

# Behebungsschritte bei einem Rechenzentrumsausfall in Secure Access Dubai

## Inhalt

---

### [Einleitung](#)

[Ressourcen-Connectors](#)

[Remote Access-VPN-Profil](#)

[Netzwerk-Tunnelgruppen](#)

[Sicheres Web-Gateway](#)

[Clients mit nicht vertrauenswürdigem Zugriff](#)

### [Zugehörige Informationen](#)

---

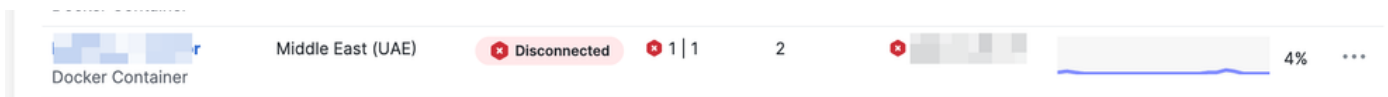
## Einleitung

Dieses Dokument enthält die Behebungsschritte bei einem Zwischenfall im Rechenzentrum von Secure Access am 2. März in Dubai.

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

## Ressourcen-Connectors

Bereits bereitgestellte Ressourcenkonnektoren werden als vom Dashboard für sicheren Zugriff getrennt angezeigt:



Bereitgestellte Ressourcenkonnektoren sind an eine einzige sichere Zugriffsregion gebunden und können nicht durch Konfigurationsänderungen geändert werden.

Um das Problem zu beheben, müssen die betroffenen Kunden die unten aufgeführten Schritte durchführen:

1. Bereitstellung eines neuen Ressourcen-Connectors
2. Verbindungsgruppen in neuen Regionen erstellen (Mumbai oder Hyderabad)
2. Zuweisen privater Ressourcen zu neuen Connector-Gruppen

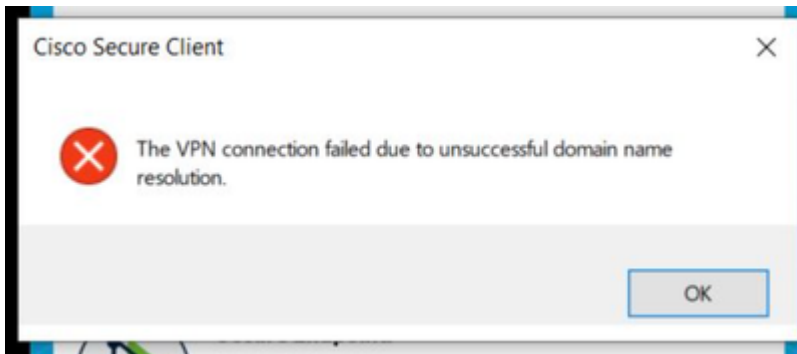
Befolgen Sie den Bereitstellungsleitfaden für Resource Connector für detaillierte Schritte zur

Bereitstellung des Resource Connectors:

## Remote Access-VPN-Profil

Remotezugriff-VPN-Clients können die Verbindung möglicherweise nicht mit verschiedenen Fehlern herstellen.

Beispielfehler:



Nur für Unternehmen mit Remote Access-VPN-Profil in Dubai Rechenzentrum:

Führen Sie die folgenden Schritte aus:

- Wählen Sie als Migrationsziel das nächstgelegene verfügbare Rechenzentrum (Mumbai oder Hyderabad) aus.
- Konfigurieren Sie VPN-IP-Pools und -Profile entsprechend der aktuellen Sitzungslast Ihres Unternehmens, und spiegeln Sie die bestehende ME-Central-Konfiguration.

Im Remote Access VPN-Bereitstellungsleitfaden finden Sie detaillierte Schritte zur Konfiguration eines neuen VPN-Profiles:

## Netzwerk-Tunnelgruppen

Führen Sie die folgenden Schritte aus, um die Region der Netzwerk-Tunnelgruppe zu ändern.:

- Gehen Sie zu den NTG-Optionen, wie hier beschrieben:
- Bearbeiten Sie Ihren vorhandenen Tunnel für die Region Naher Osten (VAE).

**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 |
|----------------------|------------------------------------------------|-------------------|-------------------------|-----------------|---------------------------|-------------------|
| <b>mec</b><br>Other  | <span style="color: orange;">⚠️ Warning</span> | Middle East (UAE) | sse-mec-1-1-1           | 6               | sse-mec-1-1-0             | 1                 |

Context menu for 'mec':  
[Edit](#)  
[View Details](#)  
[View Logs](#)  
[Delete](#)

- Ändern Sie die Region von Naher Osten (VAE) nach Indien (West).

**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:

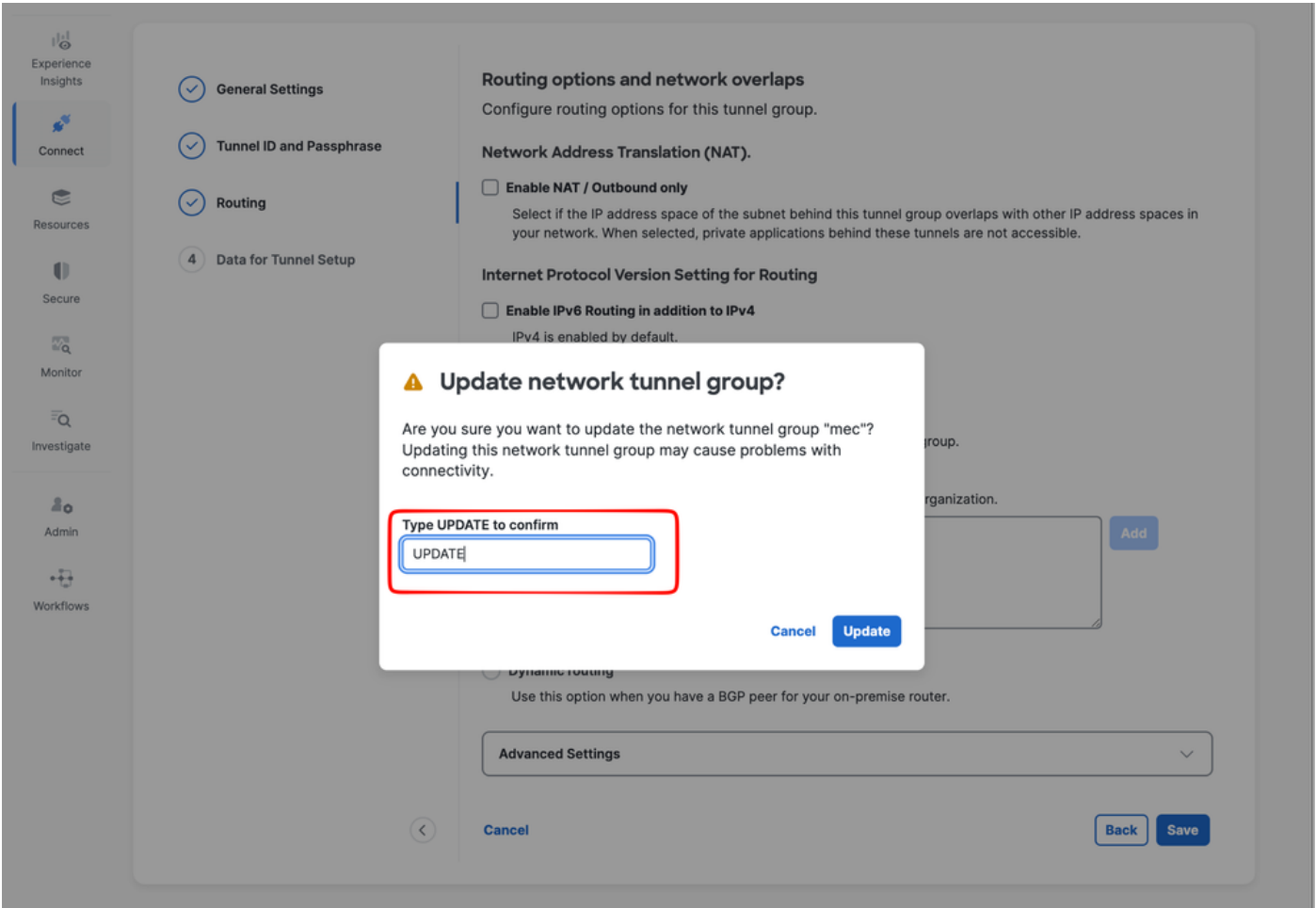
Region: ▼

- 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)**

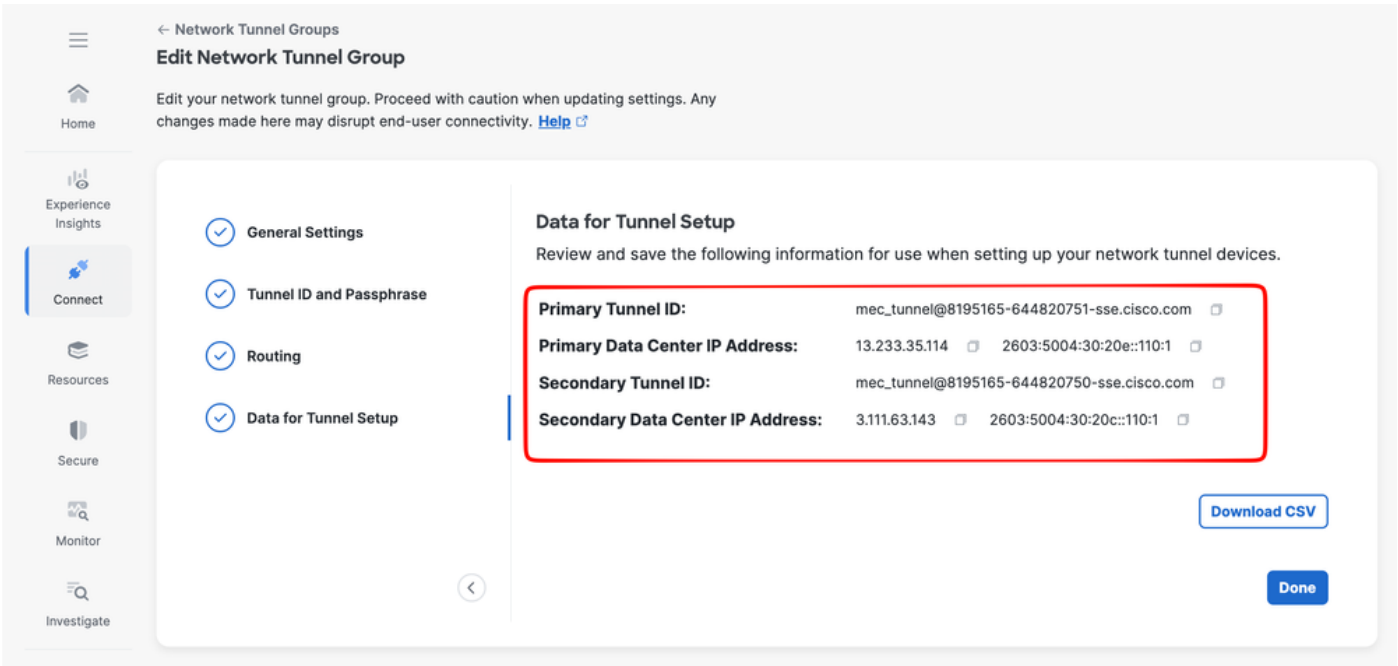
[Next](#)

- Ändern Sie keine anderen Einstellungen. Speichern Sie die Konfiguration.

- Wenn Sie dazu aufgefordert werden, geben Sie "UPDATE" ein, und bestätigen Sie.



- Verwenden Sie die angezeigten neuen IP-Adressen in Indien (West), um Ihr IPSEC CPE-Gerät zu aktualisieren.



- Bei Verwendung von Multi-Region Backhaul oder Routing-Maps müssen die BGP-Community-Werte den neuen Einstellungen von Cisco SSE entsprechend aktualisiert werden.

## Sicheres Web-Gateway

Clients, die das Roaming-Sicherheitsmodul verwenden, stellen automatisch eine Verbindung mit dem nächstgelegenen und verfügbaren Secure Access Datacenter her.

Derzeit sind keine Maßnahmen seitens der Kunden erforderlich.

## Clients mit nicht vertrauenswürdigem Zugriff

Clients, die das Zero Trust Access-Modul verwenden, stellen automatisch eine Verbindung mit dem nächstgelegenen und verfügbaren Secure Access Datacenter her.

Derzeit sind keine Maßnahmen seitens der Kunden erforderlich.

## Zugehörige Informationen

- [Status Cisco Secure Access](#)

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.