Configuring CSU for UNIX (Solaris)

Document ID: 13842

Contents

Introduction

Cisco Secure ACS for UNIX (CSU) software helps to ensure the security of the network and tracks the activity of people who successfully connect to the network. CSU acts as a TACACS+ or RADIUS server and uses authentication, authorization, and accounting (AAA) to provide network security.

CSU supports these database options to store group and user profiles and accounting information:

- SQLAnywhere (included with CSU).

  This version of Sybase SQLAnywhere does not have client/server support. However, it is optimized to perform essential AAA services with CSU.

  ⚠ **Caution:** The SQLAnywhere database option does not support profile databases that exceed 5,000 users, replication of profile information among database sites, or the Cisco Secure Distribute Session Manager (DSM) feature.
- Oracle or Sybase Relational Database Management System (RDBMS).

  To support Cisco Secure profile databases of 5,000 or more users, database replication, or the Cisco Secure DSM feature, you must pre−install an Oracle (version 7.3.2, 7.3.3, or 8.0.3) or Sybase SQL server (version 11) RDBMS to hold your Cisco Secure profile information. Database replication requires further RDBMS configuration after the Cisco Secure installation is complete.
- The upgrade of an existing database from a previous (2.x) version of CSU.

  If you upgrade from an earlier 2.x version of Cisco Secure, the Cisco Secure installation program automatically upgrades the profile database to be compatible with CSU 2.3 for UNIX.

- Importing an existing Profile database.

  You can convert existing freeware TACACS+ or RADIUS profile databases or flat files for use with this version of the CSU.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Secure ACS 2.3 for UNIX.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

CSU Configuration

Use these procedures to configure CSU.

Start the Cisco Secure Administrator Interface

Use this procedure to log in to the Cisco Secure Administrator.

1. From any workstation with a web connection to the ACS, launch your web browser.
2. Enter one of these URLs for the Cisco Secure Administrator web site:

   - If the security socket layer feature on your browser is not enabled, enter:

     ```
     http://your_server/cs
     ```

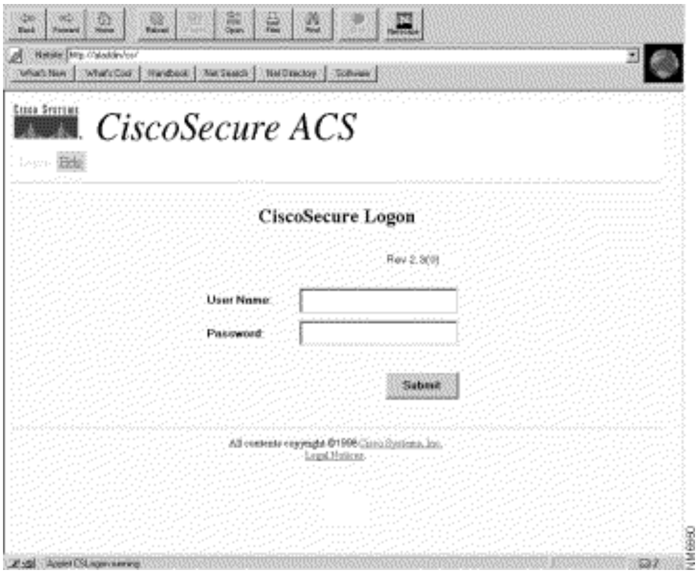
     where your_server is the host name (or the fully qualified domain name (FQDN), if host name and FQDN differ) of the SPARCstation where you installed CSU. You can also substitute the SPARCstation's IP address for your_server.
   - If the security socket layer feature on your browser is enabled, specify "https" rather than "http" as the hypertext transmission protocol. Enter:

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

     where your_server is the host name (or the FQDN, if host name and FQDN differ) of the SPARCstation where you installed CSU. You can also substitute the SPARCstation's IP address for your_server.

     Note: URLs and server names are case−sensitive. They must be typed with uppercase and lowercase letters exactly as shown.

The CSU Logon page is displayed.



CiscoSecure ACS

CiscoSecure Logon

Rev 2.3(0)

User Name:

Password:

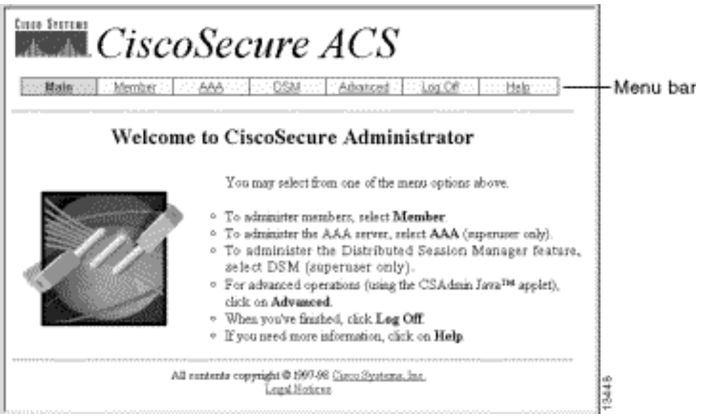
Submit

All contents copyright ©1998 Cisco Systems, Inc.
Legal Notices.

3. Enter your username and password. Click **Submit**.

   Note: The initial default username is "superuser." The initial default password is "changeme." After your initial login, you need to change the username and password immediately for maximum security.

   After you log in, the CSU main page is displayed with the main menu bar along the top. The CSU Main menu page is displayed only if the user provides a name and password that have administrator−level privileges. If the user provides a name and password that have only user−level privileges, then a different screen is displayed.



CiscoSecure ACS

Welcome to CiscoSecure Administrator

You may select from one of the menu options above.

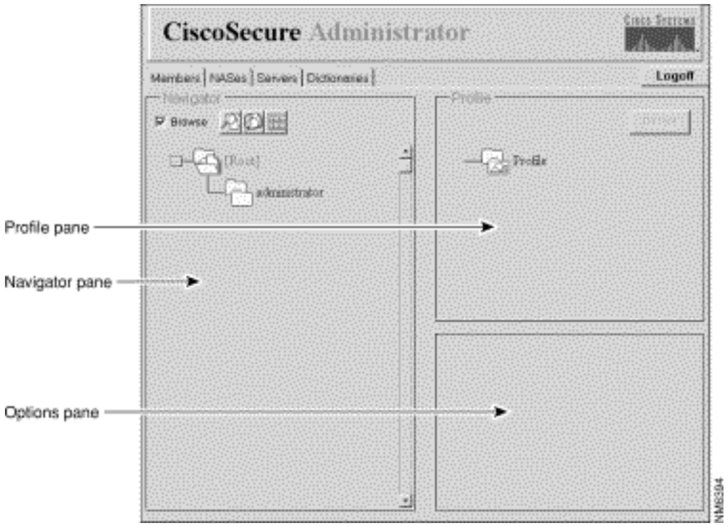
- To administer members, select **Member**.
- To administer the AAA server, select **AAA** (superuser only).
- To administer the Distributed Session Manager feature, select DSM (superuser only).
- For advanced operations (using the CSAdmin Java™ applet), click on **Advanced**.
- When you've finished, click **Log Off**.
- If you need more information, click on **Help**.

All contents copyright © 1997-98 Cisco Systems, Inc.
Legal Notices

Start the Advanced Configuration Program

Start the Java−based Cisco Secure Administrator Advanced Configuration program from any of the CSU Administrator web pages. From the menu bar of the CSU web interface, click **Advanced**, and then click **Advanced** again.

The Cisco Secure Administrator Advanced Configuration program is displayed. It might possibly take a few minutes to load.

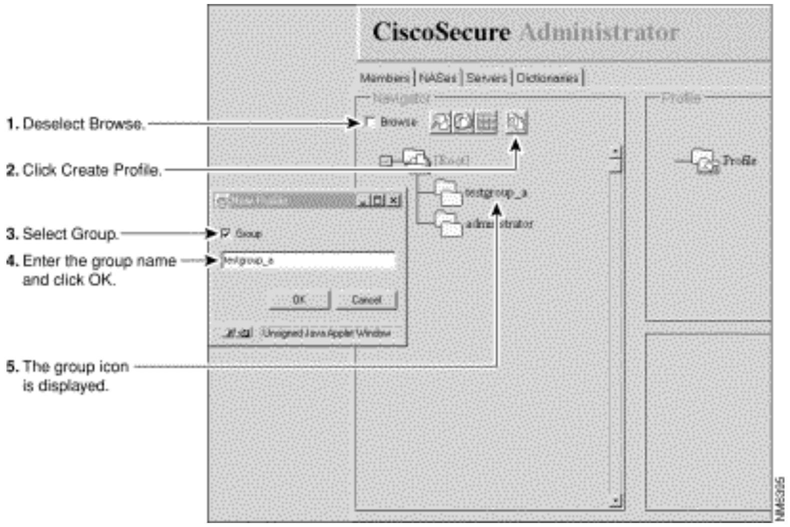


Create a Group Profile

Use the Cisco Secure Administrator Advanced Configuration program to create and configure group profiles. Cisco recommends that you create group profiles to configure detailed AAA requirements for large numbers of similar users. After the group profile is defined, use the CSU Add a User web page to quickly add user profiles to the group profile. The advanced requirements configured for the group apply to each member user.

Use this procedure to create a group profile.

1. In the Cisco Secure Administrator Advanced Configuration program, select the **Members** tab. In the Navigator pane, de−select the **Browse** check box. The Create New Profile icon displays.
2. In the Navigator pane, do one of these :
   - To create a group profile with no parent, locate and click the [**Root**] folder icon.
   - To create your group profile as the child of another group profile, locate the group that you want as the parent and click it.
   - If the group that you want to be the parent is a child group, click its parent group's folder to display it.
3. Click **Create New Profile**. The New Profile dialog box displays.
4. Select the **Group** check box, type the name of the group you want to create, and click **OK**. The new group displays in the tree.
5. After you create the group profile, assign TACACS+ or RADIUS attributes to configure specific AAA properties.



1. Deselect Browse.
2. Click Create Profile.
3. Select Group.
4. Enter the group name and click OK.
5. The group icon is displayed.

Create a User Profile in Advanced Configuration Mode

Use the Cisco Secure Administrator Advanced Configuration mode to create and configure a user profile. You can do this to customize the user profile's authorization− and accounting−related attributes in more detail than is possible with the Add a User page.

Use this procedure to create a user profile:

1. In the Cisco Secure Administrator Advanced Configuration program, select the **Members** tab. In the Navigator pane, locate and de−select **Browse**. The Create New Profile icon displays.
2. In the Navigator pane, do one of these :
   - Locate and click the group to which the user belongs.
   - If you do not want the user to belong to a group, click the [**Root**] folder icon.
3. Click **Create Profile**. The New Profile dialog box displays.
4. Make sure that the **Group** check box is de−selected.
5. Enter the name of the user you want to create and click **OK**. The new user displays in the tree.
6. After you create the user profile, assign specific TACACS+ or RADIUS attributes to configure specific AAA properties:
   - To assign TACACS+ profiles to the user profile, see Assign TACACS+ Attributes to a Group or User Profile.
   - To assign RADIUS profiles to the user profile, see Assign RADIUS Attributes to a Group or User Profile.

Strategies to Apply Attributes

Use the CSU group profile feature and TACACS+ and RADIUS attributes to implement authentication and authorization of network users through CSU.

Plan Attributes for Groups and Users

CSU's group profile feature enables you to define a common set of AAA requirements for a large number of users.

You can assign a set of TACACS+ or RADIUS attribute values to a group profile. These attribute values assigned to the group apply to any user who is a member or who is added as a member of that group.

Use the Group Profile Feature Effectively

To configure CSU to manage large numbers and various types of users with complex AAA requirements, Cisco recommends that you use the features of the Cisco Secure Administrator Advanced Configuration program to create and configure group profiles.

The group profile needs to contain all attributes that are not specific to the user. This usually means all attributes except for the password. You can then use the Add a User page of the Cisco Secure Administrator to create simple user profiles with password attributes and assign these user profiles to the appropriate group profile. The features and attribute values defined for a particular group then apply to its member users.

Parent Groups and Child Groups

You can create a hierarchy of groups. Within a group profile, you can create child group profiles. Attribute values assigned to the parent group profile are default values for the child group profiles.

Group Level Administration

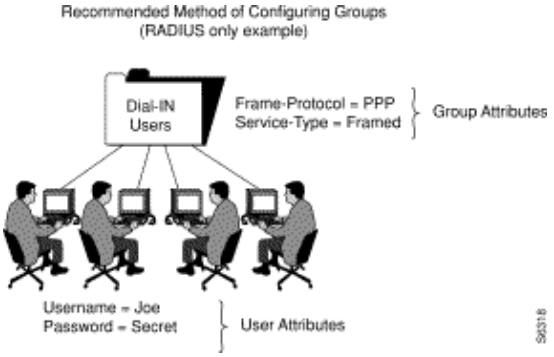
A Cisco Secure system administrator can assign individual Cisco Secure users Group Administrator status. Group Administrator status enables individual users to administer any child group profiles and user profiles that are subordinate to their group. However, it does not allow them to administer any groups or users that fall outside their group's hierarchy. Thus, the system administrator parcels out the task of administering a large network to other individuals without granting each of them equal authority.

What Attributes Do I Define for Individual Users?

Cisco recommends that you assign individual users basic authentication attribute values that are unique to the user, such as attributes that define username, password, password type, and web privilege. Assign basic authentication attribute values to your users through CSU's Edit a User or Add a User pages.

What Attributes Do I Define for Group Profiles?

Cisco recommends that you define qualification−, authorization−, and accounting−related attributes at the group level.



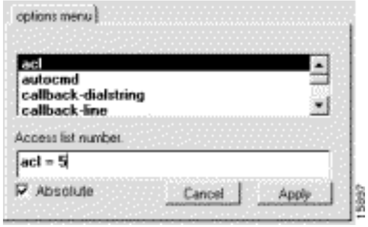
In this example, the group profile named "Dial−In Users" is assigned the attribute−value pairs Frame−Protocol=PPP and Service−Type=Framed.

What are Absolute Attributes?

A subset of the TACACS+ and RADIUS attributes in CSU can be assigned absolute status at the group profile level. An attribute value enabled for absolute status at the group profile level overrides any contending attribute values at a child group profile or member user profile level.

Within multi−level networks with several levels of group administrators, absolute attributes enable a system administrator to set selected group attribute values that group administrators at lower levels cannot override.

Attributes that can be assigned absolute status display an Absolute check box in the Attributes box of the Cisco Secure Administrator Advanced Configuration program. Select the check box to enable absolute status.



Access list number:
acl = 5
☑ Absolute

Can Group Attribute Values and User Attribute Values Conflict?

Conflict resolution among attribute values assigned to parent group profiles, child group profiles, and member user profiles depends on whether the attribute values are absolute and whether they are TACACS+ or RADIUS attributes:

- TACACS+ or RADIUS attribute values assigned to a group profile with absolute status override any contending attribute values set at a child group or user profile level.
- If a TACACS+ attribute value's absolute status is not enabled at the group profile level, it is overridden by any contending attribute value set at a child group or user profile level.
- If a RADIUS attribute value's absolute status is not enabled at the parent group level, then any contending attribute values set at a child group result in an unpredictable outcome. When you define RADIUS attribute values for a group and its member users, avoid assigning the same attribute to both the user and group profiles.

Use the Prohibit and Permit Options

For TACACS+, override the availability of inherited service values by prefixing the keyword **prohibit** or **permit** to the service specification. The **permit** keyword allows specified services. The **prohibit** keyword disallows specified services. With the use of these keywords together, you can construct "everything except" configurations. For example, this configuration allows access from all services except X.25:

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

Assign TACACS+ Attributes to a Group or User Profile

To assign specific TACACS+ services and attributes to a group or user profile, follow these steps :

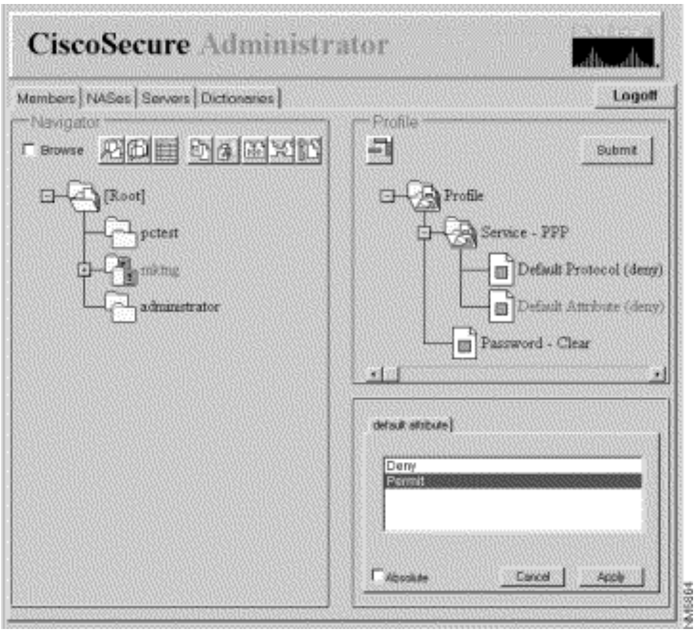
1. In the Cisco Secure Administrator Advanced Configuration program, select the **Members** tab. In the Navigator pane, click the icon for the group or user profile to which TACACS+ attributes are assigned.
2. If necessary, in the Profile pane, click the **Profile** icon to expand it.

   A list or dialog box that contains attributes applicable to the selected profile or service displays in the window at the bottom right of the screen. The information in this window changes based on which profile or service you select in the Profile pane.
3. Click the service or protocol that you want to add and click **Apply**. The service is added to the profile.
4. Enter or select the necessary text in the Attribute window.

Valid entries are explained in the Strategies for Applying Attributes section of the CSU 2.3 for UNIX Reference Guide.

Note: If you assign an attribute value at the group profile level, and the attribute you specify displays an **Absolute** check box, select that check box to assign the value absolute status. A value−assigned absolute status cannot be overridden by any contending values assigned at subordinate group profile or user profile levels.

5. Repeat steps 1 through for each additional service or protocol you need to add.
6. When all changes are made, click **Submit**.

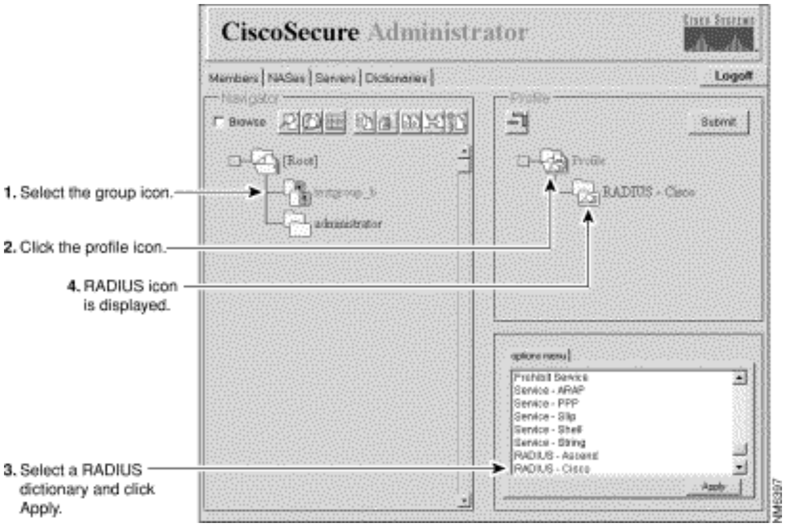


Assign RADIUS Attributes to a Group or User Profile

To assign specific RADIUS attributes to a group or user profile:

1. Assign a RADIUS dictionary to the group profile:

   a. On the Members page of the Cisco Secure Administrator Advanced Configuration program, click the **Group** or **User** icon, then click the **Profile** icon in the Profiles pane. In the Attributes pane, the Options menu displays.
   b. On the **Options** menu, click the name of the RADIUS dictionary you want the group or user to use. (For example, RADIUS − Cisco.) Click **Apply**.



1. Select the group icon.

2. Click the profile icon.

4. RADIUS icon is displayed.

3. Select a RADIUS dictionary and click Apply.

2. Add the required Check Items and Reply Attributes to the RADIUS profile:

   Note: Check items are attributes required for authentication, such as user ID and password. Reply Attributes are attributes sent to the Network Access Server (NAS) after the profile has passed the authentication procedure, such as Framed−Protocol. For lists and explanations of Check Items and Reply Attributes, refer to the RADIUS Attribute−Value Pairs and Dictionary Management in the CSU 2.3 for UNIX Reference Guide.

   a. In the Profile window, click the RADIUS − dictionaryname folder icon. (You probably need to click the profile's + symbol to expand the RADIUS folder.) The Check Items and Reply Attributes options display in the Attribute Group window.
   b. To use one or more of these attributes, click the attribute(s) you want to use, then click **Apply**. You can add more than one attribute at a time.
   c. Click the **+** symbol for the RADIUS − dictionaryname to expand the folder.

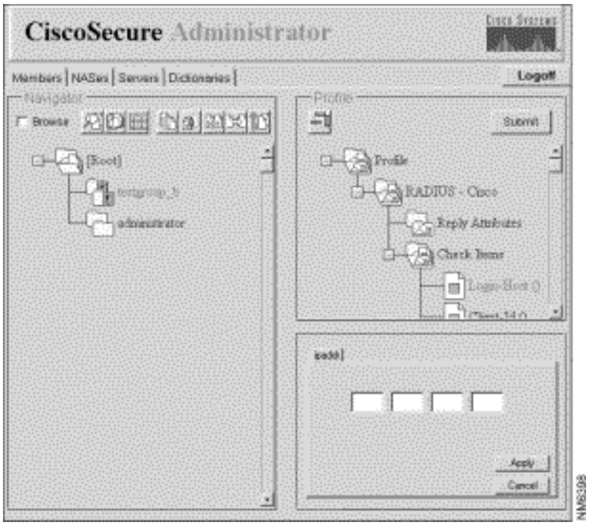
      Note: If you select the RADIUS−Cisco11.3 option, make sure that Cisco IOS® Software Release 11.3.3(T) or later is installed on your connecting NASs and add new command lines to your NAS configurations. Refer to the Fully Enabling the RADIUS−Cisco11.3 Dictionary in the CSU 2.3 for UNIX Reference Guide.
3. Specify values for the added Check Items and Reply Attributes:

   ⚠ **Caution:** For the RADIUS protocol, inheritance is additive as opposed to hierarchical. (The TACACS+ protocol uses hierarchical inheritance). For example, if you assign the same reply attributes to both the user and group profiles, authorization fails because the NAS receives twice the number of attributes. It fails to make sense of the reply attributes. Do not assign the same check item or reply attribute to both the group and user profiles.

   a. Click **Check Items** or **Reply Attributes**, or click both. A list of applicable Check Items and Reply Attributes values appears in the lower right window. Click the **+** symbol to expand the folder.
   b. Click the values you want to assign, then click **Apply**. For more information on the values, refer to RADIUS Attribute−Value Pairs and Dictionary Management in the CSU 2.3 for UNIX Reference Guide.

      Note: If you assign an attribute value at the group profile level, and the attribute you specify displays an Absolute check box, select that check box to assign the value absolute status. A value assigned absolute status cannot be overridden by any contending values assigned at subordinate group profile or user profile levels.

c. When you have finished making changes, click **Submit**.



4. To use one or more of these attributes, click the attribute(s) you want to use, then click **Apply**. You can apply more than one attribute at a time.

Assign Access Control Privilege Levels

The superuser administrator uses the web privilege attribute to assign a level of access control privilege to Cisco Secure users.

1. In the Cisco Secure Administrator Advanced Configuration program, click the user whose access control privilege you want to assign, then click the Profile icon in the Profiles pane.
2. In the Options menu, click **Web Privilege** and select one of these values.

   - **0** − Denies the user any access control privileges that include the ability to change the user's Cisco Secure password.
   - **1** − Grants the user access to the CSUser web page. This allows Cisco Secure users to change their Cisco Secure passwords. For details about how to change passwords, refer to User−Level Functions (Changing a Password) in Simple User and ACS Management.
   - **12** − Grants the user group administrator privileges.
   - **15** − Grants the user system administrator privileges.

   Note: If you select any web privilege option other than 0, you must also specify a password. To satisfy the web privilege password requirement, a single blank space is minimally acceptable.

Start and Stop CSU

Usually, CSU starts automatically when you start or restart the SPARCstation where it is installed. However, you can start CSU manually, or shut it down without shutting down the entire SPARCStation.

Log in as [Root] to the SPARCStation where you installed CSU.

To start CSU manually, type:

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

To stop CSU manually, type:

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

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Cisco Secure ACS for UNIX Support Page**
- **TACACS+ Support Page**
- **RADIUS Support Page**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 14, 2009 Document ID: 13842