

# Troubleshooting CSS and TACACS+

Document ID: 27000

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Problem

### Solution and debug Commands

- Common Mistakes

### Related Information

---

## Introduction

The Terminal Access Controller Access Control System (TACACS+) protocol provides access control for routers, Network Access Servers (NASs), or other devices through one or more daemon servers. It encrypts all traffic between the NAS and daemon using TCP communications for reliable delivery.

This document provides troubleshooting information for the Content Services Switch (CSS) and TACACS+. You can configure the CSS as a client of a TACACS+ server, providing a method for authentication of users, and authorization and accounting of configuration and non-configuration commands. This feature is available in WebNS 5.03.

**Note:** Refer to [Configuring the CSS as a Client of a TACACS+ Server](#) for more information.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

This document is not restricted to specific software and hardware versions.

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

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

## Problem

When you attempt to log in to the CSS with a TACACS+ user, the login does not work.

## Solution and debug Commands

Generally, when TACACS+ authentication does not work with a CSS, the problem is usually either a configuration issue on either the CSS or the TACACS+ server. The first thing that you need to check is whether you have configured the CSS as a client of a TACACS+ server.

When you have checked this, there is additional logging that you can use on the CSS in order to determine the problem. Complete these steps to turn on logging.

On the CSS, enter debug mode.

```
CSS# llama
CSS(debug)# mask tac 0x3
CSS(debug)# exit
CSS# configure
CSS(config)# logging subsystem security level debug-7
CSS(config)# logging subsystem netman level info-6
CSS(config)# exit
CSS# logon
```

*!--- This logs messages to the screen.*

In order to disable logging, issue these commands:

```
CSS# llama
CSS(debug)# mask tac 0x0
CSS(debug)# exit
CSS# no logon
```

These messages can appear:

```
SEP 10 08:30:10 5/1 99 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0c
SEP 10 08:30:10 5/1 100 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:30:10 5/1 101 SECURITY-7: Security Manager sending error 7 reply to
1ler 20201c00
```

These messages indicate that the CSS tries to communicate with the TACACS+ server, but the TACACS+ server rejects the CSS. **error 7** means that the TACACS+ key entered in the CSS does not match the key on the TACACS+ server.

A successful login through a TACACS+ server shows this message (note the sending **success 0** reply):

```
SEP 10 08:31:46 5/1 107 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0d
SEP 10 08:31:46 5/1 108 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:31:47 5/1 109 SECURITY-7: Security Manager sending success 0 reply to
caller 20201c00

SEP 10 08:31:47 5/1 110 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x2020
4b0d
```

## Common Mistakes

The most common mistake when you set up a CSS to work with a TACACS+ server is actually very simple. This command tells the CSS what key to use to communicate with the TACACS+ server:

```
CSS(config)# tacacs-server key system enterkeyhere
```

This key can be either clear text or DES encrypted. The clear text key is DES encrypted before the key is placed in the running configuration. To make a key clear text, put it in quotes. To make it DES encrypted, do not use quotes. The important thing is to know if the TACACS+ key is DES encrypted or if the key is clear text. After you issue the command, match the key of the CSS to the key that the TACACS+ server uses.

---

## Related Information

- **Configuring the CSS as a Client of a TACACS+ Server**
  - **Configuring TACACS+ and Extended TACACS+**
  - **Password Recovery Procedure for the Cisco CSS 11000 Series**
  - **Technical Support & Documentation – Cisco Systems**
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 03, 2004

Document ID: 27000

---