

Настройка концентратора Cisco VPN серии 3000 с целью поддержки проверки подлинности по TACACS+ для управления учетными записями

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройте TACACS + сервер](#)

[Добавьте запись для VPN 3000 Concentrator в TACACS + сервер](#)

[Добавьте учетную запись пользователя в TACACS + сервер](#)

[Отредактируйте группу на TACACS + сервер](#)

[Настройка концентратора VPN 3000](#)

[Добавьте запись для TACACS + сервер в VPN 3000 Concentrator](#)

[Модифицируйте учетную запись администратора на концентраторе VPN для TACACS + аутентификация](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет пошаговые инструкции для настройки концентраторов Cisco VPN серии 3000 для поддержки TACACS + Аутентификация для Учетных записей администратора.

Как только TACACS + сервер настроен на VPN 3000 Concentrator, локально настроенные учетные имена и пароли, такие как admin, config, интернет-провайдер, и т.д, больше не используется. Все входы в систему к VPN 3000 Concentrator передаются настроенному внешнему TACACS + сервер для пользователя и проверка пароля.

Определение уровня привилегий для каждого пользователя на TACACS + сервер определяет разрешения на VPN 3000 Concentrator для каждого TACACS + имя пользователя. Затем подойдите это с Уровнем доступа AAA, определенным под локально настроенным именем пользователя на VPN 3000 Concentrator. Это - важный момент, потому что, как только TACACS + сервер определен, локально настроенные имена пользователей на VPN 3000 Concentrator больше не действительны. Но, они все еще используются только

для подхождения возвращенного уровня привилегий от TACACS + сервер с Уровнем доступа AAA при том локальном пользователе. TACACS + имени пользователя тогда назначают привилегии, что локально настроенный пользователь VPN 3000 Concentrator определил под их профилем.

Например, описанный подробно в разделах конфигурации, TACACS + пользователь/группа настроен для возврата TACACS + Уровень привилегий 15. Под разделом Администраторов VPN 3000 Concentrator у пользователя с правами администратора есть его Уровень доступа AAA также набор к 15. Этому пользователю разрешают модифицировать конфигурацию под всеми разделами, и к файлам чтения-записи. Поскольку TACACS + Уровень привилегий и соответствие Уровня доступа AAA, TACACS + пользователю дают те разрешения на VPN 3000 Concentrator.

Как пример, если вы решаете, что пользователь должен быть в состоянии модифицировать конфигурацию, но не файлы чтения-записи, назначьте их уровень привилегий 12 на TACACS + сервер. Можно выбрать любой номер между один и 15. Затем на VPN 3000 Concentrator выберите одного из других локально настроенных администраторов. Затем, установите его Уровень доступа AAA в 12 и установите разрешения на этом пользователе, чтобы быть в состоянии модифицировать конфигурацию, но не к файлам чтения-записи. Из-за соответствующей привилегии/уровня доступа пользователь получает те разрешения, когда они входят.

Локально настроенные имена пользователей на VPN 3000 Concentrator больше не используются. Но, Права доступа и Уровни доступа AAA при каждом из тех пользователей используются для определения привилегий определенной TACACS +, пользователь добирается, когда вы входите.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Гарантируйте, что у вас есть возможность подключения с помощью IP-адреса к TACACS + сервер от VPN 3000 Concentrator. Если ваш TACACS + сервер находится к открытому интерфейсу, не забывайте открывать TACACS + (порт TCP 49) на общем фильтре.
- Гарантируйте, что резервный доступ через консоль в рабочем состоянии. Легко случайно заблокировать всех пользователей из конфигурации при первом настраивании этого. Единственный способ восстановить доступ через консоль, которая все еще использует локально настроенные имена пользователя и пароли.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Выпуск ПО Cisco VPN 3000 Concentrator 4.7.2. В (Также любой выпуск 3.0 или более позднее операционное программное обеспечение работает.)
- Выпуск 4.0 Серверов Сервера безопасного контроля доступа Cisco для Windows

(Поочередно, любой выпуск 2.4 или более позднее программное обеспечение работает.)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

[Условные обозначения](#)

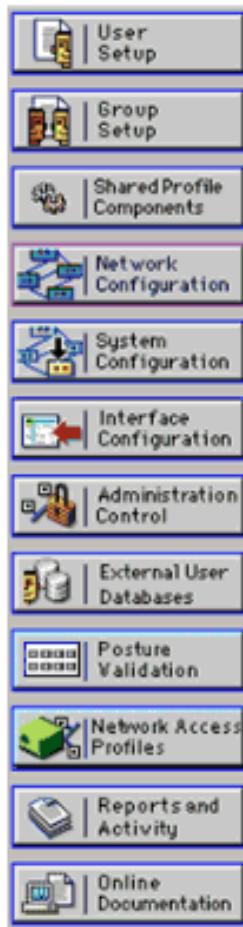
[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

[Настройте TACACS + сервер](#)

[Добавьте запись для VPN 3000 Concentrator в TACACS + сервер](#)

Выполните эти шаги для добавления записи для VPN 3000 Concentrator в TACACS + сервер.

1. Нажмите **Network Configuration** в левой панели. На вкладке **AAA Clients (Клиенты AAA)** щелкните **Add Entry (Добавить запись)**.
2. На следующем окне заполните форму для добавления Концентратора VPN как TACACS + клиент. Использование данного примера: Имя хоста для клиента AAA = **VPN3000** IP-адрес клиента AAA = **10.1.1.2** Ключ = **csacs123** Используемая аутентификация = **TACACS + (Cisco IOS)** Нажмите **Submit + Restart**.



Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="10.1.1.2"/>
Key	<input type="text" value="csacs123"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

[Добавьте учетную запись пользователя в TACACS + сервер](#)

Выполните эти шаги для добавления учетной записи пользователя в TACACS + сервер.

1. Создайте учетную запись пользователя в TACACS + сервер, который может позже использоваться для TACACS + аутентификация. Нажмите **User Setup** в левой панели, добавьте пользователя "johnsmith" и нажмите **Add/Edit**, чтобы сделать это.
2. Добавьте пароль для этого пользователя и назначьте пользователя на группу ACS, которая содержит других администраторов VPN 3000 Concentrator. **Примечание:** Данный пример определяет уровень привилегий под этим профилем группы ACS индивидуального пользователя. Если это должно быть сделано на основе для каждого пользователя, выбрать **Interface Configuration > TACACS + (Cisco IOS)** и установить **Пользовательский** флажок для сервиса Shell (exec). Только тогда опции TACACS +, описанные в этом документе, доступном под каждым профилем пользователя.

[Отредактируйте группу на TACACS + сервер](#)

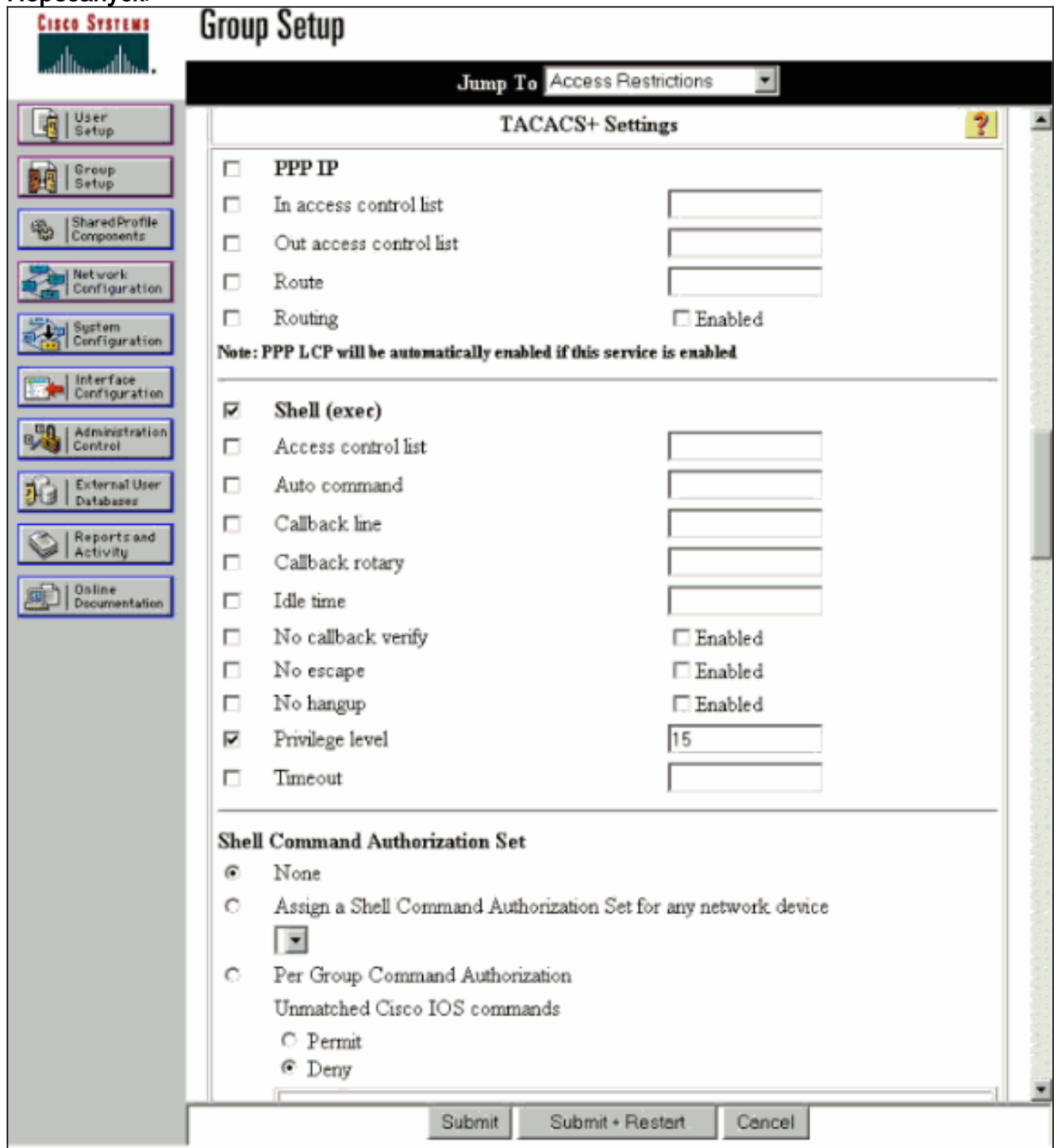
Выполните эти шаги для редактирования группы на TACACS + сервер.

1. Нажмите **Group Setup** в левой панели.
2. От раскрывающегося меню выберите группу, к которой был добавлен пользователь в

[Добавлении Учетной записи пользователя в TACACS +](#) раздел [Сервера](#), который является Группой 1 в данном примере, и нажмите **Edit Settings**.

3. На следующем окне удостоверьтесь, что эти атрибуты выбраны под TACACS +
Параметры настройки: **Shell (exec)** **Уровень привилегий = 15** После того, как сделанный, нажмите **Submit +**

Перезапуск.



The screenshot shows the Cisco Systems Group Setup interface. The main title is "Group Setup". A "Jump To" dropdown menu is set to "Access Restrictions". The "TACACS+ Settings" section is active, showing a list of configuration options. The "Shell (exec)" checkbox is checked, and the "Privilege level" is set to 15. The "Shell Command Authorization Set" is set to "None".

TACACS+ Settings

- PPP IP
- In access control list
- Out access control list
- Route
- Routing Enabled

Note: PPP LCP will be automatically enabled if this service is enabled

- Shell (exec)**
- Access control list
- Auto command
- Callback line
- Callback rotary
- Idle time
- No callback verify Enabled
- No escape Enabled
- No hangup Enabled
- Privilege level 15
- Timeout

Shell Command Authorization Set

- None
- Assign a Shell Command Authorization Set for any network device
- Per Group Command Authorization

Unmatched Cisco IOS commands

- Permit
- Deny

Buttons: Submit, Submit + Restart, Cancel

[Настройка концентратора VPN 3000](#)

[Добавьте запись для TACACS + сервер в VPN 3000 Concentrator](#)

Выполните эти шаги для добавления записи для TACACS + сервер в VPN 3000 Concentrator.

1. Выберите **Administration > Access Rights > AAA Servers > Authentication** в навигационном дереве в левой панели, и затем **нажмите Add** в правой панели. Как только вы **нажмите Add** для добавления этого сервера, локально настроенное имя пользователя/пароли на VPN 3000 Concentrator больше не используются. Гарантируйте, что резервный доступ через консоль работает в случае локаута.
2. На следующем окне заполните форму, как замечено здесь: Сервер проверки подлинности = 10.1.1.1 (IP-адрес TACACS + сервер) Порт сервера = 0 (по умолчанию) Таймаут = 4 Повторные попытки = 2 Секретный сервер = csacs123 Проверьте =

csacs123

The screenshot shows the configuration page for adding a TACACS+ administrator authentication server. The breadcrumb trail is 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.

[Модифицируйте учетную запись администратора на концентраторе VPN для TACACS + аутентификация](#)

Выполните эти шаги для изменения учетной записи администратора на Концентраторе VPN для TACACS + аутентификация.

1. Нажмите **Modify** для администрирования пользователя для изменения свойств этого пользователя.

The screenshot shows the configuration page for modifying administrator users. The breadcrumb trail is Administration | Access Rights | Administrators. The main heading is "This section presents administrator users. Any changes you make take effect immediately." The table below lists the administrator users:

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

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

2. Выберите AAA Access Level в качестве 15. Это значение может быть любым номером между один и 15. Обратите внимание на то, что это должно совпасть с TACACS + Уровень привилегий, определенный при пользователе/профиле группы на TACACS + сервер. TACACS + пользователь тогда забирает разрешения, определенные при этом пользователе VPN 3000 Concentrator для модификации конфигурации, читая/пишущий файлы, и

Т.Д.



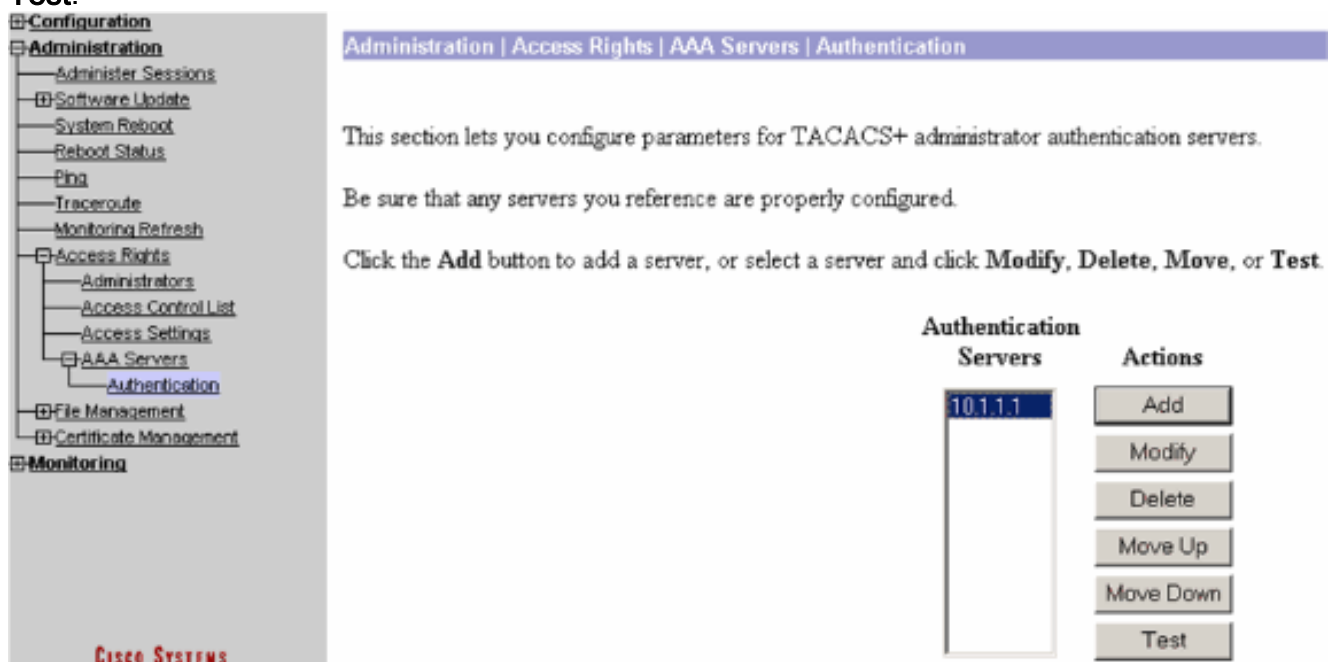
Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Выполните шаги в этих инструкциях для устранения проблем конфигурации.

1. Для тестирования аутентификации: Для TACACS + серверы Выберите **Administration > Access Rights > AAA Servers > Authentication**. Выберите свой сервер, и затем нажмите **Test**.



Примечание: Когда TACACS + сервер настроен на вкладке Administration, нет никакого способа установить пользователя для аутентификации на локальной базе данных VPN 3000. Вы можете только нейтрализация с помощью другой внешней базы данных или Сервера tacacs. Введите TACACS + имя пользователя и пароль и нажмите

OK.

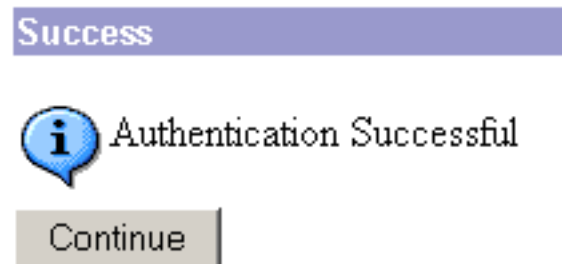
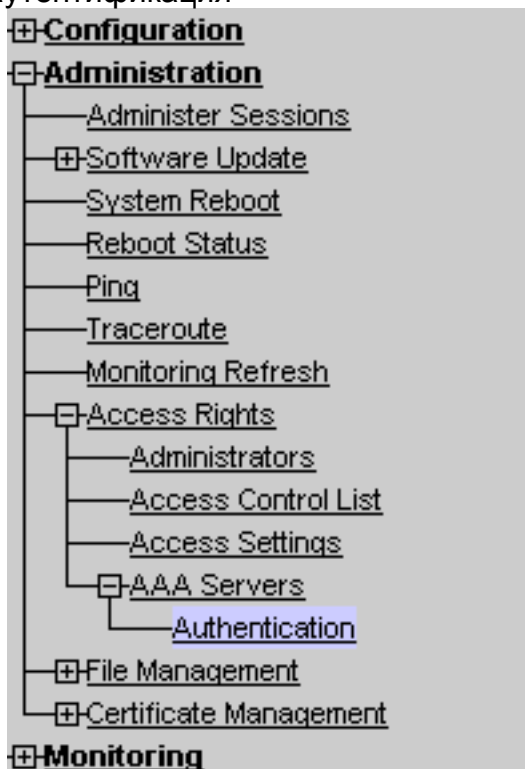
Administration | Access Rights | AAA Servers | Authentication | Test

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

Username

Password

Успешная аутентификация



появляется.

2. Если это отказывает, существует или проблема конфигурации или невозможность IP-подключения. Проверьте Вход в систему Неудачных попыток сервера ACS для сообщений, отнесенных к сбою. Если никакие сообщения не появляются в этом журнале тогда существует, вероятно, невозможность IP-подключения. TACACS + запрос не достигает TACACS + сервер. Проверьте, что фильтры применились к соответствующему интерфейсу VPN 3000 Concentrator, позволяет TACACS + (порт TCP 49) пакеты в и. Если сбой отображается как сервис, запрещенный в журнале, то сервис Shell (exec) не был правильно включен при пользователе или профиле группы на TACACS + сервер.
3. Если тестовая аутентификация успешна, но входит к VPN 3000 Concentrator, продолжают отказывать, проверять Журнал событий с фильтрацией через консольный порт. Если вы видите подобное сообщение:

```
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
```

 Это сообщение указывает на уровень привилегий, назначенный на TACACS +, сервер не имеет никакого соответствующего уровня доступа AAA ни при одном из пользователей VPN 3000 Concentrator. Например, у пользователя johnsmith есть TACACS + уровень привилегий 7 на TACACS + сервер, но ни один из пяти администраторов VPN 3000 Concentrator не имеет уровень доступа AAA 7.

Дополнительные сведения

- [Страница поддержки концентратора Cisco VPN серии 3000](#)
- [Страница поддержки Cisco VPN 3000 Series Client](#)
- [Страница технической поддержки протоколов согласования IPSec и IKE](#)
- [Страница поддержки TACACS/TACACS+](#)
- [TACACS+ в документации по IOS](#)
- [Cisco Systems – техническая поддержка и документация](#)