

# Gestione degli errori del certificato di decrittografia SSL in Secure Access

## Sommario

---

## Problema

Quando in Cisco Secure Access è abilitata la decrittografia SSL, si verificano pagine di errore relative ai certificati. Sono state ricevute più richieste relative a tre tipi specifici di errori di certificato:

- Errori di scadenza certificato server di origine
- Errori di mancata corrispondenza CN/SAN del certificato in cui il nome comune o i nomi alternativi del soggetto elencati nel certificato non corrispondono al dominio utilizzato
- Collegamento CRL incorporato nel certificato del server di origine che causa problemi di connettività

Questi errori relativi ai certificati sono simili agli avvisi che normalmente vengono visualizzati nei browser Web. Si pone la questione se Cisco Secure Access sia in grado di gestire gli errori relativi ai certificati visualizzando pagine di avviso (simili ai browser o ai filtri contenuti) e quindi consentendo l'accesso dopo la visualizzazione dell'avviso o consentendo l'accesso in tutti i casi. Inoltre, è necessario comprendere il comportamento quando la decrittografia SSL è disabilitata e se il traffico passa indipendentemente dai problemi del certificato.

## Ambiente

- Cisco Secure Access - Accesso a Internet (modulo roaming, VA, DNS, SWG, PAC, IPS, certificati)
- Funzionalità di decrittografia SSL abilitata
- Più domini con problemi di convalida del certificato
- Server di origine con vari problemi di certificato, tra cui scadenza e mancata corrispondenza

del dominio

## Risoluzione

### Limitazioni per la gestione degli errori dei certificati

La gestione degli errori relativi ai certificati non è disponibile in Cisco Secure Access. Il prodotto non supporta:

- Presentazione di pagine di avviso simili a browser per i problemi relativi ai certificati
- Configurazione di gestione degli errori dei certificati specifici del dominio
- Gestione personalizzata degli errori in base ai domini di destinazione
- Pagine di avviso in stile filtro contenuto con opzioni di sostituzione dell'utente

### Soluzione alternativa all'esclusione della decrittografia SSL

L'approccio consigliato consiste nell'escludere dalla decrittografia SSL i domini con problemi utilizzando le impostazioni di decrittografia del profilo di sicurezza. La configurazione può essere eseguita tramite:

Passare alla sezione Profilo sicurezza > Impostazioni decrittografia per escludere domini specifici dall'ispezione SSL.

Quando i domini vengono esclusi dalla decrittografia SSL, si verifica quanto segue:

- Il traffico per i domini esclusi ignora completamente l'ispezione SSL
- La convalida del certificato non viene eseguita da Secure Access
- Gli utenti non incontrano le pagine di errore dei certificati generate da Secure Access
- È possibile che gli errori del certificato originale siano ancora visibili nel browser se i problemi del certificato persistono

## Comportamento della decrittografia SSL disabilitato

Quando la decrittografia SSL è disabilitata per un dominio o a livello globale, Cisco Secure Access trasmette il traffico attraverso (inoltro) indipendentemente da eventuali problemi di certificato. Il prodotto non ispeziona né convalida i certificati quando la decrittografia non è abilitata, consentendo in modo efficace il passaggio trasparente di tutto il traffico HTTPS.

## Causa

Gli errori relativi ai certificati sono causati da problemi di convalida dei certificati legittimi nei server di origine, inclusi certificati scaduti, mancata corrispondenza di CN/SAN e problemi di connettività CRL. Cisco Secure Access esegue la convalida dei certificati come parte del processo di decrittografia SSL. Quando si verificano questi errori di convalida, il prodotto genera pagine di errore per impedire connessioni potenzialmente non sicure. Questo è il comportamento di protezione previsto dalla funzione di ispezione SSL.

## Contenuto correlato

- [Documentazione della configurazione di Cisco Secure Access Decryption](#)
- [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).