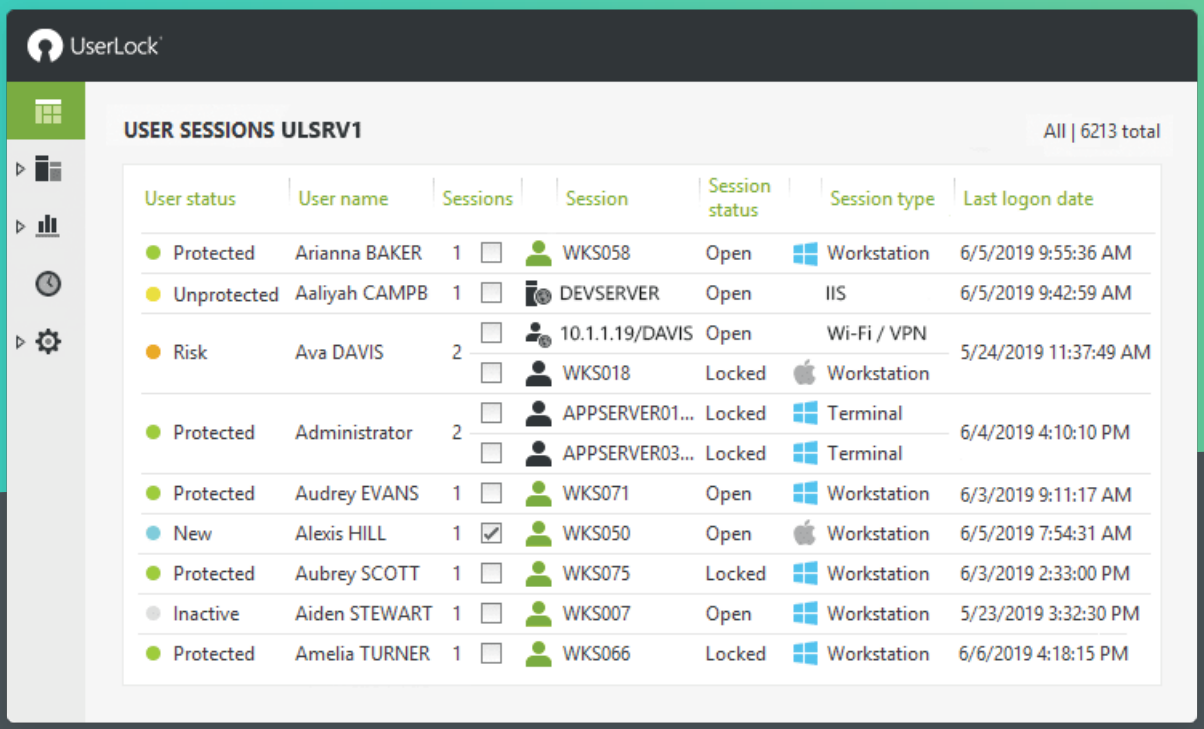
DATASHEET

UserLock

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



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

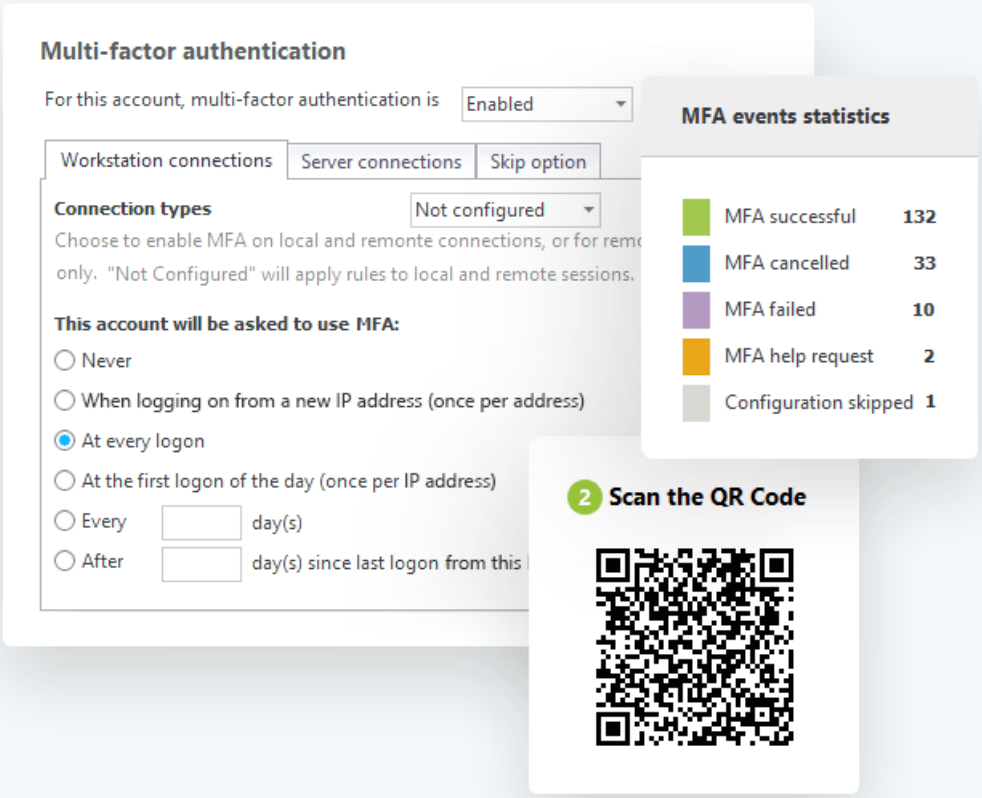
- **Avoid** network and data breaches
- **Prevent** insider threats
- **Stop** external attacks and lateral movement
- **Put a stop** to password sharing
- **Secure** wireless and remote user access
- **Protect** all user accounts – including the most privileged users
- **Monitor** and interact remotely 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

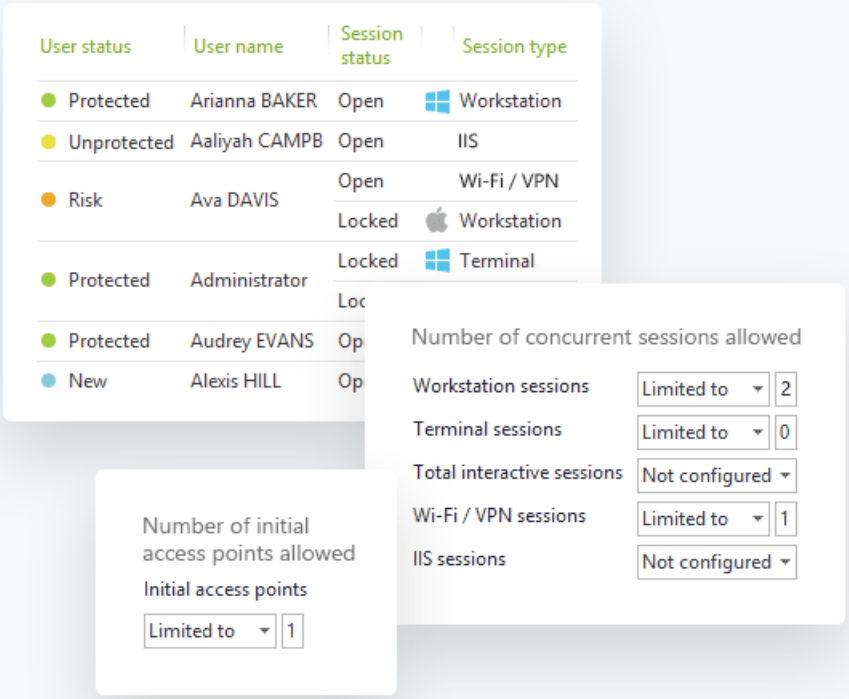
Verify the identity of all users with strong two-factor authentication (2FA) on Windows logon, RDP and VPN connections. Using authenticator applications or programmable hardware tokens such as YubiKey or Token 2, administrators can customize the circumstances under which 2FA is asked.

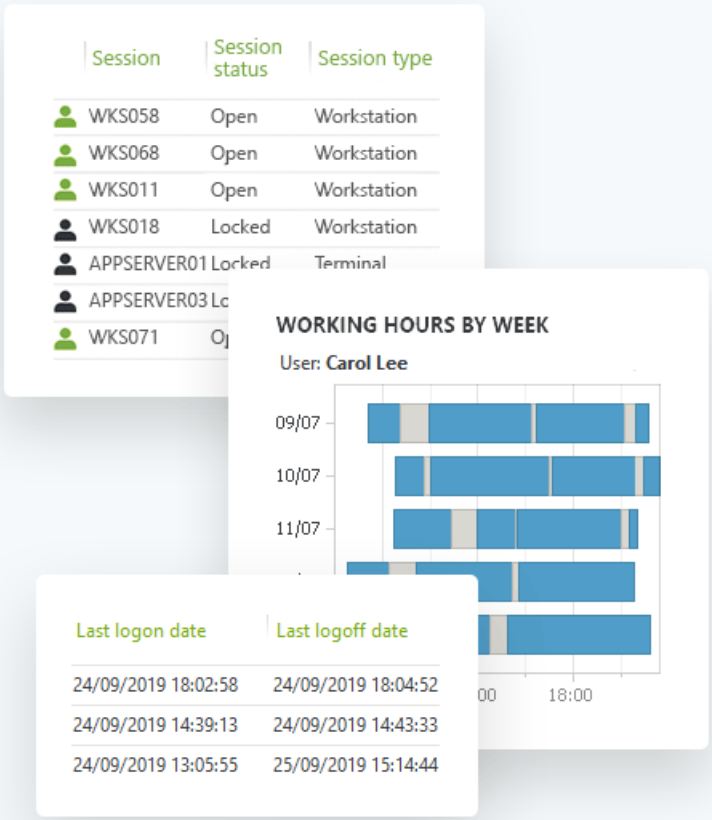


2

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.





3

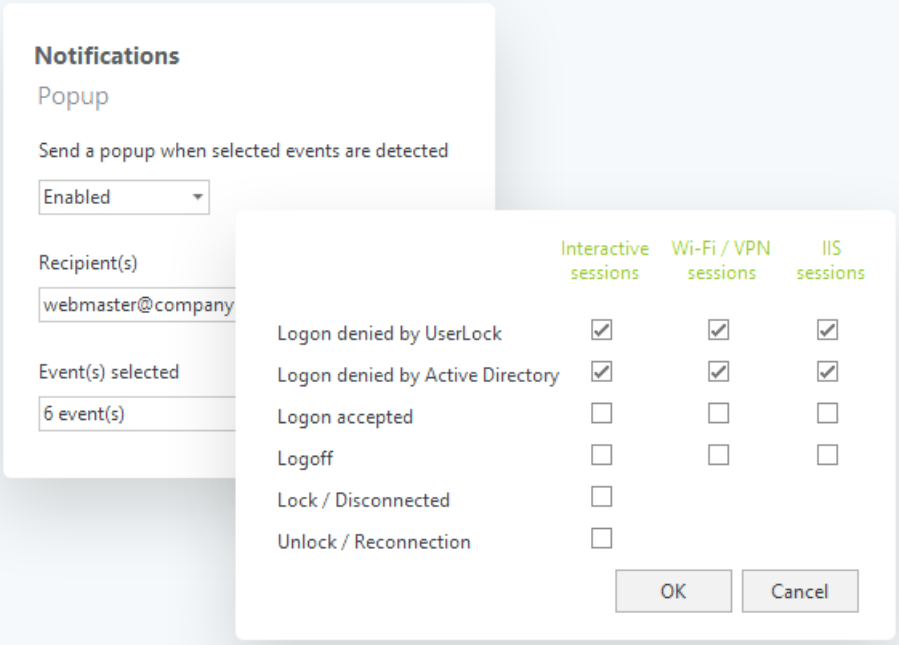
Real Time Monitoring and Reporting

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

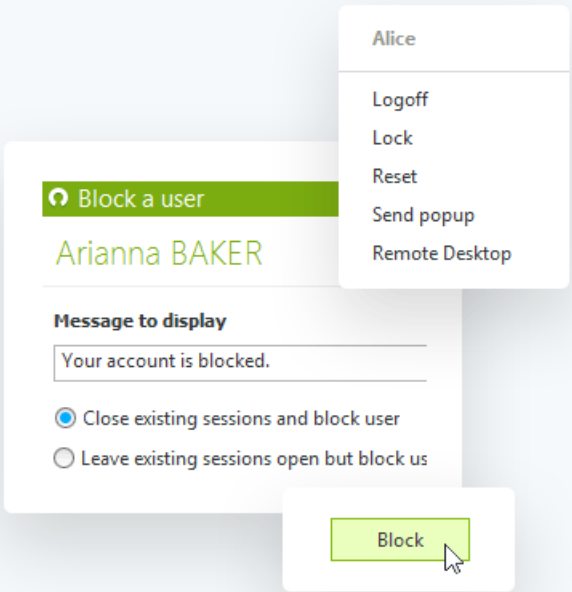
Notify IT and the user themselves of inappropriate logon activity and failed attempts.



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.



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.

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

Easy Set-Up
Fast to deploy, UserLock is installed in minutes on a standard Windows Server.

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

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

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

Backup
A UserLock backup server can be installed to guarantee failover.

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

Configuration
Supported operating systems include Windows Server 2019 and Windows 10.

TRY IT FREE
30 DAYS, FULL VERSION

START A FREE TRIAL

SYSTEM **REQUIREMENTS**

Domain	**Active Directory required (for workgroups, see the Standalone Terminal Server UserLock server type).** *Functional level of forest and domain: Windows Server 2003 or higher.*
Operating systems	UserLock supports the following operating systems: › **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