Cisco Secure Email Threat Defense に関するよくある質問

初版: 2021 年 4 月 26 日

最終更新日: 2024-09-24

目次

はじめに

このドキュメントには、Cisco Secure Email Threat Defense に関するよくある質問（FAQ）が含まれています。Cisco Secure Email Threat Defense の使用方法の詳細については、『Cisco Secure Email Threat Defense User Guide』[英語] を参照してください。

セットアップ

Cisco Secure Email Threat Defense 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。

シスコは、ユーザーの Microsoft 365 ログイン情報を物理的に受け取ることも、グローバル管理者のログイン情報をキャッシュまたは保存することもありません。Cisco Secure Email Threat Defense は、ユーザーを Microsoft の Azure アプリケーション登録プロセスにリダイレクトして、ここで Microsoft の API の認証トークンを発行できるようにします。このトークンを認証できるのはグローバル管理者のみです。

詳細については、アプリケーションの管理者権限の説明についての次の Microsoft のドキュメントを参照してください。
https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/grant-admin-consent/

Secure Email Threat Defense が Microsoft に要求するのはどのようなアクセス許可ですか？

Microsoft 365 認証モードでは、Cisco Secure Email Threat Defense から Microsoft によるアクセス許可を要求します。これらの許可は、読み取り/書き込みモードと読み取りモードのどちらを選択したかによって異なります。アクセス許可の詳細については、リンクされている Microsoft のドキュメントを参照してください。

両方の Microsoft 認証モードからの要求：**Organization.Read.All** および **User.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#organizationreadall
- https://learn.microsoft.com/en-us/graph/permissions-reference#userread

読み取り/書き込みモードからの要求：**Mail.ReadWrite**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailreadwrite

読み取りモードからの要求：**Mail.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailread

Malware Analytics/Threat Grid からウェルカムメールを受信したのはなぜですか。

Cisco Secure Email Threat Defense アカウント作成プロセスの一環として、最小限の Cisco Secure Malware Analytics（旧 Threat Grid）アカウントが作成されます。新しい Malware Analytics アカウントは、既存の Malware Analytics アカウントにリンクされていません。Cisco Secure Email Threat Defense を設定するために Malware Analytics アカウントでアクションを実行する必要はありません。

ジャーナルアドレスを確認するにはどうすればよいですか。

ジャーナルアドレスは、Cisco Secure Email Threat Defense の設定ページに表示されます。初期設定後にジャーナルアドレスを見つける必要がある場合は、[アカウントAccount)] セクションの [管理（Administration）] > [ビジネス（Business）] ページで見つけられます。

Microsoft 365 テナントを登録しようとすると、登録エラーが表示されるのはなぜですか。

以前別の Cisco Secure Email Threat Defense アカウントに登録されていたテナントを登録しようとすると、認証は失敗します。Cisco Secure Email Threat Defense では、同じ Microsoft テナント ID を持つ複数のアカウントは許可されません。

シスコはジャーナルデータをどのくらいの期間保持しますか。

データは Cisco Secure Email Threat Defense プライバシーデータシートに従って保持されます。

ユーザーを複数の Cisco Secure Email Threat Defense インスタンスに追加できますか。

ユーザーは同じ Cisco Security Cloud Sign On アカウントを使用して、複数の Cisco Secure Email Threat Defense インスタンスにアクセスできます。これにより、ログアウトして別のアカウントで再度ログインすることなく、各インスタンスを簡単に追跡できます。

[管理(Administration)] > [ユーザー(Users)] ページから新しいユーザーを作成して、他のインスタンスにユーザーを追加します。Cisco Secure Email Threat Defense 同じ Cisco Security Cloud Sign On を使用している Cisco Secure Email Threat Defense アカウントは、[ユーザー(User)] メニューから利用できますが、アクセスは同じ地域の Cisco Secure Email Threat Defense アカウントに限定されることに注意してください。

ログインの問題

Cisco Secure Email Threat Defense へのログインに関する問題の詳細情報を確認するにはどうすればよいですか。

Cisco Secure Email Threat Defense Cisco Secure Email Threat Defense では、ユーザー認証管理に Cisco Security Cloud Sign On が使用されます。FAQ を含む Cisco Security Cloud Sign On の詳細については、『Cisco Security Cloud Sign On クイックスタートガイド』を参照してください。

自分の電子メールアドレスでログインできないのはなぜですか。

Cisco Security Cloud Sign On に使用する電子メールアドレスが、Cisco Secure Email Threat Defense アカウントに関連付けられている電子メールと一致することを確認してください。お客様によっては、複数の電子メールアドレスを使用する Cisco Security Cloud Sign On アカウントをお持ちの場合もあります。Cisco Secure Email Threat Defense は、単一ユーザーの複数の電子メールアドレスをサポートしていません。Cisco Secure Email Threat Defense アカウントの作成に使用した電子メールアドレスを使用してログインする必要があります。使用された電子メールアドレスがわからない場合は、Cisco Secure Email Threat Defense 管理者に確認してください。

パスワードをリセットするにはどうすればよいですか。

Cisco Security Cloud Sign On のログインプロセス中にパスワードの入力を求められるので、[パスワードを忘れた場合（Forgot password）] をクリックして、[パスワードのリセット（Reset Password）] ページに移動します。

Microsoft アカウントで Cisco Security Cloud Sign On にサインインしようとすると、400 Bad Request エラーが表示されるのはなぜですか。

Microsoft 365 では、アカウントに名前と姓を定義する必要はありません。姓が含まれていない Microsoft アカウントで認証しようとすると、Cisco Security Cloud Sign On から次のエラーが表示されます。

400 Bad Request. Unable to create the user. Required properties are missing.

この問題に対処するには、Microsoft 365 アカウントに姓と名の両方が定義されていることを確認します。

SecureX アプリケーションポータルから Cisco Secure Email Threat Defense にアクセスするにはどうすればよいですか。

SecureX アプリケーションポータルから Cisco Secure Email Threat Defense にアクセスするには、お住まいの地域（北米、欧州、APJC（アジア太平洋地域））を探して Cisco Secure Email Threat Defense アイコンを見つけます。

Cisco Secure Email Threat Defense インスタンスを切り替えるにはどうすればよいですか。

同じ Security Cloud Sign On アカウントを使用して、複数の Cisco Secure Email Threat Defense インスタンスにアクセスできます。これにより、ログアウトして別のアカウントで再度ログインすることなく、各インスタンスを簡単に追跡できます。Cisco Secure Email Threat Defense 同じ Cisco Security Cloud Sign On アカウントを使用している Cisco Secure Email Threat Defense アカウントは、[ユーザー（User）] メニューから利用できますが、同じ地域のアカウントに限定されることに注意してください。

Cisco Secure Email Threat Defense の動作ステータスを確認するにはどうすればよいですか？

Cisco Secure Email Threat Defense がダウンしているか、問題があると思われる場合は、[システムステータス（System Status）] ページを確認してください。このページには、[ユーザープロファイル（User Profile）] メニューから、または https://ciscosecureemailthreatdefense.statuspage.io から直接アクセスできます。

Cisco Secure Email Threat Defense と Microsoft 365

Cisco Secure Email Threat Defense は、Microsoft 365 の許可リストに含まれる送信者またはドメインを優先しますか。

はい。Cisco Secure Email Threat Defense は、スパムおよびグレイメールメッセージに関して、Microsoft 365 のスパムフィルタ許可リストに追加された送信者とドメインを受け入れます。MS 許可リストは、脅威の判定（BEC、詐欺、悪意がある、フィッシング）では使用されません。これらの項目は、ポリシー設定に従って修復されます。

Microsoft Defender では、https://security.microsoft.com/antispam からこの設定にアクセスできます。

Microsoft の MSAllowList ヘッダーにおける最近の変更により、個々のユーザがメールボックス内の許可リストを設定することを組織が許可しており、メッセージがユーザの許可リストに含まれる場合、Microsoft 許可リストが Cisco Secure Email Threat Defense で常に適用されることはありません。Cisco Secure Email Threat Defense でこれらの設定を適用する場合は、[ポリシー（Policy）] ページの [スパムまたはグレイメールと判定されたMicrosoft Safe Senderメッセージを修復しない（Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts）] チェックボックスをオンにします。Safe Sender フラグは、スパムとグレイメールの判定では適用されますが、脅威の判定では適用されません。つまり、スパムまたはグレイメールと判定された Safe Sender メッセージは修正されません。

Cisco Secure Email Threat Defense は、ユーザが Outlook で迷惑メールに対して実行するアクションを優先しますか。

ユーザーは、[送信者をブロックしない（Never Block Sender）] や [安全な送信者に追加（Add to Safe Senders）] などの Outlook の迷惑メールオプションを使用してメールにマークを付けることができます。Cisco Secure Email Threat Defense でこれらの設定を適用する場合は、[ポリシー（Policy）] ページの [スパムまたはグレイメールと判定されたMicrosoft Safe Senderメッセージを修復しない（Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts）] チェックボックスをオンにします。Safe Sender フラグは、スパムとグレイメールの判定では適用されますが、脅威の判定では適用されません。つまり、スパムまたはグレイメールと判定された Safe Sender メッセージは修正されません。

ジャーナリングサイズの制限とは何ですか。

150 MB を超えるメッセージは、Microsoft 365 によるジャーナリングの対象にはなりません。

Cisco Secure Email Threat Defense にすべてのドメインが表示されないのはなぜですか。

Cisco Secure Email Threat Defense は、テナントに関連付けられた電子メール機能を持つドメインをインポートします。ドメインに電子メール機能がない場合、Cisco Secure Email Threat Defense には表示されません。

Microsoft 365 のジャーナリングに関する詳細情報はどこで入手できますか。

Microsoft のドキュメント https://docs.microsoft.com/en-us/exchange/security-and-compliance/journaling/journaling を参照してください。

メッセージと検索

メッセージが誤って分類されたことをシスコに通知するにはどうすればよいですか。

メッセージが正しく分類されなかった（誤検出または検出漏れ）と思われる場合は、メッセージを再分類できます。このフィードバックは、今後の分類に影響を与えるために使用される場合があります。

一部のメッセージが [メッセージ（Messages）] ページに 2 回表示されるのはなぜですか。

重複エントリは、Microsoft で 1 つの電子メールに対して複数のジャーナルが作成された結果生じます。この現象は、さまざまな原因で発生する可能性があります。たとえば、Exchange 管理者が設定したメールルールや、ドメイン外ユーザーのグループに送信されたメールなどです。

非公開受信者とはどういう意味ですか。

非公開受信者とは、電子メールに受信者がリストされていないことを示します。たとえば、BCC（ブラインドカーボンコピー）が受信者に送信された場合です。Cisco Secure Email Threat Defense は BCC 受信者を追跡しませんが、検出と修復は影響を受けません。

サポート

Cisco Secure Email Threat Defense のドキュメントにアクセスするにはどうすればよいですか。

[ヘルプ(Help)] メニューを使用して Cisco Secure Email Threat Defense から直接、または次のリンクから Cisco Secure Email Threat Defense のドキュメントにアクセスできます。

- Cisco Secure Email Threat Defense ユーザーガイド
- Cisco Secure Email Threat Defense リリースノート

Cisco Secure Email Threat Defense の設定と使用に関するサポートを受けるにはどうすればよいですか。

Cisco Secure Email Threat Defense の設定と使用については、Email Security Customer Success チーム(etd-acivations@cisco.com)までお問い合わせください。

カスタマーサポートに連絡するにはどうすればよいですか。

Cisco Secure Email Threat Defense PoV(Proof of Value)評価のお客様は、cmd-support@cisco.com に電子メールをお送りください。

フルライセンスの Cisco Secure Email Threat Defense のお客様の場合:

- オンラインサポートケースを開く:https://www.cisco.com/c/en/us/support/index.html
- 電子メール:TAC@cisco.com
- 各国の CiscoTAC の連絡先:https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

注:ケースを開くには、Cisco Secure Email Threat Defense 契約を cisco.com アカウントにリンクする必要があります。cisco.com アカウントをまだお持ちでない場合は、こちらからアカウントを作成してください。