Esempio di configurazione di Cisco Secure Services Client con PEAP/GTC WPA

Sommario

Introduzione

In questo documento viene descritto come configurare PEAP (Protected Extensible Authentication Protocol)/GTC (Generic Token Card) con accesso protetto Wi-Fi (WPA) sul client Cisco Secure Services.

Prerequisiti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Services Client versione 4.0Cisco Secure Services Client è disponibile per il download sul sito Cisco.com Software Center (solo utenti registrati).
- Windows XP SP2 o 2000 SP4 minimo

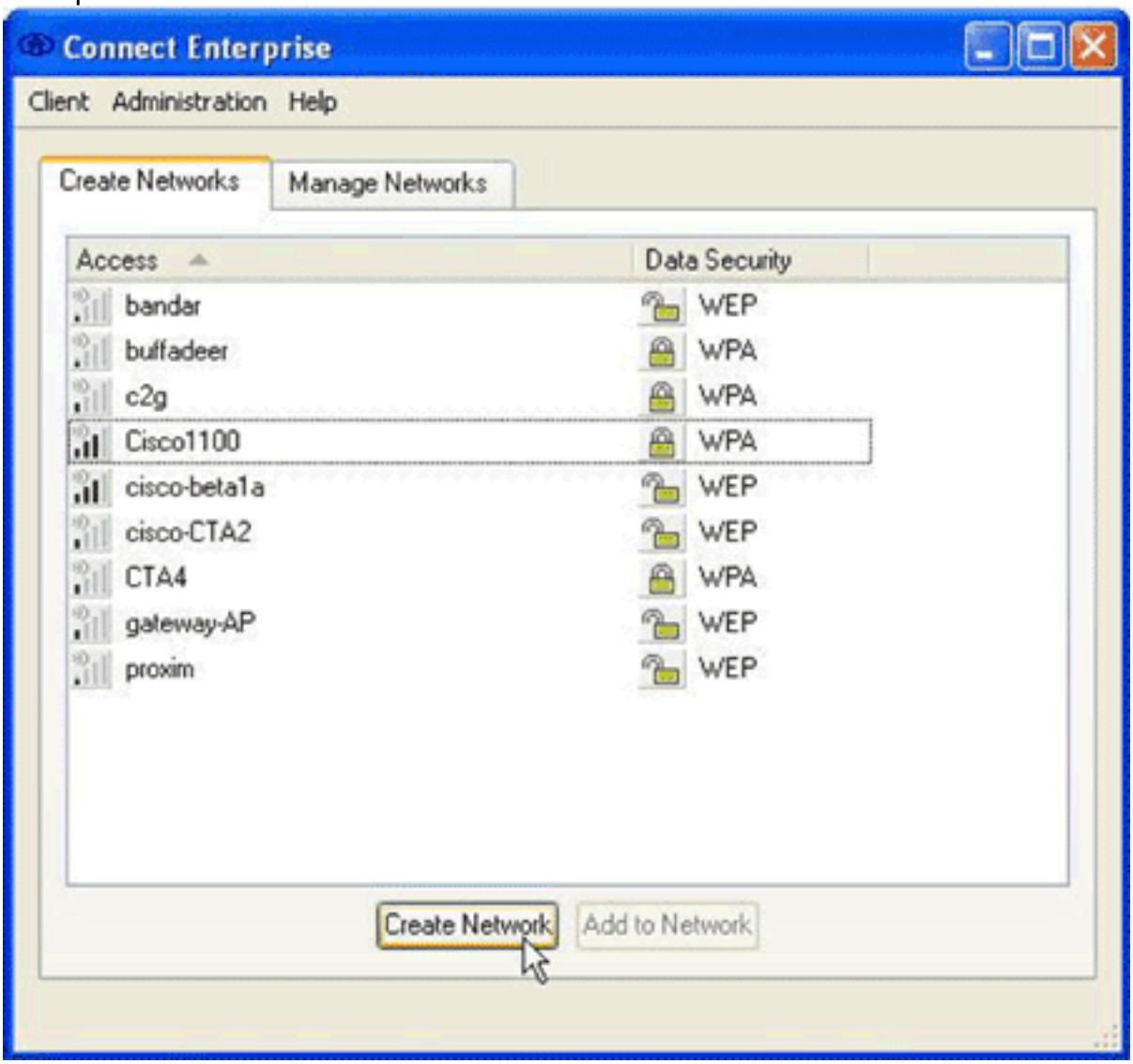
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

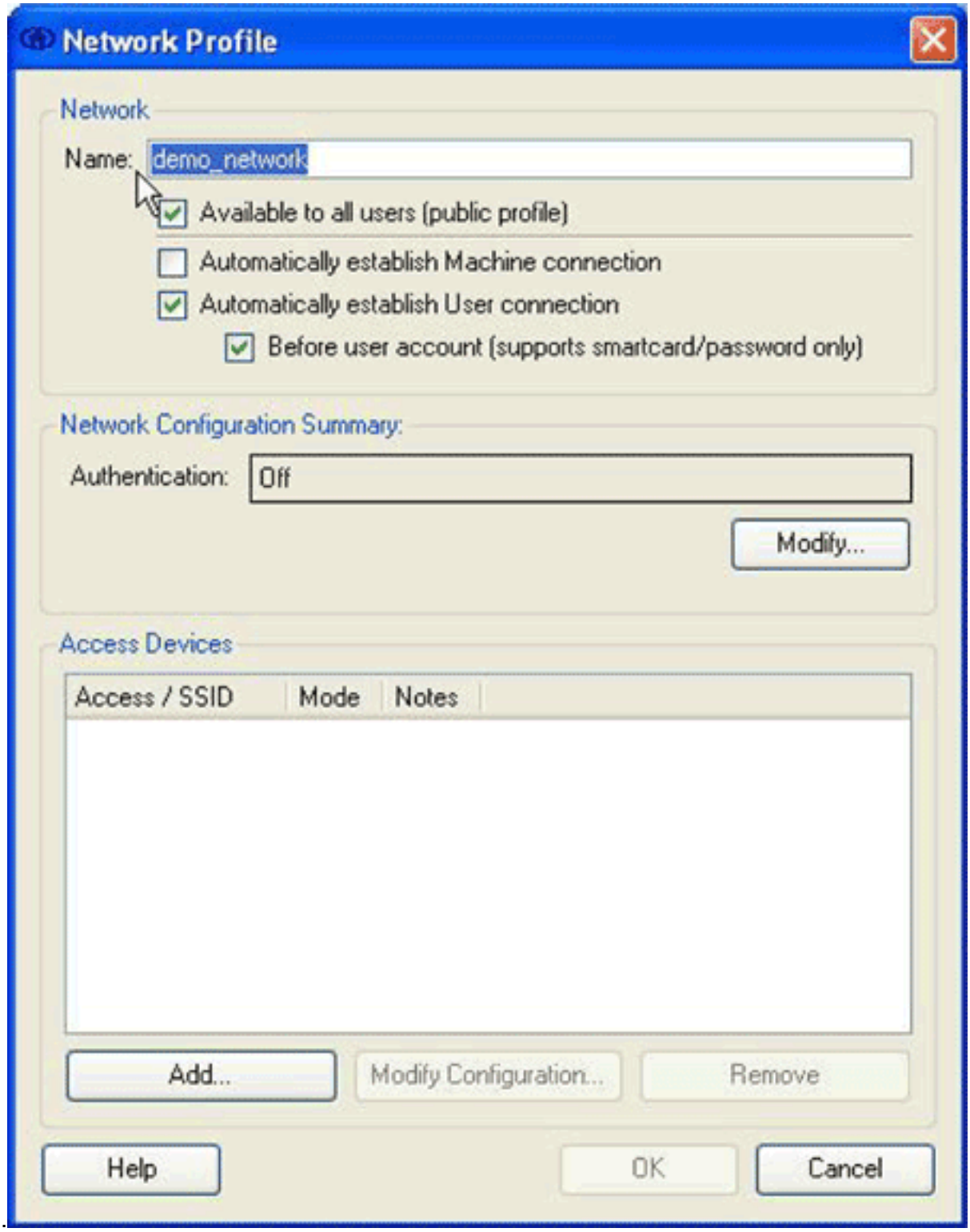
Configurazione di Cisco Secure Services Client con PEAP/GTC WPA

Per configurare Cisco Secure Services Client con PEAP/GTC WPA, attenersi alla seguente procedura:

1. Fare clic con il pulsante destro del mouse sull'icona Cisco Secure Services Client nella barra delle applicazioni, quindi selezionare **Open** (Apri).**Nota:** se non si è connessi a una rete, l'icona sulla barra delle applicazioni è ombreggiata.Verrà visualizzata la finestra di dialogo Connetti
   Enterprise.



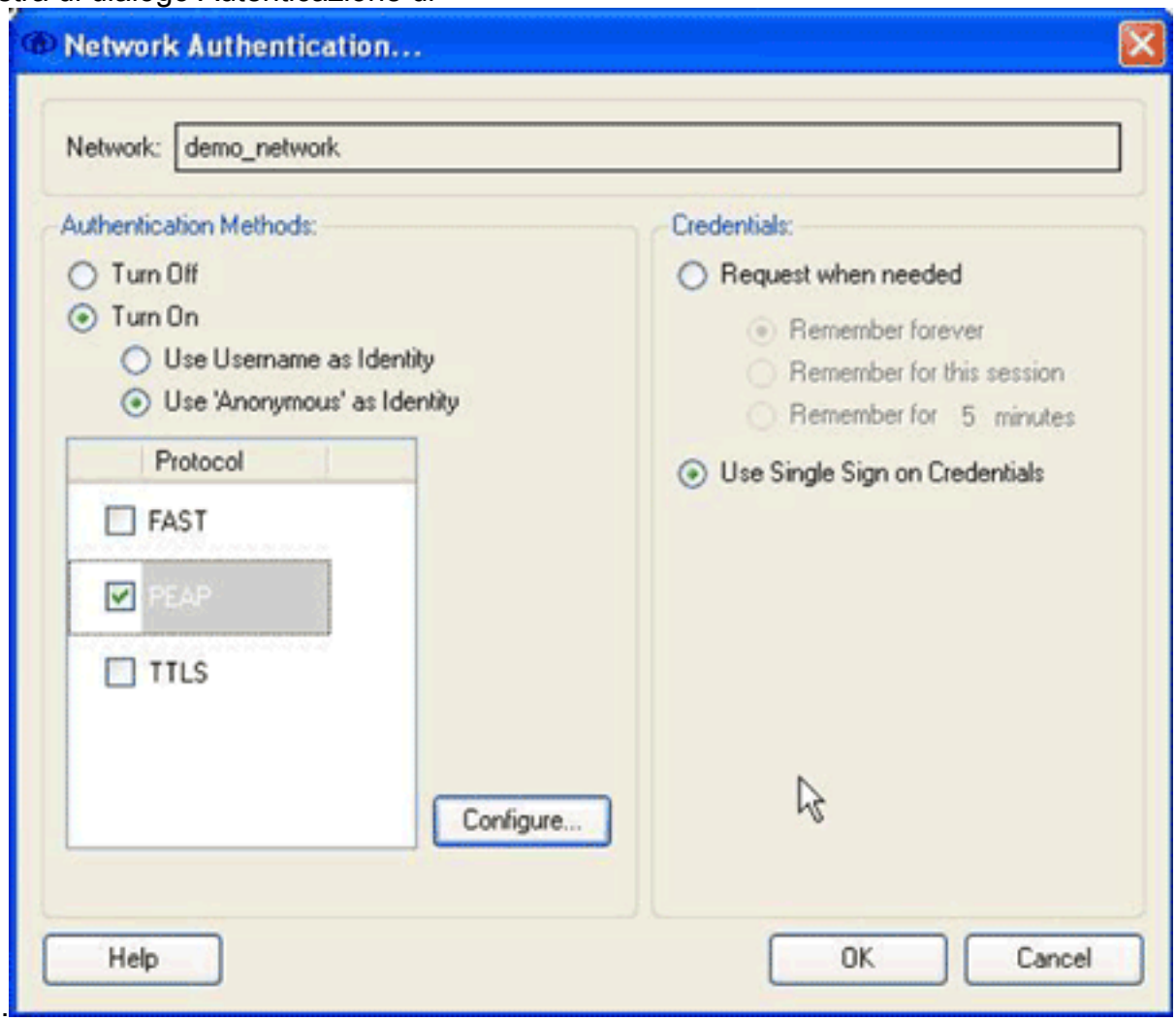
2. Fare clic sulla scheda **Crea reti**.Nell'area Crea reti vengono visualizzate le reti che trasmettono il relativo SSID (Service Set Identifier).
3. Fare clic sul pulsante **Crea rete**.Verrà visualizzata la finestra di dialogo Profilo di



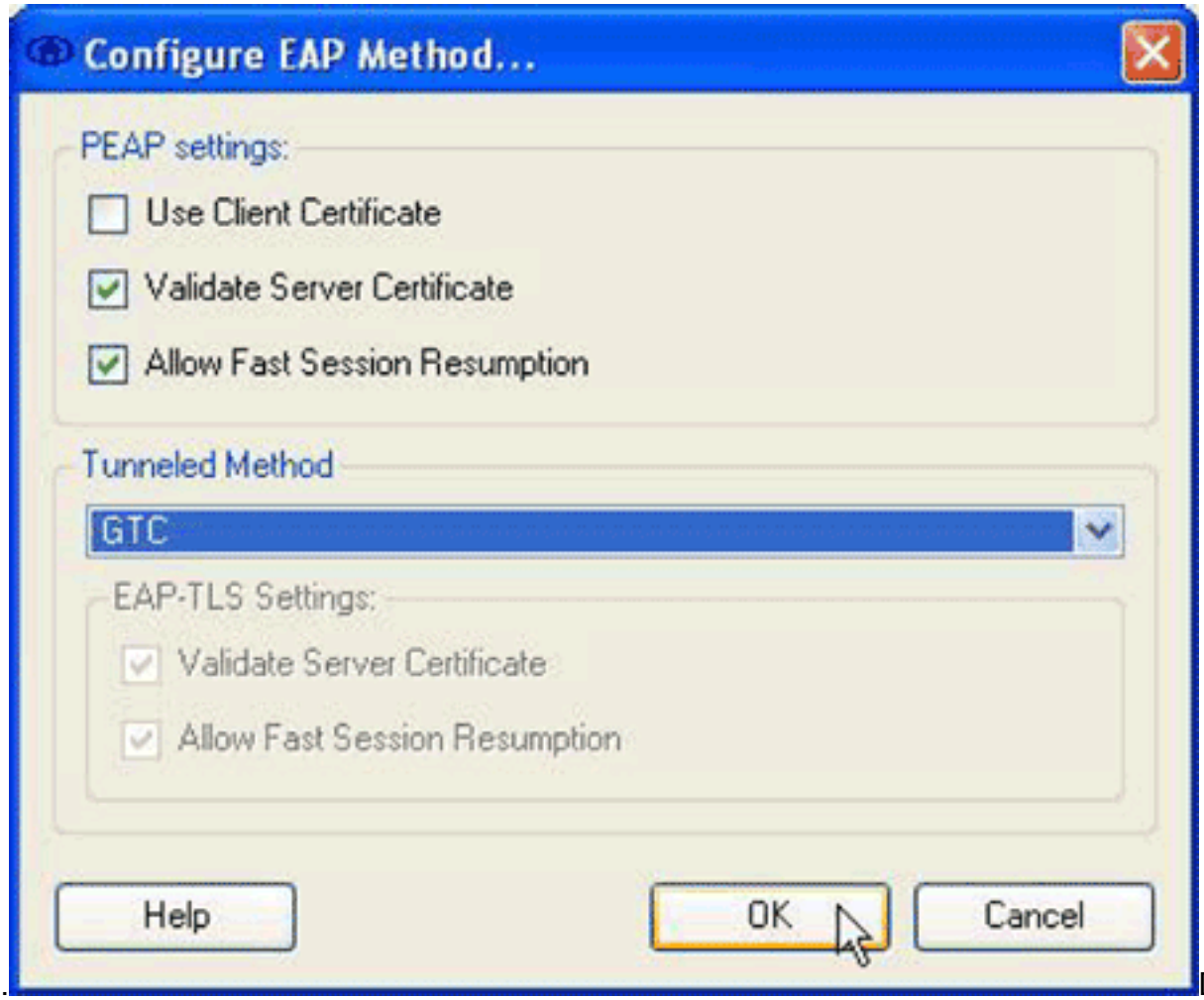
rete.

4. Nell'area Rete configurare le opzioni seguenti:Nel campo Nome, immettere un nome per la rete.Questo nome viene visualizzato come SSID per la rete. Per questo esempio, il nome è *demo_network*.Selezionare la casella di controllo **Disponibile per tutti gli utenti (profilo pubblico)**.Selezionare la casella di controllo **Stabilisci automaticamente connessione utente** e verificare che la casella di controllo Stabilisci automaticamente connessione computer non sia selezionata.Selezionare la casella di controllo **Prima dell'account utente (supporta solo smart card/password)**.**Nota:** se la casella di controllo **Prima dell'account utente (supporta solo smart card/password)** è selezionata, l'autenticazione procede immediatamente dopo l'immissione delle credenziali, ma prima dell'accesso al dominio. Se si utilizzano certificati utente, non selezionare la casella di controllo **Prima dell'account utente (supporta solo smart card/password)**. Poiché non sono disponibili prima dell'accesso a Windows, non è possibile utilizzare certificati utente con accessi al dominio.

5. Nell'area Riepilogo configurazione di rete, fare clic sul pulsante **Modifica**.Verrà visualizzata la finestra di dialogo Autenticazione di rete.

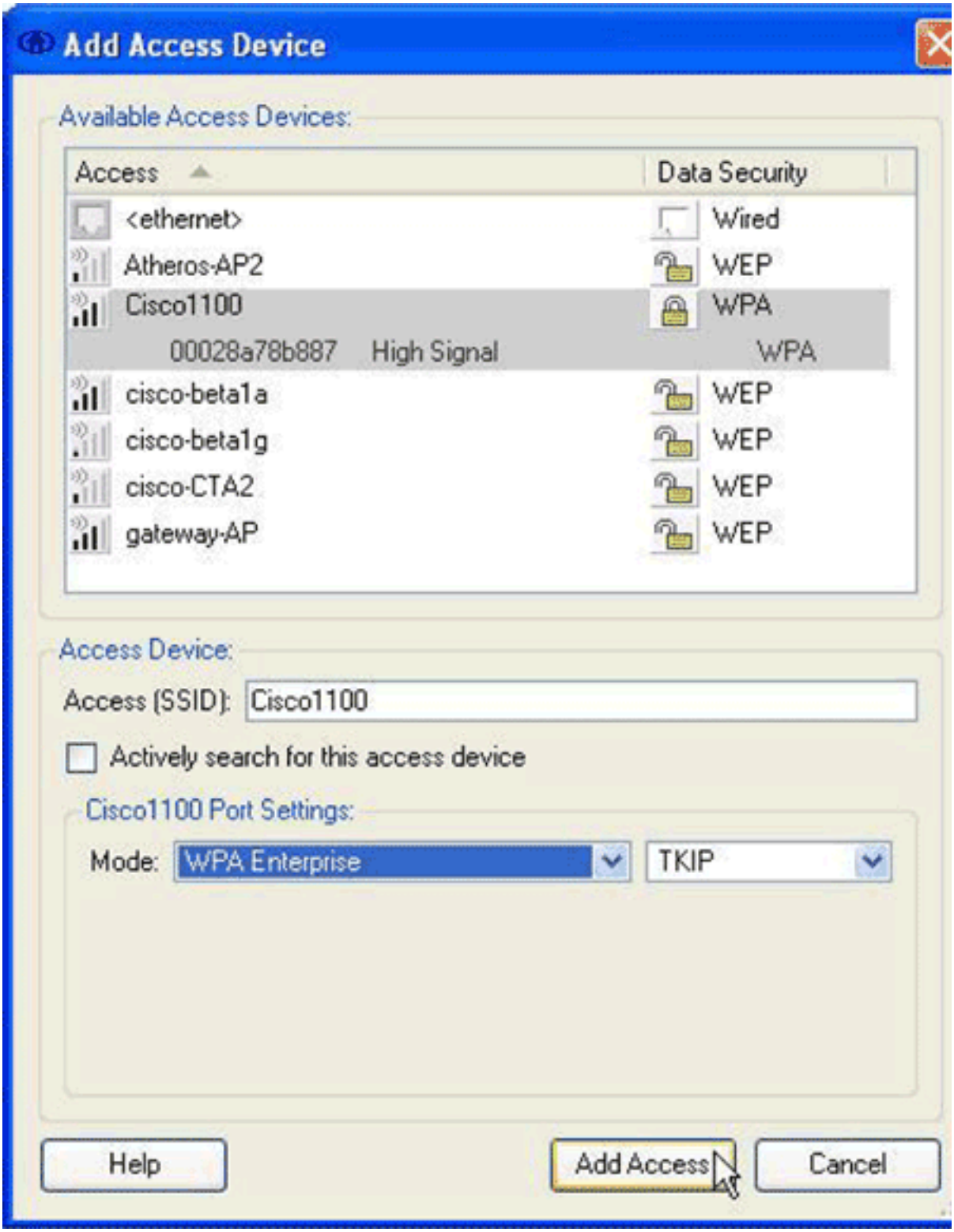


6. Nella finestra di dialogo Autenticazione di rete configurare le opzioni seguenti:Nell'area Credenziali fare clic sul pulsante di opzione **Usa credenziali Single Sign-on**.Nell'area Metodi di autenticazione fare clic sul pulsante di opzione **Attiva**, quindi scegliere **Usa 'Anonimo' come identità**.Il pulsante di opzione Attiva consente di popolare l'elenco dei protocolli visualizzato nell'area Metodi di autenticazione. Il pulsante di opzione Usa 'Anonimo' come identità consente di limitare l'elenco ai soli protocolli di autenticazione tramite tunneling.Selezionare la casella di controllo **PEAP** e quindi fare clic su **Configura**.Verrà visualizzata la finestra di dialogo Configura metodo



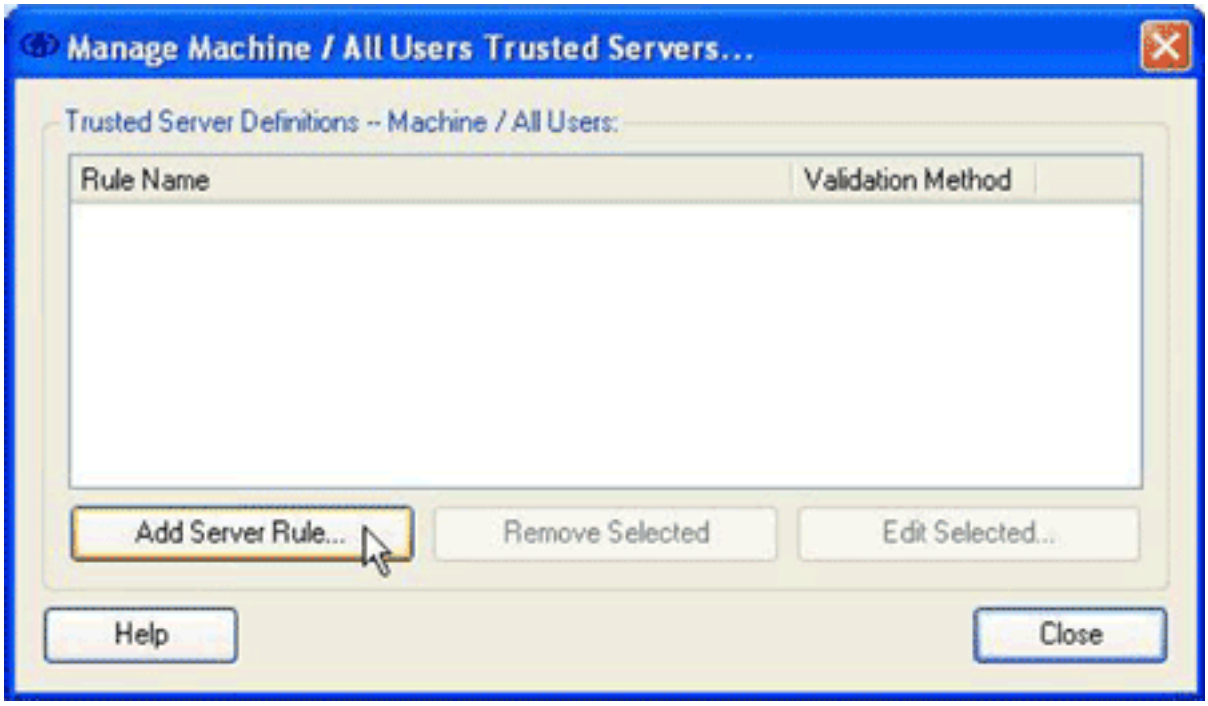
EAP.De selezionare la casella di controllo **Usa certificato client**.Selezionare le caselle di controllo **Convalida certificato server** e **Consenti riavvio rapido sessione**.Dal menu a discesa Metodo di tunneling, scegliere **GTC**.Fare clic su **OK** per tornare alla finestra di dialogo Autenticazione di rete e quindi su **OK** per tornare alla finestra di dialogo Profilo di rete.

7. Nell'area Dispositivi di accesso della finestra di dialogo Profilo di rete, fare clic su **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi periferica di accesso.

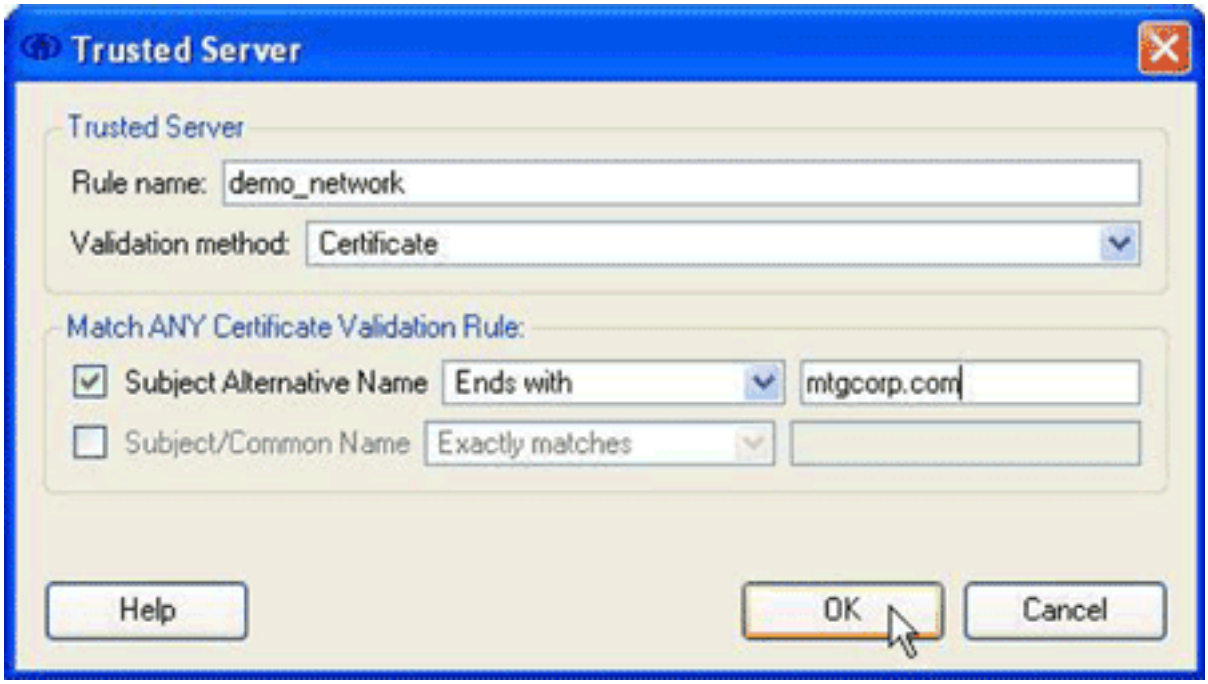


8. Nella finestra di dialogo Aggiungi dispositivi di accesso scegliere il dispositivo che si desidera configurare e quindi fare clic su **Aggiungi accesso**.**Nota:** se il dispositivo che si desidera configurare è nel campo, il SSID del dispositivo dovrebbe essere visualizzato nell'elenco Dispositivi di accesso disponibili. Se il dispositivo non viene visualizzato, immettere il SSID per il dispositivo nel campo Accesso (SSID), immettere le impostazioni della porta nell'area Impostazioni porta Cisco 1100 e quindi fare clic su **Aggiungi accesso**.
9. Nella finestra di dialogo Profilo di rete fare clic su **OK** per tornare alla finestra di dialogo Connetti Enterprise.
10. Nella finestra di dialogo Connetti Enterprise, scegliere **Server trusted > Gestisci computer / Tutti gli utenti server trusted** dal menu Client.Verrà visualizzata la finestra di dialogo Gestisci computer/Tutti gli utenti - Server

trusted.



11. Fare clic su **Aggiungi regola server**.Verrà visualizzata la finestra di dialogo Server trusted.



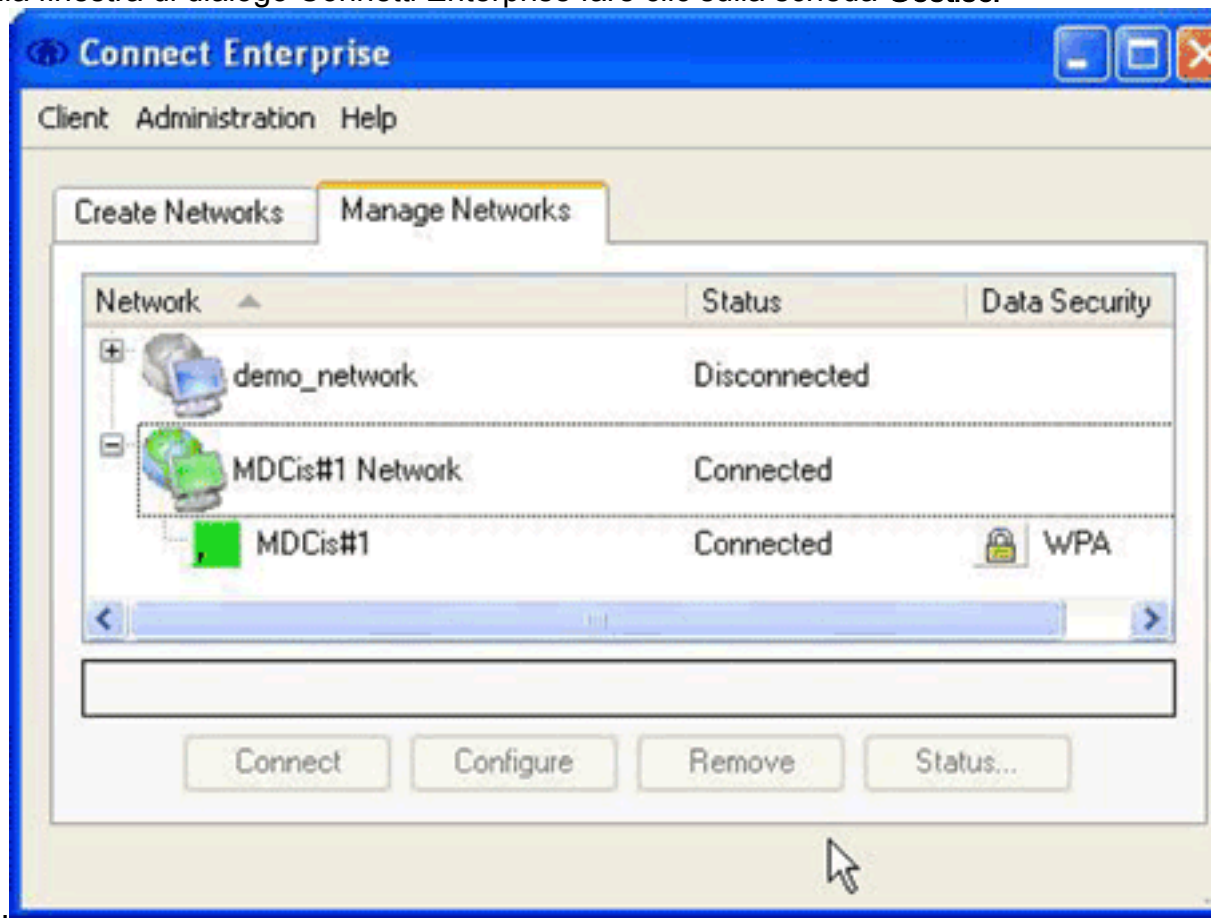
12. Nella finestra di dialogo Server trusted configurare le opzioni seguenti:Nel campo Nome regola immettere un nome per la regola.Dal menu a discesa Metodo di convalida, scegliere **Certificato**.Nell'area Corrispondenza qualsiasi regola di convalida dei certificati configurare le opzioni per la regola.Per creare una regola, è necessario conoscere il contenuto del certificato del server e immettere tali valori nell'area Corrispondenza qualsiasi regola di convalida del certificato. Ad esempio, se il nome alternativo del soggetto contiene il nome di dominio di un server, *mtgcorpserver.mtgcorp.com*, scegliere **Termina con** dal menu a discesa Nome alternativo del soggetto, quindi immettere **mtgcorp.com** nel campo di testo.Fare clic su **OK** per tornare alla finestra di dialogo Gestisci computer / Tutti gli utenti - Server trusted.
13. Nella finestra di dialogo Gestisci computer/Tutti gli utenti - Server trusted fare clic su **Chiudi** per tornare alla finestra di dialogo Connetti organizzazione.

La configurazione è completa ed è possibile connettersi alla rete.

Connetti alla rete

Per connettersi alla nuova rete, attenersi alla seguente procedura:

1. Nella finestra di dialogo Connetti Enterprise fare clic sulla scheda **Gestisci reti**.



2. Disconnettersi da qualsiasi rete connessa alla scheda utilizzata dalla nuova rete.
3. Dall'elenco Rete, selezionare il nuovo profilo di rete e fare clic su **Connetti**.

Se la configurazione e la connessione hanno esito positivo, l'icona di Cisco Secure Services Client sulla barra delle applicazioni viene visualizzata in verde.

Nota: se nel computer è installato un software antivirus configurato per l'analisi della directory di registro di Cisco Secure Services Client, è possibile che l'autenticazione di Cisco Secure Services Client richieda cicli elevati della CPU. Per migliorare le prestazioni, configurare il software antivirus in modo da escludere la directory di registro del client di Cisco Secure Services.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems