

セキュアアクセスにおけるドバイDCの機能停止の修復手順

内容

[はじめに](#)

[リソースコネクタ](#)

[リモートアクセスVPNプロファイル](#)

[ネットワークトンネルグループ](#)

[セキュアWebゲートウェイ](#)

[ゼロトラストアクセスクライアント](#)

[関連情報](#)

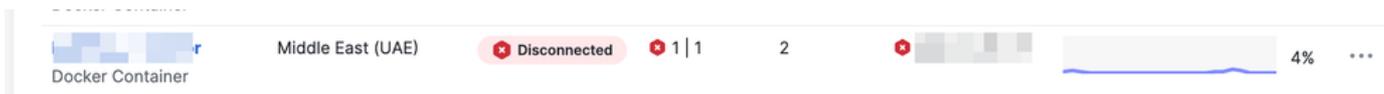
はじめに

本書では、3月2日に発生したSecure Access Dubai DCインシデントの修復手順について説明します。

<https://status.sse.cisco.com/incidents/7h28mb7mr5zl>

リソースコネクタ

すでに展開されているリソースコネクタは、セキュアアクセスダッシュボードから切断されていることが表示されます。



配備されたリソースコネクタは、単一のセキュアアクセス領域にバインドされます。これは、構成変更によって変更することはできません。

この問題を修正するには、該当するお客様が次に示す手順に従う必要があります。

1. 新しいリソースコネクタを展開する
2. 新しい領域(ムンバイまたはハイデラバード)にコネクタグループを作成する
2. プライベートリソースを新しいコネクタグループに割り当てる

リソースコネクタの導入に関する詳細な手順については、『リソースコネクタ導入ガイド』を参照してください。

リモートアクセスVPNプロフィール

リモートアクセスVPNクライアントは、さまざまなエラーが発生すると接続の確立に失敗する可能性があります。

エラー例：



ドバイDCのリモートアクセスVPNプロフィールを持つ組織のみ：

次の手順に従ってください。

- ・ 移行ターゲットとして最も近い使用可能なデータ・センター（ムンバイまたはハイデラバード）を選択します。
- ・ 組織の現在のセッション負荷に合わせてVPN IPプールとプロフィールを設定し、既存のME-Central設定をミラーリングします。

新しいVPNプロフィールの設定に関する詳細な手順については、『リモートアクセスVPN導入ガイド』に従ってください。

ネットワークトンネルグループ

ネットワークトンネルグループ領域を変更するには、次の手順に従ってください：

- ・ 次の説明に従ってNTGオプションに移動します：
- ・ 中東(UAE)リージョンの既存のトンネルを編集します。

Network Connections
 Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)

Connector Groups **Network Tunnel Groups** FTDs

Network Tunnel Groups 8 total

2 Disconnected ❗ 3 Warning ⚠️ 3 Connected ✅

Network Tunnel Groups
 A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Search: mec Region: ▼ Status: ▼ 1 Tunnel Group [+ Add](#)

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
mec Other	⚠️ Warning	Middle East East (UAE)	sse-mec-1-1-1	6	sse-mec-1-1-0	1

Actions: Edit, View Details, View Logs, Delete

- ・ 地域を中東(UAE)からインド (西部) に変更します。

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name:

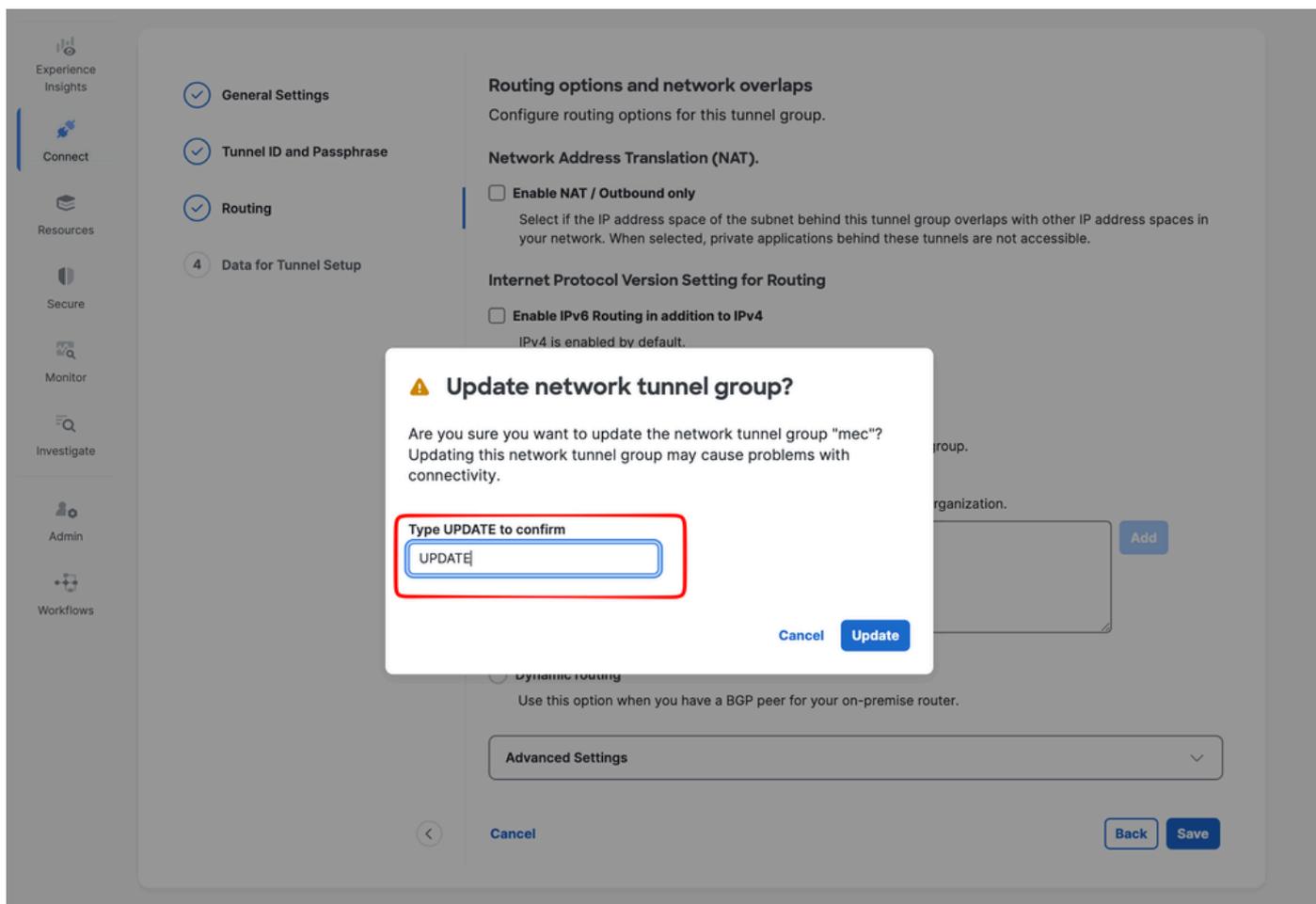
Region: Middle East (UAE) ^

- Africa (South Africa)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Osaka)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Australia (Sydney)
- Brazil
- Canada (Central)
- Canada (West)
- Europe (Germany)
- Europe (Milan)
- Europe (Spain)
- Europe (Stockholm)
- India (South)
- India (West)

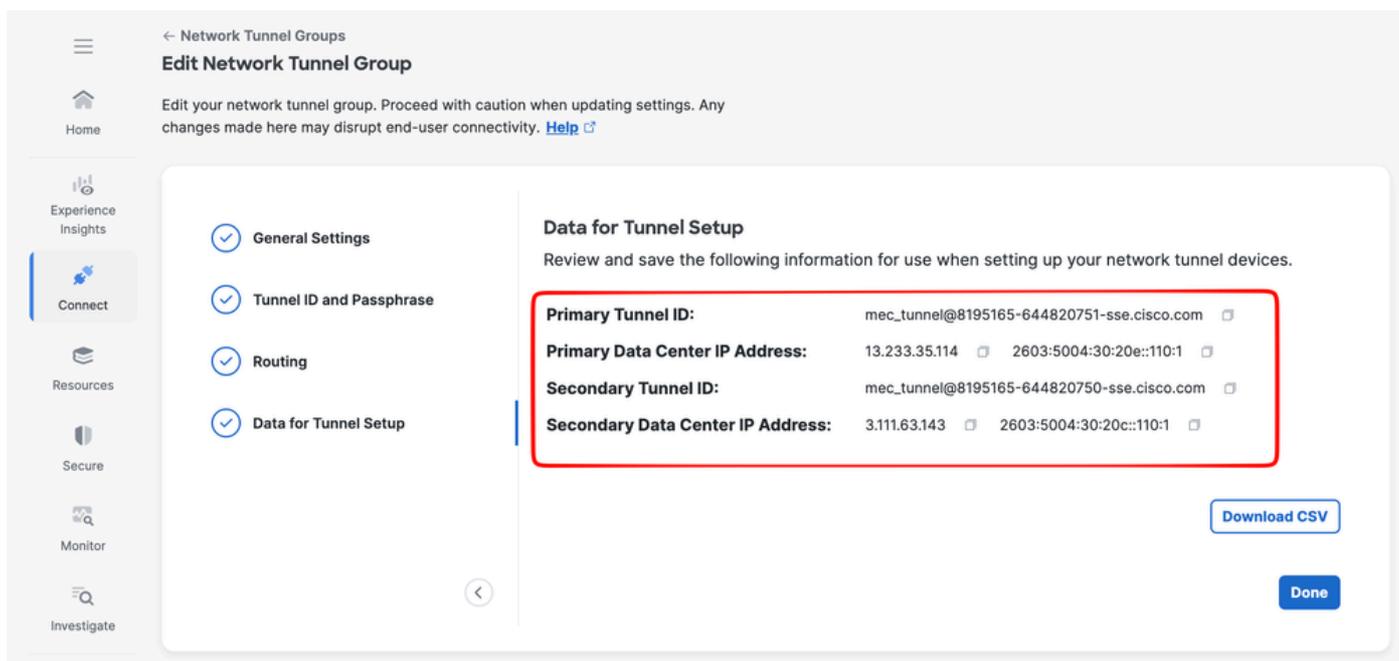
[Next](#)

- ・ 他の設定は変更しないでください。設定を保存します。

- ・ プロンプトが表示されたら、「UPDATE」と入力して確認します。



- ・ 表示されている新しいインド (西) のIPアドレスを使用して、IPSEC CPEデバイスを更新します。



- ・ マルチリージョンバックホールまたはルートマップを使用している場合は、Cisco SSEからの新しい設定に従ってBGPコミュニティ値を更新します。

セキュアWebゲートウェイ

Roaming Security Moduleを使用するクライアントは、次に最も近くて使用可能なセキュアアクセスデータセンターに自動的に接続します。

現時点でお客様からのアクションは不要です。

ゼロトラストアクセスクライアント

ゼロトラストアクセスモジュールを使用するクライアントは、次に最も近くて利用可能なセキュアアクセスデータセンターに自動的に接続します。

現時点でお客様からのアクションは不要です。

関連情報

- ・ [ステータスCisco Secure Access](#)

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。