



Rohos[®] Logon Key
Rohos[®] Logon Key Server version

Administrator Guide.
Installation and USB Key management
Updated: October 2010.



Contents

| | |
|--|----|
| 1. About this guide..... | 3 |
| 2. Legal Information | 3 |
| 3. Introduction to Rohos Logon Key | 4 |
| 3.1 Purpose..... | 4 |
| 3.2 Main Features..... | 4 |
| 3.3 Logon Model..... | 6 |
| 3.4 Software and Hardware Requirements | 10 |
| 4. Usage Guide..... | 11 |
| 4.1 Rohos Logon Key server version..... | 11 |
| 4.2 USB Key Management utility..... | 11 |
| 4.3 Setting up USB Key login profile..... | 13 |
| 4.4 Rohos Remote Config Utility | 14 |
| 4.6 Setup Windows Terminal Server computer..... | 17 |
| 4.7 Customize login window | 18 |
| 4.8 Installing Rohos Logon Key into workstations | 19 |
| 4.9 MSI package options..... | 19 |
| 4.10 Disabling USB flash drive for user access..... | 20 |
| 5. Rohos Logon Key Internals | 21 |
| 5.1 Components | 21 |
| 5.2 USB Key profiles..... | 22 |
| 5.3 Registry keys..... | 22 |
| 6. Examples..... | 24 |
| How to try Rohos Logon Key in the company? | 24 |
| Example 1. Windows Active Directory based on the network. Local login..... | 25 |
| 7. Troubleshooting | 25 |
| 7.1 Error strings | 25 |
| 8. Contacts and updates | 27 |

1. About this guide

This document is designed for IT Administrators and contains information about installing and operating Rohos® Logon Key in the computer network.

What you can read first: How to try Rohos Logon Key in the company? (see Chapter 6) and other examples of deployment.

NOTE: This document is currently in progress.

Have a question? Contact: info@rohos.com

The latest version of this guide: <http://www.rohos.com/RohosWelcomeUserGuide.pdf>

2. Legal Information

Copyright Information

Copyright 2006-2010 Tesline- Service SRL

All rights reserved

This manual reflects Version 2.7 of the Rohos Logon Key application, USB Key Management utility, MSI installation package.

Disclaimer

The information contained herein is believed to be accurate as of the date of publication; however, Tesline-Service SRL will not be liable for any damages, including indirect or consequential, from the use of the software or reliance on the accuracy of this information. The information contained herein is subject to change without notice.

Copyright

Distribution of the software or documentation, whole or partly, to any other system or to any other part may be considered as a misappropriation of information about trade secrets and confidential processes which are the property of Tesline-Service SRL and/or other parties.

License Conditions

For the specific terms of your license, consult the readme.txt, license.txt, or other license document that accompanies your software or license type, either as a text file or as part of the software Packaging.

For additional license conditions and copies of this software and/or documentation, please contact your supplier.

Rights of Brand Marks

Rohos® is the trademark of Tesline-Service SRL.

All the registered and unregistered trademarks contained herein are the sole property of their respective owners.

Microsoft, Windows and Windows 2000, Windows XP, Windows Vista are registered trademarks of Microsoft Corporation.

3. Introduction to Rohos Logon Key

3.1 Purpose

The program lets users access to Windows computer in an easy, fast and secure way using USB Key (USB flash drive). Rohos Logon Key is considered to be the most convenient and user-friendly password replacement solution on the market.

3.2 Main Features

- Rohos Logon Key set ups USB flash drive with your user name and password so that they will be automatically entered when you enter Windows.
- Program **supports the following Windows logon configurations:**
 - Login into WindowsXP/Vista home computer;
 - Login into a workstation joined to Active Directory (Windows Domain), Novell Netware services;
 - Access to remote desktop on the Windows terminal server.
- **Computer can be locked** or user session can be finished (log off) as soon USB flash drive has been disconnected from USB port;
- Keyless mode allows disconnecting USB Key for some minutes without locking computer. For example if user needs to connect some device to USB port. As time passes the computer will be blocked (see **USB_REMOVAL, Chapter 4.9**);
- USB flash drive can be used for computer security. It allows you to enter your user account only using USB Key;
- In order to protect access to USB flash drive, you may use PIN code. PIN code can be entered by means of virtual keyboard which is protected from password tracking and from PIN code steal by output spy;
- USB Key Management utility allows you to setup USB flash drives for hundreds of users quickly and easily;
- Rohos application does not replace msgina.dll thus not creating any problems with compatibility;
- Rohos supports password renewal policy; the password is renewed on the USB Key;

- Safe Mode. The access with the USB key works also by the loading Windows in Safe Mode.

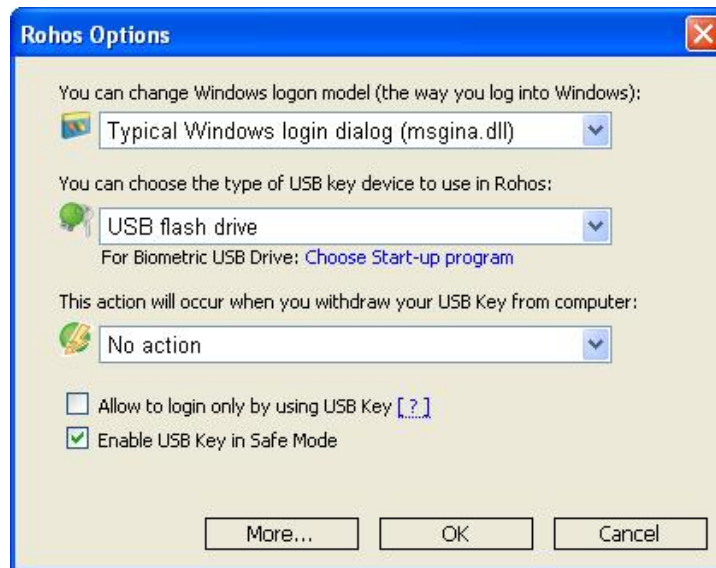
USB Key security features:

- **USB Key cannot be duplicated.** Key logon profile is bound up with a USB flash drive serial number.
- **USB Key originality.** By default USB Key is bound up with a computer where it was created for login. The other USB Key will be ignored by the program (even with a valid logon profile). Computer owner can forbid using any other USB Key except the 1st one for login.
- **Protected password.** By default USB Key does not contain your Windows password in plain form, but only Encryption Key pair that is used to reconstruct password for login operation.
- **Two-factor authentication** by using PIN code for USB Key. This is a small password with only 3 attempts to enter, it is required when performing login by using USB Key;
- USB Key that was created by USB Key Manager Tool cannot be modified on home computer (for example, Logon profiles cannot be cleared or modified using Rohos Logon Key program)
- Rohos Logon Key can **disable user access to USB flash drives** and removable media connected to computer through USB port;

3.3 Logon Model

Rohos Logon Key supports various Windows logon configurations. It allows using it both on the personal computer/laptop and on the corporate workstation joined to Windows/Novell network.

The program integrates into any Windows logon configuration by using one of the Logon model listed below:



Picture 1
User can manually choose Logon model

Logon model supported by Rohos:

- Rohos welcome screen (gina.dll)
- Windows XP/Vista welcome screen + Rohos
- Windows native authentication (msgina.dll)
- Rohos Credential Provider Windows Vista

The program automatically determines the best Logon model when you are installing it. This choice depends on the Windows version and login screen settings (for example fast user switching used, typical login dialog box used, custom Gina installed, etc.).

However, user can always choose specified Logon model manually by using: MSI installation package option or Rohos options dialog box.

Rohos welcome screen (gina.dll)

This method is based on the MsGINA.dll replacement. It totally replaces the Windows authentication and identification module (gina.dll) by a customized version of the authentication module (rohos_ui.dll).

Drawbacks:

- It disables fast user switching in Windows XP.

Choose this method only if you want to:

- See the users list in the welcome screen in Windows 2000;
- Use your own background image in the welcome screen;
- Use bigger (up to 90*90 pics) user icons on the login screen;
- Use enhanced system security dialog box called by Ctrl+Alt+Del with network security function (shared resource/connections);



Rohos welcome screen 1

Windows XP/Vista welcome screen and Rohos

This method is recommended for Windows XP/Vista home computers.

-
- It does not disable fast user switching feature
-

Drawbacks:

- Password expiration/renewal function with USB Key update is not supported;



Windows XP / Vista welcome screen + Rohos 1

Windows native authentication (msgina.dll)

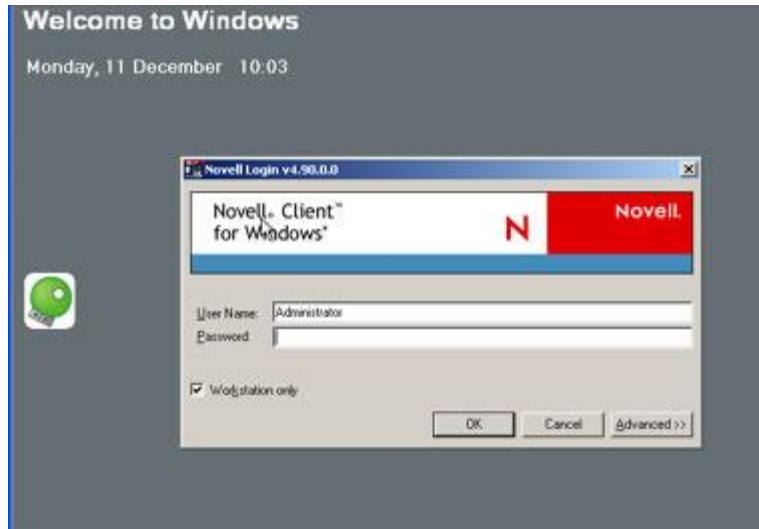
This is the best Logon model for:

- Windows 2000/2003 Server (if you plan to use remote desktop access by USB Key)
- Windows 2000/XP workstations joined to Windows Active Directory (Windows Domain) or Novell network.

Rohos Logon Key does not replace the module GINA.dll. The security policies remain unaltered. As a result the computer run will be just as stable and secure as before Rohos has been installed. Rohos supports integration with msgina.dll, nwgina.dll, ctxgina.dll.

It is highly recommended to use this method in the following cases:

- On a Terminal Server computer to access to Remote Desktop via USB flash drive;
- If you use password expiration/renewal security policies;
- On workstations joined to Active Directory/ Novell networks.



Windows native authentication + Rohos
(in this case Novell Login)

Novell Client notice:

- Rohos Logon Key enters user name and password into 'User Name' and 'Password' appropriate fields of Novell Login dialog box automatically;
- Password renewal/change is not supported (for Rohos Logon Key version 2.0)



Welcome screen in Windows Vista/Seven via Rohos Credential Provider

Rohos Credential Provider

It is a special component for Windows Vista, which implements a new user authentication method. Users see this component in the form of a user icon on the Windows logon screen.

Rohos Credential Provider appears on the Windows logon screen in the form of an icon of a USB key. Connect a configured USB drive, and the component will read from it a list of logon profiles (user credentials) for authorization in the system. If necessary, it will also request a PIN code from the USB drive (two-factor authentication).

These profiles are then passed to the local security system for authentication.

Rohos Credential Provider will be automatically registered on the system following installation (on computers running Windows Vista).

Note: On installation, the program automatically selects an appropriate Logon Model.

Learn more about on our website:

http://www.rohos.com/welcome-screen/rohos_credential_provider.htm


3.4 Software and Hardware Requirements

In order to run Rohos Logon Key properly, PC with the following minimum requirements is needed:

- Intel Pentium (or compatible) 166Mhz processor
- 16 MB RAM
- 1 or more MB free space on Hard Disk
- At least 1 USB 2.0 or USB 1.1 USB port

The following devices support:

- Regular USB flash drives compatible with Windows 2000/XP/2003;
- U3 smart flash drives;
- SD/MMC memory cards;
- USB tokens: Aladdin eToken PRO, Futako HiToken, Aktiv ruToken, uaToken, SafeNet iKey , CryptoIdentity, ePass.
- Fingerprint USB flash drives: Transcend, Apacer, LG.
- BlueTooth enabled devices (Pocket PC, Mobile)

 In our tests U3 smart drives work slower than regular USB flash drives because U3 smart drives handles additional virtual CD-ROM device.

Rohos Logon Key software supports the following operating systems:

- Windows XP (Home and Professional) with or without SP1 or SP2;
- Windows 2000 Professional with SP4 installed;
- Windows 2000 Server (all versions) with SP4 installed;
- Windows 2003 (all versions);

- Windows Vista (all versions, x64);

Note: Internet Explorer 5.5 or higher is needed in order to use Rohos Center control panel.

4. Usage Guide

Here you will find out how to install Rohos Logon Key in a particular network environment

You should read Chapter 4.1 “Use of Rohos Logon Key Server Version” if you are going to:

- Install Rohos Logon Key over a network workstations;
- Setup a dozen and more of USB flash drives as access keys;
- Use “remote desktop access via USB key” feature;

4.1 *Rohos Logon Key server version*

Rohos Logon Key Server version is specially designed to be installed into Administrator’s computer. It allows carrying out following tasks:

- Centralized USB Keys management.
Setup USB key for the access to any computer in the network in the USB Key Management utility;
- To configure USB Keys for the access to the remote desktop;
- To change Rohos Logon settings remotely on the workstation joined to Active Directory;

Note: It’s not necessary to install this version on the server computer. On the Terminal Server should be installed the regular version of Rohos Logon Key.

4.2 *USB Key Management utility*

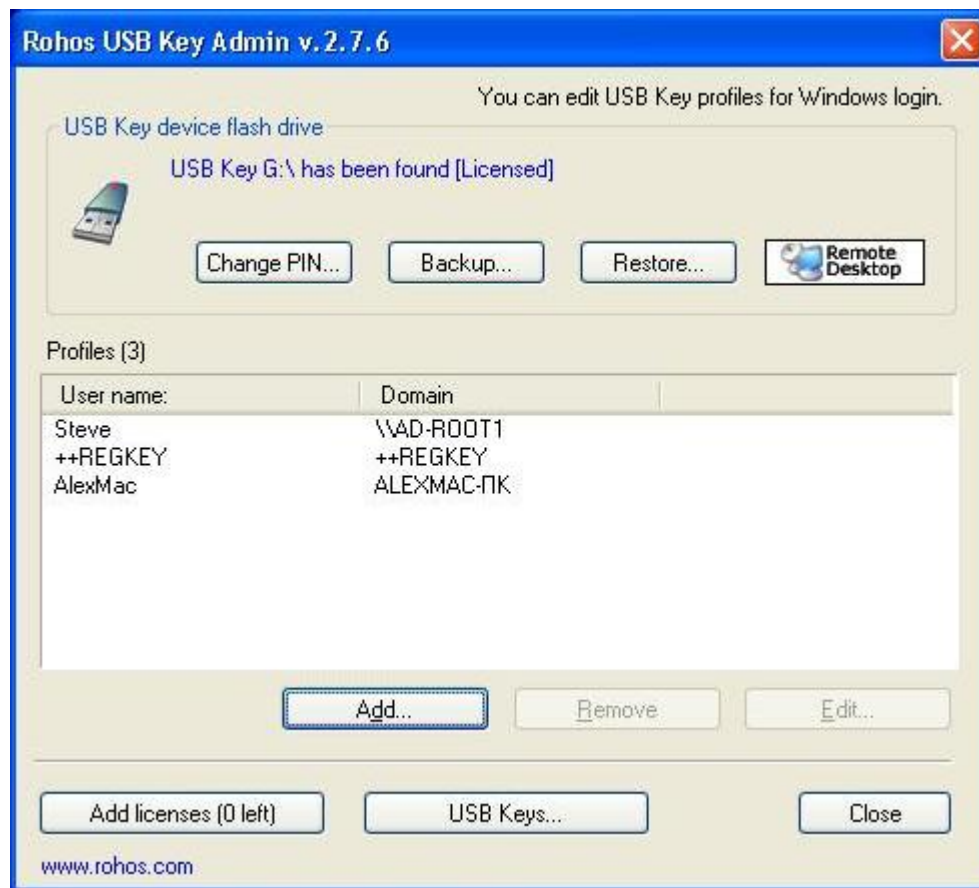
This utility is intended for Administrators only. It can be used to set up several tens and hundreds of USB flash drives for authentication purpose.

The USB Key Management Utility has the following functions:

- **Create/Delete login profiles** on the USB flash drive. Copy/Paste profiles from one USB drive into another.

- **Create a backup and restore USB Key logon profiles.** The Utility automatically names backup files and uses backup's folder.
- **Set up a PIN code** for USB Key protection;
- Create and use **roaming logon profiles** on a USB Key. It allows you to log in into any computer on the network. Roaming profile has "" blank computer name;
- **Setup USB Key for Remote Desktop Login (RDP)**
Copy Rohos Remote Login component into USB stick. Use this feature if you don't want to install Rohos Logon Key into any computer you log in from.
- License management: The program automatically stores License Key on the USB Key (from the Key list file), so that when a user log in into his/her computer for the first time, the program on the client's computer becomes a registered one.

The button Remote Desktop copies into USB flash drive Rohos Login component to access to Remote Desktop. Use this feature if you don't want to install Rohos Logon Key into computer you have access from to Remote Desktop.



USB Key manager main window

“**Add Licenses**” button allows to set a licenses key list. These licenses will be used to make pre-licensed USB tokens. Thus you don't need to enter license key into each PC where Rohos Logon Key is installed.

Click “**USB Keys**” button to review all registered USB tokens.

4.3 Setting up USB Key login profile

Please, note that you should correctly set up user profile on USB Key according to your network environment. You can do it with User profile Editor dialog:

The screenshot shows a dialog box titled "Setup users". Inside, there is a message: "Here you can create or edit login profile on the USB Key." Below this are four input fields: "User name:" containing "Steve", "Password:" containing five dots, "Confirmation:" containing five dots, and "Domain:" containing "\\AD-ROOT1". There is also a text area for "Computer where to login, or empty string for roaming profile." and a note at the bottom: "Please read Rohos Usage Guide for details." At the bottom right are "OK" and "Cancel" buttons.

Edit/View logon profile.

“User name” field

Here you should enter user name. UPN format is supported (username@domain.com)

“Password” field

Here you should enter user password.

Binding USB key profile to a single computer:

If user password has a “****” prefix then Rohos Logon Key will put here a password hash (instead of a real password) when password expiration/renewal occurs. This will bind this profile only to one computer. User will be able to log in only into this computer.

“Computer name” field

This is the most important field in the login profile. Rohos Logon Key uses this field in order to determine whether the profile and USB Key in a whole can be used in a particular computer for login or not.

- If you plan to use USB Key **for Local Login** into standalone or network joined workstation.
 - The name of local computer (or “”) should be shown in the Domain field;
- If you plan to use USB Key **for Remote Desktop login** into Windows Terminal Server or Windows XP computer.

- Domain field must have the name of Windows Terminal Server computer or Windows XP computer where you are going to log in (or "").
- Domain field should have the name of Windows Domain (AD) with "\\\" prefix. For example: "\\PD_SERVER01"

If **domain is "" blank** then this profile and USB key in a whole can be used to access to any workstation in the network or remote desktop. (Rohos Logon Key should be installed accordingly).

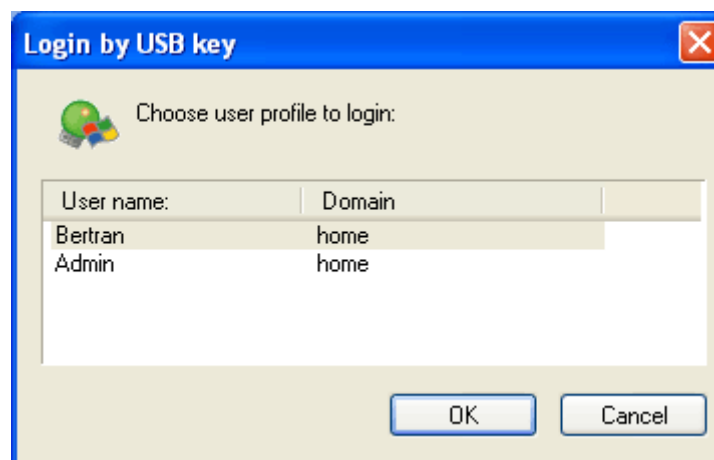
Multiple login profiles on the USB Key.

It is possible to have up to 64 login profiles on the USB Key.

Each profile is purposed to log in into a particular computer. For example login profile with computer name "Computer01" can be used to log in into Computer01 only. This profile and USB Key in general will be ignored by Rohos on other computers (with Rohos Logon installed).

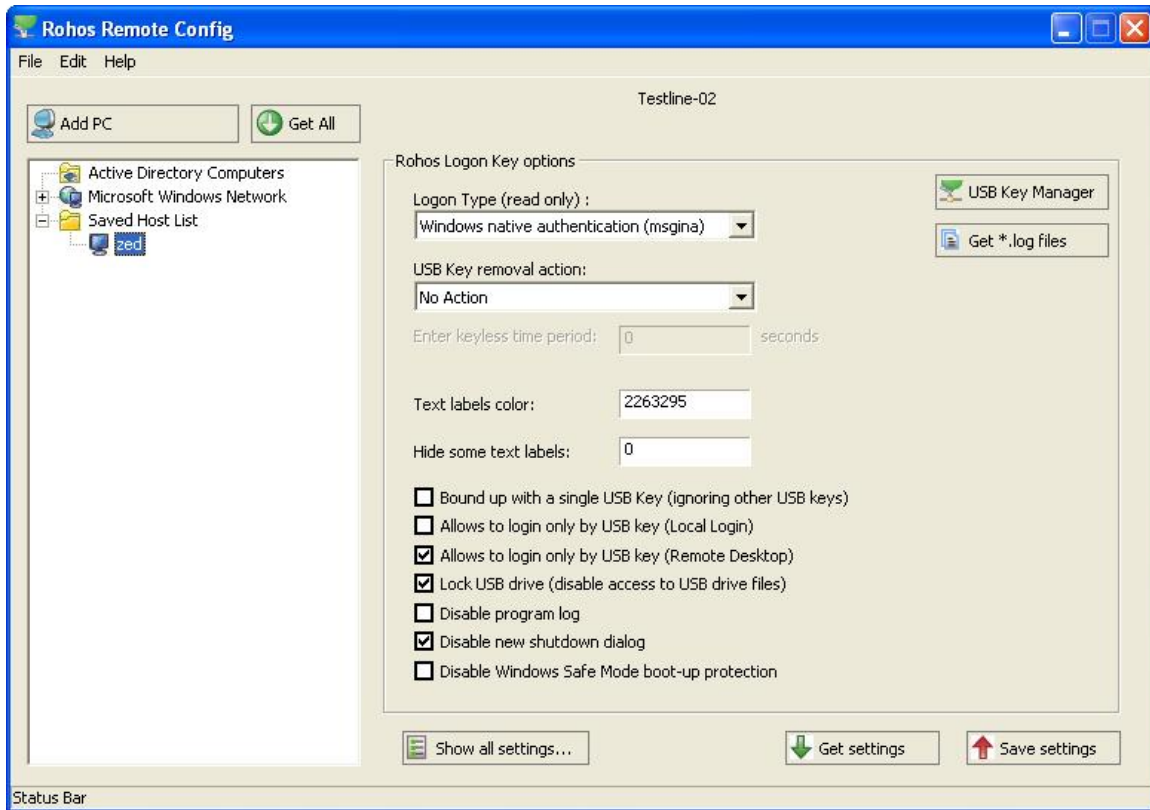
This feature can be used to allow users to log in into allowed computers.

If there are several login profiles on the Key, Rohos automatically determine which one to use for login. If 2 and more can be used then Rohos displays "Choose user profile" dialog:



4.4 Rohos Remote Config Utility

This Utility allows the administrator (Active Directory) to change settings of Rohos Logon Key on the remote workstation.



The main window of the Rohos Remote Config Utility

- Shows the list of computers where Rohos Logon Key is installed;
- Edit Rohos Logon settings on a remote computer;
- Allows to edit logon profiles on a USB key connected to remote computer;

How to use it:

1. Open the program.
2. Click "Add PC" button, enter computer name on where Rohos Logon Key is installed. OK.
3. Click on that computer on the "Saved Host List" and on the "Settings list" you will see Rohos Registry setting on that remote computer. (if there are nothing, click Update on the right)
4. Or click on Microsoft Windows Network and see the list of computers where Rohos Logon Key is installed.

System requirements:

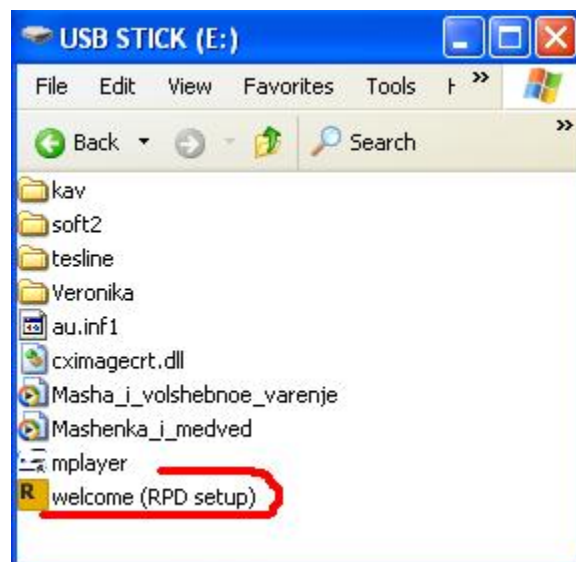
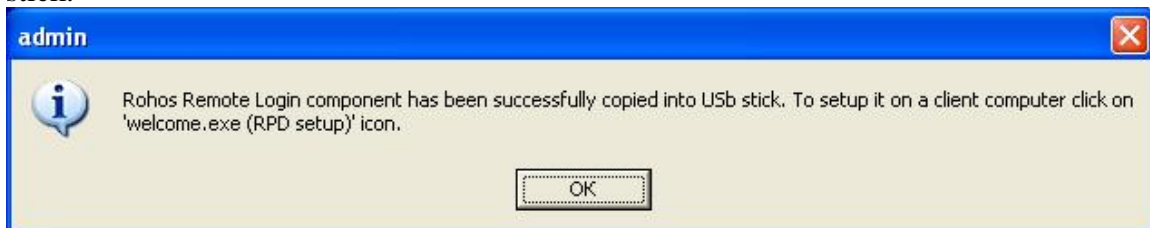
- Rohos Remote Config must be run under Active Directory Administrator user account.
- Rohos Logon Key should be installed on the remote computer
- Remote computer should be connected to Windows Active Directory services.
- Remote Registry service should be enabled on the computer.

4.5 Setup USB Key for Remote Desktop Login

If you don't want to install Rohos Logon Key into any workstation from where user makes remote connection, you can use this feature.

To configure USB Key profile for remote desktop login see **Domain** field description in Setting up USB key profile section (see Chapter 4.3).

Use "Remote Desktop" button to setup USB key with remote login component into USB stick.



'Welcome' application

Firstly, user should start ‘welcome (RDP setup)’ application (on any Windows 2000\XP computer from where user has an access to remote desktop);
Then Remote Desktop application should be restarted in order to apply Rohos login plug-in.

- ❗ It will copy remote login plug-in into Windows folder and register it with Windows remote desktop application.

Lear more about Remote Desktop login with USB Key:

4.6 Setup Windows Terminal Server computer

Into Windows terminal server computer should be installed Rohos Logon Key regular version (it’s unnecessary to install the server version) if you want users to access to remote desktop via USB key. This installation requires computer restart.

- ❗ After Rohos Logon Key has been installed, remote and regular users can
- ❗ use manual password entry and USB Key login as well. To disable manual password entry use “**USB Only login**” registry key.

Please note that “Windows native authentication method” (see Chapter 3.3) should be used on the server computer. Program should choose it automatically while installing it.

For Windows Vista: logon model “Rohos Credential Provider” must be used.

After installation you can:

- Install Rohos Logon Key server version into your local (Admin’s) workstation to set up USB flash drive for login (using USB Key Management utility, see Chapter 4.2)
- Set up Terminal Server welcome screen (login screen) with a custom text messages and USB key picture if you wish;

4.7 Customize login window



Elements that can be customized on the login screen

Welcome screen (login screen) can be customized with a custom text messages and USB key picture

. You can do it in the following ways:

- Using Rohos Center (Configure options link)
- MSI options (during installations) – see Chapter 4.9.
- Modifying Rohos registry values (see Chapter 5.3).



Configure options dialog box.

4.8 Installing Rohos Logon Key into workstations

To install Rohos Logon Key in network workstations you can use MSI package.

- It is specially designed, so you can set up program settings during installation. MSI package public options (see Chapter 4.9) can be changed using msiexec command line;
- It sets up restricted access rights to registry settings installed by Rohos Logon Key. This prevents users from change of program settings via Windows registry or Rohos Center.
- It does not install program shortcuts into Start menu;
- Working time counter is disabled by default;

4.9 MSI package options

Options that can be changed via command line (in msiexec.exe):

- **LOGON_MODE=2**
(*automatic choice by default*)
Enforces program to use a particular Logon model (login):
1 - Rohos Logon Key (gina.dll)
2 - Windows XP/Vista welcome screen + Rohos
3 - Windows native authentication (MsGINA.dll) + Rohos
- **LOGON_CAPTION="Welcome to the company"**
(*by default = "Welcome to windows"*)
Welcome screen caption text (big one)
- **LOGON_TEXT=" "**
(*by default = ""*)
Welcome screen text notice (small text under the clock)
- **DISABLE_LOG=1**
(*by default =0*)
Turns off all LOG files that can be produced by Rohos Logon Key program.
- **USB_KEY_LOGIN_ONLY=1**
(*by default =0*)
Disables ALL users to log in via password entry manually. (Enforces to log in only via USB key). This option replaces the same user level settings from Rohos Center.
(use Safe mode if you want to log in manually)
- **USB_REMOVAL=1**
(*by default =0*)
1- Locks computer upon USB stick withdrawal.
2- Log off

- 3 – Shutdown computer
- 4 – Hibernate
- 5 – Screensaver

If this value is >50, it means keyless mode - time interval in seconds during which user can work without USB Key (see keyless mode feature)

(This option replaces the same settings from Rohos)

- **DISABLE_SHUTDOWNDLG=1**
(by default =0)
Does not replace typical Windows shutdown dialog box with Rohos one.
- **DISABLE_CENTER=1**
(by default =0)
Disables to open Rohos window.

Note: Users cannot change program settings because program registry (HKLM\Software\Rohos) are intended for reading only for users.

- **REG_NUMBER=""**
(by default =0)
Rohos Logon Key registration number (license)
- **LOCK_USB="1"** ("All", "0")
Experimental feature:
The program can disable user to access to USB removable drives. This can prevent users from copying/reading files into USB flash drives and removable disks from office workstations, bringing Trojan/Virus software to the company or from using illegal software inside the company.
"1" - block only USB login Key that is used to access to Windows.
"All" - block all USB flash drives, removable disks and media that are connected to the computer.
"0" – (default value) Do not block an access to USB removable drives.
Read more: http://www.rohos.com/welcome-screen/view.php?m_id=1389

For example, command line could be (silent install):

```
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 Disabling USB flash drive for user access

Experimental feature:

Rohos Logon Key can **disable user access to USB flash drives** and removable media connected to computer;

In Rohos Logon Key 2.0 we have added an experimental feature to **disable access to USB flash drives** and other removable media.

The program can disable user access to USB removable drives. This can prevent users from copying/reading files into USB flash drives and removable disks from office workstations, bringing Trojan/Virus software to the company or from using illegal software inside the company.

How it works.

When user plugs-in any USB flash drive into computer, Rohos Logon Key blocks Removable volume for any read/write operations immediately. It is not possible to work with the USB flash drive on the office PC using any program.

- Outside office PC USB flash drive works as regular, because Rohos Logon Key does not modify its content;
- It is possible to use USB flash drive to access Windows;
- As no Application inside user desktop cannot have an access USB flash drive, even Rohos. It is not possible to use Rohos or USB Key Management utility to change USB Key login profiles or change PIN code.

How to block access to USB flash drive

- Use MSI package option: LOCK_USB="1" ("All", "0") while installing.
- Or setup Windows registry value to block an access to USB device:
Key: **HKEY_LOCAL_MACHINE\SOFTWARE\Rohos**
ValueName: **LockUSBKey**.
Values:
"1" - block only USB login Key that is used to access Windows.
"All" - block all USB flash drives, removable disks and media that is connected to computer.
"0" – (default value) Do not block access to USB removable drives.

Please contact at info@rohos.com if you are interested in this feature

5. Rohos Logon Key Internals

5.1 Components

Rohos Logon Key components:

- Welcome.exe – Rohos Center (Control Panel), install/uninstall routines, login screen component;
- Rohos_ui.dll –GINA module that replaces or makes a proxy layer;
- Rohos_obj.dll – remote login component that integrates into Remote Desktop Application;
- Rohos_cp.dll – Rohos credential provider for Windows Vista.

- Ntserv.exe – welcome-screen service (used in Windows XP\Vista welcome screen + Rohos authentication method, see Chapter 3.3)
- cximagecrt.dll – image processing library.

5.2 USB Key profiles


Rohos Logon Key stores all passwords information in the _rohos\roh.roh file. This file is encrypted with AES encryption algorithm with a default password or PIN code if it is used.

USB Key protection

- USB Key cannot be duplicated. Rohos prevents Key duplicate. Key logon profile is bound up with a USB flash drive serial number.
- USB Key originality can be protected by PIN that is used for encrypting profiles.
- USB Key that was created by USB Manager Tool cannot be modified on home computer (for example, Logon profiles cannot be cleared or modified by user using Rohos Logon Key program)

5.3 Registry keys

Rohos Logon Key uses Windows registry to store all program options.

 Please note that only **MSI** and **RW Server version** installation packages set restricted access rights to Rohos registry values, thus preventing users from modifying program settings using Windows registry editor or Rohos window.

The **full access is granted only to Administrators group and SYSTEM.**

HKEY_LOCAL_MACHINE\SOFTWARE\Rohos

| Key's name | Description and Definition (DWORD or string) |
|-----------------------------|---|
| CheckUSBserial | 1- bound up the program to the last configured USB key. By default 1 is after the first USB key was configured |
| DisableLog | 1 – disables log files 0 – (by default) enables logging |
| DisableRohosShutdown | 1 – disables Rohos shutdown dialog 0 – (by default) enables it |
| LockUSBKey | 1 – disables USB login key for user 0 – (by default) enables “all” - disables all connected USB flash drives. |
| LogonType | Do not modify. See Chapter 3.3 Logon model, MSI option Logon Type (see Chapter 4.8)) |

| | |
|---------------------------------|--|
| RohosPath | Actual path to the program. Do not modify |
| USB_Only_login | 1 – disable manual password entry. Allows to log in only by USB key. 0 – (by default) enables manual password entry |
| USB_Key_remove_behaviour | 1 – locks Windows desktop after USB Key withdrawal from USB port. 0 – (by default) no reaction. >50 – means time interval in seconds during which user can work without USB Key (see keyless mode feature) |
| USBLoginPicture | The USB Key icon on the login desktop. (by default) “green USB device” Full Path to gif/jpg/bmp/png file. Max 150*150 pics. |
| DisableSafeMode | 1 – disables the operation of the program in Safe Mode. |
| HeaderTextColor | (RGB) the color of the texts on the welcome screen. |
| NoTextLabels | Disables defined texts on the welcome screen (clock, date). |
| DisableUSBatRDP | 1 – allows using the access to Remote Desktop typing in the password. (even if USB_Only_login=1) |
| DisableTimeLimits | 1 – Disables working time counter - to calculate the amount of time spent on the PC during a day/week, and to display it in the shutdown/logoff window 0 – (by default) enables. |

The following values are only used in “Rohos welcome screen (gina.dll)” (see Chapter 3.3) logon model:

| | |
|---------------------------|---|
| LoginPicture | Background picture for login screen. |
| CtrlAltDel | What happens when user presses CAD: 1 – Opens typical WinNT style security dialog. 2 – Locks workstation 0 – (by default) opens Task Manager in Windows XP, or CAD dialog in Win2000 |
| DisableAdminUnlock | 1 - Disables Administrator to unlock user session. 0 – (by default) |

| | |
|----------------------------|---|
| DisableTypicalLogin | 1 - Disables typical login dialog, where user name, password and domain can be entered. 0 – (by default) |
| WelcomeScreenHelp | Help string that is displayed on right-bottom of the login screen. “” – turns off this help. |

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon :

LegalNoticeCaption - Login screen caption with big font. (“Welcome to Windows” by default);

LegalNoticeText2 – Login screen notice text with smaller font. (“” by default)

6. Examples

In this section you will find out real deployment examples.



Prolonging trial time up to 60 days.

We realize that testing time of the Rohos Logon Key software requires more than 15 days. Therefore 15-day testing time can be extended to 60-days. Make a request to get a prolongation Registration Key in order to thoroughly test Rohos Logon Key in your company.

Contact: info@rohos.com.

How to try Rohos Logon Key in the company?

Please read this chapter if you are going to use the solution in the **company with more than 20 associates**.

Rohos Logon Key offers such an innovation that affects Network Administration parts and company associates. Therefore we recommend **trying it with the help of focus group**:

- Select a small department or group of computer users in the company where you can try Rohos password replacement solution with USB Keys;
- You will need **10 USB flash drives** for test. (See 3.4).

Installation recommendations:

- Do not disable login via manual password entry from the beginning of the test.

Divide your test into 2 stages:

1. Test the general USB key login possibility within the focus group;
2. Test all the USB Key login features during the actual rollout of the entire solution in the small department (room).

After that you can install Rohos on the rest of the network.

Example 1. Windows Active Directory based on the network. Local login.

First, install Rohos Logon Key Server version (see Chapter 4.1) into your (Admin's) workstation.

How you can plan the rollout:

1. Set up a USB Key with a default password fore each person. (Using USB Key Management utility, see Chapter 4.2);
2. Install the application on the workstations using MSI package with USB only login option (see Chapter 4.9) or others;
3. Set back the users password to default with option to change it by next logon (Default password that is used to setup USB Key);
4. Hand out the USB Keys;
5. User shall log on with the flash drive and change password. (The password will be updated to USB flash drive);
6. From now on the user can only logon with USB flash drive.

What next:

- User Support (US) personnel can use remote desktop access (via password or USB key) in order assist users. In this case you should configure USB key for each US person with remote login component (see Chapter 4.3) or install Rohos Logon Key there.

7. Troubleshooting

Faced with the bug, unknown program behavior or any issues?

We will be glad to support and resolve the issue, but we need log files of the program:

C:\program files\rohos*.log

7.1 Error strings

What does an error mean?

"USB Key was not configured for this computer, it will be ignored"

You may see it in the following cases:

1. The USB key was not configured for this computer, i.e. it does not have a valid logon profile for this PC (no login profile with the local computer name or "").

“Domain” field in login profile should contain: computer name where you log in, “” (blank line) or \\ domain name- only if “Rohos welcome screen gina.dll” is used.

To resolve this error:

-Install USB Keys Management utility and set up profile accordingly

2. This is a 'stranger' USB Key and it is ignored by Rohos logon because the computer owner already has configured its USB flash drive for this computer. By default Rohos bounds up to the first configured USB Key. Even USB Keys that was configured with a USB Key Management utility will be ignored.

The following registry value enables this security option:

HKEY_LOCAL_MACHINE\SOFTWARE\Rohos - **CheckUSBserial=1**

To resolve this error:

- Clear the **CheckUSBserial** value or setup this USB flash drive on the local computer using Rohos Logon Key main window.

3. USB Key was created by simple Rohos files copy operation into another USB flash drive.

To resolve this error:

- Set up USB Key over again

Demo Key. Key registration is required

It means that USB Key setup has been made using USB Key Management utility without license keys

To resolve this error:

- Add license keys to USB Key Management utility

"Your Rohos license does not support this feature. Please upgrade your license."

Usually it means that the USB Key contains several login profiles and personal license is used.

To resolve this error:

- [Purchase](#) a business license or have only a single login profile on the USB Key (clear it and re-configure again).

The benefits of business license:

- Use a single USB Key to log in into multiple computers/user accounts.
- You can log in into [Remote Desktop login](#) by USB flash drive.
- Support for Novel Client for Windows
- Support for Windows Domain, Active Directory.

8. Contacts and updates

Web sites:

USA: www.rohos.com

France: www.rohos.fr

Russia: www.rohos.ru

Germany: www.rohos.net

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

Updates and release notes: <http://www.rohos.com/welcome-screen/download.htm>

The latest version of this guide: <http://www.rohos.com/RohosWelcomeUserGuide.pdf>

Address:

Tesline-Service SRL

10, Calea Iesilor str.

MD-2069, Chisinau

Republic of Moldova.

Tel.: (+373 22) 740-242

(GMT: +3:00) working hours: 9:00-17:00, (no phone technical support).