HOW TO

Configurare firewall su base utente, digital input e time triggered

SIEMENS

Contents

Configurare firewall su base utente, digital input e time triggered

Premessa

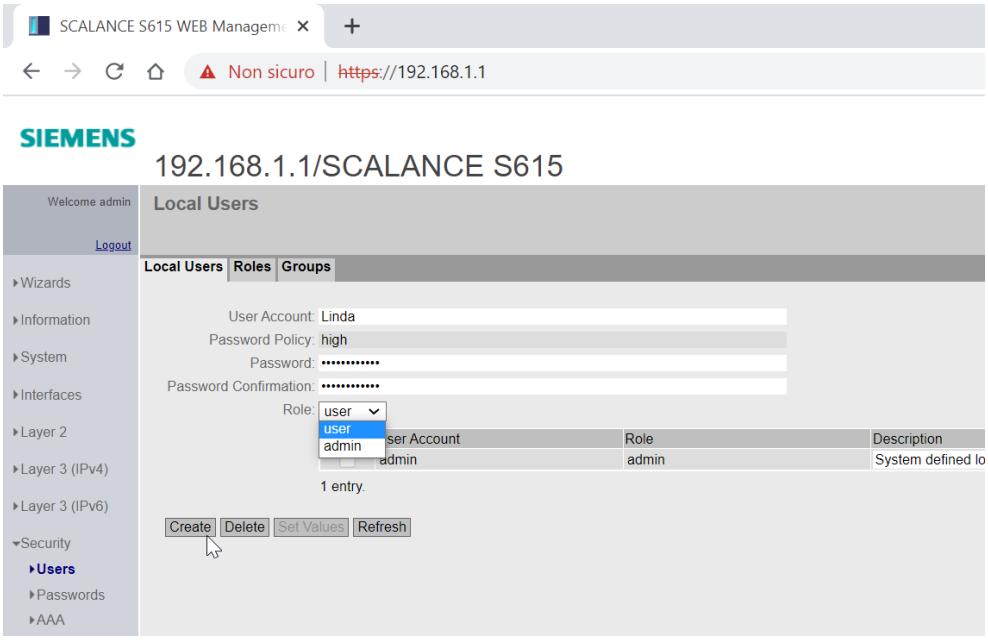
La seguente guida illustra le funzionalità relative ai firewall su base utente, Digital Input e Time Triggered sui modelli Siemens Scalance S e M e come queste possono essere configurate mediante la gestione web (WBM).

Queste funzionalità permettono di inserire delle regole di firewall che possono essere attivate mediante l'inserimento di credenziali (username e password) per un tempo limitato, tramite l'attivazione di un ingresso digitale sullo Scalance o sulla base di una definizione temporale.

La guida è valida per le versioni firmware fino alla 7.1 per Scalance S615/M800 e 2.3 per Scalance SC600. Per l'utilizzo di queste funzionalità si raccomanda l'aggiornamento firmware dei vecchi dispositivi in quanto introdotte di recente.

Configurazione degli utenti per utilizzo nelle regole di firewall

Per utilizzare la funzionalità User Specific, che consente di abilitare regole di firewall su base utente, occorre prima configurare degli utenti. Questi possono essere creati dal menu **Security → Users.** Inserire le credenziali (username e password), specificare il ruolo (user = accesso in sola lettura o admin= accesso in lettura e scrittura) e cliccare su **"Create".**



Una volta creato l'utente, questo va indicato come utente in grado di effettuare l'accesso da remoto. Sotto la voce "Remote Access", selezionare dal menu a tendina il parametro:

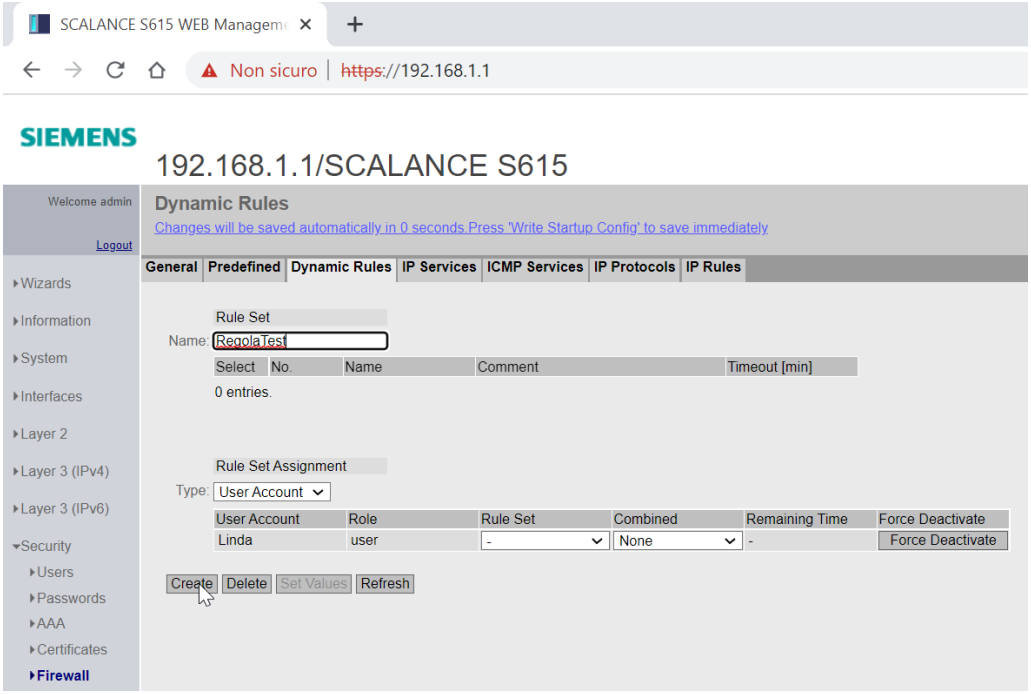
- "only" se si intende creare un utente che ha il solo accesso alle regole di firewall
- "additional" se si intende creare un utente che ha accesso sia alle regole di firewall che al WBM dello Scalance

Al termine della scelta, cliccare **"Set Values".**

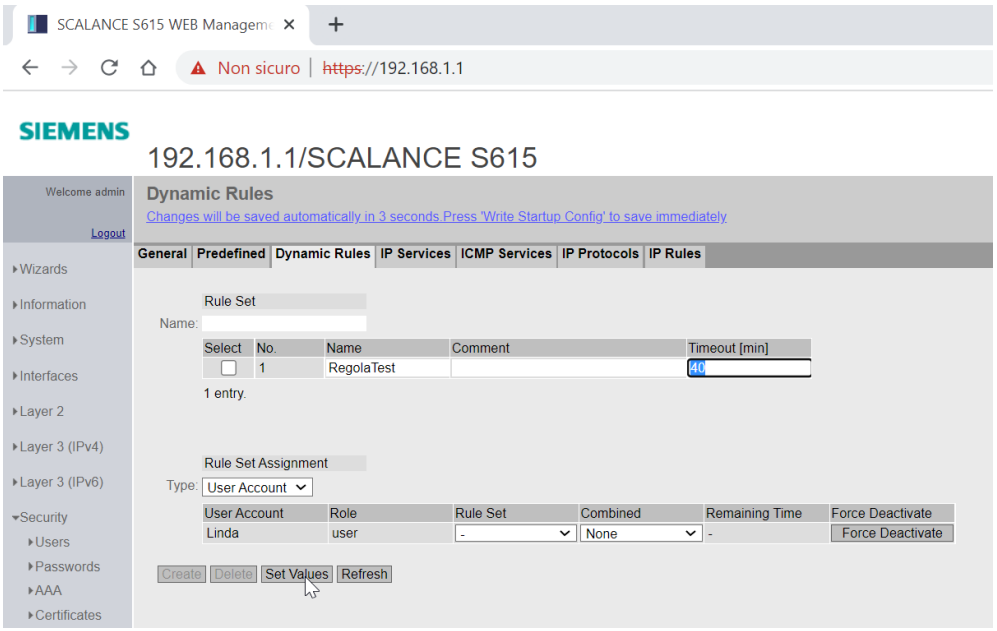
N.B: anche l'utente di default admin ha la possibilità di essere utilizzato per le regole di firewall ma ovviamente è sempre meglio evitare di diffondere le credenziali amministrative preferendo l'uso di utenze ad hoc.

Configurazione regole di firewall con attivazione su base utenti

Successivamente in **Security → Firewall → Dynamic Rules** bisogna creare dei "Rule Set" assegnando un nome identificativo nel campo "Name" e cliccando **"Create".**

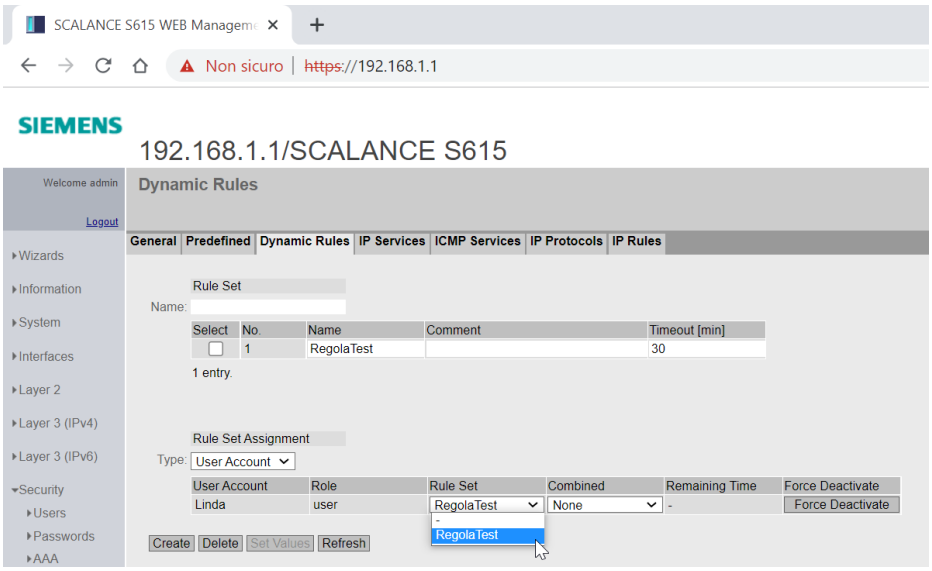


La validità della regola ha un tempo limitato, al default: 30 minuti.
E' possibile modificare la durata sotto la voce "Timeout". A seguito di modifiche, è necessario cliccare su "Set Values".

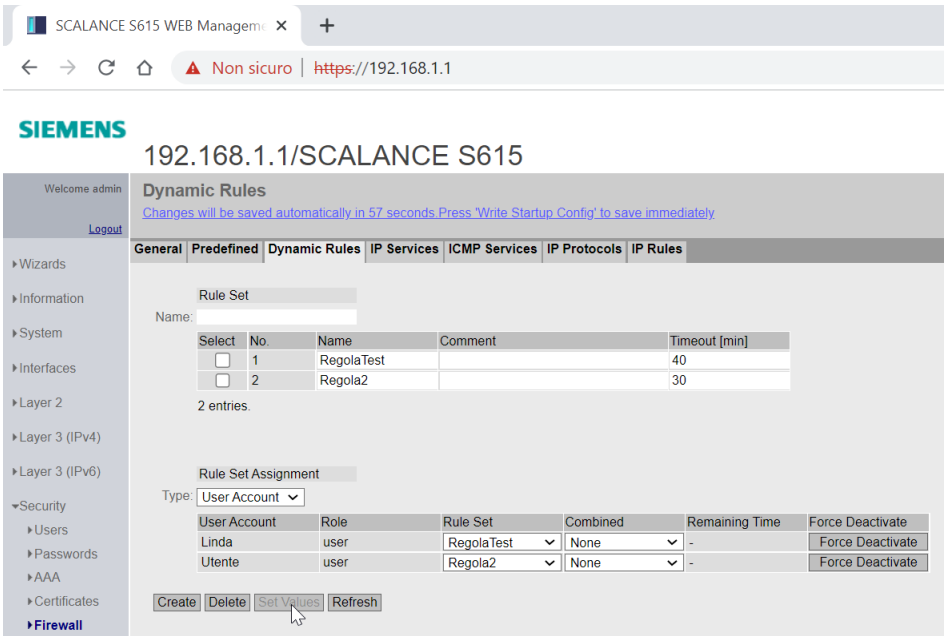


Per definire una regola su base utente, nella tabella relativa al Rule Set Assignement, verificare di avere selezionato "User Account" in corrispondenza della voce "Type".

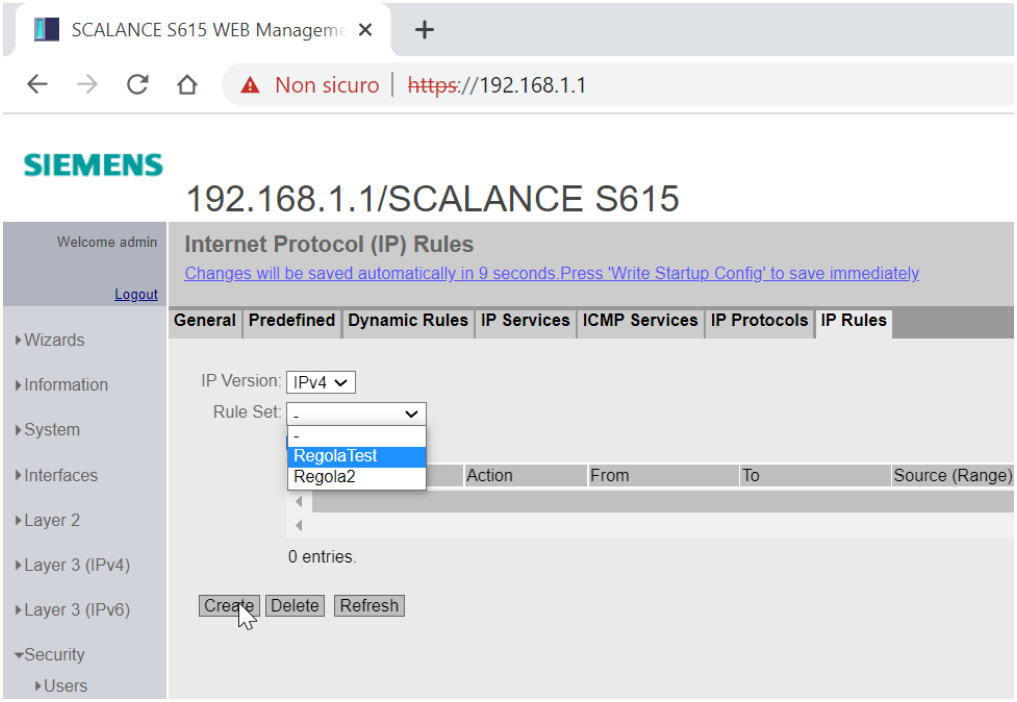
Per l'utente corrispondente alla voce "User Account" assegnare dal menu tendina "Rule Set" la regola definita in precedenza. Cliccare **"Set Values".**
Così facendo, nel caso specifico in esempio, per l'utente Linda risulterà valida la regola RegolaTest.



Se sono stati creati più utenti e più regole, prestare attenzione ad effettuare le associazioni corrette, secondo le proprie necessità.

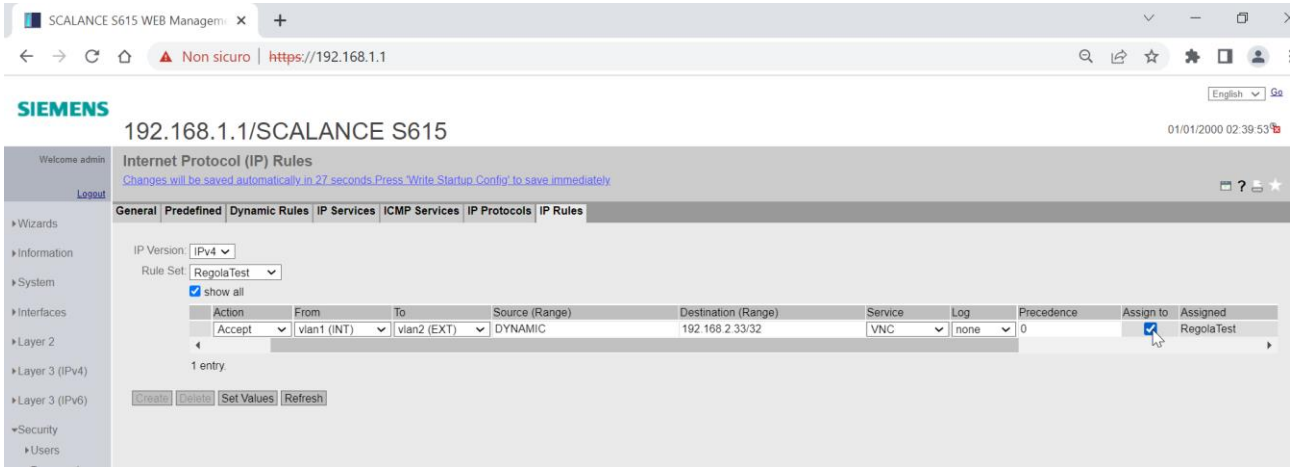


Nel Tab "IP Rules" selezionare la regola dal menu a tendina in corrispondenza della voce "Rule Set". Cliccare sul tasto **"Create".**

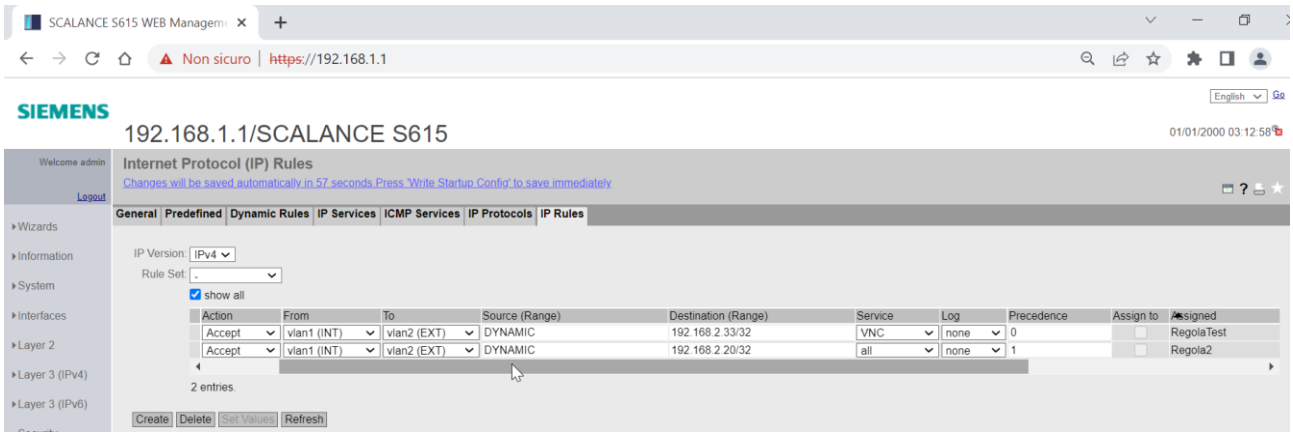


Impostare i campi della tabella a seconda della regola di firewall da implementare (From, To, Source Range, Destination Range, Service). Per una spiegazione dettagliata si rimanda allo specifico manuale.

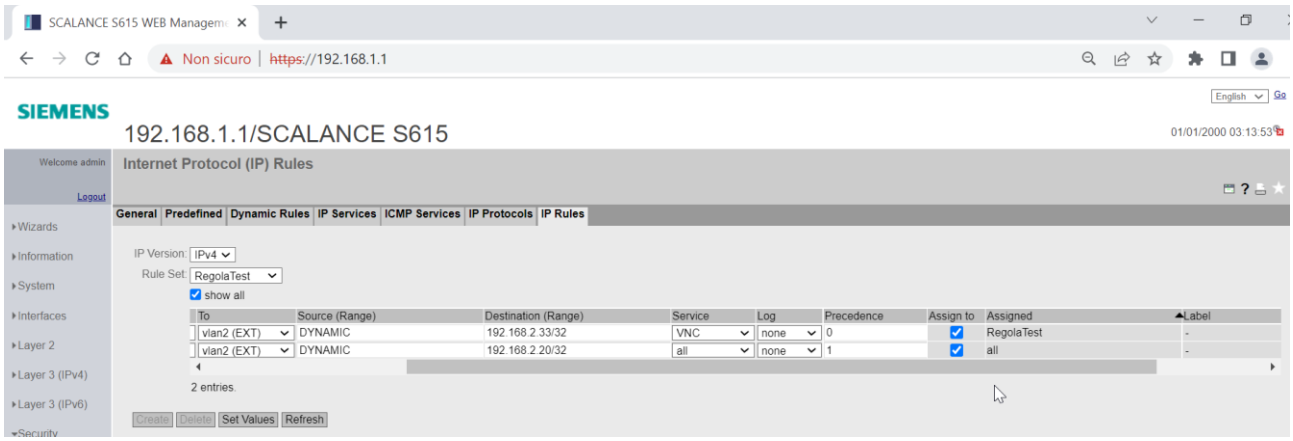
Successivamente spuntare la casella “Assign to” in modo da assegnare la regola di firewall al Rule Set selezionato. Sotto la voce “Assigned” apparirà il nome del Rule Set al quale la regola di firewall è stata assegnata.



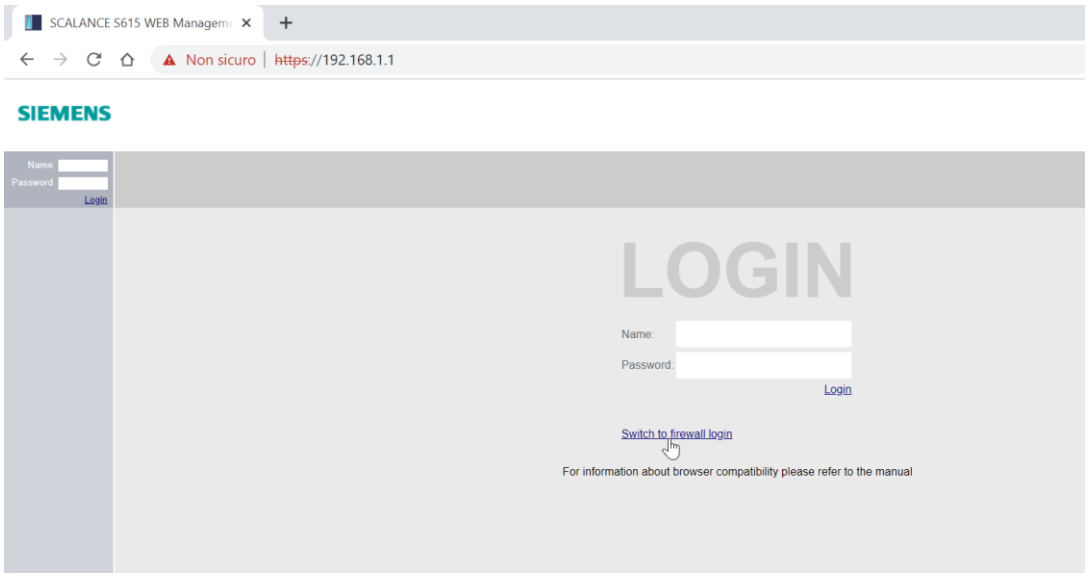
Eseguire la stessa operazione per tutte le regole necessarie. Al termine cliccare su **“Set Values”.**



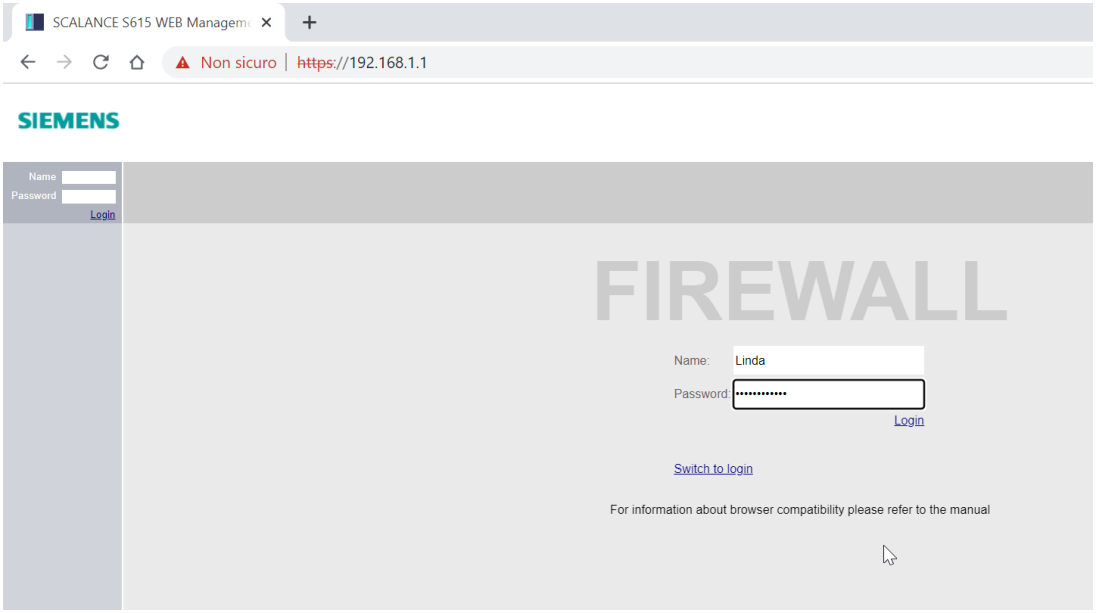
Qualora la stessa regola di firewall venga assegnata a tutti i rule set disponibili, nella colonna “Assigned” compare la voce “all”, come riportato in immagine.
Lo stesso accade se è stato definito un solo rule set.



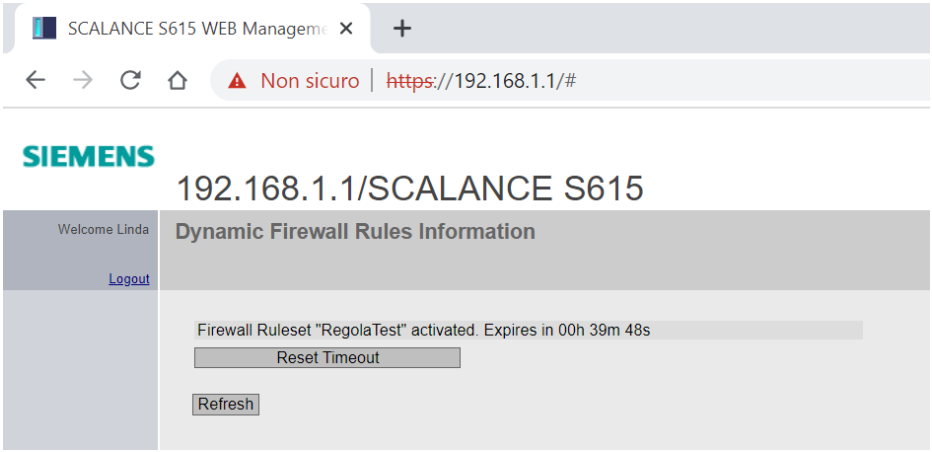
Il campo “Source(Range)”, se precedentemente impostato a 0.0.0.0/0, assume valore DYNAMIC. Questo significa che il “Source(Range)” corrisponde all’indirizzo IP del device da cui l’utente si collega.
Per utilizzare le regole di firewall, l’utente dovrà prima accedere alla pagina web del firewall scegliendo “switch to firewall login”



Nella pagina che si apre, inserire le credenziali dell'utente e cliccare su login.



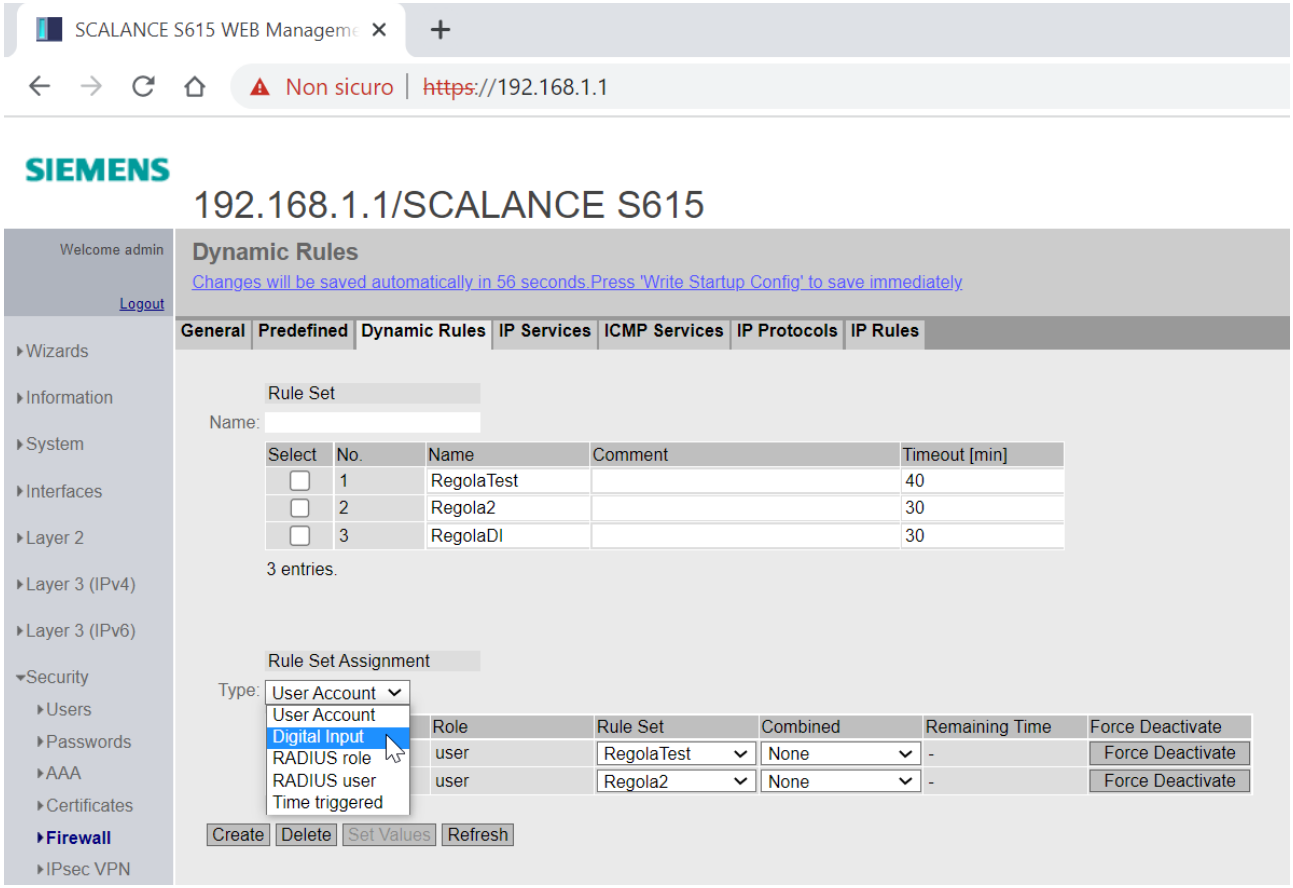
A questo punto la regola funzionerà per il timeout impostato.



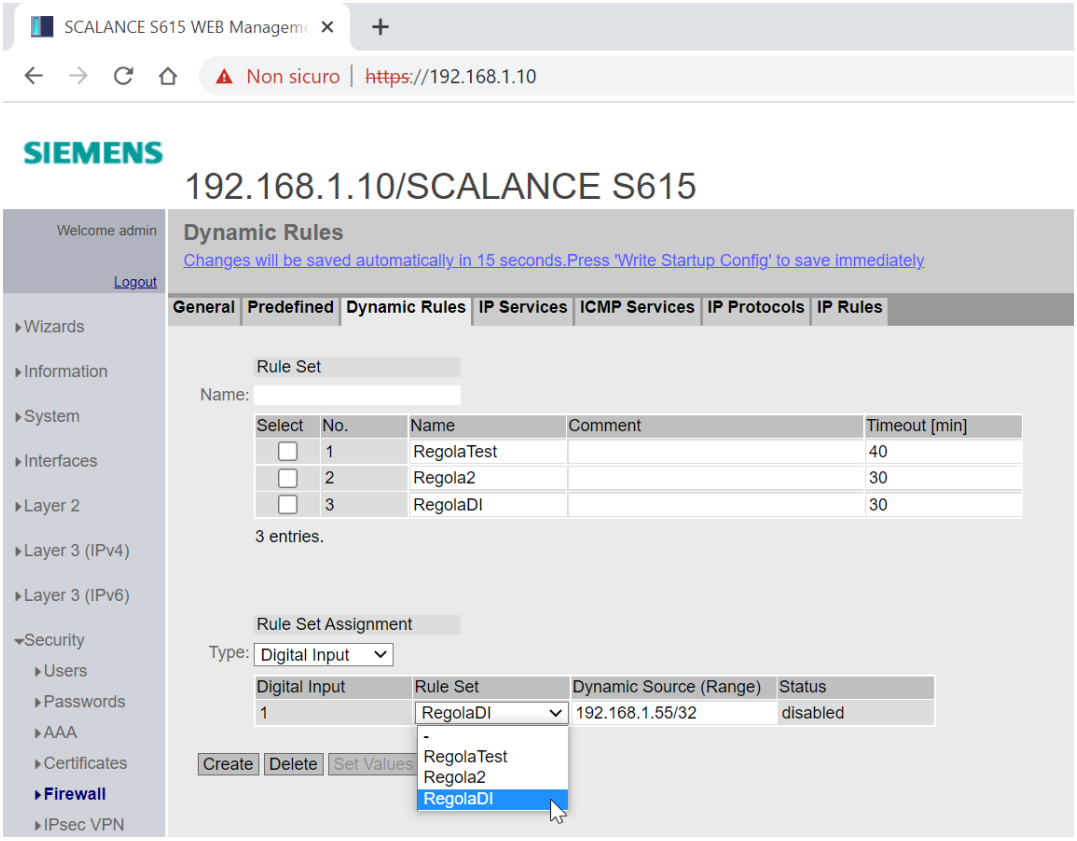
Se si vuole rinnovare il tempo di utilizzo della regola, è possibile resettare il timeout. In questo modo l'utente otterrà nuovamente il tempo iniziale per l'utilizzo della regola.

Configurazione regole di firewall con attivazione su base digital input

Per definire delle regole di firewall attivabili sulla base di un ingresso digitale, procedere in **Security → Firewall → Dynamic Rules** e creare il "Rule Set" assegnando un nome identificativo nel campo "Name" e cliccando **"Create".**
Modificare l'eventuale tempo di Timeout, come spiegato nel capitolo precedente.
Una volta creato il rule set, nella tabella relativa al "Rule Set Assignment", selezionare "Digital Input" dal menu a tendina in corrispondenza della voce "Type".

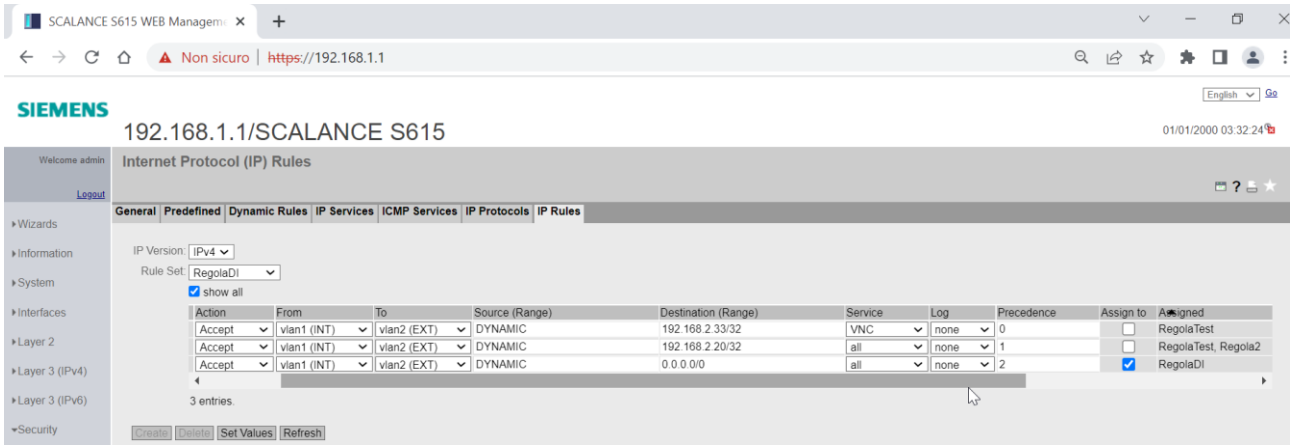


A questo punto assegno il Rule Set al Digital Input selezionando la regola dal menu a tendina in corrispondenza della colonna "Rule Set".



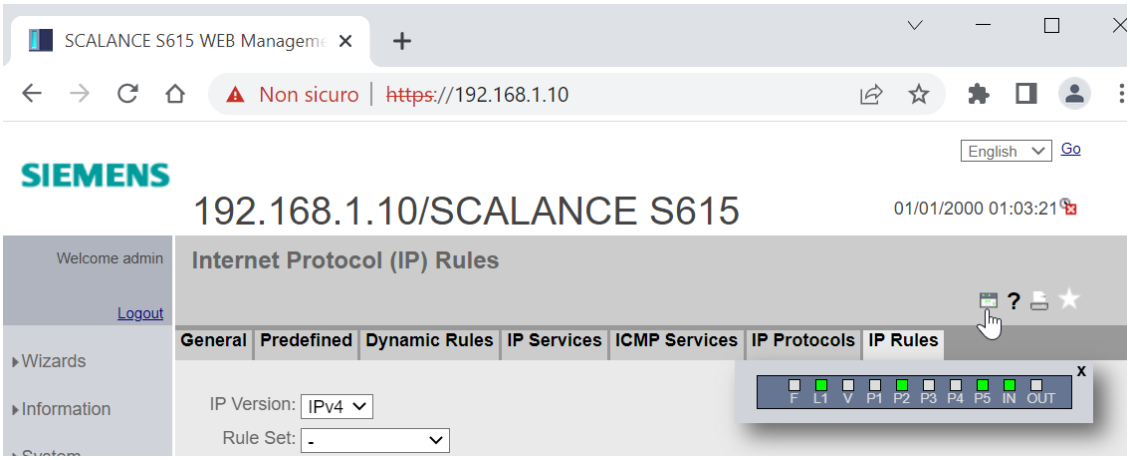
E' possibile specificare gli indirizzi IP autorizzati all'attivazione del digital input, inserendoli nel campo "Dynamic Source (Range)".
Al termine della configurazione, cliccare **"Set Values".**
Nella colonna "Status" è possibile verificare l'attivazione della regola (disabled/enabled).

Il resto della configurazione è del tutto similare al firewall su base utente.
Procede nel tab **"IP Rules"**. Selezionare la regola corrispondente nel menu a tendina "Rule Set" e cliccare su **"Create".**
Dopo aver definito i campi della regola, inserire la spunta in corrispondenza della colonna "Assign to".
Cliccare su "**Set Values**".

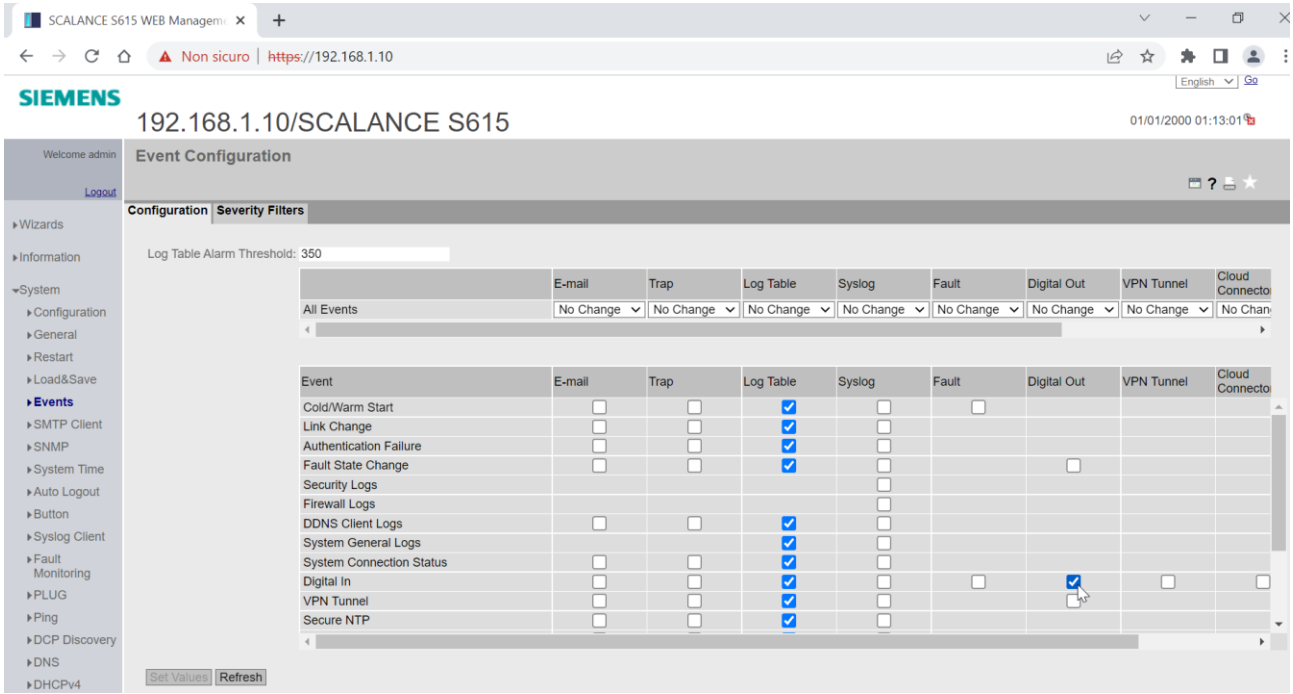


Se il "Source(Range)" era stato definito con 0.0.0.0/0, questo valore viene sostituito dalla voce DYNAMIC e vale quanto specificato in tabella "Rule Set Assignment", come mostrato in precedenza.

Questa regola viene attivata esclusivamente quando viene fornita tensione all'ingresso digitale disponibile sul dispositivo. E' possibile verificare lo status dell'ingresso digitale dal WBM cliccando sul tasto indicato dalla manina nell'immagine qui sotto. Se il quadratino in corrispondenza della dicitura DI è verde, significa che l'ingresso riceve tensione.



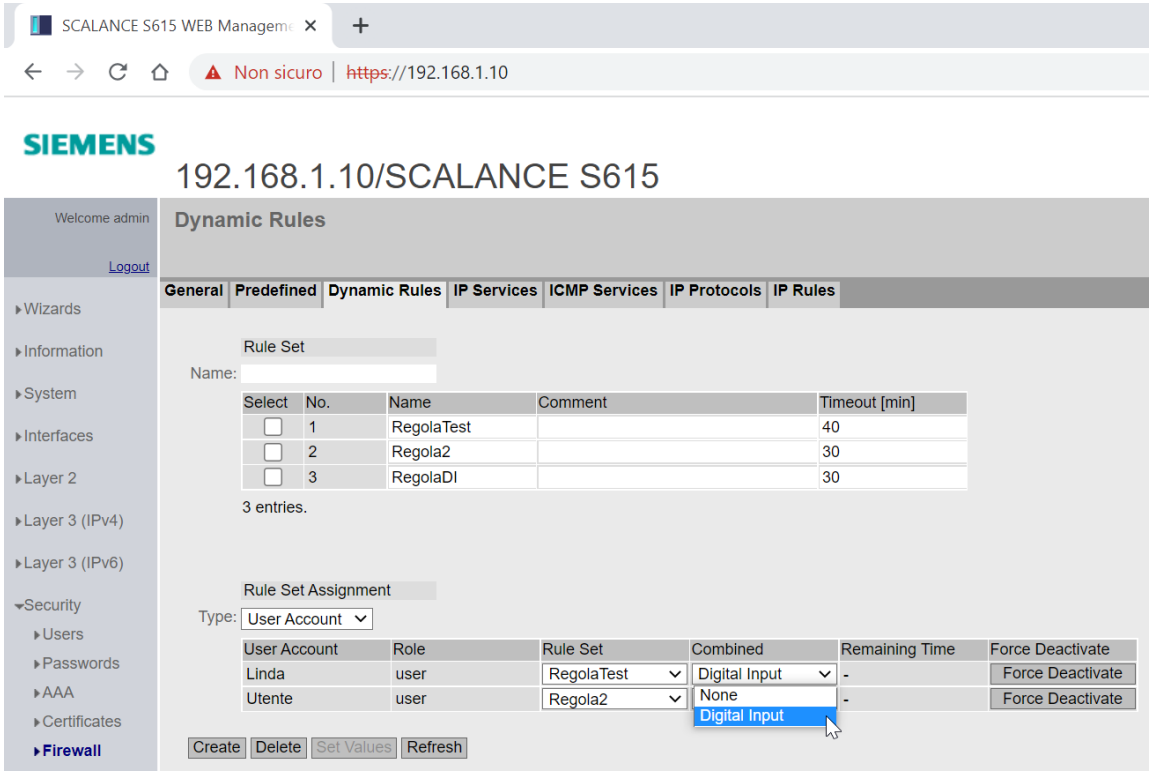
In alternativa è possibile impostare nel menu **System → Events** la **spunta** sulla colonna "Digital Out" in corrispondenza della riga "Digital In". Al termine della configurazione cliccare "Set Values".
In questo modo viene restituito un feedback sottoforma di tensione sui morsetti del DO. La stessa informazione è disponibile sul led DO del dispositivo.



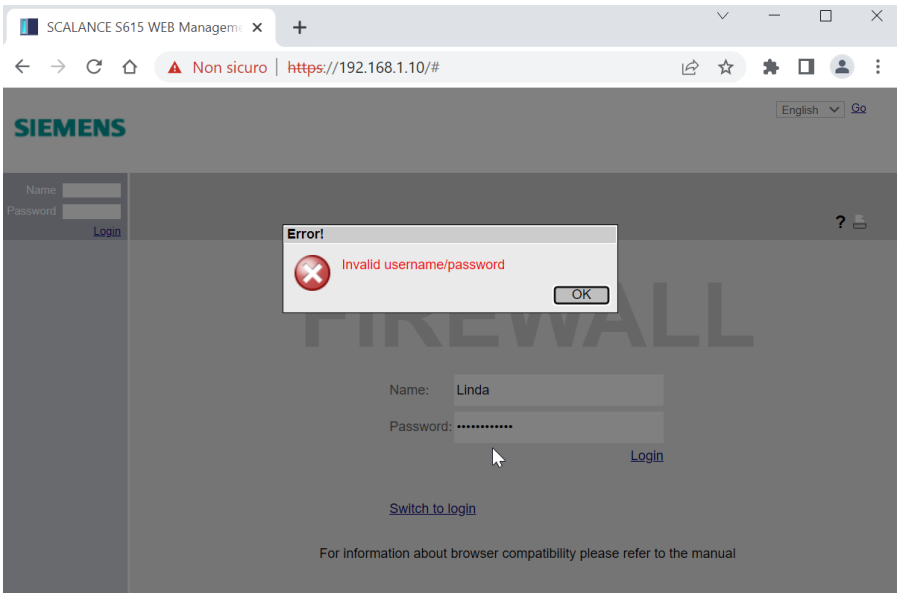
Configurazione di regole di firewall con attivazione su base utente e digital input

E' possibile definire delle regole di firewall attivabili solo se contemporaneamente soddisfatti i requisiti di un corretto login da parte di un utente e di attivazione di un ingresso digitale.
Per configurare questa opzione, riprendere passo-passo le istruzioni riportate nel paragrafo "Configurazione regole di firewall con attivazione su base utenti" trattato in precedenza, dopo aver correttamente definito gli utenti (vedi paragrafo: "Configurazione degli utenti per utilizzo nelle regole di firewall").

Oltre ai passaggi precedentemente descritti, selezionare dal menu a tendina in corrispondenza della colonna "Combined" la voce **"Digital Input"** per quei rule set per i quali entrambi i criteri, utente e digital input, devono essere soddisfatti contemporaneamente per l'attivazione della regola. Cliccare su **"Set Values"**.

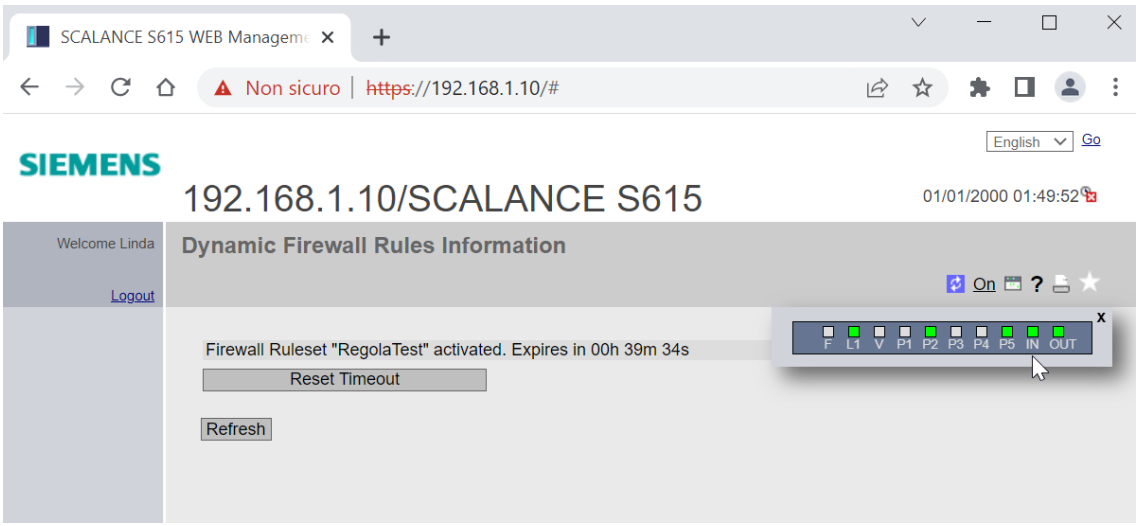


Per l'attivazione della regola, procedere sulla pagina del WBM e cliccare su "switch to firewall login", come già indicato in precedenza.
Inserire le credenziali corrette.
Se l'ingresso digitale non è alimentato mentre viene effettuato il login, viene generato un messaggio "Invalid username/password".



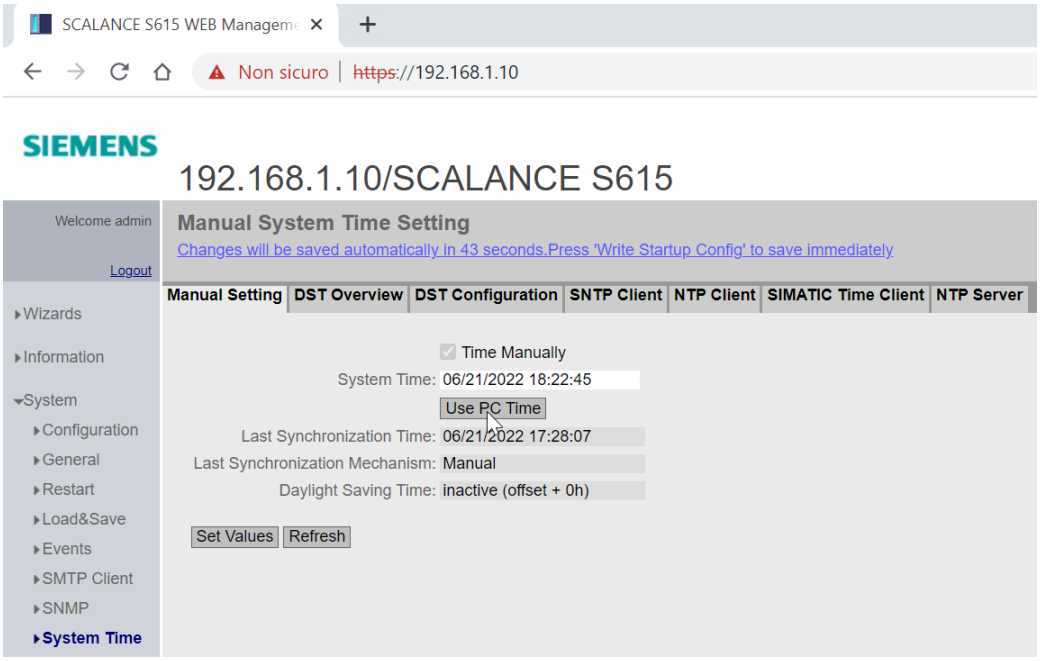
L'attivazione della regola avviene correttamente quando entrambi i requisiti vengono verificati, utente e ingresso digitale!

E' quindi opportuno procedere con il login sul firewall garantendo la tensione sui morsetti dell'ingresso digitale.

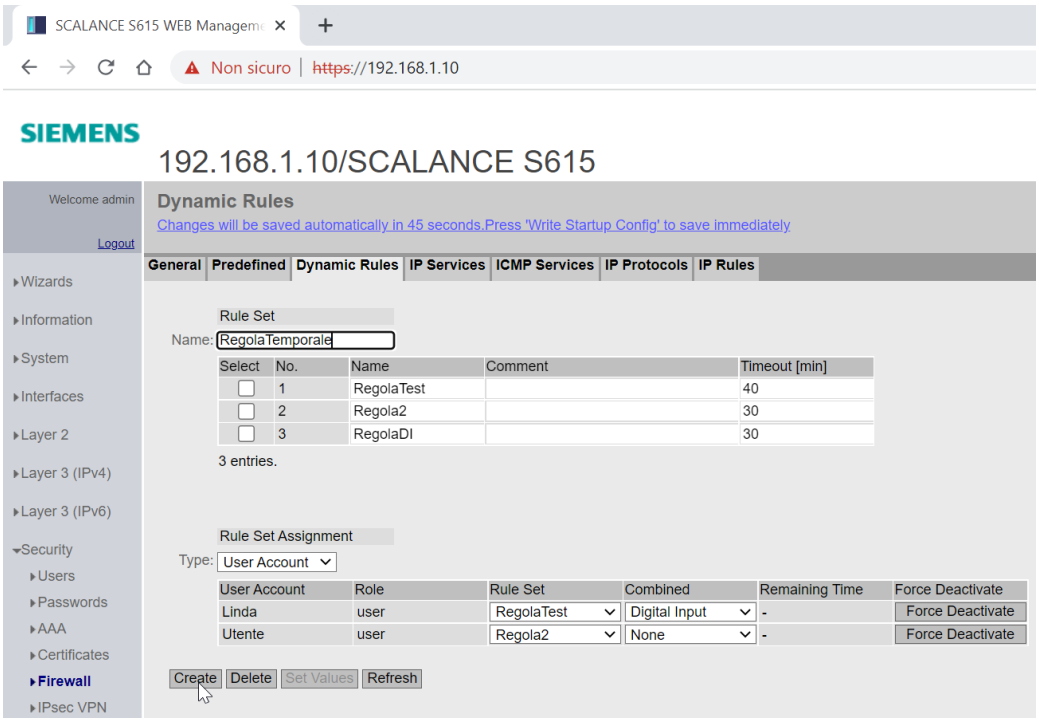


Configurazione di regole di firewall con attivazione su base durata temporale

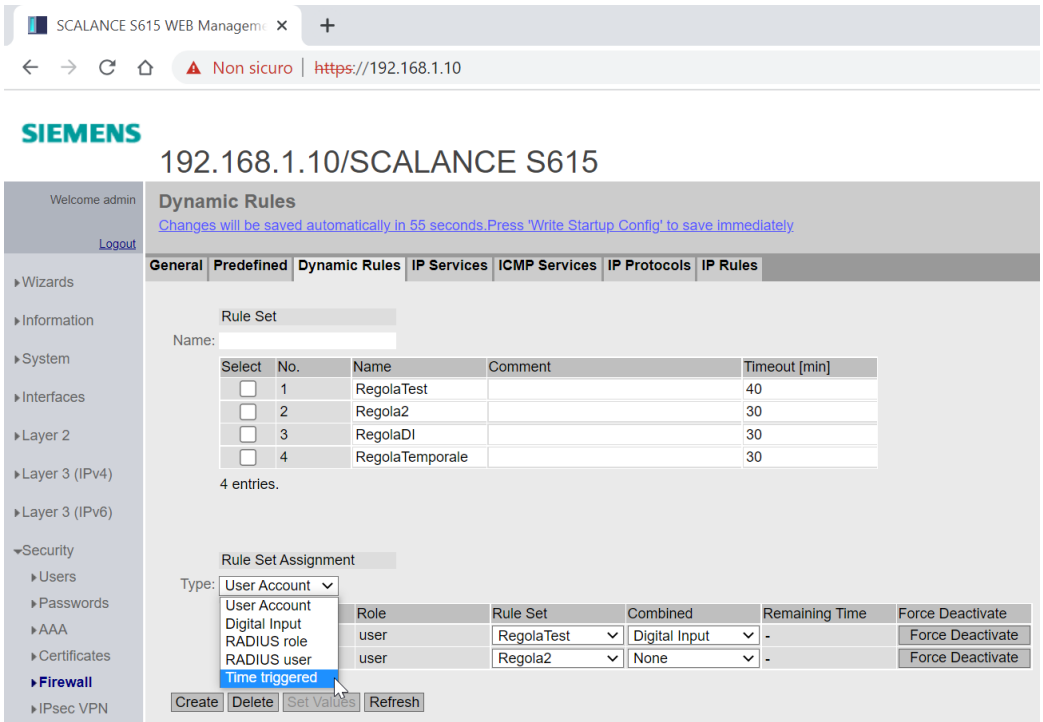
Per definire delle regole di firewall attivabili su base temporale procedere in primo luogo con la sincronizzazione dell'orario del dispositivo. Questo è un prerequisito fondamentale per la corretta attivazione delle regole.
Procedere dal menu System → System Time.
E' possibile assegnare il tempo del PC al dispositivo cliccando su "Use PC Time" e poi applicare le modifiche cliccando su "Set Values".
Questa scelta, seppur pratica, non è l'ottimale. Per ulteriori dettagli, consultare la guida dedicata.



Dopo aver correttamente impostato il tempo del dispositivo, procedere alla creazione del rule set, come visto in precedenza.
Accedere al menu **Security → Firewall → Dynamic Rules.**
Inserire un nome identificativo in corrispondenza del campo "Name" e cliccare su **"Create"**.



Selezionare la voce "**Time Triggered**" dal menu "Type" in corrispondenza della tabella "Rule Set Assignment".



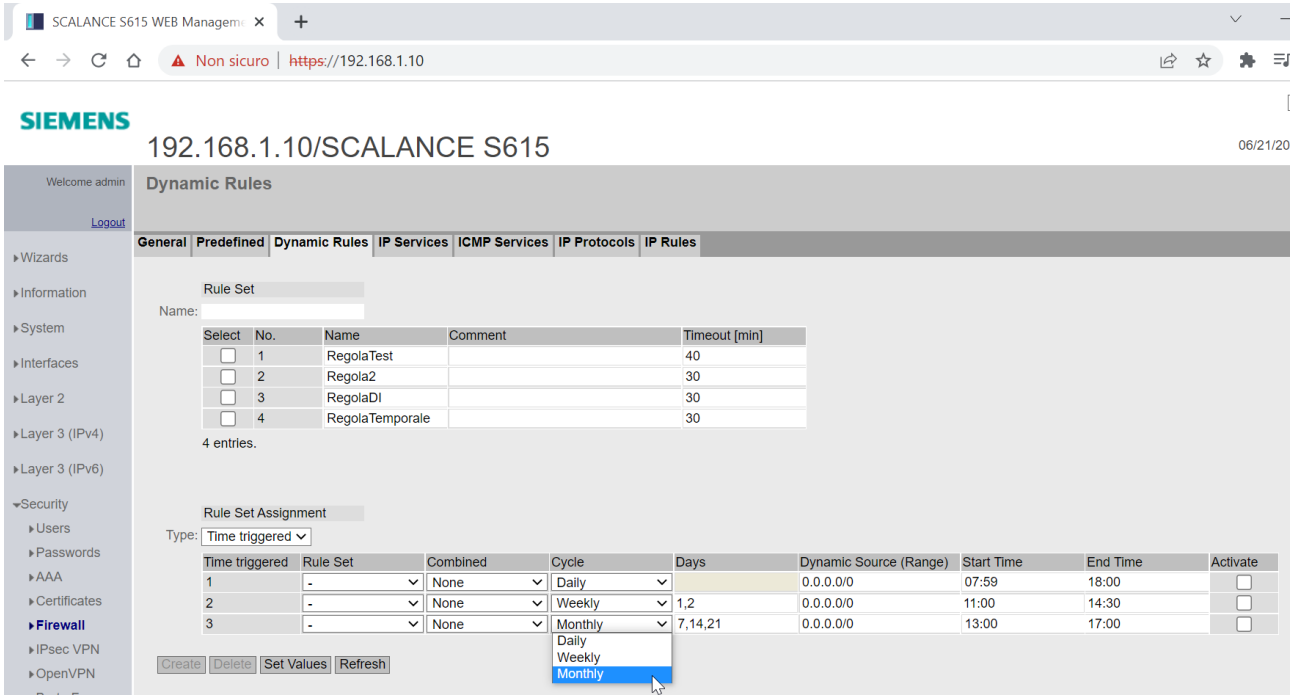
E' possibile definire fino a tre regole temporali differenti andando a personalizzare le righe della tabella.
I trigger temporali possono essere eseguiti su base giornaliera, settimanale o mensile: specificare con il menu a tendina in corrispondenza della colonna "Cycle" la ripetizione del trigger temporale.

- Selezionando "**Daily**", l'intervallo temporale viene definito per ogni giorno

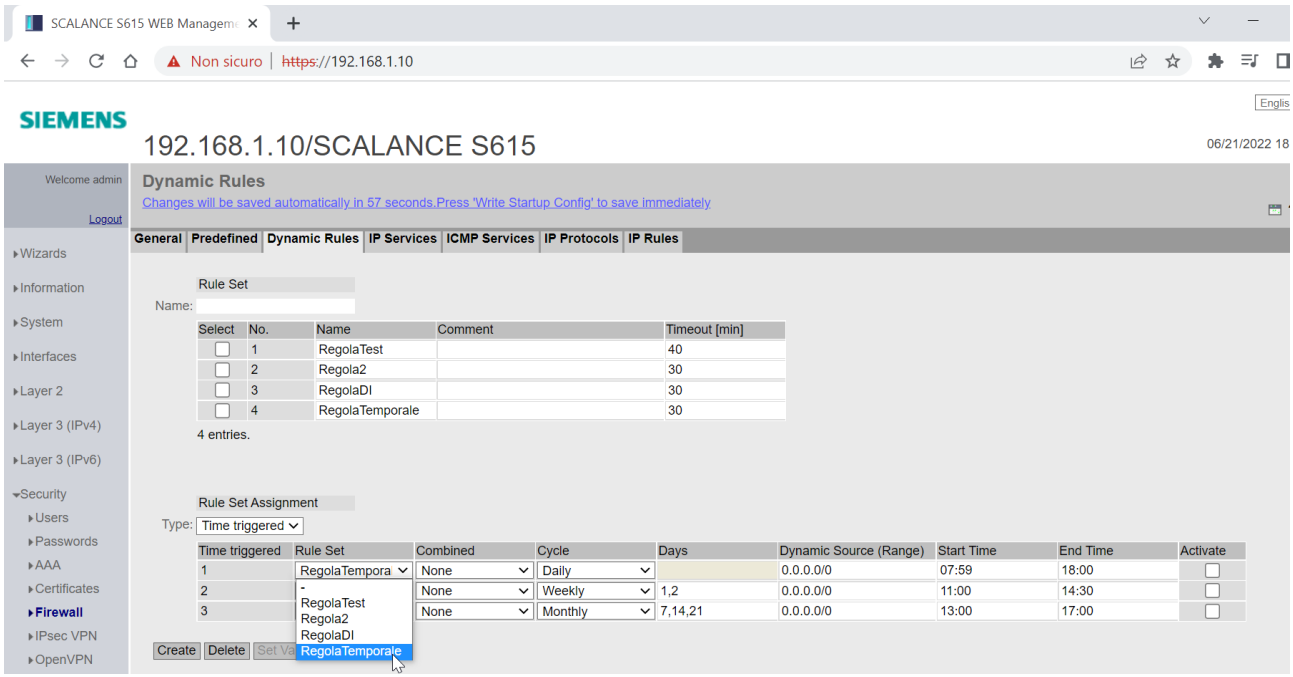
- Selezionando "**Weekly**", l'intervallo temporale viene definito per i giorni della settimana specificati in corrispondenza della colonna "**Days**". Possono essere assegnati valori da 1 a 7, dove 1 indica il lunedì e 7 la domenica. Per una selezione di più giorni, intervallare i valori numerici con una virgola.
- Selezionando "**Monthly**", l'intervallo temporale viene definito per i giorni del mese specificati in corrispondenza della colonna "**Days**". Possono essere assegnati valori da 1 a 31. Per una selezione di più giorni, intervallare i valori numerici con una virgola.

In corrispondenza delle colonne "**Start Time" ed "End Time**" specificare rispettivamente l'orario di inizio e di fine dell'intervallo temporale in questione.

Nel caso riportato in immagine, la riga 1 della tabella definisce l'intervallo di tempo che va dalle 7:59 alle 18 di ogni giorno, la riga 2 definisce l'intervallo di tempo che va dalle 11 alle 14:30 dei giorni lunedì e martedì della settimana, la riga 3 definisce l'intervallo di tempo che va dalle 13 alle 17:00 dei giorni 7, 14 e 21 del mese.

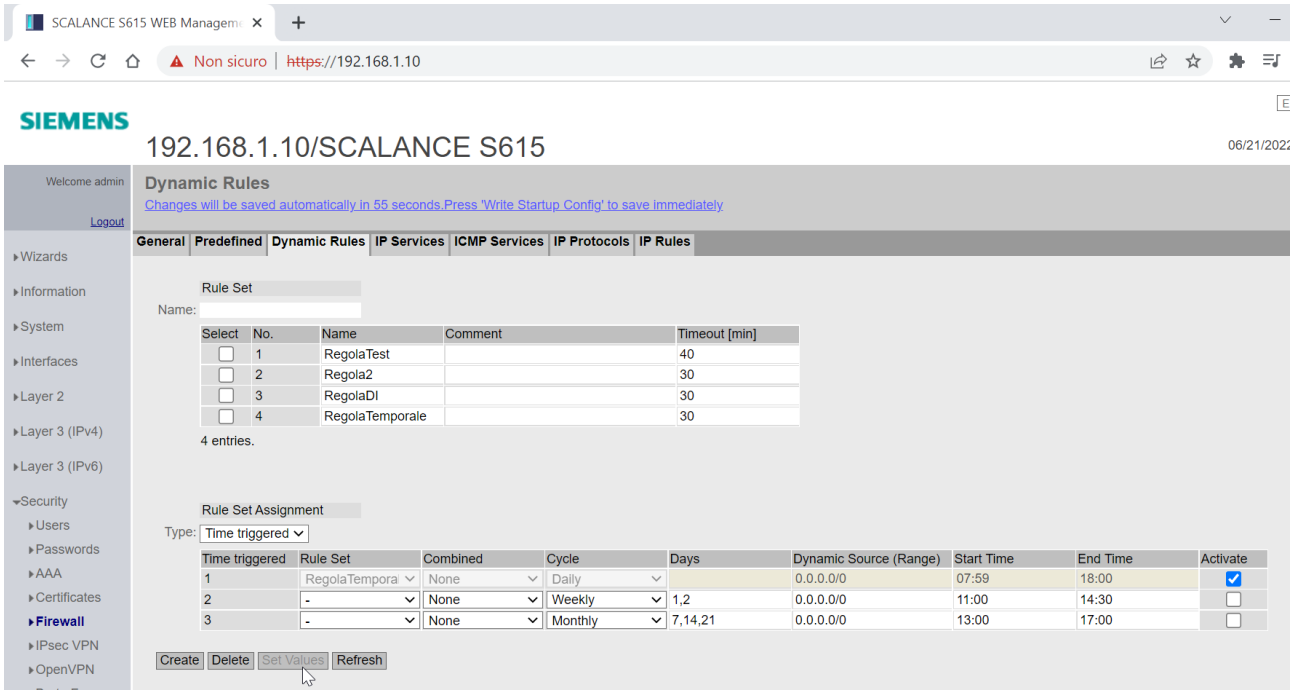


Assegnare la riga di interesse al rule set precedentemente creato selezionandolo dal menu a tendina in corrispondenza della colonna "**Rule Set**".
Cliccare "**Set Values**".



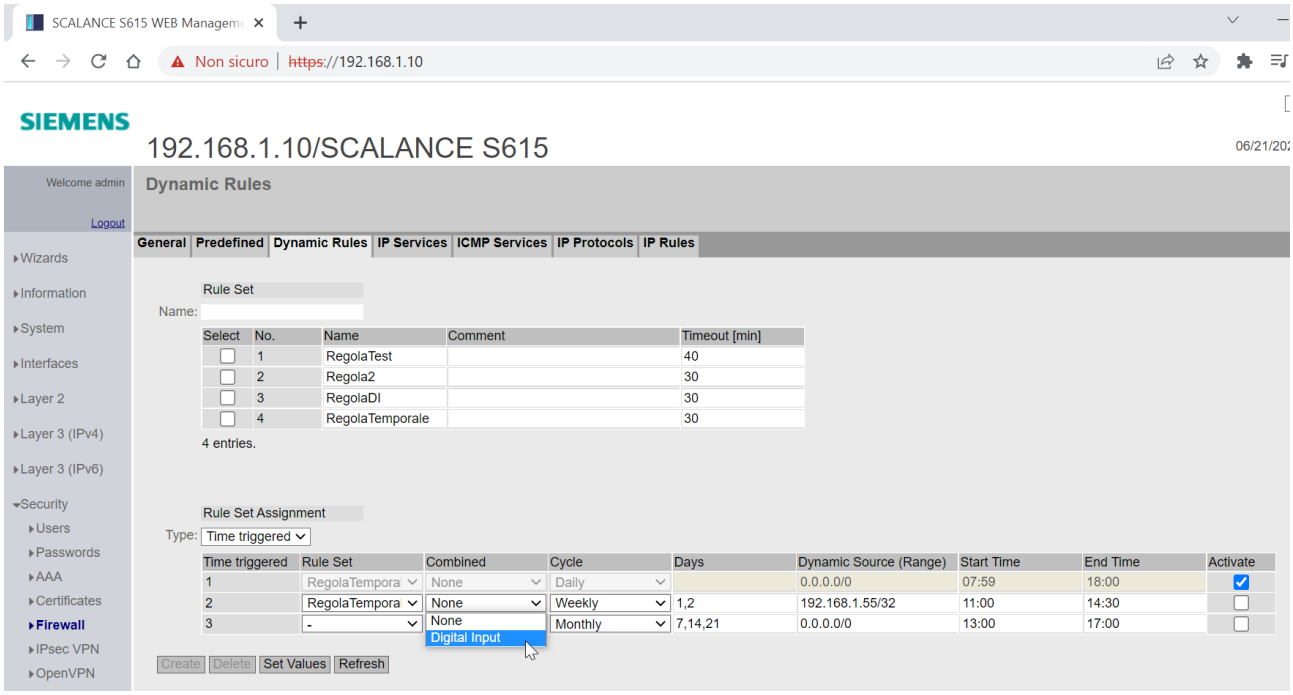
N.B: Per poter correttamente utilizzare la regola definita è necessario abilitare la spunta in corrispondenza della colonna "Activate"! e cliccare "Set Values".

I campi della riga attivata assumeranno colore giallo e non potranno essere modificati se non disabilitando la spunta.

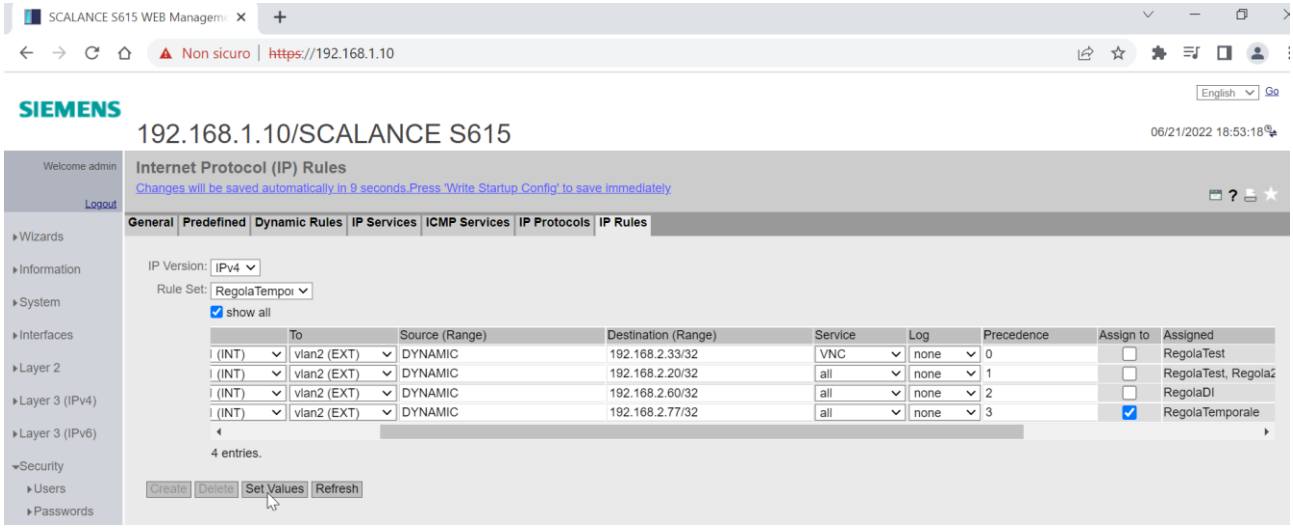


E' possibile specificare gli indirizzi IP autorizzati per la comunicazione quando la regola viene attivata, inserendoli nel campo "**Dynamic Source (Range)**".
E' altresì possibile combinare l'utilizzo delle regole su base temporale con quelle legate all'attivazione dell'ingresso digitale.

Per creare una regola che richieda il verificarsi contemporaneo di queste due condizioni, selezionare dal menu a tendina in corrispondenza della colonna **"Combined"** la voce **"Digital Input"**.
Al termine della configurazione, cliccare **"Set Values".**



Il resto della configurazione è del tutto similare a quanto riportato per i casi precedenti.
Procede nel tab **"IP Rules"**. Selezionare la regola corrispondente nel menu a tendina "Rule Set" e cliccare su **"Create".**
Dopo aver definito i campi della regola, inserire la spunta in corrispondenza della colonna "Assign to".
Cliccare su "**Set Values**".



La regola viene attivata automaticamente al verificarsi delle condizioni temporali specificate.