TAC Vista

Программное обеспечение TAC

Руководство по установке

TAC Vista

Программное обеспечение TAC

Руководство по установке

Содержание

Введение

Справочная информация

Введение

1 Об этом Руководстве

1 Об этом Руководстве

Это руководство описывает определенный процесс. Для информации относительно определенных изделий, обратитесь к руководствам рассматриваемых изделий.

Для информации относительно того, как устанавливать программное обеспечение, мы адресуем Вас к инструкциям, поставляемым с программным обеспечением.

Для информации относительно изделий сторонних производителей, мы адресуем Вас к инструкциям, поставляемым с их продукцией.

Если вы найдете ошибки и/или неточные описания в этом руководстве, пожалуйста, свяжитесь с вашим представителем TAC.

Примечание

- Мы постоянно дополняем и корректируем нашу документацию. Это руководство также может быть обновлено.

  Пожалуйста обратитесь к каталогу Docnet на нашем сайте www.tac.ru для получения последней версии.

1.1 Структура

Это руководство разделено на следующие разделы:

- **Введение**
  Раздел Введение содержит информацию относительно того, как структурировано данное руководство, и как оно должно использоваться, для нахождения информации наиболее эффективным способом.
- **Справочная информация**
  Раздел Справочная информация содержит более подробную информацию относительно различных частей раздела "Подготовка к работе". Он также содержит информацию относительно альтернативных решений, не описанных в разделе "Подготовка к работе".

1.2 Типографские соглашения

В руководстве имеется специально выделенный текст, означающий:

Предупреждение

- Предупреждает вас о возможных ошибках или определенных действиях, которые могут привести к физическим неполадкам оборудования.

Внимание

- Используется для предупреждений, невыполнение которых может привести к серьезным последствиям.

Важно

- Содержит дополнительную информацию, существенную для завершения задачи.

Примечание

- Содержит текст, выделяющий определенную информацию.

Совет

- Содержит дополнительную информацию, не существенную для завершения данной задачи.

Углублённо

- Содержит информацию, касающуюся сложных задач или задач с ограниченным доступом.

СПРАВОЧНАЯ ИНФОРМАЦИЯ

2 Установка TAC Vista Server

Поскольку TAC Vista Server и компоненты, включённые в пакет TAC Vista Config, являются приложениями на основе .NET, Вам необходимо начинать с установки .NET Framework. TAC Vista Server использует базу данных Microsoft SQL Desktop Engine 2000 (MSDE). MSDE база данных включена в пакет TAC Vista Config. Вам необходимо установить TAC Vista Config перед установкой TAC Vista Server.

Важно чтобы Вы выполняли установку в следующем порядке:

- .NET Framework Redistributable Version 2.0 Package
- TAC Vista Config 1.3.0
- TAC Vista Server 5.0.0

2.1 Пакет .NET Framework Redistributable версии 2.0

Вы можете скачать пакет Microsoft .NET Framework Redistributable версии 2.0 с сайта Microsoft.

2.2 TAC Vista Config 1.3.0

TAC Vista Config 1.3.0 TAC Vista Server 5.0.0, включая TAC Vista Workstation, Вы можете загрузить из корпоративной сети TAC extranet.

Пакет TAC Vista Config содержит Microsoft SQL Server 2000 (MSDE2000) с Service Pack 4. Если Вы хотите пользоваться этим сервером SQL, выберите установку по умолчанию, что приведет к **установке Microsoft SQL Server, MSDE 2000**. В этом случае база данных будет управляться (поддерживаться) Вистой.

Если у Вас уже установлена версия Enterprise или Standard базы данных SQL, выберите при установке опцию **A Microsoft SQL server is already installed**. За дополнительной информацией как установить версию Enterprise или Standard базы данных SQL обратитесь к руководству по установке *Установка TAC Vista с Microsoft SQL Server 2000 версии Standard или Enterprise*.

За дополнительной информацией как обновить Ваш сервер SQL обратитесь к руководству по установке:

- *Обновление Microsoft SQL Server 2000 MSDE до версии Standard или Enterprise или*

- *Обновление управляемой пользователем SQL базы данных*

Важно

- Если Вы устанавливаете TAC Vista с CD диска "TAC Software" пакет TAC Vista Config включен в процесс установки. В этом случае *не* требуется установка TAC Vista Config отдельно перед запуском инсталляционного CD.

2.3 TAC Vista Server 5.0.0

TAC Vista Server 5.0.0, включая TAC Vista Workstation, может быть загружен из корпоративной сети TAC extranet..

Рекомендуется, чтобы Вы установили Microsoft Excel перед установкой TAC Vista Server. MS Excel требуется для формирования отчетов в Висте (Vista).

Также рекомендуется, чтобы Вы установили правильную версию среды Java environment перед установкой TAC Vista Server. Вы можете загрузить нужную версию Java из корпоративной сети TAC extranet..

Внимание

- Если у Вас установлен один или более сертификатов для работы веб-сервера, удалите их перед установкой Висты.
- Переустановите сертификаты после инсталляции.
- За дополнительной информацией обращайтесь:

  http://support.microsoft.com/kb/309398

Примечание

- Если Вы устанавливаете TAC Vista с CD диска "TAC Software", Вы найдете доступные Вам программы в пункте меню TAC Vista 5.
- Для установки TAC Vista Server 5.0.0 с TAC Vista Workstation с инсталляционного CD, выберите TAC Vista Full Install.

2.3.1 Полная установка TAC Vista (Full Install)

Если Вы запустите полную установку TAC Vista (Full Install) с CD диска "TAC Software", Вы сможете произвести групповую установку несколько компонентов. Автоматически запустится процесс установки для всех выбранных программ.

Возможны три варианта установки:

- Типовой (Typical)
- Полный (Full)
- Пользовательский (Custom)

Варианты установки с CD диска включают следующие программы:

Таблица 2.1:

Тип установки	Типовой	Полный	Пользова-тельский
TAC Vista Config	X	X	X
TAC Vista Server с Workstation Pro и TAC Графический Редактор	X	X	X
INet Host Tool		X	
TAC Xbuilder	X	X	X
TAC Vista Web Applications		X	
TAC Vista OPC Server		X	
TAC Vista OPC Server для Danduc		X	
TAC Vista OPC Server для I/NET		X	
Echelon LNS Server			
TAC I-talk Collector и Interface	X	X	X

По умолчанию некоторые программы уже выбраны в варианте Пользовательский (Custom). Если Вы захотите, Вы сможете отказаться от установки некоторых компонентов, отменив их выбор.

Внимание

- В процессе установки с CD диска, Вам будет предложено перезагрузить компьютер после завершения установки некоторых компонентов. **Пожалуйста, *не* перезагружайте компьютер пока на будет окончена установка *всех* программ (включенных в тот вариант, который Вы выбрали).**
- Когда установка будет завершена Вам необходимо перезагрузить Ваш компьютер.

3 Настройки безопасности Windows для TAC Vista

Это руководство приминимо для TAC Vista IV и TAC Vista 5 и описывает необходимые настройки в случае когда TAC Vista работает в среде Windows XP с установленным Service Pack 2 (SP2). Здесь также описываются необходимые настройки для случая, когда TAC Vista с веб доступом работает в среде Windows Server 2003 Service Pack 1 (SP1).

В Windows XP SP2 и Windows Server 2003 SP1, корпорация Microsoft внедрила несколько технологий безопасности, которые повышают надежность компьютера.

Некоторые из изменений относятся к IP и DCOM коммуникациям. Поскольку Vista использует DCOM для передачи данных, Вам необходимо сконфигурировать настройки безопасности COM, чтобы сделать возможным обмен данными. TAC Vista серверы (передача Сервер-Сервер) используют TCP/IP для общения.

Windows Firewall SP2, включенный в XP, и Windows Firewall SP1, включенный в Windows Server 2003, по умолчанию активны и блокируют входящий трафик. Таким образом, Вам необходимо сконфигурировать Windows Firewall, чтобы открыть для Vista возможность обмена данными.

Важно

- Руководством подразумевается, что Вы имеете предварительно установленную и не сконфигурированную операционную систему Windows XP SP2 или Windows Server 2003 SP1.
- Ваш Windows Firewall может быть настроен в соответствии с политикой и быть выключенным или включенным, с запретом внесения любых исключений. В этом случае обратитесь в Ваш отдел по информационным технологиям (IT).

Примечание

- В этом руководстве под **My Computer** (Мой компьютер) подразумевается локальная система в целом. **My Computer** не имеет отношения к имени локального компьютера.

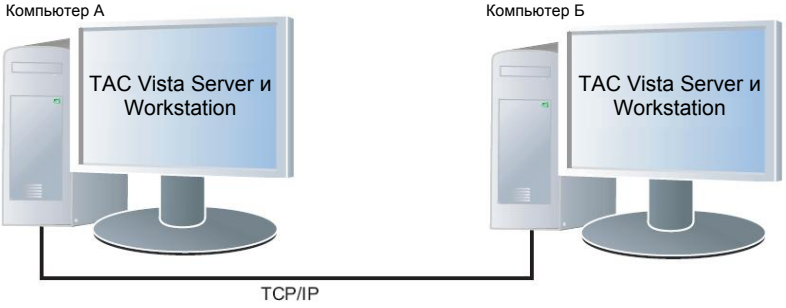
3.1 Система Vista с одним сервером Vista

В системе с сервером Vista (Vista Server) и Рабочей станцией (Workstation), установленными на локальный компьютер, не требуется вносить изменения в настройки безопасности COM.

Примечание

- Автономная Vista не осуществляет коммуникации по сети. То есть отсутствуют входящие пакеты. Нет необходимости вносить исключения в правила Windows Firewall. Когда Вы запускаете сервер Vista, Windows спросит желаете ли Вы блокировать программу сервера (Приложение TACOS). Вы можете блокировать приложение так долго, как долго Vista Workstation работает в автономном режиме.

3.2 Система Vista с несколькими серверами Vista



В системе с сервером Vista (Vista Server) и Рабочей станцией (Workstation), установленными на два или более компьютера (удаленные коммуникации), не требуется вносить изменения в настройки безопасности COM. Вам необходимо настроить Windows Firewall для разрешения входящих сообщений для сервера Vista.

3.2.1 Настройка исключений в Windows Firewall

В системе с несколькими серверами Vista Вам необходимо сделать исключение в правилах Windows Firewall для приложения TACOS, что бы позволить серверу Vista получать входящие сообщения.

Для настройки исключения в Windows Firewall

1 Запустите TAC Vista Server (далее – сервер TAC Vista).

2 В предупреждении **Windows Security Alert**, нажмите **Unblock** (Разблокировать).

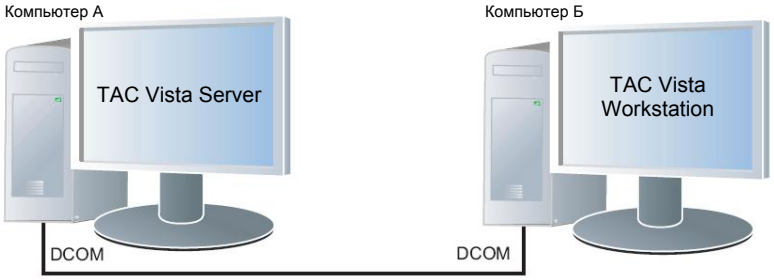
Важно

- Повторите эту процедуру для всех серверов Vista, которые участвуют в сетевых коммуникациях.

Примечание

- Окно **Windows Security Alert** появляется только первый раз, когда запускается приложение сервера Vista.
- Когда Вы разблокируете приложение сервера Vista (TACOS.exe), оно будет добавлено в список исключений Windows Firewall. IP порты, которые используются для осуществления коммуникаций Vista, также добавятся в этот список.
- Если вы захотите разблокировать ранее блокированное приложение, Вам будет необходимо добавить его в список исключений Windows Firewall.
- Что бы внести программу в список исключений Windows Firewall, в Windows Firewall выберите вкладку **Exceptions** (Исключения), нажмите **Add Program** (Добавить программу), найдите TACOS.exe, нажмите **OK**, и затем ещё раз **OK**.
- В этом случае Вам также необходимо вручную добавить IP порты, через которые сервер Vista осуществляет коммуникации в список исключений Windows Firewall.
- По умолчанию Vista использует TCPPORT 45612.

3.3 Система Vista с удалённым доступом в домене



В системе с сервером Vista, установленном на одном компьютере, и Vista Workstation, установленной на другом компьютере в домене, Вам необходимо настроить Windows Firewall для разрешения входящих коммуникаций с сервером Vista. Вам также необходимо изменить настройки безопасности COM для возможности коммуникаций по сети.

3.3.1 Настройка исключений в Windows Firewall

В системе с удалёнными рабочими станциями Vista, Вам необходимо сделать исключение в правилах Windows Firewall для приложения TACOS, что бы разрешить входящие в компьютер сообщения.

Как разблокировать сервер Vista (то есть, как внести приложение в список исключений Windows Firewall), см. раздел 3.2.1 «Настройка исключений в Windows Firewall», на странице 18.

3.3.2 Настройка исключений для порта в Windows Firewall

В системе с удалёнными рабочими станциями Vista, Вам необходимо сделать исключение в правилах Windows Firewall для порта 135 (DCOM) для разрешения коммуникаций через этот порт.

Чтобы установить исключение для порта в Windows Firewall

1 На компьютере, на котором запущен сервер Vista, запустите Windows Firewall.

Совет

- Вы можете получить доступ к Windows Firewall из Панели управления (Control Panel).

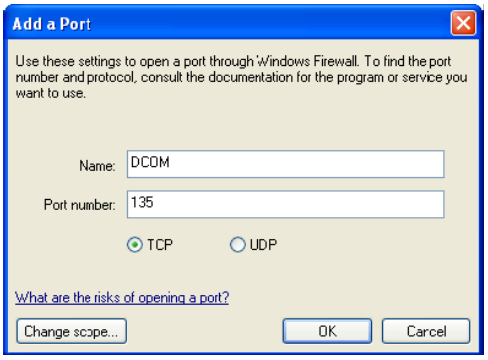
2 Выберите вкладку **Exceptions** (Исключения).

3 Нажмите **Add Port** (Добавить порт).

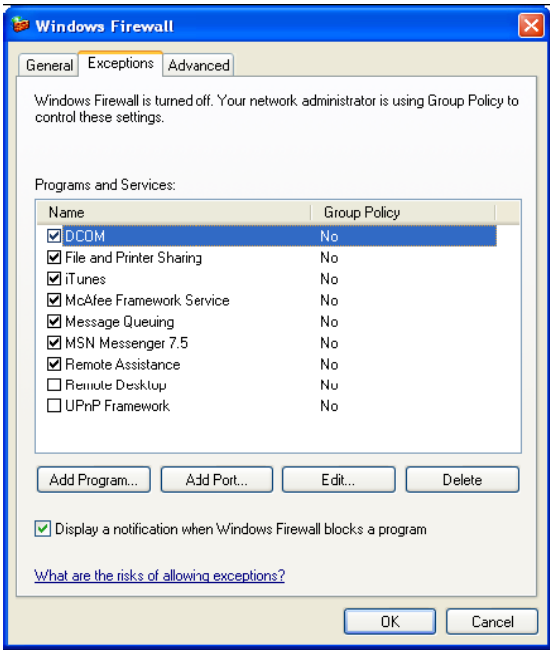
4 В поле **Name** (Имя) напечатайте "DCOM".

5 В поле **Port Number** (Номер порта) наберите "135".

6 Выберите **TCP**.



7 Нажмите **OK**.



8 Нажмите **OK**.

Примечание

- Здесь Вы настраиваете исключающее правило только для порта 135 (DCOM), не для Vista TCPPORT.

Повторите эту процедуру на компьютере, на котором работает удаленная Vista Workstation.

3.3.3 Настройка прав доступа для My Computer

Вам необходимо сконфигурировать настройки безопасности COM для осуществления коммуникаций по сети.

Имеются два типа настройки прав доступа в COM Security (Безопасность COM):

- Access permissions (Права доступа)
- Launch and Activation permissions (Разрешения на запуск и активацию)

Права доступа определяют учётную запись, имеющую права для запуска приложения. Вам необходимо установить права доступа на обоих компьютерах, и на том где работает сервер Vista и на том где установлена рабочая станция (Vista Workstation).

В рассматриваемом случае Вам не нужно настраивать разрешения на запуск и активацию.

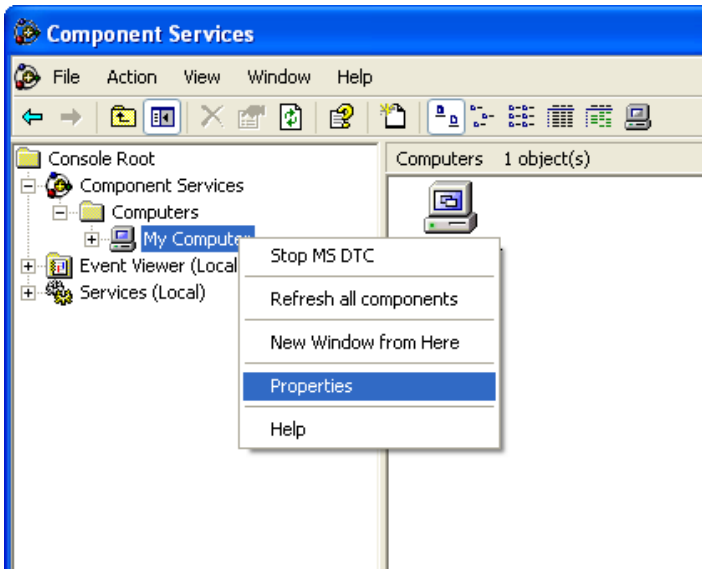
Для настройки Прав доступа для My Computer

1 На компьютере с сервером Vista, запустите Component Services (Службы компонентов).

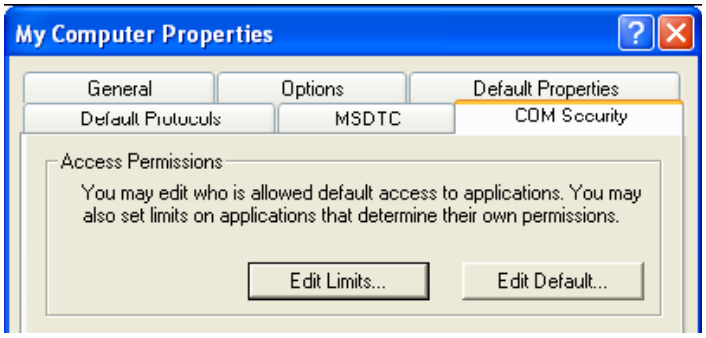
Совет

- Вы можете получить доступ к Службе компонентов в Панели управления в меню Administrative Tools (Администрирование).

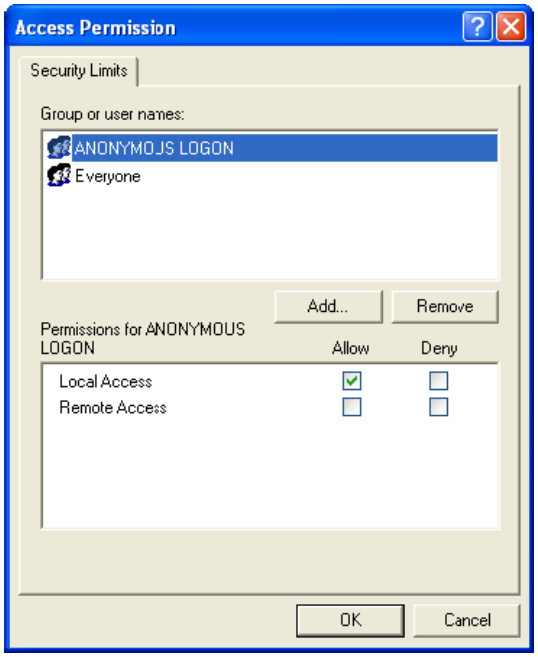
2 Выберите в структуре путь Component Services\Computers**My Computer** (Службы компонентов\Компьютеры\Мой компьютер), и потом нажмите **Properties** (Свойства).



3 Выберите вкладку **COM Security** (Безопасность COM).

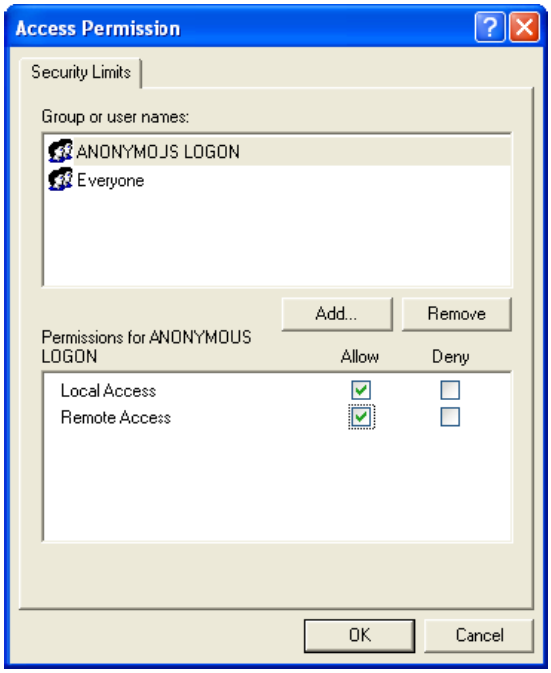


4 В зоне **Access Permission** (Права Доступа**)**, нажмите **Edit Limits** (Изменить ограничения).



5 В зоне **Group or user names** (Группы или пользователи), выберите **ANONYMOUS LOGON** (АНОНИМНЫЙ ВХОД).

6 В колонке **Allow** (Разрешить), выберите **Remote Access** (Удалённый доступ).



Примечание

- Предоставляя удалённой учётной записи АНОНИМНЫЙ ВХОД права удалённого доступа, Вы даёте Vista Workstation возможность обращения к серверу Vista.

7 Нажмите **OK**.

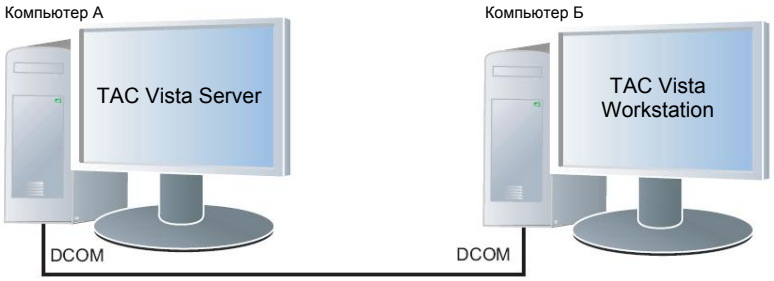
Важно

- Вам необходимо перезагрузить Ваш компьютер, чтобы изменения в настройках DCOM вступили в силу.

Примечание

- На компьютерах с установленной Vista Workstation Вам необходимо предоставить удалённой учётной записи АНОНИМНЫЙ ВХОД права удалённого доступа, что бы дать серверу Vista возможность обращения к рабочим станциям (обратный вызов).

3.4 Система Vista с удалённым доступом в Рабочей группе или не-NT домене



В системе с сервером Vista, установленном на одном компьютере, и Vista Workstation, установленной на другом компьютере, в Рабочей группе или не-NT домене, Вам необходимо настроить Windows Firewall для разрешения входящих коммуникаций с сервером Vista. Вам также необходимо изменить настройки безопасности COM для возможности коммуникаций по сети.

3.4.1 Настройка исключений в Windows Firewall

В системе с несколькими серверами Vista, Вам необходимо сделать исключение в правилах Windows Firewall для приложения TACOS, что бы разрешить входящие в компьютер сообщения.

Как разблокировать сервер Vista (то есть, как внести приложение в список исключений Windows Firewall), см. раздел 3.2.1 «Настройка исключений в Windows Firewall», на странице 18.

3.4.2 Настройка исключений для порта в Windows Firewall

В системе с несколькими серверами Vista, Вам необходимо сделать исключение в правилах Windows Firewall для порта 135 (DCOM) для разрешения коммуникаций через этот порт. Вам необходимо произвести эти действия на всех компьютерах с установленным сервером Vista.

Как настроить исключение в правилах Windows Firewall см. раздел 3.3.2 «Настройка исключений для порта в Windows Firewall», на странице 20.

3.4.3 Настройка прав доступа для My Computer

Права доступа определяют учётную запись, имеющую права для запуска приложения. Вам необходимо установить права доступа на обоих компьютерах, и на том где работает сервер Vista и на том где установлена рабочая станция (Vista Workstation).

Примечание

- Права доступа для **My Computer** (Мой компьютер) в системе Vista с удалённым доступом в Рабочей группе или не-NT домене будут такими же как Права доступа для **Мой компьютер** в системе Vista с удалённым доступом в домене.

Как настроить права доступа DCOM, см. раздел 3.3.3 «Настройка прав доступа для My Computer», на странице 21.

3.4.4 Настройка Launch and Activation Permissions (Разрешений на запуск и активацию) на My Computer

Вам необходимо сконфигурировать настройки безопасности COM для осуществления коммуникаций по сети.

Имеются два типа настройки прав доступа в COM Security (Безопасность COM):

- Access permissions (Права доступа)
- Launch and Activation permissions (Разрешения на запуск и активацию)

Разрешения на запуск и активацию определяют учётную запись, имеющую права для запуска основанного на технологии COM приложения, например сервер TAC Vista, как по сети, так и локально.

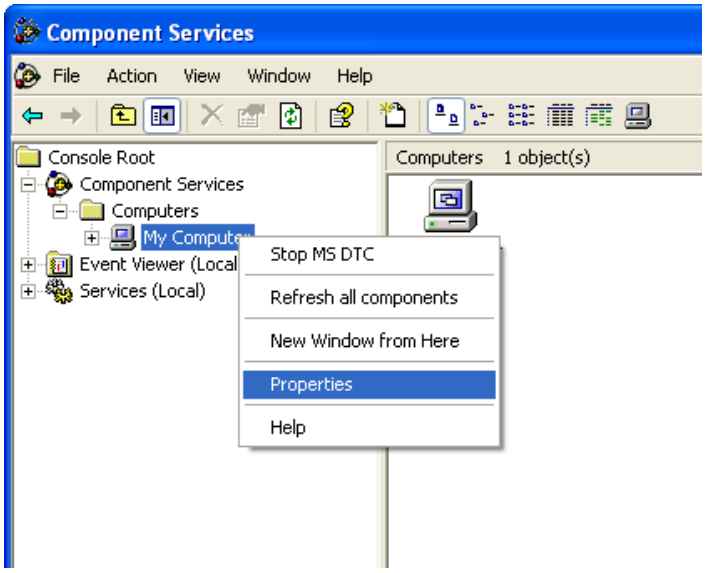
Для настройки Разрешений на запуск и активацию для My Computer

1 На компьютере с сервером Vista, запустите Component Services (Службы компонентов).

Совет

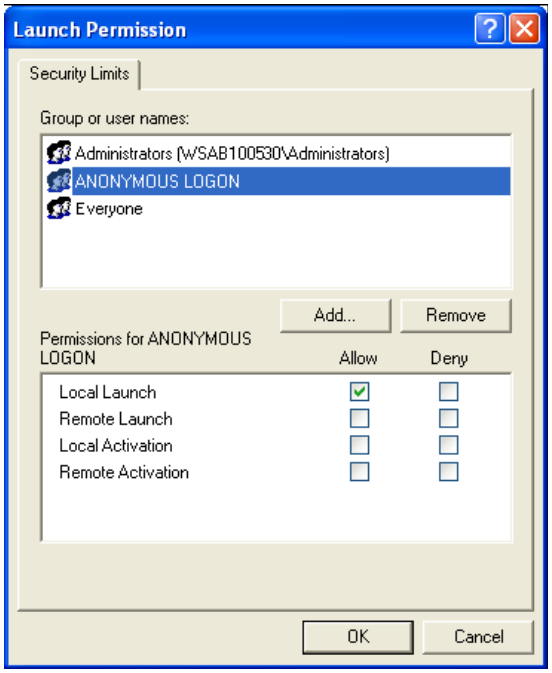
- Вы можете получить доступ к Службе компонентов из Панели управления в меню Administrative Tools (Администрирование).

2 Выберите в структуре путь Component Services\Computers**My Computer** (Службы компонентов\Компьютеры\Мой компьютер), и потом нажмите **Properties** (Свойства).



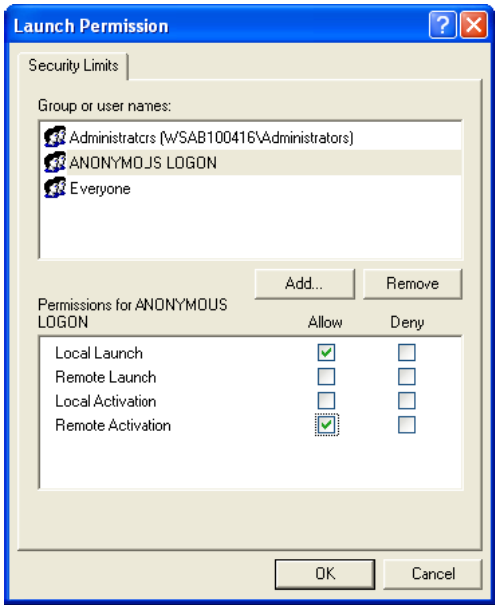
3 Выберите вкладку **COM Security** (Безопасность COM).

4 В зоне **Разрешения на запуск и активацию**, нажмите **Edit Limits** (Изменить ограничения).



5 В зоне **Group or user names** (Группы или пользователи), выберите **ANONYMOUS LOGON** (АНОНИМНЫЙ ВХОД).

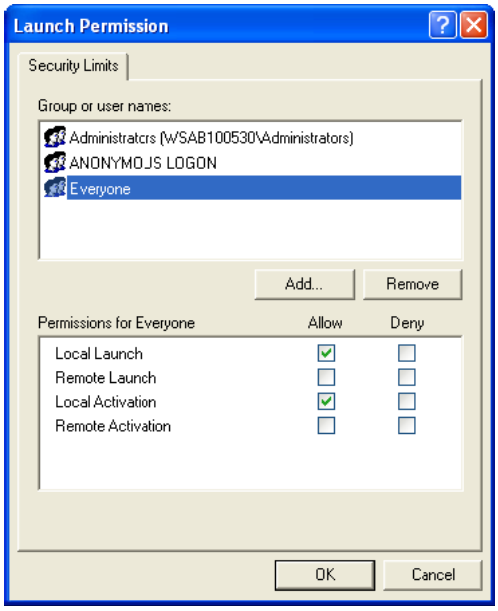
6 В колонке **Allow** (Разрешить), выберите **Remote Activation** (Удаленная активация).



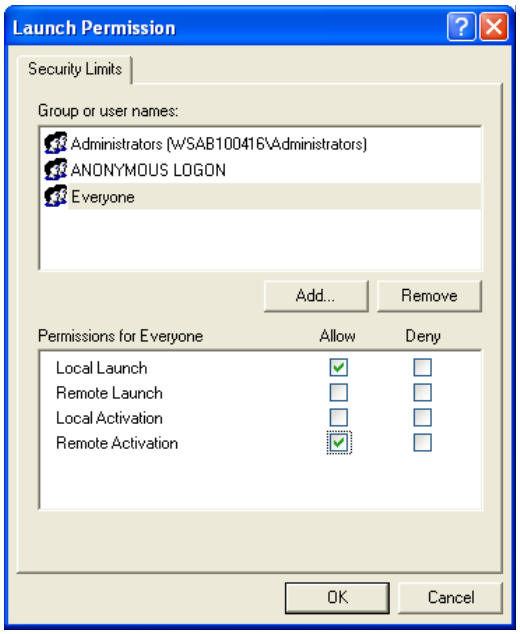
Примечание

- Предоставляя учётной записи АНОНИМНЫЙ ВХОД разрешение на удалённую активацию, Вы даёте Vista Workstation возможность обращения к удалённому серверу Vista.
- На компьютерах с установленной Vista Workstation Вам необходимо предоставить удаленной учётной записи АНОНИМНЫЙ ВХОД разрешение на удаленную активацию, что бы дать серверу Vista возможность доступа к рабочей станции (обратный вызов).

7 В поле **Group or user names** (Группы или пользователи), выберите **Everyone** (Все).



8 В колонке **Allow** (Разрешить), выберите **Remote Activation** (Удаленная активация).



Примечание

- Предоставляя учётной записи АНОНИМНЫЙ ВХОД разрешение на удалённую активацию, Вы даёте Vista Workstation возможность обращения к удалённому серверу Vista..

9 Нажмите **OK**.

Повторите эти действия на всех компьютерах с сервером Vista.

Примечание

- На компьютерах с установленной Vista Workstation Вам необходимо предоставить удалённой учётной записи **Все** разрешение на удалённую активацию, что бы дать серверу Vista возможность доступа к рабочей станции (обратный вызов).

3.4.5 Настройка Launch and Activation Permissions (Разрешений на запуск и активацию) для TACOS

Разрешения на запуск и активацию определяют учётную запись, имеющую права для запуска основанного на технологии COM приложения, например сервер TAC Vista, как по сети, так и локально.

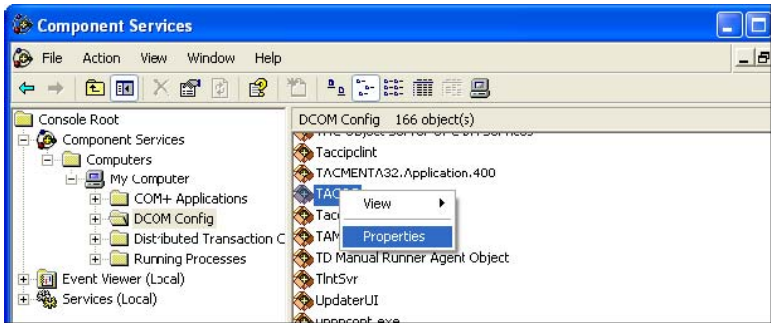
Для настройки Разрешений на запуск и активацию для TACOS

1 На компьютере с сервером Vista, запустите Component Services (Службы компонентов).

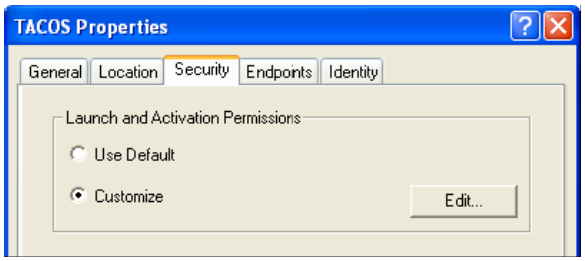
Совет

- Вы можете получить доступ к Службе компонентов из Панели управления в меню Administrative Tools (Администрирование).

2 Выберите в структуре путь Component Services\Computers**My Computer**\DCOM Config\TACOS (Службы компонентов\Компьютеры\Мой компьютер\Настройка DCOM\TACOS), и потом нажмите **Properties** (Свойства).

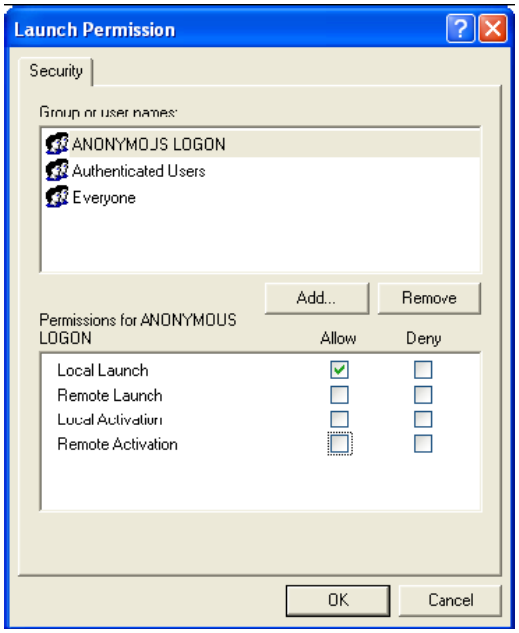


3 Выберите вкладку **Security** (Безопасность).

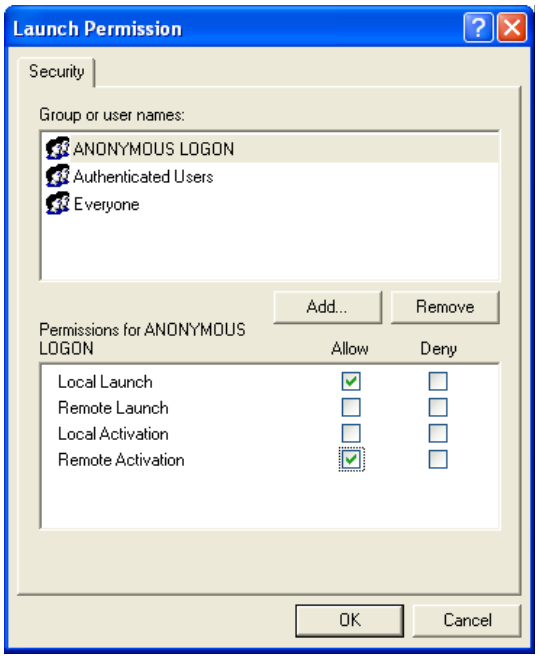


4 В зоне **Разрешения на запуск и активацию**, выберите **Customize** (Настроить) и затем нажмите **Edit** (Изменить).

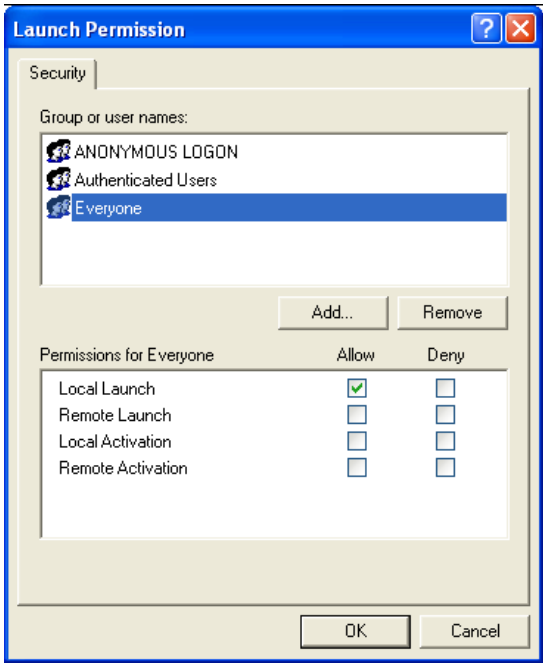
5 В открывшемся окне **Launch Permissions** (Разрешение на запуск), в поле **Group or user names** (Группы или пользователи), выберите ANONYMOUS LOGON (АНОНИМНЫЙ ВХОД).



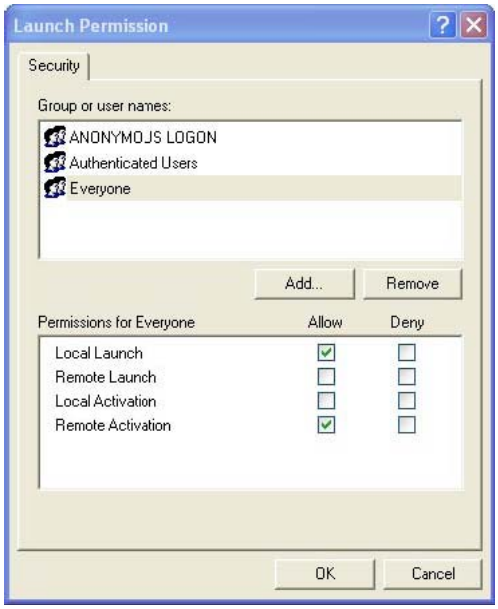
6 В колонке **Allow** (Разрешить), выберите **Remote Activation** (Удаленная активация).



7 В поле **Group or user names** (Группы или пользователи), выберите **Everyone** (Все).



8 В колонке **Allow** (Разрешить), выберите **Remote Activation** (Удаленная активация).



9 Нажмите **OK**.

Повторите эти действия на всех компьютерах с сервером Vista.

3.4.6 Настройка прав доступа для TACOS

Права доступа определяют учётную запись, имеющую права для запуска приложения.

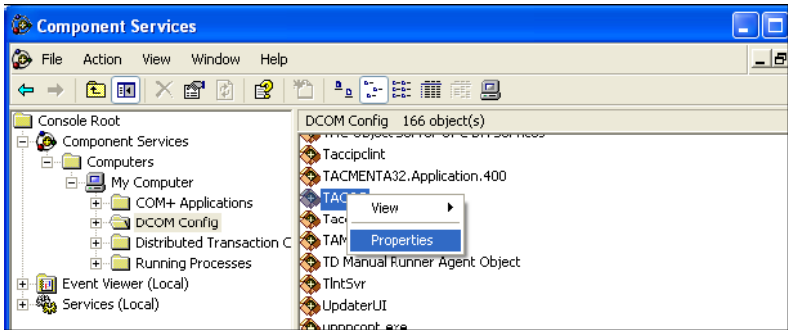
Для настройка прав доступа на TACOS

1 На компьютере с сервером Vista, запустите Component Services (Службы компонентов).

Совет

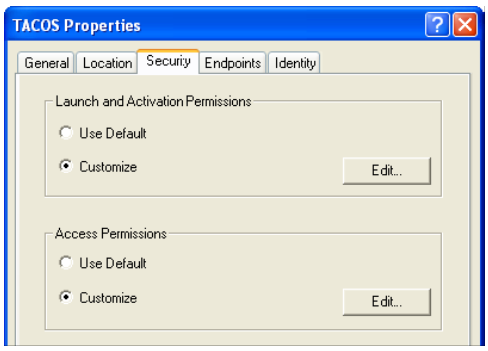
- Вы можете получить доступ к Службе компонентов из Панели управления в меню Administrative Tools (Администрирование).

2 Выберите в структуре путь Component Services\Computers**My Computer**\DCOM Config\TACOS (Службы компонентов\Компьютеры\Мой компьютер\Настройка DCOM\TACOS), и потом нажмите **Properties** (Свойства).



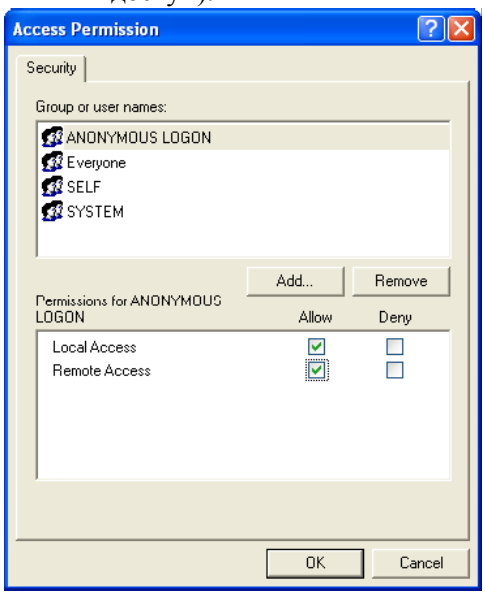
3 Выберите вкладку **Security** (Безопасность).

4 В зоне **Права доступа**, выберите **Customize** (Настроить) и затем нажмите **Edit** (Изменить).



5 В открывшемся окне **Access Permissions** (Разрешение на доступ), в поле Group or user names (Группы или пользователи), выберите **ANONYMOUS LOGON** (АНОНИМНЫЙ ВХОД).

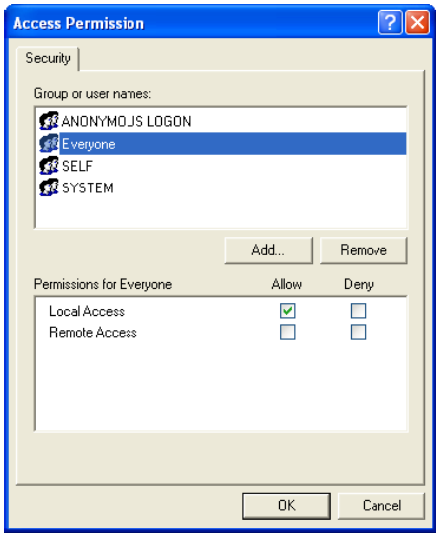
6 В колонке **Allow** (Разрешить), выберите **Remote Access** (Удаленный доступ).



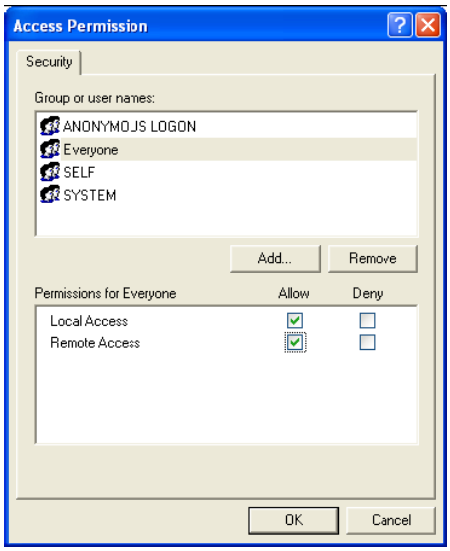
Примечание

- Предоставляя учётной записи АНОНИМНЫЙ ВХОД разрешение на удалённый доступ, Вы даёте Vista Workstation возможность обращения к удаленному серверу Vista.
- На компьютерах с установленной Vista Workstation Вам необходимо предоставить удалённой учётной записи АНОНИМНЫЙ ВХОД разрешение на удалённый доступ, что бы дать серверу Vista возможность обращения к рабочей станции (обратный вызов).

7 В поле **Group or user names** (Группы или пользователи), выберите **Everyone** (Все).



8 В колонке **Allow** (Разрешить), выберите **Remote access** (Удалённый доступ).



Примечание

- Предоставляя учётной записи **Все** разрешение на удалённый доступ, Вы даёте Vista Workstation возможность обращения к удалённому серверу Vista.

9 Нажмите **OK**.

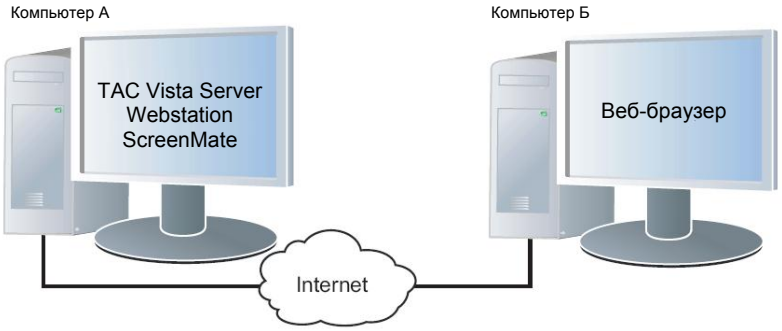
Важно

- Вам необходимо перезагрузить Ваш компьютер, чтобы изменения в настройках DCOM вступили в силу.

Повторите эти действия на всех компьютерах с сервером Vista.

3.5 Система Vista с веб доступом

В системе с сервером Vista, Vista Webstation (версия 4.3.0 или старше), и Vista ScreenMate (версия 4.3.0 или старше), установленными на один компьютер, и веб-браузером, установленном на другом компьютере, Вам необходимо изменить разрешения для учётной записи NETWORK SERVICE (или ASPNET, если вы работаете с Windows XP SP2) для возможности коммуникаций между Webstation и Vista Server.



Важно

- Обеспечение работы TAC Vista Webstation с системой Windows XP заказчика здесь не рассматривается.
- Здесь в этом руководстве подразумевается работа TAC Vista с Windows Server 2003 Service Pack 1 (SP1).

3.5.1 Настройка Launch and Activation Permissions (Разрешений на запуск и активацию) для My Computer

Разрешения на запуск и активацию определяют учётную запись, имеющую права для запуска основанного на технологии COM приложения, например сервер TAC Vista, как по сети, так и локально.

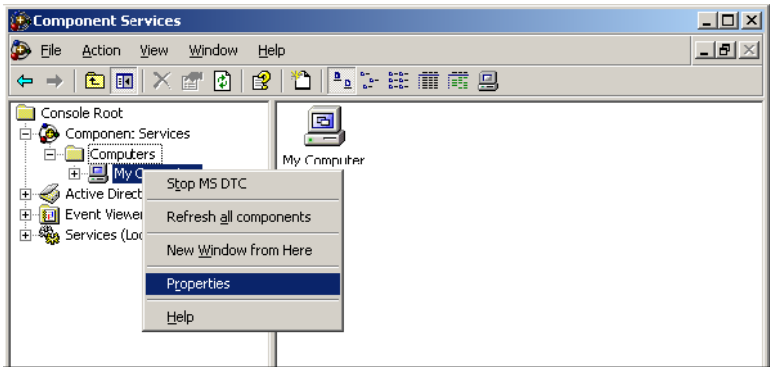
Для настройки Разрешений на запуск и активацию для My Computer

1 На компьютере с сервером Vista, запустите Component Services (Службы компонентов).

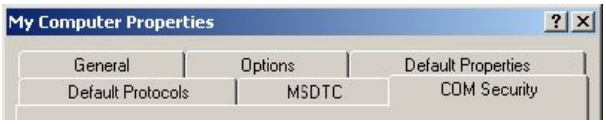
Совет

- Вы можете получить доступ к Службе компонентов из Панели управления в меню Administrative Tools (Администрирование).

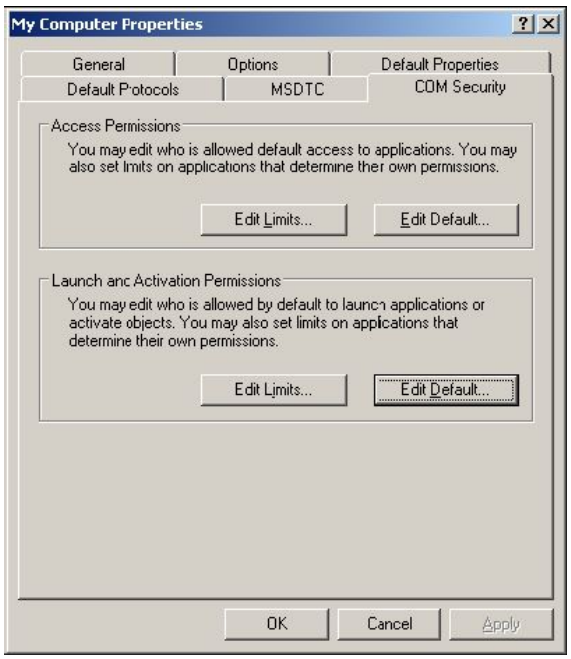
2 Выберите в структуре путь Component Services\Computers**My Computer** (Службы компонентов\Компьютеры\Мой компьютер), и потом нажмите **Properties** (Свойства).



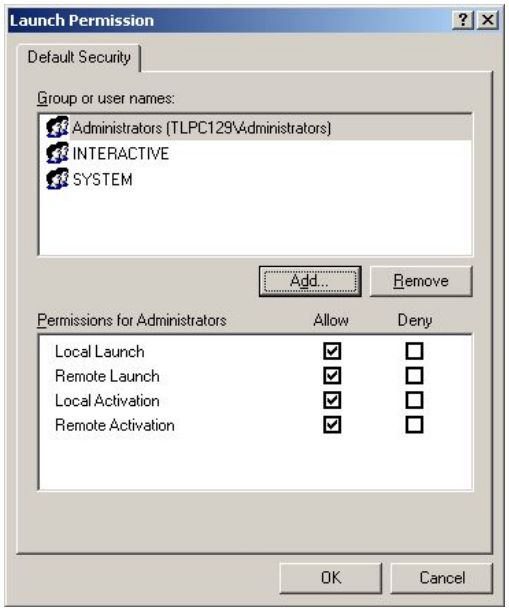
3 Выберите вкладку **COM Security** (Безопасность COM).



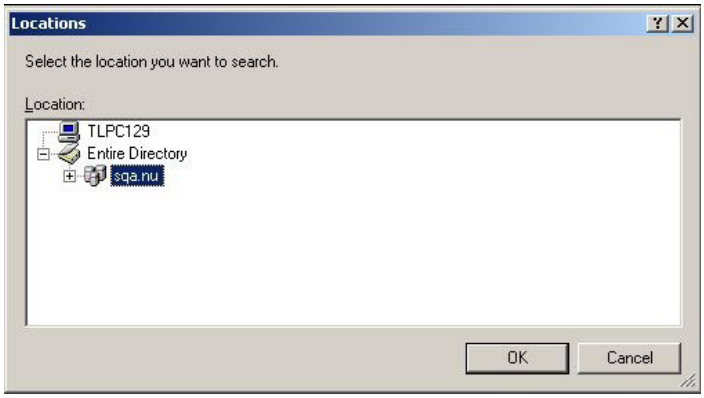
4 В зоне **Разрешения на запуск и активацию**, нажмите **Edit Default** (Изменить настройки по умолчанию).



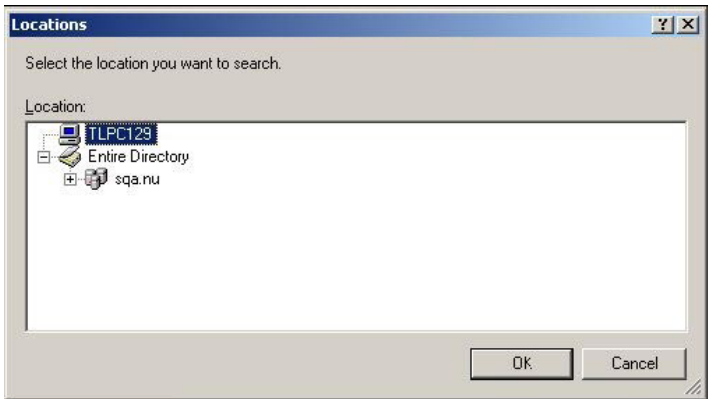
5 Нажмите **Add** (Добавить).



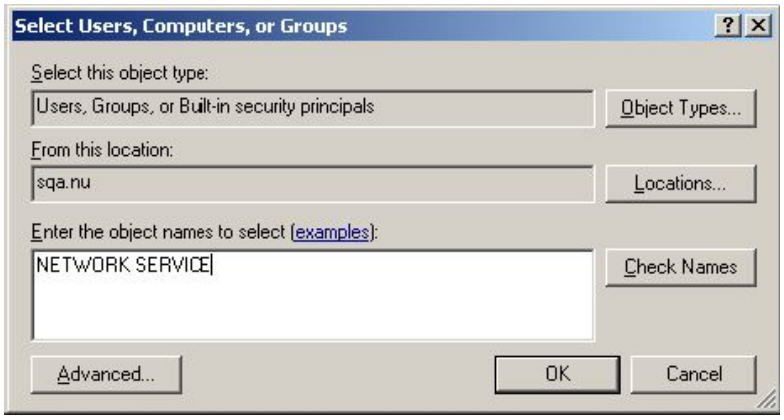
6 В открывшемся окне **Select Users and Groups** (Выбор: Пользователи, Компьютеры или Группы), нажмите **Location**s (Размещение).



7 В окне **Locations** (Размещение), выделите имя локального компьютера и затем нажмите **OK**.



8 В окне **Select Users and Groups** (Выбор: Пользователи, Компьютеры или Группы), в разделе **Enter the object names to select** (Введите имена выбираемых объектов) наберите "NETWORK SERVICE".



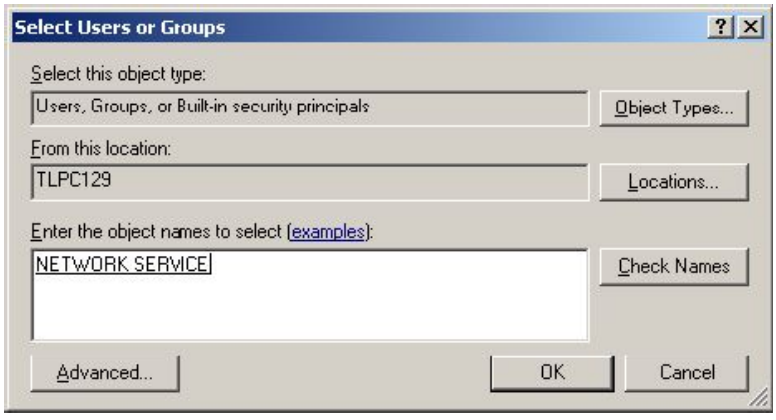
Важно

- Если Вы работаете в среде Windows XP SP2, наберите "ASPNET" вместо "NETWORK SERVICE".
- Обеспечение работы TAC Vista Webstation с системой Windows XP заказчика здесь не рассматривается.

Примечание

- NETWORK SERVICE и ASPNET – это учётные записи компьютера, под которыми работают службы сервера. Учётные записи обеспечивают безопасную среду для работы.

9 Нажмите **Check Names** (Проверить имена).



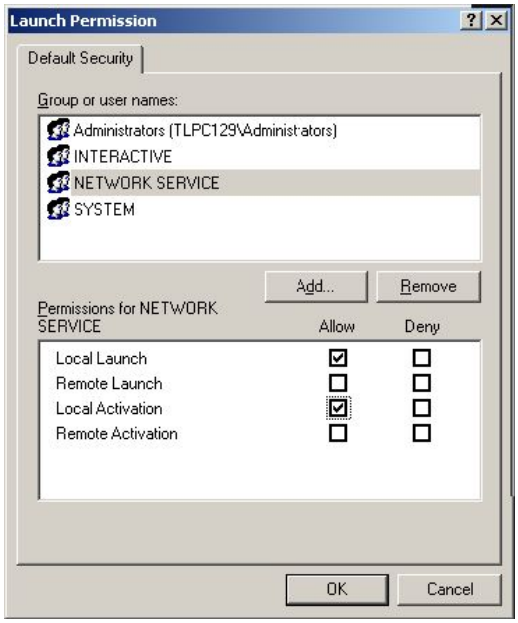
10 Нажмите **OK**.

11 В окне **Launch Permission** (Разрешение на запуск), выберите NETWORK SERVICE.

Важно

- Если Вы работаете в среде Windows XP SP2, выберите ASPNET вместо NETWORK SERVICE.

12 В колонке **Allow** (Разрешить), выберите **Local Activation** (Локальная активация).



Примечание

- Предоставляя учётной записи NETWORK SERVICE или ASPNET разрешение на локальный доступ, Вы даёте учётной записи возможность обращения к серверу Vista.

13 Нажмите **OK**.

Важно

- Вам необходимо перезагрузить Ваш компьютер, чтобы изменения в настройках DCOM вступили в силу.

4 Установка TAC Vista Webstation

Если Вы хотите работать с приложениями TAC Vista Web в среде Windows Server 2003 Standard Edition, должны быть установлены Internet Information Services (IIS, Информационные службы Интернета) и ASP.NET 2.0.

4.1 Активация ASP.NET 2.0

Кроме того, ASP.NET 2.0 должен быть разрешен запуск (по умолчанию запрещен).

Для активации ASP.NET 2.0

1. В меню **Start** (Пуск) откройте **Administrative Tools** (Администрирование) и затем запустите **Internet Information Services (IIS) Manager**.
2. В окне **Internet Information Services (IIS) Manager**, в структуре **Internet Information Service**, раскройте ветвь под сервером, на котором установлены приложения TAC Vista Web (обычно там перечислен только локальный компьютер), и затем выберите **Web Service Extensions**.
3. В окне **Web Service Extensions**, нажмите **ASP.NET v2.0**
4. Click **Allow** (Разрешить).

   Состояние ASP.NET 2.0 изменится с **Prohibite**d (Запрещено) на **Allowed** (Разрешено).
5. Закройте **Internet Information Services (IIS) Manager**.

4.2 Темы Webstation

В дополнение к включенным в пакет Webstation/ScreenMate темам, Вы можете добавлять и настраивать Ваши собственные темы.

В папке Style каталога, в который установлены TAC Vista Web Applications, имеются подпапки с различными темами.

Чтобы создать новую тему

1. Среди имеющихся тем выберите тему наиболее близкую к Вашей новой теме и затем скопируйте её.
2. Назовите новую папку так, как Вы хотите чтобы тема отображалась в списке тем в веб настройках TAC Vista и в TAC Vista Webstation.

3 Откройте новую папку.

Все страницы используют файл Webstation.css для формирования общего макета. Отредактируйте файл Webstation.css для внесения общих изменений.

В дополнение к этому файлу, каждая страница Webstation/ScreenMate использует специальный CSS файл, назначение файлов понятно из их названий. Редактируйте этот файл для локальных изменений.

4 Вы можете отредактировать файлы CSS в соответствии с Вашими желаниями. Для этого понадобится хорошее знание HTML и CSS.

5 Запустите TAC Vista Web Settings (веб настройки) и выберите **Theme - Colors and Fonts** (Тема – Цвета и шрифты).

Теперь Вы можете просмотреть список тем, чтобы убедиться, что новая тема добавлена в перечень.

Если Вы выберите новую тему, картинка в поле предпросмотра будет неправильная. Исправим это позже.

6 Нажмите **OK** чтобы выбрать новую тему.

7 Выйдите из TAC Vista Web Settings.

8 Запустите Webstation и проверьте результат.

9 Если Вы удовлетворены результатами, сделайте снимок экрана для правильного отображения в поле просмотра и сохраните как файл формата .gif в подпапке изображений (images) в созданной Вами папке темы. Файл необходимо назвать preview.gif.

Возможно, в папке уже существует файл с таким названием, поскольку Вы скопировали эту папку темы со всеми вложениями. Прежде чем Вы перезапишете существующий файл preivew.gif проверьте его графические размеры и сохраните Ваш новый скриншот с теми же размерами.

4 Запустите TAC Vista Web Settings и выберите **Theme - Colors and Fonts** (Тема – Цвета и шрифты).

Теперь Вы можете просмотреть список тем, чтобы убедиться, что новая тема имеет правильное отображение в поле просмотра.

6 Выйдите из TAC Vista Web Settings.

12 Откройте подпапку с изображениями (images) в созданной Вами папке темы и измените изображения нужным Вам образом.

13 Включите вид Thumbnails (Эскизы) в Windows чтобы просматривать уменьшенные копии изображений.

Не изменяйте графические размеры этих изображений.

Если Вы посмотрите на изображения и на окно Webstation одновременно, Вы сможете увидеть, где эти изображения используются. Если Вы предпочитаете просматривать вашу тему во время работы над ней, запустите TAC Vista Webstation и выберите тему, с которой Вы работаете. Вы сможете периодически обновлять экран и видеть сделанные изменения.

4.3 SSL – Secure Sockets Layer

Для повышения безопасности во время обмена информацией между веб-браузером и веб-сервером, шифрование коммуникаций, работающее по HTTPS должно быть настроено использовать протокол SSL (Secure Sockets Layer).

Прежде чем SSL может быть использован, необходимо создать и зарегистрировать сертификат SSL для веб-сервера, а нашем случае Internet Information Server (IIS).

Обычно, когда SSL используется для работы программ, к которым имеется открытый доступ, приобретается надежный SSL сертификат у аккредитованной компании, такой как Verisign. Для временной защиты или тестирования можно использовать "самоподписанный" цифровой сертификат. Формально этот сертификат предлагает такое же шифрование, как и сертификат, выпушенный Центром сертификации, однако, это может быть воспринято как снижение безопасности, потому что сервер собственника не был проверен Центром сертификации. "Самоподписанные" сертификаты могут вызывать появление окон предупреждений в веб-браузере.

Один из пригодных методов создания "самоподписанного" сертификата – это использование инструмента по названием SelfSSL. SelfSSL создан корпорацией Microsoft и поставляется в составе IIS 6 Resource Kit. Программы могут быть загружены с сайта Microsoft.

Чтобы скачать SelfSSL посетите www.microsoft.com и задайте поиск для SelfSSL. Загрузите инструменты IIS 6.0 Resource Kit и установите, следуя инструкциям.

Когда установка завершится Вам необходимо запустить SelfSSL.exe с соответствующими параметрами для установки сертификата и регистрации его для IIS. Например,

```
selfssl.exe /V:365
```

эта команда установит сертификат, действующий 365 дней.

Можно получить больше информации о формате команды, написав

```
selfssl.exe /?
```

в командной строке.

После установки программы Вы сможете использовать как HTTPS так и стандарт HTTP. Если Вы хотите работать только по HTTPS, это необходимо настроить в IIS. Для получения дополнительной информации обратитесь к документации Microsoft по IIS.

Примечание

- Первый раз запустив TAC Webstation, установленную на сервере, использующем SelfSSL, Вы получите сообщение, говорящее что-то вроде **Certificate not signed by a trusted authority** (Сертификат не подписан надежным источником). Подтвердите сертификат.

4.4 Локализация

Локализация добавляется установкой соответствующего language pack (пакета локализации). Пакет локализации определяет как язык, так и страну/регион. Если пакет локализации для Вашей страны ещё не доступен, Вы, тем не менее, можете установить национальный формат даты и т.п. Язык нельзя изменить без пакета локализации. Установка локализации основана на Microsoft Windows.

Для изменения или установки страны/региона используются настройки Vista WebApplications. Возможные варианты показаны в списке Localization (Локализация) на странице Localization (Локализация).

Вы можете добавить локализацию в список, создав пустую папку с именем определенного вида. Имя должно отвечать стандарту RFC 1766 и быть в формате "<код языка>-<код страны/региона>", где <код языка> - код из двух строчных букв в соответствии с ISO 639-1 и <код страны/региона> - код из двух прописных букв в соответствии с ISO 3166.

Например, U.S. English (США-английский) это "en-US" и Finnish-Swedish (Финляндия-шведский) is "sv-SF"; этот тип формата называется "localization pair" (парой локализации).

В случае если код языка из двух строчных букв не доступен, используется трёхбуквенный код в соответствии с ISO 639-2; например, трёхбуквенный код "div" применяется для обществ, использующих язык Dhivehi.

Пара локализации должна соответствовать списку локализаций в Microsoft .NET:

http://../webstation/CultureInfoNames.aspx

где .. заменяется сетевым адресом Vista Webstation.

Для добавления локализации

1. С помощью Windows Explorer зайдите в папку локализаций Vista Webstation, обычно

   C:\Inet- pub\wwwroot\TACVistaWeb401\Bin

2. Создайте новую папку с именем в формате:<код языка>-<код страны/региона>

   Имя папки должно соответствовать коду локализации, представленному в файле

   http://../webstation/CultureInfoNames.aspx

   где .. заменяется сетевым адресом Vista Webstation.

   Новую папку можно оставить пустой.

3. Запустите Vista Web Applications Settings и установите новую локализацию.

4.5 Использование сжатия HTTP

Если Ваш сайт занимает большую часть полосы пропускания или если вы хотите более эффективно использовать Вашу полосу пропускания, Вы можете разрешить сжатие HTTP. Сжатие HTTP увеличивает скорость передачи между браузерами, поддерживающими эту возможность, и IIS. Вы можете сжимать только статические файлы, или как статические файлы так и динамические ответы приложения. Если полоса пропускания Вашей сети ограничена и загрузка Вашего процессора уже достаточно высока, сжатие HTTP может быть полезным. Это справедливо особенно для статических файлов.

Для получения дополнительной информации о Сжатии HTTP посетите сайт www.microsoft.com и задайте поиск для "Utilizing HTTP Compression" (Использование сжатия HTTP), "IIS 6.0 Compression with Windows Server 2003" (IIS 6.0 сжатие с Windows Server 2003), и "HOW TO: Specify Additional Document Types for HTTP Compression" (КАК: Определить дополнительные типы документов для сжатия HTTP).

4.6 Использование окон Vista Webstation в веб-порталах или как окон автономного браузера

Все окна, имеющие иконку "Add to Favorites" (Добавить в избранное) на панели инструментов, могут быть использованы как автономные окна или как встроенная часть, например, веб-портала.

Ссылки Vista Webstation необходимо немного изменить, прежде чем Вы сможете их использовать.

Для получения и изменения ссылки

1. Откройте окно в Vista Webstation.
2. На панели инструментов окна нажмите **Add to Favorites** (Добавить в избранное).
3. С помощью Вашего браузера сохраните ссылку.
4. С помощью Вашего браузера найдите ссылку в разделе Favourites (Избранное) и откройте свойства ссылки. Обычно ссылка выглядит как:

   http://.../webstation/Default-Page.aspx?frameset=true&page=...

5. В части "frameset=false", измените true на false, в нашем примере:

   http://.../webstation/Default-Page.aspx?frameset= false&page=...

Эта ссылка теперь может использована как автономное окно. Ссылка может быть использована также для веб-портала. Проконсультируйтесь с Вашим вебмастером о следующих действиях.

4.7 Запрет перезапуска и остановки рабочих процессов

Если Webstation и/или ScreenMate используются редко, Вы можете столкнуться с дополнительными задержками во время загрузки страницы входа в систему.

Вы можете повысить производительность, предотвратив выгрузку из памяти сервера приложений WebStation или Screen-Mate.

Для запрета перезапуска рабочего процесса

1. В IIS Manager, раскройте пункт локальный компьютер, раскройте пункт **Application Pools**, кликните правой клавишей мыши на пункте application pool для настройки, и затем нажмите **Properties** (Свойства).
2. На вкладке **Recycling** уберите флажок в пункте **Recycle worker processes (in minutes)**.
3. Нажмите **OK**.

Для запрета остановки рабочего процесса

1. В IIS Manager, раскройте пункт локальный компьютер, раскройте пункт **Application Pools**, кликните правой клавишей мыши на пункте application pool для настройки, и затем нажмите **Properties** (Свойства).
2. На вкладке **Performance**, в разделе **Idle timeout**, уберите флажок в пункте **Shutdown worker process after being idle for (time in minutes)**.
3. Нажмите **OK**.

Примечание

- Эти настройки будут действовать для всех приложений в измененном разделе application pool.

04-00001-01-ru

Europe / Headquarters
Malmö, Sweden +46 40 38 68 50

Americas
Dallas, TX
+1 972-323-1111

Asia-Pacific
Sydney, Australia
+61 2 9700 1555

www.tac.com