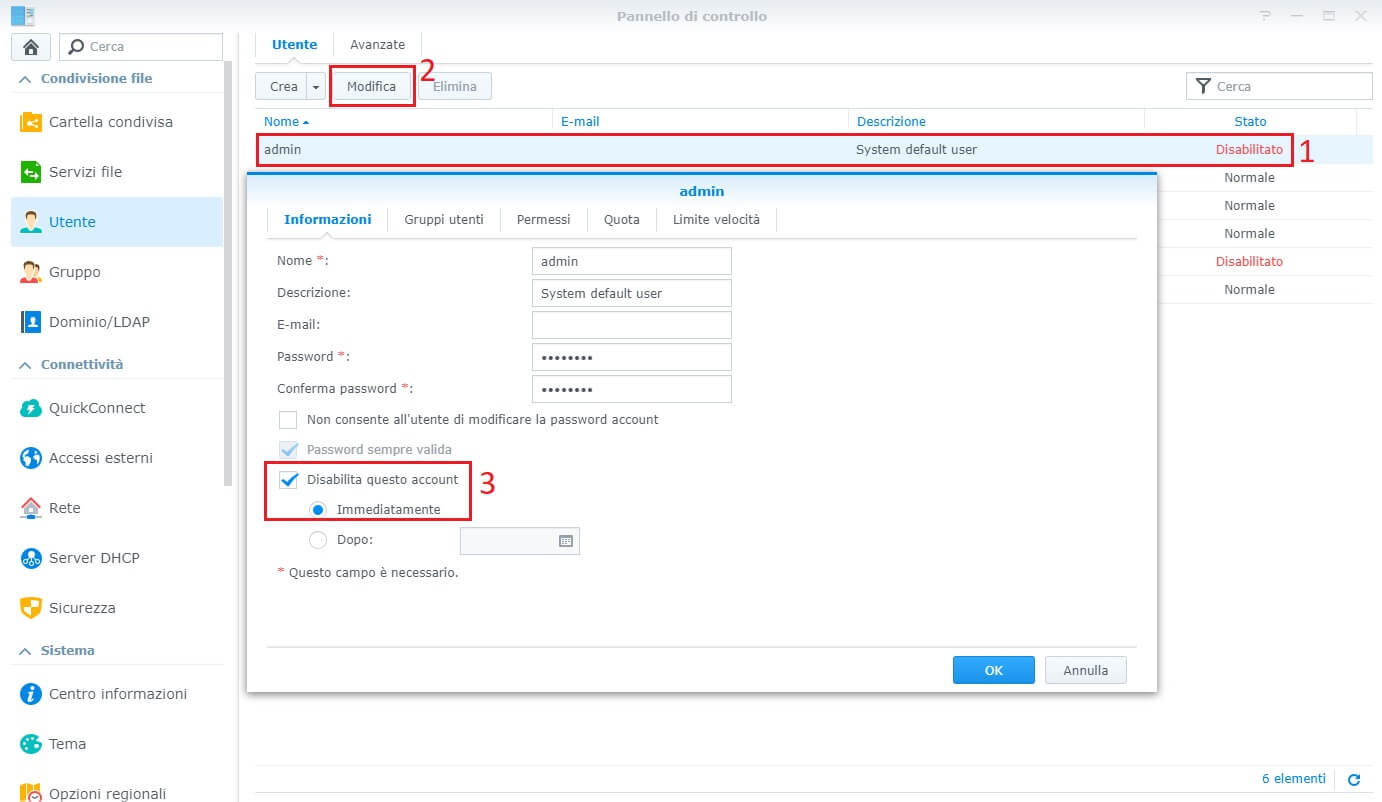
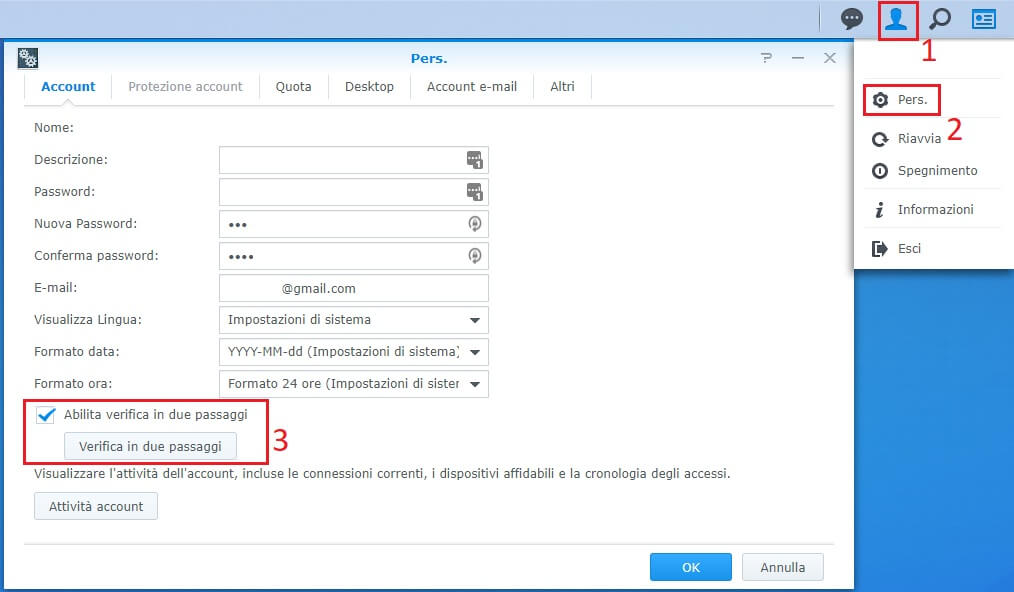
**Opzioni sicurezza nas Synology**

1. disabilitare l’account amministratore attivo di default



1. impostare la sicurezza e la complessità delle password dal pannello di controllo > Utenti e Gruppi > Avanzate > Impostazioni Password
2. abilitare l’autenticazione a due fattori dal percorso Opzioni > Personale > Account



Vi comparirà una schermata dove vi verrà chiesta una mail di emergenza, in caso smarriate il vostro telefono. Cliccate avanti e vi comparirà un QR code.

Sul vostro smartphone installate Google Authenticator e aprite l’applicazione. Cliccate sul simbolo “+” e eseguite la scansione del QR mostratovi dal NAS.

Non appena il QR code verrà letto vi comparirà un codice che dovrete inserire nella finestra che vi mostrerà il NAS per verificare che sia tutto ok. Cliccate su “Avanti” e avrete finito.

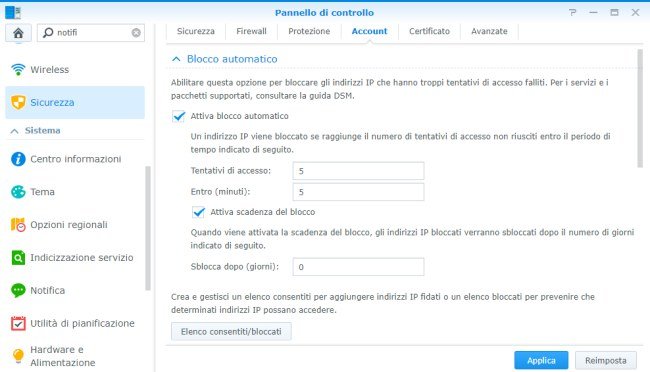
Se perdete il telefono, disinstallate l’app o formattate il vostro telefono, dovrete rifare tutta la procedura, andando a recuperare il codice momentaneo tramite la mail inserita ad inizio procedura.

1. limitare il numero di tentativi di accesso da parte di un indirizzo IP dal percorso Pannello di Controllo > Sicurezza > Account

Puoi configurare una serie di impostazioni di sicurezza nel Pannello di controllo > scheda Sicurezza per proteggere i tuoi account utente.

Blocco automatico IP

Apri il Pannello di controllo e vai su Sicurezza > Blocco automatico . Abilita il blocco automatico per bloccare automaticamente gli indirizzi IP dei client che non riescono ad accedere entro un determinato numero di volte e periodo. Gli amministratori possono anche inserire nella blacklist indirizzi IP specifici per prevenire potenziali attacchi di forza bruta o denial-of-service.



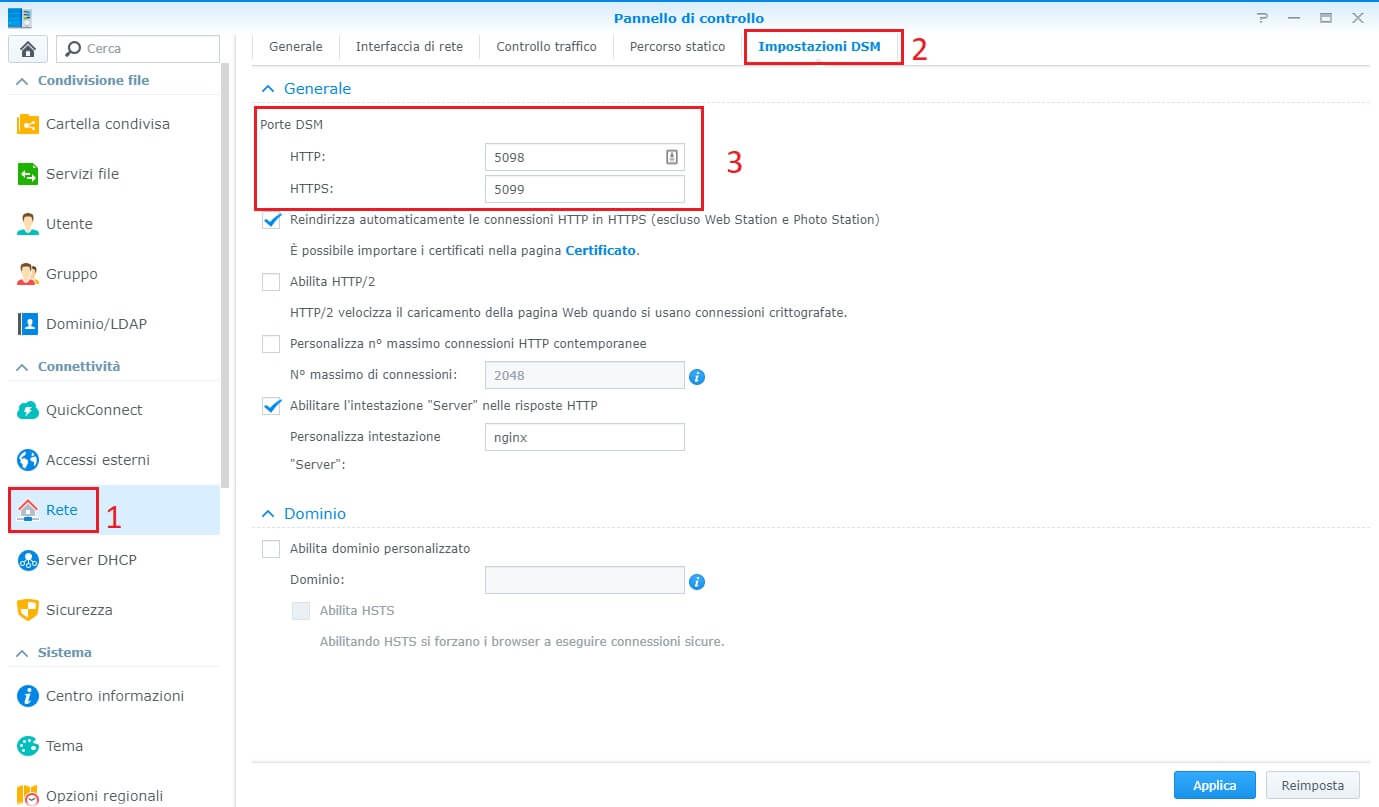
1. abilitare la protezione DDOS dal percorso Pannello di Controllo > Sicurezza > Protezione > Abilitare protezione DoS
2. cambiare le porte utilizzate di default per l’accesso, le porta preimpostate sono:

HTTP: 5000

HTTPS: 5001

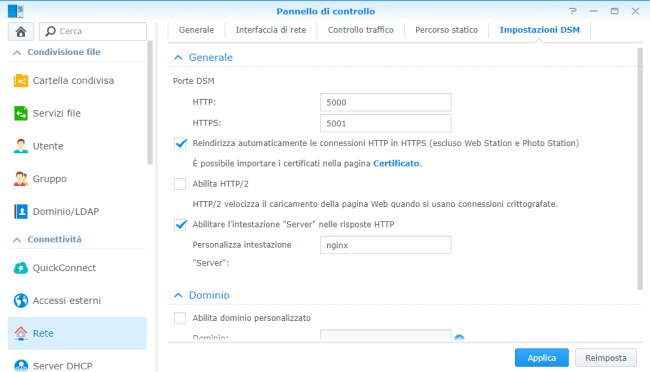
SSH: 22

possibile farlo dal percorso Pannello di Controllo > Terminal & SNMP > Terminal > Porte SSH Predefinite. È anche una buona idea cambiare la porta SSH (22) predefinita se usi regolarmente l'accesso alla shell.



Nel campo “HTTP” e “HTTPS” inserite il numero che volete compreso tra 1500 e 10000. E’ consuetudine inserire nel campo “HTTPS” un valori maggiore di UNA unità rispetto al valore impostato su “HTTP“, ma non è un obbligo.

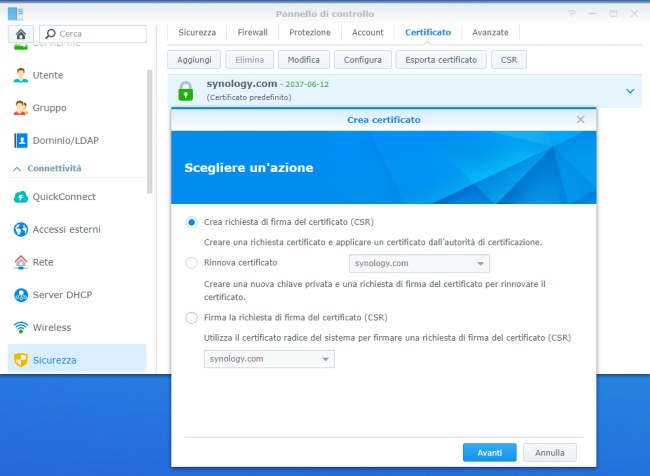
1. Abilita HTTPS Con HTTPS abilitato, puoi crittografare e proteggere il traffico di rete tra Synology NAS e i client connessi, che protegge dalle forme comuni di intercettazione o attacchi man-in-the-middle. Vai su Pannello di controllo > Rete > Impostazioni DSM . Seleziona la casella di controllo Reindirizza automaticamente le connessioni HTTP a HTTPS



Al riavvio dei servizi web sul NAS Synology, si otterrà un errore molto simile al seguente: **connessione privata** . Sebbene, di primo acchito, l'errore possa sembrare piuttosto minaccioso, la sua comparsa è del tutto normale perché il NAS Synology sta sì utilizzando una connessione HTTPS ma essa non impiega alcun certificato digitale valido, rilasciato da un'autorità di certificazione riconosciuta.

Per procedere, bisognerà fare clic su Avanzate e quindi su Procedi su… (non sicuro).

Per far scomparire l'errore relativo al certificato digitale non valido, si deve digitare Sicurezza nella casella di ricerca del Pannello di controllo, selezionare la scheda Certificato e cliccare sul pulsante CSR.



Scegliendo Crea richiesta di firma del certificato si otterrà un file compresso contenente il file .CSR da sottoporre a un'autorità di certificazione per ottenere il certificato digitale corrispondente al nome a dominio indicato.

I NAS Synology integrano anche una funzionalità per ricevere (e rinnovare) un certificato gratuito attraverso il servizio Let's Encrypt:

1. HTTPS Parte 2 – Crittografiamo

I certificati digitali svolgono un ruolo chiave nell'abilitazione di HTTPS, ma sono spesso costosi e difficili da mantenere, soprattutto per gli utenti non aziendali. DSM dispone del supporto integrato per Let's Encrypt, un'organizzazione di emissione di certificati gratuita e automatizzata, per consentire a chiunque di proteggere facilmente le proprie connessioni.

Se hai già un dominio registrato o stai utilizzando DDNS, vai su Pannello di controllo > Sicurezza > Certificato . Fai clic su Aggiungi un nuovo certificato > Ottieni un certificato da Let's Encrypt , per la maggior parte degli utenti, dovresti selezionare "Imposta come certificato predefinito"\*. Inserisci il tuo nome di dominio per ottenere un certificato. Una volta ottenuto un certificato, assicurati che tutto il tuo traffico passi attraverso HTTP

1. esegui Security Advisor Security Advisor è un'applicazione preinstallata in grado di scansionare il NAS alla ricerca di problemi di configurazione DSM comuni
2. crittografa le cartelle condivise. Per crittografare le cartelle condivise esistenti, vai su Pannello di controllo > Cartella condivisa e Modifica la cartella. Imposta una chiave di crittografia nella scheda Crittografia e DSM inizierà a crittografare la cartella. Consigliamo vivamente di salvare il file chiave generato in una posizione sicura, poiché i dati crittografati non possono essere recuperati senza la passphrase utilizzata o il file chiave.