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/

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。

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。