Содержание

[Руководство пользователя DirectAccess Connectivity Assistant (DCA) 2.0 2](#_Toc332027370)

[Использование программного обеспечения DCA 2](#_Toc332027371)

[Значок DirectAccess Connectivity Assistant в области уведомлений 2](#_Toc332027372)

[Проверка наличия подключения DirectAccess и его состояния 2](#_Toc332027373)

[Использование двухфакторной проверки подлинности — с помощью одноразовых паролей и смарт-карты 9](#_Toc332027374)

[Расширенная диагностика 9](#_Toc332027375)

[Использование локального разрешения DNS 10](#_Toc332027376)

# Руководство пользователя DirectAccess Connectivity Assistant (DCA) 2.0

Введение

Данное руководство предназначено для пользователей DirectAccess, на компьютерах которых установлено приложение DirectAccess Connectivity Assistant (DCA) 2.0.

DCA 2.0 повышает эффективность подключений к корпоративной сети с клиентского компьютера, позволяя выполнять проверку подлинности на основе одноразовых паролей.

Используя DCA 2.0, вы можете выполнять следующие задачи.

1. [Проверка наличия подключения DirectAccess и его состояния](#z1)

2. [Использование двухфакторной проверки подлинности — с помощью одноразовых паролей и смарт-карты](#z2)

3. [Расширенная диагностика](#z3)

4. [Использование локального разрешения DNS](#z4)

## Использование программного обеспечения DCA

В этом разделе приведены сведения об использовании DirectAccess Connectivity Assistant (DCA) 2.0 для повышения удобства и производительности подключения DirectAccess, выполнения проверки подлинности на основе одноразовых паролей (OTP) и устранения возможных проблем с подключением DirectAccess.

### Значок DirectAccess Connectivity Assistant в области уведомлений

После установки DCA на компьютере в области уведомлений пользовательского интерфейса появляется соответствующий значок. Этот значок предоставляет информацию о текущем состоянии подключения к корпоративной сети. Если вам не удается получить доступ к корпоративным ресурсам, воспользуйтесь этим значком, чтобы проверить, не сообщает ли DCA о каких-либо проблемах с подключением к корпоративной сети через DirectAccess. Если навести указатель мыши на значок DCA, появляется текстовое сообщение о текущем состоянии подключения DirectAccess.

### Проверка наличия подключения DirectAccess и его состояния

Щелкнув значок DCA, можно открыть всплывающее окно, содержащее дополнительную информацию о текущем состоянии подключения DirectAccess. Сведения в этом окне включают пошаговые инструкции, которые можно выполнить для восстановления подключения.

В следующей таблице описываются состояния подключения DirectAccess.

| **Состояние подключения** | **Сведения** | **Действие** |
| --- | --- | --- |
| Подключение к корпоративной сети работает | Отсутствие символов предупреждения или ошибки в значке DirectAccess означает, что DirectAccess работает надлежащим образом. Примечание. Если компьютер расположен в корпоративной сети, отображается это состояние. | Нет |
| Подключение к корпоративной сети не работает | Символ ошибки в виде красного значка X указывает на отсутствие подключения DirectAccess. | Такие ошибки, которые обычно связаны с неполадками в работе сервера DirectAccess, должны устраняться администратором DirectAccess. |
| Для подключения к корпоративной сети требуется действие пользователя | Символ предупреждения в виде восклицательного знака в желтом треугольнике указывает, что DirectAccess не работает надлежащим образом. | Для доступа ко всем ресурсам необходимо действие пользователя. Значок предупреждения отображается до тех пор, пока не будет выполнено требуемое действие. |

Для каждого состояния подключения DirectAccess предусмотрен ряд сообщений, которые можно просмотреть, щелкнув значок DCA. Сводные сведения об этих сообщениях приведены в следующей таблице.

| **Состояние подключения** | **Отображаемое сообщение** | **Сведения** |
| --- | --- | --- |
| Подключение DirectAccess отсутствует | Операционная система Windows на компьютере не поддерживает DirectAccess. Обратитесь к администратору. | DCA 2.0 работает только с операционными системами Windows 7 Максимальная и Windows 7 Корпоративная. |
| Компонент DirectAccess настроен неправильно. Если проблема продолжает возникать, обратитесь к администратору. | Компьютер не настроен для использования DirectAccess. Это можно проверить в журналах по умолчанию, создаваемых в окне Advanced Diagnostics (Расширенная диагностика). |
| Компьютеру не удается подключиться к серверу DirectAccess. Если проблема продолжает возникать, обратитесь к администратору сайта. | Приложению DCA не удается установить связь с сервером DirectAccess. DCA определяет состояние подключения DirectAccess, пытаясь получить доступ к сетевому серверу, назначенному администратором. Состояние подключения можно проверить в журналах по умолчанию, создаваемых в окне Advanced Diagnostics (Расширенная диагностика).  Если для записи журнала по умолчанию netsh dns show state указано значение Network Location Behavior : Never use Direct Access settings, это может быть вызвано неправильным значением в разделе реестра HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\EnableDAForAllNetworks. Эту проблему можно решить, изменив значение этого раздела реестра с 2 на 0. |
| Невозможно разрешить имена корпоративной сети. Если проблема продолжает возникать, обратитесь к администратору. | Операционной системе Windows не удается разрешить имена ресурсов в корпоративной сети. |
| Компьютер не может подключиться к некоторым корпоративным ресурсам. Если проблема продолжает возникать, обратитесь к администратору. | Приложению DCA не удается получить доступ к одному или нескольким тестовым ресурсам в корпоративной сети. Состояние подключения можно проверить в журналах по умолчанию, создаваемых в окне Advanced Diagnostics (Расширенная диагностика). |
| Подключение компьютера к некоторым корпоративным ресурсам потеряно. Если проблема продолжает возникать, обратитесь к администратору. | Приложению DCA не удается получить доступ к одному или нескольким тестовым ресурсам в корпоративной сети. Состояние подключения можно проверить в журналах по умолчанию, создаваемых в окне Advanced Diagnostics (Расширенная диагностика). |
|  | Приложение DirectAccess Connectivity Assistant настроено неправильно. Если проблема продолжает возникать, обратитесь к администратору. | В DCA отсутствуют данные, которые должны быть настроены администратором. Текущую конфигурацию можно посмотреть в журналах по умолчанию, создаваемых в окне Advanced Diagnostics (Расширенная диагностика). Настройки DCA хранятся в следующем разделе реестра: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\DirectAccessConnectivityAssistant |
| Параметры разрешения имен настроены неправильно. Обратитесь к администратору сайта. | На компьютере повреждена таблица политики разрешения имен, или групповая политика клиента содержит ошибку. Таблица политики разрешения имен используется DirectAccess при разрешении имен для корпоративных ресурсов. |
| Не удается проверить сертификат проверки подлинности. Подключение к списку отзыва сертификатов IP-HTTPS недоступно. Обратитесь к администратору. | Не удается получить доступ к интернет-списку отзыва сертификатов. Сертификат сервера, необходимый для IP-HTTPS, должен быть проверен по списку отзыва сертификатов. IP-HTTPS — это технология туннелирования, которая используется в DirectAccess для передачи трафика IPv6 по IPv4-сети Интернет. |
| Компьютер неправильно настроен для DirectAccess. Протокол IPv6 включен неверно. | Отключены некоторые или все необходимые технологии туннелирования. Обмен данными с сервером DirectAccess происходит по протоколу IPv6. При отключении технологий туннелирования клиент DirectAccess не может установить связь с сервером DirectAccess. |
| Для подключения DirectAccess требуется действие пользователя | Компьютер не соответствует требованиям по обеспечению корпоративной работоспособности. | Если в корпоративной сети проверяется работоспособность компьютера (например, проверяется, установлены ли антивирусные программы или обновления системы безопасности), компьютер, не отвечающий требованиям, не сможет подключиться к корпоративным ресурсам. Во всплывающем диалоговом окне DCA будет предоставлена соответствующая информация и отображены ссылки, которые помогут решить проблему. Например, ссылка на клиентское программное обеспечение, устраняющее проблемы с работоспособностью компьютера. |
| Для доступа к корпоративным ресурсам с помощью DirectAccess требуются учетные данные. Блокирование и разблокировка компьютера с помощью смарт-карты или одноразового пароля. | Администратор может задать обязательное использование смарт-карт или одноразового пароля для доступа к корпоративным ресурсам через DirectAccess. Это сообщение отображается при первой попытке компьютера получить доступ к корпоративному ресурсу при недоступности учетных данных для двухфакторной проверки подлинности, разблокировке с помощью имени пользователя и пароля, а также при пробуждении компьютера из спящего режима или гибернации. См. раздел [Использование двухфакторной проверки подлинности — с помощью одноразовых паролей и смарт-карты](#z2). |
| Компонент DirectAccess настроен для разрешения имен с помощью локальных параметров разрешения. Чтобы восстановить подключение, выберите параметр разрешения имен на сервере DirectAccess. | Приложение DCA настроено для разрешения имен с использованием метода разрешения, который задан локально на компьютере. Чтобы получить доступ к корпоративным ресурсам, необходимо снять флажок Use local DNS resolution (Использовать локальное разрешение DNS) и включить параметр Use corporate DNS resolution (Использовать корпоративное разрешение DNS). Это можно сделать, выбрав параметр в меню справа или перезагрузив компьютер. |
| Подключение к Интернету недоступно. Убедитесь, что компьютер подключен к Интернету. | Операционной системе Windows не удается подключиться к Интернету. |
| Компьютер неправильно настроен для DirectAccess. Необходимо включить брандмауэр Windows. | Чтобы при подключении к серверу DirectAccess можно было использовать IPsec, необходимо включить брандмауэр Windows. IPsec требуется для проверки подлинности DirectAccess. |
| Вы вошли в систему под учетной записью, отличной от учетной записи домена. Войдите в систему под учетной записью домена или заблокируйте и снова разблокируйте компьютер с помощью смарт-карты. | Чтобы подключиться к DirectAccess, войдите на локальный компьютер под учетной записью домена. |

### Использование двухфакторной проверки подлинности — с помощью одноразовых паролей и смарт-карты

Если щелкнуть значок DCA, появляется параметр Блокирование и разблокировка компьютера с помощью смарт-карты или одноразового пароля. Выбор этого параметра приводит к блокировке компьютера. При разблокировке компьютера необходимо выбрать Другие учетные данные, а затем выбрать соответствующий способ проверки подлинности.

 Проверка подлинности на основе одноразовых паролей: введите учетные данные OTP, включая ПИН-код (необязательно), за которым следует код маркера.

 Проверка подлинности с помощью смарт-карты: Вставьте смарт-карту в слот и введите ПИН-код (необязательно).

### Расширенная диагностика

Щелкнув значок DCA правой кнопкой мыши, можно открыть меню, которое позволяет взаимодействовать с DCA. При выборе параметра Расширенная диагностика в контекстном меню DCA открывается диалоговое окно Расширенная диагностика. В этом диалоговом окне представлены подробные сведения о всех текущих проблемах, обнаруженных приложением DCA. Эти дополнительные сведения можно использовать для устранения проблемы или определения пути ее обхода.

После выбора параметра Расширенная диагностика DCA немедленно начинает сбор данных о DCA и клиенте DirectAccess в файл журнала. Создаваемые журналы сжимаются в CAB-файл, который затем можно отправить по электронной почте администратору DirectAccess. Для просмотра файлов журналов можно щелкнуть ссылку в разделе Открыть каталог журналов. Для отправки файлов журналов администратору DirectAccess щелкните команду Журналы электронной почты, чтобы открыть новое сообщение электронной почты. Файлы журналов будут уже вложены в сообщение, и в строке адреса будет указана предварительно определенная контактная информация администратора DirectAccess. Добавьте в текст сообщения любую информацию, описывающую возникшую проблему, и нажмите кнопку Отправить для передачи сообщения электронной почты администратору DirectAccess. Включенную в журнал информацию можно использовать для определения источника проблем с подключением. В случае невозможности подключения к тестовым ресурсам, заданным администратором, журналы включают имена таких ресурсов в текст сообщения об ошибке.

Чтобы проверить версию установленного приложения DCA, можно нажать кнопку О программе в диалоговом окне Расширенная диагностика.

Из окна Расширенная диагностика можно также вызвать процесс проверки подлинности с помощью смарт-карты или одноразового пароля. Для этого необходимо щелкнуть ссылку Блокирование и разблокировка компьютера с помощью смарт-карты или одноразового пароля, если она доступна.

### Использование локального разрешения DNS

По умолчанию параметр Использовать разрешение корпоративных DNS-имен включен и запросы имен разрешаются корпоративным DNS-сервером через подключение DirectAccess. Сюда включаются запросы полных доменных имен и однокомпонентных имен, таких как http://hrweb.

В некоторых случаях требуется доступ к однокомпонентным именам, которые не могут быть разрешены корпоративным DNS-сервером. Чтобы получить доступ к этим ресурсам, щелкните правой кнопкой мыши значок DCA и выберите команду Использовать разрешение местных DNS-имен. Когда этот параметр включен, DCA будет использовать для разрешения имен механизмы DNS (LLMNR и NetBios) на локальном компьютере, вместо того чтобы отправлять запрос через DirectAccess на корпоративный DNS-сервер.

Например, если вы находитесь в расположении клиента с компьютером, на котором установлена программа DirectAccess, и хотите посетить веб-сайт http://thissite в сети клиента с включенным параметром "Использовать разрешение корпоративных DNS-имен", запрос отправляется на ваш корпоративный DNS-сервер и происходит следующее.

 Если в вашей корпоративной интрасети имеется ресурс с именем http://thissite, тогда запрос будет разрешен на этот корпоративный веб-сайт.

 Если же корпоративного сайта с именем http://thissite нет, тогда разрешение имен не будет выполнено, за исключением ситуации, когда корпоративные настройки могут разрешить это имя.

В обоих случаях вы не сможете получить доступ к сайту в сети клиента, если не будет задан параметр "Использовать разрешение местных DNS-имен". При использовании параметра локального разрешения DNS учитывайте следующее.

 Локальное разрешение имен доступно только тогда, когда оно разрешено администратором DirectAccess.

 Локальное разрешение имен действует только при подключении из Интернета. При подключении непосредственно к корпоративной сети оно не будет иметь никакого эффекта.

 При выборе локального разрешения имен в области уведомлений DCA отображается желтый значок предупреждения, чтобы напомнить о необходимости включения корпоративного разрешения DNS после завершения доступа к локальному ресурсу.

 Если выполнялось отключение и повторное подключение к сети и серверу DirectAccess (например, если перезапускался компьютер), параметр Use corporate DNS resolution (Использовать корпоративное разрешение DNS) будет включен автоматически после возобновления подключения DirectAccess. Чтобы продолжить использование локального разрешения имен, необходимо повторно выбрать параметр Use local DNS resolution (Использовать разрешение местных DNS-имен).