Lock-and-Key: Dynamische Zugriffslisten

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Überlegungen zum Spoofing
Leistung
Verwendung von Lock-and-Key-Zugriff
Zugriffsbetrieb mit Lock-and-Key-Zugriff
Beispielkonfiguration und Fehlerbehebung
Netzwerkdiagramm
Verwenden von TACACS+
Verwenden von RADIUS
Zugehörige Informationen

Einführung

Mithilfe von Lock-and-Key-Zugriff können Sie dynamische Zugriffslisten einrichten, die über einen Benutzerauthentifizierungsprozess Zugriff auf einen bestimmten Quell-/Zielhost pro Benutzer gewähren. Der Benutzerzugriff wird über eine Cisco IOS® Firewall dynamisch und ohne Beeinträchtigung der Sicherheitsbeschränkungen zugelassen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. In diesem Fall bestand die Laborumgebung aus einem 2620 Router mit Cisco IOS® Software Release 12.3(1). 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 (Technische Tipps zu Konventionen von Cisco).

Überlegungen zum Spoofing

Durch Lock-and-Key-Zugriff kann ein externes Ereignis eine Öffnung in der Cisco IOS Firewall vornehmen. Nachdem diese Öffnung vorhanden ist, ist der Router anfällig für Spoofing der Quelladresse. Um dies zu verhindern, bieten Sie Verschlüsselungsunterstützung durch IP-Verschlüsselung mit Authentifizierung oder Verschlüsselung.

Spoofing ist ein Problem mit allen vorhandenen Zugriffslisten. Durch den Lock-and-Key-Zugriff wird dieses Problem nicht behoben.

Da der Lock-and-Key-Zugriff einen potenziellen Pfad durch Ihre Netzwerk-Firewall einleitet, müssen Sie einen dynamischen Zugriff in Betracht ziehen. Ein anderer Host, der Ihre authentifizierte Adresse imitiert, erhält Zugriff hinter der Firewall. Bei dynamischem Zugriff besteht die Möglichkeit, dass ein nicht autorisierter Host, der Ihre authentifizierte Adresse manipuliert, Zugriff hinter der Firewall erhält. Der Zugriff auf Lock-and-Key verursacht kein Problem mit dem Adressen-Spoofing. Das Problem wird hier nur als Problem für den Benutzer identifiziert.

Leistung

In diesen beiden Situationen ist die Leistung beeinträchtigt.

- Jede dynamische Zugriffsliste erzwingt eine Neuerstellung der Zugriffslisten auf der Silizium-Switching-Engine (SSE). Dadurch verlangsamt sich der SSE-Switching-Pfad vorübergehend.
- Dynamische Zugriffslisten erfordern die Leerlaufzeitüberschreitung (selbst wenn die Zeitüberschreitung standardmäßig übernommen wird). Daher können dynamische Zugriffslisten nicht auf SSE-Switches umgestellt werden. Diese Einträge werden im Protokoll-Fast-Switching-Pfad behandelt.

Achten Sie auf die Konfigurationen der Border Router. Remote-Benutzer erstellen Zugriffslisteneinträge auf dem Border Router. Die Zugriffsliste wächst und schrumpft dynamisch. Einträge werden dynamisch aus der Liste entfernt, nachdem die Leerlaufzeitüberschreitung oder die maximale Zeitüberschreitungsdauer abgelaufen sind. Große Zugriffslisten beeinträchtigen die Paketvermittlungsleistung.

Verwendung von Lock-and-Key-Zugriff

Hier sind zwei Beispiele für den Einsatz von Lock-and-Key-Zugriffsrechten aufgeführt:

- Wenn Sie möchten, dass ein Remotehost über das Internet auf einen Host im Internet zugreifen kann. Lock-and-Key-Zugriffsrechte schränken den Zugriff über Ihre Firewall hinaus auf individueller Host- oder Netzwerkbasis ein.
- Wenn ein Teil der Hosts in einem Netzwerk auf einen Host in einem Remote-Netzwerk zugreifen soll, das durch eine Firewall geschützt ist. Mit dem Lock-and-Key-Zugriff können Sie nur eine bestimmte Gruppe von Hosts für den Zugriff aktivieren, indem Sie sie über einen

TACACS+- oder RADIUS-Server authentifizieren lassen.

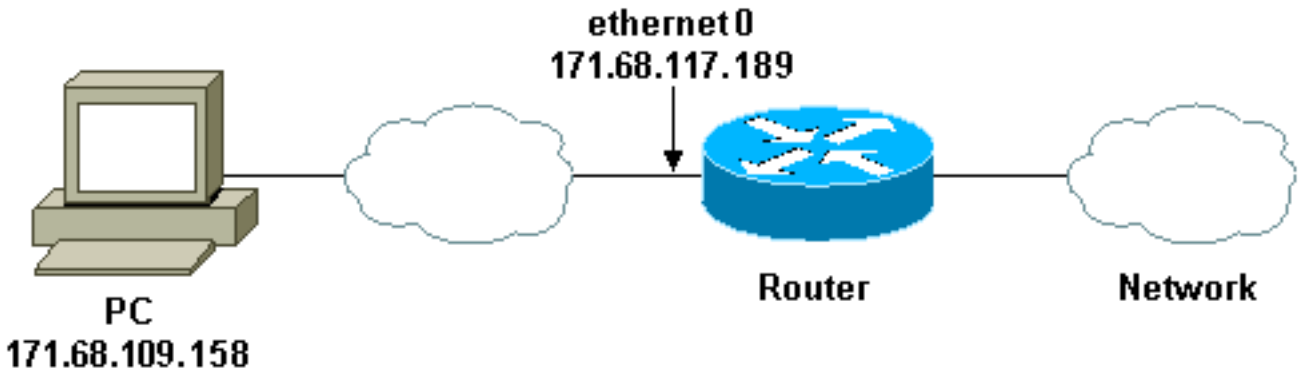
Zugriffsbetrieb mit Lock-and-Key-Zugriff

Dieser Prozess beschreibt den Vorgang für den Lock-and-Key-Zugriff.

1. Ein Benutzer öffnet eine Telnet-Sitzung mit einem Grenzrouter, der für den Lock-and-Key-Zugriff konfiguriert ist.
2. Die Cisco IOS-Software empfängt das Telnet-Paket. Er führt einen Benutzerauthentifizierungsprozess durch. Der Benutzer muss die Authentifizierung bestehen, bevor der Zugriff zugelassen wird. Der Authentifizierungsprozess erfolgt über den Router oder einen zentralen Zugriffsserver wie einen TACACS+- oder RADIUS-Server.

Beispielkonfiguration und Fehlerbehebung

Netzwerkdiagramm



Cisco empfiehlt die Verwendung eines TACACS+-Servers für den Authentifizierungsabfrageprozess. TACACS+ bietet Authentifizierungs-, Autorisierungs- und Accounting-Services. Darüber hinaus bietet es Protokollunterstützung, Protokollspezifikationen und eine zentrale Sicherheitsdatenbank.

Sie können den Benutzer auf dem Router oder mit einem TACACS+- oder RADIUS-Server authentifizieren.

Hinweis: Diese Befehle sind global, sofern nicht anders angegeben.

Auf dem Router benötigen Sie einen **Benutzernamen** für die lokale Authentifizierung des Benutzers.

```
username test password test
```

Wenn **Anmeldename lokal** auf den vty-Zeilen vorhanden ist, wird dieser Benutzername verwendet.

```
line vty 0 4
```

```
login local
```

Wenn Sie dem Benutzer nicht vertrauen, dass er den Befehl **access-enable** ausgibt, haben Sie folgende Möglichkeiten:

- Ordnen Sie das Timeout dem Benutzer auf Benutzerbasis zu.

  ```
  username test autocommand access-enable host
  timeout 10
  ```

  oder
- Erzwingen Sie, dass alle Telnet-Benutzer dasselbe Timeout haben.

  ```
  line vty 0 4
  login local
  autocommand access-enable host timeout 10
  ```

Hinweis: Die **10** in der Syntax ist die *Leerlaufzeitüberschreitung* in der Zugriffsliste. Sie wird durch das absolute Timeout in der dynamischen Zugriffsliste überschrieben.

Definieren Sie eine erweiterte Zugriffsliste, die angewendet wird, wenn sich ein Benutzer (ein beliebiger Benutzer) beim Router anmeldet und der **Befehl access-enable** ausgegeben wird. Die maximale absolute Zeit für dieses "Loch" im Filter ist auf 15 Minuten eingestellt. Nach 15 Minuten schließt das Loch, ob es von irgendjemandem benutzt wird oder nicht. Der Name **testlist** muss vorhanden sein, ist jedoch nicht von Bedeutung. Beschränken Sie die Netzwerke, auf die der Benutzer Zugriff hat, indem Sie die Quell- oder Zieladresse konfigurieren (hier ist der Benutzer nicht beschränkt).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Definieren Sie die Zugriffsliste, die erforderlich ist, um alle Komponenten außer Telnet in den Router zu blockieren (um ein Loch zu öffnen, muss der Benutzer Telnet zum Router verwenden). Die IP-Adresse hier ist die Ethernet-IP-Adresse des Routers.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Am Ende wird implizit **alles** verweigern (hier nicht eingegeben).

Wenden Sie diese Zugriffsliste auf die Schnittstelle an, auf der die Benutzer eintreffen.

```
interface ethernet1
       ip access-group 120 in
```

Sie sind fertig.

So sieht der Filter derzeit auf dem Router aus:

```
Router#show access-lists
```

```
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Benutzer, die Zugriff auf Ihr internes Netzwerk erhalten, sehen erst dann etwas, wenn sie Telnet zum Router verwenden.

Hinweis: Die **10** hier ist die *Leerlaufzeitüberschreitung* der Zugriffsliste. Sie wird durch das absolute Timeout in der dynamischen Zugriffsliste überschrieben.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

Der Filter sieht so aus.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Der Filter für diesen einen Benutzer weist eine Lücke auf, die auf der Quell-IP-Adresse basiert. Wenn jemand anders das macht, sehen Sie *zwei Löcher*.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Diese Benutzer können über ihre *Quell*-IP-Adresse vollständigen IP-Zugriff auf beliebige Ziel-IP-Adressen haben.

Verwenden von TACACS+

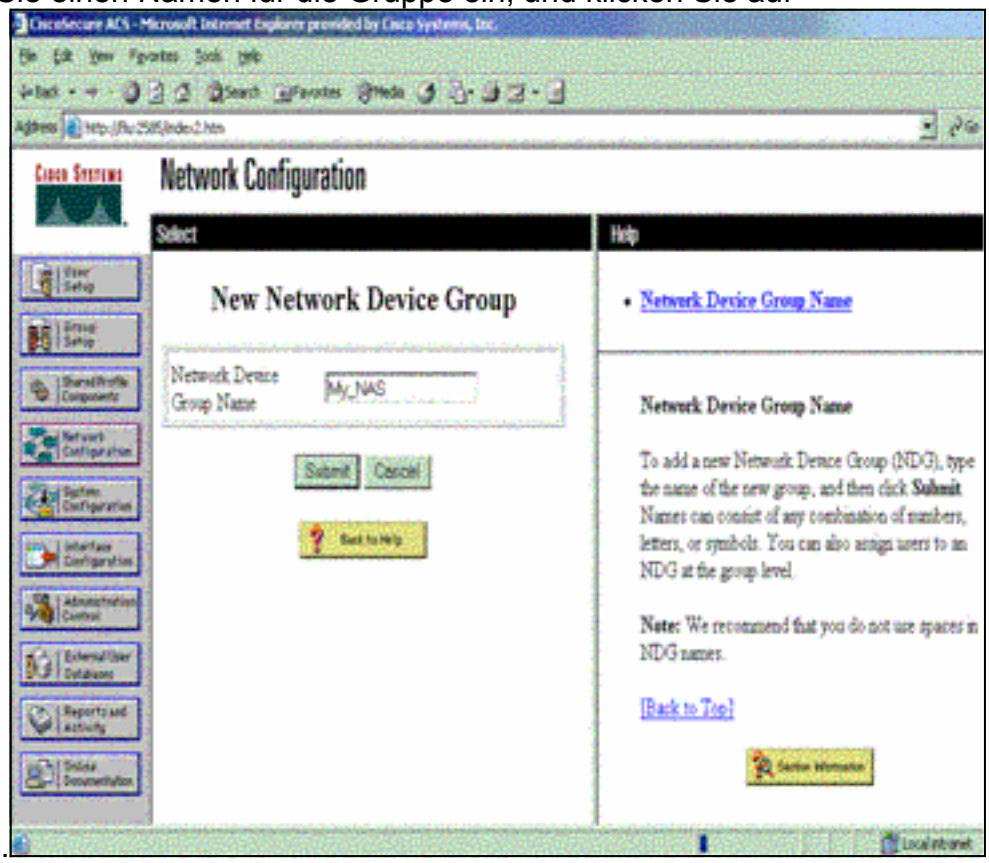
Konfigurieren von TACACS+

Konfigurieren Sie einen TACACS+-Server, um die Authentifizierung und Autorisierung auf dem TACACS+-Server zu erzwingen, um TACACS+ zu verwenden, wie die folgende Ausgabe zeigt:

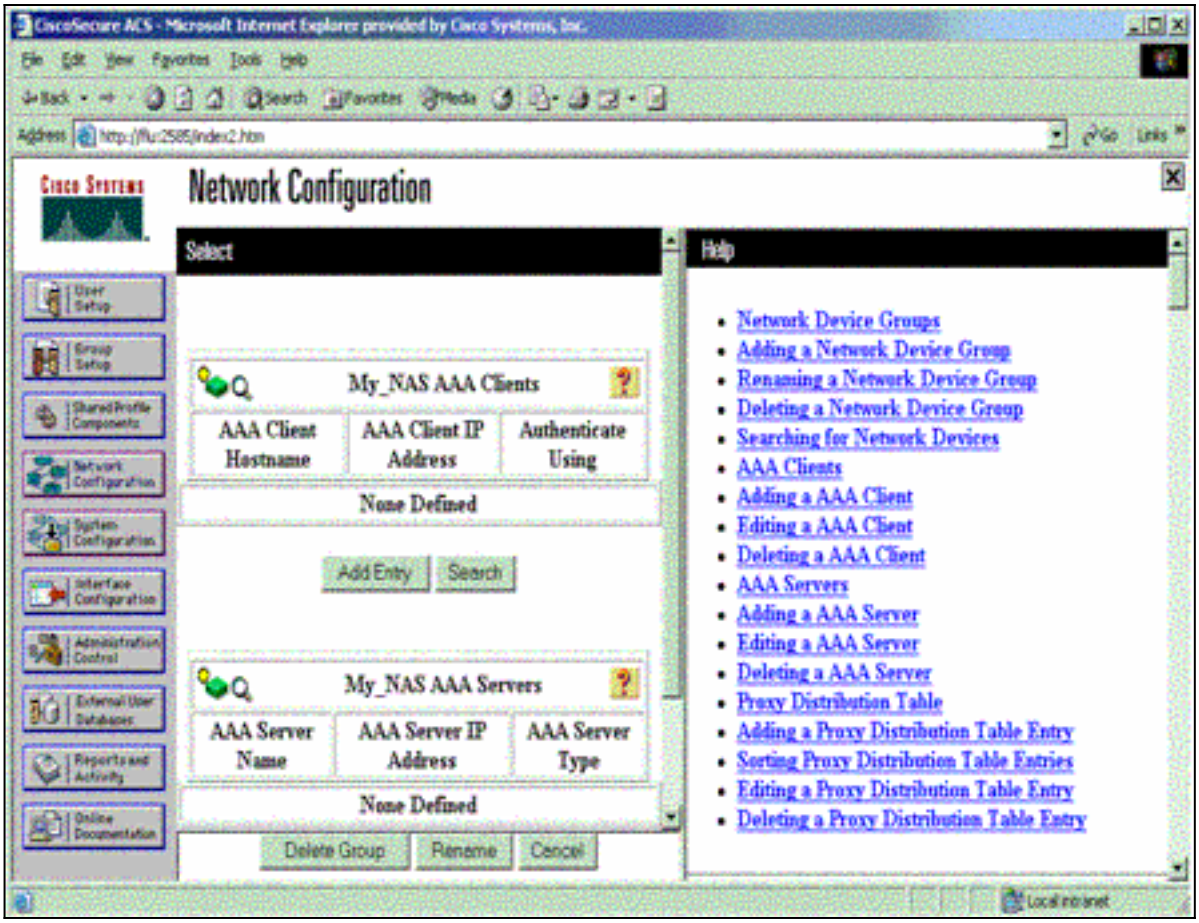
```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

Gehen Sie wie folgt vor, um TACACS+ auf Cisco Secure ACS für Windows zu konfigurieren:

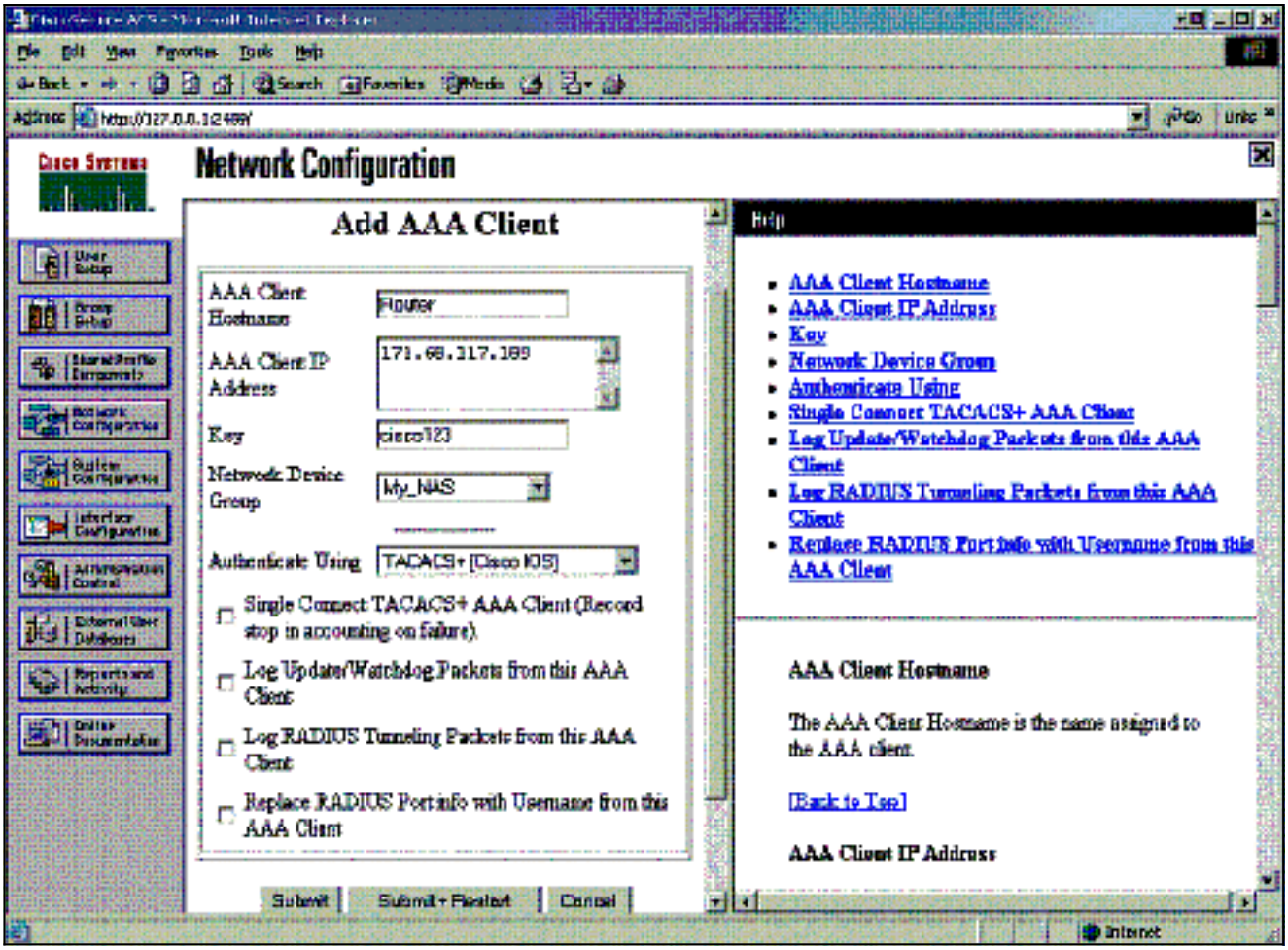
1. Öffnen Sie einen Webbrowser. Geben Sie die Adresse Ihres ACS-Servers in Form von **http://*<IP_address oder DNS_name>*:2002 ein**. (In diesem Beispiel wird der Standardport 2002 verwendet.) Melden Sie sich als admin an.
2. Klicken Sie auf **Netzwerkkonfiguration**. Klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um eine Netzwerkgerätegruppe zu erstellen, die die Netzwerkzugriffsserver (NAS) enthält. Geben Sie einen Namen für die Gruppe ein, und klicken Sie auf **Senden**.



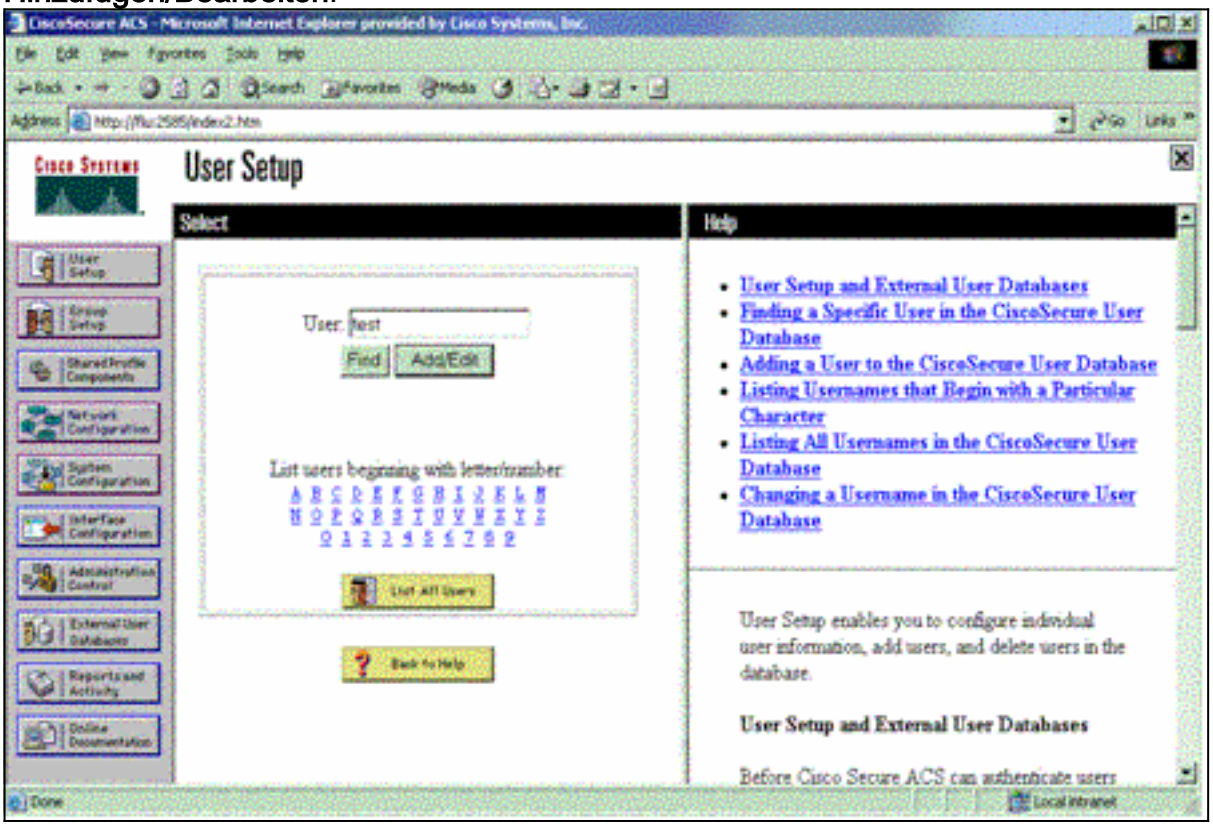
3. Klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um einen AAA-Client (Authentication, Authorization, Accounting) (NAS) hinzuzufügen.



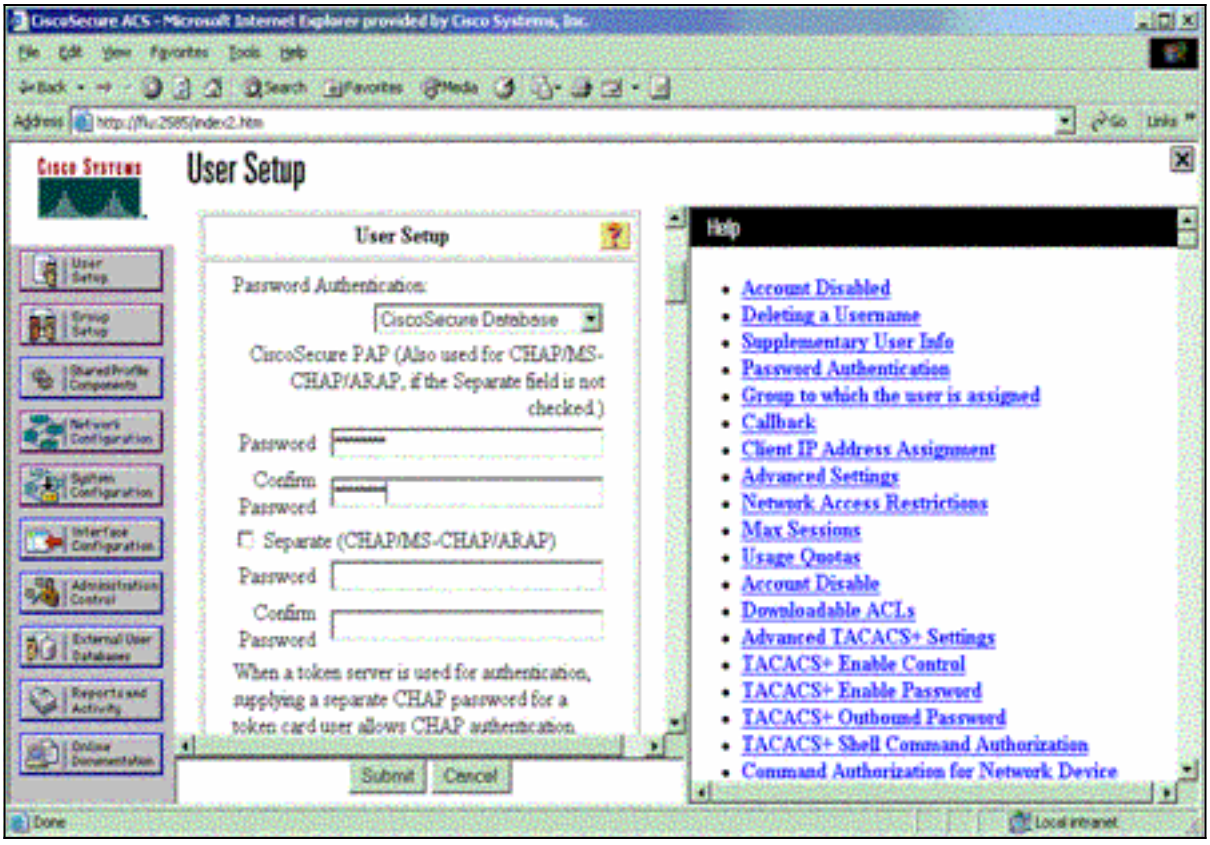
4. Geben Sie den Hostnamen, die IP-Adresse und den Schlüssel ein, der zur Verschlüsselung der Kommunikation zwischen dem AAA-Server und dem NAS verwendet wird. Wählen Sie **TACACS+ (Cisco IOS)** als Authentifizierungsmethode aus. Wenn Sie fertig sind, klicken Sie auf **Senden +Neu starten**, um die Änderungen zu übernehmen.



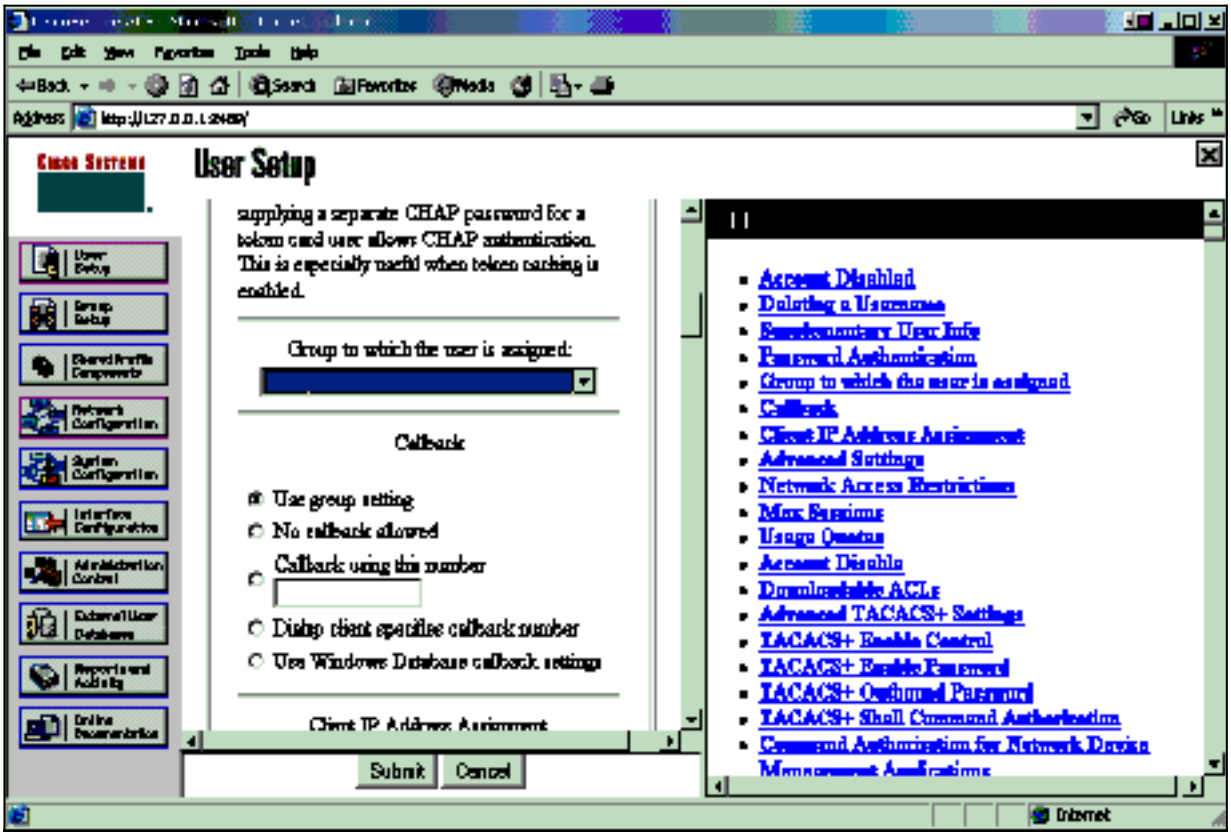
5. Klicken Sie auf **User Setup**, geben Sie eine Benutzer-ID ein, und klicken Sie auf **Hinzufügen/Bearbeiten**.



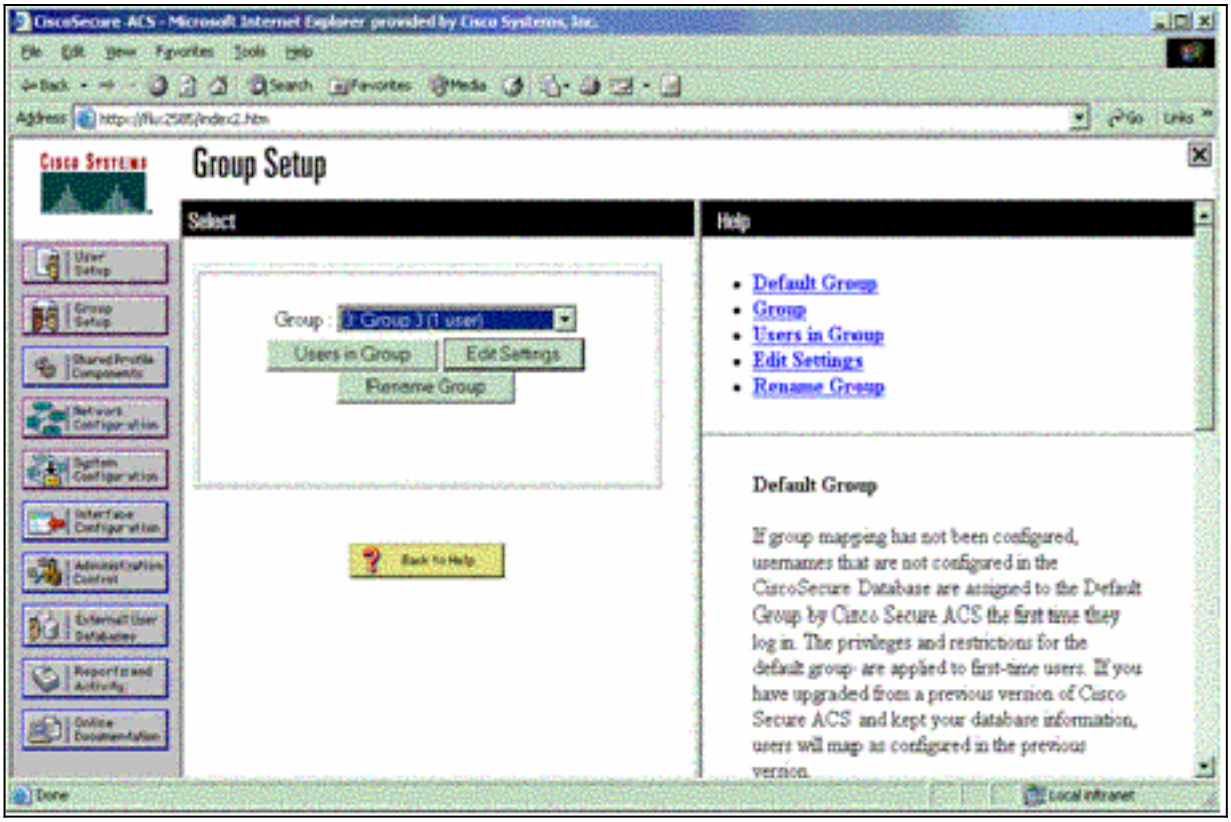
6. Wählen Sie eine Datenbank für die Benutzerauthentifizierung aus. (In diesem Beispiel ist der Benutzer "test" (Test), und die interne Datenbank des ACS wird für die Authentifizierung verwendet.) Geben Sie ein Kennwort für den Benutzer ein, und bestätigen Sie das Kennwort.



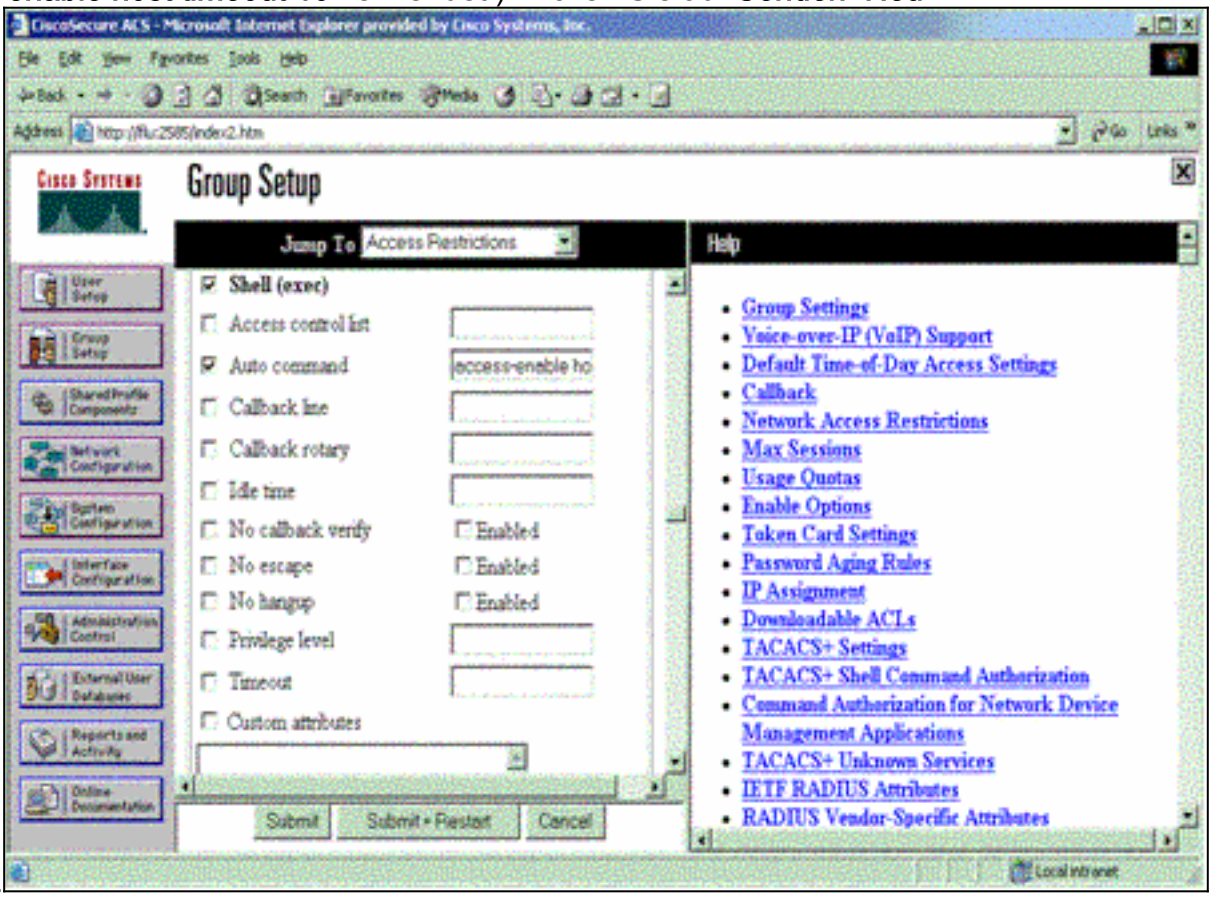
7. Wählen Sie die Gruppe aus, der der Benutzer zugewiesen ist, und aktivieren Sie die Option **Gruppeneinstellung verwenden**. Klicken Sie auf **Senden**.



8. Klicken Sie auf **Gruppeneinrichtung**. Wählen Sie die Gruppe aus, der der Benutzer in Schritt 7 zugewiesen wurde. Klicken Sie auf **Einstellungen bearbeiten**.



9. Blättern Sie nach unten zum Abschnitt TACACS+ Settings (TACACS+-Einstellungen). Aktivieren Sie das Kontrollkästchen für **Shell Exec**. Aktivieren Sie das Kontrollkästchen **Auto Command (Automatisch)**. Geben Sie den Auto-Befehl ein, der nach erfolgreicher Autorisierung des Benutzers ausgeführt werden soll. (In diesem Beispiel wird der Befehl **access-enable host timeout 10** verwendet.) Klicken Sie auf **Senden+Neu starten**.



[Fehlerbehebung in TACACS+]

Verwenden Sie diese **Debug-**Befehle auf dem NAS, um TACACS+-Probleme zu beheben.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug tacacs authentication**: Zeigt Informationen über den TACACS+-Authentifizierungsprozess an. Nur in einigen Softwareversionen verfügbar. Falls nicht verfügbar, verwenden Sie nur **Debugtaktiken**.
- **debug tacacs authorization** (**Berechtigung debug takacs**): Zeigt Informationen über den TACACS+-Autorisierungsprozess an. Nur in einigen Softwareversionen verfügbar. Falls nicht verfügbar, verwenden Sie nur **Debugtaktiken**.
- **debug tacacs events**: Zeigt Informationen aus dem TACACS+-Hilfsprozess an. Nur in einigen Softwareversionen verfügbar. Falls nicht verfügbar, verwenden Sie nur **Debugtaktiken**.

Verwenden Sie diese Befehle, um AAA-Probleme zu beheben:

- **debug aaa authentication**: Zeigt Informationen zur AAA/TACACS+-Authentifizierung an.
- **debug aaa autorization**: Zeigt Informationen zur AAA/TACACS+-Autorisierung an.

Die folgende **Debug-**Beispielausgabe zeigt einen erfolgreichen Authentifizierungs- und Autorisierungsprozess auf dem ACS TACACS+-Server.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
```

```
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Verwenden von RADIUS

Konfigurieren von RADIUS

Um RADIUS zu verwenden, konfigurieren Sie einen RADIUS-Server so, dass die Authentifizierung auf dem RADIUS-Server mit Autorisierungsparametern (der automatische Befehl) erzwungen wird, die im anbieterspezifischen Attribut 26 nach unten gesendet werden, wie hier gezeigt:

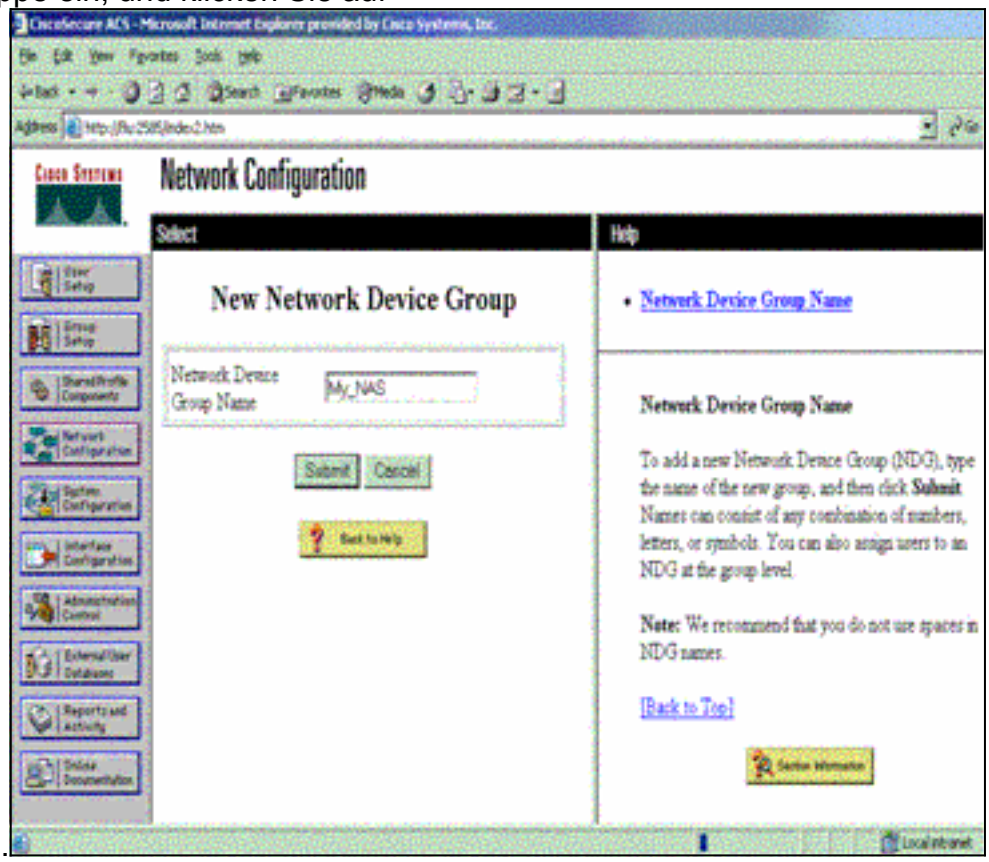
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Gehen Sie wie folgt vor, um RADIUS auf Cisco Secure ACS für Windows zu konfigurieren:

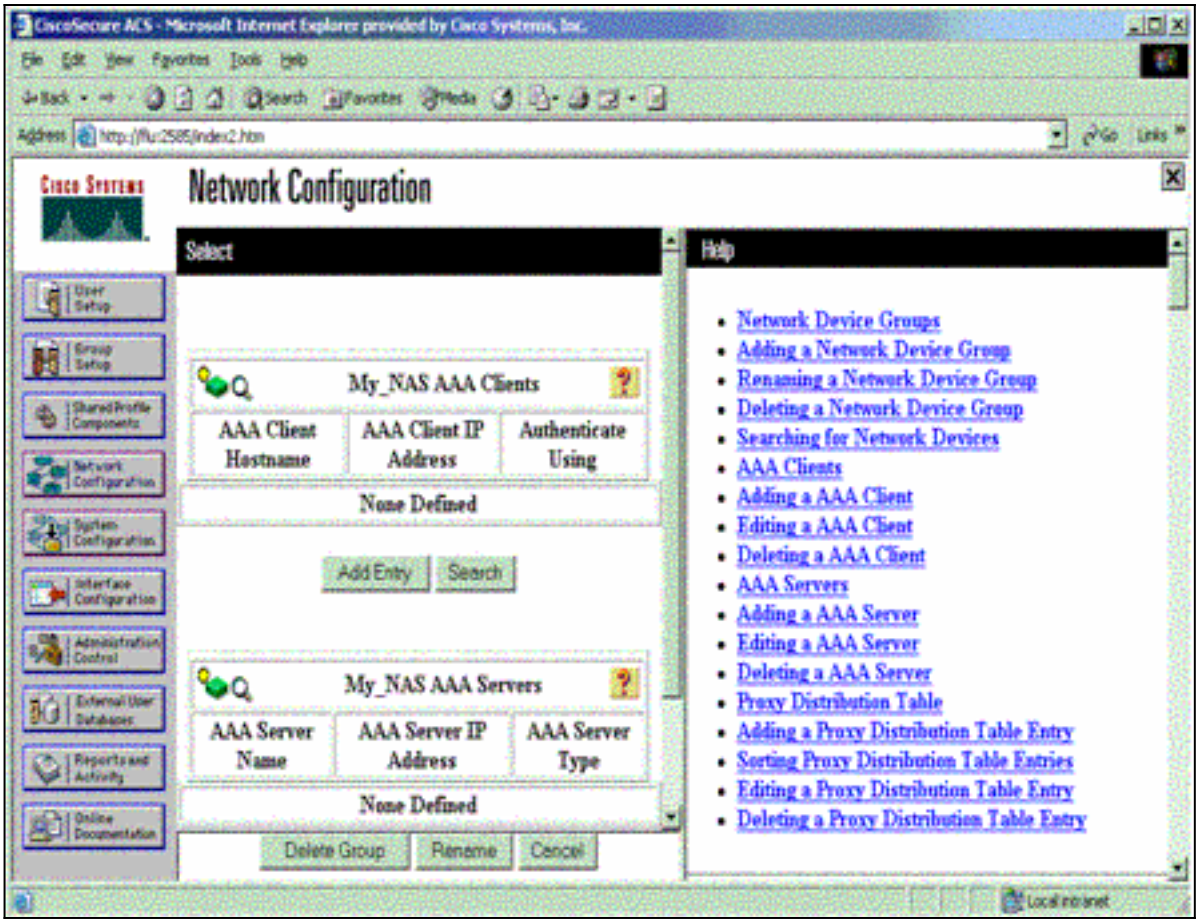
1. Öffnen Sie einen Webbrowser, und geben Sie die Adresse Ihres ACS-Servers in Form von

http://*<IP_address oder DNS_name>*:2002 ein. (In diesem Beispiel wird der Standardport 2002 verwendet.) Melden Sie sich als admin an.

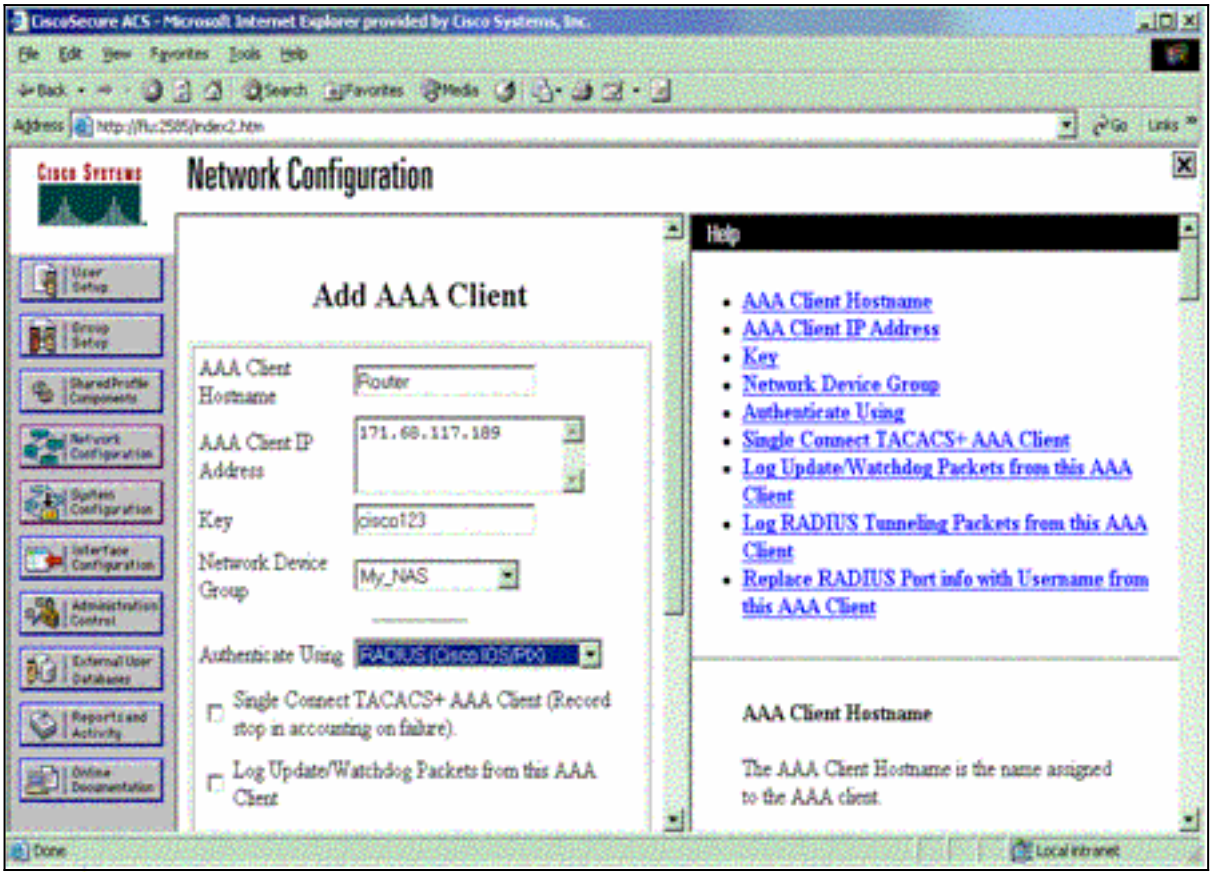
2. Klicken Sie auf **Netzwerkkonfiguration**. Klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um eine Netzwerkgerätegruppe zu erstellen, die das NAS enthält. Geben Sie einen Namen für die Gruppe ein, und klicken Sie auf **Senden**.



3. Klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um einen AAA-Client (NAS) hinzuzufügen.

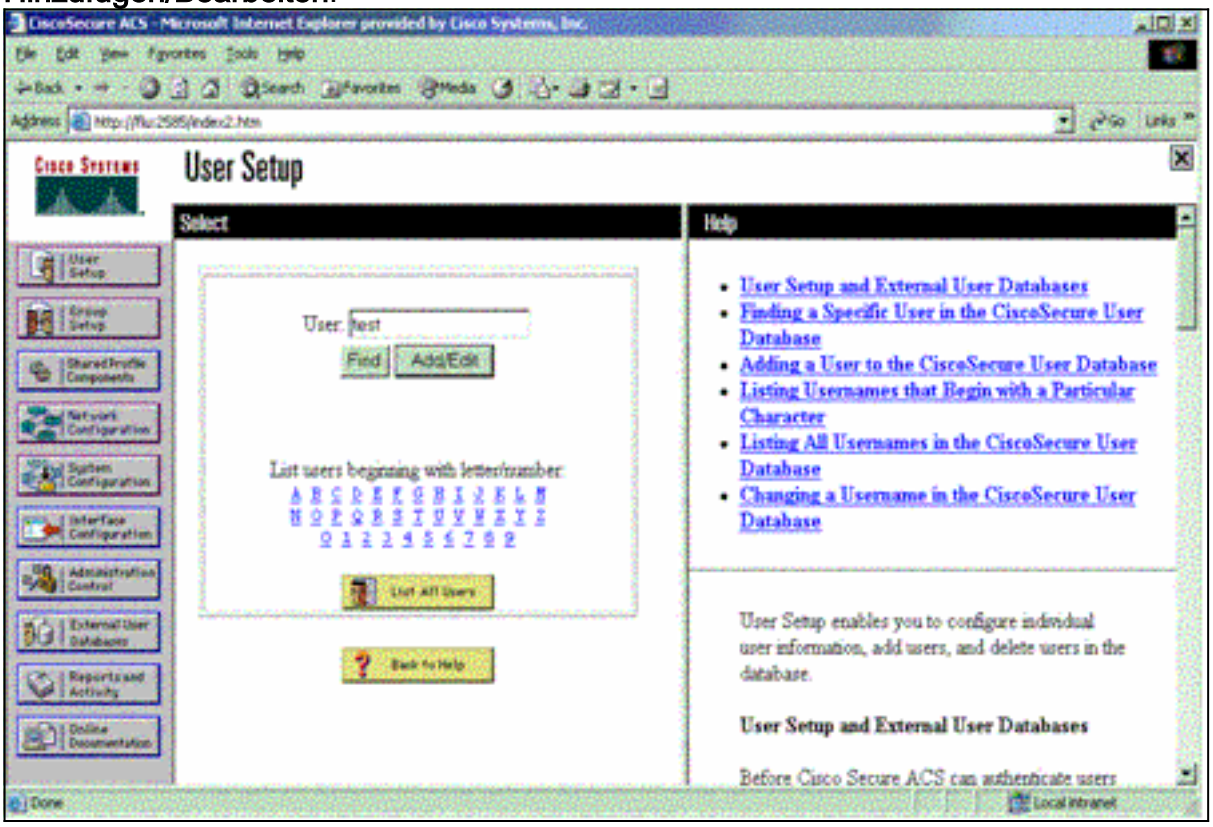


4. Geben Sie den Hostnamen, die IP-Adresse und den Schlüssel ein, der zur Verschlüsselung der Kommunikation zwischen dem AAA-Server und dem NAS verwendet wird. Wählen Sie als Authentifizierungsmethode **RADIUS (Cisco IOS/PIX)** aus. Wenn Sie fertig sind, klicken Sie auf **Senden +Neu starten**, um die Änderungen zu übernehmen.

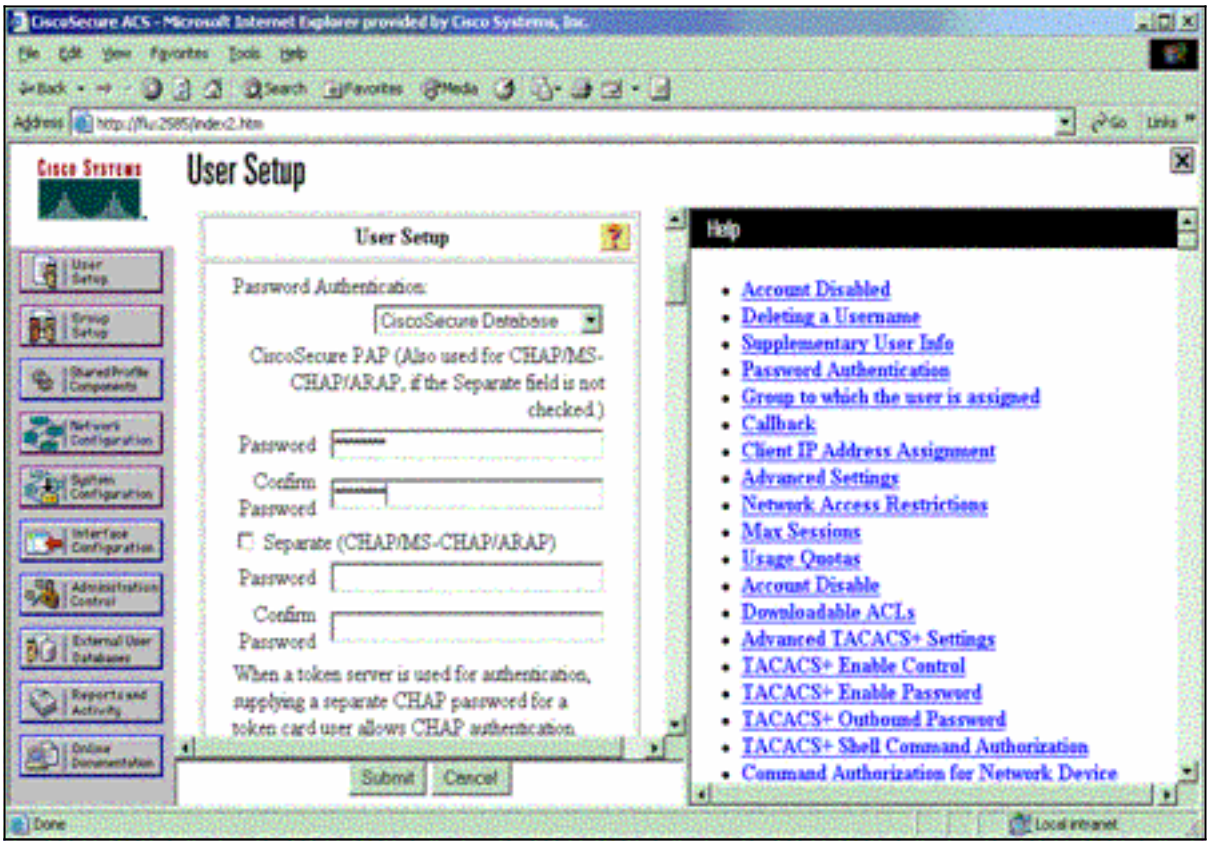


5. Klicken Sie auf **User Setup**, geben Sie eine Benutzer-ID ein, und klicken Sie auf

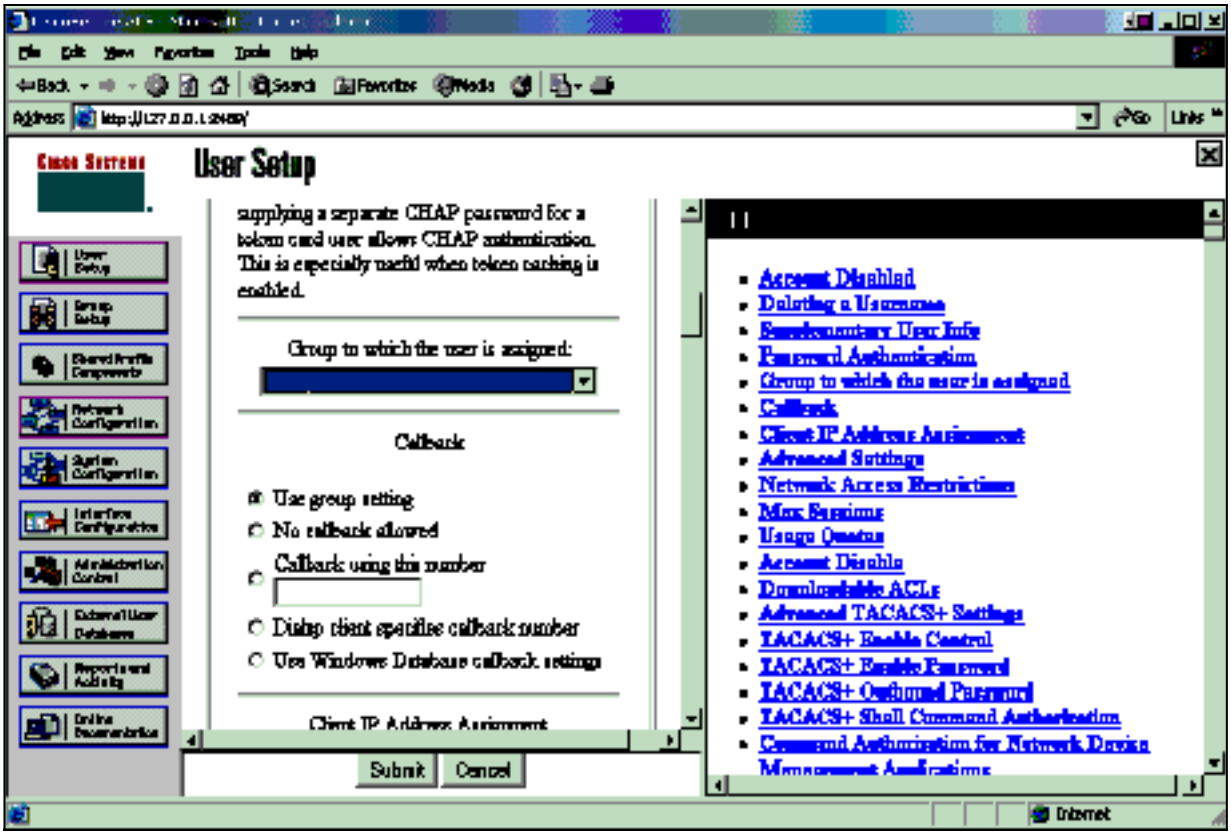
Hinzufügen/Bearbeiten.



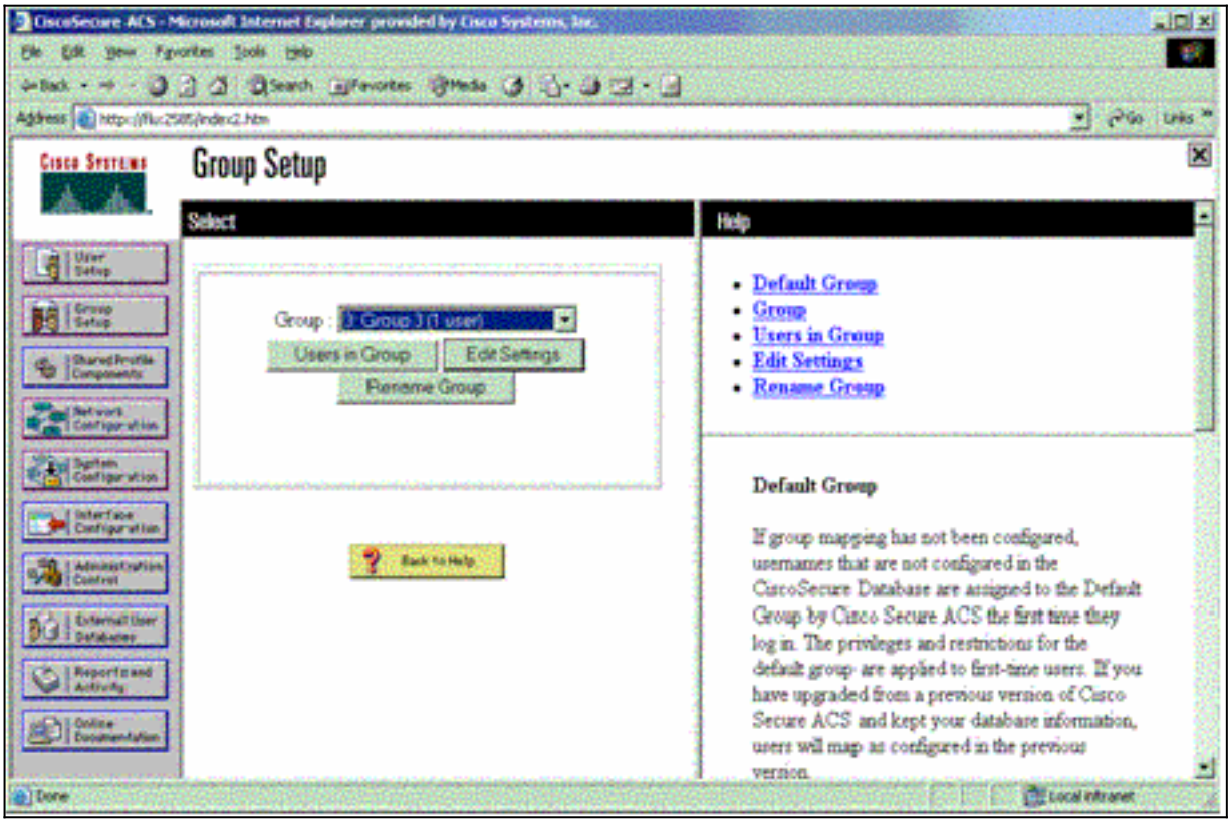
6. Wählen Sie eine Datenbank für die Benutzerauthentifizierung aus. (In diesem Beispiel ist der Benutzer "test" (Test), und die interne Datenbank des ACS wird für die Authentifizierung verwendet.) Geben Sie ein Kennwort für den Benutzer ein, und bestätigen Sie das Kennwort.



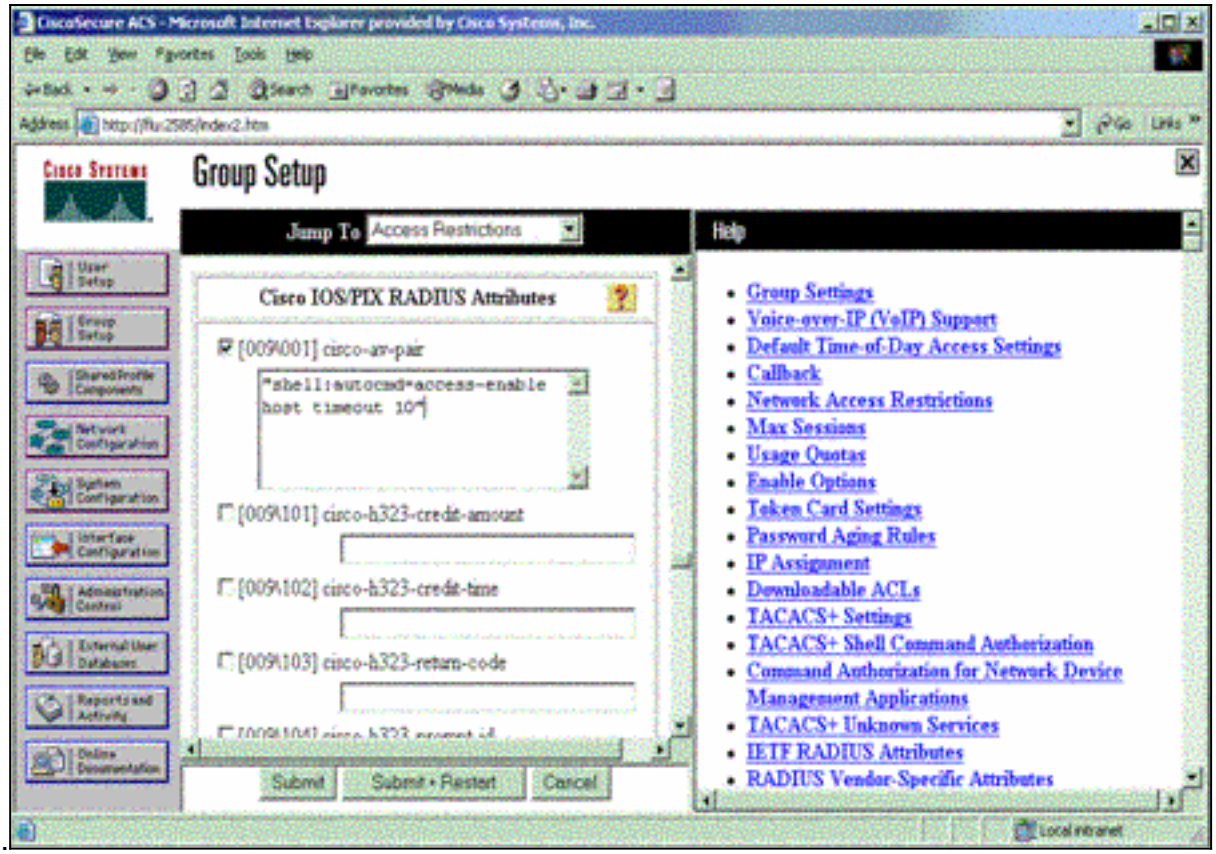
7. Wählen Sie die Gruppe aus, der der Benutzer zugewiesen ist, und aktivieren Sie die Option **Gruppeneinstellung verwenden**. Klicken Sie auf **Senden**.



8. Klicken Sie auf **Gruppeneinrichtung**, und wählen Sie die Gruppe aus, der der Benutzer im vorherigen Schritt zugewiesen wurde. Klicken Sie auf **Einstellungen bearbeiten**.



9. Blättern Sie nach unten zum Abschnitt Cisco IOS/PIX RADIUS Attributes (Cisco IOS/PIX RADIUS-Attribute). Aktivieren Sie das Kontrollkästchen für **cisco-av-pair**. Geben Sie den Befehl **shell** ein, der nach erfolgreicher Autorisierung des Benutzers ausgeführt werden soll. (In diesem Beispiel wird **shell:autocmd=access-enable host timeout 10** verwendet.) Klicken Sie auf **Senden+Neu**

starten. 

Fehlerbehebung bei RADIUS

Verwenden Sie diese **Debug-**Befehle auf dem NAS, um RADIUS-Probleme zu beheben.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug radius**: Zeigt Informationen an, die RADIUS zugeordnet sind.

Verwenden Sie diese Befehle, um AAA-Probleme zu beheben:

- **debug aaa authentication**: Zeigt Informationen zur AAA/TACACS+-Authentifizierung an.
- **debug aaa autorization**: Zeigt Informationen zur AAA/TACACS+-Autorisierung an.

Die Beispiel-**Debug-**Ausgabe hier zeigt einen erfolgreichen Authentifizierungs- und Autorisierungsprozess für den für RADIUS konfigurierten ACS.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=====================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
```

```
RADIUS:  AAA Unsupported     [152] 5
RADIUS:   74 74 79                        [tty]
RADIUS(00000003): Storing nasport 66 in rad_db
RADIUS/ENCODE(00000003): dropping service type,
  "radius-server attribute 6 on-for-login-auth" is off
RADIUS(00000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(00000003): acct_session_id: 1
RADIUS(00000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
  BE B5 07 BD E9 05 5B 5D
RADIUS:  User-Name           [1]   7   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port            [5]   6   66
RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
  Access-Accept, len 93
RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
  68 4B C3 FC 25 21 47 CD
RADIUS:  Vendor, Cisco       [26]  51
RADIUS:   Cisco AVpair       [1]   45
  "shell:autocmd=access-enable host timeout 10"
RADIUS:  Class               [25]  22
RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
RADIUS:   31 2F 36 36                  [1/66]
RADIUS(00000003): Received from id 21645/1
AAA/AUTHOR/EXEC(00000003): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Zugehörige Informationen

- Cisco IOS Lock-and-Key-Sicherheit
- Support-Seite für TACACS/TACACS+
- TACACS+ in der IOS-Dokumentation
- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems