

Experience Insights UIページロードエラーと Thousand Eyesモジュールのダウンロードの失敗

内容

お問い合わせ内容

Experience Insights UIインターフェイス内でページの読み込みエラーが発生し、ThousandEyesモジュール (TE jsonファイル) のダウンロードを試行するとエラーが発生します。これらのエラーにより、Experience Insightsデータにアクセスできず、エンドポイントの展開に必要なIntuneパッケージの作成がブロックされます。具体的な症状としては、Experience InsightsインターフェイスからThousandEyes統合モジュールを取得しようとしたときに、UIページが正しくロードされず、ダウンロードが失敗することがあります。

環境

セキュアアクセス – エクスペリエンスの分析 (パフォーマンスメトリック、エンドポイントエージェント)

解決策

この問題を解決するには、Thousand EyesとSecure Accessの組織との統合を再試行する必要があります。次の手順を実行する必要があります。

はじめる前に

組織管理者ロールを持つアクティブなCisco Thousand Eyeアカウント。詳細については、『[ロールベースアクセスコントロール](#)』および『[Thousand Eyesに組み込まれているロールと権限](#)』のドキュメントを参照してください。

- セキュアアクセスのアクティベーションの電子メール通知を受信した管理者は、Thousand Eyesのアクティベーションの電子メール通知も受信します。アクティベーション電子メールを受信してから72時間以内にThousand Eyesのプロビジョニング手順に従います。アクティベーション電子メールの有効期限が切れている場合は、[Thousand Eyesのログインページ](#)にアクセスして、[パスワードを忘れた場合]をクリックします。

Thousand Eyesログインアカウントグループは、Experience Insightsとの統合に適しています。

ログインアカウントグループは、Thousand EyesテストとSecure Access Experience Insightsに対するエージェントの可視性を決定します。詳細については、Thousand Eyesのドキュメントの「[What is an Account Group?](#)」を参照してください。

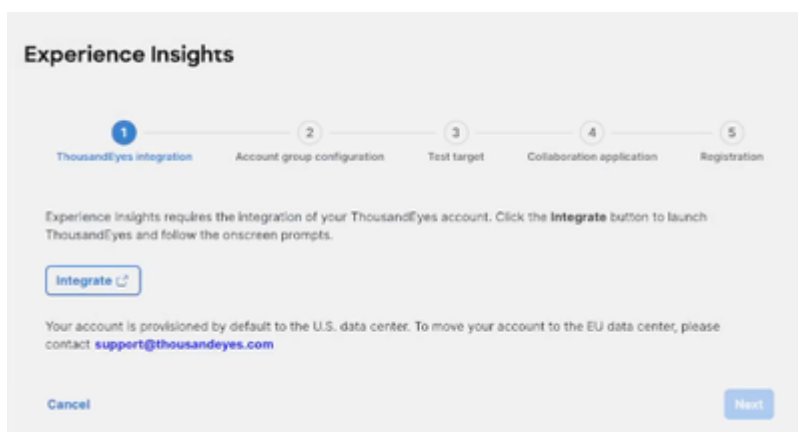
- 統合アカウントのThousand Eyesユーザプロフィールには、セキュアアクセスとの統合用のログインアカウントグループが必要です。詳細は、『[Role-Based Access Control: Login Account Group](#)』および『[Role-Based Access Control: Account Groups Screen](#)』（Thousand Eyesマニュアル）を参照してください。

統合

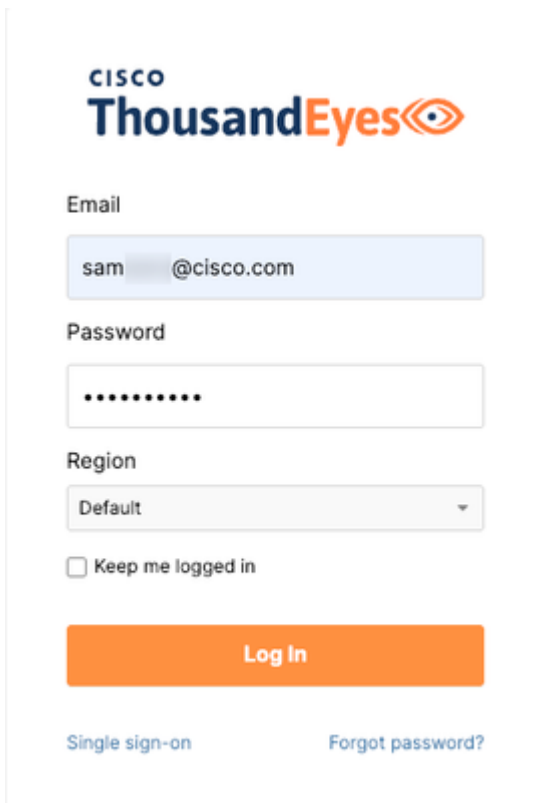
Experience Insightsには、Thousand Eyesアカウントの統合が必要です。

Experience Insights > Insights Management > Managementに移動し、Begin on boardingをクリックします。

Thousand Eyesを起動するには、Integrateボタンをクリックします。



Organization Adminロールを持つアカウントを使用してThousand Eyesにログインします。



次のセキュアアクセス権限をThousand Eyesで認可することを確認します。

Read organization : 組織のクレデンシャル、アカウントグループ、ユーザ、ユーザイベント、ロール、権限、使用状況、およびクォータの読み取りを許可します。

エンドポイントエージェントの管理 : エンドユーザがエンドポイントエージェントを管理できません。

エンドポイントテストの管理 : エンドユーザがエンドポイントテストを管理できるようにします。

タグの管理 : エンドユーザがタグとラベルを管理できるようにします。

Read tests : エンドユーザがテストとそれぞれの結果を読み取ることを許可します。

OAuth 2.0の千眼

Thousand Eyesは、OAuth 2.0プロトコルを使用して、Thousand Eyesデータへのアクセスを制限したセキュアなアクセスを許可します。詳細については、「[ThousandEyesを使用したOAuth 2.0](#)」を参照してください。

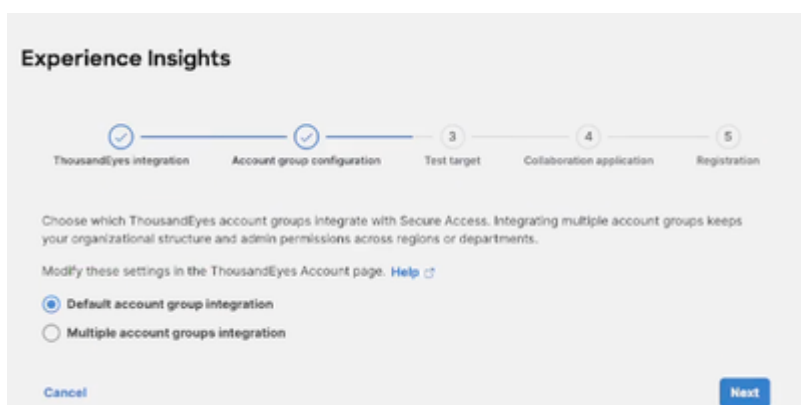
確認後、Experience Insights on boardingウィザードがリロードされ、Integration successfulメッセージが表示されるまで待つから、Nextをクリックします。

アカウントグループの構成

Thousand Eyeアカウントグループ統合を選択します。デフォルトのアカウントグループ統合または複数のアカウントグループ統合です。統合後に、統合方法を変更するには、Secure Access to Account Management > Account group integrationの順に選択します。

既定のアカウントグループ統合：この統合を選択すると、既定のアカウントグループにのみ2つの既定のテストが作成されます。オンボーディングの完了後にこれらのテストを編集する必要がある場合は、Account Managementに移動します。詳細については、「既定のテストターゲットの編集」を参照してください。

複数のアカウントグループの統合: [複数のアカウントグループ]を選択すると、セキュアアクセスとの最初の統合を行ったThousand Eyesユーザーに関連付けられたすべてのThousandEyesアカウントグループとテストが表示されます



既定のテストターゲット

合成ネットワークテストでは、エンドポイントで最も一般的に使用されているセキュリティ接続方法を選択します。テストターゲットオプションには、ゼロトラストアクセス、RAVPN、およびSWGローミングモジュールが含まれます。

- 総合テストでは、宛先までのユーザの移動におけるパフォーマンスの問題を特定します。オンボーディング後、テストターゲットを変更して、カスタムのパブリックまたはプライベートアプリケーションを含めることができます。

Onboard Experience Insights

Select the security connection method that is most commonly used by your endpoints for the synthetic network test. Post-onboarding, you can change the target, including selecting a custom (public or private application) target.

Zero Trust Access
 RAVPN
 SWG Roaming Module

Cancel Back Next

統合コラボレーションアプリケーション

- 組織のプライマリコラボレーションアプリケーション (Webex、Zoom、Microsoft Teams、またはNone) を選択して、全体的なヘルススコアを含む、ユーザインタラクション時のパフォーマンスのリアルタイムサマリーを表示します。選択内容は後で更新できます

Onboard Experience Insights

Select your organization's primary collaboration application to view a real-time summary of its performance during user interactions, including overall health score. You can update your selection later.

Webex
 Zoom
 Microsoft Teams
 None

Cancel Back Next

サウザンドアイズエージェント

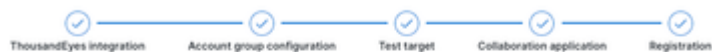
パフォーマンスを監視するには、エンドポイントをSecure Access組織に登録する必要があります。

- Cisco Secure Clientをエンドポイントに導入すると、Thousand Eyes Endpoint Agentがインストールされました。

Thousand Eyes Endpoint Agentは、エンドポイントがVPN、ZTA、またはRoamingモジュールに接続すると、自動的にセキュアアクセス組織に登録されます

セキュリティ接続にVPN、ZTA、またはRoamingモジュールを使用していないエンドポイントに、Thousand Eyes Endpoint Agentを手動で登録します。

Onboard Experience Insights



Choose how endpoints register with ThousandEyes to monitor their performance. The endpoint agent will be installed on your endpoints when Cisco Secure Client is downloaded.

Automatic registration

Endpoints will automatically register to your ThousandEyes default account group when they connect to VPN, ZTA, or SWG roaming module.

Command scripts

For endpoints that don't automatically register, copy and paste these command scripts on the endpoint or via MDM.

Windows script	Copy
Mac script	Copy

Manual registration

Register the ThousandEyes endpoint agent by copying and pasting the command script on the endpoint or via MDM.

Cancel

Back Done

- このプロセスでは、特定のエンドポイントにコマンドスクリプトをコピーして貼り付けます。登録スクリプトには、組織に固有のThousand Eyes接続文字列が含まれています。組織の接続文字列は、`-register`引数の後にあるパラメータです。

Windows

```
"C:\Program Files (x86)\Cisco\Cisco Secure Client\ThousandEyes Endpoint Agent\csc_te_agent"  
—register <接続文字列>
```

Mac

```
sudo /Applications/Cisco/Cisco\ Secure\ Client\ -\ ThousandEyes\ Endpoint\  
Agent.app/Contents/MacOS/csc_te_agent —register <接続文字列>
```

Experience Insights > Configure Accountの順に移動して、組織の登録スクリプトを見つけます。これらのスクリプトには、オンボーディングの完了後にいつでもアクセスできます。

エンドポイントのオペレーティングシステムに適したコマンドスクリプトをコピーします。

- ターゲットエンドポイントで、コピーしたスクリプトを貼り付けて実行します。

次の作業

Experience Insightsオンボーディングウィザードと1つ以上のエンドポイントの登録が完了すると、ThousandEyesエンドポイントエージェントによって報告されたデータがExperience Insightsダッシュボードに表示されます。

- Experience Insights > Endpointsに移動して、エンドポイントがデータを報告していることを確認します。

詳細については、次の資料を参照してください。

[Cisco Secure Client ThousandEyesエンドポイントエージェントモジュール](#)

[WindowsおよびmacOSデバイスでのCisco Secure Clientの使用の開始](#)

[Cisco Secure Clientのダウンロード](#)

[Microsoft Intune経由でCisco ThousandEyes Moduleを展開する \(MDMの例 \)](#)

原因

無効なアクセストークンを示すWeb開発者ツールを参照して問題を特定しました。

関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

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。