Руководство по установке Clearway CA 26.3.0 с помощью инсталлятора

Документация Clearway CA

6 November, 2026

Table of Contents

1 Введение ... 6
1.1 Установка пакета в Linux ... 6
1.2 Запуск и открытие веб-интерфейса ... 6
1.3 Остановка и повторный запуск ... 7
1.4 Режим командной строки ... 7
2 Чек-лист перед установкой Clearway CA 2026.3 ... 8
2.1 Серверы и доступ ... 8
2.2 Данные для заполнения мастера ... 8
2.3 Дополнительные условия ... 8
2.4 Проверка в графическом инсталляторе ... 9
3 Архитектура и порядок развёртывания ... 10
4 Требования и подготовка ... 12
4.1 Операционная система и ресурсы ... 12
4.2 Имена, подключения и учётные записи ... 13
4.3 Программные зависимости ... 13
4.4 Сетевые соединения ... 13
5 Работа с мастером ... 15
6 Общие параметры и значения по умолчанию ... 18
7 Проверка пререквизитов ... 19
8 Быстрая установка ... 21
8.1 Сервер ... 21
8.2 Сбор данных ... 21
8.3 База данных ... 22
8.4 Аутентификация ... 22
8.5 Проверка и результат ... 25
9 Центр сертификации ... 26
9.1 Сервер ... 26
9.2 Сбор данных ... 26
9.3 Точка распространения ... 27

9.4 База данных ... 28
9.5 Проверка и результат ... 29
9.6 Файлы и службы ... 30
9.7 Выпуск сертификата выдающего ЦС ... 30
9.8 Настройка выдающего ЦС ... 31
9.9 Сбор данных ... 31
9.10 Точка распространения ... 31
10 Аутентификация (OpenID) ... 33
10.1 Сервер ... 33
10.2 Сбор данных ... 33
10.3 ЦС ... 33
10.4 База данных ... 34
10.5 Статическая учётная запись ... 35
10.6 Настройка токена ... 35
10.7 Интеграция с LDAP ... 36
10.8 Проверка и результат ... 38
10.9 Файлы и службы ... 39
10.10 Подключение по LDAPS и права групп ... 39
11 MS-WSTEP ... 41
11.1 Сервер ... 41
11.2 Сбор данных ... 41
11.3 ЦС ... 42
11.4 LDAP ... 42
11.5 Учетная запись MS-WSTEP ... 43
11.6 Учетная запись Kerberos ... 43
11.7 Проверка и результат ... 44
11.8 Файлы и службы ... 44
11.9 Kerberos и HTTP-служба ... 45
11.10 Получение политики и сертификата на Windows ... 46
12 Контрольная панель ... 48
12.1 Сервер ... 48
12.2 Сбор данных ... 48

12.3 ЦС 49
12.4 Аутентификация 50
12.5 Проверка и результат 51
12.6 Файлы и службы 52
12.7 Доверие к сертификатам перед первым входом 52
13 Сервис публикации 54
13.1 Сервер 54
13.2 Проверка и результат 54
13.3 Файлы и службы 55
14 OCSP 56
14.1 Сервер 56
14.2 Сбор данных 56
14.3 ЦС 56
14.4 База данных 57
14.5 Проверка и результат 58
14.6 Файлы и службы 58
15 Архиватор 59
15.1 Сервер 59
15.2 База данных 59
15.3 Архивная база данных 60
15.4 Проверка и результат 61
15.5 Файлы и службы 62
16 SCEP 63
16.1 Сервер 63
16.2 Сбор данных 63
16.3 ЦС 63
16.4 База данных 64
16.5 Аутентификация 65
16.6 Проверка и результат 66
16.7 Файлы и службы 66
17 Точки распространения CRL и сертификатов 68
18 Резервное копирование 69

18.1 Сервер 69
18.2 Проверка и результат 69
18.3 Файлы и службы 70
18.4 Проверка состава и первый запуск копирования 70
19 Обновление установленного компонента 72
20 Обработка ошибок и проверка служб 73
21 История развёртываний 75
22 Дополнительные компоненты 76
22.1 Выпуск JWT 76
22.2 Тестовые данные 77
23 Проверка установленного комплекса 79
23.1 Вход и соединение с ЦС 79
23.2 Выпуск и отзыв сертификата 79
23.3 OCSP и публикация списков отзыва 80
23.4 SCEP и резервная копия 80
24 Обновление Clearway CA до 2026.3.0 81
24.1 Шаги обновления 81
24.2 Обновление без инсталлятора 81

1 Введение

Руководство описывает установку Clearway CA с помощью инсталлятора. Оно предназначено для администратора, который подготавливает серверы, задаёт параметры компонентов и проверяет результат развёртывания.

Инсталлятор запускается на рабочем месте оператора и подключается к целевым серверам Linux по SSH. Его веб-интерфейс работает в браузере. Компоненты могут находиться на одном сервере или на нескольких серверах в соответствии с выбранным сценарием.

1.1 Установка пакета в Linux

На рабочем месте оператора нужны Linux, права sudo и браузер. Скопируйте полученный DEB-пакет в отдельный каталог и откройте в нём терминал.

```
sudo apt-get install ./clearway-ca-installer_<версия>_amd64.deb
```

Замените <версия> на версию полученного файла. Дождитесь завершения установки. Проверьте, что пакет зарегистрирован и команда запуска доступна:

```
dpkg-query -W clearway-ca-installer
command -v itc-installer
```

Вторая команда должна вывести /usr/bin/itc-installer. Пакет содержит среду выполнения инсталлятора, поэтому отдельно устанавливать .NET для его запуска не требуется.

1.2 Запуск и открытие веб-интерфейса

```
itc-installer
```

Запускайте приложение от обычной учётной записи. Оставьте терминал открытым. Строка Application started и сообщение о прослушивании порта 5224 подтверждают запуск. На том же рабочем месте откройте адрес:

```
https://localhost:5224/installer
```

Адрес localhost указывает на компьютер, где открыт браузер. Если инсталлятор работает в виртуальной машине, откройте браузер внутри неё. При предупреждении о самоподписанном сертификате проверьте адрес и сертификат перед переходом к приложению.

Если лицензионное соглашение ещё не принято, ознакомьтесь с ним. При согласии установите флажок «Я принимаю условия лицензионного соглашения» и нажмите «Принимаю». После принятия откроется выбор компонента; адрес страницы изменится на /deploy.

1.3 Остановка и повторный запуск

Для остановки нажмите Ctrl+C в терминале инсталлятора. Для повторного запуска выполните itc-installer от той же учётной записи. Служебная база deployer.db и журнал находятся в ~/.local/share/itc-installer.

1.4 Режим командной строки

Для запуска консольного мастера выполните itc-installer cli в интерактивном терминале.

2 Чек-лист перед установкой Clearway CA 2026.3

2.1 Серверы и доступ

- [ ] Определены состав компонентов и серверы, на которых они будут размещены.
- [ ] Версии ОС и ресурсы серверов соответствуют разделу «Требования к программному и аппаратному обеспечению».
- [ ] На серверах предусмотрено свободное место для баз данных, журналов и резервных копий.
- [ ] Время на серверах синхронизировано.
- [ ] Назначены DNS-имена сервисов. Проверено их разрешение с рабочего места установки, серверов и клиентских устройств.
- [ ] С рабочего места установки проверено подключение по SSH к каждому целевому серверу. Учётные записи подключения имеют права sudo.
- [ ] Настроены сетевые соединения по таблице портов для выбранных компонентов. Порты размещаемых сервисов не заняты посторонними приложениями.
- [ ] Серверы имеют доступ к репозиториям, необходимым для установки зависимостей, либо зависимости установлены заранее.

2.2 Данные для заполнения мастера

- [ ] Подготовлены имена и адреса серверов, реквизиты SSH-подключения.
- [ ] Определены имя и тип ЦС, данные владельца сертификата и алгоритм ключа.
- [ ] Определены технологическая учётная запись и каталоги установки. При использовании стандартных значений: itc-svc и /opt/itc.
- [ ] Выбрано размещение баз данных. Подготовлены имена БД, учётных записей и пароли для устанавливаемых компонентов.
- [ ] Выбран способ аутентификации. Подготовлены реквизиты администратора и адрес электронной почты, запрашиваемые мастером.

2.3 Дополнительные условия

- [ ] Для выдающего ЦС: согласован порядок подписания запроса вышестоящим ЦС и получения сертификата и цепочки доверия.
- [ ] Для существующего PostgreSQL: проверены совместимость версии, подключение с серверов компонентов и права учётных записей на используемые БД.
- [ ] Для подключения к PostgreSQL по TLS: подготовлены сертификаты и параметры проверки доверия и имени сервера.
- [ ] Для внешнего провайдера аутентификации: подготовлены адрес издателя и параметры клиента.

- [ ] Для LDAP/Active Directory: подготовлены адреса серверов каталога, параметры поиска пользователей и реквизиты подключения.
- [ ] Для MS-WSTEP: подготовлены домен Active Directory и учётная запись с правом ввода сервера в домен.

2.4 Проверка в графическом инсталляторе

- [ ] Установлен инсталлятор нужной версии. В браузере на рабочем месте установки открывается https://localhost:5224/installer.
- [ ] Принято лицензионное соглашение и выбран нужный сценарий установки.
- [ ] Проверены введённые параметры, включая автоматически подставленные значения.
- [ ] Для устанавливаемого компонента завершена проверка пререквизитов. Недостающие зависимости настроены, обязательные проверки имеют статус «Проверено», кнопка «Выполнить развёртывание» доступна.

3 Архитектура и порядок развёртывания

Компонент	Назначение
Центр сертификации	Корневой ЦС создаёт корень доверия. Выдающий ЦС получает сертификат от вышестоящего ЦС и выпускает сертификаты конечных субъектов.
Аутентификация (OpenID)	Обеспечивает вход в веб-сервисы по встроенной учётной записи или через LDAP/Active Directory.
Контрольная панель	Предоставляет веб-интерфейс управления ЦС и вспомогательными сервисами.
Сервис публикации	Публикует сертификаты и списки отзыва по заданиям, настроенным в контрольной панели.
OCSP	Возвращает статус сертификата по данным БД ЦС и подписывает ответ сертификатом OCSP.
Архиватор	Переносит устаревшие записи из рабочей БД ЦС в архивную БД.
Резервное копирование	Создаёт резервные копии узлов и БД ЦС. Задания настраиваются в контрольной панели.
SCEP	Обрабатывает запросы на выпуск сертификатов от устройств и клиентов SCEP.
MS-WSTEP	Предоставляет службы CEP/CES для доменных Windows-клиентов с аутентификацией Kerberos.
Точка распространения (CDP/AIA)	Публикует списки отзыва и сертификаты ЦС по HTTP. Настраивается в сценарии ЦС.

Для установки всех сервисов на одном сервере используйте «Быстрая установка». Сценарий создаёт корневой ЦС, OpenID, контрольную панель, публикацию, SCEP, OCSP, архиватор и резервное копирование. MS-WSTEP в него не входит.

Для раздельного размещения включите «Расширенная установка». Сначала разверните ЦС. Если нужна иерархия, подготовьте корневой ЦС, затем выдающий и завершите его настройку. После этого установите OpenID и контрольную панель. Публикация и резервное копирование устанавливаются на сервер контрольной панели. Остальные сервисы подключаются к готовому ЦС.

Корневой и выдающий ЦС размещайте на разных серверах: их стандартные каталоги и служба minica.service совпадают. Совместное размещение веб-сервисов должно учитывать существующую конфигурацию Nginx, имена и занятые порты.

4 Требования и подготовка

4.1 Операционная система и ресурсы

Серверные компоненты устанавливаются в Linux. Для работы по этому руководству используйте поддерживаемый дистрибутив с доступом к его пакетным репозиториям.

Дистрибутив из требований поставки	Редакция и совместимость
Astra Linux	1.7.5.9 и 1.8.1.6
Linux Server	24.04.03
ОС Альт	11.0, несертифицированная; 10.2.2, сертифицированная, с ограничениями и правами sudo.
РЕД ОС	8.0.2
Debian	Совместимость ограничена, нужны права sudo.

Вариант из требований к продукту	Ресурсы и нагрузка
Минимальный единый сервер	4 vCPU, 4 ГБ RAM, 256 ГБ диска; до 100 сертификатов в сутки.
Базовый единый сервер	4 vCPU, 8 ГБ RAM, 512 ГБ диска; до 5000 сертификатов в сутки.
ЦС при раздельном размещении	2 vCPU, 2 ГБ RAM, 80 ГБ диска.
OpenID при раздельном размещении	2 vCPU, 2 ГБ RAM, 40 ГБ диска.
Вспомогательные сервисы	2 vCPU, 4 ГБ RAM, 40 ГБ диска. Учитывайте объём журналов, архивной БД и резервных копий.

Подготовьте место для роста баз данных и журналов. Объём резервных копий зависит от состава и срока хранения заданий. Синхронизируйте время на всех серверах и клиентах; проверка времени запросов ЦС использует параметр max-dt-sec.

4.2 Имена, подключения и учётные записи

Назначьте сервисам постоянные DNS-имена. Имена, введённые в поля Alias или «Имя сервера», попадут в сертификаты и адреса клиентов. Проверьте разрешение этих имён с рабочего места оператора, целевых серверов и клиентских устройств.

Для подключения инсталлятора подготовьте SSH-учётные записи с правами sudo.

По умолчанию службы работают от itc-svc. Инсталлятор создаёт технологическую учётную запись, назначает владельца каталогов и включает linger для пользовательских служб systemd. Не заменяйте её учётной записью root.

4.3 Программные зависимости

Мастер проверяет и при необходимости устанавливает PostgreSQL, Nginx, OpenSSL, ГОСТ-движок OpenSSL, jq и другие зависимости выбранного компонента. Для резервного копирования нужны pg_dump и pg_restore. Для MS-WSTEP дополнительно требуются средства LDAP, Kerberos и ввода сервера в домен.

Версию PostgreSQL мастер выбирает из доступных поддерживаемых пакетов. При существующей БД проверьте совместимость сервера и клиентских утилит.

4.4 Сетевые соединения

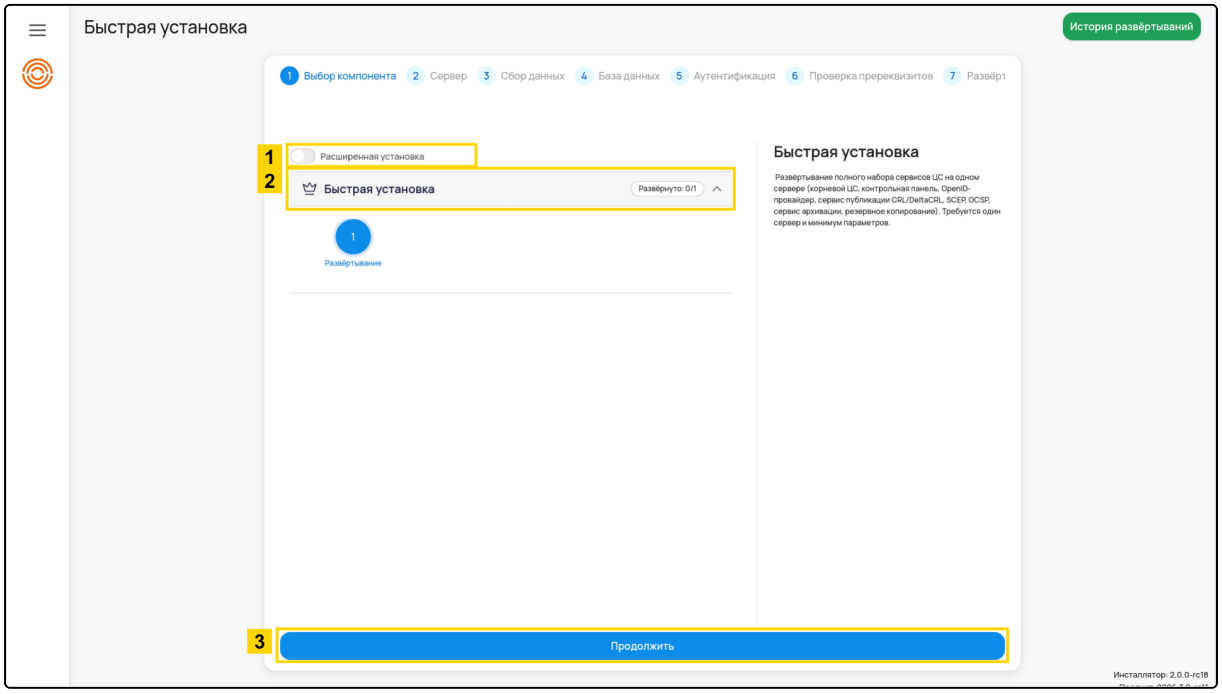
Соединение	Назначение
Рабочее место оператора → серверы, TCP 22	SSH для установки, настройки и передачи файлов.
Браузер → локальный инсталлятор, TCP 5224	Веб-интерфейс мастера по HTTPS.
Клиенты → веб-сервисы, TCP 443	Контрольная панель, OpenID, SCEP и MS-WSTEP через Nginx.
Клиенты → CDP/AIA, TCP 80	Получение сертификатов и списков отзыва.
Сервисы → ЦС, TCP 9443	Защищённое подключение к API ЦС. HTTP-интерфейс ЦС использует TCP 9080; доступ к нему задаётся принятой схемой размещения.
Сервисы → PostgreSQL, TCP 5432	Подключение к рабочей, служебным и архивной БД.
Клиенты → OCSP, TCP 8888	Запрос статуса сертификата по адресу /ocsp.

Соединение	Назначение
OpenID и MS-WSTEP → каталог	Разрешите DNS, LDAP и Kerberos в соответствии с настройками домена и используемым транспортом.

Внутренние порты приложений, опубликованных через Nginx, не нужно открывать всем клиентам. Правила доступа к PostgreSQL ограничьте адресами подключающихся сервисов. Требования к защищённому соединению с БД и настройке pg_hba.conf определите до ввода системы в эксплуатацию.

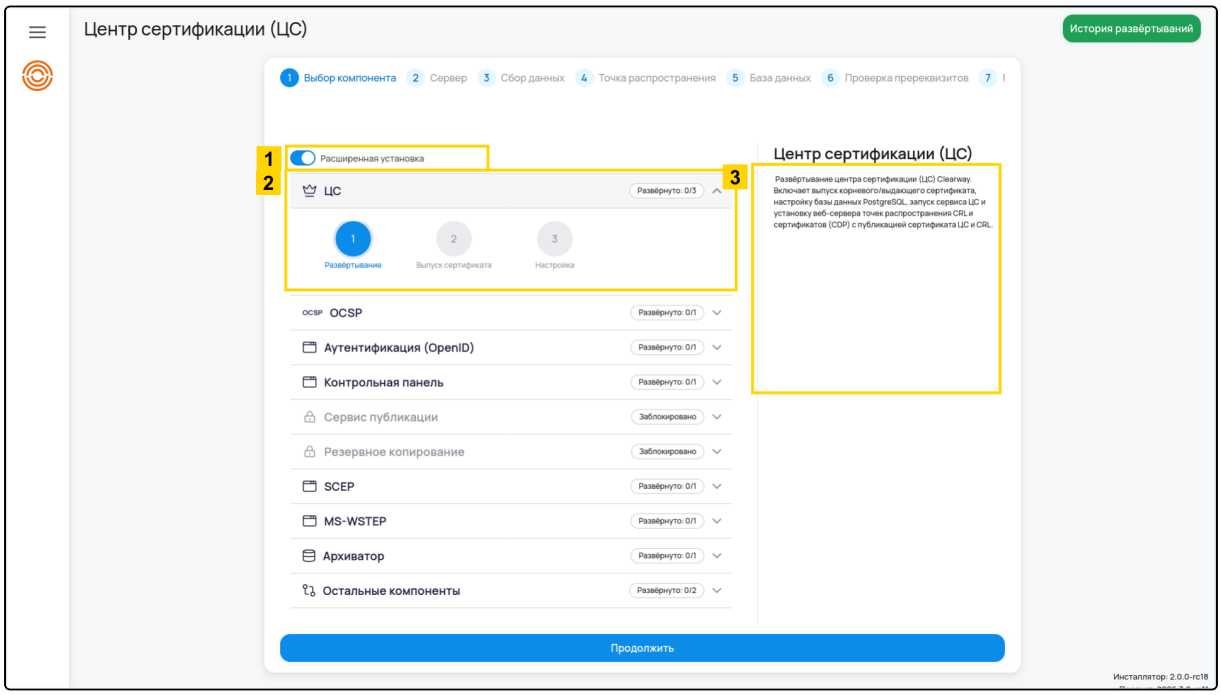
5 Работа с мастером

Главная страница показывает быстрый сценарий. Переключатель «Расширенная установка» открывает отдельные группы. Выберите группу и компонент, прочитайте описание справа и нажмите «Продолжить». Верхняя строка показывает этапы выбранного компонента.



1 Рисунок 1. Выбор быстрого сценария.

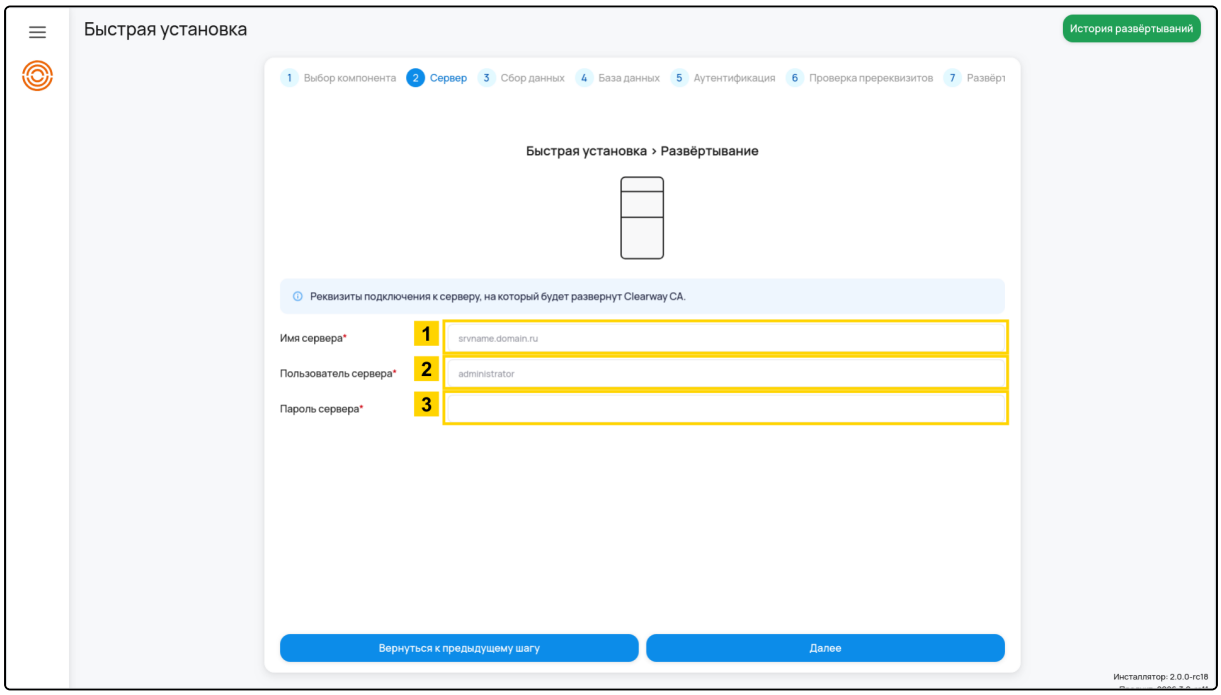
1. Переключатель открывает отдельные группы установки.
2. Выбранный сценарий и его состав.
3. Кнопка перехода к параметрам сервера.



2 Рисунок 2. Группы расширенной установки.

1. Включён режим расширенной установки.
2. Группа «ЦС» объединяет развёртывание, выпуск сертификата и настройку.
3. Описание выбранной группы помогает проверить её назначение.

На этапе «Сервер» введите имя узла, пользователя и пароль. Мастер проверит подключение, определит сведения об ОС и доступные параметры. В последующих формах заполните поля со звёздочкой. Переключатель «Расширенные настройки» показывает дополнительные значения, например технологическую учётную запись и каталог установки.



3 Рисунок 3. Реквизиты подключения к серверу.

1. Имя сервера, доступного с рабочего места оператора.
2. Учётная запись с правами sudo.
3. Пароль этой учётной записи.

Поле «Внешний ЦС» означает ЦС на другом сервере. Оно не обозначает сторонний продукт: встроенный сценарий выпуска сертификатов использует установленный Clearway CA и утилиту mclient. При включении переключателя заполните реквизиты дополнительного SSH-подключения.

Аналогично, переключатели внешней БД и внешней точки распространения открывают параметры соответствующих серверов. Не путайте SSH-учётную запись операционной системы и учётную запись PostgreSQL.

Результаты предыдущих компонентов могут подставляться в следующую форму. Проверьте их перед продолжением, особенно если меняете сервер или работаете в новом сеансе. Для возврата используйте «Вернуться к предыдущему шагу».

Пропуск доступен только там, где он предусмотрен сценарием. Для выдающего ЦС можно пропустить встроенный выпуск сертификата, если его подписывает внешний корневой ЦС. Запрос нужно передать на подпись отдельно, а полученный сертификат загрузить на этапе настройки.

6 Общие параметры и значения по умолчанию

Параметр	Значение и источник
Имя сервера для SSH	FQDN или IP-адрес из плана размещения. Используется для подключения инсталлятора.
Alias / имя сервиса	DNS-имя для клиентов и сертификата. Если подставлено имя ОС, проверьте его пригодность для клиентского доступа.
Технологическая учётная запись	itc-svc. Должна владеть каталогами и пользовательскими службами.
Каталог сервисов	/opt/itc. Отдельный ЦС: /opt/itc/minica; OCSP: /opt/itc/ocsp.
Каталог CDP/AIA	/opt/itc/web; внутри создаются cdp и aia.
Учётная запись и БД ЦС	cwi-ca. Пароль задайте при создании БД или возьмите действующий для существующей БД.
Учётная запись и БД OpenID	cwi-openid. Пароль задаётся отдельно от БД ЦС.
Учётная запись и БД SCEP	cwi-scep. Сервис использует PostgreSQL.
Архивная БД	База cwi-ca-archive, учётная запись cwi-ca-archiver.
Subject сертификата ЦС	По умолчанию CN=RootCA,O=Company,C=RU. Замените атрибуты на данные своей организации.
Статическая учётная запись	Email используется как логин; пароль задаётся при установке OpenID.
Адрес издателя OpenID	https://<имя-сервера>/openid. Укажите этот же адрес в клиентах.

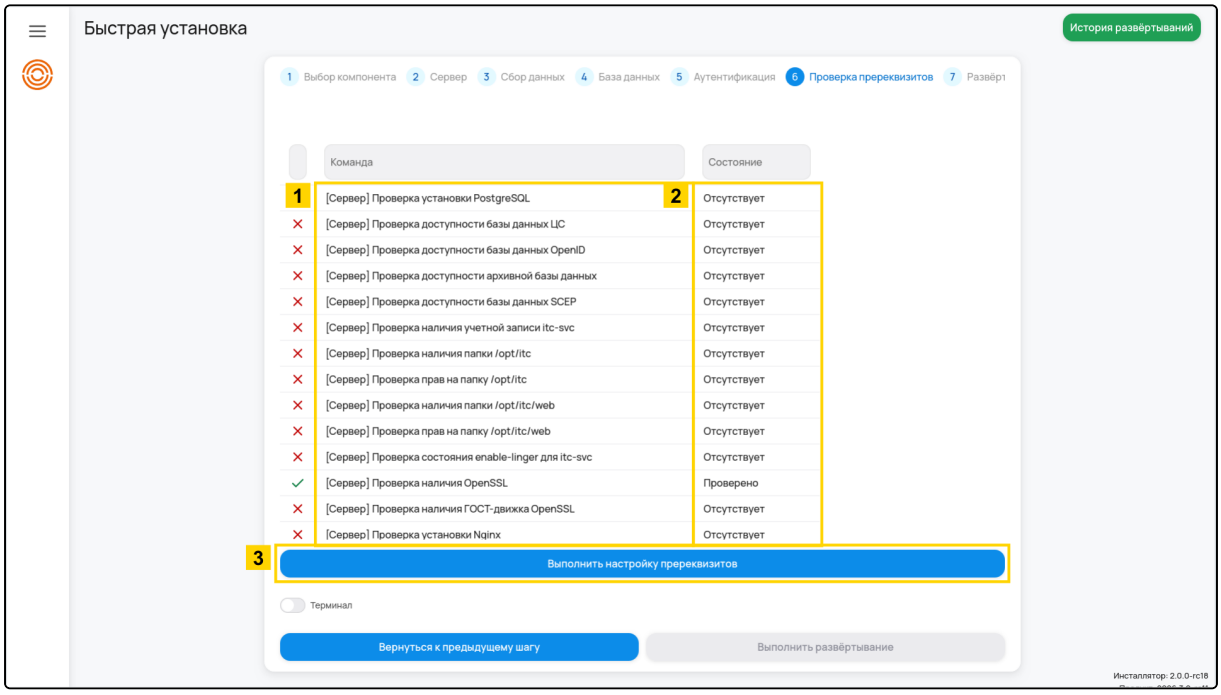
Значения по умолчанию сокращают объём ввода, но не заменяют согласование имён, паролей и адресов. Для существующей системы используйте её фактические значения. Пути ниже приведены для стандартного каталога установки.

В полях паролей создаваемых учётных записей PostgreSQL одинарная кавычка недопустима. Это ограничение формы относится к БД ЦС, OpenID, SCEP и архивной БД.

7 Проверка пререквизитов

Перед развёртыванием мастер проверяет серверы и зависимости. Состав проверок зависит от компонента и выбранного размещения. В таблице отображаются команда и состояние.

Состояние	Что означает
Ожидание	Проверка ещё не выполнена.
В процессе	Проверка или настройка выполняется. Дождитесь окончания.
Проверено	Условие выполнено.
Отсутствует	Условие не выполнено; может потребоваться настройка.



4 Рисунок 4. Проверка готовности сервера.

1. Список проверяемых условий.
2. Состояние каждой проверки.
3. Автоматическая настройка недостающих зависимостей.

Если доступна кнопка «Выполнить настройку пререквизитов», нажмите её и дождитесь завершения. Мастер может установить пакеты, создать пользователя и БД, назначить права и подготовить systemd. После успешных проверок становится доступно «Выполнить развёртывание».

Переключатель «Терминал» показывает журнал команд. Если прогресс остановился, сначала проверьте, выполняется ли команда на сервере. Не запускайте параллельно второй менеджер пакетов. Если требуется ручной ввод, дождитесь завершения или остановки текущей команды, затем выполните необходимое действие по SSH и повторите проверку.

Если браузер перестал получать обновления, проверьте связь с процессом инсталлятора и состояние операции в истории. Обновление страницы само по себе не означает, что операция на сервере остановилась. Не повторяйте развёртывание, пока не установлено состояние предыдущей операции.

8 Быстрая установка

Этот сценарий разворачивает основные сервисы на одном сервере. Подготовьте сервер, DNS-имя, SSH-доступ, четыре пароля PostgreSQL и данные встроенного администратора. Выберите «Быстрая установка» и нажмите «Продолжить».

8.1 Сервер

Реквизиты подключения к серверу, на который будет развернут Clearway CA.

Параметр	Как заполнить
Имя сервера	FQDN или IP-адрес целевого сервера, на который будет выполнена установка всех сервисов ЦС.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

8.2 Сбор данных

Основные параметры стенда: alias сервера, Subject корневого сертификата, каталог точек распространения.

Параметр	Как заполнить
Alias сервера (расширенные настройки)	Имя, которое будет указываться при обращении к сервисам; на это имя будут выпущены TLS-сертификаты и ссылки CDP/AIA. По умолчанию совпадает с именем сервера, определённым командой hostname.
Атрибут Subject сертификата ЦС	Subject корневого сертификата ЦС в формате DistinguishedName. Сертификат будет сгенерирован автоматически в процессе установки. По умолчанию: CN=RootCA,O=Company,C=RU.
Алгоритм ключа ЦС	Выберите алгоритм ключа корневого ЦС. Доступны RSA 4096, ECDSA P-256, ECDSA P-521, Ed25519 и ГОСТ Р 34.10-2012 на 256 или 512 бит. Для Ed25519 нужен OpenSSL 3. TLS и служебные ключи используют RSA; ГОСТ-движок устанавливается независимо от выбора. По умолчанию: RSA 4096.

Параметр	Как заполнить
Путь к папке публикации (расширенные настройки)	Каталог точек распространения CRL и сертификатов (CDP/AIA), который отдается веб-сервером по путям /cdp и /aia. По умолчанию: /opt/itc/web.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будут работать все сервисы. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы всех устанавливаемых сервисов. По умолчанию: /opt/itc.

8.3 База данных

Пароли учетных записей локального PostgreSQL (БД ЦС, БД OpenID, архивная БД, БД SCEP).

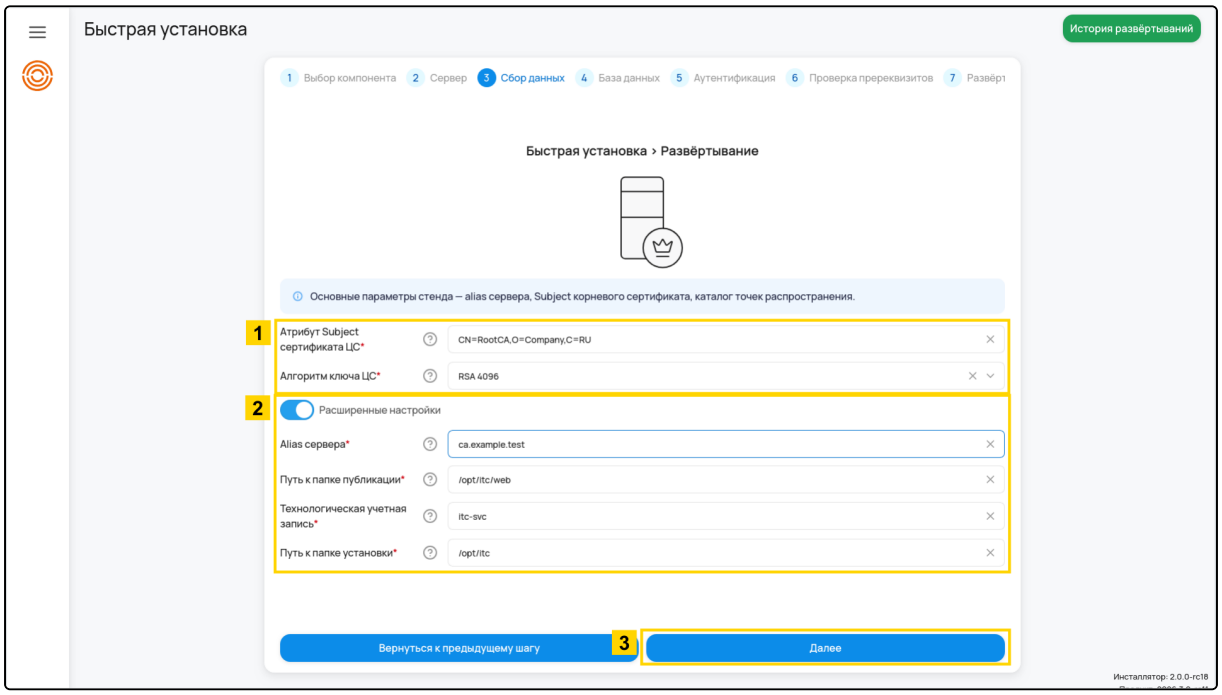
Параметр	Как заполнить
Пароль БД ЦС	Пароль учетной записи cwi-ca в локальной базе данных PostgreSQL. Используется ЦС, OCSP-сервисом и сервисом архивации.
Пароль БД OpenID	Пароль учетной записи cwi-openid в локальной базе данных PostgreSQL.
Пароль архивной БД	Пароль учетной записи cwi-ca-archiver в локальной архивной базе данных PostgreSQL.
Пароль БД SCEP	Пароль учетной записи cwi-scep в локальной базе данных PostgreSQL.

8.4 Аутентификация

Email и пароль встроенной учетной записи администратора контрольной панели.

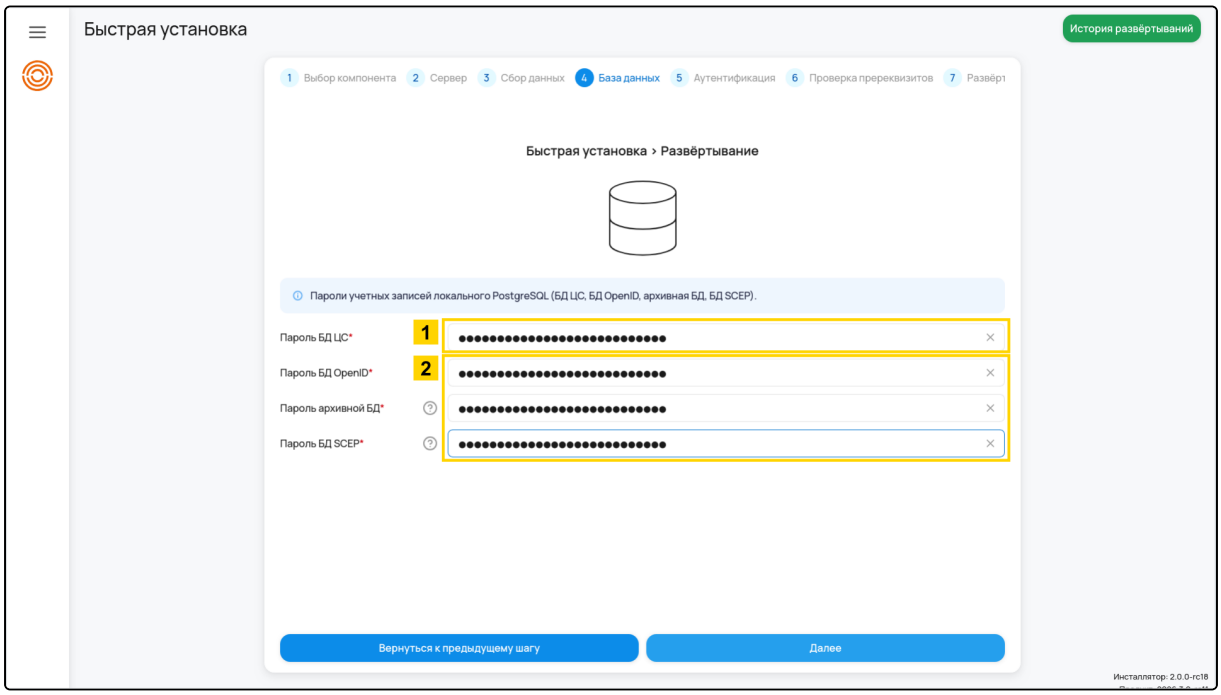
Параметр	Как заполнить
Email администратора	Адрес электронной почты встроенной учетной записи администратора контрольной панели (используется как логин). Позволяет входить без подключения к внешнему каталогу. По умолчанию: admin@company.ru.

Параметр	Как заполнить
Пароль администратора	Пароль встроенной учетной записи администратора контрольной панели. В конфигурацию сохраняется только bcrypt-хэш.



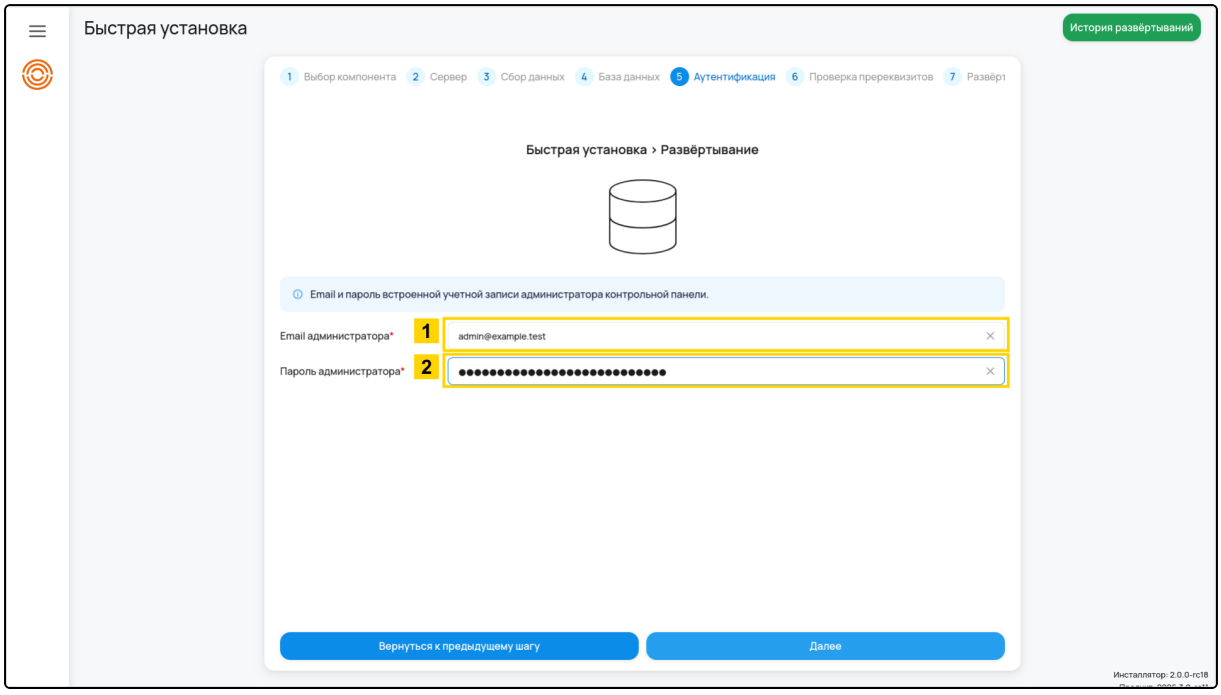
5 Рисунок 5. Параметры быстрого развёртывания.

1. Subject и алгоритм ключа корневого ЦС.
2. Расширенные настройки для имени сервера и каталогов.
3. Переход к параметрам баз данных.



6 Рисунок 6. Пароли служебных баз данных.

1. Пароль рабочей БД ЦС.
2. Отдельные пароли БД OpenID, архиватора и SCEP.



7 Рисунок 7. Встроенный администратор.

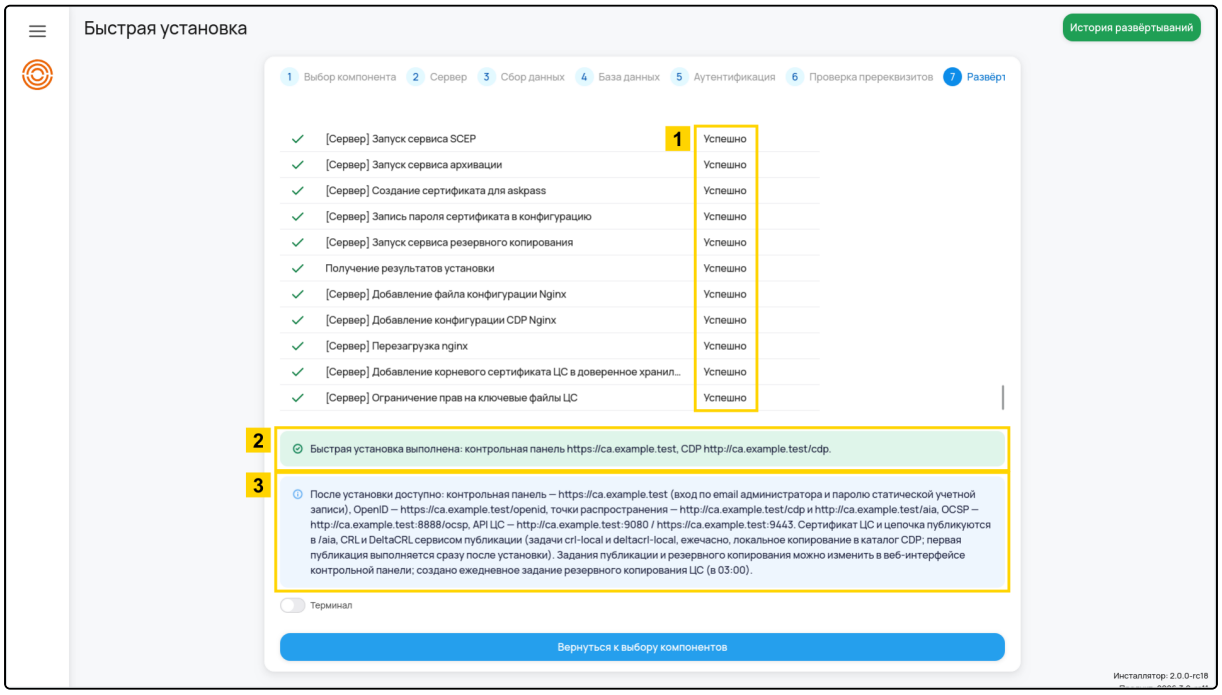
1. Email для входа в контрольную панель.
2. Пароль статической учётной записи.

8.5 Проверка и результат

Мастер проверит четыре базы данных, каталоги, права, linger, OpenSSL и ГОСТ-движок, Nginx, jq, утилиты резервного копирования и доверенное хранилище ОС.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

После успешного развёртывания сохраните ca.crt из результата. Перед первым входом настройте доверие браузера к сертификату ЦС, как описано в разделе «Контрольная панель». Затем откройте https://<имя-сервера> и войдите с указанными Email и паролем. OpenID доступен по https://<имя-сервера>/openid, CDP и AIA по HTTP, OCSP по http://<имя-сервера>:8888/ocsp. Проверьте состояние ЦС и сервисов в контрольной панели.



8 Рисунок 8. Завершение быстрой установки.

1. Успешное выполнение команд.
2. Сообщение о завершении сценария и адрес панели.
3. Адреса сервисов и действия после установки.

Сценарий создаёт задания crl-local и deltacrl-local для ежечасной публикации CRL и DeltaCRL; первая публикация выполняется при установке. Также создаётся ежедневное задание резервного копирования на 03:00. Проверьте задания, часовой пояс, каталог хранения и срок хранения копий в контрольной панели.

9 Центр сертификации

В расширенном режиме выберите группу «ЦС». Она содержит «Развёртывание», «Выпуск сертификата» и «Настройка». Тип ЦС выбирается внутри первого компонента. Для корневого ЦС два последующих компонента пропускаются автоматически; для выдающего они завершают создание цепочки доверия.

9.1 Сервер

Укажите SSH-реквизиты сервера ЦС. Учётная запись должна иметь права sudo. Эти данные используются для удалённой установки; сервис будет работать от отдельной технологической учётной записи.

Параметр	Как заполнить
Имя сервера ЦС	FQDN или IP-адрес целевого сервера, на который будет выполнена установка ЦС.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка ЦС.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

9.2 Сбор данных

Параметры сертификата ЦС: тип центра сертификации, атрибуты Subject и адреса точек распространения, которые будут включены в сертификат.

Параметр	Как заполнить
Тип центра сертификации	Определяет роль ЦС. Корневой ЦС имеет самоподписанный сертификат и подписывает сертификаты подчинённых ЦС. Выдающий ЦС получает сертификат от корневого и выпускает сертификаты конечных субъектов. По умолчанию: Корневой ЦС. Варианты: Корневой ЦС, Выдающий ЦС.
Алгоритм ключа ЦС	Выберите алгоритм ключа ЦС. Доступны RSA 4096, ECDSA P-256, ECDSA P-521, Ed25519 и ГОСТ Р 34.10-2012 на 256 или 512 бит. Для Ed25519 нужен OpenSSL 3. TLS-сертификат и служебные ключи шифрования и KRA создаются на RSA. ГОСТ-движок устанавливается при любом выборе. По умолчанию: RSA 4096.

Параметр	Как заполнить
Alias сервера ЦС (расширенные настройки)	Имя, которое будет указываться при обращении к серверу ЦС; на это имя будет выпущен TLS-сертификат. По умолчанию совпадает с именем сервера, определённым командой hostname. Обязательное поле.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы установленного ЦС. По умолчанию: /opt/itc/minica.
Атрибут Subject сертификата ЦС	Укажите DN сертификата ЦС, например CN=RootCA,O=Company,C=RU. Для выдающего ЦС задайте его собственное имя, например CN=IssuingCA,O=Company,C=RU. По умолчанию: CN=RootCA,O=Company,C=RU.
Сертификат KRA	Файл сертификата агента восстановления ключей (KRA). Если не указан, ключевая пара KRA будет сгенерирована автоматически в процессе установки. Поле можно оставить пустым.

9.3 Точка распространения

Для корневого ЦС задайте размещение точки распространения. При выборе выдающего ЦС этот экран пропускается: CDP настраивается после загрузки подписанного сертификата.

Параметр	Как заполнить
Точка распространения на отдельном сервере	Включите, если сервер точек распространения CRL и сертификатов (веб-сервер CDP) развёртывается на отдельном сервере, отличном от сервера ЦС. При выключении веб-сервер будет установлен на сервере ЦС. По умолчанию: Выключено.
Имя сервера точек распространения	FQDN или IP-адрес сервера, на который будет выполнена установка веб-сервера точек распространения (CDP).
Пользователь сервера точек распространения	Учетная запись на сервере точек распространения с правами sudo, от имени которой выполняется установка и настройка веб-сервера.
Пароль сервера точек распространения	Пароль учетной записи для подключения к серверу точек распространения по SSH.

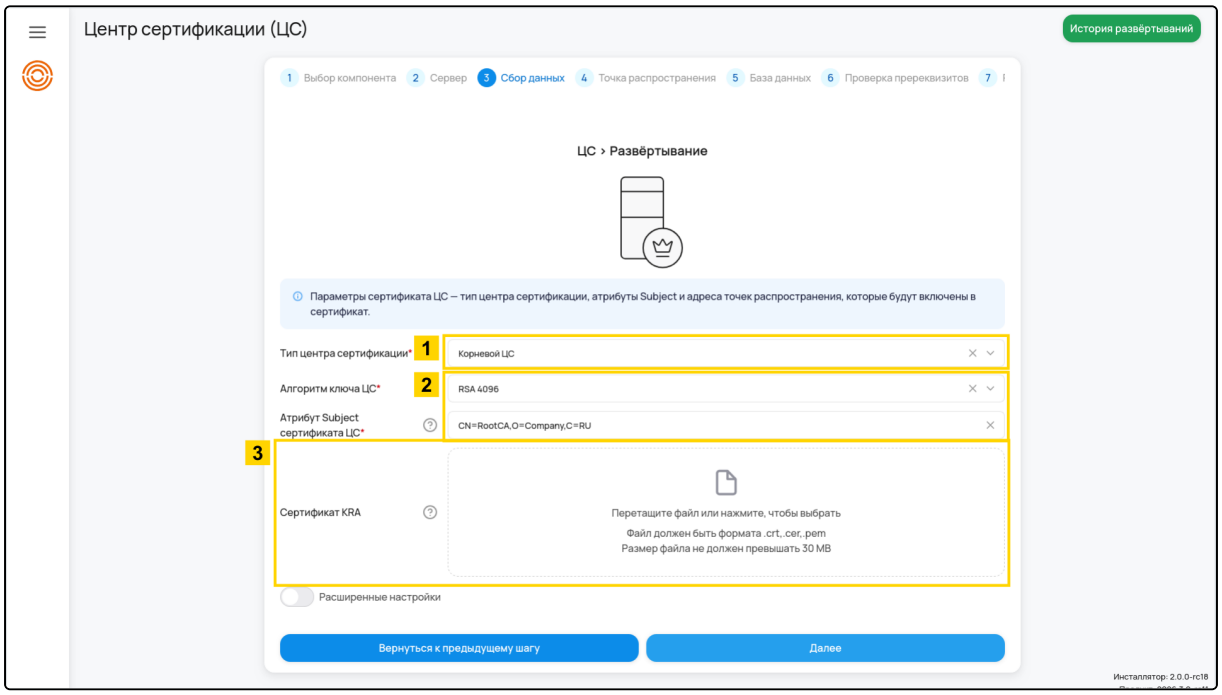
Параметр	Как заполнить
Alias сервера точек распространения (расширенные настройки)	Имя, которое будет указываться в расширениях CDP и AIA выпущенных сертификатов и в конфигурации веб-сервера. Необязательно: если оставить пустым, будет использовано имя сервера точек распространения, определённое на нём командой hostname. Поле можно оставить пустым.
Технологическая учетная запись сервера точек распространения (расширенные настройки)	Учетная запись: владелец папки публикации сертификатов и CRL. От её имени создаётся структура папок. По умолчанию: Технологическая учётная запись ЦС.
Путь к папке публикации (расширенные настройки)	В указанной папке будут располагаться публикуемые файлы сертификатов и CRL. По умолчанию: /opt/itc/web.

9.4 База данных

Выберите локальную или внешнюю БД. Для внешней БД дополнительно укажите SSH-реквизиты её сервера. При повторной установке используйте действующий пароль существующей учётной записи PostgreSQL.

Параметр	Как заполнить
Внешняя база данных	Включите, если база данных ЦС расположена на отдельном сервере, отличном от сервера ЦС. При включении потребуется указать реквизиты подключения к серверу БД. По умолчанию: Выключено при новой установке. При обновлении определяется по существующему подключению к БД.
Имя сервера БД	FQDN или IP-адрес сервера базы данных ЦС. Используется для подключения по SSH при установке и настройке БД.
Пользователь сервера БД	Учетная запись на сервере БД с правами sudo, от имени которой выполняется установка и настройка PostgreSQL.
Пароль сервера БД	Пароль учетной записи для подключения к серверу БД по SSH.
Имя учетной записи в БД ЦС (расширенные настройки)	Имя учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД ЦС. По умолчанию: cwi-ca.
Пароль учетной записи в БД ЦС	Пароль учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД ЦС. При повторной установке укажите действующий пароль существующей учетной записи БД.

Параметр	Как заполнить
Имя базы данных ЦС (расширенные настройки)	Имя базы данных ЦС. Будет использоваться для подключения к ней. По умолчанию: cwi-ca.



9 Рисунок 9. Параметры центра сертификации.

1. Выбор корневого или выдающего ЦС.
2. Алгоритм ключа и Subject.
3. Необязательный сертификат агента восстановления ключей.

9.5 Проверка и результат

Проверяются БД, права на каталоги, технологическая учётная запись, OpenSSL, ГОСТ-движок, linger и зависимости точки распространения.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Для корневого ЦС результат содержит ca.csr, ca.crt и ca-tls.crt. Мастер создаёт корневой сертификат, цепочку, ключи JWT, шаблоны tls, subca и ocsp, включает TLS и публикацию CDP/AIA. Для выдающего ЦС на этом этапе формируется ca.csr; завершите выпуск сертификата и настройку.

9.6 Файлы и службы

Объект	Назначение
/opt/itc/minica/conf/minica.yml	Основная конфигурация ЦС и строка подключения к БД.
/opt/itc/minica/conf/mclient.yml	Конфигурация утилиты mclient.
/opt/itc/minica/ca	Ключ, сертификат ЦС и цепочка доверия.
minica.service	Пользовательская служба ЦС.

9.7 Выпуск сертификата выдающего ЦС

Откройте компонент «Выпуск сертификата». Подключитесь к корневому ЦС и передайте CSR, полученный на этапе развёртывания выдающего ЦС. Укажите технологическую учётную запись и каталог корневого ЦС. Проверка mclient ping должна завершиться успешно.

Параметр	Как заполнить
Имя сервера ЦС	FQDN или IP-адрес сервера ЦС, на котором будет выполнен выпуск сертификата.
Пользователь сервера	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH и запуск mclient для выпуска сертификата.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.
Запрос на сертификат	Запрос на сертификат (CSR) подчинённого ЦС, сформированный при его развёртывании. Подписывается корневым ЦС по шаблону subca. По умолчанию: Файл из результата предыдущего компонента, если он доступен в текущем сеансе.
Технологическая учетная запись (расширенные настройки)	Учетная запись, от имени которой выполняются скрипты на сервере ЦС. Должна совпадать с владельцем папки установки ЦС. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. По умолчанию: /opt/itc/minica.

Нажмите «Выполнить развёртывание». Корневой ЦС подпишет запрос по шаблону subca. Сохраните sub-ca.crt. Если сертификат подписывает другой корневой ЦС, пропустите этот

компонент и получите сертификат по принятой у вас процедуре; он должен соответствовать ключу на сервере выдающего ЦС.

9.8 Настройка выдающего ЦС

Откройте компонент «Настройка» и подключитесь к серверу выдающего ЦС. Загрузите сертификат корневого ЦС и подписанный сертификат выдающего ЦС. Затем задайте параметры точки распространения.

9.9 Сбор данных

Сертификаты корневого и выдающего ЦС для формирования цепочки доверия, а также параметры размещения файлов.

Параметр	Как заполнить
Сертификат корневого ЦС	Файл сертификата корневого ЦС, выпустившего сертификат выдающего ЦС. Используется для формирования цепочки доверия.
Сертификат ЦС	Файл сертификата Выдающего ЦС, подписанный на Корневом ЦС. По умолчанию: Файл из результата предыдущего компонента, если он доступен в текущем сеансе.
Alias сервера ЦС (расширенные настройки)	Имя, которое будет указываться при обращении к серверу ЦС; на это имя будет выпущен TLS-сертификат. По умолчанию совпадает с именем сервера, определённым командой hostname. Обязательное поле.
Технологическая учетная запись (расширенные настройки)	Учетная запись, указанная при установке ЦС и являющаяся владельцем папки установки. От её имени выполняется установка сертификата. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Путь к папке установки (расширенные настройки)	Папка, в которую были установлены файлы ЦС. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.

9.10 Точка распространения

Параметры сервера точек распространения CRL и сертификатов: реквизиты подключения и веб-сервера, на котором клиенты будут получать сертификаты и списки отзыва (CDP/AIA).

Параметр	Как заполнить
Точка распространения на отдельном сервере	Включите, если сервер точек распространения CRL и сертификатов (веб-сервер CDP) развёртывается на отдельном сервере, отличном от сервера ЦС. При выключении веб-сервер будет установлен на сервере ЦС. По умолчанию: Выключено.
Имя сервера точек распространения	FQDN или IP-адрес сервера, на который будет выполнена установка веб-сервера точек распространения (CDP).
Пользователь сервера точек распространения	Учетная запись на сервере точек распространения с правами sudo, от имени которой выполняется установка и настройка веб-сервера.
Пароль сервера точек распространения	Пароль учетной записи для подключения к серверу точек распространения по SSH.
Alias сервера точек распространения (расширенные настройки)	Имя, которое будет указываться в расширениях CDP и AIA выпущенных сертификатов и в конфигурации веб-сервера. Необязательно: если оставить пустым, будет использовано имя сервера точек распространения, определённое на нём командой hostname. Поле можно оставить пустым.
Технологическая учетная запись сервера точек распространения (расширенные настройки)	Учетная запись: владелец папки публикации сертификатов и CRL. От её имени создаётся структура папок. По умолчанию: Технологическая учётная запись ЦС.
Путь к папке публикации (расширенные настройки)	В указанной папке будут располагаться публикуемые файлы сертификатов и CRL. По умолчанию: /opt/itc/web.

После проверок запустите развёртывание. Мастер установит сертификат, сформирует chain.pem, выпустит TLS-сертификат и запустит ЦС. Сохраните ca.crt, ca-tls.crt и chain.pem из результата. Проверьте доступность сервиса через mclient и публикацию сертификатов и CRL.

10 Аутентификация (OpenID)

Выберите «Аутентификация (OpenID)». Один компонент разворачивает провайдер, подготавливает БД, выпускает TLS-сертификат через выбранный ЦС и при необходимости добавляет LDAP. До начала должен работать ЦС, доступный по SSH и через mclient.

10.1 Сервер

Реквизиты подключения к серверу, на который будет установлен OpenID-провайдер.

Параметр	Как заполнить
Имя сервера OpenID	FQDN или IP-адрес сервера, на который будет выполнена установка сервиса OpenID.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка сервиса OpenID.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

10.2 Сбор данных

Основные параметры OpenID-сервера: имя сервера, технологическая учетная запись и путь установки.

Параметр	Как заполнить
Имя сервера	Имя сервера, используемое в nginx (server name) и в выпускаемом TLS-сертификате. По умолчанию соответствует имени целевого сервера.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: /opt/itc.

10.3 ЦС

Параметры подключения к серверу ЦС для выпуска TLS-сертификата.

Параметр	Как заполнить
Внешний ЦС	Включите, если центр сертификации (ЦС) расположен на отдельном сервере, отличном от сервера OpenID. При включении потребуется указать реквизиты подключения к серверу ЦС. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера ЦС	FQDN или IP-адрес сервера центра сертификации, выпускающего TLS-сертификат для сервиса OpenID. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера ЦС	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH для выпуска TLS-сертификата. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера ЦС	Пароль учетной записи для подключения к серверу ЦС по SSH.
Технологическая учетная запись (расширенные настройки)	Укажите технологическую учётную запись установленного ЦС. От её имени мастер запускает mclient на сервере ЦС. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. Используется для выпуска TLS-сертификата. По умолчанию: Каталог установленного ЦС; при отсутствии значения используется /opt/itc/minica.

10.4 База данных

Параметры подключения к базе данных OpenID: локальная или внешняя БД и учетные данные.

Параметр	Как заполнить
Внешняя база данных	Включите, если база данных сервиса OpenID расположена на отдельном сервере, отличном от сервера OpenID. При включении потребуется указать реквизиты подключения к серверу БД. По умолчанию: Выключено.
Имя сервера БД	FQDN или IP-адрес сервера базы данных сервиса OpenID. Используется для подключения по SSH при установке и настройке БД.
Пользователь сервера БД	Учетная запись на сервере БД с правами sudo, от имени которой выполняется установка и настройка PostgreSQL.

Параметр	Как заполнить
Пароль сервера БД	Пароль учетной записи для подключения к серверу БД по SSH.
Имя учетной записи в БД OpenID (расширенные настройки)	Имя учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД сервиса OpenID. По умолчанию: cwi-openid.
Пароль учетной записи в БД OpenID	Пароль учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД сервиса OpenID. При повторной установке укажите действующий пароль существующей учетной записи БД.
Имя базы данных OpenID (расширенные настройки)	Имя базы данных сервиса OpenID. Будет использоваться для подключения к ней. По умолчанию: cwi-openid.

10.5 Статическая учётная запись

Данные встроенной учетной записи: позволяют входить без подключения к внешнему каталогу.

Параметр	Как заполнить
Email статической учётной записи	Адрес электронной почты встроенной учётной записи (используется как логин). Позволяет входить без подключения к внешнему каталогу. По умолчанию: admin@company.ru.
Имя статической учётной записи	Отображаемое имя встроенной учётной записи (claim preferred username/username). По умолчанию: admin.
Пароль статической учётной записи	Пароль встроенной учётной записи. В конфигурацию сохраняется только bcrypt-хэш.

10.6 Настройка токена

Укажите канонический адрес издателя, срок действия id-токена и ограничения refresh-токенов и пользовательских сессий.

Параметр	Как заполнить
Адрес издателя OpenID (issuer)	Канонический адрес провайдера. Он должен совпадать с адресом издателя в настройках клиентов и быть доступен им по сети. Для установленного Clearway OpenID используйте https://<имя-сервера>/openid. По умолчанию: https://<имя-сервера>/openid.

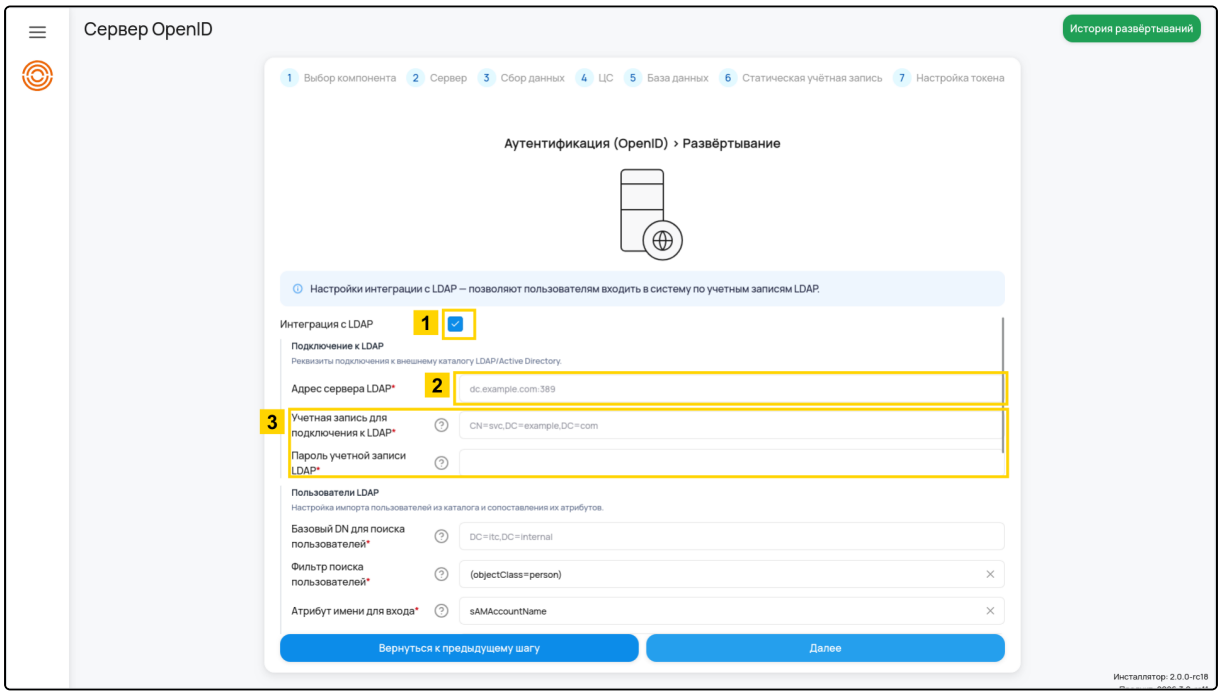
Параметр	Как заполнить
Время жизни id-токена (расширенные настройки)	Срок действия id-токена (idToken). Указывается в формате длительности, например 2m, 1h. По умолчанию: 5m.
Лимит параллельных сессий (расширенные настройки)	Максимальное число одновременных сессий пользователя. 1: допускается только одна сессия. По умолчанию: 5.
Политика при превышении лимита сессий (расширенные настройки)	Действие при достижении лимита параллельных сессий. По умолчанию: Отклонять новую сессию (reject). Варианты: Отклонять новую сессию (reject), Завершать самую старую сессию (terminate oldest). _
Время жизни refresh-токена (расширенные настройки)	Абсолютный срок действия refresh-токена. Указывается в формате длительности, например 1h. По умолчанию: 24h.
Допустимое время бездействия refresh-токена (расширенные настройки)	Время бездействия, по истечении которого refresh-токен становится недействительным. Указывается в формате длительности, например 3m. По умолчанию: 30m.

10.7 Интеграция с LDAP

Если используется внешний каталог, включите «Интеграция с LDAP» и заполните появившиеся блоки. Получите адрес сервера, DN, учётные данные и схему атрибутов у администратора каталога. Встроенная статическая учётная запись сохраняется.

Параметр	Как заполнить
Интеграция с LDAP	Включите, чтобы аутентифицировать пользователей через внешний каталог LDAP/Active Directory. В конфигурацию сервиса добавляется секция connectors (периодический импорт пользователей и групп, сопоставление LDAP-групп с ролями MiniCA). Встроенная статическая учётная запись при этом сохраняется. По умолчанию: Выключено.
Подключение к LDAP / Адрес сервера LDAP	FQDN или IP-адрес и порт сервера каталогов (LDAP/Active Directory). Формат <host>:<port>, например dc.example.com:389.
Подключение к LDAP / Учетная запись для подключения к LDAP	Учетная запись, от имени которой выполняется подключение к серверу каталогов для поиска пользователей и групп.
Подключение к LDAP / Пароль учетной записи LDAP	Пароль учетной записи, используемой для подключения к серверу каталогов.

Параметр	Как заполнить
Пользователи LDAP / Базовый DN для поиска пользователей	Базовый DN (Distinguished Name), от которого выполняется поиск учетных записей пользователей. Например DC=example,DC=com.
Пользователи LDAP / Импорт пользователей по запросу (расширенные настройки)	Если включено, пользователь импортируется из каталога «на лету» при входе, а не только при периодической синхронизации. По умолчанию: Включено.
Пользователи LDAP / Фильтр поиска пользователей	LDAP-фильтр для отбора учетных записей пользователей. Например (objectClass=person). По умолчанию: (objectClass=person).
Пользователи LDAP / Атрибут имени для входа	Атрибут LDAP, значение которого пользователь вводит при входе. Для Active Directory обычно sAMAccountName. По умолчанию: sAMAccountName.
Пользователи LDAP / Атрибут идентификатора пользователя	Атрибут LDAP, используемый как уникальный идентификатор пользователя. Для Active Directory обычно sAMAccountName. По умолчанию: sAMAccountName.
Пользователи LDAP / Атрибут электронной почты	Атрибут LDAP, из которого берется адрес электронной почты пользователя. Для Active Directory обычно userPrincipalName. По умолчанию: userPrincipalName.
Пользователи LDAP / Атрибут отображаемого имени	Атрибут LDAP, из которого берется отображаемое имя пользователя. Для Active Directory обычно displayName. По умолчанию: displayName.
Пользователи LDAP / Атрибут предпочитаемого имени	Атрибут LDAP, используемый как предпочитаемое имя пользователя (preferred username). Для Active Directory обычно sAMAccountName. По _ умолчанию: sAMAccountName.
Группы LDAP / Базовый DN для поиска групп	Базовый DN (Distinguished Name), от которого выполняется поиск групп. Например DC=example,DC=com.
Группы LDAP / Импорт групп по запросу (расширенные настройки)	Если включено, группы импортируются из каталога «на лету» при входе пользователя, а не только при периодической синхронизации. По умолчанию: Включено.
Группы LDAP / Фильтр поиска групп	LDAP-фильтр для отбора групп. Например (objectClass=group). По умолчанию: (objectClass=group).
Группы LDAP / Атрибут имени группы	Атрибут LDAP, из которого берется имя группы. Для Active Directory обычно cn. По умолчанию: cn.



10 Рисунок 10. Подключение внешнего каталога в OpenID.

1. Переключатель интеграции с LDAP.
2. Адрес сервера каталогов.
3. Учётная запись и пароль для служебного подключения.

10.8 Проверка и результат

Проверяются установленный ЦС, PostgreSQL, доступность БД, технологическая учётная запись, каталоги, linger, OpenSSL, Nginx и доверенное хранилище ОС.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Настройте доверие браузера к сертификату ЦС по разделу «Контрольная панель». Откройте адрес issuer и проверьте доступность провайдера. После установки контрольной панели выполните вход статической учётной записью. Если включён LDAP, отдельно проверьте вход тестового пользователя каталога и назначенные ему роли. Наличие подключения к LDAP само по себе не подтверждает права в ЦС.

10.9 Файлы и службы

Объект	Назначение
/opt/itc/openid/config.json	Адрес issuer, БД, статическая учётная запись, параметры токенов, клиенты и LDAP-коннекторы.
/opt/itc/itc/nginx/openid.conf	Публикация OpenID через Nginx.
openid.service	Пользовательская служба аутентификации.

Для LDAP проверьте DN поиска и фильтры на своём каталоге. Значения sAMAccountName, userPrincipalName, displayName и cn подходят для типовой схемы AD, но должны соответствовать фактическим атрибутам. Сопоставление групп каталога и ролей проверьте в конфигурации OpenID и настройках прав ЦС.

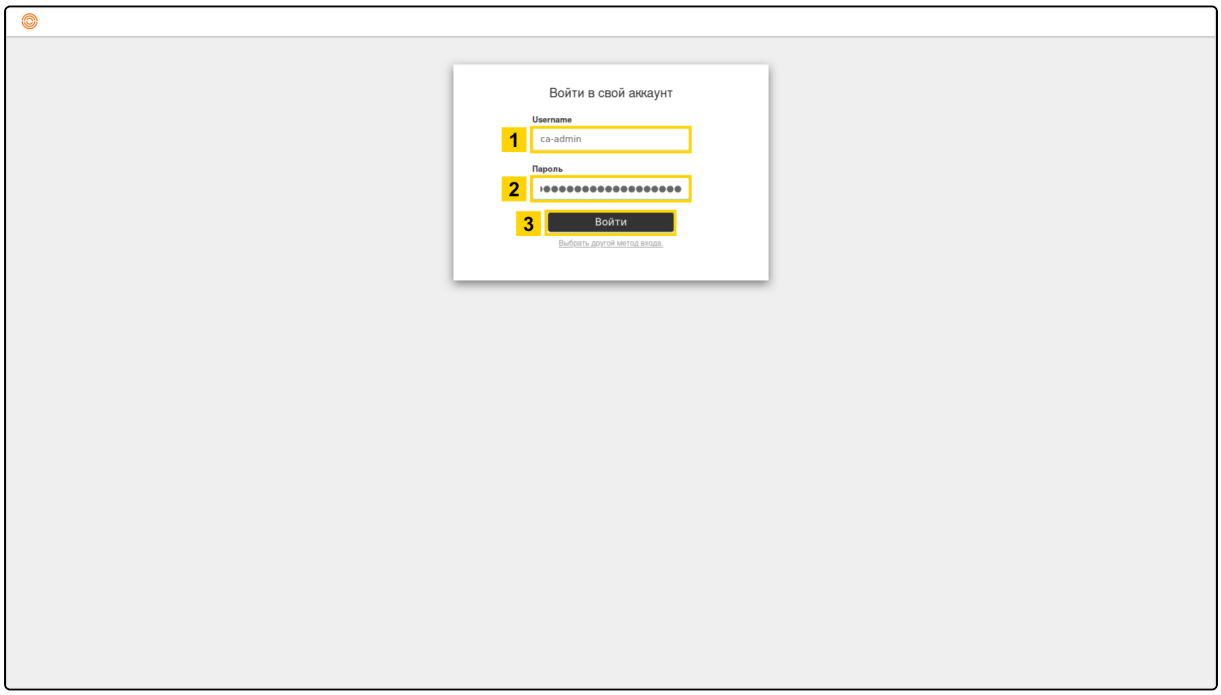
10.10 Подключение по LDAPS и права групп

Создаваемый LDAP-коннектор содержит insecureNoSSL: true. Указание порта 636 в форме само по себе не включает LDAPS. Для защищённого подключения установите сертификат TLS на контроллере домена и подготовьте сертификат его ЦС на сервере OpenID. В /opt/itc/openid/config.json измените следующие поля внутри connectors[].config, сохранив остальные настройки:

```
{
  "host": "dc01.example.test:636",
  "insecureNoSSL": false,
  "rootCA": "/etc/ssl/certs/ad-root-ca.pem"
}
```

Замените имя контроллера и путь к сертификату ЦС на свои значения. Сертификат контроллера должен содержать указанное DNS-имя. Перезапустите openid.service от имени технологической учётной записи и проверьте вход пользователя каталога. Не отключайте проверку сертификата при ошибке доверия: проверьте имя, цепочку и доступность файла rootCA.

В шаблоне предусмотрены группы CWCA_Administrator, CWCA_Auditor и CWCA_User. Проверьте их наличие и соответствие ролям вашей системы. После изменения карты групп пользователь должен выйти из панели и войти снова.



11 Рисунок 11. Вход учётной записью каталога.

1. Имя пользователя в формате, заданном в настройке userSearch.
2. Пароль доменной учётной записи.
3. Кнопка входа; после подтверждения разрешений должна открыться контрольная панель.

11 MS-WSTEP

Сценарий разворачивает CEP и CES Adapter для запроса сертификатов доменными Windows-клиентами. Подготовьте действующий домен Active Directory, DNS, синхронизацию времени, сервисную учётную запись LDAP и отдельную учётную запись с правом ввода компьютера в домен. Сервер Clearway CA должен быть установлен и доступен.

Выберите группу «MS-WSTEP». Выпуск TLS-сертификата, получение JWT и настройка подключения к ЦС входят в единое развёртывание.

11.1 Сервер

Реквизиты подключения к серверу, на который будет установлен сервис MS-WSTEP.

Параметр	Как заполнить
Имя сервера MS-WSTEP	FQDN или IP-адрес сервера, на который будет выполнена установка сервиса MS-WSTEP (CEP/CES).
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка сервиса MS-WSTEP.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

11.2 Сбор данных

Основные параметры сервиса: alias сервера, технологическая учетная запись и путь установки.

Параметр	Как заполнить
Alias сервера	Имя, которое будет указываться при обращении к серверу MS-WSTEP; на это имя будет выпущен TLS-сертификат. По умолчанию совпадает с именем сервера, определённым командой hostname. Обязательное поле.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будут работать сервисы. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: /opt/itc.

11.3 ЦС

Параметры подключения к серверу ЦС для выпуска TLS-сертификата сервиса.

Параметр	Как заполнить
Внешний ЦС	Включите, если центр сертификации (ЦС) расположен на отдельном сервере, отличном от сервера MS-WSTEP. При включении потребуется указать реквизиты подключения к серверу ЦС. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера ЦС	FQDN или IP-адрес сервера центра сертификации, выпускающего TLS-сертификат для сервиса MS-WSTEP. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера ЦС	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH для выпуска TLS-сертификата. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера ЦС	Пароль учетной записи для подключения к серверу ЦС по SSH.
Сертификат ЦС	Сертификат центра сертификации в формате PEM/DER. Используется сервисом MS-WSTEP для проверки цепочки доверия при выдаче сертификатов. По умолчанию: Файл из результата предыдущего компонента, если он доступен в текущем сеансе.
Технологическая учетная запись (расширенные настройки)	Укажите технологическую учётную запись установленного ЦС. От её имени мастер запускает mclient на сервере ЦС. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. Используется для выпуска TLS-сертификата. По умолчанию: Каталог установленного ЦС; при отсутствии значения используется /opt/itc/minica.

11.4 LDAP

Параметры подключения к домену: в каталоге сервисы CEP/CES ищут шаблоны сертификатов и точки выдачи.

Параметр	Как заполнить
Адрес LDAP-сервера	Адрес домен-контроллера (LDAP), к которому подключаются сервисы CEP/CES для поиска шаблонов сертификатов и точек выдачи.
Домен Active Directory	Имя домена Active Directory (например itc.internal), в который вводится сервер. Используется при вводе в домен и работе Kerberos.
Базовый DN LDAP	Укажите корневой DN своего каталога, например DC=example,DC=test. Получите его у администратора AD; значение DC=ru замените, если оно не соответствует вашему домену. По умолчанию: DC=ru.

11.5 Учетная запись MS-WSTEP

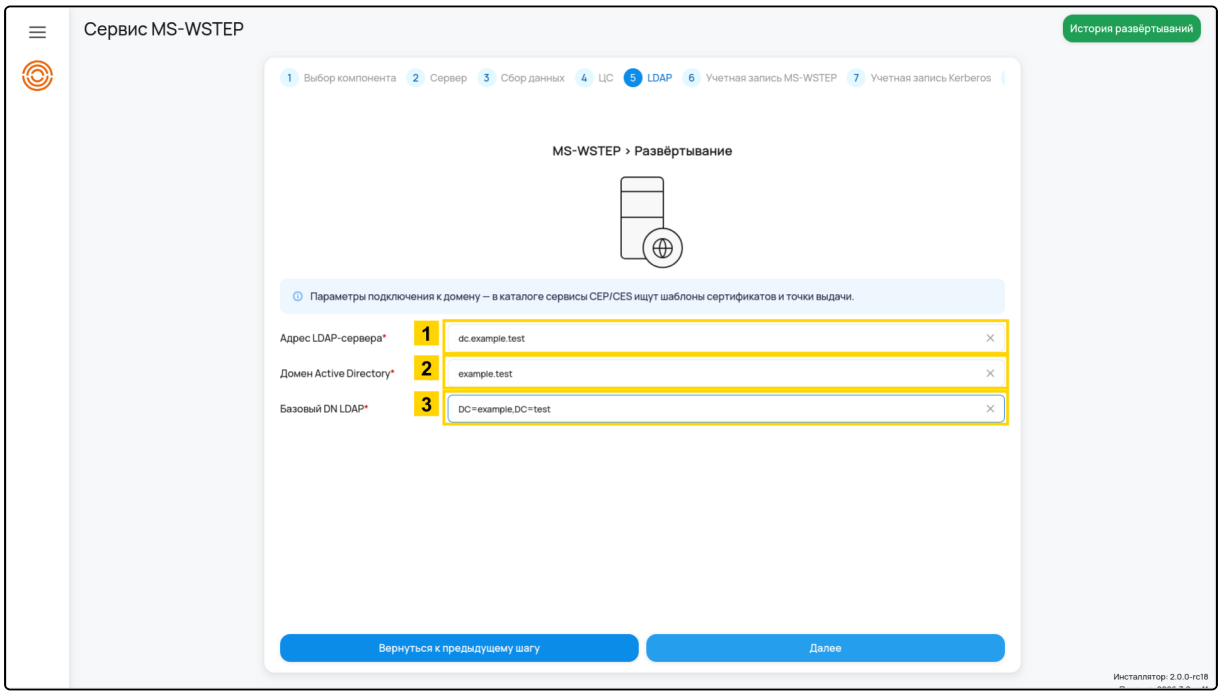
Учетная запись LDAP, от имени которой сервис будет обращаться к каталогу.

Параметр	Как заполнить
Учетная запись LDAP	Учетная запись для подключения к LDAP. Допускается формат user@domain или DOMAIN\user.
Пароль учетной записи LDAP	Пароль сервисной учетной записи для подключения к LDAP.

11.6 Учетная запись Kerberos

Учетные данные администратора домена: настраивают Kerberos-аутентификацию, чтобы доменные устройства запрашивали сертификаты автоматически.

Параметр	Как заполнить
Учетная запись администратора домена	Учетная запись с правами ввода компьютеров в домен (например admin ad). Используется однократно при вводе машины в домен. _
Пароль администратора домена	Пароль учетной записи администратора домена. Используется однократно для ввода машины в домен и не сохраняется.



12 Рисунок 12. Параметры домена для MS-WSTEP.

1. Адрес контроллера домена.
2. DNS-имя домена Active Directory.
3. Базовый DN поиска в каталоге.

11.7 Проверка и результат

Проверяются ЦС, доступность LDAP, обнаружение домена, keytab, технологическая учётная запись, каталоги, linger, OpenSSL, Nginx, jq и средства LDAP/Kerberos.

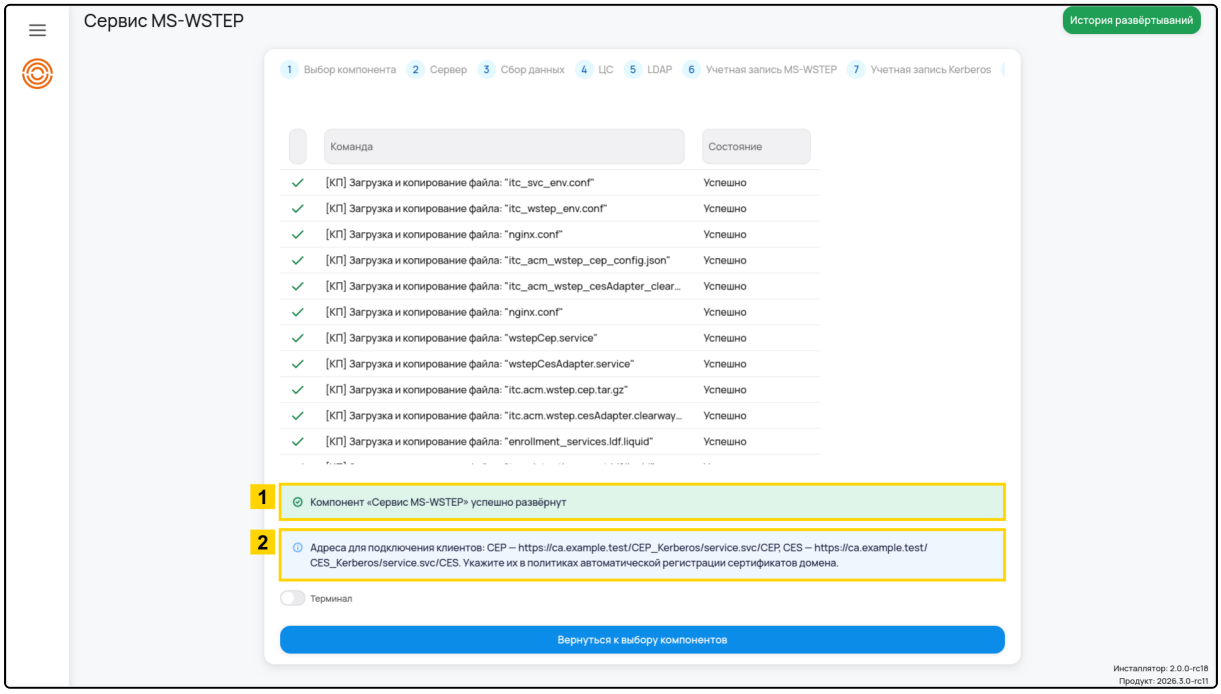
Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Мастер вводит сервер в домен, настраивает Kerberos, выпускает сертификаты и JWT, разворачивает службы CEP/CES и Nginx. Сохраните enrollment_services.ldf, template_tls_export.ldf и add_enrollment_policy.ps1 из результата.

11.8 Файлы и службы

Объект	Назначение
/opt/itc/itc/config/itc acm wstep cepconfig.json	Параметры службы CEP.

Объект	Назначение
/opt/itc/itc/config/itc acm wstep cesAdapter clearwayCa config.json	Подключение CES к каталогу и ЦС.
/opt/itc/itc wstep env.conf	Окружение служб с параметрами LDAP.
wstepCep.service и wstepCesAdapter.service	Пользовательские службы CEP и CES.



13 Рисунок 13. Завершение развёртывания MS-WSTEP.

1. Мастер сообщает об успешном развёртывании компонента.
2. Адреса CEP и CES для настройки доменных клиентов.

11.9 Kerberos и HTTP-служба

Проверьте членство Linux-сервера в домене и наличие ключей службы HTTP для DNS-имени, по которому клиенты обращаются к CEP/CES. Если HTTP SPN отсутствует, добавьте его через adcli и обновите keytab:

```
realm list
sudo klist -k /etc/krb5.keytab
sudo adcli update --domain=example.test \
  --host-fqdn=ca.example.test \
```

```
  --add-service-principal=HTTP/ca.example.test
```

После команды снова проверьте keytab: в нём должна быть запись HTTP/ca.example.test@EXAMPLE.TEST. Файл должен быть доступен технологической учётной записи CEP/CES и закрыт для остальных пользователей. Проверьте KRB5_KTNAME в файле окружения служб. Затем перезапустите wstepCep и wstepCesAdapter.

11.10 Получение политики и сертификата на Windows

На тестовом доменном Windows-клиенте добавьте корневой сертификат ЦС в доверенные корневые центры компьютера. Проверьте DNS и HTTPS сервера Clearway. Откройте PowerShell от имени администратора, затем зарегистрируйте политику CEP:

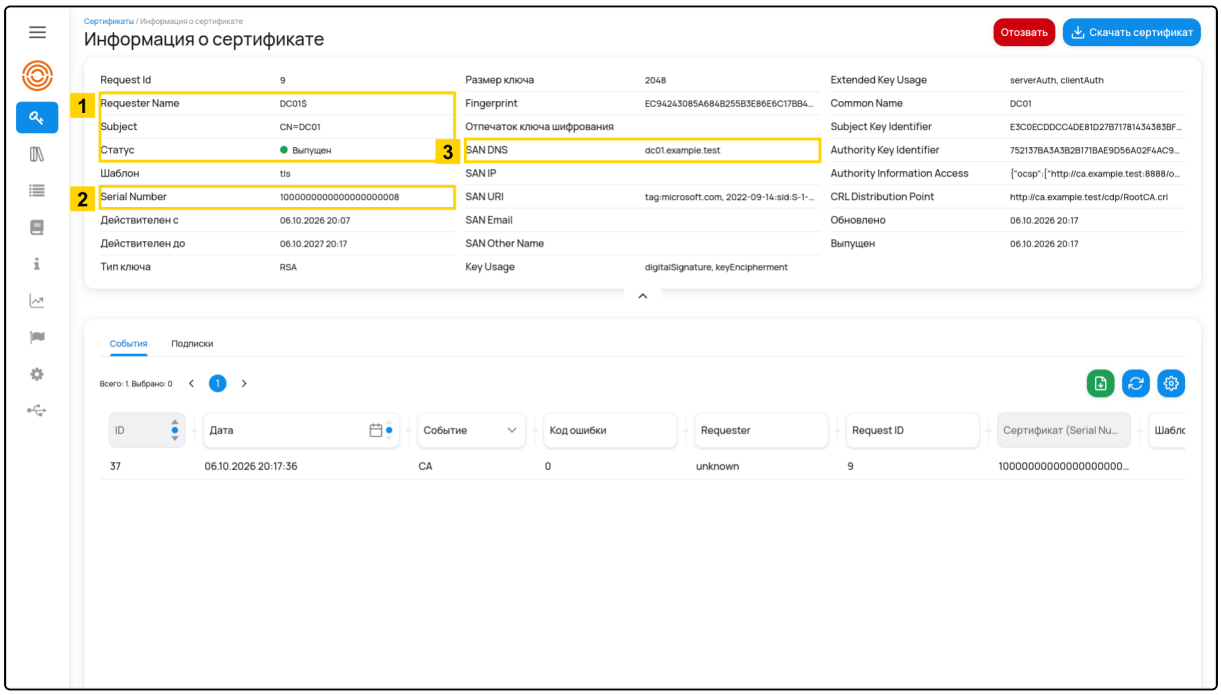
```
$url = 'https://ca.example.test/CEP_Kerberos/service.svc/CEP'
Add-CertificateEnrollmentPolicyServer -Url $url -Context Machine
Get-CertificateEnrollmentPolicyServer -Url $url `
  -Context Machine -Scope All
```

В результате должны быть адрес вашего CEP, AuthType: Kerberos и Context: Machine. Эта команда не включает автоматическую регистрацию. Настраивайте её отдельно после проверки ручной выдачи.

Запросите сертификат по опубликованному шаблону tls в хранилище локального компьютера:

```
Set-Location Cert:\LocalMachine\My
$result = Get-Certificate -Template tls -Url $url `
  -CertStoreLocation Cert:\LocalMachine\My
$result.Status
$result.Certificate | Format-List Subject,Issuer,SerialNumber,`
  Thumbprint,NotAfter,HasPrivateKey,DnsNameList
```

Ожидается статус Issued. Проверьте имя компьютера, SAN, издателя, срок действия, наличие закрытого ключа и цепочку доверия. Найдите тот же серийный номер в контрольной панели Clearway. Только после этой проверки считайте установку MS-WSTEP завершённой.



14 Рисунок 14. Сертификат доменного компьютера в контрольной панели.

1. Запрос поступил от учётной записи компьютера; статус сертификата «Выпущен».
2. Серийный номер для сверки с сертификатом в хранилище Windows.
3. DNS-имя компьютера в SAN сертификата.

Если установка остановилась на удалении временных LDF-файлов, проверьте их владельца и пользователя завершающего SSH-шага. Кнопка «Перезапустить» запускает сценарий заново, включая выпуск сертификатов; она не продолжает только неудачный шаг. Сначала сохраните результаты и устраните причину сбоя.

12 Контрольная панель

До установки подготовьте ЦС и провайдер аутентификации. Выберите «Контрольная панель». Мастер сам выпускает TLS-сертификат и JWT для подключения к ЦС, устанавливает веб-приложение и записывает конфигурацию.

12.1 Сервер

Реквизиты подключения к серверу, на который будет установлена контрольная панель.

Параметр	Как заполнить
Имя сервера контрольной панели	FQDN или IP-адрес сервера, на который будет выполнена установка контрольной панели.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка контрольной панели.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

12.2 Сбор данных

Основные параметры контрольной панели: alias сервера, технологическая учетная запись и путь установки.

Параметр	Как заполнить
Alias сервера	Имя, которое будет указываться при обращении к серверу контрольной панели; на это имя будет выпущен TLS-сертификат. По умолчанию совпадает с именем сервера, определённым командой hostname. Обязательное поле.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: /opt/itc.

12.3 ЦС

Параметры подключения к серверу ЦС для выпуска TLS-сертификата и установки сертификата ЦС.

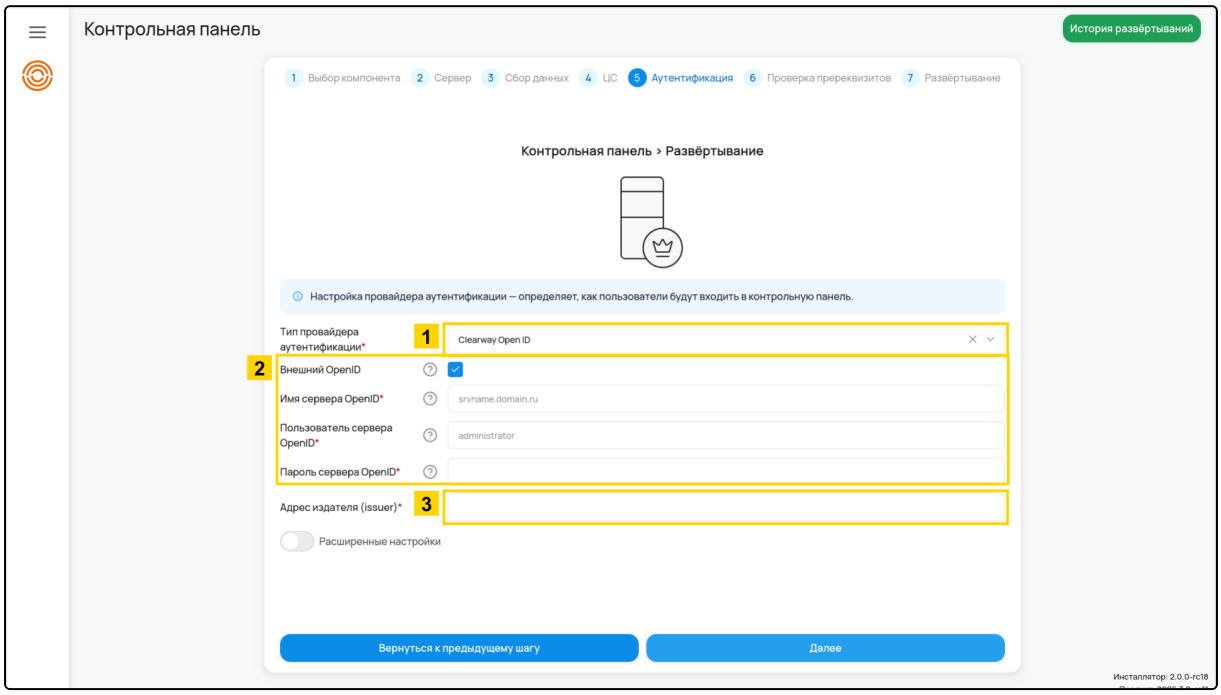
Параметр	Как заполнить
Внешний ЦС	Включите, если центр сертификации (ЦС) расположен на отдельном сервере, отличном от сервера контрольной панели. При включении потребуется указать реквизиты подключения к серверу ЦС. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера ЦС	FQDN или IP-адрес сервера центра сертификации, выпускающего TLS-сертификат для контрольной панели. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера ЦС	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH для выпуска TLS-сертификата. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера ЦС	Пароль учетной записи для подключения к серверу ЦС по SSH.
Название ЦС (расширенные настройки)	Название ЦС для имён файлов (<название>-jwt.key, <название>-jwt.crt, <название>.jwt, <название>.crt) и идентификатор записи в общем конфигурационном файле сервисов itc api miniCA config.json _ _ _ (MiniCa.<название>). Допускаются только латинские буквы, цифры и дефис. Если не указано: используется имя сервера ЦС (или сервера КП, если ЦС совмещён с ней). Поле можно оставить пустым.
Сертификат ЦС	Сертификат центра сертификации в формате PEM/DER. Используется контрольной панелью для проверки цепочки доверия при обращении к ЦС. Файл на сервере называется по названию ЦС. По умолчанию: Файл из результата предыдущего компонента, если он доступен в текущем сеансе.
Технологическая учетная запись (расширенные настройки)	Укажите технологическую учётную запись установленного ЦС. От её имени мастер запускает mclient на сервере ЦС. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. Используется для выпуска TLS-сертификата. По умолчанию: Каталог установленного ЦС; при отсутствии значения используется /opt/itc/minica.

12.4 Аутентификация

Выберите Clearway OpenID или Keycloak. Для Clearway OpenID мастер регистрирует контрольную панель в конфигурации провайдера. При внешнем размещении укажите SSH-реквизиты сервера OpenID. Для Keycloak подготовьте зарегистрированный клиент и укажите его идентификатор и имя поля ролей в токене.

Параметр	Как заполнить
Тип провайдера аутентификации	Выбор системы аутентификации, через которую пользователи входят в контрольную панель. По умолчанию: Clearway Open ID. Варианты: Clearway Open ID, Keycloak.
Внешний OpenID	Включите, если сервис OpenID расположен на отдельном сервере, отличном от сервера контрольной панели. При включении потребуется указать реквизиты подключения к серверу OpenID. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера OpenID	FQDN или IP-адрес сервера OpenID, на котором установлен сервис аутентификации. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера OpenID	Учетная запись на сервере OpenID, от имени которой выполняется подключение по SSH. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера OpenID	Пароль учетной записи для подключения к серверу OpenID по SSH.
Адрес издателя (issuer)	URL провайдера аутентификации (issuer), по которому выполняется валидация токенов. Формат https://<fqdn>/realms/<realm> для Keycloak или https://<fqdn>/openid для Clearway OpenID. По умолчанию: Адрес издателя из ранее введённых настроек OpenID или контрольной панели.
Идентификатор клиента	Идентификатор клиента (client id) контрольной панели, _ зарегистрированный в провайдере аутентификации Keycloak.
Claim для ролей JWT	Имя claim в JWT-токене, из которого берётся список ролей пользователя для авторизации в контрольной панели. По умолчанию: roles.
Технологическая учетная запись OpenID (расширенные настройки)	Технологическая учетная запись на сервере OpenID, от имени которой работает сервис OpenID. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.

Параметр	Как заполнить
Путь к папке установки OpenID (расширенные настройки)	Путь к папке установки сервиса OpenID на сервере OpenID. По умолчанию: Каталог установленного OpenID; при отсутствии значения используется /opt/itc.



15 Рисунок 15. Настройка аутентификации контрольной панели.

1. Тип провайдера аутентификации.
2. Подключение к OpenID при раздельном размещении.
3. Адрес издателя токенов.

12.5 Проверка и результат

Мастер проверяет ЦС, а для Clearway OpenID также установленный провайдер и jq на его сервере. На сервере панели проверяются каталоги, права, Nginx, jq, linger и доверенное хранилище.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Перед первым входом выполните настройку доверия, описанную ниже. Затем откройте https://<имя-сервера-контрольной-панели>. Браузер должен перейти к провайдеру аутентификации, а после входа вернуться в панель. Проверьте отображение ЦС и доступные пользователю операции.

12.6 Файлы и службы

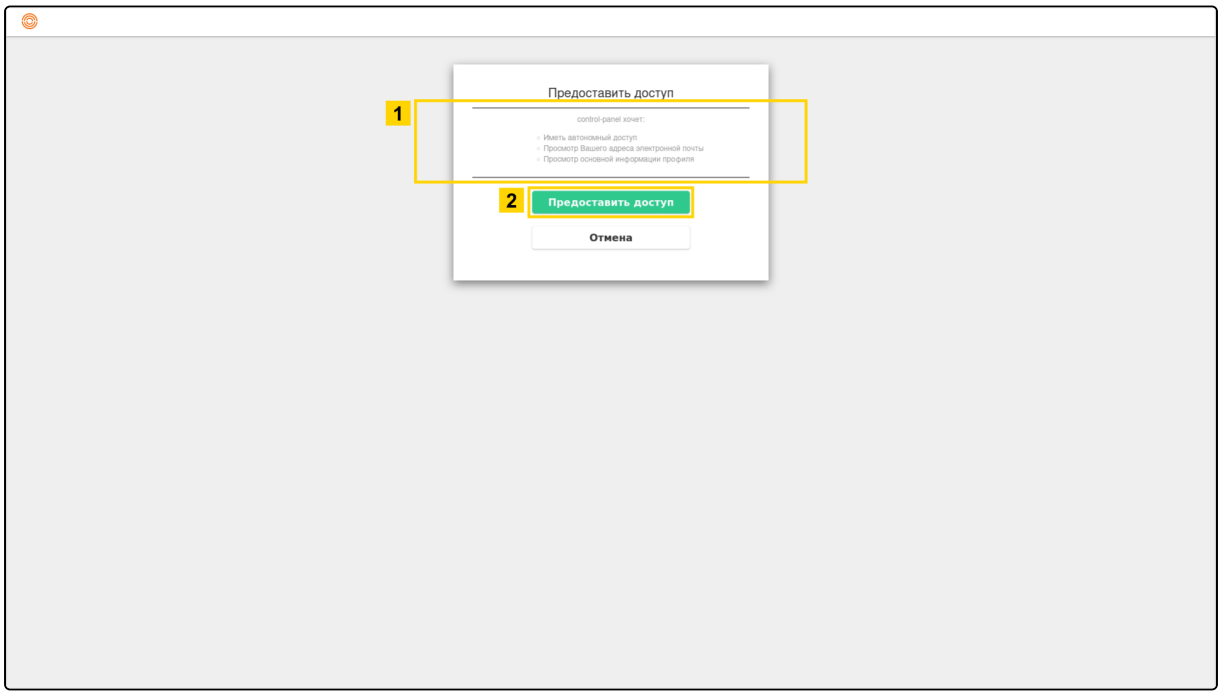
Объект	Назначение
/opt/itc/itc/config/itc api miniCA cont _ _ _ rolPanel config.json _	Параметры контрольной панели.
/opt/itc/itc/config/itc api miniCA confi _ _ _ g.json	Общая конфигурация подключения к ЦС.
/opt/itc/itc/nginx	Конфигурации публикации веб-сервисов.
controlPanel.service	Пользовательская служба контрольной панели.

12.7 Доверие к сертификатам перед первым входом

На компьютере, где открывается контрольная панель, установите корневой сертификат ЦС в доверенное хранилище, используемое браузером. Если TLS-сертификаты выпущены выдающим ЦС, также установите промежуточный сертификат. Используйте сертификаты из результатов развёртывания и настройки соответствующих ЦС. Установка доверия на сервере инсталлятором не заменяет настройку клиентского браузера.

Перезапустите браузер и откройте <issuer>/.well-known/openid-configuration. Подставьте полный адрес издателя вместе с путём /openid или /realms/<realm>, если он входит в issuer; уберите лишний завершающий слеш. JSON с конфигурацией провайдера должен открыться без предупреждений TLS. После этого откройте контрольную панель. Если предупреждение остаётся, исправьте имя или цепочку сертификата, не отключая проверку.

При входе OpenID может запросить согласие на передачу контрольной панели сведений профиля, адреса электронной почты и автономный доступ. Проверьте имя клиента control-panel и нажмите «Предоставить доступ». После перехода в панель ознакомьтесь с сообщением о правилах работы и нажмите «Подтвердить».



16 Рисунок 16. Согласие при первом входе.

1. Имя клиента и запрашиваемые разрешения.
2. Кнопка подтверждения доступа контрольной панели.

13 Сервис публикации

Сначала установите контрольную панель. В расширенном режиме выберите «Сервис публикации». Его сервер, технологическая учётная запись и каталог наследуются от панели; эти поля недоступны для редактирования.

13.1 Сервер

Сервис публикации устанавливается на сервер контрольной панели: реквизиты подключения, технологическая учетная запись и путь установки наследуются из её настроек.

Параметр	Как заполнить
Имя сервера контрольной панели	FQDN или IP-адрес сервера контрольной панели, на который будет выполнена установка сервиса публикации. Наследуется из компонента контрольной панели. Поле заполняется автоматически и недоступно для изменения.
Пользователь сервера	Учетная запись на сервере контрольной панели, от имени которой выполняется установка и настройка сервиса публикации. Наследуется из компонента контрольной панели. Поле заполняется автоматически и недоступно для изменения.
Пароль сервера	Пароль учетной записи для подключения к серверу контрольной панели по SSH.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: Наследуется из настроек контрольной панели. Поле заполняется автоматически и недоступно для изменения.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: Наследуется из настроек контрольной панели. Поле заполняется автоматически и недоступно для изменения.

13.2 Проверка и результат

Проверяются технологическая учётная запись, каталог, права и Nginx.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

После завершения откройте раздел публикации в контрольной панели и создайте задания для нужных ЦС и точек распространения. Проверьте путь назначения, расписание и результат первого запуска. Установка сервиса в расширенном режиме не заменяет создание заданий.

13.3 Файлы и службы

Объект	Назначение
/opt/itc/itc/config/itc api miniCA publication config.json	Задания и параметры сервиса публикации.
publication.service	Пользовательская служба публикации.

Если панель показывает ошибку сервиса, проверьте статус publication.service, его журнал и адрес подключения в настройках панели. Отдельно проверьте, что файл CRL обновился в целевом каталоге и доступен клиентам по опубликованному URL.

14 OCSP

Выберите «OCSP». Подготовьте сертификат обслуживаемого ЦС, SSH-доступ к нему и реквизиты его рабочей БД. Мастер выпускает сертификат подписи OCSP-ответов и настраивает сервис одним компонентом.

14.1 Сервер

Реквизиты подключения к серверу, на который будет установлен OCSP-сервис.

Параметр	Как заполнить
Имя сервера	FQDN или IP-адрес целевого сервера, на который будет выполнена установка сервиса OCSP.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка сервиса OCSP.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

14.2 Сбор данных

Основные параметры OCSP-сервиса: определяют адрес, по которому клиенты будут проверять статус сертификатов.

Параметр	Как заполнить
Alias сервера	Имя, которое будет указываться при обращении к серверу OCSP; на это имя будет выпущен OCSP-сертификат. По умолчанию совпадает с именем сервера, определённым командой hostname. Обязательное поле.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы установленного компонента. По умолчанию: /opt/itc/ocsp.

14.3 ЦС

Параметры подключения к серверу ЦС для выпуска сертификата OCSP-сервиса.

Параметр	Как заполнить
Внешний ЦС	Включите, если центр сертификации (ЦС) расположен на отдельном сервере, отличном от сервера OCSP. При включении потребуется указать реквизиты подключения к серверу ЦС. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера ЦС	FQDN или IP-адрес сервера центра сертификации, выпускающего OCSP-сертификат для сервиса. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера ЦС	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH для выпуска OCSP-сертификата. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера ЦС	Пароль учетной записи для подключения к серверу ЦС по SSH.
Сертификат ЦС	Сертификат выдающего ЦС в формате PEM/DER, выпустившего сертификаты, статус которых проверяет сервис OCSP. Файл будет размещён в $PATH/conf/ca.crt. По умолчанию: Файл из результата предыдущего компонента, если он доступен в текущем сеансе.
Технологическая учетная запись (расширенные настройки)	Укажите технологическую учётную запись установленного ЦС. От её имени мастер запускает mclient на сервере ЦС. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. Используется для выпуска OCSP-сертификата. По умолчанию: Каталог установленного ЦС; при отсутствии значения используется /opt/itc/minica.

14.4 База данных

Параметры подключения к БД ЦС, из которой OCSP-сервис получает информацию о статусе сертификатов.

Параметр	Как заполнить
Имя сервера БД	FQDN или IP-адрес сервера, содержащего БД ЦС. БД должна быть установлена на предыдущем этапе инсталляции ЦС. По умолчанию: Параметр ранее установленной базы данных ЦС.

Параметр	Как заполнить
Имя учетной записи в БД ЦС	Имя учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД ЦС. По умолчанию: Параметр ранее установленной базы данных ЦС.
Пароль учетной записи в БД ЦС	Пароль учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД ЦС. При повторной установке укажите действующий пароль существующей учетной записи БД.
Имя базы данных ЦС	Имя базы данных ЦС. Будет использоваться для подключения к ней. По умолчанию: Параметр ранее установленной базы данных ЦС.

14.5 Проверка и результат

Проверяются установленный ЦС, доступ к БД, технологическая учётная запись, каталоги, права, OpenSSL и linger.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Сохраните mocsp.crt. Проверьте работу mocsp.service, доступность http://<имя-сервера>:8888/ocsp и ответ на запрос по известному сертификату этого ЦС. Проверьте подпись ответа и соответствие возвращаемого статуса данным ЦС.

14.6 Файлы и службы

Объект	Назначение
/opt/itc/ocsp/conf/mocsp.yml	Адрес прослушивания, сертификаты и подключение OCSP к БД ЦС.
/opt/itc/ocsp/conf/ca.crt	Сертификат ЦС, чей статус сертификатов проверяет сервис.
mocsp.service	Пользовательская служба OCSP.

Сервис должен читать БД того ЦС, который выпустил проверяемые сертификаты. Нельзя заменить сертификат этого ЦС сертификатом другого узла только потому, что они принадлежат одной иерархии.

15 Архиватор

Архиватор переносит записи из рабочей БД ЦС в отдельную архивную БД. Подготовьте реквизиты обеих баз и согласуйте сроки переноса. Архивирование изменяет содержимое рабочей БД; оно не заменяет резервное копирование.

15.1 Сервер

Реквизиты подключения к серверу, технологическая учетная запись и путь установки сервиса архивации.

Параметр	Как заполнить
Имя сервера архивации	FQDN или IP-адрес сервера, на который будет выполнена установка сервиса архивации.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка сервиса архивации.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: /opt/itc.

15.2 База данных

Параметры подключения к рабочей базе данных ЦС, из которой сервис будет переносить архивные данные.

Параметр	Как заполнить
Имя сервера БД	FQDN или IP-адрес сервера, содержащего БД ЦС. БД должна быть установлена на предыдущем этапе инсталляции ЦС. По умолчанию: Параметр ранее установленной базы данных ЦС.
Имя учетной записи в БД ЦС	Имя учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД ЦС. По умолчанию: Параметр ранее установленной базы данных ЦС.

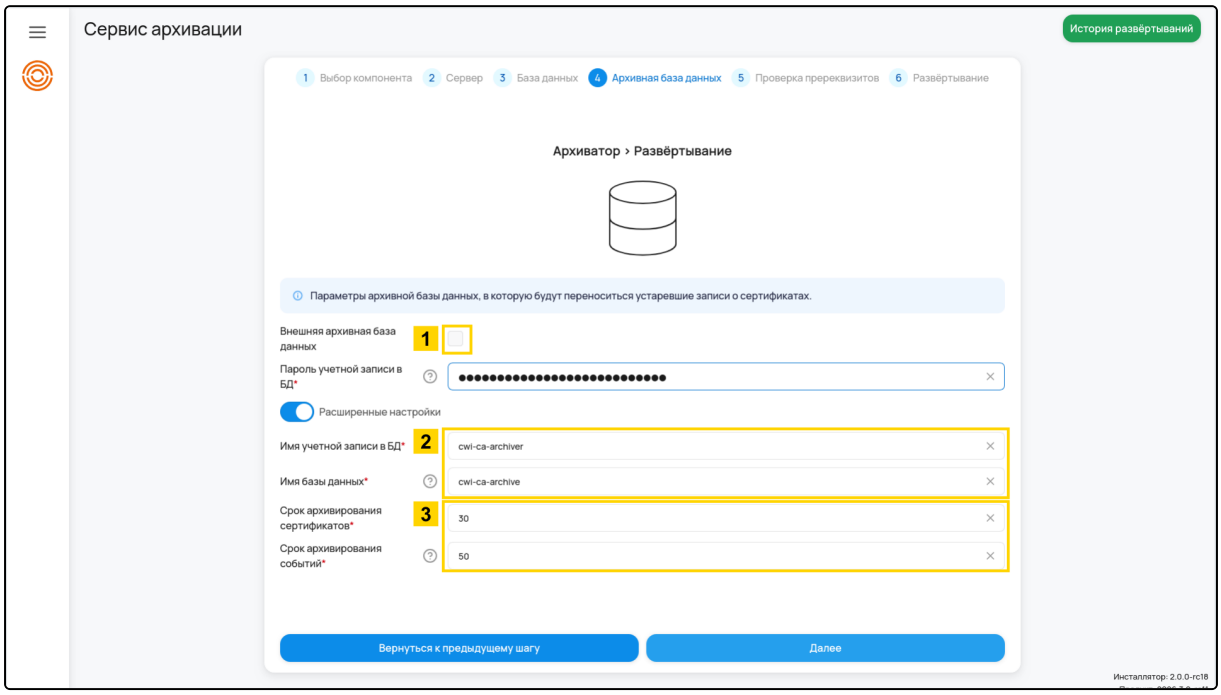
Параметр	Как заполнить
Пароль учетной записи в БД ЦС	Пароль учетной записи в БД PostgreSQL. Будет использоваться для подключения к БД ЦС. При повторной установке укажите действующий пароль существующей учетной записи БД.
Имя базы данных ЦС	Имя базы данных ЦС. Будет использоваться для подключения к ней. По умолчанию: Параметр ранее установленной базы данных ЦС.

15.3 Архивная база данных

Параметры архивной базы данных, в которую будут переноситься устаревшие записи о сертификатах.

Параметр	Как заполнить
Внешняя архивная база данных	Включите для архивной БД на отдельном сервере. Если переключатель выключен, архивная БД создаётся локально на сервере архиватора. По умолчанию: Выключено.
Имя сервера БД	FQDN или IP-адрес сервера архивной базы данных. Используется для подключения по SSH при установке и настройке архивной БД.
Пользователь сервера БД	Учетная запись на сервере архивной БД с правами sudo, от имени которой выполняется установка и настройка PostgreSQL.
Пароль сервера БД	Пароль учетной записи для подключения к серверу архивной БД по SSH.
Имя учетной записи в БД (расширенные настройки)	Имя учетной записи в БД PostgreSQL для архивной базы. Будет использоваться сервисом архивации для подключения к архивной БД. По умолчанию: cwi-ca-archiver.
Пароль учетной записи в БД	Пароль учетной записи в БД PostgreSQL для архивной базы. Будет использоваться сервисом архивации для подключения к архивной БД. При повторной установке укажите действующий пароль существующей учетной записи БД.
Имя базы данных (расширенные настройки)	Имя архивной базы данных ЦС. Будет использоваться сервисом архивации для подключения к ней. По умолчанию: cwi-ca-archive.
Срок архивирования сертификатов (расширенные настройки)	Возраст сертификатов в днях, старше которого они переносятся из рабочей БД ЦС в архивную базу данных. По умолчанию: 30.

Параметр	Как заполнить
Срок архивирования событий (расширенные настройки)	Возраст событий и запросов в днях, старше которого они переносятся из рабочей БД ЦС в архивную базу данных. По умолчанию: 50.



17 Рисунок 17. Параметры архивной базы данных.

1. Размещение архивной БД.
2. Учётная запись и имя архивной базы.
3. Сроки переноса сертификатов и событий.

15.4 Проверка и результат

Проверяются каталоги, права, linger, PostgreSQL, учётная запись архивной БД, сама база и доступ к ней.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

После установки проверьте archiver.service и его журнал. Стандартная задача запускается по расписанию @daily. Проверьте, что источник указывает на рабочую БД ЦС, а назначение на архивную, и что сроки хранения соответствуют принятой политике.

15.5 Файлы и службы

Объект	Назначение
/opt/itc/itc/config/itc api miniCA archiver config.json _	Источник, назначение, расписание и сроки архивирования.
archiver.service	Пользовательская служба архиватора.

16 SCEP

Выберите «SCEP». Подготовьте действующий ЦС, его сертификат, провайдер аутентификации и реквизиты БД SCEP. Один компонент выпускает TLS- и SCEP-сертификаты, получает JWT, создаёт подключение к PostgreSQL и запускает адаптер.

16.1 Сервер

Реквизиты подключения к серверу, на который будет установлен SCEP-сервис.

Параметр	Как заполнить
Имя сервера SCEP	FQDN или IP-адрес сервера, на который будет выполнена установка сервиса SCEP.
Пользователь сервера	Учетная запись на целевом сервере с правами sudo, от имени которой выполняется установка и настройка сервиса SCEP.
Пароль сервера	Пароль учетной записи для подключения к целевому серверу по SSH.

16.2 Сбор данных

Основные параметры сервиса: alias сервера, технологическая учетная запись и путь установки.

Параметр	Как заполнить
Alias сервера	Имя, которое будет указываться при обращении к серверу SCEP; на это имя будут выпущены TLS- и SCEP-сертификаты. По умолчанию совпадает с именем сервера, определённым командой hostname. Обязательное поле.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: itc-svc.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: /opt/itc.

16.3 ЦС

Параметры подключения к серверу ЦС для выпуска TLS-сертификатов сервиса.

Параметр	Как заполнить
Внешний ЦС	Включите, если центр сертификации (ЦС) расположен на отдельном сервере, отличном от сервера SCEP. При включении потребуется указать реквизиты подключения к серверу ЦС. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера ЦС	FQDN или IP-адрес сервера центра сертификации, выпускающего TLS- и SCEP-сертификаты для сервиса SCEP. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера ЦС	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH для выпуска TLS-сертификата. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера ЦС	Пароль учетной записи для подключения к серверу ЦС по SSH.
Сертификат ЦС	Сертификат центра сертификации в формате PEM/DER. Используется сервисом SCEP для проверки цепочки доверия при выдаче сертификатов. По умолчанию: Файл из результата предыдущего компонента, если он доступен в текущем сеансе.
Технологическая учетная запись (расширенные настройки)	Укажите технологическую учётную запись установленного ЦС. От её имени мастер запускает mclient на сервере ЦС. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. Используется для выпуска TLS-сертификата. По умолчанию: Каталог установленного ЦС; при отсутствии значения используется /opt/itc/minica.

16.4 База данных

Параметры базы данных PostgreSQL для хранения данных SCEP-сервиса.

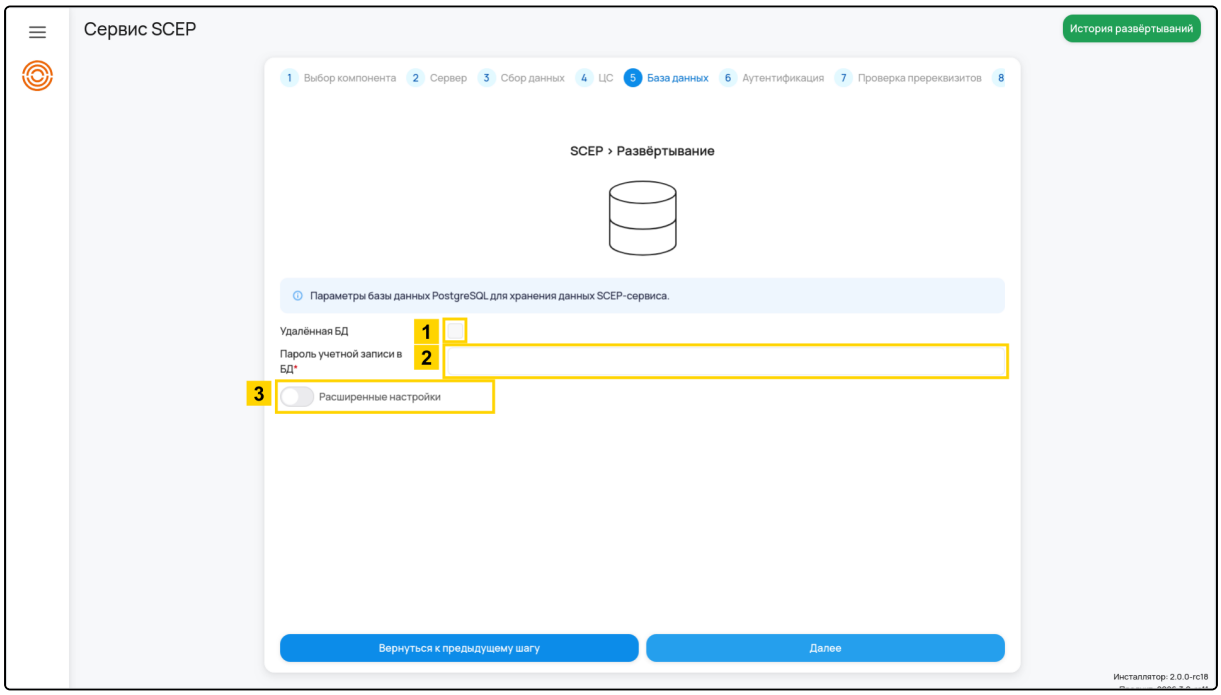
Параметр	Как заполнить
Удалённая БД	Включите, если база данных PostgreSQL SCEP-сервиса расположена на отдельном сервере. При выключенной опции PostgreSQL будет установлен на сервере SCEP, если его там нет. По умолчанию: Выключено.

Параметр	Как заполнить
Имя сервера БД	FQDN или IP-адрес сервера базы данных PostgreSQL.
Пользователь сервера БД	Учетная запись на сервере базы данных PostgreSQL с правами sudo, от имени которой создаются учетная запись и база данных SCEP-сервиса.
Пароль сервера БД	Пароль учетной записи для подключения к серверу базы данных PostgreSQL по SSH.
Учетная запись в БД (расширенные настройки)	Имя учетной записи PostgreSQL, от имени которой SCEP-сервис подключается к своей базе данных. По умолчанию: cwi-scep.
Пароль учетной записи в БД	Пароль учетной записи PostgreSQL. При повторной установке укажите действующий пароль существующей учетной записи.
Имя базы данных (расширенные настройки)	Имя базы данных PostgreSQL SCEP-сервиса. Схема данных создается сервисом автоматически при первом запуске. По умолчанию: cwi-scep.

16.5 Аутентификация

Параметры аутентификации SCEP-запросов: адрес издателя (issuer).

Параметр	Как заполнить
Адрес издателя (issuer)	URL провайдера аутентификации (issuer), по которому выполняется валидация токенов. Формат https://<fqdn>/realms/<realm> для Keycloak или https://<fqdn>/openid для Clearway OpenID. По умолчанию: Адрес издателя из ранее введённых настроек OpenID или контрольной панели.



18 Рисунок 18. База данных SCEP.

1. Переключатель размещения PostgreSQL.
2. Пароль учётной записи SCEP.
3. Расширенные параметры имени БД и пользователя.

16.6 Проверка и результат

Проверяются ЦС, PostgreSQL, права пользователя БД, доступ к БД, каталоги, Nginx, jq, OpenSSL, linger и доверенное хранилище.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Проверьте scepAdapter.service, подключение к БД и журнал запуска. Настройте тестовый SCEP-клиент на опубликованный адрес сервиса, выполните получение сертификата ЦС и тестовый запрос сертификата. Проверьте результат в ЦС.

16.7 Файлы и службы

Объект	Назначение
/opt/itc/itc/config/itc acm scepAdapte _ _ r clearwayCa config.json _ _	Подключения SCEP к PostgreSQL, ЦС и провайдеру аутентификации.

Объект	Назначение
/opt/itc/itc/nginx/scep.conf	Путь публикации SCEP через Nginx.
scepAdapter.service	Пользовательская служба SCEP.

В конфигурации Nginx путь /api/scep перенаправляется на локальный сервис 127.0.0.1:8440/api. Для клиента используйте опубликованный адрес https://<имя-сервера>/api/scep/v1/scep и проверьте его по действующей конфигурации Nginx. Пароль существующей БД указывайте повторно при переустановке; новый пароль в форме не меняет автоматически уже заданный пароль PostgreSQL.

17 Точки распространения CRL и сертификатов

Точка распространения настраивается внутри сценария ЦС. Для корневого ЦС её параметры вводятся при развёртывании, для выдающего при завершении настройки. По умолчанию используется сервер ЦС; для другого сервера включите «Точка распространения на отдельном сервере».

Параметр	Как заполнить
Точка распространения на отдельном сервере	Включите, если сервер точек распространения CRL и сертификатов (веб-сервер CDP) развёртывается на отдельном сервере, отличном от сервера ЦС. При выключении веб-сервер будет установлен на сервере ЦС. По умолчанию: Выключено.
Имя сервера точек распространения	FQDN или IP-адрес сервера, на который будет выполнена установка веб-сервера точек распространения (CDP).
Пользователь сервера точек распространения	Учетная запись на сервере точек распространения с правами sudo, от имени которой выполняется установка и настройка веб-сервера.
Пароль сервера точек распространения	Пароль учетной записи для подключения к серверу точек распространения по SSH.
Alias сервера точек распространения (расширенные настройки)	Имя, которое будет указываться в расширениях CDP и AIA выпущенных сертификатов и в конфигурации веб-сервера. Необязательно: если оставить пустым, будет использовано имя сервера точек распространения, определённое на нём командой hostname. Поле можно оставить пустым.
Технологическая учетная запись сервера точек распространения (расширенные настройки)	Учетная запись: владелец папки публикации сертификатов и CRL. От её имени создаётся структура папок. По умолчанию: Технологическая учётная запись ЦС.
Путь к папке публикации (расширенные настройки)	В указанной папке будут располагаться публикуемые файлы сертификатов и CRL. По умолчанию: /opt/itc/web.

В каталоге публикации создаются подкаталоги cdp для списков отзыва и aia для сертификатов. Nginx публикует их по адресам http://<имя-сервера>/cdp и http://<имя-сервера>/aia. Имя точки распространения используется в расширениях выпускаемых сертификатов.

После установки проверьте доступ к конкретным файлам сертификатов и CRL с клиентской машины. Убедитесь, что пути в расширениях сертификата совпадают с опубликованными URL. Для регулярного обновления списков настройте задания сервиса публикации; при быстрой установке такие задания создаются автоматически.

18 Резервное копирование

Установите контрольную панель, затем выберите «Резервное копирование». Сервис разворачивается на сервере панели. Имя сервера, пользователь, технологическая учётная запись и путь наследуются от неё; введите пароль SSH для подключения.

18.1 Сервер

Сервис резервного копирования устанавливается на сервер контрольной панели: реквизиты подключения, технологическая учетная запись и путь установки наследуются из её настроек.

Параметр	Как заполнить
Имя сервера контрольной панели	FQDN или IP-адрес сервера контрольной панели, на который будет выполнена установка сервиса резервного копирования. Наследуется из компонента контрольной панели. Поле заполняется автоматически и недоступно для изменения.
Пользователь сервера	Учетная запись на сервере контрольной панели, от имени которой выполняется установка и настройка сервиса резервного копирования. Наследуется из компонента контрольной панели. Поле заполняется автоматически и недоступно для изменения.
Пароль сервера	Пароль учетной записи для подключения к серверу контрольной панели по SSH.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки. От её имени будет работать сервис. По умолчанию: Наследуется из настроек контрольной панели. Поле заполняется автоматически и недоступно для изменения.
Путь к папке установки (расширенные настройки)	В указанной папке будут располагаться файлы устанавливаемого компонента. По умолчанию: Наследуется из настроек контрольной панели. Поле заполняется автоматически и недоступно для изменения.

18.2 Проверка и результат

Мастер проверяет подготовленные каталоги, зависимости сервиса и утилиты PostgreSQL, необходимые для копирования БД.

Дождитесь завершения проверок. Если доступна автоматическая настройка, нажмите «Выполнить настройку пререквизитов». После успешной проверки нажмите «Выполнить развёртывание» и дождитесь результата.

Откройте резервное копирование в контрольной панели и создайте задания для нужных узлов ЦС и БД. Проверьте каталоги хранения, расписание, доступ к узлам и результат первого копирования. Проверку восстановления выполняйте в отдельном подготовленном окружении.

18.3 Файлы и службы

Объект	Назначение
/opt/itc/itc/config/itc api miniCA backup config.json _	Параметры сервиса резервного копирования.
/opt/itc/itc/config/itc api miniCA config.json	Общая конфигурация подключений к ЦС.
backup.service	Пользовательская служба резервного копирования.

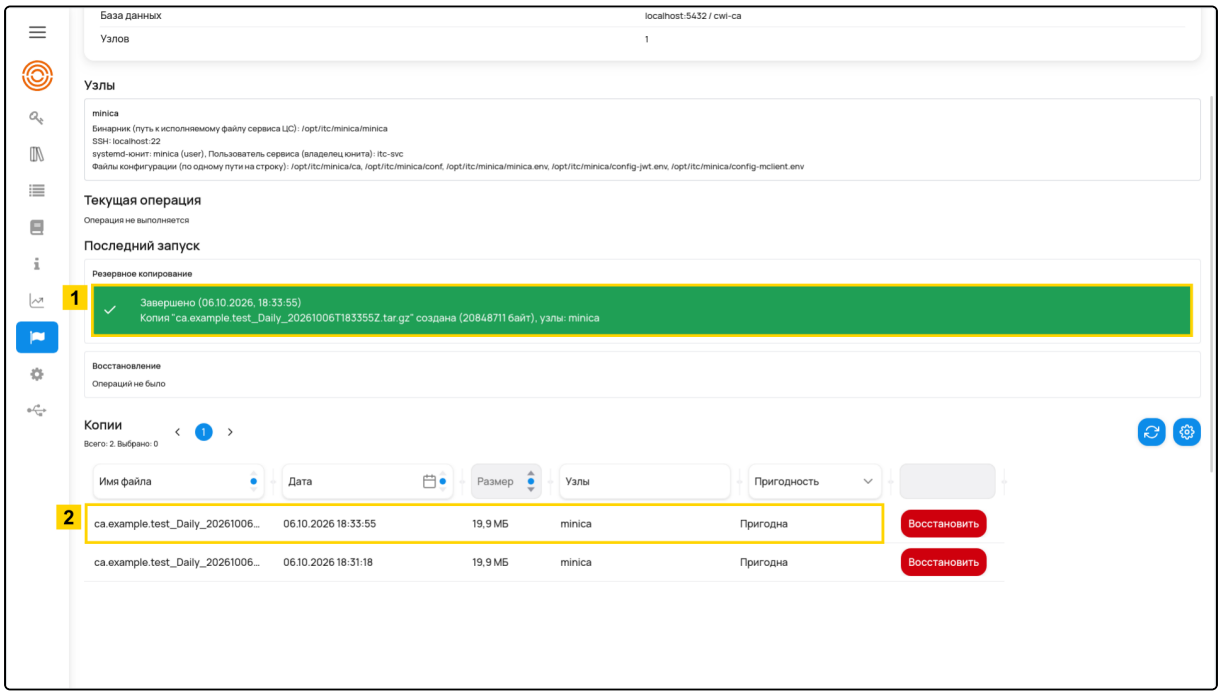
При быстрой установке создаётся ежедневное задание на 03:00. В расширенном сценарии создайте задания в панели после установки сервиса. Наличие активной службы не подтверждает наличие пригодной для восстановления копии; проверьте результат задания и восстановление.

18.4 Проверка состава и первый запуск копирования

Откройте «Задачи» → «Резервное копирование» и щёлкните по строке задания. В параметрах узла проверьте список файлов конфигурации. Включите каталог ключевого материала ЦС, например /opt/itc/minica/ca, перед каталогом /opt/itc/minica/conf. Также сохраните используемые env-файлы. В задании должны быть указаны правильная база данных, исполняемый файл ЦС и пользователь его службы.

Нажмите «Запустить копирование» и подтвердите операцию. Дождитесь состояния «Завершено» и появления архива в списке. Проверьте содержимое копии: дамп БД, ключ и сертификат ЦС, ключи шифрования и восстановления, конфигурацию и исполняемый файл. Статус «Пригодна» в интерфейсе не заменяет проверку состава архива и тест восстановления на отдельном сервере.

Архивы содержат закрытые ключи и реквизиты доступа. Ограничьте доступ к каталогу копий технологической учётной записью: каталог 0700, файлы 0600. Для backup.service задайте UMask=0077 через пользовательский drop-in systemd и перезапустите службу. Отдельно сохраните настройки и БД OpenID, конфигурацию CEP/CES и домена: задание копирования ЦС не включает их автоматически.



19 Рисунок 19. Результат резервного копирования.

1. Результат последнего копирования.
2. Созданный архив и его состояние.

19 Обновление установленного компонента

Для компонентов, поддерживающих обновление, мастер определяет установленную версию и считывает существующие пути и технологическую учётную запись. Сценарии миграции предусмотрены для ЦС, контрольной панели, сервиса публикации, OCSP и архиватора.

Перед обновлением сохраните резервную копию данных и конфигурации. Подготовьте доступ к исходной установке и действующие пароли. Выберите соответствующую группу, подключитесь к серверу и проверьте распознанные параметры. Не подставляйте стандартные пути вместо фактических.

Во время обновления мастер может останавливать сервис, заменять исполняемые файлы и применять миграции БД. Дождитесь завершения и проверьте состояние службы, доступность интерфейса и основные операции. При ошибке сохраните журнал и определите, какие действия уже выполнены, прежде чем повторять запуск.

Отсутствие сценария обновления у компонента не означает, что повторное развёртывание безопасно для существующей конфигурации. Для такого компонента используйте порядок обновления, предусмотренный его поставкой.

20 Обработка ошибок и проверка служб

Симптом	Проверка и действие
Не открывается мастер	Проверьте процесс itc-installer, адрес https://localhost:5224/installer и журнал запуска. Откройте браузер на том же рабочем месте.
Ошибка подключения к серверу	Проверьте DNS/IP, TCP 22, SSH-пользователя, пароль и права sudo. Уточните причину в журнале SSH и терминале мастера.
Не проходит проверка PostgreSQL	Проверьте состояние службы, адрес БД, имя пользователя, действующий пароль, pg hba.conf и сетевой доступ. Ошибка _ подключения не всегда означает отсутствие СУБД.
Не устанавливается пакет зависимости	Проверьте доступность репозитория ОС и вывод менеджера пакетов. Дождитесь завершения других операций apt/dnf.
Ошибка проверки сертификата	Проверьте срок действия, DNS-имя, соответствие ключу и цепочку доверия. Убедитесь, что загружен сертификат нужного ЦС или сервиса.
Не работает вход в панель	Проверьте доступность issuer с браузера и сервера панели, совпадение адресов и настройки клиента у провайдера. Для LDAP отдельно проверьте поиск пользователя и роли.
Панель не подключается к ЦС	Проверьте DNS и TCP 9443 с сервера панели, сертификат ЦС, параметры JWT и общий файл конфигурации подключения.
Ошибка MS-WSTEP	Проверьте DNS домена, время, членство сервера в AD, keytab, доступ к LDAP и журналы CEP/CES.
Сервис публикации или копирования недоступен	Проверьте соответствующую службу, её журнал и настройки подключения в контрольной панели. Затем проверьте отдельное задание.
Прогресс не обновляется	Проверьте состояние операции на сервере и в истории развёртываний. Повторяйте шаг только после завершения или остановки предыдущей операции.

Для пользовательских служб выполняйте команды в сеансе технологической учётной записи. При стандартном имени сначала перейдите в её сеанс:

```
sudo -iu itc-svc
export XDG_RUNTIME_DIR=/run/user/$(id -u)
export DBUS_SESSION_BUS_ADDRESS=unix:path=$XDG_RUNTIME_DIR/bus
```

```
systemctl --user status minica.service
journalctl --user -u minica.service -n 100 --no-pager
```

Замените minica.service на имя проверяемой службы. Проверьте linger командой loginctl show-user itc-svc -p Linger. При успешной настройке вывод содержит Linger=yes.

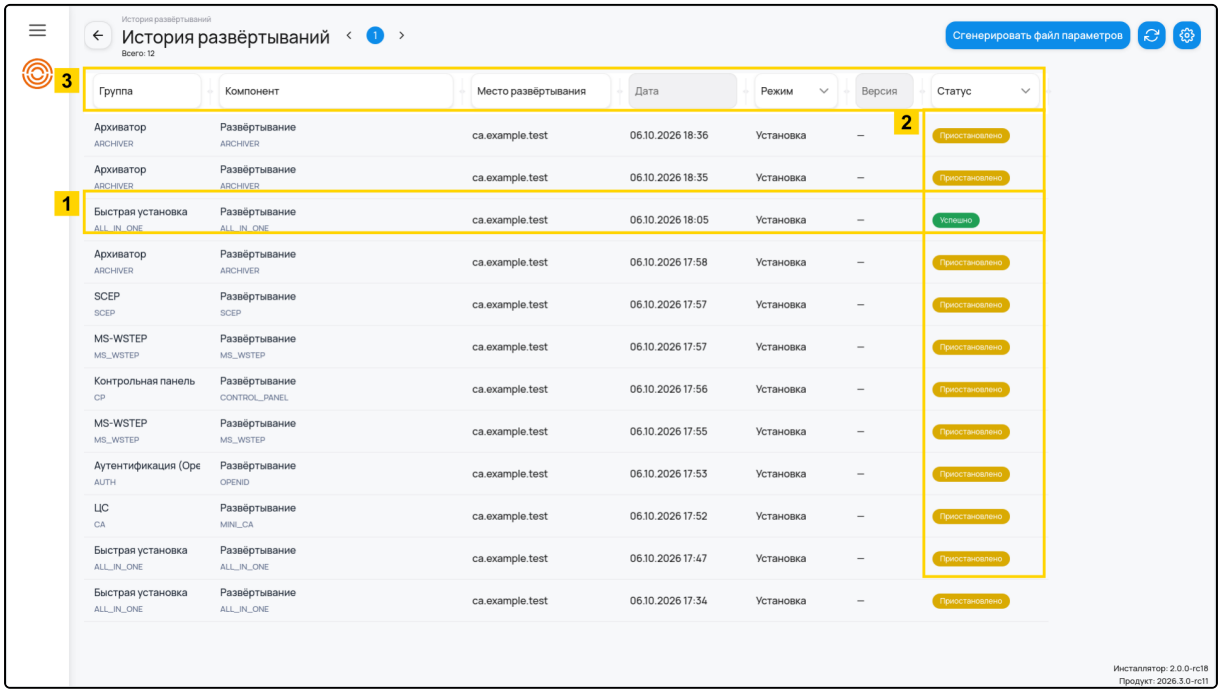
Для проверки ЦС в том же сеансе используйте его фактический каталог:

```
export MCLIENT_CONF=/opt/itc/minica/conf/mclient.yml
/opt/itc/minica/mclient ping
```

Перед передачей журнала в поддержку удалите из копии пароли, токены и закрытые ключи. Сохраните названия ошибок, этап, имя компонента и сведения о том, какие действия уже выполнены.

21 История развёртываний

Кнопка «История развёртываний» в правом верхнем углу открывает сохранённые операции. Используйте историю для поиска выполненного компонента, просмотра результата и разбора ошибок.



20 Рисунок 20. История развёртываний.

1. Успешно завершённое развёртывание.
2. Статусы сохранённых операций.
3. Поиск и фильтры таблицы.

Откройте нужную запись. Сверьте параметры, результаты, пререквизиты, выполненные команды и журнал терминала. Если операция завершилась ошибкой или была приостановлена, установите состояние сервера перед повторным запуском.

Файлы сертификатов и запросов сохраните в предназначенное для них место. Доступ к истории и служебным файлам инсталлятора должен быть у администраторов, которым разрешена работа с параметрами развёртывания.

22 Дополнительные компоненты

Группа «Остальные компоненты» содержит отдельный выпуск JWT для контрольной панели и создание тестовых данных. Они используются после подготовки соответствующего ЦС и сервисов.

22.1 Выпуск JWT

Компонент добавляет подключение контрольной панели к выбранному ЦС. Укажите сервер панели, реквизиты ЦС, его сертификат и название подключения. Затем задайте имя JWT и роль токена. Роль должна соответствовать операциям, которые разрешены панели на этом ЦС.

Параметр	Как заполнить
Имя сервера контрольной панели	FQDN или IP-адрес сервера, на котором установлена контрольная панель. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера	Учетная запись на сервере контрольной панели, от имени которой выполняется подключение по SSH. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пароль сервера	Пароль учетной записи для подключения к серверу контрольной панели по SSH.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки контрольной панели. По умолчанию: Учётная запись из параметров контрольной панели; если она не задана, itc-svc.
Путь к папке установки КП (расширенные настройки)	Путь к папке установки контрольной панели на целевом сервере. По умолчанию: Каталог из параметров контрольной панели; если он не задан, /opt/itc.
Внешний ЦС	Включите, если центр сертификации (ЦС) расположен на отдельном сервере, отличном от сервера контрольной панели. При включении потребуется указать реквизиты подключения к серверу ЦС. По умолчанию: Зависит от размещения сервиса и выбранного сервера.
Имя сервера ЦС	FQDN или IP-адрес сервера центра сертификации, выпускающего JWT для контрольной панели. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.
Пользователь сервера ЦС	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH. По умолчанию: Значение из ранее введённых параметров соответствующего сервера.

Параметр	Как заполнить
Пароль сервера ЦС	Пароль учетной записи для подключения к серверу ЦС по SSH.
Название ЦС (расширенные настройки)	Название ЦС для имён файлов (<название>-jwt.key, <название>-jwt.crt, <название>.jwt, <название>.crt) и идентификатор записи в общем конфигурационном файле сервисов itc api miniCA config.json _ _ _ (MiniCa.<название>). Допускаются только латинские буквы, цифры и дефис. Если не указано: используется имя сервера ЦС (или сервера КП, если ЦС совмещён с ней). Поле можно оставить пустым.
Сертификат ЦС	Сертификат центра сертификации в формате PEM/DER. Используется контрольной панелью для проверки цепочки доверия при обращении к этому ЦС. Файл на сервере называется по названию ЦС.
Технологическая учетная запись ЦС (расширенные настройки)	Укажите технологическую учётную запись установленного ЦС. От её имени мастер запускает mclient на сервере ЦС. По умолчанию: Учётная запись ранее установленного сервиса; при отсутствии значения используется itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. По умолчанию: Каталог установленного ЦС; при отсутствии значения используется /opt/itc/minica.
Имя JWT (jwt-name)	Значение параметра jwt-name выпускаемого токена. По умолчанию: ControlPanel.
Роль JWT (jwt-role)	Значение параметра jwt-role выпускаемого токена. По умолчанию: admin.

Мастер формирует ключевую пару на сервере панели, выпускает JWT через mclient и добавляет запись MiniCa.<название> в /opt/itc/itc/config/itc_api_miniCA_config.json. Файлы <название>-jwt.key, <название>-jwt.crt и <название>.jwt размещаются в /opt/itc/itc/certs. Для другого ЦС повторите компонент с его реквизитами и отдельным названием.

22.2 Тестовые данные

Компонент выпускает тестовые сертификаты и отзывает заданную часть. Используйте его на предназначенном для проверки ЦС: повторный запуск добавляет новую пачку записей и обновляет CRL. Удаление ранее выпущенных сертификатов не выполняется автоматически.

Параметр	Как заполнить
Имя сервера ЦС	FQDN или IP-адрес сервера выдающего ЦС.

Параметр	Как заполнить
Пользователь сервера	Учетная запись на сервере ЦС, от имени которой выполняется подключение по SSH.
Пароль сервера	Пароль учетной записи для подключения к серверу ЦС по SSH.
Технологическая учетная запись (расширенные настройки)	Учетная запись: владелец папки установки ЦС, от её имени выполняется выпуск. По умолчанию: itc-svc.
Путь к папке установки ЦС (расширенные настройки)	Путь к папке установки ЦС, в которой расположен исполняемый файл mclient. По умолчанию: /opt/itc/minica.
Количество сертификатов	Сколько тестовых сертификатов выпустить за один запуск. Миллион выпускается часами. По умолчанию: 1000000.
Отзывать каждый N-й	Отзыв каждого N-го выпущенного сертификата (50: каждый пятидесятый). 0: не отзывать. По умолчанию: 50.
Срок действия, дней	Срок действия выпускаемых сертификатов в днях. По умолчанию: 366.
Шаблон сертификата	Имя шаблона сертификата на ЦС. При установке создаются шаблоны tls и ocsp. По умолчанию: tls.
Префикс Common Name	Префикс Common Name выпускаемых сертификатов. По умолчанию: seed.

Укажите число сертификатов, периодичность отзыва, срок действия, шаблон и префикс Common Name. В одной пачке используется один закрытый ключ; различаются Common Name и серийные номера. Большие пачки могут выпускаться несколько часов. После завершения проверьте количество записей, статусы отозванных сертификатов, CRL и ответы OCSP.

23 Проверка установленного комплекса

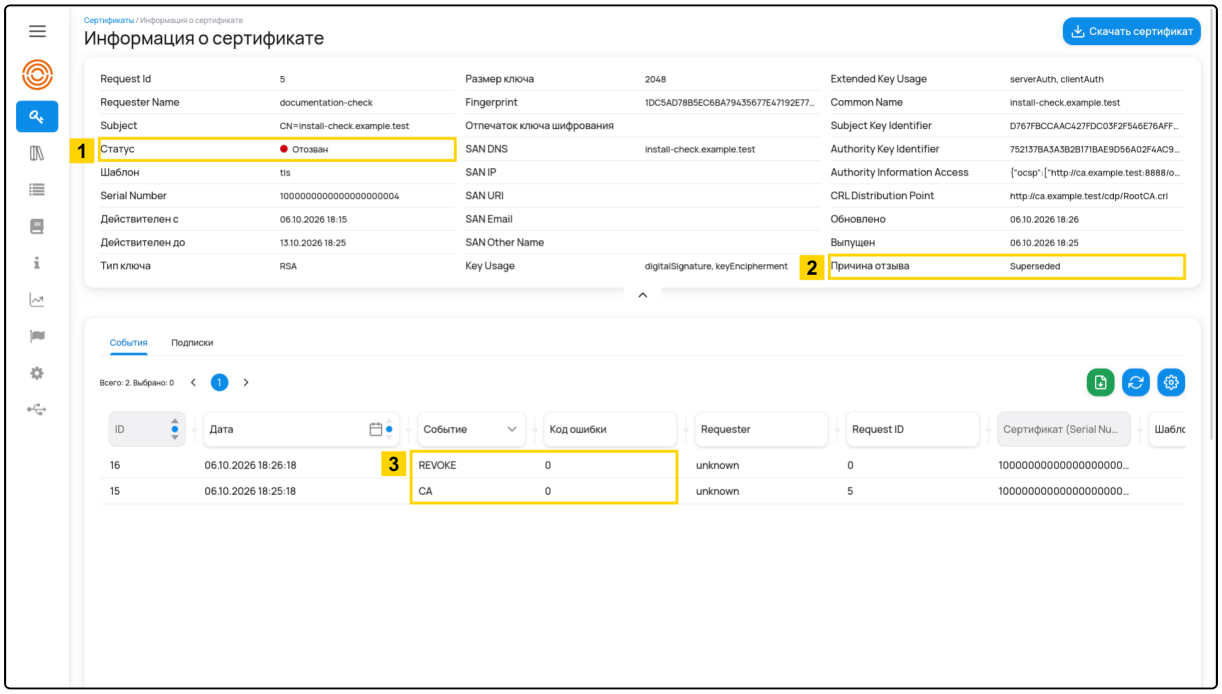
Проверяйте комплекс с рабочего места пользователя. Успешный запуск служб подтверждает только их состояние; для проверки связей между компонентами выполните операции с тестовым сертификатом.

23.1 Вход и соединение с ЦС

Откройте контрольную панель по её DNS-имени и войдите учётной записью администратора. Проверьте доступность подключённого ЦС и загрузку списка сертификатов. Если подключён LDAP, отдельно выполните вход доменной учётной записью и проверьте её права.

23.2 Выпуск и отзыв сертификата

Выпустите сертификат для тестового DNS-имени по шаблону tls. Скачайте сертификат и цепочку доверия. Проверьте Subject, SAN, издателя и срок действия. Затем отзовите этот сертификат с выбранной причиной и убедитесь, что его статус изменился на «Отозван». Для этой проверки используйте отдельный сертификат: отзыв действующего сертификата сервиса нарушит его работу.



21 Рисунок 21. Проверка тестового сертификата после отзыва.

1. Статус сертификата изменился на «Отозван».
2. Указана выбранная причина отзыва.
3. В журнале видны события выпуска CA и отзыва REVOKE с кодом ошибки 0.

23.3 OCSP и публикация списков отзыва

До отзыва проверьте, что OCSP возвращает good, а после отзыва: revoked. Проверьте подпись ответа по доверенной цепочке. Получайте адрес OCSP из сертификата или из согласованной конфигурации. Сертификат издателя в запросе должен соответствовать ЦС, выпустившему проверяемый сертификат.

```
openssl ocsp -issuer issuer.crt -cert test.crt \
  -url http://<имя-сервера>:8888/ocsp -CAfile chain.pem -resp_text
```

В разделе задач публикации запустите задание CRL, затем скачайте файл по адресу CDP из сертификата. Проверьте издателя и срок действия CRL. Серийный номер отозванного сертификата должен присутствовать в опубликованном списке.

23.4 SCEP и резервная копия

Для SCEP проверьте ответы GetCACaps и GetCACert по опубликованному адресу. Эти операции подтверждают доступность сервиса и выдачу цепочки; отдельно выполните запрос сертификата с реального SCEP-клиента, если этот протокол используется в вашей установке.

Создайте резервную копию, как описано в разделе «Резервное копирование», и проверьте её содержимое. Испытание восстановления выполняйте на отдельном подготовленном экземпляре по процедуре восстановления. Наличие архива и статус «Пригодна» не подтверждают успешное восстановление.

24 Обновление Clearway CA до 2026.3.0

24.1 Шаги обновления

Применяются к любой установке, включая обновлённую инсталлятором: конфигурация `conf/minica.yml` при обновлении сохраняется как есть.

1. Настройте TLS для подключения к PostgreSQL. ЦС и mOCSP теперь требуют TLS с проверкой цепочки и имени сервера и не стартуют без настроенного блока `database.tls`. При самоподписанном сертификате БД укажите `ca-cert` или явно разрешите работу без шифрования. Параметр `database.allow-without-tls` устарел MCA-1695[1]
2. Добавьте в роль `admin` (секция `jwt.roles` файла `conf/minica.yml`) новые права ротации ключей ЦС: `new-ca-req`, `new-ca-cert`, `ca-rotation-status`, `new-root-ca-cert`, `cancel-ca-rotation`. Без них операции ротации вернут ошибку доступа. У новых установок права уже включены в роль MCA-1539[2]
3. Примените миграции БД ЦС: при обновлении инсталлятором они выполняются автоматически; если ЦС обновляется вручную, выполните шаги из раздела «Обновление без инсталлятора» MCA-1679[3]

24.2 Обновление без инсталлятора

Если ЦС ставился и обновляется вручную, SQL-миграции БД применяются самостоятельно: инсталлятор в этом случае не запускается. Файлы миграций лежат в папке `sql/` рядом с этим документом и применяются к базе данных ЦС (та же БД, что указана в `conf/minica.yml`) до запуска новых бинарников, в порядке возрастания имён:

1. `20260715124034_minica-v2.9.x-add-template-lower-indexes.up.sql`: индексы по `LOWER(template)` в таблицах `cert` и `csr`.
2. `20260909154123_minica-v2.9.x-enable-pg-trgm.up.sql`: расширение `pg_trgm` для индексированного поиска по подстроке.
3. `20260909154124_minica-v2.9.x-add-cert-subj-trgm-index.up.sql`: GIN-индекс по колонке `subj` таблицы `cert`.
4. `20260917120000_minica-v2.9.x-ca-rotation.up.sql`: значение статуса `CA_ROTATION` и таблица журнала ротации ключей ЦС.

Применение (каждый файл отдельным запуском):

---

1 https://tasks.clearwayintegration.com/browse/MCA-1695
2 https://tasks.clearwayintegration.com/browse/MCA-1539
3 https://tasks.clearwayintegration.com/browse/MCA-1679

```
psql -h <хост> -U <пользователь> -d <база ЦС> -f <>
```

Миграции идемпотентны, повторный запуск безопасен. Ограничения:

- Файл 3 выполняется с `CREATE INDEX CONCURRENTLY`, его нельзя оборачивать в явную транзакцию (`BEGIN` / `COMMIT`).
- Для файла 2 нужны права на установку расширений. В PostgreSQL 13 и новее `pg_trgm` доверенное расширение и ставится без суперпользователя, на более старых версиях нужен суперпользователь.

Установленному через инсталлятор ЦС ничего из этого делать не требуется: миграции применяются шагом обновления автоматически.