CSU-Konfiguration für UNIX (Solaris)

Inhalt

Einführung

Die Cisco Secure ACS für UNIX (CSU)-Software gewährleistet die Sicherheit des Netzwerks und verfolgt die Aktivitäten von Personen, die erfolgreich eine Verbindung zum Netzwerk herstellen. CSU fungiert als TACACS+- oder RADIUS-Server und verwendet zur Gewährleistung der Netzwerksicherheit Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA).

CSU unterstützt die folgenden Datenbankoptionen zum Speichern von Gruppen- und Benutzerprofilen sowie Abrechnungsinformationen:

- SQLAnywhere (im CSU enthalten).Diese Version von Sybase SQLAnywhere bietet keine Client-/Server-Unterstützung. Sie ist jedoch für die Ausführung wichtiger AAA-Services mit CSU optimiert.**Vorsicht:** Die SQLAnywhere-Datenbankoption unterstützt keine Profildatenbanken mit mehr als 5.000 Benutzern, die Replikation von Profilinformationen zwischen Datenbankstandorten oder die Funktion Cisco Secure Distribution Session Manager (DSM).
- Oracle oder Sybase Relational Database Management System (RDBMS).Um Cisco Secure Profile-Datenbanken mit 5.000 oder mehr Benutzern, Datenbankreplikation oder der Cisco Secure DSM-Funktion zu unterstützen, müssen Sie ein Oracle (Version 7.3.2, 7.3.3 oder

8.0.3)- oder Sybase SQL Server (Version 11)-RDBMS vorinstallieren, um Ihre Cisco Secure-Profildaten zu speichern. Für die Datenbankreplikation ist nach Abschluss der Cisco Secure-Installation eine weitere RDBMS-Konfiguration erforderlich.
- Aktualisierung einer vorhandenen Datenbank von einer früheren (2.x) Version von CSU.Wenn Sie ein Upgrade von einer früheren 2.x-Version von Cisco Secure durchführen, aktualisiert das Cisco Secure-Installationsprogramm die Profildatenbank automatisch auf Kompatibilität mit CSU 2.3 für UNIX.
- Importieren einer vorhandenen Profildatenbank.Sie können vorhandene Freeware-TACACS+- oder RADIUS-Profildatenbanken oder Flat-Dateien für die Verwendung mit dieser CSU-Version konvertieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure ACS 2.3 für UNIX.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

CSU-Konfiguration

Verwenden Sie diese Verfahren, um CSU zu konfigurieren.

Starten Sie die Cisco Secure Administrator Interface.

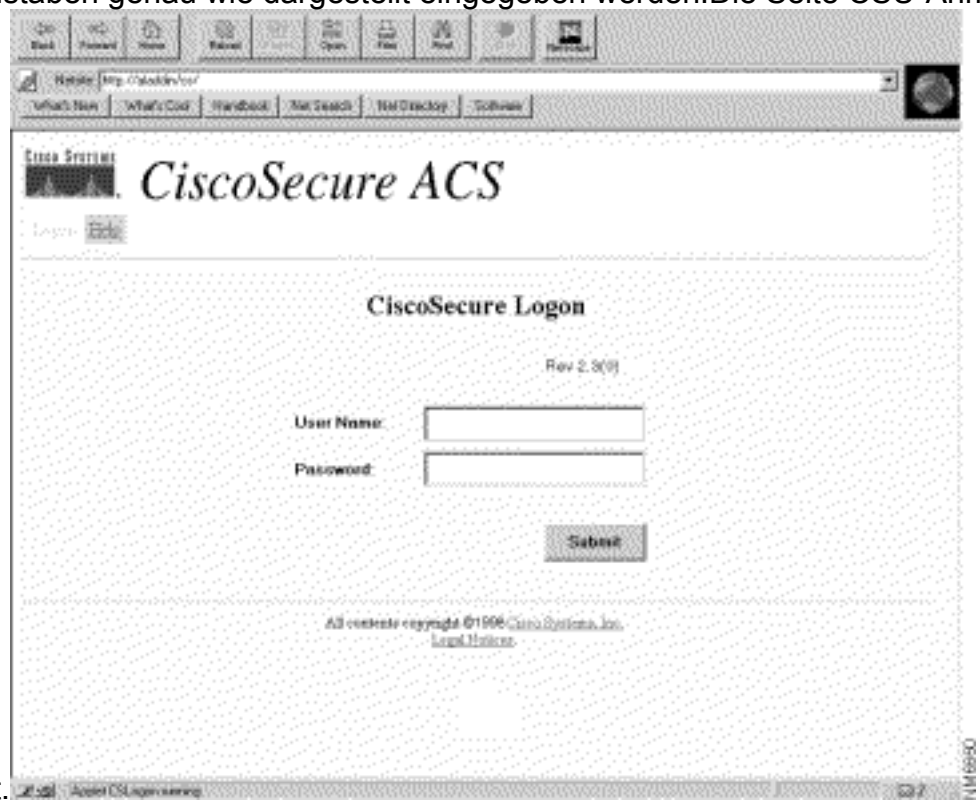
Mit diesem Verfahren melden Sie sich beim Cisco Secure Administrator an.

1. Starten Sie Ihren Webbrowser von jeder Workstation mit Webverbindung zum ACS.
2. Geben Sie eine der folgenden URLs für die Cisco Secure Administrator-Website ein:Wenn die Funktion für die Sicherheitssocklebene in Ihrem Browser nicht aktiviert ist, geben Sie Folgendes ein:
   ```
   http://your_server/cs
   ```
   Dabei ist your_server der Hostname (oder der vollqualifizierte Domänenname (FQDN), wenn sich Hostname und FQDN unterscheiden) der SPARCstation, auf der Sie CSU installiert haben. Sie können auch die IP-Adresse der SPARCstation für Ihren_Server ersetzen.Wenn

die Funktion für den Sicherheitssockel-Layer in Ihrem Browser aktiviert ist, geben Sie als Hypertext-Übertragungsprotokoll "https" und nicht "http" an. Eingabe:

```
https://your_server/cs
```

Dabei ist your_server der Hostname (oder, wenn sich der Hostname und der FQDN unterscheiden) der SPARCstation, auf der Sie CSU installiert haben. Sie können auch die IP-Adresse der SPARCstation für Ihren_Server ersetzen.**Hinweis:** Bei URLs und Servernamen wird zwischen Groß- und Kleinschreibung unterschieden. Sie müssen mit Groß- und Kleinbuchstaben genau wie dargestellt eingegeben werden.Die Seite CSU-Anmeldung wird angezeigt.

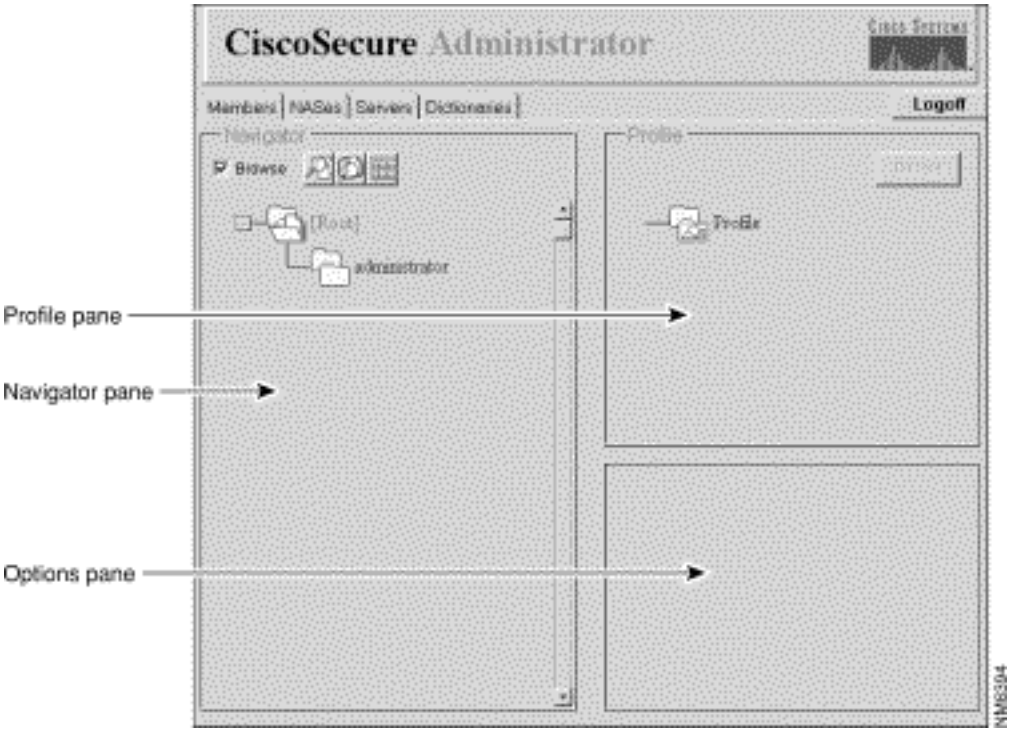


3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Klicken Sie auf **Senden**.**Hinweis:** Der erste Standardbenutzername ist "Superuser". Das ursprüngliche Standardkennwort lautet "changeme". Nach der ersten Anmeldung müssen Sie Benutzername und Kennwort sofort ändern, um maximale Sicherheit zu gewährleisten.Nach der Anmeldung wird die CSU-Hauptseite mit der Hauptmenüleiste oben angezeigt. Die Seite für das Hauptmenü der CSU wird nur angezeigt, wenn der Benutzer einen Namen und ein Kennwort mit Administratorrechten bereitstellt. Wenn der Benutzer einen Namen und ein Kennwort bereitstellt, die nur über Berechtigungen auf Benutzerebene verfügen, wird ein anderer Bildschirm angezeigt.

Starten des erweiterten Konfigurationsprogramms

Starten Sie das Java-basierte Cisco Secure Administrator Advanced Configuration-Programm von einer beliebigen CSU Administrator-Webseite aus. Klicken Sie in der Menüleiste der CSU-Webschnittstelle auf **Erweitert** und dann erneut auf **Erweitert**.

Das Cisco Secure Administrator Advanced Configuration-Programm wird angezeigt. Das Laden kann möglicherweise einige Minuten dauern.



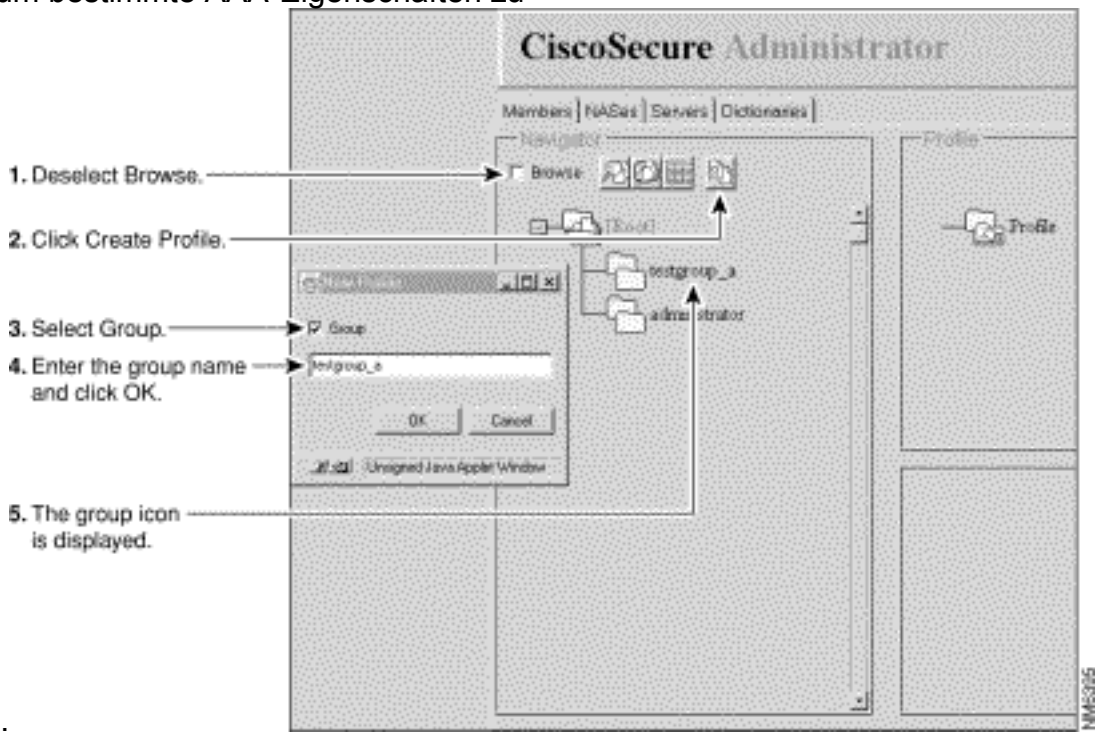
Erstellen eines Gruppenprofils

Verwenden Sie das Cisco Secure Administrator Advanced Configuration-Programm, um Gruppenprofile zu erstellen und zu konfigurieren. Cisco empfiehlt, Gruppenprofile zu erstellen, um detaillierte AAA-Anforderungen für eine große Anzahl ähnlicher Benutzer zu konfigurieren. Nachdem das Gruppenprofil definiert wurde, können Sie mithilfe der CSU Add a User-Webseite schnell Benutzerprofile zum Gruppenprofil hinzufügen. Die für die Gruppe konfigurierten erweiterten Anforderungen gelten für jeden Mitgliedsbenutzer.

Verwenden Sie diese Prozedur, um ein Gruppenprofil zu erstellen.

1. Wählen Sie im Cisco Secure Administrator Advanced Configuration-Programm die Registerkarte **Mitglieder** aus. Deaktivieren Sie im Navigationsbereich das Kontrollkästchen **Durchsuchen**. Das Symbol Neues Profil erstellen wird angezeigt.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:Um ein Gruppenprofil ohne übergeordnete Elemente zu erstellen, suchen Sie das Ordnersymbol [**Root**], und klicken Sie darauf.Wenn Sie Ihr Gruppenprofil als untergeordnetes Element eines anderen Gruppenprofils erstellen möchten, suchen Sie die Gruppe, die Sie als übergeordnetes Element festlegen möchten, und klicken Sie darauf.Wenn es sich bei der Gruppe, die Sie als übergeordnet betrachten möchten, um eine untergeordnete Gruppe handelt, klicken Sie auf den Ordner der übergeordneten Gruppe, um diese anzuzeigen.
3. Klicken Sie auf **Neues Profil erstellen**. Das Dialogfeld Neues Profil wird angezeigt.

4. Aktivieren Sie das Kontrollkästchen **Gruppe**, geben Sie den Namen der Gruppe ein, die Sie erstellen möchten, und klicken Sie auf **OK**. Die neue Gruppe wird in der Struktur angezeigt.
5. Nachdem Sie das Gruppenprofil erstellt haben, weisen Sie TACACS+- oder RADIUS-Attribute zu, um bestimmte AAA-Eigenschaften zu konfigurieren.



Erstellen eines Benutzerprofils im erweiterten Konfigurationsmodus

Verwenden Sie den Cisco Secure Administrator Advanced Configuration-Modus, um ein Benutzerprofil zu erstellen und zu konfigurieren. So können Sie die Autorisierungs- und Accounting-Attribute des Benutzerprofils detaillierter anpassen, als dies mit der Seite Benutzer hinzufügen möglich ist.

Verwenden Sie diese Prozedur, um ein Benutzerprofil zu erstellen:

1. Wählen Sie im Cisco Secure Administrator Advanced Configuration-Programm die Registerkarte **Mitglieder** aus. Suchen Sie im Navigationsbereich die Option **Durchsuchen**, und deaktivieren Sie sie. Das Symbol Neues Profil erstellen wird angezeigt.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:Suchen und klicken Sie auf die Gruppe, der der Benutzer angehört.Wenn Sie nicht möchten, dass der Benutzer einer Gruppe angehört, klicken Sie auf das Symbol für den Ordner [**Root**].
3. Klicken Sie auf **Profil erstellen**. Das Dialogfeld Neues Profil wird angezeigt.
4. Stellen Sie sicher, dass das Kontrollkästchen **Gruppe** deaktiviert ist.
5. Geben Sie den Namen des Benutzers ein, den Sie erstellen möchten, und klicken Sie auf **OK**. Der neue Benutzer wird in der Struktur angezeigt.
6. Nachdem Sie das Benutzerprofil erstellt haben, weisen Sie bestimmte TACACS+- oder RADIUS-Attribute zu, um bestimmte AAA-Eigenschaften zu konfigurieren:Informationen zum Zuweisen von TACACS+-Profilen zum Benutzerprofil finden Sie unter Zuweisen von TACACS+-Attributen zu einer Gruppe oder einem Benutzerprofil.Informationen zum Zuweisen von RADIUS-Profilen zum Benutzerprofil finden Sie unter Zuweisen von RADIUS-Attributen zu einer Gruppe oder einem Benutzerprofil.

Strategien zum Anwenden von Attributen

Verwenden Sie die CSU-Gruppenprofilfunktion und die TACACS+- und RADIUS-Attribute, um die Authentifizierung und Autorisierung von Netzwerkbenutzern über CSU zu implementieren.

Planattribute für Gruppen und Benutzer

Mit der Funktion für Gruppenprofile von CSU können Sie eine Reihe gemeinsamer AAA-Anforderungen für eine große Anzahl von Benutzern definieren.

Sie können einem Gruppenprofil einen Satz von TACACS+- oder RADIUS-Attributwerten zuweisen. Diese der Gruppe zugewiesenen Attributwerte gelten für alle Benutzer, die Mitglied oder Mitglied dieser Gruppe sind.

Effektive Verwendung der Gruppenprofilfunktion

Um CSU für die Verwaltung einer großen Anzahl von Benutzern und verschiedener Benutzertypen mit komplexen AAA-Anforderungen zu konfigurieren, empfiehlt Cisco die Verwendung der Funktionen des Cisco Secure Administrator Advanced Configuration-Programms zum Erstellen und Konfigurieren von Gruppenprofilen.

Das Gruppenprofil muss alle Attribute enthalten, die nicht benutzerspezifisch sind. Dies bedeutet in der Regel alle Attribute außer dem Kennwort. Anschließend können Sie auf der Seite "Benutzer hinzufügen" des Cisco Secure Administrator einfache Benutzerprofile mit Kennwortattributen erstellen und diese Benutzerprofile dem entsprechenden Gruppenprofil zuweisen. Die für eine bestimmte Gruppe definierten Features und Attributwerte gelten dann für die zugehörigen Member-Benutzer.

Übergeordnete Gruppen und untergeordnete Gruppen

Sie können eine Gruppenhierarchie erstellen. In einem Gruppenprofil können Sie untergeordnete Gruppenprofile erstellen. Dem übergeordneten Gruppenprofil zugewiesene Attributwerte sind Standardwerte für die untergeordneten Gruppenprofile.

Gruppenebene Verwaltung

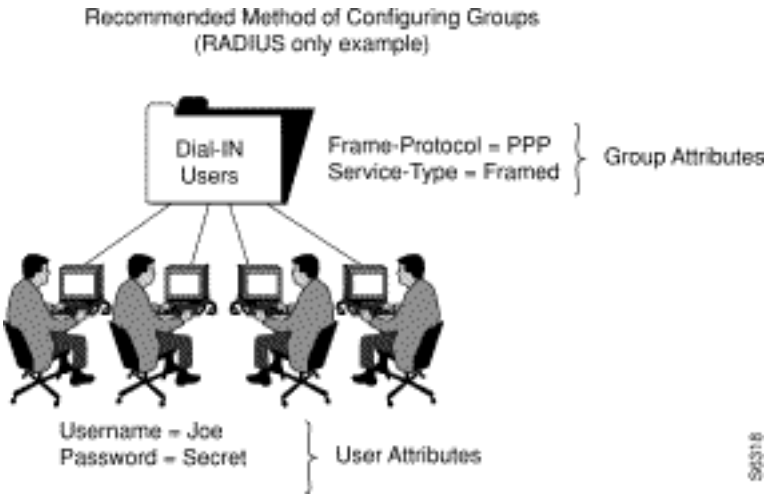
Ein Cisco Secure System Administrator kann einzelnen Cisco Secure User Group Administrator-Status zuweisen. Mit dem Gruppenadministratorstatus können einzelne Benutzer untergeordnete Gruppenprofile und Benutzerprofile verwalten, die ihrer Gruppe untergeordnet sind. Es ist ihnen jedoch nicht gestattet, Gruppen oder Benutzer zu verwalten, die nicht in die Hierarchie ihrer Gruppe fallen. Der Systemadministrator übernimmt somit die Verwaltung eines großen Netzwerks an andere Personen, ohne ihnen die gleiche Autorität zu verleihen.

Welche Attribute definiere ich für einzelne Benutzer?

Cisco empfiehlt, einzelnen Benutzern grundlegende Authentifizierungsattribute zuzuweisen, die für den Benutzer eindeutig sind, z. B. Attribute zur Definition von Benutzername, Kennwort, Kennworttyp und Webberechtigung. Weisen Sie den Benutzern über die CSUs Benutzer bearbeiten oder Benutzerseiten hinzufügen einfache Authentifizierungsattribute zu.

Welche Attribute definiere ich für Gruppenprofile?

Cisco empfiehlt, auf Gruppenebene Attribute in Bezug auf Qualifizierung, Autorisierung und Abrechnung festzulegen.



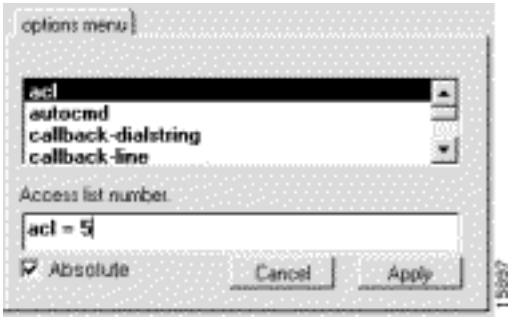
In diesem Beispiel wird dem Gruppenprofil "Dial-In Users" (Einwahlbenutzer) die Attributwertpaare Frame-Protocol=PPP und Service-Type=Framed zugewiesen.

Was sind absolute Attribute?

Einem Teil der TACACS+- und RADIUS-Attribute in CSU kann auf Gruppenprofilebene der absolute Status zugewiesen werden. Ein Attributwert, der auf Gruppenprofilebene für den absoluten Status aktiviert ist, überschreibt alle konkurrierenden Attributwerte in einem untergeordneten Gruppenprofil oder auf Ebene des Mitgliederbenutzerprofils.

In Netzwerken mit mehreren Ebenen von Gruppenadministratoren ermöglichen absolute Attribute einem Systemadministrator, bestimmte Gruppenattribute festzulegen, die von Gruppenadministratoren auf niedrigeren Ebenen nicht überschrieben werden können.

Für Attribute, denen der absolute Status zugewiesen werden kann, wird im Feld "Attribute" des Cisco Secure Administrator Advanced Configuration-Programms ein Kontrollkästchen Absolut angezeigt. Aktivieren Sie das Kontrollkästchen, um den absoluten Status zu aktivieren.



Können Attributwerte und Benutzerattributwerte miteinander in Konflikt stehen?

Die Konfliktlösung zwischen Attributwerten, die übergeordneten Gruppenprofilen, untergeordneten Gruppenprofilen und Memberbenutzerprofilen zugewiesen sind, hängt davon ab, ob die Attributwerte absolut sind und ob es sich um TACACS+- oder RADIUS-Attribute handelt:

- TACACS+- oder RADIUS-Attributwerte, die einem Gruppenprofil mit dem absoluten Status zugewiesen sind, überschreiben alle auf einer untergeordneten Gruppen- oder Benutzerprofilebene festgelegten Attributwerte, die den Wettbewerb betreffen.
- Wenn der absolute Status eines TACACS+-Attributwerts auf Gruppenprofilebene nicht aktiviert ist, wird er von jedem Attributwert überschrieben, der auf einer untergeordneten Gruppen- oder Benutzerprofilebene festgelegt wurde.
- Wenn der absolute Status eines RADIUS-Attributwerts auf der Ebene der übergeordneten Gruppe nicht aktiviert ist, führen alle in einer untergeordneten Gruppe festgelegten Attributwerte, die den Konflikt verursachen, zu einem unvorhersehbaren Ergebnis. Wenn Sie RADIUS-Attributwerte für eine Gruppe und die zugehörigen Member-Benutzer definieren, vermeiden Sie die Zuweisung desselben Attributs für das Benutzer- und Gruppenprofil.

Verwenden der Verbots- und Genehmigungsoptionen

Überschreiben Sie für TACACS+ die Verfügbarkeit geerbter Dienstwerte, indem Sie dem Schlüsselwort **allow** oder **permit** der Dienstspezifikation voranstellen. Das **permit**-Schlüsselwort ermöglicht angegebene Dienste. Das Schlüsselwort **noch** ausschließen lässt bestimmte Dienste zu. Wenn Sie diese Schlüsselwörter zusammen verwenden, können Sie "alles außer" Konfigurationen erstellen. Diese Konfiguration ermöglicht beispielsweise den Zugriff von allen Diensten mit Ausnahme von X.25:

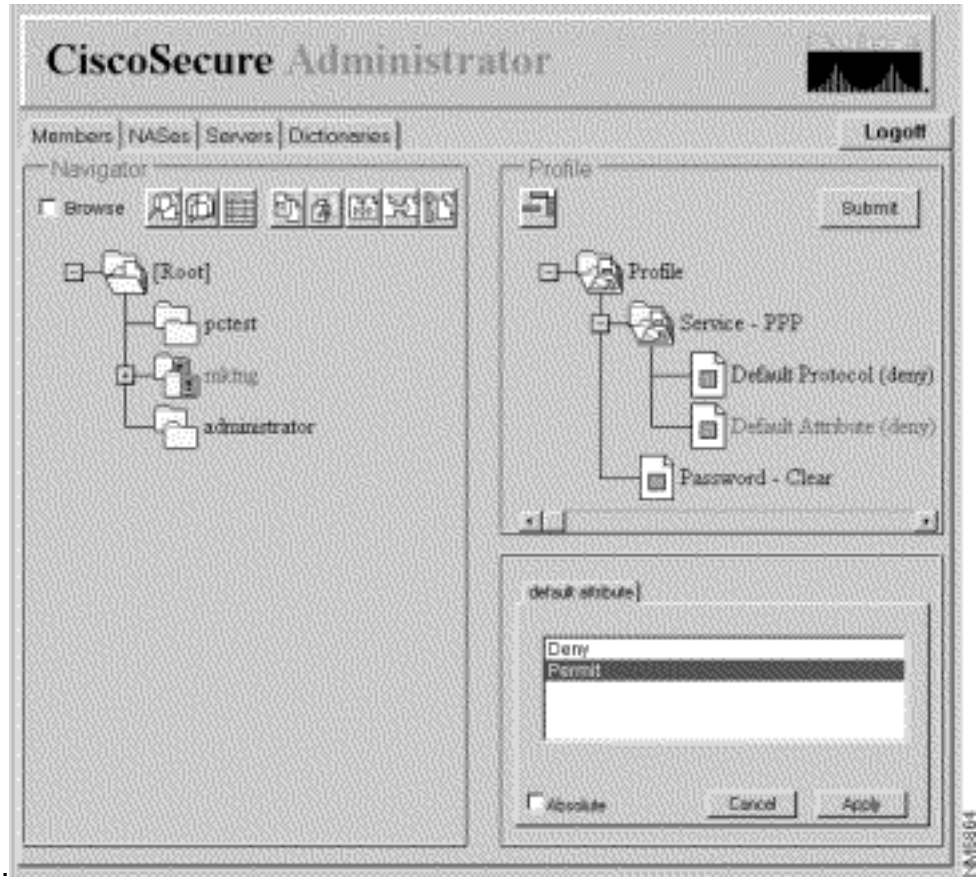
```
default service = permit
prohibit service = x25
```

Zuweisen von TACACS+-Attributen zu einer Gruppe oder einem Benutzerprofil

Um einer Gruppe oder einem Benutzerprofil bestimmte TACACS+-Services und -Attribute zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie im Cisco Secure Administrator Advanced Configuration-Programm die Registerkarte **Mitglieder** aus. Klicken Sie im Bereich Navigator auf das Symbol für die Gruppe oder das Benutzerprofil, der bzw. dem TACACS+-Attribute zugewiesen sind.
2. Klicken Sie ggf. im Bereich "Profil" auf das **Profil-**Symbol, um es zu erweitern.Eine Liste oder ein Dialogfeld mit Attributen, die für das ausgewählte Profil oder den ausgewählten Service gelten, wird unten rechts im Bildschirm angezeigt. Die Informationen in diesem Fenster ändern sich, je nachdem, welches Profil oder welchen Service Sie im Profilbereich auswählen.
3. Klicken Sie auf den Dienst oder das Protokoll, den Sie hinzufügen möchten, und klicken Sie auf **Übernehmen**. Der Service wird dem Profil hinzugefügt.
4. Geben Sie den gewünschten Text im Attributfenster ein, oder wählen Sie ihn aus.Gültige Einträge werden im Abschnitt Strategien für die Anwenden von Attributen im CSU 2.3 für UNIX-Referenzhandbuch erläutert.**Hinweis:** Wenn Sie einen Attributwert auf Gruppenprofilebene zuweisen und das von Ihnen angegebene Attribut ein **Absolutes** Kontrollkästchen anzeigt, aktivieren Sie dieses Kontrollkästchen, um den absoluten Wert zuzuweisen. Ein wertzugewiesener absoluter Status kann nicht durch Werte überschrieben werden, die auf untergeordneten Gruppen- oder Benutzerprofilebenen zugewiesen sind.
5. Wiederholen Sie die Schritte 1 bis für jeden zusätzlichen Dienst oder jedes zusätzliche Protokoll, den Sie hinzufügen müssen.
6. Wenn alle Änderungen vorgenommen wurden, klicken Sie auf

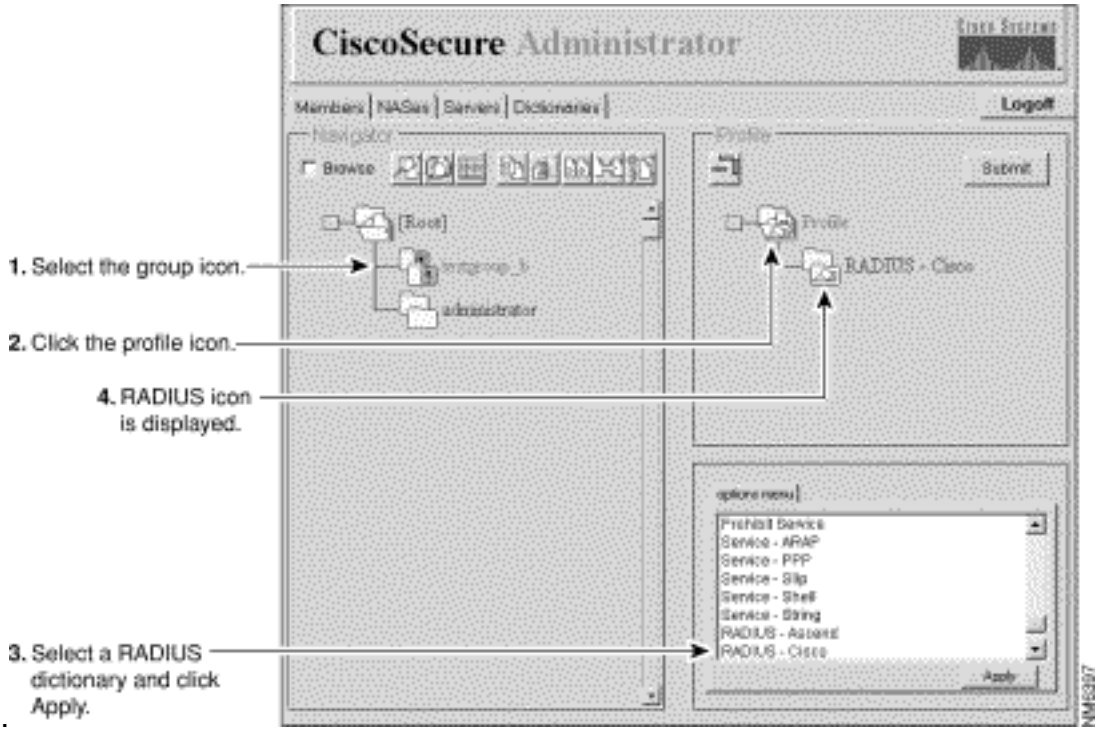
Senden.



Zuweisen von RADIUS-Attributen zu einer Gruppe oder einem Benutzerprofil

So weisen Sie einer Gruppe oder einem Benutzerprofil bestimmte RADIUS-Attribute zu:

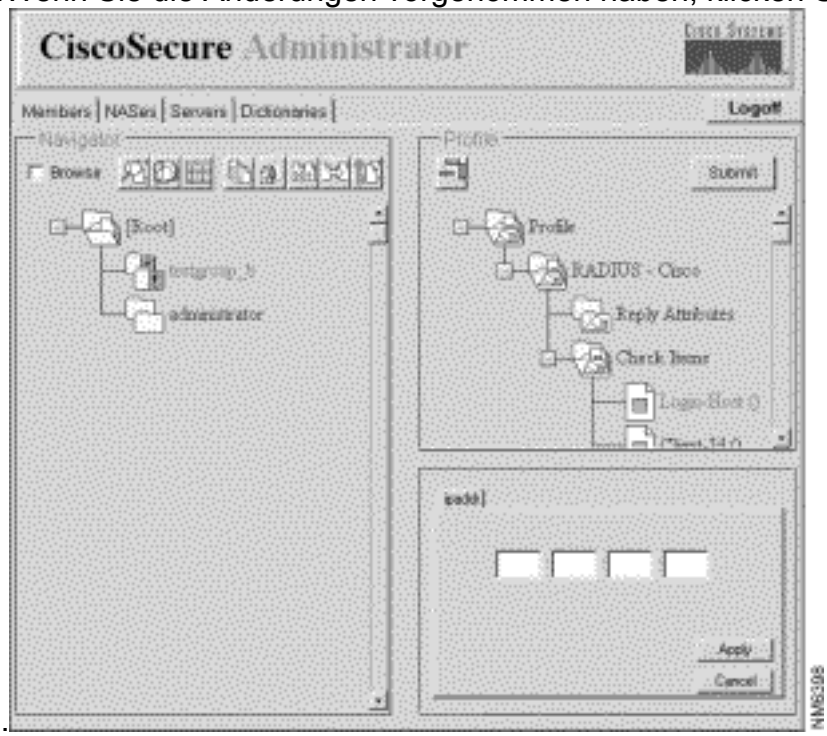
1. Zuweisen eines RADIUS-Wörterbuchs zum Gruppenprofil:Klicken Sie auf der Seite "Members" des Cisco Secure Administrator Advanced Configuration-Programms auf das Symbol **Gruppe** oder **Benutzer** und anschließend im Bereich Profile auf das Symbol **Profil**. Im Bereich Attribute wird das Menü Optionen angezeigt.Klicken Sie im Menü **Optionen** auf den Namen des RADIUS-Wörterbuchs, das die Gruppe oder der Benutzer verwenden soll. (Zum Beispiel RADIUS - Cisco.) Klicken Sie auf



Übernehmen.

2. Fügen Sie dem RADIUS-Profil die erforderlichen Check Items (Elemente prüfen) und Reply Attributes (Attribute antworten) hinzu:**Hinweis:** Check-Elemente sind Attribute, die für die Authentifizierung erforderlich sind, z. B. Benutzer-ID und Kennwort. Reply Attributes sind Attribute, die an den Network Access Server (NAS) gesendet werden, nachdem das Profil die Authentifizierungsverfahren durchlaufen hat, z. B. Framed-Protocol. Listen und Erklärungen zu Check Items and Reply Attributes finden Sie im RADIUS Attribute-Value Pairs und Dictionary Management im CSU 2.3 for UNIX Reference Guide.Klicken Sie im Fenster Profil auf das Symbol RADIUS - dictionaryname im Ordner. (Sie müssen wahrscheinlich auf das Symbol + des Profils klicken, um den RADIUS-Ordner zu erweitern.) Die Optionen Elemente überprüfen und Attribute antworten werden im Fenster Attributgruppe angezeigt.Um eines oder mehrere dieser Attribute zu verwenden, klicken Sie auf die Attribute, die Sie verwenden möchten, und klicken Sie dann auf **Übernehmen**. Sie können mehrere Attribute gleichzeitig hinzufügen.Klicken Sie auf das **+** Symbol für RADIUS - dictionaryname, um den Ordner zu erweitern.**Hinweis:** Wenn Sie die Option RADIUS-Cisco11.3 auswählen, stellen Sie sicher, dass die Cisco IOS® Softwareversion 11.3.3(T) oder höher auf Ihren NAS-Verbindungsgeräten installiert ist, und fügen Sie Ihren NAS-Konfigurationen neue Befehlszeilen hinzu. Das UNIX-Referenzhandbuch finden Sie im Dokument Vollständige Aktivierung des RADIUS-Cisco11.3-Wörterbuchs im CSU 2.3.
3. Geben Sie Werte für die hinzugefügten Check-Elemente und Reply-Attribute an:**Vorsicht:** Beim RADIUS-Protokoll ist Vererbung additiv und nicht hierarchisch. (Das TACACS+-Protokoll verwendet hierarchische Vererbung). Wenn Sie z. B. den Benutzer- und Gruppenprofilen dieselben Antwortattribute zuweisen, schlägt die Autorisierung fehl, da das NAS die doppelte Anzahl von Attributen erhält. Die Antwortattribute sind nicht sinnvoll. Weisen Sie der Gruppe und den Benutzerprofilen nicht dasselbe Check-Element oder dasselbe Antworten-Attribut zu.Klicken Sie auf **Artikel prüfen** oder **Attribute antworten**, oder klicken Sie auf beides. Im unteren rechten Fenster wird eine Liste der entsprechenden Werte für Check Items und Reply Attributes (Elemente prüfen und Attribute antworten) angezeigt. Klicken Sie auf das **+** Symbol, um den Ordner zu erweitern.Klicken Sie auf die Werte, die Sie zuweisen möchten, und klicken Sie dann auf **Übernehmen**. Weitere Informationen zu den Werten finden Sie im RADIUS Attribut-Wert-Paare und Wörterbuchverwaltung im CSU 2.3 für UNIX-Referenzhandbuch.**Hinweis:** Wenn Sie auf Gruppenprofilebene einen Attributwert

zuweisen und das von Ihnen angegebene Attribut ein Kontrollkästchen Absolut anzeigt, aktivieren Sie dieses Kontrollkästchen, um den absoluten Wert zuzuweisen. Ein Wert, dem ein absoluter Status zugewiesen wurde, kann nicht durch Werte überschrieben werden, die auf der Ebene der untergeordneten Gruppenprofile oder Benutzerprofile zugewiesen wurden.Wenn Sie die Änderungen vorgenommen haben, klicken Sie auf Senden.



4. Um eines oder mehrere dieser Attribute zu verwenden, klicken Sie auf die Attribute, die Sie verwenden möchten, und klicken Sie dann auf **Übernehmen**. Sie können mehrere Attribute gleichzeitig anwenden.

Berechtigungsstufen für die Zugriffskontrolle zuweisen

Der Superuser-Administrator verwendet das Attribut "webprivilege", um Cisco Secure-Benutzern eine Berechtigungsstufe für die Zugriffskontrolle zuzuweisen.

1. Klicken Sie im Cisco Secure Administrator Advanced Configuration-Programm auf den Benutzer, dessen Zugriffssteuerungsberechtigung Sie zuweisen möchten, und klicken Sie anschließend im Profilbereich auf das Symbol Profile (Profil).
2. Klicken Sie im Menü Optionen auf **Webberechtigung** und wählen Sie einen dieser Werte aus.**0** - Verweigert dem Benutzer Zugriffskontrollberechtigungen, die die Änderung des Cisco Secure Password des Benutzers beinhalten.**1** - Gewährt dem Benutzer Zugriff auf die CSUser-Webseite. So können Cisco Secure-Benutzer ihre Cisco Secure-Passwörter ändern. Weitere Informationen zum Ändern von Kennwörtern finden Sie unter Funktionen auf Benutzerebene (Ändern eines Kennworts) unter Einfache Benutzer- und ACS-Verwaltung.**12** - Gewährt der Benutzergruppenadministrator Berechtigungen.**15** - Gewährt den Systemadministratorberechtigungen des Benutzers.**Hinweis:** Wenn Sie eine andere Webberechtigungsoption als 0 auswählen, müssen Sie auch ein Kennwort angeben. Um die Anforderung des Passworts für Webberechtigungen zu erfüllen, ist ein einziger Leerzeichen minimal zulässig.

CSU starten und anhalten

In der Regel wird die CSU automatisch gestartet, wenn Sie die SPARCstation, auf der sie installiert ist, starten oder neu starten. Sie können CSU jedoch manuell starten oder herunterfahren, ohne die gesamte SPARCS-Station herunterzufahren.

Melden Sie sich als [Root] bei der SPARCS-Station an, in der Sie CSU installiert haben.

Um die CSU manuell zu starten, geben Sie Folgendes ein:

```
# /etc/rc2.d/S80CiscoSecure
```

Um die CSU manuell zu beenden, geben Sie Folgendes ein:

```
# /etc/rc0.d/K80CiscoSecure
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Support-Seite für Cisco Secure ACS für UNIX
- Support-Seite für TACACS+
- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems