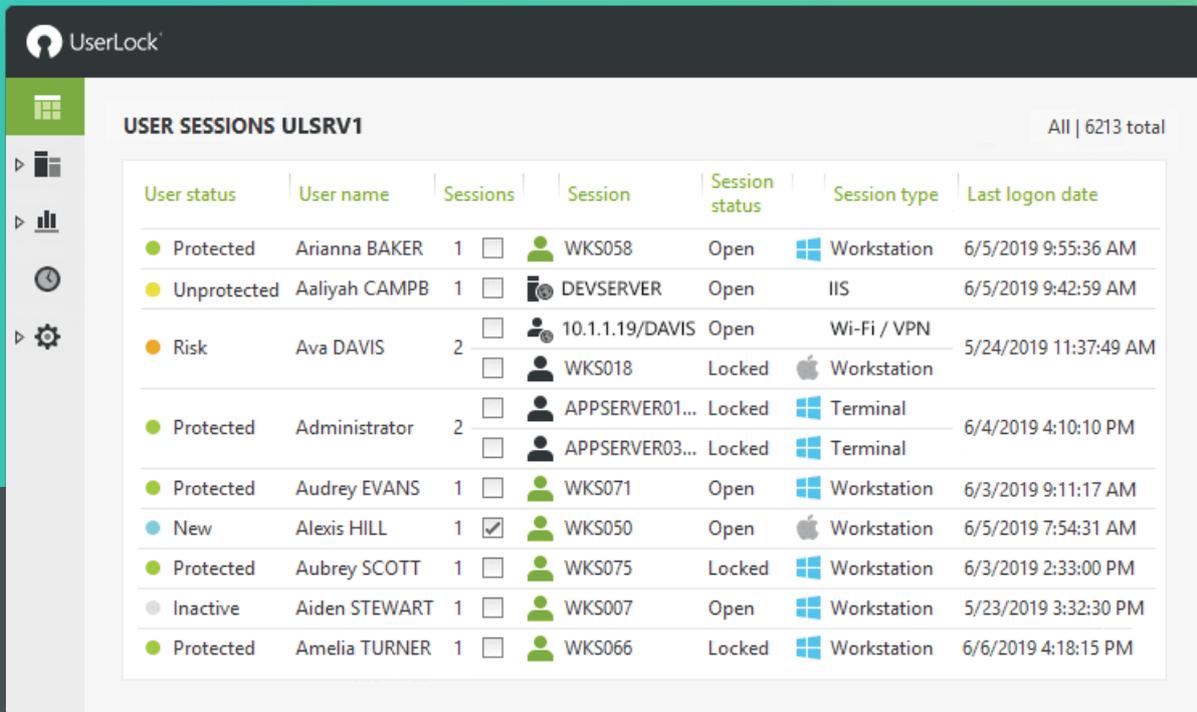


Two-Factor Authentication and Access Management. The Easy Way.



The screenshot shows the UserLock interface with a table titled "USER SESSIONS ULSRV1" and a total of 6213 sessions. The table has the following columns: User status, User name, Sessions, Session, Session status, Session type, and Last logon date. The data is as follows:

User status	User name	Sessions	Session	Session status	Session type	Last logon date
Protected	Arianna BAKER	1	WKS058	Open	Workstation	6/5/2019 9:55:36 AM
Unprotected	Aaliyah CAMPB	1	DEVSERVER	Open	IIS	6/5/2019 9:42:59 AM
Risk	Ava DAVIS	2	10.1.1.19/DAVIS	Open	Wi-Fi / VPN	5/24/2019 11:37:49 AM
			WKS018	Locked	Workstation	
Protected	Administrator	2	APPSERVER01...	Locked	Terminal	6/4/2019 4:10:10 PM
			APPSERVER03...	Locked	Terminal	
Protected	Audrey EVANS	1	WKS071	Open	Workstation	6/3/2019 9:11:17 AM
New	Alexis HILL	1	WKS050	Open	Workstation	6/5/2019 7:54:31 AM
Protected	Aubrey SCOTT	1	WKS075	Locked	Workstation	6/3/2019 2:33:00 PM
Inactive	Aiden STEWART	1	WKS007	Open	Workstation	5/23/2019 3:32:30 PM
Protected	Amelia TURNER	1	WKS066	Locked	Workstation	6/6/2019 4:18:15 PM

The Challenge

Whether it's from exploited users, careless errors, malicious actions or external attacks, your **employees' login credentials are being effortlessly compromised**. What's more, your anti-virus, anti-intrusion, firewall and other technologies are not going to flag anything unusual. Those tools believe that the person accessing your network is exactly who they say they are - an authenticated user with authorized access!

Knowing how prevalent misused credentials are in data breaches, organizations need to **better protect access from everyone within a company** – not just the privileged users/administrators, because any account with access to data that is sensitive, privileged or otherwise valuable is at risk.

| The Solution

By adding two-factor authentication, contextual restrictions and real-time insight around logons, UserLock helps administrators to **secure, monitor and respond to users' access**, even when credentials are compromised.

Furthermore with UserLock, access to any data/resource is now always **identifiable and attributed** to one individual user. This accountability discourages an insider from acting maliciously and makes all users more careful with their actions.

Key Benefits

- **Avoid** network and data breaches
- **Prevent** insider threats
- **Stop** external attacks and lateral movement
- **Put a stop** to password sharing
- **Secure** wireless and remote user access
- **Protect** all user accounts – including the most privileged users
- **Monitor** and interact remotely with any user session
- **Accurate** logon logoff forensics
- **Manage** employee working hours
- **Optimize** shared workstation usage
- **Meet compliance regulations** such as GDPR, PCI DSS, HIPAA, SOX...

ACCESS SECURITY **FAR BEYOND** NATIVE WINDOWS FEATURES

1

Two Factor Authentication

Verify the identity of all users with strong two-factor authentication (2FA) on Windows logon, RDP and VPN connections. Using authenticator applications or programmable hardware tokens such as YubiKey or Token 2, administrators can customize the circumstances under which 2FA is asked.

Multi-factor authentication

For this account, multi-factor authentication is **Enabled**

Workstation connections | Server connections | Skip option

Connection types **Not configured**

Choose to enable MFA on local and remote connections, or for remote connections only. "Not Configured" will apply rules to local and remote sessions.

This account will be asked to use MFA:

- Never
- When logging on from a new IP address (once per address)
- At every logon
- At the first logon of the day (once per IP address)
- Every day(s)
- After day(s) since last logon from this

MFA events statistics

MFA successful	132
MFA cancelled	33
MFA failed	10
MFA help request	2
Configuration skipped	1

2 Scan the QR Code

2

Contextual Access Policy and Restrictions

Restrictions can be established to limit when an account can logon, from which machines, devices, country or IP addresses, using only approved session types (including Wi-Fi, VPN and IIS) and number of concurrent sessions, helping to reduce the risk of inappropriate use.

User status	User name	Session status	Session type
Protected	Arianna BAKER	Open	Workstation
Unprotected	Aaliyah CAMPB	Open	IIS
Risk	Ava DAVIS	Open	Wi-Fi / VPN
		Locked	Workstation
Protected	Administrator	Locked	Terminal
		Loc	
Protected	Audrey EVANS	Op	
New	Alexis HILL	Op	

Number of concurrent sessions allowed	
Workstation sessions	Limited to 2
Terminal sessions	Limited to 0
Total interactive sessions	Not configured
Wi-Fi / VPN sessions	Limited to 1
IIS sessions	Not configured

Number of initial access points allowed	
Initial access points	Limited to 1

Session	Session status	Session type
WKS058	Open	Workstation
WKS068	Open	Workstation
WKS011	Open	Workstation
WKS018	Locked	Workstation
APPSERVER01	Locked	Terminal
APPSERVER03	Lo	
WKS071	Op	

WORKING HOURS BY WEEK
User: Carol Lee

Last logon date	Last logoff date
24/09/2019 18:02:58	24/09/2019 18:04:52
24/09/2019 14:39:13	24/09/2019 14:43:33
24/09/2019 13:05:55	25/09/2019 15:14:44

3

Real Time Monitoring and Reporting

Every logon is monitored and tested against existing policies to determine if a logon should be allowed. Full visibility gives insight into any anomalous account behavior that may indicate a potential threat. A centralized audit helps ensure detailed and accurate insights about who was connected, from which system(s), since what time, for how long, etc.

4

IT and End-User Alerting

Notify IT and the user themselves of inappropriate logon activity and failed attempts.

Notifications

Popup

Send a popup when selected events are detected

Enabled ▼

Recipient(s)

webmaster@company

Event(s) selected

6 event(s)

	Interactive sessions	Wi-Fi / VPN sessions	IIS sessions
Logon denied by UserLock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logon denied by Active Directory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logon accepted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logoff	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lock / Disconnected	<input type="checkbox"/>		
Unlock / Reconnection	<input type="checkbox"/>		

OK
Cancel

5

An Immediate Response to Logon Behavior

Allows IT to interact with a suspect session, to lock the console, log off the user, or even block them from further logons.

Alice

- Logoff
- Lock
- Reset
- Send popup
- Remote Desktop

Block a user

Arianna BAKER

Message to display

Your account is blocked.

Close existing sessions and block user

Leave existing sessions open but block us

Block

THE PERFECT ACCESS SECURITY PARTNER FOR WINDOWS ACTIVE DIRECTORY!



Reduce Complexity

Works seamlessly alongside your existing investment in Active Directory. No modifications are made to accounts, structure or schema.



Powershell Integration

Helps expedite and/or schedule certain tasks and execute personalized requests on the information within UserLock.



Avoid User Disruption

Easily adopted by end-users with the best balance of security and usability.



Backup

A UserLock backup server can be installed to guarantee failover.



Easy Set-Up

Fast to deploy, UserLock is installed in minutes on a standard Windows Server.



Webhooks & API

Integrate the valuable data managed by UserLock, with other solutions to improve overall IT security management.



Scale Effortlessly

AD Group level controls and an automated deployment engine makes implementation easy for larger user bases.



Configuration

Supported operating systems include Windows Server 2019 and Windows 10.



Cost Effective Security

Accurate and effective security, UserLock maximizes your chances of stopping a threat before it starts.



TRY IT FREE
30 DAYS, FULL VERSION

START A FREE TRIAL

SYSTEM REQUIREMENTS

Domain	<p>Active Directory required (for workgroups, see the Standalone Terminal Server UserLock server type).</p> <p><i>Functional level of forest and domain: Windows Server 2003 or higher.</i></p>
Operating systems	<p>UserLock supports the following operating systems:</p> <ul style="list-style-type: none">➤ For UserLock Server: Windows Server 2008 and above➤ For UserLock Console: Windows 7 and above, Windows Server 2008 and above➤ For workstations to protect: Windows XP and above, Mac El capitan and above➤ For servers to protect: Windows 2003 and above, Citrix, any terminals using RDP sessions or ICA sessions.

➤ FOR ALL INFORMATION ON REQUIREMENTS

ABOUT IS DECISIONS

IS Decisions is a global software company specializing in Security and Access Management. Trusted by over 3400 organizations, it offers proven solutions for both small to medium-sized businesses (SMBs) and large organizations, including some of the most regulated and security-conscious in the world.



IS Decisions

Technopôle IZARBEL - Créaticité Bât. A - BP12 - 64210 Bidart - FRANCE
Phone: +33 5.59.41.42.20 - Fax: +33 5.59.41.42.21
www.isdecisions.com - info@isdecisions.com

Silver
Microsoft
Partner