Konfigurationsbeispiel für Cisco Secure Services Client mit PEAP/GTC WPA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie Protected Extensible Authentication Protocol (PEAP)/Generic Token Card (GTC) Wi-Fi Protected Access (WPA) auf dem Cisco Secure Services Client konfigurieren.

Voraussetzungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure Services Client Version 4.0Der Cisco Secure Services Client kann vom Cisco.com Software Center heruntergeladen werden (nur registrierte Kunden).
- Windows XP SP2 oder 2000 SP 4 (mindestens)

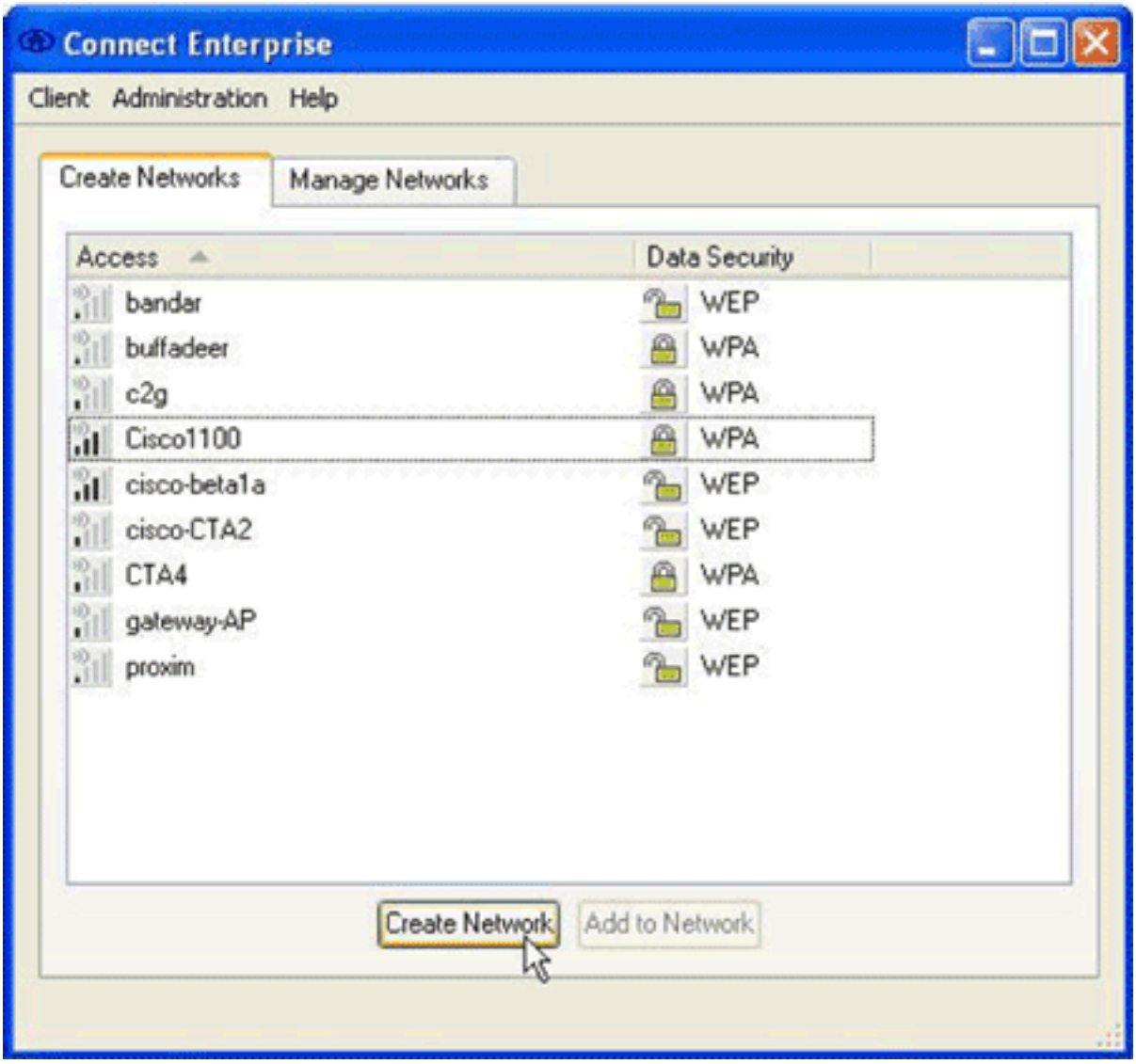
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

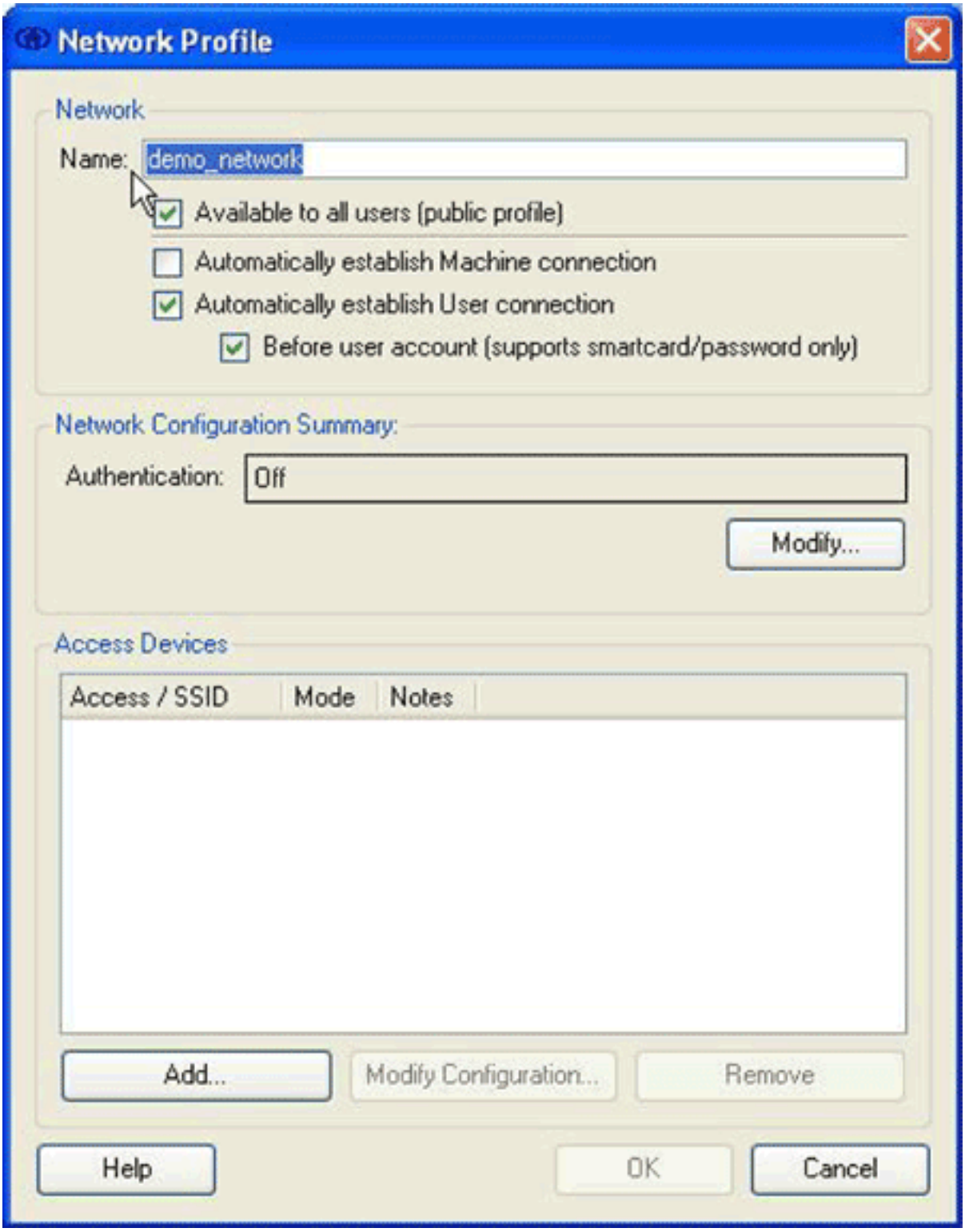
Konfigurieren des Cisco Secure Services Client mit PEAP/GTC WPA

Gehen Sie wie folgt vor, um den Cisco Secure Services Client mit PEAP/GTC WPA zu konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol für den Cisco Secure Services Client, und wählen Sie **Öffnen** aus.**Hinweis:** Wenn Sie nicht mit einem Netzwerk verbunden sind, ist das Taskleistensymbol dunkel.Das Dialogfeld "Enterprise verbinden" erscheint.



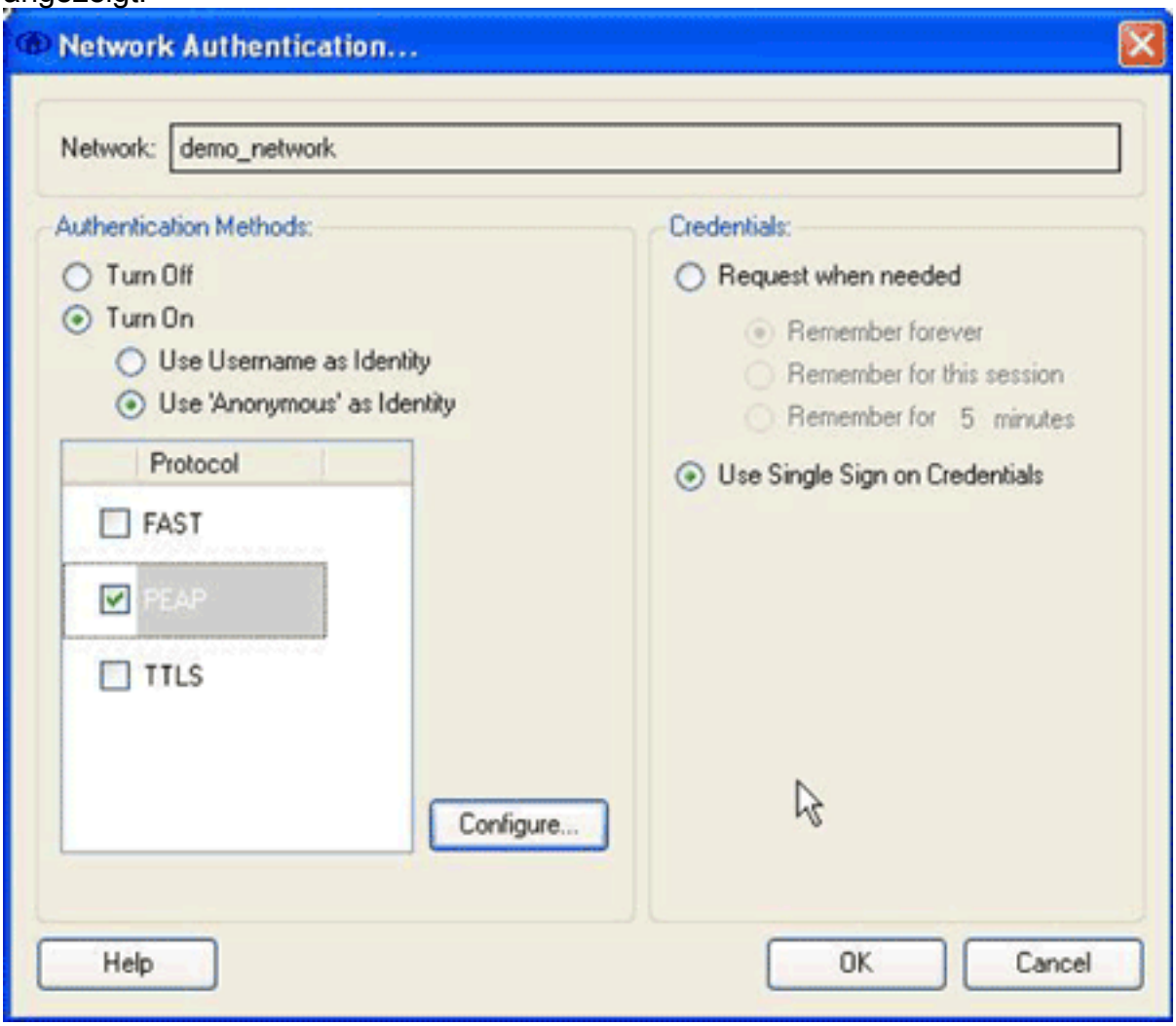
2. Klicken Sie auf die Registerkarte **Create Networks (Netzwerke erstellen)**.Im Bereich "Netzwerke erstellen" werden die Netzwerke angezeigt, die ihre Service Set Identifier (SSID) übertragen.
3. Klicken Sie auf die Schaltfläche **Create Network (Netzwerk erstellen)**.Das Dialogfeld Netzwerkprofil wird
angezeigt.



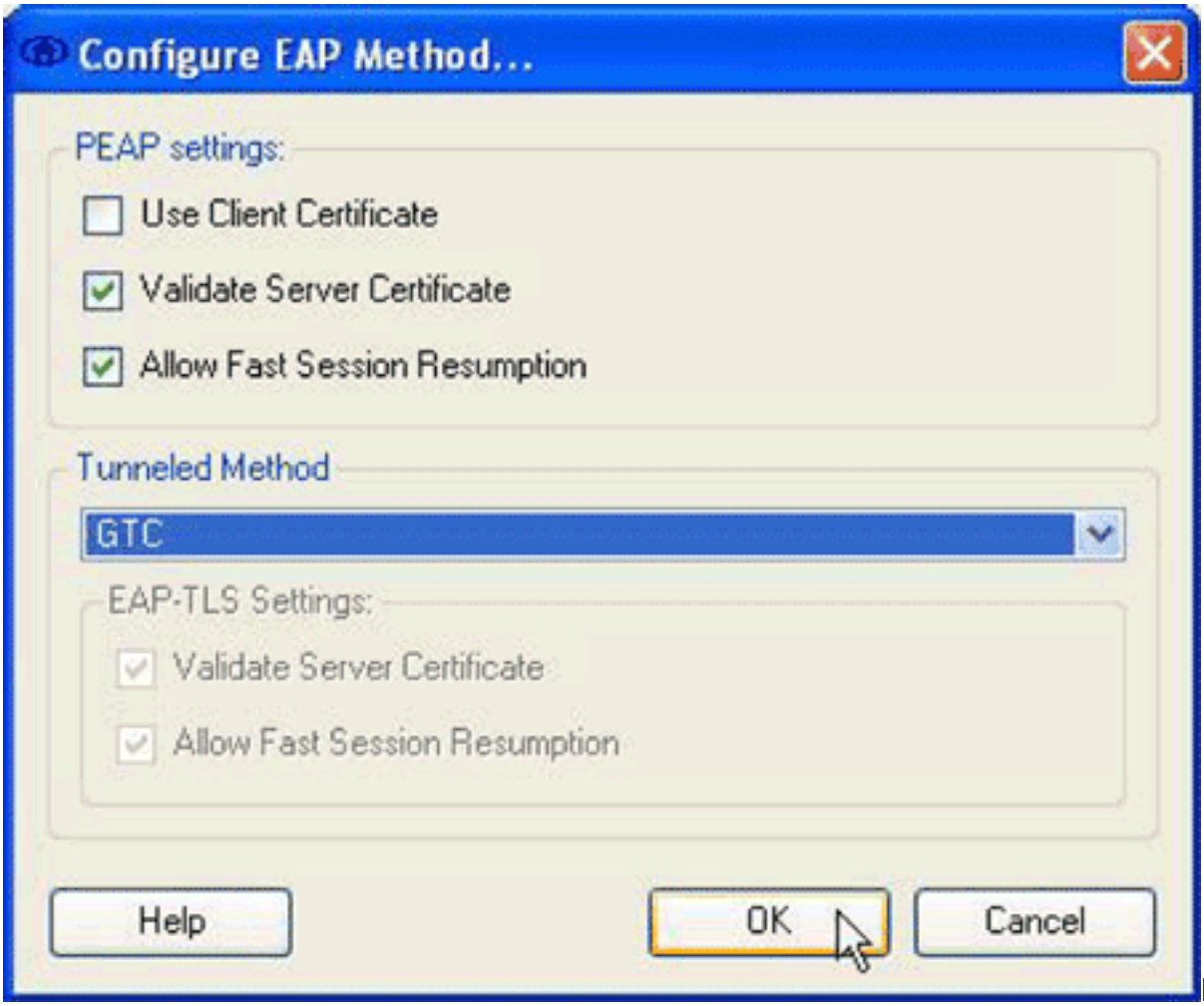
4. Konfigurieren Sie im Netzwerkbereich folgende Optionen:Geben Sie im Feld Name einen Namen für Ihr Netzwerk ein.Dieser Name wird als SSID für dieses Netzwerk angezeigt. In diesem Beispiel lautet der Name *demo_network*.Aktivieren Sie das Kontrollkästchen **Verfügbar für alle Benutzer (öffentliches Profil)**.Aktivieren Sie das Kontrollkästchen **Benutzerverbindung automatisch herstellen**, und überprüfen Sie, ob das Kontrollkästchen Automatisch Verbindung herstellen nicht aktiviert ist.Aktivieren Sie das Kontrollkästchen **Before user account (nur Smartcard/Kennwort unterstützt)**.**Hinweis:** Wenn das Kontrollkästchen **Before user account (unterstützt nur Smartcard/Kennwort)** aktiviert ist, wird die Authentifizierung unmittelbar nach Eingabe der Anmeldeinformationen, jedoch vor der Domänenanmeldung fortgesetzt. Wenn Sie Benutzerzertifikate verwenden, aktivieren Sie nicht das Kontrollkästchen **Before user account (unterstützt nur Smartcard/Kennwort)**. Da sie vor der Windows-Anmeldung nicht verfügbar sind, können Sie Benutzerzertifikate nicht mit

Domänenanmeldungen verwenden.

5. Klicken Sie im Bereich "Network Configuration Summary" (Netzwerkkonfigurationsübersicht) auf die Schaltfläche **Modify** (Ändern).Das Dialogfeld Netzwerkauthentifizierung wird angezeigt.

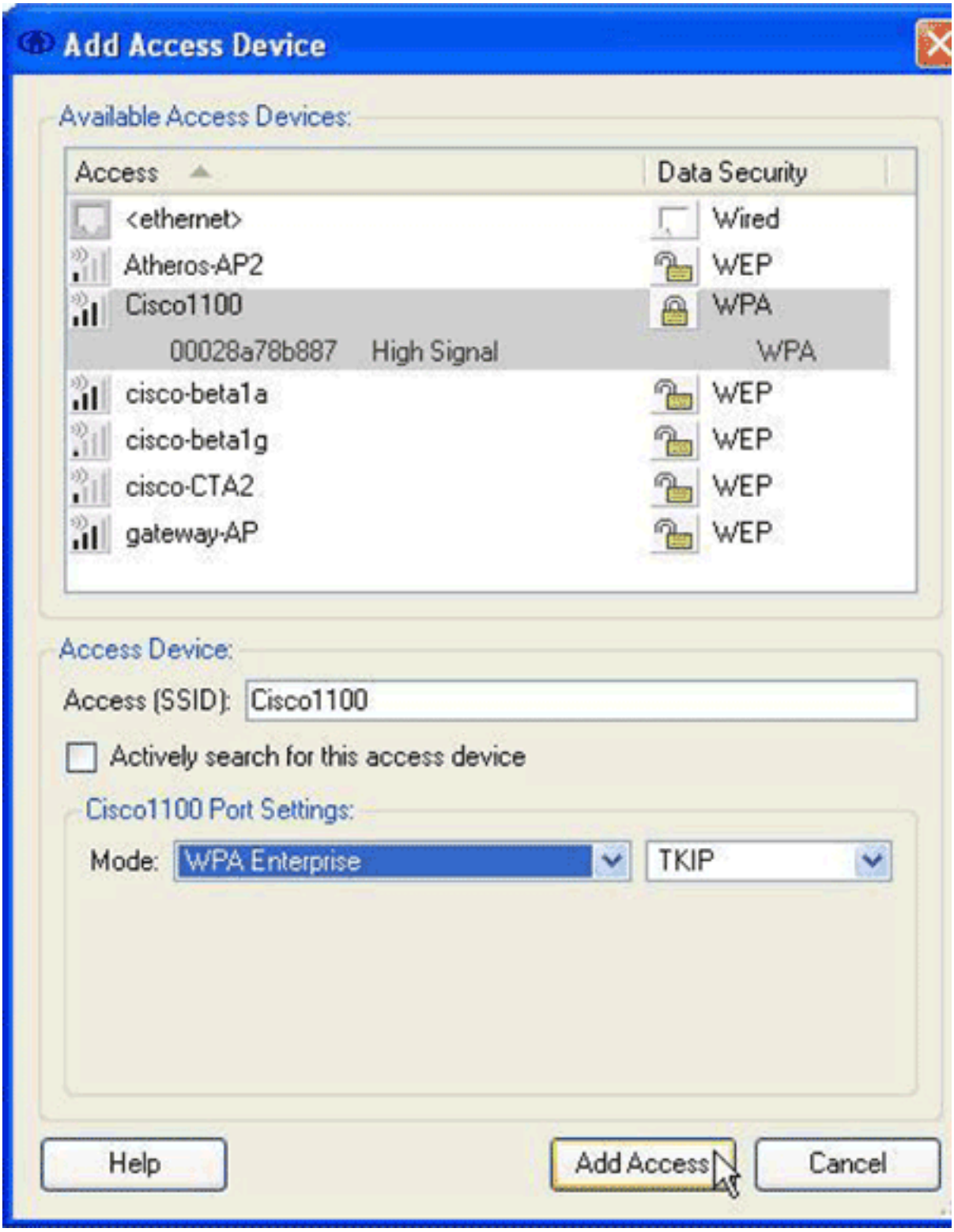


6. Konfigurieren Sie im Dialogfeld Netzwerkauthentifizierung die folgenden Optionen:Klicken Sie im Bereich Anmeldeinformationen auf das Optionsfeld **Single Sign on Credentials (Single-Anmeldung für Anmeldeinformationen verwenden)**.Klicken Sie im Bereich Authentifizierungsmethoden auf das Optionsfeld **Aktivieren** und anschließend auf **Anonyme Identität verwenden**.Das Optionsfeld Aktivieren füllt die Protokollliste aus, die im Bereich Authentifizierungsmethoden angezeigt wird. Das Optionsfeld 'Anonym' als Identität verwenden beschränkt die Liste auf getunnelte Authentifizierungsprotokolle.Aktivieren Sie das Kontrollkästchen **PEAP**, und klicken Sie dann auf **Konfigurieren**.Das Dialogfeld "EAP-Methode konfigurieren" wird
angezeigt.



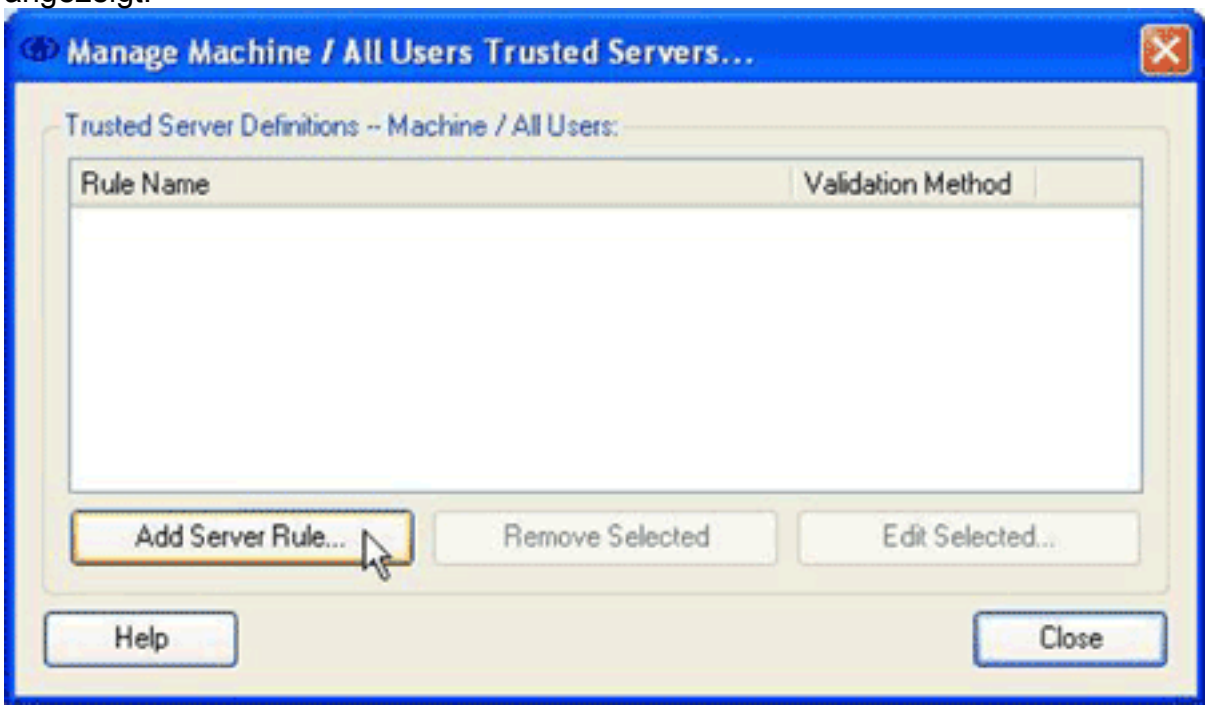
Deaktivieren Sie das Kontrollkästchen **Clientzertifikat verwenden**.Aktivieren Sie die Kontrollkästchen **Serverzertifikat validieren** und **schnelle Sitzungsumgebung zulassen**.Wählen Sie im Dropdown-Menü Tunneled Method (Getunnelte Methode) die Option **GTC aus**.Klicken Sie auf **OK**, um zum Dialogfeld Netzwerkauthentifizierung zurückzukehren, und klicken Sie dann auf **OK**, um zum Dialogfeld Netzwerkprofil zurückzukehren.

7. Klicken Sie im Dialogfeld Netzwerkprofil im Bereich Zugriffsgeräte auf **Hinzufügen**.Das Dialogfeld Zugriffsgerät hinzufügen wird angezeigt.

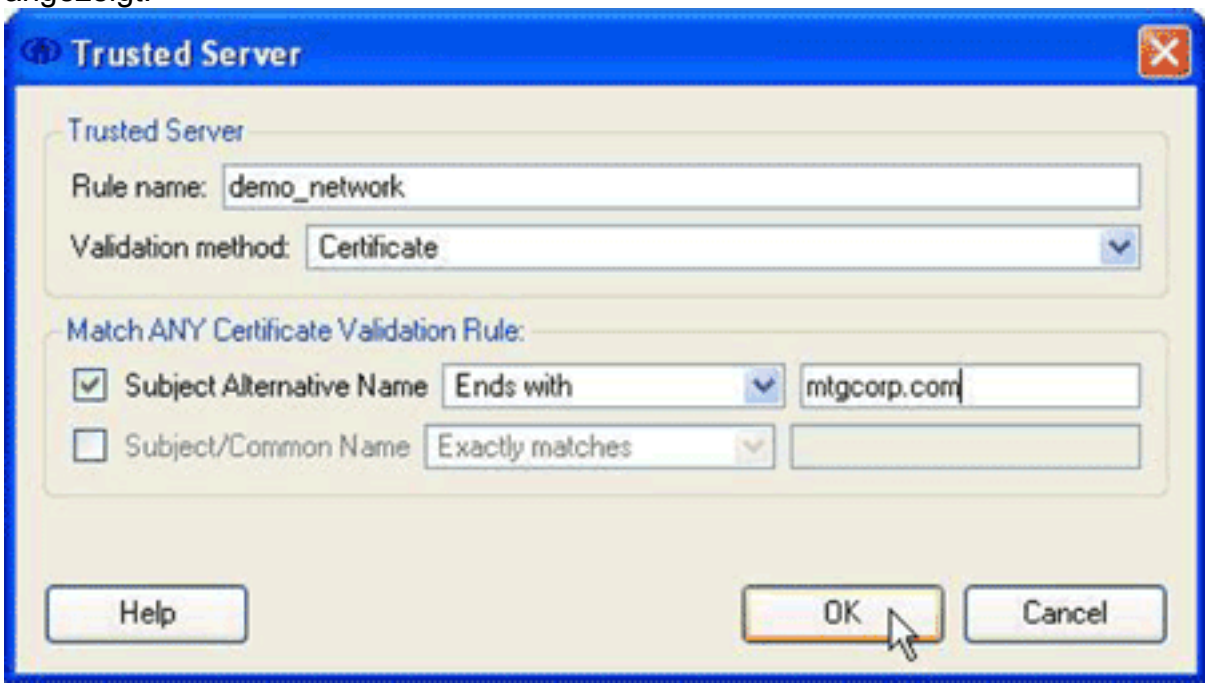


8. Wählen Sie im Dialogfeld Zugriffsgeräte hinzufügen das Gerät aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Zugriff hinzufügen**.**Hinweis:** Wenn sich das zu konfigurierende Gerät im Bereich befindet, sollte die SSID für dieses Gerät in der Liste Verfügbare Zugriffsgeräte angezeigt werden. Wenn das Gerät nicht angezeigt wird, geben Sie die SSID für das Gerät im Feld Access (SSID) ein, geben Sie die Porteinstellungen im Bereich Cisco 1100 Port Settings (Porteinstellungen für Cisco 100) ein, und klicken Sie dann auf **Add Access (Zugriff hinzufügen)**.
9. Klicken Sie im Dialogfeld Netzwerkprofil auf **OK**, um zum Dialogfeld Enterprise verbinden zurückzukehren.
10. Wählen Sie im Dialogfeld "Connect Enterprise" (Enterprise-Verbindung) **im** Menü Client die Option **Trusted Servers (Vertrauenswürdige Server) > Manage Machine (Computer**

verwalten) / All Users Trusted Servers (Alle Benutzer vertrauenswürdigen Server) aus.Das Dialogfeld System verwalten / Alle Benutzer Vertrauenswürdige Server wird angezeigt.



11. Klicken Sie auf **Serverregel hinzufügen**.Das Dialogfeld Vertrauenswürdiger Server wird angezeigt.



12. Konfigurieren Sie im Dialogfeld Vertrauenswürdiger Server die folgenden Optionen:Geben Sie im Feld Regelname einen Namen für die Regel ein.Wählen Sie im Dropdown-Menü Validierungsmethode die Option **Zertifikat aus**.Konfigurieren Sie im Bereich "Zuordnen einer Zertifikatsvalidierungsregel" Optionen für die Regel.Um eine Regel zu erstellen, müssen Sie den Inhalt des Serverzertifikats kennen und diese Werte im Bereich "Match ANY Certificate Validation Rule" (JEDE Zertifikatsvalidierungsregel zuordnen) eingeben. Wenn der alternative Betreff-Name z. B. den Domänennamen eines Servers *mtgcorpserver.mtgcorp.com* enthält, wählen Sie **Ends with (Mit** dem Betreff Alternativer Name) aus dem Dropdown-Menü aus, und geben Sie **mtgcorp.com** in das Textfeld ein.Klicken Sie auf **OK**, um zum Dialogfeld "Manage Machine/All Users Trusted Servers"

(System verwalten/Alle Benutzer vertrauenswürdige Server) zurückzukehren.

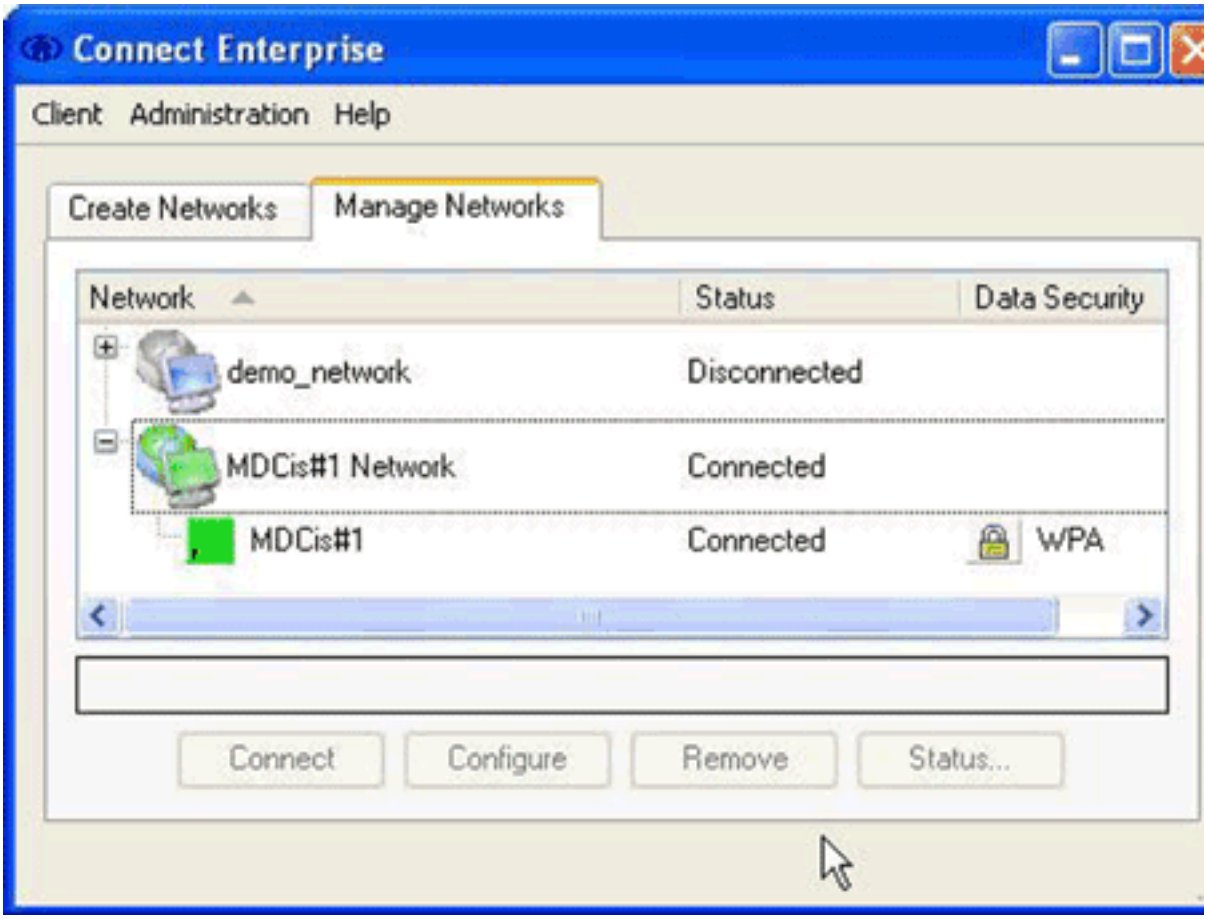
13. Klicken Sie im Dialogfeld System verwalten/Alle Benutzer Vertrauenswürdige Server auf **Schließen**, um zum Dialogfeld Enterprise verbinden zurückzukehren.

Die Konfiguration ist abgeschlossen, und Sie können eine Verbindung zum Netzwerk herstellen.

Verbindung zum Netzwerk herstellen

Gehen Sie wie folgt vor, um eine Verbindung zum neuen Netzwerk herzustellen:

1. Klicken Sie im Dialogfeld "Enterprise verbinden" auf die Registerkarte **Netzwerke verwalten**.



2. Trennen Sie die Verbindung zu einem Netzwerk, das mit dem Adapter verbunden ist, der vom neuen Netzwerk verwendet wird.
3. Wählen Sie aus der Liste Netzwerk das neue Netzwerkprofil aus, und klicken Sie auf **Verbinden**.

Nach erfolgreicher Konfiguration und Verbindung wird das Taskleistensymbol für den Cisco Secure Services Client grün angezeigt.

Hinweis: Wenn Virenschutzsoftware auf Ihrem Computer installiert ist und für die Analyse des Protokollverzeichnisses des Cisco Secure Services Client konfiguriert ist, kann es bei der Authentifizierung des Cisco Secure Services Client zu hohen CPU-Zyklen kommen. Um die Leistung zu verbessern, konfigurieren Sie Ihre Virenschutzsoftware so, dass das Protokollverzeichnis des Cisco Secure Services Client ausgeschlossen wird.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems