# Creazione di una richiesta di firma del certificato su un'ESA

## Sommario



## Introduzione

In questo documento viene descritto come creare una richiesta di firma di certificato (CSR) in Email Security Appliance (ESA).

## Creazione di un CSR su un'ESA

A partire dalla versione AsyncOS 7.1.1, l'ESA può creare un certificato autofirmato per uso personale e generare un CSR da inviare a un'autorità di certificazione e ottenere il certificato pubblico. L'autorità di certificazione restituisce un certificato pubblico attendibile firmato da una chiave privata. Usare la pagina **Network > Certificates** nella GUI o il comando **certconfig** nella CLI per creare il certificato autofirmato, generare il CSR e installare il certificato pubblico attendibile.

Se si acquista o si crea un certificato per la prima volta, cercare in Internet "Certificati server SSL per servizi Autorità di certificazione" e scegliere il servizio più adatto alle esigenze dell'organizzazione. Seguire le istruzioni del servizio per ottenere un certificato.

## Procedura di configurazione sulla GUI

1. Per creare un certificato autofirmato, fare clic su **Add Certificate** nella pagina Network > Certificates (Rete > Certificati) nella GUI (o sul comando **certconfig** nella CLI). Nella pagina Aggiungi certificato scegliere **Crea certificato autofirmato**.
2. Immettere le seguenti informazioni per il certificato autofirmato: Nome comune: il nome di dominio completo.Organizzazione: il nome legale esatto dell'organizzazione.Unità organizzativa - Sezione dell'organizzazione.Città (Locality) - Città in cui l'organizzazione si trova legalmente.Stato (Provincia) - Stato, contea o regione in cui l'organizzazione si trova legalmente.Paese: abbreviazione ISO (International Organization for Standardization) del paese in cui l'organizzazione ha sede legale.Durata prima della scadenza: numero di giorni prima della scadenza del certificato.Dimensione chiave privata: dimensione della chiave privata da generare per il CSR. Sono supportati solo i bit 2048 e 1024.

3. Per visualizzare le informazioni relative al certificato e alla firma, fare clic su **Avanti**.
4. Immettere un nome per il certificato. AsyncOS assegna il nome comune per impostazione predefinita.
5. Se si desidera inviare un CSR per il certificato autofirmato a un'autorità di certificazione, fare clic su **Scarica richiesta di firma certificato** per salvare il CSR in formato PEM (Privacy Enhanced Mail) in un computer locale o di rete.
6. Per salvare il certificato ed eseguire il commit delle modifiche, fare clic su **Submit** (Invia). Se non si esegue il commit delle modifiche, la chiave privata verrà persa e non sarà possibile installare il certificato firmato.

Quando l'autorità di certificazione restituisce il certificato pubblico attendibile firmato da una chiave privata, fare clic sul nome del certificato nella pagina Certificati e immettere il percorso del file nel computer locale o in rete per caricare il certificato. Verificare che il certificato pubblico attendibile ricevuto sia in formato PEM o in un formato convertibile in PEM prima di caricarlo nell'accessorio. Gli strumenti per completare questa procedura sono inclusi in OpenSSL, software gratuito disponibile all'indirizzo http://www.openssl.org.

Se si carica il certificato dall'autorità di certificazione, il certificato esistente viene sovrascritto. È inoltre possibile caricare un certificato intermedio correlato al certificato autofirmato. È possibile utilizzare il certificato con un listener pubblico o privato, con i servizi HTTPS di un'interfaccia IP, con l'interfaccia LDAP (Lightweight Directory Access Protocol) o con tutte le connessioni TLS (Transport Layer Security) in uscita ai domini di destinazione.

## Informazioni correlate

- Guida completa alla configurazione di TLS su ESA
- Documentazione e supporto tecnico – Cisco Systems