

How to Configure the Cisco VPN 3000 Concentrator to Support TACACS+ Authentication for Management Accounts

Document ID: 12088

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure the TACACS+ Server

- Add an Entry for the VPN 3000 Concentrator in the TACACS+ Server
- Add a User Account in the TACACS+ Server
- Edit the Group on the TACACS+ Server

Configure the VPN 3000 Concentrator

- Add an Entry for the TACACS+ Server in the VPN 3000 Concentrator
- Modify the Admin Account on the VPN Concentrator for TACACS+ Authentication

Verify

Troubleshoot

Related Information

Introduction

This document provides step-by-step instructions in order to configure the Cisco VPN 3000 Series Concentrators to support the TACACS+ Authentication for Management Accounts.

As soon as a TACACS+ server is configured on the VPN 3000 Concentrator, the locally configured account names and passwords such as admin, config, isp, and so forth, are no longer used. All logins to the VPN 3000 Concentrator are sent to the configured external TACACS+ server for user and password verification.

The definition of a privilege level for each user on the TACACS+ server determines the permissions on the VPN 3000 Concentrator for each TACACS+ username. Then, match that up with the AAA Access Level defined under the locally configured username on the VPN 3000 Concentrator. This is an important point because as soon as a TACACS+ server is defined, the locally configured usernames on the VPN 3000 Concentrator are no longer valid. But, they are still used only in order to match up the returned privilege level from the TACACS+ server, with the AAA Access Level under that local user. The TACACS+ username is then assigned the privileges that the locally configured VPN 3000 Concentrator user has defined under their profile.

For example, described in detail in the configuration sections, a TACACS+ user/group is configured to return a TACACS+ Privilege Level of 15. Under the Administrators section of the VPN 3000 Concentrator, the admin user has its AAA Access Level also set to 15. This user is allowed to modify the configuration under all sections, and to read/write files. Because TACACS+ Privilege Level and AAA Access Level match, the TACACS+ user is given those permissions on the VPN 3000 Concentrator.

As an example, if you decide that a user needs to be able to modify the configuration, but *not* read/write files, assign them a privilege level of 12 on the TACACS+ server. You can pick any number between one and 15. Then, on the VPN 3000 Concentrator, pick one of the other locally configured administrators. Next, set its AAA Access Level to 12, and set the permissions on this user in order to be able to modify the configuration,

but not to read/write files. Because of the matching privilege/access level, the user gets those permissions when they login.

The locally configured usernames on the VPN 3000 Concentrator are no longer used. But, the Access Rights and AAA Access Levels under each of those users are used in order to define the privileges a particular TACACS+ user gets when you login.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Ensure that you have IP connectivity to the TACACS+ server from the VPN 3000 Concentrator. If your TACACS+ server is towards the public interface, do not forget to open the TACACS+ (TCP port 49) on the public filter .
- Ensure backup access via the console is operational. It is easy to accidentally lock all users out of the configuration when you first set this up. The only way to recover access is via the console, which still uses the locally configured usernames and passwords.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN 3000 Concentrator Software Release 4.7.2.B (Alternatively, any release of 3.0 or later OS software works.)
- Cisco Secure Access Control Server for Windows Servers Release 4.0 (Alternately, any release of 2.4 or later software works.)

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.

Configure the TACACS+ Server

Add an Entry for the VPN 3000 Concentrator in the TACACS+ Server

Complete these steps in order to add an entry for the VPN 3000 Concentrator in the TACACS+ server.

1. Click **Network Configuration** in the left panel. Under AAA Clients, click **Add Entry**.
2. On the next window, fill out the form to add the VPN Concentrator as the TACACS+ client. This example uses:

- ◆ AAA Client Hostname = **VPN3000**
- ◆ AAA Client IP Address = **10.1.1.2**
- ◆ Key = **csacs123**
- ◆ Authenticate using = **TACACS+ (Cisco IOS)**

Click **Submit + Restart**.

Network Configuration

Edit

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Add a User Account in the TACACS+ Server

Complete these steps in order to add a user account in the TACACS+ server.

1. Create a user account in the TACACS+ server that can be later used for TACACS+ authentication. Click **User Setup** in the left panel, add user "johnsmith" and click **Add/Edit** in order to do this.
2. Add a password for this user, and assign the user to an ACS group that contains the other VPN 3000 Concentrator administrators.

Note: This example defines the privilege level under this particular user ACS group profile. If this is to be done on a per-user basis, choose **Interface Configuration > TACACS+ (Cisco IOS)** and check the **User** box for the Shell (exec) service. Only then are the TACACS+ options described in this document available under each user profile.

Edit the Group on the TACACS+ Server

Complete these steps to edit the group on the TACACS+ server.

1. Click **Group Setup** in the left panel.
2. From the drop-down menu, choose the group the user was added to in the Add a User Account in the TACACS+ Server section, which is Group 1 in this example, and click **Edit Settings**.
3. On the next window, make sure that these attributes are selected under TACACS+ Settings:

- ◆ **Shell (exec)**
- ◆ **Privilege level = 15**

Once done, click **Submit + Restart**.

Configure the VPN 3000 Concentrator

Add an Entry for the TACACS+ Server in the VPN 3000 Concentrator

Complete these steps in order to add an entry for the TACACS+ server in the VPN 3000 Concentrator.

1. Choose **Administration > Access Rights > AAA Servers > Authentication** in the navigation tree in the left panel, and then click **Add** in the right panel.

As soon as you click **Add** in order to add this server, locally configured username/passwords on the VPN 3000 Concentrator are no longer used. Ensure backup access via the console works in case of a lock-out.

2. On the next window, fill out the form as seen here:

- ◆ Authentication Server = **10.1.1.1** (IP address of TACACS+ server)
- ◆ Server Port = **0** (default)
- ◆ Timeout = **4**
- ◆ Retries = **2**

◆ Server Secret = csacs123

◆ Verify = csacs123

The screenshot shows a configuration window titled "Administration | Access Rights | AAA Servers | Authentication | Add". The main heading is "Configure and add a TACACS+ administrator authentication server." The form contains the following fields:

- Authentication Server:** 10.1.1.1 (with instruction: "Enter IP address or hostname.")
- Server Port:** 0 (with instruction: "Enter the server TCP port number (0 for default).")
- Timeout:** 4 (with instruction: "Enter the timeout for this server (seconds)")
- Retries:** 2 (with instruction: "Enter the number of retries for this server.")
- Server Secret:** csacs123 (with instruction: "Enter the server secret.")
- Verify:** csacs123 (with instruction: "Re-enter the server secret.")

Buttons for "Add" and "Cancel" are located at the bottom of the form.

Modify the Admin Account on the VPN Concentrator for TACACS+ Authentication

Complete these steps to modify the admin account on the VPN Concentrator for TACACS+ authentication.

1. Click **Modify** for the user admin in order to modify the properties of this user.

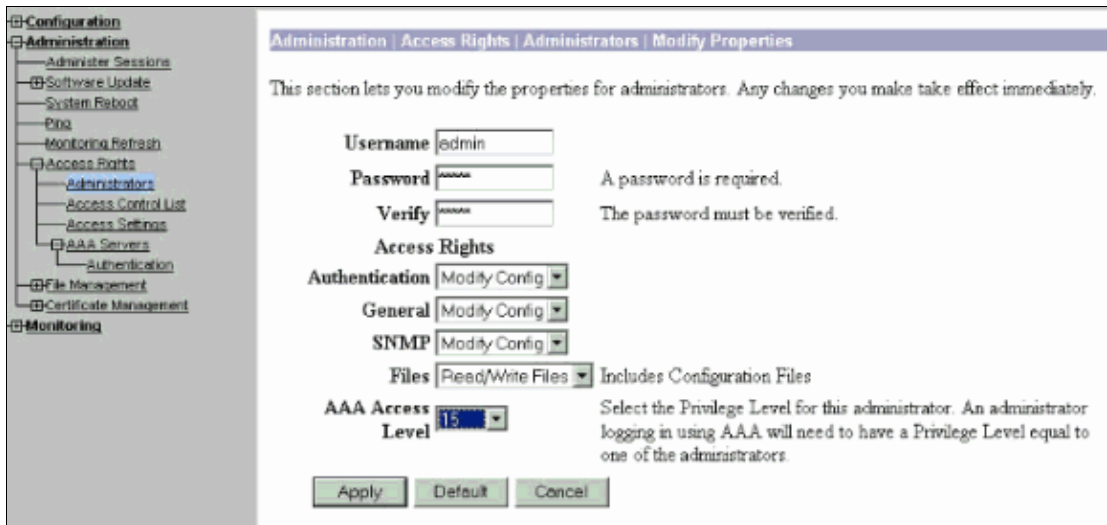
The screenshot shows a configuration window titled "Administration | Access Rights | Administrators". The main heading is "This section presents administrator users. Any changes you make take effect immediately." The table below lists administrator users with their properties and enabled status.

Group Number	Username	Properties	Administrator Enabled
1	admin	Modify	<input checked="" type="checkbox"/>
2	config	Modify	<input type="checkbox"/>
3	isp	Modify	<input type="checkbox"/>
4	mis	Modify	<input type="checkbox"/>
5	user	Modify	<input type="checkbox"/>

Buttons for "Apply" and "Cancel" are located at the bottom of the table.

2. Choose the AAA Access Level as **15**.

This value can be any number between one and 15. Note that it must match the TACACS+ Privilege Level defined under the user/group profile on the TACACS+ server. The TACACS+ user then picks up the permissions defined under this VPN 3000 Concentrator user for the modification of the configuration, reading/writing files, and so forth.



Verify

There is currently no verification procedure available for this configuration.

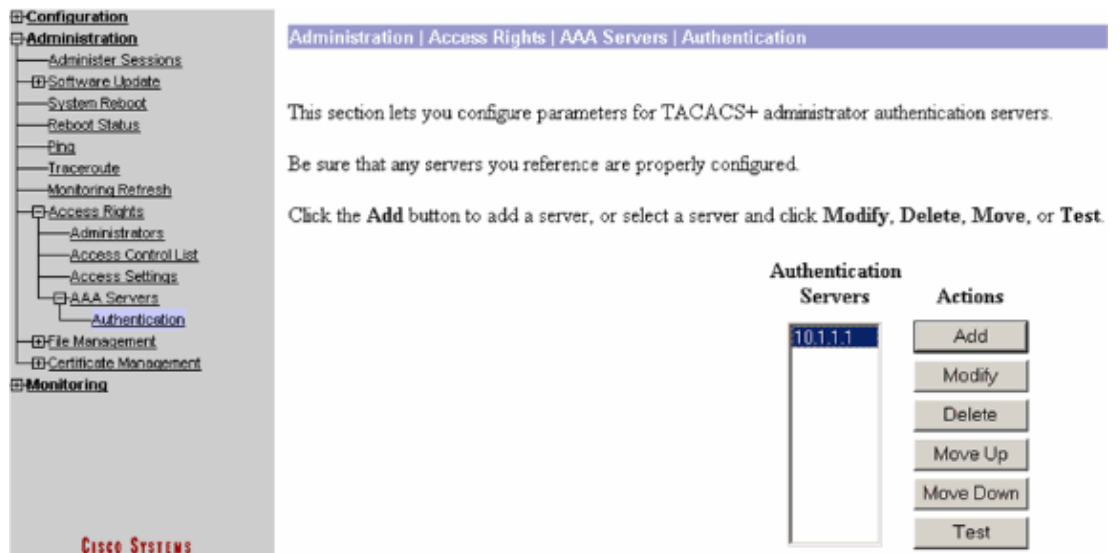
Troubleshoot

Complete the steps in these instructions in order to troubleshoot your configuration.

1. In order to test the authentication:

For TACACS+ Servers

- a. Choose **Administration > Access Rights > AAA Servers > Authentication**.
- b. Select your server, and then click **Test**.



Note: When the TACACS+ server is configured on the Administration tab, there is no way to set up the user to authenticate on the VPN 3000 local database. You can only fallback using another external database or TACACS server.

- c. Enter the TACACS+ username and password and click **OK**.

Administration | Access Rights | AAA Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

Username

Password

A successful authentication appears.

The image shows a configuration tree on the left and a success message dialog on the right. The tree is expanded to show the 'Authentication' option under 'AAA Servers'. The success message dialog has a blue header 'Success', an information icon, the text 'Authentication Successful', and a 'Continue' button.

2. If it fails, there is either a configuration problem or an IP connectivity issue. Check the Failed Attempts Log on the ACS server for messages related to the failure.

- ◆ If no messages appear in this log then there is probably an IP connectivity issue. The TACACS+ request does not reach the TACACS+ server. Verify the filters applied to the appropriate VPN 3000 Concentrator interface allows TACACS+ (TCP port 49) packets in and out.
 - ◆ If the failure displays as service denied in the log, then the Shell (exec) service has not been correctly enabled under the user or group profile on the TACACS+ server.
3. If the test authentication is successful, but logins to the VPN 3000 Concentrator continue to fail, check the Filterable Event Log via the console port.

If you see a similar message:

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
Status: <REFUSED> authorization failure. NO Admin Rights
```

This message indicates the privilege level assigned on the TACACS+ server has no matching AAA access level under any of the VPN 3000 Concentrator users. For example, user johnsmith has a TACACS+ privilege level of 7 on the TACACS+ server, but none of the five VPN 3000 Concentrator administrators have an AAA access level of 7.

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
 - [Cisco VPN 3000 Series Client Support Page](#)
 - [IPSec Negotiation/IKE Protocols Support Page](#)
 - [TACACS/TACACS+ Support Page](#)
 - [TACACS+ in IOS Documentation](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 31, 2006

Document ID: 12088
