Настроить DCM Cisco? Поддержка удаленной аутентификации

Содержание

Введение

Этот документ описывает Менеджера цифрового контента (DCM) Cisco softwareRemote Аутентификация с помощью RADIUS.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с версией программного обеспечения 16 DCM Cisco и выше.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение Cisco DCM v16.10 и выше.
- Сервер RADIUS, работающий с freeRadius программным обеспечением с открытым исходным кодом.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

В V16.10 DCM новая характеристика была представлена, который позволяет учетным записям пользователя, настроенным на сервере RADIUS использоваться для доступа к DCM, документ GUI.This описывает настройку, требуемую на DCM и сервере RADIUS для использования этой функции.

Учетные записи GUI на DCM

В версиях 16.0 и ниже учетных записей пользователя, требуемых обратиться к GUI, были локальны для DCM, т.е. создал, модифицировал, использовал и удалил на DCM.

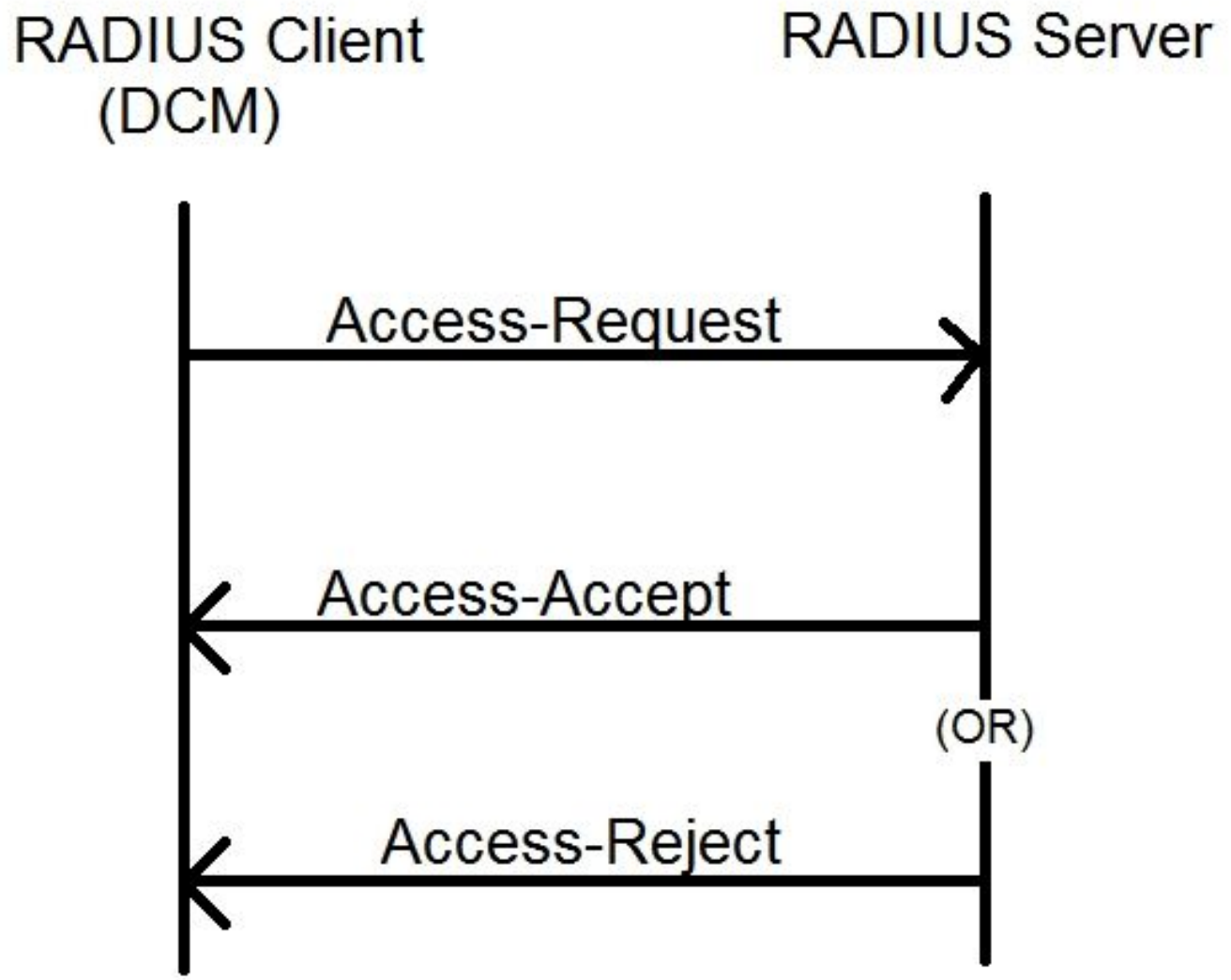
Учетная запись пользователя графического интерфейса может принадлежать одной из этих групп:

- Администраторы (полное управление)
- Пользователи (Чтение-запись)
- Гости (только для чтения)
- Автоматизация инициирует (Внешние триггеры)
- Администраторы DTF (конфигурация Ключа DTF)

Удаленная аутентификация

Идея удаленной аутентификации состоит в том, чтобы иметь централизованный набор учетных записей пользователя, которые могут использоваться для доступа к устройству, приложению, сервис и т.д.

Шаги , показанные в образе , объясняют, что происходит, когда вы используете удаленную аутентификацию:



Шаг 1. Пользователь вводит вход в систему и пароль (учетная запись пользователя, настроенная на сервере RADIUS) на странице входа на GUI DCM.

Шаг 2. DCM передает сообщение Access-Request с учетными данными к серверу RADIUS.

Шаг 3. Сервер RADIUS проверяет, прибыл ли запрос от одного из настроенных клиентов и для существования учетной записи пользователя на ее DB/файле и проверяет, если пароль корректен или нет, после которого любое из следующих сообщений возвращены к DCM

- Access-Accept – Это означает, что учетные данные допустимы. Настроенные атрибуты RADIUS возвращены.
- Access-Reject – Это означает, что учетные данные недопустимы, и сервер RADIUS может быть настроен для передачи некоторых атрибутов RADIUS для информирования сбоя.
- Проблема доступа – Это означает, что серверу RADIUS нужны некоторые дополнительные сведения для проверки подлинности пользователя. Не обработанный в DCM.

В случае, если сервер RADIUS передает Access-Reject, проверки DCM, если учетная запись

пользователя локальна для самого DCM, и процедура проверки подлинности для этого придерживается.
Пользователь пройден повторную проверку подлинности в интервале 15 минут (внутренне), чтобы подтвердить, что имя пользователя/пароль все еще допустимо, и пользователь принадлежит одной из групп учетной записи GUI. Если аутентификация отказывает, текущий рабочий пользовательский сеанс считают недопустимым, и все привилегии отозваны для пользователя.

Настройте сервер RADIUS

Для использования подарка учетных записей пользователя на сервере RADIUS для доступа к GUI, эти действия должны быть выполнены:

DCM должен быть настроен как клиент к серверу RADIUS.

1. Добавьте IP DCM как клиент для сервера RADIUS.

2. Добавьте общий секретный ключ к конфигурации клиента (этот общий секретный ключ должен совпасть с тем, настроенным на DCM, видеть Настройку раздела DCM).

3. Рекомендуется иметь другой общий секретный ключ для каждого DCM.

4. Длина общего секретного ключа должна быть по крайней мере 22 символа длиной.

5. Общий секретный ключ должен быть максимально случайным.

   Пример хорошего общего секретного ключа: ‘89w% 7w*78619ew8r4$6 @q! 9we# % %^rnEWR @#QEws13&4^ sf54gsf4! fg3sdf# sdf$d3g44fg3%2s2345’

Для учетной записи пользователя сообщение Access-Accept от сервера RADIUS должно иметь атрибут RADIUS, который определяет группу учетной записи GUI, которой принадлежит пользователь. Название атрибута может быть выбрано и должно быть настроено в файле параметров настройки на DCM.

Это - формат строки, которая должна быть передана как значение за атрибутом от сервера RADIUS:

OU = <group_name_string> group_name_string может быть одним из них:

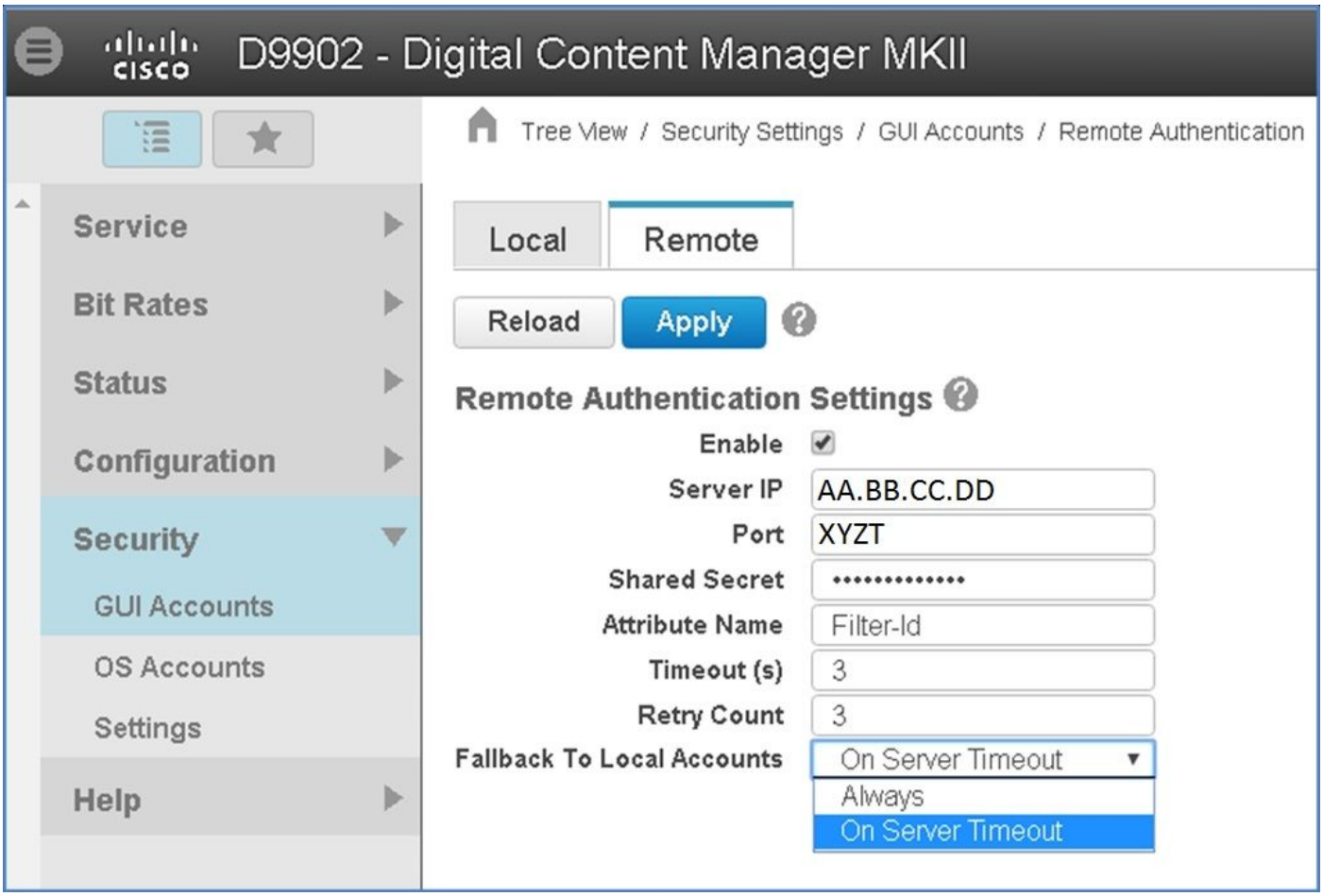
Группа	Строка имени группы
Администраторы (полное управление)	администраторы
Пользователи (Чтение-запись)	пользователи
Гости (только для чтения)	гости
Триггеры автоматизации (Внешний Триггеры)	автоматизация
Администраторы DTF (ключ DTF !--- конфигурацию	dtfadmins

Настройте DCM Cisco

Для включения функции удаленной аутентификации на DCM, Учетная запись администратора GUI требуется.
Эти шаги указывают, как настроить удаленную аутентификацию:

Шаг 1. Вход в систему к DCM с помощью Учетной записи администратора.

Шаг 2. Перейдите к **Безопасности> Учетные записи GUI** и выберите вкладку **Remote**, как показано в образе:



Шаг 3. Настройте параметры, требуемые для связи RADIUS:

- Enable - Эта установка определяет, должна ли поддержка Удаленной аутентификации быть включена или нет. Когда включен проверенный остаток полей parameter.
- IP - сервер - IP-адрес сервера RADIUS.
- Порт - Порт, на котором сервер RADIUS прислушивается к пакетам проверки подлинности (обычно 1812, но может быть настроен к другим значениям).
- Тайна - Это - общий секретный ключ, который используется для шифрования пароля прежде, чем передать Пакет RADIUS к серверу. Эта тайна должна совпасть с, который настроил на сервере RADIUS, где это используется для дешифрования пароля.
- Название атрибута - название атрибута, в котором данные авторизации получены от

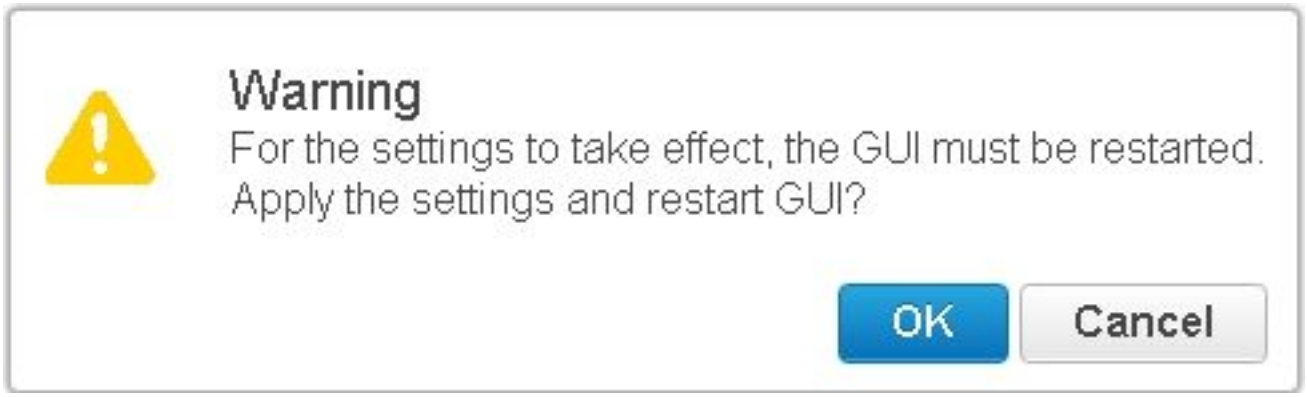
сервера RADIUS.

- Таймаут (в секундах) - Эта установка используется для связи между сервером RADIUS и DCM. Это - время, когда DCM должен ждать ответа от сервера RADIUS для определенного запроса прежде, чем завершить запрос.

- Число повторов - Число раз, которое должен быть передан Запрос RADIUS в случае, если предыдущие запросы вызваны таймаут.

- Нейтрализация К Локальным учетным записям - Эта установка доступна от версии 19.0 DCM и далее. DCM позволяет входить в систему использования GUI (локальная) учетная запись, которая создана с помощью GUI. Опция, **На Server Timeout** позволяет нейтрализации к локальным учетным записям в случае, если сервер RADIUS не может быть достигнут, и не, когда отказала аутентификация. Опция, **Всегда** позволяет нейтрализации всегда – даже когда отказала аутентификация.

Шаг 4. . Поскольку изменения применены, предупреждение, показанное в образе , отображено. Нажмите **OK**, и интерфейс пользователя перезапущен.



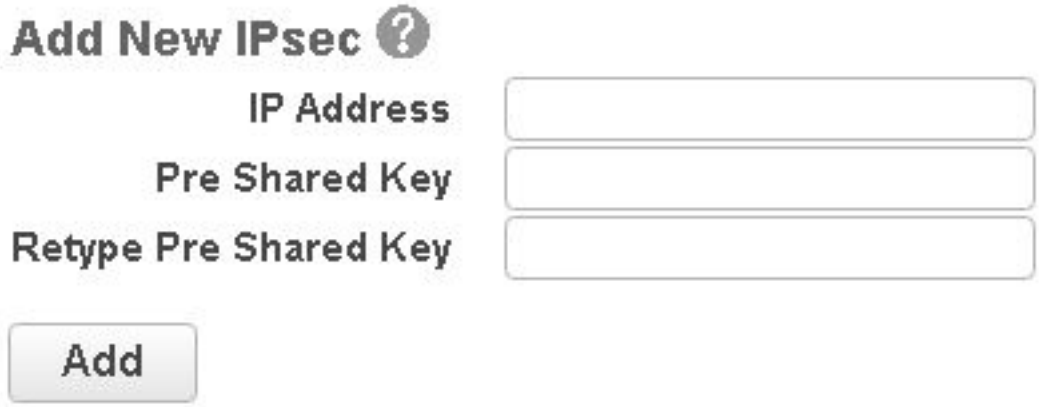
Шаг 5. . Теперь DCM готов к удаленной аутентификации.

Настройте IPSec на DCM:

1. Войдите в систему DCM с помощью учетной записи GUI, которая принадлежит группе безопасности Администраторов.

2. Перейдите к **Configuration> System**. Страница System Settings появляется.

3. См. **Add New** область **IPsec**, как показано в образе.



4. В поле IP Address введите IP-адрес нового узла IPsec (сервер RADIUS).

5. В **Пред** поля **Общий ключ** и *Retype Pre Shared Key*, войдите *Пред Общий ключ* для нового узла IPsec.

6. **Нажмите Add**. Новый узел IPsec добавлен к таблице Параметров настройки IPsec.

> **Примечание:** Для конфигурации IPSec на машине, на которой работает сервер RADIUS, ссылаются на документацию/публикацию, которой предоставляют продукт.

Вопросы обеспечения безопасности

- Общий секретный ключ сохранен в ясном в файловой системе DCM.
- Зашифрованный пароль сохранен в памяти о DCM для использования в повторной проверке подлинности на время сеанса.
- Учитывая эти два элемента выше, рекомендуется ограничить, у кого есть доступ устранения проблем к DCM.
- Настоятельно рекомендуется использовать IPSec для обеспечения канала связи между DCM и RADIUS
  сервер.

Ограничения и ограничения

- Поддержка удаленной аутентификации только доступна для учетных записей GUI, не для учетных записей ОС.
- Повторная проверка подлинности сделана в интервале 15 минут. Пример: Если группа пользователя была изменена, время наихудшего случая, потраченное для изменения для взятия влияния, составляет 15 минут.
- Если учетная запись пользователя допустима или не и затем проверяет локальную базу данных, если удаленная аутентификация включена, первые проверки DCM с сервером

RADIUS. В случае использования локальных учетных записей, которые не существуют на сервере RADIUS, на сервере RADIUS было бы сообщение ошибки проверки подлинности.

Установите freeRadius

Этот раздел показывает как пример, как установить freeRadius для использования в качестве сервера удаленной аутентификации для DCM. Это для получений информации только,

Cisco не предоставляет или поддерживает freeRadius. Предполагается, что файлы конфигурации для freeRadius найдены под**/etc/freeRadius/**(проверьте распределение).

После установки freeRadius пакет модифицируют эти файлы.

- Модифицируйте**/etc/freeradius/clients.conf**
  Шаг 1. Добавьте запись для IP DCM к списку клиентов.
  Шаг 2. Добавьте общий ключ в конфигурации клиента и оставьте другие параметры для установки по умолчанию.

  Рекомендуется иметь уникальный общий секретный ключ для каждого DCM.
  Длина общего секретного ключа должна быть по крайней мере 22 символа длиной.
  Общий секретный ключ должен быть максимально случайным.

  Пример хорошего общего секретного ключа:
  ‘89w% 7w*78619ew8r4$6 @q! 9we# % %^rnEWR @#QEws13&4^ sf54gsf4! fg3sdf# sdf$d3g44fg3%2s2345’

- Модифицируйте**/etc/freeradius/radiusd.conf** для изменения порта, на котором сервер RADIUS должен слушать (обычно 1812)

- Модифицируйте**/etc/freeradius/users** для добавления новых пользователей.

- Убедитесь для добавления атрибута RADIUS, в котором сведения авторизации передаются DCM в этом формате:
  <Название атрибута> = **'OU = <group_name>'**

  Наименование атрибута: Это - название стандартного атрибута RADIUS, на котором данные авторизации передаются DCM group_name, может быть одно из придерживающегося:
  администраторы - у пользователя, который принадлежит этой группе, будут администраторские привилегии т.е. Полное управление.
  пользователи - у пользователя, который принадлежит этой группе, будут привилегии чтения-записи.
  гости - у пользователя, который принадлежит этой группе, будет привилегия только для чтения.

автоматизация - Используемый для автоматизации (Внешние триггеры).
dtfadmins - Администратор DTF (Конфигурация Ключа DTF)

Пример:
Нешифрованный пароль steve: = "тестирование"
Filter-Id = "OU=administrators"

- (Ре) запускает сервер RADIUS для изменений для вступления в силу.
- Гарантируйте, что конфигурация межсетевого экрана сервера RADIUS позволяет внешний доступ выбранному
порт.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Для отладки целей некоторые дополнительные журналы были введены в Журнал мониторинга безопасности. Для просмотра этого журнала, перешли к **странице Help> Traces** в GUI DCM.

В этом разделе описываются, что искать в журналах, чем проблемы могли быть и возможные решения.

Строка журнала	Попытка удаленного входа в систему отказала: Запрос к серверу RADIUS был вызван таймаут.
Проблема	DCM не в состоянии связаться с сервером RADIUS.
Возможное решение	• Проверьте, что IP-адрес сервера RADIUS, предоставленный в конфигурации удаленной аутентификации в DCM, фактически корректен. • Гарантируйте, что сервер RADIUS доступен от DCM. • Гарантируйте, что DCM настроен как допустимый клиент на сервере RADIUS (сервер RADIUS тихо отбрасывает Пакеты запроса доступа от неизвестных клиентов). • Гарантируйте, что общий секретный ключ, настроенный на DCM, совпадает с общи секретным ключом, настроенным на сервере RADIUS для того определенного DCM (Если сервер не обладает общим секретным ключом для клиента, запрос тихо отброшен.)
Строка журнала	Попытка удаленного входа в систему отказала: [Errno 10054] существующее соединение был насильственно закрыт удаленным хостом.
Проблема	DCM передал Запрос RADIUS к указанному IP - серверу. Однако приложение сервера RADIUS не слушает на порту, заданном в параметрах настройки удаленной аутентификации.
Возможное решение	• Гарантируйте, что работает сервер RADIUS.

	• Проверьте, что Номер порта, заданный в Конфигурации RADIUS на сервере, совпадает с тем, настроенным на DCM.
Строка журнала	Попытка удаленного входа в систему отказала: Недопустимое заданное название атрибута или ответ от сервера RADIUS недостающие данные авторизации.
Проблема	Существует проблема с ответом, полученным от сервера RADIUS.
Возможное решение	• Гарантируйте, что сервер RADIUS передает атрибут (настроенный на DCM) в ответе ‘Access-Accept’.
	• Гарантируйте, что параметр **Названия атрибута**, настроенный на параметрах настройки удаленной аутентификации DCM, является точным именем, как задано в пользовательской конфигурации на сервере RADIUS.
Строка журнала	Недопустимые данные авторизации получены от сервера RADIUS.
Проблема	Аутентификация успешно выполнилась, но ответ, полученный от сервера RADIUS, содержит недопустимые данные авторизации т.е. название группы безопасности.
Возможное решение	• Гарантируйте, что имя группы, настроенное на сервере RADIUS для того пользователя, является одним из названия группы безопасности, заданного в сервере RADIUS Настройки раздела.
	• Гарантируйте, что формат строки, настроенной на сервере RADIUS, согласно тому заданному в сервере RADIUS Настройки раздела.