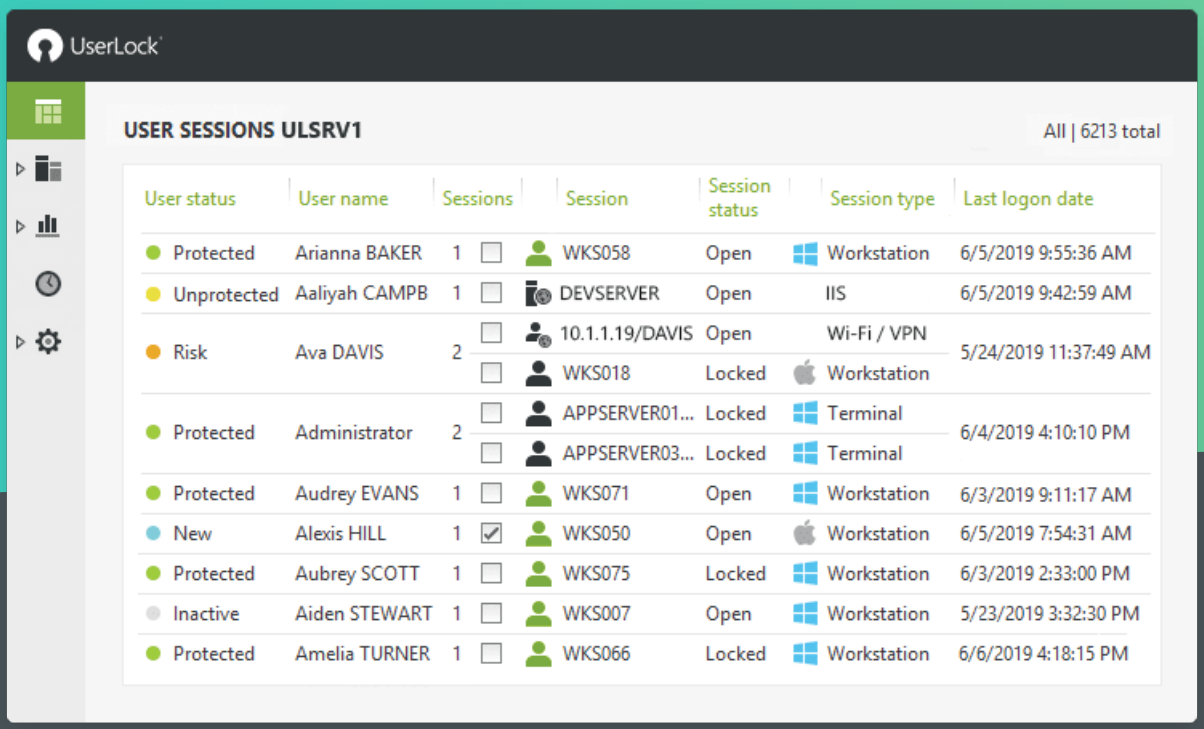
DATASHEET

UserLock

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



The **Challenge**

Whether because of exploited users, careless errors, malicious actions or external attacks, your **employees' login credentials can be effortlessly compromised**. And when they are, your anti-virus, anti-intrusion, firewall and other security technologies won't flag anything unusual. Those tools believe that if the person accessing your network enters the right credentials, then they are exactly who they say they are – an authenticated user with authorized access!

Knowing that the majority of data breaches stem from compromised credentials, organizations need to **better protect access for all employee logins** – not just the privileged users/administrators. Any account with access to data that is sensitive, privileged or otherwise valuable is at risk.

A Comprehensive **Solution**

By adding two-factor authentication (2FA), single sign-on (SSO), contextual restrictions and real-time insight around logon activity, UserLock helps administrators **secure, monitor and respond to user access**, preventing damage before it's done.

And with UserLock, access to any data or 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. It's also necessary for many organizations to fulfill common compliance or cyber-insurance requirements.

Protection Across Common Use Cases

Learn more

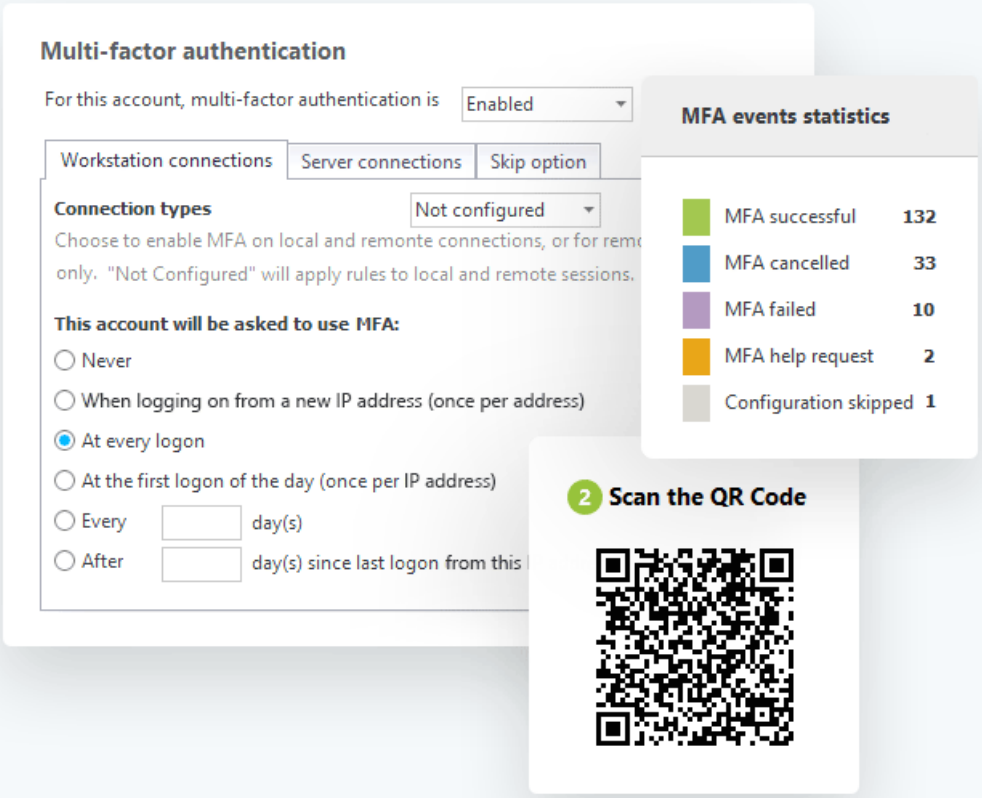
- **Secure** all employee access
- **Secure** privileged access
- **Secure** access to cloud apps
- **Secure** remote access
- **Streamline** session management
- **Get accurate** logon logoff forensics
- **Manage** working hours
- **Meet** compliance & insurance requirements
- **Stop** security breaches

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, Remote Desktop (RDP & RD Gateway), IIS, VPN and Cloud Applications. Using authenticator applications or programmable hardware tokens such as YubiKey or Token 2, administrators can customize the circumstances under which 2FA is asked.

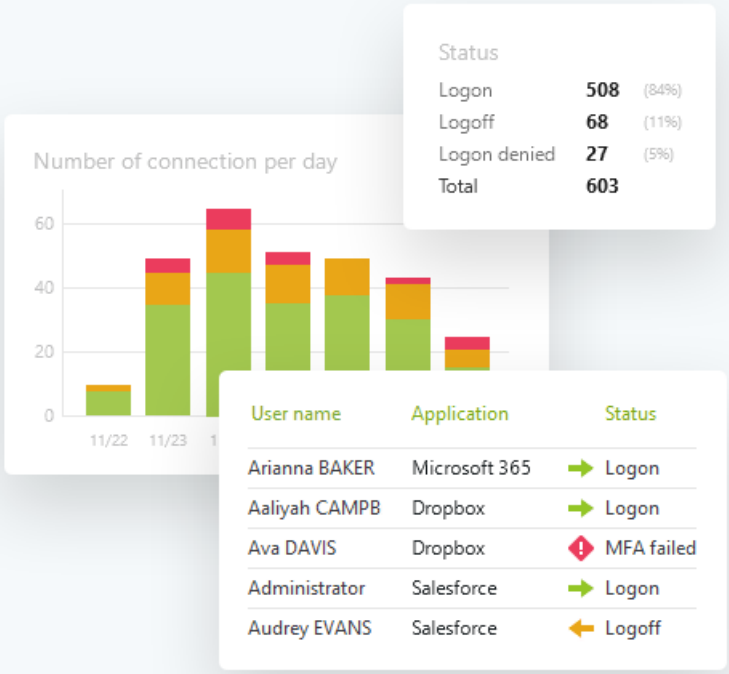


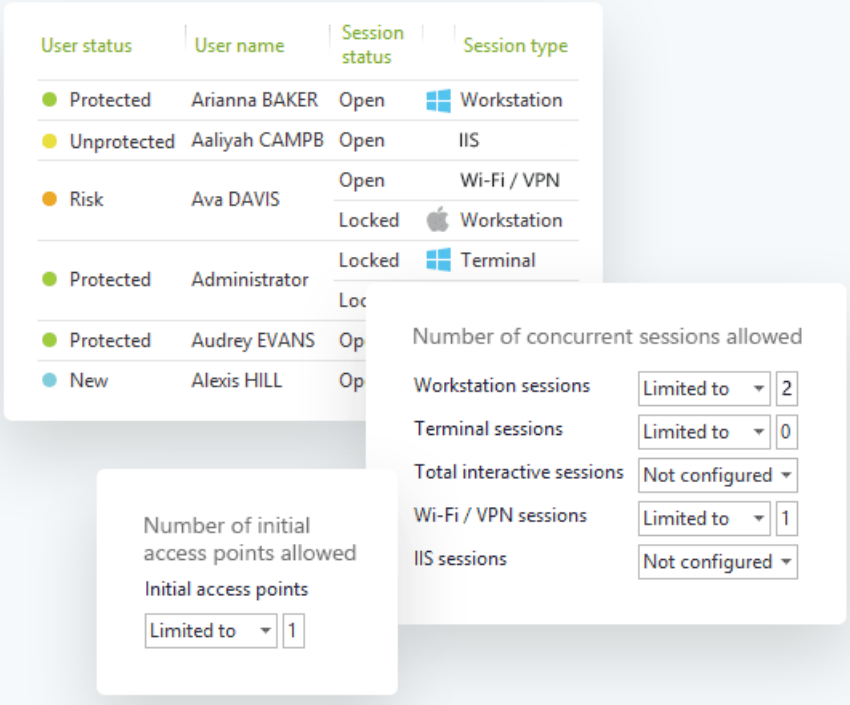
2

Single Sign-On

UserLock Single Sign-On (SSO) gives employees secure and frictionless access to Microsoft 365 and cloud applications – from wherever they work – using only their on-premises Active Directory (AD) credentials with SAML 2.0 federated authentication.

Organizations can retain AD as the authoritative identity provider, while extending it to work with the cloud.





3

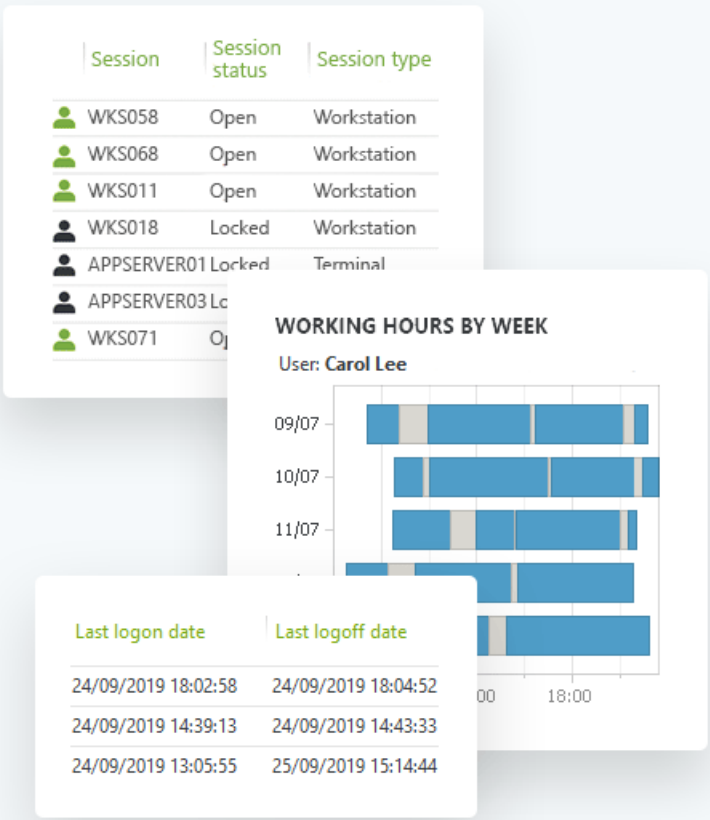
Contextual Access Policy and Restrictions

Administrators can set rules to authorize, deny or limit any login (including remote access) based on contextual factors like machine, location, time, session type, or number of simultaneous connections.

4

Real Time Monitoring and Reporting

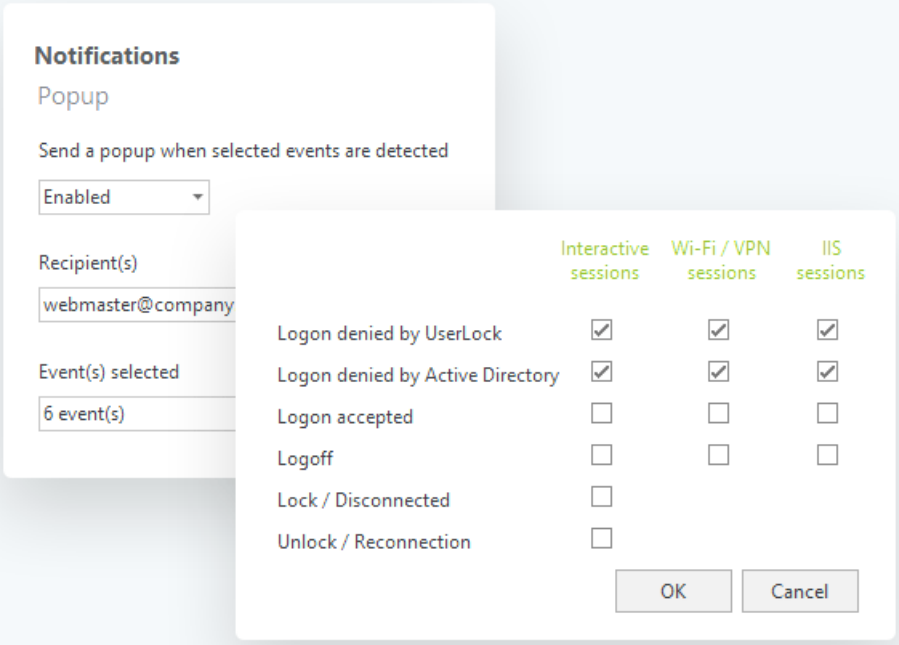
Real-time visibility into all user access gives administrators insights into potential threats and the ability to respond to any session, directly from the console And, a centralized audit for reporting on all AD user login activity allows administrators to report on who was connected, from which system(s), since what time, for how long, etc.



5

IT and End-User Alerts

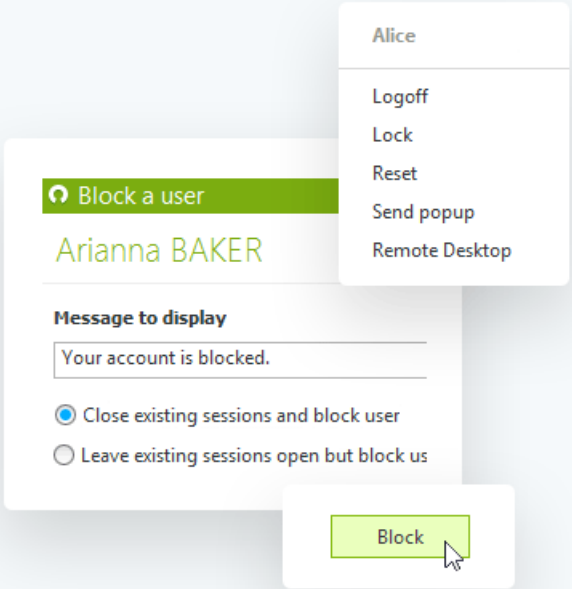
Set up alerts to notify IT and the user themselves of inappropriate logon activity and failed attempts.



6

An Immediate Response to Logon Behavior

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



THE **GO-TO ACCESS MANAGEMENT PARTNER** FOR ON-PREMISES AND HYBRID ACTIVE DIRECTORY ENVIRONMENTS!

Reduce Complexity
Works seamlessly alongside your existing investment in Active Directory, reducing complexity and frustration for IT teams. No modifications are made to accounts, structure or schema.

Easily Adopted
Easily adopted by end-users with the best balance of security and usability. Granular controls allow for customized restrictions that protect access without getting in the way of employee productivity.

Easy Set-Up
Quick to deploy and intuitive to manage, administrators can set up UserLock in minutes on a standard Windows Server.

Scale Effortlessly
AD Group level controls and an automated deployment engine make implementation easy for any number of users.

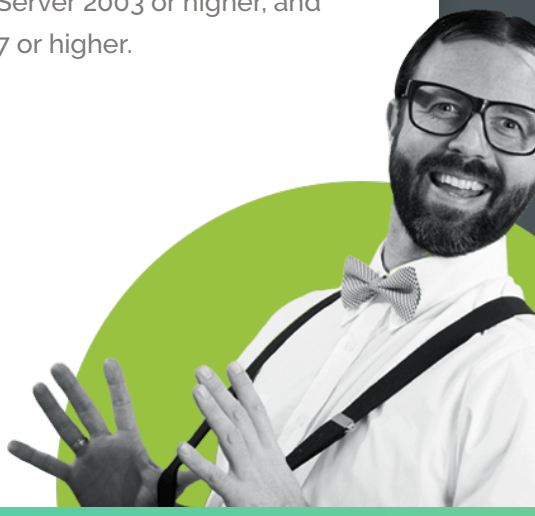
Enables Cost-Effective Security
Building on your investment in AD, UserLock offers additional, effective and affordable security.

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

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

Includes Failover Safeguards
A UserLock backup server can be installed to guarantee failover.

System Requirements
Supported operating systems include Windows Server 2003 or higher, and Windows 7 or higher.



TRY THE FULL VERSION FOR FREE WITH OUR 30 DAYS TRIAL

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 2003 and above › **For UserLock Console**: Windows 7 and above, Windows Server 2003 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 access management and MFA for on-premises and hybrid active directory environments. Trusted by over 3400 organizations, we offer proven solutions for both small to medium-sized businesses (SMBs) and large organizations, including some of the most regulated and security-conscious organizations 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