Configurazione di Cisco VPN 3000 Concentrator con Microsoft RADIUS

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Installare e configurare il server RADIUS in Windows 2000 e Windows 2003
Installare il server RADIUS
Configurazione di Microsoft Windows 2000 Server con IAS
Configurazione di Microsoft Windows 2003 Server con IAS
Configurazione di Cisco VPN 3000 Concentrator per autenticazione RADIUS
Verifica
Risoluzione dei problemi
Autenticazione WebVPN non riuscita
Autenticazione utente non riuscita con Active Directory
Informazioni correlate

Introduzione

Microsoft Internet Authentication Server (IAS) e Microsoft Commercial Internet System (MCIS 2.0) sono attualmente disponibili. Il server Microsoft RADIUS è utile perché utilizza Active Directory nel controller di dominio primario per il proprio database utenti. Non è più necessario gestire un database separato. Supporta anche la crittografia a 40 bit e a 128 bit per le connessioni VPN Point-to-Point Tunneling Protocol (PPTP). Per ulteriori informazioni, fare riferimento all'elenco di controllo Microsoft: Per ulteriori informazioni, configurare IAS per la documentazione sull'accesso remoto e VPN .

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Installare e configurare il server RADIUS in Windows 2000 e Windows 2003

Installare il server RADIUS

Se il server RADIUS (IAS) non è già installato, eseguire la procedura seguente per installarlo. Se il server RADIUS è già installato, continuare con la procedura di configurazione.

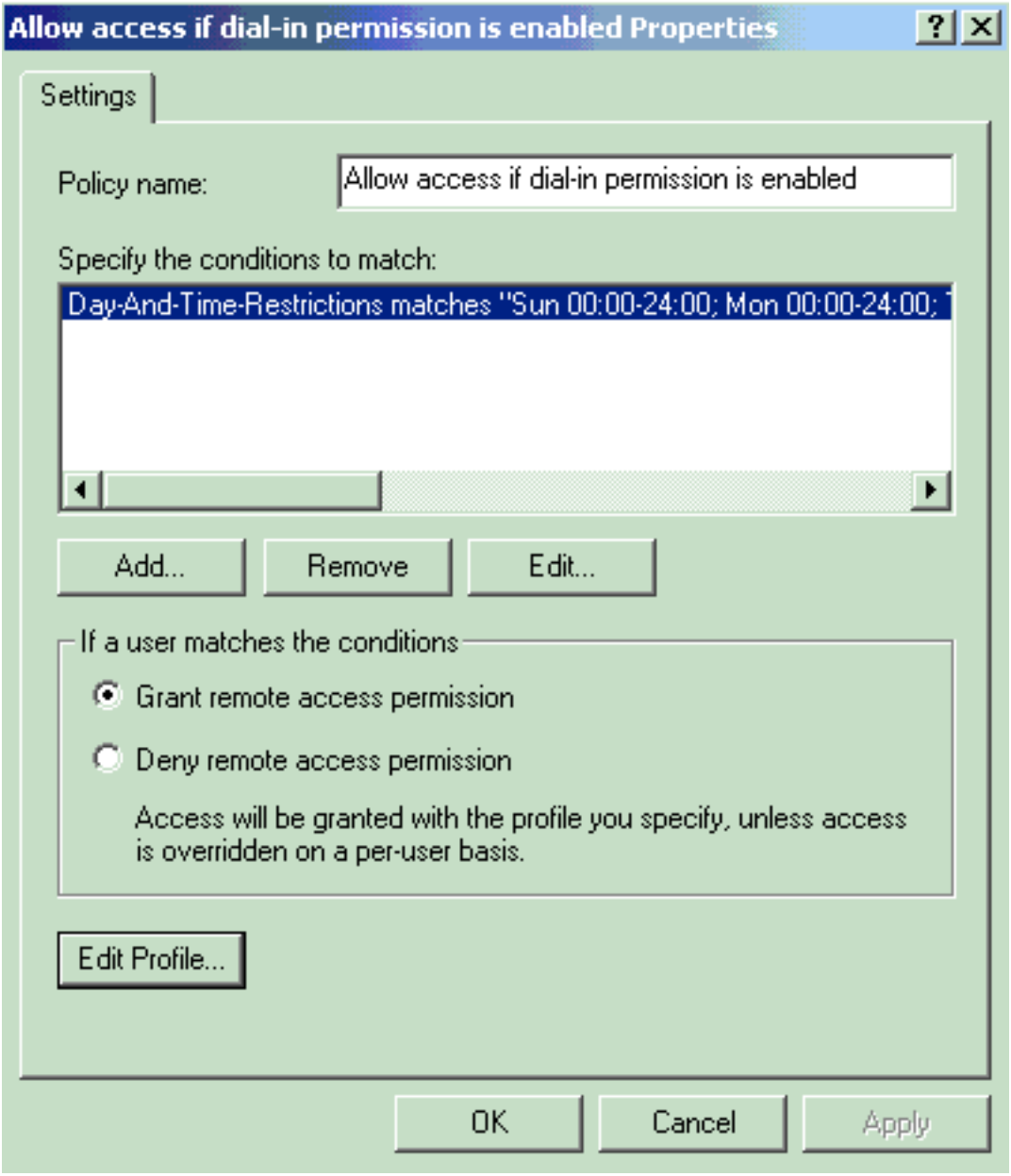
1. Inserire il CD di Windows Server e avviare il programma di installazione.
2. Fare clic su **Installa componenti aggiuntivi** e quindi su **Aggiungi/Rimuovi componenti di Windows**.
3. In Componenti fare clic su **Servizi di rete**, senza selezionare o deselezionare la casella di controllo, e quindi fare clic su **Dettagli**.
4. Selezionare **Internet Authentication Service** e fare clic su **OK**.
5. Fare clic su **Next** (Avanti).

Configurazione di Microsoft Windows 2000 Server con IAS

Completare la procedura descritta di seguito per configurare il server RADIUS (IAS) e avviare il servizio in modo da renderlo disponibile per l'autenticazione degli utenti nel concentratore VPN.

1. Scegliere **Start > Programmi > Strumenti di amministrazione > Servizio di autenticazione Internet**.
2. Fare clic con il pulsante destro del mouse su **Servizio di autenticazione Internet** e scegliere **Proprietà** dal sottomenu visualizzato.
3. Andare alla scheda RADIUS per esaminare le impostazioni delle porte.Se le porte UDP (User Datagram Protocol) di autenticazione e accounting RADIUS sono diverse dai valori predefiniti specificati (1812 e 1645 per l'autenticazione, 1813 e 1646 per l'accounting) in Autenticazione e accounting, digitare le impostazioni della porta. Al termine, fare clic su **OK**.**Nota:** non modificare le porte predefinite. Separare le porte utilizzando le virgole per utilizzare più impostazioni di porta per le richieste di autenticazione o accounting.
4. Fare clic con il pulsante destro del mouse su **Client** e scegliere **Nuovo client** per aggiungere il concentratore VPN come client di autenticazione, autorizzazione e accounting (AAA) al server RADIUS (IAS).**Nota:** se la ridondanza è configurata tra due Cisco VPN 3000 concentrator, anche il Cisco VPN 3000 concentrator di backup deve essere aggiunto al server RADIUS come client RADIUS.
5. Immettere un nome descrittivo e selezionare **Raggio protocollo**.
6. Definire il concentratore VPN con un indirizzo IP o un nome DNS nella finestra successiva.
7. Selezionare **Cisco** dalla barra di scorrimento Client-Vendor.
8. Immettere un segreto condiviso.**Nota:** devi ricordare il segreto *esatto* che usi. Queste informazioni sono necessarie per configurare VPN Concentrator.
9. Fare clic su **Finish** (Fine).

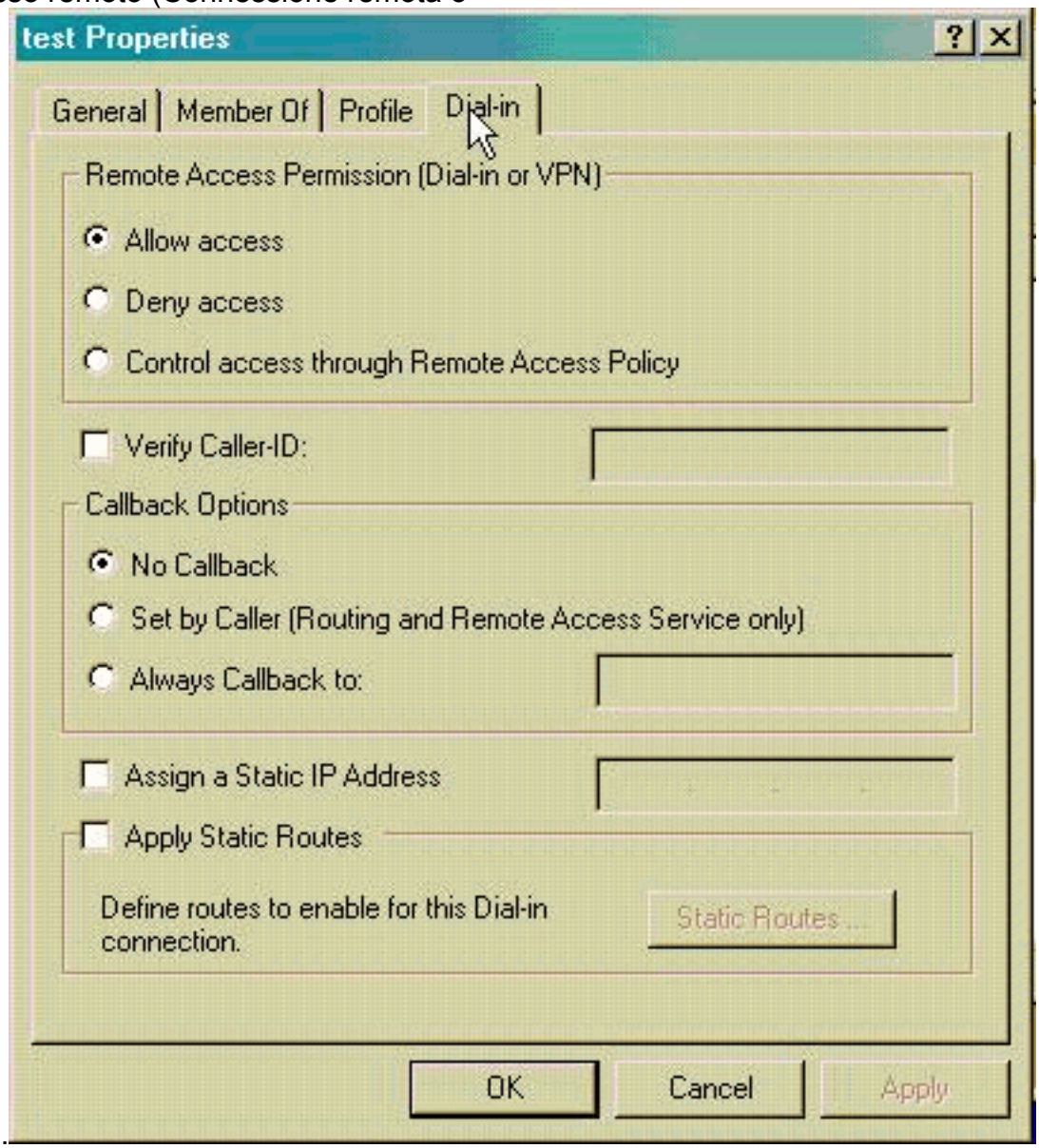
10. Fare doppio clic su **Criteri di accesso remoto** e quindi sul criterio visualizzato sul lato destro della finestra.**Nota:** dopo l'installazione di IAS, dovrebbe già esistere un criterio di accesso remoto.In Windows 2000 l'autorizzazione viene concessa in base alle proprietà della connessione remota di un account utente e ai criteri di accesso remoto. I criteri di accesso remoto sono un insieme di condizioni e impostazioni di connessione che consentono agli amministratori di rete una maggiore flessibilità nell'autorizzazione dei tentativi di connessione. Il servizio Routing e Accesso remoto di Windows 2000 e lo IAS di Windows 2000 utilizzano entrambi i criteri di accesso remoto per determinare se accettare o rifiutare i tentativi di connessione. In entrambi i casi, i criteri di accesso remoto vengono archiviati localmente. Per ulteriori informazioni sull'elaborazione dei tentativi di connessione, consultare la documentazione di Windows 2000 IAS.



11. Per configurare le proprietà della connessione remota, scegliere **Concedi autorizzazione di accesso remoto** e fare clic su **Modifica profilo**.
12. Selezionare il protocollo da utilizzare per l'autenticazione nella scheda Autenticazione. Selezionare **Microsoft Encrypted Authentication versione 2** e deselezionare tutti gli altri protocolli di autenticazione.**Nota:** le impostazioni in questo profilo chiamate in ingresso devono corrispondere a quelle nella configurazione di VPN 3000 Concentrator e del client chiamate in ingresso. In questo esempio viene utilizzata l'autenticazione MS-CHAPv2

senza crittografia PPTP.

13. Nella scheda Crittografia selezionare solo **Nessuna crittografia**.
14. Per chiudere il profilo di Accesso remoto, fare clic su **OK**, quindi su **OK** per chiudere la finestra dei criteri di accesso remoto.
15. Fare clic con il pulsante destro del mouse su **Servizio di autenticazione Internet** e scegliere **Avvia servizio** dall'albero della console.**Nota:** è possibile utilizzare questa funzione anche per arrestare il servizio.
16. Completare questi passaggi per modificare gli utenti in modo da consentire la connessione.Scegliere **Console > Aggiungi/Rimuovi snap-in**.Fare clic su **Aggiungi** e scegliere **lo snap-in Utenti e gruppi locali**.Fare clic su **Add**.Assicurarsi di selezionare **Computer locale**Fare clic su **Fine** e **OK**.
17. Espandere **Utenti e gruppi locali** e fare clic sulla cartella **Utenti** nel riquadro sinistro. Nel riquadro destro fare doppio clic sull'utente (utente VPN) a cui si desidera consentire l'accesso.
18. Andare alla scheda Connessione remota e scegliere **Consenti accesso** in Autorizzazione di accesso remoto (Connessione remota o VPN).



19. Per completare l'azione, fare clic su **Apply** (Applica) e **OK**. Se desiderato, è possibile chiudere la finestra Gestione console e salvare la sessione.Gli utenti modificati possono ora accedere al concentratore VPN con il client VPN. Tenete presente che il server IAS

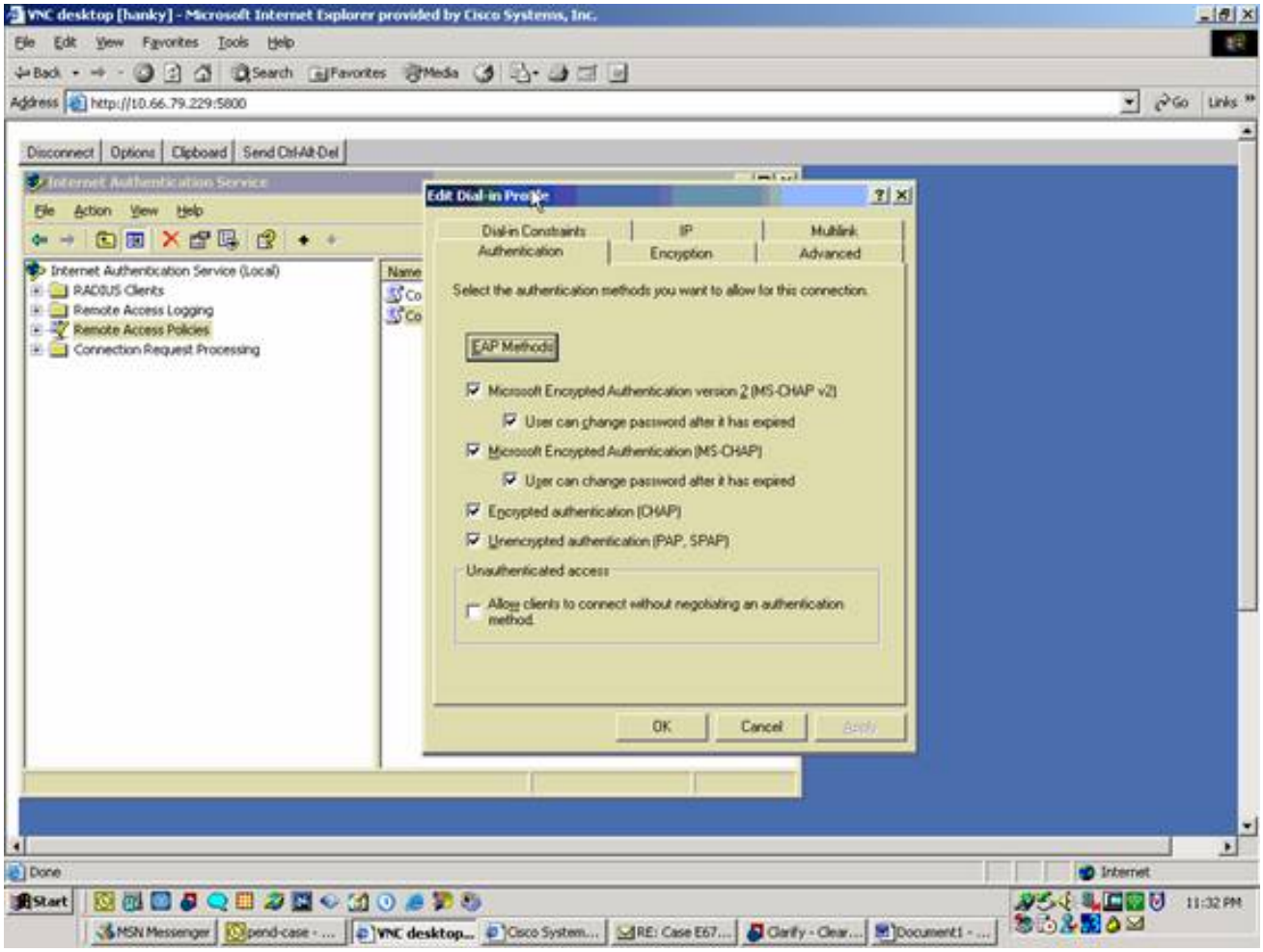
autentica solo le informazioni utente. VPN Concentrator esegue ancora l'autenticazione del gruppo.

Configurazione di Microsoft Windows 2003 Server con IAS

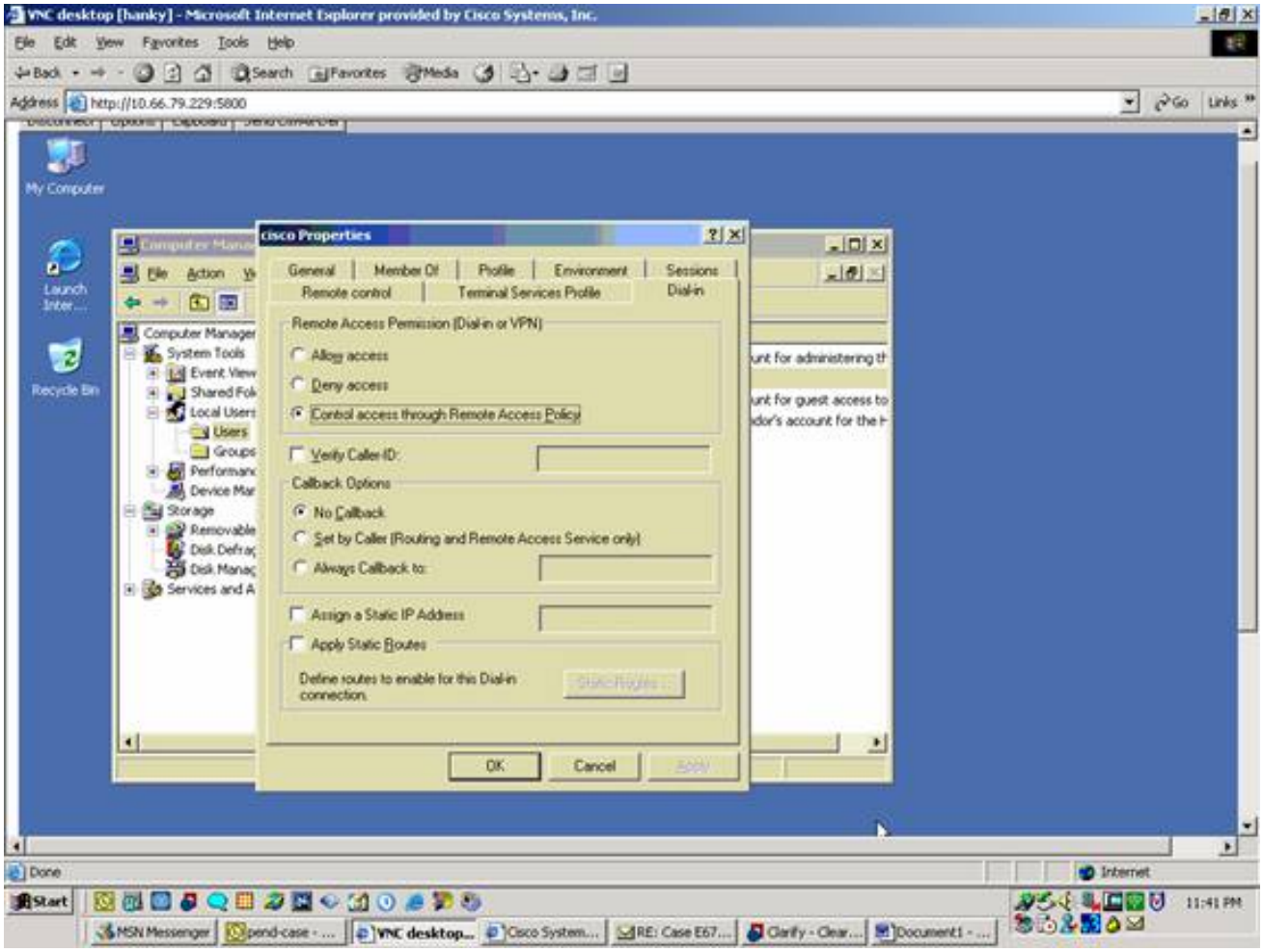
Completare questa procedura per configurare il server Microsoft Windows 2003 con IAS.

Nota: in questa procedura si presuppone che IAS sia già installato nel computer locale. In caso contrario, aggiungerlo tramite **Pannello di controllo > Installazione applicazioni**.

1. Scegliere **Strumenti di amministrazione > Servizio di autenticazione Internet** e fare clic con il pulsante destro del mouse su **Client RADIUS** per aggiungere un nuovo client RADIUS. Dopo aver digitato le informazioni sul client, fare clic su **OK**.
2. Immettere un nome descrittivo.
3. Definire il concentratore VPN con un indirizzo IP o un nome DNS nella finestra successiva.
4. Selezionare **Cisco** dalla barra di scorrimento Client-Vendor.
5. Immettere un segreto condiviso.**Nota:** devi ricordare il segreto *esatto* che usi. Queste informazioni sono necessarie per configurare VPN Concentrator.
6. Fare clic su **OK** per completare l'operazione.
7. Fare clic su **Criteri di accesso remoto**, fare clic con il pulsante destro del mouse su **Connessioni ad altri server di accesso** e scegliere **Proprietà**.
8. Per configurare le proprietà della connessione remota, scegliere **Concedi autorizzazione di accesso remoto** e fare clic su **Modifica profilo**.
9. Selezionare il protocollo da utilizzare per l'autenticazione nella scheda Autenticazione. Selezionare **Microsoft Encrypted Authentication versione 2** e deselezionare tutti gli altri protocolli di autenticazione.**Nota:** le impostazioni in questo profilo chiamate in ingresso devono corrispondere a quelle nella configurazione di VPN 3000 Concentrator e del client chiamate in ingresso. In questo esempio viene utilizzata l'autenticazione MS-CHAPv2 senza crittografia PPTP.
10. Nella scheda Crittografia selezionare solo **Nessuna crittografia**.
11. Al termine, fare clic su **OK**.



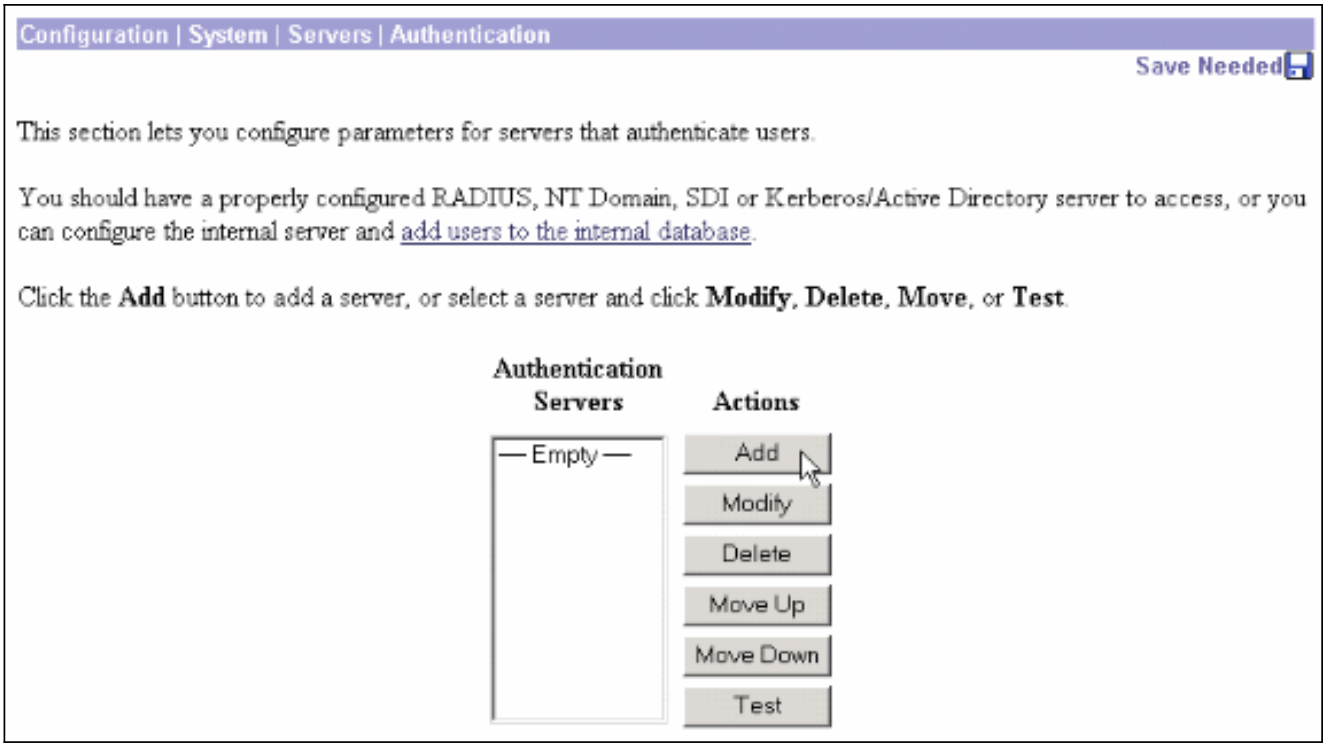
12. Fare clic con il pulsante destro del mouse su **Servizio di autenticazione Internet** e scegliere **Avvia servizio** dall'albero della console.**Nota:** è possibile utilizzare questa funzione anche per arrestare il servizio.
13. Scegliere **Strumenti di amministrazione > Gestione computer > Utilità di sistema > Utenti e gruppi locali**, fare clic con il pulsante destro del mouse su **Utenti** e scegliere **Nuovi utenti** per aggiungere un utente all'account del computer locale.
14. Aggiungere l'utente con la password Cisco "vpnpassword" e controllare le informazioni del profilo.Nella scheda Generale, assicurarsi che l'opzione **Password Never Expired** (Password non scaduta) sia selezionata anziché l'opzione User Must Change Password (Modifica password obbligatoria).Nella scheda Chiamate in ingresso scegliere l'opzione **Consenti accesso** (o lasciare l'impostazione predefinita Controlla accesso tramite Criteri di accesso remoto).Al termine, fare clic su
OK.



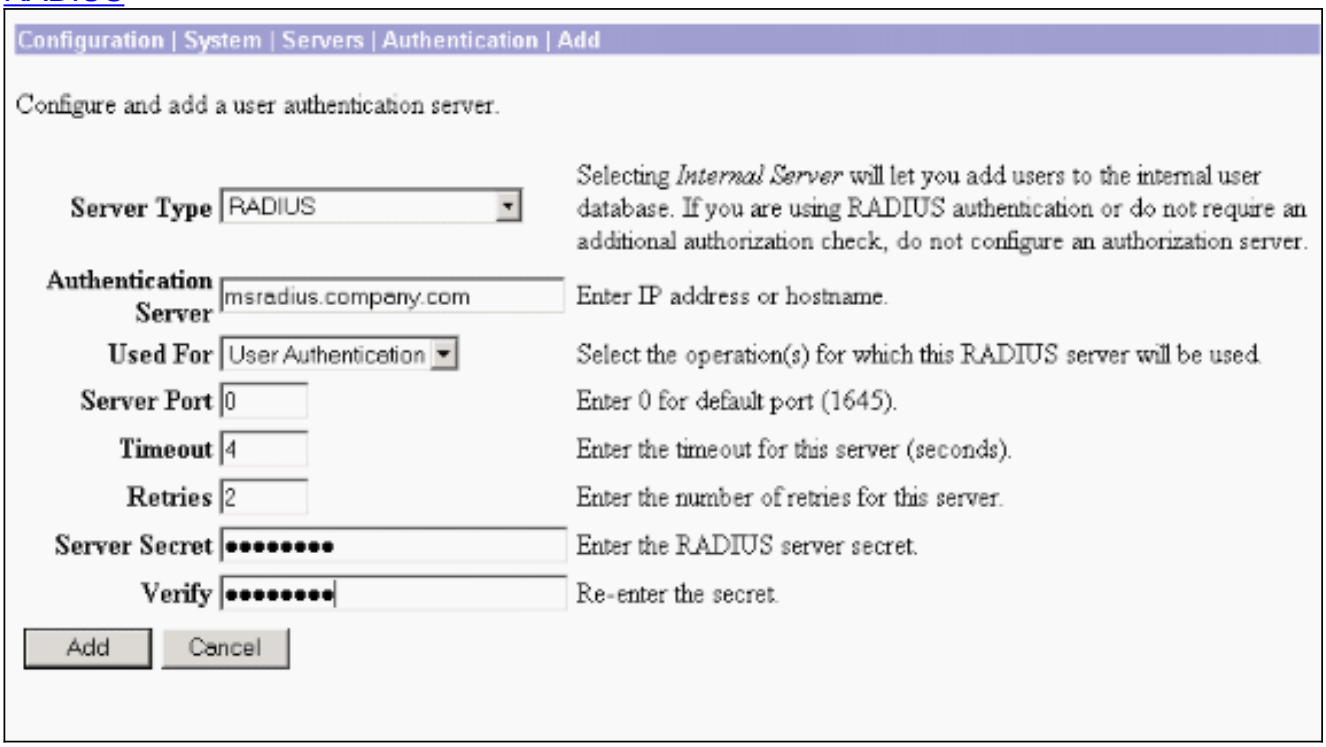
Configurazione di Cisco VPN 3000 Concentrator per autenticazione RADIUS

Completare questa procedura per configurare Cisco VPN 3000 Concentrator per l'autenticazione RADIUS.

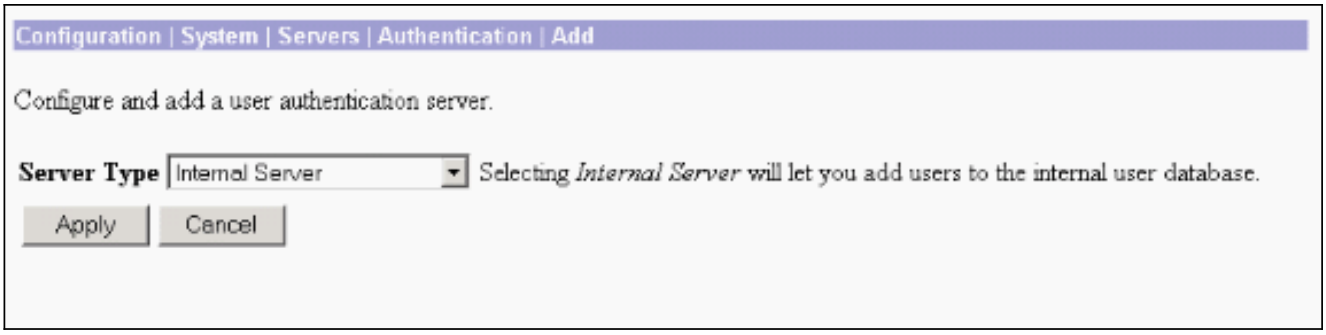
1. Collegarsi a VPN Concentrator con il browser Web e scegliere **Configurazione > Sistema > Server > Autenticazione** dal menu del frame a sinistra.



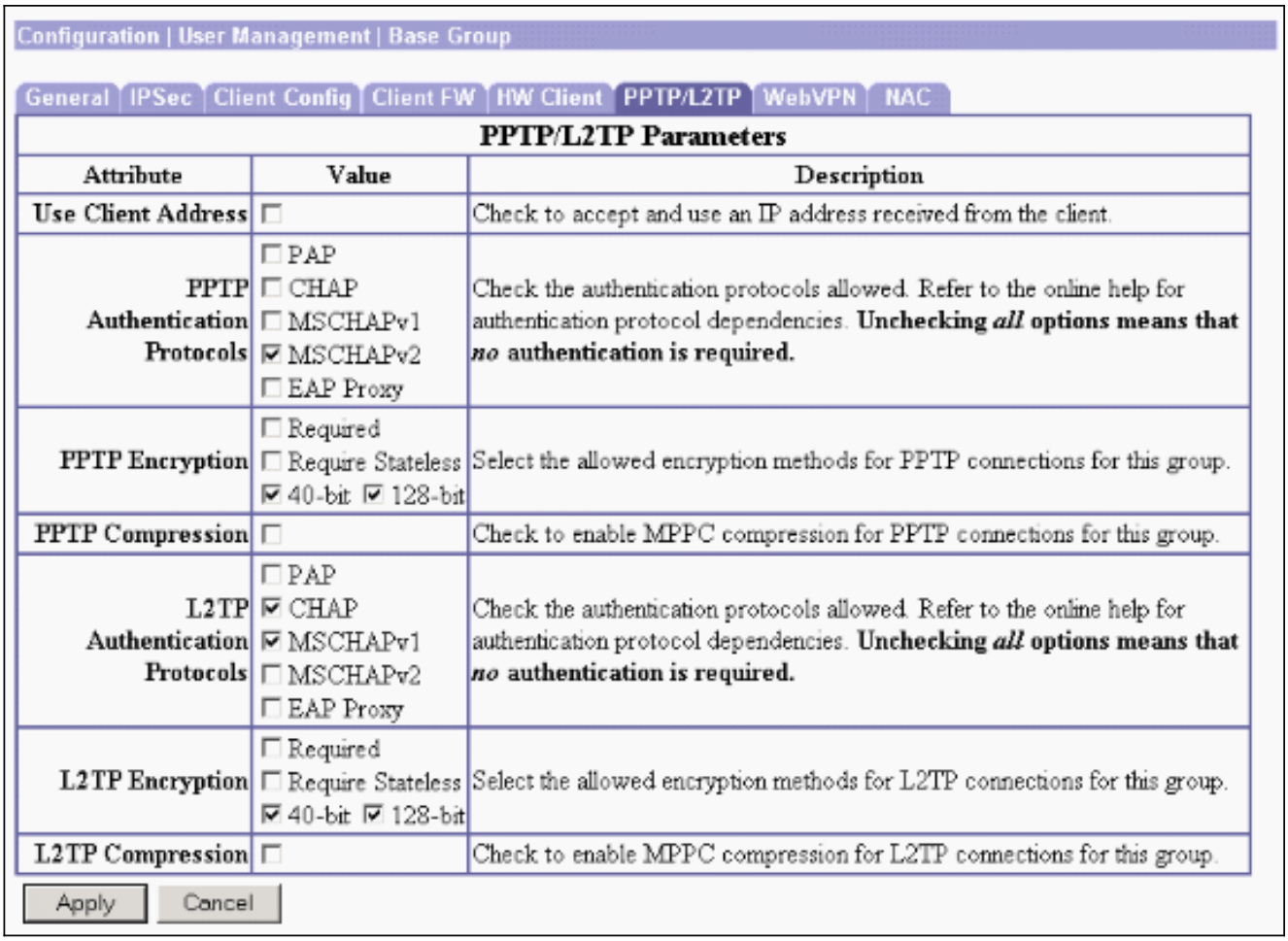
2. Fare clic su **Add** (Aggiungi) e configurare queste impostazioni.Tipo server = RADIUSServer di autenticazione = Indirizzo IP o nome host del server RADIUS (IAS)Porta server = 0 (0=predefinito=1645)Segreto server = come al passaggio 8 della sezione [Configurazione del server RADIUS]



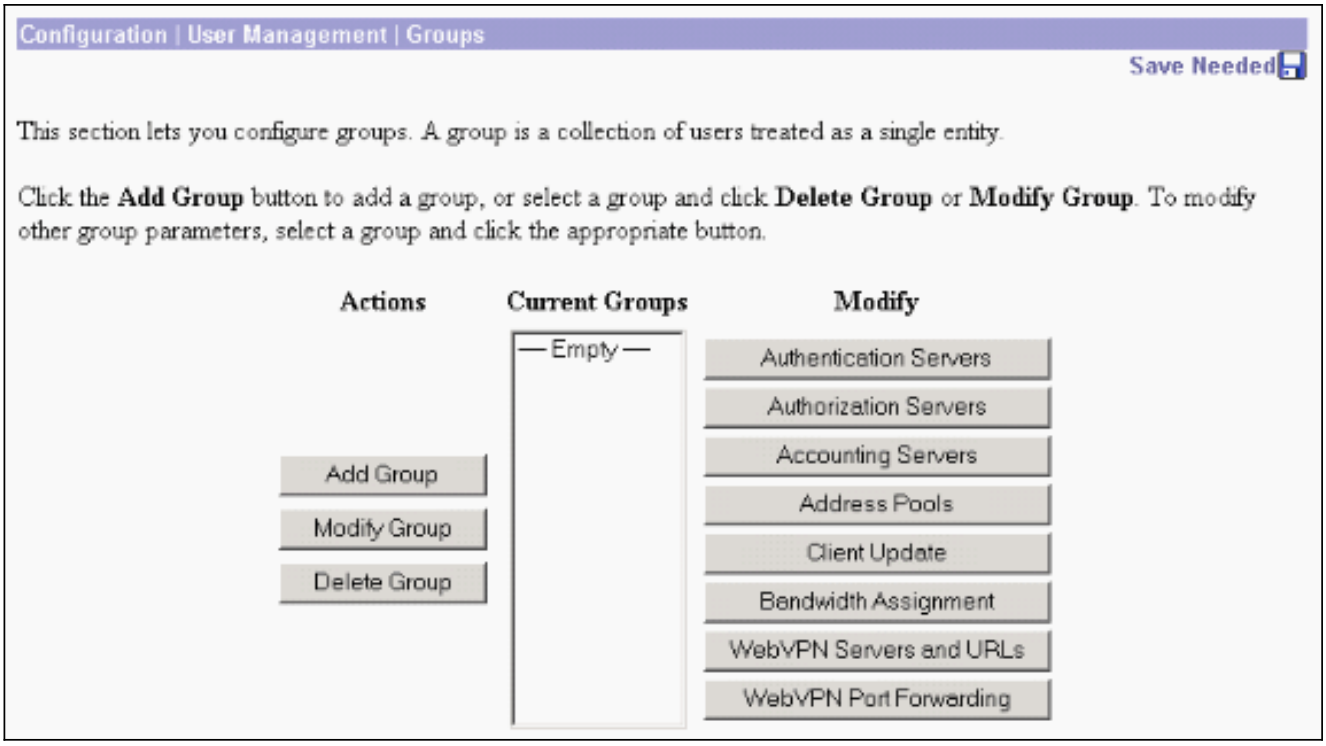
3. Per aggiungere le modifiche alla configurazione corrente, fare clic su **Add** (Aggiungi).
4. Fare clic su **Aggiungi**, scegliere **Server interno** per Tipo server e fare clic su **Applica**.Questa operazione è necessaria in seguito per configurare un gruppo IPSec (è necessario solo il tipo di server = Server interno).



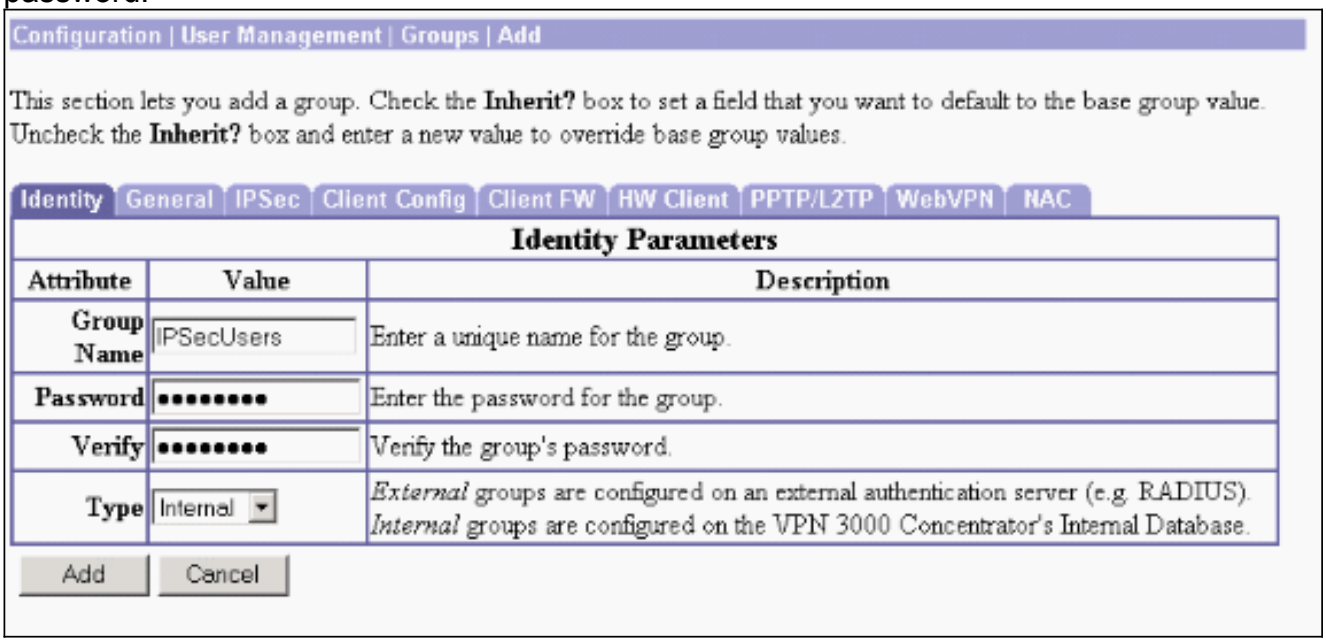
5. Configurare VPN Concentrator per utenti PPTP o per utenti VPN Client.**PPTP**Completare questa procedura per configurare per gli utenti PPTP.Scegliere **Configurazione > Gestione utente > Gruppo base**, quindi fare clic sulla scheda **PPTP/L2TP**.Scegliere **MSCHAPv2** e deselezionare altri protocolli di autenticazione nella sezione Protocolli di autenticazione PPTP.



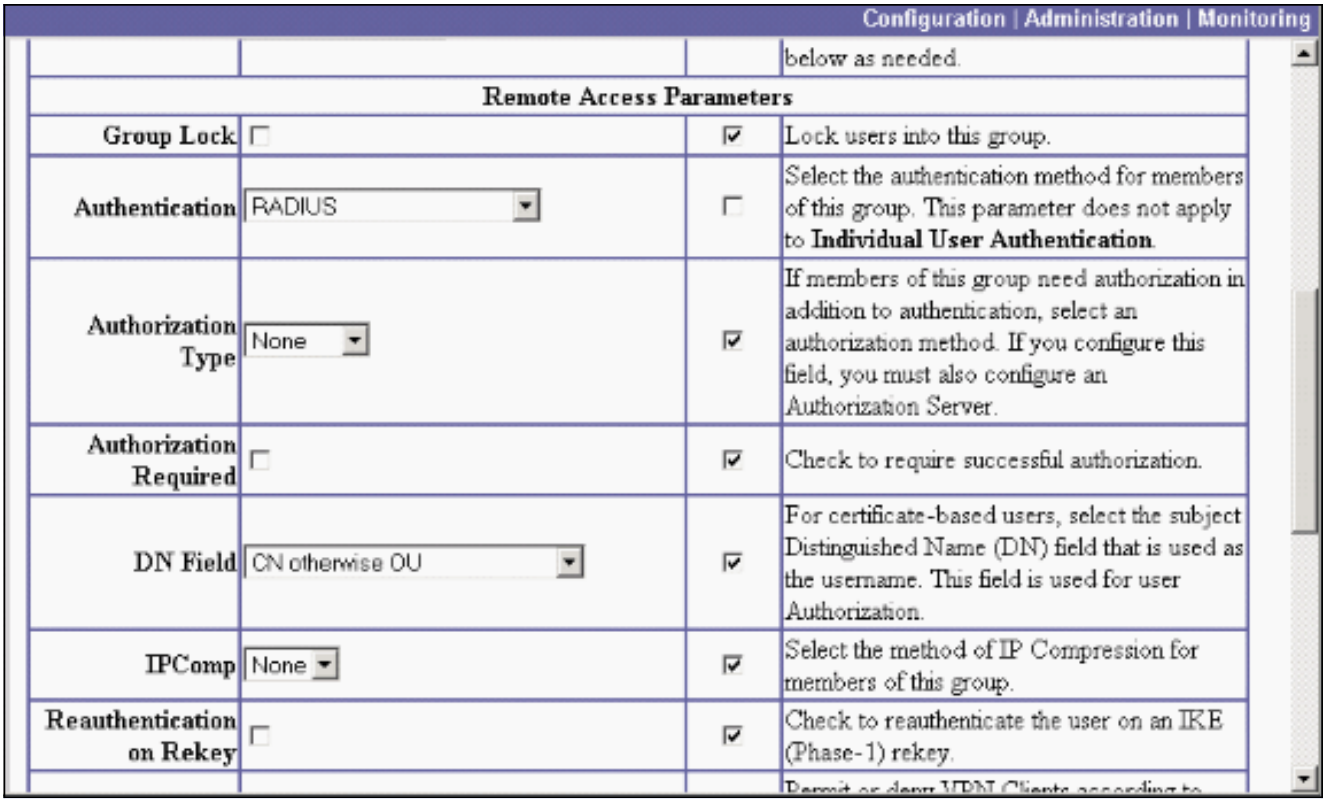
Fare clic su **Apply** (Applica) nella parte inferiore della pagina per aggiungere le modifiche alla configurazione in esecuzione.Ora, quando gli utenti PPTP si connettono, vengono autenticati dal server RADIUS (IAS).**Client VPN**Completare questa procedura per configurare per gli utenti client VPN.Per aggiungere un nuovo gruppo, scegliere **Configurazione > Gestione utente > Gruppi** e fare clic su
Aggiungi.



Digitare un nome di gruppo, ad esempio UtentiIPSec, e una password.



Questa password viene utilizzata come chiave già condivisa per la negoziazione del tunnel.Passare alla scheda IPSec e impostare Authentication (Autenticazione) su **RADIUS**.



In questo modo i client IPsec potranno essere autenticati tramite il server di autenticazione RADIUS.Per aggiungere le modifiche alla configurazione corrente, fare clic su **Add** (Aggiungi) nella parte inferiore della pagina.Quando i client IPSec si connettono e utilizzano il gruppo configurato, vengono autenticati dal server RADIUS.

Verifica

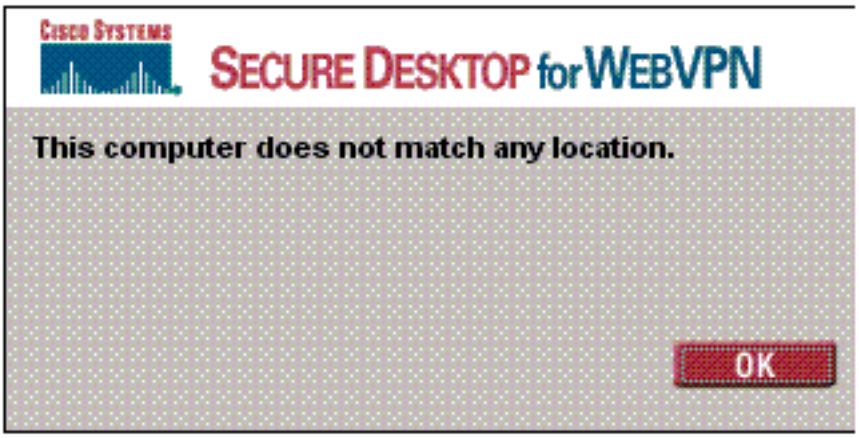
Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Autenticazione WebVPN non riuscita

Le informazioni contenute in queste sezioni permettono di risolvere i problemi relativi alla configurazione.

- **Problema:** Gli utenti WebVPN non sono in grado di eseguire l'autenticazione sul server RADIUS, ma possono eseguire l'autenticazione con il database locale del concentratore VPN. Vengono visualizzati errori quali "Accesso non riuscito" e questo



messaggio. **Causa**: Questo tipo di problemi spesso si verifica quando viene utilizzato un database diverso da quello interno del concentratore. Gli utenti WebVPN accedono al gruppo base quando si connettono per la prima volta al concentratore e devono utilizzare il metodo di autenticazione predefinito. Spesso questo metodo viene impostato sul database interno del concentratore e non è un server RADIUS o di altro tipo configurato.**Soluzione**: Quando un utente WebVPN esegue l'autenticazione, Concentrator controlla l'elenco dei server definiti in **Configurazione > Sistema > Server > Autenticazione** e utilizza quello superiore. Assicurarsi di spostare all'inizio dell'elenco il server con cui si desidera autenticare gli utenti WebVPN. Ad esempio, se il metodo di autenticazione deve essere RADIUS, è necessario spostare il server RADIUS all'inizio dell'elenco per eseguire il push dell'autenticazione.**Nota:** solo perché gli utenti WebVPN inizialmente hanno raggiunto il gruppo base non significa che sono limitati al gruppo base. È possibile configurare ulteriori gruppi WebVPN nel concentratore e assegnare gli utenti a tali gruppi dal server RADIUS con la popolazione dell'attributo 25 con **OU=*nomegruppo***. Per ulteriori informazioni, fare riferimento a Blocco di utenti in un gruppo di concentratori VPN 3000 tramite server RADIUS.

Autenticazione utente non riuscita con Active Directory

Nel server Active Directory, nella scheda Account della finestra di dialogo Proprietà utente dell'utente che ha generato l'errore, è possibile visualizzare questa casella di controllo:

[x] Non richiede preautenticazione

Se questa casella di controllo non è selezionata, **selezionarla** e provare a eseguire di nuovo l'autenticazione con questo utente.

Informazioni correlate

- Cisco VPN serie 3000 concentrator
- Client hardware Cisco VPN 3002
- Negoziazione IPSec/protocolli IKE
- Pagina di supporto per RADIUS (Remote Authentication Dial-In User Service)
- RADIUS (Remote Authentication Dial-In User Service)
- Documentazione e supporto tecnico – Cisco Systems