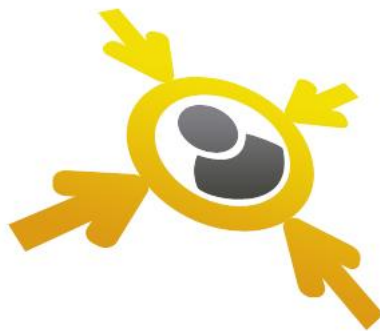


## UserLock Getting Started Guide Version 6



For additional information, please contact IS Decisions at one of the following:

 **+335.59.41.42.20**  
Phone

 **+335.59.41.42.21**  
Fax

 **[www.isdecisions.com](http://www.isdecisions.com)**  
Web

 **[info@isdecisions.com](mailto:info@isdecisions.com)**  
Email

## Introduction

The *UserLock Getting Started Guide* is designed to provide step by step installation instructions and configuration for the major features. The goal is to quickly familiarize yourself with the *Windows* console and the basic *UserLock* concepts. Additional features like the *Standalone Terminal server*, *Web console*, *RAS agent/policy*, *IIS agent/policy*, *Workstation* and *Time restrictions*, etc. are fully described into the [software help file](#).

If you run into issues or questions during your evaluation, installation or migration, we invite you to contact our [technical support team](#).

## Table Of Contents

<b>1. INSTALL THE USERLOCK SERVER .....</b>	<b>3</b>
1.1. USERLOCK INSTALLATION WIZARD .....	3
1.2. USERLOCK CONFIGURATION WIZARD .....	5
<b>2. INTERFACE DESCRIPTION .....</b>	<b>6</b>
<b>3. DEPLOY THE USERLOCK DESKTOP AGENT .....</b>	<b>7</b>
<b>4. SET A CONCURRENT SESSION LIMIT TO 1 FOR EVERYONE .....</b>	<b>10</b>
<b>5. RUN A SESSION HISTORY REPORT .....</b>	<b>13</b>
<b>6. USERLOCK SETTINGS .....</b>	<b>15</b>
6.1. PRIORITY BETWEEN PROTECTED ACCOUNTS.....	15
6.2. MESSAGE PERSONALIZATION.....	16

For additional information, please contact IS Decisions at one of the following:

## 1. Install the UserLock server

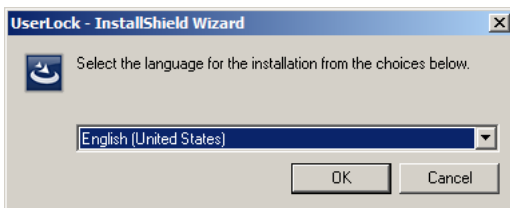
The first thing to do is to install the *UserLock primary server* in the network zone you want to protect. The installation can be done on a server member of the domain. There is no requirement to use a *Domain Controller* server. Any *Windows 2000/2003/2008/2008R2* server can be the host without being dedicated.

The installation process is composed by two quick steps: the *UserLock Installation wizard* and the *UserLock Configuration wizard*.

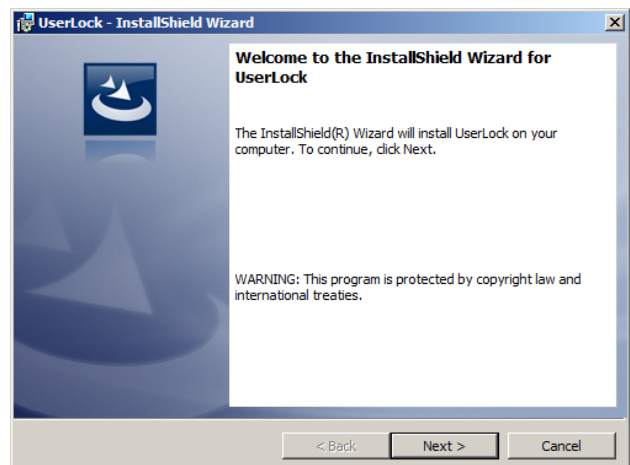
### 1.1. UserLock Installation wizard

Download the installation package [here](#).  
Name of the file package: *UserLock\_x86.exe*

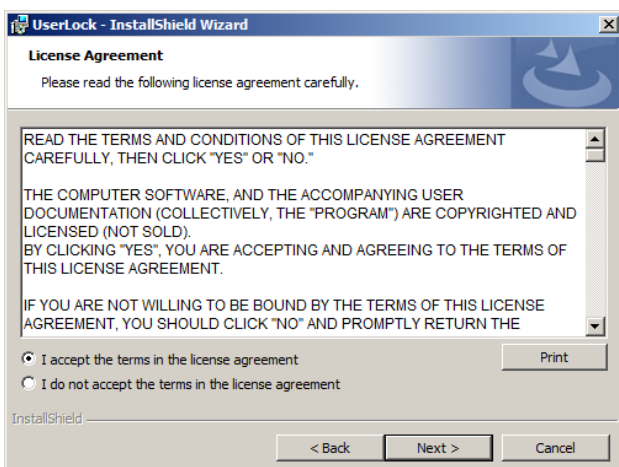
The package is the same for the *English* and *French* language and is compatible with *32* and *64 bits* platform. Execute the downloaded package on the host server to launch the installation process.



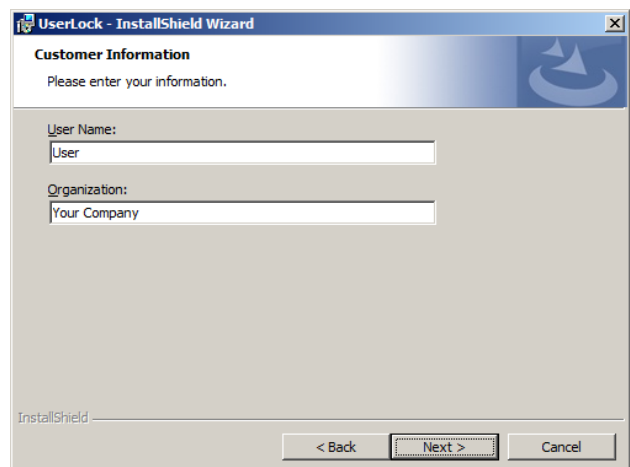
1. Choose your language.



2. Welcome. Click on *Next >*.

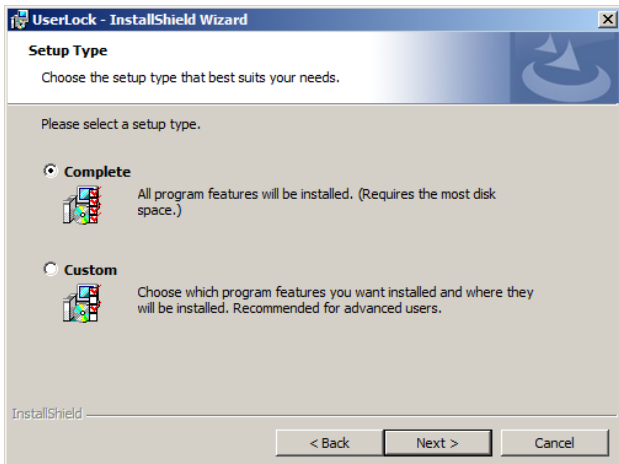


3. *License Agreement*. Read carefully the *End User License Agreement*, accept it and click *Next >*.

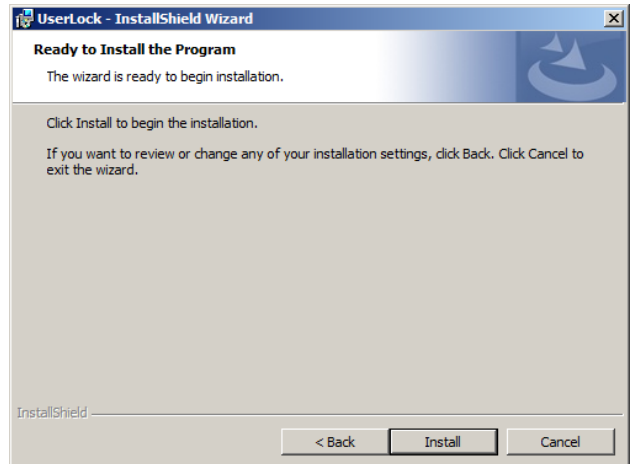


4. Enter your customer references and click *Next >*.

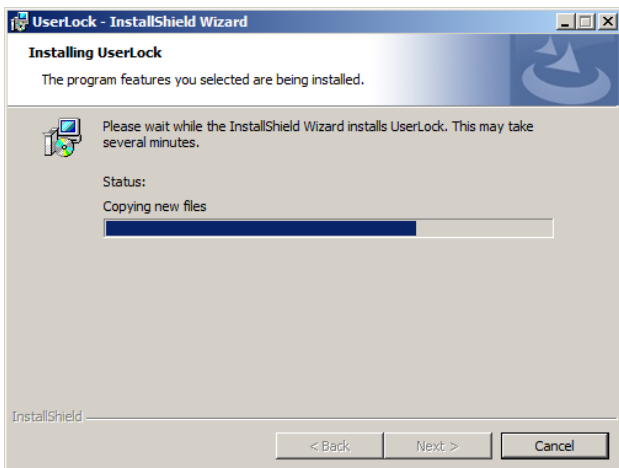
For additional information, please contact IS Decisions at one of the following:



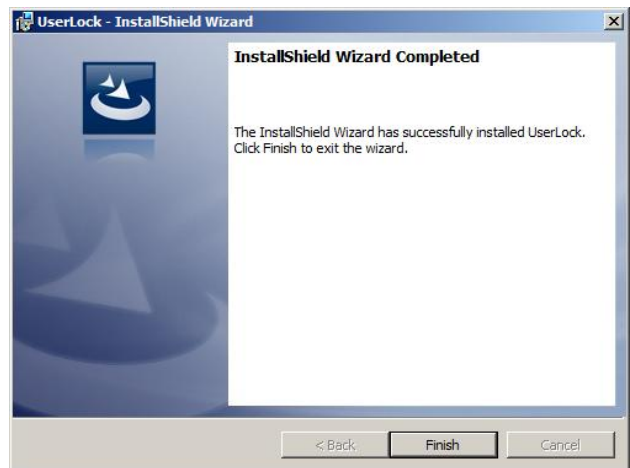
5. Keep the *Complete* box checked and click *Next* >.



6. *UserLock* is ready to install. Click on *Install*.



7. Installing *UserLock*.



8. *UserLock* is installed. Click on *Finish*.  
The *UserLock Configuration wizard* will open.

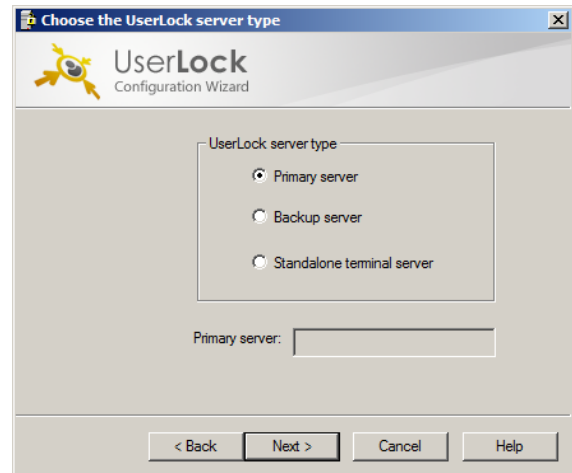
For additional information, please contact IS Decisions at one of the following:

## 1.2. UserLock Configuration wizard

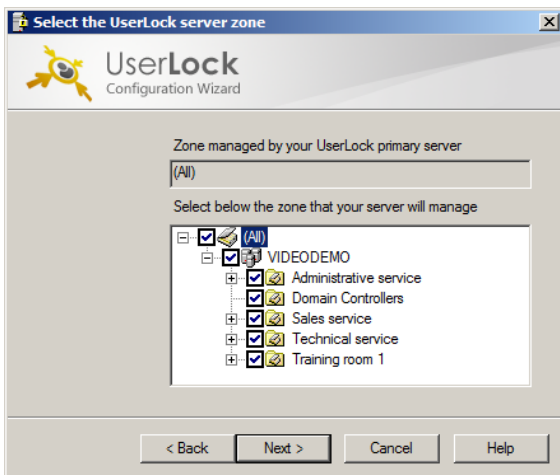
Once you've finished the software installation, the *Configuration wizard* will open.



1. Welcome. Click on *Next >*.



2. Choose the *Primary* server type. Click on *Next >*.



3. *Protected Zone*. Select the network zone to monitor with UserLock: *All*, a *domain* or a multi *Organization Unit* selection. Click on *Next >*.



4. Service account. Enter a domain administrator account and password to run the *UserLock* service. Click on *Next >*.

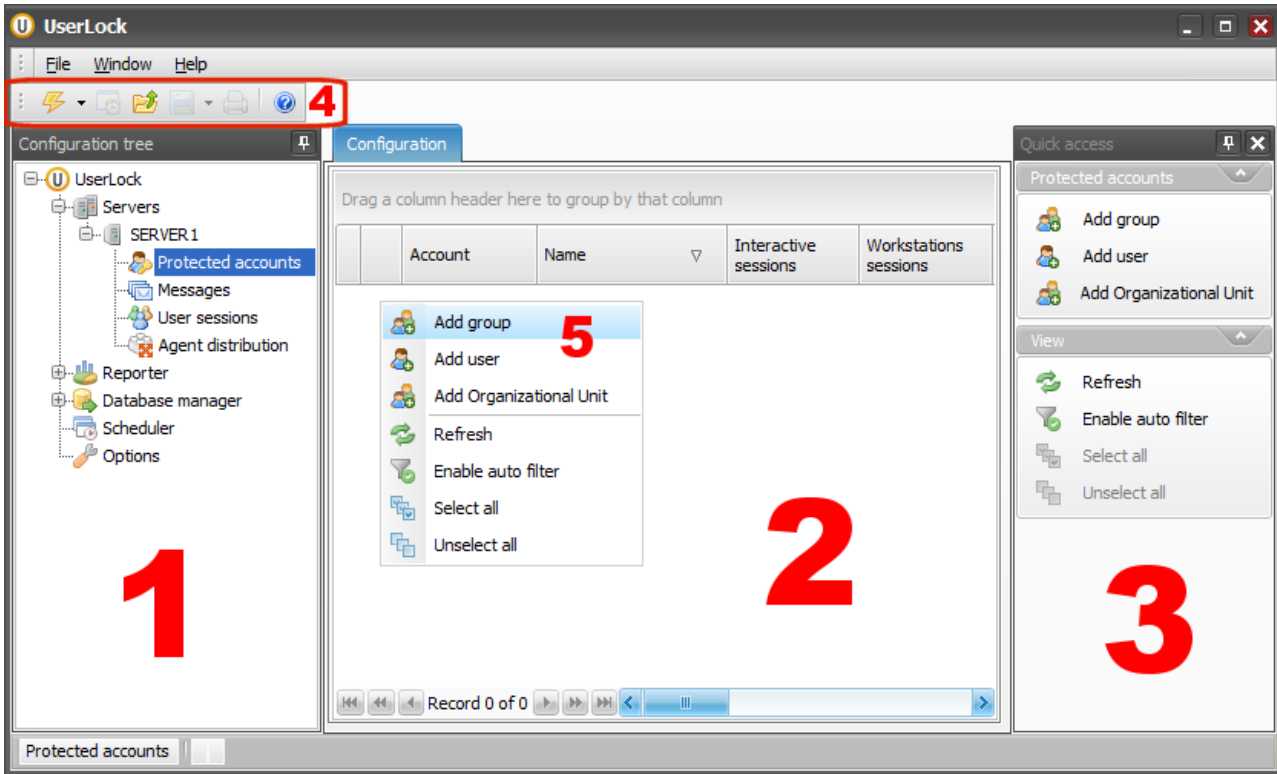


5. *UserLock* server is now set. Click on *Finish*.

For additional information, please contact IS Decisions at one of the following:

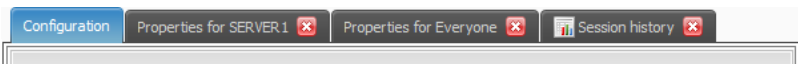
## 2. Interface description

UserLock console is composed by 5 main navigation elements.



**1: Configuration tree:** allows you to navigate through *UserLock* features.

**2: Central window:** Displays the different *UserLock* views, the configuration form for the selected feature in the *Configuration tree*, and reports. This window can display several tabs.

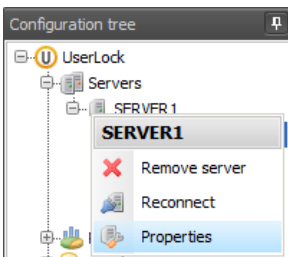


**3: Quick access panel:** Shortcuts for the features selected in the *Configuration tree*.

**4: Tool bar:** Allows you to *Launch* an action, the *scheduler*, open a *XML UserLock file*, *Save/export a report*, *print* a report or open the help file. This tool bar will be expanded when *Report* are displayed for more actions.

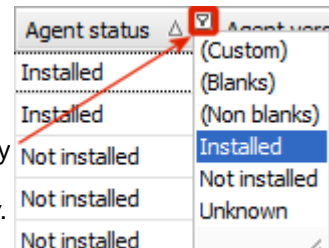


**5: Context menu.** You can also interact with objects displaying the *context menu* (right click). It allows the same actions as those in the *Quick access panel*.



You can also display the *context menu* on *Configuration tree* node to display specific settings menus.

Filters are available on every column displayed in *central window*.



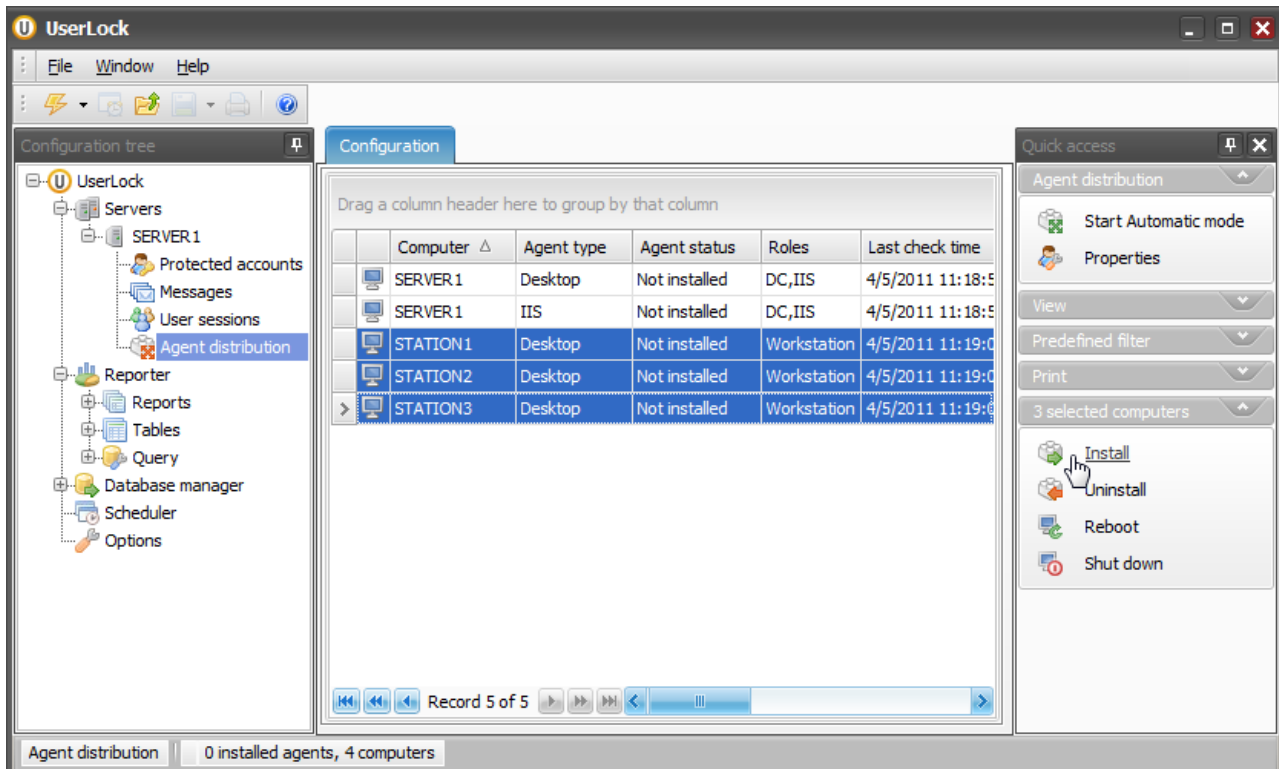
For additional information, please contact IS Decisions at one of the following:

### 3. Deploy the UserLock desktop agent

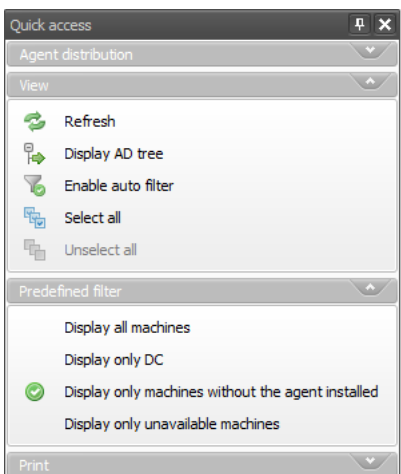
The *UserLock desktop agent* allows you to set *UserLock* policies for user sessions. You can deploy it on every computer in your *protected zone* with an *operating system* from *Windows 2000* to *Windows Seven*. You can also target servers from *Windows 2000* to *W2008 R2* to monitor your server sessions and the terminal sessions.

Select *Agent distribution* in the *Configuration tree* to open the agent deployment engine.

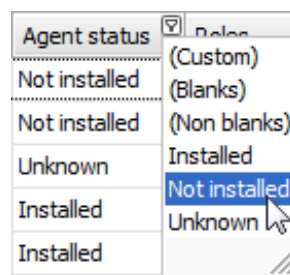
There are two way to process your remote agent installation. You can select the target computer(s) in the list displayed in the *central window* and click on *Install* in the *Quick access* panel or through the *context menu* (right-click).



A new tab will open in the *Central window* to display the deployment process status and results. As you can see there can be several agent types in the *Agent type* column. If you want to know more about these different *UserLock agents*, you can visit the [full online help](#).

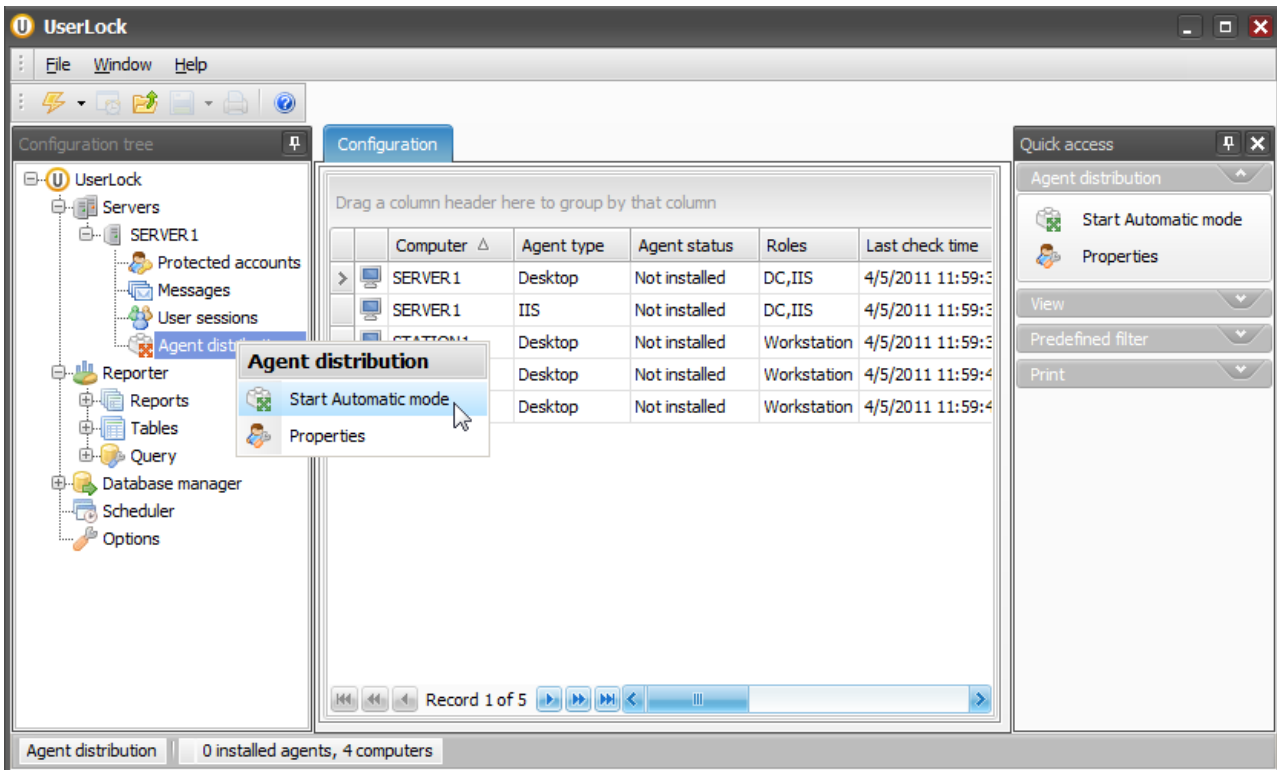


If the list of computers displayed in the *Agent distribution* view is too lengthy, you can change the *View* from the *Quick access* panel, using the *Predefined filter*, or the filter from each column head ([Chapter 2](#)).



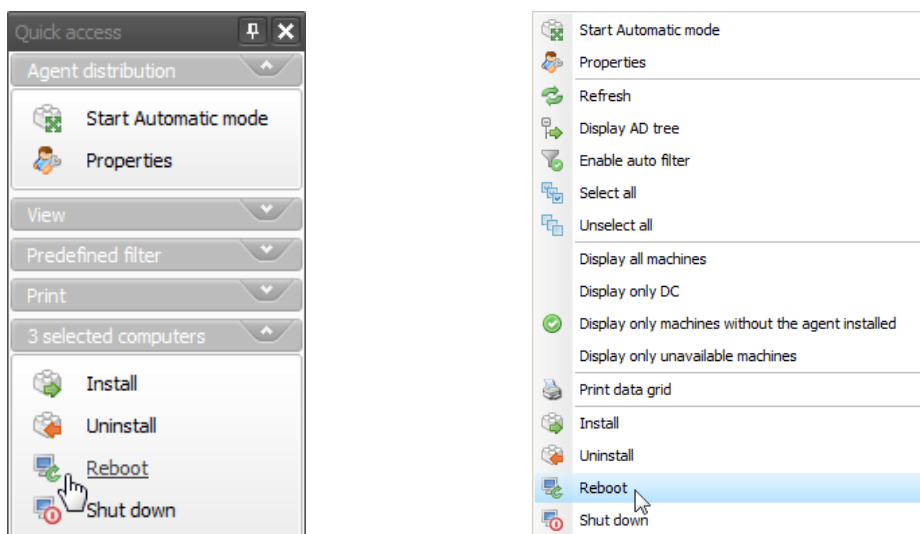
For additional information, please contact IS Decisions at one of the following:

Or you can enable the *Automatic mode* with a right click on the *Agent deployment* menu in the *Configuration tree* and then click on *Start Automatic mode*. If it's not already present, the *UserLock desktop agent* will be automatically deployed on every workstation that is a member of the *protected zone*. By default the automatic deployment excludes the servers and only concerns the *desktop agent*.



This mode is useful when you add a new computer to your *Protected zone*. You will have nothing to do as the *Automatic mode* will detect the *desktop agent* absence and will install it.

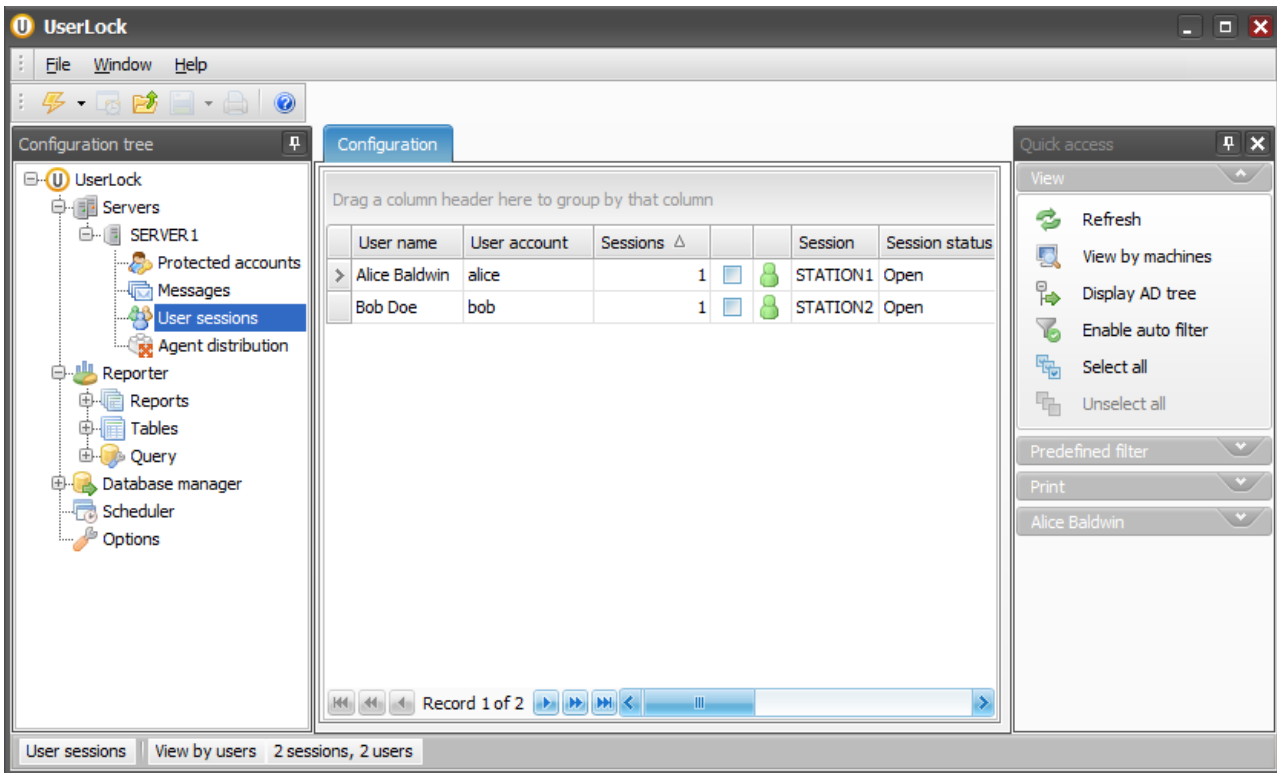
Note that the agent activation on older *Operating systems W2000, W2003 and XP* requires a reboot. You can restart the computers if needed directly in *Agent distribution* view. Select the computer(s) and click on *Reboot* in the *Quick access* panel or through the *context menu* (right-click).



You can also schedule this reboot during non business hours independently from *UserLock*.

For additional information, please contact IS Decisions at one of the following:

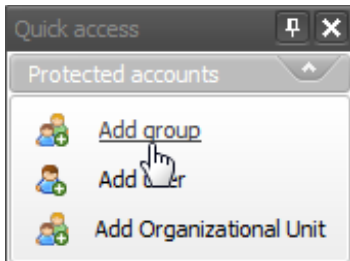
Once the *desktop agent* is deployed on a machine, every session event will be logged and stored in the database. You can check if the agent is enabled and working by opening a session on a computer where you previously installed it and then displaying the *User sessions* view into *UserLock console*.



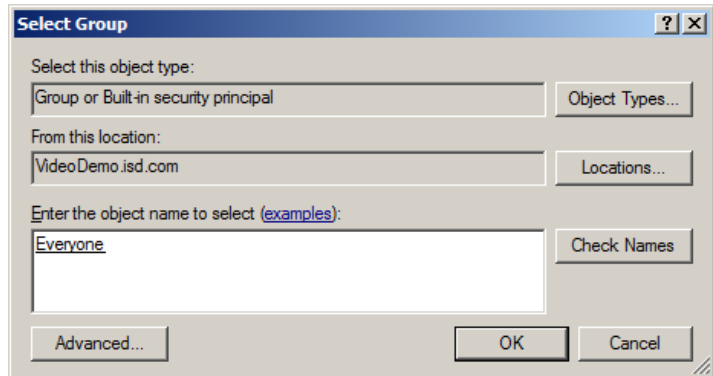
For additional information, please contact IS Decisions at one of the following:

## 4. Set a concurrent session limit to 1 for everyone

The *UserLock* policies are managed through the *Protected accounts*. Click on *Protected accounts* in the *Configuration tree*. Then in the *Quick access* panel, click on *Add group*. The *Select group* window will open. Type *everyone* and click on *Check Names* button to verify the *Active Directory* name group. Then click *Ok*.

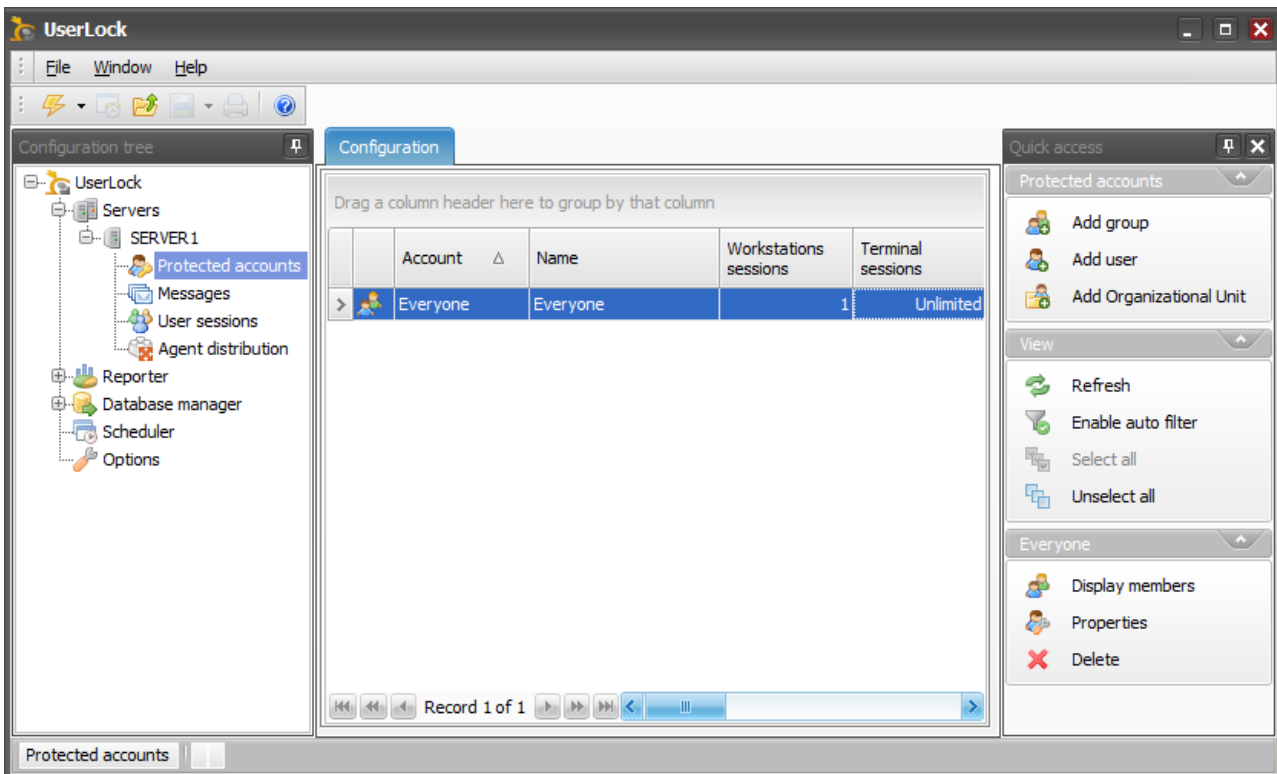


Click on *Add Group*.



Type *everyone* and click on *Check Names* then *Ok*.

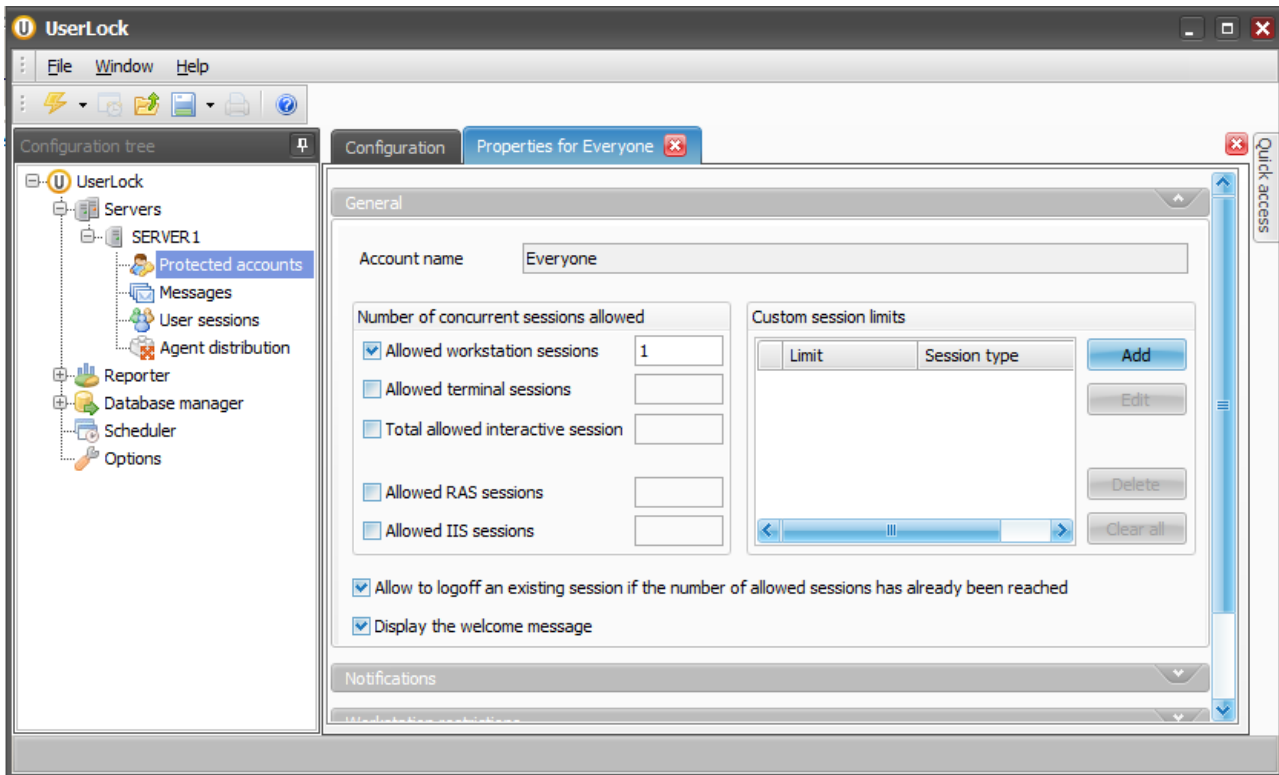
The new *Group Protected account* will be added to the list into the *Central window*. By default, a new *Protected account* is set with no defined rules.



For additional information, please contact IS Decisions at one of the following:

Display the *Properties* of this *Protected account* by selecting the line in the *Central windows* and then clicking on *Properties* in the *Quick access* panel. You can also directly double-click on the line or use the *context menu*.

Check the *Allowed workstation sessions* box and type in the limit.



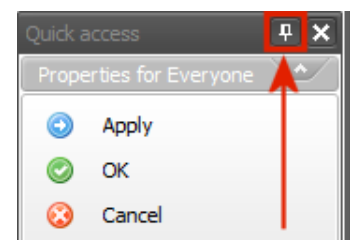
You can also enable two practical options for users:

- *Allow to logoff an existing session if the number of allowed sessions has already been reached*  
Users would be able to remotely close an opened session to logon a new one. This will avoid going back to the previous machine they logged into and gain time.
- *Display the welcome message*  
The *welcome message* is an informative popup displayed at logon. It informs users on previous logins: last login time, last computer(s), and last denied login(s) ([if requirements set](#)).

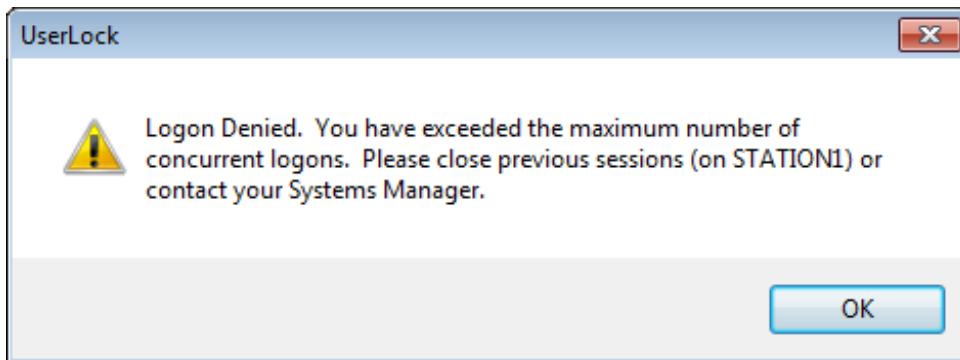
Validate the configuration of this *Protected account* click on *Ok* in the *Quick access* panel.

**Notice:** You can see on the picture that the *Quick access* panel can be reduced by clicking on the icon on the left. Just passed the mouse over the tab to display it again.

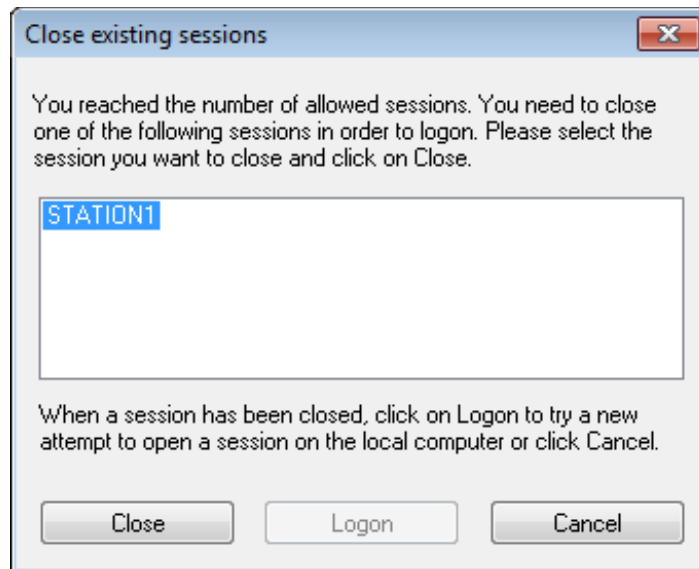
You can also hide the *Configuration tree* in the same way.



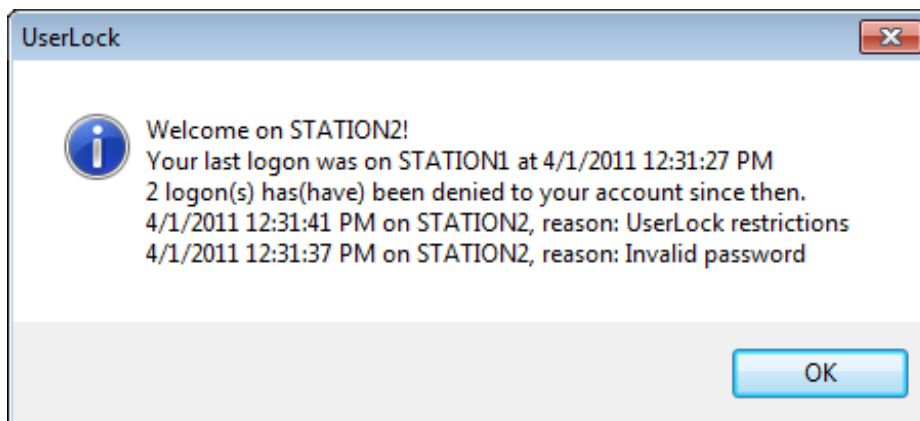
Once your *Protected account* is validated, users will be limited to one concurrent session. If they try to open a second session with the same *User account*, they will be denied by *UserLock* on all workstations where the *UserLock agent* is deployed.



Logon denied pop-up.



Logon denied pop-up with the option  
*Allow to logoff an existing session if the number of allowed sessions has already been reached.*

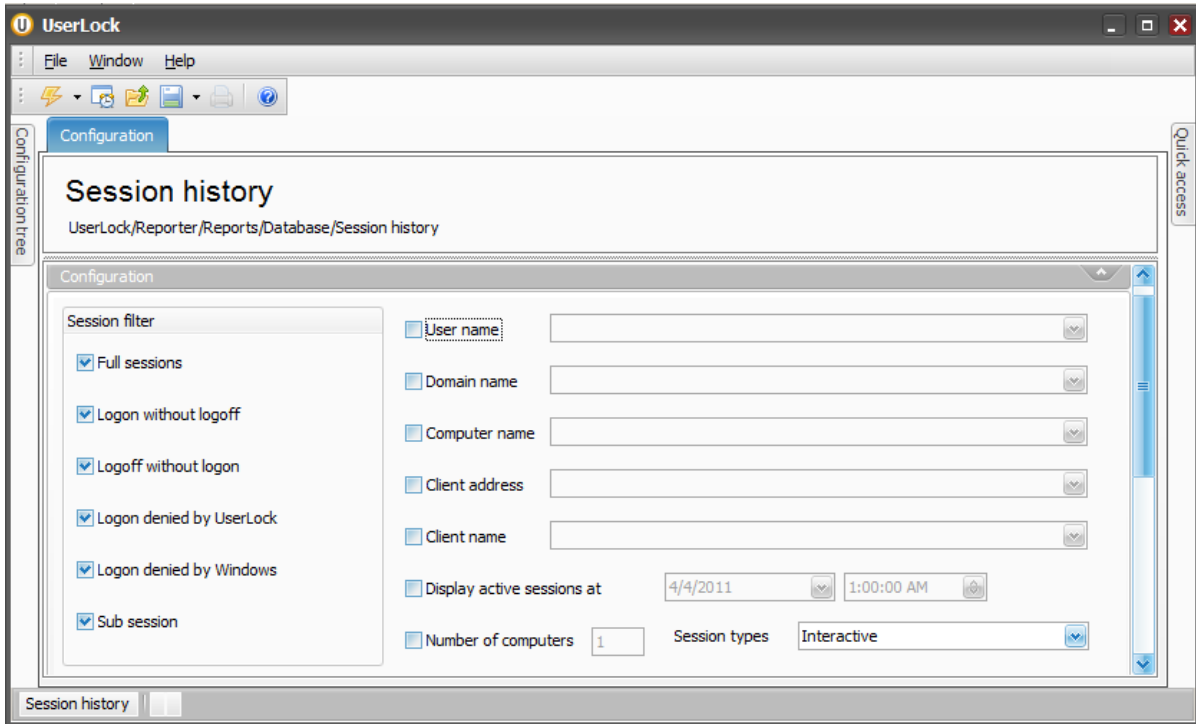


Welcome message at user successful logon.

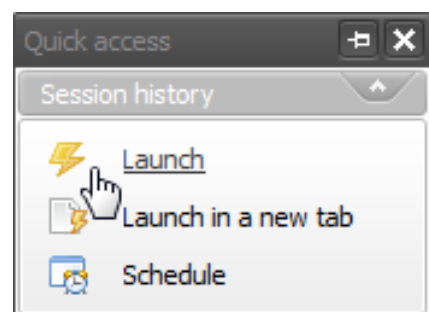
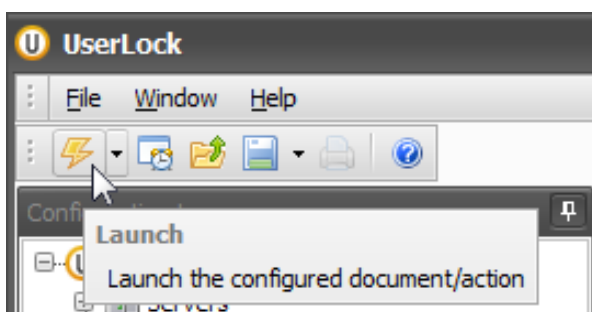
For additional information, please contact IS Decisions at one of the following:

## 5. Run a Session history report

During your tests on the *Protected account*, the events were inserted into the *Database*. You can see all session events on *Reports*: Deploy the *Reporter* node from the *Configuration tree* and select *Session history*. The *Central window* will display the configuration options, filters and group parameters.

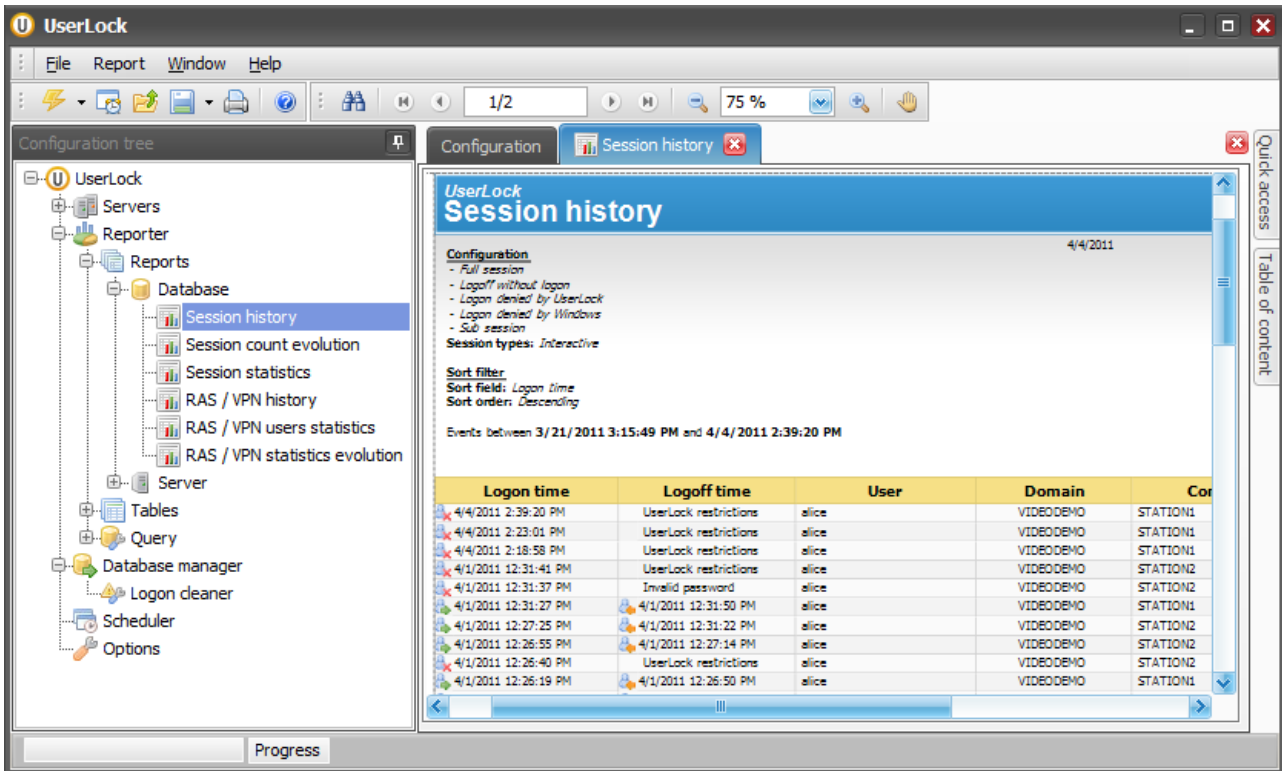


Different sections are available to set your reports: *Configuration*, *Sort/Group*, *Time*, *Database* and *Report Layout*. You can run it directly without any setting changes by clicking on the *Launch* button in the *Tool bar* or in the *Quick access* panel.

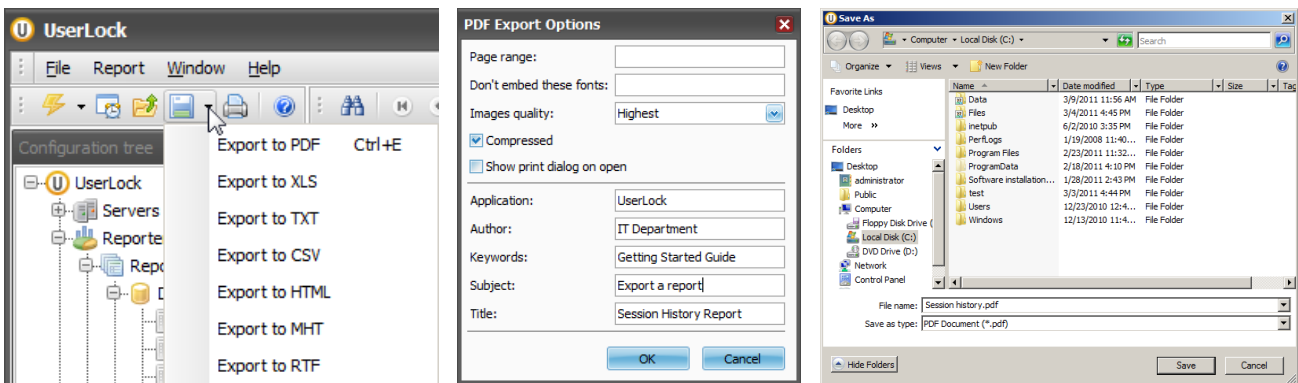


For additional information, please contact IS Decisions at one of the following:

The *Session history* report will open in a new tab.



You can then print or export this report in different formats.



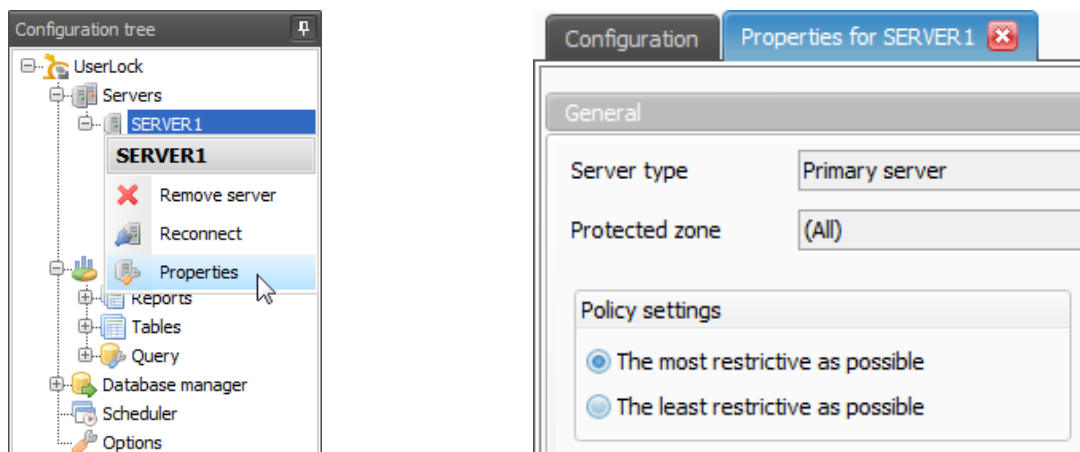
Different reports are available in the *UserLock console*. They are fully [described in the help file](#). You can also choose to [schedule reports](#) and choose to receive them periodically by email as attached documents.

For additional information, please contact IS Decisions at one of the following:

## 6. UserLock settings

### 6.1. Priority between Protected accounts

By default the priority between several *Group/OU (Organization Unit) Protected accounts* is set to the most restrictive. It means that if a user is linked to several *Group* or *OU Protected accounts*, the restriction which will be reached the first will be applied. This setting can be switched to the opposite in the server *Properties*. Do a right click on the server icon in the *Configuration tree* to display the server *context menu* and click on *Properties* to open it. Choose the wanted behavior and click on *Ok* in the *Quick access panel* to save the change.



**Notice:** A *Protected account* set for a user account will always override the *Group/OU Protected accounts* policies. In other words, a *User Protected account* can be considered as rule of exception.

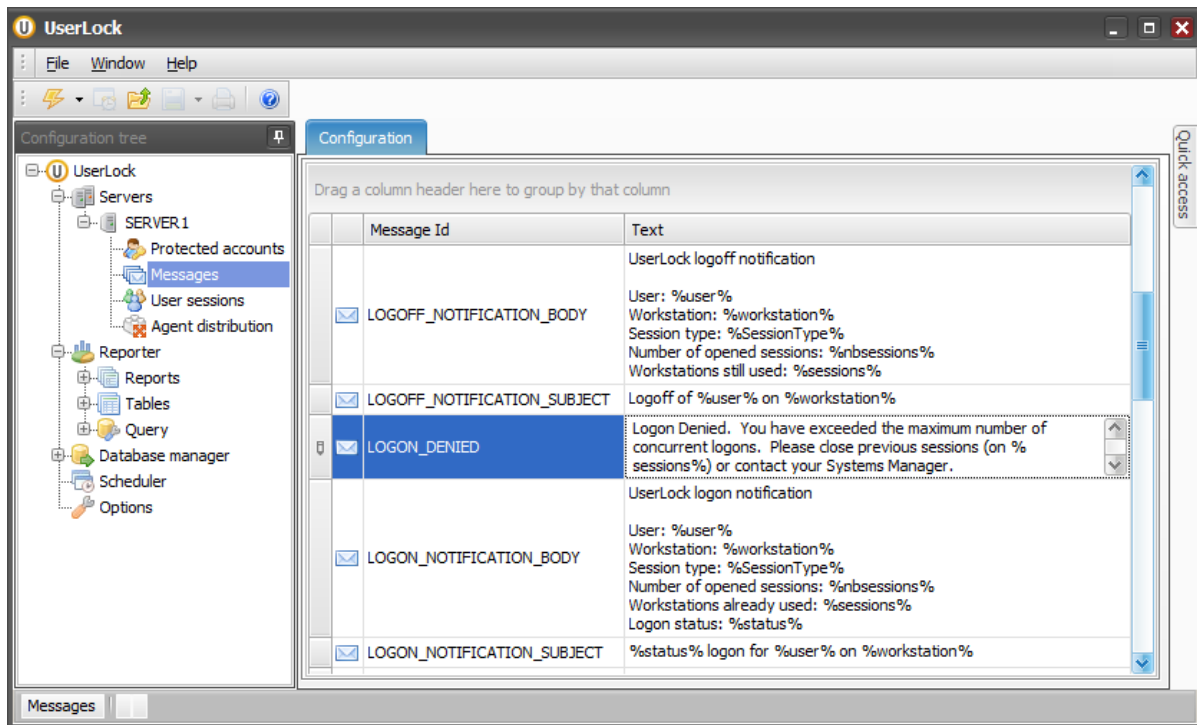
If for any reason you need to give unlimited session access to a specific user, you can create a *User Protected account* for this specific user and leave all default settings to unlimited. Even if he is a member of a group which has a *Group Protected account*, this user won't have any limit.

For additional information, please contact IS Decisions at one of the following:

## 6.2. Message personalization

You can modify the *UserLock* notifications displayed to users when a specific event happens. This is useful to localize in your language or to give more information/details about *UserLock* policies to your users.

Select *Messages* in the *Configuration tree*. In the *Central window*, click on the message you want to change and the edit cursor will appear. Modify it as wanted. All modifications will be saved automatically.



These messages contain text and dynamic variables included between two percentage characters: *%Dynamic\_Variable%*. To understand when the notification messages are displayed and the meaning of each dynamic variable, you can read the [UserLock online help](#).

For additional information, please contact IS Decisions at one of the following: