SIEMENS

SIMATIC

# TIA Portal Cloud Connector

Руководство по эксплуатации




07/2016
A5E37384252-AA

# Важная информация

**Система предупреждений**

Данное руководство содержит особые замечания, призванные обратить внимание пользователя на обстоятельства, связанные с безопасностью для персонала и имущества. Замечания, касающиеся безопасности для жизни и здоровья персонала, отмечены значком с восклицательным знаком. Варианты оформления замечаний с разной степенью риска представлены ниже:

| ⚠ **Опасность** |
|---|
| Замечание, игнорирование которого **приведет** к гибели или **причинит** тяжелый ущерб здоровью людей. |

| ⚠ **Предупреждение** |
|---|
| Замечание, игнорирование которого **может привести** к гибели или **может причинить** тяжелый ущерб здоровью людей. |

| ⚠ **Предостережение** |
|---|
| Замечание, игнорирование которого **может причинить** легкий ущерб здоровью людей. |

| **Предостережение** |
|---|
| Замечание, игнорирование которого может причинить ущерб оборудованию и имуществу. |

В случае, когда одновременно присутствуют риски с разным уровнем опасности, следует замечание об опаснейшем из имеющихся рисков. Замечания, отмеченные как опасные для жизни и здоровья людей, могут содержать также информацию о рисках для имущества.

**Квалификация персонала**

Продукт/система, описанные в данной документации, предназначены для использования только персоналом, имеющим соответствующую квалификацию и подготовку и в соответствии с актуальной документацией, в частности, содержащей необходимые замечания, касающиеся безопасности для персонала и имущества. Квалифицированный персонал - это персонал, который используя свои знания и опыт, способен оценить все риски и избежать потенциальных опасностей при работе с представленным продуктом/системой.

**Правильное использование продукции Siemens**

Необходимо учитывать следующее:

| ⚠ **Предупреждение** |
|---|
| Продукты Siemens предназначены только для задач, указанных в каталоге, и в соответствии с технической документацией. Применение изделий других производителей возможно при наличии рекомендаций и разрешений Siemens. При транспортировке, хранении, сборке, установке, пуске, наладке, эксплуатации и обслуживании необходимо использовать только рекомендованные режимы и действия. Во всех случаях необходимо обеспечивать регламентированные условия окружающей среды. Вся необходимая информация может быть получена из актуальной документации Siemens. |

**Торговые марки**

Все названия, помеченные символом ®, являются зарегистрированными торговыми марками Siemens AG. Другие наименования, используемые в данной документации, также могут быть торговыми марками, неправомерное использование которых сторонними участниками может нарушать права их владельцев.

**Отказ от ответственности**

Мы проверили содержание данной публикации на соответствие описанному программному и аппаратному обеспечению. Так как нельзя заранее предусмотреть всех возможных изменений, мы не можем гарантировать их полное соответствие на текущий момент. Тем не менее информация в данной документации регулярно просматривается и все необходимые изменения включаются в последующие издания.

# Содержание

# Вводная информация по TIA Portal Cloud Connector 1

## 1.1 Вопросы безопасности

Siemens предлагает изделия и проекты, поддерживающие функции промышленной безопасности, обеспечивающие безопасную работу оборудования, систем управления, механизмов, приборов и сетей.

Для защиты установок, систем, механизмов и сетей от киберугроз, необходимо выполнить, и постоянно поддерживать, всеобъемлющую, отвечающую современным требованиям концепцию производственной безопасности. Продукты и проекты Siemens представляют только один из элементов такой концепции.

Пользователь обязан предусмотреть меры по предотвращению несанкционированного доступа к установкам, системам, механизмам и сетям. Системы, механизмы и компоненты должны подключаться к сети предприятия или интернету только в случае производственной необходимости с использованием соответствующих мер защиты (например, с использованием файрволов и сегментации сети) на локальном уровне.

Необходимо учитывать руководящие документы Siemens по обеспечению вопросов безопасности. Для получения дополнительной информации по вопросам промышленной безопасности обратитесь к следующему источнику: (http://www.siemens.com/industrialsecurityhttp://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx).

Изделия и проекты Siemens постоянно совершенствуются с целью повышения эффективности и безопасности их использования. Siemens настоятельно рекомендует пользователям регулярно получать информацию об обновлениях продуктов, чтобы всегда использовать самые последние их версии. Использование же версий продуктов, которые больше не поддерживаются производителем, или необеспечение своевременного их обновления может привести к существенному росту киберугроз.

Для получения своевременной информации о появлении обновлений для продуктов Siemens подпишитесь на рассылку Siemens Industrial Security RSS Feed по ссылке: (http://www.siemens.com/industrialsecurityhttp://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx).

## 1.2 Основы работы с TIA Portal Cloud Connector

**Функция TIA Portal Cloud Connector**

Среда проектирования TIA Portal обеспечивает пользователю работу в виртуальной среде. TIA Portal Cloud Connector является опционным ПО для целого ряда продуктов с поддержкой доступа к интерфейсам локальных PG/PC. С его помощью соответствующие устройства SIMATIC могут функционировать в среде TIA Portal в приватном (частном) облаке с использованием доступа к удаленному рабочему столу Remote Desktop.

Вы можете использовать ПО TIA Portal Cloud Connector как расширение для доступа из виртуальной среды (VM) к устройствам SIMATIC, локально подключенным к Вашему PG/PC. Для этого необходимо инсталлировать ПО TIA Portal Cloud Connector в VM и на PG/PC, к которому устройства SIMATIC подключены. ПО TIA Portal Cloud Connector также обеспечивает удаленный доступ к устройствам SIMATIC, подключенным к другому PG/PC, из VM с интерфейсом Remote Desktop, даже если ПО TIA Portal Cloud Connector установлено в частной сети. Такой доступ был бы невозможен без ПО TIA Portal Cloud Connector.

Использование виртуальных машин VM вместе с TIA Portal Cloud Connector обеспечивает следующие преимущества:

- поддержка современных приватных облачных инфраструктур посредством:
  - полной масштабируемости,
  - отсутствия требования инсталляции на отдельных рабочих станциях,
  - централизованной техподдержки и администрирования TIA Portal в VM,
  - централизованного хранения данных соответствующих проектов и библиотек;
- внутрисетевой доступ к PLC и HMI-устройствам;
- безопасные соединения по протоколу HTTPS (для Windows 8.1 или новее);
- поддержка всех локальных интерфейсов рабочих станций;
- быстрый доступ к TIA Portal различных версий;
- более эффективное использование доступных лицензий;
- простое техобслуживание механизмов.

**Способ приобретения ПО TIA Portal Cloud Connector**

ПО TIA Portal Cloud Connector поставляется вместе со следующими программными продуктами SIMATIC в версии TIA Portal V14.0:

- STEP 7 Basic
- STEP 7 Professional
- WinCC Basic
- WinCC Professional
- WinCC Comfort/Advanced

Для использования ПО TIA Portal Cloud Connector на PG/PC требуется приобрести отдельную лицензию.

**Примечание**

ПО TIA Portal Cloud Connector предназначено только для задач разработки с TIA Portal. Интерактивный доступ во время производственного процесса (например, SCADA) не допускается. Это особенно актуально в аспекте вопроса безопасности.

**Конфигурирование ПО TIA Portal Cloud Connector**

Перед установкой соединения с помощью TIA Portal Cloud Connector необходимо сконфигурировать параметры TIA Portal Cloud Connector. Конфигурация зависит от коммуникационной роли Вашего устройства. ПО TIA Portal Cloud Connector может быть установлено на устройства, выполняющие следующие роли в сети:

- Сетевая роль устройства - "User device" ("Устройство пользователя"):

  "Устройство пользователя" или "пользовательское устройство" - это Ваша рабочая станция - PG/PC, к которой подключено соответствующее оборудование. При этом нет необходимости устанавливать программное обеспечение TIA Portal на данное устройство.

  Такая коммуникационная роль ("User device") назначается устройству по умолчанию в случае обособленной установки ПО TIA Portal Cloud Connector, другими словами, при его инсталляции отдельно от ПО TIA Portal.

  См. также:
  Конфигурирование ПО TIA Portal Cloud Connector на PG/PC (страница 34)

- Сетевая роль устройства - "Remote device" ("Удаленное устройство"):

  "Удаленное устройство" - это VM, то есть виртуальная машина (виртуальная среда), в которой установлено ПО TIA Portal.

  Такая коммуникационная роль ("Remote device") назначается устройству по умолчанию в случае одновременной установке на нем ПО TIA Portal Cloud Connector и ПО TIA Portal.

  См. также:
  Конфигурирование ПО TIA Portal Cloud Connector в VM (страница 36)

**См. также**

Пользовательский интерфейс TIA Portal Cloud Connector (страница 8)

Примеры применения TIA Portal Cloud Connector (страница 17)

Особенности работы с виртуальной машиной (страница 20)

Использование сертификатов (страница 21)

Системные требования (страница 23)

Подготовка виртуальной машины (VM) к работе (страница 27)

Использование виртуальной машины (VM) (страница 33)

## 1.3 Пользовательский интерфейс TIA Portal Cloud Connector

Пользовательский интерфейс TIA Portal Cloud Connector состоит из следующих элементов:

- поле ввода на панели задач интерфейса Windows
- окно настроек TIA Portal Cloud Connector
- окно отображения состояния TIA Portal Cloud Connector
- информационное окно TIA Portal Cloud Connector
- отображение TIA Portal в строке состояния

**Значок TIA Portal Cloud Connector на панели задач Windows**

После запуска TIA Portal Cloud Connector появляется значок Cloud Connector в информационной области панели задач интерфейса Windows. Если щелкнуть правой кнопкой манипулятора "мышь" на этом значке, то откроется меню в интерфейсе TIA Portal Cloud Connector.

Ниже показан значок TIA Portal Cloud Connector на панели задач интерфейса Windows, если коммуникационные партнеры недоступны:

Этот значок меняет цвет при изменении состояния доступности коммуникационных партнеров.

Ниже показано меню в информационной области для случая установления коммуникационной роли устройства "Remote device" ("удаленное устройство"):


Это меню обеспечивает активацию следующих опций:

- "Enable communication": Эта опция позволяет активировать установление коммуникационных связей для удаленного и для пользовательского устройства.
- "Configuration (remote device/user device)": Эта опция позволяет настроить параметры ОП TIA Portal Cloud Configurator для соответствующей сетевой роли.
- "Status display": Эта опция активирует отображение информации обо всех операциях.
- "About": Эта опция открывает информационное окно "About" для TIA Portal Cloud Connector. В частности, в этом окне Вы можете найти номер версии ПО.
- "Help": Эта опция открывает интерактивную справку TIA Portal Cloud Connector.
- "Exit": Эта опция закрывает TIA Portal Cloud Connector.

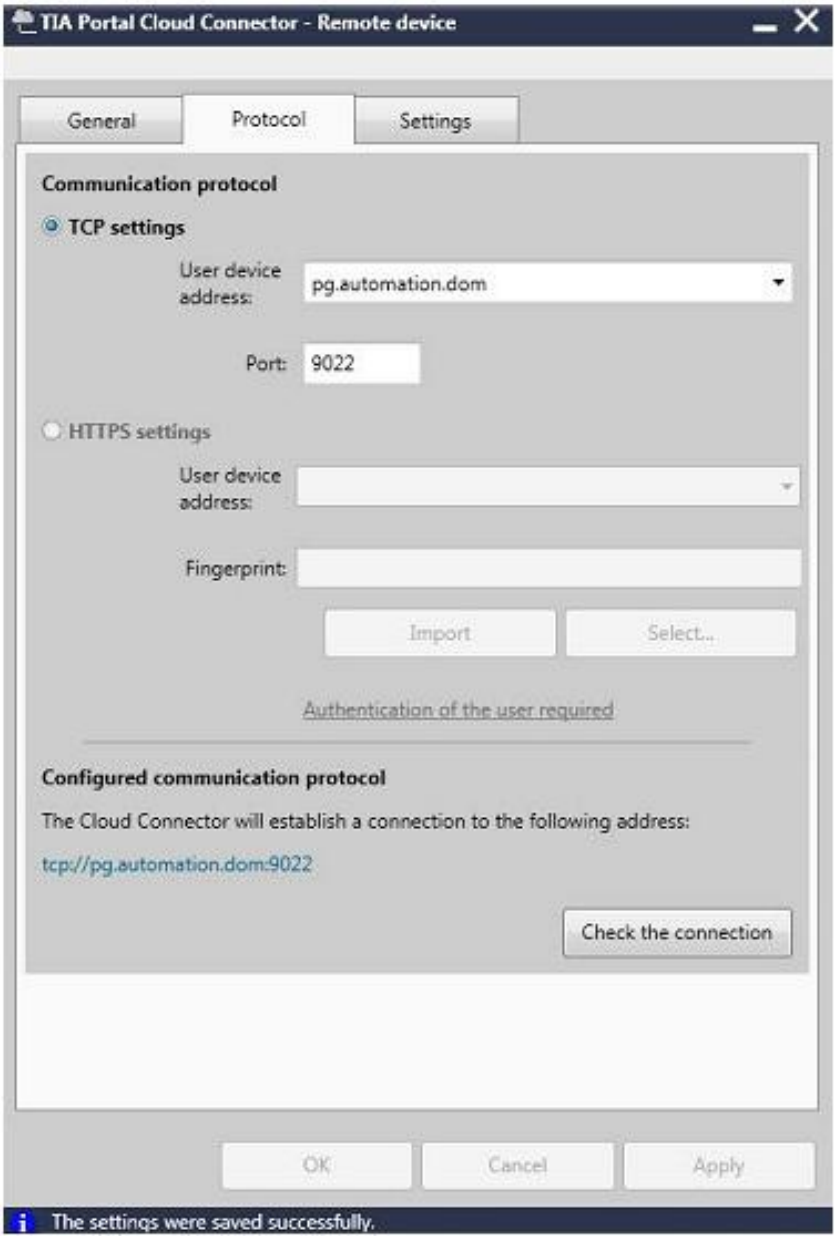
**Окно настроек TIA Portal Cloud Connector**

Опции пользовательского интерфейса TIA Portal Cloud Connector зависят от выбранной сетевой роли устройства.

Ниже показаны несколько вкладок в интерфейсе TIA Portal Cloud Connector для сетевой роли "Remote device" ("удаленное устройство"):

На вкладке "General" Вы можете выбрать вариант сетевой роли устройства и активировать коммуникационные соединения:

На вкладке "Protocol" Вы можете отредактировать настройки коммуникационного соединения:



На вкладке "Settings" Вы можете выбрать опции запуска программы, языка интерфейса и режима аутентификации пользователя:

Ниже в таблице представлен обзор всех настроек и элементов управления для сетевой роли устройства "Remote device" ("удаленное устройство"):

| **Вкладка** | **Область** | **Опция / кнопка** | **Описание** |
|---|---|---|---|
| General | Communication role | User device | Для использования пользовательского PG/PC с подключенным SIMATIC-устройством |
| | | Remote device | Для использования виртуальной среды (VM) в "приватном облаке" на сервере, в котором установлен TIA Portal, используемый с устройства пользователя посредством подключения к удаленному рабочему столу (Remote Desktop). |
| | Cloud Connector communication | Enable communication<br>Disable communication | Для активации/деактивации коммуникационного соединения с рабочей станцией на PG/PC |
| Protocol | Communication protocol | | Для выбора протокола коммуникационного обмена. Может быть выбран протокол TCP или HTTPS (Windows 8.1 или новее). |
| | TCP settings | User device address | Для указания IP-адреса или имени пользовательского устройства |
| | | Port | Для указания номера сетевого порта |
| | HTTPS settings | User device address | Для указания IP-адреса или имени пользовательского устройства |
| | | Fingerprint | Для установки достоверности сертификата |
| | | Import | Для импорта имеющегося сертификата в хранилище сертификатов Windows. Вы можете использовать импортированный сертификат для шифрования данных для пересылки с HTTPS. |
| | | Select | Для выбора ранее импортированного сертификата для шифрования данных |
| | Configured communication protocol | Check the connection | Для тестирования коммуникационного соединения |
| Settings | Autostart | Enable automatic start of the Cloud Connector | Для активации/деактивации автоматического запуска TIA Portal Cloud Connector при запуске системы |
| | Language | Select language | Для выбора языка пользовательского интерфейса для TIA Portal Cloud Connector |
| | User authentication | Name of the user certificate | Для отображения названия используемого пользовательского сертификата |
| | | Fingerprint | Для вычисления контрольной суммы сертификата для установления его достоверности |
| | | Create | Для создания нового сертификата для аутентификации пользователя |
| | | Select | Для выбора имеющегося сертификата из хранилища сертификатов Windows |
| | | Export | Для экспорта используемого пользовательского сертификата |

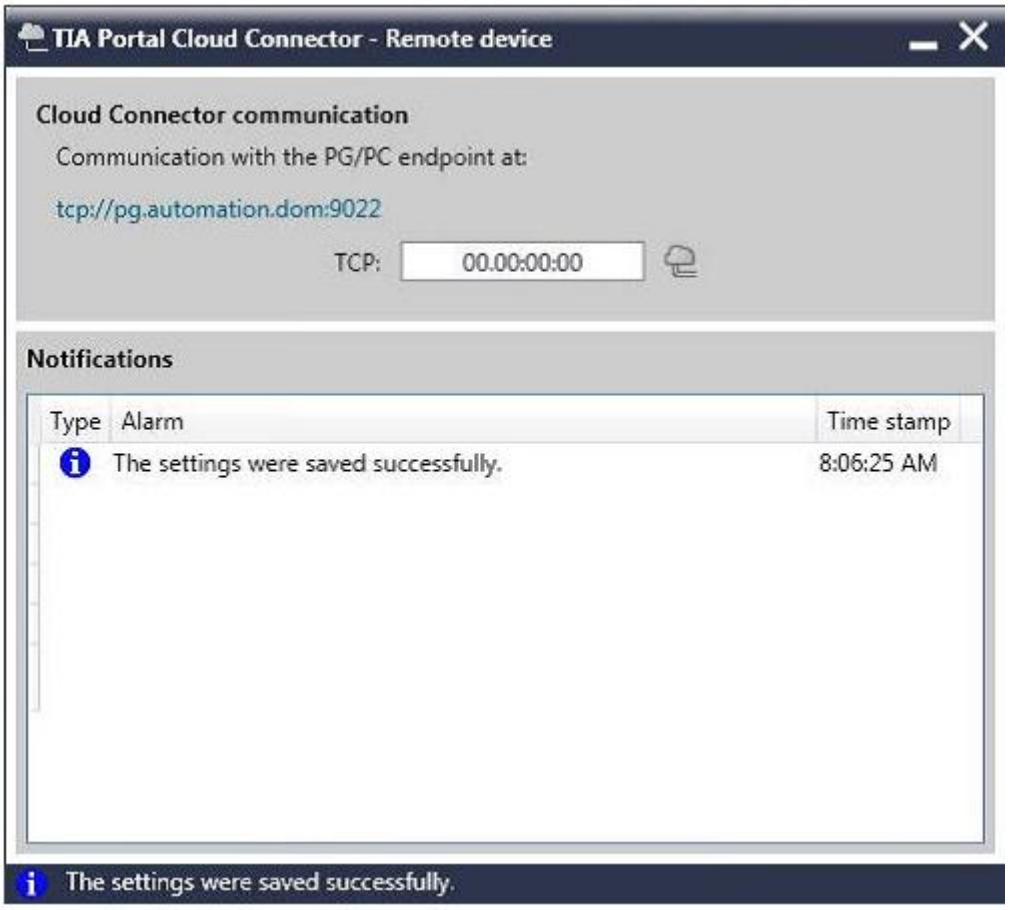
Ниже в таблице представлен обзор всех настроек и элементов управления для сетевой роли устройства "User device" ("пользовательское устройство"):

| **Вкладка** | **Область** | **Опция / кнопка** | **Описание** |
|---|---|---|---|
| General | Communication role | User device | Для использования пользовательского PG/PC с подключенным SIMATIC-устройством |
| | | Remote device | Для использования виртуальной среды (VM) в "приватном облаке" на сервере, в котором установлен TIA Portal, используемый с устройства пользователя посредством подключения к удаленному рабочему столу (Remote Desktop). |
| | Cloud Connector communication | Enable communication<br>Disable communication | Для активации/деактивации коммуникационного соединения с рабочей станцией на PG/PC |
| Protocol | TCP endpoint | Port | Для указания номера сетевого порта. Номер порта пользовательского устройства должен соответствовать номеру порта удаленного устройства. |
| | HTTPS endpoint | User device address | Для указания IP-адреса или имени пользовательского устройства |
| | | Fingerprint | Для установки достоверности сертификата |
| | | Create | Для создания нового сертификата для шифрования данных. |
| | | Export | Для экспорта используемого пользовательского сертификата |
| | | Select | Для выбора имеющегося сертификата из хранилища сертификатов Windows |
| Настройки | Autostart | Enable automatic start of the Cloud Connector | Для активации/деактивации автоматического запуска TIA Portal Cloud Connector при запуске системы |
| | Language | Select language | Для выбора языка пользовательского интерфейса для TIA Portal Cloud Connector |
| | User authentication | Trusted user certificates | Для отображения списка всех имеющихся и списка доверенных пользовательских сертификатов |
| | | Import | Для импорта пользовательского сертификата, который был создан на удаленном устройстве в хранилище сертификатов Windows. |
| | | Add | Для добавления сертификата из хранилища сертификатов Windows в список доверенных сертификатов. |
| | | Remove | Для удаления выбранного сертификата из списка доверенных сертификатов. Тем не менее удаленный таким образом сертификат остается в хранилище сертификатов Windows. |

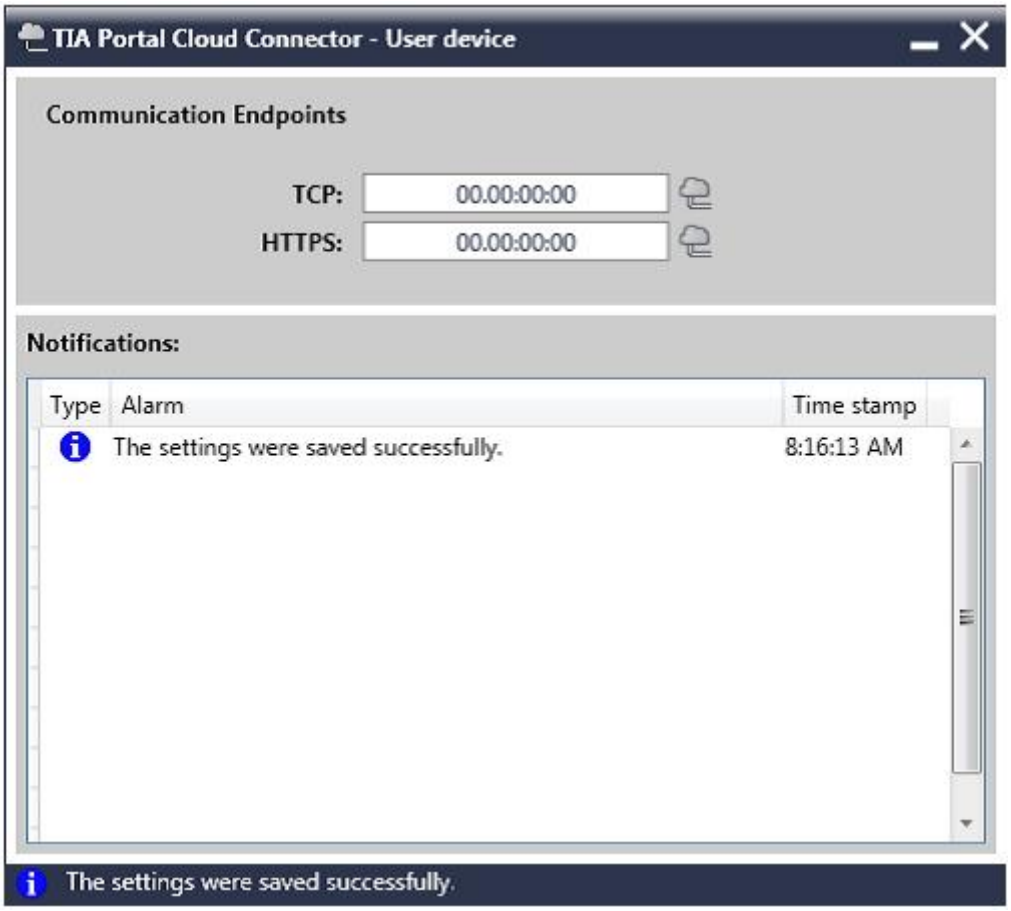
**Отображение текущего режима и состояния TIA Portal Cloud Connector**

В окне состояния отображается информация, предупреждения и сообщения об ошибках, возникающих при использовании TIA Portal Cloud Connector.

Ниже показано окно состояния для коммуникационной роли "Remote device" ("удаленное устройство"):



Ниже показано окно состояния для коммуникационной роли "User device" ("пользовательское устройство"):



**Информационное окно TIA Portal Cloud Connector - About**

Ниже показано окно с информацией об установленном ПО TIA Portal Cloud Connector.


**Отображение TIA Portal в строке состояния**

В строке состояния TIA Portal отображается текущее состояние коммуникационного соединения с SIMATIC-устройствами с помощью TIA Portal Cloud Connector. Дополнительный значок-пиктограмма в строке состояния сообщает о состоянии соединения с помощью TIA Portal Cloud Connector:

**См. также**

Основы работы с TIA Portal Cloud Connector (страница 6)

Примеры применения TIA Portal Cloud Connector (страница 17)

Особенности работы с виртуальной машиной (страница 20)

Использование сертификатов (страница 21)

Системные требования (страница 23)

Подготовка виртуальной машины (VM) к работе (страница 27)

Использование виртуальной машины (VM) (страница 33)

## 1.4 Примеры применения TIA Portal Cloud Connector

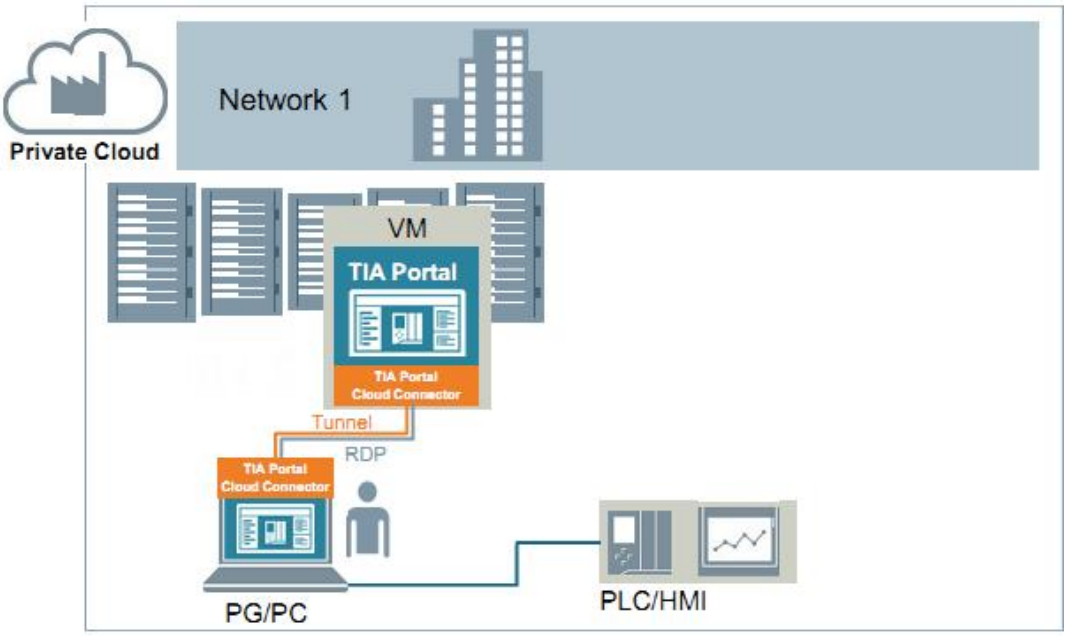
Аналоговыми значениями могут описываться, например, следующие физические параметры среды в рабочей зоне.

- Температура
- Давление

**Доступ к оборудованию, подключенному к PG/PC**

ПО TIA Portal устанавливается в корпоративном приватном облаке. При этом нет необходимости инсталлировать TIA Portal на пользовательские PG/PC. Оборудование (PLC/HMI) для автоматизации процесса подключается к пользовательским PG/PC. TIA Portal Cloud Connector инсталлируется в VM и на пользовательский PG/PC. Для установки TIA Portal Cloud Connector на PG/PC требуется отдельная лицензия. Пользователь регистрируется в виртуальной среде VM с использованием подключения к удаленному рабочему столу (Remote Desktop) и может работать с ПО TIA Portal как обычно. Использование TIA Portal Cloud Connector обеспечивает доступ к оборудованию, подключенному к PG/PC.

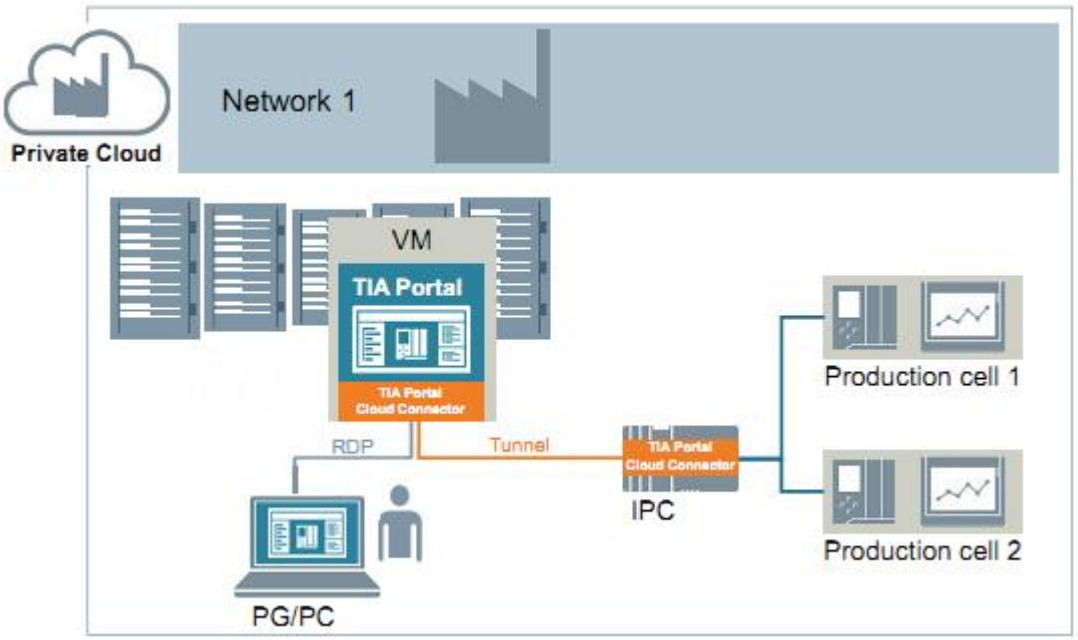
Ниже представлена иллюстрация использования TIA Portal Cloud Connector в виртуальной среде; при этом оборудование для автоматизации технологического процесса подключено к PG/PC:

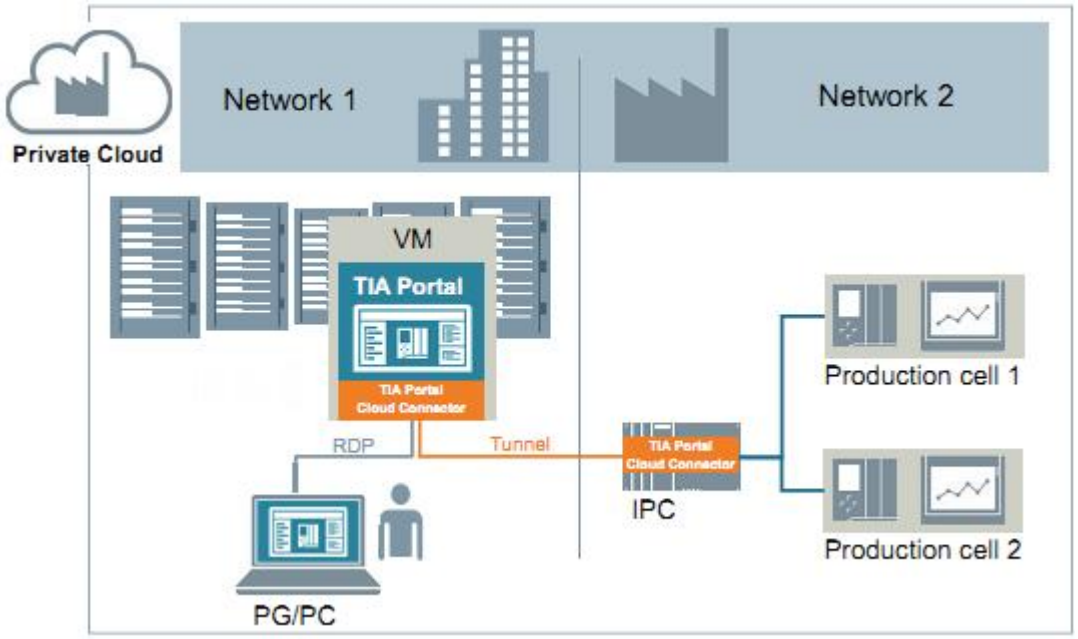


**Доступ к оборудованию, подключенному к отдельной рабочей станции PG/PC**

ПО TIA Portal устанавливается в виртуальной машине. При этом TIA Portal не устанавливается на Вашем PG/PC. Оборудование для автоматизации процесса подключается к отдельной станции (в нашем примере - IPC), включенной в ту же сеть, в которой находится Ваша станция (Network1 - см. верхний рисунок), или в другую сеть (Network2 - см. нижний рисунок). В нашем примере ПО TIA Portal Cloud Connector установлено на станции IPC и в VM. Используя подключение к удаленному рабочему столу (Remote Desktop), Вы входите в VM, где можете работать с TIA Portal как обычно. Между VM и IPC устанавливается соединение с помощью TIA Portal Cloud Connector, благодаря чему обеспечивается доступ к оборудованию для автоматизации (PLC/HMI).

Ниже представлена иллюстрация использования TIA Portal Cloud Connector в виртуальной среде; при этом оборудование для автоматизации технологического процесса подключено к другой рабочей станции (в данном примере - IPC):



**См. также**

Основы работы с TIA Portal Cloud Connector (страница 6)
Пользовательский интерфейс TIA Portal Cloud Connector (страница 8)
Особенности работы с виртуальной машиной (страница 20)
Использование сертификатов (страница 21)
Системные требования (страница 23)
Подготовка виртуальной машины (VM) к работе (страница 27)
Использование виртуальной машины (VM) (страница 33)

## 1.5 Особенности работы с виртуальной машиной

**Симуляция**

Для симуляции PLC-программы сначала необходимо деактивировать TIA Portal Cloud Connector. В то же время для симуляции HMI-устройств деактивация TIA Portal Cloud Connector не требуется.

**Использование пакетов обновления и сервисных пакетов**

Пакеты обновления и сервисные пакеты могут инсталлироваться в шаблон VM и впоследствии - в соответствующие VM. Для этого необходимо использовать встроенные средства обновления (update) в TIA Portal.

Для получения дополнительной информации обратитесь к информационной системе TIA Portal.

**См. также**

Основы работы с TIA Portal Cloud Connector (страница 6)

Пользовательский интерфейс TIA Portal Cloud Connector (страница 8)

Примеры применения TIA Portal Cloud Connector (страница 17)

Использование сертификатов (страница 21)

Системные требования (страница 23)

Подготовка виртуальной машины (VM) к работе (страница 27)

Использование виртуальной машины (VM) (страница 33)

# 1.6 Использование сертификатов

**Использование сертификатов в TIA Portal Cloud Connector**

При использовании Windows, начиная с версии Windows 8.1, Вы можете применять протокол HTTPS для повышения безопасности коммуникаций. TIA Portal Cloud Connector поддерживает использование сертификатов для обеспечения безопасных коммуникаций посредством HTTPS-соединения.

Для установления безопасного соединения между пользовательским устройством и удаленным устройством требуются следующие сертификаты:

- Сертификат для шифрования данных
- Сертификат для аутентификации пользователя

Если сертификат недоступен, или если сертификаты пользовательского устройства и удаленного устройства не соответствуют друг другу, то коммуникационная связь блокируется.

**Сертификат для шифрования данных**

Необходимо создать сертификат для шифрования данных на пользовательском устройстве. Затем этот сертификат через локальный привод удаленного устройства может быть импортирован в TIA Portal Cloud Connector. При установлении соединения между устройствами проводится проверка подлинности сертификатов. Если сертификаты достоверны, тогда коммуникации между устройствами поддерживаются после установления достоверности сертификата для аутентификации пользователя.

**Сертификат для аутентификации пользователя**

Необходимо создать сертификат для шифрования данных на удаленном устройстве. Затем этот сертификат копируется на пользовательское устройство и импортируется в TIA Portal Cloud Connector. При установлении соединения между устройствами проводится проверка подлинности сертификатов. Если соответствующие сертификаты достоверны, тогда между устройствами поддерживаются коммуникации по защищенному протоколу.

**См. также**

Основы работы с TIA Portal Cloud Connector (страница 6)

Пользовательский интерфейс TIA Portal Cloud Connector (страница 8)

Примеры применения TIA Portal Cloud Connector (страница 17)

Особенности работы с виртуальной машиной (страница 20)

Создание сертификата для шифрования данных (страница 38)

Экспорт сертификата для шифрования данных (страница 39)

Импорт сертификата для шифрования данных (страница 40)

Выбор сертификата для шифрования данных (страница 41)

Создание сертификата для аутентификации пользователя (страница 42)

Экспорт сертификата для аутентификации пользователя (страница 43)

Импорт сертификата для аутентификации пользователя (страница 44)

Добавление сертификата для аутентификации пользователя (страница 45)

Выбор сертификата для аутентификации пользователя (страница 46)

Удаление сертификата для аутентификации пользователя (страница 47)

# Системные требования 2

## 2.1 Системные требования к PG/PC

**Поддерживаемые операционные системы**

Чтобы использовать TIA Portal Cloud Connector на Вашем PG/PC должна быть установлена одна из следующих операционных систем:

- Windows 7 (64-bit)
- Windows 8.1 (64-bit)
- Windows 10 (64-bit)

**Примечание**

Необходимо учитывать, что:

- TIA Portal Cloud Connector не может использоваться в 32-разрядных операционных системах;
- операционная система должна быть обновлена до последней версии; для этого регулярно выполняйте все критические обновления Windows;
- TIA Portal Cloud Connector не может использоваться, если установлен пакет SIMATIC NET.

**Лицензии для TIA Portal Cloud Connector**

Для работы с ПО TIA Portal Cloud Connector необходимо действующий лицензионный ключ (License Key) для каждого устройства, которое Вы определяете как "User device" ("пользовательское") в TIA Portal Cloud Connector. Лицензионный ключ не требуется для устройств, определяемых как "remote devices" ("удаленное устройство").

Вы можете добавить лицензионный ключ (License Key) при инсталляции или переслать его с использованием менеджера лицензий Automation License Manager после инсталляции.

**См. также**

Системные требования к VM (страница 24)

Лицензии (страница 26)

## 2.2 Системные требования к VM

**Поддерживаемые "гостевые" операционные системы и платформы виртуализации**

Вы можете использовать TIA Portal в виртуальной машине (VM). Для этого может быть использована одна из следующих платформ виртуализации в указанной ниже или в более новой версии:

- VMware vSphere Hypervisor (ESXi) V6.0
- Microsoft Windows Server 2012 R2 Hyper-V
- Microsoft Windows Azure Pack V1.0

Вы можете установить в VM один или несколько пакетов ПО:

- SIMATIC STEP 7 Basic
- SIMATIC STEP 7 Professional
- SIMATIC WinCC Basic
- SIMATIC WinCC Comfort/Advanced
- SIMATIC WinCC Professional

В добавление к этим пакетам ПО Вы можете установить также дополнительные опционные пакеты STEP 7 и WinCC.

**Примечание**

**Совместное использование ПО TIA Portal Cloud Connector с ПО SIMATIC NET**

ПО TIA Portal Cloud Connector не может использоваться, если в VM установлен пакет SIMATIC NET.

В зависимости от выбранного ПО в VM поддерживаются различные "гостевые" операционные системы:

| "Гостевая" операционная система | SIMATIC STEP 7 Basic | SIMATIC STEP 7 Professional | SIMATIC WinCC Basic | SIMATIC WinCC Professional | SIMATIC WinCC Advanced |
|---|---|---|---|---|---|
| Windows Server 2008 R2 StdE SP1 (full installation) (64-bit) | – | × | – | × | × |
| Windows Server 2012 R2 StdE (full installation) (64-bit) | × | × | × | × | × |
| Windows 7 Home Premium SP1 (64-bit) | × | – | × | – | – |
| Windows 7 Professional SP1 (64-bit) | × | × | × | × | × |
| Windows 7 Enterprise SP1 (64-bit) | × | × | × | × | × |
| Windows 7 Ultimate SP1 (64-bit) | × | × | × | × | × |
| Windows 8.1 (64-bit) | × | – | × | – | – |
| Windows 8.1 Professional (64-bit) | × | × | × | × | × |
| Windows 8.1 Enterprise (64-bit) | × | × | × | × | × |
| - операционная система не поддерживается<br>× операционная система поддерживается | | | | | |

**Примечание**

Необходимо учитывать, что:

- 32-разрядные "гостевые" операционные системы в VM не поддерживаются;
- требования к оборудованию для "гостевых" операционных систем такие же как и у TIA-продуктов;
- программатор SIMATIC USB Prommer не поддерживается;
- для использования SD-карты в VM сначала необходимо инициализировать ее в VM как съемный носитель; как выполнить инициализацию носителя, Вы можете узнать в справочной системе Вашей платформы виртуализации;
- операционная система должна быть обновлена до последней версии; для этого регулярно выполняйте все критические обновления Windows.

### Инсталляция TIA Portal Cloud Connector

Имеется два способа инсталляции TIA Portal Cloud Connector:

- Вы можете активировать опцию установки TIA Portal Cloud Connector во время инсталляции программных пакетов SIMATIC, упомянутых выше. При этом TIA Portal Cloud Connector устанавливается вместе с пакетами ПО SIMATIC.
- Вы можете инсталлировать TIA Portal Cloud Connector независимо от программных пакетов SIMATIC. Установочный файл находится в папке "Support" на установочном носителе. Вы можете сделать этот установочный файл доступным по сети. Как администратор в VM Вы можете написать скрипт для автоматической установки TIA Portal Cloud Connector. Необходимо помнить однако, что для установки TIA Portal Cloud Connector требуется лицензия для каждого PG/PC.

### Лицензии для TIA Portal Cloud Connector

Для работы с TIA Portal Cloud Connector в VM лицензия TIA Portal Cloud Connector не требуется, если для устройства была сконфигурирована коммуникационная роль - "удаленное устройство" ("Remote device").

### См. также

Системные требования к PG/PC (страница 23)

Лицензии (страница 26)

## 2.3 Лицензии

**Лицензии для ПО SIMATIC**

Для каждой установки в виртуальной среде различных пакетов ПО SIMATIC TIA Portal (STEP 7, WinCC) требуется отдельная лицензия. Если шаблон VM копируется или клонируется, то эта копия рассматривается как отдельная инсталляция. Тем не менее для TIA Portal в PG/PC, используемом для доступа к VM, лицензия не требуется, если не выполняется локальная установка этого программного обеспечения.

При активации программного обеспечения с помощью "плавающих" лицензионных ключей может использоваться сервер лицензий.

**Лицензии для TIA Portal Cloud Connector**

Для работы с TIA Portal Cloud Connector для каждого устройства, которое Вы определяете в TIA Portal Cloud Connector как "пользовательское" ("user device"), необходим действующий лицензионный ключ. Лицензионный ключ не требуется для устройств, определяемых как "удаленные" ("remote device").

Вы можете добавить лицензионный ключ непосредственно при инсталляции ПО или после инсталляции - с использованием менеджера лицензий Automation License Manager.

**См. также**

Системные требования к PG/PC (страница 23)

Системные требования к VM (страница 24)

# Подготовка виртуальной машины (VM) к работе 3

## 3.1 Создание нового шаблона VM

Вы можете использовать следующие платформы виртуализации:

- VMware vSphere Hypervisor (ESXi) V6.0
- Microsoft Windows Server 2012 R2 Hyper-V
- Microsoft Windows Azure Pack V1.0

В соответствии с используемой платформой виртуализации для виртуальной машины (VM) создается определенный шаблон. Дополнительную информацию по данному вопросу Вы можете найти в справочной системе используемой платформы виртуализации.

Среда разработки SIMATIC в VM устанавливается так же как на любом PG/PC.

**Основные шаги по созданию нового шаблона виртуальной машины**

1. Установите ПО для создания виртуальной среды (виртуальной машины) VM.
2. Установите в VM необходимое ПО SIMATIC, например, SIMATIC STEP 7 (TIA Portal V14 или новее) или SIMATIC WinCC (TIA Portal V14 или новее) в соответствующей комплектации (Basic, Professional, Comfort/Advanced).

**Примечание**

Процедура инсталляции ПО TIA Portal в виртуальной машине (VM) идентична процедуре инсталляции ПО TIA Portal на PG/PC. Дополнительную информацию по данному вопросу Вы можете найти в инструкциях по инсталляции TIA Portal.

3. При необходимости установите соответствующие опционные пакеты ПО, например, SIMATIC STEP 7 Safety Advanced.
4. При необходимости установите соответствующие дополнительные совместимые пакеты ПО, которые должны быть доступны для всех пользователей.
5. Сконфигурируйте VM в соответствии с пользовательскими требованиями.
6. Следуйте инструкциям по созданию шаблона для Вашей платформы виртуализации.

**Результат**

В результате сформирован шаблон VM, который Вы можете скопировать для дальнейшего использования. Помните, что для использования копии шаблона VM необходимы лицензии. Для управления лицензиями Вы можете использовать сервер лицензий.

**См. также**

Централизованное сохранение настроек пользователя и проекта (страница 28)

Использование сервера лицензий (страница 30)

Инсталляция TIA Portal Cloud Connector в VM (страница 30)

## 3.2 Централизованное сохранение настроек пользователя и проекта

Если пользователи виртуальной машины VM сохраняют свои настройки и проекты в VM, то при удалении VM эти настройки и проекты безвозвратно теряются. Для использования настроек и проектов в других VM их необходимо хранить вне VM. Вы можете задать переменные среды для VM, которые будут определять пути сохранения пользовательских настроек и проектов. Задайте переменные среды перед первым запуском TIA Portal. Если переменные среды не определены до первого запуска TIA Portal, то TIA Portal сохраняет файл настроек в папке по умолчанию и в дальнейшем использует этот файл. Пока существует этот файл, TIA Portal игнорирует любые переменные среды, которые были определены позднее.

В соответствующих переменных среды Вы можете задать следующие параметры:

- Путь для сохранения пользовательских настроек. Все настройки пользователя сохраняются в заданной директории.
- Путь для сохранения пользовательских проектов. Заданный путь используется как путь сохранения вновь созданного проекта. Тем не менее Вы можете сохранять проект в различных указанных директориях.

Переменные среды могут быть определены вручную или с помощью скрипта. Вы можете создать отдельные скрипты для определения места хранения настроек и места хранения проектов, или же можете создать один скрипт для одновременного определения всех переменных среды.

Файл настроек имеет одинаковое имя для всех пользователей. Для каждого пользователя должна быть создана отдельная директория, чтобы обеспечить для него сохранение собственного файла настроек. Иначе при работе нескольких пользователей файл настроек будет постоянно перезаписываться. С помощью тега путь доступа к файлу настроек может быть привязан к регистрационному имени пользователя.

**Пример структуры директорий централизованного хранения настроек**

Настройки сохраняются в директории "User Settings", к которой обеспечивается общий доступ по сети. Структура подразделов в разделе "UserSettings" показана ниже:

```
UserSettings
      User1
      User2
      User3
```

"User1", "User2" и "User3" - имена пользователей виртуальной среды VM.

В переменной среды путь указывается так: "\\MyServer\UserSettings\%USERNAME%".

В этом примере "MyServer" - доступный компьютер в сети. "%USERNAME%" - тег имени пользователя. Такой тег полезен при смене пользователя, когда изменяется регистрационное имя пользователя. В многопользовательской системе целесообразно сохранять скрипт в разделе автозагрузок (Autostart). При этом при каждой смене пользователя переменная среды вновь будет инициализироваться, и таким образом файл настроек будет соответствовать новому пользователю.

**Необходимые условия**

- Все пользователи имеют доступ к серверу в режиме записи.
- Созданы соответствующие директории для отдельных пользователей.

**Задание переменных среды с использованием скрипта**

Процедура для определения переменных среды с использованием скрипта:

1. Создайте новый скрипт и откройте его для редактирования. Или же Вы можете открыть для редактирования уже имеющийся скрипт.
2. Добавьте следующие строки в скрипт:
   `setx TiaUserSettingsPath \\<Server>\<Settings>\%USERNAME%`
   `setx TiaDefaultProjectPath \\<Server>\<Projects>\%USERNAME%`
   Замените описания "`<Server>\<Settings>`" и "`<Server>\<Projects>`" директориями в сети, которые предназначены для хранения соответственно настроек и проектов.
3. Сохраните скрипт.
4. Для использования скрипта другими пользователями скопируйте его в папку "Autostart" операционной системы.
   Тег "%USERNAME%" заменяется именем пользователя при его регистрации в PG/PC. Таким образом обеспечивается локализация личных проектов и настроек пользователя.

Если Вы хотите использовать раздельные скрипты для инициализации мест хранения настроек и проектов, тогда выполните шаги 1…4 для каждого скрипта отдельно, добавив в каждый соответствующую строку `setx Tia…` (пункт 2).

**Задание переменных среды вручную**

Процедура для определения переменных среды в ручном режиме:

1. Запустите VM, для которой Вы хотите создать шаблон.
2. В Windows откройте диалог для определения переменных среды.
3. Создайте новый системный тег с именем "TiaUserSettingsPath".
4. В качестве значения параметра задайте путь к директории в сети, в которой должны быть сохранены пользовательские настройки. В качестве имени пользователя задайте тег "%USERNAME%".
5. Подтвердите выполненные изменения кнопкой "OK".
6. Создайте другой системный тег с именем "TiaDefaultProjectPath".
7. В качестве значения параметра задайте путь к директории в сети, в которой должны сохраняться пользовательские проекты. Вы можете задать имя пользователя в виде тега "%USERNAME%". Если тег "%USERNAME%" будет пропущен, то все проекты будут сохраняться в одной директории.
8. Подтвердите выполненные изменения кнопкой "OK".

   Тег "%USERNAME%" заменяется именем пользователя при его регистрации в PG/PC. Таким образом обеспечивается локализация личных проектов и настроек пользователя.

**См. также**

Создание нового шаблона VM (страница 27)

Использование сервера лицензий (страница 30)

Инсталляция TIA Portal Cloud Connector в VM (страница 30)

## 3.3 Использование сервера лицензий

**Введение**

Во время инсталляции TIA Portal или TIA Portal Cloud Connector устанавливается также менеджер лицензий Automation License Manager (ALM). Менеджер лицензий потребуется Вам для управления лицензиями.

Вы можете найти дополнительную информацию по использованию менеджера лицензий Automation License Manager и настройкам сервера лицензий в документации по Automation License Manager.

**См. также**

Создание нового шаблона VM (страница 27)

Централизованное сохранение настроек пользователя и проекта (страница 28)

Инсталляция TIA Portal Cloud Connector в VM (страница 30)

## 3.4 Инсталляция TIA Portal Cloud Connector в VM

Вы можете инсталлировать TIA Portal Cloud Connector в VM двумя путями:

- Инсталляция TIA Portal Cloud Connector вместе с TIA Portal
  Для этого необходимо активировать опцию установки "TIA Portal Cloud Connector" в процессе инсталляции TIA Portal.
- Инсталляция TIA Portal Cloud Connector отдельно от TIA Portal
  Для этого необходимо запустить программу установки TIA Portal Cloud Connector на установочном носителе с дистрибутивом TIA Portal. Также Вы можете сделать этот установочный файл доступным для других пользователей, обеспечив общий доступ к сетевому ресурсу.

**Процедура инсталляции TIA Portal Cloud Connector вместе с TIA Portal**

Процедура инсталляции TIA Portal Cloud Connector вместе с TIA Portal:

1. Вставьте установочный носитель с дистрибутивом в соответствующий привод.
   Программа установки запускается автоматически, если не отключен автозапуск Autostart в PG или PC.
2. Если программа установки не активируется автоматически, запустите двойным щелчком файл "Start.exe".
   При этом открывается окно выбора языка интерфейса программы инсталляции ПО.
3. Выберите язык интерфейса программы инсталляции ПО.
4. Для получения информации о программе или о процедуре инсталляции, щелкните соответственно на "Read Notes" или на "Installation Notes".
   При этом открывается окно соответствующей справки.
5. После просмотра информации закройте справку и выполните щелчок на кнопке продолжения "Next".
   При этом открывается диалог для выбора языка интерфейса программы.

6. Выберите соответствующий язык пользовательского интерфейса ПО и выполните щелчок на кнопке продолжения "Next".

   **Примечание**

   Английский язык ("English") всегда устанавливается как основной язык программы.

   При этом открывается диалог для выбора языка пользовательского интерфейса программного обеспечения.

7. Выполните щелчок на кнопке "User-defined" ("Определяется пользователем").
8. Отметьте элемент управления чекбокс "TIA Portal Cloud Connector". При необходимости отметьте также чекбоксы для других программных продуктов, которые необходимо установить.
9. Для создания на рабочем столе ярлыка для TIA Portal отметьте чекбокс "Create desktop shortcut".
10. Для изменения целевой директории для инсталляции программного обеспечения выполните щелчок на кнопке "Browse" ("Просмотр") и выберите новую папку. При этом необходимо учитывать, что общая длина адреса для установленного ПО не должна превышать 89 символов.
11. Выполните щелчок на кнопке продолжения "Next".
    При этом открывается диалоговое окно с информацией об условиях использования ПО.
12. Для продолжения установки необходимо прочесть и квитировать соглашение по использованию ПО, после чего выполните щелчок на кнопке продолжения "Next".
    Если требуется настроить допуск пользователей к программе установки TIA Portal, открывается соответствующий диалог.
13. Для продолжения установки ПО подтвердите выполненные настройки и выполните щелчок на кнопке продолжения "Next".
    При этом открывается окно с обзором опций установки.
14. Проверьте опции установки. Если необходимо выполнить какие-либо изменения, для возврата к соответствующим предыдущим окнам с настройками используйте кнопку возврата - "Back". После всех настроек и корректировок опций процедуры установки ПО с помощью кнопки "Next" перейдите к следующему диалоговому окну запуска процедуры с кнопкой "Install".
15. В открывшемся окне выполните щелчок на кнопке "Install". При этом запускается процесс установки выбранного программного обеспечения.

    **Примечание**

    Если во время инсталляции ПО система не обнаруживает лицензионный ключ, тогда Вы можете воспользоваться опцией передачи лицензии на Ваш PC. Также Вы можете выполнить передачу лицензии позднее с использованием менеджера лицензий Automation License Manager. После завершения процедуры Вы получите сообщение об успешном завершении установки ПО.

16. После инсталляции ПО может потребоваться перезагрузка PC. Для этого активируйте кнопку "Yes, restart my computer now." Затем выполните щелчок на кнопке перезапуска компьютера "Restart".
17. Если перезагрузка PC не произошла, выключите компьютер кнопкой "Exit".

**Процедура инсталляции Cloud Connector отдельно от TIA Portal**

Процедура инсталляции Cloud Connector отдельно от TIA Portal:

1. Вставьте установочный носитель с дистрибутивом в соответствующий привод или укажите адрес доступа к дистрибутиву ПО.
   Вы можете найти установочный файл в разделе "Support" на установочном носителе с дистрибутивом.
2. Двойным щелчком запустите на выполнение установочный файл "TIA Portal Cloud Connector_<Version>.exe". При этом выдается запрос системы UAC Windows.
3. Квитируйте запрос UAC с помощью кнопки "Yes".
   При этом открывается диалоговое окно процедуры инсталляции.
4. Выполните щелчок на кнопке продолжения "Next". После этого отображается окно со списком доступных языков для интерфейса программы инсталляции ПО.
5. Выберите язык интерфейса процедуры инсталляции ПО и выполните щелчок на кнопке продолжения "Next".
   При этом распаковываются необходимый файл дистрибутива и открывается следующее диалоговое окно.
6. Закройте открытые программы и выполните щелчок на кнопке продолжения "Next".
   После этого отображается окно с условиями использования ПО.
7. Подтвердите согласие с условиями использования ПО и выполните щелчок на кнопке продолжения "Next".
   При этом отображаются доступные программы и необходимый объем памяти для инсталляции.
8. Выполните щелчок на кнопке продолжения "Next".
   При этом открывается окно с обзором опций установки.
9. Отметьте чекбокс для применения изменений.
10. Выполните щелчок на кнопке продолжения "Next".
    При этом открывается окно с обзором устанавливаемых программ.
11. Выполните щелчок на кнопке запуска инсталляции "Install".
    При этом запускается процедура установки ПО.
12. После инсталляции ПО может потребоваться перезагрузка PC. Для этого активируйте кнопку "Yes, restart my computer now." Затем выполните щелчок на кнопке завершения "Finish".

**См. также**

Создание нового шаблона VM (страница 27)

Централизованное сохранение настроек пользователя и проекта (страница 28)

Использование сервера лицензий (страница 30)

# Использование виртуальной машины (VM) 4

## 4.1 Инсталляция TIA Portal Cloud Connector на PG/PC

**Примечание**

Необходимо учитывать, что:

- для TIA Portal Cloud Connector необходимо действующая лицензия;
- должны быть выполнены настройки файрвола Windows: необходимым условием для входящего соединения является внесение порта, используемого для TIA Portal Cloud Connector, в категорию разрешенных для удаленного соединения - на вкладке "Exceptions" ("Исключения") для сервиса удаленных соединений "Siemens SCP Remote Connection"; стандартное значение здесь: "Any" ("без исключений").

**Процедура**

Для инсталляции TIA Portal Cloud Connector выполните следующие действия:

1. Вставьте установочный носитель с дистрибутивом в соответствующий привод или укажите адрес доступа к дистрибутиву ПО. Вы можете найти установочный файл в разделе "Support" на установочном носителе с дистрибутивом.
2. Двойным щелчком запустите на выполнение установочный файл "TIA Portal Cloud Connector_<Version>.exe". При этом отображается окно с запросом UAC Windows.
3. Квитируйте запрос системы UAC с помощью кнопки "Yes".
   При этом открывается диалоговое окно процедуры инсталляции.
4. Выполните щелчок на кнопке продолжения "Next". При этом открывается окно выбора языка интерфейса для программы инсталляции.
5. Выберите язык интерфейса программы инсталляции и выполните щелчок на кнопке "Next". При этом распаковывается дистрибутив и открывается следующее окно.
6. Закройте открытые программы и выполните щелчок на кнопке продолжения "Next". После этого отображается окно с условиями использования ПО.
7. Подтвердите согласие с условиями использования ПО и выполните щелчок на кнопке продолжения "Next". При этом отображаются доступные программы и необходимый объем памяти для инсталляции.
8. Выполните щелчок на кнопке "Next". При этом открывается окно опций установки.
9. Отметьте чекбокс для применения выполненных изменений.
10. Выполните щелчок на кнопке "Next" - отображаются устанавливаемые программы.
11. Выполните щелчок на кнопке "Install" - запускается процедура установки программ.
12. После инсталляции может потребоваться перезагрузка PC. Для этого активируйте кнопку "Yes, restart my computer now." Затем выполните щелчок на кнопке "Finish".

**См. также**

Конфигурирование ПО TIA Portal Cloud Connector на PG/PC (страница 34)

Конфигурирование ПО TIA Portal Cloud Connector в VM (страница 36)

Интерактивное подключение посредством TIA Portal Cloud Connector (страница 48)

Использование виртуальной машины VM в автономном режиме (страница 49)

## 4.2 Конфигурирование ПО TIA Portal Cloud Connector на PG/PC

**Примечание**

Для подключения PG/PC к VM необходимо определить коммуникационный протокол. Для обеспечения безопасности, начиная с версии операционной системы Windows 8.1, всегда используйте протокол HTTPS.

**Конфигурирование TCP-соединения**

Для конфигурирования TCP-соединения для PG/PC выполните следующие действия:

1. Щелкните правой кнопкой манипулятора "мышь" на ярлыке TIA Portal Cloud Connector в информационной области панели задач и выберите в контекстном меню опцию конфигурирования "Configuration".
2. В открывшемся окне TIA Portal Cloud Connector на вкладке настроек "Settings" выберите язык пользовательского интерфейса TIA Portal Cloud Connector.
3. На вкладке общих параметров "General" выберите тип устройства в сети.

   При необходимости измените тип на "User device" ("устройство пользователя").
4. Перейдите на вкладку параметров протокола "Protocol".
5. Отметьте чекбокс "TCP endpoint" ("точка TCP-соединения").
6. Задайте порт, через который должны осуществляться коммуникации.

   Порт должен соответствовать настройкам одного из удаленных устройств.
7. Откройте вновь вкладку общих параметров "General".
8. Выполните щелчок на кнопке активации коммуникаций "Enable communication" в области "Cloud Connector Communication".

**Конфигурирование HTTPS-соединения**

Для конфигурирования HTTPS-соединения для PG/PC выполните следующие действия:

1. Откройте контекстное меню на ярлыке TIA Portal Cloud Connector в информационной области панели задач и выберите команду конфигурирования "Configuration".

   При этом откроется окно TIA Portal Cloud Connector.
2. Откройте вкладку настроек "Settings" и измените, если требуется, язык пользовательского интерфейса TIA Portal Cloud Connector.
3. Перейдите на вкладку общих параметров "General" и выберите тип устройства в сети.

   При необходимости измените тип устройства на "пользовательское" - "User device".
4. Перейдите на вкладку параметров протокола "Protocol".
5. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения").
6. Создайте новый сертификат для шифрования данных или выберите имеющийся сертификат из хранилища сертификатов Windows.

   См. также:

   Создание сертификата для шифрования данных (страница 38)

   Выбор сертификата для шифрования данных (страница 41)

7. Если отсутствует сертификат для аутентификации пользователя на пользовательском устройстве, создайте его на удаленном устройстве и скопируйте его на свое устройство.

   См. также: Создание сертификата для аутентификации пользователя (стр. 41).

8. Перейдите на вкладку настроек "Settings".
9. Импортируйте новый сертификат для аутентификации пользователя или добавьте существующий сертификат из хранилища сертификатов Windows в список доверенных сертификатов.

   См. также:

   Импорт сертификата для аутентификации пользователя (страница 44)

   Добавление сертификата для аутентификации пользователя (страница 45)

10. Откройте вновь вкладку общих параметров "General".
11. Для активации коммуникаций выполните щелчок на кнопке "Enable communication" в области "Cloud Connector Communication".

**Результат**

Ваша станция PG/PC готова для установления связи с VM.

**См. также**

Инсталляция TIA Portal Cloud Connector на PG/PC (страница 33)

Конфигурирование ПО TIA Portal Cloud Connector в VM (страница 36)

Интерактивное подключение посредством TIA Portal Cloud Connector (страница 48)

Использование виртуальной машины VM в автономном режиме (страница 49)

## 4.3 Конфигурирование ПО TIA Portal Cloud Connector в VM

**Примечание**

Необходимо выбрать протокол для установления соединения между PG/PC и VM. Для обеспечения безопасности, начиная с Windows 8.1, Вы всегда должны использовать протокол HTTPS. Необходимо также выполнить идентификацию коммуникационного партнера перед установкой коммуникационного соединения.

**Конфигурирование TCP-соединения**

Для конфигурирования TCP-соединения в VM выполните следующие действия:

1. Установите подключение к удаленному рабочему столу "Remote Desktop" VM.
2. Щелкните правой кнопкой манипулятора "мышь" на ярлыке TIA Portal Cloud Connector в информационной области панели задач и выберите в контекстном меню опцию конфигурирования "Configuration".
3. В открывшемся окне TIA Portal Cloud Connector на вкладке настроек "Settings" выберите язык пользовательского интерфейса TIA Portal Cloud Connector.
4. На вкладке общих параметров "General" выберите тип устройства в сети. При необходимости измените тип на "Remote device" ("удаленное устройство").
5. Откройте вкладку параметров протокола "Protocol".
6. В области информации о коммуникационном протоколе ("Communication protocol") активируйте опцию настройки TCP "TCP Settings".
7. Введите IP-адрес пользовательского устройства или выберите автоматическое назначение IP-адреса - "Automatic configuration".
8. Задайте порт, через который должны осуществляться коммуникации. Порт должен соответствовать порту, указанному на пользовательском устройстве.
9. Откройте вновь вкладку общих параметров "General".
10. Выполните щелчок на кнопке активации соединений "Enable communication" в области "Cloud Connector Communication".

**Конфигурирование HTTPS-соединения**

Для конфигурирования HTTPS-соединения для VM выполните следующие действия:

1. Установите подключение к удаленному рабочему столу "Remote Desktop" к VM.
2. Щелкните правой кнопкой манипулятора "мышь" на ярлыке TIA Portal Cloud Connector в информационной области панели задач и выберите в контекстном меню опцию конфигурирования "Configuration".
   При этом откроется окно параметризации TIA Portal Cloud Connector.
3. Откройте вкладку настроек "Settings" и измените, если требуется, язык пользовательского интерфейса TIA Portal Cloud Connector.
4. Откройте вкладку общих параметров "General" и выберите тип устройства в сети. При необходимости измените тип на "Remote device" ("удаленное устройство").
5. Откройте вкладку параметров протокола "Protocol".
6. В области информации о коммуникационном протоколе "Communication protocol" активируйте опцию HTTPS-настроек - выделите чекбокс "HTTPS settings".
7. Введите IP-адрес пользовательского устройства или выберите автоматическое назначение IP-адреса - "Automatic configuration".

8. Импортируйте новый сертификат для шифрования данных, установленный на пользовательском устройстве, или выберите существующий сертификат из хранилища сертификатов Windows.

   См. также:

   Импорт сертификата для шифрования данных (страница 40)

   Выбор сертификата для шифрования данных (страница 41)

9. Перейдите на вкладку настроек "Settings".
10. Создайте новый сертификат для аутентификации пользователя или выберите существующий сертификат из хранилища сертификатов Windows.

    См. также:

    Создание сертификата для аутентификации пользователя (страница 42)

    Выбор сертификата для аутентификации пользователя (страница 46)

11. Откройте вновь вкладку общих параметров "General".
12. Выполните щелчок на кнопке "Enable communication" в области "Cloud Connector Communication".

**Результат**

TIA Portal Cloud Connector готов для коммуникаций. После активации обоих коммуникационных партнеров обеспечивается доступ пользовательского устройства к SIMATIC-устройствам (PLC / HMI) в локальной сети.

**См. также**

Инсталляция TIA Portal Cloud Connector на PG/PC (страница 33)

Конфигурирование ПО TIA Portal Cloud Connector на PG/PC (страница 34)

Интерактивное подключение посредством TIA Portal Cloud Connector (страница 48)

Использование виртуальной машины VM в автономном режиме (страница 49)

# 4.4 Использование сертификатов (только для HTTPS)

## 4.4.1 Создание сертификата для шифрования данных

Начиная с Windows 8.1, Вы можете использовать HTTPS-соединение для коммуникаций. Для обеспечения безопасности путем шифрования данных требуется соответствующий сертификат, который должен быть в наличии на пользовательском устройстве, с которым будет связываться удаленное устройство.

**Процедура**

Для создания сертификата для шифрования данных выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на пользовательском устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню пункт "Configuration (user device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения").
   При этом становятся доступны кнопка создания "Create" и кнопка выбора "Select".
5. Выполните щелчок на кнопке "Create" ("Создать").
   При этом откроется диалоговое окно опции сохранения "Save as".
6. Выберите в открывшемся окне место сохранения сертификата и задайте также имя для сертификата.
7. Выполните щелчок на кнопке "Save" ("Сохранить").

**Результат**

Сертификат для шифрования данных создан и может быть использован для точки HTTPS-соединения на пользовательском устройстве. Кроме того он сохраняется в заданном пользователем хранилище в виде файла с расширением ".cer"; из этого хранилища этот файл может быть скопирован на удаленное устройство. Сертификат также добавляется в хранилище сертификатов Windows.

**См. также**

Использование сертификатов (страница 21)

Экспорт сертификата для шифрования данных (страница 39)

Импорт сертификата для шифрования данных (страница 40)

Выбор сертификата для шифрования данных (страница 41)

### 4.4.2 Экспорт сертификата для шифрования данных

Вы можете экспортировать используемый сертификат для шифрования данных в любое время.

**Необходимые условия**

Сертификат для шифрования данных должен быть создан на устройстве пользователя и при этом должен отображаться в окне параметров для точки HTTPS-соединения пользовательского устройства.

**Процедура**

Для экспорта сертификата для шифрования данных выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на пользовательском устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню пункт "Configuration (user device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения").
   При этом становятся доступны кнопки "Create", "Select" и "Export".
5. Выполните щелчок на кнопке функции экспорта "Export".
   При этом откроется диалоговое окно опций сохранения "Save as".
6. Выберите место сохранения сертификата и задайте имя сертификата.
7. Выполните щелчок на кнопке "Save" ("Сохранить").

**Результат**

Используемый сертификат для шифрования данных сохраняется в заданном пользователем хранилище в виде файла с расширением ".cer".

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для шифрования данных (страница 38)

Импорт сертификата для шифрования данных (страница 40)

Выбор сертификата для шифрования данных (страница 41)

### 4.4.3 Импорт сертификата для шифрования данных

Для установления HTTPS-соединения между пользовательским устройством и удаленным устройством сертификат для шифрования данных, имеющийся на пользовательском устройстве, необходимо импортировать для TIA Portal Cloud Connector на удаленном устройстве.

**Необходимые условия**

- Сертификат для шифрования данных имеется на пользовательском устройстве.
- Сертификат для шифрования данных был скопирован на удаленное устройство.

**Процедура**

Для импорта сертификата для шифрования данных для TIA Portal Cloud Connector удаленного устройства выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на пользовательском устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню пункт "Configuration (user device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения").
   При этом становятся доступны кнопка импорта "Import" и кнопка выбора "Select".
5. Выполните щелчок на кнопке функции импорта "Import".
   При этом откроется окно "Open" для навигации по структуре папок.
6. Выберите соответствующий файл сертификата в навигационном окне. Файлы сертификатов имеют расширение ".cer".
7. Выполните щелчок на кнопке активации выбора "Open".

**Результат**

Сертификат для шифрования данных импортирован, и он в любой момент может быть использован для коммуникаций. Сертификат также добавляется в хранилище сертификатов Windows.

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для шифрования данных (страница 38)

Экспорт сертификата для шифрования данных (страница 39)

Выбор сертификата для шифрования данных (страница 41)

### 4.4.4 Выбор сертификата для шифрования данных

Вы можете выбрать сертификат для шифрования данных из хранилища сертификатов Windows. Это может быть сделано на пользовательском устройстве так же как на удаленном устройстве.

**Необходимые условия**

Сертификат для шифрования данных должен быть создан заранее (для пользовательского устройства) или импортирован (на удаленное устройство) и доступен в хранилище сертификатов Windows.

**Процедура**

Для выбора и последующего использования имеющегося сертификата для шифрования данных из хранилища сертификатов Windows выполните следующие действия:

1. Откройте TIA Portal Cloud Connector щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню для пользовательского устройства команду "Configuration (user device)" или для удаленного устройства - команду "Configuration (remote device)".
   При этом откроется окно для настройки конфигурации TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Для пользовательского устройства выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения"), или для удаленного устройства выделите чекбокс "HTTPS settings" ("настройки HTTPS").
   При этом становится доступна кнопка выбора "Select".
5. Выполните щелчок на кнопке функции выбора "Select".
   При этом открывается диалоговое окно опций безопасности "Windows Security", в котором отображаются доступные сертификаты.
6. Выберите соответствующий сертификат. При необходимости Вы можете вывести на экран дополнительные параметры сертификата.
7. Выполните щелчок на кнопке "OK".

**Результат**

Выбранный сертификат для шифрования данных теперь активирован для коммуникаций с использованием протокола HTTPS. Для обеспечения коммуникаций один и тот же сертификат должен быть установлен на пользовательском устройстве и удаленном устройстве.

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для шифрования данных (страница 38)

Экспорт сертификата для шифрования данных (страница 39)

Импорт сертификата для шифрования данных (страница 40)

### 4.4.5 Создание сертификата для аутентификации пользователя

Начиная с Windows 8.1, Вы можете использовать HTTPS-соединение для коммуникаций. Для обеспечения безопасности потребуется сертификат для аутентификации пользователя; он создается на удаленном устройстве для использования с пользовательского устройства.

**Процедура**

Для создания сертификата для аутентификации пользователя выполните следующие действия:

1. Откройте TIA Portal Cloud Connector щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows на удаленном устройстве.
2. Выберите в контекстном меню опцию "Configuration (remote device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Активируйте элемент управления чекбокс "HTTPS settings".
   Область для аутентификации пользователя становится активной на вкладке настроек "Settings".
5. Перейдите на вкладку настроек "Settings".
6. Выполните щелчок на кнопке "Create" ("Создать") в области идентификации пользователя "User authentication".
   При этом открывается диалог "TIA Portal Cloud Connector - User authentication".
7. Задайте имя для нового сертификата в поле "Certificate name".
8. Выполните щелчок на кнопке "Browse" ("Просмотр").
   При этом открывается диалоговое окно опций сохранения "Save as".
9. Выберите место сохранения и введите имя файла для сертификата.
10. Выполните щелчок на кнопке "Save" ("Сохранить").
11. Выберите дату, с которой сертификат должен быть действительным.
12. Выберите дату, до которой сертификат должен быть действительным.
13. Выполните щелчок на кнопке "OK".

**Результат**

Сертификат для аутентификации пользователя создан и может использоваться на удаленном устройстве. Кроме того он сохраняется в заданном пользователем хранилище в виде файла с расширением ".cer"; из этого хранилища этот файл может быть скопирован на пользовательское устройство. Сертификат также добавляется в хранилище сертификатов Windows.

**См. также**

Использование сертификатов (страница 21)

Экспорт сертификата для аутентификации пользователя (страница 43)

Импорт сертификата для аутентификации пользователя (страница 44)

Добавление сертификата для аутентификации пользователя (страница 45)

Выбор сертификата для аутентификации пользователя (страница 46)

Удаление сертификата для аутентификации пользователя (страница 47)

### 4.4.6 Экспорт сертификата для аутентификации пользователя

Для использования сертификата для аутентификации пользователя на удаленном устройстве необходимо экспортировать этот сертификат на пользовательское устройство. Вы можете экспортировать сертификат для аутентификации в любое время.

**Необходимые условия**

Сертификат для аутентификации пользователя должен быть создан на удаленном устройстве заранее; он отображается на вкладке настроек "Settings" в области "User authentication".

**Процедура**

Для экспорта сертификата для аутентификации пользователя выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на удаленном устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню опцию "Configuration (remote device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Активируйте элемент управления чекбокс "HTTPS settings".
   Область для аутентификации пользователя становится активной на вкладке настроек "Settings".
5. Перейдите на вкладку настроек "Settings".
6. Выполните щелчок на кнопке функции экспорта "Export" в области идентификации пользователя "User authentication".
   При этом открывается диалоговое окно опций сохранения "Save as".
7. Выберите место сохранения и задайте имя для сертификата.
8. Выполните щелчок на кнопке "Save" ("Сохранить").

**Результат**

Используемый сертификат для аутентификации пользователя сохраняется в заданном пользователем хранилище в виде файла с расширением ".cer".

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для аутентификации пользователя (страница 42)

Импорт сертификата для аутентификации пользователя (страница 44)

Добавление сертификата для аутентификации пользователя (страница 45)

Выбор сертификата для аутентификации пользователя (страница 46)

Удаление сертификата для аутентификации пользователя (страница 47).

### 4.4.7 Импорт сертификата для аутентификации пользователя

Для установления HTTPS-соединения между пользовательским устройством и удаленным устройством необходимо импортировать сертификат для аутентификации пользователя, созданный на удаленном устройстве, для TIA Portal Cloud Connector пользовательского устройства.

**Необходимые условия**

- Сертификат для аутентификации пользователя был создан на удаленном устройстве.
- Сертификат для аутентификации пользователя был скопирован на локальный привод удаленного устройства.

**Процедура**

Для импорта сертификата для аутентификации пользователя выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на пользовательском устройстве с использованием контекстного меню для TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в меню опцию конфигурирования "Configuration (user device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения").
   Область для аутентификации пользователя становится активной на вкладке настроек "Settings".
5. Перейдите на вкладку настроек "Settings".
6. Выполните щелчок на кнопке функции импорта "Import" в области идентификации пользователя "User authentication".
   При этом откроется окно "Open" для навигации по структуре папок.
7. Выберите соответствующий файл сертификата в окне навигации по структуре папок. Файлы сертификатов имеют расширение ".cer".
8. Выполните щелчок на кнопке активации выбора "Open".

**Результат**

Сертификат для аутентификации пользователя импортирован и добавлен в список доверенных сертификатов. Вы можете использовать этот список для определения удаленных устройств, с которыми пользовательское устройство будет устанавливать коммуникационную связь. Такие устройства должны иметь такие же сертификаты для аутентификации пользователя, что и пользовательское устройство.

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для аутентификации пользователя (страница 42)

Экспорт сертификата для аутентификации пользователя (страница 43)

Добавление сертификата для аутентификации пользователя (страница 45)

Выбор сертификата для аутентификации пользователя (страница 46)

Удаление сертификата для аутентификации пользователя (страница 47)

### 4.4.8 Добавление сертификата для аутентификации пользователя

Вместо описанного выше способа импорта сертификата Вы также можете добавить сертификат в список доверенных сертификатов непосредственно из хранилища сертификатов Windows.

**Необходимые условия**

Соответствующий сертификат для аутентификации пользователя доступен в хранилище сертификатов Windows.

**Процедура**

Для добавления сертификата для аутентификации пользователя из хранилища сертификатов Windows выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на удаленном устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню пункт "Configuration (user device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения").
   Область для аутентификации пользователя становится активной на вкладке настроек "Settings".
5. Перейдите на вкладку настроек "Settings".
6. Выполните щелчок на кнопке для добавления "Add" в области идентификации пользователя "User authentication".
   При этом откроется окно "Select certificate", в коотором отображаются доступные сертификаты.
7. Выберите соответствующий сертификат. При необходимости Вы можете открыть для просмотра параметры сертификата.
8. Выполните щелчок на кнопке квитирования "OK".

**Результат**

Сертификат из хранилища сертификатов Windows добавлен в список доверенных сертификатов. Вы можете использовать этот список для определения удаленных устройств, с которыми пользовательское устройство будет устанавливать коммуникационную связь. Такие устройства должны иметь такие же сертификаты для аутентификации пользователя, что и пользовательское устройство.

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для аутентификации пользователя (страница 42)

Экспорт сертификата для аутентификации пользователя (страница 43)

Импорт сертификата для аутентификации пользователя (страница 44)

Выбор сертификата для аутентификации пользователя (страница 46)

Удаление сертификата для аутентификации пользователя (страница 47)

### 4.4.9 Выбор сертификата для аутентификации пользователя

Вместо создания нового сертификата на удаленном устройстве Вы можете выбрать имеющийся сертификат из хранилища сертификатов Windows.

**Необходимые условия**

Сертификат для аутентификации пользователя был создан заранее и доступен в хранилище сертификатов Windows.

**Процедура**

Для выбора сертификата для аутентификации пользователя из хранилища сертификатов Windows выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на удаленном устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню опцию "Configuration (remote device)".
   При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Активируйте элемент управления чекбокс "HTTPS settings".
   Область для аутентификации пользователя становится активной на вкладке настроек "Settings".
5. Перейдите на вкладку настроек "Settings".
6. Выполните щелчок на кнопке функции выбора "Select" в области идентификации пользователя "User authentication".
   При этом открывается окно "Windows Security", в котором отображаются доступные сертификаты.
7. Выберите соответствующий сертификат. При необходимости Вы можете вывести на экран дополнительные параметры сертификата.
8. Выполните щелчок на кнопке "OK".

**Результат**

Сертификат для аутентификации пользователя теперь доступен на удаленном устройстве. При необходимости этот сертификат может быть экспортирован для обеспечения обмена с пользовательским устройством.

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для аутентификации пользователя (страница 42)

Экспорт сертификата для аутентификации пользователя (страница 43)

Импорт сертификата для аутентификации пользователя (страница 44)

Добавление сертификата для аутентификации пользователя (страница 45)

Удаление сертификата для аутентификации пользователя (страница 47)

### 4.4.10 Удаление сертификата для аутентификации пользователя

Вы можете удалить сертификат для аутентификации пользователя из списка доверенных сертификатов на пользовательском устройстве в любое время.

**Процедура**

Для удаления сертификата для аутентификации пользователя из списка доверенных сертификатов выполните следующие действия:

1. Откройте TIA Portal Cloud Connector на пользовательском устройстве щелчком правой кнопки манипулятора "мышь" на значке TIA Portal Cloud Connector в информационной области панели задач интерфейса Windows.
2. Выберите в контекстном меню опцию конфигурации "Configuration (user device)". При этом откроется окно для конфигурирования TIA Portal Cloud Connector.
3. Перейдите на вкладку параметров протокола "Protocol".
4. Выделите чекбокс "HTTPS endpoint" ("точка HTTPS-соединения"). Область для аутентификации пользователя становится активной на вкладке настроек "Settings".
5. Перейдите на вкладку настроек "Settings".
6. Выберите сертификат, который необходимо удалить из списка доверенных сертификатов.
7. Выполните щелчок на кнопке функции удаления "Remove" в области идентификации пользователя "User authentication".

**Результат**

Сертификат для аутентификации пользователя на пользовательском устройстве удаляется из списка доверенных сертификатов. Коммуникационная связь с удаленным устройством, для которого использовался этот сертификат, с этим сертификатом больше недоступна.

**См. также**

Использование сертификатов (страница 21)

Создание сертификата для аутентификации пользователя (страница 42)

Экспорт сертификата для аутентификации пользователя (страница 43)

Импорт сертификата для аутентификации пользователя (страница 44)

Добавление сертификата для аутентификации пользователя (страница 45)

Выбор сертификата для аутентификации пользователя (страница 46)

# 4.5 Интерактивное подключение посредством TIA Portal Cloud Connector

### Введение

Если Вы используете TIA Portal Cloud Connector для подключения к оборудованию, то работа с использованием TIA Portal не отличается от использования обычного интерактивного подключения к этому оборудованию. Как только Вы активируете коммуникационный туннель, Вы получаете возможность компилировать, загружать и выполнять мониторинг Ваших данных как при обычном интерактивном подключении.

Для получения дополнительной информации по установлению и использованию интерактивного подключения обратитесь к справочной системе для TIA Portal.

### Обзор возможных значений графического индикатора состояния подключения

При применении интерактивного подключения посредством TIA Portal Cloud Connector Вы можете использовать графический индикатор состояния подключения в информационной области панели задач интерфейса Windows для наблюдения за состоянием этого подключения.

В следующей ниже таблице представлено отображение и значения для графического индикатора состояния подключения:

| Символ | Значение |
|---|---|
|  | Коммуникационная связь не установлена |
|  | Коммуникационная связь установлена, но нет обмена данными между TIA Portal и устройствами SIMATIC. |
|  | Коммуникационная связь установлена, и идет обмен данными между TIA Portal и устройствами SIMATIC. |
|  | Обмен данными между TIA Portal и устройствами SIMATIC прерван. Дисплей состояния (status display) информирует пользователя дополнительной информацией о возникшей проблеме. |

### Дисплей состояния (status display)

В информационной области панели задач интерфейса Windows отображается дисплей состояния (status display) удаленного и пользовательского устройства. Этот дисплей позволяет открыть окно для удаленного ("TIA Portal Cloud Connector - Remote device") или пользовательского ("TIA Portal Cloud Connector - User device") устройств. Это окно отображает предупреждения (**warning**) и сообщения об ошибках (**error**) в TIA Portal Cloud Connector. Кроме того оно показывает длительность TCP- / HTTPS-соединений.

Вы можете скрыть дисплей состояния в любое время.

### См. также

Инсталляция TIA Portal Cloud Connector на PG/PC (страница 33)

Конфигурирование ПО TIA Portal Cloud Connector на PG/PC (страница 34)

Конфигурирование ПО TIA Portal Cloud Connector в VM (страница 36)

Использование виртуальной машины VM в автономном режиме (страница 49)

## 4.6 Использование VM в автономном режиме

Виртуальная машина поддерживает также автономный режим. Для этого VM копируется с удаленного устройства на PG/PC. После этого VM запускается на PG/PC и TIA Portal используется с оборудованием в сети или с подключенным к PG/PC.

При этом для использования VM имеются следующие варианты:

- Оборудование подключено к PG/PC по Ethernet и размещено в той же сети
- Оборудование подключено к PG/PC по Ethernet или Profibus и включено в иную сеть

При этом могут быть использованы следующие сценарии:

- Если оборудование подключено непосредственно к PG/PC по Ethernet или USB, то может быть установлено соединение типа "мост" ("Bridged").
  При таком типе соединения TIA Portal Cloud Connector должен быть отключен в VM.
- Если оборудование подключено по интерфейсу USB или через сетевую карту, то может быть использована опция "Host-only" ("только станция"). При этом TIA Portal Cloud Connector активирован в VM, и может использоваться интерфейс PROFIBUS.

После локального использования VM опять можно скопировать на удаленное устройство.

**Необходимые условия**

- На PG/PC установлено ПО для использования с VM, например, VMware Workstation.
- Менеджер лицензий Automation License Manager установлен на PG/PC.

**Передача VM с удаленного устройства на PG/PC**

Для использования VM в автономном режиме выполните следующие действия:

1. Скопируйте VM с удаленного устройства на PG/PC. Эта процедура зависит от используемой VM. При необходимости обратитесь к справочной системе VM.
2. Откройте менеджер лицензий Automation License Manager и перешлите соответствующие лицензии для ПО SIMATIC в TIA Portal на локальный привод.
3. Скопируйте соответствующие данные проекта с сервера на Ваш локальный привод.
4. Запустите VM и сконфигурируйте параметры сети. Учитывайте все рекомендации.

**Передача VM с PG/PC на удаленное устройство**

Для обратной передачи VM на удаленное устройство выполните следующие действия:

- Скопируйте VM с Вашего локального PG/PC на удаленное устройство. Эта процедура зависит от используемой виртуальной машины. Для получения дополнительной информации обратитесь к справочной системе VM.
- Откройте менеджер лицензий Automation License Manager и перешлите соответствующие лицензии с Вашего локального PG/PC на ALM Server.
- Скопируйте соответствующие данные проекта с Вашего PG/PC на сервер.

**См. также**

Инсталляция TIA Portal Cloud Connector на PG/PC (страница 33)

Конфигурирование ПО TIA Portal Cloud Connector на PG/PC (страница 34)

Конфигурирование ПО TIA Portal Cloud Connector в VM (страница 36)

Интерактивное подключение посредством TIA Portal Cloud Connector (страница 48)

# Предметный указатель

## У



## Ц



## Э