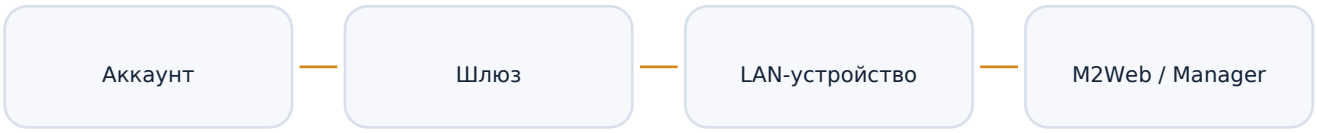
PLCLink

Руководство пользователя

Регистрация, шлюзы Link G2, доступ к оборудованию и решение типовых проблем.



Содержание соответствует опубликованным статьям справки PLCLink. Актуальная версия доступна на cloud.plclink.ru/help/.

Содержание

Основы PLCLink 3

Связь 11

M2Web 13

PLCLink Manager 16

Сессии 21

Шлюзы 22

Тарифы и баланс 32

Телеметрия 36

Протоколы 39

PLCLink Mobile 42

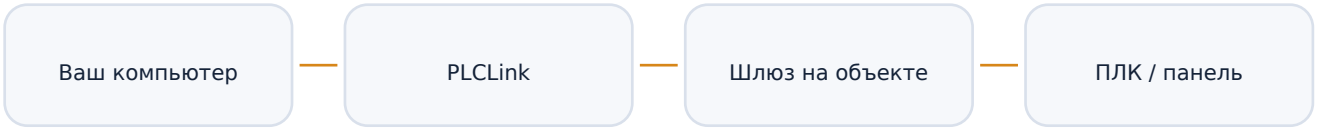
Безопасность 43

Диагностика 47

FAQ 50

Нажмите на раздел в содержании или используйте закладки PDF. Ссылки под заголовками ведут к актуальным статьям в справке.

Основы PLCLink



Что такое PLCLink

Открыть статью в справке

PLCLink - это сервис управляемого инженерного доступа к оборудованию на объекте. На объект устанавливается шлюз PLCLink, он сам подключается к серверу, а инженер получает доступ к устройствам за шлюзом через кабинет, M2Web или PLCLink Manager.

Что сделать

1. Установите шлюз на объекте.

2. Добавьте шлюз в кабинет по Gateway ID и activation code.

3. Обновите список LAN-устройств или добавьте устройство вручную.

4. Откройте web-интерфейс через M2Web или инженерную сессию через PLCLink Manager.

Если не получилось

Если непонятно, с чего начать, передайте в поддержку задачу объекта: какие устройства есть, какие IP-адреса известны и какой доступ нужен инженеру.

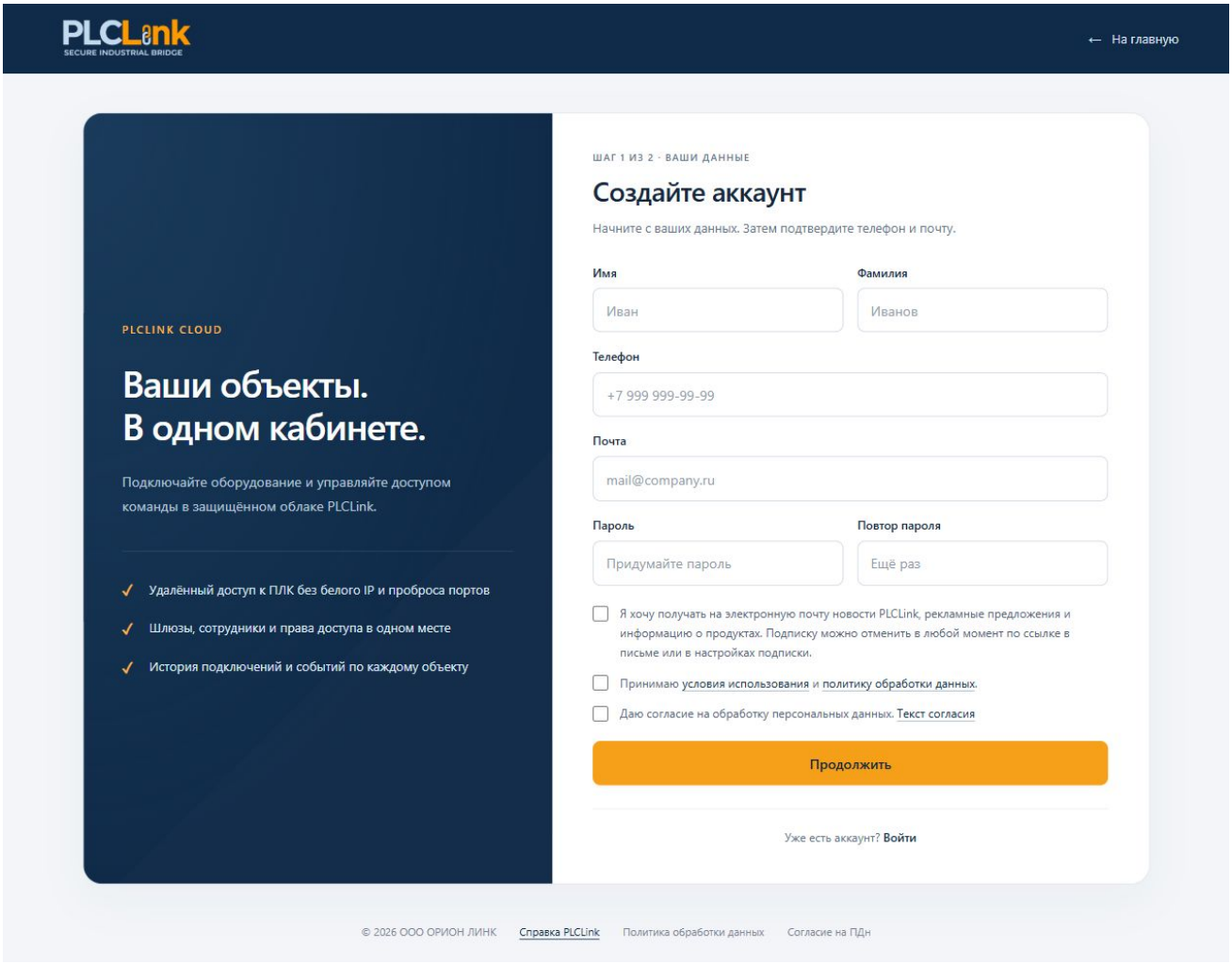
Регистрация: почта и телефон

Открыть статью в справке

Создайте личный аккаунт, чтобы войти в кабинет PLCLink и подключить оборудование своей компании. Подготовьте доступ к почте и телефону: они понадобятся для подтверждения контактов и восстановления доступа.

1. Откройте регистрацию

На странице входа нажмите «Регистрация». Заполняйте форму своими данными: имя и фамилия будут видны коллегам в команде. Для общей работы каждому сотруднику лучше использовать собственный аккаунт и приглашение в компанию.



Первый шаг регистрации PLCLink: личные данные, контакты, пароль и согласия.

2. Укажите контакты и пароль

Введите телефон и email без опечаток. Убедитесь, что можете принять сообщение на этот номер и открыть почту. Укажите пароль и повторите его в соседнем поле. Если форма показывает требования к паролю или ошибку в поле, исправьте её перед продолжением.

Ознакомьтесь с условиями и обязательными согласиями внизу формы. Согласие на новости и предложения — отдельный необязательный пункт: выбирайте его по своему желанию. Нажмите «Продолжить» и следуйте следующему шагу формы.

3. Завершите подтверждение контактов

Используйте ссылку или код, которые предлагает текущий экран подтверждения. Открывайте письмо, отправленное для вашей последней попытки. Не пересылайте коды коллегам и не публикуйте их в обращении поддержки.

Если письмо не пришло, проверьте правильность адреса, папки «Спам» и «Рассылки». При повторной отправке дождитесь интервала, указанного в интерфейсе. Для телефона проверьте номер и доступность приёма сообщений. Не создавайте несколько аккаунтов подряд, чтобы обойти задержку: сначала завершите начатую регистрацию.

4. Проверьте компанию в кабинете

После завершения регистрации откройте кабинет и посмотрите выбранную компанию в левой панели. Если вас пригласили в существующую компанию, завершите принятие приглашения и переключитесь на неё. Пустой список в собственной компании не означает, что шлюзы приглашавшей организации удалены.

Если подключаете собственный новый объект, переходите к статье «Как добавить шлюз в кабинет». Если должны работать с чужим объектом, попросите владельца пригласить вас и назначить нужные права; activation code чужого шлюза для этого не требуется.

Если не получилось

Если код не приходит после повторной отправки, сообщите поддержке время попытки и текст ошибки. Сам код и пароль не отправляйте.

Несколько компаний: переключение и данные

Открыть статью в справке

Один пользователь может состоять в нескольких компаниях. Выбранная компания определяет, какие шлюзы, устройства, команда, счета и сессии видны в кабинете. Права проверяются отдельно в каждой компании.

Что сделать

1. Откройте переключатель компании в кабинете.

2. Выберите нужную организацию.

3. Убедитесь, что название компании и список шлюзов изменились.

4. Перед добавлением шлюза или пополнением баланса снова проверьте выбранную компанию.

Если не получилось

Если шлюз не виден, передайте поддержке название выбранной компании и Gateway ID без кода активации.

Из чего состоит PLCLink

Открыть статью в справке

PLCLink состоит из облачного кабинета, выпущенного заводом шлюза Link G2, транспортного сервера, PLCLink Manager для инженерных сессий, M2Web для веб-интерфейсов оборудования и отдельного мобильного PWA-кабинета.

Что сделать

1. PLCLink Cloud хранит учетные записи, шлюзы, устройства, права, тарифы и журнал.

2. Шлюз держит исходящее соединение с транспортом и открывает доступ к LAN-устройствам.

3. PLCLink Manager нужен для инженерных программ и промышленных протоколов.

4. M2Web открывает web-интерфейсы устройств прямо из браузера.

Если не получилось

Если нужно понять, какой компонент отвечает за проблему, укажите, где именно ошибка: кабинет, M2Web, Manager, шлюз или LAN-устройство.

Как пригласить коллегу

Открыть статью в справке

Владелец или сотрудник с правом управления командой приглашает коллегу по почте. На Free доступен только владелец; на Стандарте — пять мест вместе с владельцем; на Pro тарифного лимита мест нет. Действующее неподтверждённое приглашение тоже занимает место.

Что сделать

1. Выберите компанию, откройте «Команда» и создайте приглашение.

2. Укажите почту коллеги и разрешённую роль.

3. Коллега открывает ссылку из письма и входит именно с указанной почтой. Если аккаунта нет, нужно зарегистрироваться и подтвердить контакты, затем снова открыть ссылку приглашения.

4. После принятия коллега выбирает приглашавшую компанию в кабинете.

5. Проверьте статус участника и доступные ему шлюзы. Если срок приглашения истёк, отправьте новое.

Если не получилось

Укажите компанию, почту приглашённого и статус приглашения; не отправляйте пароли.

Быстрый старт: первая сессия

Открыть статью в справке

Эта инструкция ведёт от нового шлюза до первого ответа ПЛК. Для начала достаточно одного устройства. После проверки вы сможете добавить остальные ПЛК и панели по той же схеме.

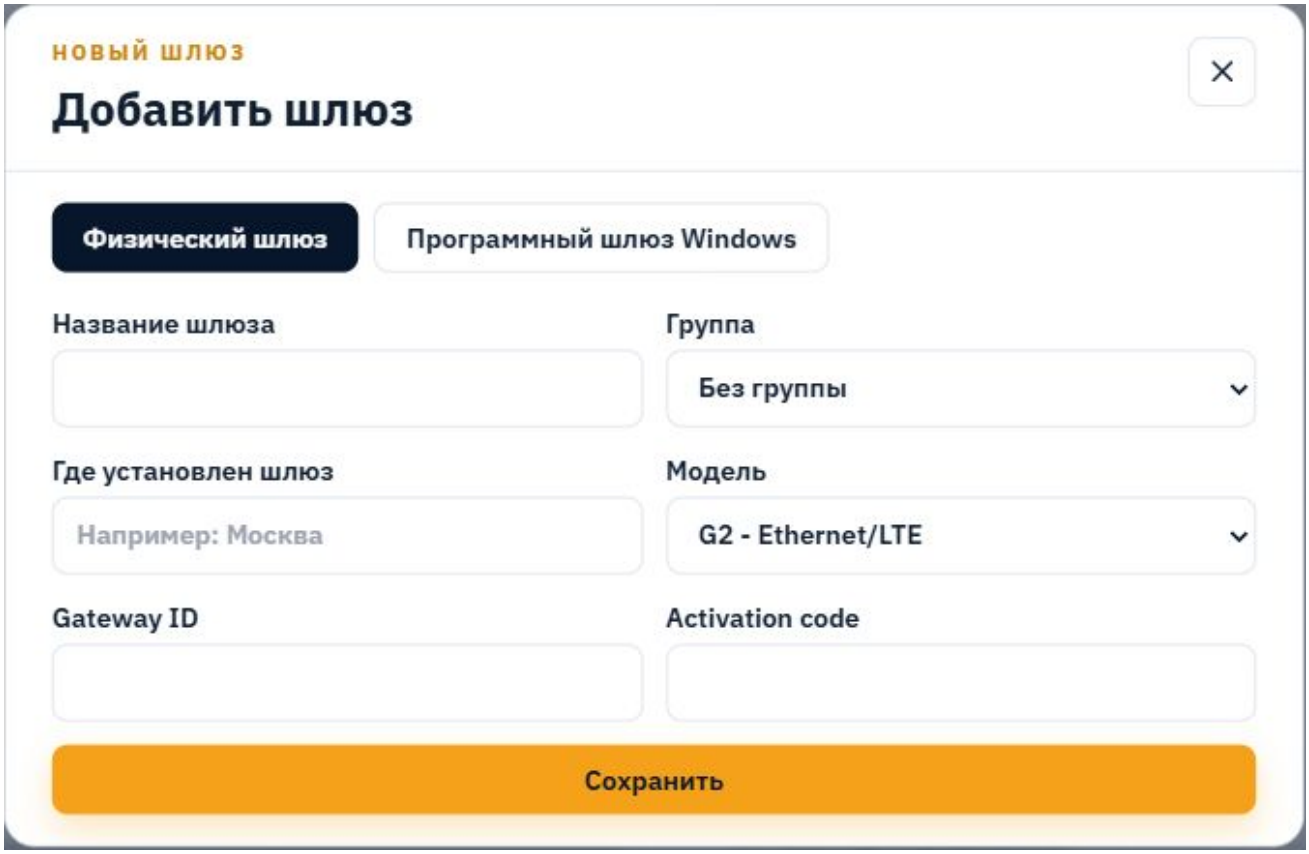
1. Подготовьте объект

Подключите ПЛК к LAN шлюза, обеспечьте шлюзу интернет через WAN или SIM-карту и подайте питание по руководству вашей модели. Запишите IP и маску ПЛК, а также протокол и порт нужного сервиса. Подробности — в статье «Link G2: назначение и подключение».

Пример для дальнейших шагов: ПЛК 192.168.1.10, маска 255.255.255.0; свободный LAN IP шлюза 192.168.1.1. Реальные адреса объекта могут отличаться. Важно, чтобы адреса устройств не повторялись, а LAN шлюза и ПЛК находились в одной подсети.

2. Войдите и привяжите шлюз

Создайте аккаунт, подтвердите контакты по подсказкам регистрации и выберите компанию. В разделе «Шлюзы» нажмите «Добавить шлюз». Укажите понятное имя объекта, модель, Gateway ID и activation code. Для первого объекта можно оставить «Без группы».

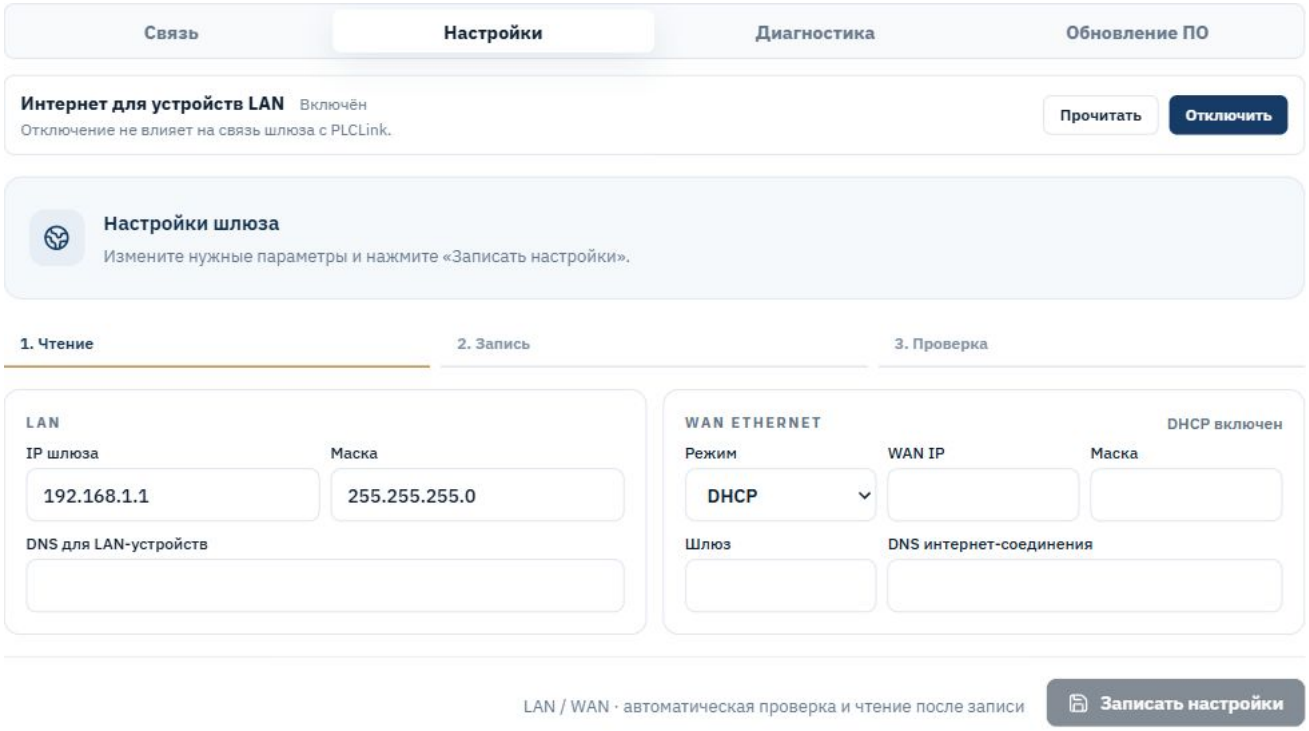


Форма привязки: сначала выберите компанию, затем добавьте физический шлюз по его идентификатору и коду.

Сохраните и дождитесь появления карточки. Проверьте связь шлюза с PLCLink. Если карточка есть, но шлюз не в сети, сначала разберитесь с питанием и интернетом на объекте — добавление новых записей не восстановит канал связи.

3. Сверьте LAN в кабинете

Откройте «Связь и настройки шлюза» → «Настройки». Дождитесь автоматического чтения. Сравните IP и маску LAN с сетью ПЛК; при необходимости измените их, нажмите «Записать настройки» и дождитесь контрольного чтения.

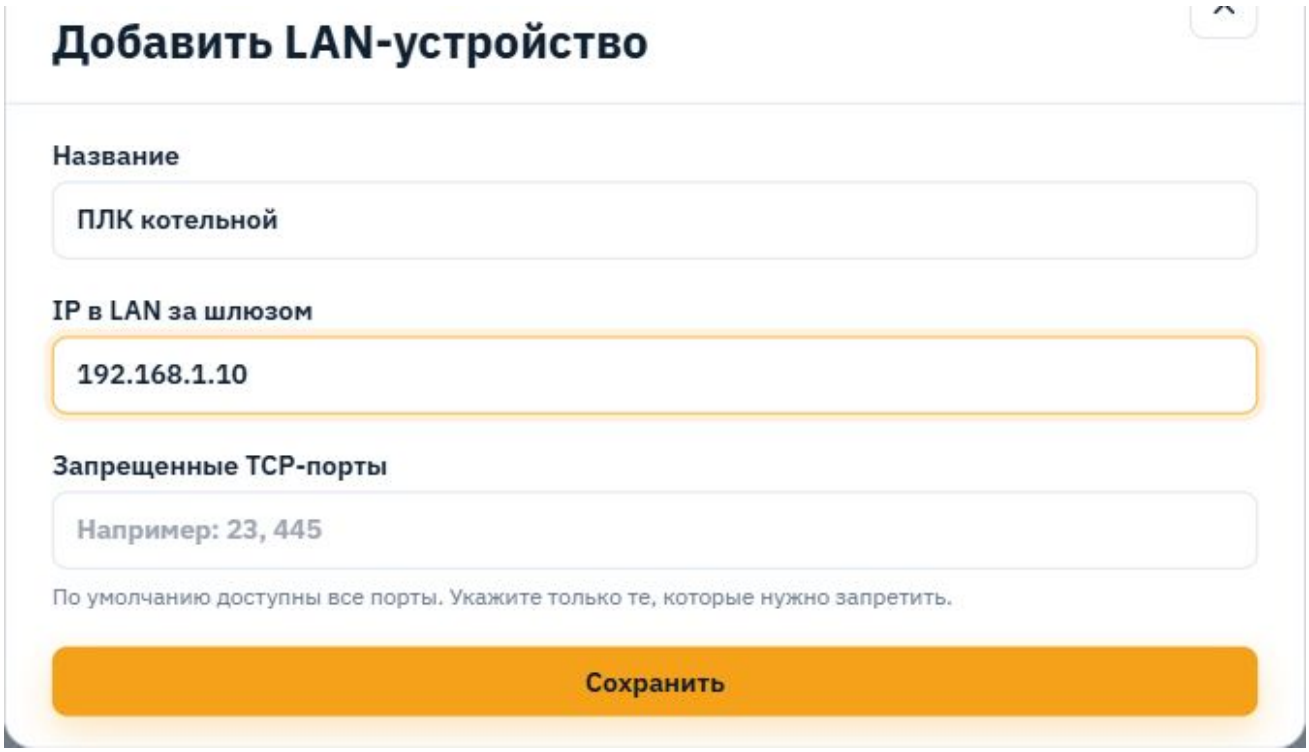


Чтение и запись LAN/WAN выполняются во вкладке «Настройки». На снимке LAN шлюза — 192.168.1.1/24.

Полная инструкция «Настройка LAN/WAN шлюза» объясняет каждое поле и действия при расхождении результатов. Для первого подключения не меняйте параметры, назначение которых вам пока неизвестно.

4. Добавьте устройство

Разверните шлюз и нажмите «Добавить вручную». Задайте имя ПЛК и его реальный IP — в примере 192.168.1.10. Если ограничения портов не нужны, оставьте поле «Запрещённые TCP-порты» пустым. Сохраните запись.



Запись LAN-устройства содержит адрес ПЛК, а не адрес самого шлюза.

5. Выберите способ работы

Для веб-страницы оборудования используйте M2Web: в строке ПЛК выберите HTTP/HTTPS и порт именно его веб-сервера, затем нажмите глобус. Например, HTTP:80 для веб-настроек или HTTP:8080 для визуализации, если так настроено устройство.



Браузерное подключение: выберите протокол и порт, затем нажмите глобус.

Для CODESYS, OPC или другой инженерной программы скачайте PLCLink Manager из кабинета. Войдите, выберите компанию и ПЛК, откройте сессию. В инженерной программе используйте виртуальный IP, показанный Manager, с рабочим портом устройства.

6. Убедитесь, что получен ответ

Первое подключение завершено, когда открылась нужная веб-страница либо инженерная программа получила данные от ПЛК. Только зелёный статус шлюза или надпись об открытой сессии этот результат не заменяют.

Если ответа нет, последовательно проверьте: связь шлюза с PLCLink, LAN IP и маску, адрес ПЛК в карточке, протокол и порт, права доступа. Запишите время попытки и текст ошибки. Закончив инженерную работу, остановите сессию в Manager.

Если не получилось

Если подключение не получилось, начните со статьи «Шлюз онлайн, а устройство или M2Web не открывается». Для поддержки запишите идентификатор шлюза, адрес устройства, порт, способ подключения и точное время попытки.

Основные термины PLCLink

Открыть статью в справке

Шлюз - физическое устройство PLCLink на объекте. LAN-устройство - любое оборудование за шлюзом: ПЛК, HMI, камера, серверный ПК. Группа - площадка или объект. Сессия - активный инженерный доступ. M2Web - web-доступ из браузера. Virtual IP - адрес, который Manager выдает устройству на ПК инженера.

Что сделать

1. Для объекта создайте группу.
2. В группу добавьте шлюзы.
3. За шлюзом храните LAN-устройства.
4. Для доступа запускайте M2Web или сессию Manager.
5. Для диагностики смотрите статусы шлюза, устройства и последние события.

Если не получилось

Если термин в интерфейсе непонятен, задайте вопрос ассистенту: он объяснит его в контексте PLCLink.

Связь

Шлюз не в сети

Открыть статью в справке

Статус «Не в сети» означает, что у сервиса нет актуального подтверждения связи со шлюзом. Проверьте питание, интернет на объекте и выбранный канал подключения. Наличие SIM-карты само по себе не подтверждает доступность мобильного интернета.

Что сделать

1. Проверьте питание шлюза и индикацию на корпусе.

2. После включения дайте шлюзу время установить связь.

3. В сведениях о шлюзе откройте «Связь» и посмотрите время последнего соединения и канал доступа.

4. Для WAN Ethernet проверьте кабель и наличие интернета в сети объекта.

5. Для SIM проверьте условия тарифа, доступность интернета и сигнал у оператора. При ограничениях мобильной сети обычный интернет может быть недоступен даже при хорошем сигнале.

6. Если связь не восстанавливается, сообщите в поддержку идентификатор шлюза, время, оператора и результаты проверок.

Если не получилось

Gateway ID, время последней связи, активный канал доступа, WAN IP, оператор SIM, что менялось на объекте перед пропаданием связи.

Шлюз онлайн, но LAN-устройство недоступно

Открыть статью в справке

Статус шлюза и статус LAN-устройства - разные вещи. Шлюз может быть онлайн, но конкретное устройство за ним может быть выключено, отключено от Ethernet, иметь другой IP-адрес или не отвечать на проверку доступности.

Что сделать

1. Убедитесь, что шлюз онлайн.

2. Раскройте шлюз и проверьте статус нужного LAN-устройства.

3. Проверьте физическое подключение устройства.

4. Проверьте, что IP-адрес устройства в кабинете совпадает с реальным IP на объекте.

5. Нажмите Обновить список устройств.

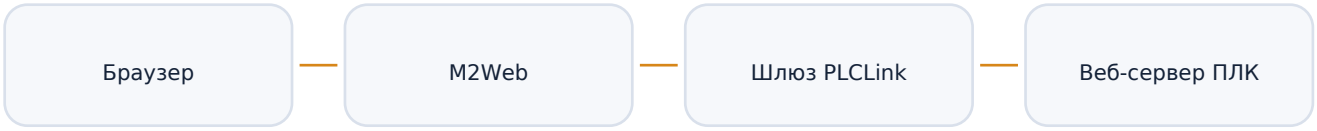
6. Если устройство добавлено вручную, проверьте, что доступ к нему разрешен.

7. Если устройство отвечает на ping, но web/протокол не работает, проверьте конкретный порт сервиса.

Если не получилось

Gateway ID, имя устройства, real IP, virtual IP, порт/протокол, результат обновления списка устройств.

M2Web



Как открыть Web-интерфейс устройства через M2Web

Открыть статью в справке

M2Web открывает веб-интерфейс ПЛК или панели в браузере через PLCLink. Установка Manager для этого не нужна. На самом устройстве должен работать HTTP- или HTTPS-сервер; наличие Ethernet-разъёма ещё не означает наличие веб-страницы.

1. Узнайте адрес веб-сервиса

Проверьте в документации или у инженера, по какому протоколу и порту открывается нужная страница. Например, веб-настройки ПЛК могут работать по HTTP на 80, а визуализация — по HTTP на 8080. HTTPS часто использует 443, но конкретное устройство может быть настроено иначе.

Адреса и порты примера не универсальны. Если локально нужная страница открывается как http://192.168.1.10:8080, для M2Web нужны именно HTTP и 8080. Выбор HTTPS или порта 80 приведёт к обращению к другому сервису либо к ошибке.

2. Выберите устройство, протокол и порт

Откройте «Шлюзы», разверните объект и найдите строку нужного ПЛК. Справа расположены выбор протокола, выбор порта и кнопка с глобусом. Проверьте реальный IP в строке: похожие имена устройств легко перепутать.



Кнопки M2Web в строке устройства: HTTP/HTTPS, порт и глобус для открытия страницы.

Выберите протокол и порт целевого веб-сервера. Разрешение доступа к устройству и права вашей роли также должны позволять подключение. Если нужного варианта порта нет в доступном списке, не выбирайте случайный: обратитесь к администратору компании или в поддержку с точным адресом локальной страницы.

3. Откройте страницу

Нажмите глобус «Открыть Web». Дождитесь открытия страницы в новой вкладке. Если вкладка не появилась, проверьте, не заблокировал ли браузер всплывающее окно для кабинета, и повторите действие.

Если оборудование показывает собственную форму входа, используйте учётную запись этого ПЛК или панели. Пароль от PLCLink не является автоматически паролем оборудования. После входа проверьте нужный экран или визуализацию.

4. Откройте второй сервис при необходимости

Для второй страницы того же ПЛК вернитесь к строке устройства, выберите её протокол и порт и снова нажмите глобус. Например, HTTP:80 для настроек и HTTP:8080 для визуализации — это два разных веб-сервиса одного IP. Порт второго сервиса не нужно подставлять в уже открытый адрес PLCLink вручную.

5. Если страница не открылась

Сообщение об отсутствии ответа M2Web не доказывает, что ПЛК физически отключён. Проверьте по порядку: правильный ли выбран ПЛК; верны ли HTTP/HTTPS и порт; работает ли эта страница локально; разрешён ли доступ; есть ли связь шлюза с PLCLink.

Если страница открывается, но отсутствуют картинки, кнопки или значения визуализации, сохраните скриншот и точное время. Сообщите модель и версию ПО устройства, протокол и порт, какой экран не работает и открывается ли он локально. Это поможет отличить сетевую проблему от особенностей веб-визуализации.

Если не получилось

Gateway ID, имя устройства, real IP, выбранный порт, схема http/https, скриншот ошибки браузера.

Веб-визуализация через M2Web: совместимость

Открыть статью в справке

M2Web предназначен для HTTP/HTTPS-интерфейсов оборудования, включая веб-визуализации. Совместимость зависит от того, как конкретная панель использует адреса, авторизацию и соединения. Ошибка одного интерфейса не означает, что устройство отключено или что все визуализации не поддерживаются.

Что сделать

1. Проверьте фактический протокол и порт веб-сервера.

2. Откройте интерфейс устройства локально на объекте и сравните поведение.

3. Если проблема только через M2Web, запишите модель, версию ПО, порт, путь страницы и действие, вызывающее ошибку.

4. Передайте эти данные и время попытки в поддержку. Для проверки можно открыть тот же веб-сервис через виртуальный IP в Manager.

Если не получилось

Передайте модель устройства, URL внутри M2Web, что именно не открывается, и нужен ли WebSocket/HTTPS.

Web-страница устройства открывается, но выглядит сломанной

Открыть статью в справке

Если главная страница открылась, а кнопки, изображения или визуализация не работают, соединение с веб-сервером уже установлено. Нужно выяснить, какой именно запрос или раздел не работает; менять сетевые настройки шлюза наугад не требуется.

Что сделать

1. Убедитесь, что выбран порт нужного веб-сервиса.

2. Обновите вкладку и повторите конкретное действие.

3. Сравните с локальным открытием на объекте или открытием того же порта через виртуальный IP Manager.

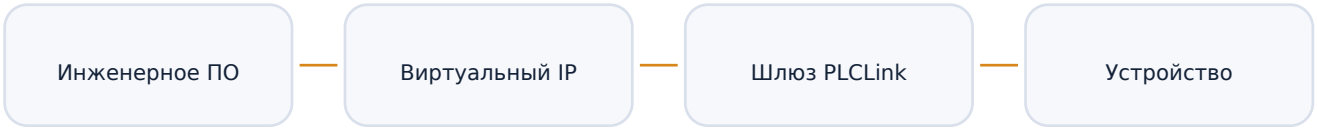
4. Запишите модель и версию ПО оборудования, порт, путь страницы и время ошибки.

5. Отправьте скриншот и описание в поддержку. Не прикладывайте пароль устройства или ссылку с секретом сессии.

Если не получилось

URL M2Web, модель устройства, какие вкладки ломаются, скриншот консоли браузера, если доступен.

PLCLink Manager



Что такое PLCLink Manager

Открыть статью в справке

PLCLink Manager - десктопное приложение для инженера. Оно получает список шлюзов и устройств из PLCLink Cloud, открывает инженерные сессии и дает локальный virtual IP для работы программ вроде CODESYS, OPC, Modbus-клиентов, VNC или SSH.

Что сделать

1. Скачайте PLCLink Manager из левого меню кабинета.
2. Установите приложение на ПК инженера.
3. Войдите под учетной записью PLCLink.
4. Выберите шлюз и устройство.
5. Откройте сессию и используйте выданный virtual IP.

Если не получилось

Если Manager не запускается или не входит, передайте версию Manager, Windows, лог приложения и email учетной записи.

Обновление Manager при открытых сессиях

Открыть статью в справке

Обновление Manager меняет приложение, через которое идут инженерные подключения. Перед обновлением завершите сессии, чтобы не оборвать работу с контроллером. Если обновление недоступно внутри приложения, используйте актуальный установщик из кабинета.

Что сделать

1. Сохраните проект и закройте обмен в инженерной программе.
2. Остановите активные сессии Manager.
3. Нажмите обновление в Manager и дождитесь завершения установки.
4. Запустите новую версию и откройте нужные сессии заново.

Если не получилось

Передайте версию до и после обновления, Windows и текст ошибки.

Установка и обновление PLCLink Manager

Открыть статью в справке

PLCLink Manager устанавливается на компьютер Windows, с которого вы будете работать с удалённым оборудованием. Например, это ноутбук с CODESYS или компьютер с OPC-сервером. На самом объекте соединение обеспечивает шлюз.

1. Скачайте релиз из кабинета

Войдите в кабинет PLCLink и нажмите «Скачать Manager» в левом меню. Используйте установщик из этого раздела: тестовые сборки, переданные для отдельных испытаний, не являются обычным клиентским релизом.

Дождитесь завершения загрузки. Если файл не появился, откройте список загрузок браузера и проверьте сообщение об ошибке или блокировке. Не ищите установщик на сторонних сайтах и не отключайте защиту Windows ради неизвестного файла.

2. Установите приложение

Запустите скачанный установщик и следуйте его шагам. Для установки сетевых компонентов могут потребоваться права администратора Windows. На корпоративном компьютере согласуйте установку с системным администратором.

После установки запустите PLCLink Manager. При обновлении сначала завершите рабочие сессии, чтобы не прервать обмен с ПЛК во время замены приложения. Если установщик просит перезапуск системы, сохраните работу и выполните его до проверки соединения.

3. Войдите и выберите компанию

Используйте свой аккаунт PLCLink. Выберите компанию, в которой находится нужный шлюз. Список оборудования зависит от членства и прав; пустой список сначала проверяйте по выбранной компании, а не по переустановке приложения.

Если вход выполнен, но нужного объекта нет, сравните выбранную компанию в Manager и кабинете. Затем попросите владельца проверить доступ к шлюзу. Доступ к финансам и доступ к оборудованию — разные права.

4. Проверьте первое подключение

Найдите устройство и откройте сессию. После успешного открытия Manager показывает адрес доступа — виртуальный IP. Именно этот адрес указывается в инженерной программе вместо LAN IP удалённого ПЛК.

Подробный пример приведён в статье «Как открыть инженерную сессию». В конце работы остановите сессию. Для сообщения об ошибке сохраните версию Manager, Gateway ID, время попытки и текст ошибки; пароль и коды подтверждения передавать не нужно.

Если не получилось

Передайте версию Manager, ссылку/дату скачивания, Windows build и текст ошибки установки.

Как открыть инженерную сессию

Открыть статью в справке

Инженерная сессия соединяет программу на вашем компьютере с конкретным устройством за шлюзом. Она подходит для работы с CODESYS, Modbus TCP, OPC и другим поддерживаемым сетевым ПО. ПЛК выбирается в Manager, а инженерная программа обращается к выданному виртуальному IP.

1. Проверьте исходные данные

Убедитесь, что ПЛК добавлен к нужному шлюзу с правильным реальным IP. Узнайте порт и способ подключения используемой программы. Например, TCP 1200 может использоваться вашим CODESYS-контроллером, а TCP 502 — Modbus TCP. Используйте параметры именно своего оборудования.

На объекте должны быть питание ПЛК, подключение LAN и связь шлюза с PLCLink. У вашей роли должен быть доступ к запуску сессии. Запрещённые порты в правилах устройства остаются запрещёнными и внутри открытой сессии.

2. Откройте сессию в Manager

Войдите в PLCLink Manager, выберите компанию и разверните нужный шлюз. Найдите устройство по имени и реальному IP, затем нажмите «Открыть». Дождитесь подтверждения запуска сессии и появления адреса доступа.

Открытая сессия означает, что доступ организован. Это ещё не подтверждение ответа конкретного протокола ПЛК: окончательная проверка выполняется в инженерной программе. Если кнопка запуска недоступна, прочитайте причину в Manager и проверьте права и связь шлюза.

3. Укажите виртуальный IP в программе

Скопируйте IP доступа из строки устройства. Например, реальный ПЛК может иметь адрес 192.168.1.10, а Manager назначит ему адрес вида 198.19.x.x. Не копируйте этот пример буквально: используйте точное значение из своей сессии.

В CODESYS или OPC-программе замените адрес подключения к ПЛК на выданный виртуальный IP. Порт и остальные настройки протокола оставьте соответствующими оборудованию. Автоматический поиск устройств в сети не заменяет проверку соединения по конкретному адресу.

4. Проверьте обмен и параллельную работу

Выполните обычное подключение или чтение данных из программы. Если ответ получен, канал работает. Несколько программ могут обращаться к одному устройству по разным разрешённым портам одновременно. Например, CODESYS и Modbus TCP не требуют искусственно ограничивать всю сессию одним портом.

Если связи нет, сравните порт, виртуальный IP и настройки протокола с локальным рабочим подключением. Не расширяйте разрешения наугад. Работа веб-страницы по HTTP:80 не подтверждает, что инженерный сервис слушает TCP:1200, и наоборот.

5. Завершите работу

После окончания обмена нажмите «Стоп» у активной сессии в Manager. Проверьте, что сессия завершилась. На Free каждая сессия ограничена 30 минутами; после завершения можно сразу подключиться заново. На Стандарте и Pro тарифного ограничения длительности нет.

Если завершить сессию не удаётся, откройте раздел «Сессии» в кабинете и проверьте доступное действие завершения. Сообщите поддержке номер сессии, время и ошибку. Не удаляйте устройство или шлюз только ради закрытия одного подключения.

Если не получилось

Передайте Gateway ID, устройство, virtual IP, порт/протокол и request/session ID из Manager.

Несколько программ и устройств одновременно

Открыть статью в справке

Одна сессия Manager к устройству позволяет разным программам одновременно обращаться к его разрешённым портам. Например, CODESYS и OPC-сервер могут работать с одним виртуальным IP. Для другого устройства открывается отдельная сессия. Тарифного ограничения количества параллельных сессий нет; ограничения самого оборудования и права доступа сохраняются.

Что сделать

1. Откройте сессию к устройству в Manager.

2. Укажите его виртуальный IP в каждой инженерной программе.

3. В каждой программе задайте порт её сервиса по документации оборудования.

4. Проверьте, что эти порты не запрещены в кабинете.

5. Для второго устройства откройте ещё одну сессию и используйте его виртуальный IP.

Если не получилось

Передайте Gateway ID, список устройств, virtual IP, session ID и сообщение Manager.

PLCLink Manager не открывает инженерную сессию

Открыть статью в справке

Для открытия сессии нужны доступная связь шлюза с PLCLink, разрешённое устройство, права сотрудника и возможность запуска подключений по состоянию баланса. Количество уже открытых сессий само по себе не является тарифным ограничением.

Что сделать

1. Проверьте выбранную компанию в Manager и кабинете.

2. Проверьте связь шлюза, права на устройство и баланс компании.

3. Прочитайте сообщение Manager: недоступность устройства и запрет доступа — разные причины.

4. Сохраните журнал Manager и точное время неудачной попытки.

5. Если проблема повторяется, передайте журнал в поддержку. Перед перезапуском Manager завершите работу в остальных активных сессиях.

Если не получилось

Gateway ID, устройство, real IP, virtual IP, request_id, session_id, время попытки, лог Manager.

Сессии

Активные сессии

Открыть статью в справке

Сессия даёт временный доступ к выбранному устройству. Открытая сессия и ответ самого ПЛК — разные состояния: соединение со шлюзом ещё не доказывает обмен с оборудованием. Завершайте ненужные сессии, чтобы закрыть удалённый доступ.

Что сделать

1. В Manager найдите устройство с открытой сессией и нажмите «Стоп».

2. Либо откройте раздел «Сессии» в кабинете и завершите нужную активную сессию, если у вас есть это право.

3. Дождитесь подтверждения закрытия.

4. Если закрыть не удаётся, передайте в поддержку номер сессии и время попытки. Не ориентируйтесь только на цвет индикатора устройства.

Если не получилось

Передайте session ID, Gateway ID, устройство, время открытия и закрытия Manager/шлюза.

Статус устройства и проверки во время сессии

Открыть статью в справке

Автоматические проверки устройства могут приостанавливаться во время инженерного обмена, чтобы не мешать оборудованию. «Нет свежих данных» означает отсутствие свежей проверки, а не подтверждённое отключение ПЛК. Ответ оборудования и активная сессия учитываются отдельно.

Что сделать

1. Посмотрите текст статуса рядом с устройством.

2. Если инженерная программа успешно получает ответы, сохраните текущую сессию и продолжайте работу.

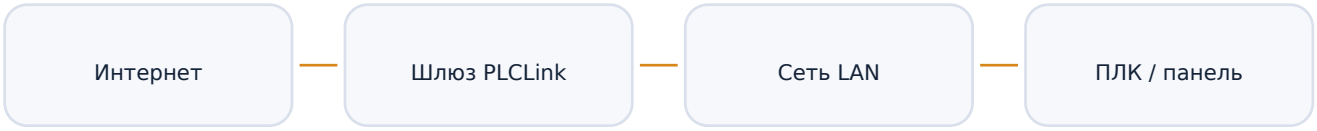
3. По завершении работы закройте сессию и дождитесь очередной проверки.

4. Если состояние долго не обновляется, запишите время и отправьте в поддержку скриншот и журнал Manager.

Если не получилось

Если сканирование блокируется без видимой активной сессии, передайте Gateway ID и время попытки.

Шлюзы



Link G2: назначение и подключение

Открыть статью в справке

Link G2 соединяет оборудование на объекте с PLCLink через интернет. На объекте он подключается к сети ПЛК и панелей, а вы работаете из браузера или PLCLink Manager. Начните с одного контроллера: так проще проверить подключение, прежде чем добавлять остальные устройства.

1. Подготовьте всё необходимое

Понадобятся шлюз Link G2, подходящий источник питания по маркировке вашего устройства, Ethernet-кабель, ПЛК или панель с известным IP-адресом и доступ к интернету. Для мобильного подключения нужны SIM-карта с передачей данных и антенна, предусмотренная комплектацией. Держите под рукой Gateway ID и activation code из комплекта шлюза: они понадобятся для привязки в кабинете.

Запишите IP-адрес ПЛК, маску сети и порт нужного сервиса. Например: ПЛК — 192.168.1.10, маска — 255.255.255.0, веб-интерфейс — HTTP, порт 80. Это пример, а не обязательные настройки: реальные значения возьмите из проекта или инструкции вашего оборудования.

2. Подключите оборудование к LAN

LAN — это локальная сеть оборудования. Подключите Ethernet-порт ПЛК к порту LAN шлюза. Если устройств несколько, используйте сетевой коммутатор: порт LAN шлюза и все устройства подключаются к нему. Ориентируйтесь на маркировку корпуса; не подключайте кабель ПЛК в WAN по привычке.

Адрес LAN шлюза должен находиться в одной подсети с устройствами и быть свободным. Для ПЛК 192.168.1.10 с маской 255.255.255.0 подойдёт, например, свободный адрес шлюза 192.168.1.1 с той же маской. Два устройства с одинаковым адресом работать корректно не будут. Не меняйте существующий адрес ПЛК без необходимости: удобнее согласовать LAN шлюза с сетью объекта.

3. Подготовьте интернет для шлюза

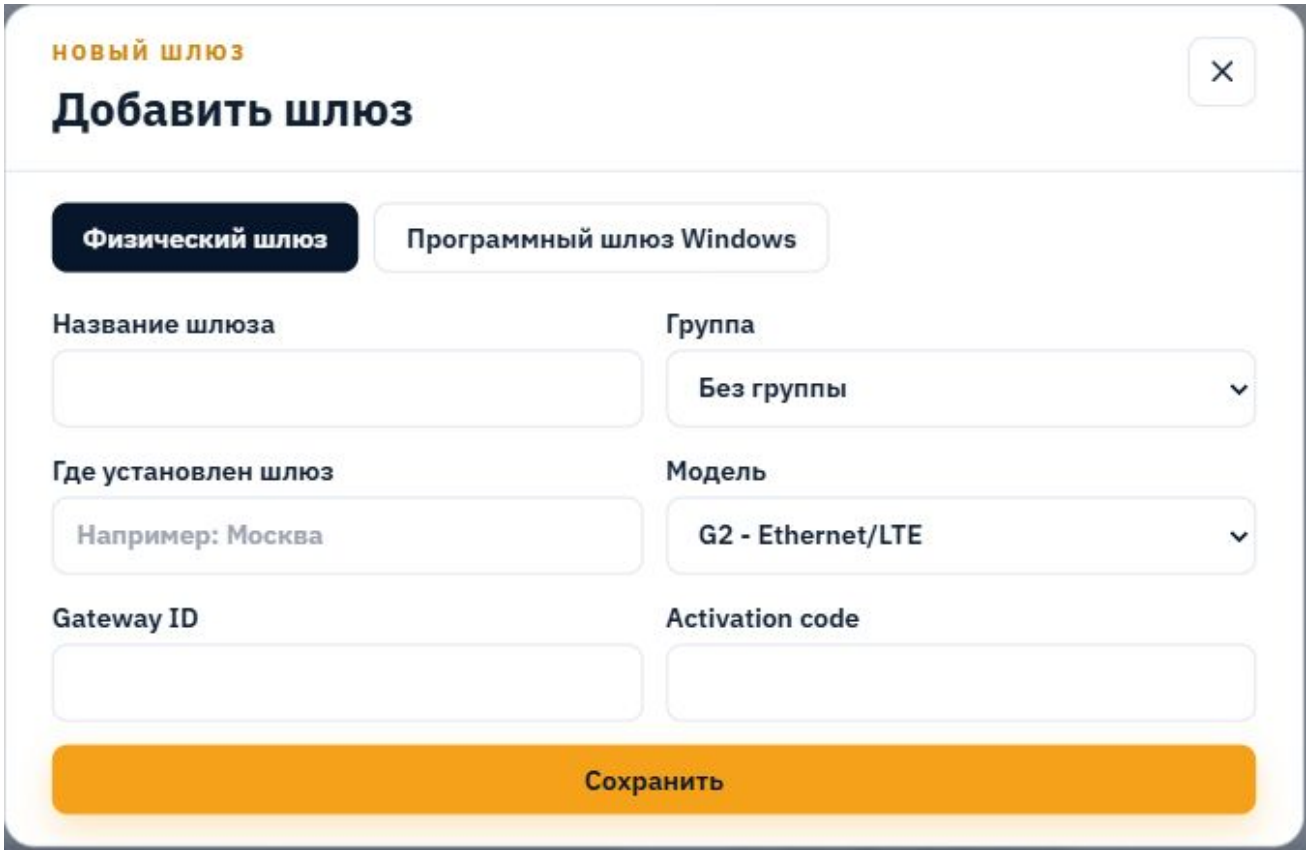
При подключении по Ethernet кабель от маршрутизатора объекта подключается к WAN. Если сеть выдаёт адреса автоматически, используется DHCP. Если администратор выдал статические параметры, понадобятся WAN IP, маска, адрес маршрутизатора и DNS. LAN и WAN должны быть разными подсетями: например, LAN 192.168.1.0/24 и WAN 192.168.10.0/24.

При мобильном подключении установите SIM-карту и подключите антенну согласно руководству вашей модификации шлюза. У SIM-карты должны быть доступны передача данных и связь с серверами PLCLink. Наличие уровня сигнала ещё не означает, что оператор пропускает интернет-трафик. При ограничениях мобильного интернета доступность зависит от оператора и региона.

Шлюз сам устанавливает исходящее соединение с PLCLink. Для обычного сценария не нужен белый IP на объекте и проброс входящих портов на маршрутизаторе. Если в сети организации есть ограничения исходящего доступа, согласуйте подключение с её администратором.

4. Подайте питание и привяжите шлюз

Проверьте напряжение и полярность по маркировке вашей модели, затем подайте питание. Дождитесь загрузки. Откройте кабинет, выберите нужную компанию и нажмите «Добавить шлюз». Пошаговое заполнение формы разобрано в статье «Как добавить шлюз в кабинет».



Форма привязки физического шлюза. Gateway ID и activation code берутся из комплекта вашего устройства.

После сохранения в разделе «Мои шлюзы» появится карточка. Статус «в сети» означает связь шлюза с PLCLink. Доступность каждого ПЛК проверяется отдельно: зелёная карточка шлюза сама по себе не подтверждает правильный IP или порт контроллера.

5. Проверьте LAN и добавьте первый ПЛК

Откройте «Связь и настройки шлюза» → «Настройки» и дождитесь чтения фактических параметров. Сверьте LAN IP и маску с подготовленным примером. Если нужно изменить параметры, используйте инструкцию «Настройка LAN/WAN шлюза»: она показывает чтение, запись и проверку результата.

Разверните карточку шлюза и добавьте ПЛК через «Добавить вручную». Для веб-интерфейса выберите M2Web; для CODESYS, OPC или другой инженерной программы — PLCLink Manager. Успешный первый результат: открывается нужная страница ПЛК либо инженерная программа устанавливает связь по виртуальному IP.

Если не получилось

Если Link G2 не выходит в сеть, укажите способ подключения к интернету, WAN IP, индикацию на корпусе и время включения.

Шлюз не удаётся активировать

Открыть статью в справке

Готовый к работе физический шлюз поставляется с идентификатором и кодом активации. Если кабинет сообщает, что выпуск шлюза не завершён, потребуется проверка продавцом или поддержкой. Самостоятельная смена модели, адресов или повторная регистрация аккаунта эту ошибку не исправят.

Что сделать

1. Сверьте Gateway ID на этикетке.

2. Проверьте код активации.

3. Добавьте шлюз в выбранную компанию.

4. При сообщении о незавершённом выпуске обратитесь к продавцу или поддержке; повторный ввод кода проблему не исправит.

Если не получилось

Передайте Gateway ID и подтверждение покупки. Полный код активации не публикуйте.

Первая связь с оборудованием: контрольный список

Открыть статью в справке

Для доступа нужен выпущенный и привязанный шлюз, его соединение с PLCLink, добавленное LAN-устройство, право сотрудника и подходящий способ доступа. M2Web открывает веб-панель в браузере, Manager нужен для инженерных программ.

Что сделать

1. Проверьте компанию и статус шлюза «В сети».

2. Добавьте LAN-устройство с реальным IP.

3. Проверьте доступность устройства и разрешённые порты.

4. Для HTTP/HTTPS используйте M2Web.

5. Для CODESYS, Modbus TCP и других программ откройте сессию Manager.

Если не получилось

Сохраните Gateway ID, реальный IP устройства, протокол, порт, время попытки и текст ошибки.

Изменение LAN-адреса шлюза

Открыть статью в справке

После записи нового LAN-адреса шлюз применяет сетевые параметры; на это время связь с устройствами может прерваться. Подтверждение в кабинете означает успешное завершение операции, а не только отправку команды. Новый адрес шлюза и адреса LAN-устройств должны соответствовать сети объекта.

Что сделать

1. Сохраните работу и завершите инженерные сессии.

2. Откройте вкладку «Настройки» шлюза и дождитесь чтения параметров.

3. Укажите LAN IP и маску, согласованные с сетью оборудования.

4. Нажмите «Записать настройки» и дождитесь автоматической проверки фактических значений.

5. При ошибке чтения используйте «Повторить чтение». Если связь потеряна, проверьте WAN/LTE и обратитесь в поддержку.

Если не получилось

Передайте Gateway ID, прежний и новый LAN IP, маску и время операции. Не меняйте физический шлюз по удалённой инструкции поддержки без проверки сети объекта.

Gateway ID и activation code

Открыть статью в справке

Gateway ID и код активации выдаются с конкретным шлюзом Link G2. Привязать можно только шлюз, выпуск которого завершён в Factory. Храните код активации в тайне: его используют для привязки шлюза к компании.

Что сделать

1. Найдите Gateway ID на лицевой панели шлюза.

2. Найдите activation code рядом с ним.

3. В кабинете нажмите Добавить шлюз.

4. Введите Gateway ID и activation code без лишних пробелов.

5. Сохраните шлюз.

Если не получилось

Полный activation code передавайте только по защищенному каналу поддержки. В обычных обращениях достаточно Gateway ID и последних 2-3 символов кода.

Как добавить шлюз в кабинет

Открыть статью в справке

Привязка добавляет физический шлюз в выбранную компанию. После этого он появляется у сотрудников, которым разрешён доступ. Перед началом подготовьте Gateway ID и activation code из комплекта устройства. Код активации храните как пароль: на общих скриншотах его быть не должно.

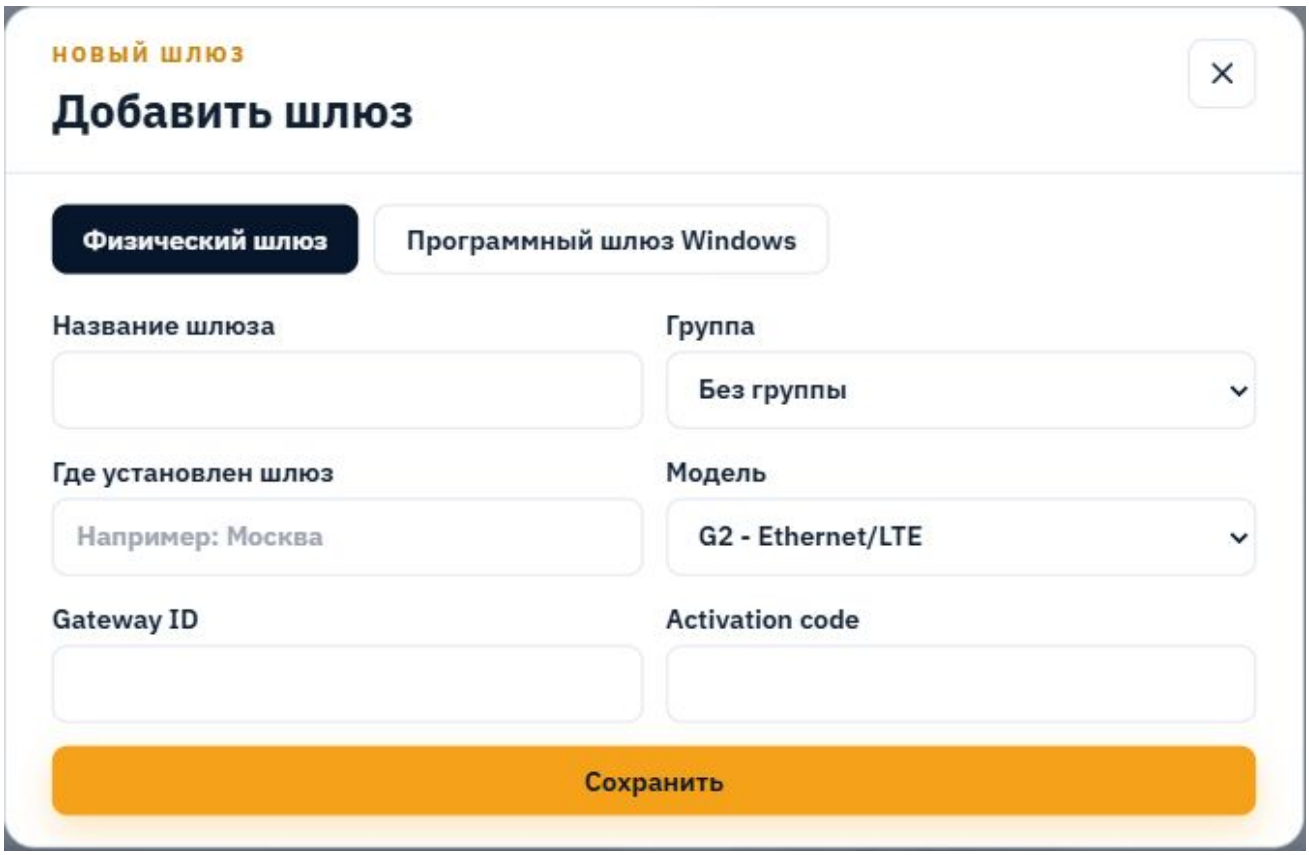
1. Выберите компанию

Войдите в кабинет и посмотрите название компании в нижней части левого меню. Если у вас несколько компаний, сначала переключитесь на ту, которой принадлежит оборудование. Привязка и последующие начисления относятся именно к выбранной компании.

Откройте раздел «Шлюзы». На Free можно привязать один шлюз суммарно; если место уже занято, сначала решите, к какой компании и тарифу относится новый объект. Создавать вторую карточку для одного и того же физического шлюза не нужно.

2. Откройте форму привязки

Нажмите «Добавить шлюз» и выберите физический шлюз. Для Link G2 используйте соответствующую модель. Форма программного шлюза Windows предназначена для другого сценария и не заменяет привязку G2.



Добавление физического шлюза: название, группа, место установки, модель и данные активации.

3. Заполните сведения об объекте

«Название шлюза» — понятное имя для списка, например «Котельная — основной шкаф». Коллегам будет проще найти объект по этому имени, чем по заводскому идентификатору.

«Группа» помогает организовать несколько объектов. Для первого шлюза можно оставить «Без группы» и распределить объекты позже. «Где установлен шлюз» — описание места, например «Здание А, шкаф автоматики». Это подпись для людей, она не настраивает сеть.

«Gateway ID» — идентификатор самого шлюза. Перенесите его из комплекта без лишних пробелов. «Activation code» — код привязки этого устройства. Не используйте пароль от кабинета или код другого шлюза.

4. Сохраните и проверьте карточку

Нажмите «Сохранить» один раз и дождитесь ответа. Карточка должна появиться в «Моих шлюзах». Разверните её стрелкой слева: здесь будут устройства за шлюзом. Пока ПЛК не добавлены, пустой список устройств нормален.

Если шлюз подключён к питанию и интернету, дождитесь обновления связи. Привязка и связь — разные состояния: добавленная карточка может показывать «не в сети», если устройство ещё не вышло в интернет. Не отвязывайте его только из-за этого; сначала проверьте питание и интернет на объекте.

5. Перейдите к настройке сети

Когда шлюз на связи, откройте «Связь и настройки шлюза» → «Настройки». Прочитайте фактические LAN-параметры, затем добавьте ПЛК. Не подставляйте IP из чужого примера: адреса должны соответствовать вашей сети.

Если форма сообщает, что шлюз уже привязан, повторная отправка того же кода не поможет. Проверьте выбранную компанию и предыдущую привязку. Если код не принимается у нового устройства, передайте поддержке Gateway ID и текст ошибки, но не публикуйте activation code.

Если не получилось

Gateway ID, модель шлюза, аккаунт клиента, текст ошибки при добавлении. Полный activation code передавать только по защищенному каналу поддержки.

Где установлен шлюз

Открыть статью в справке

Поле места установки помогает клиенту и поддержке понимать, на каком объекте находится шлюз. Если место не указано вручную, сервер может использовать примерную геолокацию по доступным данным связи, когда такая информация есть.

Что сделать

1. При добавлении шлюза начните вводить населенный пункт или объект.

2. Если точный адрес неизвестен, оставьте поле пустым.

3. Позже можно изменить место установки в настройках шлюза.

4. Для сервисных зон используйте группы объектов.

Если не получилось

Если место установки отображается неверно, укажите правильный населенный пункт, объект и Gateway ID.

Настройка LAN/WAN шлюза

Открыть статью в справке

LAN — сеть ПЛК и панелей за шлюзом. WAN — Ethernet-подключение самого шлюза к интернету. Ниже показано, как прочитать действующие настройки, изменить нужные поля и убедиться, что шлюз применил изменения.

1. Подготовьте адреса до изменения

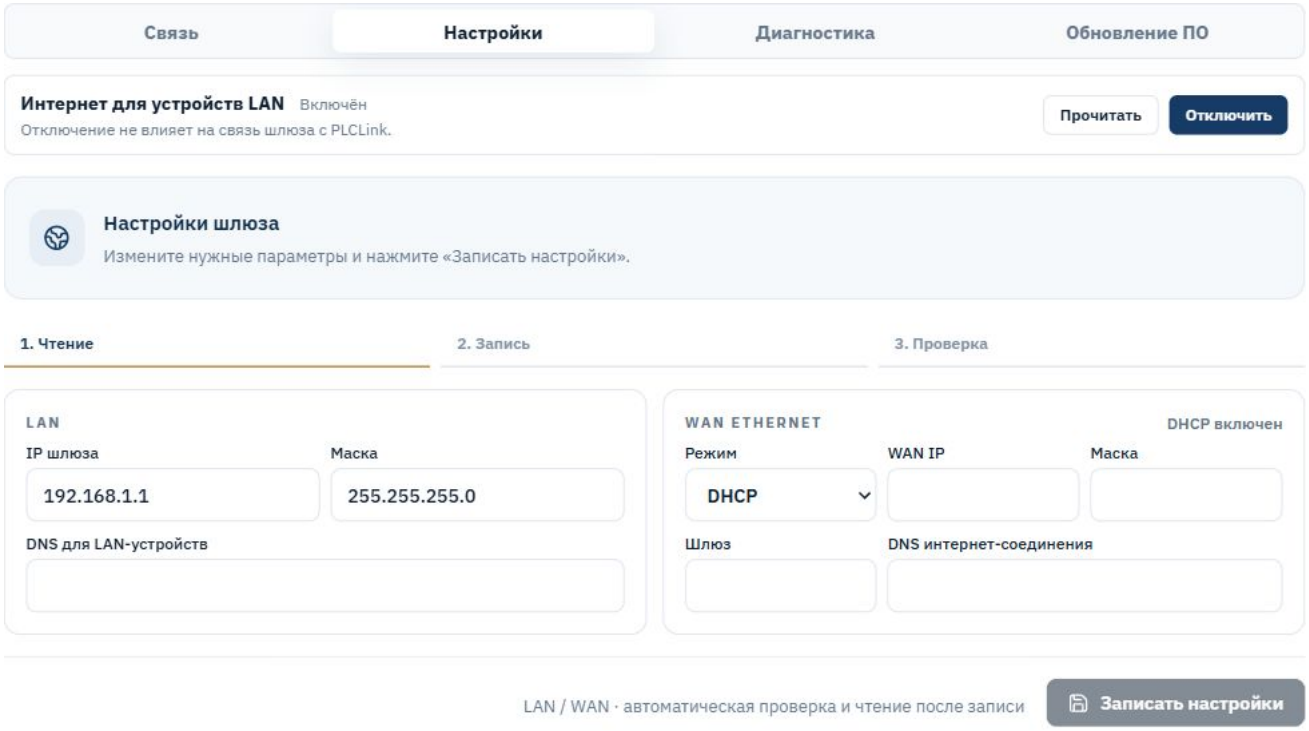
Узнайте реальный IP и маску ПЛК. В примере ПЛК имеет адрес 192.168.1.10 и маску 255.255.255.0. Для LAN шлюза используем свободный адрес 192.168.1.1 с той же маской. Для второго ПЛК можно использовать другой свободный адрес этой сети, например 192.168.1.11.

Адрес шлюза не должен совпадать с адресом ПЛК, маршрутизатора или другого устройства. Если оборудование уже работает в сети 192.168.3.0/24, подберите свободный LAN IP в этой сети, а не копируйте 192.168.1.1. LAN и WAN не должны использовать одну и ту же подсеть.

Меняйте сетевые параметры в согласованное время: изменение может прервать удалённую работу. Сохраните старые значения и обеспечьте возможность проверки на объекте, особенно при изменении WAN.

2. Откройте настройки и дождитесь чтения

В разделе «Шлюзы» найдите нужный объект. Нажмите кнопку «Связь и настройки шлюза» и откройте вкладку «Настройки». Кабинет запрашивает фактические значения у устройства автоматически. Пока идёт чтение, дождитесь завершения; пустое поле во время загрузки ещё не означает, что параметр не задан.



Фактические настройки LAN/WAN: LAN IP 192.168.1.1, маска 255.255.255.0; для WAN выбран DHCP.

На снимке показан конкретный пример. Он не задаёт обязательные адреса для вашего объекта. Сверяйте прежде всего значения, полученные от собственного шлюза.

3. Заполните блок LAN

«IP шлюза» — адрес LAN-интерфейса Link G2. В нашем примере это 192.168.1.1. В это поле нельзя вводить адрес ПЛК 192.168.1.10: адрес ПЛК будет указан отдельно при добавлении устройства.

«Маска» определяет локальную подсеть. Для приведённого примера используется 255.255.255.0. Она должна соответствовать настройкам оборудования. Если на объекте другая маска, используйте согласованную сетевую схему.

«DNS для LAN-устройств» относится к разрешению доменных имён. Для обращения к ПЛК по известному IP DNS не заменяет правильные IP и маску. Не вписывайте случайный DNS и не меняйте пустое значение без необходимости; при работе устройств с доменными именами используйте параметры, согласованные с администратором сети.

4. Проверьте WAN Ethernet

В режиме DHCP адресные параметры выдаёт маршрутизатор объекта. Поля статического WAN IP, маски и шлюза в этом режиме недоступны для ручного ввода. DHCP относится к WAN и не означает, что вы должны изменить статический IP ПЛК.

Если нужен статический режим, подготовьте полный набор значений: свободный WAN IP, маску, адрес маршрутизатора и DNS интернет-соединения. Эти параметры выдаёт администратор сети объекта. Нельзя переносить сюда LAN-адрес ПЛК или придумывать адрес маршрутизатора.

При использовании SIM-карты настройки WAN Ethernet не являются настройками сотового оператора. Текущий канал связи смотрите во вкладке «Связь». Отдельный блок «Интернет для устройств LAN» управляет выходом LAN-устройств в интернет; не переключайте его только ради изменения IP шлюза.

5. Запишите и дождитесь проверки

Измените только нужные поля и нажмите «Записать настройки». Если ничего не меняли, кнопка может быть неактивна. После отправки кабинет выполняет запись и контрольное чтение. Дождитесь окончания всей последовательности «Чтение → Запись → Проверка»; не отправляйте ту же команду несколько раз подряд.

Успешный результат — фактические значения после чтения соответствуют введённым и нет сообщения о расхождении. Сам факт нажатия кнопки ещё не подтверждает применение конфигурации. Если появилось «Нужно проверить состояние», прочитайте сообщение и повторите чтение доступной кнопкой; не продолжайте менять значения наугад.

6. Проверьте доступ к ПЛК

Вернитесь к карточке шлюза. В записи LAN-устройства должен быть указан реальный IP ПЛК — в примере 192.168.1.10, а не адрес шлюза 192.168.1.1. Откройте нужный веб-сервис через M2Web или подключитесь через Manager.

Если шлюз остаётся в сети, а ПЛК недоступен, проверьте кабель LAN, питание ПЛК, его IP и маску, отсутствие одинаковых адресов и порт выбранного сервиса. Если после изменения WAN пропала связь с самим шлюзом, понадобится проверка интернет-параметров на объекте: кабинет не сможет прочитать их с отключившегося устройства.

Если не получилось

Передайте Gateway ID, текущие LAN/WAN параметры, что меняли и какой результат показал кабинет.

Обновление внутреннего ПО шлюза

Открыть статью в справке

Наличие обновления проверяется в карточке шлюза. Устанавливайте предложенную сервисом версию для вашей модели. Перед обновлением сохраните работу в инженерном ПО и завершите подключения; во время установки связь может временно пропасть.

Что сделать

1. Откройте сведения о шлюзе и вкладку «Обновление ПО».

2. Сверьте текущую версию и доступное обновление.

3. Если обновление доступно, запустите его и дождитесь результата.

4. Не отключайте питание во время установки.

5. После восстановления связи проверьте версию и доступность оборудования. При ошибке сохраните сообщение и обратитесь в поддержку.

Если не получилось

Передайте Gateway ID, текущую версию ПО, доступную версию, время запуска OTA и статус операции.

Тарифы и баланс

Когда списания приостанавливаются

Открыть статью в справке

Если в компании нет добавленных шлюзов, платный тариф не списывает средства. Если все шлюзы непрерывно офлайн, первые четыре суток оплачиваются, а с начала пятых суток (после 96 часов) списания приостанавливаются. При возвращении любого шлюза онлайн начисления возобновляются без доначисления за паузу; следующий период полного офлайна считается заново.

Что сделать

1. Откройте «Финансы» выбранной компании.

2. Проверьте тариф, баланс и состояние шлюзов.

3. Если списания не совпадают с правилом, сохраните дату и время офлайна и историю операций.

4. Передайте данные в поддержку.

Если не получилось

Укажите компанию, Gateway ID шлюзов, даты офлайна и строки списаний.

Бонус за первую активацию физического шлюза

Открыть статью в справке

При первой активации каждого нового физического шлюза Link G2 или Link G4 компания получает на баланс сумму, равную трём месяцам тарифа «Стандарт» для одного шлюза. При текущей цене 390 ₽ в месяц это 1 170 ₽. Бонус начисляется один раз на физический шлюз; повторная привязка, перенос между компаниями или восстановление удалённого шлюза нового бонуса не дают.

Что сделать

1. Приобретите новый физический шлюз Link G2 или Link G4.

2. Выберите компанию, на баланс которой должен поступить бонус.

3. Впервые активируйте шлюз в системе.

4. Проверьте начисление 1 170 ₽ в разделе «Финансы».

5. Регистрация аккаунта и активация программного шлюза такого бонуса не дают.

Если не получилось

Если бонус не появился, укажите компанию, Gateway ID и время первой активации.

Тарифные ограничения и активные сессии

Открыть статью в справке

Тариф действует для выбранной компании. На Free можно привязать один шлюз и работать с каждой сессией до 30 минут; после завершения можно сразу подключиться снова. На Стандарте и Pro длительность не ограничена. Тарифного лимита одновременных сессий Manager и M2Web нет.

Что сделать

1. Проверьте выбранную компанию и тариф в разделе «Финансы».

2. На Free учитывайте время каждой сессии и сохраняйте работу до её завершения.

3. Если подключение не открывается, проверьте баланс, права, связь шлюза и текст ошибки. Закрывать другую сессию только ради тарифного лимита не требуется.

Если не получилось

Аккаунт, тариф, Gateway ID, сколько сессий открыто, какую сессию не удается запустить.

Тарифы Free, Стандарт и Pro

Открыть статью в справке

Free — 0 ₽: один шлюз, один пользователь, каждая сессия до 30 минут, журнал за 7 дней. После завершения можно сразу подключиться снова.

Стандарт — 390 ₽ × число привязанных активных шлюзов в месяц: доступ 24/7, до пяти пользователей вместе с владельцем, готовые роли и журнал за 3 календарных месяца.

Pro — 1 490 ₽ за компанию + 290 ₽ × число привязанных активных шлюзов в месяц, включая первый. Пользователи без тарифного лимита, индивидуальные права, гостевой доступ до 365 дней, API-токены, журнал за 3 календарных года и экспорт CSV/PDF. Например, один шлюз — 1 780 ₽ в месяц.

Одновременные сессии не ограничены тарифом. Программные и физические шлюзы учитываются вместе; доступность функций зависит также от модели оборудования и выпущенной версии приложения.

Если шлюзов нет, платные списания приостановлены, включая базовую часть Pro. Если все шлюзы непрерывно офлайн 96 часов, списания приостанавливаются с начала пятых суток. Выход любого шлюза онлайн возобновляет оплату без доначислений за паузу. Стоимость делится на ежедневные списания с учётом длины календарного месяца.

Что сделать

1. Выберите компанию.

2. Откройте «Финансы».

3. Сверьте число активных шлюзов, месячную стоимость и доступные права.

4. Перед понижением тарифа устраните перечисленные кабинетом ограничения.

Если не получилось

Укажите компанию, текущий тариф и ожидаемое действие.

Счёт для юридического лица и пополнение

Открыть статью в справке

Компания может пополнить баланс доступным в кабинете способом оплаты. Для безналичной оплаты используются реквизиты юридического лица и счёт. Баланс отражает подтверждённые операции; одна лишь заявка на платёж не считается пополнением.

Что сделать

1. Выберите нужную компанию и откройте «Финансы».
2. Проверьте реквизиты и действующий тариф.
3. Создайте запрос на счёт или выберите доступный способ пополнения.
4. После оплаты проверьте статус операции и баланс.

Если не получилось

Передайте номер счёта или операции, компанию и дату оплаты без данных банковской карты.

Часовой пояс финансовых операций

Открыть статью в справке

Даты ежедневных списаний относятся к часовому поясу биллинга компании. Они могут отличаться от даты на компьютере инженера или на объекте. При смене тарифа новая цена применяется к следующему ежедневному списанию; уже проведённая операция текущего дня не пересчитывается.

Что сделать

1. Откройте «Финансы» выбранной компании.
2. Проверьте часовой пояс.
3. При необходимости измените его уполномоченным сотрудником.
4. Сверьте даты следующих операций.

Если не получилось

Укажите компанию, ожидаемый и фактический часовой пояс и дату операции.

Баланс и пополнение

Открыть статью в справке

Баланс компании используется для ежедневной оплаты PLCLink. Пополнение и бонус — отдельные операции в истории. Минимальная сумма пополнения в кабинете — 100 ₽. Оплата появляется на балансе после подтверждения, а не в момент создания счёта.

Что сделать

1. Выберите компанию и откройте «Финансы».

2. Нажмите «Пополнить баланс» и укажите сумму.

3. Выберите предложенный кабинетом способ оплаты; для безналичной оплаты проверьте реквизиты и счёт.

4. После оплаты проверьте баланс и историю операций.

5. Если платёж не появился, отправьте в поддержку номер счёта, сумму и дату оплаты; повторно оплачивать счёт не нужно.

Если не получилось

Аккаунт, сумма, тариф, время операции и статус платежа.

Телеметрия

Дашборд и состояние парка шлюзов

Открыть статью в справке

Дашборд показывает общие показатели выбранной компании. Состояние «В сети» означает связь шлюза с PLCLink; состояние LAN-устройства и действующая инженерная сессия проверяются отдельно. При переключении компании показатели меняются.

Что сделать

1. Выберите компанию.
2. Сверьте количество шлюзов и число шлюзов в сети.
3. Откройте конкретный шлюз для подробной связи и устройств.
4. При расхождении обновите страницу и проверьте выбранную компанию.

Если не получилось

Укажите компанию, Gateway ID и время расхождения.

Трафик и история сессий

Открыть статью в справке

Учёт трафика и история инженерных подключений относятся к выбранной компании. Статистика помогает понять нагрузку и найти время возникновения проблемы. Состояние шлюза и фактический обмен с LAN-устройством — разные показатели.

Что сделать

1. Переключитесь на нужную компанию.
2. Откройте «Трафик» или «Сессии».
3. Выберите период и шлюз.
4. Сопоставьте время события с журналом и логом Manager.

Если не получилось

Передайте период, компанию, Gateway ID и номер сессии, если он есть.

Геолокация и место установки шлюза

Открыть статью в справке

Место установки можно указать в карточке шлюза. Приблизительная геолокация по сети не заменяет адрес объекта и может быть неточной. Для работы команды полезно хранить понятное название площадки и группу объектов.

Что сделать

1. Откройте карточку шлюза в выбранной компании.

2. Укажите место установки и группу.

3. Проверьте, что коллеги видят правильный объект.

4. При переносе шлюза обновите описание.

Если не получилось

Укажите Gateway ID и ожидаемое место установки.

Телеметрия шлюза

Открыть статью в справке

Телеметрия показывает, как шлюз связан с PLCLink: канал доступа, WAN IP, transport region, версию внутреннего ПО, время последней связи и состояние сотового канала, если SIM установлена и модем передает данные.

Что сделать

1. В строке шлюза нажмите иконку информации.

2. Откройте вкладку Связь.

3. Проверьте Канал доступа, WAN IP и Последняя связь.

4. Если установлена SIM, проверьте оператор, сеть, RSRP/RSRQ/SINR.

5. Если данных SIM нет, значит шлюз сейчас не передает активную SIM-телеметрию.

Если не получилось

Передайте Gateway ID, время последней связи, активный канал доступа, WAN IP и показатели сотового канала, если они есть.

WAN Ethernet и сотовый канал: что активное

Открыть статью в справке

Шлюз может быть подключен к интернету через WAN Ethernet, при этом SIM может быть вставлена и передавать телеметрию сотового канала. Активный канал доступа показывает, через что шлюз сейчас связан с PLCLink.

Что сделать

1. Откройте телеметрию шлюза.

2. Посмотрите поле Канал доступа.

3. Если указано WAN Ethernet, шлюз работает через проводную сеть.

4. Если есть SIM-телеметрия, она отображается отдельным блоком с оператором и качеством сигнала.

5. Наличие SIM не означает, что интернет сейчас идет через сотовый канал.

Если не получилось

Если активный канал отображается неверно, передайте WAN IP, оператора SIM, время последней telemetry и способ физического подключения.

Что значит плохой сотовый сигнал

Открыть статью в справке

Плохой сигнал может давать задержки, потери и периодические разрывы сессий. Важны не только уровень сигнала, но и качество: RSRP, RSRQ и SINR. Даже если шлюз онлайн, слабый радиоканал может ухудшать работу инженерной сессии.

Что сделать

1. Откройте телеметрию шлюза.

2. Проверьте оператора, режим сети и band.

3. Оцените RSRP: чем ближе к -80 dBm, тем лучше; около -100 dBm и хуже уже требует внимания.

4. Оцените RSRQ/SINR: плохое качество может давать задержки и потери.

5. При слабом сигнале попробуйте вынести антенну или изменить место установки.

Если не получилось

Передайте Gateway ID, оператор, RSRP, RSRQ, SINR, band, место установки и время проблемы.

Протоколы

Modbus TCP через PLCLink

Открыть статью в справке

Modbus TCP работает через инженерную сессию PLCLink Manager. Из-за мобильных и удаленных каналов задержки могут быть выше локальной сети, поэтому в OPC/SCADA-клиентах стоит увеличивать timeout и не задавать слишком частый опрос.

Что сделать

1. Откройте сессию к устройству.
2. Используйте virtual IP и порт 502 в OPC/SCADA-клиенте.
3. Увеличьте timeout ответа.
4. Настройте разумный период опроса.
5. Если бывают ошибки, проверьте качество канала и журнал клиента.

Если не получилось

Gateway ID, real IP, virtual IP, порт, timeout OPC/SCADA, период опроса и пример ошибки.

OPC UA через PLCLink

Открыть статью в справке

OPC UA можно использовать через PLCLink Manager, если OPC UA server доступен по TCP из LAN за шлюзом. Нужно учитывать сертификаты OPC UA и то, что endpoint может содержать старый адрес устройства.

Что сделать

1. Откройте сессию к устройству или серверному ПК.
2. В OPC UA клиенте используйте virtual IP и порт OPC UA, обычно 4840.
3. Проверьте сертификаты клиента и сервера.
4. Если endpoint возвращает real IP, настройте endpoint/hostname на стороне OPC UA server.
5. Увеличьте таймауты при работе через сотовые сети.

Если не получилось

Gateway ID, virtual IP, endpoint OPC UA, порт, текст ошибки клиента и параметры сертификатов.

COM и RS-485: доступность и подготовка

Открыть статью в справке

Прозрачный удалённый COM-доступ проходит отдельную проверку совместимости. Наличие COM в тарифе не означает, что он уже доступен на любой модели шлюза или в публичной версии Manager. Для Link G2 используйте подтверждённые Ethernet-сценарии; последовательный доступ не следует настраивать по инструкции для LAN-устройства.

Что сделать

1. Уточните в поддержке доступность COM для вашей модели шлюза и версии Manager.

2. Сообщите модель оборудования, интерфейс RS-232/RS-485 и протокол обмена.

3. Подготовьте параметры порта: скорость, биты данных, чётность, стоповые биты и управление потоком.

4. Настраивайте удалённый COM только по инструкции для согласованной конфигурации.

Если не получилось

Сообщите модель устройства, параметры связи и код ошибки. Монтаж линии должен выполнять специалист объекта.

CODESYS через PLCLink

Открыть статью в справке

CODESYS может работать через PLCLink Manager как обычная TCP-сессия к устройству. Для старых ПЛК мониторинг может быть чувствителен к задержкам и поведению соединения, поэтому важно использовать правильный профиль и настройки CODESYS.

Что сделать

1. Откройте сессию к ПЛК.

2. В CODESYS используйте virtual IP устройства.

3. Проверьте порт CODESYS: 1200, 1217 или 11740-11743 в зависимости от устройства.

4. Для старых контроллеров оставьте штатный blocksize, если он требуется runtime.

5. Если мониторинг рвется, сравните с прямым подключением по белому IP или локальной сети.

Если не получилось

Gateway ID, модель ПЛК, порт, virtual IP, длительность до обрыва и close reason из Manager/relay.

Web-камеры и сервисные web-панели

Открыть статью в справке

Web-камеры, панели оператора и сервисные web-интерфейсы можно открывать через M2Web или через PLCLink Manager. Для постоянного видеостриминга PLCLink не является видеосервисом, но короткая диагностика web-камер возможна.

Что сделать

1. Для простой web-панели используйте M2Web.
2. Для сложного интерфейса или потока используйте PLCLink Manager.
3. Проверьте порт устройства.
4. Не оставляйте тяжелые видеопотоки надолго без необходимости.
5. Учитывайте тарифные лимиты и качество канала.

Если не получилось

Модель камеры/панели, IP, порт, схема http/https, нужен ли MJPEG/RTSP/WebSocket.

PLCLink Mobile

Привязка шлюза по QR-коду

Открыть статью в справке

Мобильный кабинет умеет считывать QR-код шлюза и отправлять заявку на привязку в выбранную компанию. Привязка проходит те же проверки выпуска Factory и прав пользователя, что и в настольном кабинете.

Что сделать

1. Откройте PLCLink Mobile.
2. Отсканируйте QR-код на лицевой панели шлюза.
3. Проверьте модель и Gateway ID.
4. Подтвердите привязку.
5. После привязки шлюз появится в кабинете PLCLink Cloud.

Если не получилось

Передайте Gateway ID, модель шлюза, аккаунт клиента и текст ошибки preview/activate.

Мобильный кабинет PLCLink PWA

Открыть статью в справке

На телефоне PLCLink использует отдельный мобильный кабинет по адресу cloud.plclink.ru/m/. Это веб-приложение, которое можно добавить на главный экран. Инженерные Windows-программы и их сессии запускаются через PLCLink Manager на компьютере.

Что сделать

1. Откройте /m/ в браузере телефона.
2. Войдите в аккаунт.
3. Выберите компанию и проверьте доступные шлюзы.
4. При желании добавьте страницу на главный экран через меню браузера.

Если не получилось

При проблеме укажите модель телефона, браузер, выбранную компанию и действие.

Безопасность

Роли пользователей и права

Открыть статью в справке

Права назначаются для каждой компании отдельно. Владелец, администратор, инженер, наблюдатель или сотрудник с особыми правами может видеть и выполнять только разрешённые действия в выбранной компании: работу со шлюзами, устройствами, командой, финансами, M2Web и инженерными сессиями.

Что сделать

1. Откройте раздел Команда.

2. Проверьте список участников.

3. Назначьте роль по задачам пользователя.

4. Инженеру достаточно прав просмотра и запуска сессий.

5. Управление финансами и командой оставляйте владельцу или администратору.

Если не получилось

Email пользователя, организация, текущая роль и какое действие недоступно.

Вход и добровольная двухфакторная защита

Открыть статью в справке

Для обычного входа нужны почта и пароль. Владелец аккаунта может добровольно включить одноразовые коды приложения-аутентификатора и сохранить резервные коды. Если защита включена, после проверки пароля откроется отдельный экран второго фактора.

Что сделать

1. Войдите по почте и паролю.

2. Если включена двухфакторная защита, введите код приложения или резервный код.

3. Настроить или отключить защиту можно в настройках безопасности аккаунта после входа.

Если не получилось

При потере приложения и резервных кодов обратитесь в поддержку для проверки владельца аккаунта.

Восстановление пароля

Открыть статью в справке

Если пароль забыт, используйте ссылку восстановления на странице входа. Ссылка для сброса отправляется на почту учётной записи. Действующая двухфакторная защита после смены пароля продолжает защищать вход.

Что сделать

1. На странице входа нажмите «Забыли пароль?».

2. Укажите почту аккаунта.

3. Откройте письмо и задайте новый пароль.

4. Войдите снова; при включённой 2FA подтвердите второй фактор.

Если не получилось

Если доступа к почте нет, сообщите поддержке адрес аккаунта; не отправляйте старые пароли.

Роли сотрудников и доступ к объектам

Открыть статью в справке

Права сотрудника действуют только в выбранной компании. На Стандарте используются готовые роли, а на Pro можно ограничивать отдельные действия и доступ к шлюзам или группам. Гостевой доступ Pro имеет дату окончания, максимум 365 дней; после окончания доступ прекращается.

Что сделать

1. Выберите компанию и откройте «Команда».

2. Откройте участника и назначьте роль по его задачам.

3. На Pro при необходимости ограничьте шлюзы, группы и отдельные действия. Для гостя задайте срок доступа.

4. Сохраните и проверьте разрешения с сотрудником.

5. Если сотрудник не видит объект, сначала проверьте выбранную компанию и выданные права.

Если не получилось

При неверной видимости укажите компанию, роль и действие; не передавайте пароли сотрудников.

Безопасность activation code и токенов

Открыть статью в справке

Код активации позволяет привязать выпущенный шлюз к компании. Его нельзя публиковать в открытых чатах или на скриншотах. Полные API-токены, cookies и служебные ключи не передавайте в обычном обращении поддержки.

Что сделать

1. Храните activation code вместе с документами шлюза.
2. Не отправляйте полный код в открытых каналах.
3. При обращении достаточно Gateway ID и описания проблемы.
4. Если код скомпрометирован, обратитесь в поддержку для проверки привязки.
5. Для сервисных операций используйте защищенный канал.

Если не получилось

Gateway ID, аккаунт, признаки компрометации, кто имел доступ к коду.

API-токены для интеграций

Открыть статью в справке

API-токены доступны на Pro и дают программный доступ только в пределах предоставленных прав. Создавайте отдельный токен для каждой интеграции, храните его как пароль и отзывайте, когда он больше не нужен. Перед переходом на младший тариф активные токены необходимо отозвать. Не вставляйте секреты в публичные скрипты или обращения поддержки.

Что сделать

1. Откройте настройки аккаунта и раздел API-токенов.
2. Создайте токен для конкретной интеграции.
3. Сохраните секрет в защищённом хранилище.
4. При подозрении на утечку удалите токен и выпустите новый.

Если не получилось

Для диагностики достаточно названия интеграции и времени ошибки; значение токена не отправляйте.

Персональные данные и удаление аккаунта

Открыть статью в справке

Контактные данные аккаунта используются для входа и связи по работе сервиса. Управление согласиями и запросом на удаление доступно в предусмотренных настройках аккаунта. Удаление может затронуть доступ к компаниям и их объектам.

Что сделать

1. Откройте настройки аккаунта и проверьте контакты и согласия.
2. При необходимости запросите удаление через доступный сценарий.
3. Перед удалением убедитесь, что у компании остаётся другой уполномоченный владелец.
4. Если сценарий недоступен, обратитесь в поддержку.

Если не получилось

Укажите почту аккаунта и запрос; не отправляйте пароль или код подтверждения.

Журнал действий и обращение в поддержку

Открыть статью в справке

Журнал помогает установить, кто и когда менял объекты или запускал операции в выбранной компании. Если статья не решила проблему, создайте обращение в поддержку с техническим контекстом. Секреты, пароли и полный код активации в открытом тексте не отправляйте.

Что сделать

1. Выберите компанию и найдите время события в «Журнале».
2. Запишите Gateway ID, устройство, действие и результат.
3. Откройте «Поддержка» и создайте обращение.
4. Приложите допустимые скриншоты и логи без секретов.

Если не получилось

Если кабинет недоступен, используйте опубликованные на сайте контакты поддержки.

Диагностика

Шлюз онлайн, а устройство или M2Web не открывается

Открыть статью в справке

Статус шлюза «В сети» подтверждает связь шлюза с PLCLink, но не доказывает доступность конкретного устройства в его LAN. Проверяйте IP, подсеть, порт, протокол и права сотрудника отдельно.

Что сделать

1. Проверьте выбранную компанию и право доступа.
2. В карточке шлюза проверьте реальный IP устройства и статус проверки.
3. Сверьте LAN IP и маску шлюза с сетью оборудования.
4. Для M2Web проверьте HTTP/HTTPS и порт; для Manager — активную сессию и virtual IP.
5. Повторите попытку и запишите точное время.

Если не получилось

Передайте Gateway ID, IP и порт устройства, способ доступа, время и текст ошибки.

M2Web не открывает страницу

Открыть статью в справке

Сообщение о неудачном подключении M2Web означает, что веб-сервис не ответил на выбранный запрос. Причиной может быть неверный порт, HTTP вместо HTTPS, выключенный веб-сервер, запрет доступа или проблема связи. Это не доказательство физического отключения ПЛК.

Что сделать

1. Проверьте компанию, права сотрудника и разрешение доступа к устройству.
2. Проверьте связь шлюза с PLCLink и реальный IP устройства.
3. Сверьте протокол и порт с настройками веб-сервера: 80, 443 и 8080 — только распространённые примеры.
4. Если есть доступ на объект, проверьте тот же адрес и порт локально.
5. Повторите попытку и запишите время, выбранные параметры и точный текст ошибки.

Если не получилось

Gateway ID, device ID/name, real IP, порт, схема http/https, URL M2Web и скриншот ошибки.

Сессия Modbus TCP / OPC UA / CODESYS периодически рвется

Открыть статью в справке

Периодические обрывы могут быть вызваны задержками канала, таймаутами инженерного ПО, поведением ПЛК, потерей связи шлюза или рестартом transport-соединения. PLCLink закрывает зависшие сессии и должен позволять открыть новую сессию.

Что сделать

1. Проверьте, не потерял ли шлюз связь.
2. Увеличьте timeout в OPC/SCADA/CODESYS, если канал удаленный или сотовый.
3. Снизьте частоту опроса, если идет постоянный обмен.
4. Проверьте журнал Manager: close reason, session_id, длительность.
5. Сравните с прямым подключением, если возможно.
6. Если обрыв повторяется стабильно, передайте логи в поддержку.

Если не получилось

Gateway ID, устройство, протокол, порт, session_id, close reason, длительность до обрыва, логи Manager и OPC/SCADA.

SCADA/OPC периодически показывает ошибки обмена

Открыть статью в справке

Удаленный канал может иметь задержки выше локальной сети. Если OPC server или SCADA настроены на короткие таймауты и частый опрос, могут появляться сообщения вроде 'нет ответа' или 'ответ не соответствует запросу'.

Что сделать

1. Увеличьте timeout ответа устройства.
2. Увеличьте интервал опроса тегов.
3. Уменьшите количество одновременных запросов.
4. Проверьте качество канала и сигнал, если используется сотовая связь.
5. Проверьте, что в момент ошибок не запускается сканирование LAN.
6. Сравните стабильность с локальным подключением.

Если не получилось

Лог OPC/SCADA, Gateway ID, период опроса, timeout, число тегов, протокол и время ошибок.

Когда передавать проблему в поддержку

Открыть статью в справке

Обратитесь в поддержку, если инструкция не решила проблему, возникает повторяющаяся ошибка или требуется помощь с оплатой и доступом. Опишите ожидаемый и фактический результат: это полезнее общего сообщения «не работает».

Что сделать

1. Выберите компанию и откройте «Поддержка».

2. Опишите проблему и уже выполненные проверки.

3. Для связи с оборудованием укажите идентификатор шлюза, IP устройства, протокол, порт и точное время попытки.

4. Приложите скриншот ошибки или журнал Manager, если он есть.

5. Не включайте пароли, коды активации и токены.

Если не получилось

Если вход в кабинет недоступен, используйте контакт поддержки, указанный на странице входа или в документах вашего заказа.

FAQ

Группы объектов

Открыть статью в справке

Группы помогают объединять шлюзы по площадкам, городам, сервисным зонам или объектам. Удаление группы не удаляет шлюзы: они переходят в Без группы.

Что сделать

1. Нажмите Создать группу.
2. Укажите название, например город или объект.
3. При добавлении или изменении шлюза выберите группу.
4. Чтобы изменить группу, откройте Изменить.
5. Чтобы удалить группу, используйте действие внутри формы изменения.

Если не получилось

Если шлюз оказался не в той группе, укажите Gateway ID, старую группу и новую группу.

LAN-устройства за шлюзом

Открыть статью в справке

LAN-устройство - любое оборудование за шлюзом: ПЛК, HMI, камера, серверный ПК, Raspberry, OPC UA server или другое Ethernet-устройство. Устройство можно найти автоматическим обновлением списка или добавить вручную.

Что сделать

1. Раскройте шлюз в кабинете.
2. Нажмите Обновить список устройств.
3. Если устройство не найдено, нажмите Добавить вручную.
4. Укажите имя, real IP и параметры доступа.
5. Проверьте статус доступности после обновления.

Если не получилось

Передайте Gateway ID, real IP, имя устройства, известно ли устройство по ping/ARP и какой порт нужен.

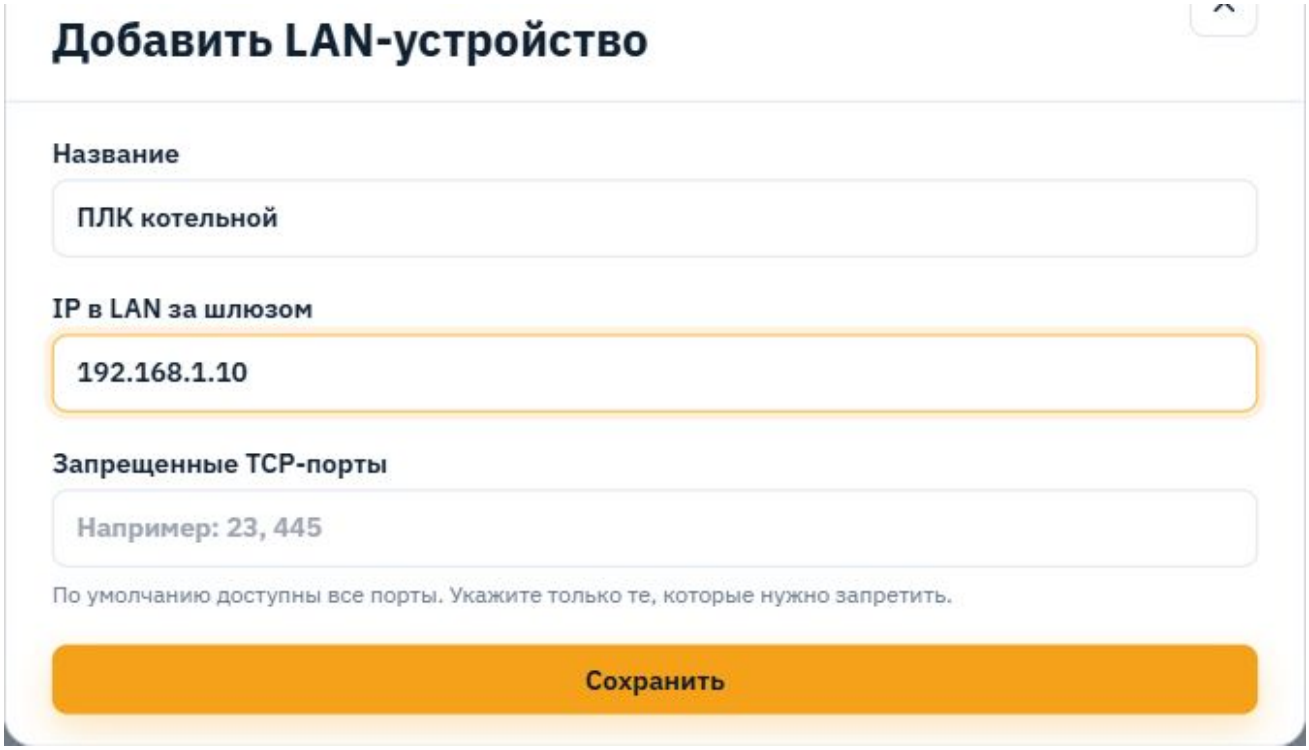
Как добавить LAN-устройство вручную

Открыть статью в справке

Добавление LAN-устройства создаёт в кабинете запись о ПЛК, панели или другом оборудовании за шлюзом. Эта операция не меняет IP самого оборудования и не включает его веб-сервер. Сначала выясните адрес устройства и подключите его к LAN шлюза.

1. Найдите нужный шлюз

Выберите компанию и откройте «Шлюзы». Разверните карточку объекта стрелкой слева. В блоке «Устройства за шлюзом» нажмите «Добавить вручную». Убедитесь, что работаете с нужным объектом: одинаковые адреса ПЛК могут встречаться на разных площадках.



Добавление ПЛК: укажите понятное название и реальный LAN IP. Поле запрещённых портов можно оставить пустым.

2. Укажите имя и реальный IP

В поле «Название» введите, например, «ПЛК котельной». В поле «IP» укажите адрес контроллера в сети объекта, например 192.168.1.10. Не вводите сюда адрес шлюза, внешний IP объекта или виртуальный IP из Manager.

Для ПЛК 192.168.1.10/24 LAN шлюза может иметь свободный адрес 192.168.1.1/24. Если эти подсети не согласованы, создание записи в кабинете само по себе проблему не исправит. Настройки сети разбираются в статье «Настройка LAN/WAN шлюза».

3. Разберитесь с полем запрещённых портов

Это список ЗАПРЕЩЁННЫХ TCP-портов. Если ограничений не требуется, оставьте его пустым: в этой форме пустое поле означает, что TCP-порты не запрещены данным списком. Не вписывайте 502 или 1200, чтобы «разрешить Modbus или CODESYS»: вы получите обратный результат и заблокируете указанные порты.

Если нужно запретить конкретные сервисы, укажите их порты через запятую, например 23,445. Итоговый доступ также зависит от прав сотрудника и остальных правил компании. Эта форма не отменяет ограничения, настроенные в других местах.

4. Сохраните и проверьте устройство

Нажмите «Сохранить». В списке появится строка с именем и IP. Наличие строки означает, что запись создана; доступность подтверждается отдельно. «Нет свежих данных» — отсутствие актуальной проверки, а не доказательство отключённого кабеля.

Для веб-интерфейса выберите протокол и порт в этой строке, затем кнопку с глобусом. Для инженерной программы откройте сессию в Manager и используйте выданный виртуальный IP. Если соединения нет, сначала проверьте реальный IP и порт службы, затем настройки LAN и кабель на объекте.

Если не получилось

Gateway ID, имя устройства, real IP, virtual IP, порт/протокол, результат обновления списка устройств.

Обновление списка устройств

Открыть статью в справке

Обновление списка устройств отправляет команду агенту на шлюзе. Агент проверяет устройства в LAN и возвращает найденные адреса. Устройства, которые пользователь удалил вручную, автоматически не возвращаются в список.

Что сделать

1. Раскройте шлюз.

2. Нажмите Обновить список устройств.

3. Дождитесь завершения проверки.

4. Если найденные устройства появились, проверьте имена и доступ.

5. Если нужного устройства нет, добавьте его вручную.

Если не получилось

Если список не обновляется, передайте Gateway ID, время нажатия, ожидаемый IP устройства и известно ли устройство в ARP/ping на объекте.

Устройство удалили, но потом добавили снова

Открыть статью в справке

При удалении устройства его запись скрывается, а история сохраняется. Если вернуть тот же реальный IP за тем же шлюзом, система может восстановить существующую запись и виртуальный адрес. После восстановления обязательно проверьте название, адрес и права: по этому IP на объекте уже может находиться другое оборудование.

Что сделать

1. Откройте форму изменения нужного устройства и удалите запись, если доступ больше не нужен.

2. Чтобы вернуть устройство, добавьте его реальный IP через «Добавить вручную».

3. Проверьте название, виртуальный IP и разрешённые порты.

4. Откройте новую сессию и убедитесь, что отвечает нужное оборудование.

Если не получилось

Передайте Gateway ID, real IP, прежний virtual IP и время удаления/восстановления.