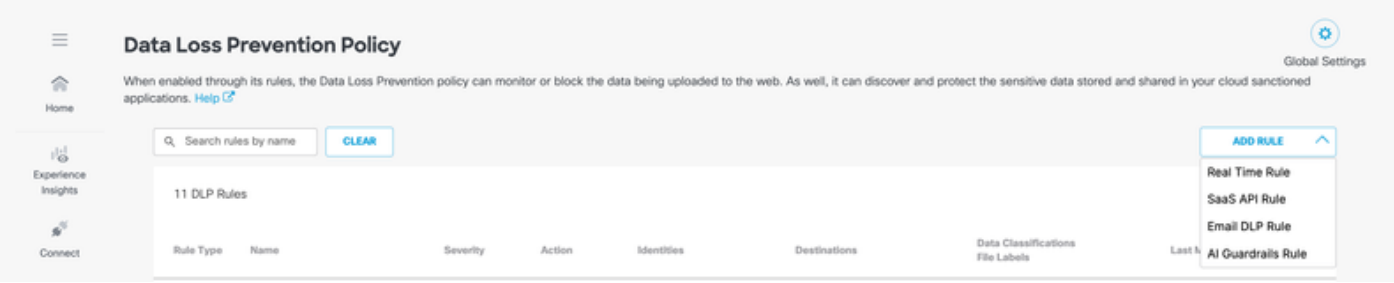
Secure > Policy > Data Loss Prevention Policy > Add Rule > Email DLP Rule

これにより、新しい電子メールルールの追加ページが開きます。

Cisco Secure Accessには、電子メールDLPルールを作成する方法が2つあります。

- 定義済みのDLPテンプレートを使用して電子メールDLPルールを作成します
- カスタムDLPテンプレートを使用した電子メールDLPルールの作成

図 1.電子メールDLPルールの作成に移動



オプション1：事前定義されたDLPテンプレートを使用した電子メールDLPルールの作成

ステップ3：基本ルール情報の設定

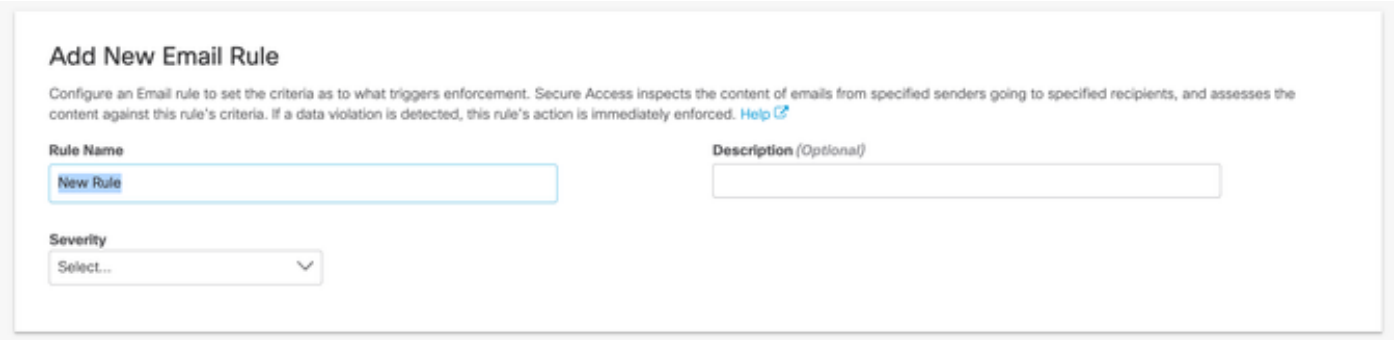
ADD RULE > Email DLP Ruleウィンドウに移動し、

Add New Email Ruleウィンドウで、次の詳細情報を入力します。

- ルール名
  電子メールDLPルールの内容を表す名前を入力します。
- 説明
  ルールの目的の簡単な要約を提供します。
- 重大度
  ポリシーに適切な重大度レベルを選択します。

- 低い
- 中間
- 高
- Critical

これらのフィールドは、管理、レポート、および運用の可視性に関するルールを分類するのに役立ちます。



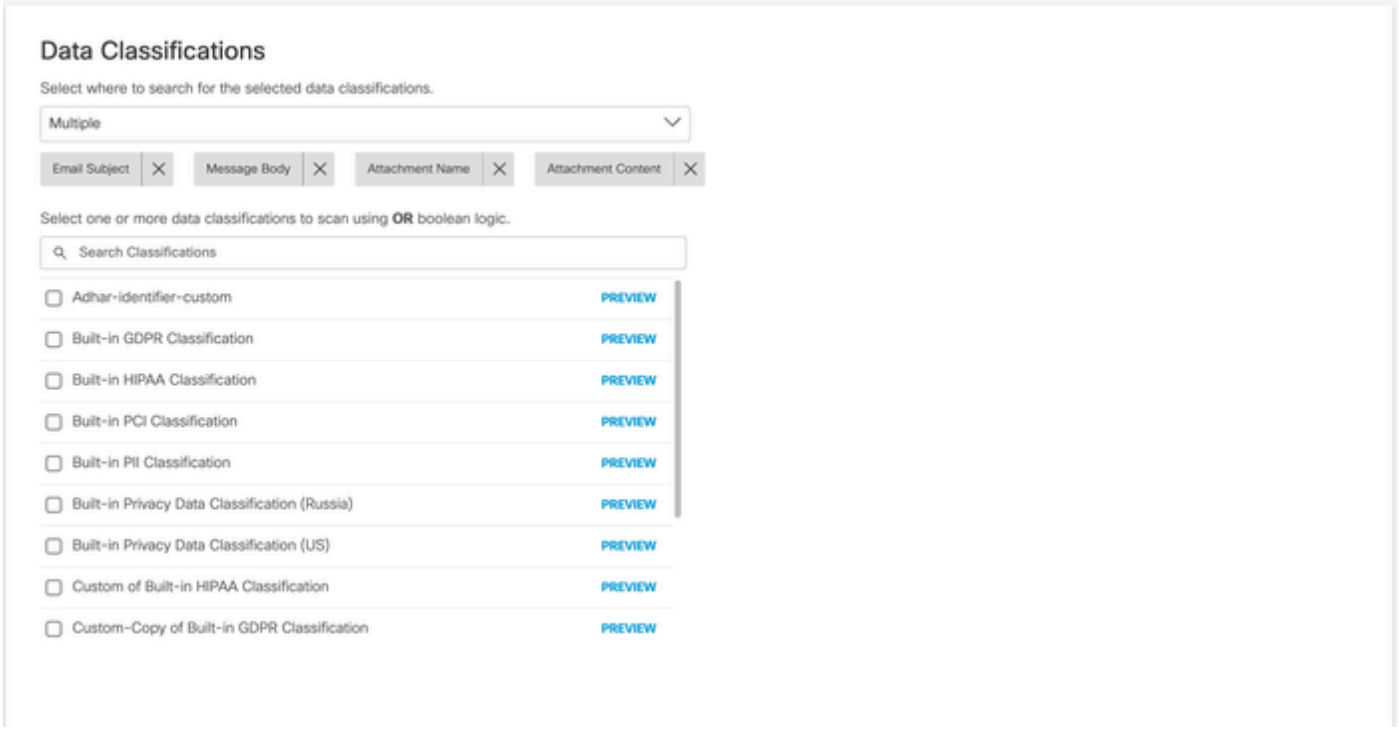
手順4：データ分類の選択

Data Classificationsの下で、DLP違反の可能性がある電子メールコンテンツを検査するために使用される、事前定義されたDLPテンプレートを選択します。

次に、選択した分類を一致させる場所を選択します。サポートされる検査場所は次のとおりです。

- 電子メールの件名
- メッセージ本文
- 添付ファイル名
- 添付ファイルの内容

これにより、ポリシーは機密情報のメッセージの内容と添付ファイルの両方を検査できます。



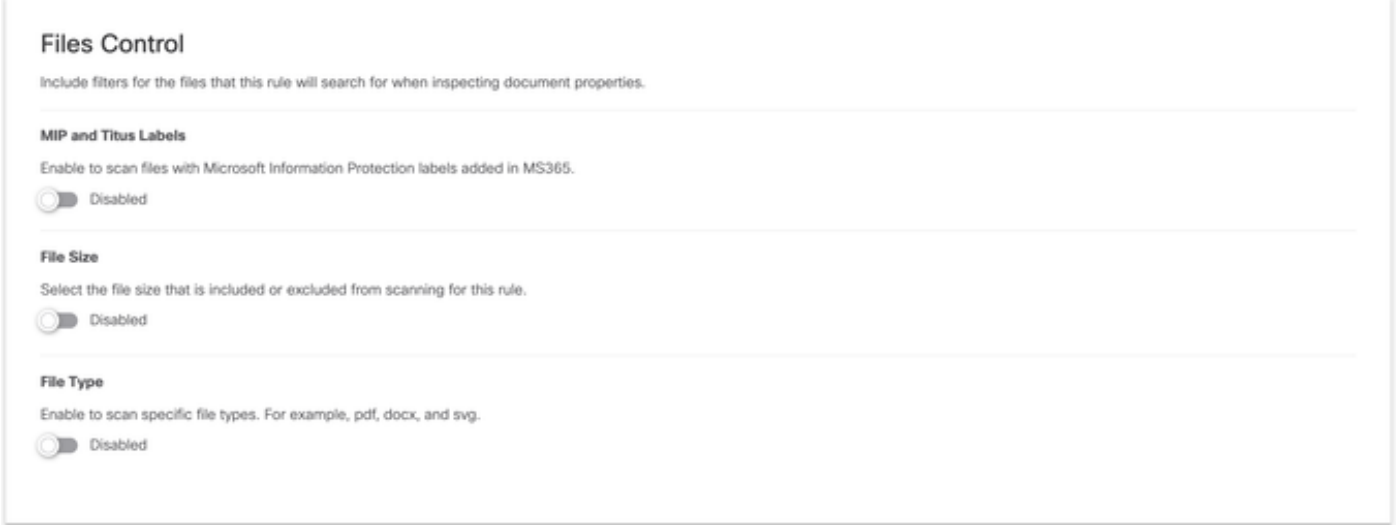
ステップ5：ファイルコントロールの設定

Files Controlの下で、ルールのファイルベースの検査基準を設定します。

これには、次のサポートが含まれます。

- MIPラベル
- Titusラベル

これらの設定は、DLPの強制で、添付ファイルに関連付けられたセンシティビティ・ラベルまたはメタデータを考慮する必要がある場合に便利です。



ステップ6：送信者スコープの定義

Sendersセクションで、ポリシーを適用する送信者を指定します。

使用可能なオプションは次のとおりです。

- すべての送信者
- 特定の送信者
- 特定の送信者を除外する

これにより、規則を広く適用したり、選択したユーザーまたはグループに制限したりできます。

手順7：受信者の範囲を定義する

Recipientsセクションで、ポリシー評価に含める、または除外するユーザまたはグループを選択します。

使用可能なオプションは次のとおりです。

- すべてのユーザーを含める
- 特定のユーザーを含める
- 特定のユーザーを除外する

これにより、目的の受信者に基づいてポリシーを適用できます。

ステップ8：ポリシーアクションの選択

アクションセクションで、DLPルールに違反していると明確に識別される電子メールをCisco Secure Accessが処理する方法を選択します。

使用可能なアクションは次のとおりです。

- モニタ
  電子メールが許可され、イベントがログに記録されて表示とレポートが行われます。
- Block
  電子メールは、機密データの送信を防ぐためにドロップされます。

注：現時点では、肯定的に識別される電子メールは、Monitorアクションで許可するか、またはBlockアクションでドロップすることができます。

重要：電子メールのDLPアクションはCisco Secure Accessでのみ設定されます。Eメールがセキュアアクセスによってブロックされている場合、そのイベントはCisco ETDメッセージトラッキングにも表示されます。

ステップ9：ユーザ通知の設定

通知オプションは、受信者だけが使用できます。

User Notificationsで、電子メールがDLPポリシーに一致したときにユーザに通知するかどうかを設定します。
「アクターのマネージャ」または「カスタム受信者」に通知するオプションがあります。「カスタム受信者」は誰でもかまいません。

必要に応じて、電子メールメッセージテンプレートをデフォルトからカスタム通知に設定します。

通知を有効にすると、ユーザの認知度が向上し、繰り返し発生するポリシー違反を減らすことができます。この設定は、組織の運用およびコンプライアンス要件に従って構成します。

ステップ9：ユーザ通知の設定

ユーザ通知は、セキュリティ認識を高め、コンプライアンスを確保するための強力なツールです。電子メールによってDLPポリシーがトリガーされたときにユーザまたは管理者に警告することで、違反に関するフィードバックとコンテキストを即座に提供できます。

注：通知設定は、主に電子メールの受信者と指定された関係者を対象としています。

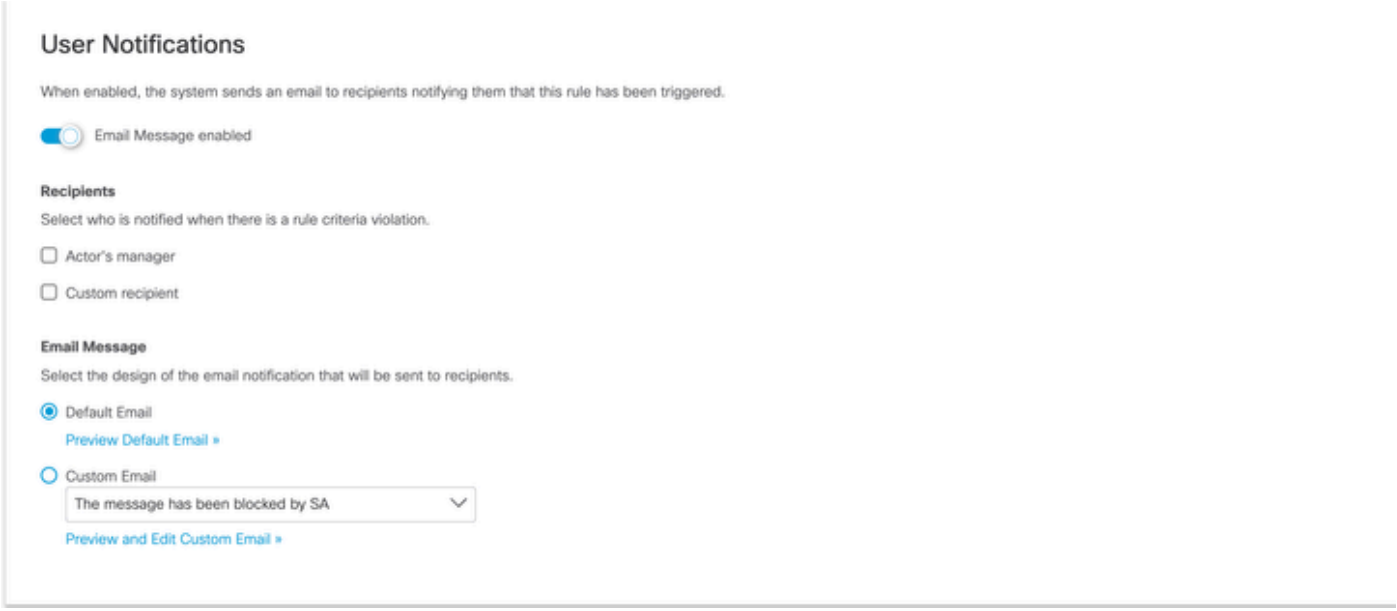
通知を構成するには、次の手順に従います。

1. 通知の受信者を定義する: User Notificationssectionで、アラートを受信するユーザを指定します。次の2つの主要なオプションがあります。
    - アクターのマネージャ：ポリシー違反をトリガーしたユーザのマネージャに通知を直接送信します。
    - カスタム受信者：任意の電子メールアドレス（セキュリティオペレーションセンターや特定の部門の責任者など）を指定できます。
2. メッセージテンプレートの選択:DefaultnotificationテンプレートまたはCustomnotificationのいずれかを選択できます。
    - 推奨事項：組織に特定のコンプライアンスメッセージングまたは内部ブランディング要件がある場合は、CustomerOptionを使用して電子メールの本文をカスタマイズし、

受信者に明確で実用的な指示を提供します。

3. 確認と保存：設定が完了したら、設定が組織の運用ポリシーとコンプライアンスポリシーに合っていることを確認します。

ベストプラクティス：これらの通知を有効にすると、機密データの処理手順に関する情報をリアルタイムでユーザに提供できるため、繰り返し発生するポリシー違反を効果的に減らすことができます。



注：通知オプションは、テナント設定とポリシー設定によって異なる場合があります。

ステップ10：ルールを確認して保存する

ルールの設定が完了したら、次の手順を実行します。

1. すべての設定を確認します。
2. 選択したデータ分類、検査範囲、送信者と受信者の条件、およびアクションが、目的のポリシー動作と一致していることを確認します。
3. [保存]をクリックして、電子メールDLPルールを作成します。

電子メールDLPポリシーがCisco Secure Accessでアクティブになります。

オプション2：カスタムDLPテンプレートを使用した電子メールDLPルールの作成

カスタムDLPテンプレートの作成には、カスタム識別子の定義とデータ分類の設定の2つの主要なフェーズがあります。

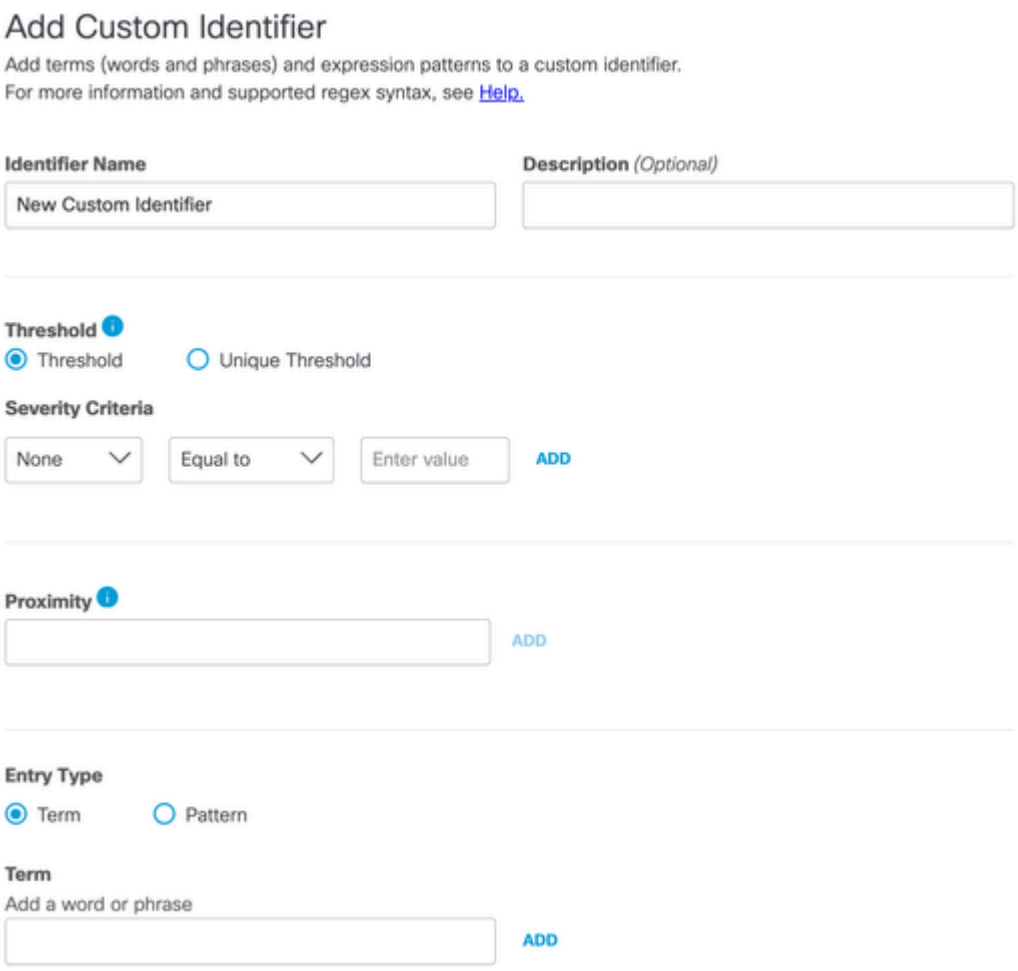
注：データ分類エンジンは柔軟性が高く、1つのカスタム識別子、またはAND/ORブール演算子でリンクされたカスタム識別子と事前定義された識別子の組み合わせを使用してポリシーを構築できます。

ステップ11：カスタムIDの作成

検出用の新しいデータパターンを定義するには、次の手順を実行します。

1. Secure Accessdashboardにログインします。
2. Secure > Data Classificationの順に移動します。
3. [カスタム識別子の追加]をクリックします。
4. Add Custom Identifierwindowで次のパラメータを設定します。

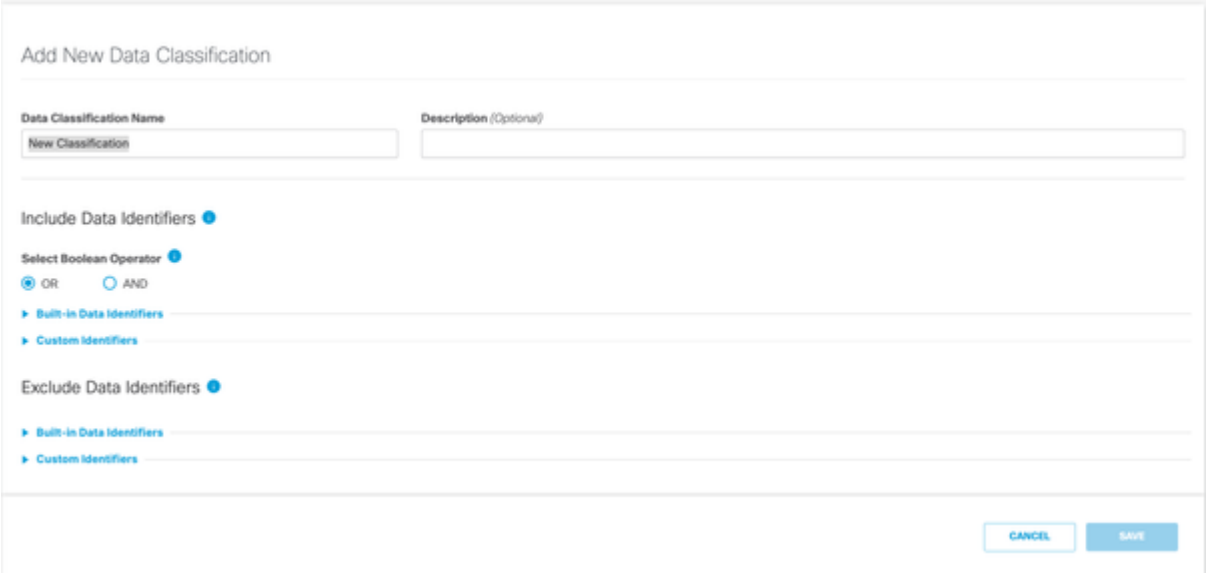
- 名前と説明：検出するデータ型の一意の名前と簡単な説明を指定します。
- Threshold：
  - Threshold：検出されたデータの合計頻度を監視します。
  - 固有しきい値:重複を無視して、一意の発生の数のみを監視します。
- 重大度の基準:検出の頻度に基づいて重大度レベル(非常に低い、低い、中、高い)を割り当てます。これらは、等しい、より大きい、より小さい、または範囲などの比較演算子を使用して定義できます。
- Proximity：近接スレッショルドを設定します。これは、この識別子で個別の用語ごとではなく、まとめて定義されるすべての用語およびパターンに適用されます。
- エントリ・タイプ：システムによるデータの識別方法を定義します。
  - 用語：特定の単語または語句。
  - パターン：特定のデータ形式（クレジットカード番号や内部プロジェクトコードなど）を検出するために使用される正規表現。



ステップ12：データ分類の設定

カスタム識別子を保存すると、データ分類オブジェクトに統合できます。

1. Secure > Data Classification > Addの順に移動します（右上隅のボタンを使用）。
2. 使用可能なリストから、新しく作成したカスタムIDを選択します。
3. （オプション）AND/ORロジックを使用してカスタムIDと定義済みIDを組み合わせて、検出範囲を絞り込みます。
4. 電子メールDLPポリシーで使用できるように設定を保存します。
5. 詳細については、以下のスクリーンショットを参照してください。
6. ステップ4 ～ 10と同じ手順を実行し、カスタムデータ分類を使用してポリシーを作成します。



この設定により、お客様の組織は、内部データ構造とコンプライアンス要件に合わせて調整された機密情報を検出できます。

トラブルシュート

電子メールDLPルールが期待どおりに動作しない場合は、次の点を確認してください。

ルールが電子メールと一致しません

- correctdata classification テンプレートが選択されていることを確認します。
- 関連するインスペクションの場所が有効になっていることを確認します。
  - 電子メールの件名
  - メッセージ本文
  - 添付ファイル名
  - 添付ファイルの内容
- 送信者フィルタと受信者フィルタによって、テスト電子メールが意図せずに除外されないようにします。

電子メールはブロックされません

- ルールアクションがBlockand notMonitorに設定されていることを確認します。
- ルールが保存され、有効になっていることを確認します。
- 電子メールの内容が、設定されているDLP基準に正しく一致していることを確認します。

DLPイベントはETDには表示されません

- Cisco ETDとCisco Secure Accessが正しく統合されていることを確認します。
- ETDが関連する電子メールトラフィックをアクティブに処理していることを確認します。
- Cisco Secure Accessにポリシーイベントが最初に存在するかどうかを確認します。

添付ファイルに基づく一致は検出されません

- 検査スコープ内で添付ファイルの名前と添付ファイルの内容のいずれかまたは両方が選択されていることを確認します。
- MIPorTitusareなどのラベルがルールロジックの一部である場合は、ファイル制御設定を確認します。

ベスト プラクティス

EメールDLPポリシーを導入する際は、次のベストプラクティスを考慮してください。

- enforcingBlockの前にポリシーの動作を検証するには、Monitormodeで開始します。
- わかりやすいルール名を使用すると、管理が容易になります。
- 意図しない一致を減らすために、送信者と受信者の条件の範囲を注意深く設定します。
- 広範な導入の前に、代表的なデータを使用してテストします。
- ETDメッセージトラッキングを定期的にレビューして、ブロックまたはモニタ対象の電子メールアクティビティを検証します。
- ビジネス固有のデータ識別子が必要な場合は、カスタムテンプレートを使用します。

要約

Cisco Secure Accessは、Cisco Secure AccessとCisco Email Threat Defenseの統合型導入において、電子メールDLPポリシーを設定するための中央プラットフォームです。ETDは可視性とメッセージトラッキングを提供しますが、すべてのDLPルールの作成、分類の選択、適用アクション、および通知はセキュアアクセスで設定されます。

管理者は、事前定義またはカスタムのDLPテンプレートを使用して、電子メールのコンテンツと添付ファイルを検査し、送信者と受信者の範囲を定義して、モニタアクションまたはブロックアクションを適用することで、電子メールによる機密データの損失を防止できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。