UserLock®
What's new in UserLock?

Version 8

www.isdecisions.com

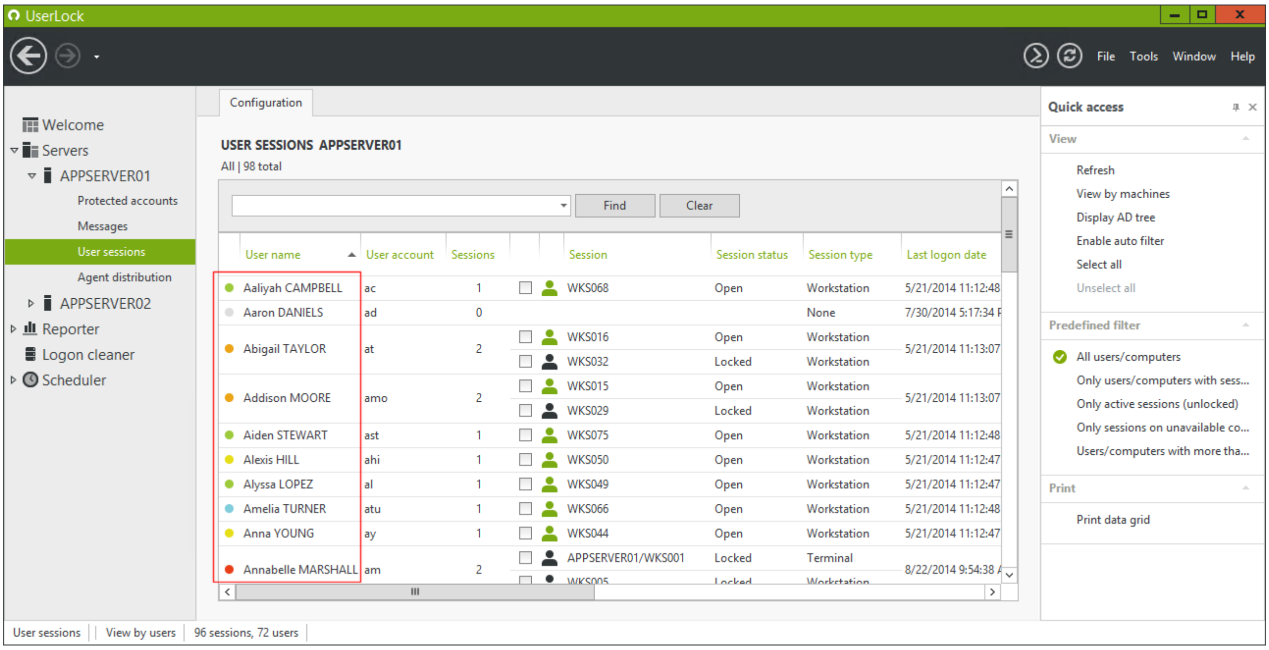
Table Of Contents

1. The User Status, a new risk assessment to better detect suspicious access behavior

UserLock's real-time monitoring now incorporates a **risk indicator** to better identify suspicious or inappropriate access behavior and potential threats to network security.

By correlating each user's access events with their customized authentication controls, the **new 'User Status'** helps deliver a more complete view of your organization's network activity and security risks.

The status assigned to each user evolves according to the users actions when accessing or attempting to access the network. Activity deemed as a **risk** or **high risk** is clearly flagged, alerting administrators in real-time about suspicious, disruptive or unusual logon connections.



USER SESSIONS APPSERVER01

All | 98 total

User name	User account	Sessions		Session	Session status	Session type	Last logon date
● Aaliyah CAMPBELL	ac	1	□	WKS068	Open	Workstation	5/21/2014 11:12:48
● Aaron DANIELS	ad	0				None	7/30/2014 5:17:34 P
● Abigail TAYLOR	at	2	□	WKS016	Open	Workstation	5/21/2014 11:13:07
			□	WKS032	Locked	Workstation	
● Addison MOORE	amo	2	□	WKS015	Open	Workstation	5/21/2014 11:13:07
			□	WKS029	Locked	Workstation	
● Aiden STEWART	ast	1	□	WKS075	Open	Workstation	5/21/2014 11:12:48
● Alexis HILL	ahi	1	□	WKS050	Open	Workstation	5/21/2014 11:12:47
● Alyssa LOPEZ	al	1	□	WKS049	Open	Workstation	5/21/2014 11:12:47
● Amelia TURNER	atu	1	□	WKS066	Open	Workstation	5/21/2014 11:12:48
● Anna YOUNG	ay	1	□	WKS044	Open	Workstation	5/21/2014 11:12:47
● Annabelle MARSHALL	am	2	□	APPSERVER01/WKS001	Locked	Terminal	8/22/2014 9:54:38 A
			□	WKS005	Locked	Workstation	

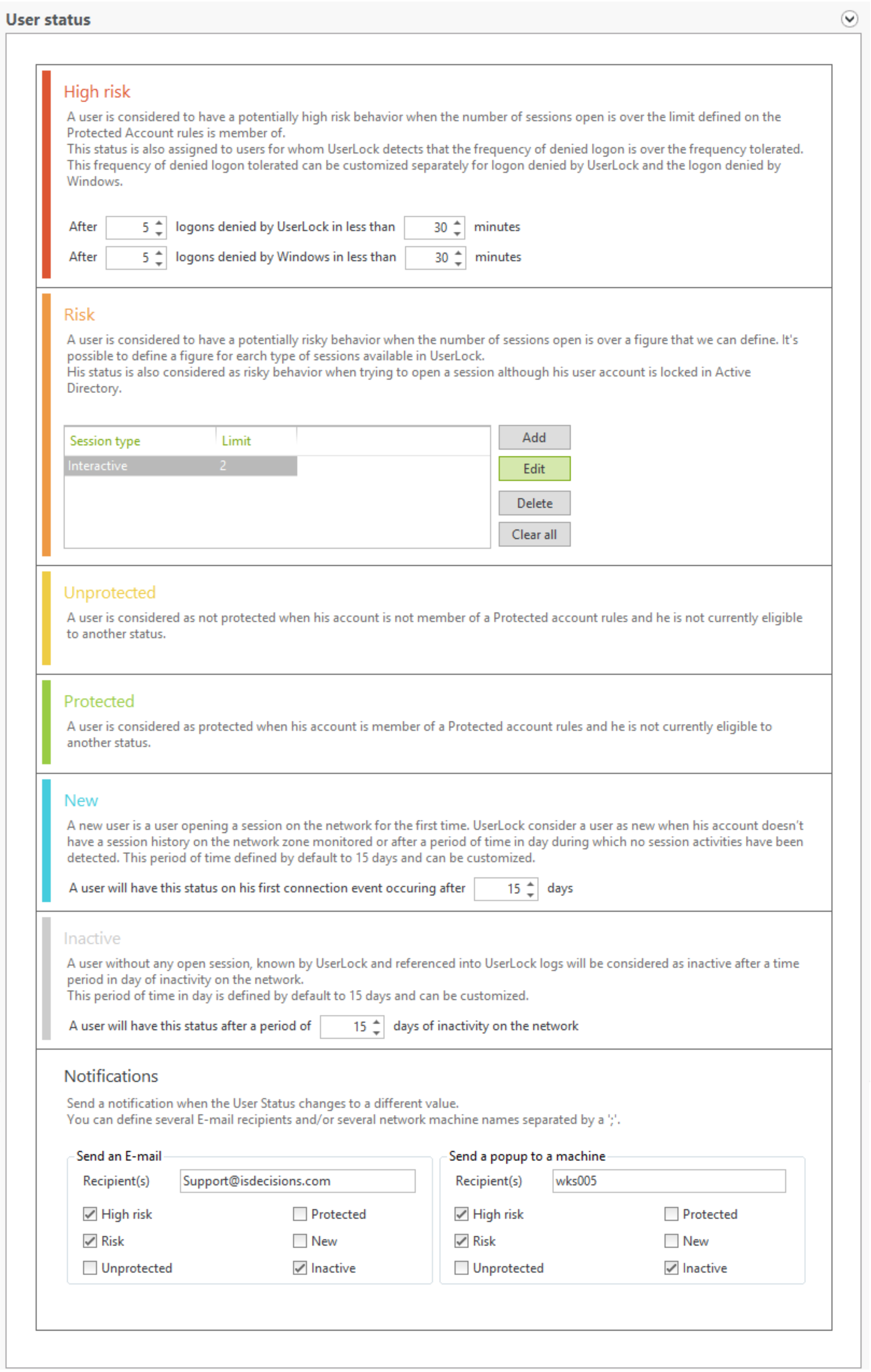
User sessions | View by users | 96 sessions, 72 users

● Inactive ● New ● Unprotected ● Protected ● Risk ● High risk

With UserLock deployed, administrators can detect and react immediately in the case of such behavior, reducing the risk of any security breach.

- Email alerts can also be defined to warn on user status change.
- A history of the User Status changes is kept for auditing and reporting.

The different settings that trigger a change in 'User Status' can be adapted to meet the needs of your organization's network activity. These are managed within the UserLock Server Properties and Alert Notifications.



User status

High risk

A user is considered to have a potentially high risk behavior when the number of sessions open is over the limit defined on the Protected Account rules is member of.
This status is also assigned to users for whom UserLock detects that the frequency of denied logon is over the frequency tolerated.
This frequency of denied logon tolerated can be customized separately for logon denied by UserLock and the logon denied by Windows.

After 5 logons denied by UserLock in less than 30 minutes
After 5 logons denied by Windows in less than 30 minutes

Risk

A user is considered to have a potentially risky behavior when the number of sessions open is over a figure that we can define. It's possible to define a figure for earch type of sessions available in UserLock.
His status is also considered as risky behavior when trying to open a session although his user account is locked in Active Directory.

Session type	Limit
Interactive	2

Unprotected

A user is considered as not protected when his account is not member of a Protected account rules and he is not currently eligible to another status.

Protected

A user is considered as protected when his account is member of a Protected account rules and he is not currently eligible to another status.

New

A new user is a user opening a session on the network for the first time. UserLock consider a user as new when his account doesn't have a session history on the network zone monitored or after a period of time in day during which no session activities have been detected. This period of time defined by default to 15 days and can be customized.

A user will have this status on his first connection event occuring after 15 days

Inactive

A user without any open session, known by UserLock and referenced into UserLock logs will be considered as inactive after a time period in day of inactivity on the network.
This period of time in day is defined by default to 15 days and can be customized.

A user will have this status after a period of 15 days of inactivity on the network

Notifications

Send a notification when the User Status changes to a different value.
You can define several E-mail recipients and/or several network machine names separated by a ';'.

Send an E-mail

Recipient(s) Support@isdecisions.com

☑ High risk ☐ Protected
☑ Risk ☐ New
☐ Unprotected ☑ Inactive

Send a popup to a machine

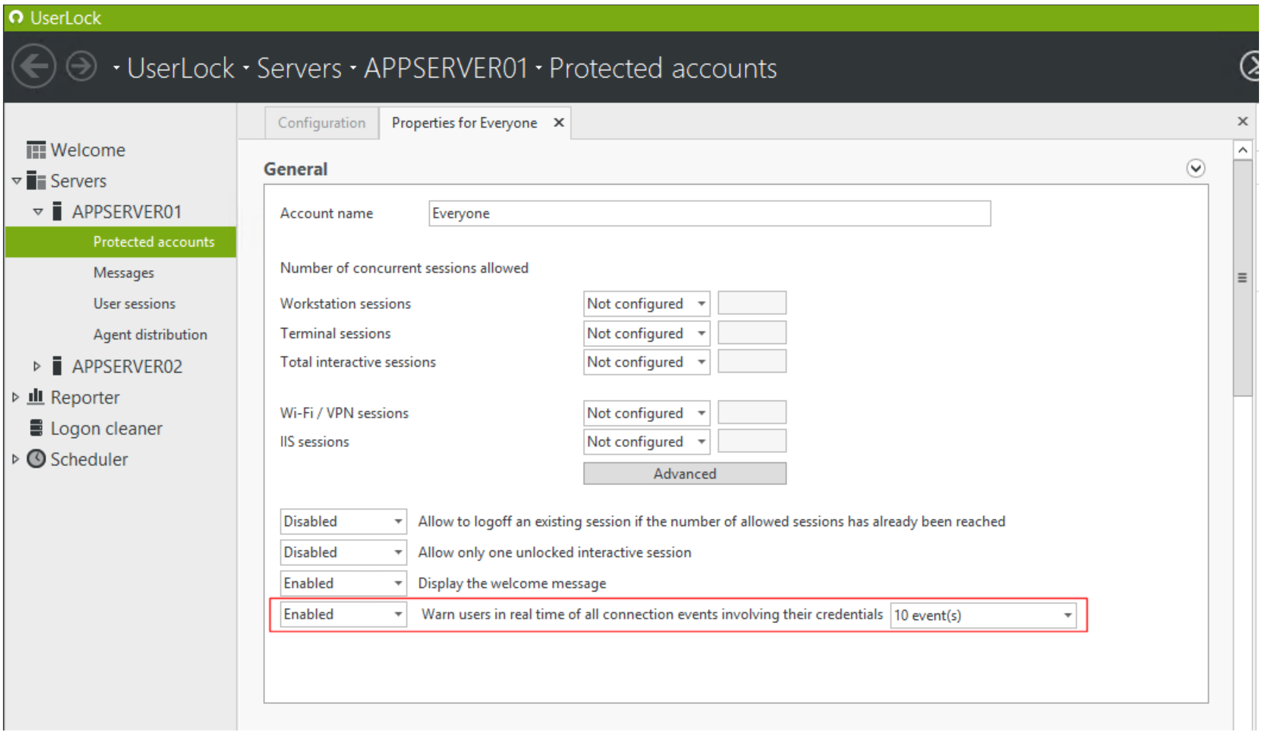
Recipient(s) wks005

☑ High risk ☐ Protected
☑ Risk ☐ New
☐ Unprotected ☑ Inactive

2. Real-Time Alerts on credential-based-attacks

UserLocks' notification system now alerts users in real-time when their own credentials are used – successfully or not – to connect to the network. Users will be able to assess the situation and inform their IT department who can react immediately to any fraudulent use of compromised credentials.

You can find this new feature called "Warn users in real time of all connection events involving their credentials" in Protected account settings, on the first section "General".



UserLock

UserLock · Servers · APPSERVER01 · Protected accounts

- Welcome
- Servers
  - APPSERVER01
    - Protected accounts
    - Messages
    - User sessions
    - Agent distribution
  - APPSERVER02
- Reporter
- Logon cleaner
- Scheduler

Configuration | Properties for Everyone

General

Account name: Everyone

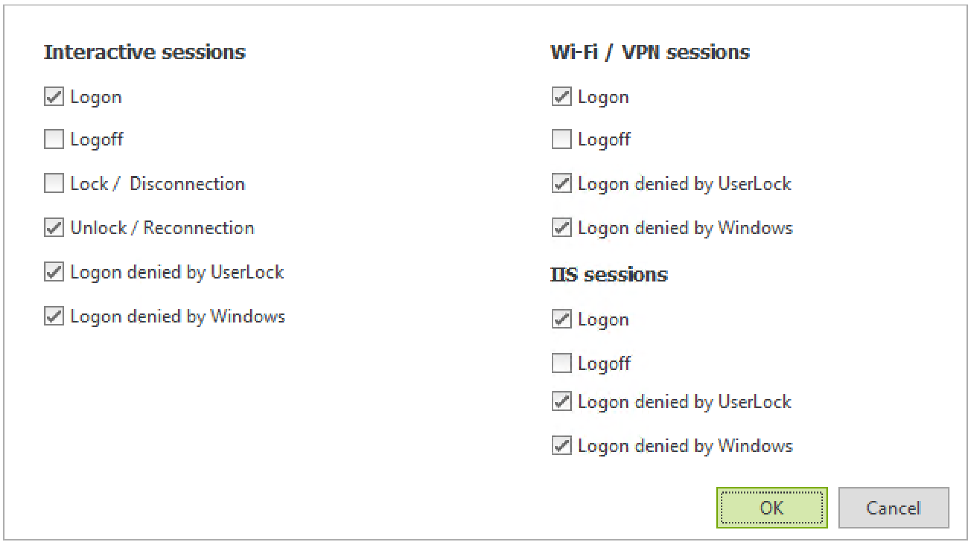
Number of concurrent sessions allowed

Workstation sessions	Not configured
Terminal sessions	Not configured
Total interactive sessions	Not configured
Wi-Fi / VPN sessions	Not configured
IIS sessions	Not configured

Advanced

Disabled	Allow to logoff an existing session if the number of allowed sessions has already been reached
Disabled	Allow only one unlocked interactive session
Enabled	Display the welcome message
Enabled	Warn users in real time of all connection events involving their credentials 10 event(s)

Events triggering the pop-up notification to the credentials owner can be set for all members of the Protected account rule from dropdown list:



Interactive sessions

☑ Logon

☐ Logoff

☐ Lock / Disconnection

☑ Unlock / Reconnection

☑ Logon denied by UserLock

☑ Logon denied by Windows

Wi-Fi / VPN sessions

☑ Logon

☐ Logoff

☑ Logon denied by UserLock

☑ Logon denied by Windows

IIS sessions

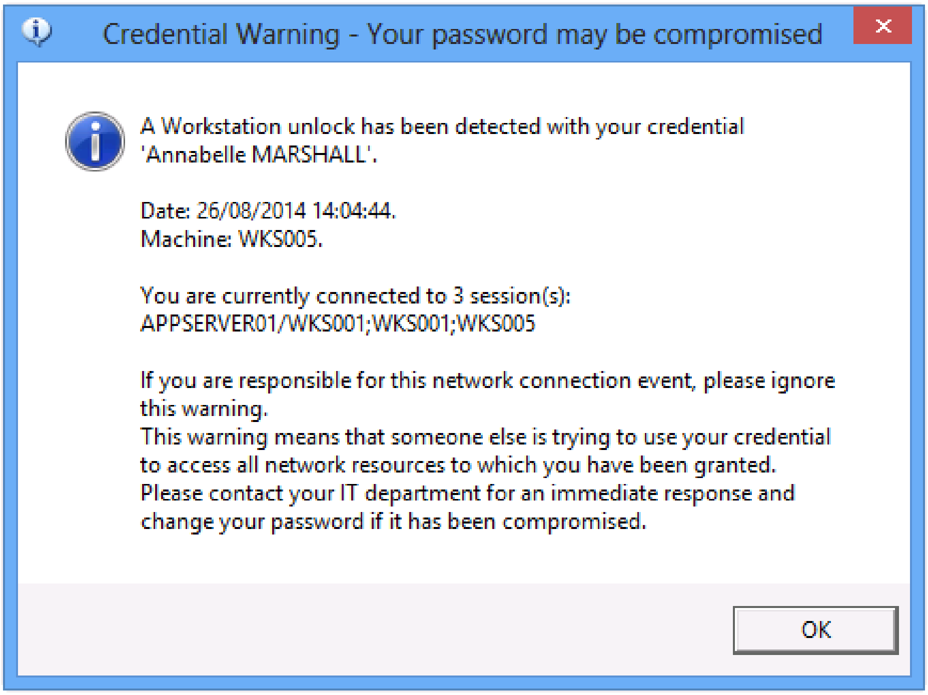
☑ Logon

☐ Logoff

☑ Logon denied by UserLock

☑ Logon denied by Windows

When UserLock detects any selected event from this list occurring for the credentials of a user member from this rule, a Warning message will be displayed to all other current active sessions of the credentials owner:



Credential Warning - Your password may be compromised

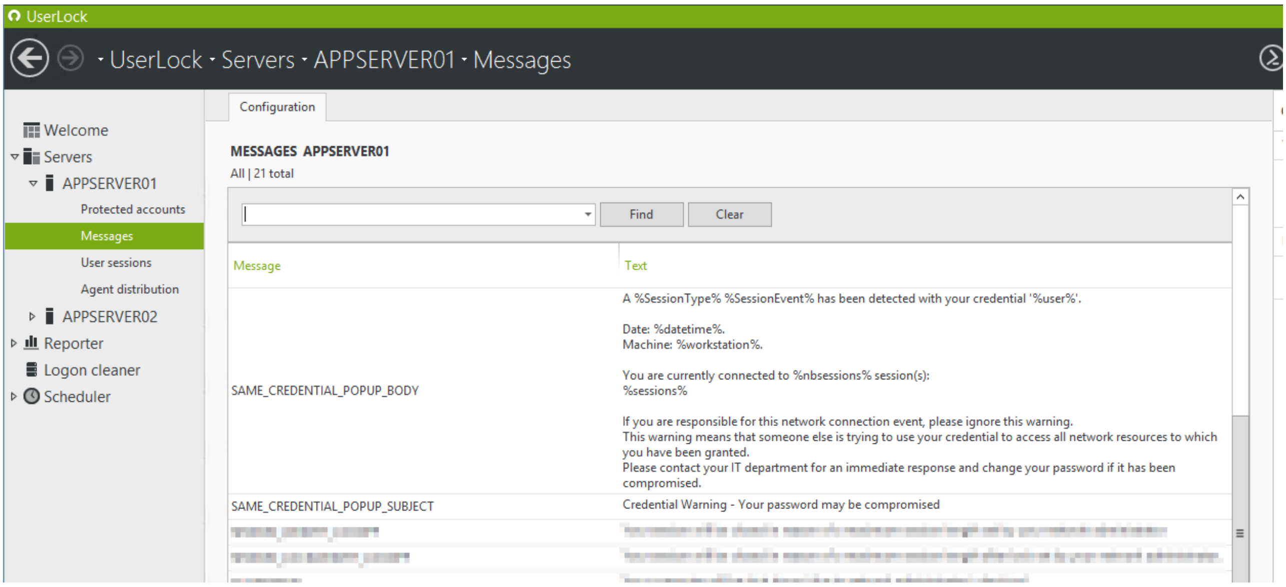
A Workstation unlock has been detected with your credential 'Annabelle MARSHALL'.

Date: 26/08/2014 14:04:44.
Machine: WKS005.

You are currently connected to 3 session(s):
APPSERVER01/WKS001;WKS001;WKS005

If you are responsible for this network connection event, please ignore this warning.
This warning means that someone else is trying to use your credential to access all network resources to which you have been granted.
Please contact your IT department for an immediate response and change your password if it has been compromised.

The subject and the content of this warning message can be fully personalized to suit your organization environment.



MESSAGES APPSERVER01
All | 21 total

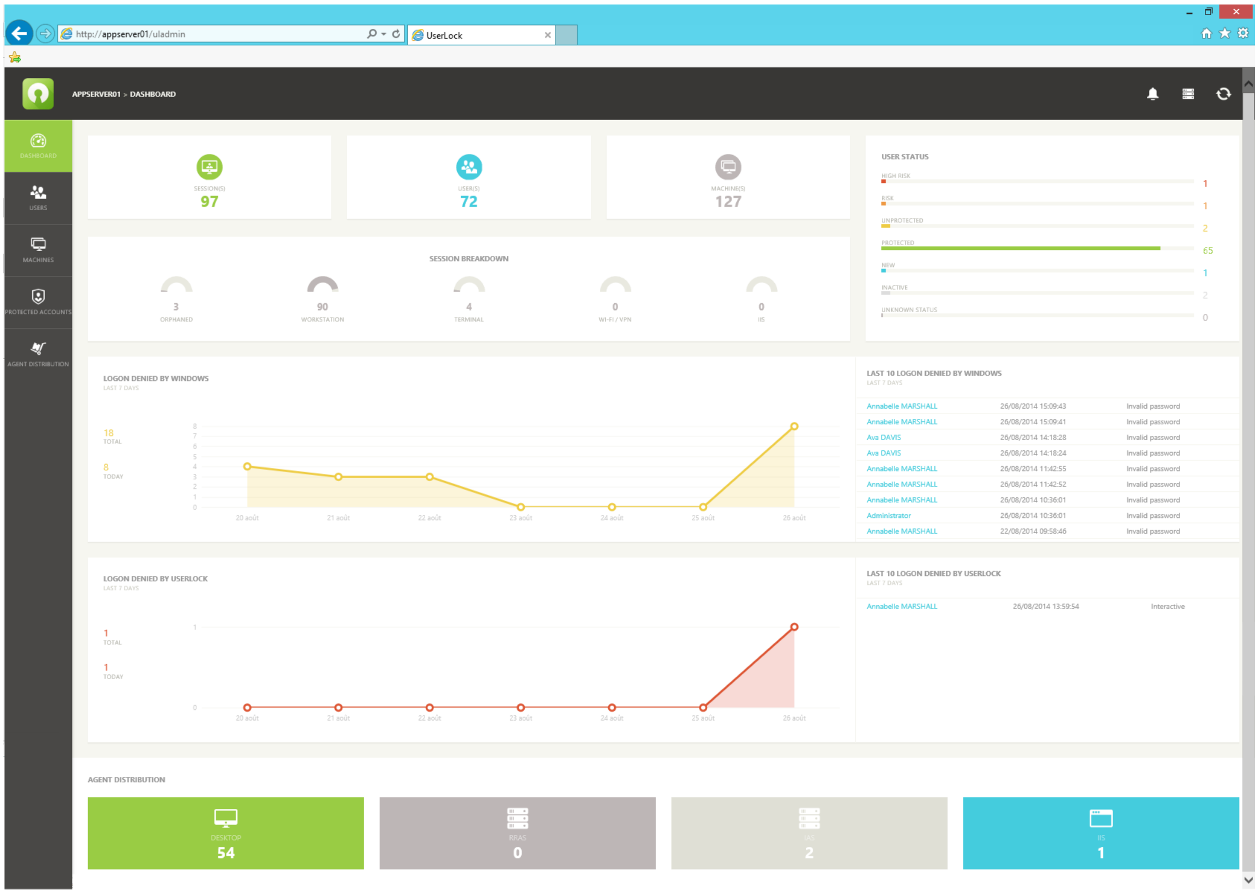
Message	Text
SAME_CREDENTIAL_POPUP_BODY	A %SessionType% %SessionEvent% has been detected with your credential '%user%'. Date: %datetime%. Machine: %workstation%. You are currently connected to %nbsessions% session(s): %sessions% If you are responsible for this network connection event, please ignore this warning. This warning means that someone else is trying to use your credential to access all network resources to which you have been granted. Please contact your IT department for an immediate response and change your password if it has been compromised.
SAME_CREDENTIAL_POPUP_SUBJECT	Credential Warning - Your password may be compromised
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

3. A new Web Console to provide rapid response from any device

The UserLock web interface allows IT to manage network access security remotely. **A redesign has helped facilitate the administration of UserLock from any device: mobile, tablet or computer enabling a rapid response to inappropriate access and mitigation against the insider threat.**

Unlike the typical complicated solutions designed for IT users, we spend considerable effort and energy on incorporating innovative and simple UX to help meet the expectations of today's more consumer driven tech users.

This new Web console will enrich UserLock user experience thanks to its touch ready technology, comprehensive and ergonomic navigation and graphical dashboards.



LAST 10 LOGON DENIED BY WINDOWS
LAST 7 DAYS

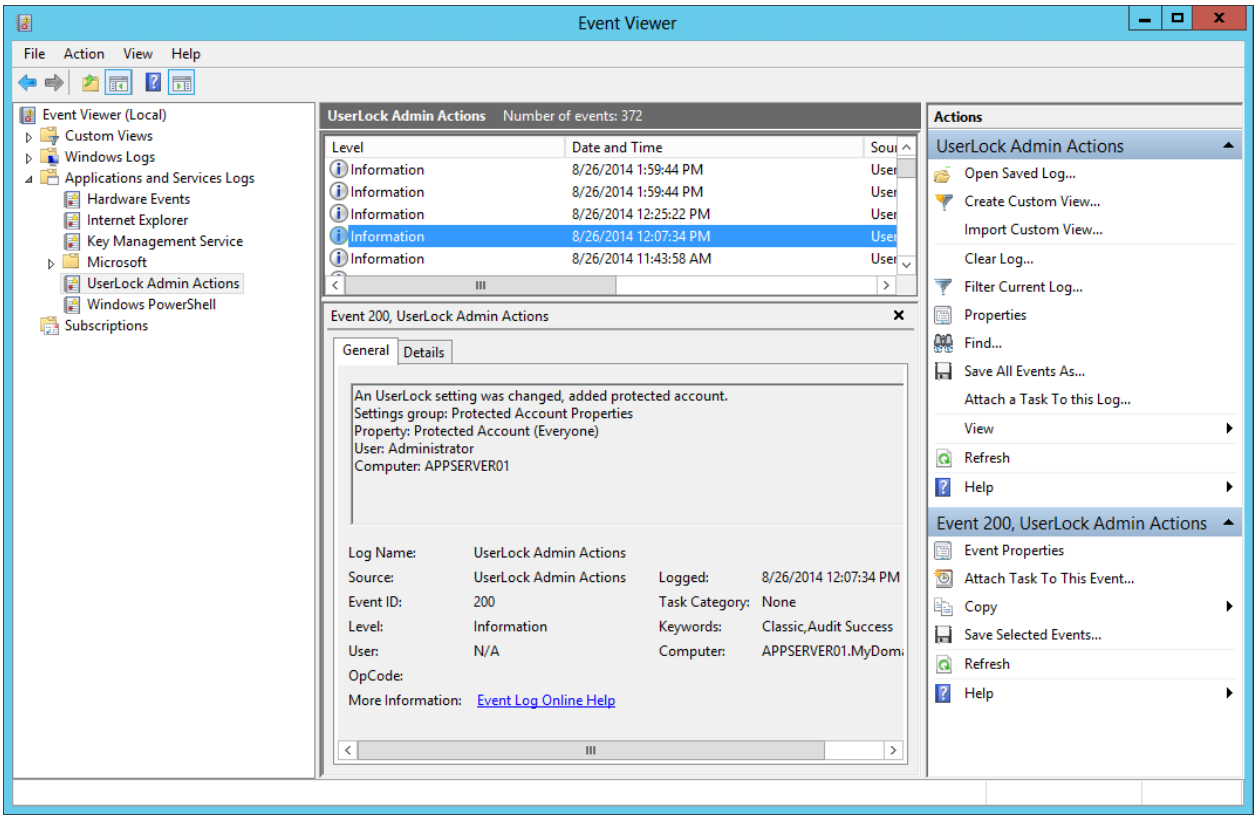
Annabelle MARSHALL	26/08/2014 15:09:43	Invalid password
Annabelle MARSHALL	26/08/2014 15:09:41	Invalid password
Ava DAVIS	26/08/2014 14:18:28	Invalid password
Ava DAVIS	26/08/2014 14:18:24	Invalid password
Annabelle MARSHALL	26/08/2014 11:42:55	Invalid password
Annabelle MARSHALL	26/08/2014 11:42:52	Invalid password
Annabelle MARSHALL	26/08/2014 10:36:01	Invalid password
Administrator	26/08/2014 10:36:01	Invalid password
Annabelle MARSHALL	22/08/2014 09:58:46	Invalid password

LAST 10 LOGON DENIED BY USERLOCK
LAST 7 DAYS

Annabelle MARSHALL	26/08/2014 13:59:54	Interactive

4. Privileged User Monitoring

UserLock now protects against any abuse from its privileged users (UserLock System Administrators) who manage UserLock's own settings, logs and policy rules.
All modifications are now stringently monitored, audited and archived in a Windows Application event log.



UserLock Admin Actions Number of events: 372

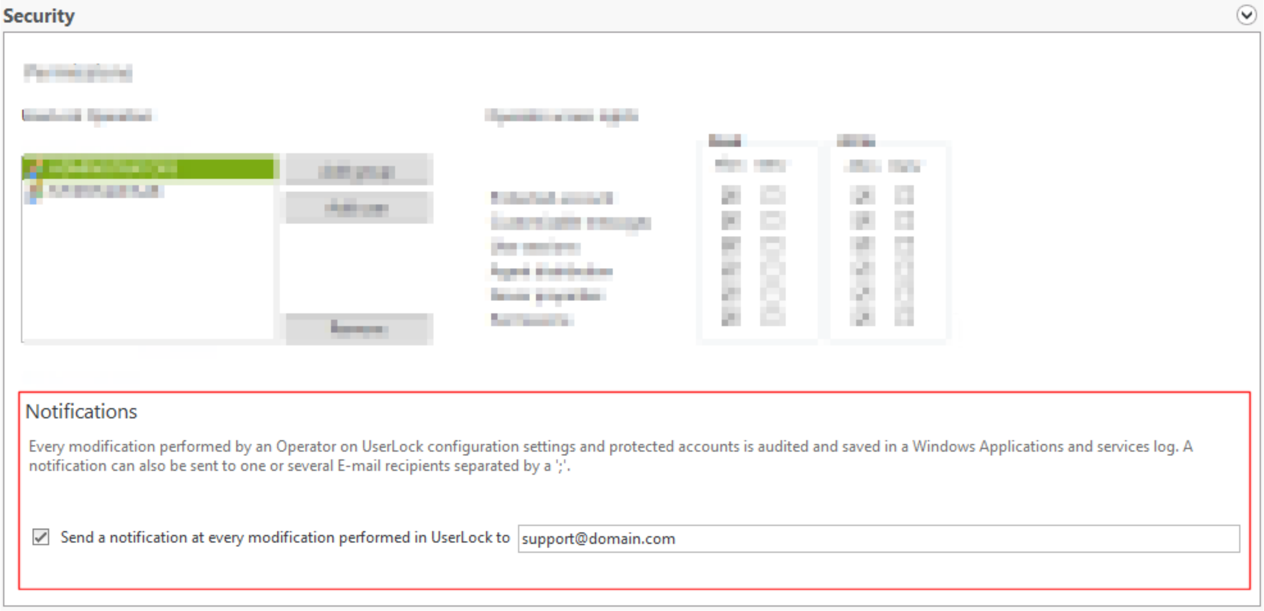
Level	Date and Time	Sou
Information	8/26/2014 1:59:44 PM	User
Information	8/26/2014 1:59:44 PM	User
Information	8/26/2014 12:25:22 PM	User
Information	8/26/2014 12:07:34 PM	User
Information	8/26/2014 11:43:58 AM	User

Event 200, UserLock Admin Actions

An UserLock setting was changed, added protected account.
Settings group: Protected Account Properties
Property: Protected Account (Everyone)
User: Administrator
Computer: APPSERVER01

Log Name:	UserLock Admin Actions		
Source:	UserLock Admin Actions	Logged:	8/26/2014 12:07:34 PM
Event ID:	200	Task Category:	None
Level:	Information	Keywords:	Classic,Audit Success
User:	N/A	Computer:	APPSERVER01.MyDom
OpCode:			
More Information:	Event Log Online Help		

Additionally, an alert can be triggered for any setting or policy modification through the Security Section of the UserLock Server Properties:



Notifications

Every modification performed by an Operator on UserLock configuration settings and protected accounts is audited and saved in a Windows Applications and services log. A notification can also be sent to one or several E-mail recipients separated by a ';'.

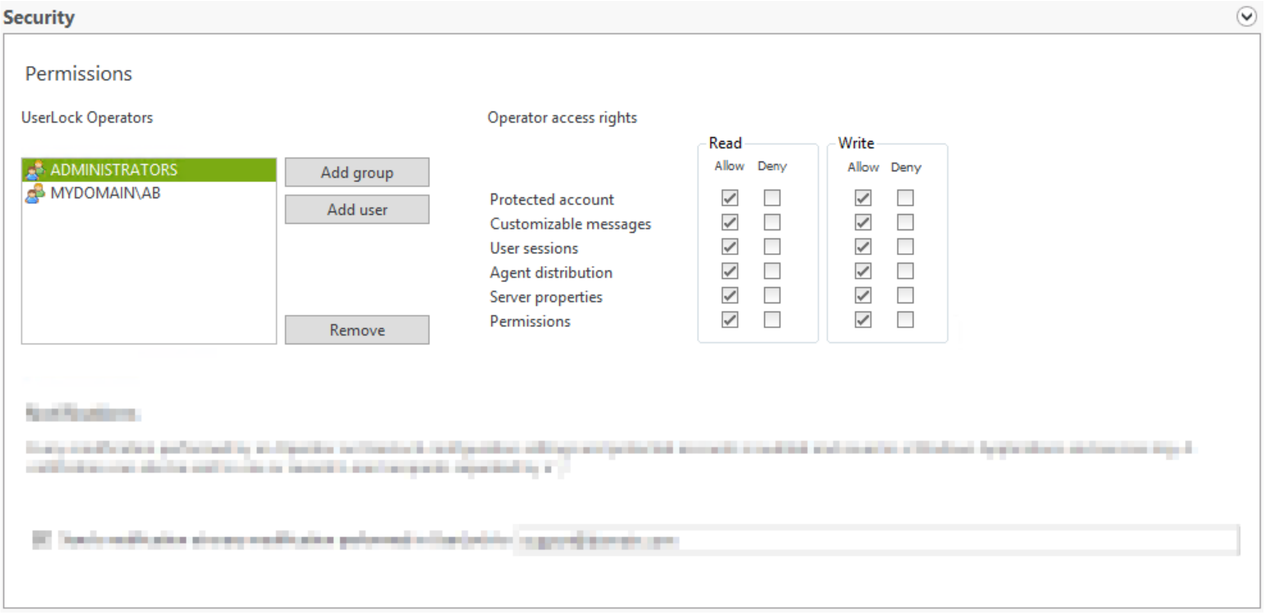
☑ Send a notification at every modification performed in UserLock to support@domain.com

5. More granularity in UserLock administration permissions

UserLock 8 now offers **further granularity when setting permission rights for privileged users**. Access to the different features is split on two privileges, 'Read' to display the section information and 'Write' which authorizes modifications.

In parallel with the new monitoring of all privilege user actions, this **delegated administration feature** allows organizations to extend the administration and management of UserLock across different trusted users.

Depending on the specific privileges assigned to the user, several operators can now manage UserLock and create and enforce policies to meet their business requirements and the changing needs of their organization.



ADMINISTRATORS
MYDOMAIN\AB

Operator access rights

	Read		Write	
	Allow	Deny	Allow	Deny
Protected account	☑	□	☑	□
Customizable messages	☑	□	☑	□
User sessions	☑	□	☑	□
Agent distribution	☑	□	☑	□
Server properties	☑	□	☑	□
Permissions	☑	□	☑	□

[redacted]

The securing of all system administrators actions ensures organizations can follow and audit the different modifications made by different users who have been granted permission rights to manage UserLock. This answers the need for many major regulations and compliance requirements.

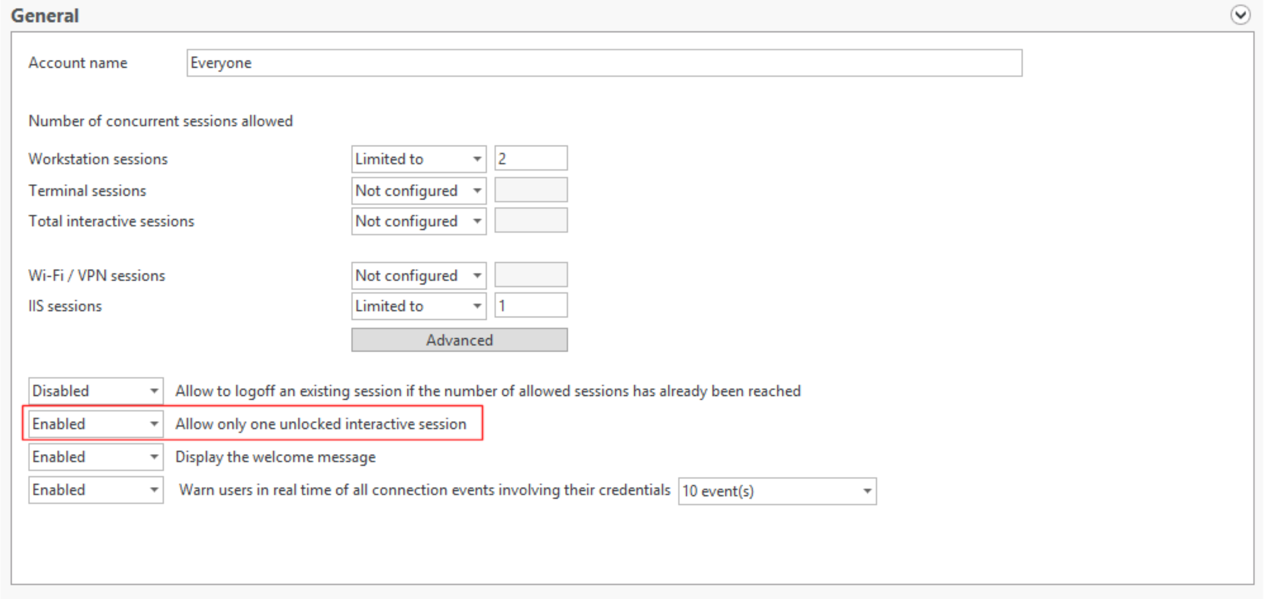
6. Single Active Session

UserLock 8 helps further minimize the security risk from concurrent logins while offering more flexibility to improve your employees' productivity.

UserLock allows administrators to specify and enforce the number of simultaneous sessions per authenticated user. On exceeding the defined maximum the only option currently offered is to remotely logoff an existing session or abort their new login attempt. As the logoff is forced, any open documents that are not saved are lost.

UserLock 8 introduces **a new flexibility** to its controlled user access policy. **By distinguishing between an active session and a locked session** a user can now open as many interactive sessions as they want but only one can be active at a time (a single active session).

Opening a new session has the immediate effect of locking the previous session if open. Therefore if a user requires access from another location it is no longer necessary to force an immediate logoff on their previous session, **thus avoiding the loss of any unsaved documents**.
Fully integrated with all other existing controls and restrictions, organizations now have even more granularity when customizing their user access policy to meet the needs of their employees and security policies.



General

Account name: Everyone

Number of concurrent sessions allowed

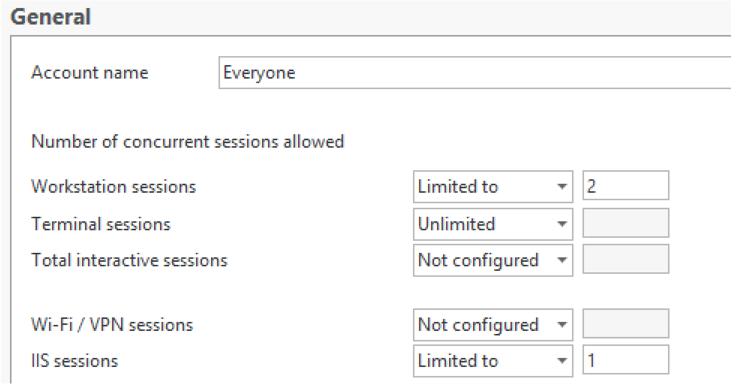
Workstation sessions	Limited to	2
Terminal sessions	Not configured	
Total interactive sessions	Not configured	
Wi-Fi / VPN sessions	Not configured	
IIS sessions	Limited to	1

Disabled	Allow to logoff an existing session if the number of allowed sessions has already been reached
Enabled	Allow only one unlocked interactive session
Enabled	Display the welcome message
Enabled	Warn users in real time of all connection events involving their credentials 10 event(s)

For example, when enabled, a single active session can further minimize the security risk of concurrent logins and reduce network vulnerability to such dangers as password sharing or credential-based-attacks. With direct access to previous sessions protected through automatic locking, an administrator can increase the number of permitted user sessions whilst limiting or even preventing the number of concurrent logins allowed.

7. More…

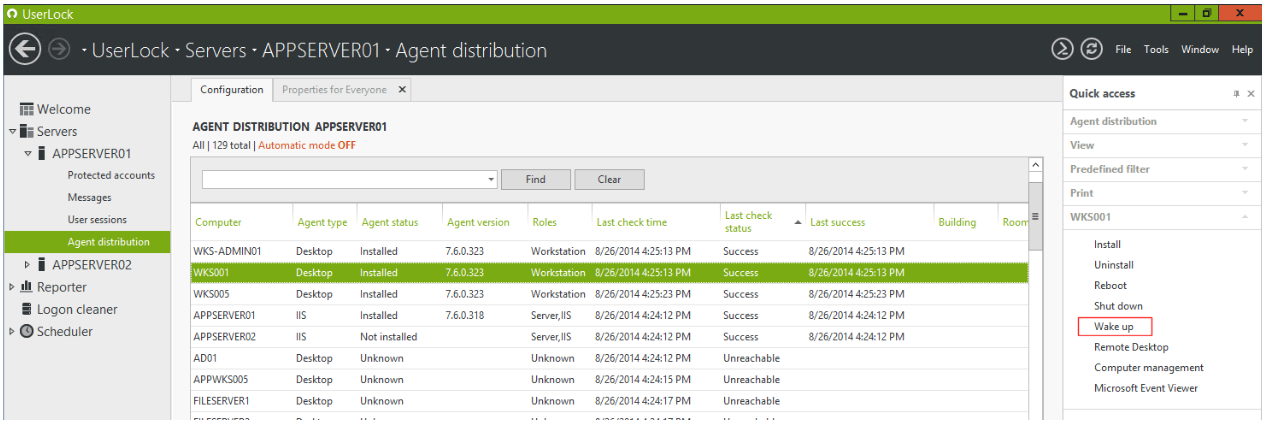
- All restrictions for each protected account have a "Not configured" status based on the GPO model, improving the granularity of restriction priority.



General

Account name	Everyone	
Number of concurrent sessions allowed		
Workstation sessions	Limited to	2
Terminal sessions	Unlimited	
Total interactive sessions	Not configured	
Wi-Fi / VPN sessions	Not configured	
IIS sessions	Limited to	1

- UserLock offers now a Wake on Lan feature to wake up any computer which has the technology requirements.



AGENT DISTRIBUTION APPSERVER01

All | 129 total | Automatic mode OFF

Computer	Agent type	Agent status	Agent version	Roles	Last check time	Last check status	Last success	Building	Room
WKS-ADMIN01	Desktop	Installed	7.6.0.323	Workstation	8/26/2014 4:25:13 PM	Success	8/26/2014 4:25:13 PM		
WKS001	Desktop	Installed	7.6.0.323	Workstation	8/26/2014 4:25:13 PM	Success	8/26/2014 4:25:13 PM		
WKS005	Desktop	Installed	7.6.0.323	Workstation	8/26/2014 4:25:23 PM	Success	8/26/2014 4:25:23 PM		
APPSERVER01	IIS	Installed	7.6.0.318	Server,IIS	8/26/2014 4:24:12 PM	Success	8/26/2014 4:24:12 PM		
APPSERVER02	IIS	Not installed		Server,IIS	8/26/2014 4:24:12 PM	Success	8/26/2014 4:24:12 PM		
AD01	Desktop	Unknown		Unknown	8/26/2014 4:24:12 PM	Unreachable			
APPWKS005	Desktop	Unknown		Unknown	8/26/2014 4:24:15 PM	Unreachable			
FILESERVER1	Desktop	Unknown		Unknown	8/26/2014 4:24:17 PM	Unreachable			

- Logons denied by Windows are now detected for Terminal, Wi-Fi/VPN and IIS sessions.

- Logons denied by UserLock are now displaying the restriction reason.

- The UserLock service is now logged as NETWORK SERVICE to use less privilege. When some actions required more privileges, the UserLock service will impersonate with the specified account.

- A new diagnostic tool is now available when hitting the "F12" key to facilitate any technical support investigation.

- Database performances have been improved and when database connectivity errors occur during a database insertion, a specific queue conserves data until the insertion process is successfully performed.

- All remote action performances are now performed faster thanks to new multi-thread technologies.

- More information is available in the User session view: Session logon time, last activity time, and Client IP address for all session types; Client Name for interactive & Wi-Fi/VPN sessions.

- Reports can now be filtered by any Active Directory group or Organizational Unit and the Time section offers new relative time criteria to facilitate report generation & schedule.

- Protected Account notification allows more criteria for pop-up and E-mail alerts.

- The User Sessions view by machine is now available on the Backup Server (without AD path/tree options). Note that the "Only sessions on unavailable computers" filter can't be used on this mode.

- Full session synchronization between the Backup Server and the Primary Server is now possible on demand.