



Cryptallit

Руководство администратора системы

Версия: 1.1

Дата: 01.07.2022г.

Оглавление

<i>Термины и определения</i>	2
<i>Общие сведения</i>	3
Назначение Системы	3
Описание компонентов Системы	3
<i>Установка и удаление программ</i>	4
Сервер управления.....	4
Консоль администратора	5
Агент рабочей станции	7
Файловый сервер.....	10
<i>Настройка Системы</i>	10
<i>Управление сетевыми ресурсами</i>	15
Общие характеристики сетевых ресурсов	15
Удаление сетевого ресурса.....	18
<i>Управление пользователями</i>	19
Создание учетной записи пользователя.....	19
Изменение свойств пользователя	20
Удаление пользователей	21
<i>Управление свойствами групп</i>	22
Создание группы.....	22
.....	23
Изменение свойств группы.....	23
Удаление группы	24
Управление доступом к защищенным ресурсам.....	24
Добавление пользователей в группу	24
Доступ к сетевому ресурсу для группы	26

Термины и определения

КА	Консоль администратора
АРС	Агент рабочей станции
СУ	Сервер управления
ФС	Файловый сервер
СР	Сетевой ресурс
ИР	Идентификатор ресурса
ПО	Программное обеспечение

Общие сведения

Назначение Системы

Cryptallit — это автоматизированная система управления дистанционного доступа к информационным ресурсам, которая реализует максимально удобный и простой способ управления большим количеством учетных записей пользователей. Программные агенты системы функционируют на рабочих станциях пользователей. Эффективно собирая информацию о конфигурационных параметрах учетной записи пользователей, агент передает собранную информацию в единую базу данных системы. На основе этой информации будет осуществляться управление конфигурационными профилями пользователей.

В программе реализованы следующие функции:

- Управление доступом к информационным ресурсам;
- Автоматизация ИТ-процессов по управлению учетными записями пользователей.

Решаемые задачи:

- Оптимизация состава и структуры учетных записей пользователей;
- Автоматизированное формирование групп пользователей;
- Сбор информации о ресурсах инфраструктуры;
- Защита файлового сервера в облаке при помощи интеграции с Crypto Pro CSP

Описание компонентов Системы

Система состоит из программных компонентов, взаимодействующих между собой посредством сетевых или программных интерфейсов:

- Агент рабочей станции (АРС) - выполняет основную бизнес-логику приложения и сбор информации о пользователях. Предоставляет пользователю доступ на сервер.
- Сервер управления (СУ) – реализует служебные функции управления Системой. На нем хранится и обрабатывается вся информация о пользовательских учетных записях, параметрах системы и конфигурации компонентов Системы.
- Файловый сервер (ФС) – обеспечивает хранение и доступ пользователей к сетевым ресурсам. Файловый сервер является неактивным компонентом Системы, предназначенный только для хранения массивов информации.
- Консоль администратора ИБ (КА) – предоставляет интерфейс управления и настройки конфигурационных параметров Системы. а также возможность управления режимами функционирования компонентов Системы

Установка и удаление программ

Сервер управления

Технические требования для установки сервера управления, описаны в таблице 1:

Таблица 1- Технические требования СУ

Характеристика	Необходимое значение
Сервер управления (СУ)	
Среда функционирования	Операционная система Windows Server Аппаратная или виртуальная платформа с архитектурой Intel x64
Объем оперативной памяти	Не менее 1Gb
Объем памяти на HDD сервера	Не менее 2Gb
Учетная запись	Администратор системы

Установка сервера управления

- ▶ *Интерфейс установки сервера управления состоит из последовательности окон (шагов). Чтобы переключаться между окнами установки программы, требуется использовать кнопки **Назад** и **Установить**. Работа по установке программы завершается нажатием на кнопку **Готово**. Чтобы прекратить работу по установке программы на любом этапе, следует нажать на кнопку **Отмена**.*

Для установки Сервера управления выполните следующие шаги:

1. Запустите установочный файл `cl-server-x.x.x.xx-x64.msi` с правами Администратора сервера
2. Прочитайте и примите условия лицензионного соглашения. Подтвердите установку, нажав на кнопку **Установить**. Для отмены установки нажмите **Отмена**.

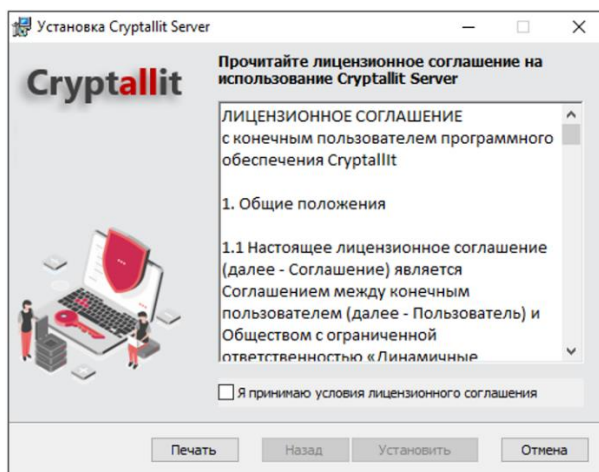


Рисунок 1

3. Подтвердите завершение установки, нажав клавишу **Готово**.

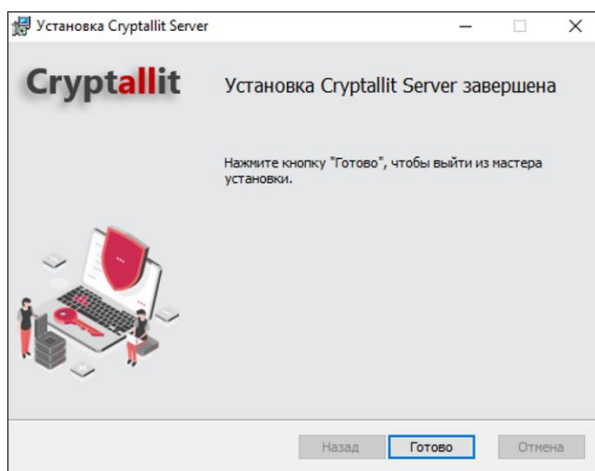


Рисунок 2

Консоль администратора

Технические требования к компьютеру, на который устанавливается Консоль администратора, описаны в таблице 2:

Таблица 2- Технические требования КА

Характеристика	Необходимое значение
Консоль администратора ИБ (КА)	
Среда функционирования	Операционная система Windows 10 / 11 Аппаратная или виртуальная платформа с архитектурой Intel x64
Объем оперативной памяти	Не менее 1Gb
Объем памяти на HDD сервера	Не менее 2Gb
Учетная запись	Администратор системы с правом установки прикладного и системного ПО

Установка консоли администратора КА

- ▶ *Интерфейс установки консоли администратора КА (далее – КА) состоит из последовательности окон (шагов). Чтобы переключаться между окнами установки программы, требуется использовать кнопки **Назад** и **Далее**. Работа по установке программы завершается нажатием на кнопку **Завершить**. Чтобы прекратить работу по установке программы на любом этапе, следует нажать на кнопку **Отмена**.*

Для установки КА выполните следующие действия:

1. Запустите установочный файл: cl-mc-x.x.x.xx-x64.msi. на рабочей машине с правами Администратора сервера. Примите условия лицензионного соглашения.

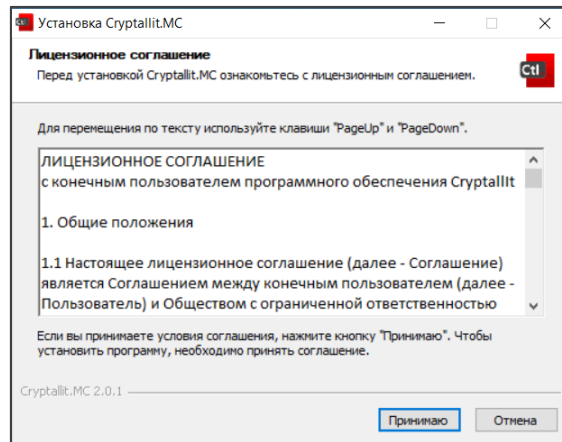


Рисунок 3

2. Модуль КА может быть установлен несколькими способами:

- Индивидуальным – программа будет доступной только для текущего пользователя,
- Общим – программа будет доступна для всех пользователей рабочей станции)

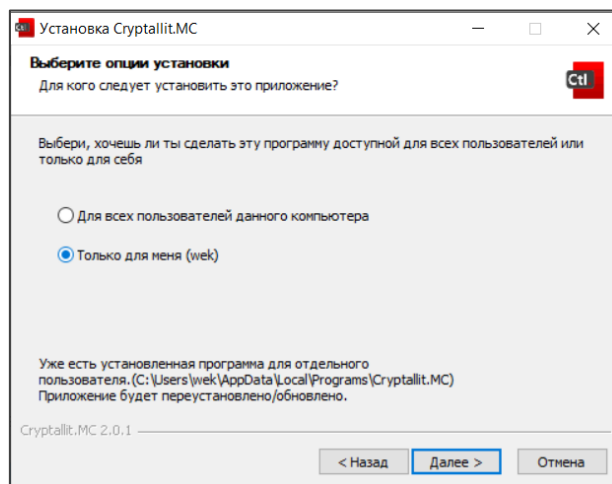


Рисунок 4

3. Выберите папку, в которую будет установлена программа

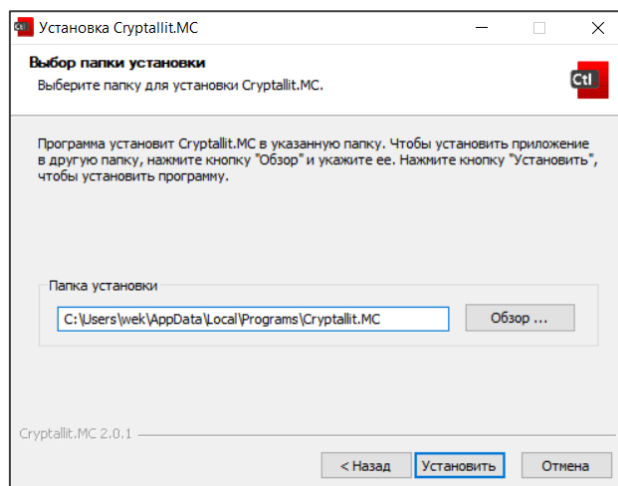


Рисунок 5

4. Подтвердите завершение установки, нажав на кнопку Готово.

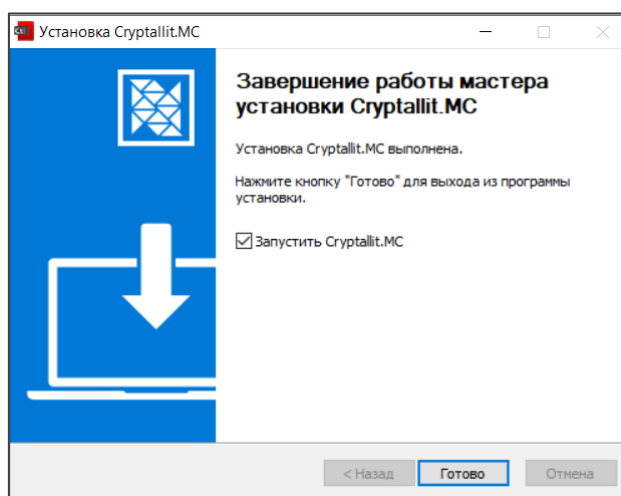


Рисунок 6

Агент рабочей станции

Агент рабочей станции - выполняет основные операции системы. Предоставляет пользователю доступ на ресурс. Технические характеристики для установки представлены в таблице 3:

Таблица 3 - Характеристики агента рабочей станции

Характеристика	Необходимое значение
Агент рабочей станции	
Среда функционирования	Операционная система Windows 10 / 11 Аппаратная или виртуальная платформа с архитектурой Intel x64
Объем оперативной памяти	Не менее 1Gb
Объем памяти на HDD сервера	Не менее 2Gb

Установка агента рабочей станции

- ▶ *Интерфейс агента рабочей станции состоит из последовательности окон (шагов). Чтобы переключаться между окнами установки программы, требуется использовать кнопки **Назад** и **Установить**. Разрешите приложению внести изменения на устройстве, нажав **Да**. Работа по установке программы завершается нажатием на кнопку **Готово**. Чтобы прекратить работу по установке программы на любом этапе, следует нажать на кнопку **Отмена**.*

Для установки агента рабочей станции выполните следующие действия:

1. Запустите установщик cl-workstation-x.x.x.xx-x64.msi на рабочей станции из сеанса пользователя. Ознакомьтесь и примите условия лицензионного соглашения.

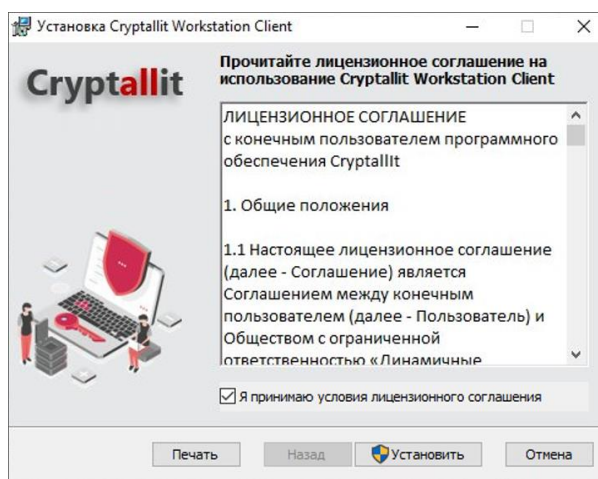


Рисунок 7

2. На системный запрос подтверждения изменений на рабочей станции ответить «Да»

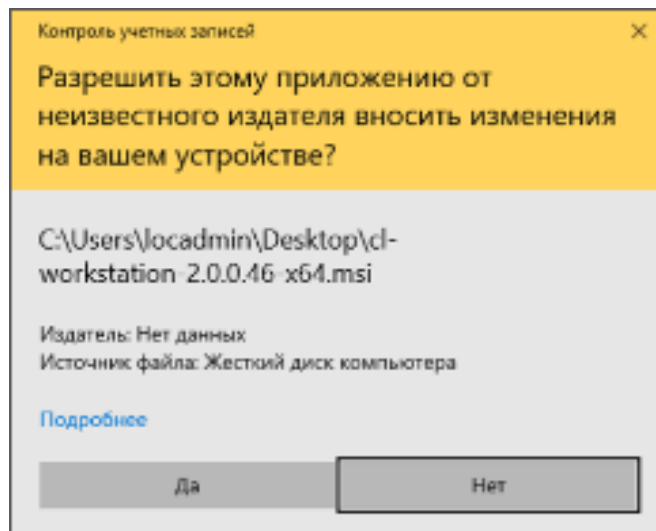


Рисунок 8

3. Подтвердите завершение установки, нажав на кнопку Готово.

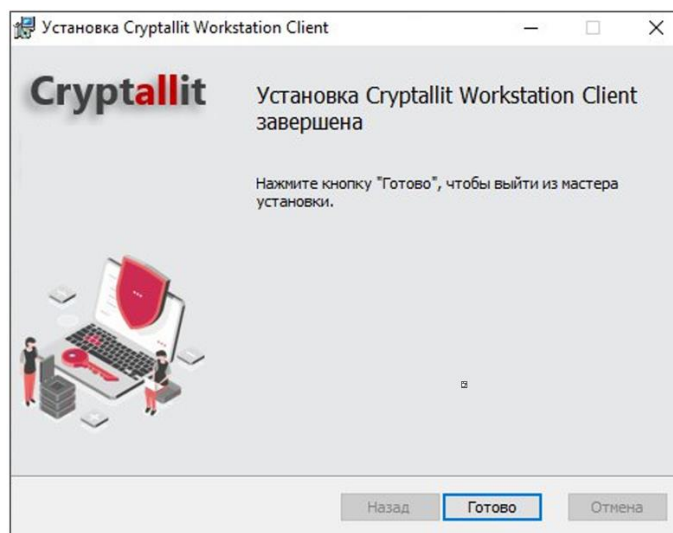


Рисунок 9

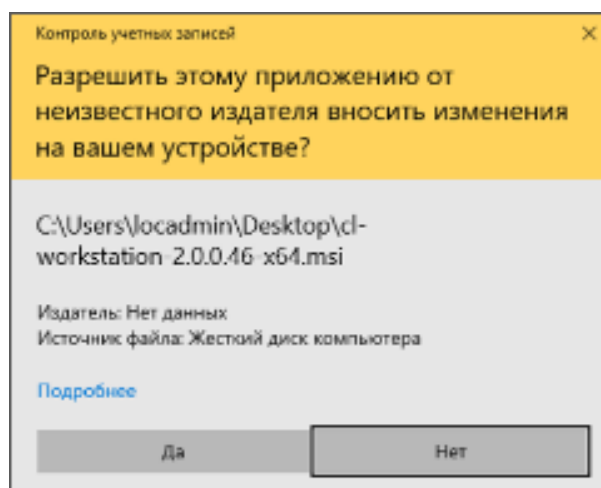


Рисунок 10

1. Подтвердите завершение установки, нажав на кнопку «Готово».

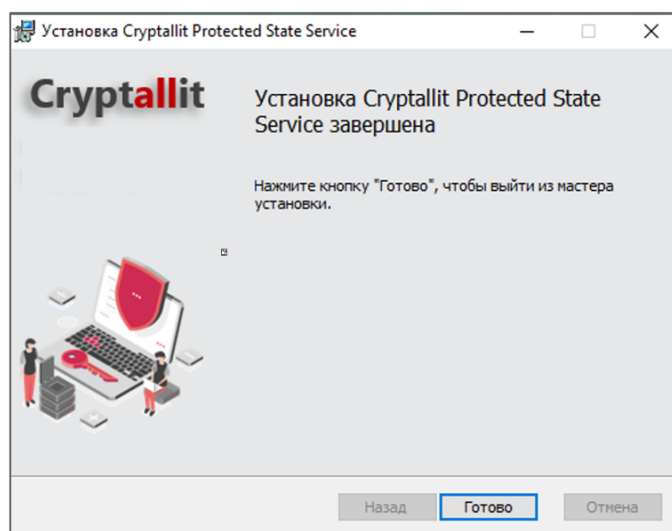


Рисунок 11

Файловый сервер

Технические требования необходимы для установки Файлового сервера, представлены в таблице 5:

Таблица 4- Технические требования ЗШР

Характеристика	Необходимое значение
Защищенный файловый сервер (ЗФС)	
Среда функционирования	Существующий сервер, на котором размещены файловые архивы и организован доступ по протоколу SMB3.0 Или Новый тестовый файловый сервер ориентировочно аналогичный по характеристикам с существующим.
Объем оперативной памяти	-
Объем памяти на HDD сервера	-
Учетная запись	-

Настройка Системы

После установки программ системы Cryptallit необходимо произвести ряд общесистемных настроек на компонентах.

Разрешение доступа к СУ по сети

- ▶ Для работы СУ необходимо разрешить сетевые подключения к нему в Windows Firewall. Для этого лучше всего создать правило для этого приложения, а не для порта 41254, который используется по умолчанию, но может быть изменен.

Для создания правил выполните следующие действия:

1. Откройте Windows Defender Firewall (для быстрого запуска используйте команду `wf.msc` в окне Run)
2. Создайте правило, разрешающее входящие соединения по протоколу TCP для приложения: `'%Cryptallit\Server\ControlService.exe'`. Данное правило является службой Cryptallit.

Другие параметры правил оставьте по умолчанию, или же настройте в соответствии со своим сетевым оборудованием.

- ▶ Служба Cryptallit по умолчанию использует порт 41254. Это значение можно поменять в Реестре.
- ▶ Команда для добавления правила:

```
netsh advfirewall firewall add rule name="Cryptallit" dir=in action=allow Program="%ProgramFiles%\Cryptallit\Server\ControlService.exe"
```

Настройка DNS для быстрого обнаружения СУ

Агенты рабочих станций (далее - APC) по умолчанию запрашивают в локальной службе DNS сервис с именем `_ctl._tcp`. Если запись имеется, то APC автоматически настраивает связь или подключение сетевой компьютер с сервером управления и порт в соответствии с полученными значениями. В этом случае ручной настройки в APC не требуется, что упрощает и ускоряет их развертывание, поэтому рекомендуется создавать SRV-запись в сетевом домене (или доменах) установлены рабочие станции с APC. Для управления DNS-записями необходим административный доступ к управлению службой DNS, который обычно есть у сетевого администратора организации.

SRV запись для СУ должна иметь следующий вид:

```
SRV name: _ctl
Protocol: _tcp
Hostname: <имя СУ>.<имя домена>
Port: 41254
```

Проверить наличие записи можно командой nslookup:

```
nslookup -type=srv _ctl._tcp"
```

Ответ будет примерно таким, если в домене ctl.zone обнаружена такая запись:

```
_ctl._tcp.ctl.zone      SRV service location:
  priority              = 0
  weight                = 0
  port                  = 41254
  svr hostname          = ctldev.ctl.zone
ctldev.ctl.zone internet address = 10.10.10.100
```

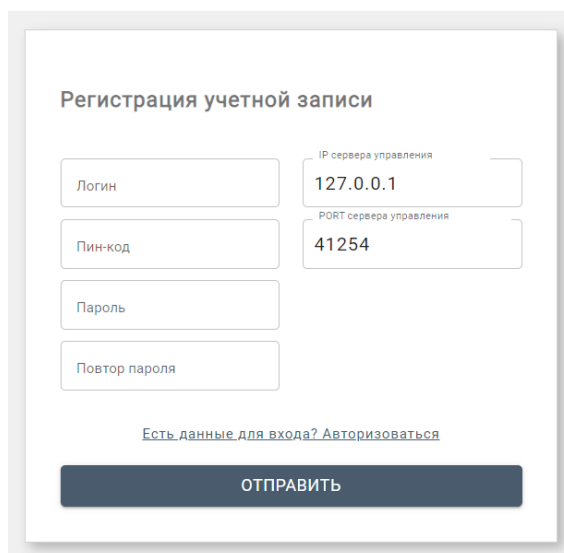
Настройки консоли администрирования

Для управления параметрами Системы необходимо запустить КА и выполнить регистрацию первой учетной записи администратора.

- ▶ *Приложение КА запускается стандартным способом из панели меню «Пуск». Для запуска необходимо выбрать в меню программу «Cryptallit.MC».*

Регистрация администратора

При первом запуске КА будет отображено окно регистрации администратора. Под термином «регистрация» в данном случае подразумевается создание учетной записи FirstAdmin.



The screenshot shows a web-based registration form titled "Регистрация учетной записи" (Registration of account). The form contains several input fields: "Логин" (Login), "Пин-код" (PIN code), "Пароль" (Password), and "Повтор пароля" (Repeat password). On the right side, there are two fields for server settings: "IP сервера управления" (Management server IP) with the value "127.0.0.1" and "PORT сервера управления" (Management server PORT) with the value "41254". Below the form, there is a link that says "Есть данные для входа? Авторизоваться" (Have login data? Authorize) and a large blue button labeled "ОТПРАВИТЬ" (SEND).

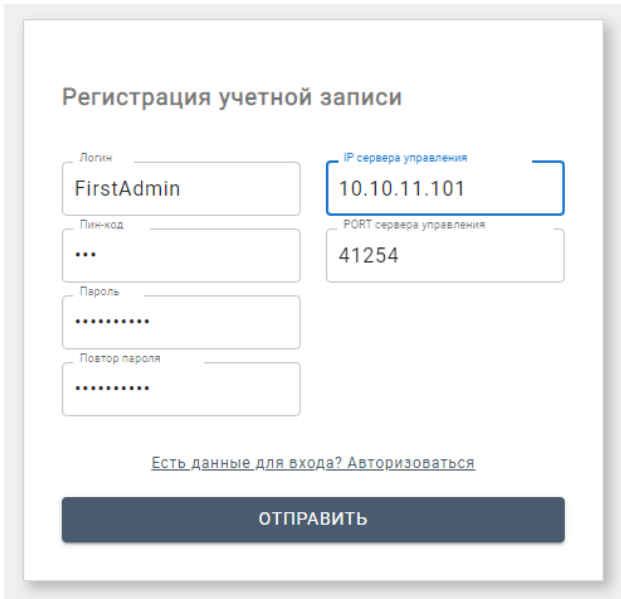
Рисунок 12

- ▶ *Регистрация первого администратора системы производится с заданными (предустановленными) значениями некоторых параметров, после успешной регистрации и входа в систему администратору рекомендуется создать вторую (альтернативную) учетную запись администратора системы и в дальнейшем использовать именно ее.*

1. Для регистрации учетной записи администратора необходимо заполнить следующие поля:

- **Логин:** FirstAdmin
- **Пин-код:** 123 (предустановленное, одноразовое значение пин-кода)
- **Пароль:** Введите пароль
- **Повтор пароля:** Повторите ввод пароля
- **IP сервера управления:** Введите IP адрес сервера СУ
- **PORT сервера управления:** Введите порт - по умолчанию 41254 (или альтернативный порт если был переназначен при конфигурировании СУ)

2. Нажмите на кнопку «Отправить».



The image shows a registration form titled "Регистрация учетной записи" (Registration of an account). The form contains several input fields: "Логин" (Login) with the value "FirstAdmin", "Пин-код" (PIN code) with three dots, "Пароль" (Password) with seven dots, and "Повтор пароля" (Repeat password) with seven dots. On the right side, there are two fields: "IP сервера управления" (Management server IP) with the value "10.10.11.101" and "PORT сервера управления" (Management server PORT) with the value "41254". Below the form, there is a link that says "Есть данные для входа? Авторизоваться" (Have login data? Authorize) and a dark blue button labeled "ОТПРАВИТЬ" (SEND).

Рисунок 13

Первый вход в сеанс КА

После успешного прохождения регистрации необходимо осуществить первый вход в сеанс КА.

1. Для этого необходимо в окне «Регистрация учетной записи» нажать на ссылку «Есть данные для входа? Авторизоваться». В результате откроется окно входа с систему

Авторизация

Логин: FirstAdmin

Пароль:

IP сервера управления: 10.10.11.101

PORT сервера управления: 41254

[Регистрация учетной записи администратора](#)

ОТПРАВИТЬ

Рисунок 14

2. В открывшемся окне «Авторизация» необходимо ввести данные учетной записи:

- **Логин:** FirstAdmin
- **Пароль:** Введите пароль
- **IP и PORT сервера управления:** будут заполнены автоматически.

3. После успешного входа в систему откроется Главное окно КА

Cryptallit.MC

Всего пользователей: 0

Рабочих ресурсов: 0

Объем данных: ~ 16

Главная

Пользователи

Ресурсы

Режим эксплуатации

Администрирование

Пользовательское соглашение

Рейтинг групп по количеству пользователей

Пользователи

Время непрерывной работы системы

15:31

Дата и время предыдущего сеанса

03.3.23 15:31

Режим защиты

Задания на ввод в эксплуатацию

Выполненные задания: 00

Рейтинг ресурсов по количеству пользователей

Ресурсы по идентификаторам

Не резервировано ключей шифрования: 00

Успешная авторизация пользователя FirstAdmin

Рисунок 15

Управление сетевыми ресурсами

Общие характеристики сетевых ресурсов

Ресурс – это защищенная сетевая папка, содержащая массивы файлов и папок, доступ к которой предоставляется только авторизованным пользователям. Доступ к сетевым ресурсам организован при помощи стандартного протокола SMB3.0.

Управление сетевыми ресурсами осуществляется через программу **Cryptallit.MC** – раздел «Ресурсы».

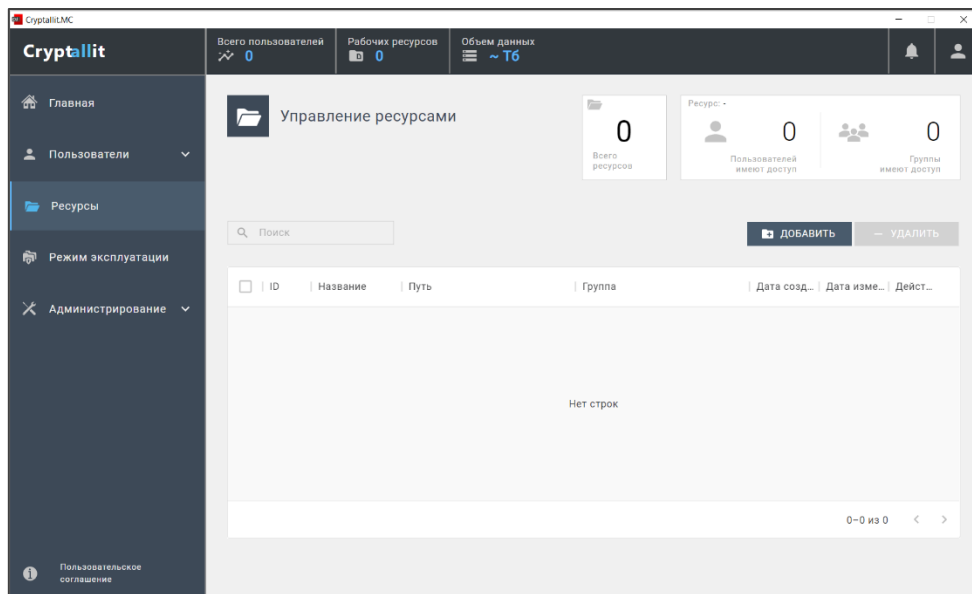


Рисунок 16

Создание ресурс ресурса

1. Для создания ресурс ресурса необходимо нажать на кнопку «**Добавить**» после чего откроется диалоговое окно создания ресурс ресурса.

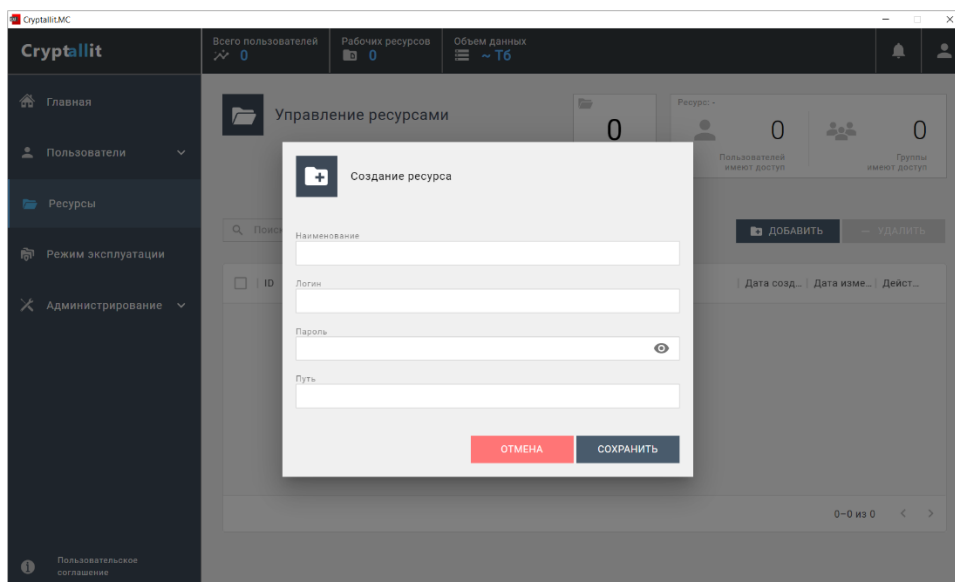


Рисунок 17

2. В диалоговом окне необходимо ввести параметры создаваемого ресурса:

- **Наименование:** Название создаваемого ресурса
- **Логин:** имя учетной записи пользователя SMB, которому будет разрешен доступ на чтение и запись в ЗР.
- **Пароль:** пароль учетной записи пользователя SMB
- **Путь:** путь к папке SMB, которая выбрана в качестве ЗР

► *Клиентское ПО для рабочей станции – APC будет осуществлять доступ по протоколу SMB к сетевому ресурсу с использованием учетной записи, которая вводится в данном диалоговом окне.*

Если папки, указанной в поле «Путь» еще не существует, необходимо создать ее с использованием данные введенной учетной записи SMB.

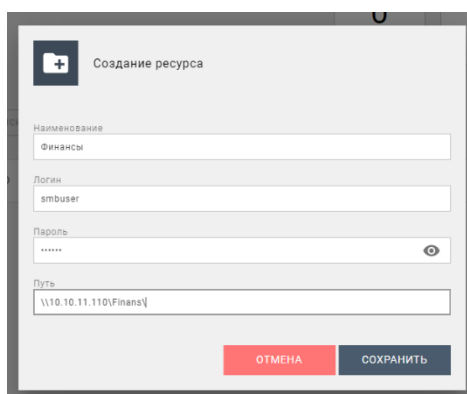


Рисунок 18

3. После заполнения формы диалогового окна создания нажмите на кнопку «Сохранить». В основной таблице раздела «Ресурсы» появится созданный ресурс.

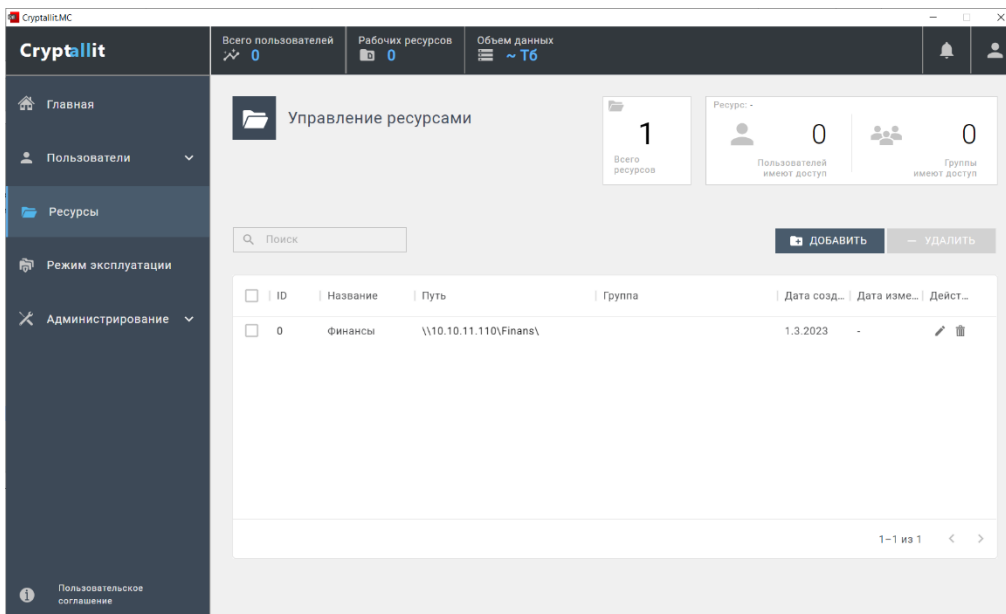


Рисунок 19

Изменение свойств ресурс ресурса

1. Для изменения свойств ресурс ресурса необходимо кликнуть по иконке «✎» соответствующей записи в таблице раздела «Ресурсы». Откроется окно «Свойства ресурс ресурса».

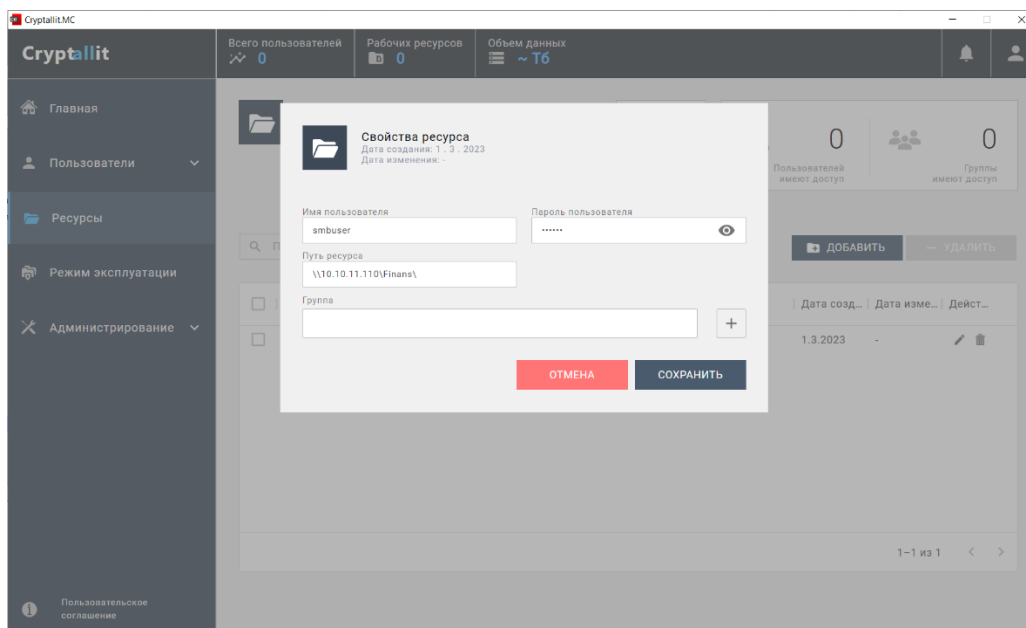


Рисунок 20

2. В данном окне можно изменить значения полей:

- **Имя пользователя:** Имя пользователя учетной записи SMB
- **Пароль пользователя:** Пароль пользователя учетной записи SMB
- **Путь ресурса:** Путь сетевой папки SMB, в которой размещен ЗР
- **Группа:** Группы, доступ на ЗР, которых разрешен.

3. Для сохранения изменений нажмите на кнопку «Сохранить».

Удаление сетевого ресурса

1. Для удаления выделите соответствующий ресурс в таблице раздела «Ресурсы», кликнув мышью на запись в таблице, далее выберите кнопку «Удалить».

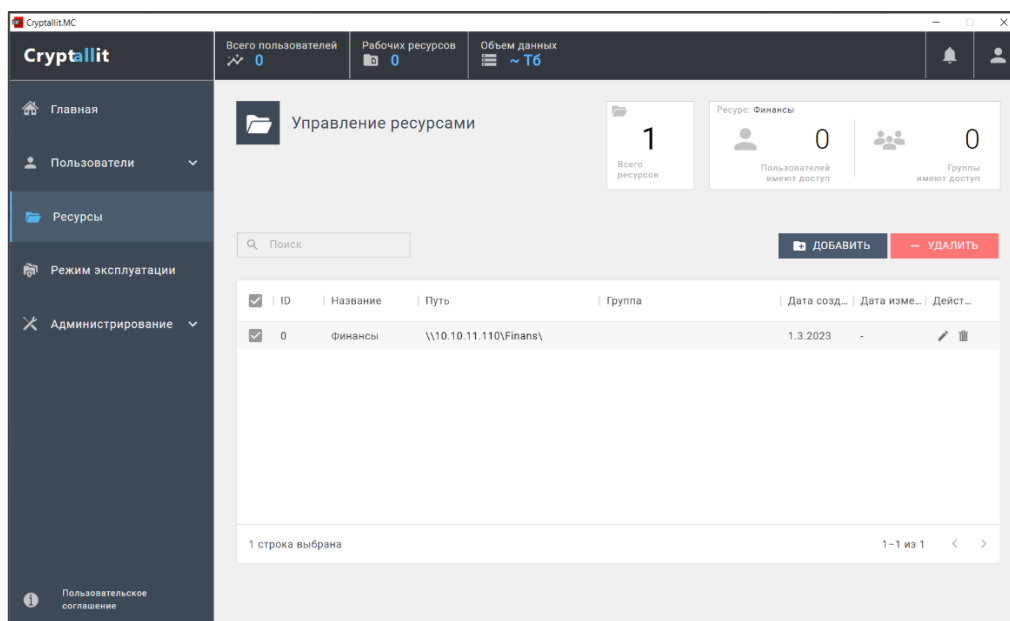


Рисунок 21

2. В подтверждение операции нажмите на кнопку «Удалить».

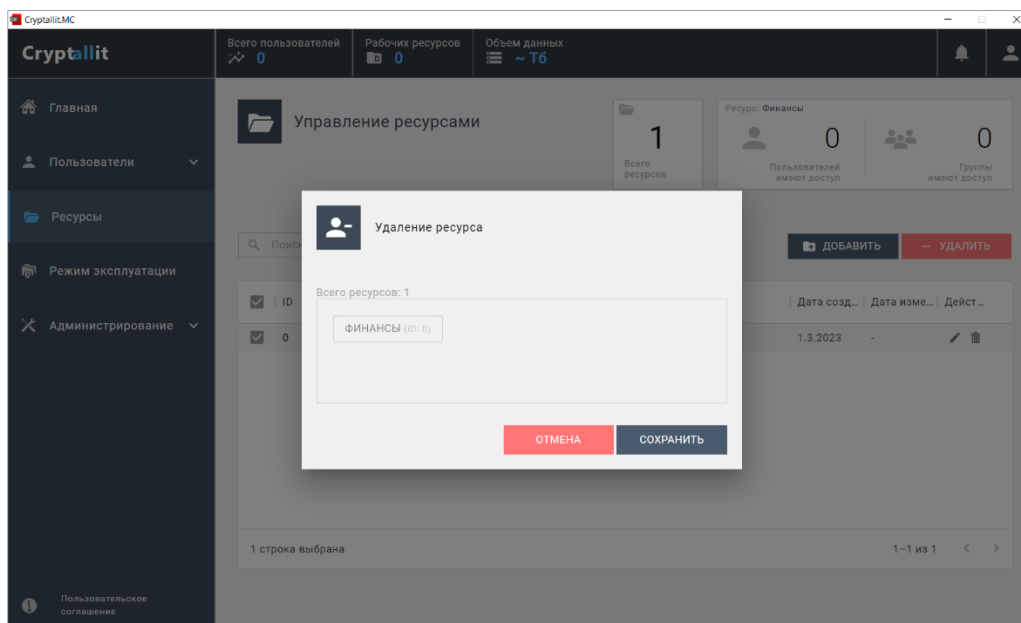


Рисунок 22

Управление пользователями

Создание учетной записи пользователя

1. Для создания учетной записи пользователя необходимо перейти в раздел КА «Пользователи» → «Управление пользователями», после чего нажмите на кнопку «Добавить».

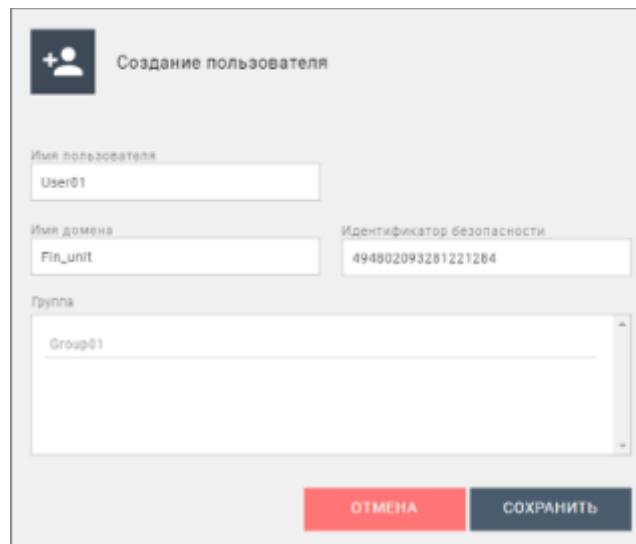


Рисунок 23

2. В диалоговом окне «Свойства пользователя» заполните следующую информацию о добавляемой учетной записи:

- **Логин:** Имя пользователя (login учетной записи пользователя на его рабочей станции)
- **Имя рабочей станции:** системное имя рабочей станции пользователя
- **Уникальный идентификатор:** SID – системный идентификатор ОС, на рабочей станции пользователя
- **Имя домена AD:** Наименование OU домена MS AD, в который включена рабочей станция пользователя
- **Пин-код:** Одноразовый пин-код, необходимый для регистрации пользователя. Подробную информацию смотри в разделе «Регистрация пользователей»
- **Группа:** Группа в системе Cryptallit в которую необходимо включить создаваемого пользователя.

3. Далее нажмите на кнопку «Сохранить», после чего в таблице подраздела «Управление пользователями» появится добавленная запись.

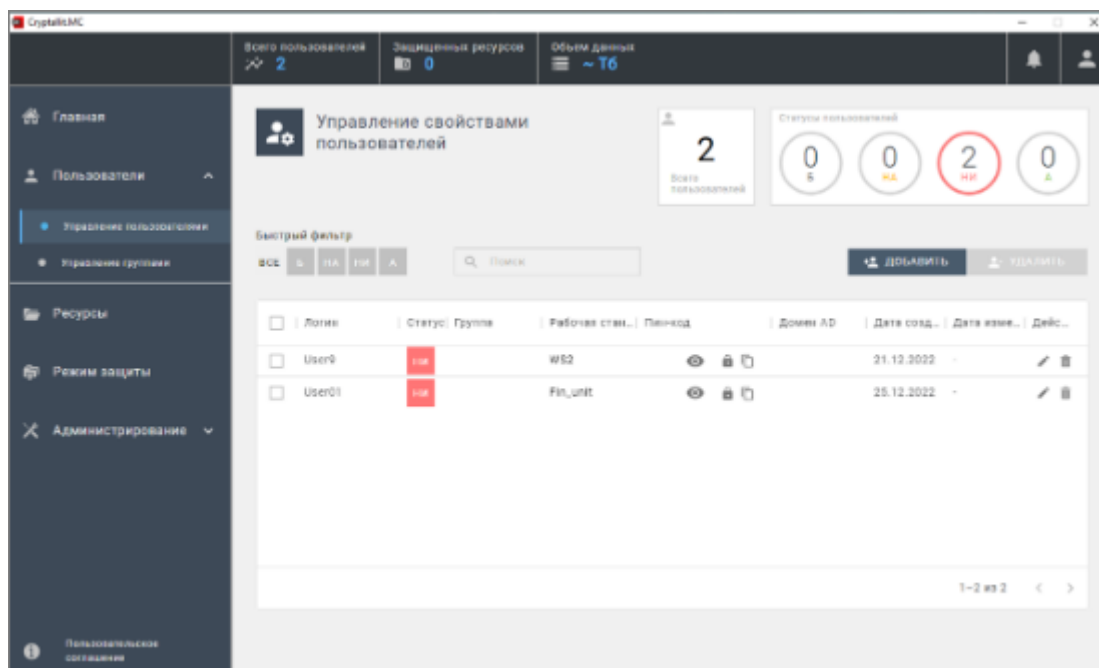


Рисунок 24

Изменение свойств пользователя

1. Для изменения свойств пользователя необходимо кликнуть по иконке «✎» соответствующей записи в таблице подраздела «Пользователи». Откроется окно «Свойства пользователя».

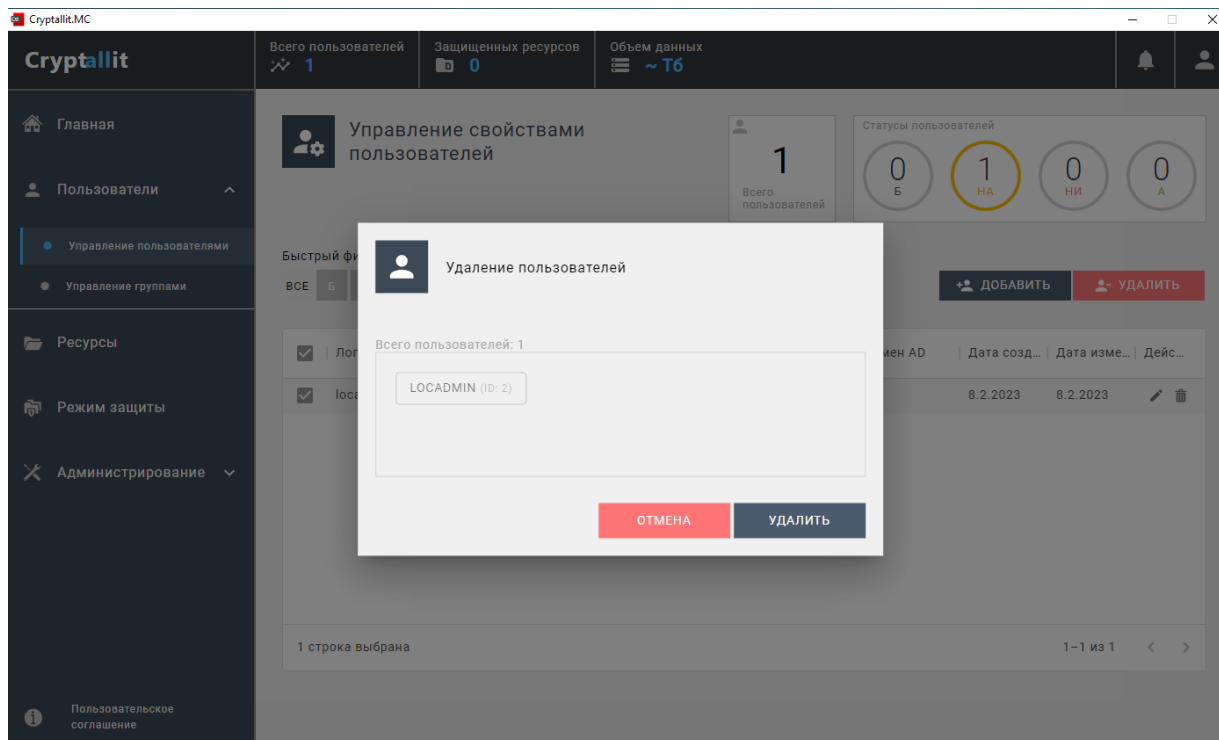
Рисунок 25

2. В диалоговом окне «Свойства пользователя» измените соответствующую информацию. Изменения информации осуществляется аналогично описанным в разделе Создание учетной записи пользователя.

3. После внесения изменений, нажмите на кнопку «Сохранить».

Удаление пользователей

1. Для удаления учетной записи пользователя выберите соответствующего пользователя в таблице раздела «Управление свойствами пользователей», кликнув мышью по записи. Далее нажмите на кнопку «Удалить».

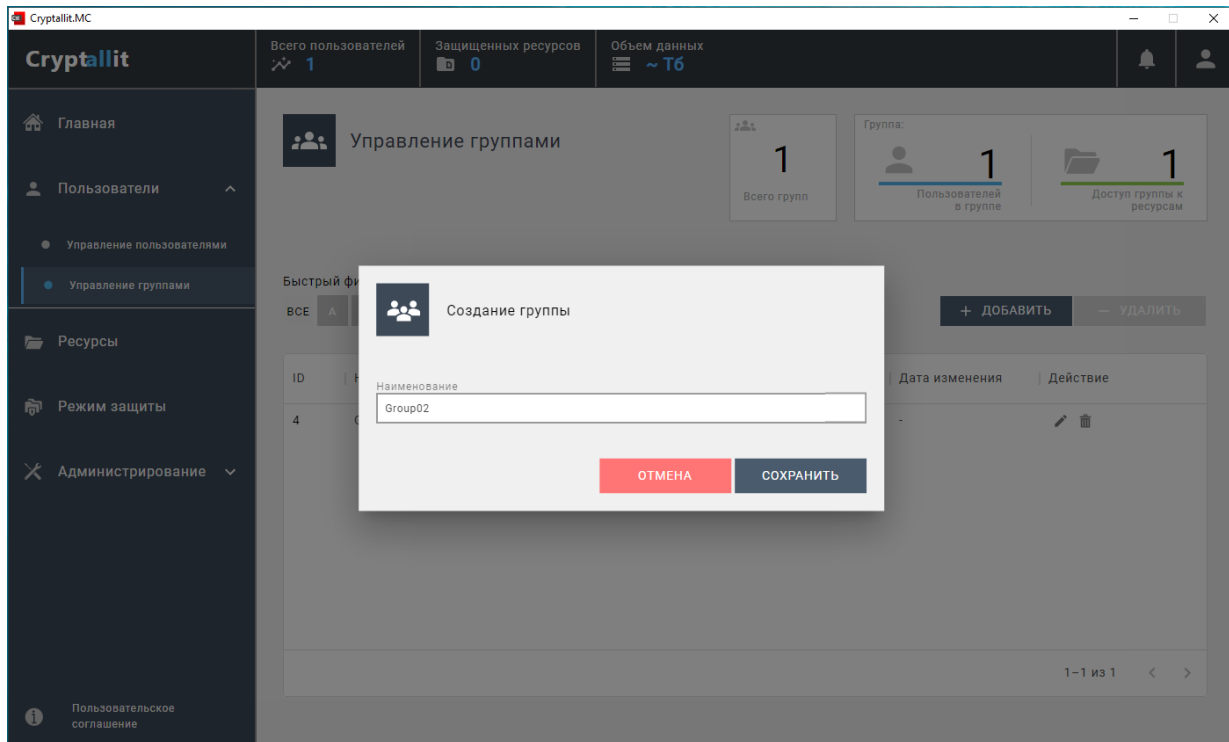


2. В подтверждение операции нажмите на кнопку «Сохранить».

Управление свойствами групп

Создание группы

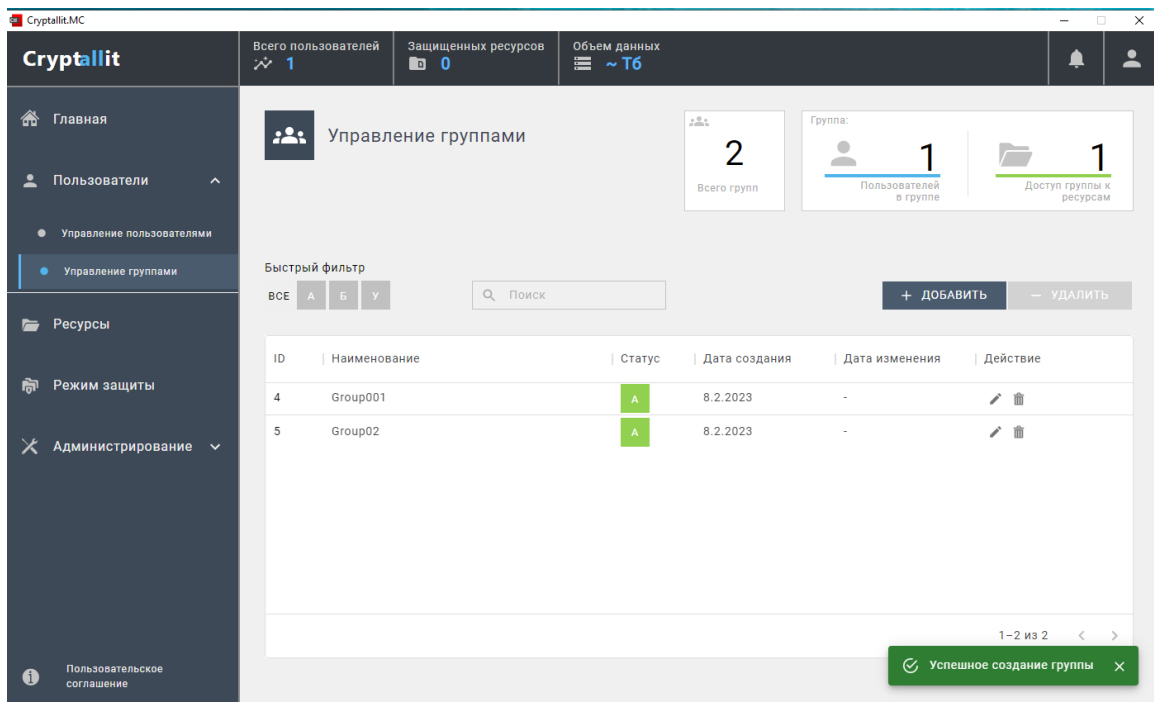
1. Для создания группы перейдите в раздел КА, далее выберите «Пользователи» → «Управление группами», после чего нажмите на кнопку «Добавить».



2. В открывшемся диалоговом окне введите параметры создаваемой группы:

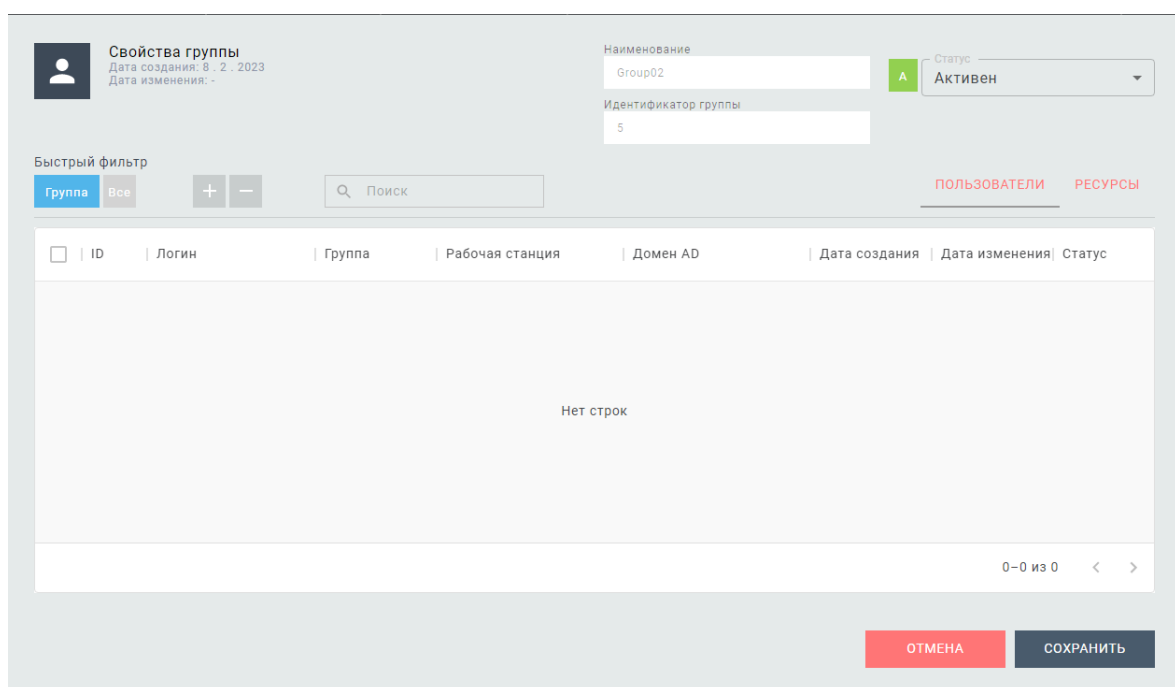
- **Наименование:** Название создаваемого ресурса
- **Логин:** имя учетной записи пользователя SMB, которому будет разрешен доступ на чтение и запись в ЗР.
- **Пароль:** пароль учетной записи пользователя SMB
- **Путь:** путь к папке SMB, которая выбрана в качестве ЗР

3. После заполнения формы диалогового окна нажмите на кнопку «Сохранить». В основной таблице раздела «Управление свойствами групп» появится созданная группа.



Изменение свойств группы

1. Для изменения свойств группы кликните по иконке «✎» соответствующей записи в таблице подраздела «Управление свойствами группы». Откроется окно «Свойства группы»

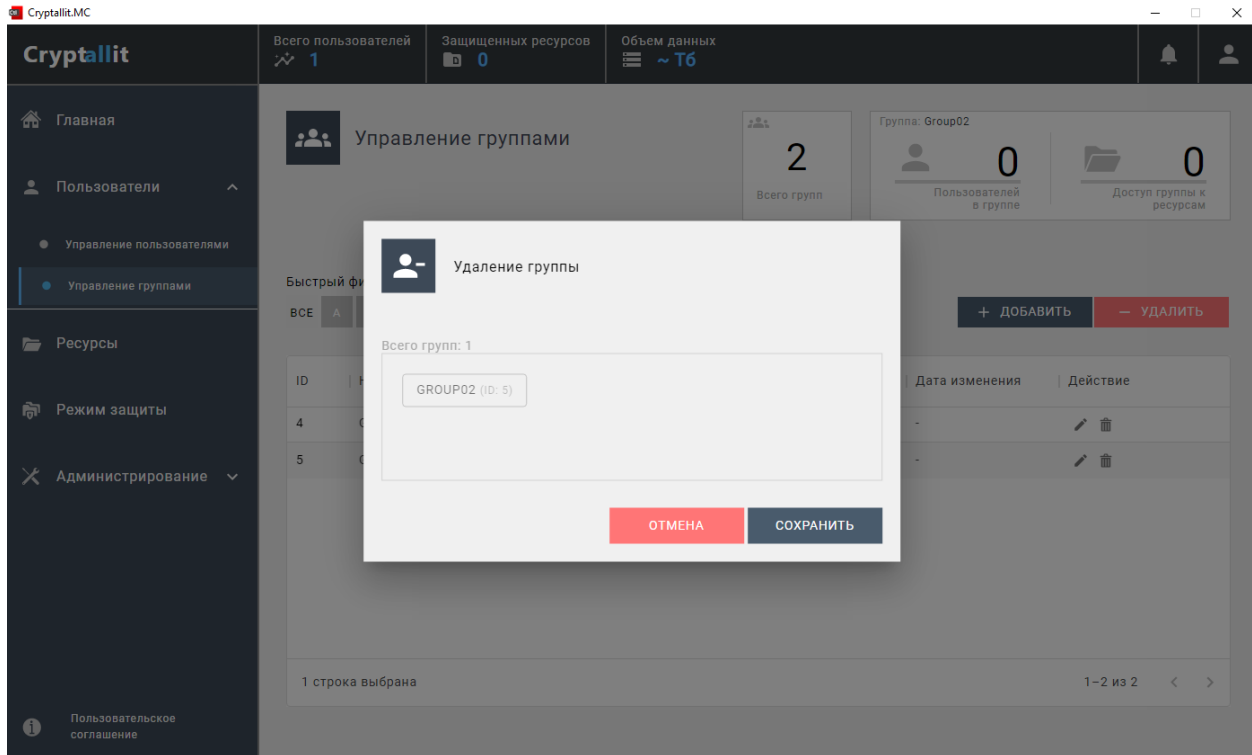


2. В диалоговом окне «Свойства группы» измените соответствующую информацию. Изменения информации осуществляется аналогично описанным в разделе Создание группы.

3. После внесения изменений, нажмите на кнопку «Сохранить».

Удаление группы

1. Для удаления группы выделите соответствующую запись таблицы раздела «Управление свойствами групп», кликнув мышью по записи. Далее нажмите на кнопку «Удалить».



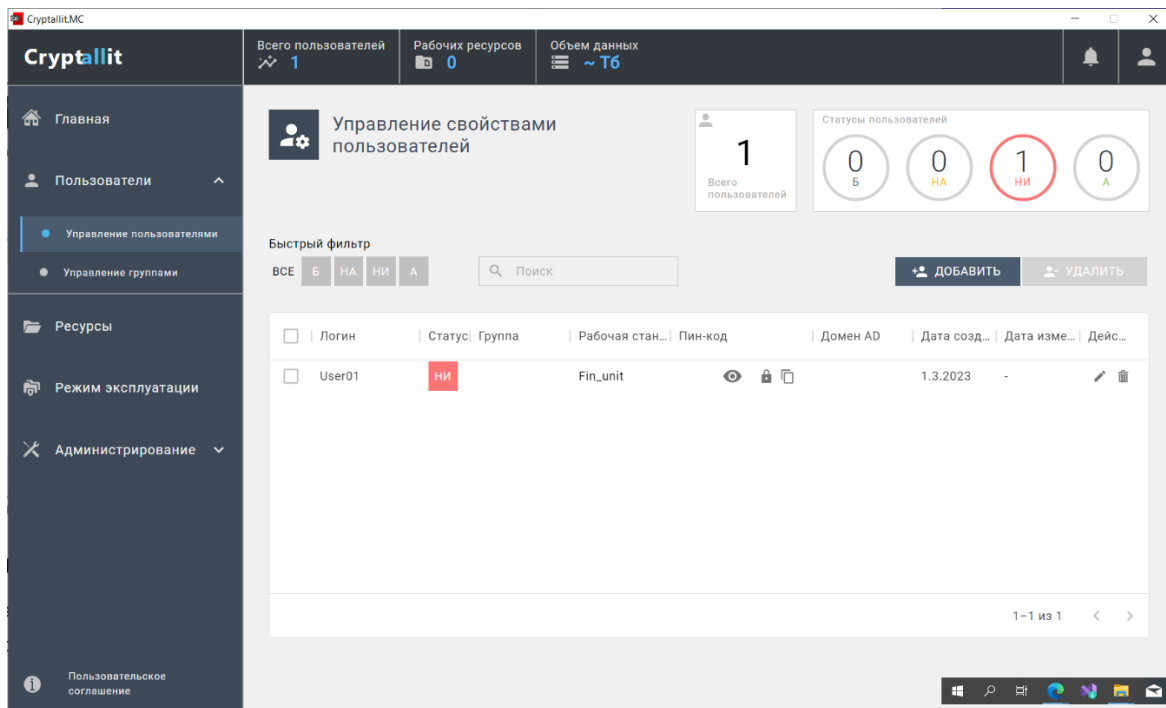
2. В подтверждение операции нажмите на кнопку «Сохранить».

Управление доступом к защищенным ресурсам

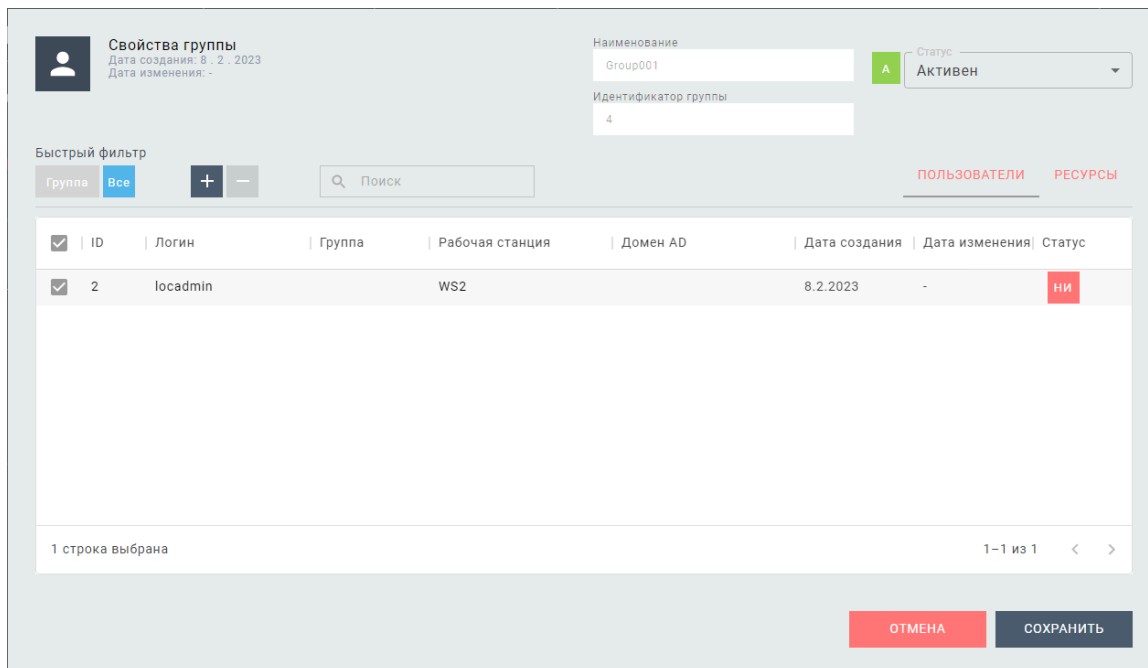
Управление доступом пользователей к защищенным ресурсам осуществляется посредством настройки параметров групп. На соответствующих вкладках производится разрешение доступа группы к соответствующему защищенному ресурсу и добавление пользователей в эту группу.

Добавление пользователей в группу

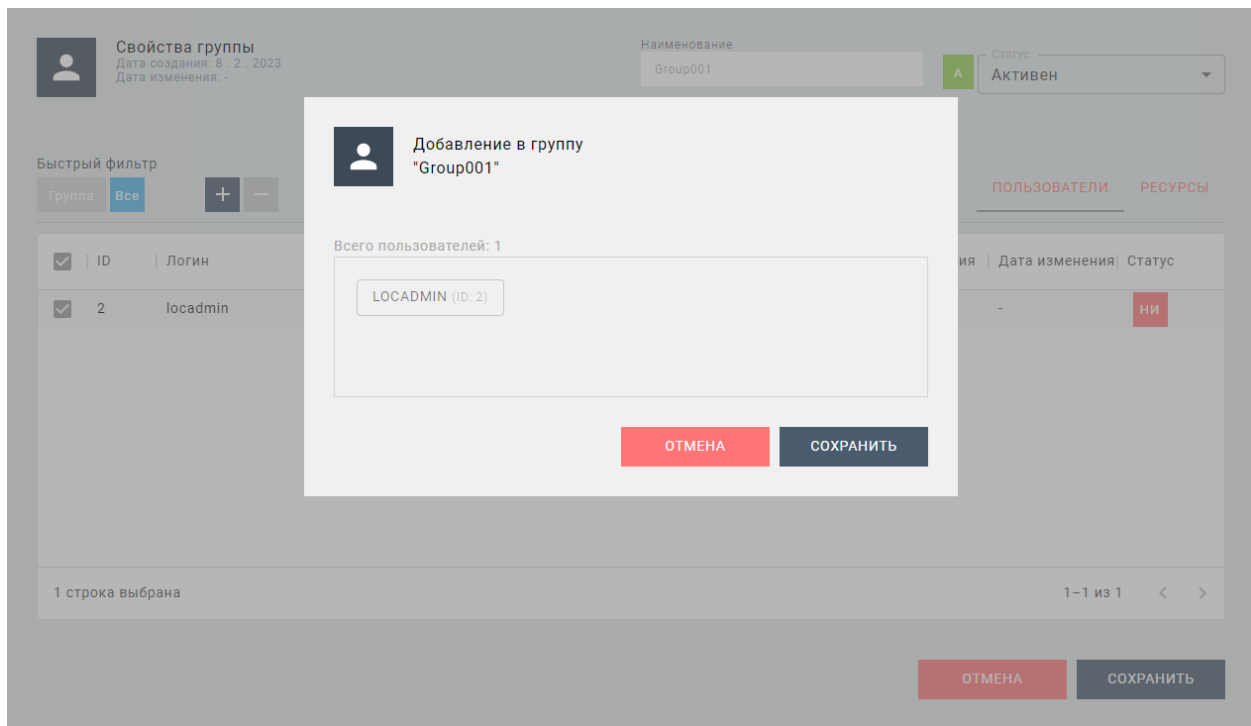
Для добавления учетной записи пользователя в группу необходимо открыть окно свойств группы (см. Изменение свойств группы) и перейти на вкладку ПОЛЬЗОВАТЕЛИ.



Для осуществления выбора необходимо воспользоваться быстрым фильтром «Все», отобразив все учетные записи пользователей.

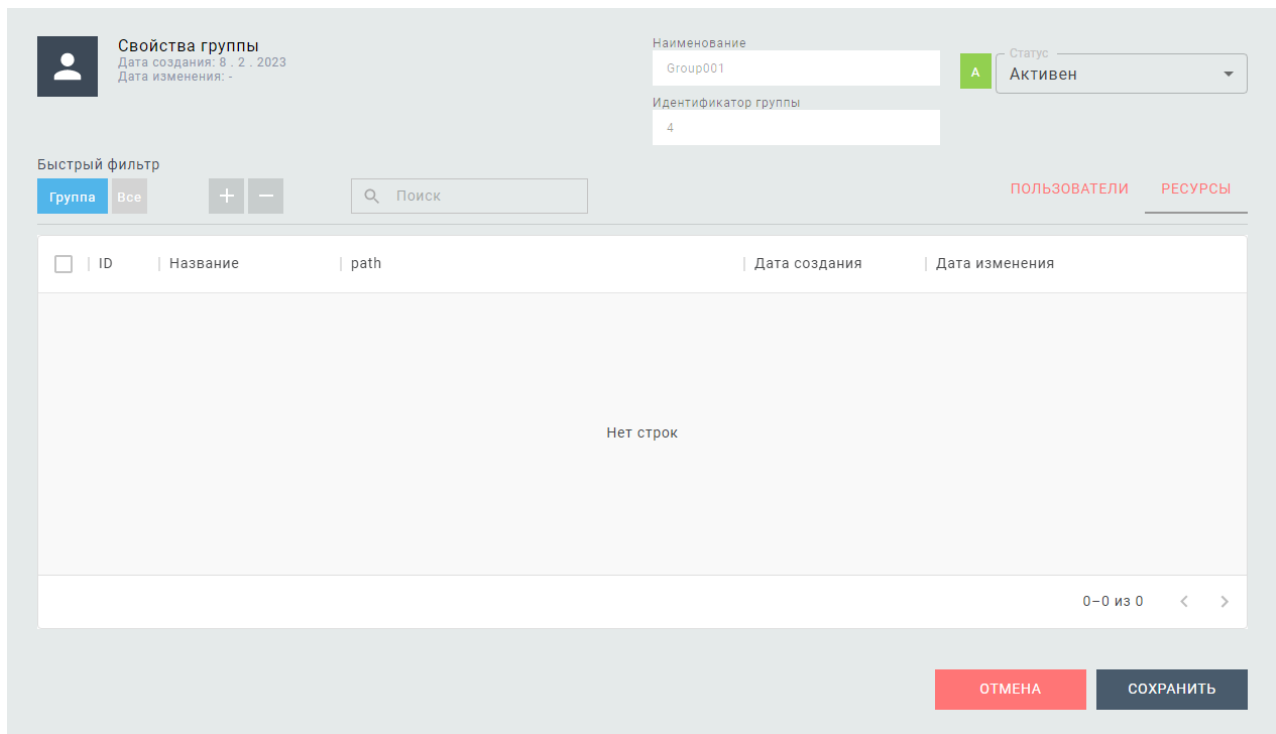


Выделив соответствующие учетные записи необходимо нажать на кнопку + и подтвердить операцию добавления нажав на кнопку «Сохранить»



Доступ к сетевому ресурсу для группы

Для разрешения доступа группы к защищенному ресурсу необходимо открыть окно свойств группы (см. Изменение свойств группы) и перейти на вкладку РЕСУРСЫ



Для осуществления выбора необходимо воспользоваться быстрым фильтром «Все», отобразив все защищенные ресурсы.

Свойства группы
Дата создания: 8. 2. 2023
Дата изменения: -

Наименование: Group001
Идентификатор группы: 4
Статус: Активен

Быстрый фильтр: Группа Все + - Поиск

ПОЛЬЗОВАТЕЛИ РЕСУРСЫ

<input checked="" type="checkbox"/>	ID	Название	path	Дата создания	Дата изменения
<input checked="" type="checkbox"/>	0	Resource001	\\CTLFS\ctl	8.2.2023	-

1 строка выбрана 1-1 из 1

ОТМЕНА СОХРАНИТЬ

Выделив соответствующие защищенные ресурсы необходимо нажать на кнопку + и подтвердить операцию добавления нажав на кнопку «Сохранить»

Свойства группы
Дата создания: 8. 2. 2023
Дата изменения: -

Наименование: Group001
Идентификатор группы: 4
Статус: Активен

Быстрый фильтр: Группа Все + - Поиск

ПОЛЬЗОВАТЕЛИ РЕСУРСЫ

Добавление в группу "Group001"

Всего ресурсов: 1


RESOURCE001 (ID: 0)

ОТМЕНА СОХРАНИТЬ

1 строка выбрана 1-1 из 1

ОТМЕНА СОХРАНИТЬ

В результате произведенного разрешения на доступ к защищенному ресурсу пользователи группы со статусом НА (не авторизован) меняют статус на А (авторизован) и смогут осуществлять доступ к защищенному ресурсу через APC агент рабочей станции

**Свойства группы**
Дата создания: 8.2.2023
Дата изменения: -

Наименование
Group001 A Статус
Активен

Идентификатор группы
4

Быстрый фильтр
Группа Все + -

ПОЛЬЗОВАТЕЛИ РЕСУРСЫ

<input type="checkbox"/>	ID	Логин	Группа	Рабочая станция	Домен AD	Дата создания	Дата изменения	Статус
<input type="checkbox"/>	2	locadmin	Group001	WS2		8.2.2023	8.2.2023	A

1-1 из 1 < >

ОТМЕНА СОХРАНИТЬ