

# Errore handshake TLS risorsa privata basata su browser ZTA

## Sommario

---

## Problema

Gli utenti non sono in grado di accedere a una risorsa privata basata su browser tramite Cisco Secure Access.

Durante il tentativo di connessione, si verificano i seguenti sintomi:

- L'handshake a tre vie TCP viene completato correttamente, ma la negoziazione TLS non riesce dopo il completamento del client.
- La connessione all'URL mappato SSE pubblico (<https://example-orgid.ztna.sse.cisco.io>) raggiunge l'autenticazione Cisco ma restituisce l'errore HTTP 404.
- Dopo aver aggiunto il nome di dominio completo (FQDN) alla configurazione della risorsa privata, il traffico reindirizza al prompt di autenticazione ma, dopo l'autenticazione, genera una pagina vuota.
- I file HAR mostrano le risposte HTTP 200, ma l'handshake TLS non viene completato.
- Il motivo del blocco viene visualizzato come: "Accesso privato: i dati di postura recuperati per il dispositivo sono troppo vecchi/devono essere aggiornati".

## Ambiente

- SSE (Cisco Secure Access)
- ID organizzazione accesso sicuro: xxxx
- Accesso di rete ZTNA (Zero Trust Network Access) basato su browser
- Risorsa privata: example.net

- Risorsa privata di lavoro per il confronto: abc.net
- Configurazione certificato con caratteri jolly

## Risoluzione

Il problema è stato risolto configurando la risorsa privata in modo che utilizzi la stessa configurazione del certificato di una risorsa privata funzionante.

Sono state intraprese le azioni descritte nelle sezioni seguenti.

### Passaggio 1: Analizza configurazione di lavoro

Confrontare la risorsa privata con errori (example.net) con una risorsa privata di lavoro (abc.net) per identificare le differenze di configurazione.

Risorsa di lavoro utilizzata:

- Usa un URL nel tuo dominio, opzione
- Riferimento alla coppia certificato/chiave jolly esistente

### Passaggio 2: Analisi acquisizione pacchetti

Eseguire l'analisi dell'acquisizione dei pacchetti utilizzando Wireshark per confermare l'errore dell'handshake TLS:

- Verifica del completamento dell'handshake a tre vie TCP.
- Conferma esito negativo della negoziazione TLS dopo l'esecuzione del client.
- Raccogli elementi di diagnostica: file HAR, bundle DART e acquisizioni di pacchetti.

## Passaggio 3: Verifica certificato

Accedere all'applicazione tramite la connessione RAVPN per verificare la presentazione del certificato:

- Confermare che il sito Web example.net presenta un certificato con caratteri jolly.
- Documentare i dettagli del certificato per il riferimento alla configurazione.

## Passaggio 4: Configura risorsa privata

Applicare lo stesso approccio alla configurazione utilizzato dalla risorsa privata di lavoro:

- Configurare la risorsa privata per l'utilizzo dell'opzione Usa un URL nel dominio.
- Fare riferimento alla coppia di chiavi/certificati jolly esistente.
- Verificare che il nome di dominio completo (FQDN) sia configurato correttamente nel campo delle risorse private.

## Passaggio 5: Convalida

Verificare l'accesso basato su browser per confermare la configurazione e risolvere il problema:

- Verificare il completamento dell'handshake TLS.
- Confermare il corretto flusso di autenticazione.
- Convalida l'accessibilità dell'applicazione dopo l'autenticazione.

## Causa

La causa principale è una mancata corrispondenza nella configurazione della risorsa privata. La risorsa privata con errori non è stata configurata per fare riferimento in modo corretto al certificato

con caratteri jolly presentato dall'applicazione di destinazione. Handshake TLS non riuscito. La configurazione della risorsa privata non è stata allineata alla configurazione del certificato utilizzata dal server applicazioni. Configurando la risorsa privata in modo che utilizzi l'opzione Use a URL in your domain (Usa un URL nel dominio) e facendo riferimento alla coppia certificato/chave jolly esistente (corrispondente alla configurazione di lavoro), la negoziazione TLS è stata completata correttamente.

## Contenuto correlato

- [Guida di riferimento Cisco per l'accesso sicuro](#)
- [Supporto tecnico Cisco e download](#)

### 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).