管理

[管理（Administration）]ページでは、アカウントの状態と、アカウントに関連付けられているクラウド サービス プロバイダーの全体的なステータスを確認できます。

管理

[管理（Administration）]ページでは、アカウントの状態と、アカウントに関連付けられているクラウド サービス プロバイダーの全体的なステータスを確認できます。

API キー

このページを表示するには、**[管理（Administration）]** > **[管理（Management）]** > **[APIキー（API Keys）]**に移動します。

検索

検索バーで、キーワードを使用して API キーのリストを検索またはフィルタ処理します。検索が機能するには、少なくとも 3 つの文字を指定する必要があります。

API キーテーブルとアクション

この表は、クラウド サービス プロバイダー向けに Multicloud Defense コンポーネントが作成するすべての API キーを示します。ロール、キー ID 、キーが Multicloud Defense に追加された日付、およびキーの有効期限が表示されます。

ここから API キーを作成または削除できます。これらのキーは Multicloud Defense によって生成されるもので、クラウド サービス プロバイダーが通信を維持するために作成する可能性のあるキーとは関係ないことに注意してください。詳細については、このまま読み進めてください。

Multicloud Defense での API キーの作成

API キーを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [APIキー（API Keys）]**に移動します。

ステップ 2 [API キーの作成（Create API Key）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 Multicloud Defense によって自動生成される [電子メールアドレス（Email Address）] を確認します。このオプションは変更できません。

ステップ 5 ドロップダウンメニューを使用して、次の主要なロールのいずれかを選択します。

- **admin_read_only**：このロールではやり取りが制限されるため、変更やアクションは行えません。使用可能なデータの「表示」のみが可能です。
- **admin_read_rw**：このロールでは、使用可能なデータの読み取りと変更が可能です。

ステップ 6 [APIキーのライフタイム（日数）（API Key Lifetime (days)）] に適切な値を入力します。デフォルト値は 365 日です。

ステップ 7 [保存（Save）] をクリックします。

Multicloud Defense からの API キーの削除

API キーを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [APIキー（API Keys）]**に移動します。

ステップ 2 テーブルから API キーを選択し、チェックボックスをオンにして強調表示します。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 [はい（Yes）] をクリックして、キーを削除することを確認します。キーは Multicloud Defense から直ちに削除されます。

アカウントレベル設定

このページには、アプリケーションタグやカスタムタグなど、Multicloud Defense で使用されるタグの一部が表示されます。詳細については、このまま読み進めてください。

アプリケーションタグ

アプリケーションタグは文字列であり、プロセスまたはスレッドを自動分類するための分類基準の1つとして使用されます。タグ付けを使用すると、独自の要件に基づいてアプリケーションをグループ化して、アプリケーションを検索して脆弱性を見つけることができます。すべてのクラウド サービス プロバイダーがアプリケーションタグの使用をサポートしているわけではないことに注意してください。

（注） 一度に作成できるアプリケーションタグは1つだけです。新しいタグを作成する**必要がある**場合は、既存のタグを削除してから、新しいアプリケーションタグを作成する必要があります。

アプリケーションタグの作成

アプリケーションタグを作成するには、次の手順を実行します。これらのタグは内部使用専用であり、クラウド サービス プロバイダーのインターフェイスからは認識または使用できない場合があることに注意してください。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [アカウント（Account）]**に移動します。

ステップ 2 [アプリケーションタグ（Application Tag）] テーブルで、[作成（Create）] をクリックします。

ステップ 3 アプリケーションタグのタイプは、デフォルトで `APPLICATION_TAG_KEYS` です。

ステップ 4 [説明（Description）] にタグの簡単な説明を入力します。これは、同様の名前または概念を持つ可能性のある他のタグを識別または区別するのに役立ちます。

ステップ 5 少なくとも 1 つの [値（Value）] を入力します。複数の値を作成するには、各値の後に `Enter` を押します。これらの値では大文字と小文字が区別されます。

ステップ 6 [保存（Save）] をクリックします。タグが作成され、テーブルで使用できるようになります。

アプリケーションタグの編集

Multicloud Defense で作成された既存のアプリケーションタグを編集するには、次の手順を実行します。この手順は、クラウド サービス プロバイダーのインターフェイスで作成されたタグを編集するために使用することはできません。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [アカウント（Account）]**に移動します。

ステップ 2 [アプリケーションタグ（Application Tag）] テーブルで、編集するアプリケーションタグを探し、左側のチェックボックスをオンにして強調表示します。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 次のパラメータを変更します。

- [説明（Description）]：説明を編集または削除できます。
- [タグ値（Tag Values）]：ここでタグを追加または削除できます。

ステップ 5 [保存（Save）] をクリックします。または、変更を保存せずにいつでもキャンセルできます。

アプリケーションタグの削除

既存のアプリケーションタグを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[アカウント（Account）]**に移動します。

ステップ 2 [アプリケーションタグ（Application Tag）] テーブルで、編集するアプリケーションタグを探し、左側のチェックボックスをオンにして強調表示します。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 [はい（Yes）] をクリックして、このアプリケーションタグを削除することを確認します。

カスタムタグ

カスタムタグは、ある項目に関する詳細情報を示す単純なデータであり、同じタグを持つ関連項目を簡単に見つけることができます。タグを使用すると、オブジェクト、ポリシー、ルールなどを簡単に特定または区別できます。

カスタムタグの作成

Multicloud Defense でカスタムタグを作成するには、次の手順を実行します。これらのタグは内部使用専用であり、クラウド サービス プロバイダーのインターフェイスからは認識または使用できない場合があることに注意してください。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[アカウント（Account）]**に移動します。

ステップ 2 [カスタムタグ（Custom Tag）] テーブルで、[作成（Create）] をクリックします。

ステップ 3 タグの[値（Value）]を入力します。これは、同様の名前または概念を持つ可能性のある他のタグを識別または区別するのに役立ちます。

ステップ 4 少なくとも 1 つの [値（Value）] を入力します。

ステップ 5 [保存（Save）] をクリックします。タグが作成され、テーブルで使用できるようになります。

カスタムタグの編集

既存のカスタムタグを変更するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [アカウント（Account）]**に移動します。

ステップ 2 [カスタムタグ（Custom Tag）] テーブルで、編集するアプリケーションタグを探し、左側のチェックボックスをオンにして強調表示します。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 次のパラメータを変更します。

- キー（Key）
- 値（Values）

ステップ 5 [保存（Save）] をクリックします。または、変更を保存せずにいつでもキャンセルできます。

カスタムタグの削除

既存のカスタムタグを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [アカウント（Account）]**に移動します。

ステップ 2 [カスタムタグ（Custom Tag）] テーブルで、編集するアプリケーションタグを探し、左側のチェックボックスをオンにして強調表示します。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 [はい（Yes）] をクリックして、このアプリケーションタグを削除することを確認します。

System

[システム（System）] ページは、少なくとも 1 年分の更新をカタログ化する履歴ドキュメントです。これらの詳細情報は、一般的な知識、適切なリリースノートのバージョンの検索、および製品のヘルプのためにシスコサポートに連絡する際に使用できます。ここには、次の情報が表示されます。

コンポーネント

このセクションには、Multicloud Defense Controller とユーザーインターフェイス両方の最新バージョンが表示されます。このページから以前のバージョンへの更新またはロールバックを強制することはできません。

ゲートウェイイメージ

ゲートウェイイメージのテーブルには、Multicloud Defense Gateway がアップグレードされたタイミング、ゲートウェイのバージョンとその期間、ゲートウェイが確立されているタイムゾーンが示されます。

Talos/ネットワーク侵入

このテーブルには、Cisco Talos インテリジェンスグループ からのすべての更新が表示されます。これらの更新は、通常の製品ソフトウェアリリースとは別にシスコ製品にプッシュされます。

Web の保護

このテーブルには、最新の Web アプリケーションの脆弱性と脅威に対するすべての Web アプリケーション ファイアウォール（WAF）コアおよび Trustwave ルールの更新が表示されます。

計測

[計測（Metering）] ページには、Multicloud Defense の全体的な使用状況と、クラウド サービス プロバイダー用に作成されたゲートウェイインスタンスの両方について、使用状況のグラフが表示されます。

フィルタ

ページの上部にあるフィルタを活用して、ページに表示されるデータを決定できます。このビューを変更するには、月と年を選択します。これらのフィルタ設定を使用して、使用状況レポートを生成できます。

使用状況レポートの生成

このページから、2 つのオプションのいずれかの使用状況レポートを生成できます。**[管理（Administration）] > [管理（Management）] > [計測（Metering）]**に移動し、ページの [フィルタ（Filter）] セクションの [ダウンロード（Download）] ドロップダウンオプションを展開して、使用状況またはインスタンスを選択します。ファイルは .csv ファイルとしてローカルにダウンロードされます。フィルタリングオプションを使用して、レポートを生成する期間を決定します。

使用状況レコード

[使用状況レコード（Usage Records）] テーブルには、テナントに関連付けられているアカウントの数、アカウントが対話に費やした時間数、および [フィルタ（Filter）] セクションで選択

した日付が表示されます。使用状況/月の比率から、最もアクティブであった日を判断できます。

インスタンスレコード

[インスタンスレコード（Instance Records）] テーブルには、次のインスタンス統計情報が表示されます。

- アカウント名。
- クラウド サービス プロバイダーごとのアカウントタイプ。
- インスタンス ID です。
- インスタンスタイプ。
- 可用性ゾーン。
- ゲートウェイ。
- [開始（Started）]：ゲートウェイインスタンスが作成された日時。
- [終了（Ended）]：ゲートウェイインスタンスが期限切れまたは終了した日時。

アラートプロファイル

[管理（Administration）] > **[アラートプロファイル（Alert Profiles）]**に移動して、次の管理ビューにアクセスします。

[サービス（Services）] ページと [アラート（Alerts）] ページはどちらも Multicloud Defense からのアラートに焦点を当てています。[アラート（Alerts）] ページはアラートの送信先に焦点を当て、[アラート（Alerts）] ページは設定されたエンドポイントに送信されるアラートの詳細を示します。理想的な設定を行うには、両方のページでエントリの設定に十分な時間を割き、ダッシュボード内でアラートの機会をうまく全体的に最適化してください。

サービス

このページを表示するには、**[管理（Administration）]** > **[管理（Management）]** > **[サービス（Service）]**に移動します。

サービスは、アラートの**送信先**に焦点を当てます。このページのオプションを正常に設定するには、サードパーティ製アプリケーションから条件を指定する必要があることに注意してください。

検索

検索バーで、キーワードを使用してサービスのリストを検索またはフィルタ処理します。検索が機能するには、少なくとも 3 つの文字を指定する必要があります。

サービステーブルとアクション

この表は、クラウド サービス プロバイダー向けに Multicloud Defense コンポーネントが作成するすべてのサービスを示します。名前、サービスのタイプ、サービスが更新された日付を確認できます。

ここから サービスを作成または削除できます。これらのサービスは Multicloud Defense によって生成されるもので、クラウド サービス プロバイダーが提供する可能性のあるサービスとは関係ないことに注意してください。

サービスの作成

サービスを作成するには、以下の手順を実行します。

始める前に

サードパーティのメッセージングアプリケーションで、サービスの通知または統合を有効にする、または許可する必要があります。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、同様の名前を持つ他のサービスを区別するのに役立ちます。

ステップ 5 ドロップダウンメニューを使用して、サービスの [タイプ（Type）] を選択します。

- Pager Duty。
- ServiceNow。
- Slack。
- Datadog。
- Microsoft Sentinel。
- Microsoft Teams。
- Webex。
- Splunk。

ステップ 6 プロンプトが表示されたら、サービスタイプに応じて次のエントリを入力します。

- API キー（API Key）。
- API URL。

- Azure ログテーブル名（Azure Log Table Name）。
- Azure ログ分析ワークスペース ID（Azure Log Analytics Workspace ID）。
- （Splunk の場合はオプション）インデックス（Index）。

ステップ 7 [保存（Save）] をクリックします。

サービスの編集

既存のサービスを編集するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [サービス（Services）]**に移動します。
ステップ 2 テーブル内でサービスを探して選択し、強調表示します。
ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[編集（Edit）] をクリックします。
ステップ 4 サービスの次の項目を変更します。

- 名前
- [説明（Description）]
- タイプ
- タイプ固有の設定条件。

ステップ 5 [保存（Save）] をクリックして、変更を確定します。任意の時点で [キャンセル（Cancel）] をクリックすると、ウィンドウを閉じて変更をキャンセルできます。

次のタスク

変更を表示するには、ページを**更新**する必要がある場合があります。

サービスのクローン

既存のサービスのクローンを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [サービス（Services）]**に移動します。
ステップ 2 テーブル内でサービスを探して選択し、強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[クローン（Clone）] をクリックします。

ステップ 4 サービスのクローンが生成されます。デフォルトでは、サービスの**タイプ**とサービス固有の設定基準のみが保持されます。

ステップ 5 [名前（Name）] に一意の名前を入力します。

ステップ 6 （任意）説明を入力します。

ステップ 7 [保存（Save）] をクリックして、変更を確定します。任意の時点で [キャンセル（Cancel）] をクリックすると、ウィンドウを閉じて変更をキャンセルできます。

次のタスク

テーブルへの変更または追加内容を表示するには、ページを**更新**する必要がある場合があります。

サービスのエクスポート

既存のサービスをエクスポートするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [サービス（Services）]**に移動します。

ステップ 2 テーブル内でサービスを探して選択し、強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[エクスポート（Export）] をクリックします。

ステップ 4 Multicloud Defense でエクスポートウィザードが生成されます。

ステップ 5 [ダウンロード（Download）] をクリックして Terraform をローカルにダウンロードするか、[コードのコピー（Copy Code）] をクリックして JSON リソースをコピーし、Terraform スクリプトに手動で貼り付けます。

ステップ 6 Terraform プロンプト内で、ウィンドウの下半分に表示されるコマンドを実行します：`terraform import "ciscomcd_alert_profile". "servicename" <number in table>`。

ステップ 7 Terraform 内のプロンプトに従って、タスクを完了します。ダッシュボードではこれ以上の手順はありません。

サービスの削除

既存のサービスを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [管理（Management）] > [サービス（Services）]**に移動します。

ステップ 2 テーブル内でサービスを探して選択し、強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[削除（Delete）] をクリックします。

ステップ 4 [はい（Yes）] をクリックして、サービスを削除することを確認します。

ステップ 5 サービスが Multicloud Defense から削除されます。

アラート

[アラート（Alerts）] ページは、サードパーティのエンドポイントに送信される**アラート**に焦点を当てています。アラートとサービスの両方を設定して、アラートの機会を利用することを強くお勧めします。

アラートの作成

アラートを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つ他のサービスを区別するのに役立ちます。

ステップ 5 [アラートプロファイル（Alert Profile）] を選択します。現時点で使用可能な唯一のオプションは、`Pagerduty` です。

ステップ 6 ドロップダウンメニューを使用して、アラートの [タイプ（Type）] を選択します。

- システムログ（System Logs）。
- 監査ログ（Audit Logs）。
- 検出（Discovery）。

ステップ 7 （任意）ドロップダウンメニューを使用して、[サブタイプ（Sub Type）] を選択します。以下のオプションは、手順 6 で選択した [タイプ（Type）] に応じて変更されたり、使用できない場合があることに注意してください。

- ゲートウェイ（Gateway）。
- アカウント（アカウント）。
- コントローラ（Controller）。
- インサイトルール（Insights Rule）。

ステップ 8 ドロップダウンメニューを使用して、[重大度（Severity）] のレベルを選択します。

- 情報（Info）。
- 警告。
- [Medium（中）]：
- High.
- クリティカル。

ステップ 9 [有効（Enabled）] チェックボックスはデフォルトでオンになります。このオプションは、アラートプロファイルがアクティブで使用可能かどうかを指定します。無効になっている場合、アラートの発行時に Multicloud Defense はそのアラートプロファイルを含めません。

次のタスク

サービスして、これらのアラートの送信先を指定します。

アラートの編集

既存のアラートを編集するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[アラート（Alert）]**に移動します。
ステップ 2 テーブル内でアラートを探して選択し、強調表示します。
ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[編集（Edit）] をクリックします。
ステップ 4 アラートプロファイルのフィールドと選択を編集します。選択内容に応じて、使用可能なフィールドの一部が変わる場合があることに注意してください。
ステップ 5 [保存（Save）] をクリックして、変更を確定します。任意の時点で [キャンセル（Cancel）] をクリックすると、変更をキャンセルして編集ウィンドウを閉じることができます。

アラートの複製

既存のアラートを複製するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[アラート（Alert）]**に移動します。
ステップ 2 テーブル内でアラートを探して選択し、強調表示します。
ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[編集（Edit）] をクリックします。

ステップ 4 アラートのクローンが生成されます。デフォルトでは、**アラートプロファイル**と**タイプ**のみが保持されます。

ステップ 5 アラートの残りのフィールドと選択内容を編集します。選択内容に応じて、使用可能なフィールドの一部が変わる場合があることに注意してください。

ステップ 6 [保存（Save）] をクリックして、変更を確定します。任意の時点で [キャンセル（Cancel）] をクリックすると、変更をキャンセルして編集ウィンドウを閉じることができます。

アラートのエクスポート

既存のアラートをエクスポートするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[アラート（Alert）]**に移動します。

ステップ 2 テーブル内でアラートを探して選択し、強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[エクスポート（Export）] をクリックします。

ステップ 4 Multicloud Defense でエクスポートウィザードが生成されます。

ステップ 5 [ダウンロード（Download）] をクリックして Terraform をローカルにダウンロードするか、[コードのコピー（Copy Code）] をクリックして JSON リソースをコピーします。

ステップ 6 Terraform スクリプトに手動で貼り付けます。

ステップ 7 Terraform プロンプト内で、ウィンドウの下半分に表示されるコマンドを実行します：`terraform import "ciscomcd_alert_rule"."alertname" <number in table>`。

ステップ 8 Terraform プロンプト内のプロンプトに従って、タスクを完了します。[閉じる（Close）] をクリックして Multicloud Defense のエクスポートウィンドウを閉じます。ダッシュボードではこれ以上の手順はありません。

アラートの削除

既存のアラートを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[管理（Management）]** > **[アラート（Alert）]**に移動します。

ステップ 2 テーブル内でアラートを探して選択し、強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューを展開し、[削除（Delete）] をクリックします。

ステップ 4 [はい（Yes）] をクリックして、サービスを削除することを確認します。

ステップ 5 アラートが Multicloud Defense から削除されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。