Акронис Инфозащита

# Acronis Защита Данных Облачная

Версия 2.0

Портал управления

**РУКОВОДСТВО АДМИНИСТРАТОРА**

Редакция: 02.11.2019

# Содержание

# 1 Об этом документе

Этот документ предназначен для администраторов, которые хотят использовать портал управления.

# 2 О портале управления

Портал управления — это веб-интерфейс облачной платформы, на котором предоставляются службы защиты данных.

Хотя для каждой службы есть свой веб-интерфейс (консоль службы), портал управления позволяет администраторам контролировать использование служб, создавать учетные записи пользователей и отделов, формировать отчеты и выполнять другие действия.

## 2.1 Учетные записи и отделы

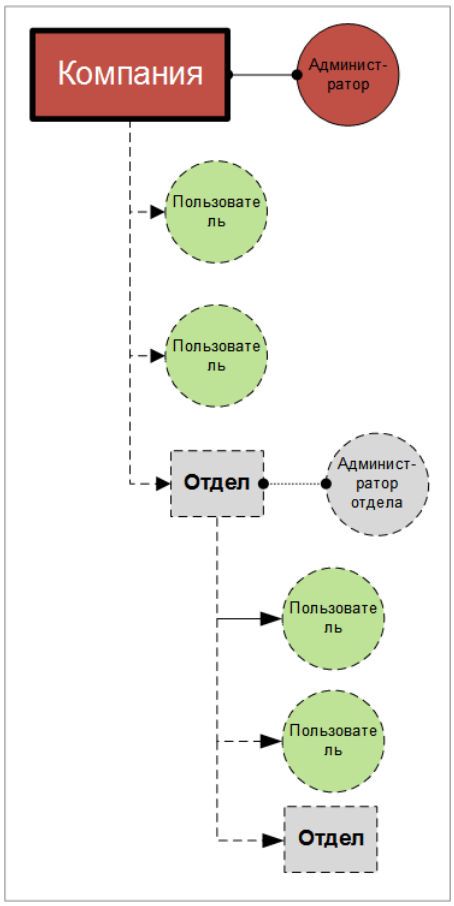
Учетные записи бывают двух типов: администраторы и пользователи.

- **Администраторы** имеют доступ к порталу управления. Они имеют роль администратора во всех службах.
- **Пользователи** не имеют доступа к порталу управления. Их доступ к службам и их роли определяются администратором.

Администраторы могут создавать отделы, которые обычно соответствуют отделам или подразделениям организации. Каждая учетная запись существует на уровне компании или в отделе.

Администратор может управлять отделами, учетными записями администратора и пользователя на своем уровне иерархии или на уровнях ниже.

На указанной ниже диаграмме показаны три уровня иерархии — компания и два отдела. Дополнительные отделы и учетные записи показаны пунктирной линией.




В таблице ниже приведены операции, которые могут выполнять администраторы и пользователи.

| Операция | Пользователи | Администраторы |
|---|---|---|
| Создать отделы | Нет | Да |
| Создание учетных записей | Нет | Да |
| Загрузить и установить программное обеспечение | Да | Да |
| Использовать службы | Да | Да |
| Создание отчетов об использовании сервиса | Нет | Да |

## 2.2 Управление квотами

**Квоты** позволяют установить ограничения на использование службы для клиента.

На портале управления можно просмотреть квоты на использование службы, выделенные поставщиком услуг для вашей организации. Управление этими квотами для вас недоступно.

Однако вы можете управлять квотами в отношении службы для своих пользователей.

## 2.2.1 Просмотр квот для вашей организации

На портале управления выберите **Обзор** > **Использование**. На открывшейся панели мониторинга показаны квоты, выделенные для вашей организации. Квоты для каждой службы указаны на отдельной вкладке.

### 2.2.1.1 Квоты резервного копирования

Можно указать квоту облачного хранилища данных, квоту локального резервного копирования и максимальное количество машин/устройств/веб-сайтов, которые может защитить пользователь. Доступны указанные ниже квоты.

#### Квоты для устройств

- **Рабочие станции**
- **Серверы**
- **Виртуальные машины**

Машина/устройство считаются защищенными, если к ним применен как минимум один план резервного копирования. При превышении количества устройств пользователь не может применить план резервного копирования к дополнительным устройствам.

#### Квоты для хранилища данных

- **Локальное резервное копирование**

  Квота **Локальное резервное копирование** ограничивает общий размер локальных резервных копий, созданных с использованием облачной инфраструктуры. Для этой квоты нельзя задать превышение.
- **Облачные ресурсы**

Квота хранения данных ограничивает общий размер резервных копий, размещенных в облачном хранилище данных. При выходе за пределы значения превышения квоты хранения резервной копии резервное копирование не выполняется.

## 2.2.2 Определение квот для пользователей

**Квоты** позволяют установить ограничения на использование службы для пользователя. Чтобы задать квоты для пользователя, выберите его на вкладке **Пользователи**, затем щелкните значок карандаша в разделе **Квоты**.

При превышении квоты на адрес электронной почты пользователя отправляется оповещение. Если превышение квоты не задано, квота считается «**мягкой**». Это значит, что ограничения по использованию сервиса резервного копирования, не применяются.

Если для квоты указано превышение, она считается «**жесткой**». **Превышение** позволяет пользователю превысить квоту на указанное значение. При превышении, большем максимального, налагаются ограничения на использование соответствующей службы.

**Пример**

**Мягкая квота**. Для количества рабочих станций пользователь вы установили квоту, равную 20. Когда количество защищенных рабочих станций пользователя достигнет 20, он получит соответствующее уведомление по электронной почте, но сервис резервного копирования останется доступным для него.

**Жесткая квота**. Для количества рабочих станций пользователь установил квоту со значением 20 и превышение со значением 5. Когда количество защищенных рабочих станций пользователя достигнет 20, он получит уведомление по электронной почте; когда же оно достигнет 25, сервис резервного копирования будет отключен.

#### 2.2.2.1 Квоты резервного копирования

Можно указать квоту хранилища резервных копий и максимальное количество машин/устройств/веб-сайтов, которые может защитить пользователь. Доступны указанные ниже квоты.

**Квоты для устройств**

- **Рабочие станции**
- **Серверы**
- **Виртуальные машины**

Машина/устройство считаются защищенными, если к ним применен как минимум один план резервного копирования. При превышении по количеству устройств, большем максимального, пользователь не сможет применить план резервного копирования к дополнительным устройствам.

**Квота для хранилища данных**

- **Хранилище резервных копий**

Квота хранения данных ограничивает общий размер резервных копий, размещенных в облачном хранилище данных. При выходе за пределы значения превышения квоты хранения резервной копии резервное копирование не выполняется.

## 2.3 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Google Chrome 29 или более поздней версии
- Mozilla Firefox 23 или более поздней версии
- Opera 16 или более поздней версии
- Windows Internet Explorer 11 или более поздней версии
- Microsoft Edge 25 более поздней версии
- Safari 8 или более поздней версии в macOS

В других веб-браузерах (включая браузеры Safari, запущенные в других операционных системах) может неправильно отображаться интерфейс пользователя или могут быть недоступны некоторые функции.

# 3 Пошаговые инструкции

Приведенные ниже пошаговые инструкции помогут выполнить основные операции на портале управления. В них описано, как:

- Активировать учетную запись администратора
- Получение доступа к порталу управления и службам

- Создание отдела
- Создание учетной записи пользователя

## 3.1 Активация учетной записи администратора

Подписавшись на услугу, вы получите сообщение электронной почты с указанной ниже информацией.

- **Ссылка для активации учетной записи**. Щелкните эту ссылку и задайте пароль для учетной записи администратора. Запомните имя для входа, которое отображается на странице активации учетной записи.
- **Ссылка на страницу входа**. При этом потребуется указать имя для входа и пароль из предыдущего шага.

## 3.2 Доступ к порталу управления и службам

1. Откройте страницу входа. Адрес страницы входа был указан в сообщении электронной почты со сведениями об активации.
2. Введите имя пользователя и щелкните **Продолжить**.
3. Введите пароль и щелкните **Вход**.
4. Выполните одно из следующих действий:
   - Чтобы войти на портал управления, щелкните **Портал управления**.
   - Чтобы войти в службу, щелкните имя службы.

Для переключения между порталом управления и консолями служб щелкните  значок в верхнем правом углу и выберите пункт **Портал управления** или службу, к которой необходимо перейти.

## 3.3 Навигация на портале управления

Используя портал управления, в каждый данный момент времени вы работаете в компании или в отделе. Это указано в верхнем левом углу.

По умолчанию выбран самый верхний уровень иерархии, который доступен вам. Щелкните имя отдела, чтобы развернуть иерархию. Чтобы вернуться назад на более верхний уровень, щелкните имя в верхнем левом углу.

Во всех части пользовательского интерфейса будут отображаться только та компания или отдел, в которых вы работаете в данный момент. Например:

- Кнопка **Создать** позволяет создать отдел или учетную запись пользователя только в этой компании или в этом отделе.
- На вкладке **Отделы** отображаются только те отделы, которые являются непосредственно дочерними для этой компании или отдела.
- На вкладке **Пользователи** отображаются только те учетные записи пользователей, которые существуют в компании или отделе.

## 3.4 Создание отдела

Пропустите этот шаг, если не хотите создавать упорядочивать учетные записи пользователей в отделы.

Если вы планируете создать отделы позже, имейте в виду, что существующие учетные записи невозможно переместить между отделами или между компанией и отделами. Сначала необходимо создать отдел, а затем заполнить его учетными записями.

***Порядок создания отдела***

1. Войдите на портал управления.
2. Перейдите к отделу, в котором необходимо создать новый отдел.
3. В верхнем правом углу последовательно выберите пункты **Создать** > **Отдел**.
4. В поле **Имя** укажите имя нового отдела.
5. [Дополнительно] В поле **Язык** измените язык по умолчанию для уведомлений, отчетов и программного обеспечения, который будет использоваться в этом отделе.
6. Выполните одно из следующих действий:
   - Чтобы создать администратора отдела, нажмите кнопку **Далее**, а затем следуйте шагам, описанным в разделе "Создание учетной записи пользователя" (стр. 8), начиная с шага 4.
   - Чтобы создать отдел без администратора, щелкните **Сохранить и закрыть**. Администраторов и пользователей можно добавить в отдел позже.

Новый созданный отдел появится на вкладке **Отделы**.

Чтобы изменить настройки отдела или указать контактную информацию, выберите отдел на вкладке **Клиенты**, а затем щелкните значок карандаша в том разделе, который нужно изменить.

## 3.5 Создание учетной записи пользователя

Пропустите этот шаг, если не нужно создавать дополнительные учетные записи пользователей.

Возможно, необходимо будет добавить дополнительные учетные записи в следующих случаях:

- Учетные записи администратора компании: чтобы делиться обязанностями по управлению с другими пользователями.
- Учетные записи администратора отдела: для делегирования управления другим пользователям, для которых права доступа будут ограничены рамками соответствующих отделов.
- Учетные записи пользователя: чтобы включить для пользователей только доступ к поднабору служб.

***Порядок создания учетной записи пользователя***

1. Войдите на портал управления.
2. Перейдите к отделу, в котором необходимо создать новую учетную запись пользователя.
3. В верхнем правом углу последовательно выберите пункты **Создать** > **Пользователь**.
4. Укажите приведенную ниже информацию для учетной записи:
   - **Электронная почта**
   - Необязательно:**Имя**
   - Необязательно: **Фамилия**
   - [Дополнительно] Чтобы указать имя входа, отличное от указанного адреса электронной почты, снимите флажок **Использовать адрес электронной почты как имя входа**, а затем укажите имя входа.

***Внимание!*** *У каждой учетной записи должно быть уникальное имя входа.*

5. [Дополнительно] В поле **Язык** измените язык по умолчанию для уведомлений, отчетов и программного обеспечения, который будет использоваться для этой учетной записи.
6. Выберите службы, к которым пользователь будет иметь доступ и роли в каждой службе.
   - Если установлен флажок **Администратор компании**, пользователь будет иметь доступ к порталу управления и роль администратора во всех службах.
   - Если установлен флажок **Администратор отдела**, у пользователя будет доступ к порталу управления. При этом, в зависимости от службы, пользователь может иметь или не иметь роль администратора.
   - В противном случае пользователь будет иметь роли, которые выбраны в выбранных службах.
7. Нажмите кнопку **Создать**.

Созданная учетная запись пользователя появится на вкладке **Пользователи**.

Чтобы изменить настройки пользователя или указать настройки уведомления и квот для пользователя, выберите его на вкладке **Пользователи**, а затем щелкните значок карандаша в том разделе, который нужно изменить.

## 3.6 Настройки двухфакторной проверки подлинности

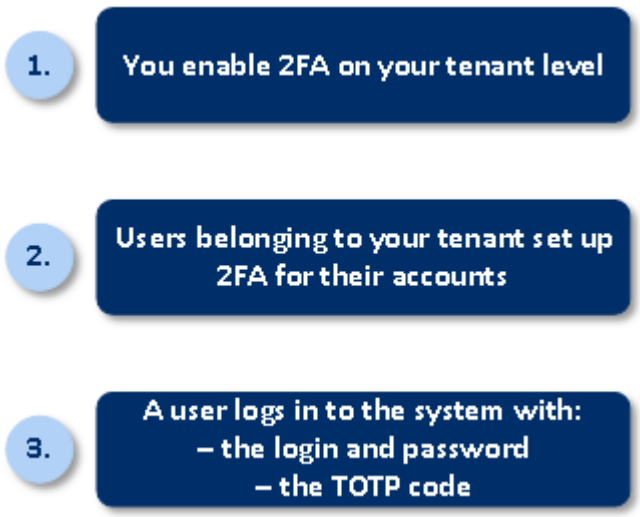
**Двухфакторная проверка подлинности (2FA)** — это тип многофакторной проверки подлинности, обеспечивающий идентификацию пользователей с помощью комбинации двух различных факторов.

- Фактор знания, что-то, что пользователь знает (PIN-код или пароль)
- Фактор владения, что-то, что пользователь имеет (токен)
- Фактор свойства, что-то, что является частью пользователя (биометрика)

Двухфакторная проверка подлинности обеспечивает дополнительную защиту от несанкционированного доступа к учетной записи.

Платформа поддерживает проверку подлинности с использованием алгоритма генерации одноразового пароля на основе времени **TOTP (Time-based One-Time Password)**. Если в системе включена проверка подлинности с использованием TOTP, для доступа к системе пользователи кроме обычного пароля должны ввести одноразовый код TOTP. Иными словами, сначала пользователь вводит пароль (первый фактор), а затем — код TOTP (второй фактор). Код TOTP генерируется в приложении проверки подлинности на устройстве второго фактора на основе текущего значения таймера и секретного ключа, предоставленных платформой.

## Принципы работы




1. Двухфакторная проверка подлинности включается (стр. 12) на уровне организации.
2. Все пользователи в организации должны установить приложение проверки подлинности на устройствах второго фактора. Такими устройствами могут быть мобильные телефоны, ноутбуки, настольные или планшетные ПК. Это приложение будет использоваться для генерации одноразовых кодов TOTP. Рекомендуемые генераторы кодов:
   - Google Authenticator

     Версия для iOS (https://itunes.apple.com/sg/app/google-authenticator/id388497605?mt=8)

     Версия для Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_SG)
   - Microsoft Authenticator

     Версия для iOS (https://app.adjust.com/n094ls?campaign=appstore_ios&fallback=https://itunes.apple.com/app/microsoft-authenticator/id983156458)

     Версия для Android (https://app.adjust.com/n094ls?campaign=appstore_android&fallback=https://play.google.com/store/apps/details?id=com.azure.authenticator)

***Важно!*** *Необходимо убедиться, что время на устройстве с приложением проверки подлинности установлено правильно и соответствует фактическому.*

3. Пользователи организации должны выйти из системы и заново войти в нее.
4. После ввода учетных данных пользователям будет предложено настроить двухфакторную проверку подлинности для своих учетных записей.
5. Им необходимо будет отсканировать QR-код в приложении проверки подлинности. Если возникнут проблемы со сканированием QR-кода, пользователи могут вручную ввести в приложение проверки подлинности секретный ключ TOTP, который отображается под QR-кодом.

***Важно!*** *Настоятельно рекомендуется сохранить QR-код или секретный ключ TOTP. Для этого можно распечатать QR-код, записать секретный ключ TOTP или воспользоваться приложением, которое поддерживает резервное копирование кодов в облако. При утрате устройства второго фактора секретный ключ TOTP позволит сбросить настройки двухфакторной проверки подлинности.*

6. В приложении проверки подлинности генерируется одноразовый код TOTP. Он генерируется заново каждые 30 секунд.
7. После ввода пароля пользователям необходимо ввести код TOTP на экране «Настройки двухфакторной проверки подлинности».
8. В результате выполнения этих процедур будет активирована двухфакторная проверка подлинности для пользователей.

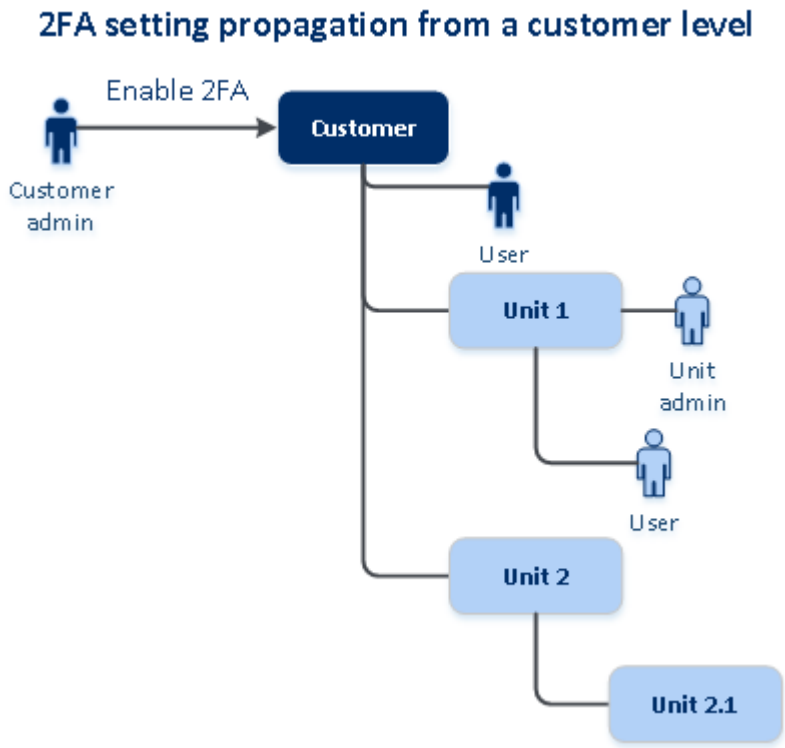
С этого момента при входе в систему после ввода учетных данных у пользователей будет запрашиваться одноразовый код TOTP, сгенерированный в приложении проверки подлинности. При входе в систему пользователи могут пометить используемый браузер как доверенный. После этого при последующих входах в систему с этого браузера код TOTP не будет запрашиваться.

### 3.6.1 Распространение настроек двухфакторной проверки подлинности на уровни клиента

Двухфакторная проверка подлинности задается на уровне **организации**. Настроить двухфакторную проверку подлинности можно только для собственной организации.

Настройки двухфакторной проверки подлинности распространяются по уровням клиента следующим образом:

- Отделы автоматически наследуют настройки двухфакторной проверки подлинности от организации их клиента.




***Примечание***
*1. Невозможно настроить двухфакторную проверку подлинности на уровне отдела.*
*2. Можно настраивать параметры двухфакторной проверки подлинности для пользователей дочерних организаций (отделов).*

## 3.6.2 Настройка двухфакторной проверки подлинности для вашего клиента

### Порядок включения двухфакторной проверки подлинности для вашего клиента

1. На портале управления выберите **Настройки** > **Безопасность**.
2. С помощью ползунка включите двухфакторную проверку подлинности. Для подтверждения действия щелкните **Включить**.

Индикатор выполнения показывает количество пользователей, которые настроили двухфакторную проверку подлинности для своих учетных записей. В результате двухфакторная проверка подлинности будет включена для вашей организации. Теперь все пользователи организации должны настроить двухфакторную проверку подлинности в своих учетных записях. После этого при входе пользователей в систему кроме учетных данных у них будет запрашиваться код TOTP.

На вкладке **Пользователи** появится столбец **Статус 2FA**. Данные этого столбца позволяют узнать, какие пользователи настроили двухфакторную проверку подлинности для своих учетных записей.

### Порядок отключения двухфакторной проверки подлинности для вашего клиента

1. На портале управления выберите **Настройки** > **Безопасность**.
2. С помощью ползунка отключите двухфакторную проверку подлинности. Для подтверждения действия щелкните **Отключить**.
3. (Если хотя бы один пользователь настроил двухфакторную проверку подлинности в организации.) Введите код TOTP из приложения проверки подлинности на мобильном устройстве.

Двухфакторная проверка подлинности для вашей организации будет отключена, будут удалены все секретные коды, а также информация о доверенных браузерах. Всем пользователям для входа в систему понадобятся только имя входа и пароль. На вкладке **Пользователи** будет скрыт столбец **Статус 2FA**.

## 3.6.3 Управление двухфакторной проверкой подлинности для пользователей

На портале управления на вкладке **Пользователи** можно отслеживать настройки двухфакторной проверки подлинности для всех пользователей и сбрасывать их.

### Мониторинг

На портале управления на вкладке **Пользователи** можно просмотреть список всех пользователей в организации. В столбце **Статус 2FA** указано, настроена ли двухфакторная проверка подлинности для пользователя.

### Порядок сброса двухфакторной проверки подлинности для пользователя

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия.
2. Щелкните **Сбросить двухфакторную проверку подлинности**.

3. Введите код TOTP, сгенерированный в приложении проверки подлинности на устройстве второго фактора, а затем щелкните **Сбросить**.

После этого пользователь сможет снова настроить двухфакторную проверку подлинности.

### Порядок сброса доверенных браузеров для пользователя

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия.
2. Щелкните **Сбросить все доверенные браузеры**.
3. Введите код TOTP, сгенерированный в приложении проверки подлинности на устройстве второго фактора, а затем щелкните **Сбросить**.

После сброса всех доверенных браузеров для пользователя при следующем входе ему необходимо будет указать код TOTP.

Пользователи могут сбрасывать информацию обо всех доверенных браузерах и параметры двухфакторной проверки подлинности самостоятельно. Это можно сделать при входе в систему, нажав соответствующую ссылку и введя код TOTP для подтверждения операции.

### Порядок отключения двухфакторной проверки подлинности для пользователя

Вам может понадобиться отключить двухфакторную проверку подлинности для отдельного пользователя, не отключая ее для всех остальных. Такая необходимость может возникнуть, если данный пользователь используется для доступа к API.

***Важно!*** *Не переводите обычных пользователей в категорию пользователей услуги с тем, чтобы отключить двухфакторную проверку подлинности. В противном случае у пользователей могут возникнуть проблемы при входе в систему.*

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия.
2. Щелкните **Отметить как сервисную учетную запись**. В результате пользователь получит особый статус двухфакторной проверки подлинности, который называется **Учетная запись службы**.
3. [Если у клиента есть хотя бы один пользователь, который настроил двухфакторную проверку подлинности] Для подтверждения отключения введите код TOTP, сгенерированный в приложении проверки подлинности на устройстве второго фактора.

### Порядок включения двухфакторной проверки подлинности для пользователя

Вам может понадобиться включить двухфакторную проверку подлинности для пользователя, для которого она была отключена ранее.

1. На портале управления на вкладке **Пользователи** найдите пользователя, для которого необходимо изменить настройки, а затем щелкните значок многоточия.
2. Щелкните **Отметить как обычную учетную запись**. В результате пользователю необходимо будет настроить двухфакторную проверку подлинности или указывать код TOTP при входе в систему.

## 3.6.4 Сброс двухфакторной проверки подлинности при утрате устройства второго фактора

Для сброса доступа к учетной записи при утрате устройства второго фактора можно применить один из описанных ниже подходов.

- Восстановите секретный ключ TOTP (QR-код или буквенно-цифровой код) с резервной копии.

  На другом устройстве второго фактора добавьте сохраненный секретный ключ TOTP в приложение проверки подлинности, установленное на этом устройстве.
- Обратитесь к администратору с просьбой сбросить настройки двухфакторной проверки подлинности для вашей учетной записи (стр. 12).

### 3.6.5 Защита от атак методом перебора

В ходе атаки методом перебора злоумышленник пытается получить доступ к системе, многократно отправляя пароли в надежде подобрать верную последовательность.

Защита от атак методом перебора основана на cookie-файлах устройства.

Параметры защиты от таких атак предварительно заданы на платформе.

| **Параметр** | **Ввод пароля** | **Ввод кода TOTP** |
|---|---|---|
| Максимальное число попыток | 10 | 5 |
| Период ограничения числа попыток (после которого ограничение сбрасывается) | 15 мин (900 с) | 15 мин (900 с) |
| Применение блокировки | Максимальное число попыток + 1 (11-я попытка) | Максимальное число попыток |
| Период блокировки | 5 мин (300 с) | 5 мин (300 с) |

Если вы включили двухфакторную проверку подлинности, cookie-файл устройства выдается клиенту (браузеру) только после удачной проверки подлинности с использованием двух факторов (пароль и код TOTP).

Если используется доверенный браузер, cookie-файл устройства выдается после удачной проверки подлинности с использованием одного фактора (пароля).

Попытки ввода кода TOTP регистрируются для каждого пользователя, а не для устройства. Это означает, что, если пользователь попытается ввести код TOTP с других устройств, он все равно будет заблокирован.

# 4 Мониторинг

Чтобы получить информацию об использовании служб и операциях, щелкните **Обзор**.

## 4.1 Использование

На вкладке **Использование** предоставлен обзор использования служб (включая квоты). На ней также можно получить доступ к консолям служб.

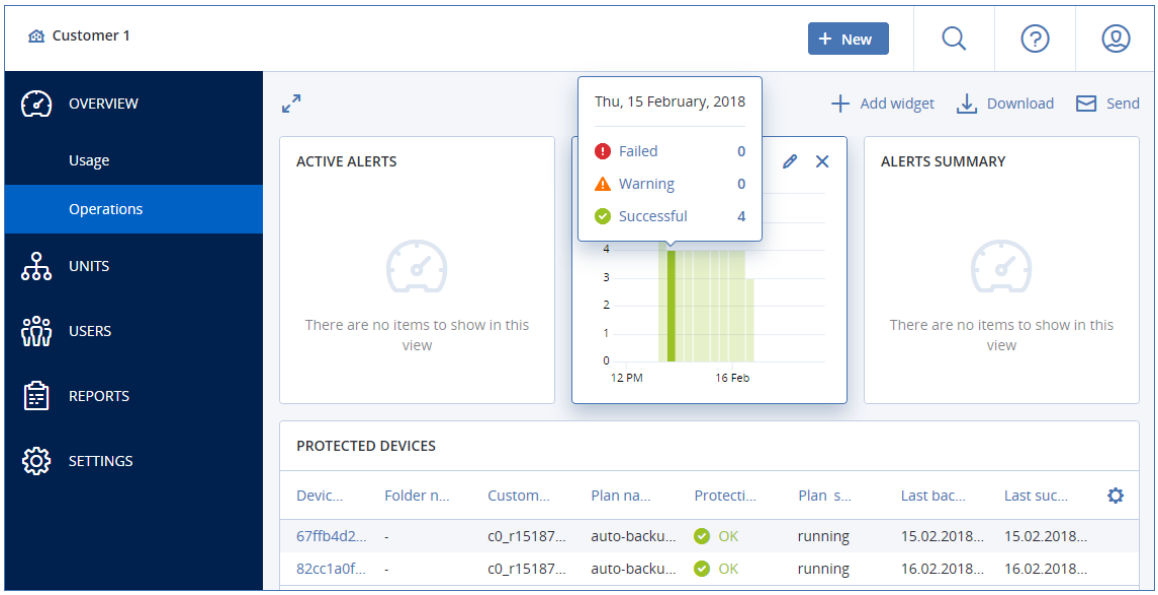
# 4.2 Операции

Панель мониторинга **Операции** доступна только для администраторов компании при работе на уровне компании.

На панели мониторинга **Операции** есть несколько настраиваемых виджетов, которые позволяют выполнить обзор операций, относящихся к сервису резервного копирования. Виджеты для других служб будут доступны в следующих выпусках.

Виджеты обновляются каждые две минуты. У виджетов есть активные элементы, на которые можно нажать для анализа возникших неполадок, их диагностики и устранения. Вы можете загрузить текущее состояние панели мониторинга или отправить его по электронной почте в файле формата .pdf и (или) .xlsx.

Вы можете выбирать из целого ряда виджетов, представленных в виде таблиц, линейчатых диаграмм и списков. Можно добавить несколько виджетов одного типа с разными фильтрами.




***Порядок изменения расположения виджетов на панели мониторинга***

Перетащите виджеты, щелкнув их имена.

***Порядок изменения виджета***

Щелкните значок карандаша рядом с именем виджета. Изменение виджета позволяет переименовать его, изменить диапазон времени и задать фильтры.

***Порядок добавления виджета***

Щелкните **Добавить виджет** и выполните одно из следующих действий:

- Щелкните виджет, который необходимо добавить. Виджет будет добавлен с настройками по умолчанию.
- Чтобы изменить виджет перед его добавлением, щелкните значок шестерни, когда виджет выбран. После изменения виджета щелкните **Готово**.

***Порядок удаления виджета***

Щелкните значок X рядом с именем виджета.

# 5 Отчеты

Чтобы получить доступ к отчетам об использовании служб и операциях, щелкните **Отчеты**.

## 5.1 Использование

В отчетах об использовании предоставлены исторические данные об использовании служб.

### Тип отчета

Можно выбрать один из указанных ниже типов отчета:

- **Текущее использование**

  В отчете содержатся показатели текущего использования службы.
- **Сводка за период**

  В отчете содержатся показатели использования службы за конец указанного периода и разница между показателями в начале и в конце указанного периода.
- **Ежедневно за период**

  В отчете содержатся показатели использования службы и данные об их изменении за каждый день указанного периода.

### Область отчета

Можно выбрать область отчета из указанных ниже значений:

- **Непосредственные пользователи и партнеры**

  В отчете будут содержаться показатели использования службы только для непосредственных дочерних отделов компании или отдела, в котором вы работаете.
- **Все пользователи и партнеры**

  В отчете будут содержаться показатели текущего использования службы для всех дочерних отделов компании или отдела, в котором вы работаете.
- **Все клиенты, партнеры и пользователи**

  В отчете будут содержаться показатели текущего использования службы для всех дочерних отделов компании или отдела, в котором вы работаете, а также для всех пользователей в отделах.

### Запланированные отчеты

Запланированный отчет охватывает показатели использования службы за последний полный календарный месяц. Данные отчеты формируются в 23:59:59 (по времени UTC) в первый день месяца и отправляются во второй день месяца. Они отправляются всем администраторам компании или отдела, которые в пользовательских параметрах установили флажок **Запланированные отчеты использования**.

#### *Порядок включения или отключения запланированного отчета*

1. Войдите на портал управления.
2. Убедитесь, что вы работаете в компании самого верхнего уровня, которая вам доступна.
3. Щелкните **Отчеты** > **Использование**.
4. Нажмите кнопку **Запланированные**.
5. Установите или снимите флажок **Отправлять ежемесячный сводный отчет**.
6. В разделе **Уровень детализации** выберите область отчета, как описано выше.

### Пользовательские отчеты

Пользовательский отчет формируется по требованию. Его невозможно запланировать. Отчет отправляется на ваш адрес электронной почты.

***Порядок формирования пользовательского отчета***

1. Войдите на портал управления.
2. Выберите отдел (стр. 7), для которого необходимо создать отчет.
3. Щелкните **Отчеты** > **Использование**.
4. Щелкните **Настраиваемый**.
5. В разделе **Тип** выберите тип отчета, как описано выше.
6. [Недоступно для отчета типа **Текущее использование**] В поле **Период** выберите период отчета:
   - **Текущий календарный месяц**
   - **Предыдущий календарный месяц**
   - **Пользовательские**
7. [Недоступно для отчета типа **Текущее использование**] Чтобы указать настраиваемый период создания отчетности, выберите начальную и конечную дату. В противном случае пропустите этот шаг.
8. В разделе **Уровень детализации** выберите область отчета, как описано выше.
9. Чтобы создать отчет, нажмите кнопку **Сформировать и отправить**.

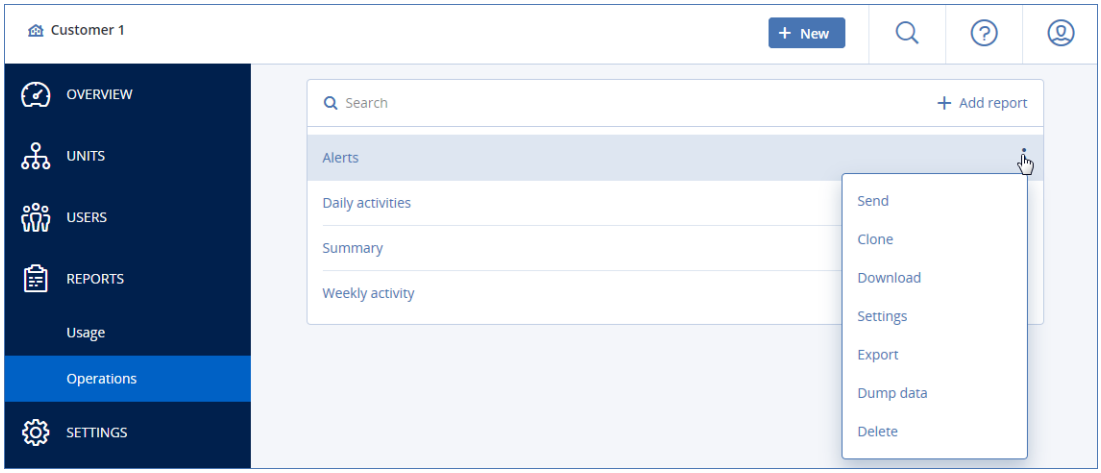
## 5.2 Операции

Отчеты **Операции** доступны только для администраторов компании при работе на уровне компании.

Отчет об операциях может включать в себя любой набор виджетов панели мониторинга **Операции** . Во всех виджетах отображается сводная информация для всей компании. Во всех виджетах показаны параметры для одного диапазона времени. Этот диапазон можно изменить в настройках отчета.

Для просмотра отчета щелкните его имя.

Чтобы получить доступ к операциям в отчете, щелкните значок в виде вертикального многоточия в строке отчета. Такие же операции доступны из отчета.



Вы можете использовать предварительно созданные отчеты или создать пользовательский отчет.

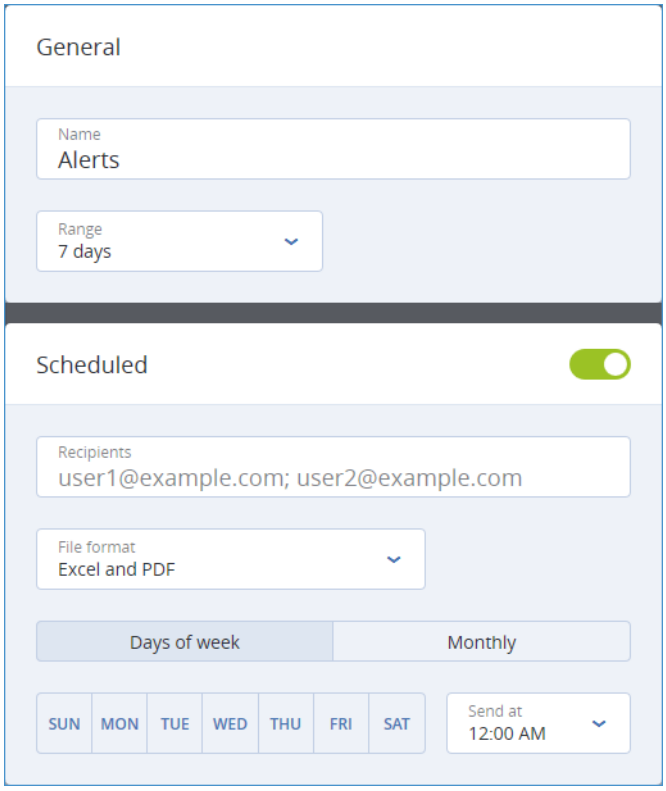
### Добавление отчета

1. Щелкните **Добавить отчет**.
2. Выполните одно из следующих действий:
   - Чтобы добавить предопределенный отчет, щелкните его имя.
   - Чтобы добавить настраиваемый отчет, щелкните **Настраиваемый**, выберите имя отчета (по умолчанию назначаются имена типа **Custom(1)**) и добавьте виджеты в отчет.
3. [Необязательно] Для изменения положения виджетов перетащите их.
4. [Необязательно] Измените отчет, как описано ниже.

### Изменение отчета

Чтобы изменить отчет, щелкните его имя и выберите пункт **Настройки**. При изменении отчета можно выполнить следующие действия:

- Переименовать отчет.
- Изменить диапазон времени для всех виджетов, включенных в отчет.
- Запланировать отправку отчета по электронной почте в формате PDF и (или) XLSX.




### Планирование отчета

1. Щелкните имя отчета и выберите пункт **Настройки**.
2. Включите переключатель **Запланировано**.
3. Укажите адреса электронной почты получателей.
4. Выберите формат отчета: .pdf, .xlsx или и то, и другое.
5. Выберите дни и время отправки отчета.
6. Щелкните **Сохранить** в верхнем правом углу.

### Экспорт и импорт структуры отчета

Структуру отчета (набор виджетов и настройки отчета) можно экспортировать и импортировать в файл .json.

Чтобы экспортировать структуру отчета, щелкните имя отчета, щелкните значок в виде вертикального многоточия в правом верхнем углу и выберите пункт **Экспорт**.

Для импорта структуры отчета щёлкните **Добавить отчет** и выберите пункт **Импорт**.

### Дамп данных отчета

Дамп данных отчета в файле .csv можно отправить по электронной почте. Дамп содержит все данные отчета (без фильтрации) за определенный промежуток времени.

ПО динамически генерирует дамп данных. При указании большого промежутка времени данное действие может долго выполняться.

***Дамп данных отчета***

1. Щелкните имя отчета.
2. Нажмите значок в виде вертикального эллипса в правом верхнем углу и затем нажмите **Дамп данных**.
3. Укажите адрес электронной почты получателей.
4. В **Диапазон времени** укажите диапазон времени.
5. Щелкните **Отправить**.

# 6 Журнал аудита

Чтобы посмотреть журнал аудита, щелкните пункт **Журнал аудита**.

В журнал аудита в хронологическом порядке заносятся следующие события:

- операции, выполняемые пользователями на портале управления;
- системные сообщения о достижении и использовании квот.

В журнале отображаются события во всей организации или в подразделении, в котором вы работаете в настоящий момент, а также его дочерних подразделениях. Чтобы посмотреть более подробные сведения о событии, щелкните по нему.

Журнал ежедневно очищается. События удаляются через 180 дней.

## Поля журнала аудита

Для каждого события в журнале отображаются указанные ниже данные.

- **Событие**

  Краткое описание события. Пример: **Клиент создан**, **Клиент удален**, **Пользователь создан**, **Пользователь удален**, **Квота достигнута**.

- **Серьезность**

  Принимает перечисленные ниже значения.

  - **Ошибка**

    Обозначает ошибку.

  - **Предупреждение**

Обозначает действие с потенциально отрицательным эффектом. Пример: **Клиент удален**, **Пользователь удален**, **Квота достигнута**.

- **Уведомление**

  Обозначает событие, которое может требовать внимания. Пример: **Клиент обновлен**, **Пользователь обновлен**.

- **Информация**

  Нейтральное изменение или действие информационного характера. Пример: **Клиент создан**, **Пользователь создан**, **Квота обновлена**.

- **Дата**

  Дата и время события.

- **Имя объекта**

  Объект, с которым была выполнена операция. Например для события **Пользователь обновлен** объектом является пользователь, свойства которого были изменены. Для событий, связанных с квотами, объектом является квота.

- **Клиент**

  Название отдела, к которому относится объект. Например для события **Пользователь обновлен** клиентом является отдел, в котором расположен пользователь. Для события **Квота достигнута** клиентом является пользователь, для которого достигнута данная квота.

- **Инициатор**

  Имя пользователя, инициировавшего событие. Для системных сообщений и событий, инициируемых администраторами верхнего уровня, в качестве инициатора отображается **Система**.

- **Клиент инициатора**

  Название отдела, к которому относится инициатор. В случае системных сообщений и событий, инициируемых администраторами верхнего уровня, это поле остается пустым.

- **Метод**

  Показывает, было ли событие инициировано через веб-интерфейс или через API.

- **IP-адрес**

  IP-адрес машины, с которой инициировано событие.

### Фильтрация и поиск

События можно фильтровать по описанию, серьезности и дате. Кроме того, можно искать события по объектам, отделам, инициаторам и отделам инициаторов.

# 7 Дополнительные примеры

## 7.1 Ограничение доступа к веб-интерфейсу

Можно ограничить доступ к веб-интерфейсу, указав список IP-адресов, с которых пользователям будет разрешено выполнять вход.

Это ограничение также действует для доступа к порталу управления через API.

Это ограничение применяется только на том уровне, на котором оно задано. Это *не* применяется к участникам дочерних отделов.

***Порядок ограничения доступа к веб-интерфейсу***

1. Войдите на портал управления.
2. Найдите отдел (стр. 7), в котором необходимо ограничить доступ.
3. Щелкните **Настройки** > **Безопасность**.
4. Установите флажок **Включить управление входом**.
5. В поле **Разрешенные IP-адреса** укажите разрешенные IP-адреса.

   Можно ввести любые из указанных ниже параметров, используя в качестве разделителя точку с запятой:

   - IP-адреса, например 192.0.2.0
   - Диапазоны IP-адресов, например 192.0.2.0–192.0.2.255
   - Подсети, например 192.0.2.0/24
6. Нажмите кнопку **Сохранить**.

## 7.2 Ограничение доступа к вашей компании

Администраторы компании могут ограничить доступ к компании для администратора более высокого уровня.

Если доступ к компании ограничен, администраторы более высокого уровня могут только менять свойства компании. Они вообще не видят учетные записи и дочерние отделы.

***Порядок ограничения доступа к компании***

1. Войдите на портал управления.
2. Щелкните **Настройки** > **Безопасность**.
3. Снимите флажок **Разрешить администраторам из родительских клиентов управлять этим клиентом**.
4. Нажмите кнопку **Сохранить**.