Настройка разблокировки устройств

Разблокировка устройств реализована в двух режимах:

1. **Online режим** подразумевает, что рабочая станция пользователя, к которой подключено заблокированное устройство, имеет соединение с сервером RutokenKeyBox. Соединение с сервером необходимо для проведения аутентификации пользователя при помощи ответов на секретные вопросы. Для связи рабочих станций пользователей с сервером RutokenKeyBox при online-разблокировке рекомендуется использовать защищенное соединение (https).
2. Разблокировка в **Offline режиме** осуществляется оператором Рутокен KeyBox по принципу аутентификации вида запрос-ответ (англ. challenge-response authentication mechanism).
   При исчерпании заданного числа попыток ввода PIN-кода, пользователь получает сообщение о том, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный 16 символьный код-запрос. Пользователю необходимо связаться с оператором системы (например, по телефону) и подтвердить свою личность.

Настройка разблокировки устройств через групповые политики

Для включения возможности **online**-разблокировки устройств настройте соответствующую групповую политику. Эта политика должна распространяться на **рабочие станции пользователей** Рутокен KeyBox.

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 > Client** .
6. Включите политику **Сервер разблокировки смарт-карт** (Smart card unlocking server) и укажите её значения:

   - в параметре **URL сервиса** (Service URL) укажите ссылку на компонент **credprovapi**, размещенный на сервере RutokenKeyBox.

     https://<FQDN сервера RutokenKeyBox>/cm/credprovapi
   - в параметре **Проверять сертификат сервера** (Verify server certificate) установите значение **Да**, если необходимо проводить проверку подлинности сертификата сервера. Установите **Нет** (значение по умолчанию), если проверку подлинности проводить не требуется.

7. Свяжите этот объект политики с группой, членами которой являются рабочие станции пользователей системы Рутокен KeyBox.
8. Нажмите **Применить** (Apply) и выполните обновление политик.

В случае необходимости настройте дополнительные политики, определяющие работу сервиса разблокировки:

Задать разъяснения для offline-разблокировки (Set explanations for offline unlocking)

Политика применяется к рабочим станциям пользователей. Если политика **выключена или не определена**, то при offline-разблокировке устройства текст разъяснения в Credential Provider не отображается.
Если политика **включена** то, при offline-разблокировке устройства в Credential Provider будет отображаться указанный в политике текст разъяснения. Например, контактный телефон администратора Рутокен KeyBox.

Credential Providers: Отключить обертку стандартного провайдера смарт-карт (Credential Providers: Disable smart card standard provider wrapping)

Политика применяется к рабочим станциям пользователей. Если политика **выключена или не определена**, пользователь имеет возможность выполнить разблокировку смарт-карты в стандартном интерфейсе входа в ОС Windows по смарт-карте.
Если политика **включена**, то отдельная опция для разблокировки смарт-карты будет отображаться на экране входа в ОС. Такая настройка может быть использована в ситуации, когда на рабочей станции установлено стороннее ПО, запрещающее разблокировку карты через стандартный Credential Provider.

Credential Providers: Скрывать опцию "Выключить смарт-карту" (Credential Providers: Hide the "Disable the smart card" option)

Политика применяется к рабочим станциям пользователей. Если политика **выключена или не определена**, пользователь имеет возможность выполнить выключение смарт-карты в интерфейсе входа в ОС Windows.
Если политика **включена**, то опция для выключения смарт-карты не будет отображаться на экране входа в ОС.

Настройка разблокировки устройств вне домена Windows

В случае, когда сервер RutokenKeyBox и рабочие станции пользователей находятся вне домена Windows, путь к приложению **credprovapi** необход имо прописать в реестре каждой клиентской рабочей станции. Для этого создайте файл реестра (.reg) со следующим содержанием:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RutokenKeyBox\Client]
"CredProvAPIURL"=""
"AdminDetails"=""
"DisableServerCertificateChecking"=dword:00000000
"DisableSuspendCP"=dword:00000000
"DisableWrapperCP"=dword:00000000
```

В параметре **CredProvAPIURL** задайте адрес приложения credprovapi на сервере RutokenKeyBox.

В параметре **AdminDetails** задайте текст разъяснения для пользователя.

В параметре **DisableServerCertivicateChecking** установите значение **0** (значение по умолчанию), если необходимо проводить проверку подлинности сертификата сервера RutokenKeyBox. Установите **1** (dword:00000001), если проверку подлинности проводить не требуется.

В параметре **DisableSuspendCP** установите значение **0** (значение по умолчанию), если в интерфейсе ОС необходимо отображать кнопку "Выключение смарт-карты" или значение **1** (dword:00000001), если кнопку "Выключение смарт-карты" отображать не требуется.

В параметре **DisableWrapperCP** установите значение **0** (значение по умолчанию), если необходимо выполнять разблокировку смарт-карты с использованием стандартного Credential Provider. Установите значение **1** (dword:00000001), если необходимо использовать отдельный Credential Provider.

Ниже приведен пример .reg-файла для сервера RutokenKeyBox с именем машины *rutokenkeybox.demo.local*, включенной проверкой подлинности сертификата сервера, отключенным отображением кнопки "Выключить смарт-карту" и включенной опцией разблокировки смарт-карты в отдельном Credential Provider на экране входа в ОС:
Пример:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RutokenKeyBox\Client]
"CredProvAPIURL"="https://rutokenkeybox.demo.local/cm/credprovapi"
"AdminDetails"="      1607"
"DisableServerCertificateChecking"=dword:00000000
"DisableSuspendCP"=dword:00000001
"DisableWrapperCP"=dword:00000001
```