



UserLock[®]

What's new in UserLock?

Version 6

www.isdecisions.com

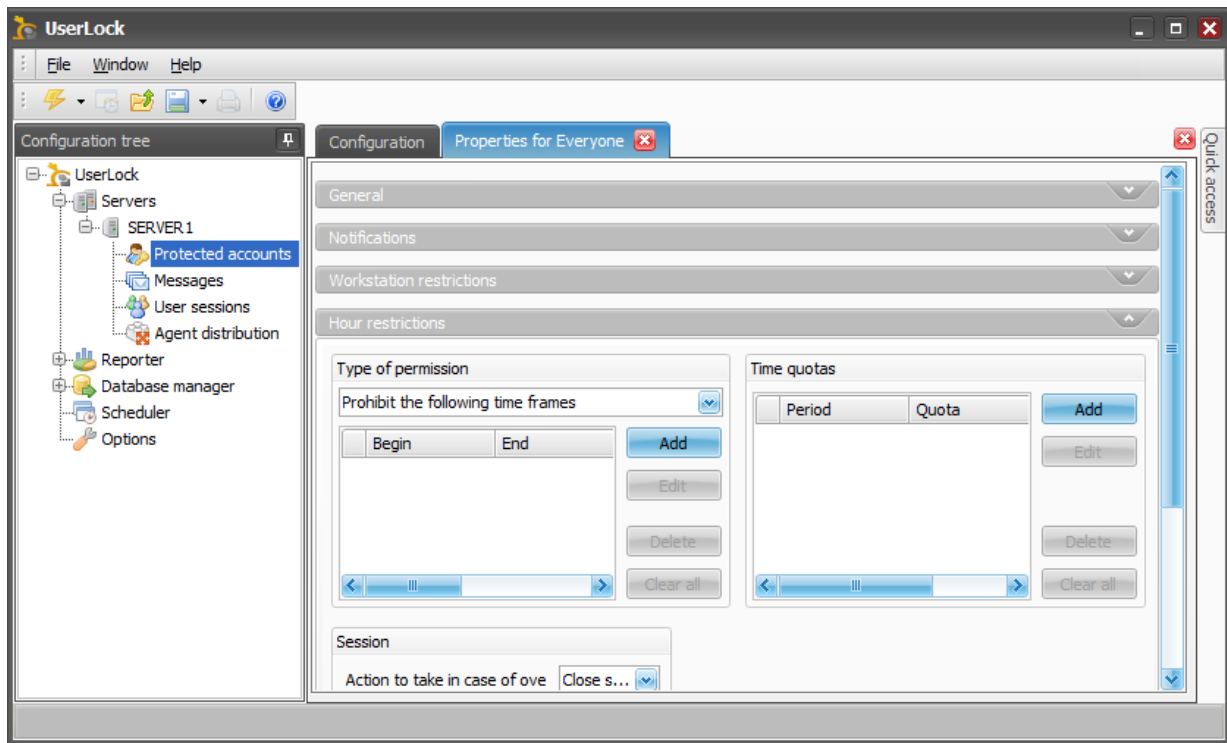
Table Of Contents

- 1. Time quotas 3
- 2. New Protected Account type 5
- 3. Audit and display session with local accounts 5
- 4. Protected zone composed by several Domains or Organizational Units. 5
- 5. Workstation restrictions by Organizational Unit..... 6
- 6. Protection of Internet Information Services (IIS) sessions 7
- 7. New reports 9
 - 7.1. RAS sessions reports..... 9
 - 7.2. Session count evolution report..... 10
- 8. More features 11
- 9. New improvements 11

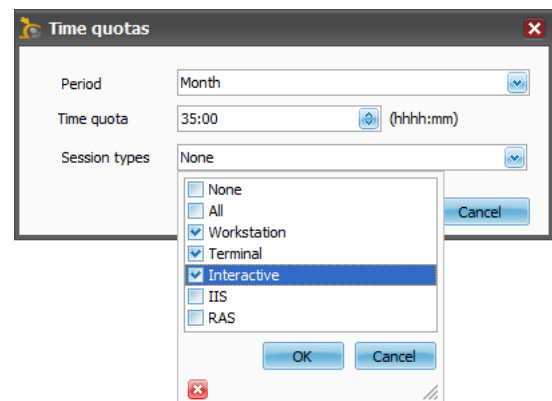
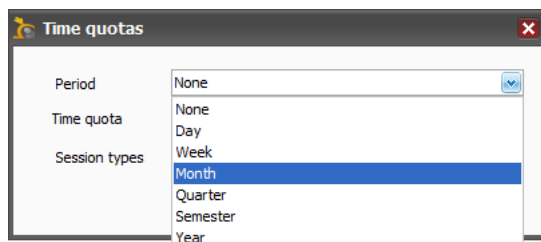


1. Time quotas

The *Time quotas* are now available in *UserLock 6.0* through the *Protected Account* properties, in the *Hour restrictions* section. It allows defining a time value for a period.



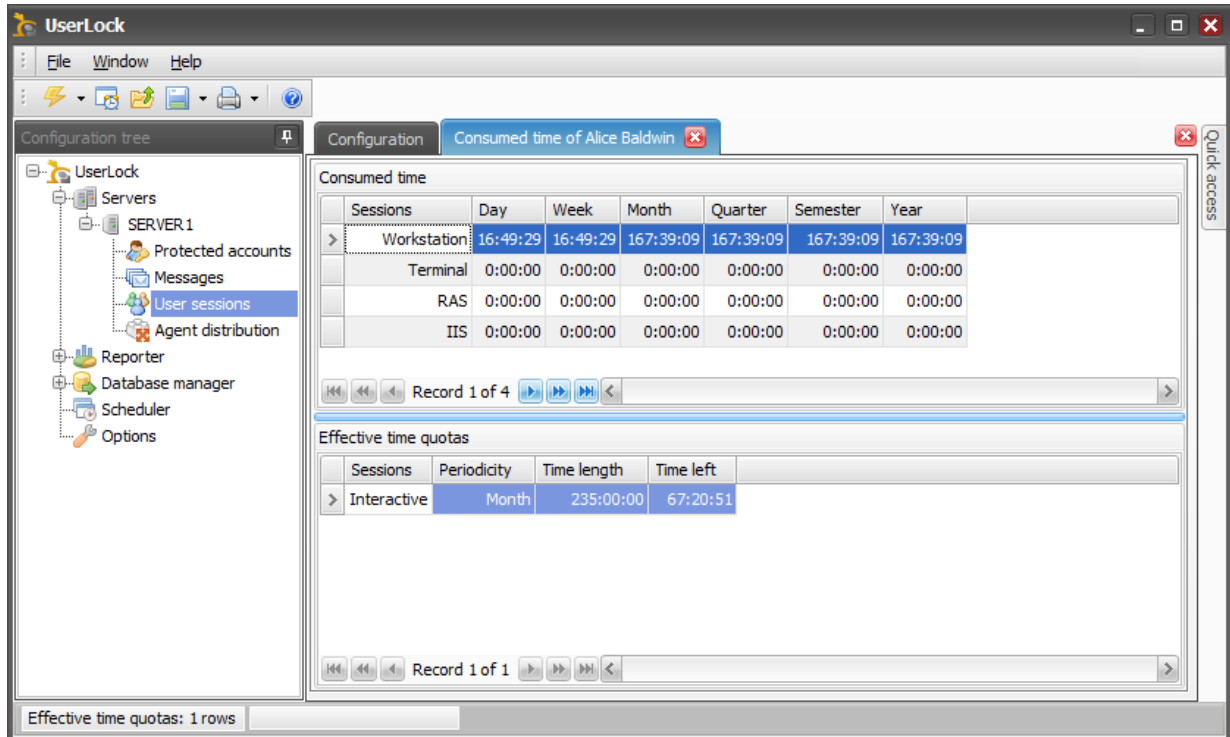
The value is set in hours/minutes and the available periods can be a day, a week, a month, a quarter, a semester or a year. You can choose from all available session types: *All*, *Workstation*, *Terminal*, *Interactive* (*Workstation* + *Terminal*), *IIS* or *RAS*.



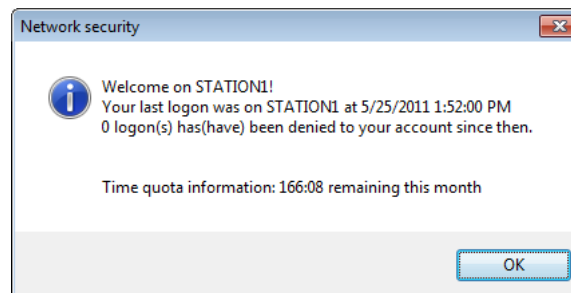
Several *Time quotas* can be defined for a same *Protected Account*. You can therefore set a different *Time quota* for each type of session.



You can check the consumed time status in the *User sessions* view. Just do a right-click on a user in the list and click on *Display consumed time* in the context menu.



The time remaining for the users *Time quota* is automatically displayed in the *Welcome* message. If several quotas can be applied to a user, the information from the quota that will be first to expire is displayed.



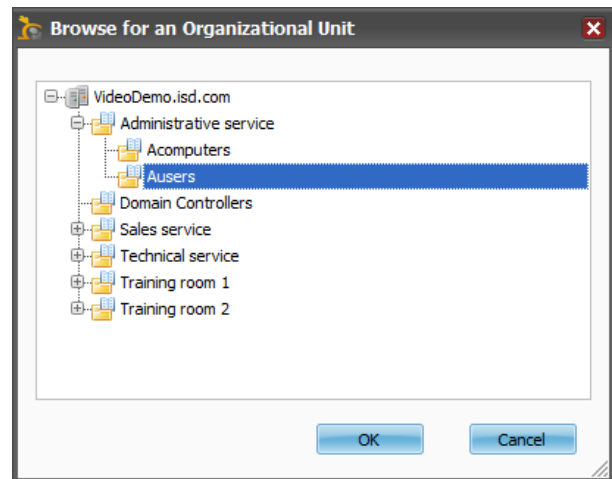
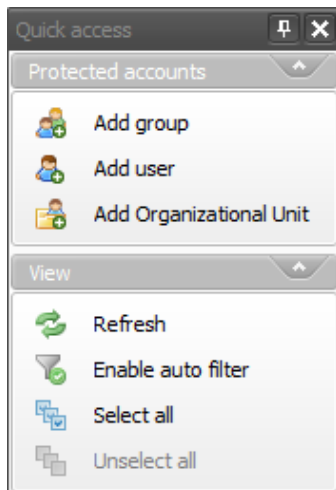
Please take note: The Welcome message include the Time quota information tag only on new UserLock installations. For any upgrade, you need to add manually to the Welcome message the dynamic variable "%quotainformation%".



2. New Protected Account type

Limited to a *User Protected Account* and a *Group Protected Account* in prior versions, you can now define a *UserLock* policy for an *Organizational Unit Protected Account*.

Select the *Protected Account* menu in the *Configuration tree* and click on *Add Organizational Unit* in the *Quick access* pane. A browser wizard will open permitting you to select the user *Organizational Unit* you want to monitor.

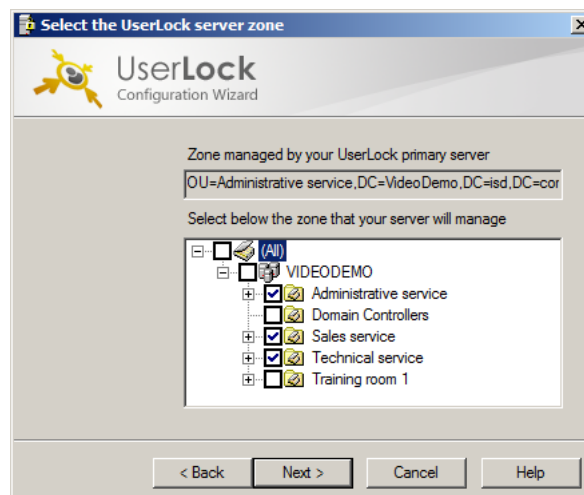


3. Audit and display session with local accounts

The local sessions are now audited and displayed in *UserLock console*. You can remotely logoff the local sessions or simply do reporting.

4. Protected Zone composed by several Domains or Organizational Units.

The *UserLock Protected zone* can be defined choosing several *Domains* or *Organizational Units*. The *Configuration wizard* now displays an *Active Directory* tree with check boxes permitting multi-selection.

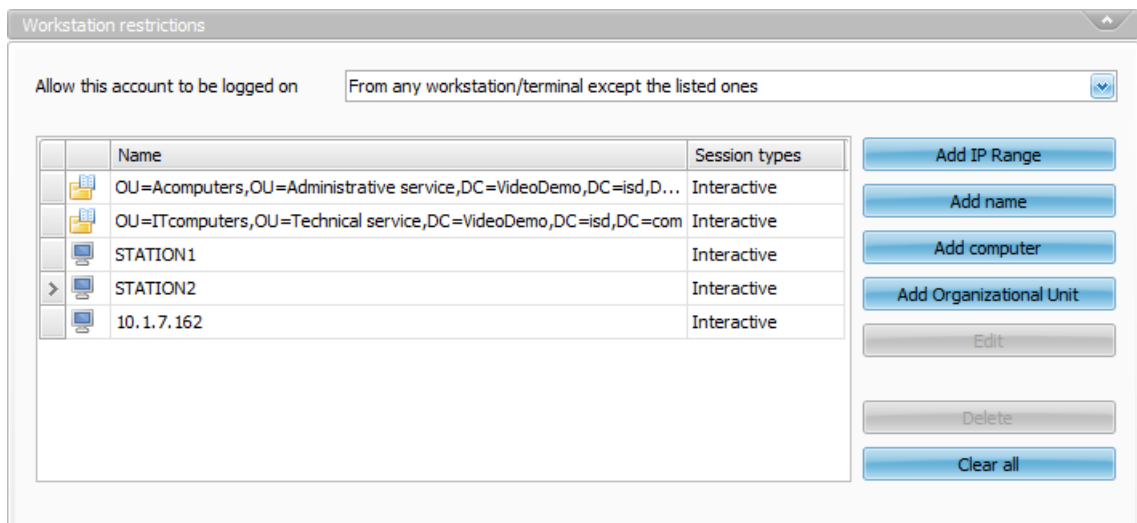
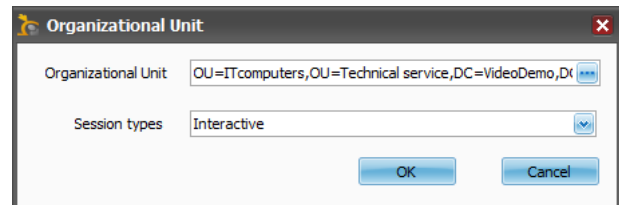
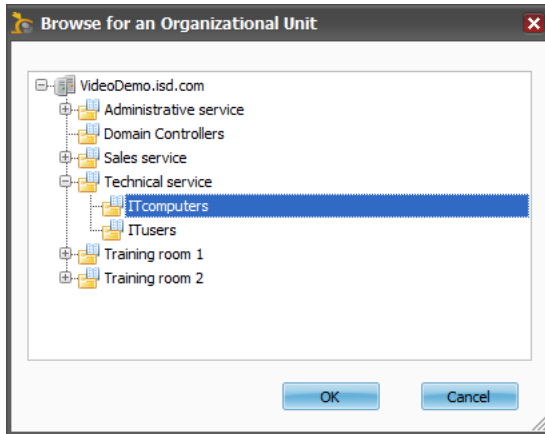


Note that the built-in *Computers* container is not displayed (a container is not an *OU*). Neither are empty *Organizational Units* (without any computer included).



5. Workstation restrictions by Organizational Unit

The *Workstation restrictions* on a *Protected Account* can be now defined using computers *Organizational Units*.



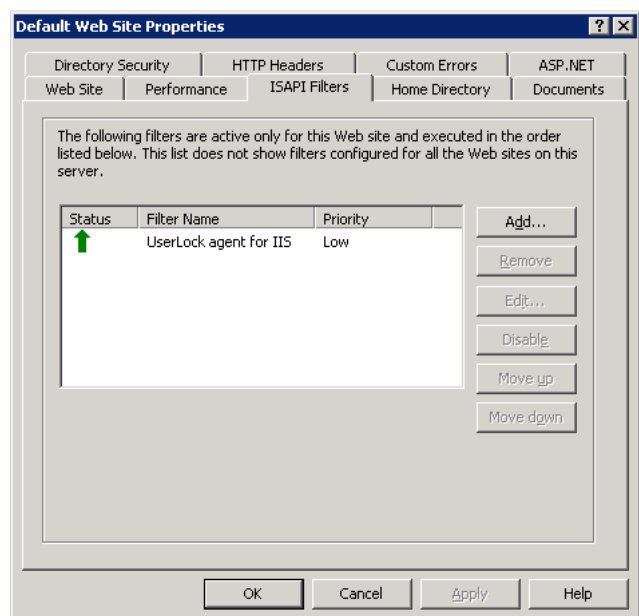
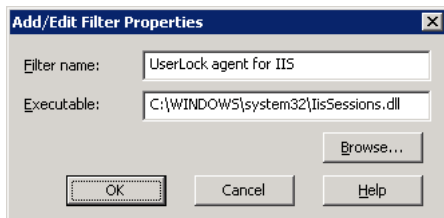
6. Protection of Internet Information Services (IIS) sessions

UserLock 6 adds a new type of monitored session on top of *Workstation*, *Terminal* and *RAS*: the *Internet Information Services (IIS) sessions*. This new feature allows you to define by *Protected Account* the number of maximum concurrent IIS sessions on a specific IIS application like *Outlook Web Access* or *Intranet* site. You can also use the generated logs for reports.

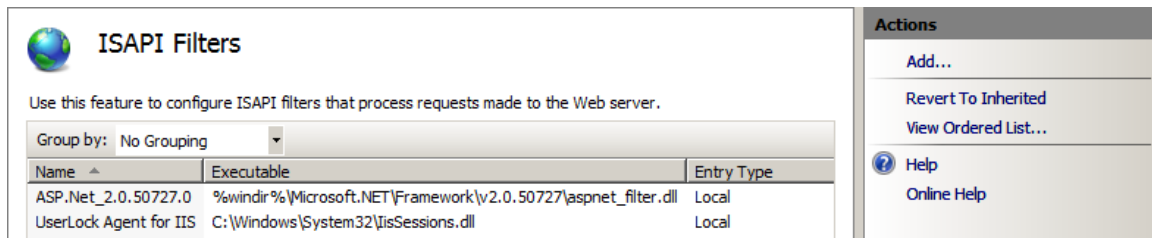
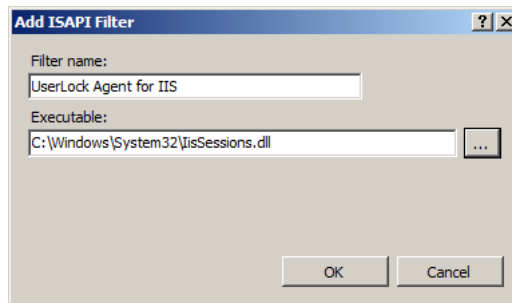
To supervise the IIS sessions, you need to deploy and set the *UserLock IIS agent*. The *Agent distribution* engine automatically detects the servers where *Internet Information Services* is installed and running. To deploy the *UserLock IIS agent*, right click on the corresponding line and click on *Install*.

This agent uses the *ISAPI Filters* technologies. Once the agent is deployed, you need to configure the Web Site *ISAPI Filters* settings on the target server in *IIS Manager*. Depending on the server *Operating System* version, you can set it as below:

- For *Windows 2003* server
 - ✓ Display the *Properties* of the target Web site by right-click in the menu tree.
 - ✓ In the *ISAPI Filters* tab, click on *Add...* button.
 - ✓ Choose a name for the *UserLock* filter and browse to the *UserLock IIS Agent*:
C:\WINDOWS\system32\IisSessions.dll
 - ✓ Click on *OK*.

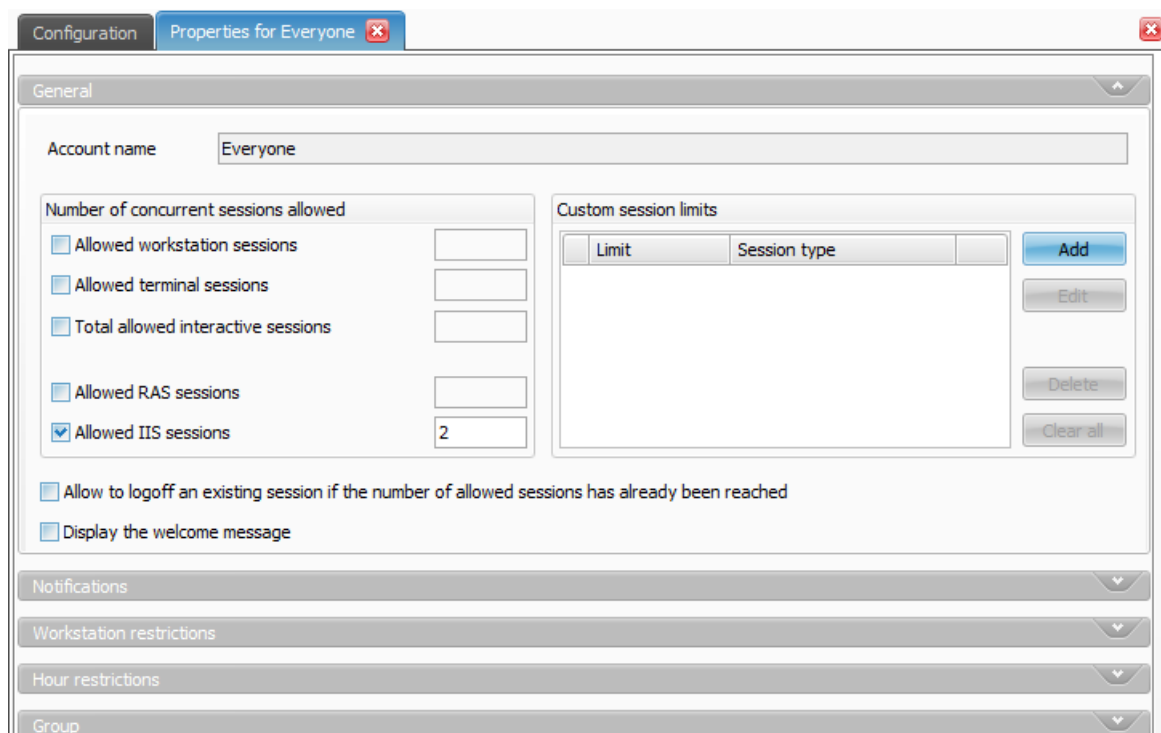


- For W2008 server and W2008 R2 server
 - ✓ Select the target Web site in the menu tree.
 - ✓ In the central windows, double-click on *ISAPI Filters* icon.
 - ✓ In the *Actions* pane, click on *Add...*
 - ✓ Choose a name for the *UserLock* filter and browse to the *UserLock IIS Agent*:
 - ✓ C:\WINDOWS\system32\IisSessions.dll
 - ✓ Click on OK.



The *UserLock IIS agent* will be enabled quickly. If you want to activate it immediately, restart the *Application pool* corresponding to the target Web site. Once the agent is registered, all *IIS sessions* for this Web site will be logged into the *UserLock Database*. They will be also displayed in real time in the *User sessions* view in the *UserLock console*.

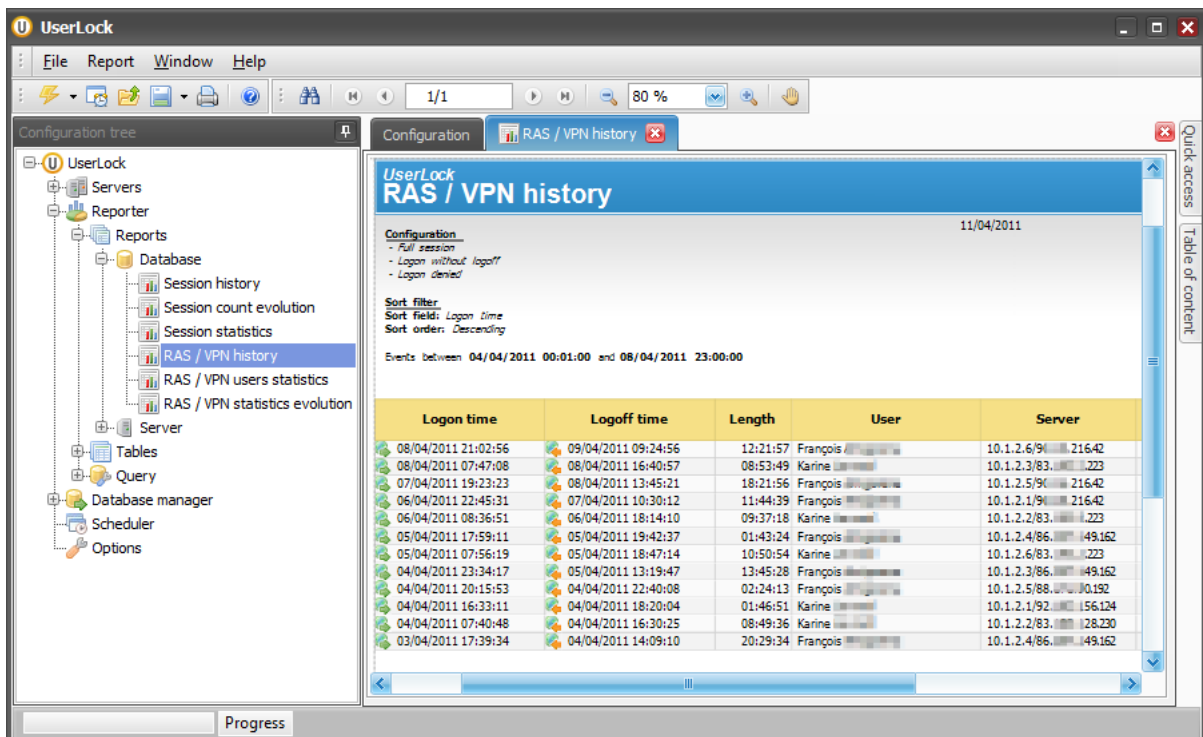
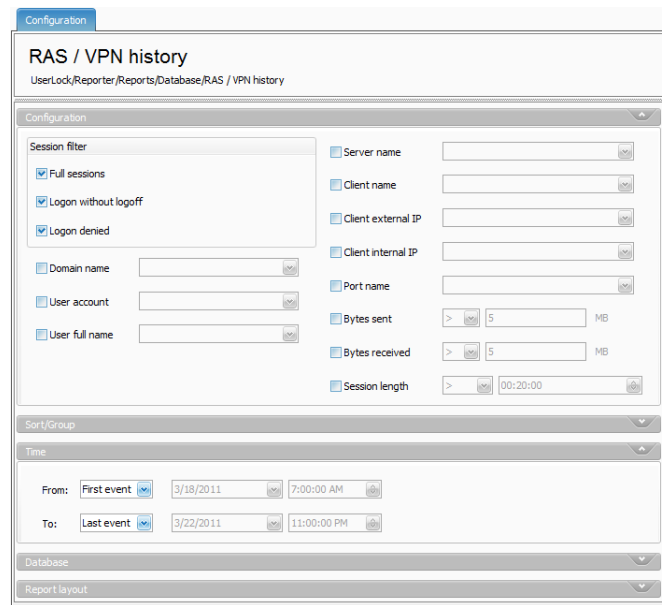
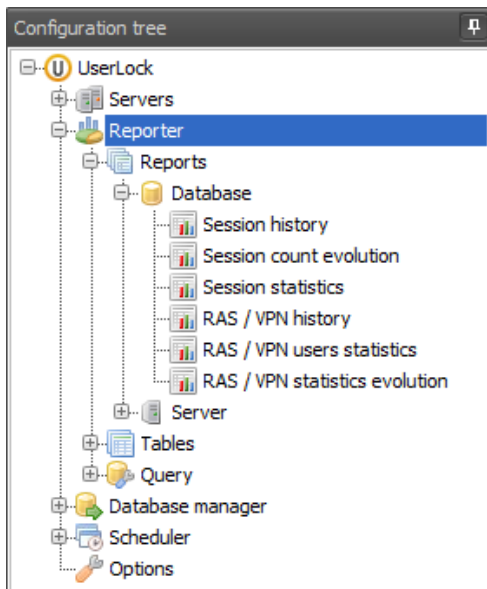
In the *Protected Account Properties*, you can define a limit for the concurrent *IIS sessions*.



7. New Reports

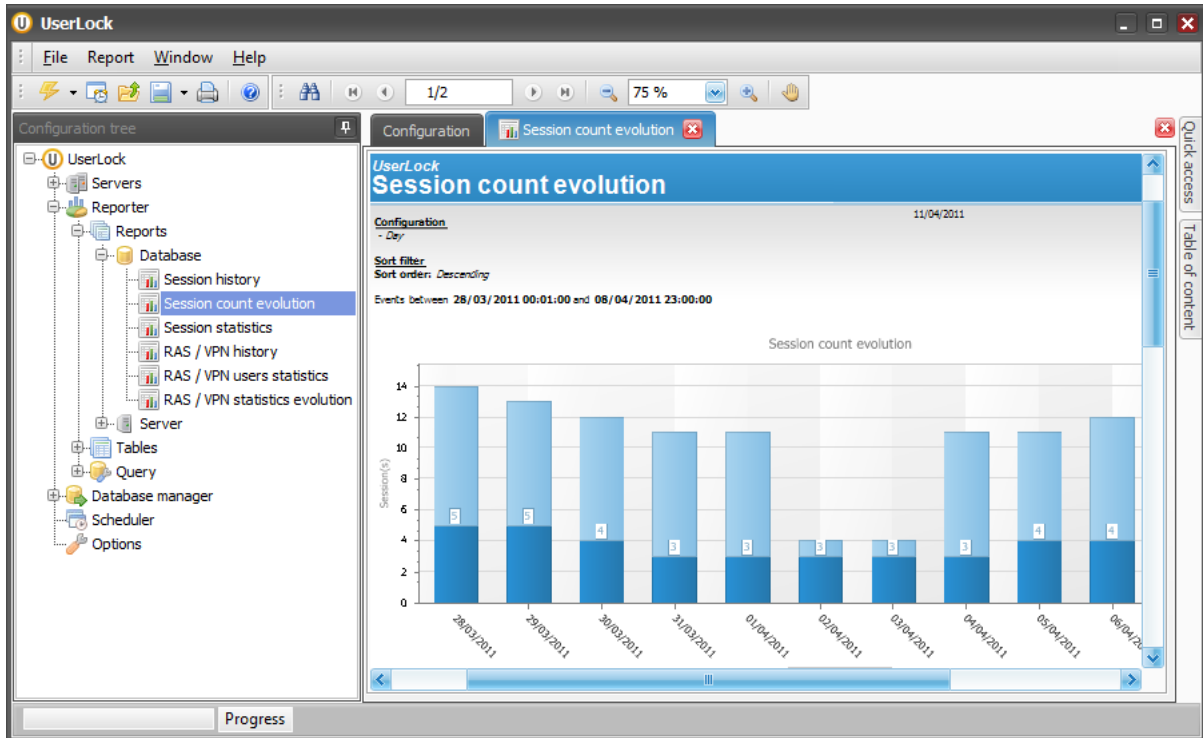
7.1. RAS sessions Reports

Three specialized reports for *RAS/VPN sessions* are now available through the *Reporter*.
You can display history, statistics and a graphical report displaying the evolution of RAS sessions number.
The *RAS/VPN reports* are configured to allow several personalization options: filters, sort group, time range choice etc.



7.2. Session count evolution report

A new graphical report is now available. This report displays the evolution of the total opened sessions. You can choose the period and the *Group mode*.



8. More features

- You can display **the effective user accounts members of a Protected Account**. It allows you to check on the rules that will be applied to each user.
- If the protection is down due to a network issue or server failure, **a new security process** can be enabled in the server *Properties*. Once the *UserLock agents* can successfully communicate again with the servers, **UserLock can force session logoffs** if the user has exceeded his number of authorized simultaneous sessions.
- **A new pop-up technology** has been introduced for the logon/logoff event notifications to replace the *Microsoft Messenger* popup technology that has been deprecated since the introduction of *Windows Vista*.
- The administrator can now **send popup messages to users** from the *User sessions* view in the *UserLock console*.
- You can now display the **Active Directory tree in the User sessions** view.
- **The last user is displayed** in *User sessions view by machines*.
- In the *Agent distribution* view **the last time the agent was successfully checked** is saved in memory and displayed in the **column Last success**.

9. New improvements

- **Performance with many Protected Accounts** has been improved:
 - ✓ *Protected Accounts* view is **loaded faster**,
 - ✓ **Synchronization** of *Protected Account* modifications with the *Backup server* is **more efficient**, (only modified *Protected Accounts* are synchronized).
- **Improvements in user account resolutions.**
 In the previous versions of *UserLock* only the *SID* of each user account was saved in the *UserLock configuration file*. All user accounts were resolved during the service startup. In large environment or when the connectivity to the *Active Directory* was slow, it was leading to a long startup time.

 In *UserLock 6*, the user name is additionally saved in the *UserLock configuration file*. The service no longer requires contacting the *Active Directory* during his startup thus accelerating its initialization.
- **Improvements synchronizing updates from the Active Directory**
 In the previous versions of *UserLock*, user names were only updated when the service was starting. If users were renamed you needed to restart the *UserLock* service to update them.
 In *UserLock 6*, user names are updated every day: you don't need to restart the *UserLock* service.
- The *UserLock* service account **no longer requires administrative rights** on the *UserLock* server.

