

Cisco Business Dashboard - Vaak gestelde vragen

Doel

Cisco Business Dashboard Network Management is software waarmee u uw gehele netwerk, inclusief uw Cisco-apparaten, eenvoudig kunt beheren via uw webbrowser. Het ontdekt, controleert, en vormt automatisch alle ondersteunde apparaten van Cisco in uw netwerk. Deze software stuurt u ook meldingen over firmware updates en informatie over de apparaten in uw netwerk die niet langer door garantie ondersteund worden.

Dit artikel bevat de antwoorden op vaak gestelde vragen bij het opzetten, configureren en oplossen van Cisco Business Dashboard Network Management.

Veelgestelde vragen

Inhoud

Algemeen

1. [Welke talen worden ondersteund door Cisco Business Dashboard Network Management?](#)

ontdekking

2. [Welke protocollen gebruikt Cisco Business Dashboard om mijn apparaten te beheren?](#)
3. [Hoe ontdekt Cisco Business Dashboard mijn netwerk?](#)
4. [Doet Cisco Business Dashboard netwerkscans?](#)

Configuratie

5. [Wat gebeurt er wanneer een nieuw apparaat wordt ontdekt? Zal de configuratie worden gewijzigd?](#)
6. [Wat gebeurt er als ik een apparaat van de ene naar de andere apparaatgroep verplaats?](#)

Veiligheidsoverwegingen

7. [Welke poortbereiken en -protocollen worden door Cisco Business Dashboard Network Manager vereist?](#)
8. [Welke poortbereiken en -protocollen worden door Cisco Business Dashboard Network Probe vereist?](#)
9. [Hoe veilig is de communicatie tussen Cisco Business Dashboard en Cisco Business Dashboard Probe?](#)
10. [Heeft Cisco Business Dashboard 'achterdeur' toegang tot mijn apparaten?](#)

11. [Hoe veilig zijn de aanmeldingsgegevens die in Cisco Business Dashboard worden opgeslagen?](#)
12. [Hoe herstel ik een verloren wachtwoord voor de Web User Interface \(UI\)?](#)
13. [Wat is de standaardgebruikersnaam en -wachtwoord voor de virtuele machine-lader?](#)

Externe toegang

14. [Wanneer ik verbinding maak met het web UI van een apparaat van Cisco Business Dashboard Network Management, is de sessie veilig?](#)
15. [Waarom logt mijn afstandstoegangssessie met een apparaat onmiddellijk uit als ik een externe toegangssessie naar een ander apparaat open?](#)
16. [Waarom faalt mijn afstandstoegangssessie met een fout als: Toegangsfout: Entiteit te groot aanvragen, HTTP-headerveld groter dan ondersteunde grootte?](#)

Software update

17. [Hoe houd ik het Dashboard-besturingssysteem op de hoogte?](#)
18. [Hoe update ik Java op het Dashboard?](#)
19. [Hoe houd ik het Sonde-besturingssysteem op de hoogte?](#)
20. [Hoe houd ik het Som-besturingssysteem bij wanneer ik een Raspberry Pi gebruik?](#)

Algemeen

[1. Welke talen worden ondersteund door Cisco Business Dashboard Network Management?](#)

Cisco Business Dashboard Network Management wordt vertaald in de volgende talen:

- Chinees
- Engels
- Frans
- Duits
- Japans
- Spaans

ontdekking

[2. Welke protocollen gebruikt Cisco Business Dashboard om mijn apparaten te beheren?](#)

Cisco Business Dashboard gebruikt een verscheidenheid aan protocollen om het netwerk te ontdekken en te beheren. Het exacte protocol dat voor een bepaald apparaat wordt gebruikt, varieert afhankelijk van het type apparaat. Deze protocollen omvatten:

- Multicast Domain Name System (mDNS) en DNS-servicedetectie — Dit protocol wordt ook bekend als Bonjour. Het lokaliseert apparaten zoals printers, andere computers, en de services die deze apparaten op een lokaal netwerk aanbieden. Klik [hier](#) voor meer informatie

over mDNS. Klik [hier](#) voor meer informatie over DNS-servicedetectie.

- Cisco Discovery Protocol (CDP) - een eigen Cisco-protocol dat wordt gebruikt om informatie te delen over andere rechtstreeks aangesloten Cisco-apparatuur, zoals de versie van het besturingssysteem en IP-adres.
- Link Layer Discovery Protocol (LLDP) — een verkoopneutraal protocol dat wordt gebruikt om informatie te delen over andere rechtstreeks aangesloten apparatuur, zoals de versie van het besturingssysteem en het IP-adres.
- Simple Network Management Protocol (SNMP) - een netwerkbeheerprotocol dat wordt gebruikt voor het verzamelen van informatie en het configureren van netwerkapparaten zoals servers, printers, knooppunten, switches en routers op een IP-netwerk (Internet Protocol).
- RESTCONF — Een ontwerp van de Internet Engineering Task Force (IETF) die beschrijft hoe een ABBYY-gegevensmodellering van de volgende generatie (YANG) op een RESTful-interface in kaart moet worden gebracht. Klik [hier](#) voor meer informatie.

[3. Hoe ontdekt Cisco Business Dashboard mijn netwerk?](#)

De Cisco Business Dashboard Probe bouwt een eerste lijst van apparaten in het netwerk van het luisteren naar CDP, LLDP, en mDNS advertenties. De sonde sluit dan aan op elk apparaat dat een ondersteund protocol gebruikt en verzamelt extra informatie zoals CDP en LDP nabijheidstabellen, Media Access Control (MAC) adrestabellen en bijbehorende apparaatlijsten. Deze informatie wordt gebruikt om extra apparaten in het netwerk te identificeren, en het proces herhaalt tot alle apparaten zijn ontdekt.

[4. Doet Cisco Business Dashboard netwerkscans?](#)

Cisco Business Dashboard scant het bredere netwerk niet actief. De sonde zal het ARP protocol gebruiken om IP te scannen en het is direct aangesloten op, maar zal geen andere adresbereik proberen te scannen. De sonde zal ook elk ontdekt apparaat testen op de aanwezigheid van een webserver en SNMP server op de standaardpoorten.

Configuratie

[5. Wat gebeurt er wanneer een nieuw apparaat wordt ontdekt? Zal de configuratie worden gewijzigd?](#)

Nieuwe apparaten zullen worden toegevoegd aan de standaardinstelling van het apparaat. Als de configuratieprofielen zijn toegewezen aan de standaardapparatengroep, dan zal die configuratie ook op pas ontdekte apparaten worden toegepast.

[6. Wat gebeurt er als ik een apparaat van de ene naar de andere apparaatgroep verplaats?](#)

Alle Virtual Local Area Network (VLAN) of Wireless Local Area Network (WLAN) configuratie die is gekoppeld aan profielen die momenteel op de oorspronkelijke apparaatgroep worden toegepast en niet op de nieuwe apparaatgroep worden toegepast, wordt verwijderd en VLAN of WLAN-configuratie die wordt gekoppeld aan profielen die worden toegepast op de nieuwe groep en niet worden toegepast op de oorspronkelijke groep, wordt aan het apparaat toegevoegd. De instellingen voor de systeemconfiguratie worden overschreven door profielen die op de nieuwe groep worden toegepast. Als er geen systeemconfiguratieprofielen zijn gedefinieerd voor de nieuwe groep, dan zal de systeemconfiguratie voor het apparaat niet veranderen.

Veiligheidsoverweging

7. Welke poortbereik en -protocollen worden door Cisco Business Dashboard Network Manager vereist?

De volgende tabel bevat de protocollen en poorten die door Cisco Business Dashboard worden gebruikt:

Port	Richting	Protocol	Gebruik
TCP 22	Inkomend	SSH	Opdrachtlijn toegang tot het dashboard. SSH wordt standaard uitgeschakeld aan de hand van het Cisco-beeld van de virtuele machine.
TCP 80	Inkomend	HTTP	Web toegang tot het dashboard.
TCP 443	Inkomend	HTTPS multiplexing TCP	Omleidingen naar beveiligde webserver (poort 443). Beveiligde toegang via internet tot Dashboard. Communicatie tussen Probe en Dashboard.
TCP 5000-51000	Inkomend	HTTPS	Externe toegang tot apparaten.
TCP 53	Uitgaand	DNS	Domain Name Solutions.
UDP 123	Uitgaand	NTP	Tijd-synchronisatie.
TCP 443	Uitgaand	HTTPS	Toegang tot Cisco-webservices voor informatie zoals softwareupdates, ondersteuningsstatus en end-of-life meldingen. Toegang tot OS- en toepassingsupdate-services.
UDP 5353	Uitgaand	mDNS	Multicast DNS-servicerespots voor lokaal netwerk dat adverteert met de Manager

8. Welke poortbereiken en protocollen worden door Cisco Business Dashboard Probe vereist?

De volgende tabel toont de protocollen en poorten die door Cisco Business Dashboard Probe worden gebruikt:

Port	Richting	Protocol	Gebruik
TCP 22	Inkomend	SSH	Opdracht-lijn toegang tot sonde. SSH wordt standaard uitgeschakeld aan de hand van het Cisco-beeld van de virtuele machine.
TCP 80	Inkomend	HTTP	Webtoegang tot Probe. Omleidingen naar beveiligde webserver (poort 443)
TCP 443	Inkomend	HTTPS	Beveiliging van webtoegang tot Probe.
UDP 5353	Inkomend	mDNS	Multicast DNS-servicerespots via het lokale netwerk. Gebruikt voor apparaatontdekking.
UDP 53	Uitgaand	DNS	Resolutie van domeinnaam
UDP 123	Uitgaand	NTP	Tijdsynchronisatie
TCP 80	Uitgaand	HTTP	Beheer van apparaten zonder beveiligde webdiensten.
UDP 161	Uitgaand	SNMP	Beheer van netwerkapparaten
TCP 443	Uitgaand	HTTPS multiplexing	Beheer van apparaten met beveiligde webdiensten. Toegang tot Cisco-webservices voor informatie

		zoals softwareupdates, ondersteuningsstatus en end-of-life meldingen.
	TCP	Toegang tot OS- en toepassingsupdate-services.
		Communicatie tussen Probe en Dashboard.
UDP 5353	Uitgaand mDNS	Multicast DNS-serviceresources voor het lokale netwerk dat de Probe aanmaakt.

[9. Hoe veilig is de communicatie tussen Cisco Business Dashboard Network Manager en Cisco Business Dashboard Probe?](#)

Alle communicatie tussen het Dashboard en de Probe wordt versleuteld met een TLS 1.2 sessie die is geauthentiseerd met client- en servercertificaten. De sessie wordt gestart vanuit de sonde naar het dashboard. Op het moment dat de associatie tussen het Dashboard en de Probe wordt ingesteld, moet de gebruiker zich via de Probe aanmelden op het Dashboard.

[10. Heeft Cisco Business Dashboard 'achterdeur' toegang tot mijn apparaten?](#)

Nee. Wanneer Cisco Business Dashboard een ondersteund Cisco-apparaat ontdekt, zal het proberen om het apparaat te benaderen met de standaard fabrieksreferenties voor dat apparaat met de standaard gebruikersnaam en het wachtwoord: *Cisco*, of de standaard SNMP-gemeenschap: *openbaar*. Als de apparaatconfiguratie is gewijzigd van de standaardinstelling, dan is het voor de gebruiker nodig om juiste aanmeldingsgegevens aan Cisco Business Dashboard te leveren.

[11. Hoe veilig zijn de aanmeldingsgegevens die in Cisco Business Dashboard worden opgeslagen?](#)

Credentials voor toegang tot Cisco Business Dashboard worden onomkeerbaar gehashed met behulp van het SHA512-algoritme. Credentials voor apparaten en andere services, zoals de **Cisco Active Adviseur** van **Cisco**, worden reversibel versleuteld met het AES-128-algoritme.

[12. Hoe herstel ik een verloren wachtwoord voor de Web User Interface \(UI\)?](#)

Als u het wachtwoord voor alle Admin-rekeningen in Web UI hebt verloren, kunt u het wachtwoord herstellen door te loggen op de console van de sonde en het gereedschap om **cbdprobe te herstellen**, of door te loggen op de console van de sonde en het **cisco-business-dashboard herstellingwachtwoord** uit te voeren. Dit gereedschap stelt het wachtwoord voor de cisco-account in op de standaard cisco-account of, als de cisco-account is verwijderd, wordt de account met het defaultwachtwoord opnieuw gecreëerd. Hieronder vindt u een voorbeeld van de opdrachten die moeten worden geleverd om het wachtwoord opnieuw in te stellen met behulp van dit gereedschap.

```
cisco@cisco-business-dashboard:~cisco-business-dashboard terugwinningswachtwoord Weet je het zeker? (y/n) y Het defaultwachtwoord van de cisco-account hersteld Wachtwoord voor Cisco Business Dashboard herstellen! cisco@Cisco Business DashboardProbe:~$
```

Wanneer u Cisco Business Dashboard voor AWS gebruikt, wordt het wachtwoord ingesteld op de AWS-exemplaar.

13. Wat is de standaardgebruikersnaam en het wachtwoord voor de virtuele machine-lader?

De standaardaanmeldingsgegevens voor de virtuele machine bootloader zijn gebruikersnaam:

wortel en wachtwoord: **Cisco**. Deze kunnen worden gewijzigd door het bestand te gebruiken en ja te antwoorden als u het bootloader-wachtwoord wilt wijzigen.

Externe toegang

14. Wanneer ik verbinding maak met het web UI van een apparaat van Cisco Business Dashboard Network Management, is de sessie veilig?

Cisco Business Dashboard tunnels de externe toegangssessie tussen het apparaat en de gebruiker. Het protocol dat tussen de sonde en het apparaat wordt gebruikt, hangt af van de configuratie van het eindapparaat, maar Cisco Business Dashboard zal altijd de sessie instellen met een beveiligd protocol als er een is geactiveerd (bijvoorbeeld HTTPS wordt voorkeur boven HTTP). Als de gebruiker verbinding maakt met het apparaat via het Dashboard, zal de sessie door een versleutelde tunnel gaan terwijl deze tussen het Dashboard en de Probe passeert, ongeacht de protocollen die op het apparaat zijn ingeschakeld. De verbinding tussen de webbrowser van de gebruiker en het Dashboard zal altijd HTTPS zijn.

[15. Waarom logt mijn afstandstoegangssessie met een apparaat onmiddellijk uit als ik een externe toegangssessie naar een ander apparaat open?](#)

Wanneer u toegang hebt tot een apparaat via Cisco Business Dashboard, ziet de browser elke verbinding als zijnde met dezelfde webserver (het Dashboard) en geeft deze dus koekjes van elk apparaat aan elk ander apparaat. Als meerdere apparaten dezelfde koekjesnaam gebruiken, dan is er de mogelijkheid dat het koekje van een toestel overschreven wordt door een ander apparaat. Dit wordt het vaakst gezien bij sessiekoekjes, en het resultaat is dat het koekje alleen geldig is voor het meest recent bezochte apparaat. Alle andere apparaten die dezelfde koekjesnaam gebruiken zullen het koekje als ongeldig zien en zullen uit de sessie loggen.

[16. Waarom faalt mijn externe toegangssessie met een fout als: Toegangsfout: Entiteit te groot aanvragen, HTTP-headerveld groter dan ondersteunde grootte?](#)

Nadat u veel externe toegangssessies met verschillende apparaten hebt uitgevoerd, zal de browser een groot aantal koekjes hebben opgeslagen voor het Dashboard domein. Om rond dit probleem te werken, gebruikt u de knoppen van de browser om koekjes voor het domein te verwijderen en dan de pagina opnieuw te laden.

Software update

[17. Hoe kan ik het Dashboard-besturingssysteem op de hoogte houden?](#)

Het Dashboard gebruikt de Ubuntu Linux distributie voor een besturingssysteem. De pakketten en de kern kunnen worden bijgewerkt met behulp van de standaard Ubuntu-processen. Om bijvoorbeeld een handmatige update uit te voeren, logt u in op de console als Cisco-gebruiker en voert u de opdrachten in:

```
aanpasbare update en aanpasbare upgrade uitvoeren
```

Het systeem mag niet worden opgewaardeerd tot een nieuwe Ubuntu-release en aanbevolen wordt om geen extra pakketten te installeren die verder gaan dan de pakketten die zijn meegeleverd in de virtuele machine-afbeelding van Cisco of de pakketten die zijn geïnstalleerd als onderdeel van een minimale Ubuntu-installatie.

[18. Hoe update ik Java op het Dashboard?](#)

Cisco Business Dashboard gebruikt de OpenJDK-pakketten van de Ubuntu-schappen. OpenJDK wordt automatisch bijgewerkt als onderdeel van het bijwerken van het kernbesturingssysteem.

[19. Hoe hou ik het besturingssysteem van de Probe bij?](#)

Cisco Business Dashboard gebruikt de Ubuntu Linux-distributie voor een besturingssysteem. De pakketten en de kern kunnen worden bijgewerkt met behulp van de standaard Ubuntu-processen. Om bijvoorbeeld een handmatige update uit te voeren, logt u in op de console als Cisco-gebruiker en voert u de opdrachten in:

```
aanpassen
```

```
en
```

```
stap voor stap
```

Het systeem mag niet worden opgewaardeerd tot een nieuwe Ubuntu-release en aanbevolen wordt om geen extra pakketten te installeren die verder gaan dan de pakketten die zijn meegeleverd in de virtuele machine-afbeelding van Cisco of de pakketten die zijn geïnstalleerd als onderdeel van een minimale Ubuntu-installatie.

[20. Hoe kan ik het Probe-besturingssysteem op de hoogte houden wanneer ik een Raspberry Pi gebruik?](#)

De rackpakketten en splitsingen kunnen worden bijgewerkt met behulp van de standaardprocessen die gebruikt worden voor Linux-distributies op basis van Servië. Om bijvoorbeeld een handmatige update uit te voeren, logt u in op de console als Cisco-gebruiker en voert u de opdrachten in:

```
aanpassen
```

```
en
```

```
stap voor stap
```

Het systeem mag niet worden opgewaardeerd tot een nieuwe grootschalige release van Raspbian. Aanbevolen wordt dat er geen extra pakketten worden geïnstalleerd, behalve die welke zijn geïnstalleerd als onderdeel van de "Lite" versie van de Raspbian-distributie en die welke door de installateur van de Probe worden toegevoegd.