

# Risoluzione dei problemi relativi al gadget di Cisco Unified Intelligence Center (CUIC) su HTTPS in Finesse

## Sommario

[Introduzione](#)

[Problema](#)

[Soluzione](#)

[Passaggio 1. Scaricare il certificato tomcat.pem dall'host dei gadget di terze parti.](#)

[Passaggio 2. Caricare il certificato nel server Finesse primario.](#)

[Passaggio 3. Riavviare Cisco Finesse Tomcat sul server Finesse primario.](#)

[Passaggio 4. Al termine della sincronizzazione, riavviare Cisco Finesse Tomcat sul database secondario](#)

[Server Finesse.](#)

[Un altro problema](#)

[Soluzione](#)

[Passaggio 1. Dalla pagina di amministrazione della piattaforma in Finesse, caricare il certificato CUIC tomcat come tomcat-trust](#)

[Passaggio 2. Caricare i certificati Finesse in CUIC come tomcat-trust](#)

[Passaggio 3. Riavviare questi elementi nel server di pubblicazione e nel sottoscrittore Finesse durante la finestra di manutenzione con](#)

[questi comandi](#)

[Passaggio 4. Riavviare i servizi su CUIC publisher e subscriber](#)

## Introduzione

In questo documento viene descritto come risolvere i problemi relativi ai gadget CUIC (Cisco Unified Intelligence Center) in Cisco Finesse su HTTP. Questo problema è stato rilevato durante l'implementazione dei gadget.

Contributo di Sahar Modares, Cisco TAC Engineer.

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

CUIC

Finesse

### Componente utilizzato

CUIC 10.5

Finesse 11.0

# Problema

Il nuovo gadget CUIC è stato creato con questo collegamento, nel layout di amministrazione di Finesse:

```
<gadget>/3rdpartygadget/files/WebService/WebService.xml</gadget>
```

Ma non è riuscito con questo messaggio di errore:

```
"Stato HTTP 500 - javax.net.ssl.SSLPeerUnverifyException: peer non autenticato"
```

# Soluzione

La comunicazione HTTPS deve essere consentita tra il contenitore di gadget Finesse e il sito di gadget di terze parti per il caricamento del gadget e l'esecuzione di qualsiasi chiamata API effettuata dal gadget al server di terze parti.

Il certificato deve essere firmato con un nome comune. L'URL del gadget nel layout del desktop deve utilizzare lo stesso nome (sia che utilizzi un indirizzo IP o un nome di dominio completo) del nome con cui è firmato il certificato. Se il nome del certificato e il nome nell'URL del gadget non corrispondono, la connessione non è attendibile e il gadget non viene caricato.

Per trovare il nome del certificato, immettere l'URL del gadget nel browser. Fare clic sull'icona a forma di lucchetto nella barra degli indirizzi, quindi scegliere Visualizza dettagli. Cercare il campo del nome comune.

L'host Finesse deve essere in grado di risolvere questo nome utilizzando l'host DNS immesso durante l'installazione. Per verificare che Finesse sia in grado di risolvere il nome, eseguire il comando CLI "utils network ping <hostname>".

## Passaggio 1. Scaricare il certificato tomcat.pem dall'host dei gadget di terze parti.

1. a) Accedere a Cisco Unified Operating System Administration sull'host dei gadget di terze parti (<https://FQDN/cmplatform>, dove *FQDN* è il nome di dominio completo dell'host dei gadget di terze parti).
2. b) Fare clic su Protezione>Gestione certificati.
3. c) Fare clic su Trova.
4. d) Fare clic su tomcat.pem.
5. e) Fare clic su Download e salvare il file sul desktop.

## Passaggio 2. Caricare il certificato nel server Finesse primario.

1. a) Accedere a Cisco Unified Operating System Administration sul server Finesse primario (<http://FQDN:8080/cmplatform>, dove *FQDN* è il nome di dominio completo del server Finesse).
2. b) Fare clic su Protezione>Gestione certificati.
3. c) Fare clic su Carica certificato.
4. d) Dall'elenco a discesa CertificateNamedscegliere tomcat-trust.

5. e) Fare clic su Sfoglia e individuare il file tomcat.pem scaricato nel passaggio precedente.

1. f) Fare clic su Upload File (Carica file).

**Passaggio 3. Riavviare Cisco Finesse Tomcat sul server Finesse primario.**

**Passaggio 4. Al termine della sincronizzazione, riavviare Cisco Finesse Tomcat sul database secondario**

**Server Finesse.**

## **Un altro problema**

Una volta caricato un certificato di terze parti che in questo caso è CUIC per Finesse, si prevede che il gadget venga caricato su Finesse, ma comunque non riesce con il messaggio di errore indicato nella sezione del problema.

## **Soluzione**

Viene visualizzato l'errore "javax.net.ssl.SSLPeerUnverifyException: peer non autenticato" è stato risolto con i passaggi seguenti:

**Passaggio 1. Dalla pagina di amministrazione della piattaforma in Finesse, caricare il certificato CUIC tomcat come tomcat-trust**

**Passaggio 2. Caricare i certificati Finesse in CUIC come tomcat-trust**

**Passaggio 3. Riavviare questi elementi nel server di pubblicazione e nel sottoscrittore Finesse durante la finestra di manutenzione con**

**questi comandi**

- utilizza il riavvio del servizio Cisco Tomcat
- utilizza il riavvio del servizio Cisco Finesse Tomcat

**Passaggio 4. Riavviare i servizi su CUIC publisher e subscriber**

- utilizza il riavvio del servizio Cisco Tomcat
- utilizza il servizio per riavviare il servizio di creazione di rapporti di Intelligence Center