

Umbrella VA configureren om gebruikers-IP-toewijzingen te ontvangen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[virtueel toestel](#)

[Voeg een privésleutel en certificaat toe aan de VA](#)

[Certificaat toevoegen aan de VA](#)

[HTTPS inschakelen op de VA](#)

[HTTPS-inschakeling controleren](#)

[Active Directory](#)

[Umbrella Android-client](#)

[Umbrella Chromebook-client](#)

[configuratiesequentie](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco Umbrella Virtual Appliance (VA) configureert om IP-toewijzingen van gebruikers via een beveiligd kanaal te ontvangen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

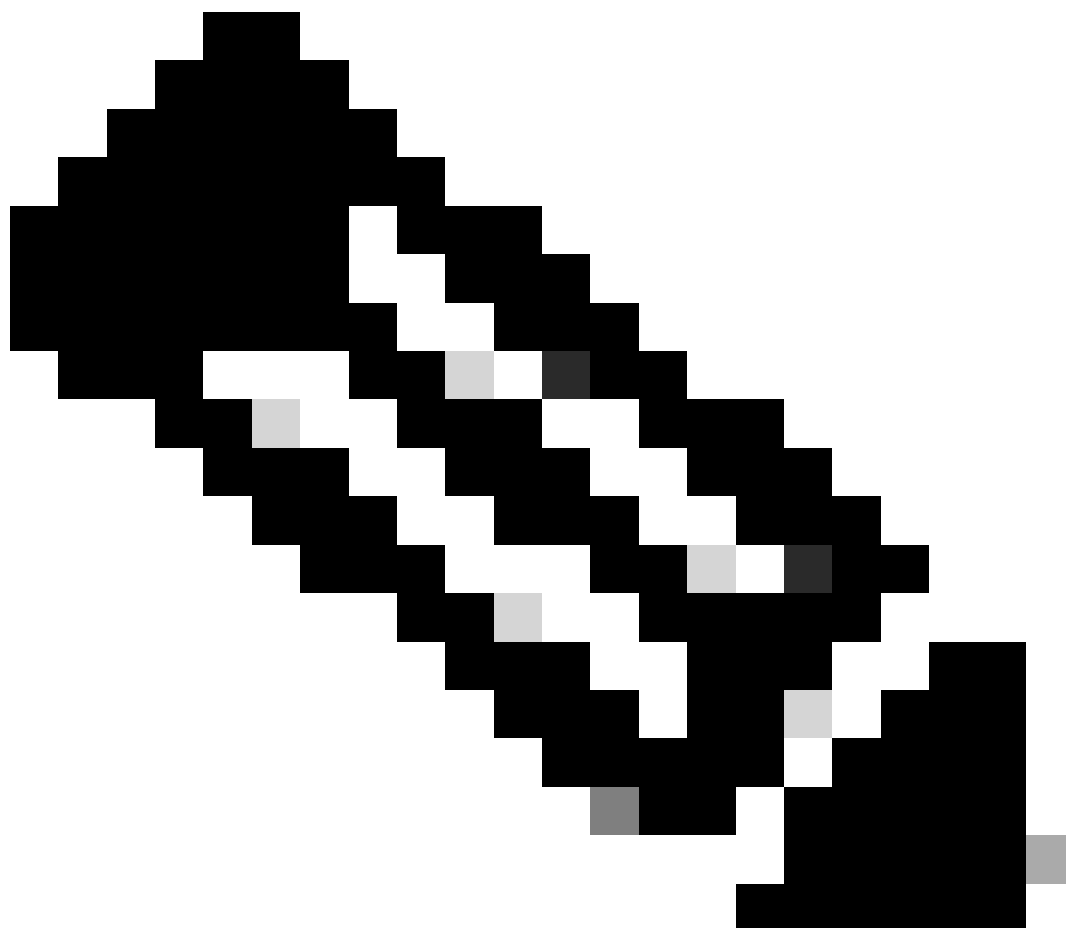
- Het maken van privésleutels, het maken van certificaten, het ondertekenen en beheren van certificaten vallen buiten het bereik van de Umbrella-componenten. Dit moet buiten deze onderdelen gebeuren.
- U moet één certificaat maken met een unieke gemeenschappelijke naam per virtueel toestel.
- U moet ook een A-record toevoegen aan uw interne DNS-server en deze algemene naam naar het IP-adres van het virtuele toestel verwijzen.
- Als het IP-adres van een virtueel apparaat moet worden gewijzigd, moet ook dit A-record dienovereenkomstig worden gewijzigd.

- De FQDN die overeenkomt met het certificaat moet worden geconfigureerd als een lokaal domein op het Umbrella-dashboard, zodat de VA dit herkent als een lokaal domein.
- Private key en certificaten moeten worden gemaakt in de .key en .cer formaat respectievelijk.
- U kunt hiervoor zelf ondertekende certificaten of CA-ondertekende certificaten gebruiken.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Virtueel apparaat met versie 2.7 of hoger
- Umbrella AD Connector moet versie 1.5 of hoger uitvoeren
- Umbrella Chromebook-clients moeten versie 1.3.3 of hoger uitvoeren



Opmerking: Als uw VA- of AD-connector eerdere versies uitvoert, kunt u [een supportticket openen met Umbrella](#) om ze te upgraden naar de respectievelijke ondersteunde versies.

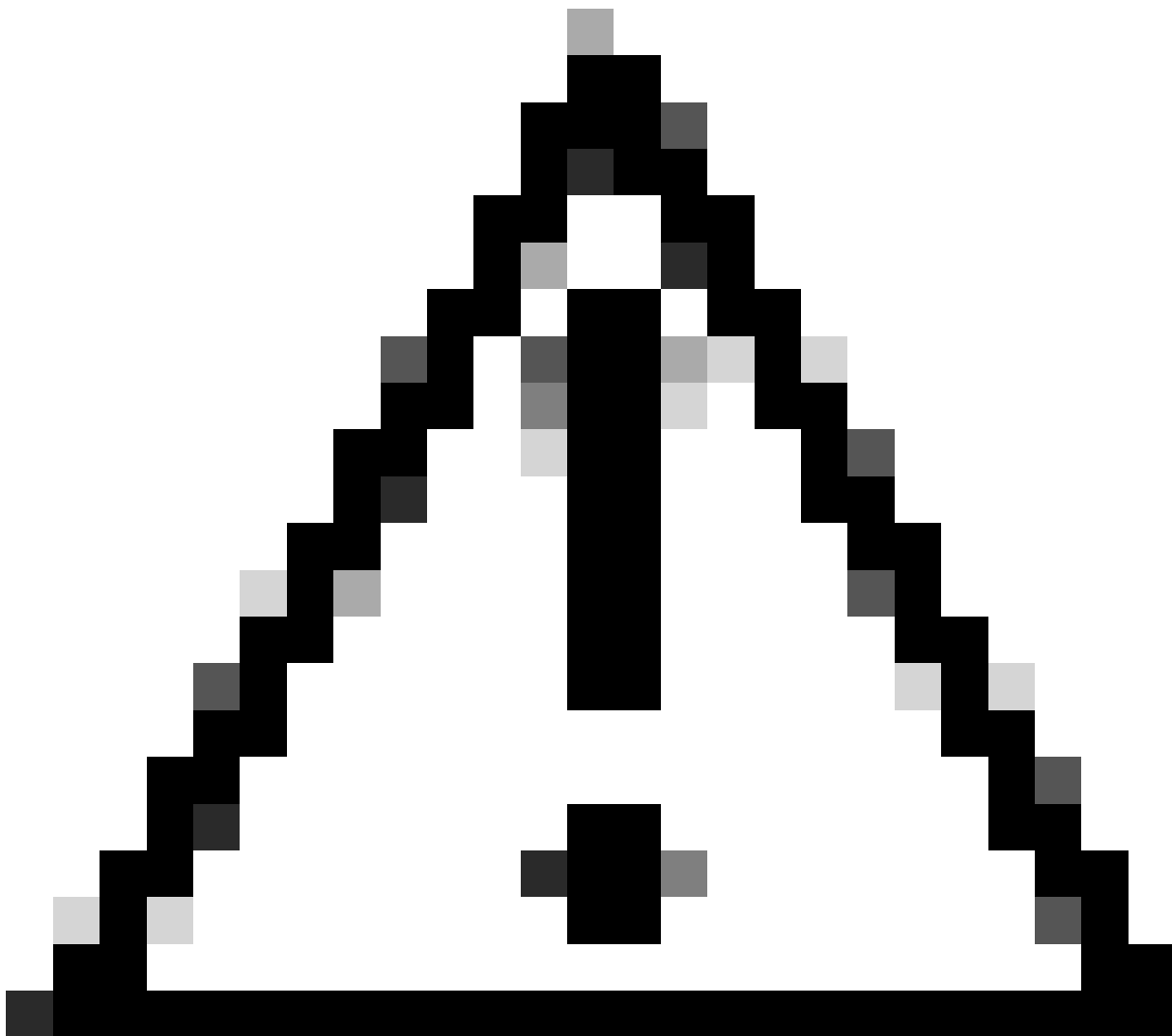
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Umbrella Virtual Appliances, met versie 2.6 of eerder, ondersteunen het ontvangen van gebruikers-IP-toewijzingen van de Umbrella Active Directory (AD)-connector en de Umbrella Chromebook Clients alleen in niet-gecodeerde vorm op poort 443. Als gevolg hiervan is een verplichte voorwaarde voor implementatie dat de AD Connector en VA of Chromebook Clients en VA alleen via een vertrouwd netwerk communiceren.

Vanaf versie 2.7 kunnen Umbrella Virtual Appliances nu AD-gebruiker-IP-toewijzingen ontvangen van de AD Connector via HTTPS, en op dezelfde manier GSuite-gebruiker-IP-toewijzingen van elke Umbrella Chromebook-client via HTTPS.

In dit artikel worden de configuratiestappen voor elke component beschreven om HTTPS-communicatie mogelijk te maken. Standaard is HTTPS-communicatie uitgeschakeld en communiceren de AD-connector en Chromebook-clients alleen via HTTP met de VA.



Waarschuwing: als u deze functie inschakelt, kan het CPU- en geheugengebruik op de VA- en de Umbrella AD-connector worden verhoogd en kan dit leiden tot een lagere DNS-doorvoer voor de VA. Het is daarom aan te raden deze functie alleen in te schakelen als dit is vereist op grond van nalegingsvereisten voor uw organisatie.

virtueel toestel

Voeg een privésleutel en certificaat toe aan de VA

Voeg de private key en het certificaat toe aan de VA:

1. Open het bestand met de privésleutel via de teksteditor.
2. Selecteer all, copy en plak de dubbele aanhalingstekens voor deze opdracht:

```
config va ssl key "paste the contents of the .key file here"
```

Certificaat toevoegen aan de VA

Om het certificaat aan de VA toe te voegen:

1. Open het certificaatbestand via teksteditor.
2. Selecteer all, copy en plak de dubbele aanhalingstekens voor de onderstaande opdracht:

```
config va ssl cert "paste the contents of the .crt file here"
```

HTTPS inschakelen op de VA

Schakel HTTPS op de VA in met deze opdracht:

```
config va ssl enable
```

HTTPS-inschakeling controleren

Controleer of HTTPS is ingeschakeld met de opdracht:

```
config va show
```

De uitvoer van deze opdracht kan de HTTPS-status en de details van het SSL-certificaat bevatten.

Voorbeeld van uitvoer:

```
HTTPS status : enabled
SSL Certificate Start Time : 2024-04-16 16:11:08
SSL Certificate Expiry Time : 2025-04-16 16:11:08
Issuer : C = US, ST = MASSACHUSETTS, L = BOSTON, O = CISCOSUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

Het kan tot 20 minuten duren voordat de VA gebeurtenissen via HTTPS ontvangt. U kunt controleren na ongeveer 20 minuten met behulp van de `config va status` opdracht. De AD-connectorstatus is in de tussenliggende periode geel (vastgelopen) en wordt groen zodra de VA gebeurtenissen via HTTPS begint te ontvangen.

Als u HTTPS wilt uitschakelen en wilt terugkeren naar HTTP, gebruikt u de opdracht `config va ssl`

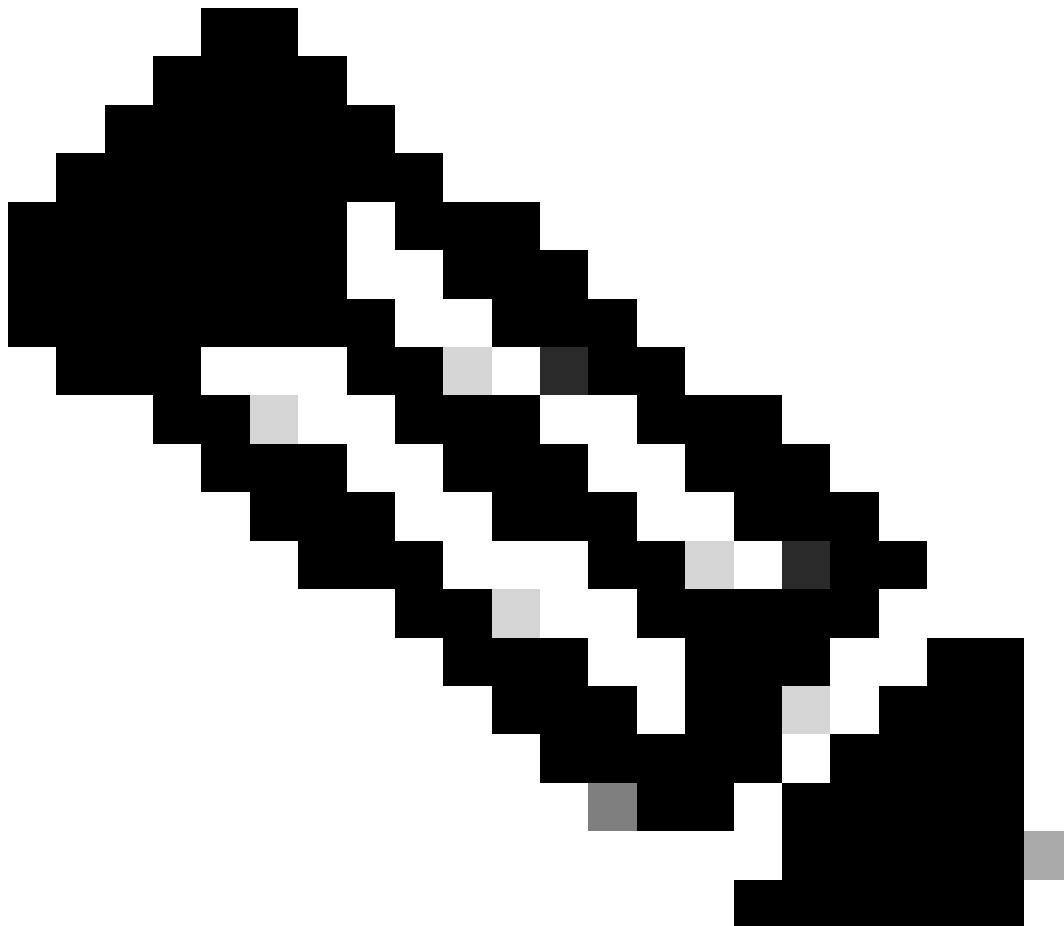
disable.

Als u HTTPS opnieuw wilt inschakelen, moet u de privésleutel en het certificaat opnieuw toevoegen en vervolgens de opdracht `config va inschakelen` gebruiken.

Active Directory

Als u een CA-ondertekend certificaat gebruikt voor elke VA, moet u ervoor zorgen dat het rootcertificaat en de afgifte van CA-certificaten voor elk VA-certificaat zijn geïnstalleerd op elk systeem waarop de AD-connector op dezelfde locatie als de VA wordt uitgevoerd.

Als u een zelf ondertekend certificaat gebruikt voor elke VA, moet u ervoor zorgen dat elk VA-certificaat is geïnstalleerd op elk systeem waarop de AD-connector wordt uitgevoerd op dezelfde overkoepelende locatie als de VA.



Opmerking: alleen certificaten voor VA's op dezelfde overkoepelende locatie als de AD-connector moeten op de AD-connector worden geïnstalleerd.

Het kan tot 20 minuten duren voordat de VA de HTTPS-status synchroniseert met Umbrella, die vervolgens wordt gesynchroniseerd met de AD-connector. Als gevolg hiervan kan het tot 20 minuten duren voordat de Connector gegevens via HTTPS naar de VA verzendt. Alle gebruikers-IP-toewijzingen die tijdens deze periode worden verzonden, worden door de VA verwijderd. Het wordt daarom aanbevolen om de configuratie op de VA alleen te wijzigen tijdens downtime-uren wanneer er geen gebruikersaanmeldingen worden verwacht.

Umbrella Android-client

Als u CA-ondertekende certificaten voor VA's gebruikt, moet u ervoor zorgen dat het rootcertificaat en de afgifte van CA-certificaten voor elk VA-certificaat worden gepusht naar en geïnstalleerd op elk Android-apparaat.

Als u zelfondertekende certificaten voor VA's gebruikt, moet u ervoor zorgen dat elk VA-certificaat wordt gepusht naar en geïnstalleerd op elk Android-apparaat.

Zodra het certificaat beschikbaar is, kan de Umbrella Android-client dit certificaat gebruiken om een HTTPS-kanaal met de VA in te stellen.

Umbrella Chromebook-client

Als u CA-ondertekende certificaten voor VA's gebruikt, moet u ervoor zorgen dat het rootcertificaat en de afgifte van CA-certificaten voor elk VA-certificaat worden gepusht naar en geïnstalleerd op elke Chromebook.

Als u zelfondertekende certificaten voor VA's gebruikt, moet u ervoor zorgen dat elk VA-certificaat wordt gepusht en op elke Chromebook wordt geïnstalleerd.

Zodra het certificaat beschikbaar is, kan de Umbrella Chromebook Client dit certificaat gebruiken om een HTTPS-kanaal met de VA in te stellen.

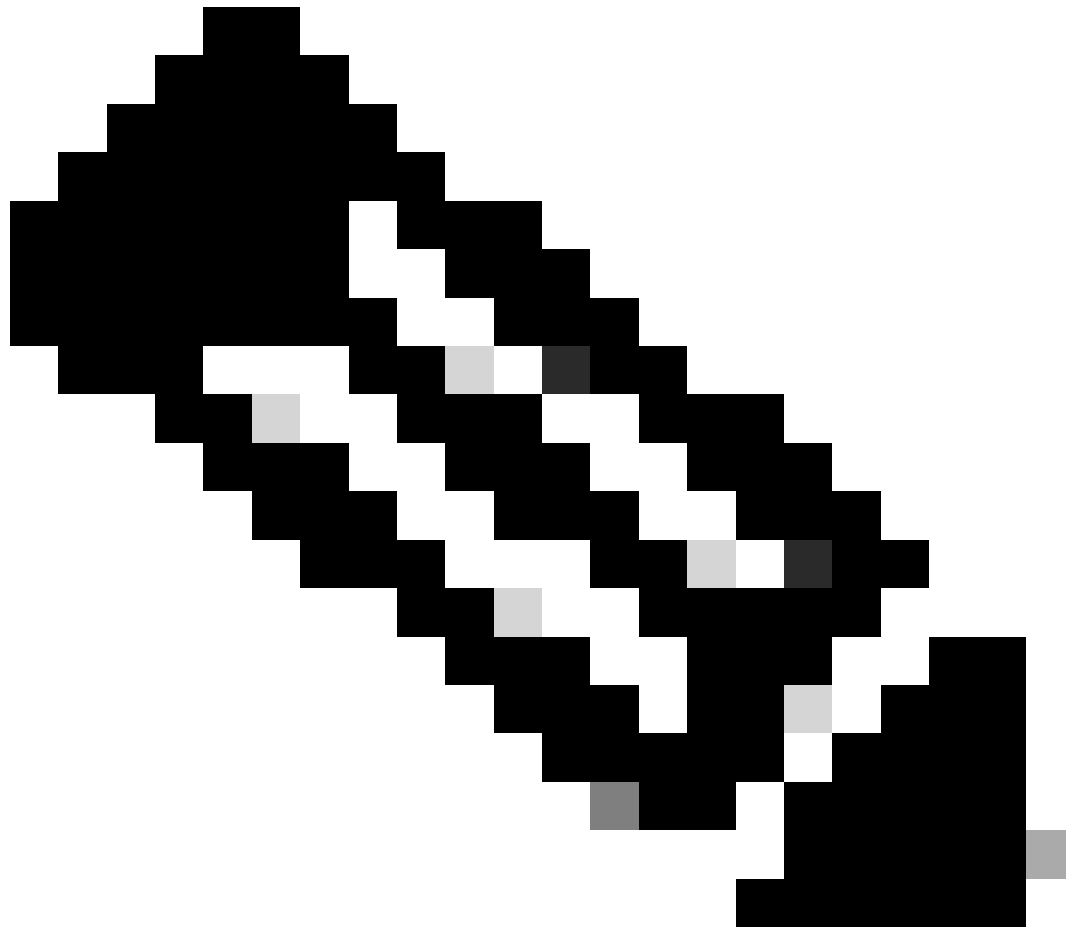
Raadpleeg voor meer informatie het artikel [Umbrella Chromebook Client: Het verzenden van gebruikers-IP-toewijzingen via een beveiligd kanaal naar de Umbrella Virtual Appliance](#).

configuratiesequentie

Zodra HTTPS is ingeschakeld op de VA, accepteert de VA geen user-IP-mappings die in platte tekst via HTTP worden verzonden. Als gevolg hiervan worden alle gebruikersaanmeldingen die via HTTP worden verzonden, verwijderd en is gebruikersattributie voor DNS-verzoeken van deze gebruikers niet beschikbaar. Het wordt daarom aanbevolen om deze componenten in deze volgorde te configureren:

1. Maak het certificaat en de privésleutel voor elke VA op basis van een door de CA ondertekend of zelf ondertekend certificaat.
2. Voeg het certificaat en de privésleutel toe aan elke VA.

3. Zorg ervoor dat het basiscertificaat en de tussenliggende moedercertificaten voor elk VA-certificaat (of VA-certificaat met zelfondertekening) zijn geïnstalleerd op elk systeem waarop de AD-connector wordt uitgevoerd op dezelfde locatie als de VA en op elke Chromebook.
 4. Schakel tijdens downtime-uren HTTPS in op de VA.
-



Opmerking: het certificaat op de VA moet worden vervangen voordat het verloopt en de tussenliggende ouder- en rootcertificaten moeten worden geïnstalleerd op de AD Connector- en Umbrella Chromebook-clients. Als dit niet gebeurt, kunnen de AD Connector en Umbrella Chromebook Clients niet communiceren met de VA.

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.