Дайте минимальное разрешение к учетной записи пользователя Active Directory, используемой клиентом User Agent Sourcefire

Содержание

Введение

Этот документ описывает, как предоставить пользователя Active Directory (AD) минимальными разрешениями, должен был сделать запрос AD контроллера домена. Клиент User Agent Sourcefire использует AD пользователя для запроса AD контроллера домена. Для выполнения запроса AD пользователь не требует никаких дополнительных разрешений.

Предварительные условия

Требования

Cisco требует, чтобы вы установили Клиента User Agent Sourcefire в системе Microsoft Windows и предоставили доступ к AD контроллеру домена.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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.

Настройка

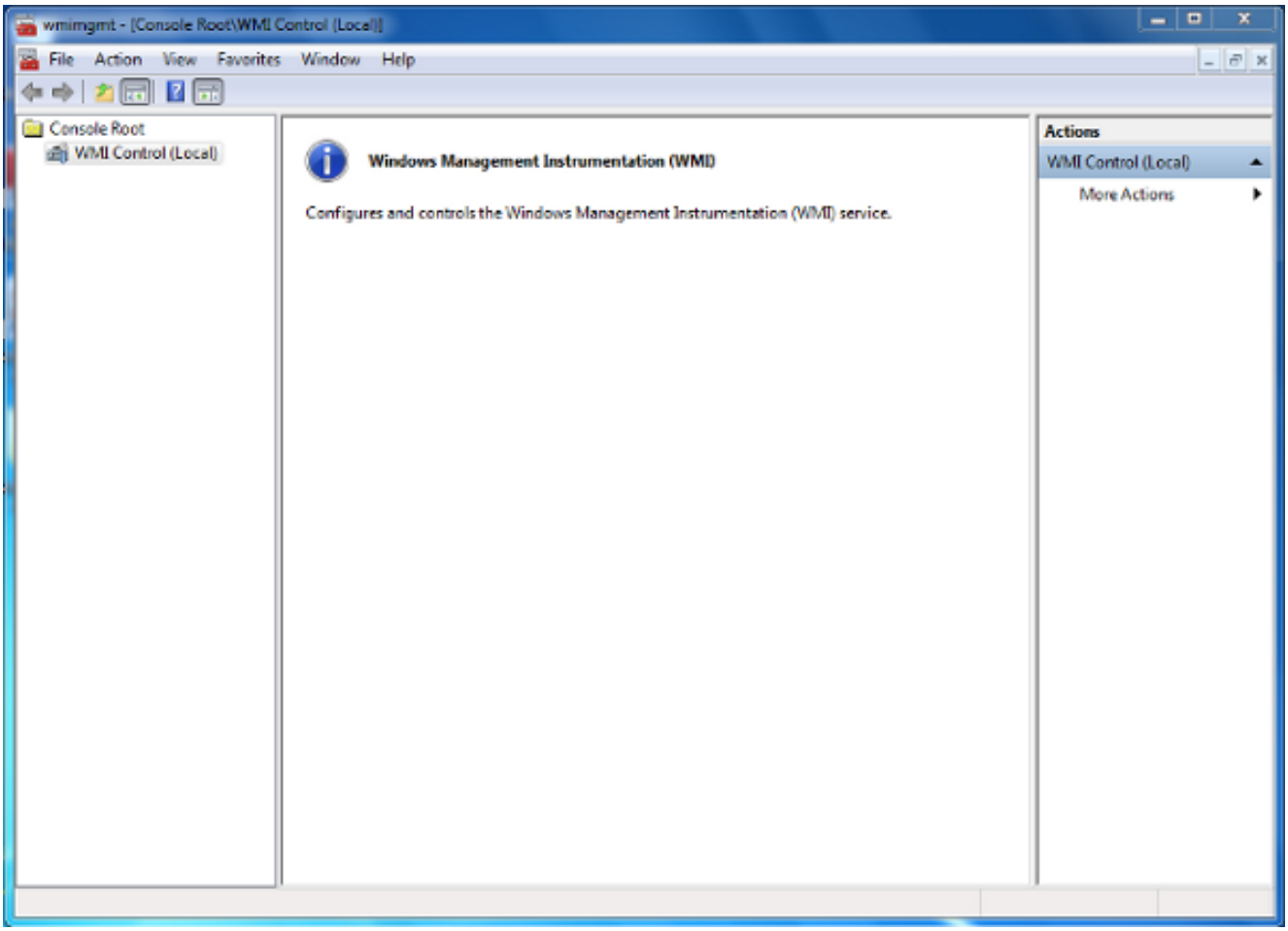
Во-первых, администратор должен создать нового AD пользователя в частности для доступа Клиента User Agent. Если этот новый пользователь не является участником группы администраторов домена (и они не должны быть), пользователю, возможно, придется быть явно данным разрешением для доступа к Журналам мониторинга безопасности инструментария управления Windows (WMI). Для давания разрешения выполните эти шаги:

1. Откройте пульт управления WMI:

   На AD сервере выберите **Меню Пуск**.

   Нажмите **Run** и введите **wmimgmt.msc**.

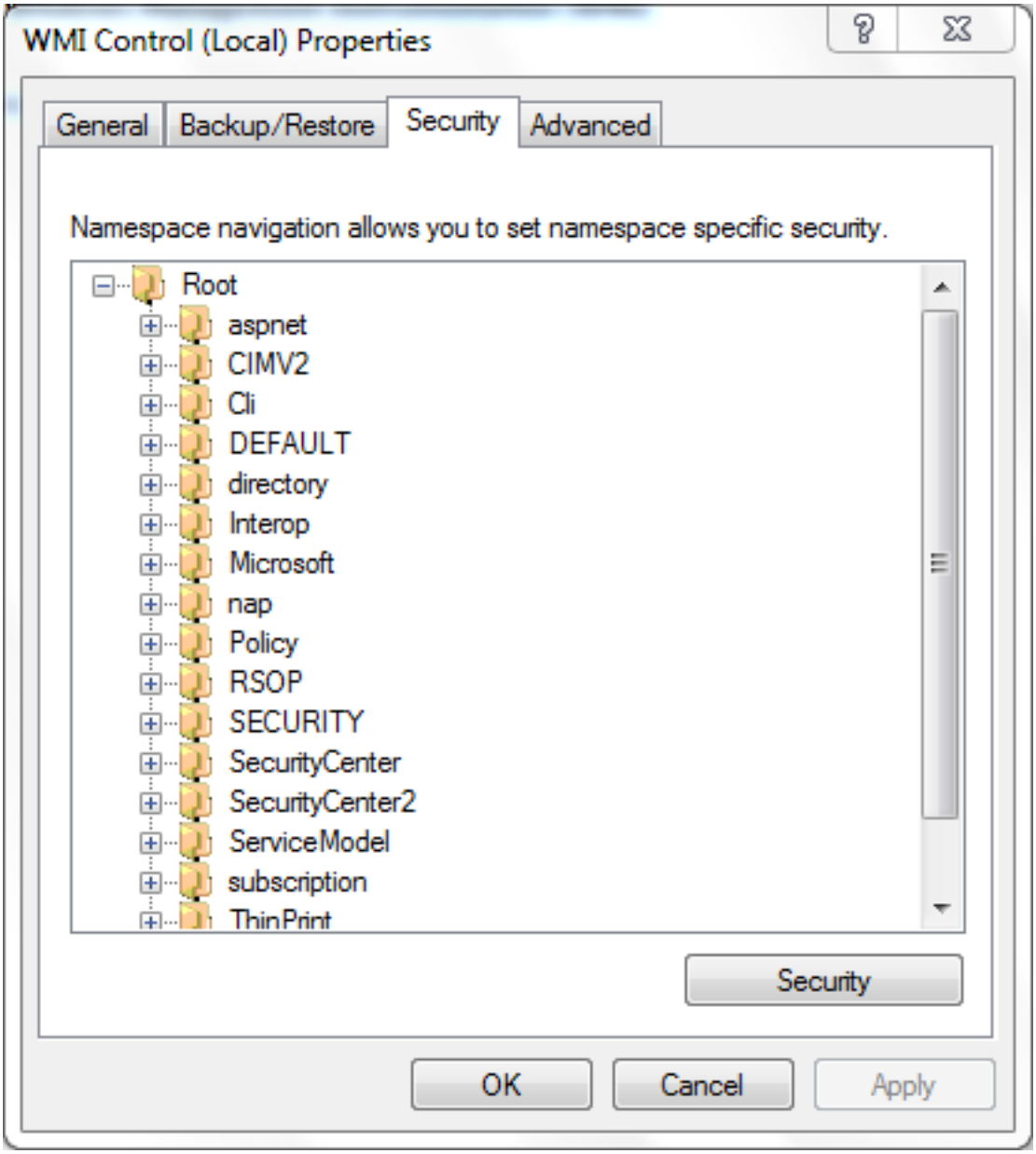
   Нажмите кнопку ОК. Пульт управления WMI появляется.



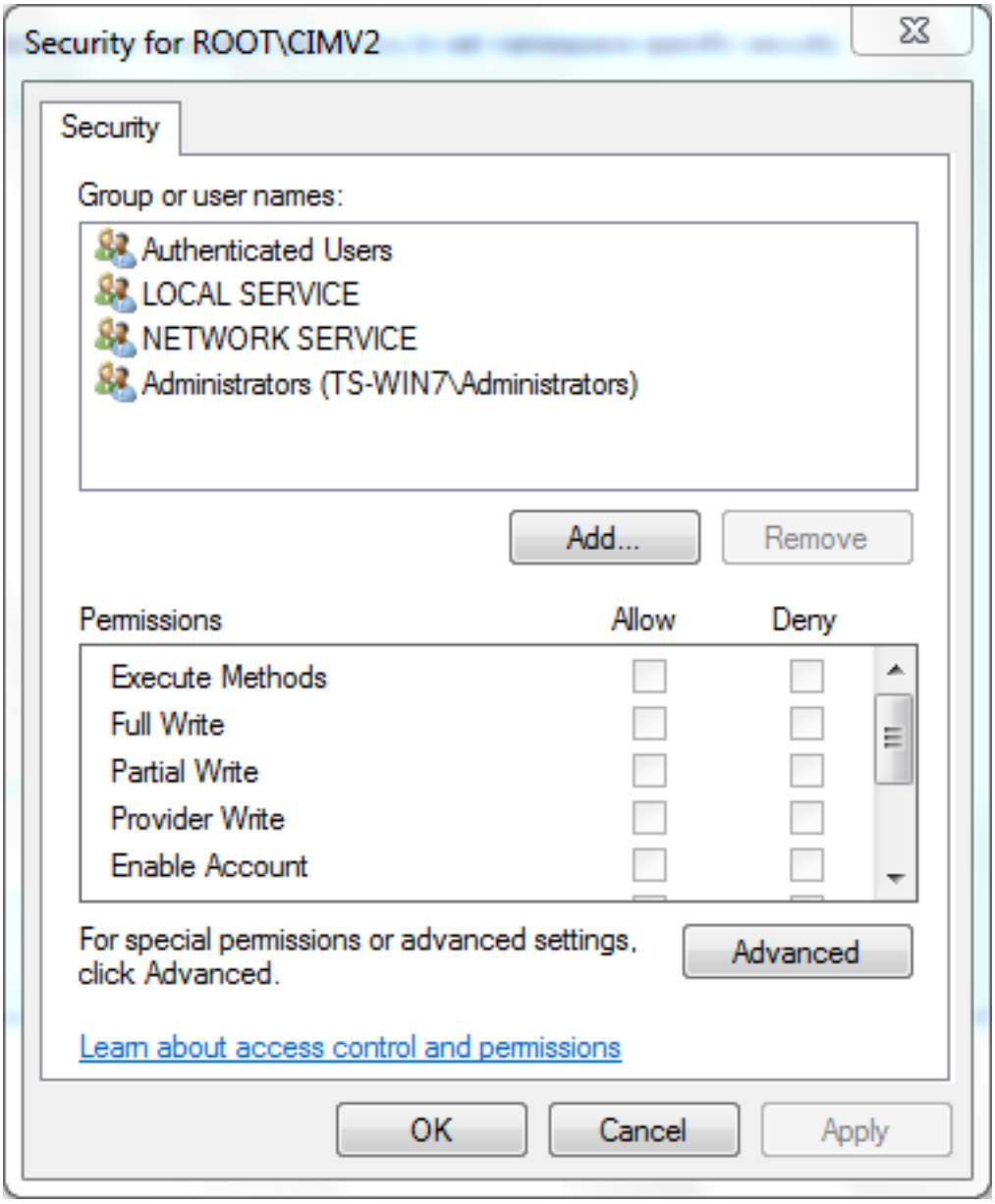
2. На дереве консоли WMI щелкните правой кнопкой мыши **Контроль за WMI** и затем нажмите **Properties**.

3. **Щелкните вкладку Безопасность.**

4. Выберите пространство имен, для которого вы хотите дать пользователю или групповому доступу (**`Root\CIMV2`**), и затем нажмите **Security**.



5. В коробке Настройки безопасности **нажмите Add**.



6. В Диалоговом окне Select Users, Computers, or Groups введите имя объекта (пользователь или группа), что вы хотите добавить. Нажмите **Check Names**, чтобы проверить вашу запись и затем нажать **OK**. Вам, возможно, придется изменить местоположение или нажать **Advanced** для запроса для объектов. Посмотрите Контекстно-зависимую **`справку (?)`** для большего количества подробности.

7. В коробке Настройки безопасности, в разделе Разрешений, выбирают **Allow** или **Deny** для давания разрешений новому пользователю или группе (самый легкий дать все разрешения). Пользователю нужно дать, по крайней мере**, Удаленные Включают** разрешения.

8. Нажмите **Apply** для сохранения изменений. Закройте окно.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

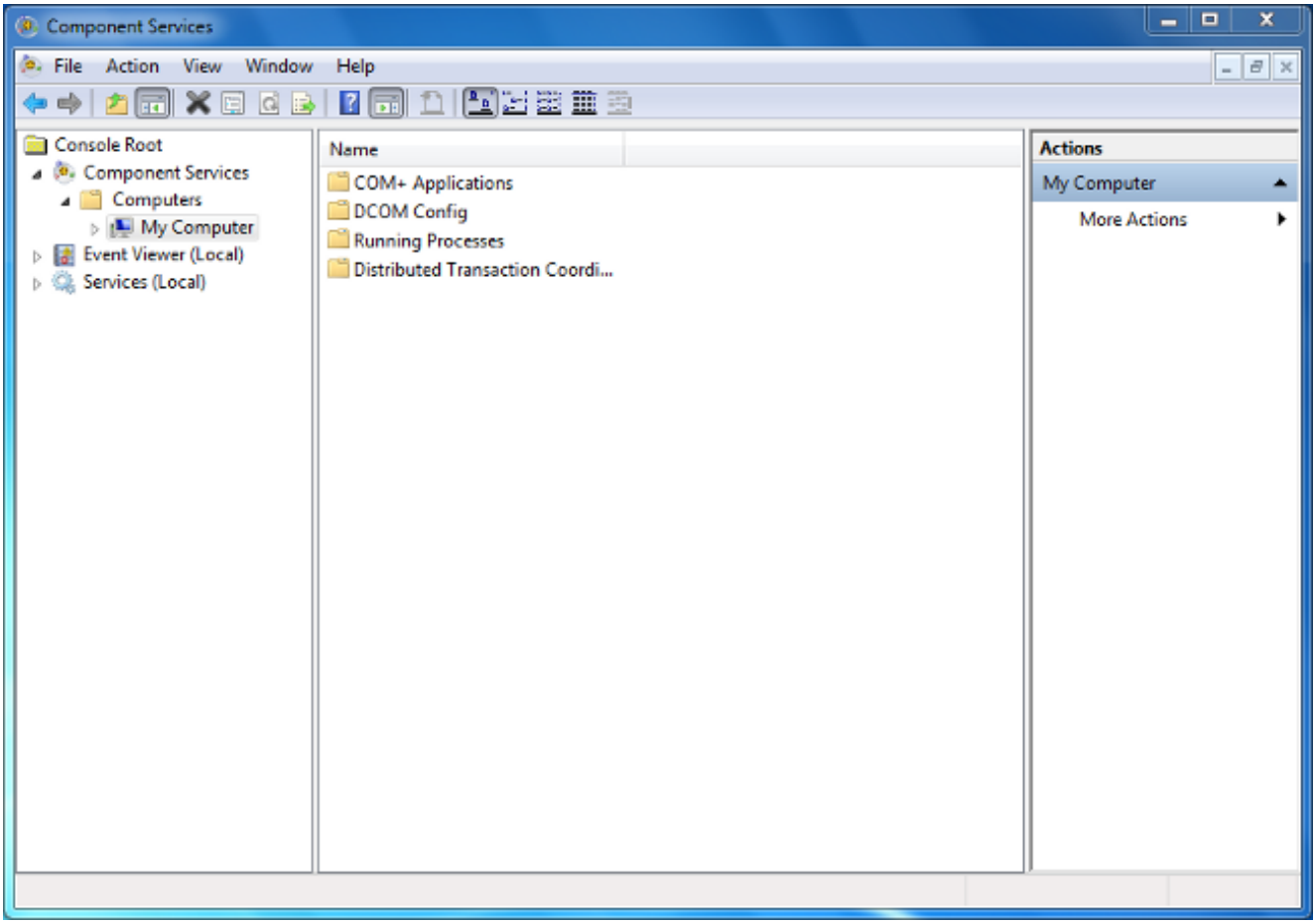
В этом разделе описывается процесс устранения неполадок конфигурации.

Если проблема сохраняется после изменений конфигурации, обновите настройки Распределенной модели компонентных объектов (DCOM) для предоставления удаленного доступа:

1. Выберите **Меню Пуск**.

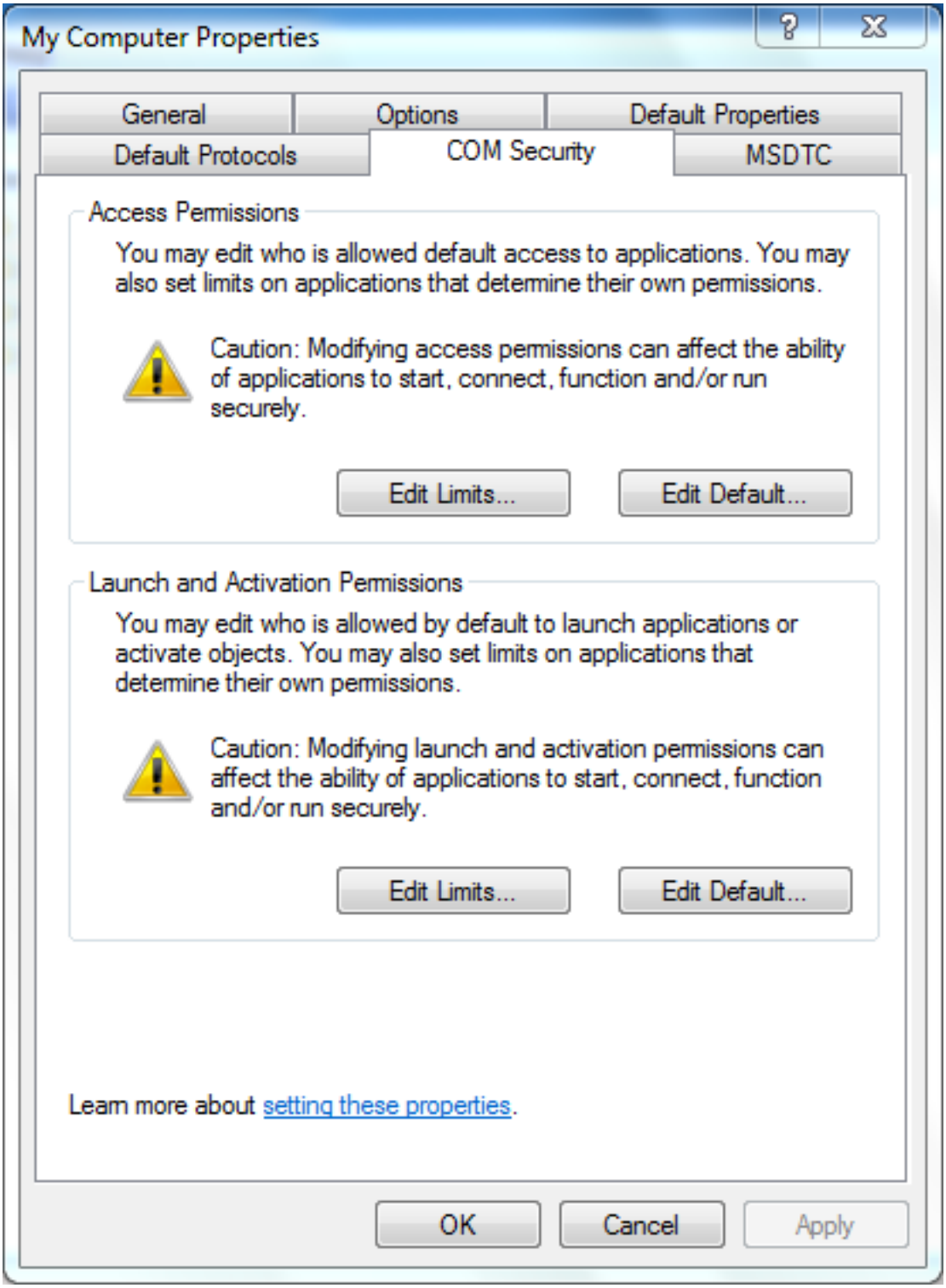
2. Нажмите **Run** и введите **DCOMCNFG**.

3. **Нажмите кнопку ОК.** Диалоговое окно Component Services появляется.



4. В диалоговом окне Component Services разверните **Сервисы компонента**, разверните **Компьютеры**, и затем щелкните правой кнопкой мыши **Мой компьютер** и выберите **Properties**.

5. В Диалоговом окне со свойствами Моего компьютера нажмите **COM Security tab**.



6. В соответствии с Разрешениями Запуска и Активации, нажмите **Edit Limits**.

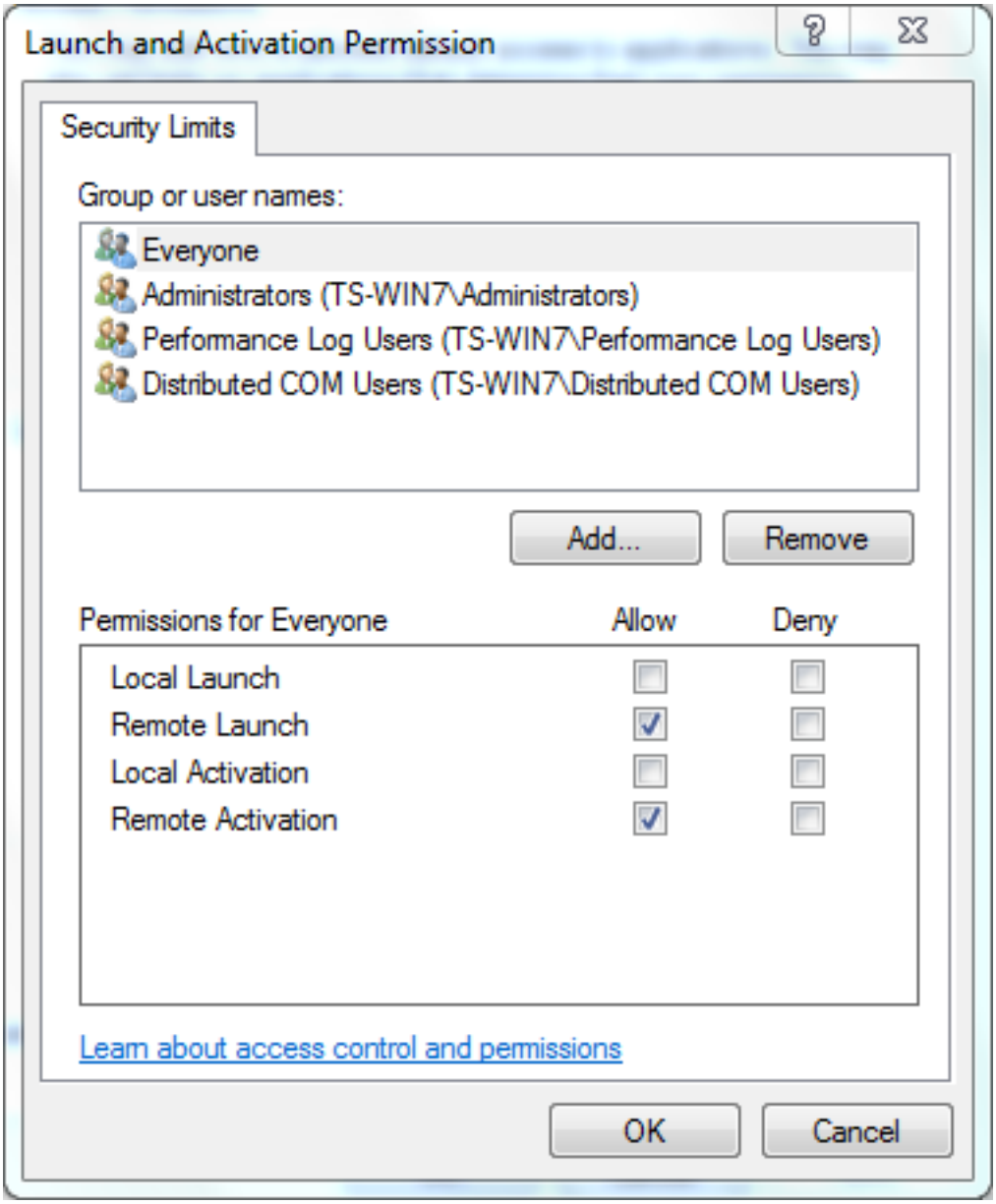
7. В диалоговом окне Launch и Activation Permission выполните эти шаги, если ваше название или ваша группа не появляются в списке Групп или имен пользователей:

   В диалоговом окне Launch и Activation Permission **нажмите Add**.

   В Диалоговом окне Select Users, Computers, or Groups введите свое имя и группу во Введении имен объекта, чтобы выбрать поле, и затем нажать **OK**.

8. В диалоговом окне Launch и Activation Permission выберите своего пользователя и

группу в разделе **имен пользователей или Группе**.



9. В столбце Allow в соответствии с Разрешениями для Пользователя проверьте флажки **Remote Launch и Remote Activation**, и затем нажмите **OK.Примечание:** Имя пользователя должно иметь права сделать запрос для данных регистрационной информации пользователя для входа на AD сервере. Для аутентификации с пользователем через прокси введите полностью определенное имя пользователя. По умолчанию домен для учетной записи, вы использовали входить в компьютер, где вы установили агента, автозаполняет поле Domain. Если пользователь, которого вы предоставляете, является участником другого домена, обновите домен для предоставленных учетных данных пользователя.
10. Если проблема сохраняется на попытке Контроллера домена включить пользователя Управлять контроль и политика Журнала мониторинга безопасности. Для добавления пользователя выполните эти шаги:

    Выберите **редактора менеджмента групповой политики**.

    Выберите **Computer Configuration> Windows Settings> Security Settings> Local Policies>**

User Rights Assignment.

Выберите **контроль Manage и Журнал мониторинга безопасности**.

Добавьте пользователя.