Содержание

Введение

Этот документ описывает, как интегрировать Cisco Security Manager с сервером Cisco Secure Access Control Server (ACS).

Cisco Secure ACS предоставляет авторизацию для выполнения команд для пользователей, которые используют приложения управления сетью, такие как Cisco Security Manager, для настройки устройств управляемой сети. Поддержка авторизации для выполнения команд оказана уникальными типами набора авторизации для выполнения команд, названными ролями в Cisco Security Manager, которые содержат ряд разрешений. Эти разрешения, также названные привилегиями, определяют действия, которые пользователи со специальными ролями могут выполнить в Cisco Security Manager.

Cisco Secure ACS использует TACACS + для передачи с приложениями управления сетью. Для Cisco Security Manager для передачи с Cisco Secure ACS необходимо настроить Сервер CiscoWorks в Cisco Secure ACS как клиент AAA, который использует TACACS +. Кроме того, необходимо предоставить Серверу CiscoWorks имя и пароль администратора, которое вы используете для вхождения в Cisco Secure ACS. При выполнении этих требований это гарантирует законность связи между Cisco Security Manager и Cisco Secure ACS.

Когда Cisco Security Manager первоначально связывается с Cisco Secure ACS, он диктует ACS Cisco создание ролей по умолчанию, которые появляются в разделе Общих компонентов профиля интерфейса HTML Cisco Secure ACS. Это также диктует службу

поддержки, которая будет авторизоваться TACACS +. Эта служба поддержки появляется на странице TACACS + (Cisco IOS®) в разделе Конфигурации интерфейса интерфейса HTML. Можно тогда модифицировать разрешения, включенные в каждую роль Cisco Security Manager, и применить эти роли к пользователям и группам пользователей.

Примечание: Не возможно интегрировать CSM с ACS 5.2, поскольку это не поддерживается.

Предварительные условия

Требования

Для использования Cisco Secure ACS удостоверьтесь что:

- Вы определяете роли, которые включают команды, требуемые для выполнения необходимых функций в Cisco Security Manager.
- Ограничение доступа к сети (NAR) включает группу устройств (или устройства), что вы хотите администрировать при применении NAR к профилю.
- Названия управляемого устройства записаны и использованы для своей выгоды тождественно в Cisco Secure ACS и в Cisco Security Manager.

Используемые компоненты

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

- Версия 3.0 Cisco Security Manager
- Версия 3.3 Cisco Secure ACS

Примечание: Удостоверьтесь, что вы выбираете совместимый CSM и версии ACS перед установкой на сетевой среде. Например, Cisco протестировала ACS 3.3 с только CSM 3.0 и остановилась для более поздних версий CSM. Так, вам рекомендуют использовать CSM 3.0 с ACS 3.3. Посмотрите Матрицу данных Compatabilty для получения дополнительной информации о различных версиях программного обеспечения.

Версии Cisco Security Manager	Протестированные версии ACS CS
3.0.0 3.0.0 SP1	Windows 3.3 (3) и 4.0 (1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Механизм решений 4.0 (1) Windows 4.0 (1)
3.1.0 3.0.2	Механизм решений 4.0 (1) Windows 4.1 (1) и 4.1 (3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Механизм решений v4.0 (1) Windows 4.1 (2), 4.1 (3) и 4.1 (4)
3.1.1 SP1	Механизм решений 4.0 (1) Windows 4.1 (4)
3.1.1 SP2	Механизм решений 4.0 (1) Windows 4.1 (4) и 4.2 (0)
3.2.0	Механизм решений 4.1 (4) Windows 4.1 (4) и 4.2 (0)

3.2.1	Механизм решений 4.1 (4) Windows 4.2 (0)

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Интегрируйте Cisco Security Manager с Cisco Secure ACS

В этом разделе описываются шаги, требуемые интегрировать Cisco Security Manager с Cisco Secure ACS. Некоторые шаги содержат несколько подшагов. Эти шаги и подшаги должны быть выполнены в заказе. Этот раздел также содержит ссылки на конкретные процедуры, используемые для выполнения каждого шага.

Выполните следующие действия:

1. **Запланируйте свою административную проверку подлинности и модель авторизации.**Необходимо выбрать административную модель перед использованием Cisco Security Manager. Это включает определение административных ролей и учетных записей, которые вы планируете использовать.**Совет:** Когда вы определяете роли и разрешения потенциальных администраторов, также рассматриваете, разрешить ли Поток операций. Этот выбор влияет, как можно ограничить доступ.
2. **Установите Cisco Secure ACS, Cisco Security Manager и CiscoWorks Common Services.**Установите версию 3.3 Cisco Secure ACS на сервере Windows 2000/2003. Установите CiscoWorks Common Services и Cisco Security Manager на другом Windows 2000/Windows 2003 Server.Дополнительные сведения см. в следующих документах:Руководство по установке для Cisco Security Manager 3.0Руководство по установке для Cisco Secure ACS для Windows 3.3**Примечание:** Посмотрите таблицу матрицы совместимости для получения дополнительной информации перед выбором версий программного обеспечения ACS и CSM.
3. **Выполните процедуры интеграции в Cisco Secure ACS.**Определите пользователей Cisco Security Manager как пользователей ACS и назначьте их на группы пользователей на основе их запланированной роли, добавьте все свои управляемые устройства (а также сервер CiscoWorks/Менеджера безопасности) как клиенты AAA и создайте пользователя административного управления. См. Процедуры Интеграции, Выполненные в Cisco Secure ACS для получения дополнительной информации.
4. **Выполните процедуры интеграции в CiscoWorks Common Services.**Настройте локального пользователя, который совпадает с администратором, определенным в Cisco Secure ACS, определите того же самого пользователя для системной идентификационной настройки и настройте ACS как режим настройки AAA.См. Процедуры Интеграции, Выполненные в CiscoWorks для получения дополнительной информации.

5. **Назначьте роли на группы пользователей в Cisco Secure ACS.**Назначьте роли на каждую группу пользователей, настроенную в Cisco Secure ACS. Процедура, которую вы используете, зависит от того, настроили ли вы сетевые группы устройств (NDGs).Посмотрите Назначают Роли на Группы пользователей в Cisco Secure ACS для получения дополнительной информации.

Процедуры интеграции, выполненные в Cisco Secure ACS

В этом разделе описываются шаги, которые необходимо выполнить в Cisco Secure ACS для интеграции его с Cisco Security Manager:

1. Определите пользователей и группы пользователей в Cisco Secure ACS
2. Добавьте управляемые устройства как клиентов AAA в Cisco Secure ACS
3. Создайте пользователя административного управления в Cisco Secure ACS

Определите пользователей и группы пользователей в Cisco Secure ACS

Все пользователи Cisco Security Manager должны быть определены в Cisco Secure ACS и назначили роль, соответствующую их рабочей функции. Самый легкий способ сделать это должно разделить пользователей на различные группы на основе каждой роли по умолчанию, доступной в ACS. Например, назначьте всех системных администраторов на одну группу, всех операторов сети другой группе, и так далее. См. Роли Cisco Secure ACS По умолчанию для получения дополнительной информации о ролях по умолчанию в ACS.

Кроме того, необходимо создать дополнительного пользователя, которому назначают роль системного администратора с полными полномочиями. Учетные данные, установленные для этого пользователя, позже используются на Системной Идентификационной Странице настройки в CiscoWorks. Посмотрите Определяют Системного Идентификационного Пользователя для получения дополнительной информации.

Обратите внимание на то, что на данном этапе вы просто назначаете пользователей на различные группы. Фактическое присвоение ролей этим группам выполнено позже, после CiscoWorks Cisco Security Manager и любые другие приложения зарегистрированы к Cisco Secure ACS.

Совет: Перед переходом, CiscoWorks Common Services Установки и Cisco Security Manager на одном сервере Windows 2000/2003. Установите Cisco Secure ACS на другом сервере Windows 2000/2003.

1. Войдите к Cisco Secure ACS.
2. Настройте пользователя с полными полномочиями:Нажмите **User Setup** на панели навигации.На странице User Setup введите имя для нового пользователя, затем нажмите **Add/Edit**.Выберите метод аутентификации из списка Проверки подлинности с помощью пароля при Настройке пользователя.Введите и подтвердите пароль для нового пользователя.Выберите **Group 1** как группу, на которую назначают пользователю.Нажмите **Submit** для создания учетной записи пользователя.
3. Повторите шаг 2 для каждого пользователя Cisco Security Manager. Cisco рекомендует разделить пользователей на группы на основе роли, каждому пользователю назначают:Группа 1? Системные администраторыGroup 2? Администраторы

безопасностиГруппа 3? Утверждающие лица безопасностиГруппа 4? Администраторы сетиГруппа 5? Утверждающие лицаГруппа 6? Операторы сетиГруппа 7? Техническая поддержкаПосмотрите Таблицу для получения дополнительной информации о разрешениях по умолчанию, привязанных к каждой роли. См. Настройку Ролей Cisco Secure ACS для получения дополнительной информации о настройке ролей пользователя.**Примечание:** На данном этапе сами группы являются наборами пользователей без любых определений роли. Вы назначаете роли на каждую группу после завершения процесса интеграции. Посмотрите Назначают Роли на Группы пользователей в Cisco Secure ACS для получения дополнительной информации.
4. Создайте дополнительного пользователя и назначьте этого пользователя на группу системных администраторов. Учетные данные, установленные для этого пользователя, позже используются на Системной Идентификационной Странице настройки в CiscoWorks. Посмотрите Определяют Системного Идентификационного Пользователя для получения дополнительной информации.
5. Продолжите добавляют управляемые устройства как клиенты AAA в Cisco Secure ACS.

Добавьте управляемые устройства как клиентов AAA в Cisco Secure ACS

Прежде чем можно будет начать импортировать устройства в Cisco Security Manager, необходимо сначала настроить каждое устройство как клиент AAA в Cisco Secure ACS. Кроме того, необходимо настроить сервер CiscoWorks/Менеджера безопасности как клиент AAA.

Если Cisco Security Manager управляет контекстами безопасности, настроенными на устройствах с функциями межсетевого экрана, который включает контексты безопасности, настроенные на FWSM для Catalyst 6500/7600 устройства, каждый контекст должен быть добавлен индивидуально к Cisco Secure ACS.

Метод, который вы используете для добавления управляемых устройств зависит от того, хотите ли вы ограничить пользователей для управления определенным набором устройств с группами сетевых устройств (NDGs). Посмотрите один из этих разделов:

- Если вы хотите, чтобы у пользователей был доступ ко всем устройствам, добавьте, что устройства, как описано в Добавляют Устройства как Клиентов AAA Без NDGs.
- Если вы хотите, чтобы у пользователей был доступ только к определенному NDGs, добавьте, что устройства, как описано в Настраивают сетевые Группы устройств для Использования в Менеджере безопасности.

Добавьте устройства как клиентов AAA без NDGs

Эта процедура описывает, как добавить устройства как клиенты AAA Cisco Secure ACS. См. *Раздел конфигурации Клиента AAA* Конфигурации сети для полной информации обо всех доступных параметрах.

Примечание: Не забудьте добавлять сервер CiscoWorks/Менеджера безопасности как клиента AAA.

1. Нажмите **Network Configuration** на панели навигации Cisco Secure ACS.
2. **Нажмите Add Запись** ниже таблицы Клиентов AAA.

3. Введите имя хоста для клиента AAA (до 32 символов) на странице Add AAA Client. Имя хоста клиента AAA должно совпасть с названием показа, которое вы планируете использовать для устройства в Cisco Security Manager.Например, если вы намереваетесь добавить доменное имя к имени устройства в Cisco Security Manager, имя хоста для клиента AAA в ACS должно быть **<device_name>. <domain_name>**.При именовании Сервера CiscoWorks рекомендуется использовать полностью квалифицированное имя хоста. Обязательно запишите имя хоста правильно. Имя хоста не чувствительно к регистру.Когда вы называете контекст безопасности, добавляете название контекста (_ **<context_name>**) к имени устройства. Для FWSM это - соглашение о записи имен:Блейд FWSM? **<chassis_name> _FW _ <slot_number>**Контекст безопасности? **<chassis_name> _FW _ <slot_number> _ <context_name>**
4. Введите IP-адрес сетевого устройства в поле AAA Client IP Address.
5. Введите общий секретный ключ в Ключевое поле.
6. Выберите **TACACS + (Cisco IOS)** из списка Используемой аутентификации.
7. Нажмите **Submit** для сохранения изменений. Устройство, которое вы добавили, появляется в таблице Клиентов AAA.
8. Повторите шаги 1 - 7 для добавления дополнительных устройств.
9. После добавления всех устройств нажмите **Submit + Перезапуск**.
10. Продолжите создают пользователя административного управления в Cisco Secure ACS.

Настройте сетевые группы устройств для использования в менеджере безопасности

Cisco Secure ACS позволяет вам настроить сетевые группы устройств (NDGs), которые содержат определенные устройства, которые будут управляемы. Например, можно создать NDGs для каждого географического региона или NDGs, которые совпадают организационной структурой. Когда используется с Cisco Security Manager, NDGs позволяют вам предоставить пользователям разные уровни разрешений, на основе устройств, которыми они должны управлять. Например, с NDGs можно назначить Пользователя системный администратор разрешения к устройствам, расположенным в Европе и разрешения Справочного стола к устройствам, расположенным в Азии. Можно тогда назначить противоположные разрешения на Пользователя Б.

NDGs не назначены непосредственно на пользователей. Скорее NDGs назначены на роли, которые вы определяете для каждой группы пользователей. Каждый NDG может быть назначен на одиночную роль только, но каждая роль может включать множественный NDGs. Эти определения сохранены как часть конфигурации для группы выбранного пользователя.

Эти темы выделяют основные шаги, требуемые для настройки NDGs:

- Активируйте опцию NDG
- Создайте NDGs
- Привяжите NDGs и роли с группами пользователей

Активируйте опцию NDG

Необходимо активировать опцию NDG, прежде чем можно будет создать NDGs и заполнить

их с устройствами.

1. Нажмите **Interface Configuration** на панели навигации Cisco Secure ACS.
2. **Нажмите кнопку Дополнительно.**
3. Прокрутите вниз, затем проверьте флажок **Network Device Groups**.
4. **Нажмите кнопку Submit (Отправить).**
5. Продолжите создают NDGs.

Создайте NDGs

Эта процедура описывает, как создать NDGs и заполнить их с устройствами. Каждое устройство может принадлежать только одному NDG.

Примечание: Cisco рекомендует создать специальный NDG, который содержит сервер CiscoWorks/Менеджера безопасности.

1. Нажмите **Network Configuration** на панели навигации.Все устройства первоначально размещены под Не Назначенный, который держит все устройства, которые не были размещены в NDG. Следует иметь в виду, что Не Назначенный не NDG.
2. Создайте NDGs:**Нажмите Add запись**.Введите имя для NDG на странице New Network Device Group. Максимальная длина составляет 24 символа. Пробелы разрешены.**Дополнительный, когда с версией 4.0 или позже:** Введите ключ, который будет использоваться всеми устройствами в NDG. При определении ключа для NDG это отвергает любые ключи, определенные для отдельных устройств в NDG.Нажмите **Submit** для сохранения NDG.Повторите шаги a через d для создания большего количества NDGs.
3. Заполните NDGs с устройствами:Нажмите название NDG в области Network Device Groups.**Нажмите Add Запись** в области AAA Clients.Определите подробные сведения устройства, чтобы добавить к NDG, затем нажать **Submit**. Посмотрите Добавляют Устройства как Клиенты AAA Без NDGs для получения дополнительной информации.Повторите шаги b и c для добавления остатка от устройств к NDGs. Единственное устройство, что можно оставить Не Назначенную категорию внутри, является AAA-сервером по умолчанию.После настройки последнего устройства нажмите **Submit + Перезапуск**.
4. Продолжите создают пользователя административного управления в Cisco Secure ACS.

Создайте пользователя административного управления в Cisco Secure ACS

Используйте страницу Administration Control в Cisco Secure ACS для определения учетной записи администратора, которая используется при определении режима настройки AAA в CiscoWorks Common Services. Посмотрите Настраивают Режим настройки AAA в CiscoWorks для получения дополнительной информации.

1. Нажмите **Administration Control** на панели навигации Cisco Secure ACS.
2. **Нажмите Add администратора**.
3. На странице Add Administrator введите имя и пароль для администратора.
4. Нажмите **Grant All** в области Administrator Privileges для обеспечения полных

административных разрешений этому администратору.
5. Нажмите **Submit** для создания администратора.

Примечание: См. Администраторов и Административную политику для получения дополнительной информации об опциях, доступных, когда вы настраиваете администратора.

Процедуры интеграции, выполненные в CiscoWorks

В этом разделе описываются шаги для завершения в CiscoWorks Common Services для интеграции его с Cisco Security Manager:

- Создайте локального пользователя в CiscoWorks
- Определите системного идентификационного пользователя
- Настройте режим настройки AAA в CiscoWorks

Выполните эти шаги после завершения процедур интеграции, выполненных в Cisco Secure ACS. Общее обслуживание выполняет фактическую регистрацию любых установленных приложений, таких как Cisco Security Manager, Сервер Автоматического обновления и Менеджер IPS в Cisco Secure ACS.

Создайте локального пользователя в CiscoWorks

Используйте Страницу настройки Локального пользователя в CiscoWorks Common Services для создания учетной записи локального пользователя, которая копирует администратора, которого вы создали на предыдущем этапе в Cisco Secure ACS. Эта учетная запись локального пользователя позже используется для системной идентификационной настройки. Видьте дополнительные сведения.

Примечание: Прежде чем вы продолжитесь, создадите администратора в Cisco Secure ACS. Посмотрите Определяют Пользователей и Группы пользователей в Cisco Secure ACS для инструкций.

1. Войдите в CiscoWorks с учетной записью **пользователя с правами администратора** по умолчанию.
2. Выберите **Server> Security from Common Services**, затем выберите **Local User Setup** из TOC.
3. **Нажмите кнопку Add.**
4. Введите то же имя и пароль, которое вы ввели при создании администратора в Cisco Secure ACS. Посмотрите, что шаг 4 в Определяет Пользователей и Группы пользователей в Cisco Secure ACS.
5. Проверьте все флажки под Ролями кроме Данных Экспорта.
6. Нажмите **OK** для создания пользователя.

Определите системного идентификационного пользователя

Используйте Системную Идентификационную Страницу настройки в CiscoWorks Common Services для создания трастового пользователя, известного как Системный Идентификационный пользователь, который включает связь между серверами, которые являются частью того же домена и процессов применения, которые расположены на том же сервере. Приложения используют Системного Идентификационного пользователя для

аутентификации процессов на локальных или удаленных Серверах CiscoWorks. Это особенно полезно, когда приложения должны синхронизироваться, прежде чем любые пользователи вошли.

Кроме того, когда основная задача уже авторизуется для зарегистрированного пользователя, Системный Идентификационный пользователь часто используется для выполнения подзадачи. Например, для редактирования устройства в Cisco Security Manager, межсвязь приложений требуется между Cisco Security Manager и Общим обслуживанием DCR. После того, как пользователь авторизуется выполнить задачу редактирования, Системный Идентификационный пользователь используется для призыва DCR.

Системный Идентификационный пользователь, которого вы настраиваете здесь, должен быть идентичен пользователю с административными (полными) разрешениями, которые вы настроили в ACS. Сбой, чтобы сделать так может привести к неспособности просмотреть все устройства и политику, настроенную в Cisco Security Manager.

Примечание: Прежде чем вы продолжитесь, создадите локального пользователя с тем же именем и паролем как этот администратор в CiscoWorks Common Services. Посмотрите Создают Локального пользователя в CiscoWorks для инструкций.

1. Выберите **Server> Security**, затем выберите **Multi-Server Trust Management> System Identity Setup** от TOC.
2. Введите имя администратора, которого вы создали для Cisco Secure ACS. Посмотрите, что шаг 4 в Определяет Пользователей и Группы пользователей в Cisco Secure ACS.
3. Введите и проверьте пароль для этого пользователя.
4. **Щелкните "Применить".**

Настройте режим настройки AAA в CiscoWorks

Используйте страницу AAA Setup Mode в CiscoWorks Common Services для определения Cisco Secure ACS как AAA-сервера, который включает требуемый порт и общий секретный ключ. Кроме того, можно определить до двух серверов резервного копирования.

Эти шаги выполняют фактическую регистрацию CiscoWorks, Cisco Security Manager, Менеджер IPS (и дополнительно, Сервер Автоматического обновления) в Cisco Secure ACS.

1. Выберите **Server> Security**, затем выберите **AAA Mode Setup** из TOC.
2. Проверьте флажок **TACACS +** под Доступными Модулями Входа в систему.
3. Выберите **ACS** как тип AAA.
4. Введите IP-адреса до трех серверов Cisco Secure ACS в области Server Details. Вторичные и третичные серверы действуют как резервные копии в случае, если отказывает основной сервер.**Примечание:** Если весь настроенный TACACS + серверы не в состоянии отвечать, необходимо войти с Локальной учетной записью CiscoWorks admin, то возвратить режим AAA к Локальной переменной Non-ACS/CiscoWorks. После TACACS + серверы восстановлены сервису, необходимо возвратить режим AAA к ACS.
5. В области Login введите имя администратора, которого вы определили на странице Administration Control Cisco Secure ACS. Посмотрите Создают Пользователя Административного управления в Cisco Secure ACS для получения дополнительной информации.

6. Введите и проверьте пароль для этого администратора.
7. Введите и проверьте общий секретный ключ, который вы ввели, когда вы добавили сервер Менеджера безопасности как клиент AAA Cisco Secure ACS. Посмотрите, что шаг 5 в Добавляет Устройства как Клиентов AAA Без NDGs.
8. Проверьте **Регистр все установленные приложения с** флажком **ACS** для регистрации Cisco Security Manager и любых других установленных приложений с Cisco Secure ACS.
9. **Чтобы сохранить изменения, нажмите Apply.** Индикатор выполнения отображает выполнение регистрации. Когда регистрация завершена, сообщение появляется.
10. Если вы интегрируете Cisco Security Manager с какой-либо версией ACS, перезапускаете Менеджера демона Cisco Security Manager сервис. Посмотрите Перезапуск Менеджер демона для инструкций.**Примечание:** После CSM 3.0.0, Cisco больше не тестирует с ACS 3.3 (x), потому что это в большой степени исправлено, и о его поддержке закончена (EOL) объявили. Поэтому необходимо использовать соответствующую версию ACS для версии CSM 3.0.1 и позже. Посмотрите таблицу матрицы совместимости для получения дополнительной информации.
11. Регистрируйте назад в Cisco Secure ACS для присвоения ролей на каждую группу пользователей. Посмотрите Назначают Роли на Группы пользователей в Cisco Secure ACS для инструкций.**Примечание:** Настройка AAA, настроенная здесь, не сохранена при удалении CiscoWorks Common Services или Cisco Security Manager. Кроме того, эта конфигурация не может быть выполнена резервное копирование и восстановлена после переустановки. Поэтому, если вы обновляете к новой версии любого приложения, необходимо реконфигурировать режим настройки AAA и повторно регистрировать Cisco Security Manager с ACS. Этот процесс не требуется для инкрементных обновлений. Если вы устанавливаете дополнительные приложения, такие как ВшS, поверх CiscoWorks, необходимо повторно регистрировать новые приложения и Cisco Security Manager.

Перезапустите менеджера демона

Эта процедура описывает, как перезапустить Менеджера демона сервера Cisco Security Manager. Необходимо сделать это для параметров настройки AAA, которые вы настроили для вступления в силу. Можно тогда регистрировать назад в CiscoWorks с учетными данными, определенными в Cisco Secure ACS.

1. Войдите в машину, на которой установлен сервер Cisco Security Manager.
2. Выберите **Start> Programs> Administrative Tools> Services** для открытия окна Services.
3. Из списка сервисов, отображенных в правой панели, выберите **Cisco Security Manager Daemon Manager**.
4. Нажмите кнопку **Restart Service** на панели инструментов.
5. Продолжите назначают роли на группы пользователей в Cisco Secure ACS.

Назначьте роли на группы пользователей в Cisco Secure ACS

После регистрации CiscoWorks, Cisco Security Manager и других установленных приложений к Cisco Secure ACS, можно назначить роли на каждую из групп пользователей, которые вы ранее настроили в Cisco Secure ACS. Эти роли определяют действия, которые пользователям в каждой группе разрешают выполнить в Cisco Security Manager.

Процедура, которую вы используете для присвоения ролей на группы пользователей зависит от того, используются ли NDGs:

- Назначьте роли на группы пользователей без NDGs
- Привяжите NDGs и роли с группами пользователей

Назначьте роли на группы пользователей без NDGs

Эта процедура описывает, как назначить роли по умолчанию на группы пользователей, когда не определены NDGs. См. Роли Cisco Secure ACS По умолчанию для получения дополнительной информации.

Примечание: Перед переходом:

- Создайте группу пользователей для каждой роли по умолчанию. Посмотрите Определяют Пользователей и Группы пользователей в Cisco Secure ACS для инструкций.
- Завершите процедуры, описанные в Процедурах Интеграции, Выполненных в Cisco Secure ACS и Процедурах Интеграции, Выполненных в CiscoWorks.

Выполните следующие действия:

1. Войдите к Cisco Secure ACS.
2. Нажмите **Group Setup** на панели навигации.
3. Выберите группу пользователей для системных администраторов из списка. Посмотрите, что шаг 2 Определяет Пользователей и Группы пользователей в Cisco Secure ACS, затем нажимает **Edit Settings**.

Привяжите NDGs и роли с группами пользователей

При соединении NDGs к ролям для использования в Cisco Security Manager необходимо создать определения в двух местах на странице Group Setup:

- Область CiscoWorks
- Область Cisco Security Manager

Определения в каждой области должны совпасть максимально близко. Когда вы привязываете настраиваемые роли или роли ACS, которые не существуют в CiscoWorks Common Services, пытаются определить максимально близкий эквивалент на основе разрешений, назначенных на ту роль.

Необходимо создать ассоциации для каждой группы пользователей, чтобы использоваться с Cisco Security Manager. Например, если у вас есть группа пользователей, которая содержит персонал службы технической поддержки для Западной области, можно выбрать ту группу пользователей, затем привязать NDG, который содержит устройства в той области с ролью Справочного стола.

Примечание: Прежде чем вы продолжитесь, активируете опцию NDG и создадите NDGs. Посмотрите Настраивают сетевые Группы устройств для Использования в Менеджере безопасности для получения дополнительной информации.

1. Нажмите **Group Setup** на панели навигации.

2. Выберите группу пользователей из списка Группы, затем нажмите **Edit Settings**.
3. Сопоставьте NDGs и роли для использования в CiscoWorks:На странице Group Setup прокрутите вниз к области CiscoWorks под TACACS + Параметры настройки.Выберите **Assign a CiscoWorks на на основание группы сетевых устройств**.Выберите NDG из списка Группы устройств.Выберите роль, к которой этот NDG должен быть привязан из второго списка.**Нажмите Add Ассоциацию**. Ассоциация появляется в коробке Группы устройств.Повторите шаги с через е для создания дополнительных ассоциаций.**Примечание:** Для удаления ассоциации выберите ее от Группы устройств, затем нажмите Remove Association.
4. Прокрутите вниз к области Cisco Security Manager и создайте ассоциации, которые совпадают максимально близко с ассоциациями, определенными в шаге 3.**Примечание:** При выборе Security Approver или Ролей администратора безопасности в Cisco Secure ACS рекомендуется выбрать Network Administrator как самую близкую эквивалентную роль CiscoWorks.
5. Нажмите **Submit** для сохранения настроек.
6. Повторите шаги 2 - 5 для определения NDGs для остатка от групп пользователей.
7. После соединения NDGs и ролей с каждой группой пользователей нажмите **Submit + Перезапуск**.

Устранение неполадок

1. Прежде чем можно будет начать импортировать устройства в Cisco Security Manager, необходимо сначала настроить каждое устройство как клиент AAA в Cisco Secure ACS. Кроме того, необходимо настроить сервер CiscoWorks/Менеджера безопасности как клиент AAA.
2. Если вы получаете журнал неудачных попыток, автор отказал с ошибкой в Cisco Secure ACS.`"service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*TestDevices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switchesauthorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"` Для решения этого вопроса удостоверьтесь, что название устройства в ACS должно быть полным доменным именем.

Дополнительные сведения

- Access Control Server Cisco Security для Windows Support Page
- Страница технической поддержки Cisco Security Manager
- Cisco Secure Access Control Server for Windows
- Руководство по конфигурации для Cisco Secure ACS 4.1
- Cisco Secure ACS онлайновое руководство по поиску и устранению проблем, 4.1
- Уведомления о дефектах безопасности продукта (включая CiscoSecure ACS для Windows)
- Cisco Systems – техническая поддержка и документация