

Client VPN

Manuale d'uso

9235970

Edizione 1

Copyright © 2004 Nokia. Tutti i diritti sono riservati.

Il contenuto del presente documento, né parte di esso, potrà essere riprodotto, trasferito, distribuito o memorizzato in qualsiasi forma senza il permesso scritto di Nokia. Nokia è un marchio registrato di Nokia Corporation. Altri nomi di prodotti e società citati nel presente documento possono essere marchi o marchi registrati dei rispettivi proprietari.

Symbian and Symbian OS are trademarks of Symbian Ltd.

SecurID is a registered trademark of RSA Security INC.

Nokia adotta una politica di continuo sviluppo. Nokia si riserva il diritto di effettuare modifiche e miglioramenti a qualsiasi prodotto descritto nel presente documento senza previo preavviso.

In nessuna circostanza Nokia sarà ritenuta responsabile di eventuali perdite di dati o di guadagni o di qualsiasi danno speciale, incidentale, consequenziale o indiretto in qualunque modo causato.

Il contenuto di questo documento viene fornito "così com'è". Fatta eccezione per quanto previsto dalla legge in vigore, non è avanzata alcuna garanzia, implicita o esplicita, tra cui, ma non limitatamente a, garanzie implicite di commerciabilità e idoneità per un fine particolare, in relazione all'accuratezza, all'affidabilità o al contenuto del presente documento. Nokia si riserva il diritto di modificare questo documento o di ritirarlo in qualsiasi momento.

La disponibilità di prodotti particolari può variare a seconda delle regioni. Per informazioni, contattare il rivenditore Nokia più vicino.

Indice

VPN (Virtual Private Network, rete privata virtuale)	4
Installazione	6
Requisiti di sistema	6
Criteri VPN	7
Installazione dei criteri VPN dai server criteri VPN.....	7
Installazione dei criteri VPN a partire da file SIS.....	8
Visualizzazione dei criteri VPN	9
Stato criteri.....	10
Stato certificato	10
Creazione di punti di accesso VPN mediante valori predefiniti.....	11
Aggiornamento dei criteri VPN.....	11
Eliminazione dei criteri VPN	12
Server criteri VPN.....	13
Connessione ai server criteri VPN	13
Installazione delle impostazioni dai file SIS.....	13
Visualizzazione di server criteri VPN	14
Aggiunta di server criteri VPN.....	14
Modifica dei server criteri VPN.....	16
Sincronizzazione dei server criteri VPN.....	16
Registrazione dei certificati VPN	17
Eliminazione dei server criteri VPN	18
Punti di accesso VPN.....	19
Visualizzazione dei punti di accesso VPN.....	19
Creazione di punti di accesso VPN	19
Eliminazione di punti di accesso VPN.....	20
Registro VPN	21
Visualizzazione del registro VPN.....	21
Cancellazione del registro VPN	21
Password dell'archivio delle chiavi.....	22
Creazione o modifica della password dell'archivio chiavi	22
Immissione delle password dell'archivio chiavi.....	22
VPN e applicazioni.....	24
Autenticazione da parte del gateway VPN	24
Guida alla soluzione dei problemi	26

1. VPN (Virtual Private Network, rete privata virtuale)

➔ Accedere a *Menu*, quindi selezionare *Strumenti* > *Impostazioni* > *Impostazioni connessione* > *VPN*.

La **rete privata virtuale** (VPN), consente di creare connessioni crittografate per accedere a informazioni aziendali quando ci si trova fuori sede. L'accesso crittografato alla rete aziendale è disponibile per e-mail, applicazioni database e Intranet.

Per creare una rete VPN, un gateway e il dispositivo cellulare eseguono l'autenticazione reciproca, quindi negoziano gli algoritmi di crittografia e autenticazione per proteggere la riservatezza e l'integrità delle informazioni da consultare.

Per utilizzare una connessione VPN, occorre innanzitutto creare i punti di accesso VPN, quindi selezionarli al momento dell'uso delle applicazioni di connessione alla rete aziendale. La connessione VPN alla rete aziendale avviene tramite un altro tipo di connessione a un punto di accesso Internet. La connessione VPN viene creata e i dati crittografati in base ai criteri VPN caricati al momento della connessione al punto di accesso VPN.

▶ **Nota:** per poter utilizzare la connessione VPN, occorre ricevere le impostazioni del server dei criteri VPN dagli amministratori, che possono inviarle tramite un file **SIS** (Symbian Installation System, sistema di installazione Symbian).

Per utilizzare la rete privata virtuale

- 1 Installare il client VPN.
Per ulteriori informazioni, consultare la sezione "Installazione" a pagina 6.
- 2 Specificare la connessione ad un server criteri VPN.

È possibile specificare le impostazioni di un server criteri VPN o installarle a partire da un file SIS.

Per ulteriori informazioni, consultare la sezione "Connessione ai server criteri VPN" a pagina 12.

 **Nota:** se i criteri VPN vengono installati a partire da file SIS, non sarà necessario creare le connessioni ai server criteri VPN.

3 Installare i criteri VPN dal server criteri VPN.

Per ulteriori informazioni, consultare la sezione "Installazione dei criteri VPN dai server criteri VPN" a pagina 7.

4 Creare i punti di accesso VPN.

I punti di accesso VPN consentono di specificare un punto di accesso Internet e i criteri VPN. Per ulteriori informazioni, consultare la sezione "Creazione dei punti di accesso VPN" a pagina 17.

 **Nota:** i punti di accesso VPN associano i criteri VPN ai punti di accesso Internet. Alla prima sincronizzazione del server criteri VPN, per ciascun criterio installato sul dispositivo cellulare vengono creati i punti di accesso VPN corrispondenti.

5 Selezionare un punto di accesso VPN durante l'uso delle applicazioni di connessione alla rete aziendale.

Per ulteriori informazioni, consultare la sezione "Connessione VPN e applicazioni" a pagina 21.

La connessione VPN viene creata a partire dalla connessione Internet.

2. Installazione

Il client VPN viene fornito come file **SIS** (Symbian Installation System) standard.

Il client VPN deve essere installato su un dispositivo cellulare compatibile seguendo la stessa procedura utilizzata per l'installazione di altri software. Per ulteriori informazioni sulle modalità di installazione del software sul dispositivo cellulare, consultare la documentazione del dispositivo cellulare.

Una volta completata l'installazione, spegnere, quindi riaccendere il dispositivo cellulare per rendere effettive le modifiche apportate.

Una volta eseguita l'installazione, il file SIS del client VPN non sarà più necessario. Eliminare il file SIS per aumentare lo spazio disponibile in memoria.

Requisiti di sistema

Durante l'installazione del client VPN, sono necessari almeno 1,5 MB di spazio disponibile nella memoria del dispositivo cellulare.

Al termine dell'installazione, il client VPN occupa 900 K di spazio nella memoria del dispositivo cellulare o sulla memory card. Per ciascun criterio VPN, sono generalmente necessari da 1 K a 16 K di memoria sul dispositivo cellulare.

3. Criteri VPN

I **criteri VPN** definiscono la modalità di autenticazione reciproca utilizzata da un dispositivo cellulare e un gateway VPN, nonché gli algoritmi utilizzati per la crittografia dei dati. I criteri VPN vengono creati, quindi memorizzati sui server criteri VPN o forniti sotto forma di file **SIS** (Symbian installation system) dagli amministratori. È possibile installare tali criteri a partire da un server criteri VPN o da file SIS.

 Accedere a [Menu](#), quindi selezionare [Strumenti](#) > [Impostazioni](#) > [Impostazioni connessione](#) > [VPN](#) > [Gestione VPN](#) > [Criteri VPN](#).

Installazione dei criteri VPN dai server criteri VPN

Per installare i criteri VPN

- 1 Premere [Si](#) non appena si accede alla vista [Criteri VPN](#) e viene richiesto di installare i criteri VPN.
- 2 Non appena viene richiesto di aggiungere i server criteri VPN, premere [Si](#).
- 3 Specificare le impostazioni di connessione a un server criteri VPN.
Per ulteriori informazioni, consultare la sezione "Connessione ai server criteri VPN" a pagina 12.
- 4 Non appena viene richiesto di effettuare la sincronizzazione del server criteri VPN, premere [Si](#).
- 5 Creare una **password dell'archivio chiavi**.

 **Glossario:** i server criteri VPN sono server della rete aziendale contenenti i criteri VPN.

 **Glossario:** la password dell'archivio chiavi consente di proteggere le chiavi private dei criteri VPN e delle connessioni del server criteri VPN da accessi non autorizzati.

 **Glossario:** il codice identificativo del server criteri VPN corrisponde all'impronta digitale che consente di identificare il certificato del server criteri VPN.

 **Glossario:** la password di importazione delle chiavi consente di proteggere le chiavi private incluse in un file di criteri VPN.

Per ulteriori informazioni, consultare la sezione "Creazione o modifica della password dell'archivio chiavi" a pagina 20.

Viene stabilita la connessione al server criteri VPN.

- 6 Verificare il **codice identificativo del server criteri VPN** per stabilire una connessione protetta.
È possibile ignorare questo punto se le impostazioni del server criteri VPN sono state installate a partire da un file SIS.
Per ulteriori informazioni, consultare la sezione "Aggiunta di server criteri VPN" a pagina 13.
- 7 Digitare le informazioni di autenticazione per accedere al server criteri VPN, quindi premere **OK**.
Tali informazioni vengono fornite dall'amministratore del server criteri VPN.

I criteri VPN vengono installati sul dispositivo cellulare.

 **1Nota:** premendo **Esci**, l'installazione dei criteri VPN non verrà effettuata. Premere **Opzioni** e selezionare **Installa criterio** per installare i criteri VPN a partire da un server criteri VPN.

Installazione dei criteri VPN a partire da file SIS

Richiedere i criteri VPN sotto forma di file SIS agli amministratori. Se i criteri VPN vengono installati dai file SIS, non sarà necessario specificare le connessioni ai server criteri VPN. Una volta installati i criteri VPN, è possibile creare i punti di accesso VPN, quindi associarli alle applicazioni.

Se i criteri VPN contengono le chiavi private e i corrispondenti certificati, gli amministratori definiscono le **password di importazione delle chiavi** per proteggere ulteriormente le chiavi private. È necessario che gli amministratori adottino una modalità di consegna della password di importazione delle chiavi estremamente sicura.

Per installare i criteri VPN a partire da file SIS

- 1 Digitare la password di importazione delle chiavi in *Password importazione chiavi*; quindi premere *OK*.
- 2 Digitare la password dell'archivio chiavi in *Password protezione chiavi*; quindi premere *OK*.

Visualizzazione dei criteri VPN

Nella vista *Criteri VPN*, sono visualizzati i criteri VPN installati sul dispositivo cellulare.

Se viene visualizzato (*nessun criterio VPN*), è necessario installare i criteri VPN. Premere *Opzioni* e selezionare *Installa criterio* per installare i criteri VPN a partire da un server criteri VPN.

Selezionare un criterio VPN per visualizzare le seguenti informazioni:

- *Descrizione*:—questo campo consente di visualizzare informazioni aggiuntive sul criterio VPN ed è definito dagli amministratori al momento della creazione di tale criterio.
- *Stato criteri*:—indica se il criterio VPN può essere utilizzato oppure se è già in uso.
- *Stato certificato*:—indica se nel dispositivo cellulare sono disponibili certificati utente validi.
- *Nome criterio*:—indica il nome assegnato dagli amministratori al criterio VPN al momento della relativa creazione.
- *Server criteri*:—indica il nome del server criteri VPN da cui è stato installato il criterio VPN in questione. Durante la definizione delle connessioni ai server criteri VPN, a questi ultimi è necessario assegnare un nome. Questo campo non è disponibile se il criterio VPN è stato installato a partire da un file SIS.
- *Data e ora aggiornamento*:—consente di visualizzare la data dell'ultimo aggiornamento del criterio VPN da parte del server criteri VPN. Questo campo non è disponibile se il criterio VPN è stato installato a partire da un file SIS.

Stato criteri

▶ **Nota:** la vista dei dettagli dei criteri VPN non viene aggiornata se lo stato del criterio viene modificato quando la vista è aperta.

Stato criteri: dispone dei valori riportati di seguito:

- *In uso*–indica che è stata creata la connessione a un punto di accesso VPN associato al criterio VPN. Quando si crea una connessione, il criterio VPN viene automaticamente utilizzato.
- *Associato al punto di accesso VPN*–indica che il criterio VPN è stato associato a uno o più punti di accesso VPN. Per utilizzare il criterio VPN, è possibile selezionare un punto di accesso VPN qualsiasi.
- *Non associato al punto di accesso VPN*–indica che per poter utilizzare il criterio VPN, è necessario associare quest'ultimo a un punto di accesso VPN.

Stato certificato

Stato certificato: dispone dei valori riportati di seguito:

- *OK*–indica che nel dispositivo cellulare è disponibile almeno un certificato valido o che non vengono utilizzati certificati per l'autenticazione da parte dei gateway VPN.
- *Scaduto*–indica che la validità di uno o più certificati è scaduta.
Se non è possibile creare una connessione VPN, aggiornare il criterio VPN per registrare nuovi certificati.
- *Nessun certificato*–indica che nel dispositivo cellulare non è presente alcun certificato richiesto.
Se non è possibile creare una connessione VPN, aggiornare il criterio VPN per registrare nuovi certificati.
- *Non ancora valido*–indica che uno o più certificati potranno essere utilizzati in futuro. Questo valore potrebbe inoltre indicare che la data e l'ora del dispositivo cellulare non sono aggiornati, che il fuso orario non è impostato correttamente o che è attivata l'ora legale.

Premere il tasto di selezione per disattivare la visualizzazione dei dettagli e tornare alla vista [Criteri VPN](#).

Creazione di punti di accesso VPN mediante valori predefiniti

Per poter utilizzare il criterio VPN, è necessario associare quest'ultimo a un punto di accesso VPN. Nella vista [Criteri VPN](#), premere [Opzioni](#), quindi selezionare [Definisci pt. ac. VPN](#).

Il client VPN mobile crea un punto di accesso VPN utilizzando le impostazioni predefinite. È possibile creare e modificare i punti di accesso VPN nella vista relativa ai punti di accesso VPN.

Questa opzione non è disponibile nel caso in cui il criterio VPN sia stato installato a partire da un file SIS.

Aggiornamento dei criteri VPN

Durante la creazione di una connessione a un punto di accesso VPN, il server criteri VPN verifica lo stato del criterio VPN. Se è stata creata una nuova versione del criterio VPN dagli amministratori, questa viene installata nel dispositivo cellulare. Se il criterio VPN è stato eliminato dal server criteri VPN dagli amministratori, esso viene rimosso anche dal dispositivo cellulare.

Le modifiche apportate diventeranno effettive alla successiva creazione di una connessione al punto di accesso VPN, in modo da non influenzare la connessione VPN in uso.

È inoltre possibile aggiornare il criterio VPN nella vista [Criteri VPN](#). Per aggiornare un criterio VPN, selezionare il criterio VPN desiderato, premere [Opzioni](#), quindi selezionare [Aggiorna criterio](#). Lo stato del criterio VPN viene verificato dal server criteri VPN.

Eliminazione dei criteri VPN

I criteri VPN vengono eliminati in modo automatico quando si effettua la sincronizzazione di un server criteri VPN dopo che da quest'ultimo sono stati eliminati i criteri VPN da parte degli amministratori. Se un criterio VPN ancora presente nel server criteri VPN viene eliminato, verrà nuovamente installato al momento della sincronizzazione dei criteri VPN dal server criteri VPN.

Per eliminare un criterio VPN, selezionare quello desiderato e premere il tasto Cancella.

Non è possibile utilizzare un punto di accesso VPN nel caso in cui venga eliminato un criterio VPN ad esso associato.

4. Server criteri VPN

È possibile installare i criteri VPN a partire dai server criteri VPN. Durante la creazione della connessione a un punto di accesso VPN, il criterio VPN ad esso associato viene automaticamente aggiornato a partire da un server criteri VPN. Per aggiornare tutti i criteri VPN, è necessario sincronizzare i server VPN con il dispositivo cellulare. Per ulteriori informazioni, vedere "Sincronizzazione dei server criteri VPN" on page 16.

 Accedere a [Menu](#), quindi selezionare [Strumenti > Impostazioni > Impostazioni connessione > VPN > Gestione VPN > Server criteri VPN](#).

Connessione ai server criteri VPN

Durante l'installazione dei criteri VPN da un server criteri VPN, viene creata una connessione protetta tra il dispositivo mobile e il server criteri VPN. Per creare la connessione protetta, è necessario dispositivo cellulare e il server criteri VPN procedano all'autenticazione reciproca.

In seguito all'autenticazione da parte del server, viene generata una chiave privata e registrato il certificato corrispondente. Il certificato consente di effettuare l'autenticazione per il server criteri VPN. La chiave privata e il certificato vengono memorizzati in un archivio chiavi del dispositivo cellulare.

 **Suggerimento:** è possibile richiedere agli amministratori un file SIS contenente le impostazioni relative alla connessione a un server criteri VPN oppure effettuare le impostazioni per il server criteri VPN.

Installazione delle impostazioni dai file SIS

È possibile installare le impostazioni del server criteri VPN nel server criteri VPN a partire da un file SIS. La procedura di installazione delle impostazioni su un dispositivo cellulare corrisponde a quella utilizzata per l'installazione di un qualsiasi altro software.

Le impostazioni contengono l'indirizzo e il certificato server del server criteri VPN. Poiché la protezione della connessione tra il dispositivo cellulare e il server criteri VPN è determinata dal certificato server, è sufficiente specificare il nome utente e la password.

Il file SIS non contiene le impostazioni del punto di accesso Internet per stabilire la connessione al server criteri VPN. Per specificare il punto di accesso Internet, modificare le impostazioni del server criteri VPN. È inoltre possibile selezionare tale punto di accesso al momento della connessione al server criteri VPN.

Se il file SIS non è stato firmato dagli amministratori, al momento dell'installazione del file SIS viene visualizzato un avviso di protezione, che è possibile ignorare se si è certi che il file SIS è stato creato dall'amministratore del server criteri VPN e non è stato modificato.

Prima di procedere all'installazione delle impostazioni da un file SIS, uscire da [VPN](#). Diversamente l'installazione non verrà effettuata.

Visualizzazione di server criteri VPN

Nella vista [Server criteri VPN](#), è contenuto l'elenco dei server criteri VPN creati.

Se viene visualizzato ([nessun server dei criteri VPN](#)), significa che è necessario creare i server criteri VPN. Per aggiungere un server criteri VPN, premere [Opzioni](#) e selezionare [Nuovo server](#).

Aggiunta di server criteri VPN

Se le impostazioni del server criteri VPN non vengono installate a partire da un file SIS, è necessario specificare le impostazioni per il server criteri VPN.

Se si stabilisce la connessione all'indirizzo di un server criteri VPN per la prima volta, occorre effettuare l'autenticazione del server criteri VPN. Richiedere agli amministratori il codice identificativo del server criteri VPN. Verificare e completare il codice identificativo del server criteri VPN.

Una volta effettuata l'autenticazione, viene registrato un certificato da utilizzare per la successiva autenticazione presso il server criteri VPN.

Per aggiungere un server criteri VPN

- 1 Nella vista *Server criteri VPN*, premere *Opzioni*, quindi selezionare *Nuovo server*.
- 2 Selezionare *Nome server criteri* per digitare un nome da assegnare al server criteri VPN e premere *OK*.
È possibile utilizzare qualsiasi nome, purché si tratti di un nome univoco all'interno della vista dei server criteri VPN.
Se questo campo viene lasciato vuoto, al suo interno viene visualizzato *Indir. server criteri*.
Il nome del server criteri viene visualizzato nell'elenco dei server criteri VPN e sulla barra dei titoli della finestra di dialogo delle impostazioni del server criteri VPN.
- 3 Selezionare *Indir. server criteri*, digitare il nome host o l'indirizzo IP del server criteri VPN da cui si desiderano installare i criteri VPN, quindi premere *OK*.
È inoltre possibile specificare un numero di porta, separato dal simbolo di due punti (:).
Richiedere l'indirizzo del server criteri agli amministratori.
- 4 Selezionare *P.to accesso Internet*, associare il server criteri VPN a un punto di accesso, quindi premere *OK*.
Il punto di accesso viene utilizzato per stabilire la connessione al server criteri VPN.
Richiedere agli amministratori il punto di accesso da selezionare.
- 5 Premere *Indietro* per salvare le impostazioni del server criteri VPN.
- 6 Premere *Si* non appena viene richiesto di **sincronizzare** il server criteri VPN.
Viene richiesto di verificare il codice identificativo del server criteri VPN.
Richiedere agli amministratori il codice identificativo del server criteri VPN.
- 7 Confrontare con attenzione il codice identificativo del server criteri VPN visualizzato con quello ricevuto dagli amministratori, digitare i caratteri mancanti nell'apposito campo, quindi premere *OK*.



Glossario: Per

sincronizzazione si intende la procedura che consente di verificare se nel server criteri VPN sono presenti criteri nuovi e aggiornati o se sono stati eliminati dei criteri.

 **Glossario:** il nome utente e la password del server criteri VPN consentono di proteggere tale server da accessi non autorizzati.

- 8 Digitare il **nome utente** nel campo *Nome utente del server dei criteri*: e la **password** nel campo *Password server criteri*: per effettuare l'autenticazione presso il server criteri VPN, quindi premere *OK*.
Richiedere il nome utente e la password di accesso agli amministratori.

Viene registrato un certificato da utilizzare per le successive autenticazioni presso il server criteri VPN e nel dispositivo cellulare vengono installati i criteri VPN.

È quindi possibile creare i punti di accesso VPN e associarli alle applicazioni. Per ulteriori informazioni, consultare la sezione "Creazione dei punti di accesso VPN" a pagina 17.

Modifica dei server criteri VPN

Selezionare un server criteri VPN nella vista *Server criteri VPN* per visualizzare o modificare le relative impostazioni.

Selezionare *Nome server criteri* per digitare un nuovo nome da assegnare al server criteri. Il nuovo nome appare nella vista *Server criteri VPN*.

Una volta installati i criteri VPN a partire dal server criteri VPN, non è possibile modificare *Indir. server criteri*, in quanto il server criteri VPN invia l'indirizzo durante la prima connessione.

Se il punto di accesso associato al server criteri VPN è stato eliminato, in *P.to accesso Internet* viene visualizzato il testo (non selezionato). Selezionare *P.to accesso Internet* per selezionare un nuovo punto di accesso. Se sono stati eliminati tutti i punti di accesso, non è possibile salvare le impostazioni.

Sincronizzazione dei server criteri VPN

Selezionare un server criteri VPN nella vista *Server criteri VPN*, premere *Opzioni*, quindi selezionare *Sincronizza server* per installare e aggiornare i criteri dal server criteri VPN.

Quest'ultimo viene analizzato per individuare se i criteri VPN sono stati aggiunti, aggiornati o eliminati.

Se il server criteri VPN contiene criteri VPN nuovi o aggiornati, questi vengono installati nel dispositivo cellulare. I criteri VPN che sono stati eliminati dal server criteri VPN dagli amministratori vengono rimossi anche dal dispositivo cellulare.

Alla prima sincronizzazione di un server criteri VPN, per ciascun criterio VPN installato sul dispositivo cellulare viene creato un punto di accesso VPN corrispondente. È possibile creare e modificare i punti di accesso VPN nella vista [Punti di accesso VPN](#).

Durante la connessione al server criteri VPN per installare o aggiornare i criteri VPN, potrebbe essere necessario effettuare la registrazione di certificati VPN dal server criteri VPN.

Registrazione dei certificati VPN

Per ogni certificato viene creata una richiesta di certificazione e inviata al server criteri VPN. Il server criteri VPN registra i certificati necessari mediante l'**autorità di certificazione**.

La richiesta di certificazione e il certificato corrispondente contengono l'identità dell'utente. A seconda della configurazione del server criteri VPN, l'identità dell'utente di tale server può essere inoltre utilizzata come identità utente nei certificati VPN. Se tale opzione non è disponibile, viene richiesto di specificare l'identità utente per un dominio specifico.

Per creare una richiesta di certificazione

- 1 Digitare l'identificativo utente del certificato relativo al dominio specifico in [Identità utente per](#) :
Gli amministratori comunicheranno le informazioni da digitare.
- 2 Premere [OK](#).

Eliminazione dei server criteri VPN

Per eliminare un server criteri VPN, selezionare quello desiderato nella vista [Server criteri VPN](#), quindi premere il tasto Cancella.

Confermare l'eliminazione dei criteri VPN installati a partire dal server criteri VPN.

5. Punti di accesso VPN

Un punto di accesso VPN è un punto di accesso virtuale che associa un criterio VPN ad un punto di accesso Internet. Per creare una connessione VPN, selezionare dall'elenco dei punti di accesso Internet un punto di accesso VPN.

➡ Accedere a *Menu*, quindi selezionare *Strumenti > Impostazioni > Impostazioni connessione > VPN > Punti di accesso VPN*.

Visualizzazione dei punti di accesso VPN

Nella vista *Punti di accesso VPN* sono visualizzati i punti di accesso VPN creati mediante il dispositivo cellulare. Il messaggio *(nessun punto di accesso VPN)* indica che non è stato creato alcun punto di accesso VPN. Per creare un nuovo punto di accesso VPN, premere *Opzioni*, quindi selezionare *Nuovo p.to accesso*.

Selezionare un punto di accesso VPN, quindi *Opzioni > Modifica* per visualizzare e modificare le informazioni riportate di seguito:

- *Nome connessione*—identifica il punto di accesso VPN incluso negli elenchi dei punti di accesso.
- *Criterio VPN*—nome del criterio VPN associato al punto di accesso VPN.
- *P.to accesso Internet*—nome del punto di accesso in base al quale viene creata la connessione VPN.
- *Indirizzo serv. proxy*—indirizzo di un server proxy all'interno della rete aziendale.
- *Numero porta proxy*—numero della porta a cui è collegato il server proxy.

Creazione di punti di accesso VPN

Alla prima apertura della vista *Punti di accesso VPN*, viene richiesto di creare un punto di accesso VPN. Premere *Sì*.

 **Suggerimento:** se nelle impostazioni dei punti di accesso VPN viene specificato un server proxy, non è necessario specificare tale server nelle impostazioni del browser Internet.

Per creare i punti di accesso VPN

- 1 Premere *Opzioni*, quindi selezionare *Nuovo p.to accesso*.
- 2 Selezionare *Nome connessione* per modificare il nome della connessione.
È possibile selezionare un nome qualsiasi.
- 3 Selezionare *Criterio VPN* per definire la modalità di crittografia della connessione.
Se l'elenco è vuoto, è necessario installare i criteri VPN a partire dai file SIS o dai server criteri VPN.
- 4 Selezionare *P.to accesso Internet* per scegliere un punto di accesso da utilizzare per la connessione VPN.
Se l'elenco è vuoto, occorre creare i punti di accesso.
- 5 Selezionare *Indirizzo serv. proxy* per digitare l'indirizzo di un server proxy all'interno della rete aziendale.
- 6 Selezionare *Numero porta proxy* per modificare il numero di porta predefinito, ovvero 80.

Eliminazione di punti di accesso VPN

Per eliminare un punto di accesso VPN, selezionare quello desiderato nella vista *Punti di accesso VPN*, quindi premere il tasto Cancella.

6. Registro VPN

Il registro VPN contiene i messaggi registrati durante le operazioni di aggiornamento e sincronizzazione dei criteri VPN e di creazione delle connessioni VPN ai gateway VPN.

Visualizzazione del registro VPN

Nella vista [Registro VPN](#) è visualizzato il numero di versione del client VPN.

È possibile visualizzare il tipo, l'ora e l'inizio dei messaggi di registro. Selezionare un messaggio di registro per visualizzarlo in modo completo.

Nella vista [Registro VPN](#), i messaggi di registro sono ordinati in base a data e ora, a partire da quelli più recenti. È possibile visualizzare i messaggi fino al momento dell'apertura della vista [Registro VPN](#). Premere [Opzioni](#), quindi selezionare [Aggiorna registro](#) per visualizzare i messaggi di registro più recenti.

I messaggi di registro contengono codici di errore, stato e motivo. In caso di errori, comunicare tali codici agli amministratori.

Cancellazione del registro VPN

I messaggi di registro vengono registrati in un buffer circolare. Se la dimensione del registro raggiunge 20 kilobyte, i nuovi messaggi di registro sostituiscono quelli meno recenti.

Per eliminare tutti i messaggi dal registro e cancellare il contenuto della vista [Registro VPN](#), premere [Opzioni](#), quindi selezionare [Cancella registro](#).

➡ Accedere a [Menu](#), quindi selezionare [Strumenti > Impostazioni > Impostazioni connessione > VPN > Gestione VPN > Registro VPN](#).

Icone:  indica un errore,  indica un avviso e  indica una descrizione.

7. Password dell'archivio delle chiavi

➡ Accedere a [Menu](#), quindi selezionare [Strumenti](#) > [Impostazioni](#) > [Impostazioni connessione](#) > [VPN](#) > [Gestione VPN](#) > [Password protezione chiavi](#).

▶ **Suggerimento:** una password dell'archivio chiavi può contenere lettere e numeri e deve essere composta da almeno sei caratteri.

La password dell'archivio chiavi consente di proteggere le chiavi private del dispositivo cellulare e delle connessioni del server criteri VPN da accessi non autorizzati.

Creazione o modifica della password dell'archivio chiavi

È possibile creare la password dell'archivio chiavi al momento dell'installazione del primo criterio VPN. Se una password dell'archivio chiavi viene scoperta o decifrata da hacker, questi ultimi possono utilizzare il dispositivo cellulare per accedere alla rete aziendale protetta da VPN. Per questo motivo, è necessario creare password dell'archivio chiavi di lunghezza sufficiente da impedirne la decifrazione. Assicurarsi di mantenere la password segreta e di non annotarla.

Per creare o modificare la password dell'archivio chiavi:

- 1 In [Nuova password archivio chiavi](#); digitare una password facile da ricordare, ma difficile da indovinare.
- 2 Selezionare [Verifica password](#); quindi digitare di nuovo la password, onde evitare errori di battitura.
- 3 Premere [OK](#) per creare la password.

Immissione delle password dell'archivio chiavi

La password dell'archivio chiavi deve essere specificata nei seguenti casi:

- Se vengono installati criteri VPN nuovi o aggiornati dai server criteri VPN.
- Se vengono utilizzate applicazioni per stabilire la connessione ai punti di accesso VPN che richiedono l'autenticazione del certificato.

▶ **Nota:** quando si digita la password, il metodo di scrittura intuitivo non è disponibile. È necessario digitare i caratteri uno alla volta. Vengono utilizzati i caratteri minuscoli per impostazione predefinita.

8. VPN e applicazioni

Se per creare una connessione VPN viene utilizzata un'applicazione, il client VPN esegue quanto segue:

- Stabilisce la connessione al punto di accesso Internet associato al punto di accesso VPN.
- Carica il criterio VPN associato al punto di accesso VPN.
- Stabilisce la connessione al gateway VPN per creare la connessione VPN.

Autenticazione da parte del gateway VPN

Per accedere alla rete aziendale, occorre dimostrare la propria identità. Il criterio VPN determina il metodo di autenticazione utilizzato:

- Autenticazione basata su certificato–È necessario disporre di un certificato firmato da un'autorità di certificazione attendibile. Per ottenere tale certificato, è possibile utilizzare la registrazione in linea oppure recuperarlo durante l'installazione del criterio VPN da un file SIS.
- Autenticazione legacy–Per l'autenticazione, è necessario disporre di nomi utenti e password o codici di protezione. I nomi utente e le password sono creati dagli amministratori, mentre i codici di protezione vengono generati mediante token SecurID, anch'essi forniti dagli amministratori.

Se per l'autenticazione si utilizzano certificati, immettere la password dell'archivio chiavi.

Se si utilizza l'autenticazione legacy, digitare le informazioni di autenticazione VPN durante l'uso delle applicazioni di connessione ai punti di accesso VPN e la negoziazione tra il dispositivo cellulare e il gateway VPN relativa alle connessioni crittografate.

Per effettuare l'autenticazione presso un gateway VPN

- 1 Digitare il nome utente VPN in *Nome utente VPN*.
- 2 Digitare la password o il codice di protezione VPN:

- Digitare la password in *Password VPN*:
 - Creare un codice di protezione SecurID, digitarlo in *Codice protezione VPN*; quindi premere *OK*.
- 3** Se il token SecurID non è sincronizzato con l'orologio di ACE/Server, viene richiesto il codice di protezione successivo che ACE/Server utilizza come nuovo riferimento per la base temporale del token.
Creare e digitare un nuovo codice di protezione in *Codice protezione successivo*:
In caso di errore, rivolgersi agli amministratori.
- 4** Premere *OK*.

9. Guida alla soluzione dei problemi

Nella tabella riportata di seguito sono elencati i messaggi di errore in ordine alfabetico, le possibili cause di tali errori e le operazioni necessarie per risolverli.

Messaggio	Causa	Soluzione
<i>Autenticazione non riuscita. Verificare nome utente e password.</i>	<ul style="list-style-type: none">• Il nome utente o la password digitati per l'autenticazione da parte del server criteri VPN o per l'accesso a VPN sono errati.• In seguito alla richiesta del codice di protezione successivo, è stato digitato un codice errato.	<ul style="list-style-type: none">• Verificare nome utente e password e tentare di nuovo.• Attendere fino a quando il codice di protezione nella vista del token SecurID non cambia, quindi digitare il codice di protezione.

Messaggio	Causa	Soluzione
<i>Password non corretta</i>	La password dell'archivio o di importazione delle chiavi digitata è errata.	<ul style="list-style-type: none"> • Verificare la password e tentare di nuovo. • Richiedere la password di importazione delle chiavi agli amministratori. La password dell'archivio delle chiavi viene invece creata dall'utente stesso.
<i>Codice di identificazione del server errato</i>	In seguito alla richiesta di immissione del codice identificativo del server criteri VPN, è stata digitata una stringa errata.	Verificare il codice identificativo del server criteri VPN confrontandolo con il codice ricevuto dagli amministratori, quindi digitare nuovamente i caratteri mancanti.
<i>Impossibile eliminare server dei criteri. È in uso.</i>	Non è possibile eliminare il server criteri VPN durante l'aggiornamento dei criteri VPN dal server. Se per creare una connessione VPN viene utilizzata un'applicazione, i criteri VPN vengono aggiornati in modo automatico.	Attendere il termine dell'aggiornamento dei criteri VPN, quindi riprovare.

Messaggio	Causa	Soluzione
<i>Impossibile attivare la connessione VPN. Aggiornare prima il criterio VPN.</i>	<ul style="list-style-type: none"> • Si è verificato un errore nell'autenticazione legacy. • Il certificato utilizzato per l'autenticazione da parte del gateway VPN è mancante, scaduto o non ancora valido. 	<ul style="list-style-type: none"> • Verificare nome utente e password e tentare di nuovo. • Selezionare un criterio VPN nella vista <i>Criteri VPN</i>, premere <i>Opzioni</i>, quindi selezionare <i>Aggiorna criterio</i> per aggiornare il criterio VPN. • Verificare le impostazioni di data e ora del dispositivo cellulare.
<i>Impossibile accedere al server dei criteri. Eliminare il server e ridefinire i dettagli.</i>	Il certificato server del server criteri VPN è scaduto.	<p>Nella vista <i>Server criteri VPN</i>:</p> <ol style="list-style-type: none"> 1 Premere <i>Opzioni</i>, quindi selezionare <i>Elimina server</i> per eliminare il server criteri VPN. 2 Premere <i>Opzioni</i> e selezionare <i>Nuovo server</i> per aggiungere di nuovo il server criteri VPN oppure richiedere all'amministratore un file SIS contenente le nuove impostazioni del server criteri VPN.

Messaggio	Causa	Soluzione
<i>Impossibile accedere al server dei criteri. Inserire nome utente e password del server.</i>	Il certificato di autenticazione del server criteri VPN è scaduto o è stato revocato dagli amministratori.	<ul style="list-style-type: none"> • Comunicare l'errore agli amministratori che provvederanno a fornire una password OTP (One-Time Password) per l'accesso. • Digitare il nome utente e la password OTP per l'autenticazione da parte del server criteri VPN. • Un nuovo certificato viene registrato in modo automatico.
<i>Impossibile accedere al server dei criteri. Per dettagli, vedere il registro VPN.</i>	Il periodo di validità del certificato di autenticazione richiesto dal server criteri VPN non è ancora iniziato.	Verificare le impostazioni di data e ora o attendere fino all'inizio del periodo di validità del certificato.

Messaggio	Causa	Soluzione
<ul style="list-style-type: none"> • <i>Impossibile aggiornare il criterio. Per dettagli, vedere il registro VPN.</i> • <i>Impossibile sincronizzare. Vedere il registro VPN per i dettagli.</i> 	Si è verificato un errore durante il download dei criteri VPN dal server criteri VPN o durante la relativa installazione sul dispositivo cellulare.	<ul style="list-style-type: none"> • Nella vista <i>Criteri VPN</i>, selezionare un certificato VPN, premere <i>Opzioni</i>, quindi selezionare <i>Aggiorna criterio</i> per aggiornare un criterio VPN. • Nella vista <i>Server criteri VPN</i>, selezionare un server criteri VPN, premere <i>Opzioni</i>, quindi selezionare <i>Sincronizza server</i> per installare i criteri a partire dal server criteri VPN.
<i>Criterio VPN eliminato. Provare a ridefinire il punto di accesso VPN.</i>	Il criterio VPN associato al punto di accesso VPN è stato eliminato perché obsoleto.	Nella vista <i>Punti di accesso VPN</i> , selezionare un punto di accesso VPN, premere <i>Opzioni</i> , quindi selezionare <i>Modifica</i> per associare un altro criterio VPN al punto di accesso VPN

Indice analitico

A

- Archivio chiavi 13
- Autenticazione basata su certificato 24
- Autenticazione legacy 24
- Autenticazione non riuscita. Verificare nome utente e password. 26
- Avvisi di protezione 14

C

Campi

- Codice protezione successivo 25
- Nome utente VPN 24
- Password VPN 24

campi

- aggiornamento 9
- Codice protezione successivo 25
- Codice protezione VPN 25
- Criterio VPN 19
- Descrizione 9
- Indir. server criteri 15
- Indirizzo serv. proxy 19
- Nome connessione 19
- Nome criterio 9
- Nome server criteri 15
- Nome utente del server dei criteri 16
- Numero porta proxy 19
- Nuova password archivio chiavi 22

- P.to accesso Internet 15, 19
- Password server criteri 16
- Server criteri 9
- Stato certificato 9
- Stato criteri 9, 10

campo Codice protezione successivo 25

Campo Codice protezione VPN 25

Campo Criterio VPN 19

Campo Descrizione 9

Campo di aggiornamento 9

Campo Indir. server criteri 15

Campo Indirizzo serv. proxy 19

Campo Nome connessione 19

Campo Nome criterio 9

Campo Nome server criteri 15

Campo Nome utente del server dei criteri 16

campo Nome utente VPN 24

Campo Numero porta proxy 19

Campo Nuova password

archivio chiavi 22

Campo P.to accesso Internet 15, 19

Campo Password server criteri 16

campo Password VPN 24

Campo Server criteri 9

Campo Stato certificato 9

Campo Stato criteri 9, 10

Certificati

- autenticazione presso i server criteri VPN 13
- registrazione 17

certificati

- identità utente 17
- stato 10

Certificati mancanti 10

Certificati non ancora validi 10

Certificati scaduti 10

Client VPN

- requisiti di sistema 6
- uso 4

Codice di protezione SecurID 25

Codice protezione successivo 25

Criteri VPN

- aggiornamento 11
- eliminazione 12
- stato 10
- visualizzazione 9

Criterio VPN eliminato. Provare a ridefinire il punto di accesso VPN. 30

I

Impossibile accedere al server dei criteri. Eliminare il server e ridefinire i dettagli. 28

- Impossibile accedere al server dei criteri. Inserire nome utente e password del server. 29
- Impossibile accedere al server dei criteri. Vedere il registro VPN per i dettagli. 29
- Impossibile aggiornare il criterio. Vedere il registro VPN per i dettagli. 30
- Impossibile attivare la connessione VPN. Aggiornare prima il criterio VPN. 28
- Impossibile eliminare server dei criteri. È in uso. 27
- Impossibile sincronizzare. Vedere il registro VPN per i dettagli. 30
- Incorrect password. 27
- Incorrect server identity code. 27
- Installazione
 - impostazioni del server criteri VPN a partire dai file SIS 13
- Installazione dei criteri VPN 16
- M**
- Messaggi di errore 26
- N**
- nessun certificato 10
- Nessun criterio VPN 9
- Nessun punto di accesso VPN 19
- Nessun server dei criteri VPN 14

- O**
- Opzione Cancella registro 21
- Opzione di aggiornamento 21
- Opzione di modifica 19
- Opzione Elimina criterio 12
- Opzione Nuovo server 14
- Opzione relativa al nuovo punto di accesso 19
- Opzione Sincronizza server 16

P

- Password archivio chiavi
 - creazione 22
 - informazioni 8, 22
- Punti di accesso VPN
 - modifica 19
 - vista 19, 20

R

- Registro VPN
 - vista 21
- Requisiti di memoria 6
- requisiti di sistema 6

S

- Server criteri VPN
 - aggiunta 14
 - connessione 13
 - installazione delle impostazioni dai file SIS 13
 - sincronizzazione 16
 - visualizzazione 14

U

Un 19

V

VPN 6

- autenticazione 24
- uso con le applicazioni 24