HOW TO

Gestione dei certificati in SINEMA RC

SIEMENS

Contents

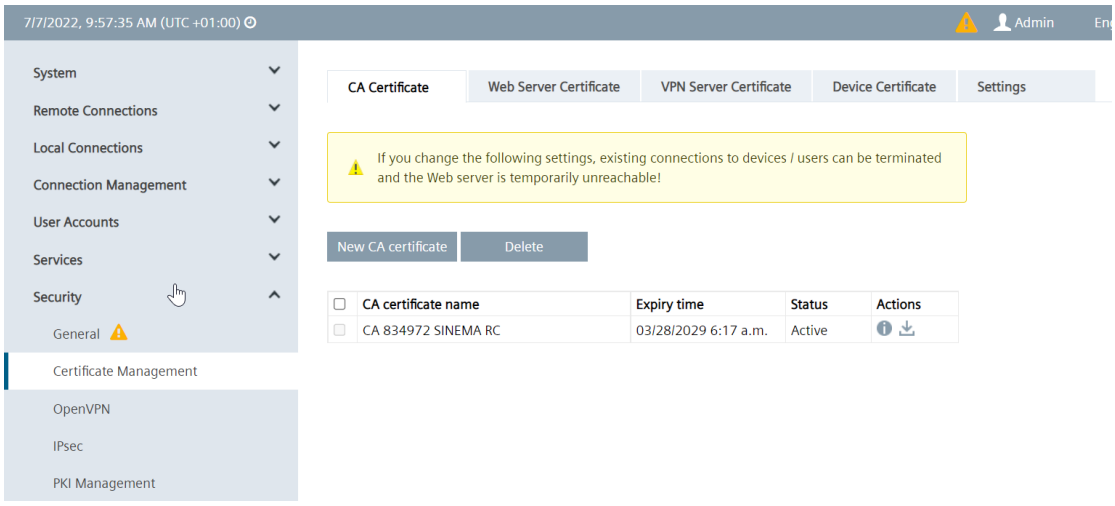
Gestione dei certificati in Sinema RC

La seguente guida illustra come il software Sinema RC Server utilizza e gestisce i diversi tipi di certificati digitali a sua disposizione
Essendo il Sinema RC una piattaforma per connessioni remote basate su VPN, un corretto utilizzo dei certificati è fondamentale.
La seguente guida è redatta con la versione SINEMA RC Server 3.1

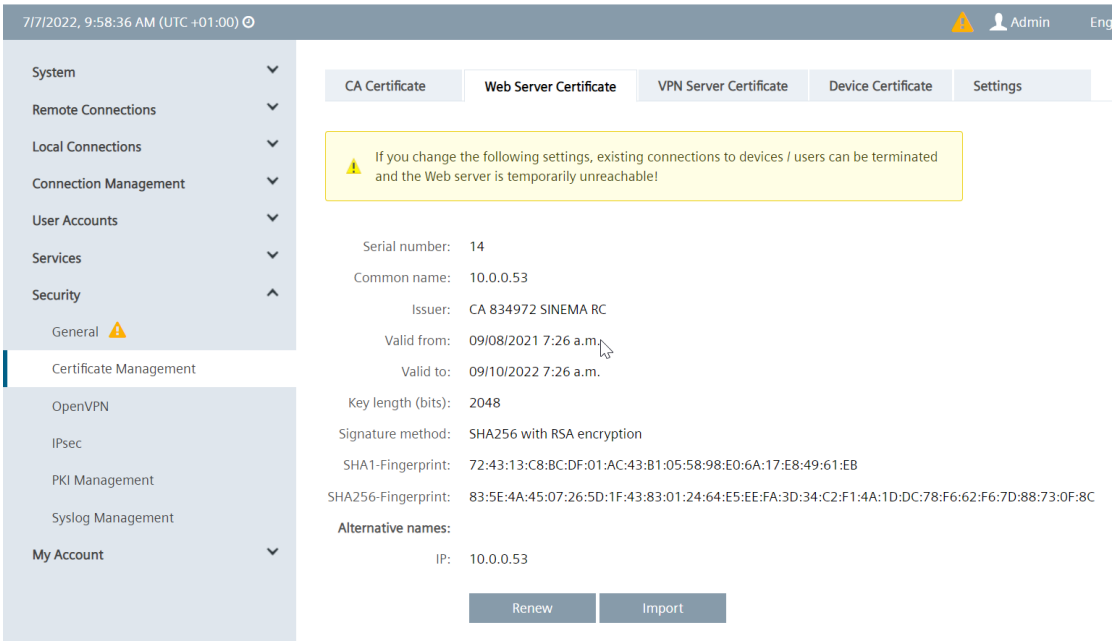
I certificati

In caso di configurazione standard OpenVPN il Sinema RC Server utilizza principalmente 3 certificati (potete vederli in Security → Certificate management)

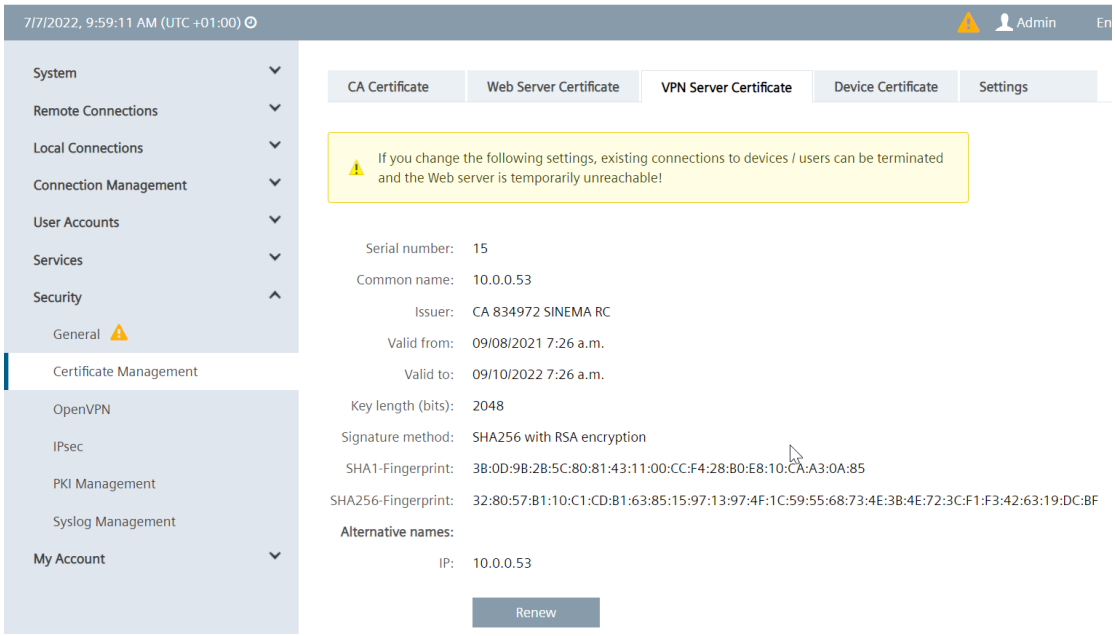
- **Certificato CA** (Certificate Authority): Self-Signed, da lui dipendono tutti gli altri certificati,
    - Durata di default: 10 anni (non modificabile)



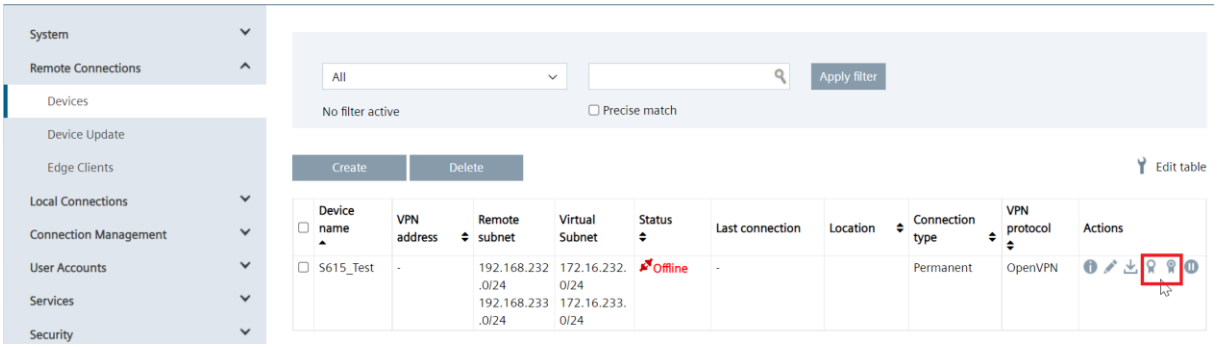
- **Certificato Web:** certificato utilizzato per la connessione HTTPS al server e quindi l'auto-enrollment,
    - Durata di default: 1 anno, la lunghezza è modificabile fino a 10 anni



- **Certificato VPN**: certificato utilizzato per la connessione OpenVPN al server
    - Durata di default: 1 anno, la lunghezza è modificabile fino a 10 anni



Inoltre, ogni device disporrà di un suo certificato che verrà generato alla creazione del device stesso la cui è durata è pari a quella impostata per i certificati VPN e Web. Il certificato può essere scaricato dalla lista dei device nei diversi formati nel menù “Remote Connections” → “Devices” cliccando sui simboli della coccarda, come indicato in immagine.

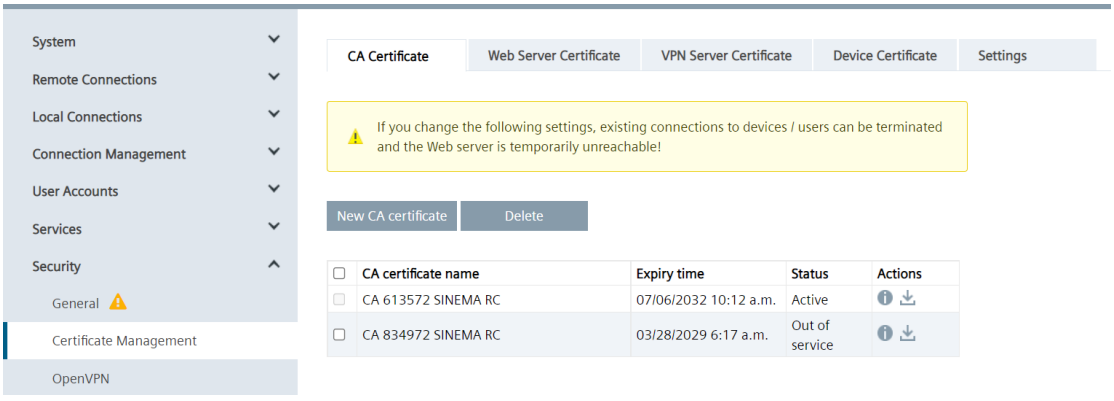


Quando un dispositivo si connette al Sinema RC Server per la prima volta, lo fa utilizzando l'HTTPS (certificato web). In tal modo esegue l'operazione di "auto-enrollment" in cui scarica la configurazione OpenVPN con i relativi parametri e il certificato device corrispondente con cui può andare a connettersi in VPN al Sinema RC Server. Inoltre, il device scarica anche il **certificato di fallback** univoco per il server.

Il certificato device ha una durata limitata che inizia il giorno di creazione del device (secondo l'ora del Sinema RC Server) e scadenza pari alla lunghezza parametrizzata nel Sinema RC Server, esso dipende dal certificato CA del Sinema RC Server.

Solo un certificato CA può essere valido in un dato momento, qualora un nuovo certificato CA venga generato tramite il pulsante "new CA certificate" o attraverso il renewal impostato nei "certificate settings", il precedente certificato CA diventerà "Out of Service".

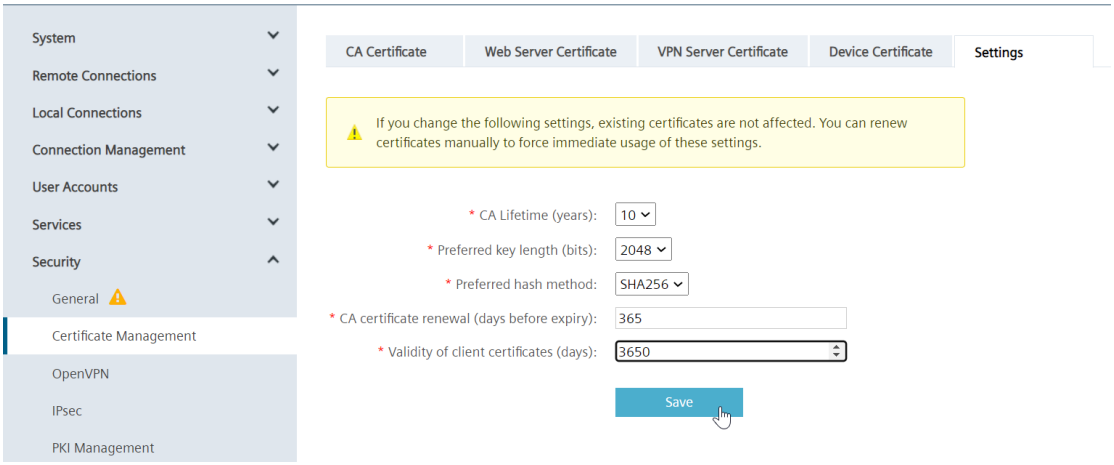
Tutti i nuovi certificati verranno generati col nuovo CA. I certificati precedenti rimarranno immagazzinati sul server anche se legati ad un certificato "out of Service".



Avere certificati Out of Service sul server deve essere una situazione temporanea e va assolutamente sistemata nel più breve tempo possibile!

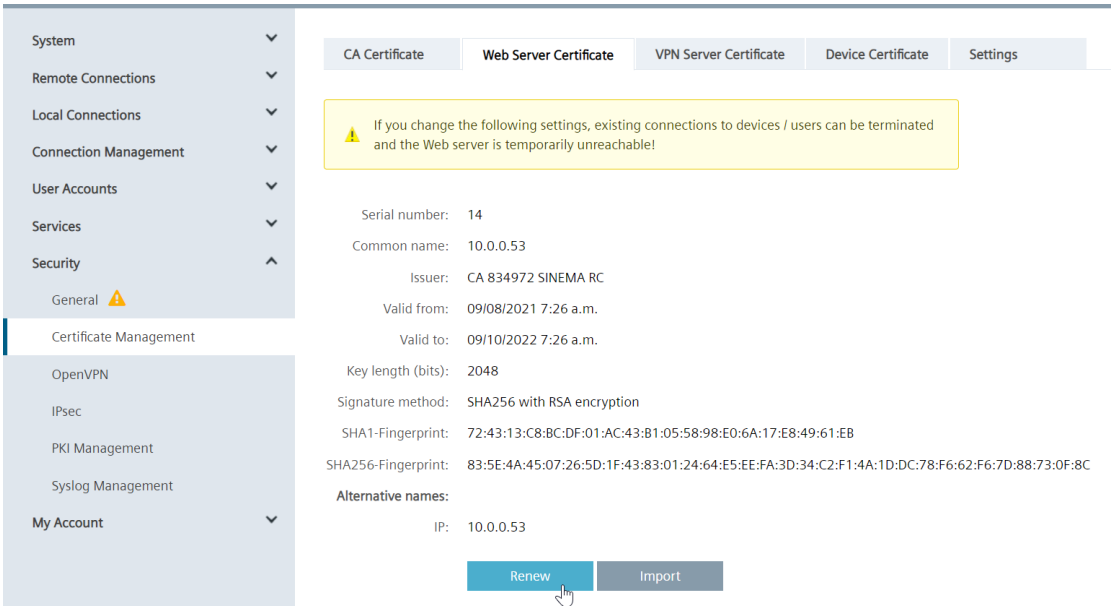
Impostazioni su certificati

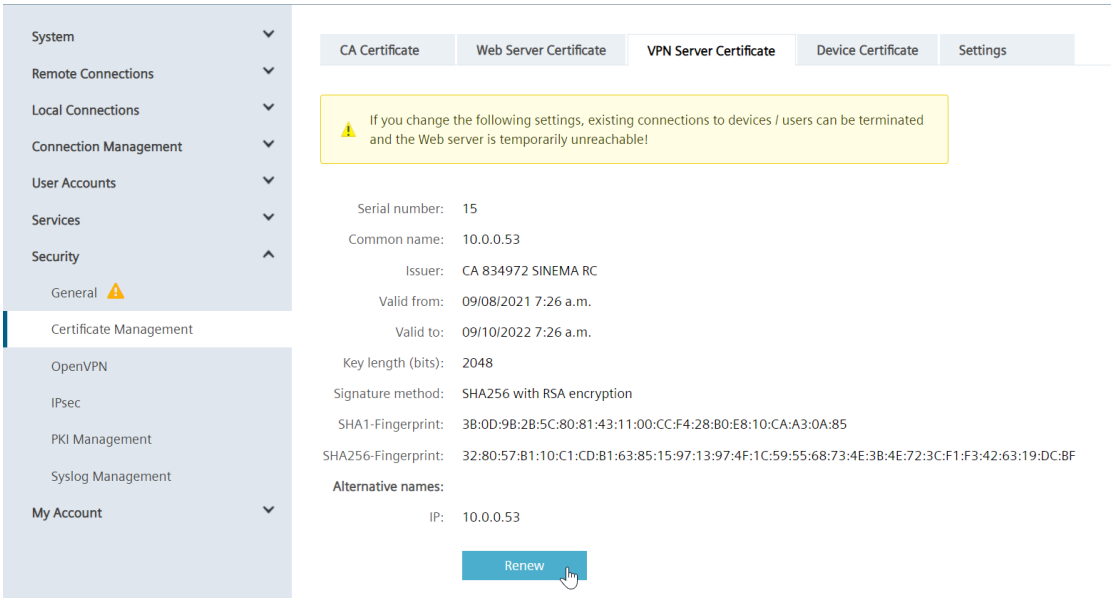
Dalle impostazioni (System → Certificate Management, tab Settings) è possibile allungare la scadenza dei certificati fino ad un massimo di 3650 giorni, modificando il campo "Validity of client certificates".



Da qui è anche possibile configurare **quanto tempo prima della scadenza è possibile rinnovare il certificato CA** del server (default 365 giorni, fino a un massimo di 3285 giorni).
Attenzione: prima un certificato CA viene rinnovato, più è probabile che ci siano certificati Out of Service ancora in utilizzo da parte dei VPN client. **Si raccomanda di evitare di modificare tale parametro** se non si ha una motivazione valida a tale scopo.

Per rendere effettiva la modifica occorre però rinnovare i certificati del Web Server (System → Certificate Management, tab Web Server Certificate e cliccare su Renew) e della VPN (System → Certificate Management, tab VPN Server Certificate e cliccare su Renew).





In generale si raccomanda di non toccare i parametri dei certificati se non si sa esattamente cosa si sta facendo e di predisporre comunque tutti i device all'uso della procedura di Fallback onde mettersi al riparo da problematiche che possono sfociare nell'assenza di comunicazione remota.

Si ricorda inoltre che l'uso di certificati di lunghezza superiore ad un anno, per quanto sicuramente più comodi da gestire, sono sconsigliati dalle principali normative di riferimento e anche i web browser di uso più comune quali Google Chrome e Mozilla Firefox a partire dal 2021 invalidano certificati di lunghezza superiore.

Procedura di Fallback

Qualora l'ora del device non corrisponda ai limiti di validità del certificato, o il certificato CA dovesse risultare non valido (scaduto o "out of service"), il device può ricorrere alla procedura di Fallback (di default su porta 6220 TCP) in cui tramite il certificato di Fallback ottiene con procedura sicura nuovamente i parametri validi e aggiornati per connettersi in VPN al Sinema RC Server (i.e. **i certificati vengono aggiornati automaticamente**). Il successo della procedura di Fallback dipende però dal fatto che il device abbia un**'ora sincronizzata** in modo da rientrare entro i parametri dei nuovi certificati generati.

Notare che il controllo sul CA viene eseguito solo nella fase iniziale, qualora il device rimanga connesso col proprio certificato questo non recederà fino alla scadenza del certificato stesso.

La **procedura di fallback mette quindi al riparo da tutte le problematiche** quali cambio di certificati in corsa o connessione del device a cambio di certificato già avvenuto. Affinché essa possa essere effettuata, sono necessari 3 fattori:

1. Il device deve essersi **connesso al server almeno una volta** (in modo da aver immagazzinato il certificato di Fallback).

2. **L'ora del device** deve essere "sufficientemente" **sincronizzata** da rientrare nella validità del nuovo certificato (si raccomanda in tal caso la sincronizzazione tramite NTP).

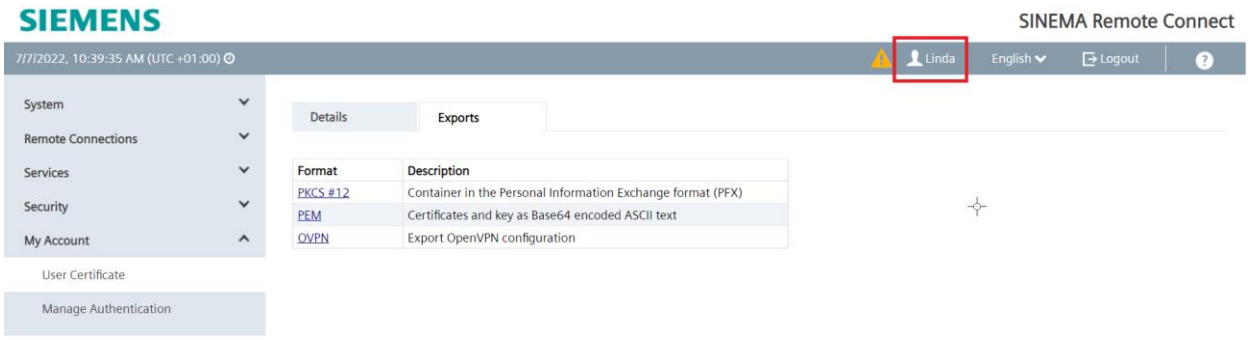
3. La comunicazione fra device e server su **porta 6220 TCP** (o la porta configurata a tale scopo) deve essere possibile → **non deve essere bloccata** la porta lato client e deve essere **correttamente inoltrata** (port forwarding) lato server.

Nota bene: il Sinema RC Client non ha problematiche di questo tipo in quanto rinegozia un nuovo tipo di connessione tramite una procedura semplificata ad ogni connessione.

Device terze parti

L'integrazione di device terze parti OpenVPN (quali ad esempio Smartphone e Tablet con Ios o Android) è possibile con il download dei certificati e della configurazione dal server ma deve tenere conto della lunghezza dei certificati e della rigenerazione degli stessi**. I device terze parti non dispongono infatti delle procedure di Fallback** dei device né delle procedure semplificate del Sinema RC Client e devono essere riparametrizzati nuovamente.

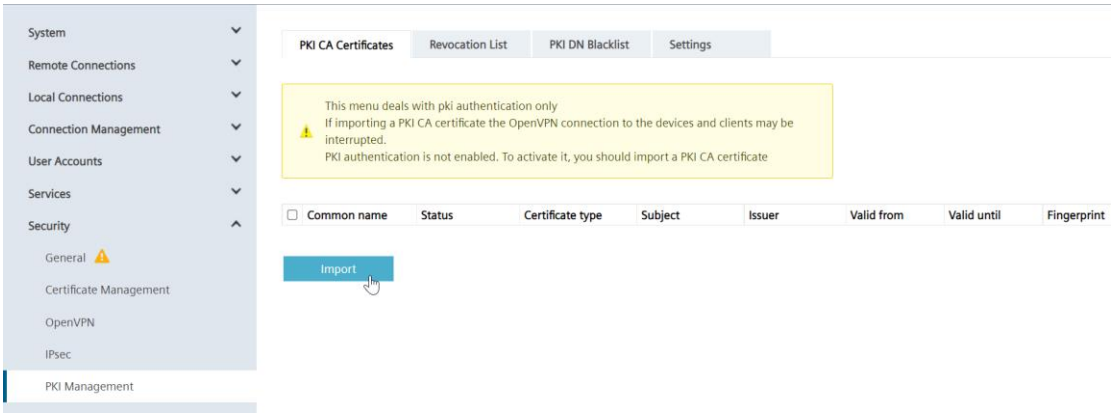
Per scaricare i certificati degli utenti da importare su applicazioni OpenVPN è **necessario autenticarsi sul Sinema RC Server con le credenziali dell'utente VPN (e non dell'amministratore!).** Dal menù "My account" → User Certificate, tab Exports è quindi possibile scaricare sia il certificato che la configurazione OpenVPN.



Importazione certificati CA

È anche possibile importare dei certificati CA, questo permette ad esempio di generare dei certificati web generati da una CA riconosciuta, che quindi siano automaticamente accettati da qualsiasi tipo di software (i.e. web browser per la pagina web del Sinema RC Server).

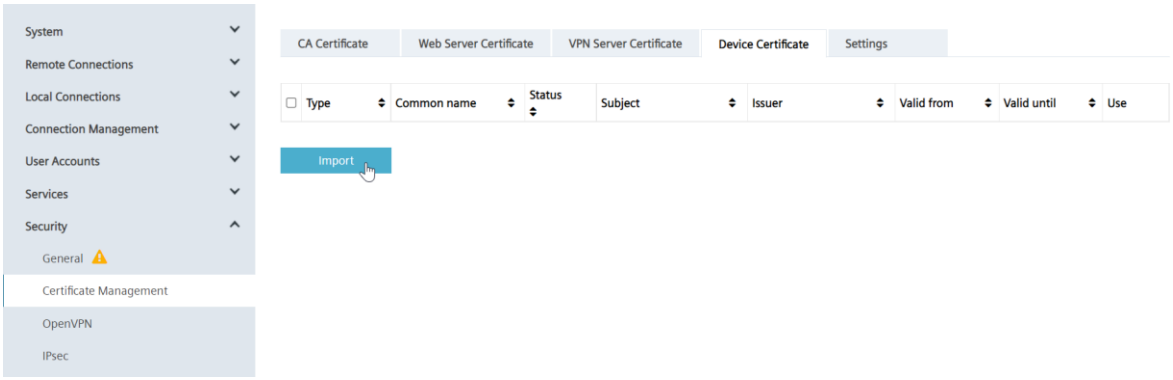
Per importare i certificati è possibile farlo dalla sezione Security → PKI Management, tab PKI CA Certificates e cliccando il tasto Import



Certificati per connessioni IPSec

È possibile anche configurare certificati per connessioni OpenVPN e soprattutto per IPSec (unico modo possibile per supportare tale protocollo) generati da tool esterni (come il software Siemens SCT).

In tale caso i certificati generati possono essere caricati sul Sinema RC Server dalla sezione Security → Certificate management → Device certificate e cliccando su Import



Con riserva di modifiche e salvo errori.
Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.
Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.