# Risoluzione dei problemi relativi agli utenti di Active Directory mancanti nel report di ricerca attività in Umbrella

## Sommario



## Introduzione

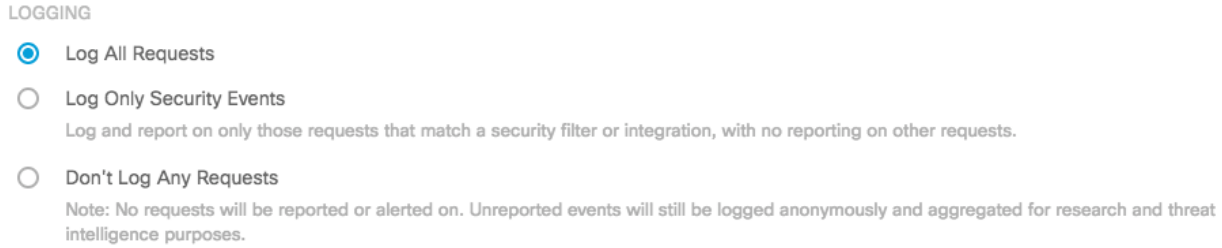
Questo documento descrive il report di ricerca attività in Cisco Umbrella. Il report di ricerca attività è un report quasi attivo di tutte le query DNS eseguite dagli utenti. Se è stata configurata l'integrazione di Cisco Umbrella Active Directory (AD), è possibile prevedere che gli utenti di AD popolino la colonna Identità nella ricerca attività. In alcuni casi, tuttavia, gli utenti non sono presenti nella colonna Identità.

## Risoluzione

Se si ritiene che gli utenti AD dovrebbero essere visualizzati direttamente nella colonna Identità in Ricerca attività, ma non sono visualizzati, oppure se ne vedono alcuni, ma non il numero previsto, di seguito sono riportati alcuni elementi da verificare:

1. Siti e Active Directory
    - Controllare tutti i componenti AD per verificare che non vi siano errori o problemi segnalati. Se su uno dei componenti vengono visualizzati indicatori di stato di colore grigio, arancione o rosso, ottenere questi dettagli e aprire una richiesta di assistenza (umbrella-support@cisco.com).
        - Test diagnostico da parte di un utente interessato (un utente non visualizzato in Ricerca attività)
        - Schermata della console dell'appliance virtuale (VA) con l'espansione di eventuali messaggi di errore
        - Registri di controllo connettore AD
2. Impostazioni registrazione
    - Nelle Impostazioni avanzate di ogni criterio, nella parte inferiore è presente una sezione relativa alla quantità da registrare. È possibile impostarlo su:
        - Registra tutte le richieste
        - Registra solo eventi di protezione
        - Non registrare richieste

- Se il criterio è attualmente impostato su "Registra solo eventi di protezione", ciò può spiegare perché non vengono visualizzate tutte le query previste o nessun risultato da alcuni utenti.




3. Correggi precedenza criteri
    - Se si applica un criterio a un'identità di rete superiore nell'elenco dei criteri rispetto al criterio utente di Active Directory, è probabile che il criterio venga applicato. Ciò significa che nella ricerca attività la rete verrà visualizzata come identità segnalata. Consulta anche la documentazione di Cisco Umbrella sulle best practice e la precedenza delle policy.

# Causa

## Dove la ricerca attività ottiene l'identità?

Quando una query DNS entra in Umbrella, supponendo che l'integrazione di AD funzioni come previsto, queste informazioni vengono passate nella query:

- Indirizzo IP interno
- Hash dell'identità AD (utente, host o entrambi)
- IP in uscita
- Dominio su cui viene eseguita la query

L'hash di identità AD viene aggiunto alla query dall'appliance virtuale, che riceve le informazioni, e dall'indirizzo IP interno corrispondente per l'evento di accesso dal connettore AD.

Cisco Umbrella quindi utilizza queste informazioni per trovare l'organizzazione e per determinare quale criterio applicare. Se non si dispone di criteri applicati in modo specifico agli utenti AD, ma ne esiste uno per le reti o i siti, Cisco Umbrella applica i criteri utilizzando quell'identità. Ciò significa che quando la query, l'identità e la risposta vengono segnalate in Ricerca attività, l'identità che ha attivato il criterio segnalato. Le altre informazioni sono ancora contrassegnate nella richiesta, quindi è ancora possibile cercare un utente AD e ottenere l'attività che segnala una rete come identità. Inoltre, se si esportano i dati di Ricerca attività in un file CSV, verranno visualizzate tutte le informazioni di identità associate alla query.

# Ulteriori informazioni

Se non si visualizzano ancora gli utenti AD, contattare il supporto tecnico (umbrella-support@cisco.com), con risultati dei test diagnostici e i registri di verifica del connettore AD pertinenti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).