

# Configura certificato di decrittografia in Appliance Web sicura

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Decrittografia HTTPS](#)

[Configura certificato di decrittografia in SWA](#)

[Carica un certificato radice e una chiave](#)

[Genera certificato e chiave per il proxy HTTPS](#)

[Importa certificato](#)

[Importa certificato proxy upstream in SWA](#)

[Importazione di un certificato SWA in un altro SWA](#)

[Importa certificato SWA nel client Windows](#)

[Importa certificato SWA nel client Mac](#)

[Importa certificato SWA in Ubuntu/Debian](#)

[Importa certificato SWA in CentOS 6](#)

[Importa certificato SWA in CentOS 5](#)

[Importazione certificato SWA in Mozilla Firefox](#)

[Importa certificato SWA in Google Chrome](#)

[Importa certificato SWA in Microsoft Edge/Internet Explorer](#)

[Importazione certificato SWA in Safari](#)

[Importa certificato SWA da Criteri di gruppo ai client](#)

[Contenuto correlato](#)

---

## Introduzione

In questo documento viene descritto come configurare i certificati di crittografia HTTPS in client SWA (Secure Web Appliance) e proxy.

---

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso amministrativo all'SWA
  - Accesso all'interfaccia grafica dell'SWA
- 

## Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

---

## Decrittografia HTTPS

La decrittografia SWA Hypertext Transfer Protocol Secure (HTTPS) utilizza i certificati radice e i file delle chiavi private caricati nell'accessorio per crittografare il traffico. Il certificato radice e i file di chiave privata caricati nell'accessorio devono essere in formato PEM.

---



Nota: Formato DER non supportato.

---

È inoltre possibile caricare un certificato intermedio firmato da un'autorità di certificazione radice. Quando SWA crea un certificato che rappresenta il certificato del server, invia il certificato caricato insieme al certificato simulato all'applicazione client. In questo modo, se il certificato intermedio è firmato da un'autorità di certificazione (CA) radice considerata attendibile dall'applicazione client, l'applicazione considera attendibile il certificato del server con errori di digitazione.

---

## Configura certificato di decrittografia in SWA

L'SWA può utilizzare un certificato esistente e una chiave privata per la decrittografia HTTPS. Tuttavia, può esserci confusione sul tipo di certificato da utilizzare, in quanto non tutti i certificati x.509 funzionano.

Esistono due tipi principali di certificati: Certificati server e Certificati radice. Tutti i certificati x.509

contengono un campo Vincoli base che identifica il tipo di certificato:

- Subject Type=Entità finale - Certificato server
  - Subject Type=CA - Certificato radice
- 

## Carica un certificato radice e una chiave

Passaggio 1. Dalla GUI, passare a Security Services e scegliere HTTPS Proxy.

Passaggio 2. Fare clic su Modifica impostazioni.

Passaggio 3. Fare clic su Utilizza certificato e chiave caricati.

Passaggio 4. Fare clic su Sfoglia nel campo Certificato per passare al file di certificato archiviato nel computer locale.

---



Nota: Se il file caricato contiene più certificati o chiavi, il proxy Web utilizza il primo certificato o chiave del file.

---

Passaggio 5. Fare clic su Sfoglia nel campo Chiave per passare al file della chiave privata.

---



Nota: La lunghezza della chiave deve essere di 512, 1024 o 2048 bit.

---

Passaggio 6. Selezionare Chiave crittografata se la chiave è crittografata.

Passaggio 7. Fare clic su Upload Files per trasferire il certificato e i file di chiave in Secure Web Appliance. Le informazioni sul certificato caricato vengono visualizzate nella pagina Modifica impostazioni proxy HTTPS.

Passaggio 8. (Facoltativo) Fare clic su Scarica certificato per trasferire le applicazioni client sulla rete.

Passaggio 9. Sottomettere e confermare le modifiche.

---

## Genera certificato e chiave per il proxy HTTPS

Passaggio 1. Dalla GUI, passare a Security Services e scegliere HTTPS Proxy.

Passaggio 2. Fare clic su Modifica impostazioni.

Passaggio 3. Scegliere Usa certificato e chiave generati.

Passaggio 4. Fare clic su Genera nuovo certificato e chiave.

Passaggio 5. Nella finestra di dialogo Genera certificato e chiave immettere le informazioni per visualizzarle nel certificato radice. È possibile immettere qualsiasi carattere ASCII ad eccezione della barra (/) nel campo Nome comune.

Passaggio 6. Fare clic su Genera.

Passaggio 7. Le informazioni sul certificato generato vengono visualizzate nella pagina Modifica impostazioni proxy HTTPS.

Passaggio 8. (Facoltativo) Fare clic su Scarica certificato per trasferirlo nelle applicazioni client della rete.

Passaggio 9. (Facoltativo) Fare clic sul collegamento Scarica richiesta di firma del certificato per inviare la richiesta di firma del certificato (CSR) a una CA.

Passaggio 10. (Facoltativo) Caricare il certificato firmato nell'appliance Web sicura dopo averlo ricevuto dalla CA. È possibile farlo in qualsiasi momento dopo aver generato il certificato sull'accessorio.

Passaggio 11. Sottomettere e confermare le modifiche.

---

## Importa certificato

### Importa certificato proxy upstream in SWA

Se SWA è configurato per utilizzare un proxy upstream e il proxy upstream è configurato per la decrittografia HTTPS, è necessario importare il certificato di crittografia del proxy upstream in SWA. È possibile gestire l'elenco dei certificati attendibili, aggiungervi certificati e rimuoverne i certificati dal punto di vista funzionale.

Passaggio 1. Dalla GUI, scegliere Rete e Gestione certificati.

Passaggio 2. Fare clic su Gestisci certificati radice attendibili nella pagina Gestione certificati.

Passaggio 3. Per aggiungere un certificato radice attendibile personalizzato con autorità di firma, non presente nell'elenco dei certificati riconosciuti da Cisco, fare clic su Importa e quindi inviare il file del certificato.

Passaggio 4. Sottomettere e confermare le modifiche.

---

### Importazione di un certificato SWA in un altro SWA

Se il certificato e la chiave HTTPS sono stati caricati in un file SWA per il proxy HTTPS e i file originali sono accessibili, è possibile importarli in un altro file SWA dal file di configurazione.

Passaggio 1. Dalla GUI di entrambi gli SWA, selezionare System Administration e fare clic su Configuration File.

Passaggio 2. Fare clic su Download file nel computer locale per visualizzare o salvare.

Passaggio 3. Scegliere Encrypt password nei file di configurazione.

Passaggio 4. (Facoltativo) Selezionate Usa nome file definito dall'utente (Use a user-defined file name) e aggiungete il nome desiderato al file di configurazione.

Passaggio 5. Fare clic su Submit (Invia) in Current Configuration (Configurazione corrente) per scaricare il file configuration .xml.

Passaggio 6. Aprire i file scaricati con editor di testo o editor XML.

Passaggio 7. Copiare questi tag dall'SWA con il certificato, copiare tutti i dati all'interno dei tag e sostituirli nel file di configurazione dell'altro SWA:

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>  
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>  
<prox_config_uploaded_cert>....</prox_config_uploaded_key>  
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

---

Passaggio 8. Salvare le modifiche nel file .xml del file SWA di destinazione.

Passaggio 9. Per importare il file di configurazione .xml modificato nell'SWA di destinazione, dalla GUI, scegliere Amministrazione sistema e fare clic su File di configurazione.

Passaggio 10. Nella sezione Carica configurazione fare clic su Carica file di configurazione dal computer locale.

Passaggio 11. Fare clic su Scegli file e scegliere il file di configurazione .xml modificato.

Passaggio 12. Fare clic su Carica per importare il nuovo file di configurazione con il certificato e la chiave.

Passaggio 13. Eseguire il commit delle modifiche se il sistema lo richiede.

---

## Importa certificato SWA nel client Windows

Per importare il certificato proxy HTTPS SWA come attendibile nei computer client con il sistema operativo Microsoft Windows, rivedere i passaggi seguenti:

Passaggio 1. Fare clic su Start nella barra delle applicazioni e digitare Gestisci certificati computer.

Passaggio 2. Nella pagina Certificati - Computer locale espandere Certificazione radice attendibile e fare clic con il pulsante destro del mouse sulla cartella Certificati.

Passaggio 3. Fare clic su Tutte le attività e scegliere Importa.

Passaggio 4. Nella pagina Importazione guidata certificati fare clic su Avanti.

Passaggio 5. Per importare il file del certificato SWA, fare clic su Sfoglia e scegliere il certificato scaricato da SWA.



Suggerimento: Per scaricare il certificato SWA, fare riferimento al punto 8 della sezione Caricamento di un certificato radice e di una chiave o Generazione di un certificato e di una chiave per il proxy HTTPS.

---

Passaggio 6. Fare clic su Inserisci tutti i certificati nella casella di controllo seguente.

Passaggio 7. Scegliere Autorità di certificazione principali attendibili e fare clic su Avanti.

Passaggio 8. Fare clic su Fine.

In alternativa, è possibile eseguire questo comando per importare il certificato in Autorità di certificazione radice attendibili.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```

---



Nota: È necessario sostituire <Path to SWA Certificate/CertificateName.crt> con il nome e il percorso del file del certificato scaricato.

---

## Importa certificato SWA nel client Mac

Passaggio 1. Scaricare il certificato del proxy HTTPS da SWA al client Mac OS.

Passaggio 2. Rinominare l'estensione del file in .crt.

Passaggio 3. Eseguire questo comando per importare il certificato come certificato attendibile:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```

---



Nota: È necessario sostituirlo con il percorso e il nome file del certificato attualmente scaricato.

---

## Importa certificato SWA in Ubuntu/Debian

Passaggio 1. Scaricare il certificato del proxy HTTPS da SWA.

Passaggio 2. Aprire il file del certificato nell'editor di testo e copiare tutto il contenuto.

Passaggio 3. Creare un nuovo file in `/usr/local/share/ca-certificates/` con un `.crt` come estensione.

Passaggio 4. Modificare il file con l'editor di testo desiderato, incollare il testo copiato nel nuovo file e salvare.

Passaggio 5. Eseguire questo comando per aggiornare i certificati nel sistema operativo.

```
sudo update-ca-certificates
```

---



Suggerimento: Se il certificato è memorizzato localmente nel client, è possibile copiarlo in `/usr/local/share/ca-certificates/` ed eseguire `sudo update-ca-certificates`.

---



Nota: In alcune versioni è necessario installare il pacchetto `ca-certificates` con questo comando: `sudo apt-get install -y certificati ca`.

---

## Importa certificato SWA in CentOS 6

Passaggio 1. Scaricare il certificato del proxy HTTPS da SWA.

Passaggio 2. Aprire il file del certificato nell'editor di testo e copiare tutto il contenuto all'interno del file.

Passaggio 3. Creare un nuovo file in `/etc/pki/ca-trust/source/anchors/` con estensione `.crt`.

Passaggio 4. Modificare il file con l'editor di testo desiderato e salvare il testo copiato in precedenza nel nuovo file.

Passaggio 5. Installare il pacchetto di certificati CA:

```
yum install ca-certificates
```

---

Passaggio 6. Eseguire questo comando per aggiornare i certificati nel sistema operativo:

```
update-ca-trust extract
```



Suggerimento: Se il certificato è archiviato localmente nel client, è possibile copiarlo in `/etc/pki/ca-trust/source/anchors/` ed eseguire l'estrazione `update-ca-trust` dopo aver installato i certificati ca.

---

## Importa certificato SWA in CentOS 5

Passaggio 1. Scaricare il certificato del proxy HTTPS da SWA.

Passaggio 2. Aprire il file del certificato nell'editor di testo e copiare tutto il contenuto del file.

Passaggio 3. Creare un nuovo file nella cartella corrente con estensione `.crt` (ad esempio, `SWA.crt`).

Passaggio 4. Modificare il file `/etc/pki/tls/certs/ca-bundle.crt` con l'editor di testo desiderato, incollare il testo copiato alla fine del file e salvare.



Suggerimento: Se il certificato è memorizzato localmente sul client (in questo esempio il nome del file è `SWA.crt`), è possibile aggiungere il certificato con questo comando: `cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt`.

---

## Importazione certificato SWA in Mozilla Firefox

Passaggio 1. Scaricare il certificato proxy HTTPS da SWA.

Passaggio 2. Rinominare l'estensione del file in `.crt`.

Passaggio 3. Aprire Firefox e fare clic sul Menu (tre barre nell'angolo superiore destro).

Passaggio 4. Scegliere Impostazioni (in alcune versioni è Opzioni).

Passaggio 5. Fare clic su Privacy & Security nel menu a sinistra e scorrere fino a Certificati.

Passaggio 6. Fare clic su Visualizza certificati.

Passaggio 7. Fare clic sulla scheda Autorità e quindi su Importa.

Passaggio 8. Scegliere il file del certificato e fare clic su Apri.

Passaggio 9. Fare clic su OK.

---

## Importa certificato SWA in Google Chrome

Passaggio 1. Scaricare il certificato proxy HTTPS da SWA.

Passaggio 2. Rinominare l'estensione del file in .crt.

Passaggio 3. Aprire Google Chrome e fare clic su Personalizza e controlla Google Chrome (tre punti nell'angolo superiore destro).

Passaggio 4. Scegliere Impostazioni.

Passaggio 5. Fare clic su Privacy e protezione dal menu a sinistra.

Passaggio 6. Scegliere Protezione.

Passaggio 7. Scorrere fino a Gestisci certificati e fare clic sul pulsante a destra.

Passaggio 8. Scegliere la scheda Autorità di certificazione fonti attendibili e fare clic su Importa.

Passaggio 9. Scegliere il file del certificato e fare clic su Apri.

Passaggio 10. Fare clic su OK.



Nota: Se si installa il certificato SWA nel sistema operativo, Google Chrome considera attendibile tale certificato e non è necessario importarlo separatamente nel browser.

---

## Importa certificato SWA in Microsoft Edge/Internet Explorer

Microsoft Edge e Internet Explorer (IE) utilizzano i certificati del sistema operativo. Se si installa il certificato SWA nel sistema operativo, non è necessario importarlo separatamente nel browser.

---

## Importazione certificato SWA in Safari

Passaggio 1. Scaricare il certificato del proxy HTTPS da SWA.

Passaggio 2. Rinominare l'estensione del file in .crt.

Passaggio 3. Nel Launchpad, selezionare Accesso portachiavi.

Passaggio 4. Dal menu File, fare clic su Aggiungi portachiavi.

Passaggio 5. Scegliere il file del certificato SWA e fare clic su Add.

Passaggio 6. Scegliere Protezione.

Passaggio 7. Scorrere fino a Gestisci certificati e fare clic sul pulsante a destra.

Passaggio 8. Scegliere la scheda Autorità di certificazione fonti attendibili e fare clic su Importa.

Passaggio 9. Scegliere il file del certificato e fare clic su Apri.

Passaggio 10. Fare clic su OK.

---

## Importa certificato SWA da Criteri di gruppo ai client

Per distribuire certificati ai computer client tramite Criteri di gruppo da Active Directory, eseguire la procedura seguente:

Passaggio 1. Scaricare il certificato del proxy HTTPS da SWA.

Passaggio 2. Rinominare l'estensione del file in .crt.

Passaggio 3. Copiare il file del certificato nel controller di dominio.

Passaggio 4. Nel controller di dominio fare clic su Start e aprire lo snap-in Gestione Criteri di gruppo.

Passaggio 5. Individuare l'oggetto Criteri di gruppo desiderato o creare un nuovo oggetto Criteri di gruppo che contenga il certificato SWA da importare nel client.

Passaggio 6. Fare clic con il pulsante destro del mouse su Oggetto Criteri di gruppo e scegliere Modifica.

Passaggio 7. Dal menu a sinistra, selezionare Configurazione computer > Criteri > Impostazioni di Windows > Impostazioni protezione > Criteri chiave pubblica.

Passaggio 8. Fare clic con il pulsante destro del mouse su Autorità di certificazione fonti attendibili e scegliere Importa.

Passaggio 9. Fare clic su Avanti nella pagina Importazione guidata certificati.

Passaggio 10. Scegliere il file del certificato SWA da importare e fare clic su Avanti.

Passaggio 11. Fare clic su Posiziona tutti i certificati nel seguente archivio e quindi su Avanti.

Passaggio 12. Verificare che le informazioni fornite siano accurate e fare clic su Fine.



Nota: In alcune condizioni, è necessario riavviare il client o eseguire gpupdate /force per applicare le modifiche nel computer client Active Directory.

---

## Contenuto correlato

- [Guida per l'utente di AsyncOS 14.5 for Cisco Secure Web Appliance - GD \(General Deployment\)](#)
- [Distribuire certificati ai computer client tramite Criteri di gruppo | Microsoft Learn](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

### 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).