WHO ARE WE?

IS Decisions makes it easy to manage and secure your Microsoft Windows environment and Active Directory structure.

TRUST AND CONFIDENCE IN **IS DECISIONS**

PROVEN IT SECURITY SOLUTIONS

Used by some of the most regulated and security-conscious organizations.

BARCLAYS

U.S.ARMY

FOR ALL SECTORS, REGARDLESS OF SIZE

Over 3,400 customers from 129 countries.

ZOODFOOD

Teleperformance
each interaction matters

University of Kent

COASTAL
Housing Group

COST-EFFECTIVE CYBER RESILIENCE

Accurate and affordable security that reduces the risk of breaches and compliance fines.

GDPR

PCI DSS COMPLIANT

HIPAA
Health Insurance Portability & Accountability Act

DEPLOYS SWIFTLY, SCALES EFFORTLESSLY & INTUITIVE TO MANAGE

Non-disruptive technology that reduces complexity for both IT Teams and End-Users.

Gold
Microsoft
Partner
Microsoft

FRANCE
CYBER
SECURITY

USERLOCK

UserLock reduces the risk of external attacks, internal security breaches and compliance issues

WHAT DOES **USERLOCK** DO ?

TWO-FACTOR AUTHENTICATION

UserLock makes it easy to enable multi-factor authentication on Windows logon and RDP connections. Verify the identity of all users and secure access to your network.

CONTROL & PROTECT

Set restrictions using the contextual information around a user's logon, to help verify all user's claimed identity, and authorize, deny or limit network access.

DETECT & RESPOND

Real-time monitoring and risk detection tools immediately alert on suspicious logon activity so you and take action quickly.

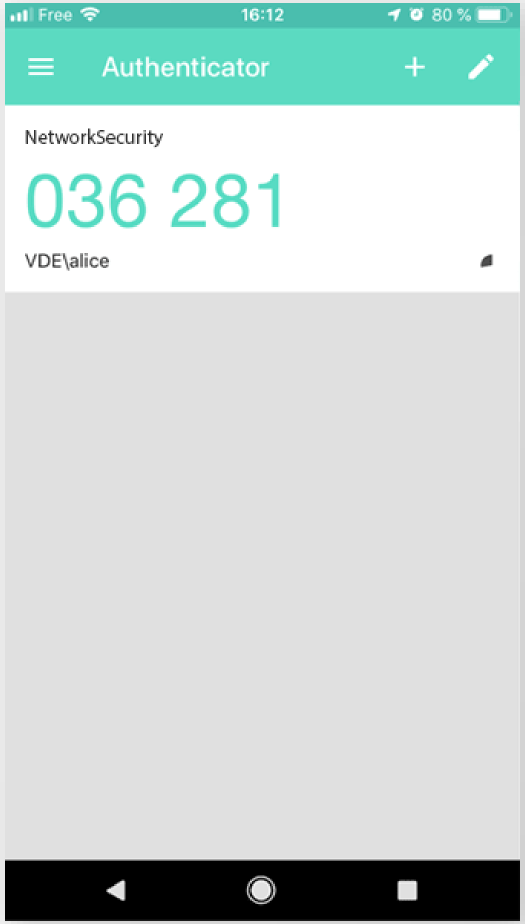
AUDIT & REPORT

A centralized audit on all network logon events provides detailed reports to track down security threats, support forensics and prove regulatory compliance.

TWO-FACTOR AUTHENTICATION

SECURE TWO-FACTOR AUTHENTICATION

UserLock supports MFA through **authenticator applications**. They offer a second factor to better protect access to the network. Relying on cryptographic algorithms for **time-based one-time passwords (TOTP)**, authenticator applications offer the most secure two-factor authentication method.



NetworkSecurity

036 281

VDE\alice

CONTROL & PROTECT

CONTEXT-AWARE RESTRICTIONS

Working alongside **Active Directory** to extend its security, UserLock can apply customized **login restrictions** by user, group or organizational unit (OU). Any logon attempts that don't satisfy these conditions are automatically **blocked**.

ORIGIN

Limit access by location with controls at workstation, device, IP range, organizational unit (OU), department, floor and building levels.

TIME

Limit access to specific timeframes and set daily, weekly or monthly time quotas, maximum session times and idle session time.

SESSION TYPE

Control workstation, terminal, Wi-Fi, VPN and IIS sessions to protect both interactive sessions and network access for remote and mobile users.

SIMULTANEOUS CONNECTIONS

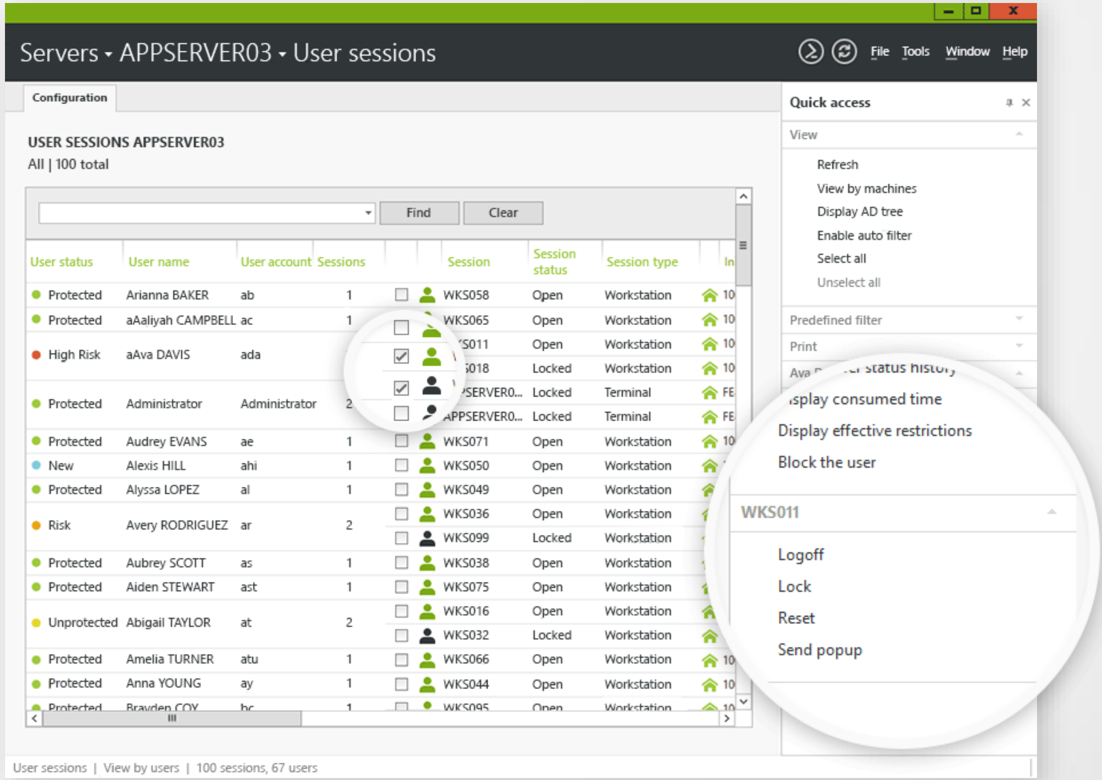
Limit the number of unique entry points and concurrent sessions to prevent simultaneous logins from a single identity.

DETECT & RESPOND

RESPOND TO SUSPICIOUS ACCESS BEHAVIOR

UserLock offers **real-time visibility** and **insight** into all users' logon and logoff activity across an entire Windows Server Active Directory network.

Get **real-time alerts** on specific connection events and **instantly react** to suspicious access behavior.



USER SESSIONS APPSERVER03

All | 100 total

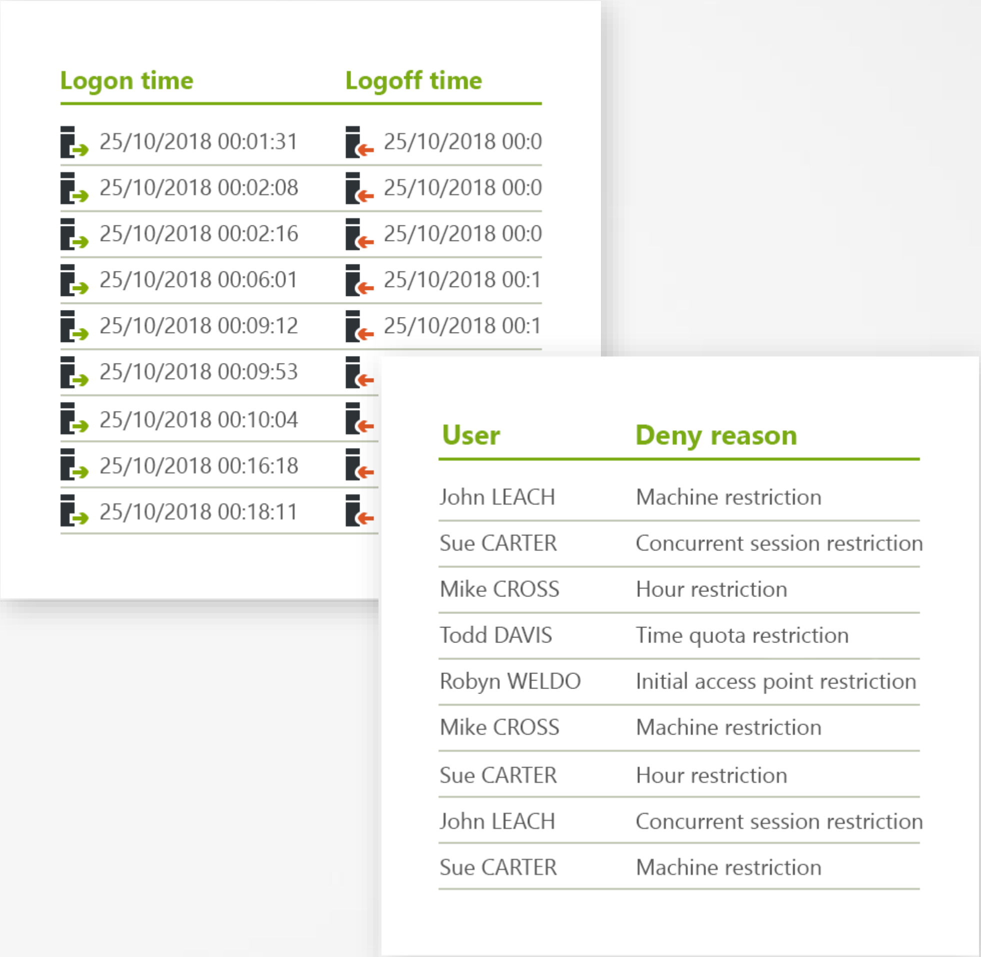
User status	User name	User account	Sessions		Session	Session status	Session type	In
● Protected	Arianna BAKER	ab	1	☐	WKS058	Open	Workstation	10
● Protected	aAaliyah CAMPBELL	ac	1	☐	WKS065	Open	Workstation	10
● High Risk	aAva DAVIS	ada		☑	S011	Open	Workstation	10
					018	Locked	Workstation	10
● Protected	Administrator	Administrator	2	☑	PSERVER0...	Locked	Terminal	FE
				☐	APPSERVER0...	Locked	Terminal	FE
● Protected	Audrey EVANS	ae	1	☐	WKS071	Open	Workstation	10
● New	Alexis HILL	ahi	1	☐	WKS050	Open	Workstation	
● Protected	Alyssa LOPEZ	al	1	☐	WKS049	Open	Workstation	
● Risk	Avery RODRIGUEZ	ar	2	☐	WKS036	Open	Workstation	
				☐	WKS099	Locked	Workstation	
● Protected	Aubrey SCOTT	as	1	☐	WKS038	Open	Workstation	
● Protected	Aiden STEWART	ast	1	☐	WKS075	Open	Workstation	
● Unprotected	Abigail TAYLOR	at	2	☐	WKS016	Open	Workstation	
				☐	WKS032	Locked	Workstation	
● Protected	Amelia TURNER	atu	1	☐	WKS066	Open	Workstation	10
● Protected	Anna YOUNG	ay	1	☐	WKS044	Open	Workstation	10
● Protected	Brayden COY	bc	1	☐	WKS095	Open	Workstation	10

User sessions | View by users | 100 sessions, 67 users

AUDIT & REPORT

AUDIT LOGON EVENTS

A **centralized audit** on all network logon events provides **detailed reports** to track down security threats, support forensics and prove regulatory **compliance**.



Logon time	Logoff time
25/10/2018 00:01:31	25/10/2018 00:0
25/10/2018 00:02:08	25/10/2018 00:0
25/10/2018 00:02:16	25/10/2018 00:0
25/10/2018 00:06:01	25/10/2018 00:1
25/10/2018 00:09:12	25/10/2018 00:1
25/10/2018 00:09:53	
25/10/2018 00:10:04	
25/10/2018 00:16:18	
25/10/2018 00:18:11	

User	Deny reason
John LEACH	Machine restriction
Sue CARTER	Concurrent session restriction
Mike CROSS	Hour restriction
Todd DAVIS	Time quota restriction
Robyn WELDO	Initial access point restriction
Mike CROSS	Machine restriction
Sue CARTER	Hour restriction
John LEACH	Concurrent session restriction
Sue CARTER	Machine restriction

INFRASTRUCTURE

UserLock works alongside Active Directory
in a Microsoft Windows Environment

NON-DISTRUPTIVE TECHNOLOGY

No modifications are made to Active Directory or its schema. UserLock works alongside Active Directory to extend not replace its security.

FAST IMPLEMENTATION

Installed on any member server of the domain, UserLock is managed from any workstation or remotely through a web interface.

FAST AGENT DEPLOYMENT

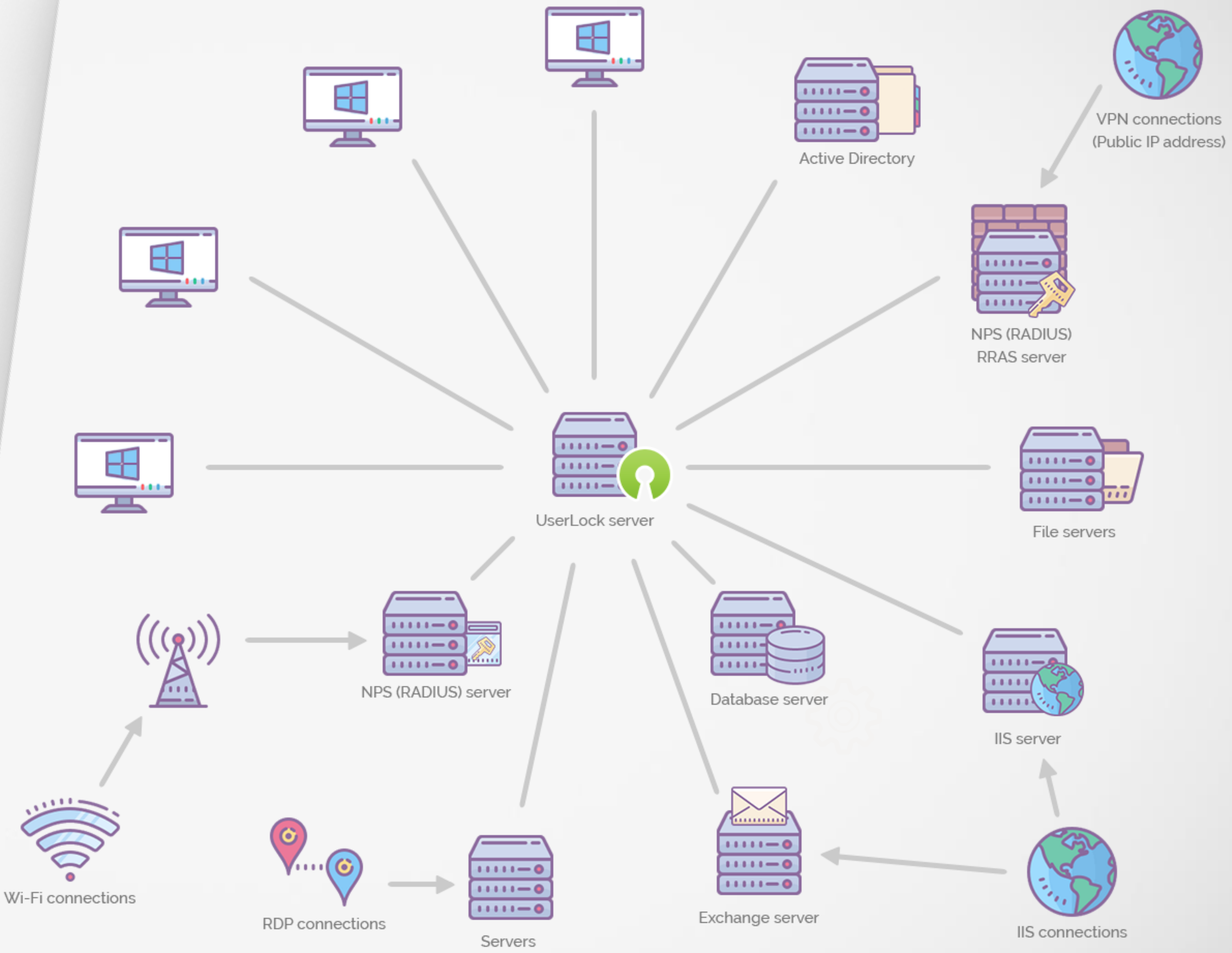
A micro agent is deployed automatically (or manually) on all machines. Once installed all access connections are detected and saved in the UserLock database.

ALL SESSION TYPES

UserLock offers a variety of agents according to the types of session it has to monitor, workstation, terminal, Wi-Fi & VPN and IIS.

INFRASTRUCTURE

UserLock is a **client server** application capable of **auditing** and **controlling** different types of user access connections.

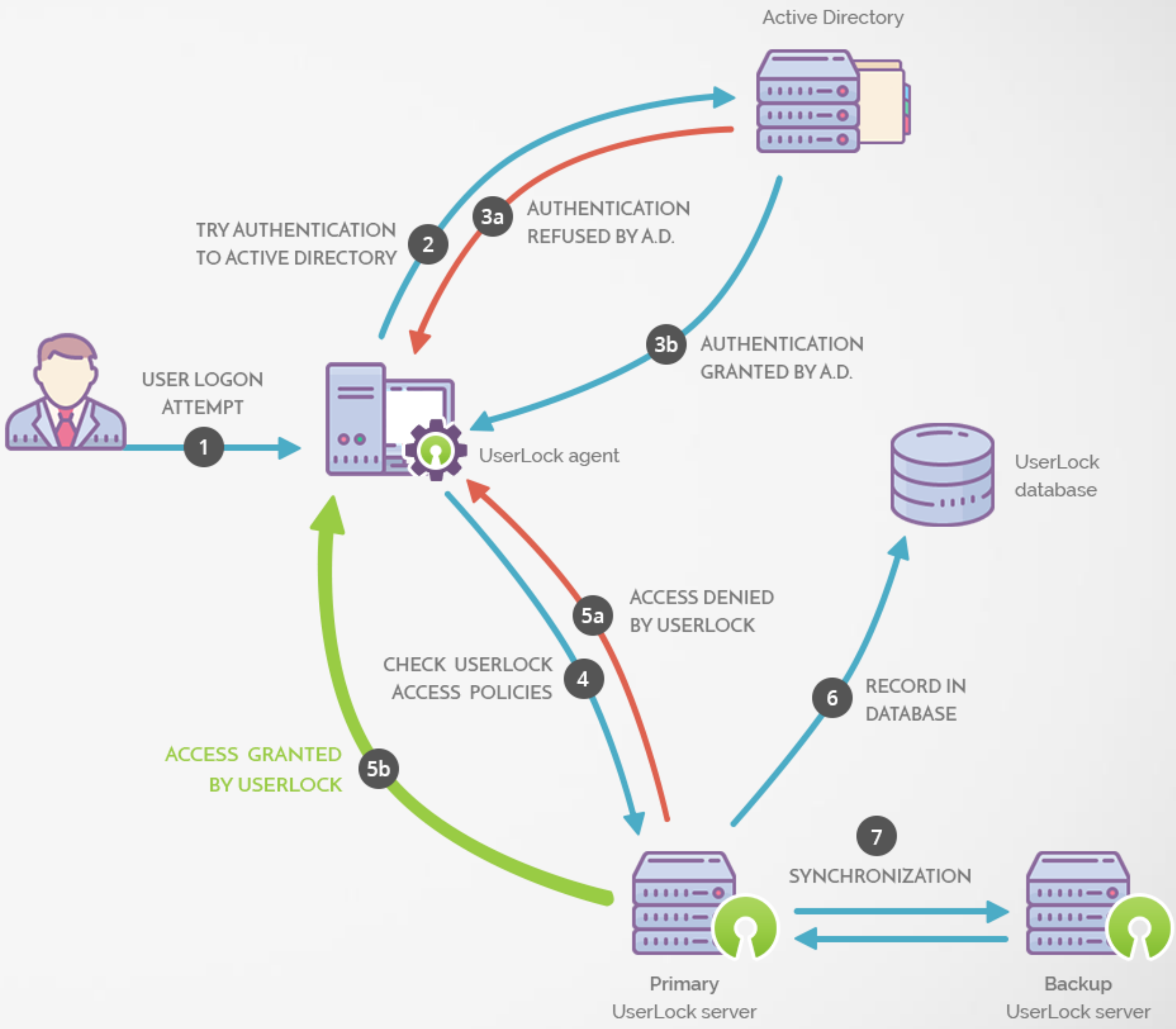


HOW **USERLOCK** WORKS

GENERAL PROCESS DESCRIPTION (1/2)

The user enters their credentials to log on or to **establish a connection** to the domain network. These credentials are verified and validated against Active Directory. If the **authentication process fails**, the connection will be refused by Windows and **UserLock does not intervene**. The agent will however notify the UserLock server about this logon failure.

Different agents are available depending on the connection type to be audited and the technology used to configure these connections. The general process is the same regardless of the agent type.

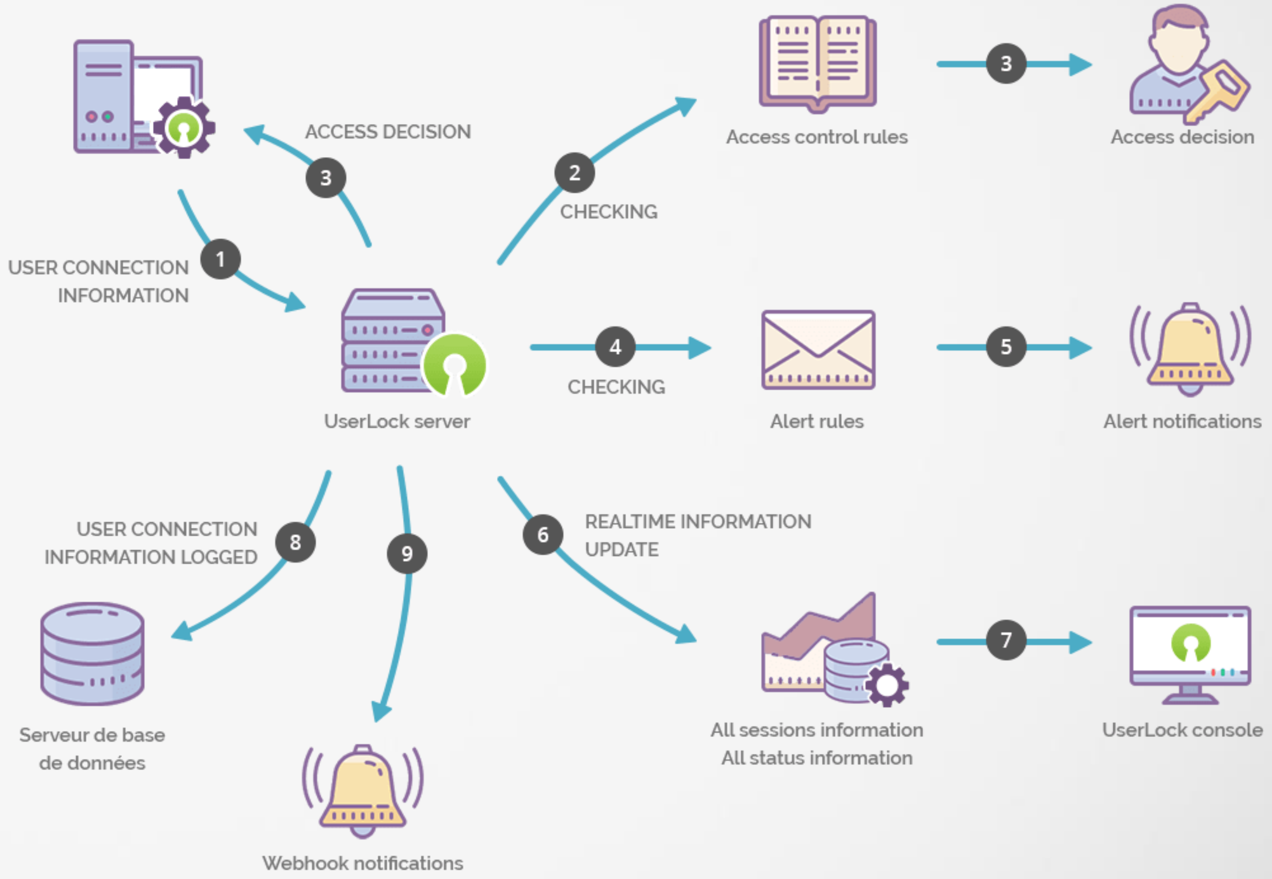


Active Directory
2
TRY AUTHENTICATION TO ACTIVE DIRECTORY
3a
AUTHENTICATION REFUSED BY A.D.
3b
AUTHENTICATION GRANTED BY A.D.
1
USER LOGON ATTEMPT
UserLock agent
UserLock database
5a
ACCESS DENIED BY USERLOCK
4
CHECK USERLOCK ACCESS POLICIES
6
RECORD IN DATABASE
5b
ACCESS GRANTED BY USERLOCK
7
SYNCHRONIZATION
Primary UserLock server
Backup UserLock server

HOW **USERLOCK** WORKS

GENERAL PROCESS DESCRIPTION (2/2)

If the **authentication is successful**, the UserLock agent will transmit to the UserLock server all information about the **context of the connection** requested. The UserLock server will then **process and analyze the data** transmitted by the agent to check access control rules, trigger any alerts, refresh session information and save the user connection event in the database. **The server then communicates its decision** to the agent regarding the acceptance or refusal of the connection requested.



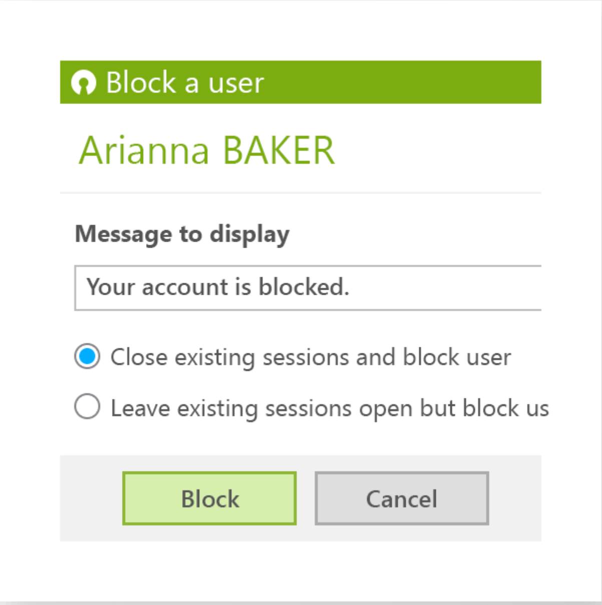
WHY DO YOU NEED **USERLOCK**? (1/2)

- **EASILY MANAGE LOGON CONTROLS, CONCURRENT SESSIONS AND ACCESS POLICIES**
  Set and enforce the legitimate access needs for all users

- **IMMEDIATELY RESPOND TO LOGON EVENTS**
  Remote interaction with any session to restrict, alert, block, report…

- **SAVE TIME AND COSTS WITH CENTRALIZED LOGON LOGOFF FORENSICS**
  Powerful 100% accurate reporting

- **ADDRESS COMPLIANCE AND AVOID FINES**
  Stopping inappropriate access ultimately starts with the logon



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

WHY DO YOU NEED **USERLOCK**? (2/2)

DEFENSE AGAINST COMPROMISED CREDENTIALS

Two-factor authentication and contextual controls deny access before damage is done

ERADICATE CERTAIN CARELESS USER BEHAVIOR

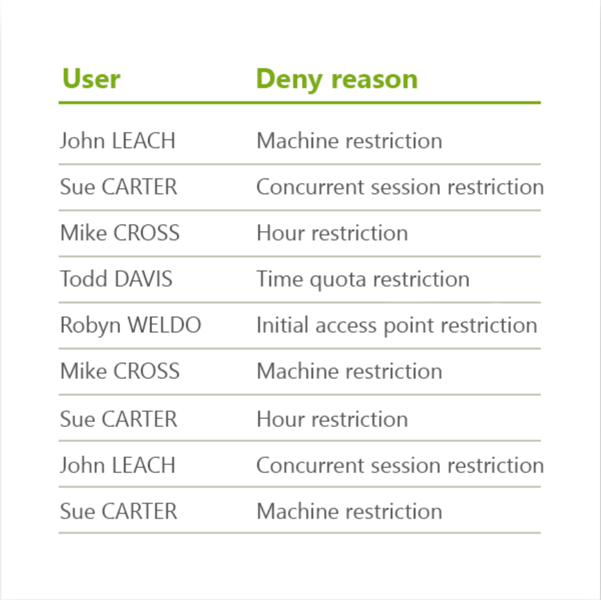
Such as password sharing, shared workstations left unlocked…

DETER MALICIOUS BEHAVIOR

Hold individual users accountable for their access and actions on the network

SECURE ANY KIND OF PRIVILEGED ACCESS

Protect both privileged account use and any account with privileged access



User	Deny reason
John LEACH	Machine restriction
Sue CARTER	Concurrent session restriction
Mike CROSS	Hour restriction
Todd DAVIS	Time quota restriction
Robyn WELDO	Initial access point restriction
Mike CROSS	Machine restriction
Sue CARTER	Hour restriction
John LEACH	Concurrent session restriction
Sue CARTER	Machine restriction

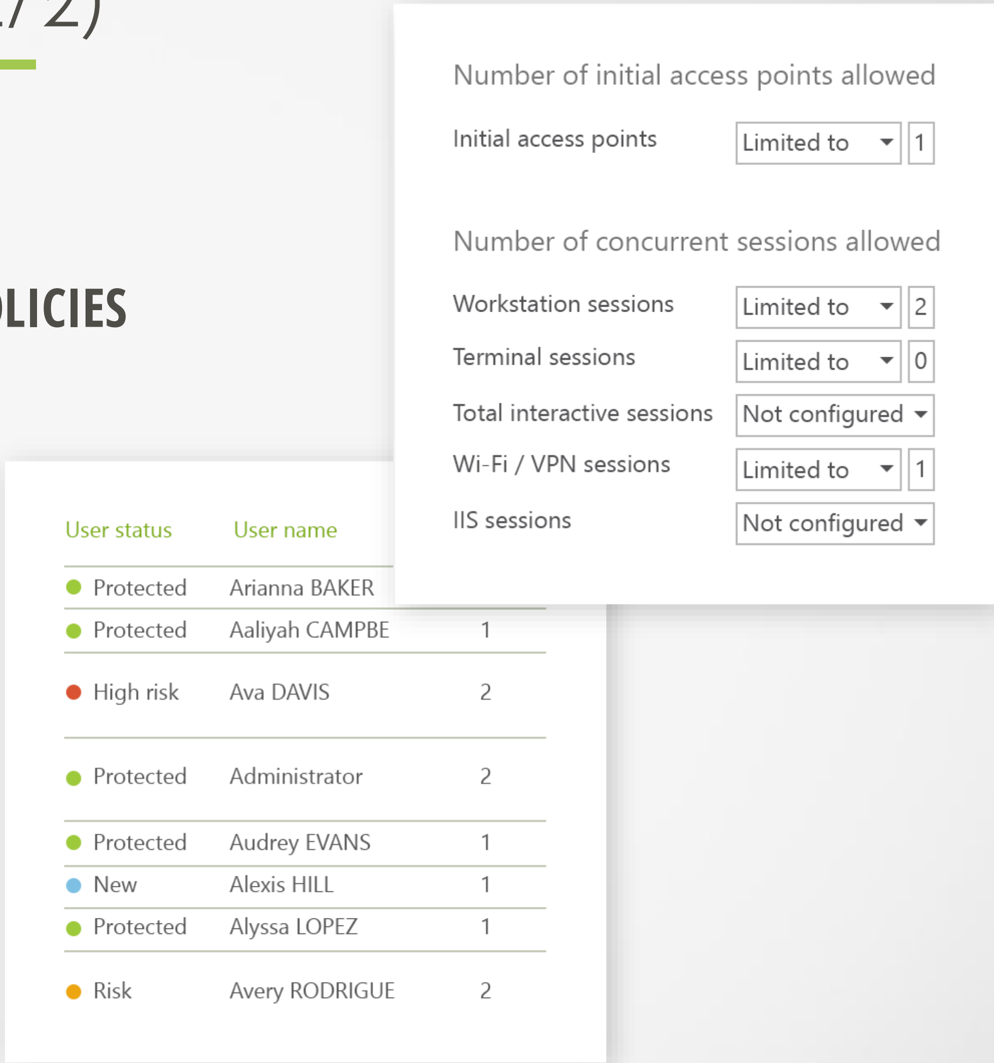
ADVANTAGES OF **USERLOCK** (1/2)

- **EASY TO USE**
  No training is necessary
- **FAST & SIMPLE TO INSTALL**
  Ready to use in minutes
- **NON-DISRUPTIVE TECHNOLOGY**
  No modification is made to Active Directory
- **TRANSPARENT FOR THE END USER**
  UserLock does not impede with productivity

ADVANTAGES OF **USERLOCK** (2/2)

SECURITY FAR BEYOND ACTIVE DIRECTORY & GROUP POLICIES

- Restrictions by group and OU
- Initial access point identification
- Concurrent logins control
- Forcing logoff
- Warning and alerts
- Notifications of previous logon
- Temporary controls



Number of initial access points allowed

Initial access points	Limited to	1

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	

User status	User name	
● Protected	Arianna BAKER	
● Protected	Aaliyah CAMPBE	1
● High risk	Ava DAVIS	2
● Protected	Administrator	2
● Protected	Audrey EVANS	1
● New	Alexis HILL	1
● Protected	Alyssa LOPEZ	1
● Risk	Avery RODRIGUE	2