



Rohos® Logon Key  
Руководство для IT Администратора  
по использованию программы

Март 2008



## Содержание

1.	О руководстве.....	3
2.	Правовая информация .....	3
3.	Введение в Rohos Logon Key .....	4
3.1	Назначение.....	4
3.2	Основные возможности программы .....	4
3.3	Режимы авторизации (logon model) .....	5
3.4	Требования к программному и аппаратному обеспечению.....	11
4.	Руководство по использованию .....	11
4.1	Использование Серверной версии .....	12
4.2	Утилита управления USB ключами .....	12
4.3	Настройка login профиля на USB ключе .....	13
4.4	Утилита – Rohos Remote Config .....	15
4.5	Настройка ключа USB для доступа к удаленному компьютеру .....	17
4.6	Настройка компьютера под управлением Windows Terminal Server .....	18
4.7	Настройка окна входа в систему .....	19
4.8	Установка Rohos Logon Key на рабочие станции (MSI пакет).....	20
4.9	Параметры пакета MSI .....	20
4.10	Отключение доступа к USB флэш драйвам и внешним носителям.....	22
5.	Компоненты Rohos Logon Key .....	23
5.1	Компоненты.....	23
5.2	Logon профайлы на USB накопителе.....	24
5.3	Настройки в Windows registry.....	24
6.	Примеры.....	26
Пробное использование программы в рамках компании .....	27	
Пример 1. Сеть, основанная на Windows Active Directory. Локальный вход в систему.....	27	
7.	Разрешение проблем.....	28
8.	Контакты и обновления.....	30

## 1. О руководстве

Данный документ предназначен для Администраторов компьютерной сети и руководителей IT отделов компании. Документ содержит информацию об установке и использовании программы Rohos Приветствие и USB ключей в компьютерной сети компании.

Сначала рекомендуем прочитать главу 6 Примеры Внедрение программы Rohos Logon Key в рамках компании.

**ПРИМЕЧАНИЕ:** Данный документ не является окончательным и находится на стадии доработки.

В случае возникновения вопросов, обращайтесь по адресу [mailbox@rohos.ru](mailto:mailbox@rohos.ru).

## 2. Правовая информация

### Данные об авторских правах

Copyright 2006-2007 Tesline-Service SRL

Авторские права защищены

В данном руководстве приведена информация о следующих компонентах программы :

- Программа Rohos Logon Key версии 2.4;
- Утилита управления USB Ключами;
- Пакет установки MSI.

### Дискламация

Вся информация, приведенная ниже, считается верной на день публикации, однако, Tesline-Service SRL не признает за собой ответственности за возможный ущерб, включая косвенный и являющийся следствием использования программного обеспечения или информации, приведенной в данном документе. Приведенная информация может быть изменена в любой момент без информирования об этом.

### Копирование программы

Распространение программного обеспечения или документации, полностью или частично в любой другой системе или предоставление их другой стороне может быть расценено как незаконное присвоение сведений о секретных и конфиденциальных технологиях и приемах, которые являются собственностью Tesline-Service SRL и других сторон.

### Условия лицензирования

Узнать специфические условия вашей лицензии вы можете в файлах readme.txt, license.txt, или в других лицензионных документах, которые поставляются с вашей версией программного обеспечения или вашим типом лицензии в виде текстовых файлов или как часть пакета установки ПО.

Для получения дополнительных лицензионных условий или копий программного обеспечения и/или документации обратитесь к вашему поставщику.

### Права на торговые марки

Все прочие зарегистрированные или незарегистрированные торговые марки, упоминаемые в данном документе, являются собственностью соответствующих владельцев.

Microsoft, Windows и Windows 2000, Windows XP, Windows Vista являются зарегистрированными торговыми марками Microsoft Corporation.

## 3. Введение в Rohos Logon Key

### 3.1 Назначение

Программа позволяет использовать обычный USB накопитель в качестве ключа для доступа в Windows и блокировки рабочего компьютера, вместо пароля.

### 3.2 Основные возможности программы

- Rohos Logon Key хранит на USB накопителе (Ключ) до 64 login профайлов для авторизации на любой компьютер в сети (где установлена программа).
- Программа интегрируется **в любую конфигурацию Windows Logon**:
  - Вход на домашний компьютер;
  - Вход на рабочую станцию, являющуюся частью Active Directory (домен Windows) или служб Novell Netware;
  - Доступ к удаленному рабочему столу на терминальном сервере Windows.
  - Компьютер под управлением Windows Vista;
- **Компьютер может быть заблокирован**, или сессия работы пользователя может быть закончена (Log off), как только USB Ключ будет извлечен из USB порта.
- Работа без USB Ключа - позволяет на несколько минут отключить USB ключ без блокировки компьютера. Например, если компьютер имеет единственный доступный USB порт и пользователь хочет вставить какое-нибудь другое устройство, а USB Ключ на время отключить. По истечении этого времени компьютер заблокируется (смотрите главу 4.9, **USB\_REMOVAL**).
- Полная замена парольной авторизации. Данная возможность позволяет входить в учетную запись только по USB ключу.
- USB ключ может быть настроен таким образом, чтобы хранить **пароль** в зашифрованном виде вместо настоящего пароля Windows. Такому USB ключу не требуется защита PIN кода.

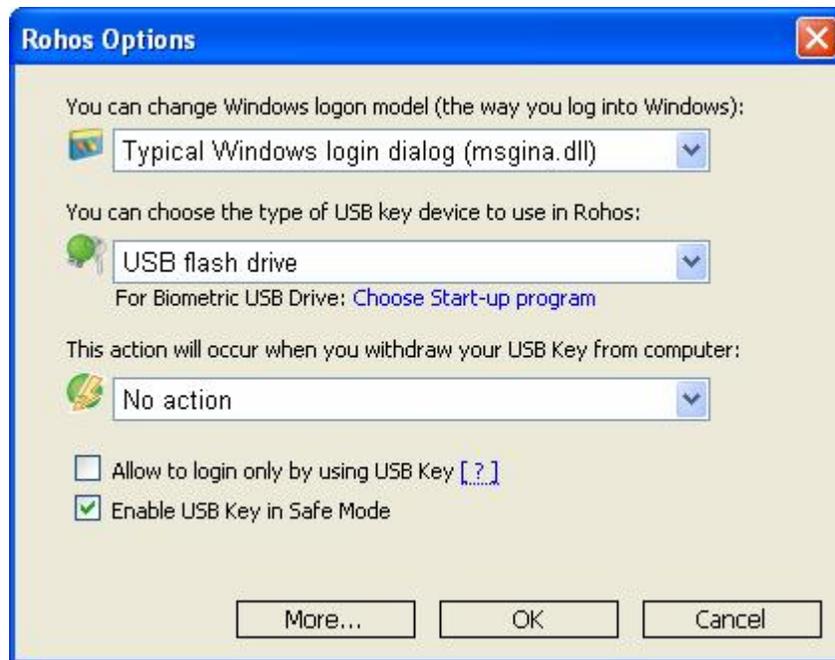
- Утилита управления USB ключом позволяет быстро и легко настроить USB Ключи для сотен пользователей.
- Программа не подменяет msgina.dll, это не приносит никаких дополнительных проблем с совместимостью;
- Поддерживает политику обновления паролей; пароль обновляется на USB Ключе;
- Защита Safe Mode. Вход по USB ключу также работает в режиме загрузки в безопасном режиме (см. Ключ в реестре DisableSafeMode)

### Защита USB Ключа

- USB Ключ невозможно подделать. Программа препятствует изготовлению дубликатов Ключей; каждый logon-профайл привязан к серийному номеру своего USB накопителя;
- Все logon профайлы на USB ключе зашифрованы;
- Защита пароля: По умолчанию на USB Ключе не содержится пароль от Windows в открытом виде;
- Двухфакторная авторизация с помощью PIN кода. USB Ключ может быть защищен PIN кодом;
- USB ключ, который был создан при помощи USB Manager tool (утилиты администрирования USB ключами), не может быть модифицирован на домашнем компьютере (например, пользователь не может очистить или модифицировать Logon профайлы на USB ключе из программы установленной дома).
- Rohos Logon Key может **отключить доступ пользователя к USB накопителю** к портативным устройствам, подключенным к компьютеру через USB порт.

### 3.3 Режимы авторизации (logon model)

Rohos Logon Key может работать в четырех различных режимах авторизации (logon). Это позволяет работать программе в любой версии Windows и в любой конфигурации Windows logon, используя один из нижеперечисленных режимов авторизации



Изображение 1

Режимы авторизации, предоставляемые программой Rohos:

- Окно входа в систему Rohos (gina.dll)
- Окно приветствия Windows XP/Vista + Rohos
- Стандартный диалог входа в Windows (msgina.dll)
- Rohos Credential Provider Windows Vista

Программа Rohos автоматически определяет наилучший режим авторизации во время установки. Выбор метода зависит от версии Windows, текущего способа аутентификации и типа окна входа в систему (например быстрая смена пользователя, welcome screen, стандартное окно входа, пользовательский Gina – такой как Novell Client или проху gina модуль).

Можно вручную выбрать способ авторизации, используя опцию пакета установки MSI или диалоговое окно свойств Rohos.

### Окно приветствия Rohos (gina.dll)

Этот метод основывается на замене модуля MsGINA.dll. При этом модуль аутентификации и идентификации Windows (gina.dll) полностью заменяется модулем аутентификации rohos\_ui.dll.

Минусы этого метода:

- Метод не позволяет производить быстрое переключение пользователей в Windows XP;

Данный метод подходит, если вы хотите:

- В Windows 2000 видеть список пользователей в окне входа в систему;

- Использовать собственный фоновый рисунок в окне входа в систему;
- Использовать в окне входа в систему иконки большего размера, чем стандартные (до 90x90 пикселей);
- Использовать усовершенствованный диалог безопасности системы, вызываемый сочетанием клавиш Ctrl+Alt+Del с функцией сетевой безопасности (обзор совместно используемых ресурсов и соединений);



Окно приветствия Rohos 1

### Окно приветствия Windows XP/Vista + Rohos

Данный метод рекомендуется для домашних ПК под управлением ОС Windows XP/Vista.

- Этот способ не отключает функцию быстрой смены пользователей в Windows XP.

Недостатки:

- Не поддерживается политика ограничения срока действия пароля или его обновления на USB ключе.



Окно приветствия Windows XP / Vista + Rohos 1

### Стандартный диалог входа в Windows (msgina.dll).

Этот режим авторизации является наилучшим в следующих случаях:

- Windows 2000/2003 Сервер (если вы планируете использовать доступ к удаленному рабочему столу посредством ключа USB);
- Рабочая станция Windows 2000/XP, подключенная к Windows Active Directory (Windows Domain) или в сеть Novell.

В этом случае Rohos не заменяет модуль GINA.dll, а встраивается в него, таким образом, оставляя политику безопасности неизменной. В результате, работа сетевой рабочей станции останется такой же стабильной и надежной, как и до установки Rohos. Программа Rohos поддерживает интеграцию с msgina.dll, nwgina.dll и ctxgina.dll.

Настоятельно рекомендуем использовать данный метод в следующих случаях:

- На терминальном сервере, чтобы обеспечить доступ к удаленному рабочему столу посредством USB Ключа;
- Если вы используете политику, ограничивающую срок действия пароля и его обновление;
- На рабочих станциях, подключенных к сети Active Directory/ Novell.



**Стандартный диалог входа в Windows + Rohos.**  
(в данном случае Novell Login)

Примечания для пользователей Novell Client:

- Rohos Logon Key автоматически вводит имя пользователя и пароль в соответствующие поля "Имя пользователя" и "Пароль" диалогового окна Novell Login.
- Обновление/изменение пароля не поддерживается (для Rohos Logon Key версии 2.0)

Для уточнения состояния поддержки Novell Client обращайтесь по адресу [mailbox@rohos.ru](mailto:mailbox@rohos.ru)



Окно приветствия в Windows Vista (Rohos Credential Provider)

### Rohos Credential Provider

Это специальный компонент для Windows Vista, который осуществляет собственный способ получения пользовательских учетных записей для входа в систему. Этот компонент отображается на экране входа в Windows (logon) в виде иконок пользователей.

Rohos Credential Provider отображается на экране входа в Windows в виде иконки USB ключа. При подключении настроенного USB накопителя, программа считывает с него список пользовательских профайлов (учетные записи) для авторизации в систему. При необходимости запрашивается PIN код от USB ключа (двухфакторная авторизация).

Далее учетные записи передаются локальной системе безопасности для аутентификации.

Rohos Credential Provider автоматически регистрируется в системе после установки программы (на компьютерах под управлением Windows Vista).

**Внимание:** после установки программа автоматически выбирает подходящий режим.

Подробнее о новой модели авторизации можно узнать на нашем сайте:

[http://www.rohos.ru/welcome/rohos\\_credential\\_provider.htm](http://www.rohos.ru/welcome/rohos_credential_provider.htm)

### **3.4 Требования к программному и аппаратному обеспечению**

Для нормального запуска Rohos необходим ПК, как минимум, со следующими характеристиками:

- Процессор Intel Pentium (или совместимый) 166Mhz
- 16 МВ оперативной памяти
- 1 или более МВ свободного пространства на жестком диске
- Как минимум 1 порт USB 2.0 или USB 1.1

Поддержка для следующих устройств:

- Обычные USB накопители совместимые с Windows 2000/XP/2003;
- U3 smart накопители;
- SD/MMC memory cards;
- USB токены: Aladdin eToken PRO/R2, Futako HiToken, Aktiv ruToken, uaToken, SafeNet iKey , CryptoIdentity, ePass.
- Биометрические USB накопители: Transcend, Apacer.
- BlueTooth устройства(Pocket PC, Mobile)

 Необходимо иметь USB/U3 smart накопитель совместимый с USB 2.0, USB 1.1, а также совместимый с Windows 2000/XP/2003.

 В наших тестах устройств U3 smart накопитель функционирует медленнее, чем обычный USB flash накопитель, поскольку U3 smart накопитель использует виртуальный CD-ROM.

Программа Rohos Logon Key совместима со следующими операционными системами:

- Windows XP (Home и Professional) с или без SP1 или SP2;
- Windows 2000 Professional с установленным SP4;
- Windows 2000 Server (все версии) с установленным SP4;
- Windows 2003 (все версии);
- Windows Vista (все версии, x64);

Примечание: Для использования панели управления Rohos должен быть установлен Internet Explorer версии 5.5 или выше.

## **4. Руководство по использованию**

В этом разделе приведено описание установки Rohos Logon Key в вашей сети.

Главу «Использование серверной версии Rohos Logon Key» особенно следует прочитать в следующих случаях:

- Массовая установка Rohos Logon Key на рабочие станции сети;
- Настройка десяти и более USB накопителей в качестве ключей доступа;
- Использование функции «Доступ к удаленному рабочему столу посредством USB ключа»;

#### 4.1 Использование Серверной версии

Серверная версия Rohos Logon Key разработана специально для установки на компьютер администратора. Она позволяет выполнять следующие задачи:

- Настраивать USB ключи для входа на любой компьютер в сети с помощью утилиты администрирования USB ключей, которая идет в комплекте;
- Настраивать USB ключи для доступа на Удаленный Рабочий стол;
- Удаленно менять настройки Rohos Logon на рабочей станции в сети.

**Внимание:** Не следует устанавливать эту версию на серверный компьютер. На Терминальный Сервер следует устанавливать обычную версию программы.

#### 4.2 Утилита управления USB ключами

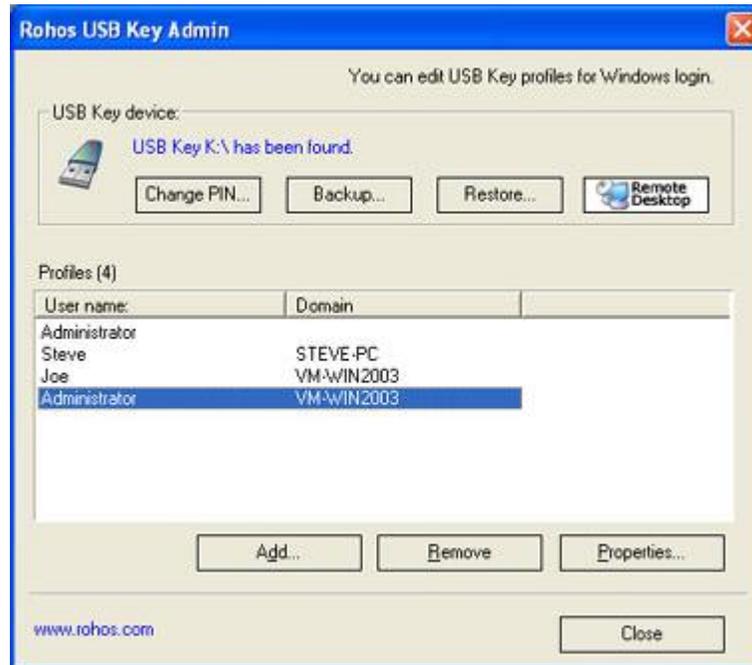
Эта утилита предназначена только для Администраторов. Она может быть использована для настройки десятков и сотен USB Ключей (накопителей) которые предназначены для аутентификации на рабочих станциях.

Утилита позволяет выполнять следующие функции:

- **Создание/Удаление профилей доступа** (login profile) на USB накопителе. Копирование/Вставка профилей с одного USB накопителя на другой;
- Создание резервной копии и восстановление профилей на USB ключе. Утилита автоматически именуется файлы резервных копий и папки, куда сохраняется резервные копии;
- **Установка PIN кода** для защиты USB ключа;
- Создание и использование **универсальных профилей аутентификации на USB ключе**. Эта функция позволяет входить в систему на любом компьютере в сети. В таком профиле вместо имени компьютера оставляется пустое место;
- **Настройка USB ключа для доступа на удаленный рабочий стол** Скопируйте компонент Rohos Удаленный Доступ на USB. Используйте эту функцию, если вы не хотите устанавливать Rohos Logon Key на любой другой компьютер, с которого вы входите на удаленный компьютер;
- Программа автоматически записывает Регистрационный Ключ (из файла со списком Ключей ) на USB ключ таким образом, что, когда пользователь в первый раз входит в свой компьютер, программа на клиентском компьютере автоматически становится зарегистрированной.

Кнопка *Remote Desktop* копирует на USB накопитель компоненту программы Rohos для доступа на удаленный рабочий стол. Используйте эту возможность в тех

случаях, когда вы не хотите устанавливать Rohos Logon Key на компьютер, с которого вы получаете доступ к удаленному рабочему столу.



Главное окно

### 4.3 Настройка login профиля на USB ключе

Вам следует обратить внимание на то, что необходимо корректно настроить профиль пользователя в соответствии с сетевой средой. Сделать это можно с помощью диалогового окна Редактора профилей пользователя:



Редактирование/Просмотр профиля входа в систему

**Поле «User name»**

В этом поле вы вводите имя пользователя. Поддерживается UPN формат (username@domain.com)

**Поле «Password»**

В это поле следует вводить пароль.

Привязка профиля USB ключа к одному компьютеру:

Если пароль содержит символы «\*\*\*» вначале, то Rohos Logon Key будет хранить на USB ключе пароль в зашифрованном виде (вместо самого пароля), когда пароль будет обновлен или истечет срок его действия. Таким образом, профиль будет привязан только к одному компьютеру, и пользователь сможет получить доступ только к нему.

**Поле «Computer name»**

Это самое важное поле в профиле. Rohos Logon Key использует данные из этого поля, чтобы определить, можно ли использовать данный профиль или USB ключ в целом для входа в систему. Если программа не обнаружит ни одного подходящего профиля, то выведет сообщение «USB Ключ не настроен для этого компьютера»

Значение поля:

- При использовании USB Ключа для **локального входа в систему** на отдельно стоящий ПК или на ПК, входящий в сеть.
  - Имя локального компьютера (или «») должно быть указано в поле «**Domain**»;
- При использовании USB Ключа для входа **на удаленный рабочий стол**.
  - В поле «**Domain**» должно быть указано имя компьютера – терминального сервера или компьютера- Windows XP к которому вы хотите иметь доступ (или «»).
- При использовании USB Ключа для входа на несколько компьютеров, подключенных к Windows Active Directory в поле «**Domain**» должно быть указано имя домена Windows. Пример: «\\PD\_SERVER01» (префикс \\ обязательно).

Если поле «**Domain**» оставлено пустым (содержит символы «»), тогда USB ключ с таким профилем может быть использован для получения доступа к любой рабочей станции в сети или к любой удаленной рабочей станции (программа Rohos Logon Key должна быть настроена соответственно).

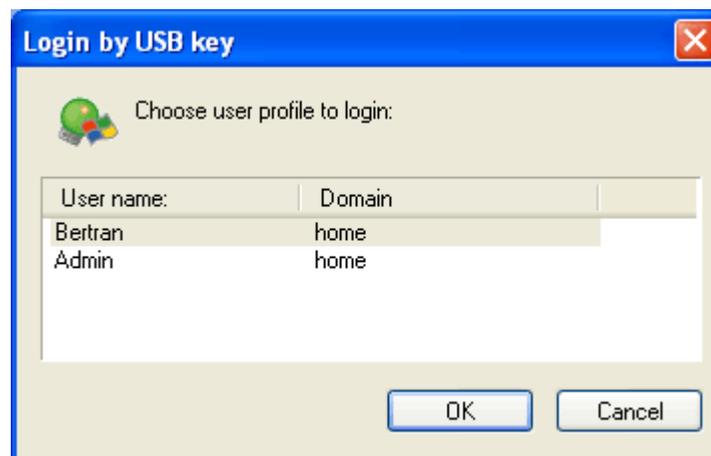
**Несколько Login профайлов на USB ключе.**

На USB ключе можно создавать до 64 Login профилей.

Каждый профиль может быть использован для доступа только к одному определенному компьютеру.

К примеру, Login профиль с именем компьютера “Computer01” может быть использован только для входа в компьютер Computer01. На других компьютерах (где инсталлирован Rohos Logon Key ) этот профиль и USB ключ не будет распознаваться. Эта функция разработана для того, чтобы пользователи имели доступ только к разрешенным компьютерам.

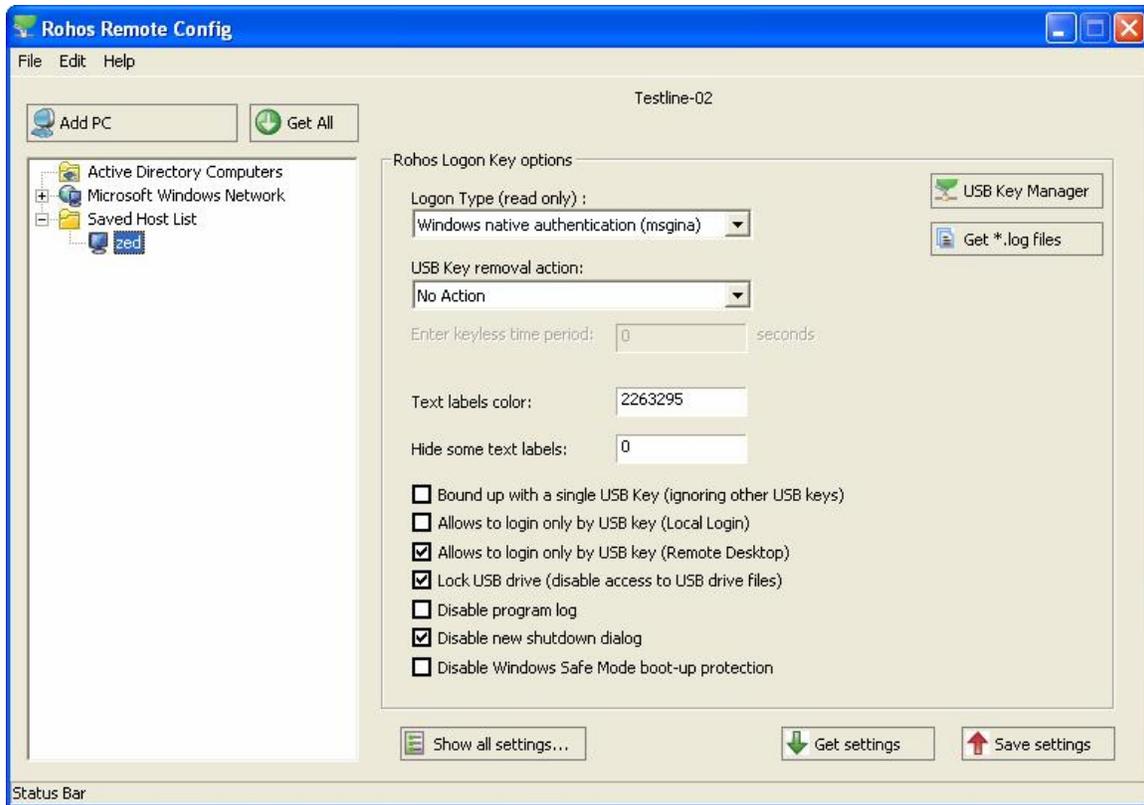
Если на ключе находятся несколько Login профилей, Rohos автоматически распознает, какой именно использовать для входа в компьютер. Если используются 2 и более Login профайла, на экране появляется диалог: «Выберите профайл пользователя».



Если программа не обнаружит ни одного подходящего профиля то выйдет сообщение «USB Ключ не настроен для этого компьютера»

#### 4.4 Утилита – Rohos Remote Config

Позволяет Администратору [Active Directory] изменять настройки “Rohos Logon Key” на удалённом компьютере подключенном к Active Directory.



Главное окно утилиты

- Показывает древо списка компьютеров на которых инсталлирована Rohos Logon Key
- Редактирует параметры настройки Rohos Logon на удаленном компьютере
- Позволяет редактировать профайлы входа на USB ключе, подключенном к удаленному компьютеру

Как использовать:

1. Откройте программу
2. Щелкните мышкой на кнопку "Add PC", добавьте имя компьютера с установленной программой Rohos Logon Key
3. Щелкните мышкой на этот компьютер из списка "Saved Host List" и на "Settings list", и появятся настройки реестра Rohos того удаленного компьютера. (если ничего не появится, щелкните на Update справа)
4. Или щелкните на Microsoft Windows Network и увидите древо списка компьютеров на которых инсталлирована Rohos Logon Key

**Системные Требования:**

- Данная программа совместима со всеми версиями Rohos Logon Key.
- Эта программа должна быть запущена в учетной записи Администратора (Active Directory)

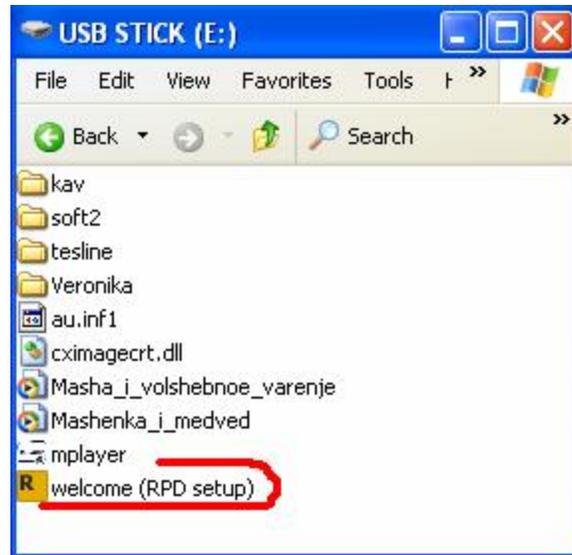
#### 4.5 Настройка ключа USB для доступа к удаленному компьютеру

Вы можете не устанавливать Rohos Logon Key на рабочие станции, с которых пользователи будут входить на удаленный рабочий стол посредством USB ключа. Вместо этого можно специальным образом настроить USB ключ.

Чтобы настроить профиль USB ключа для входа в систему на удаленной рабочей станции, смотрите описание поля «**Имя компьютера**» в главе 4.3 Настройка профиля USB ключа.

Используйте кнопку «Remote Desktop», чтобы настроить USB ключ с параметрами доступа к удаленному рабочему столу с помощью USB накопителя.





Приложение «Welcome»

Во-первых, пользователь должен запустить приложение «Welcome (RDP setup)» сам (на любом компьютере с ОС Windows 2000\XP, с которого пользователь получает доступ к удаленному рабочему столу). Затем приложение Remote Desktop необходимо перезапустить, чтобы применить плагин Rohos login.

- i В результате плагин удаленного входа будет скопирован в папку Windows и зарегистрирован приложением «Windows Remote Desktop».

#### **4.6 Настройка компьютера под управлением Windows Terminal Server**

На терминальный сервер должна быть установлена обычная версия программы, не стоит устанавливать серверную версию в том случае, если предполагается доступ пользователей к удаленному рабочему столу с использованием USB ключа. После инсталляции требуется перезагрузка.

- i После установки Rohos Logon Key и удаленные, и стационарные пользователи могут входить в систему как с помощью USB ключа, так и вводя пароль вручную. Чтобы отключить ручной ввод пароля используйте ключ регистра «**USB\_Only\_login**» (смотрите гл.5).

Обратите внимание, что на сервере должен быть использован режим авторизации «Стандартный диалог входа в Windows (msgina.dll)» (см. главу 3.3). Программа должна автоматически выбрать этот метод в процессе установки.

Для Windows Vista: должен быть использован режим авторизации “Rohos Credential Provider”

После инсталляции можно:

- Установить серверную версию Rohos Logon Key на локальный компьютер Администратора, чтобы настроить USB накопитель для входа в систему (смотрите главу 4.2 Утилиты управления USB ключом).
- Настроить окно приветствия терминального сервера (окно входа в систему) с использованием собственных текстовых сообщений и, при желании, изображения USB ключа.

#### 4.7 Настройка окна входа в систему



Элементы, которые могут быть настроены в окне входа в систему

Экран приветствия (окно входа в систему) можно изменить, добавляя собственные текстовые сообщения или рисунок USB ключа. Сделать это можно одним из следующих способов:

- Используя диалог настроек Rohos (Ссылка на опцию конфигурации);
- Используя опции MSI (во время установки) – смотрите главу 4.9 Параметры пакета MSI;
- Изменяя значения ключей Rohos в регистре (смотрите главу 5.3 Ключи регистра)



Диалоговое окно опции конфигурации

#### 4.8 Установка Rohos Logon Key на рабочие станции (MSI пакет )

Чтобы массово установить Rohos Logon Key на группу рабочих станций следует использовать пакет MSI.

- Он позволяет задать предварительные настройки программы во время инсталляции. Открытые опции пакета MSI (см. гл. 4.9) могут быть изменены с помощью командной строки msixec;
- Пакет устанавливает ограничение доступа к настройкам регистра, заданным программой Rohos Logon Key. Это позволяет предотвратить изменение настроек программы с помощью регистра Windows или программы Rohos;
- Пакет не создает ярлыки программы в меню "Пуск";
- По умолчанию выключает счетчик времени.

#### 4.9 Параметры пакета MSI

Параметры, которые могут быть изменены с помощью командной строки (в msixec.exe):

- **LOGON\_MODE=2**  
(автоматический выбор по умолчанию)  
Заставляет программу использовать тот или иной режим авторизации (входа в систему):  
1 - Rohos окно приветствия (gina.dll)  
2 - Окно приветствия Windows XP/Vista + Rohos  
3 – Стандартный диалог входа в Windows (msgina.dll) + Rohos
- **LOGON\_CAPTION="Welcome to the company"**  
(по умолчанию = "Welcome to windows")  
Текст заголовка окна приветствия (крупный текст над часами)

- **LOGON\_TEXT=""**  
(по умолчанию = "")  
Текст сообщения в окне приветствия (мелкий текст под часами)
- **DISABLE\_LOG=1**  
(по умолчанию =0)  
Отключение всех журналов о состоянии программы (лог-файлов), которые могут быть созданы программой Rohos Logon Key.
- **USB\_KEY\_LOGIN\_ONLY=1**  
(по умолчанию =0)  
Отключение ручного ввода пароля для всех пользователей (принудительный вход в систему с помощью USB ключа). Данная опция заменяет аналогичные настройки пользователей в Rohos программе.  
(Для ручного ввода пароля используйте защищенный режим)
- **USB\_REMOVAL=1**  
(по умолчанию =0)  
1 - Блокирует компьютер, если USB накопитель не подключен.  
(Данная опция заменяет аналогичные настройки пользователей в Rohos Центр.)  
2 – Выключение компьютера  
3 – Завершение сеанса  
4 – Включение спящего режима  
5 – screensaver  
Если это значение больше 50 - это значит, включается режим работы без USB ключа – Это промежуток времени в секундах, в течение которого пользователь может работать без USB ключа (смотрите Режим ввода без ключа)
- **DISABLE\_SHUTDOWNDLG=1**  
(по умолчанию =0)  
Опция позволяет отключать замену стандартного диалогового окна выключения Windows на диалоговое окно Rohos.
- **DISABLE\_CENTER=1**  
(по умолчанию =0)  
Опция запрещает открывать окно программы Rohos.

Примечание: Пользователи не могут менять настройки программы, поскольку ключи Windows реестра программы (HKLM\Software\Rohos) закрыты на запись для пользователей.

- **REG\_NUMBER=""**  
(по умолчанию =0)  
Регистрационный номер Rohos Logon Key (лицензия). Используется для 60ти дневной лицензии. Полноценная лицензия записывается ан USB ключ.

- **LOCK\_USB="1"** ("All", "0")

*Экспериментальная функция:*

Данная функция может запретить пользователям работу с USB устройствами. Это может предотвратить копирование/чтение пользователями файлов с рабочей станции на USB Ключ или внешние носители. А также копирование на рабочую станцию троянских программ или вирусов, и установку нелегального программного обеспечения на компьютеры компании.

"1" – запрещает использование только USB ключа для записи и чтения. Все остальные накопители разрешены.

"All" – блокирует все USB накопители, внешние носители, подключаемые к компьютеру.

"0" – (значение по умолчанию). Отключает блокирование доступа к внешним устройствам USB.

Более подробно: [http://www.rohos.com/welcome-screen/view.php?m\\_id=1389](http://www.rohos.com/welcome-screen/view.php?m_id=1389)

Пример командной строки (скрытая установка):

```
msiexec.exe /qn /I "c:\rohos_welcome.msi" LOGON_MODE=3
```

```
LOGON_CAPTION="Welcome to the company" DISABLE_LOG=1
```

```
USB_KEY_LOGIN_ONLY=1 USB_REMOVAL=1 DISABLE_SHUTDOWNDLG=1
```

#### 4.10 Отключение доступа к USB флэш драйвам и внешним носителям

Экспериментальная функция

Rohos Logon Key позволяет отключать **доступ к USB накопителям** и внешним носителям, подключаемым к компьютеру.

В Rohos Logon Key 2.0 была добавлена экспериментальная функция, которая позволяет **отключать доступ к USB накопителям и внешним носителям**. Эта функция позволяет пользователям отключить доступ к внешним USB носителям. Это может предотвратить копирование/чтение пользователями файлов с рабочей станции на USB накопитель или внешний носитель, а также копирование на рабочую станцию троянских программ или вирусов и установку нелегального программного обеспечения на компьютеры компании.

#### Принципы работы

Как только пользователь подключает USB накопитель к компьютеру, Rohos Logon Key блокирует любые операции чтения/записи на данное устройство. Данная функция делает невозможной работу с USB накопителем на офисном ПК. При этом:

- На любом другом компьютере USB накопитель работает как обычно, поскольку Rohos Logon Key не модифицирует содержание самого флэш драйва;

- USB накопитель по-прежнему может быть использован в качестве ключа доступа к Windows ;
- Вместе с тем, ни одно приложение, включая Rohos, не может получить доступ к USB носителю. Порограмма Rohos или утилита администрирования USB ключа не могут быть использованы для изменения профилей USB ключа или для изменения PIN кода.

Как заблокировать доступ к USB носителю

- Во время инсталляции используйте опцию из пакета MSI: LOCK\_USB="1" ("All", "0")
- Или установите значение реестра Windows для отключения доступа к USB устройству:

Key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Rohos\**

ValueName: **LockUSBKey**.

Значения:

"1" – блокирует только USB Key, который используется для доступа в Windows.

"All" – блокирует все USB накопители, внешние носители, подключаемые к компьютеру.

"0" – (значение по умолчанию). Отключает блокирование доступа к внешним устройствам USB

Если Вас заинтересовала эта функция, обращайтесь по адресу [info@rohos.com](mailto:info@rohos.com)

## 5. Компоненты Rohos Logon Key

### 5.1 Компоненты

Компоненты Rohos Logon Key:

- Welcome.exe – Программа Rohos (Панель управления), инсталлирует / деинсталлирует стандартные компоненты и компоненты окна входа в систему;
- Rohos\_ui.dll – модуль GINA, который заменяет или интегрируется в msgina.dll.
- Rohos\_obj.dll –компонент для удаленного входа в систему, который встраивается в приложение удаленного доступа к рабочему столу;
- Rohos\_cp.dll – Rohos credential provider для Windows Vista.
- Ntserv.exe – сервис окна приветствия (используется при режиме авторизации - Окно входа в систему Windows XP\Vista + Rohos (смотрите главу 3.3 Режимы авторизации.));
- cximagecrt.dll – библиотека обработки изображений.

## 5.2 Logon профайлы на USB накопителе

Rohos Logon Key хранит информацию обо всех паролях в файле \\_rohos\roh.roh. Данный файл зашифрован с помощью алгоритма шифрования AES (ключ шифрования используется по умолчанию или на основе PIN кода).

### Защита USB Ключа

- USB Ключ невозможно подделать. Программа препятствует изготовлению дубликатов Ключей; Каждый logon-профайл привязан к серийному номеру своего USB накопителя;
- USB Ключ может быть защищен PIN кодом , который используется для шифрования профайлов;
- USB ключ, который был создан при помощи USB Manager tool (утилита администрирования USB ключей), не может быть модифицирован на домашнем компьютере (например, пользователь не может очистить или модифицировать Logon профайлы на USB ключе из программы установленной дома).

## 5.3 Настройка в Windows registry

Rohos Logon Key использует реестр Windows, чтобы хранить все настройки программы.

 Пожалуйста, обратите внимание на тот факт, что только серверная версия Rohos Logon Key и версия MSI, устанавливая ограничение прав доступа к значениям регистра Rohos. Это позволяет предотвратить изменение пользователем параметров программы с помощью редактора регистра Windows или окна Программы Rohos.

**Полный доступ предоставляется только группе Администраторы и SYSTEM.**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Rohos

Название ключа	Описание и значение (DWORD или строка)
<b>CheckUSBserial</b>	1- включает привязку программы к последнему настроенному USB ключу. По умолчанию 1, после настройки первого USB ключа.
<b>DisableLog</b>	1 – отключает ведение лог файла 0 – (по умолчанию) включает ведение лог файла
<b>DisableRohosShutdown</b>	1 – отключает диалог выключения Rohos 0 – (по умолчанию) включает диалог
<b>LockUSBKey</b>	1 – отключает использование USB ключа

	0 – (по умолчанию) включает “all” – отключает все USB накопители(USB кардридеры для чтения нескольких видов карт не поддерживаются).
<b>LogonType</b>	Не изменяйте. Смотрите главу 3.3 Режимы авторизации., а также главу 4.8 Параметры MSI.
<b>RohosPath</b>	Текущий путь к папке программы. Не изменяйте это значение.
<b>USB_Only_login</b>	1 – позволяет входить в систему только с помощью USB ключа. 0 – (по умолчанию) включает ручной ввод пароля
<b>USB_Key_remove_behaviour</b>	1 – блокирует рабочий стол Windows после отключения USB ключа от USB порта. 0 – (по умолчанию) без изменений >50 – промежуток времени в секундах, в течение которого пользователь может работать без USB ключа (смотрите Режим работы без USB ключа)
<b>USBLoginPicture</b>	Рисунок USB ключа в окне входа в систему. (по умолчанию) “зеленый USB ключ” Полный путь к файлу типа gif/jpg/bmp/png. Максимальный размер изображения 150*150 пикселей.
<b>DisableSafeMode</b>	1 – Отключает работу программы в Safe Mode (загрузка Windows в режиме защиты от сбоев)
<b>HeaderTextColor</b>	(RGB) цвет надписей Rohos в окне приветствия.
<b>NoTextLabels</b>	Отключает определенные надписи Rohos (часы, дату и др.) в окне приветствия.
<b>DisableUSBatRDP</b>	1 – Разрешает использовать вход на Удаленный Рабочий Стол с помощью пароля. (при наличии USB_Only_login=1)
<b>DisableTimeLimits</b>	1 – Отключает счетчик рабочего времени, который вычисляет объем времени, проведенного за ПК в течение дня/недели. Так же

отключает изображение счетчика в окне входа в систему или выключения ПК  
0 – (по умолчанию) включает счетчик.

Следующие значения используются только при режим авторизации [“Окно приветствия Rohos \(gina.dll\)”](#) (Смотрите главу 3.3)

<b>LoginPicture</b>	Фоновый рисунок для окна входа в систему
<b>CtrlAltDel</b>	<p>Определяет действие, происходящее при нажатии на сочетание клавиш Ctrl+Alt+Del:</p> <p>1 – Открывает диалог безопасности, типичный для стиля WinNT. 2 – Блокирует рабочую станцию 0 – (по умолчанию) открывает Диспетчер Задач в WindowsXP, или диалог Ctrl+Alt+Del в Win2000</p>
<b>DisableAdminUnlock</b>	<p>1 – Отключает функцию разблокирования администратором пользовательских сессий. 0 – (по умолчанию)</p>
<b>DisableTypicalLogin</b>	<p>1 – Отключает типовое диалоговое окно для ввода имени пользователя, пароля и домена. 0 – (по умолчанию)</p>
<b>WelcomeScreenHelp</b>	<p>Строка помощи, которая отображается выше и справа от окна входа в систему. “” – отключает данную подсказку.</p>

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon :

**LegalNoticeCaption** - Текст заголовка окна входа в систему, показанный крупным шрифтом (значение по умолчанию “Welcome to Windows”);

**LegalNoticeText2** – Текст примечания в окне входа в систему, который показан мелким шрифтом (значение по умолчанию «»).

## 6. Примеры

В этом разделе вы найдете описание примеров использования программы в рамках компании.

**Продление ознакомительного периода до 60 дней.**

Пробный период может быть продлен до 60 дней. Вы можете отправить запрос на получение ключа, продлевающего ознакомительный период. Это позволит тщательно протестировать Rohos Logon Key в вашей компании. Для продления ознакомительного периода обращайтесь к нам по адресу: **mailbox@rohos.ru**.

**Пробное использование программы в рамках компании**

Прочитайте данную главу, если вы планируете использовать программу **в рамках компании**.

Программа Rohos предоставляет новые возможности, которые меняют привычный порядок работы, как для пользователей, так и администраторов. Поэтому мы рекомендуем **использовать для испытания программы фокус группу**.

- Выберите небольшое подразделение или группу пользователей, в которой можно произвести пробную инсталляцию Rohos Logon Key с выдачей USB ключей для доступа к компьютеру;
- Для тестирования понадобится некоторое количество **USB накопителей**. (см.3.4).

Рекомендации по установке:

- Не отключайте возможность ручного ввода пароля с самого начала тестирования.

Разбейте процесс испытания программы на 2 этапа:

1. Пробная инсталляция программы и испытание функции доступа к системе с помощью USB ключа среди членов фокус группы в присутствии технического специалиста (Администратора сети).
2. Испытания в «боевых» условиях без присутствия Администратора среди небольшого отдела. (см. пример1)

После таких испытаний программу Rohos можно устанавливать на остальные компьютеры сети.

**Пример 1. Сеть, основанная на Windows Active Directory.  
Локальный вход в систему.**

Вначале установите серверную версию Rohos Logon Key (смотрите главу 4.1 Использование серверной версии) на ваш компьютер (компьютер администратора).

Пример массовой инсталляции программы в сети:

1. Настройте для каждого пользователя USB Ключ с паролем по умолчанию (используйте для этого утилиту управления USB ключами, см. гл. 4.2)

2. Установите на заданный компьютер программу, используя MSI пакет с возможностью входа в систему только с помощью USB Ключа и с другими параметрами (см. 4.2.1).
3. Установите пароль по умолчанию с опцией смены пароля при следующем входе в систему (пароль по умолчанию, который используется для настройки USB Ключа).
4. Раздайте USB Ключи сотрудникам.
5. Пользователи должны войти в систему с помощью USB Ключа и тут же изменить свой пароль (пароль на USB Ключе будет обновлен).
6. После этого пользователь сможет входить в систему только с помощью USB Ключа.

Далее:

- Сотрудники службы поддержки персонала могут использовать удаленный доступ к компьютерам сотрудника (посредством пароля либо USB ключа) для оказания помощи пользователям. В этом случае необходимо для каждого пользователя с компонентом удаленного входа настроить USB Ключ (см. гл. 4.3) или установить Rohos Logon Key.

## 7. Разрешение проблем

Вы столкнулись с ошибкой, непонятным поведением программы или какой-то другой проблемой?

Мы с удовольствием поможем решить проблемную ситуацию, но для этого нам может понадобиться лог файл программы, который находится в каталоге **C:\program files\rohos\ welcome.log , rohos\_ui.log**

Сообщения об ошибках:

**Данный USB Ключ не был настроен на этом Компьютере, поэтому он будет игнорирован.**

Это ошибка может появиться в одном из случаев :

1. На USB ключе нет профайлов для входа на данный компьютер.

Поле Domain в логин профайле должно содержать: имя компьютера на который производится вход, пустая строка либо

\\имя домена - только в случае использования режима авторизации "Rohos welcome screen gina.dll ".

Решение: Установить Утилиту администрирования USB ключей и настроить профайл нужным образом

2. На данном компьютере установлен Rohos Logon Key и его владелец уже настроил единственный USB ключ. Поэтому программа отвергает другие ключи (даже тот который настроен в утилите администрирования USB ключей)

За эту опцию защиты отвечает значение в реестре Windows:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Rohos - CheckUSBserial=1

Решение: Необходимо удалить значение CheckUSBserial или настроить USB ключ на данном компьютере.

По умолчанию после установки программы CheckUSBserial=0, и включается (1) только после локальной настройки USB ключа.

3. USB ключ был создан путем копирования файлов программы Rohos на другой USB накопитель.

Решение: Настроить USB ключ заново.

### **Демонстрационный Ключ. Требуется регистрация Ключа.**

Это ошибка означает, что USB ключ настроен в утилите администрирования USB ключей без регистрационных ключей.

Решение: Добавить список регистрационных ключей.

### **Ваша лицензия не поддерживает данную функцию в программе Rohos. Пожалуйста обновите вашу лицензию до бизнес версии**

Это сообщение означает, что на ключе имеется два и более login профайлов и установлена обычная лицензия.

Решение: [Приобрести](#) и установить бизнес лицензию либо держать на USB Ключе только один профайл. (Очистить и перенастроить USB ключ)

Преимущества бизнес лицензии:

- Для входа на несколько компьютеров/учетных записей пользователей возможно использовать один единственный USB ключ.
- При помощи USB накопителя можно войти в **систему Remote Desktop (Удаленный Рабочий Стол)**
- Поддержка Novel Client для Windows
- Поддержка для Windows Domain, Active Directory

## 8. Контакты и обновления

Веб сайт: [www.rohos.ru](http://www.rohos.ru)

Франция: [www.rohos.fr](http://www.rohos.fr)

США: [www.rohos.com](http://www.rohos.com)

Германия: [www.rohos.net](http://www.rohos.net)

Локализованная Rohos Logon Key: <http://www.rohos.com/welcome-screen/translated.htm>

Обновления и примечания к версиям: <http://www.rohos.ru/news/>

### Адрес:

Tesline-Service, SRL

ул. Каля Ешилор, 10

г. Кишинэу, MD-2069

Республика Молдова.

Тел.: (+373 22) 740-242

Часы работы: 9:00-17:00 (GMT: +3:00).

Мы не оказываем поддержку программы по телефону.