

Установка и настройка агентов на рабочих станциях

Клиентская часть Агента устанавливается на рабочие станции пользователей. Необходимые для связи с сервером RutokenKeyBox настройки задаются через групповые политики или реестр Windows.

Запустите файл **IndeedCM.Agent.msi** из дистрибутива RutokenKeyBox (каталог RutokenKeyBox.Client) и выполните установку, следуя указаниям мастера. После установки Агент запустится автоматически.

Настройка параметров работы Агента через групповые политики

Для добавления административных шаблонов выполните следующие действия:

1. Скопируйте содержимое каталога **RutokenKeyBox.Client\Misc** в центральное хранилище ADMX-файлов контроллера домена **C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions**.
При использовании локального хранилища ADMX-файлов поместите шаблоны в **C:\Windows\PolicyDefinitions**.
2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве окна консоли создайте новый объект групповой политики или выберите существующий.
4. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).
5. В открывшемся **Редакторе управления групповыми политиками** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) > **Политики** (Policies) > **Административные шаблоны** (Administrative Templates) > **RutokenKeyBox** > **Agent**.
6. Включите политику **Настройка URL сервисов агентов** и укажите её значения:
 - в параметре **URL сервиса регистрации агентов** укажите веб-адрес и порт подключения к приложению **agentregistrationapi**, размещенного на сервере RutokenKeyBox.
 - в параметре **URL сервиса агентов** укажите веб-адрес и порт сервиса **agentserviceapi**.

Пример:

URL сервиса регистрации агентов: <https://srv.demo.local:3003/agentregistrationapi/>
URL сервиса агентов: <https://srv.demo.local:3003/agentserviceapi/>

7. Свяжите этот объект политики с группой, членами которой являются рабочие станции пользователей системы РутOKEN KeyBox.
8. Нажмите **Применить** (Apply) и выполните обновление политик.
Обновление политик происходит при перезагрузке рабочей станции с установленным клиентским агентом. Для принудительного обновления групповых политик без перезагрузки выполните команду **gpupdate /force**.

В случае необходимости настройте дополнительные политики, определяющие работу Агентов:

Настройки таймаутов агентов

Политика задает:

- Таймаут запросов к сервисам агента (по умолчанию: 30 с).
- Периодичность запроса проверки статуса агента (по умолчанию: 300 с).
- Периодичность запроса на обновление настроек, привязок, задач и сессий (по умолчанию: 30 с).
- Таймаут запроса отключения агента от сервера (по умолчанию: 3 с).

Настройки кэширования событий

Политика задает настройки кэширования событий:

- Период в минутах, в течение которого агент будет пытаться отправить события из кэша на сервер (по умолчанию: 10 мин).
- Количество событий, передаваемых за один раз из кэша рабочей станции пользователя на сервер (по умолчанию: 500 событий).

Настройки прокси-сервера

Политика определяет использование прокси-сервера при подключении к серверу RutokenKeyBox.

Если политика не задана или отключена, прокси-сервер использоваться не будет.
В параметре "Прокси-сервер" задается адрес прокси-сервера.

Настройки записи событий

Политика задает уровень записи событий в серверный журнал:

- Все (по умолчанию).
- Только ошибки.
- Только ошибки и предупреждения.

Настройки кэширования задач

Политика задает:

- Периодичность обновления кэша задач и отправки статуса выполнения задачи на сервер, если сразу не удалось сообщить статус серверу (по умолчанию: 60 с).
- Таймаут, при котором задачи будут удалены из кэша при очередном обновлении кэша (по умолчанию: 300 с).
- Таймаут, после которого можно будет повторно выполнить отмененную пользователем задачу (по умолчанию: 60 с).

Настройки периода проверки статуса устройств

Политика задает периодичность проверки статуса устройств (по умолчанию: 30 с):

- Блокировка PIN-кода пользователя\администратора.
- Попытки ввода неверного PIN-кода пользователя\администратора.

Настройка параметров работы Агента через реестр

Создайте файл реестра (.reg) со следующим содержанием:

```
Windows Registry Editor Version 5.00

[HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IndeedCM\Agent]
"AgentRegistrationServiceUrl"=""
"AgentServiceUrl"=""
"ProxyEnable"=""
"ProxyServer"=""
```

Для 32-разрядных ОС параметры настраиваются в ветке:

[HKKEY_LOCAL_MACHINE\SOFTWARE\RutokenKeyBox\Agent]

В параметре **AgentRegistrationServiceUrl** укажите ссылку и порт подключения к приложению **agentregistrationapi**.

В параметре **AgentServiceUrl** укажите web-адрес и порт подключения к приложению **agentserviceapi**.

Если на рабочих станциях где установлен клиентский агент используется прокси, то укажите параметры **ProxyEnable** и **ProxyServer** (URL прокси-сервера).

Возможные значения параметров:

- "ProxyEnable"=dword:00000000 - прокси не используется.
- "ProxyEnable"=dword:00000001 и "ProxyServer"="" - используются настройки прокси по умолчанию.
- "ProxyEnable"=dword:00000001 и "ProxyServer"="<URL прокси-сервера>" - используется прокси-сервер, указанный в настройке.

Ниже приведен пример содержимого .reg-файла для подключения к серверу RutokenKeyBox с именем *srv.demo.local* по протоколу *https* и порту *3003* с использованием прокси-сервера <https://192.168.10.10:443>.

Пример:

```
Windows Registry Editor Version 5.00

[HKKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IndeedCM\Agent]
"AgentRegistrationServiceUrl"="https://srv.demo.local:3003/agentregistrationapi"
"AgentServiceUrl"="https://srv.demo.local:3003/agentserviceapi"
"ProxyEnable"=dword:00000001
"ProxyServer"="https://192.168.10.10:443"
```

Распространите файл реестра и внесите изменения на рабочие станции пользователей. Для применения внесенных изменений перезагрузите рабочую станцию с установленным Агентом RutokenKeyBox или перезапустите службу **RutokenKeyBox Agent Service**.