Oplossingsstappen voor problemen met Secure Access in Dubai DC

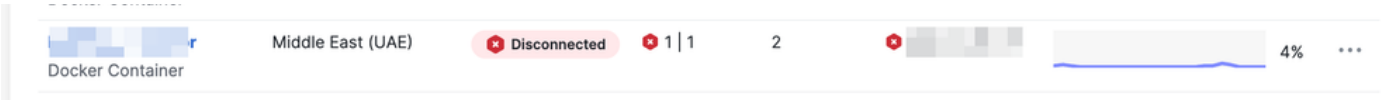
Inhoud

Inleiding

Dit document bevat de herstelstappen voor het incident met Secure Access Dubai DC op 2 maart. https://status.sse.cisco.com/incidents/7h28mb7mr5zl

Bronconnectors

Reeds geïmplementeerde Resource Connectors worden weergegeven als Verbinding verbroken met het dashboard voor beveiligde toegang:



De geïmplementeerde Resource Connectors zijn gebonden aan één Secure Access Region en dit kan niet worden gewijzigd via een wijziging van de configuratie.

Om het probleem op te lossen, moeten getroffen klanten de onderstaande stappen volgen:

1. Een nieuwe Resource Connector implementeren

2. Connectorgroepen maken in nieuwe regio('s) (Mumbai of Hyderabad)

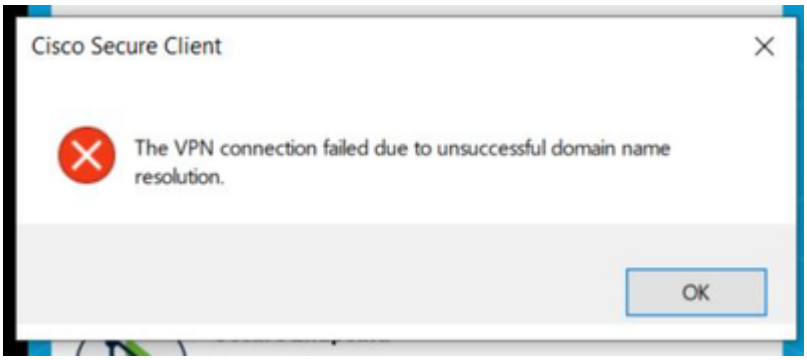
2. Privébronnen toewijzen aan nieuwe connectorgroepen

Volg de Implementatiehandleiding voor Resource Connector voor gedetailleerde stappen voor het implementeren van de Resource Connector:

VPN-profielen voor externe toegang

Remote Access VPN-clients kunnen de verbinding niet met verschillende fouten tot stand brengen.

Voorbeeldfout:



Voor organisaties die alleen een VPN-profiel voor externe toegang in Dubai DC hebben:

Volg deze stappen:
· Selecteer het dichtstbijzijnde beschikbare datacenter (Mumbai of Hyderabad) als uw migratiedoel.
· Configureer VPN IP-pools en -profielen die overeenkomen met de huidige sessielast van uw organisatie en die een afspiegeling zijn van uw bestaande ME-Central-installatie.

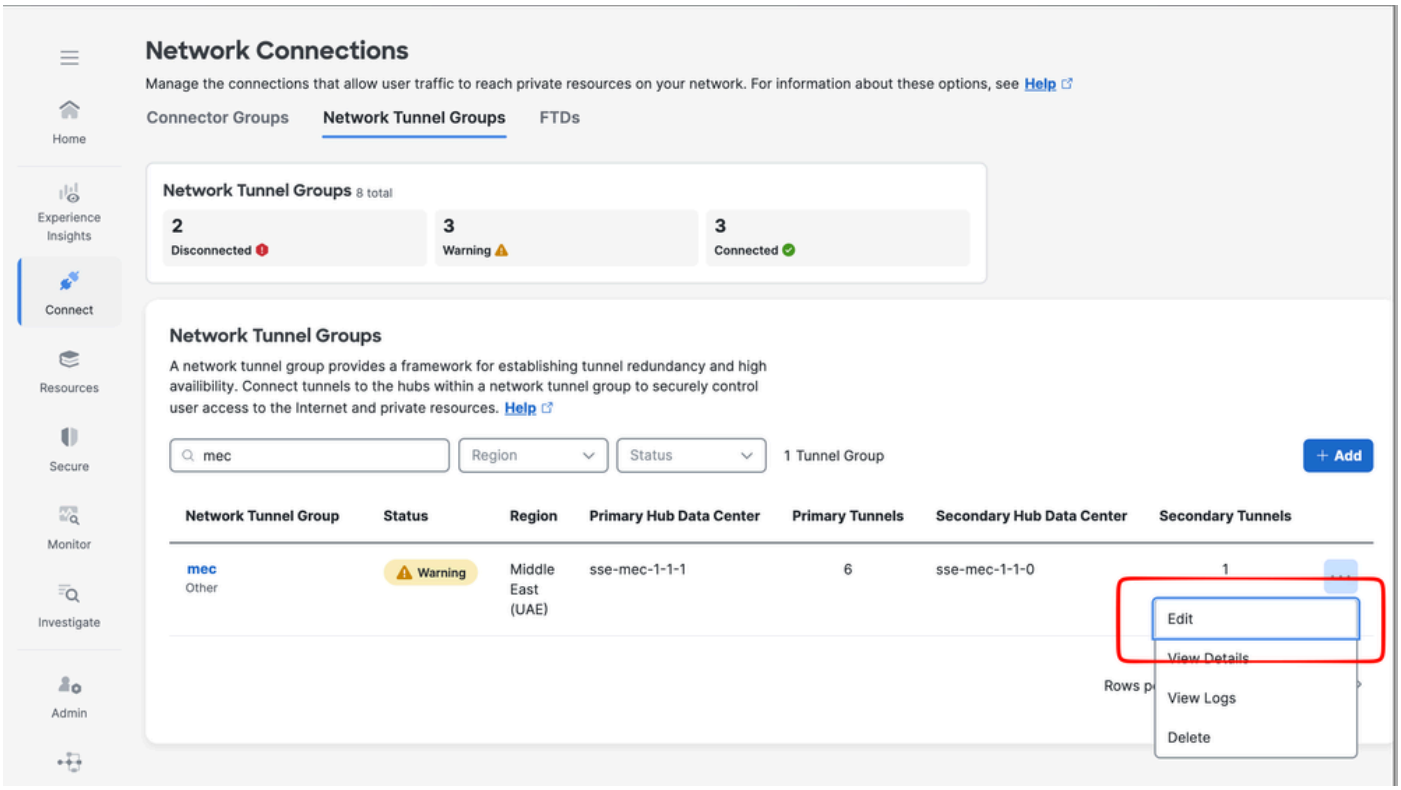
Volg de handleiding voor de implementatie van Remote Access VPN voor gedetailleerde stappen voor het configureren van een nieuw VPN-profiel:

Netwerktunnelgroepen

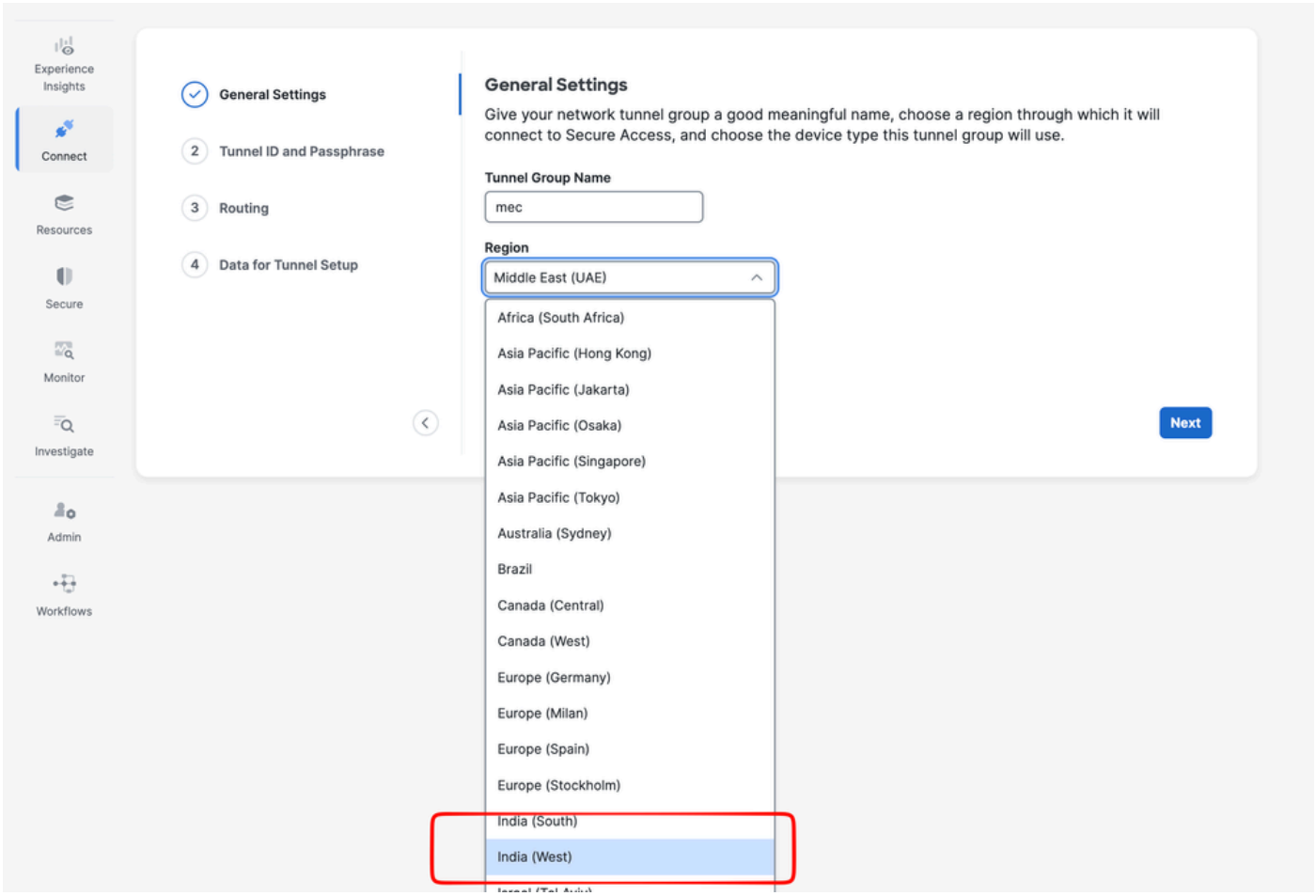
Volg deze stappen om de Network Tunnel Group-regio te wijzigen:

· Ga naar de NTG-opties zoals hier beschreven:

· Bewerk uw bestaande tunnel voor het Midden-Oosten (VAE) regio.

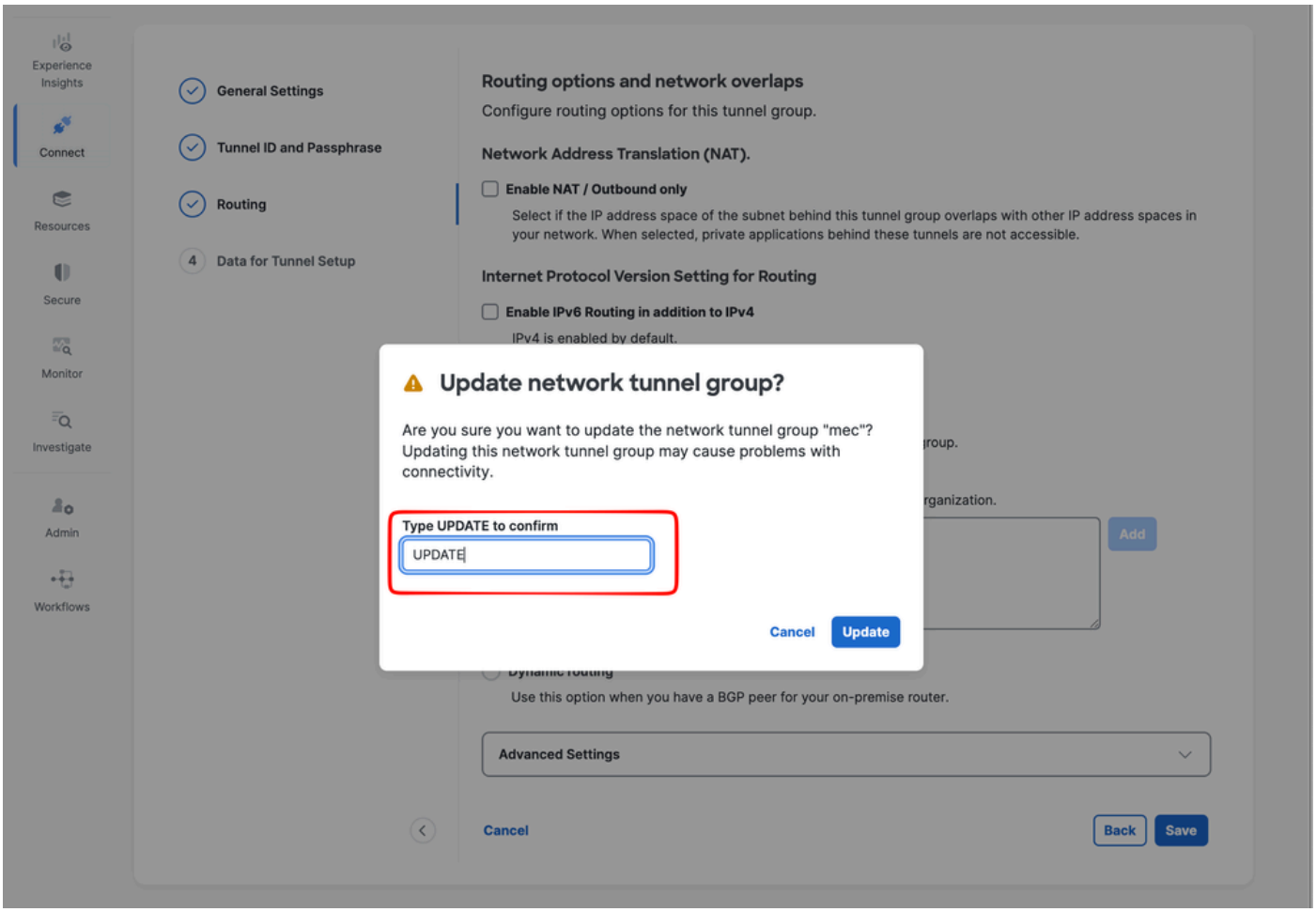


· Verander de regio van het Midden-Oosten (VAE) naar India (West).

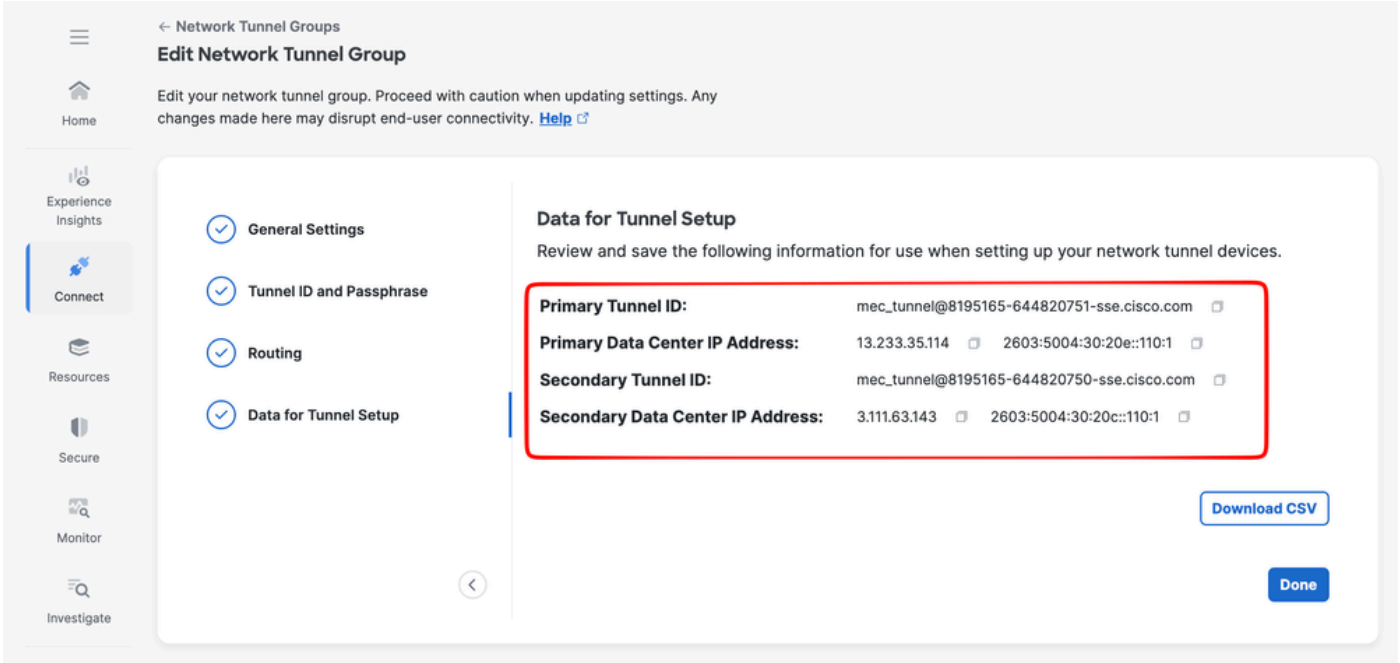


· Wijzig geen andere instellingen; sla de configuratie op.

· Typ "UPDATE" en bevestig dit wanneer u daarom wordt gevraagd.



· Gebruik de nieuwe IP-adressen in India (West) die worden weergegeven om uw IPSEC CPE-apparaat bij te werken.



· Als Multi-Region Backhaul of routekaarten worden gebruikt, werkt u de BGP-communitywaarden bij volgens de nieuwe instellingen van Cisco SSE.

beveiligde webgateway

Cliënten die gebruikmaken van de beveiligingsmodule voor roaming maken automatisch verbinding met het dichtstbijzijnde en beschikbare datacenter voor beveiligde toegang.
Er is op dit moment geen actie van klanten vereist.

Klanten met Zero Trust Access

Cliënten die de Zero Trust Access-module gebruiken, maken automatisch verbinding met het dichtstbijzijnde en beschikbare Secure Access Datacenter.
Er is op dit moment geen actie van klanten vereist.

Gerelateerde informatie

- Status Cisco Secure Access

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.