HOW TO

Configurazione per connessione a SINEMA RC senza Basic Wizard

SIEMENS

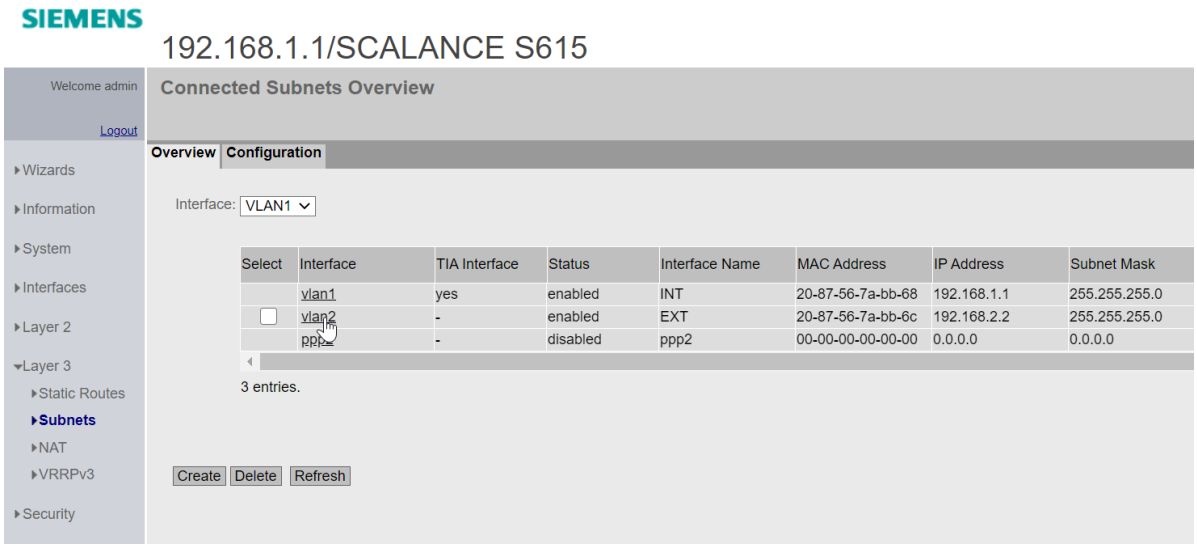
Contents

Configurazione per connessione a SINEMA RC senza Basic Wizard

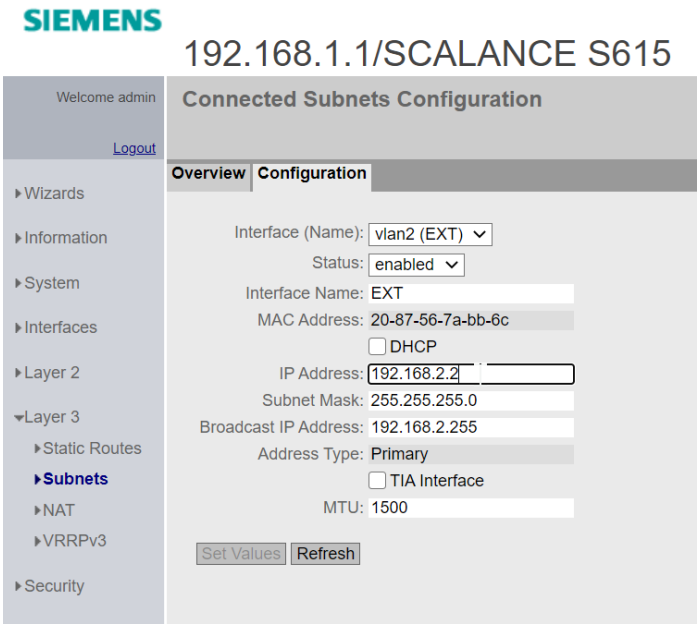
La seguente guida illustra come configurare uno Scalance S615 attraverso la sua pagina web (Web Based Management) per stabilire una connessione VPN al software Sinema Remote Connect Server.
La guida è valida fino al firmware 7.1 di Scalance S615 e server Sinema RC 3.1.
Prima di iniziare la configurazione è necessario avere a disposizione un software Sinema RC Server funzionante con almeno un dispositivo correttamente parametrizzato.
Per configurare il Sinema RC Server o per configurare gli altri parametri sullo Scalance si può fare riferimento alle guide apposite.

Configurazione senza Basic Wizard

Per la configurazione della connessione a SINEMA RC è opportuno assegnare correttamente gli indirizzi IP alle interfacce di rete. Accedere al menù **Layer 3 → Subnets**



La modifica dell'IP della singola rete può essere apportata cliccando sulla tab Configuration o direttamente sul nome dell'interfaccia. In particolare, è importante assegnare un indirizzo IP alla vlan2, di norma utilizzata per l'accesso internet che garantisce la connessione al SINEMA RC, oppure alla nuova VLAN programmata per questo scopo, se questa non lavora in DHCP.
Rimuovere il flag da DHCP e impostare i parametri di "IP Address" e "Subnet Mask" desiderati. Cliccare su "Set Values".

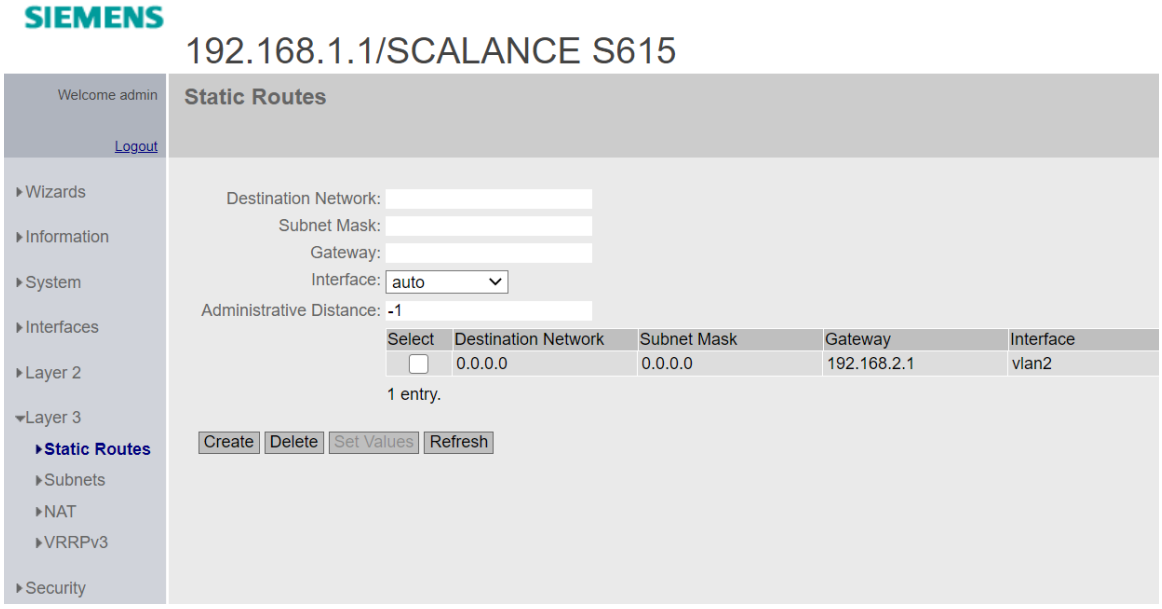


Se non lo si è già fatto, assegnare nello stesso modo gli indirizzi IP alle restanti VLAN configurate.

Qualora la rete del cliente lo richieda, l'inserimento del **default gateway** è possibile nella pagina **Layer 3 → Static Routes**.
Qui va inserita una rotta statica con i seguenti parametri:

- Destination: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Gateway: x.y.z.m (cioè l'indirizzo IP del default gateway)

Cliccare su "Create"

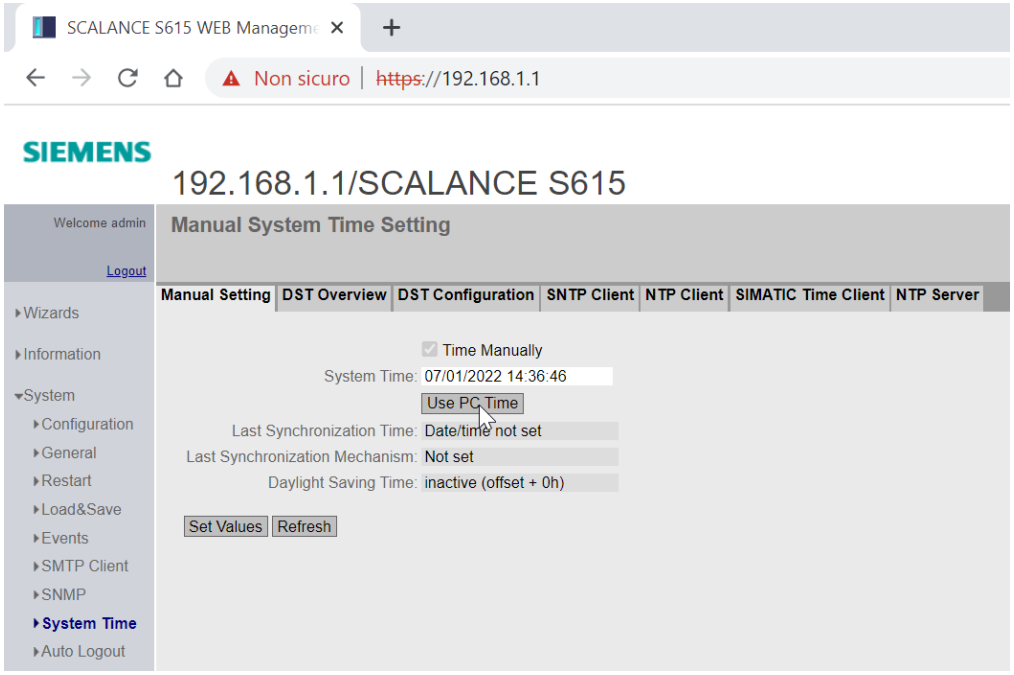


Un altro parametro fondamentale, se non già configurato in precedenza, è la parametrizzazione di **data e ora.** Questa può avvenire in modo manuale o con server **NTP.**
Accedere al menù **System → System Time**.

Sono disponibili due modalità di configurazione:

1. **Impostazione manuale**

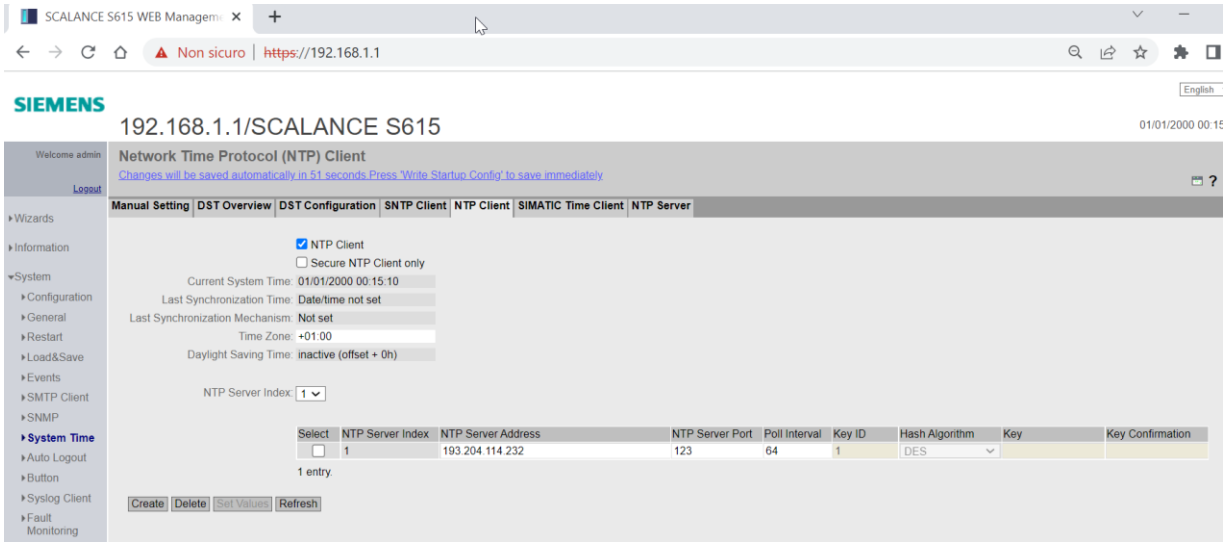
L'impostazione manuale consente all'ora di scorrere fintanto che il PC è acceso ma in caso di spegnimento rimarrà congelata e ripartirà al riavvio del dispositivo. E' quindi una configurazione rapida ma poco robusta a eventuali spegnimenti.
Per impostare il tempo cliccare su System → System Time → Manual Setting.
Premere sul pulsante "Use PC Time" e cliccare su "Set Values".



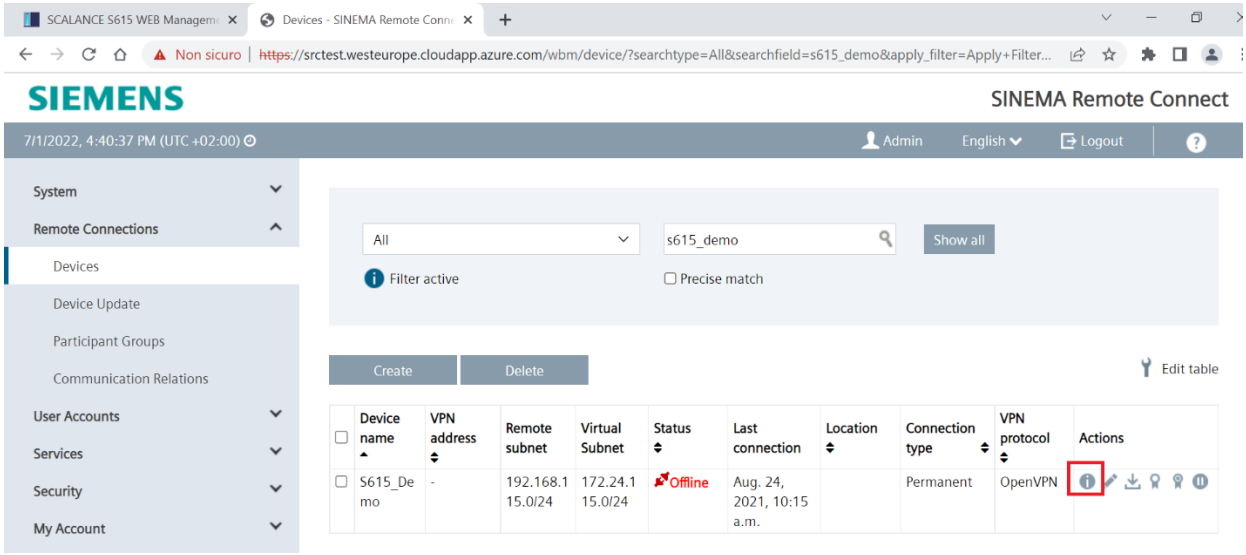
2. **Sincronizzazione con server NTP**

Accedere a System → System Time → NTP Client.
Cliccare su "Create" ed inserire **l'indirizzo IP del server NTP** da utilizzare, che di norma sono in ascolto sulla porta 123 UDP, presente all'interno della rete d'impianto o raggiungibile con la connessione internet (ad es.: 193.204.114.232)

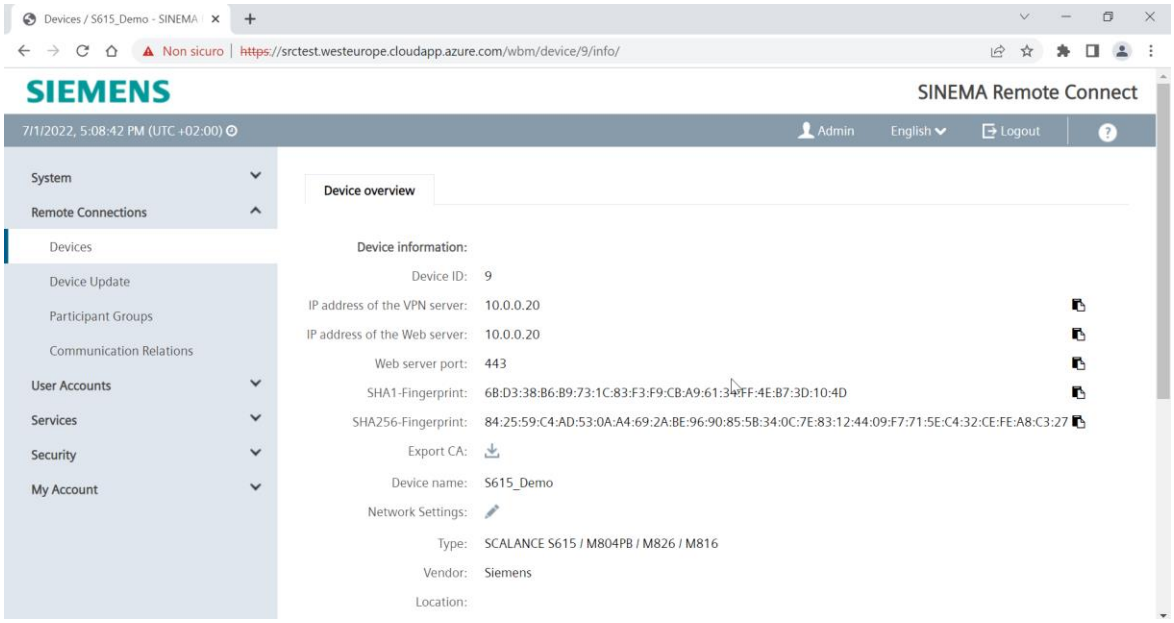
Se la porta è differente può essere specificata nell'apposito campo della tabella, dove è anche possibile impostare l'intervallo di polling sul server.
Indicare la relativa time zone e spuntare la modalità "NTP Client" o in alternativa la modalità sicura (NTPsec da non confondersi con SNTP) "Secure NTP Client Only". Cliccare "Set Values".



La parametrizzazione per la connessione a Sinema RC è disponibile in **System → Sinema RC**.
Per recuperare i valori da inserire all'interno di questa pagina, bisogna andare sul Sinema RC Server nella sezione Remote Connections → Devices. Selezionare il dispositivo cliccando sul simbolo di "I" (Informazione)

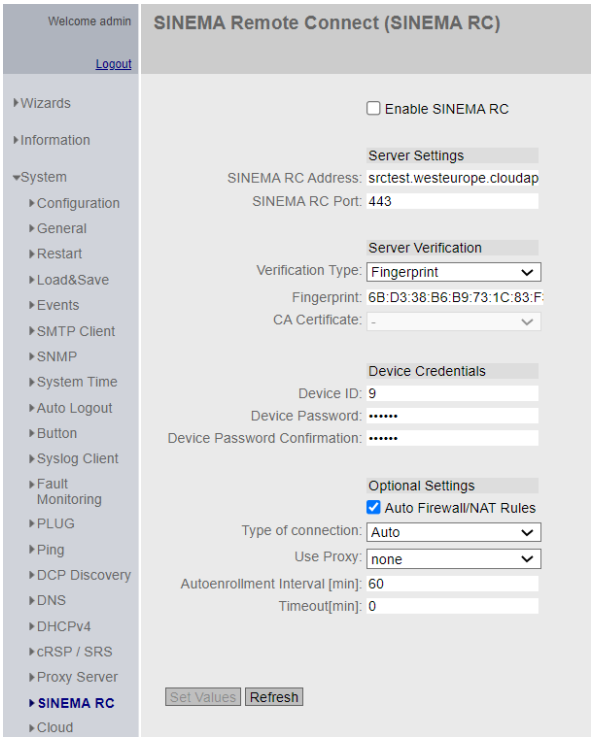


Da qui è possibile copiare tutti i valori utili per l'inserimento nella pagina di configurazione dello SCALANCE S615.



Inserire quindi i seguenti parametri:

- Device ID
- IP address oft he VPN server (IP oppure hostname)
- Web Server Port (443 se non è stata modificata in fase di configurazione del server).
- Fingerprint (scegliere quale utilizzare in base al livello di crittografia desiderato: SHA1 oppure SHA256).
- Password (non è riportata, è stata inserita in fase di creazione del device sul server, se è stata dimenticata è possibile comunque farla modificare dall'amministratore del server senza conoscere quella precedente)

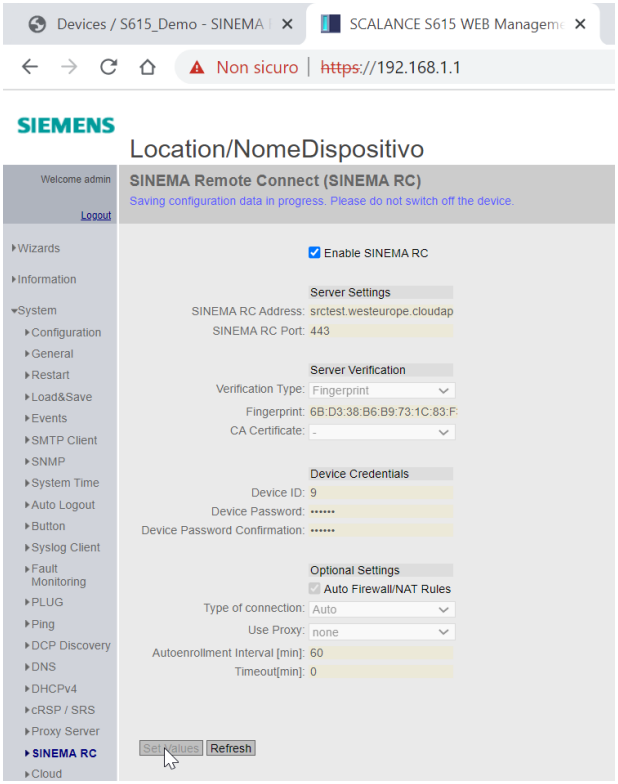


Cliccare su "Set Values".

In seguito spuntare il campo "**Enable Sinema RC**". Tutti i parametri appariranno in giallo e non saranno

più modificabili.

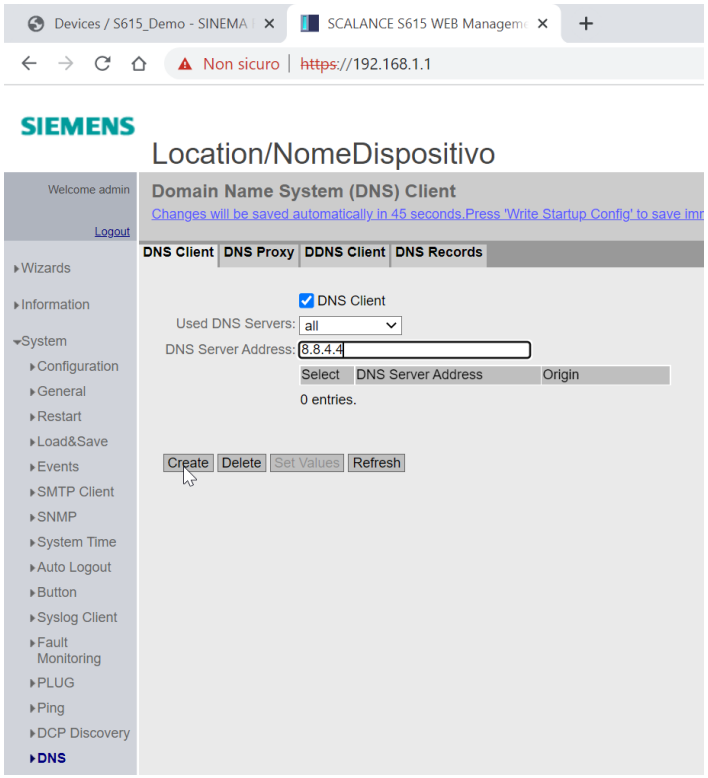
Cliccare di nuovo su “Set Values”.



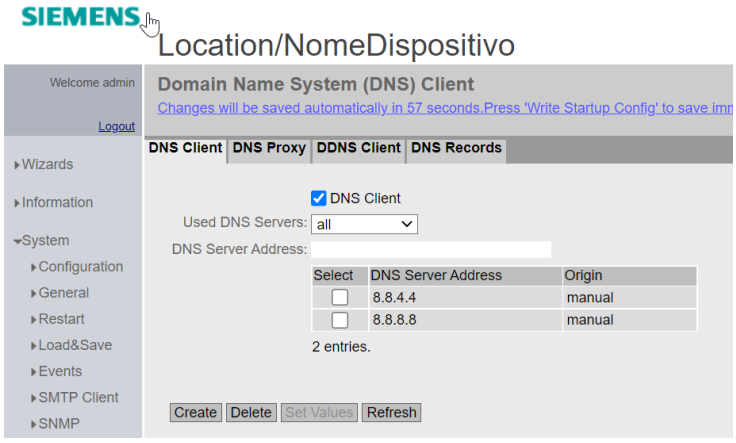
N.B.: se si è scelto di utilizzare un hostname per il Sinema RC Server e non si ha la configurazione DHCP occorre anche configurare dei server DNS per risolvere il nome del server. Seguire quindi la sezione successiva.

Configurazione DNS

Per configurare il DNS occorre scorrere il menù della pagina web dello Scalance alla voce System → DNS
Se non si ha un DNS locale o raccomandato dal proprio provider è sempre possibile utilizzare i classici DNS di Google (8.8.8.8 e 8.8.4.4) laddove sia permesso il loro raggiungimento.
Digitare l’indirizzo in corrispondenza della voce “DNS Server Address” e cliccare su “Create”.



E' possibile inserire anche più di un indirizzo.

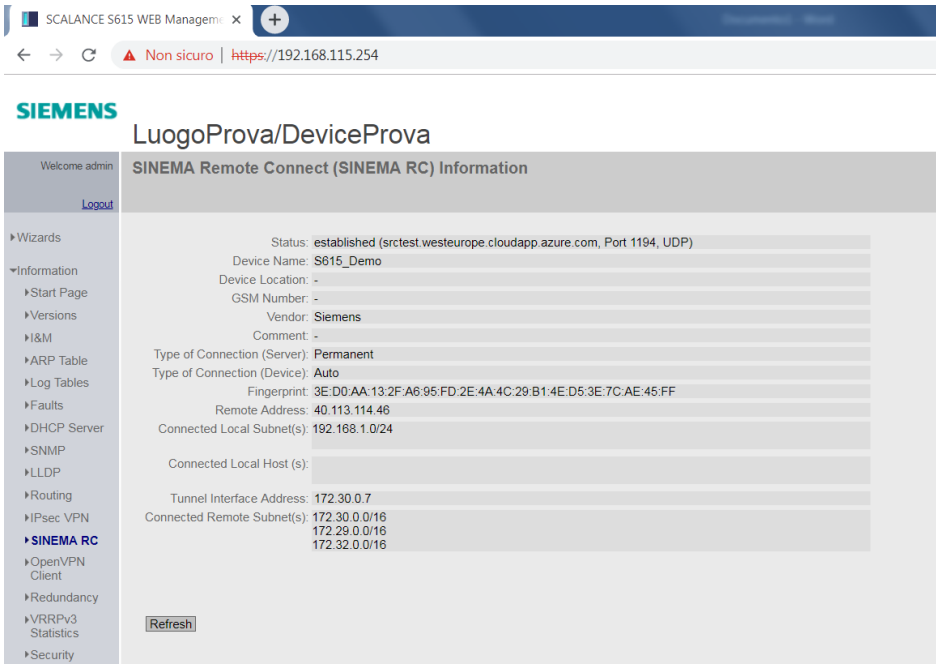


N.B.: la connessione a un server DNS pubblico implica la comunicazione su porta 53 UDP che quindi non deve essere bloccata da eventuali firewall.

Qualora si abbia un DHCP che fornisce DNS sarà presente una linea "learned" in corrispondenza della colonna "Origin".

Verifica connessione al Sinema RC

Per verificare l'avvenuta connessione è sufficiente verificare l'accensione del led a "lucchetto" sullo Scalance oppure accedere alla pagina web Information → Sinema RC.



Per essere stabilita la connessione deve essere "Established", se non è stata abilitata lo stauts è invece in "Disabled" o "Waiting for Digital Input". Se invece la configurazione rimane in "Pending" c'è un problema di connessione e va esaminato facendo del troubleshooting (seguire apposita guida).

Considerazioni sulla connettività e sulle porte di comunicazione

Lo Scalance S può essere su rete WAN con firewall e quindi può necessitare di permessi di comunicazione. In quanto client lo Scalance non necessita di abilitazioni in ingresso e/o port forwarding ma deve poter semplicemente uscire sulle seguenti porte (non devono essere bloccate dal firewall) per raggiungere il server Sinema RC:

443 TCP → porta di destinazione del web server (**HTTPS**) fondamentale per negoziare i certificati
1194 UDP → porta di comunicazione del protocollo **OpenVPN** per l'instaurazione del tunnel

Non sono fondamentali ma sono anche utilizzabili le seguenti porte:
5443 TCP → porta per connessione TCP **OpenVPN**. Qualora la connessione UDP sia instabile, il protocollo tenta la connessione in TCP su questa porta, che garantisce una maggior stabilità (è comunque impossibile imporre l'utilizzo di TCP o UDP nella configurazione del server).
6220 TCP → qualora il dispositivo sia rimasto spento o disconnesso durante la fase di rinnovo dei certificati e alla successiva connessione il certificato sia cambiato è possibile effettuare il rinnovo forzato (procedura di **fallback**) del certificato (cambio fingerprint) attraverso questa porta.

N.B: Tutte queste porte derivano direttamente dalla configurazione OpenVPN e sono parametrizzate direttamente nel Sinema RC Server. L'amministratore del server Sinema RC può quindi modificarle ma tale modifica coinvolge tutti i device. Fa eccezione la porta 443 che può invece essere modificata per singolo dispositivo nella pagina di parametrizzazione per Sinema RC. Il server rimane comunque in ascolto sulla 443 se non modificato.

Inoltre, se sono stati utilizzati NTP e/o DNS pubblici e anche necessario che non siano bloccate le porte:
53 UDP → porta di comunicazione DNS
123 UDP → porta di comunicazione NTP