# تكوين CSU ل UNIX (Solaris)

## المحتويات



## المقدمة

يساعد برنامج Cisco Secure ACS ل UNIX (CSU) في ضمان أمان الشبكة وتتبع نشاط الأشخاص الذين قاموا بالاتصال بالشبكة بنجاح. يعمل CSU كخادم TACACS+ أو RADIUS ويستخدم المصادقة والتخويل والمحاسبة (AAA) لتوفير أمان الشبكة.

تدعم CSU خيارات قاعدة البيانات هذه لتخزين ملفات تعريف المجموعات والمستخدمين ومعلومات المحاسبة:

- SQLAnywhere (مضمن مع CSU).لا يتوفر هذا الإصدار من Sybase SQLAnywhere على دعم العميل/الخادم. ومع ذلك، تم تحسينه لأداء خدمات AAA الأساسية مع CSU.**تحذير:** لا يدعم خيار قاعدة بيانات SQLAnywhere قواعد بيانات ملفات التعريف التي تتجاوز 5000 مستخدم، أو نسخ معلومات ملف التعريف المماثل بين مواقع قواعد البيانات، أو ميزة "إدارة جلسة عمل التوزيع الآمن (DSM) من Cisco".
- نظام إدارة قواعد البيانات الارتباطية Oracle أو RDBMS) Sybase).لدعم قواعد بيانات ملف التعريف الآمن من Cisco الخاصة ب 5000 مستخدم أو أكثر أو نسخ قاعدة البيانات المماثل أو ميزة DSM الآمنة من Cisco، يجب عليك التثبيت المسبق ل Oracle (الإصدار 7.3.2 أو 7.3.3 أو 8.0.3) أو Sybase SQL Server (الإصدار 11) RDBMS للاحتفاظ بمعلومات ملف التعريف الآمن من Cisco. يتطلب النسخ المتماثل لقاعدة البيانات المزيد من تكوين RDBMS بعد اكتمال تثبيت Cisco Secure.
- ترقية قاعدة بيانات موجودة من إصدار (x.2) سابق من CSU.إذا قمت بالترقية من إصدار x.2 سابق من Cisco Secure، فإن برنامج التثبيت الآمن من Cisco يقوم تلقائيا بترقية قاعدة بيانات ملف التعريف لكي تكون متوافقة مع CSU 2.3 ل UNIX.

- إستيراد قاعدة بيانات ملف تعريف موجودة.يمكنك تحويل قواعد بيانات ملف تعريف TACACS+ أو RADIUS الموجودة للبرامج المجانية أو الملفات المسطحة للاستخدام مع هذا الإصدار من CSU.

# المتطلبات الأساسية

## المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى ACS الآمن من Cisco 2.3 ل UNIX.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

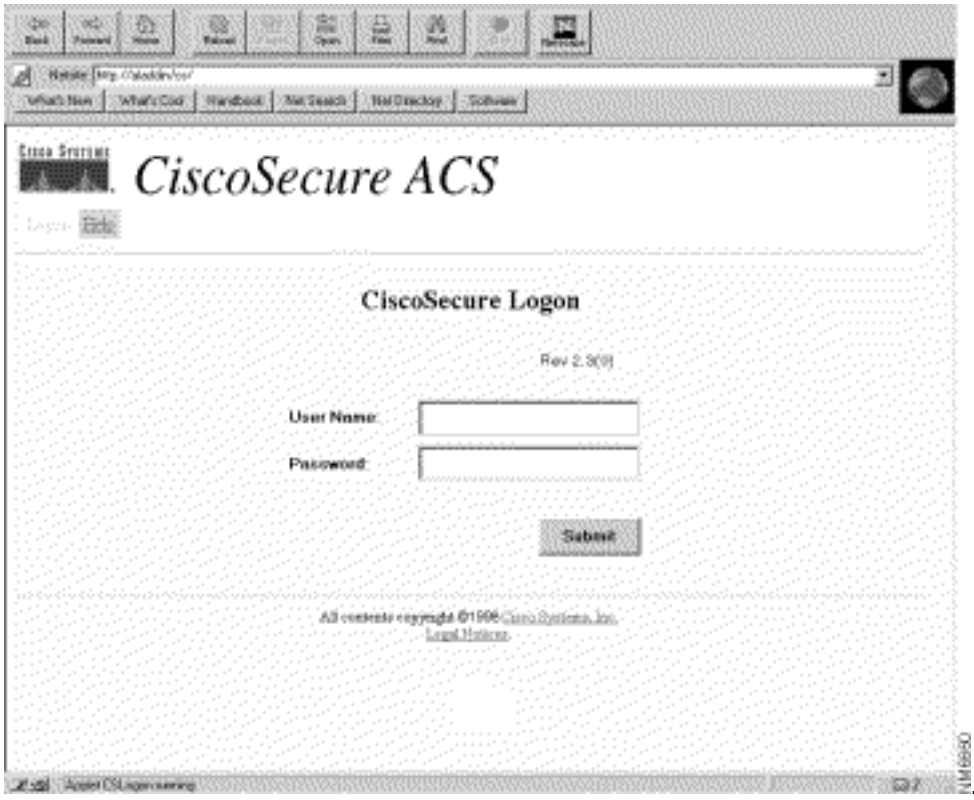
# تهيئة CSU

أستخدم هذه الإجراءات لتكوين CSU.

## بدء تشغيل واجهة المسؤول الآمنة من Cisco

أستخدم هذا الإجراء لتسجيل الدخول إلى المسؤول الآمن من Cisco.

1. من أي محطة عمل متصلة بويب إلى ACS، قم بتشغيل متصفح الويب الخاص بك.
2. أدخل أحد عناوين URL هذه لموقع Cisco Secure Administrator على الويب:في حالة عدم تمكين ميزة طبقة مأخذ توصيل الأمان على المستعرض الخاص بك، أدخل:
```
http://your_server/cs
```
حيث يكون اسم المضيف الخاص بك_server (أو اسم المجال المؤهل بالكامل (FQDN)، إذا كان اسم المضيف و FQDN يختلفان) الخاص ب SPARCstation حيث قمت بتثبيت CSU. يمكنك أيضا إستبدال عنوان IP الخاص ب SPARCstation ب_server الخاص بك.إذا تم تمكين ميزة طبقة مأخذ توصيل الأمان على المستعرض الخاص بك، فحدد "https" بدلا من "http" كبروتوكول إرسال النص التشعبي. إدخال:
```
https://your_server/cs
```
حيث يكون اسم المضيف (أو FQDN، إذا اختلف اسم المضيف و FQDN) الخاص ب SPARCstation حيث قمت بتثبيت CSU. يمكنك أيضا إستبدال عنوان IP الخاص ب SPARCstation ب_server الخاص بك.**ملاحظة:** عناوين URL وأسماء الخوادم حساسة لحالة الأحرف. يجب كتابتها بالحروف الكبيرة والحروف الصغيرة تماما كما هو موضح.يتم عرض صفحة تسجيل الدخول إلى




CSU.

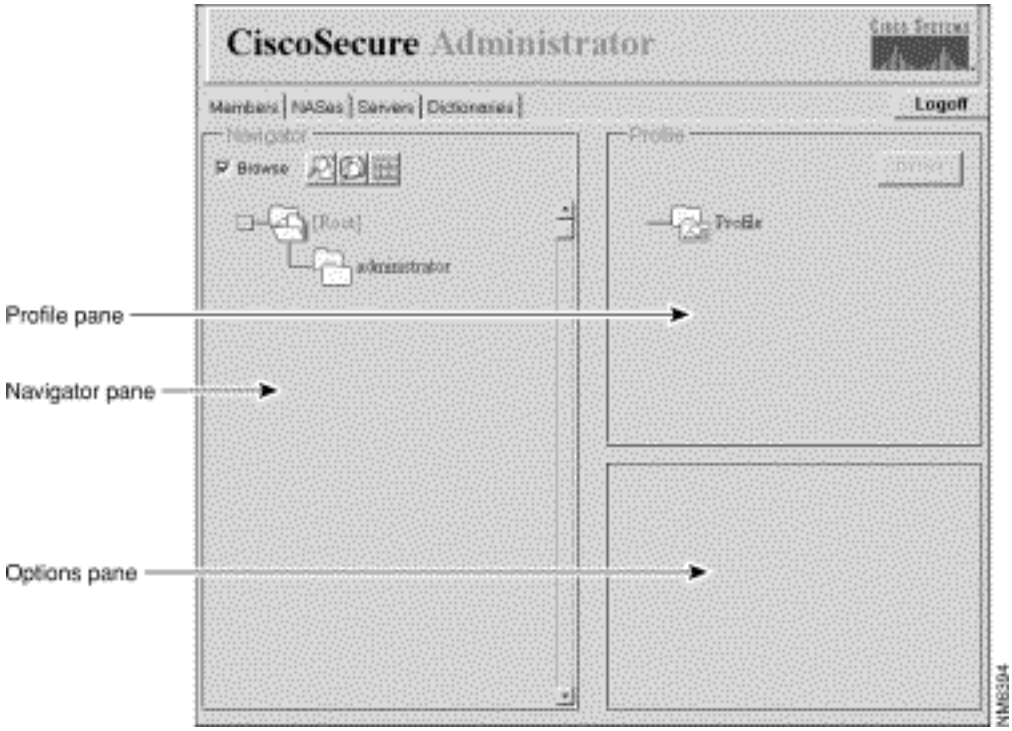
3. أدخل اسم المستخدم وكلمة المرور الخاصين بك. انقر على **إرسال**.**ملاحظة:** اسم المستخدم الافتراضي الأولي هو "مستخدم متميز." كلمة المرور الافتراضية الأولية هي "changeme". بعد تسجيل الدخول الأولي، يلزمك تغيير اسم المستخدم وكلمة المرور فورا للحصول على أقصى مستوى من الأمان.بعد تسجيل الدخول، يتم عرض الصفحة الرئيسية ل CSU مع شريط القائمة الرئيسي على طول الجزء العلوي. يتم عرض صفحة قائمة CSU الرئيسية فقط إذا قدم المستخدم اسم وكلمة مرور لهما امتيازات على مستوى المسؤول. إذا قدم المستخدم اسم وكلمة مرور لهما امتيازات على مستوى المستخدم فقط، يتم عرض شاشة


مختلفة.

## بدء برنامج التكوين المتقدم

بدء برنامج التكوين المتقدم للمسؤول الآمن من Cisco المستند إلى Java من أي من صفحات ويب مسؤول CSU. من شريط القوائم لواجهة ويب CSU، انقر فوق **خيارات متقدمة**، ثم انقر فوق **خيارات متقدمة** مرة أخرى.

يتم عرض برنامج التكوين المتقدم للمسؤول الآمن من Cisco. قد يستغرق التحميل بضع دقائق.

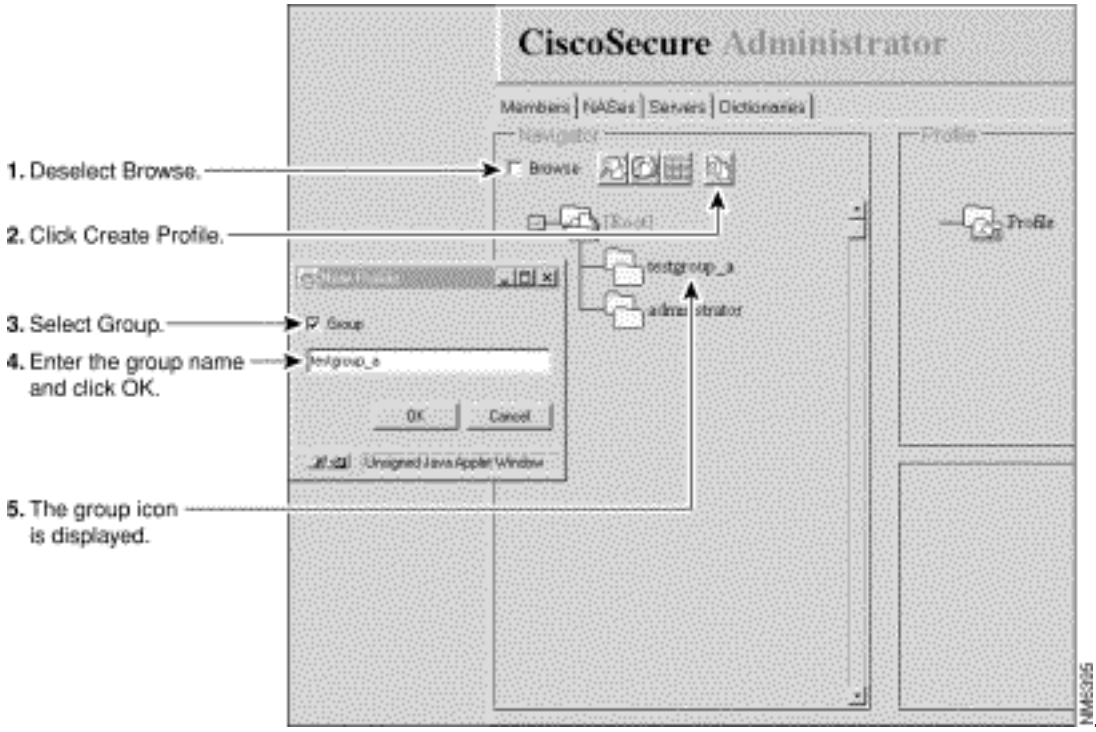



## إنشاء ملف تعريف مجموعة

أستخدم برنامج التكوين المتقدم للمسؤول الآمن من Cisco لإنشاء توصيفات المجموعات وتكوينها. توصي Cisco بإنشاء ملفات تعريف مجموعة لتكوين متطلبات AAA التفصيلية لأعداد كبيرة من المستخدمين المماثلين. بعد تحديد ملف تعريف المجموعة، أستخدم CSU إضافة صفحة ويب مستخدم لإضافة ملفات تعريف المستخدم إلى ملف تعريف المجموعة بسرعة. تنطبق المتطلبات المتقدمة التي تم تكوينها للمجموعة على كل مستخدم عضو.

أستخدم هذا الإجراء لإنشاء ملف تعريف مجموعة.

1. في برنامج التكوين المتقدم للمسؤول الآمن من Cisco، حدد علامة التبويب **أعضاء**. في لوحة المتصفح، قم بإلغاء تحديد خانة الاختيار **تصفح**. تظهر أيقونة إنشاء توصيف جديد.
2. في لوحة المتصفح، قم بتنفيذ واحد مما يلي :لإنشاء ملف تعريف مجموعة بدون أصل، حدد مكان وانقر أيقونة المجلد **[جذر]**.لإنشاء ملف تخصيص مجموعتك على هيئة فرع لملف تخصيص مجموعة أخرى، حدد مكان المجموعة التي تريد أن تكون الأصل وانقر عليها.إذا كانت المجموعة التي تريد أن تكون المجموعة الأصل هي مجموعة فرعية، فانقر فوق مجلد المجموعة الأصلية لعرضها.
3. انقر على **إنشاء توصيف جديد**. تظهر شاشة ملف تخصيص جديد.
4. حدد خانة الاختيار **مجموعة**، واكتب اسم المجموعة التي تريد إنشائها، وانقر **موافق**. تظهر المجموعة الجديدة في الشجرة.
5. بعد إنشاء ملف تعريف المجموعة، قم بتعيين سمات TACACS+ أو RADIUS لتكوين خصائص AAA



معينة.

## إنشاء ملف تعريف مستخدم في وضع التكوين المتقدم

أستخدم وضع التكوين المتقدم للمسؤول الآمن من Cisco لإنشاء ملف تعريف مستخدم وتكوينه. يمكنك القيام بذلك لتخصيص السمات المتعلقة بالتخويل والمحاسبة لملف تعريف المستخدم بتفاصيل أكثر من الممكن باستخدام صفحة إضافة مستخدم.

أستخدم هذا الإجراء لإنشاء ملف تعريف مستخدم:

1. في برنامج التكوين المتقدم للمسؤول الآمن من Cisco، حدد علامة التبويب **أعضاء**. في لوحة المتصفح، حدد مكان وقم بإلغاء تحديد **تصفح**. تظهر أيقونة إنشاء توصيف جديد.
2. في لوحة المتصفح، قم بتنفيذ واحد مما يلي :حدد موقع المجموعة التي ينتمي إليها المستخدم وانقر فوقها.إذا كنت لا تريد أن ينتمي المستخدم إلى مجموعة، انقر فوق أيقونة المجلد **[الجذر]**.
3. انقر على **إنشاء توصيف**. تظهر شاشة ملف تخصيص جديد.
4. تأكد من عدم تحديد خانة الاختيار **مجموعة**.
5. أدخل اسم المستخدم الذي تريد إنشاءه ثم انقر فوق **موافق**. يظهر المستخدم الجديد في الشجرة.
6. بعد إنشاء ملف تعريف المستخدم، قم بتعيين سمات TACACS+ أو RADIUS معينة لتكوين خصائص AAA معينة:لتعيين توصيفات TACACS+ إلى ملف تعريف المستخدم، راجع تعيين سمات TACACS+ إلى مجموعة أو ملف تعريف مستخدم.لتعيين توصيفات RADIUS لتوصيف المستخدم، راجع تعيين سمات RADIUS لمجموعة أو لتوصيف مستخدم.

## إستراتيجيات لتطبيق السمات

أستخدم ميزة ملف تعريف مجموعة CSU وسمات TACACS+ و RADIUS لتنفيذ المصادقة والتفويض لمستخدمي الشبكة من خلال CSU.

### تخطيط السمات للمجموعات والمستخدمين

تتيح لك ميزة ملف تعريف مجموعة CSU تحديد مجموعة مشتركة من متطلبات AAA لعدد كبير من المستخدمين.

يمكنك تعيين مجموعة من قيم سمات TACACS+ أو RADIUS لملف تعريف مجموعة. تنطبق قيم السمات هذه التي

تم تعيينها إلى المجموعة على أي مستخدم عضو أو تمت إضافته كعضو في هذه المجموعة.

## إستخدام ميزة ملف تعريف المجموعة بشكل فعال

لتكوين CSU لإدارة أعداد كبيرة وأنواع مختلفة من المستخدمين ذوي متطلبات AAA المعقدة، توصي Cisco باستخدام ميزات برنامج التكوين المتقدم للمسؤول الآمن من Cisco لإنشاء ملفات تعريف المجموعة وتكوينها.

يجب أن يحتوي ملف تعريف المجموعة على كافة السمات غير الخاصة بالمستخدم. هذا يعني كل السمات عادة ماعدا كلمة المرور. يمكنك بعد ذلك إستخدام صفحة إضافة مستخدم لمسؤول Cisco الآمن لإنشاء ملفات تعريف مستخدم بسيطة بسمات كلمة المرور وتعيين ملفات تعريف المستخدمين هذه إلى ملف تعريف المجموعة المناسب. ثم يتم تطبيق الميزات وقيم السمات المحددة لمجموعة معينة على المستخدمين الأعضاء بها.

## المجموعات الأصل والمجموعات التابعة

يمكنك إنشاء تسلسل هرمي من المجموعات. ضمن ملف تخصيص مجموعة، يمكنك إنشاء ملفات تخصيص مجموعة فرعية. قيم السمات المعينة لملف تعريف المجموعة الأصل هي قيم افتراضية لتوصيفات المجموعة الفرعية.

## إدارة مستوى المجموعة

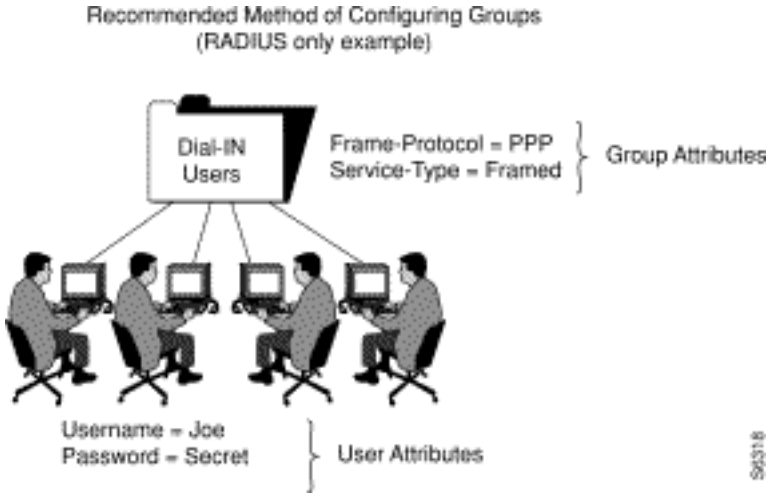
يمكن لمسؤول النظام الآمن من Cisco تعيين حالة مسؤول مجموعة المستخدمين الآمنة الفردية من Cisco. تمكن حالة "مسؤول المجموعة" المستخدمين الأفراد من إدارة أي ملفات تعريف تابعة لمجموعة فرعية وملفات تعريف مستخدم تابعة لمجموعتهم. ومع ذلك، فإنه لا يسمح لهم بإدارة أي مجموعات أو مستخدمين يقعون خارج التسلسل الهيكلي لمجموعاتهم. وبالتالي، فإن مدير النظام يوزع مهمة إدارة شبكة كبيرة على الأفراد الآخرين دون منح كل منهم سلطة متساوية.

## ما هي السمات التي أعرفها للمستخدمين المنفردين؟

توصي Cisco بتعيين قيم سمة المصادقة الأساسية للمستخدمين الفرديين التي تكون فريدة للمستخدم، مثل السمات التي تعرف اسم المستخدم وكلمة المرور ونوع كلمة المرور وامتياز الويب. قم بتعيين قيم سمات المصادقة الأساسية للمستخدمين من خلال تحرير مستخدم من قبل CSU أو إضافة صفحات مستخدم.

## ما هي السمات التي أعرفها لتوصيفات المجموعة؟

توصي Cisco بتحديد السمات المرتبطة بالتأهيل والتخويل والمحاسبة على مستوى المجموعة.



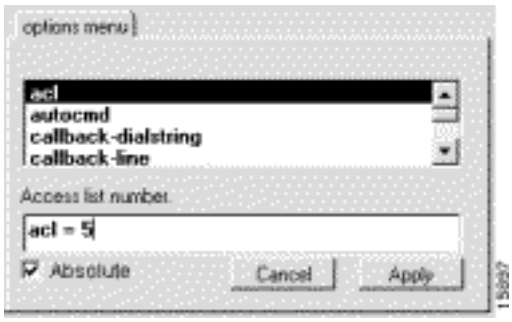

في هذا المثال، يتم تعيين ملف تعريف المجموعة المسمى "مستخدمو الطلب الهاتفي" إلى أزواج قيم السمة frame-protocol=ppp و service-type=framed.

## ما هي الصفات المطلقة؟

يمكن تعيين حالة مطلقة لمجموعة فرعية من سمات TACACS+ و RADIUS في CSU على مستوى ملف تعريف المجموعة. قيمة السمة الممكنة للحالة المطلقة على مستوى ملف تعريف المجموعة تتخطى أي قيم سمات متعارضة في ملف تعريف مجموعة فرعية أو مستوى ملف تعريف مستخدم عضو.

في الشبكات متعددة المستويات ذات المستويات المتعددة من مسؤولي المجموعة، تمكن السمات المطلقة مسؤول النظام من تعيين قيم سمات المجموعة المحددة التي لا يمكن لمسؤولي المجموعة في المستويات الأدنى تجاوزها.

تعرض السمات التي يمكن تعيين حالة مطلقة خانة إختيار Absolute في مربع سمات برنامج التكوين المتقدم للمسؤول الآمن من Cisco. حدد خانة الاختيار لتمكين الحالة المطلقة.




## هل يمكن أن تتعارض قيم سمة المجموعة مع قيم سمة المستخدم؟

يعتمد حل التعارض بين قيم السمات المعينة لملفات تعريف المجموعة الأصلية وملفات تعريف المجموعات الفرعية وملفات تعريف المستخدمين الأعضاء على ما إذا كانت قيم السمات مطلقة وما إذا كانت سمات TACACS+ أو RADIUS:

- تتجاوز قيم سمة TACACS+ أو RADIUS المعينة لملف تعريف مجموعة بحالة مطلقة أي قيم سمة متنازعة تم تعيينها على مستوى مجموعة فرعية أو ملف تعريف مستخدم.
- إذا لم يتم تمكين الحالة المطلقة لقيمة سمة TACACS+ على مستوى ملف تعريف المجموعة، يتم تجاوزها بأي قيمة سمة متنازعة يتم تعيينها على مستوى مجموعة فرعية أو ملف تعريف مستخدم.
- إذا لم يتم تمكين الحالة المطلقة لقيمة سمة RADIUS على مستوى المجموعة الأصل، فإن أي قيم سمة متنازعة تم تعيينها في مجموعة فرعية ينتج عنها نتيجة غير متوقعة. عندما تقوم بتعريف قيم سمات RADIUS لمجموعة ما ومستخدميها الأعضاء، تجنب تعيين نفس السمة لكل من توصيفات المستخدم والمجموعة.

## إستخدام خياري الحظر والسماح

بالنسبة إلى TACACS+، قم بتجاوز توفر قيم الخدمة الموروثة عن طريق التحديد المسبق للكلمة الأساسية **منع** أو **السماح** بمواصفات الخدمة. تسمح الكلمة الأساسية **السماح** بالخدمات المحددة. لا تسمح الكلمة الأساسية **ban** بالخدمات المحددة. مع إستخدام هذه الكلمات الأساسية معا، يمكنك إنشاء تكوينات "كل شيء ماعدا". على سبيل المثال، يتيح هذا التكوين الوصول من جميع الخدمات باستثناء X.25:

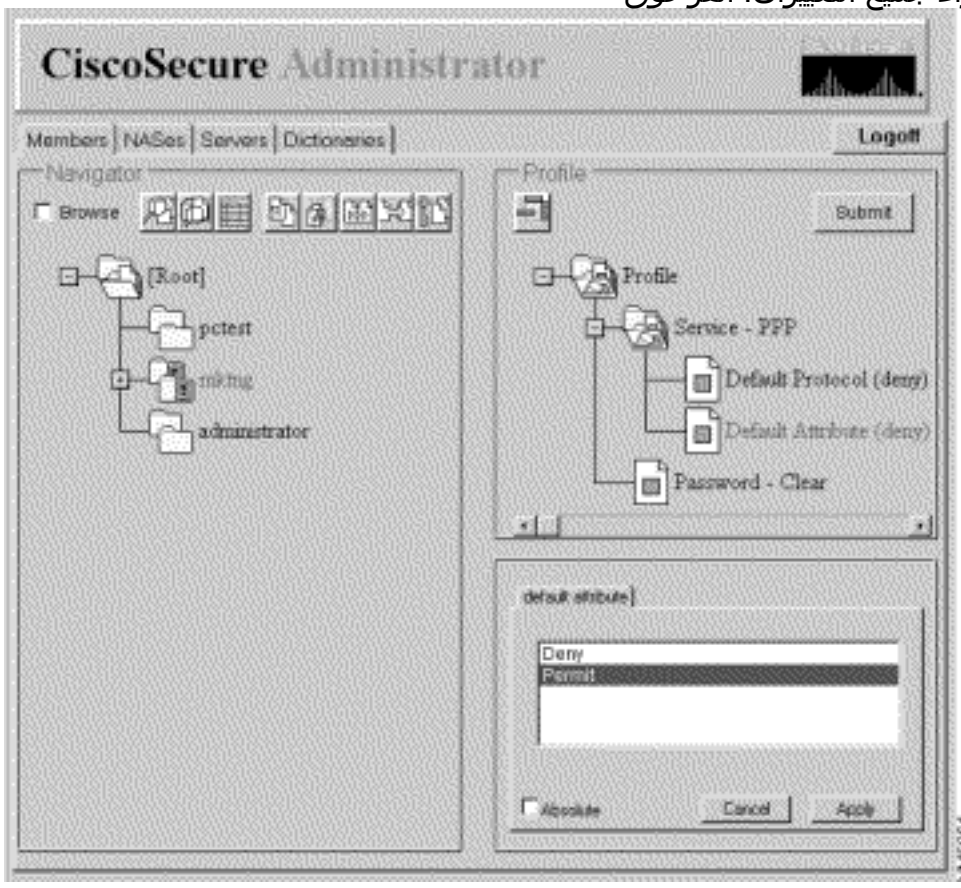
```
default service = permit
  prohibit service = x25
```

## تعيين سمات TACACS+ إلى مجموعة أو ملف تعريف مستخدم

لتعيين خدمات وسمات TACACS+ معينة على مجموعة أو ملف تعريف مستخدم، اتبع الخطوات التالية :

1. في برنامج التكوين المتقدم للمسؤول الآمن من Cisco، حدد علامة التبويب **أعضاء**. في لوحة المتصفح، انقر

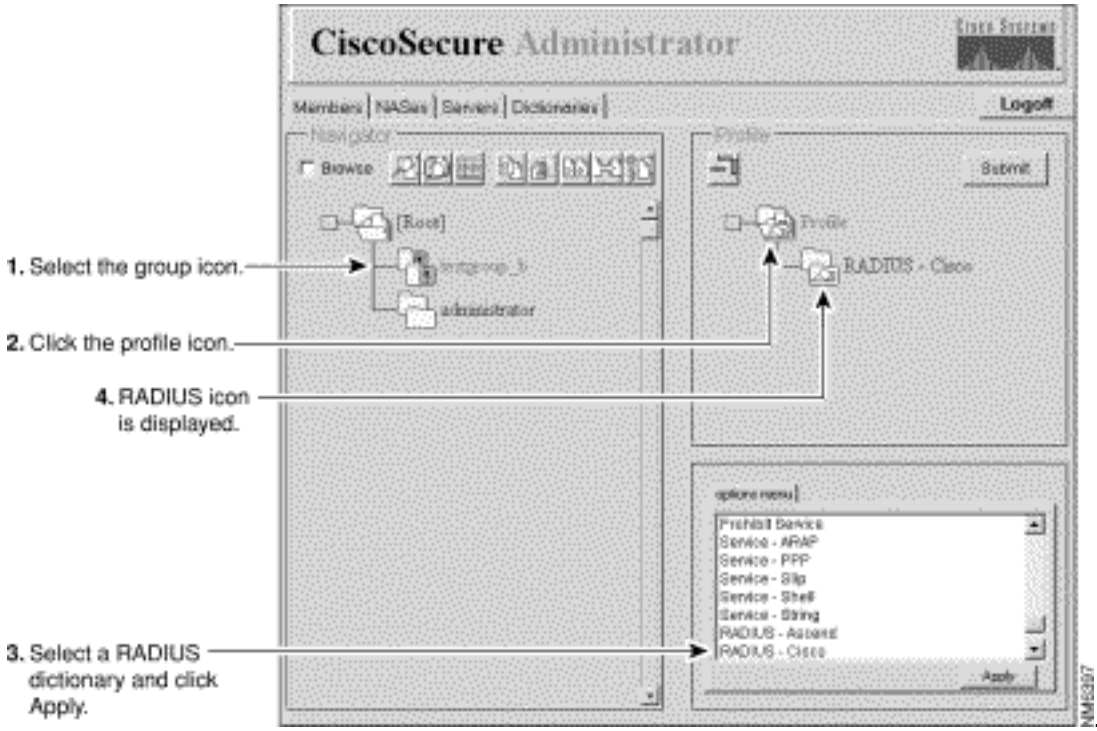
أيقونة المجموعة أو ملف تعريف المستخدم التي يتم تعيين سمات TACACS+ لها.
2. إذا كان ضروريا، في لوحة ملف التخصيص، انقر أيقونة **ملف التخصيص** لتمديده.قائمة أو شاشة تحتوي على سمات تنطبق على ملف التخصيص المحدد أو عروض الخدمة المحددة في النافذة في أسفل يمين الشاشة. تتغير المعلومات الواردة في هذا الإطار بناء على التوصيف أو الخدمة التي تحددها في لوحة التوصيف.
3. انقر فوق الخدمة أو البروتوكول الذي تريد إضافته ثم انقر فوق **تطبيق**. وتتم إضافة الخدمة إلى ملف التعريف.
4. أدخل النص اللازم أو حدده في نافذة السمة.يتم شرح الإدخالات الصحيحة في قسم إستراتيجيات تطبيق السمات في CSU 2.3 للدليل المرجعي UNIX.**ملاحظة:** إذا قمت بتعيين قيمة سمة على مستوى ملف تعريف المجموعة، وتقوم السمة التي تحددها بعرض خانة الاختيار **Absolute**، فحدد خانة الاختيار هذه لتعيين حالة القيمة المطلقة. لا يمكن تجاوز الحالة المطلقة المعينة بالقيمة بأي قيم متناظرة معينة عند مستويات ملف تعريف المجموعة الفرعية أو ملف تعريف المستخدم.
5. كرر الخطوات من 1 إلى 1 لكل خدمة أو بروتوكول إضافي تحتاج إلى إضافته.
6. عند إجراء جميع التغييرات، انقر فوق **إرسال**.




## تعيين خصائص RADIUS لمجموعة أو ملف تخصيص مستخدم

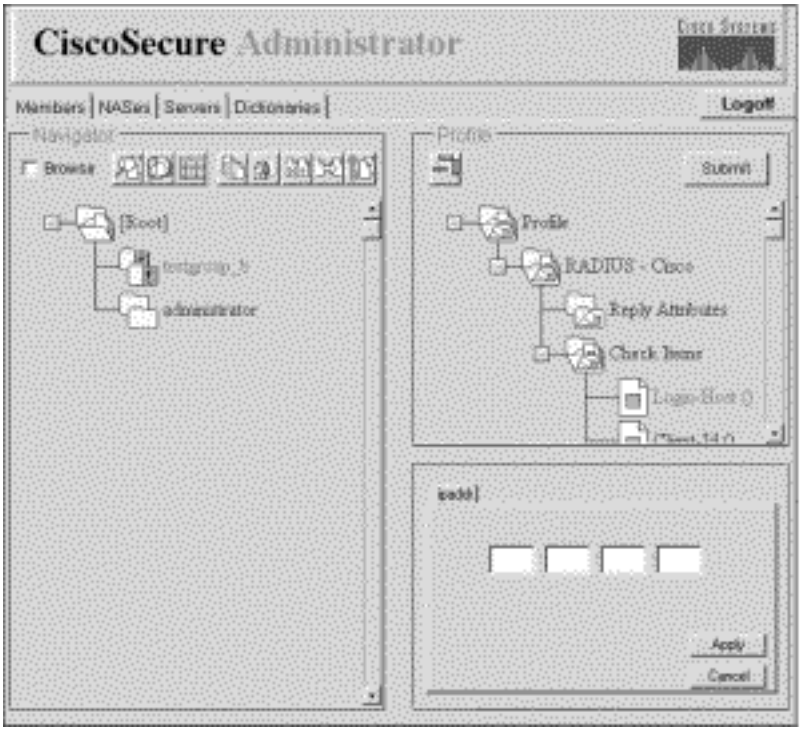
لتعيين سمات RADIUS معينة على مجموعة أو توصيف مستخدم:

1. تعيين قاموس RADIUS لملف تخصيص المجموعة:في صفحة الأعضاء ببرنامج التكوين المتقدم للمسؤول الآمن من Cisco، انقر على أيقونة **المجموعة** أو **المستخدم**، ثم انقر على أيقونة **التوصيف** في جزء التوصيفات. في لوحة الخصائص، تعرض قائمة الخيارات.في قائمة **الخيارات**، انقر اسم قاموس RADIUS الذي تريد أن تستخدمه المجموعة أو المستخدم. (على سبيل المثال، RADIUS - Cisco.) طقطقة




**يطبق**.

2. قم بإضافة عناصر التحقق المطلوبة وسمات الرد إلى ملف تخصيص RADIUS:**ملاحظة:** التحقق من أن العناصر هي سمات مطلوبة للمصادقة، مثل معرف المستخدم وكلمة المرور. سمات الرد هي سمات مرسلة إلى خادم الوصول إلى الشبكة (NAS) بعد أن اجتاز التوصيف إجراء المصادقة، مثل البروتوكول المؤطر. للقوائم والتفسيرات الخاصة بعناصر التأشير وسمات الرد، راجع أزواج قيمة سمة RADIUS وإدارة القاموس في CSU 2.3 للدليل المرجعي UNIX.في نافذة ملف التخصيص، انقر أيقونة مجلد RADIUS - DICTIONARYNAME. (من المحتمل أن تحتاج لنقر علامة + ملف التخصيص لتوسيع مجلد RADIUS.) تظهر خيارات التحقق من العناصر وسمات الرد في نافذة مجموعة السمات.لاستخدام واحدة أو أكثر من هذه السمات، انقر فوق السمة (السمات) التي تريد إستخدامها، ثم انقر فوق **تطبيق**. يمكنك إضافة أكثر من سمة في كل مرة.انقر فوق **+** رمز ل RADIUS - اسم المقطع لتوسيع المجلد.**ملاحظة:** إذا قمت بتحديد خيار RADIUS-Cisco11.3، فتأكد من تثبيت الإصدار 11.3.3(T) من برنامج Cisco IOS® Software أو إصدار أحدث على وحدات التخزين المتصلة بالشبكة (NAS) لديك وإضافة خطوط أوامر جديدة إلى تكوينات NAS. أحلت ال يمكن بالكامل ال -RADIUS Cisco11.3 قاموس في ال CSU 2.3 ل UNIX مرجع مرشد.
3. قم بتعيين قيم لعناصر التأشير المضافة وسمات الرد:**تحذير:** بالنسبة لبروتوكول RADIUS، يعد التوريث إضافة بدلا من التراتبي. (يستخدم بروتوكول TACACS+ التوريث الهرمي). على سبيل المثال، إذا قمت بتعيين نفس سمات الرد على كل من ملفات تعريف المستخدم والمجموعة، يفشل التفويض لأن NAS يستلم ضعف عدد السمات. إنه لا يفهم سمات الرد. لا تقم بتعيين نفس عنصر الشيك أو سمة الرد لكل من ملفات تعريف المجموعة والمستخدمين.انقر فوق **التحقق من العناصر** أو **سمات الرد**، أو انقر فوق كليهما. تظهر قائمة بقيم عناصر التحقق وسمات الرد القابلة للتطبيق في الإطار الأيمن السفلي. انقر فوق **+** الرمز لتوسيع المجلد.انقر فوق القيم التي تريد تعيينها، ثم انقر فوق **تطبيق**. لمزيد من المعلومات عن القيم، ارجع إلى أزواج قيمة سمة RADIUS وإدارة القاموس في CSU 2.3 للدليل المرجعي UNIX.**ملاحظة:** إذا قمت بتعيين قيمة سمة على مستوى ملف تعريف المجموعة، وتقوم السمة التي تحددها بعرض خانة الاختيار Absolute، فحدد خانة الاختيار هذه لتعيين حالة القيمة المطلقة. لا يمكن تجاوز القيمة المعينة للحالة المطلقة بأي قيم متناظرة معينة في ملف تعريف المجموعة الفرعية أو مستويات ملف تعريف المستخدم.عند الانتهاء من إجراء التغييرات، انقر فوق




**إرسال**.

4. لاستخدام واحدة أو أكثر من هذه السمات، انقر فوق السمة (السمات) التي تريد إستخدامها، ثم انقر فوق **تطبيق**. يمكنك تطبيق أكثر من سمة في كل مرة.

## تعيين مستويات امتياز التحكم بالوصول

يستخدم مسؤول المستخدم المتميز سمة امتياز الويب لتعيين مستوى من امتياز التحكم في الوصول إلى مستخدمي Cisco الآمن.

1. في برنامج "التكوين المتقدم للمسؤول الآمن من Cisco"، انقر على المستخدم الذي تريد تعيين امتياز التحكم في الوصول الخاص به، ثم انقر على أيقونة التوصيف في جزء التوصيفات.
2. في قائمة الخيارات، انقر **امتياز ويب** وحدد واحد من تلك القيم.**0** - ترفض المستخدم أي امتيازات للتحكم في الوصول تتضمن القدرة على تغيير كلمة مرور Cisco Secure الخاصة بالمستخدم.**1** - يمنح المستخدم حق الوصول إلى صفحة الويب الخاصة ب CSUser. يتيح هذا للمستخدمين الأمنين من Cisco تغيير كلمات المرور الآمنة من Cisco الخاصة بهم. للحصول على تفاصيل حول كيفية تغيير كلمات المرور، ارجع إلى الوظائف على مستوى المستخدم (تغيير كلمة المرور) في الإدارة البسيطة للمستخدم و ACS.**12** - يمنح امتيازات مسؤول مجموعة المستخدمين.**15** - تمنح امتيازات مسؤول نظام المستخدم.**ملاحظة:** إذا قمت بتحديد أي خيار امتياز ويب غير 0، فيجب عليك أيضا تحديد كلمة مرور. لإرضاء متطلب كلمة مرور امتياز الويب، يكون مسافة فارغة مفردة مقبول إلى أدنى حد.

## بدء CSU وإيقافها

عادة، تبدأ وحدة التحكم في الوصول عن بعد (CSU) تلقائيا عند بدء تشغيل محطة SPARCstation التي تم تثبيتها بها أو إعادة تشغيلها. ومع ذلك، يمكنك بدء تشغيل CSU يدويا، أو إيقاف تشغيله بدون إيقاف تشغيل SPARCStation بالكامل.

سجل الدخول ك [Root] إلى SPARCStation حيث قمت بتثبيت CSU.

لبدء CSU يدويا، اكتب:

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

لإيقاف CSU يدويا، اكتب:

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

## التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم UNIX
- صفحة دعم TACACS+
- صفحة دعم RADIUS
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).