

# Domande frequenti su Cisco Business Dashboard

## Obiettivo

Cisco Business Dashboard Network Management è un software che consente di gestire facilmente l'intera rete, inclusi i dispositivi Cisco, tramite il browser Web. Individua, controlla e configura automaticamente tutti i dispositivi Cisco supportati nella rete. Questo software invia inoltre notifiche sugli aggiornamenti del firmware e informazioni sui dispositivi della rete non più supportati dalla garanzia.

In questo articolo vengono fornite le risposte alle domande frequenti relative all'impostazione, alla configurazione e alla risoluzione dei problemi di Cisco Business Dashboard Network Management.

## Domande frequenti

### Sommario

#### Generale

1. [Quali lingue sono supportate da Cisco Business Dashboard Network Management?](#)

#### Individuazione

2. [Quali protocolli usa Cisco Business Dashboard per gestire i miei dispositivi?](#)
3. [In che modo Cisco Business Dashboard rileva la rete?](#)
4. [Cisco Business Dashboard esegue scansioni di rete?](#)

#### Configurazione

5. [Cosa succede quando viene individuato un nuovo dispositivo? La configurazione verrà modificata?](#)
6. [Cosa succede quando si sposta un dispositivo da un gruppo di dispositivi a un altro?](#)

#### Considerazioni sulla sicurezza

7. [Quali intervalli di porte e protocolli sono richiesti da Cisco Business Dashboard Network Manager?](#)
8. [Quali intervalli di porte e protocolli sono richiesti da Cisco Business Dashboard Network Probe?](#)
9. [Quanto è sicura la comunicazione tra Cisco Business Dashboard e Cisco Business Dashboard Probe?](#)
10. [Cisco Business Dashboard ha accesso tramite 'backdoor' ai miei dispositivi?](#)

11. [Quanto sono sicure le credenziali archiviate in Cisco Business Dashboard?](#)
12. [Come recuperare una password persa per l'interfaccia utente Web?](#)
13. [Quali sono il nome utente e la password predefiniti per il bootloader della macchina virtuale?](#)

## Accesso remoto

14. [Quando mi connetto all'interfaccia utente Web di un dispositivo da Cisco Business Dashboard Network Management, la sessione è sicura?](#)
15. [Perché la sessione di accesso remoto con un dispositivo si disconnette immediatamente quando si apre una sessione di accesso remoto a un altro dispositivo?](#)
16. [Perché la sessione di accesso remoto non riesce con un errore simile al seguente: Errore di accesso: Entità richiesta troppo grande. Il campo dell'intestazione HTTP supera le dimensioni supportate.](#)

## Aggiornamento software

17. [Come è possibile mantenere aggiornato il sistema operativo del dashboard?](#)
18. [Come posso aggiornare Java sul dashboard?](#)
19. [Come è possibile mantenere aggiornato il sistema operativo Probe?](#)
20. [Come posso mantenere aggiornato il sistema operativo Probe quando uso un Raspberry Pi?](#)

## Generale

1. [Quali lingue sono supportate da Cisco Business Dashboard Network Management?](#)

Cisco Business Dashboard Network Management è tradotto nelle seguenti lingue:

- Cinese
- Inglese
- Francese
- Tedesco
- Giapponese
- Spagnolo

## Individuazione

2. [Quali protocolli utilizza Cisco Business Dashboard per gestire i dispositivi?](#)

Cisco Business Dashboard utilizza una varietà di protocolli per individuare e gestire la rete. Il protocollo esatto utilizzato per un determinato dispositivo varia a seconda del tipo di dispositivo. Tali protocolli includono:

- Multicast Domain Name System (mDNS) e individuazione servizio DNS: questo protocollo è noto anche come Bonjour. Consente di individuare dispositivi quali stampanti, altri computer e i servizi offerti da tali dispositivi in una rete locale. Per ulteriori informazioni su mDNS, fare clic

- [qui](#). Per ulteriori informazioni sull'individuazione dei servizi DNS, fare clic [qui](#).
- Cisco Discovery Protocol (CDP): protocollo proprietario di Cisco utilizzato per condividere informazioni su altre apparecchiature Cisco a connessione diretta, come la versione del sistema operativo e l'indirizzo IP.
  - LLDP (Link Layer Discovery Protocol): protocollo indipendente dal fornitore utilizzato per condividere informazioni su altre apparecchiature collegate direttamente, ad esempio la versione del sistema operativo e l'indirizzo IP.
  - SNMP (Simple Network Management Protocol): protocollo di gestione di rete utilizzato per la raccolta di informazioni e la configurazione di dispositivi di rete quali server, stampanti, hub, switch e router in una rete IP (Internet Protocol).
  - RESTCONF — Bozza di IETF (Internet Engineering Task Force) che descrive come mappare una specifica del linguaggio di modellazione dei dati YANG (Another Next Generation) a un'interfaccia RESTful. Per ulteriori informazioni, fare clic [qui](#).

### [3. In che modo Cisco Business Dashboard rileva la rete?](#)

Cisco Business Dashboard Probe crea un elenco iniziale di dispositivi nella rete dall'ascolto di annunci CDP, LLDP e mDNS. La sonda si connette quindi a ciascun dispositivo utilizzando un protocollo supportato e raccoglie informazioni aggiuntive quali tabelle adiacenti CDP e LLDP, tabelle indirizzi MAC (Media Access Control) ed elenchi di dispositivi associati. Queste informazioni vengono utilizzate per identificare ulteriori dispositivi nella rete e il processo si ripete finché non vengono individuati tutti i dispositivi.

### [4. Cisco Business Dashboard esegue scansioni di rete?](#)

Cisco Business Dashboard non esegue la scansione attiva della rete più ampia. La sonda utilizzerà il protocollo ARP per analizzare la subnet IP a cui è collegata direttamente, ma non tenterà di analizzare altri intervalli di indirizzi. La sonda verificherà inoltre la presenza di un server Web e di un server SNMP sulle porte standard di ciascun dispositivo rilevato.

## Configurazione

### [5. Cosa succede quando viene individuato un nuovo dispositivo? La configurazione verrà modificata?](#)

Le nuove periferiche verranno aggiunte al gruppo di periferiche predefinito. Se i profili di configurazione sono stati assegnati al gruppo di dispositivi predefinito, la configurazione verrà applicata anche ai nuovi dispositivi individuati.

### [6. Cosa succede quando si sposta un dispositivo da un gruppo di dispositivi a un altro?](#)

Qualsiasi configurazione di VLAN (Virtual Local Area Network) o WLAN (Wireless Local Area Network) associata ai profili attualmente applicati al gruppo di dispositivi originale e non al nuovo gruppo di dispositivi verrà rimossa e la configurazione VLAN o WLAN associata ai profili applicati al nuovo gruppo e non al gruppo originale verrà aggiunta al dispositivo. Le impostazioni di configurazione del sistema verranno sovrascritte dai profili applicati al nuovo gruppo. Se per il nuovo gruppo non sono stati definiti profili di configurazione del sistema, la configurazione del sistema per il dispositivo non verrà modificata.

## Considerazioni sulla sicurezza

### [7. Quali intervalli di porte e protocolli sono richiesti da Cisco Business Dashboard Network](#)

## [Manager?](#)

Nella tabella seguente sono riportati i protocolli e le porte utilizzati da Cisco Business Dashboard:

Port	Direzione	Protocollo	Utilizzo
TCP 22	In entrata	SSH	Accesso al dashboard dalla riga di comando. SSH è disabilitato per impostazione predefinita sull'immagine della macchina virtuale Cisco.
TCP 80	In entrata	HTTP	Accesso Web al dashboard. Reindirizza al server Web protetto (porta 443).
TCP 443	In entrata	HTTPS Multiplexed TCP	Accesso Web sicuro al dashboard. Comunicazione tra probe e dashboard.
TCP 5000 -	In entrata	HTTPS	Accesso remoto ai dispositivi.
5100 TCP 53	In uscita	DNS	Risoluzione dei nomi di dominio.
UDP 123	In uscita	NTP	Sincronizzazione dell'ora.
TCP 443	In uscita	HTTPS	Accedere ai servizi Web Cisco per informazioni come aggiornamenti software, stato del supporto e avvisi di fine ciclo di vita. Accedere ai servizi di aggiornamento del sistema operativo e delle applicazioni.
UDP 5353	In uscita	mDNS	Annunci del servizio DNS multicast alla rete locale per l'annuncio di Manager

## [8. Quali intervalli di porte e protocolli sono richiesti da Cisco Business Dashboard Probe?](#)

Nella tabella seguente vengono elencati i protocolli e le porte utilizzati da Cisco Business Dashboard Probe:

Port	Direzione	Protocollo	Utilizzo
TCP 22	In entrata	SSH	Accesso al probe dalla riga di comando. SSH è disabilitato per impostazione predefinita sull'immagine della macchina virtuale Cisco.
TCP 80	In entrata	HTTP	Accesso Web a Probe. Reindirizzamento a un server Web protetto (porta 443)
TCP 443	In entrata	HTTPS	Accesso Web sicuro al probe.
UDP 5353	In entrata	mDNS	Annunci servizio DNS multicast dalla rete locale. Utilizzato per l'individuazione dei dispositivi.
UDP 53	In uscita	DNS	Risoluzione dei nomi di dominio
UDP 123	In uscita	NTP	Sincronizzazione ora
TCP 80	In uscita	HTTP	Gestione dei dispositivi senza servizi Web sicuri abilitati.
UDP 161	In uscita	SNMP	Gestione dei dispositivi di rete
TCP 443	In uscita	HTTPS Multiplexed	Gestione dei dispositivi con servizi Web protetti abilitati. Accedere ai servizi Web Cisco per

		informazioni come aggiornamenti software, stato del supporto e avvisi di fine ciclo di vita.
	TCP	Accedere ai servizi di aggiornamento del sistema operativo e delle applicazioni. Comunicazione tra probe e dashboard.
UDP 5353	In uscita mDNS	Annunci del servizio DNS multicast alla rete locale che annunciano la sonda.

## [9. Quanto è sicura la comunicazione tra Cisco Business Dashboard Network Manager e Cisco Business Dashboard Probe?](#)

Tutte le comunicazioni tra il dashboard e la sonda vengono crittografate utilizzando una sessione TLS 1.2 autenticata con certificati client e server. La sessione viene avviata dalla sonda al dashboard. Quando viene stabilita l'associazione tra il dashboard e il probe, l'utente deve accedere al dashboard tramite il probe.

## [10. Cisco Business Dashboard ha accesso tramite 'backdoor' ai miei dispositivi?](#)

No. Quando Cisco Business Dashboard rileva un dispositivo Cisco supportato, tenterà di accedere al dispositivo utilizzando le credenziali predefinite di fabbrica per il dispositivo con il nome utente e la password predefiniti: *cisco* o la community SNMP predefinita: *public*. Se la configurazione del dispositivo è stata modificata rispetto a quella predefinita, sarà necessario che l'utente fornisca le credenziali corrette a Cisco Business Dashboard.

## [11. Quanto sono sicure le credenziali archiviate in Cisco Business Dashboard?](#)

L'hash delle credenziali per l'accesso a Cisco Business Dashboard viene eseguito in modo irreversibile utilizzando l'algoritmo SHA512. Le credenziali dei dispositivi e di altri servizi, ad esempio **Cisco Active Advisor**, vengono crittografate in modo reversibile utilizzando l'algoritmo AES-128.

## [12. Come è possibile recuperare una password persa per l'interfaccia utente Web?](#)

Se la password di tutti gli account admin è stata persa nell'interfaccia utente Web, è possibile reimpostarla accedendo alla console della sonda ed eseguendo lo strumento **cbdprobe recoverpassword** oppure accedendo alla console della sonda ed eseguendo lo **strumento di recupero password cisco-business-dashboard**. Questo strumento reimposta la password predefinita dell'account cisco o, se l'account cisco è stato rimosso, lo ricreerà con la password predefinita. Di seguito è riportato un esempio dei comandi da fornire per reimpostare la password utilizzando questo strumento.

```
cisco@cisco-business-dashboard:~$ password di ripristino di cisco-business-dashboard Sei sicuro?
(s/n) s Recupero dell'account cisco tramite password predefinita completato recoverpassword Cisco
Business Dashboard riuscito! cisco@Cisco Business DashboardProbe:~$
```

Quando si utilizza Cisco Business Dashboard per AWS, la password verrà impostata sull'ID istanza AWS.

## 13. Quali sono il nome utente e la password predefiniti per il bootloader della macchina virtuale?

Le credenziali predefinite per il bootloader della macchina virtuale sono nome utente: **root** e password: **cisco**. Per modificare le password, eseguire lo strumento `config_vm` e rispondere sì alla

richiesta di modifica della password del bootloader.

## Accesso remoto

14. La sessione è sicura quando ci si connette all'interfaccia utente Web di un dispositivo da Cisco Business Dashboard Network Management?

Cisco Business Dashboard esegue il tunnel della sessione di accesso remoto tra il dispositivo e l'utente. Il protocollo utilizzato tra il probe e il dispositivo dipenderà dalla configurazione del dispositivo terminale, ma Cisco Business Dashboard stabilirà sempre la sessione utilizzando un protocollo sicuro, se abilitato (ad esempio, HTTPS verrà preferito a HTTP). Se l'utente si connette al dispositivo tramite il dashboard, la sessione passerà attraverso un tunnel crittografato mentre passa tra il dashboard e la sonda, indipendentemente dai protocolli abilitati sul dispositivo. La connessione tra il browser Web dell'utente e il dashboard sarà sempre HTTPS.

[15. Perché la sessione di accesso remoto con un dispositivo si disconnette immediatamente quando si apre una sessione di accesso remoto su un altro dispositivo?](#)

Quando si accede a un dispositivo tramite Cisco Business Dashboard, il browser vede ogni connessione come se fosse con lo stesso server Web (il Dashboard) e quindi presenta i cookie da ogni dispositivo a ogni altro dispositivo. Se più dispositivi utilizzano lo stesso nome cookie, esiste la possibilità che il cookie di un dispositivo venga sovrascritto da un altro dispositivo. Ciò si verifica più spesso con i cookie di sessione e il risultato è che il cookie è valido solo per il dispositivo visitato più di recente. Tutti gli altri dispositivi che utilizzano lo stesso nome cookie vedranno il cookie come non valido e si disconetteranno dalla sessione.

[16. Perché la sessione di accesso remoto non riesce con un errore simile al seguente: \*\*Errore di accesso: Entità richiesta troppo grande. Il campo dell'intestazione HTTP supera le dimensioni supportate?\*\*](#)

Dopo aver eseguito molte sessioni di accesso remoto con dispositivi diversi, il browser disporrà di un numero elevato di cookie memorizzati per il dominio del dashboard. Per risolvere il problema, utilizzare i controlli del browser per cancellare i cookie per il dominio e quindi ricaricare la pagina.

## Aggiornamento software

[17. Come è possibile mantenere aggiornato il sistema operativo del dashboard?](#)

Il dashboard utilizza la distribuzione Ubuntu Linux per un sistema operativo. I pacchetti e il kernel possono essere aggiornati utilizzando i processi Ubuntu standard. Ad esempio, per eseguire un aggiornamento manuale, accedere alla console come utente cisco e immettere i comandi:

```
aggiornamento sudo apt-get e aggiornamento sudo apt-get
```

Il sistema non deve essere aggiornato a una nuova versione di Ubuntu ed è consigliabile non installare pacchetti aggiuntivi oltre a quelli inclusi nell'immagine della macchina virtuale fornita da Cisco o quelli installati come parte di un'installazione minima di Ubuntu.

[18. Come è possibile aggiornare Java nel dashboard?](#)

Cisco Business Dashboard utilizza i pacchetti OpenJDK dei repository Ubuntu. OpenJDK verrà aggiornato automaticamente durante l'aggiornamento del sistema operativo principale.

[19. Come è possibile mantenere aggiornato il sistema operativo Probe?](#)

Cisco Business Dashboard utilizza la distribuzione Ubuntu Linux per un sistema operativo. I pacchetti e il kernel possono essere aggiornati utilizzando i processi Ubuntu standard. Ad esempio, per eseguire un aggiornamento manuale, accedere alla console come utente cisco e immettere i comandi:

```
aggiornamento sudo apt-get
```

e

```
aggiornamento sudo apt-get
```

Il sistema non deve essere aggiornato a una nuova versione di Ubuntu ed è consigliabile non installare pacchetti aggiuntivi oltre a quelli inclusi nell'immagine della macchina virtuale fornita da Cisco o quelli installati come parte di un'installazione minima di Ubuntu.

## [20. Come posso mantenere aggiornato il sistema operativo Probe quando uso un Raspberry Pi?](#)

I pacchetti e il kernel Raspbian possono essere aggiornati usando i processi standard usati per le distribuzioni Linux basate su Debian. Ad esempio, per eseguire un aggiornamento manuale, accedere alla console come utente cisco e immettere i comandi:

```
aggiornamento sudo apt-get
```

e

```
aggiornamento sudo apt-get
```

Il sistema non dovrebbe essere aggiornato a una nuova versione principale di Raspbian. Si consiglia di non installare ulteriori pacchetti oltre a quelli installati come parte della versione 'Lite' della distribuzione Raspbian e quelli che vengono aggiunti dal programma di installazione Probe.