# Crea certificato radice personalizzato Umbrella con Servizi certificati Active Directory

## Sommario



## Introduzione

In questo documento vengono fornite istruzioni per la creazione di un certificato radice personalizzato utilizzando Servizi certificati Active Directory di Microsoft Windows.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Una versione di Microsoft Windows Server attualmente supportata da Microsoft
- Servizi certificati Active Directory installati nel server Windows
- Account con i ruoli Servizi certificati Active Directory e Servizio Web/Servizio di registrazione Web
- Servizi certificati configurato per l'emissione di certificati con codifica UTF-8 ("UTF8STRING")

### Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

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.

## Panoramica

In questo articolo vengono fornite istruzioni per la creazione di un certificato radice personalizzato (utilizzato al posto del certificato CA radice Cisco Umbrella standard) tramite Servizi certificati Active Directory di Microsoft Windows e quindi per l'utilizzo di tale certificato radice per firmare una richiesta di firma del certificato (CSR) dalla funzionalità Certificato CA firmato da Umbrella.

## Codifica stringa certificato

Se Servizi certificati è configurato per l'utilizzo della codifica predefinita ("PRINTABLESTRING"), la catena di certificati prodotta non può essere considerata attendibile da alcuni client Web, in particolare Firefox.

Il proxy Cisco Umbrella Secure Web Gateway utilizza una catena di certificati che codifica le stringhe con la codifica UTF8STRING. Se il certificato di rilascio, ad esempio il certificato radice, che firma il CSR per creare il certificato intermedio Cisco Umbrella Customers CA è codificato con PRINTABLESTRING, la codifica del campo Subject del certificato CA Cisco Umbrella Customers è PRINTABLESTRING. Questa codifica non può corrispondere alla codifica UTF8STRING del campo Issuer nel certificato intermedio CA Cisco Umbrella R1, che è il successivo nella catena di certificati.

La RFC 5280, sezione 4.1.2.6, richiede che una catena di certificati mantenga la stessa codifica di stringa tra il campo Issuer di un certificato emesso e il campo Subject del certificato di rilascio:

"Quando il soggetto del certificato è una CA, il campo del soggetto DEVE essere codificato nello stesso modo in cui è codificato nel campo dell'emittente (sezione 4.1.2.4) in tutti i certificati rilasciati dalla CA del soggetto."

Molti browser non applicano questo requisito, ma alcuni (in particolare Firefox) lo fanno. Di conseguenza, i client Web come Firefox possono generare un errore di sito non attendibile e non caricare siti Web quando si utilizza Secure Web Gateway (SWG) con la funzionalità del certificato CA firmato dal cliente.

Per risolvere il problema, utilizzare un browser come Chrome che non applichi i requisiti della RFC 5280.

## Passaggio 1: Preparazione del modello Servizi certificati Active Directory

1. Aprire MMC Autorità di certificazione Active Directory selezionando Start > Esegui > MMC.

2. Selezionare File > Aggiungi/Rimuovi snap-in e aggiungere gli snap-in Modelli di certificato e Autorità di certificazione. Selezionare OK.

3. Espandere Modelli di certificato e fare clic con il pulsante destro del mouse su Autorità di certificazione subordinata. Fare clic su Duplica modello.

È ora possibile creare un modello di certificato personalizzato per soddisfare i requisiti elencati nella documentazione di Umbrella.

Questi sono i requisiti che vengono descritti in dettaglio al momento della creazione di questo articolo:

- Scheda Generale
  - Assegnare al modello un nome significativo.
  - Impostare il periodo di validità per 35 mesi (3 anni in meno al mese).
  - Impostare il periodo di rinnovo su 20 giorni.
- Scheda Estensioni
  - Fare doppio clic su Basic Constraints.
    - Verificare che l'opzione Rendi l'estensione critica sia selezionata.
  - In Utilizzo chiave:
    - Verificare che siano selezionate le opzioni Firma certificato e Firma CRL.
    - Deselezionare Firma digitale.
    - Assicurarsi che l'opzione Rendi l'estensione critica sia selezionata anche in questo caso.
- Selezionare Apply (Applica), quindi OK.

## Passaggio 2: Utilizzare il modello

1. In MMC configurato nel passaggio 2 del processo precedente, espandere la sezione Autorità di certificazione.

2. Nella sezione espansa di recente, fare clic con il pulsante destro del mouse sulla cartella Certificate Templates (Modelli di certificato) e selezionare New > Certificate Template to Issue (Nuovo > Modello di certificato da rilasciare).

3. Nella nuova finestra, selezionare il nome del modello di certificato creato nell'ultima sezione e selezionare OK.

L'autorità di certificazione è ora pronta a facilitare la richiesta.

## Passaggio 3: Scaricamento e firma del CSR

1. Accedere a Umbrella Dashboard (https://dashboard.umbrella.com).

2. Passare a Distribuzioni > Configurazione > Certificato radice.

3. Selezionare l'icona Add (+) nell'angolo e assegnare un nome alla CA nella nuova finestra.

4. Scaricare la richiesta di firma del certificato (CSR).

5. In una nuova scheda del browser, passare ai servizi Web per Servizi certificati Active Directory. Se si utilizza un computer locale, il valore è 127.0.0.1/certsrv/ o simile.

6. Nella nuova pagina, selezionare Richiedi certificato.

7. Selezionare Advanced Certificate Request.

8. In Richiesta salvata copiare e incollare il contenuto del CSR scaricato nel passaggio 4 (è necessario aprirlo con un editor di testo).

9. In Modello di certificato selezionare il nome del modello di certificato creato nella sezione "Preparazione del modello di Servizi certificati Active Directory" e selezionare Sottometti.

10. Selezionare Base64 Encoded, Scarica certificato e annotare il percorso del file con estensione cer.

## Passaggio 4: Caricare il CSR firmato (e il certificato radice pubblico)

1. Nel dashboard Umbrella, passare a Distribuzione > Configurazione > Certificato radice.

2. Selezionare il certificato radice creato nel Passaggio 3 della sezione precedente.

3. Selezionare Upload CA nell'angolo inferiore destro della riga*.

4. Selezionare il pulsante Sfoglia superiore (Autorità di certificazione (CSR firmato)).

5. Individuare il percorso del file con estensione cer creato nella sezione precedente e selezionare Salva.

6. Selezionare Next (Avanti), selezionare i gruppi di computer/utenti con cui si desidera utilizzare il certificato (anziché il certificato radice Cisco) e selezionare Save (Salva).

*È anche possibile caricare il certificato CA, se lo si desidera. È possibile recuperare questa informazione dall'interfaccia Web del server dell'Autorità di certificazione (http://127.0.0.1/certsrv/) e quindi selezionare Scarica un certificato CA, una catena di certificati o un CRL. Completare le istruzioni visualizzate per "Scaricare il certificato CA" in Base 64.

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).