Configurazione di Show VPN Client su RV042, RV042G e RV082 VPN Router tramite Windows

Obiettivo

Una rete privata virtuale (VPN, Virtual Private Network) consente agli utenti remoti di connettersi virtualmente a una rete privata tramite Internet. Una VPN da client a gateway consente di connettere il desktop o il laptop di un utente a una rete remota utilizzando software client VPN. Le connessioni VPN da client a gateway sono utili per i dipendenti remoti che desiderano connettersi in modo sicuro alla rete aziendale in modalità remota. Shrew VPN Client è un software configurato su un dispositivo host remoto che fornisce una connettività VPN facile e sicura.

L'obiettivo di questo documento è mostrare come configurare Show VPN Client per un computer che si connette a un RV042, RV042G o RV082 VPN Router.

Nota: in questo documento si presume che il client VPN Shrew sia già stato scaricato sul computer Windows. In caso contrario, è necessario configurare una connessione VPN da client a gateway prima di poter avviare la configurazione di Shrew VPN. Per ulteriori informazioni su come configurare la VPN da client a gateway, fare riferimento a *Configurazione di un tunnel di accesso remoto (da client a gateway) per i client VPN su router VPN RV042, RV042G e RV082*.

Dispositivi interessati

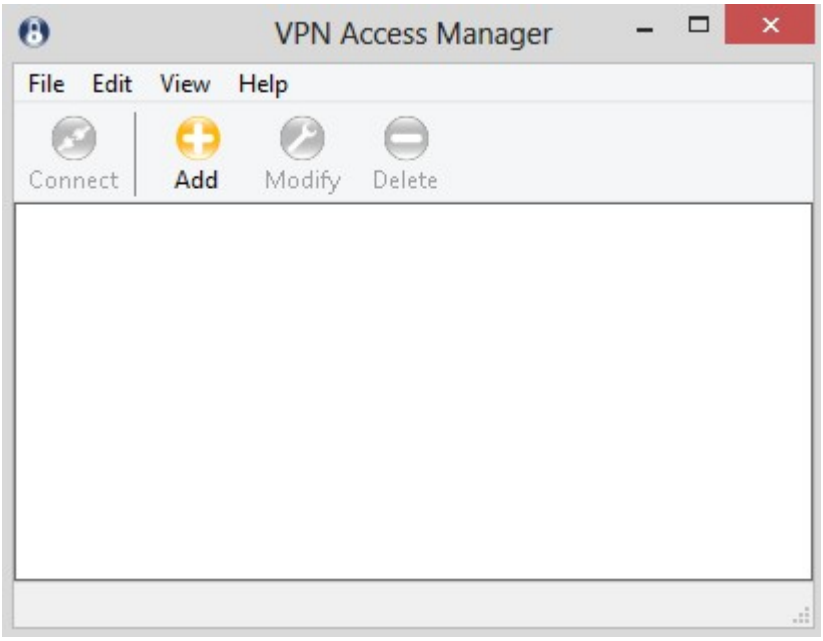
RV042
RV042G
RV082

Versione del software

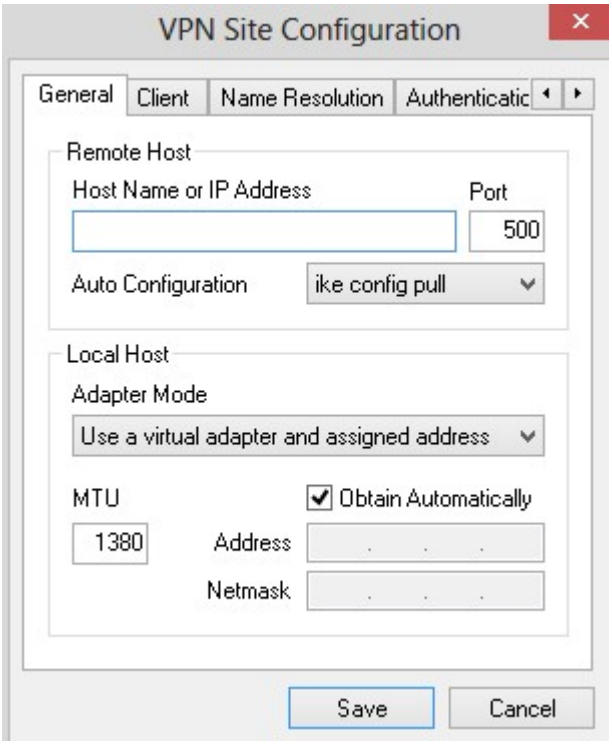
·v4.2.2.08

Configurare la connessione client VPN su Windows

Passaggio 1. Fare clic sul **programma Visualizza client VPN** nel computer e aprirlo. Viene visualizzata la finestra *Show Soft VPN Access Manager*.

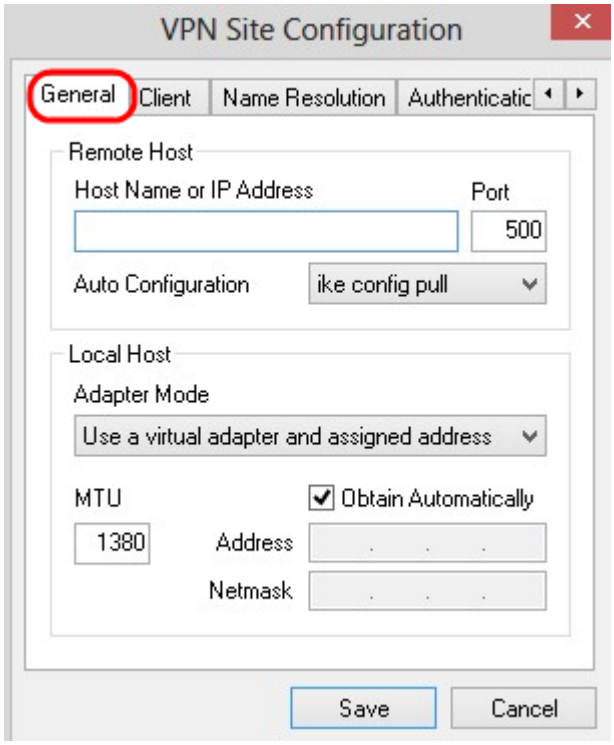


Passaggio 2. Fare clic su **Add**. Viene visualizzata la finestra *Configurazione sito VPN*:



Configurazione generale

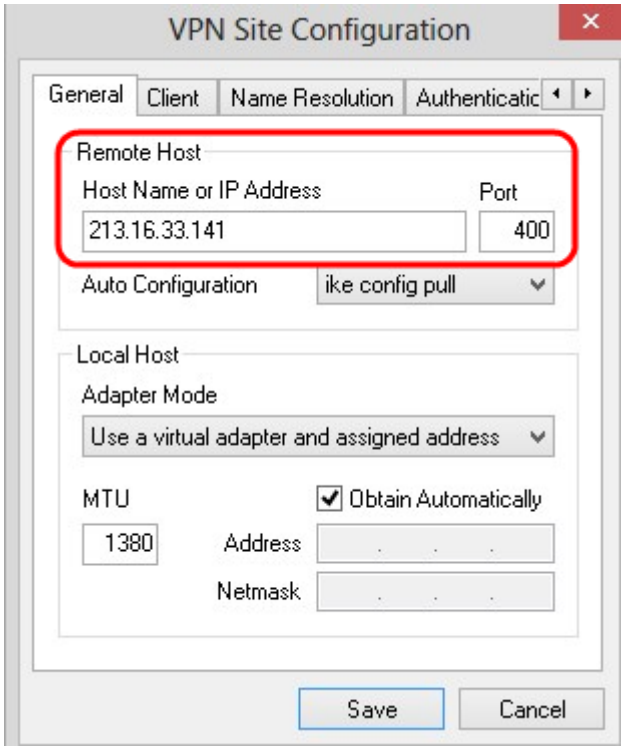
Passaggio 1. Fare clic sulla scheda **Generale**.



Nota: La sezione *Generale* viene utilizzata per configurare gli indirizzi IP dell'host remoto e locale. Questi parametri vengono utilizzati per definire i parametri di rete per la connessione da client a gateway.

Passaggio 2. Nel campo *Nome host o Indirizzo IP*, immettere l'indirizzo IP dell'host remoto, che è l'indirizzo IP della WAN configurata.

Passaggio 3. Nel campo *Porta*, immettere il numero della porta da utilizzare per la connessione. Il numero di porta utilizzato nell'esempio è 400.



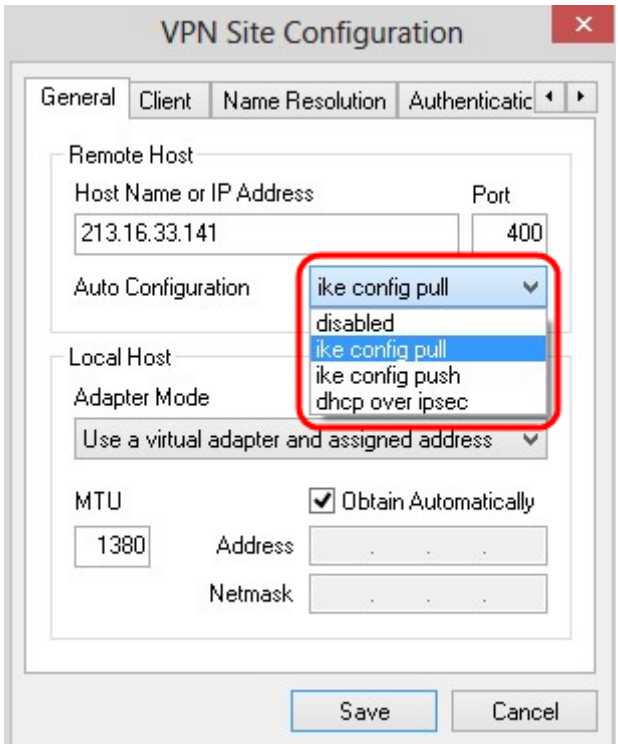
Passaggio 4. Dall'elenco a discesa *Configurazione automatica*, scegliere la configurazione desiderata.

·Disattivato: l'opzione disattivato disattiva qualsiasi configurazione client automatica.

·IKE Config Pull: consente al client di impostare le richieste da un computer. Se il computer supporta il metodo Pull, la richiesta restituisce un elenco di impostazioni supportate dal client.

·IKE Config Push: fornisce a un computer l'opportunità di offrire impostazioni al client attraverso il processo di configurazione. Se il computer supporta il metodo Push, la richiesta restituisce un elenco di impostazioni supportate dal client.

·DHCP over IPSec: consente al client di richiedere le impostazioni al computer tramite DHCP su IPSec.

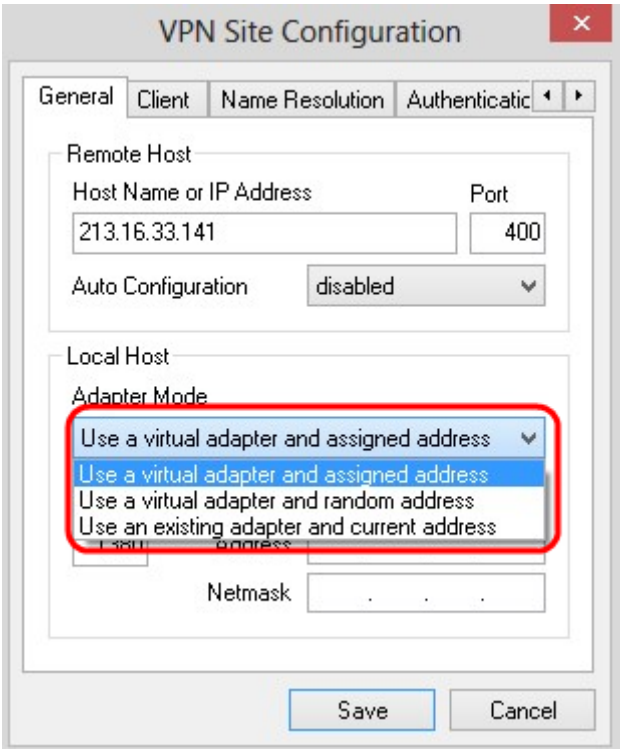


Passaggio 5. Dall'elenco a discesa *Modalità scheda*, scegliere la modalità scheda desiderata per l'host locale in base alla configurazione automatica.

·Usa scheda virtuale e indirizzo assegnato - Consente al client di utilizzare una scheda virtuale con un indirizzo specificato.

·Utilizza una scheda virtuale e un indirizzo casuale: consente al client di utilizzare una scheda virtuale con un indirizzo casuale.

·Utilizza una scheda esistente e indirizzo corrente - Utilizza una scheda esistente e il relativo indirizzo. Non è necessario immettere ulteriori informazioni.

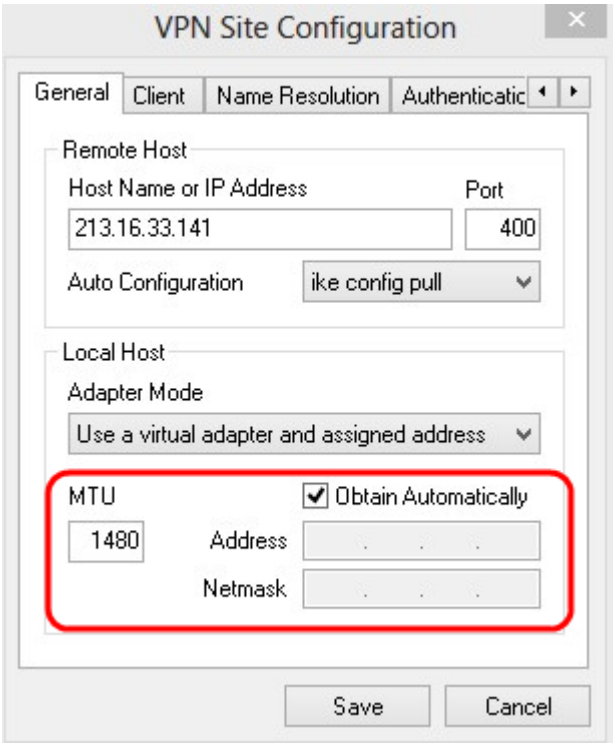


Passaggio 6. Immettere l'unità di trasmissione massima (MTU, Maximum Transmission Unit) nel campo *MTU* se si sceglie **Utilizza una scheda virtuale e un indirizzo assegnato** dall'elenco a discesa *Modalità scheda* nel passaggio 5. L'unità di trasmissione massima aiuta a risolvere i problemi di frammentazione IP. Il valore predefinito è 1380.

Passaggio 7. (Facoltativo) Per ottenere automaticamente l'indirizzo e la subnet mask tramite il server DHCP, selezionare la casella di controllo **Ottieni automaticamente**. Questa opzione non è disponibile per tutte le configurazioni.

Passaggio 8. Immettere l'indirizzo IP del client remoto nel *campo Indirizzo* se si sceglie **Utilizza una scheda virtuale e indirizzo assegnato** dall'elenco a discesa *Modalità scheda* nel Passaggio 5.

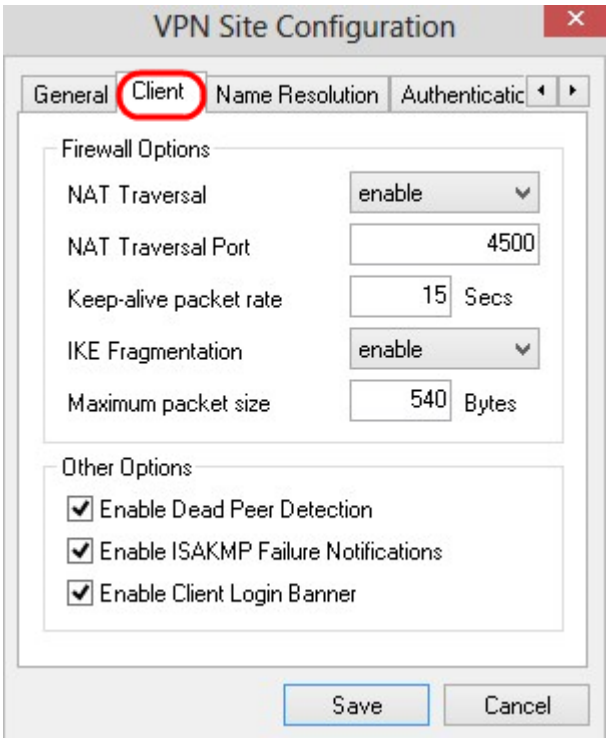
Passaggio 9. Immettere Subnet Mask dell'indirizzo IP del client remoto nel campo *Netmask* se si sceglie **Utilizza una scheda virtuale e indirizzo assegnato** dall'elenco a discesa *Modalità scheda* nel Passaggio 5.



Passaggio 10. Fare clic su **Save** per salvare le impostazioni.

Configurazione client

Passaggio 1. Fare clic sulla scheda **Client**.



Nota: nella sezione *Client* è possibile configurare le opzioni del firewall, Dead Peer Detection e ISAKMP (Internet Security Association and Key Management Protocol) Failure Notifications. Le impostazioni definiscono le opzioni di configurazione configurate manualmente e quelle ottenute automaticamente.

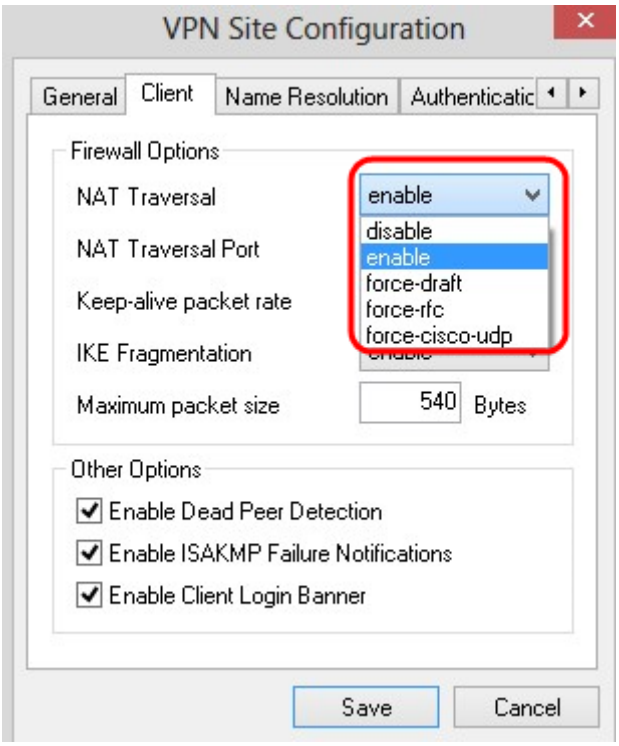
Passaggio 2. Selezionare l'opzione di attraversamento NAT (Network Address Translation) appropriata dall'elenco a discesa *NAT Traversal*.

·Disabilita: il protocollo NAT è disabilitato.

·Abilita: la frammentazione IKE viene utilizzata solo se il gateway indica il supporto tramite negoziazioni.

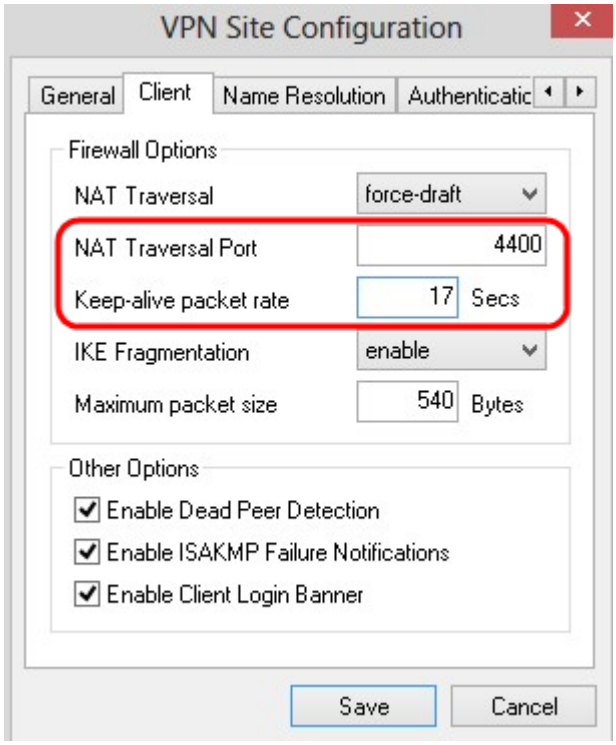
·Force Draft: versione bozza del protocollo NAT. Viene utilizzato se il gateway indica il supporto tramite la negoziazione o il rilevamento del NAT.

·Force RFC — Versione RFC del protocollo NAT. Viene utilizzato se il gateway indica il supporto tramite la negoziazione o il rilevamento del NAT.



Passaggio 3. Immettere la porta UDP per NAT nel campo *NAT Traversal Port*. Il valore predefinito è 4500.

Passaggio 4. Nel campo *Frequenza pacchetti keep-alive*, immettere un valore per la frequenza con cui vengono inviati i pacchetti keep-alive. Il valore viene misurato in secondi. Il valore predefinito è 30 secondi.

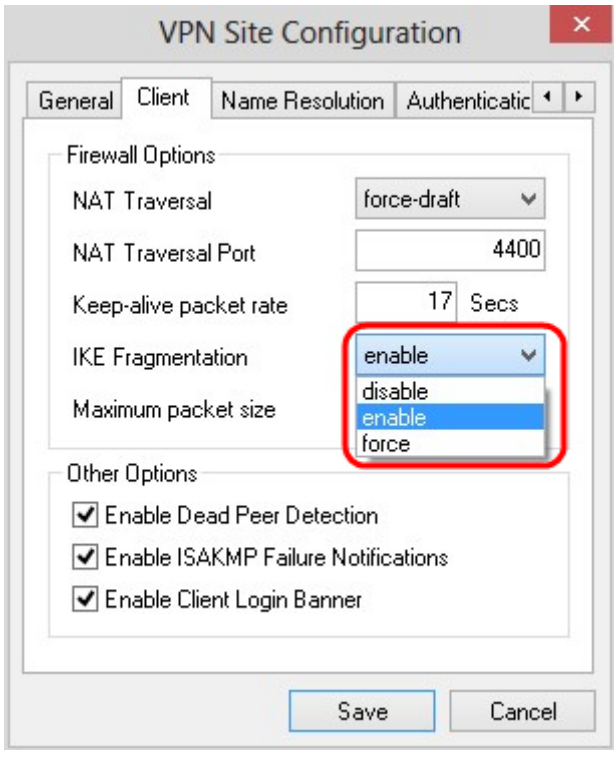


Passaggio 5. Nell'elenco a discesa *Frammentazione IKE* selezionare l'opzione appropriata.

·Disabilita: la frammentazione IKE non viene utilizzata.

·Abilita: la frammentazione IKE viene utilizzata solo se il gateway indica il supporto tramite negoziazioni.

·Force: la frammentazione IKE viene utilizzata indipendentemente dalle indicazioni o dal rilevamento.

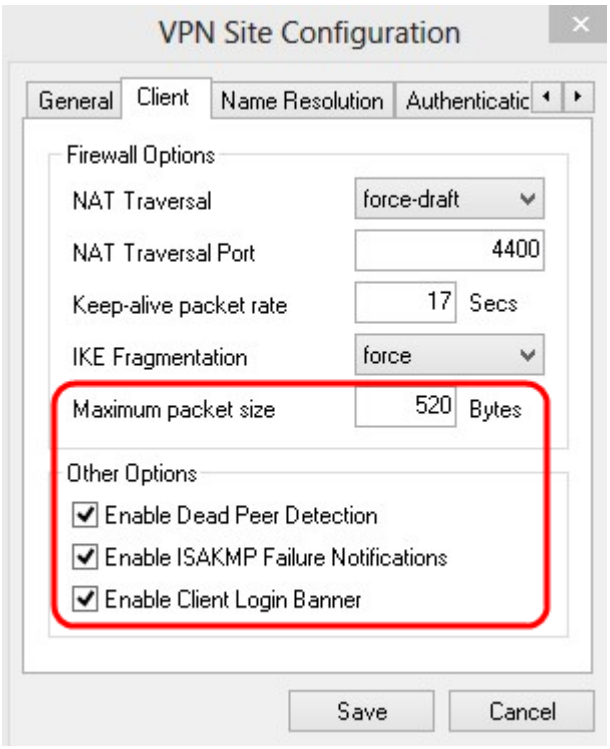


Passaggio 6. Immettere le dimensioni massime del pacchetto nel campo *Dimensioni massime pacchetto* in Byte. Se le dimensioni del pacchetto sono superiori alle dimensioni massime, viene eseguita la frammentazione IKE. Il valore predefinito è 540 byte.

Passaggio 7. (Facoltativo) Per consentire al computer e al client di rilevare quando l'altro non è più in grado di rispondere, selezionare la casella di controllo **Abilita rilevamento peer inattivi**.

Passaggio 8. (Facoltativo) Per inviare le notifiche di errore dal client VPN, selezionare la casella di controllo **Abilita notifiche di errore ISAKMP**.

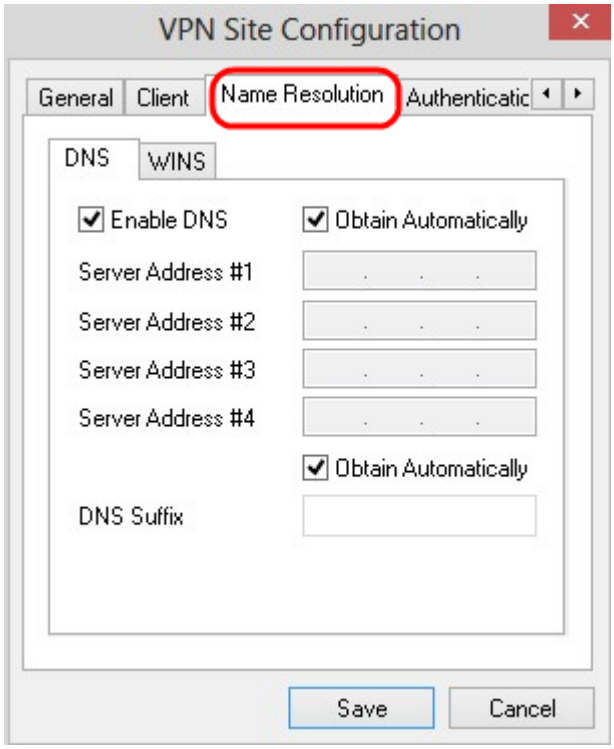
Passaggio 9. (Facoltativo) Per visualizzare un banner di accesso del client quando la connessione viene stabilita con il gateway, selezionare la casella di controllo **Abilita accesso client**.



Passaggio 10. Fare clic su **Save** per salvare le impostazioni.

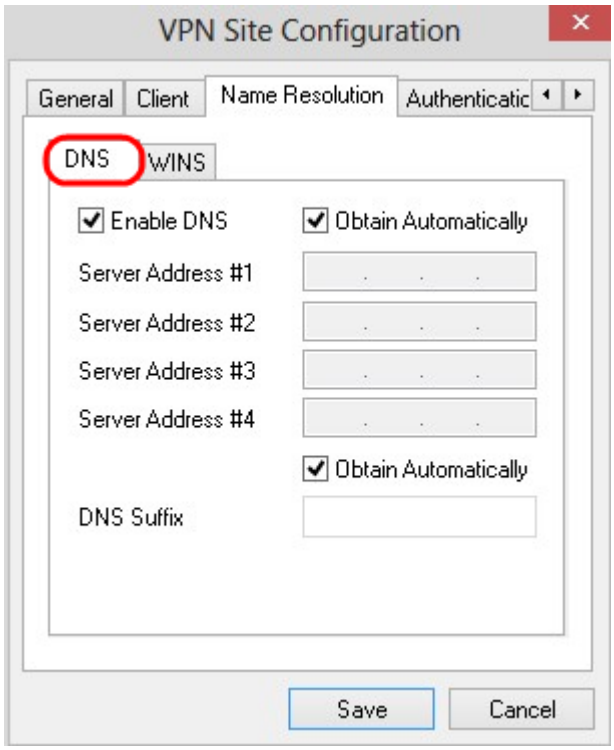
Configurazione risoluzione nome

Passaggio 1. Fare clic sulla scheda **Risoluzione nome**.



Nota: La sezione *Risoluzione nomi* viene utilizzata per configurare le impostazioni DNS (Domain Name System) e WIN (Windows Internet Name Service).

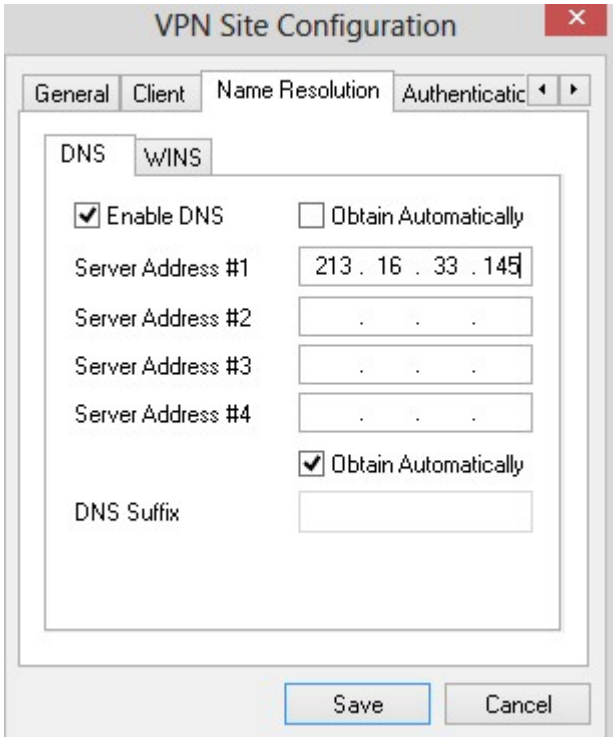
Passaggio 2. Fare clic sulla scheda **DNS**.



Passaggio 3. Selezionare **Abilita DNS** per abilitare il DNS (Domain Name System).

Passaggio 4. (Facoltativo) Per ottenere automaticamente l'indirizzo del server DNS, selezionare la casella di controllo **Ottieni automaticamente**. Se si sceglie questa opzione, andare al passaggio 6.

Passaggio 5. Immettere l'indirizzo del server DNS nel campo *Indirizzo server #1*. Se è presente un altro server DNS, immettere l'indirizzo di tali server nei restanti campi *Indirizzo server*.



Passaggio 6. (Facoltativo) Per ottenere automaticamente il suffisso del server DNS, selezionare la casella di controllo **Ottieni automaticamente**. Se si sceglie questa opzione, andare al passaggio 8.

Passaggio 7. Immettere il suffisso del server DNS nel campo *Suffisso DNS*.

Passaggio 8. Fare clic su **Save** per salvare le impostazioni.

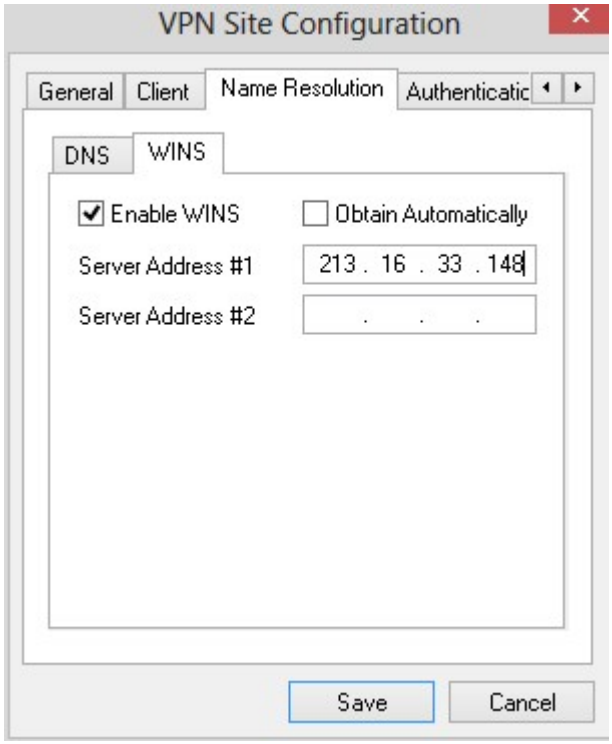
Passaggio 9. Fare clic sulla scheda **WINS**.

Passaggio 10. Selezionare **Abilita WINS** per abilitare Windows Internet Name Server (WINS).

Passaggio 11. (Facoltativo) Per ottenere automaticamente l'indirizzo del server DNS,

selezionare la casella di controllo **Ottieni automaticamente**. Se si sceglie questa opzione, andare al passaggio 13.

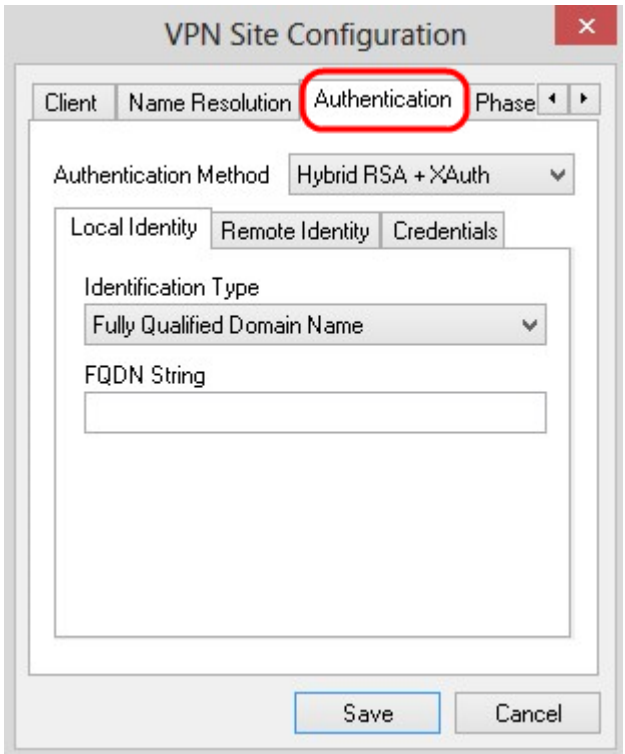
Passaggio 12. Immettere l'indirizzo del server WINS nel campo *Indirizzo server 1*. Se sono presenti altri server DNS, immettere l'indirizzo di tali server nei restanti campi *Indirizzo server* .



Passaggio 13. Fare clic su **Save** per salvare le impostazioni.

Autenticazione

Passaggio 1. Fare clic sulla scheda **Autenticazione**.



Nota: nella sezione *Autenticazione* è possibile configurare i parametri per il client in modo che gestisca l'autenticazione quando tenta di stabilire un'associazione di protezione ISAKMP.

Passaggio 2. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa *Metodo di autenticazione*.

·Hybrid RSA + XAuth: credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno nel formato dei file di certificato PEM o PKCS12 o del tipo dei file di chiave.

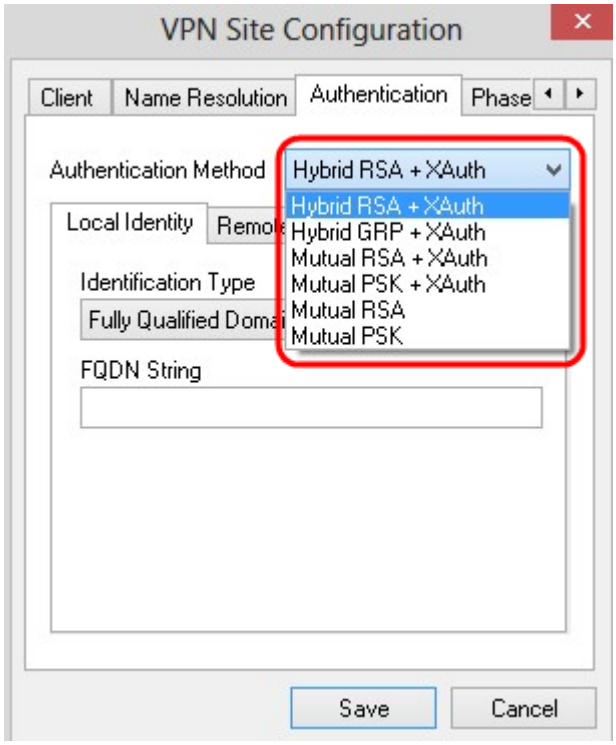
·Hybrid GRP + XAuth: credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno sotto forma di file di certificato PEM o PKCS12 e di una stringa segreta condivisa.

·RSA + XAuth reciproci: client e gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in formato PEM o PKCS12, file di certificato o tipo di chiave.

·PSK reciproco + XAuth: il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.

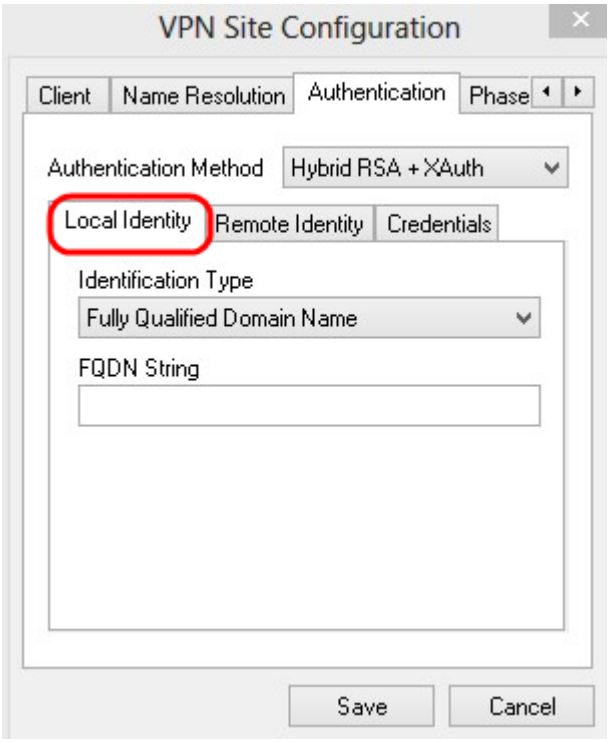
·RSA reciproca: client e gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in formato PEM o PKCS12, file di certificato o tipo di chiave.

·PSK reciproco: il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.



Configurazione identità locale

Passaggio 1. Fare clic sulla scheda **Identità locale**.



Nota: l'opzione Identità locale consente di impostare l'ID inviato al gateway per la verifica. Nella sezione *Identità locale*, il tipo di identificazione e la stringa FQDN (Fully Qualified Domain Name) sono configurati per determinare la modalità di invio dell'ID.

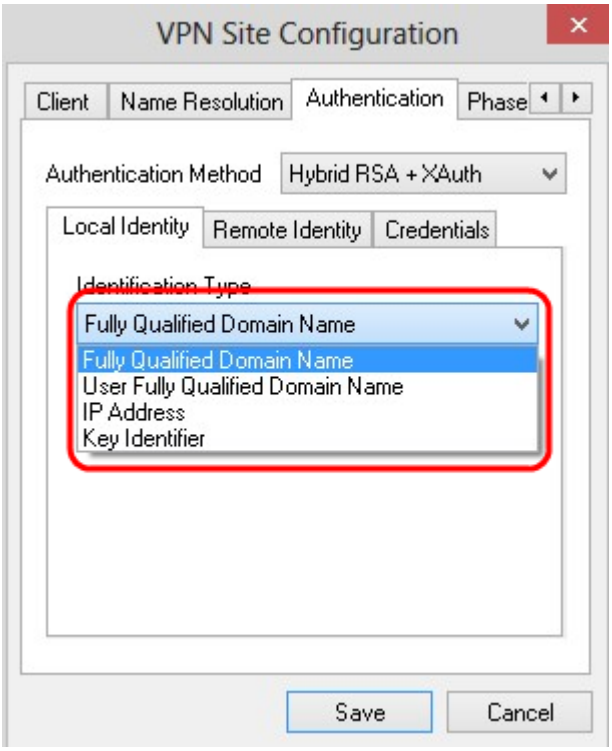
Passaggio 2. Scegliere l'opzione di identificazione appropriata dall'elenco a discesa *Tipo di identificazione*. Non tutte le opzioni sono disponibili per tutte le modalità di autenticazione.

·Nome di dominio completo: l'identificazione client dell'identità locale si basa su un nome di dominio completo. Se si sceglie questa opzione, seguire il passaggio 3 e quindi andare al passaggio 7.

·Nome di dominio completo utente: l'identificazione client dell'identità locale si basa sul nome di dominio completo dell'utente. Se si sceglie questa opzione, eseguire il passaggio 4 e quindi passare al passaggio 7.

·Indirizzo IP: l'identificazione client dell'identità locale si basa sull'indirizzo IP. Se si seleziona **Utilizza un indirizzo host locale individuato**, l'indirizzo IP viene individuato automaticamente. Se si sceglie questa opzione, eseguire il passaggio 5 e quindi andare al passaggio 7.

·Identificatore chiave: l'identificazione client del client locale è basata su un identificatore chiave. Se si sceglie questa opzione, seguire i passi 6 e 7.



Passaggio 3. Immettere il nome di dominio completo come stringa DNS nel campo *Stringa FQDN*.

Passaggio 4. Immettere il nome di dominio completo dell'utente come stringa DNS nel campo *Stringa UFQDN*.

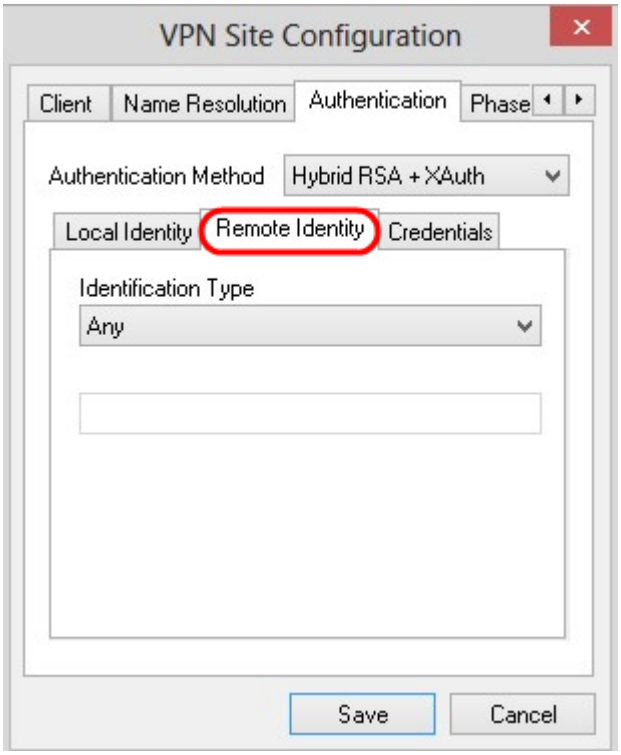
Passaggio 5. Immettere l'indirizzo IP nel campo *Stringa UFQDN*.

Passaggio 6. Immettere l'identificatore della chiave per identificare il client locale nella *stringa ID chiave*.

Passaggio 7. Fare clic su **Save** per salvare le impostazioni.

Configurazione identità remota

Passaggio 1. Fare clic sulla scheda **Identità remota**.



Nota: l'identità remota verifica l'ID dal gateway. Nella sezione *Identità remota*, il tipo di identificazione è configurato per determinare la modalità di verifica dell'ID.

Passaggio 2. Scegliere l'opzione di identificazione appropriata dall'elenco a discesa *Tipo di identificazione*.

·Qualsiasi: il client remoto può accettare qualsiasi valore o ID per l'autenticazione.

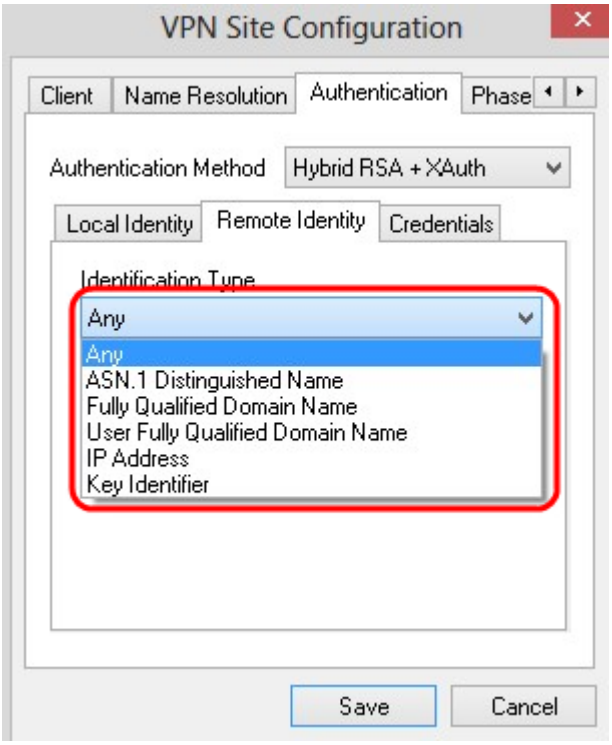
·Nome distinto ASN.1: il client remoto viene identificato automaticamente da un file di certificato PEM o PKCS12. È possibile scegliere questa opzione solo se si sceglie un metodo di autenticazione RSA nel passo 2 della sezione *Autenticazione*. Selezionare la casella di controllo **Utilizza il soggetto nel certificato ricevuto ma non confrontarlo con un valore specifico** per ricevere automaticamente il certificato. Se si sceglie questa opzione, eseguire il passaggio 3 e quindi andare al passaggio 8.

·Nome di dominio completo: l'identificazione client dell'identità remota si basa sul nome di dominio completo. È possibile scegliere questa opzione solo se si sceglie un metodo di autenticazione PSK nel passaggio 2 della sezione *Autenticazione*. Se si sceglie questa opzione, eseguire il passaggio 4 e quindi andare al passaggio 8.

·Nome di dominio completo dell'utente: l'identificazione client dell'identità remota si basa sul nome di dominio completo dell'utente. È possibile scegliere questa opzione solo se si sceglie un metodo di autenticazione PSK nel passaggio 2 della sezione *Autenticazione*. Se si sceglie questa opzione, eseguire il passaggio 5 e quindi andare al passaggio 8.

·Indirizzo IP: l'identificazione client dell'identità remota si basa sull'indirizzo IP. Se si seleziona **Utilizza un indirizzo host locale individuato**, l'indirizzo IP viene individuato automaticamente. Se si sceglie questa opzione, seguire il passaggio 6 e quindi andare al passaggio 8.

·Identificatore chiave: l'identificazione del client remoto è basata su un identificatore chiave. Se si sceglie questa opzione, seguire i passi 7 e 8.



Passaggio 3. Immettere la stringa del DN ASN.1 nel campo *Stringa DN ASN.1*.

Passaggio 4. Immettere il nome di dominio completo come stringa DNS nel campo *Stringa FQDN*.

Passaggio 5. Immettere il nome di dominio completo dell'utente come stringa DNS nel campo *Stringa UFQDN*.

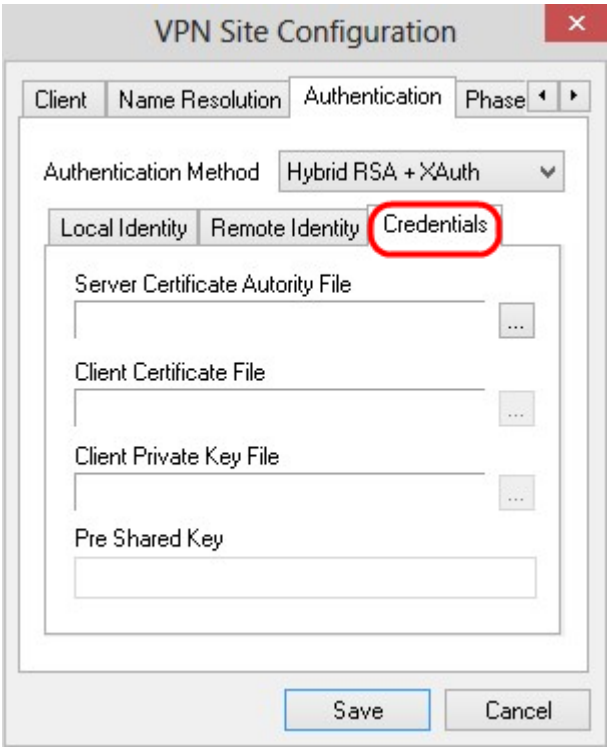
Passaggio 6. Immettere l'indirizzo IP nel campo *Stringa UFQDN*.

Passaggio 7. Immettere l'identificatore chiave per identificare il client locale nel campo *Stringa ID chiave*.

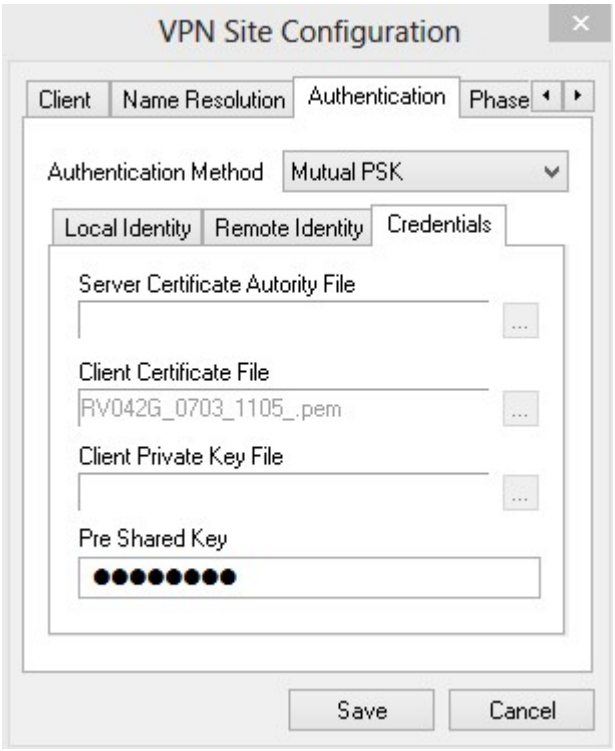
Passaggio 8. Fare clic su **Save** per salvare le impostazioni.

Configurazione credenziali

Passaggio 1. Fare clic sulla scheda **Credenziali**.



Nota: nella sezione *Credenziali* è configurata la chiave già condivisa.



Passaggio 2. Per scegliere il file del certificato del server, fare clic sul **...** accanto al campo *File Autorità di certificazione server* e scegliere il percorso in cui è stato salvato il file sul PC.

Passaggio 3. Per scegliere il file del certificato client, fare clic sul **...** accanto al campo *File certificato client* e scegliere il percorso in cui è stato salvato il file del certificato client sul PC.

Passaggio 4. Per scegliere il file della chiave privata del client, fare clic sul pulsante **..** accanto al campo *File chiave privata client* e scegliere il percorso in cui è stato salvato il file nel PC.

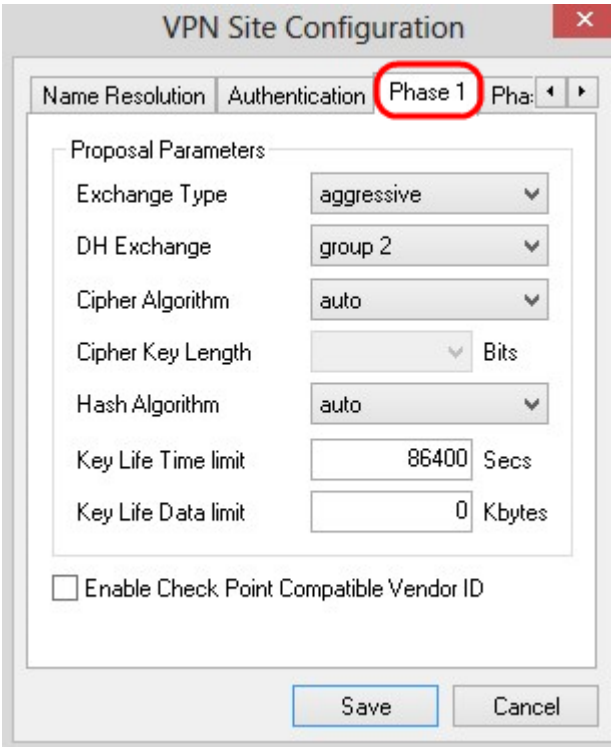
Passaggio 5. Immettere la chiave già condivisa nel campo *Chiave già condivisa*. Deve

essere la stessa chiave utilizzata durante la configurazione del tunnel.

Passaggio 6. Fare clic su **Save** per salvare le impostazioni.

Configurazione fase 1

Passaggio 1. Fare clic sulla scheda **Fase 1**.

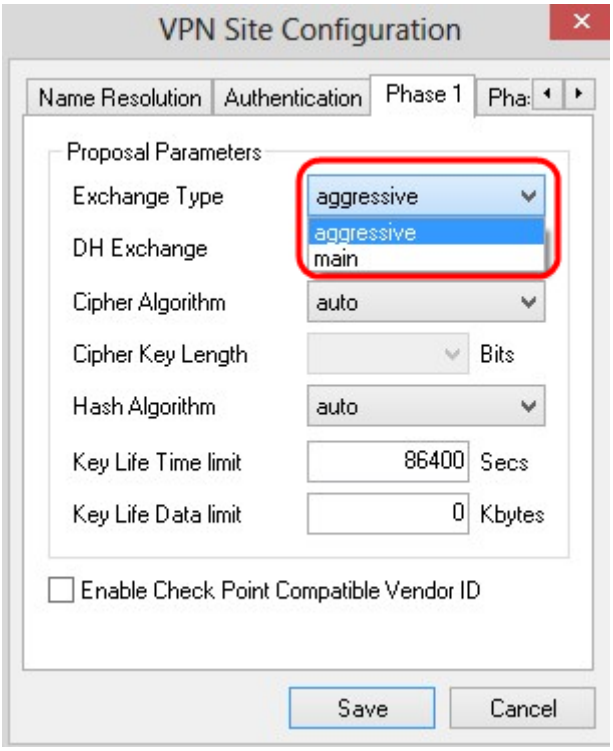


Nota: Nella sezione *Fase 1*, è possibile configurare i parametri in modo che sia possibile stabilire un'associazione di sicurezza ISAKMP con il gateway client.

Passaggio 2. Scegliere il tipo di scambio chiave appropriato dall'elenco a discesa *Tipo di scambio*.

·Principale: l'identità dei peer è protetta.

·Aggressivo: l'identità dei peer non è protetta.



Passaggio 3. Nell'elenco a discesa *DH Exchange*, scegliere il gruppo appropriato scelto durante la configurazione della connessione VPN.

Passaggio 4. Nell'elenco a discesa *Cipher Algorithm*, scegliere l'opzione appropriata scelta durante la configurazione della connessione VPN.

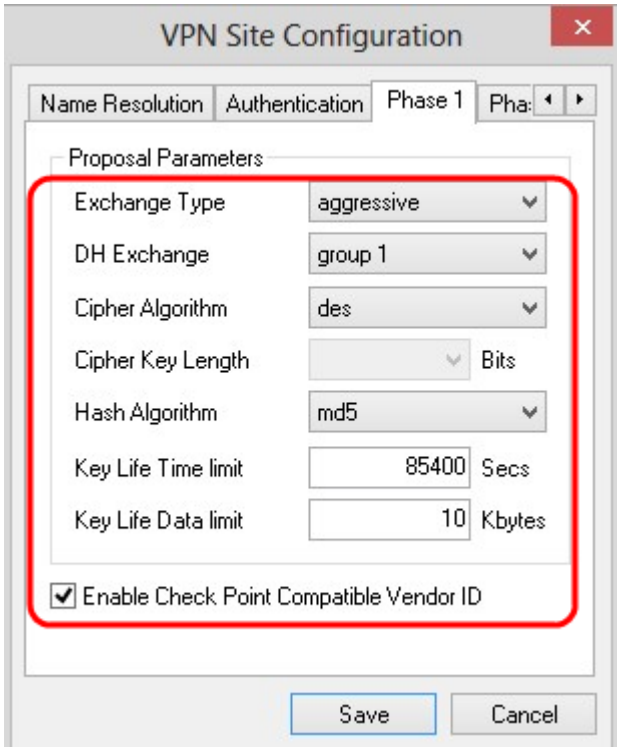
Passaggio 5. Nell'elenco a discesa *Lunghezza chiave di crittografia*, scegliere l'opzione che corrisponde alla lunghezza della chiave dell'opzione scelta durante la configurazione della connessione VPN.

Passaggio 6. Nell'elenco a discesa *Hash Algorithm*, scegliere l'opzione scelta durante la configurazione della connessione VPN.

Passaggio 7. Nel campo Limite *durata chiave*, immettere il valore utilizzato durante la configurazione della connessione VPN.

Passaggio 8. Nel campo Limite *dati durata chiave*, immettere il valore in kilobyte da proteggere. Il valore di default è 0 e la feature viene disattivata.

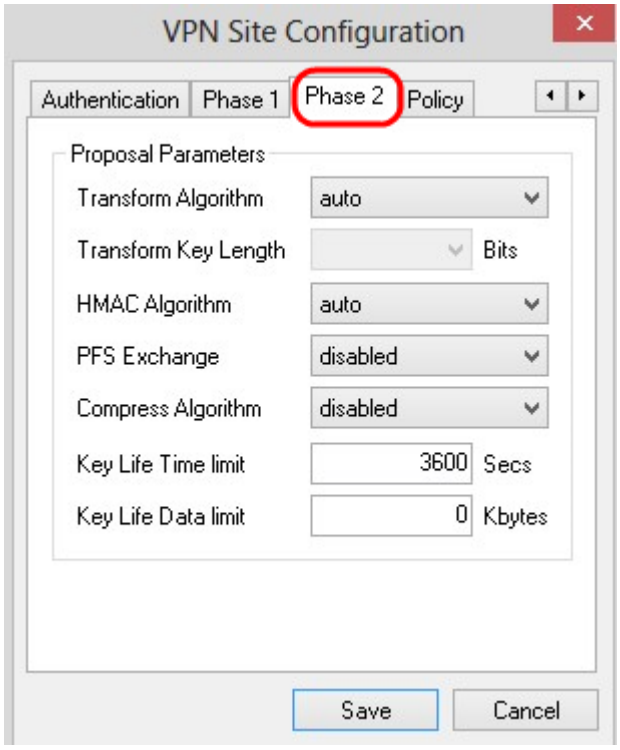
Passaggio 9. (Facoltativo) Selezionare la casella di controllo **Abilita ID fornitore compatibile con checkpoint**.



Passaggio 10. Fare clic su **Save** per salvare le impostazioni.

Configurazione fase 2

Passaggio 1. Fare clic sulla scheda **Fase 2**.



Nota: nella sezione *Fase 2*, è possibile configurare i parametri in modo che sia possibile stabilire un'associazione di sicurezza IPsec con il gateway client remoto.

Passaggio 2. Nell'elenco a discesa *Transform Algorithm*, scegliere l'opzione scelta durante la configurazione della connessione VPN.

Passaggio 3. Nell'elenco a discesa *Trasforma lunghezza chiave* scegliere l'opzione che

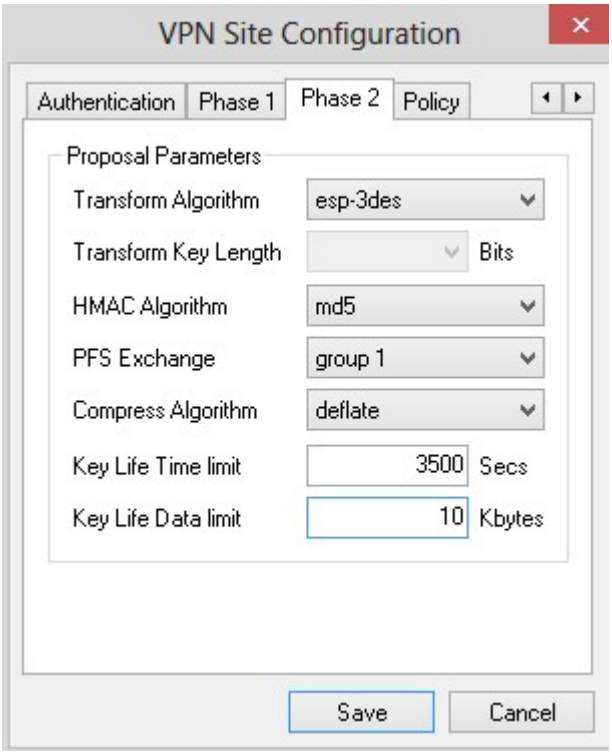
corrisponde alla lunghezza della chiave dell'opzione scelta durante la configurazione della connessione VPN.

Passaggio 4. Nell'elenco a discesa *HMAC Algorithm*, scegliere l'opzione scelta durante la configurazione della connessione VPN.

Passaggio 5. Nell'elenco a discesa *PFS Exchange* scegliere l'opzione scelta durante la configurazione della connessione VPN.

Passaggio 6. Nel campo *Limite durata chiave*, immettere il valore utilizzato durante la configurazione della connessione VPN.

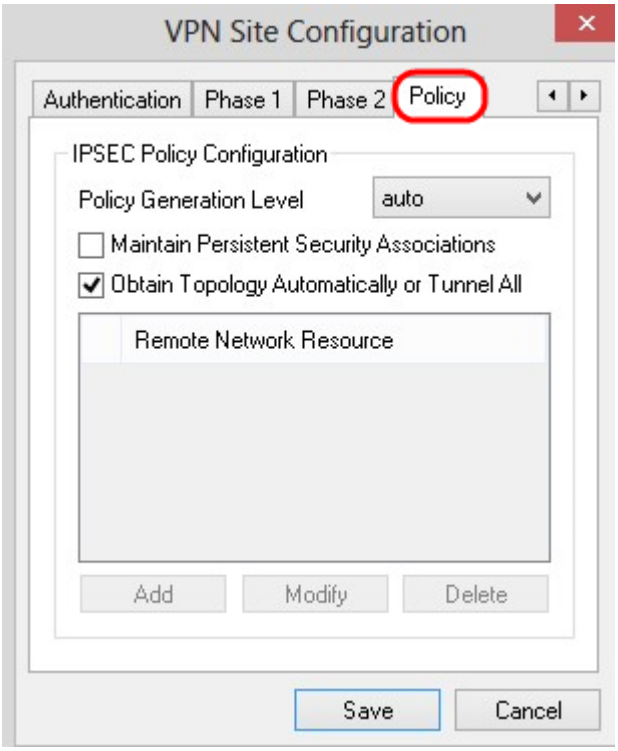
Passaggio 7. Nel campo *Limite dati durata chiave*, immettere il valore in kilobyte da proteggere. Il valore di default è 0 e la feature viene disattivata.



Passaggio 8. Fare clic su **Save** per salvare le impostazioni.

Configurazione criteri

Passaggio 1.Fare clic sulla scheda **Criterio**.



Nota: nella sezione *Criterio* è definito il criterio IPSEC, necessario affinché il client comunichi con l'host per la configurazione del sito.

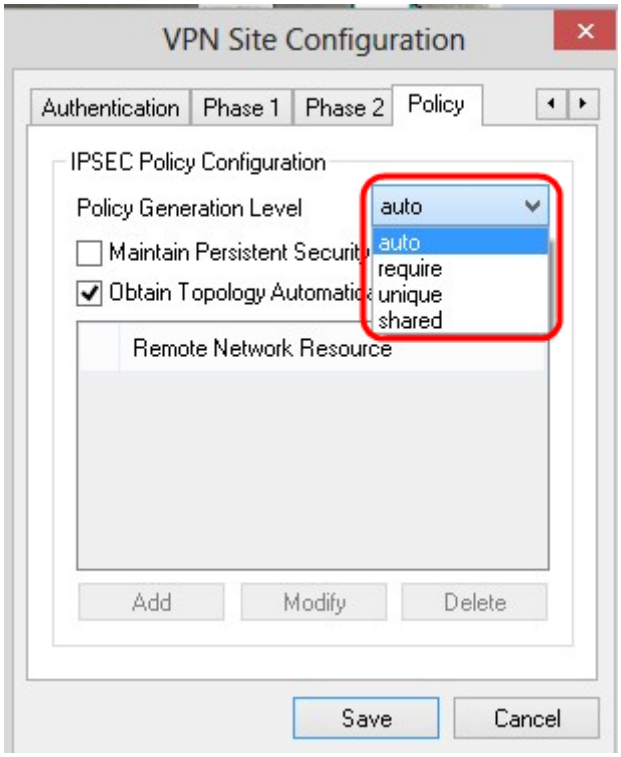
Passaggio 2. Nell'elenco a discesa *Livello di generazione criteri*, scegliere l'opzione appropriata.

·Automatico: il livello di criteri IPSec necessario viene determinato automaticamente.

·Obbligatorio: non viene negoziata un'associazione di sicurezza univoca per ogni criterio.

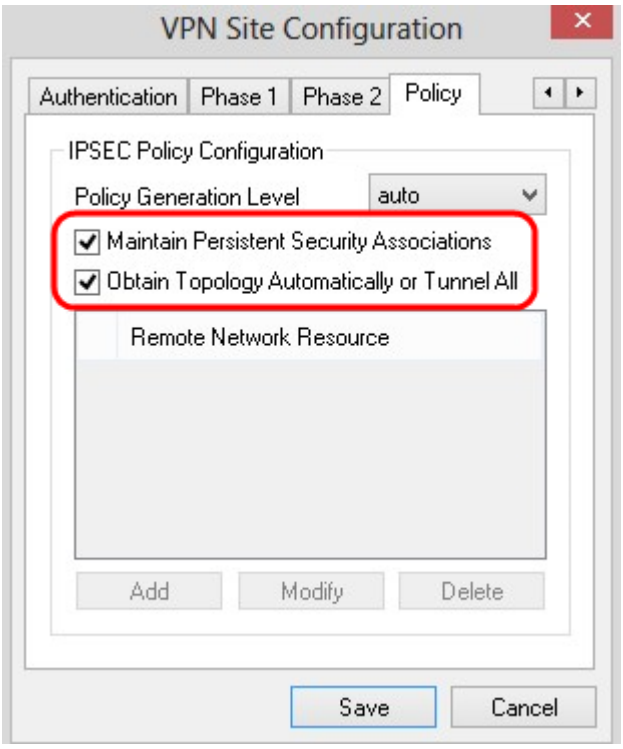
·Univoco: viene negoziata un'associazione di sicurezza univoca per ogni criterio.

·Condiviso: la policy appropriata viene generata al livello necessario.

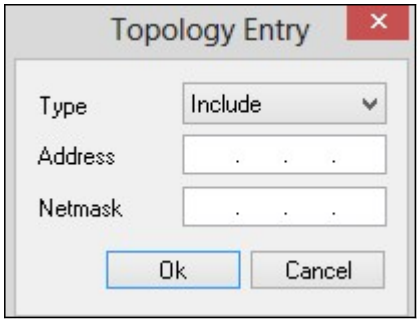


Passaggio 3. (Facoltativo) Per modificare le negoziazioni IPSec, selezionare la casella di controllo **Mantieni associazioni di protezione permanenti**. Se questa opzione è abilitata, la negoziazione viene eseguita per ogni criterio subito dopo la connessione. Se disabilitata, la negoziazione viene eseguita in base alle necessità.

Passaggio 4. (Facoltativo) Per ricevere dal dispositivo un elenco di reti fornito automaticamente o per inviare tutti i pacchetti all'RV0XX per impostazione predefinita, selezionare la casella di controllo **Ottieni topologia automaticamente o Tunnel tutto**. Se deselezionata, la configurazione deve essere eseguita manualmente. Se questa opzione è selezionata, andare al passo 10.



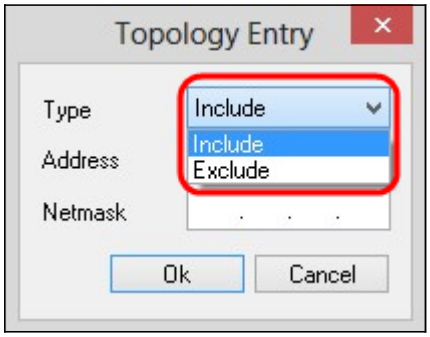
Passaggio 5. Fare clic su **Add** per aggiungere una voce Topology nella tabella. Viene visualizzata la finestra *Voce topologia*.



Passaggio 6. Nell'elenco a discesa *Tipo* scegliere l'opzione appropriata.

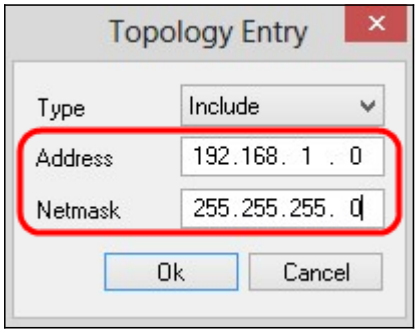
·Include: accesso alla rete tramite un gateway VPN.

·Escludi: accesso alla rete tramite connettività locale.

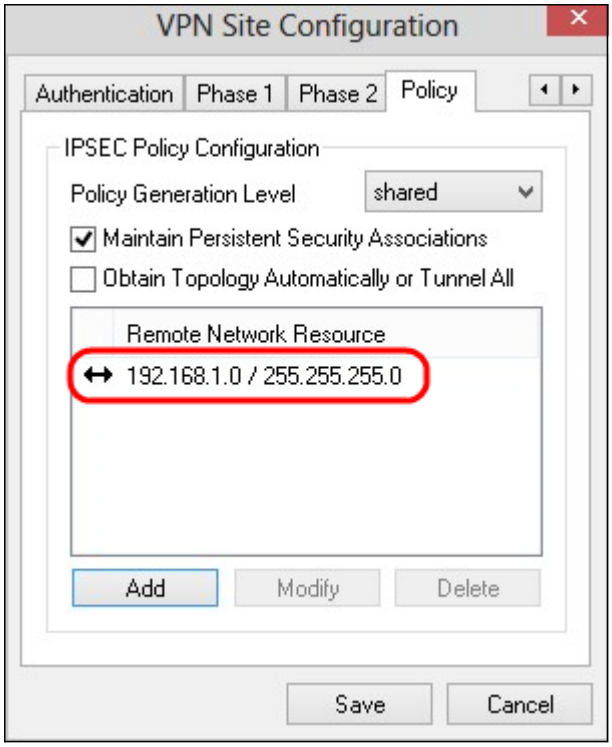


Passaggio 7. Nel campo *Address* (Indirizzo), immettere l'indirizzo IP dell'RV0XX.

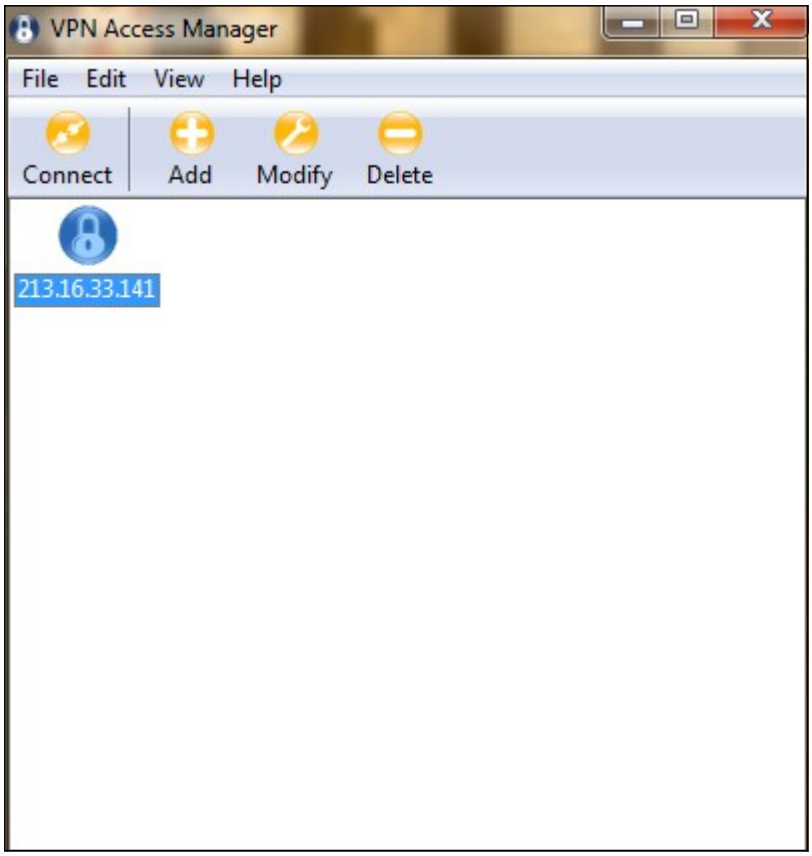
Passaggio 8. Nel campo *Netmask*, immettere l'indirizzo della subnet mask del dispositivo.



Passaggio 9. Fare clic su **OK**. L'indirizzo IP e l'indirizzo della subnet mask dell'RV0XX vengono visualizzati nell'elenco delle risorse di rete remote.



Passaggio 10. Fare clic su **Save** per visualizzare nuovamente la finestra *VPN Access Manager* in cui è visualizzata la nuova connessione VPN.

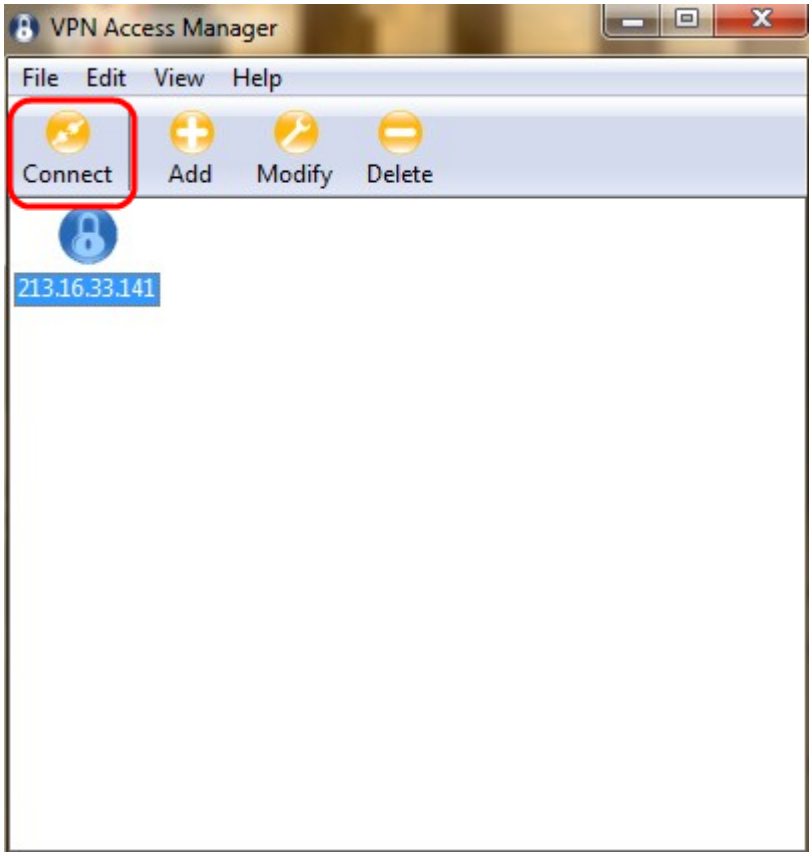


Connessione

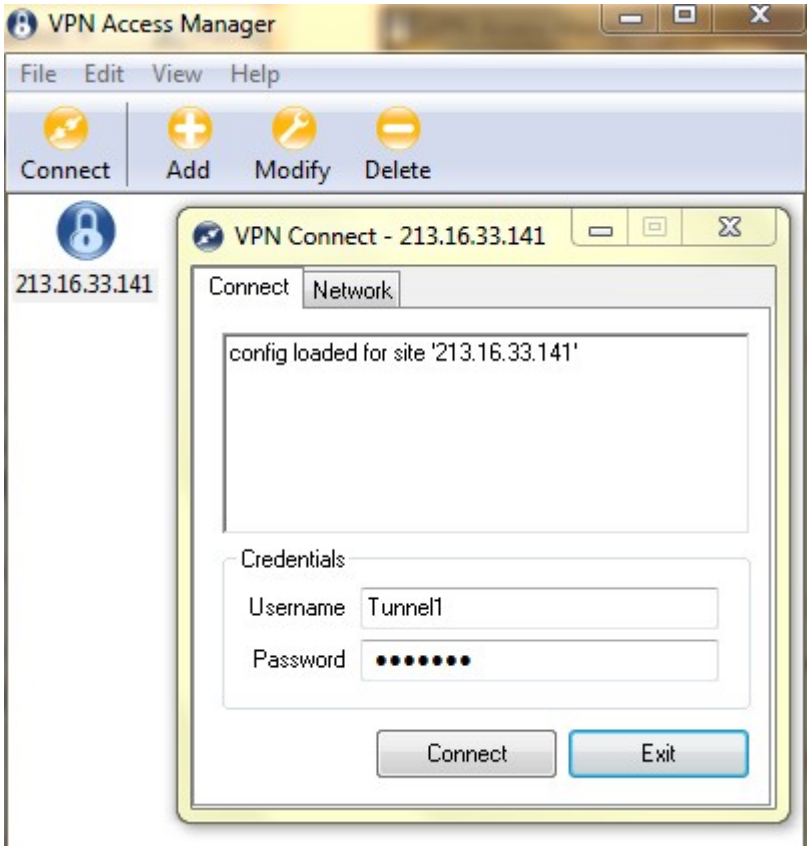
Questa sezione spiega come configurare la connessione VPN dopo aver configurato tutte le impostazioni. Le informazioni di accesso richieste sono le stesse di Accesso client VPN configurato sul dispositivo.

Passaggio 1. Fare clic sulla connessione VPN desiderata.

Passaggio 2. Fare clic su **Connetti.**



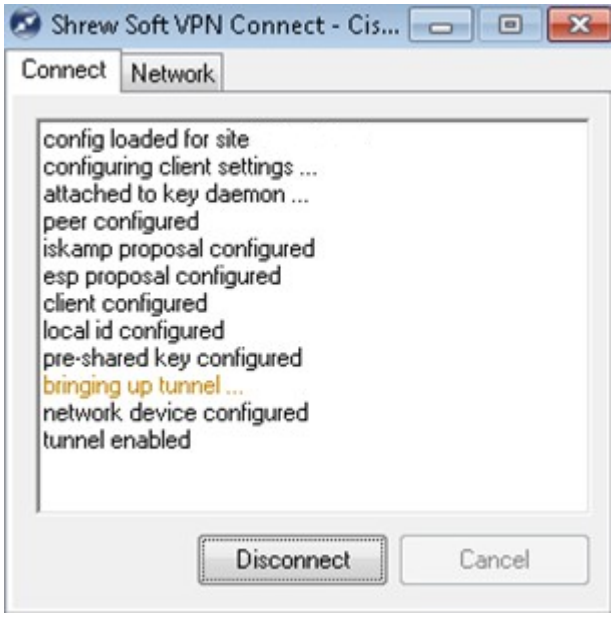
Viene visualizzata la finestra *VPN Connect*:



Passaggio 3. Immettere il nome utente per la VPN nel campo *Nome utente*.

Passaggio 4. Immettere la password per l'account utente VPN nel campo *Password*.

Passaggio 5. Fare clic su **Connetti**. Viene visualizzata la finestra *Show Soft VPN Connect*:



Passaggio 6. (Facoltativo) Per disabilitare la connessione, fare clic su **Disconnetti**.

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).