# Настройка политик

## Управление политиками

Раздел содержит список политик, расположенных по приоритету применения.

Для политик отображаются данные:

- **Приоритет** - число, указывающее порядок применения конкретной политики по отношению к остальным. Нулевой приоритет соответствует политике по умолчанию (Default policy) и применяется в самую последнюю очередь. Чем выше расположена политика, тем выше её приоритет и наоборот.
- **Имя** - название политики.
- **Описание** - произвольный текст.
- - количество пользователей, на которые действует политика.
- - количество учётных записей, на которые действует политика.
- - количество ресурсов, на которые действует политика.
- - количество доменов, на которые действует политика.


**Политика по умолчанию** содержит набор параметров для всех доступных категорий и применяется ко всем новым объектам, поэтому целесообразно начать настройку с неё.

**Политика по умолчанию применяется и к сессиям, открытым от имени пользовательских учетных записей, если к данным пользователям явно не применены другие политики.**

Откройте страницу политики, задайте нужные параметры для категорий **Учетные записи**, **Сессии**, **RDP**, и сохраните настройки.

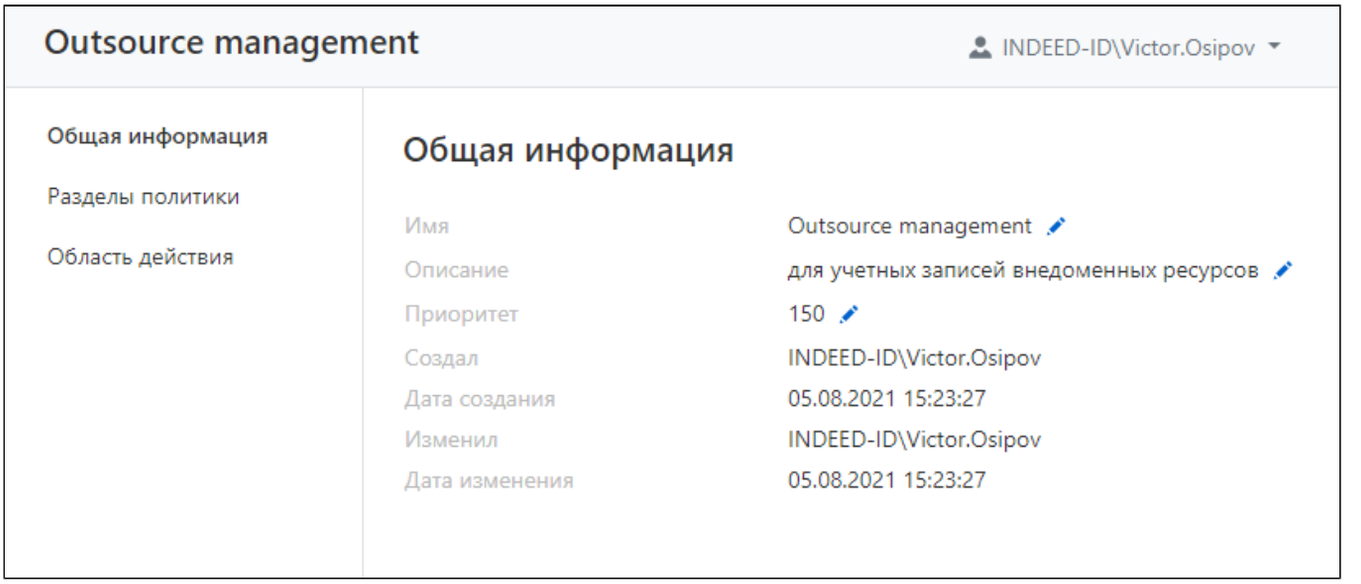
## Добавление новой политики

**Для добавления, просмотра, редактирования и удаления политик необходимы соответствующие привилегии из раздела Управление политиками (Policy.Create, Policy.Read, Policy.Update, Policy.Delete).**

Нажмите **Добавить** в разделе **Политики**, заполните поля **Имя политики**, **Описание**, и **Приоритет**. Новая политика отобразится в списке.

**Общая информация**

Откройте страницу политики, ознакомьтесь с общей информацией, при необходимости внесите правки в **Имя**, **Описание** или **Приоритет**, нажав значок карандаша

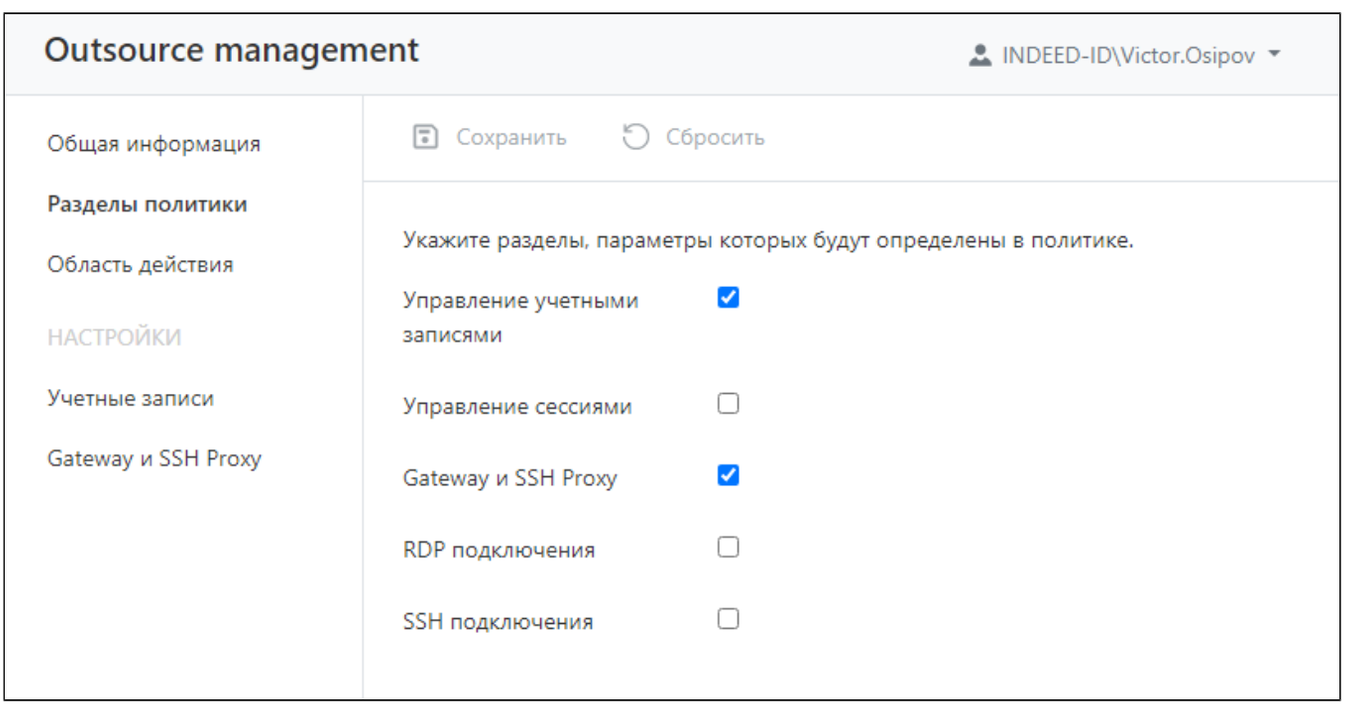


- **Имя** - название политики, устанавливается при создании новой политики, может быть изменено в любой момент эксплуатации.
- **Описание** - необязательное поле.
- **Приоритет** - числовое значение приоритета политики. Нулевой приоритет - минимальный, применяется к объектам в последнюю очередь.
- **Создал** - имя администратора Indeed PAM.
- **Дата создания** - дата и время создания политики.
- **Изменил** - имя администратора Indeed PAM, который сохранил настройки политики.
- **Дата изменения** - дата и время сохранения настроек политики.

Для редактирования **Имени**, **Описания** и **Приоритета** нажмите

#### Разделы политики

Перейдите в **Разделы политики** и отметьте разделы, параметры которых будут определены политикой, сохраните изменения. Соответствующие разделы станут доступными для настройки параметров.




Для неотмеченных разделов будут применяться другие политики по порядку их приоритета.

#### Область действия

**Для назначения политик необходимы соответствующие привилегии (Account.SetPolicy, User.SetPolicy, Resource.SetPolicy, Domain.SetPolicy).**

Содержит данные о том, к каким пользователям, учетным записям, ресурсам или доменам применена политика.

Чтобы применить политику к объекту, нажмите **Добавить**, выберите тип объекта для установки политики и далее сами объекты.

Чтобы отменить действие политики от объектов, выберите нужные объекты и нажмите **Удалить.**

### Создание копии политики

Отметьте одну политику в разделе **Политики** и нажмите **Создать копию**, заполните поля **Имя политики**, **Описание** и **Приоритет**.
Скопированная политика отобразится в списке.

### Удаление политики

Перед удалением политики убедитесь, что она не применяется ни к каким объектам.

Отметьте нужные политики в разделе **Политики** и нажмите **Удалить**.

> Политика **Default policy** недоступна для удаления.

### Изменение приоритета политики

Отметьте галочкой одну политику в разделе **Политики**, нажмите **Задать приоритет** и введите число для значения приоритета политики.

Также изменить приоритет можно открыв нужную политику и в разделе Общая информация нажать значок карандаша рядом со значением приоритета.

## Разделы политик

### Учетные записи

| Опция | Описание |
|---|---|

| | |
|---|---|
| **Показ учетных данных** | |
| Сбрасывать пароль и SSH ключ учетной записи после показа | Если опция включена, то пароль и SSH ключ привилегированной учетной записи будет сбрасываться каждый раз после просмотра пользователем в своем личном кабинете (консоли пользователя). |
| Сбрасывать пароль и SSH ключ через **X** мин. | После просмотра пароль и SSH ключ будет сброшен на случайное значение через указанное количество минут. |
| Требовать указать причину просмотра пароля и SSH ключа | Если опция включена, то пользователь каталога должен указать причину перед просмотром пароля или SSH ключа учётной записи доступа. |
| Просмотр пароля и SSH ключа требует подтверждения администратором PAM | Если опция включена, то перед каждым просмотром пользователем учетных данных администратор PAM должен подтвердить операцию. |
| Время ожидания подтверждения просмотра пароля и SSH ключа, мин. | Таймаут ожидания подтверждения просмотра пароля и SSH ключа, от 1 до 180 минут. |
| Шифровать SSH ключ сгенерированным паролем перед показом пользователю | Если опция включена, то SSH ключ будет показан в зашифрованном виде, а сгенерированный пароль шифрования - в скрытом. Ключ и пароль шифрования генерируется средствами PAM при просмотре данных каждый раз заново. |
| **Проверка и смена учетных данных** | |
| Синхронизировать ресурсы и УЗ по расписанию | Если опция включена, то будет выполняться автоматический поиск данных о ресурсах и учётных записей доступа. |
| Синхронизировать ресурсы и УЗ раз в **X** дней | Автоматический поиск данных о ресурсах и учётных записей доступа будет выполняться один раз в указанное количество дней, от 1 до 10000 дней |
| Периодически проверять пароль и SSH ключ учетной записи | Если опция включена, то будет выполняться автоматическая проверка паролей и SSH-ключей для учётных записей доступа. |
| Проверять пароль и SSH ключ раз в **X** дней | Автоматическая проверка паролей и SSH-ключей учётных записей доступа будет выполняться один раз в указанное количество дней, от 1 до 10000 дней. |
| Сбрасывать пароль и SSH ключ если обнаружено несовпадение | Если опция включена, то будет выполняться автоматический сброс паролей и ключей при расхождении в PAM и на ресурсах. |
| Удалять SSH ключи, не управляемые PAM | Если в PAM нет SSH ключа для добавленной учетной записи, а на ресурсе есть, то с ресурса все обнаруженные ключи будут удалены. |
| Проверять пароль и SSH ключ при ручной установке | Если опция включена, то при установке или изменении пароля или SSH-ключа будет выполняться их проверка. |
| Периодически изменять пароль и SSH ключ учетной записи | Если опция включена, то для учётных записей доступа будет автоматически изменяться пароль или SSH-ключ на случайное значение. |
| Изменять пароль и SSH ключ учетной записи раз в **X** дней | Автоматическое изменение пароля или SSH-ключа для учётных записей доступа будет выполняться один раз в указанное количество дней. |
| **Требования к паролю** | |
| Длина генерируемого пароля | Общее количество символов для автоматически генерируемых паролей и вводимых вручную. |

| | |
|---|---|
| Минимальная длина пароля (ручной ввод) | Минимальное количество символов при ручном изменении пароля. |
| Латинские строчные буквы | Если опция включена, то автоматически генерируемые пароли будут состоять из латинских строчных букв. При комбинации с другими настройками пароль будет содержать минимум одну латинскую строчную букву. |
| Латинские прописные буквы | Если опция включена, то автоматически генерируемые пароли будут состоять из латинских прописных букв. При комбинации с другими настройками пароль будет содержать минимум одну латинскую прописную букву. |
| Цифры | Если опция включена, то автоматически генерируемые пароли будут состоять из цифр. При комбинации с другими настройками пароль будет содержать минимум одну цифру. |
| Специальные символы | Если опция включена, то автоматически генерируемые пароли будут состоять из специальных символов. При комбинации с другими настройками пароль будет содержать минимум один специальный символ. |

## Сессии

| Опция | Описание |
|---|---|
| **Общее** | |
| Требовать указать причину подключения | Если опция включена, то при подключении к конечному ресурсу, пользователь обязан указать причину запуска сессии. |
| Ограничить длительность сессии | Настройка позволяет задать время длительности сессии до принудительного завершения. |
| Максимальная длительность сессии | Опция задействует предел длительности сессии в часах и минутах, после истечения которого сессия будет принудительно завершена. |
| Включить эксклюзивное использование учетной записи | Если опция включена, то учетная запись может быть использована только в одной активной сессии одновременно. |
| Открытие сессии требует подтверждения администратором PAM | Если опция включена, то для каждой открываемой сессии необходимо ручное подтверждение администратора PAM. |
| Время ожидания подтверждения сессии | Таймаут для подтверждения администратором PAM, в интервале от 1 до 180 минут. |
| Сбрасывать пароль и SSH ключ по завершении сессии | Сброс пароля и SSH ключа после каждой сессии. |
| **Артефакты** | |
| Сохранять текстовые логи сессии | Если опция включена, то после завершения сессии будет доступен для просмотра и скачивания текстовый лог. Поддерживается только в сессиях на Windows ресурсах при наличии PAM агента и в SSH сессиях. |
| Сохранять видео сессии | Если опция включена, то после завершения сессии будет доступна для просмотра и скачивания запись потокового видео. Поддерживается только при открытии сессий через PAM Gateway. |
| Количество кадров в секунду | Настройка определяет частоту кадров для записи потокового видео, от 1 до 10. |
| Разрешение видео | Настройка позволяет установить разрешение для записи потокового видео. |
| Ротация видео | Если опция включена, то записи потокового видео будут автоматически удаляться. |

| | |
|---|---|
| Удалять видео сессии старше X дней | Автоматическое удаление записи потокового видео старше указанного количества дней, от 1 до 10000. |
| Сохранять снимки экрана | Если опция включена, то снимки экрана сессии будут сохраняться. Поддерживается только при открытии сессий через PAM Gateway. |
| Интервал снимков, сек | Сохранение снимка экрана через указанной количество секунд, от 60 до 10000. |
| Разрешение изображения | Настройка позволяет установить разрешение снимка экрана. |
| Ротация снимков экрана | Если опция включена, то снимки экрана будут автоматически удаляться. |
| Удалять снимки экрана старше X дней | Автоматическое удаление снимков экрана старше указанного количества дней. |
| Сохранять переданные на сервер файлы | Если опция включена, то файлы при передаче с локальной машины на ресурс будут дублироваться в указанную сетевую папку. Поддерживается только для Windows ресурсов с включенным пробросом дисков (про раздел RDP - ниже). |
| Ротация переданных файлов | Если опция включена, то переданные файлы будут автоматически удаляться. |
| Удалять переданные на сервер файлы старше X дней | Автоматическое удаление файлов старше указанного количества дней, от 1 до 10000. |
| **Отправка текстового лога по syslog** | |
| По syslog будут отправлены строки текстового лога, в которых будут найдены указанные ключевые слова. Ключевое слово может быть регулярным выражением. | |

## Gateway и SSH Proxy

| Опция | Описание |
|---|---|
| Переопределить настройки подключения к Gateway | Если опция включена, то следующие настройки будут использованы вместо указанных в разделе Конфигурация |
| Адрес RDCB | IP адрес/DNS имя Remote Desktop Connection Broker |
| Имя коллекции RDCB | Имя коллекции Remote Desktop Connection Broker для Indeed PAM Gateway |
| Использовать RDGW | Подключаться к Indeed PAM Gateway с использованием Remote Desktop Gateway |
| Адрес RDGW | Адрес Remote Desktop Gateway для Indeed PAM Gateway |
| Параметры Gateway RDP файла | Параметры будут добавлены в настройки подключения RDP к PAM Gateway и заменят старые настройки. |
| Переопределить настройки SSH Proxy | Если опция включена, то следующая настройка будет использована вместо указанной в разделе Конфигурация |
| Адрес SSH Proxy | IP адрес или DNS имя и порт (необязательно). |

## RDP

Настройки применяются только при подключении к серверам по протоколу RDP.

| Опция | Описание |
| --- | --- |
| Принтеры | Если опция включена, то пользователь получит возможность пробросить принтер со своего рабочего места на конечный ресурс. |
| Буфер обмена | Если опция включена, то пользователь получит возможность использовать буфер обмена между своим рабочим местом и конечным ресурсом. |
| Смарт-карты | Если опция включена, то пользователь получит возможность пробросить смарт-карту со своего рабочего места на конечный ресурс. |
| Порты | Если опция включена, то пользователь получит возможность пробросить COM-порты со своего рабочего места на конечный ресурс. |
| Диски | Если опция включена, то пользователь получит возможность пробросить локальные диски со своего рабочего места на конечный ресурс. |
| Параметры RDP файла | Параметры, которые будут добавлены в настройки подключения RDP и заменят старые настройки. |

## SSH

Повышение привилегий.

- **Разрешить выполнять pamsu** - поддержка выполнения команд с привилегиями root в ssh сессиях на ресурсах с установленным компонентом PamSu.

Список команд разрешённых либо запрещённых для выполнения в SSH сессии.

- **Приглашение оболочки (prompt)** - регулярное выражение приглашения оболочки для корректного распознавания ввода команд.
- **Реакция на запрещенную команду** - поведение терминала в ответ на запрещённую команду: CTRL+C (отмена выполнения) либо завершение сессии.

Для составления списка контролируемых команд:

1. Нажмите кнопку **Добавить**
2. Введите команду либо регулярное выражение
3. Выберите состояние **Разрешена** либо **Запрещена**.

> Запрет на выполнение команд имеет приоритет над разрешением.
>
> Без явного разрешения команды будут считаться запрещёнными, поэтому не рекомендуется удалять последнее правило, разрешающее выполнение команд.

Для разрешения либо запрета сразу нескольких команд отметьте их флажками и нажмите соответствующую кнопку.

При работе со списком команд, а также при попытках выполнения запрещённой команды в журнале фиксируются соответствующие события.