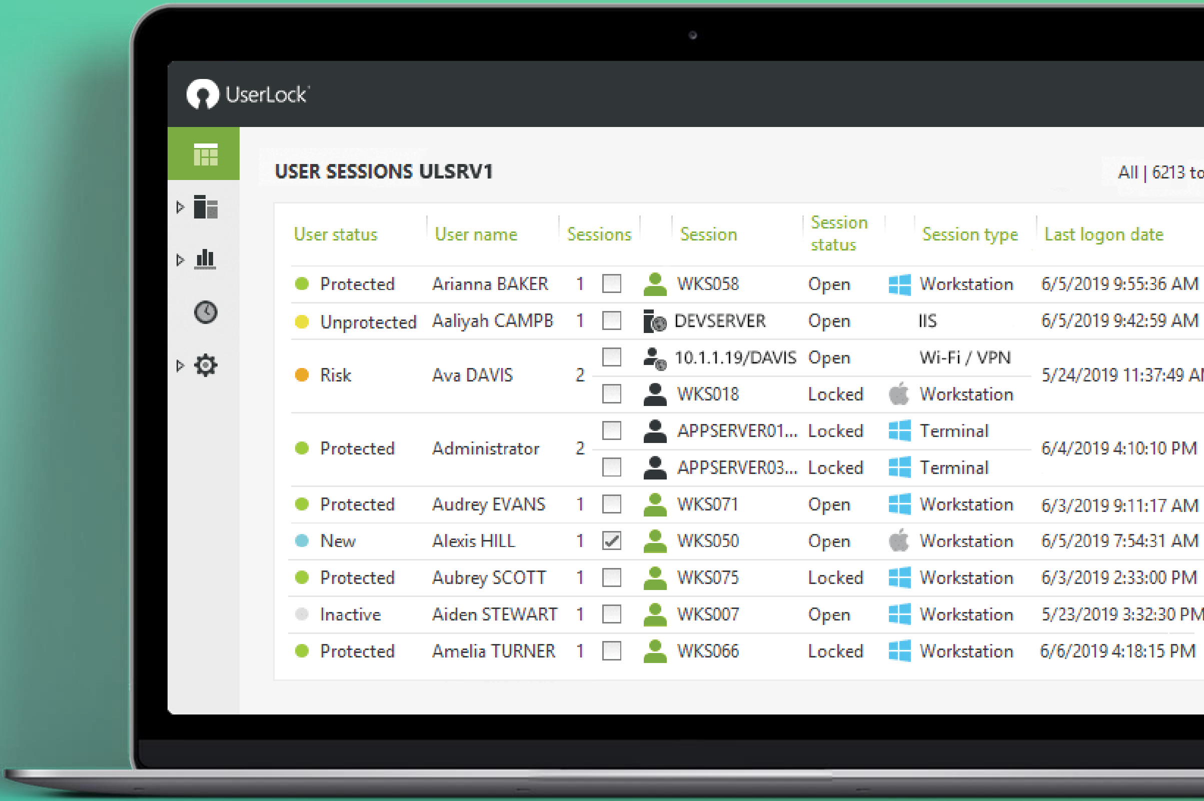
UserLock®

Provide any on-premises or hybrid Active Directory environment with secure employee access to corporate networks and cloud applications, no matter where they work.



USER SESSIONS ULSRV1

All | 6213 to

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 A
			☐	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

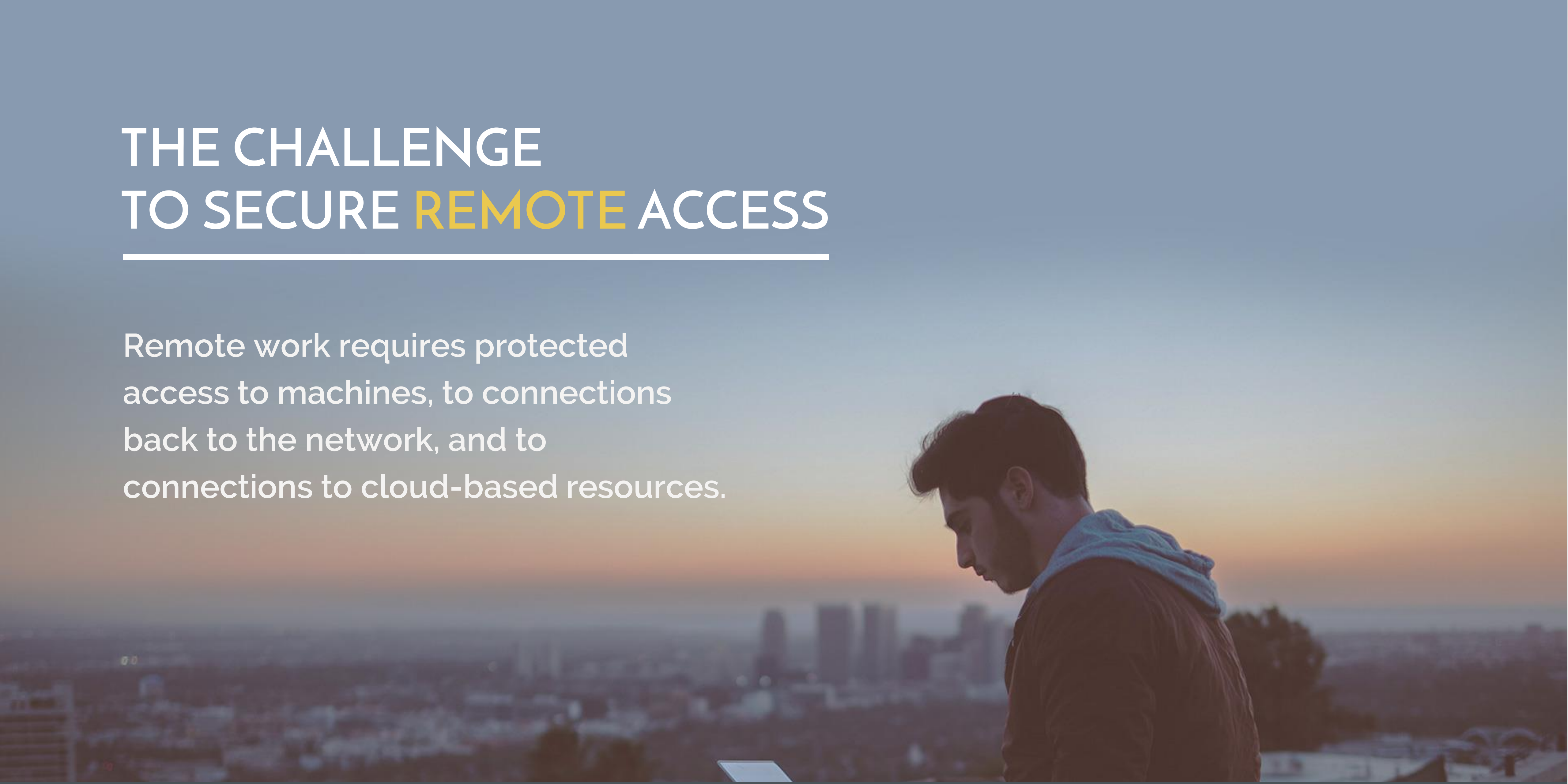
THE ACCESS SECURITY CHALLENGE

An increase in cyber-attacks, ransomware and more stringent compliance and insurance regulations means access protection has never been more important.

THE CHALLENGE TO SECURE EMPLOYEE ACCESS

Identifying suspicious activity when the adversary has valid and authorized credentials is a daunting task.

EXPLOITED USER: PHISHED CREDENTIALS
CARELESS USER: SHARED PASSWORD
MALICIOUS USER: DATA THEFT



THE CHALLENGE TO SECURE REMOTE ACCESS

Remote work requires protected access to machines, to connections back to the network, and to connections to cloud-based resources.

THE CHALLENGE TO SECURE CLOUD ACCESS

Organizations that enjoy the benefits of using the cloud can struggle to secure access to on-premises and cloud resources in a hybrid environment.

THE CHALLENGE TO SECURE ALL ACCESS

Every user has attributed access rights and privileges and is some sort of privilege user. Access security should not be used to protect only the most privileged of accounts.

THE CHALLENGE TO SECURE SMB ACCESS

Security solutions should not be any less effective for an SMB than for an enterprise client. The data is no less sensitive, the disruption no less serious.

THE CHALLENGE OF REGULATORY COMPLIANCE & CYBER INSURANCE

At the core of any compliance or insurance mandate is the desire to keep protected data secure, only allowing access to those who need it for business reasons.

> *« The wonderful thing about standards is that there are so many of them to choose from. »*
>
> Rear Admiral Grace Murray Hopper,
> Pioneering computer scientist

UserLock

OUR APPROACH

UserLock provides enterprise-caliber access management for on-premises and hybrid AD environments of any size that want a cost-effective, easy-to-use and scalable solution to protect employee access to the corporate network and cloud applications, no matter where they work.

EASY TO USE

NON-DISRUPTIVE

EASILY ADOPTED

COST EFFECTIVE

EASY TO USE

UserLock is quick to deploy, intuitive to manage, and scales effortlessly for any number of users, to ease the burden on IT.

NON-DISRUPTIVE

FOR IT TEAMS:

UserLock works seamlessly alongside your existing Active Directory infrastructure, reducing complexity and frustration.

EASILY ADOPTED

FOR USERS:

UserLock's granular controls allow for customized restrictions that protect access without unnecessarily impeding employees.

COST EFFECTIVE

Building on your investment in Active Directory, UserLock offers additional, effective and affordable security that stops threats, before damage is done.

UserLock®

Provide any on-premises or hybrid Active Directory environment with secure employee access to corporate networks and cloud applications, no matter where they work.

USERLOCK

ACTIVE DIRECTORY TWO FACTOR AUTHENTICATION & ACCESS MANAGEMENT

Secure Active Directory user logins with two factor authentication, contextual access controls and real-time monitoring and reporting.

MULTI-FACTOR AUTHENTICATION

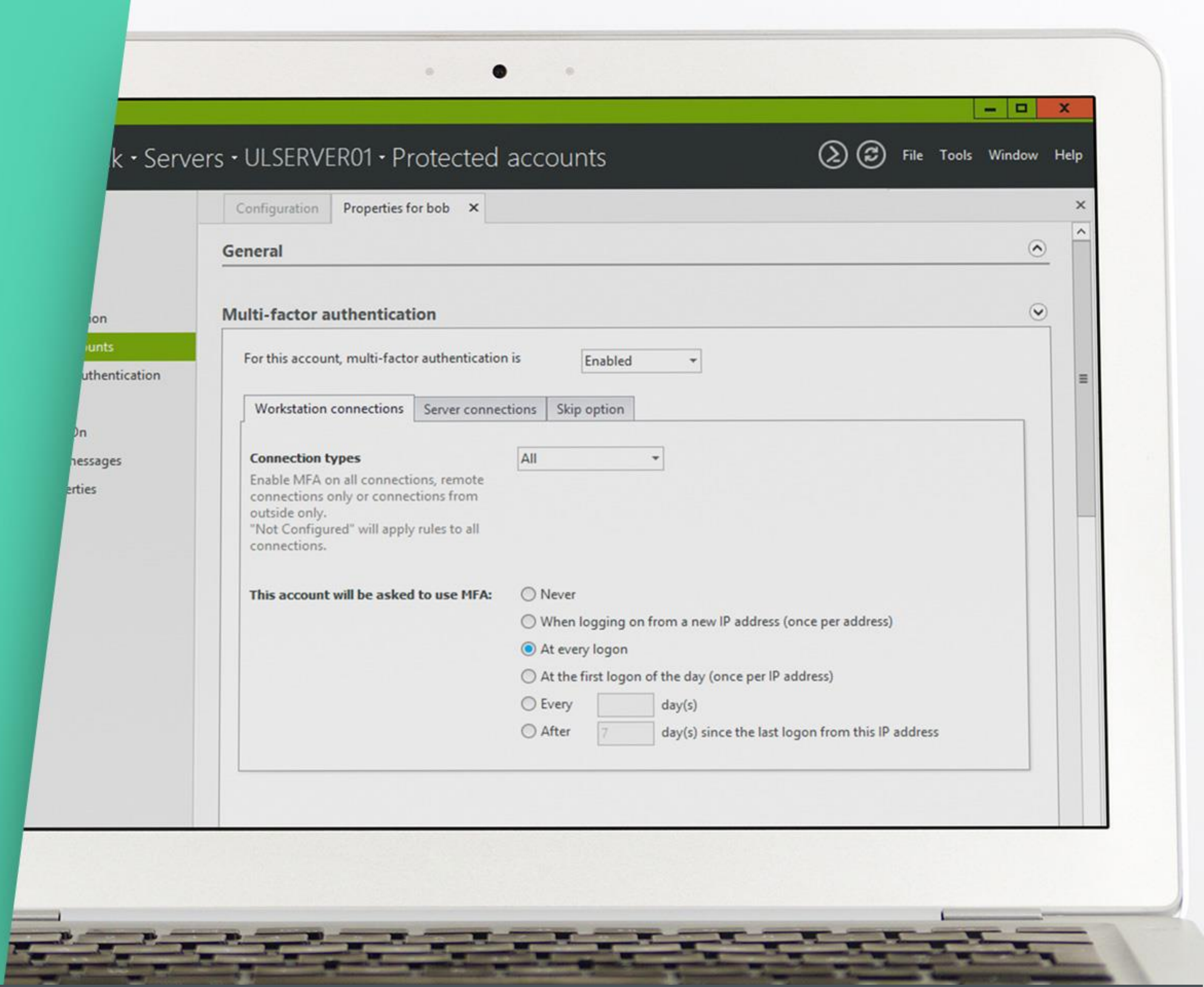
Verify and protect the identity of all users with strong two-factor authentication on Windows logon, Remote Desktop (RDP & RD Gateway), IIS, VPN and Cloud Apps.

UserLock supports authenticator applications and programmable hardware tokens such as YubiKey or Token 2.

Multi-Factor Authentication setup
Download an Authenticator Application
Scan the QR Code
O2XVNUS3WBKUSJFK
Enter the authentication code
Verify and continue
Cancel
How to install an Authenticator Application
159 384

CUSTOMIZED MFA

Avoid prompting the user for MFA each and every time. With UserLock define the frequency and circumstances for MFA.



General

Multi-factor authentication

For this account, multi-factor authentication is: Enabled

Workstation connections | Server connections | Skip option

Connection types: All

Enable MFA on all connections, remote connections only or connections from outside only.
"Not Configured" will apply rules to all connections.

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 7 day(s) since the last logon from this IP address

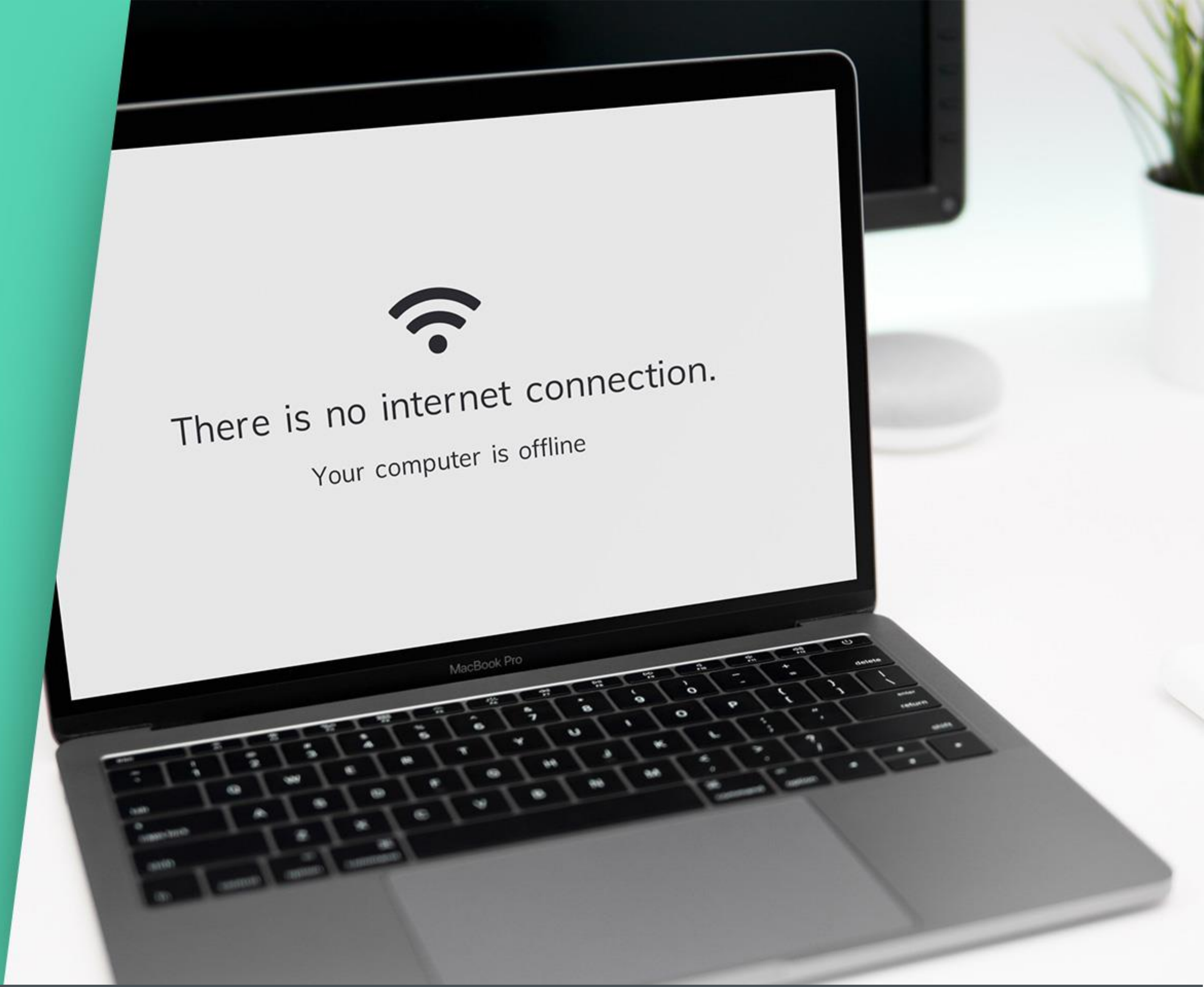
MFA FOR REMOTE WORKING

Enforce MFA to secure a variety of remote connection types (RDP, VPN, IIS).

When no such secure connection exists, MFA is still enforced via an internet connection.

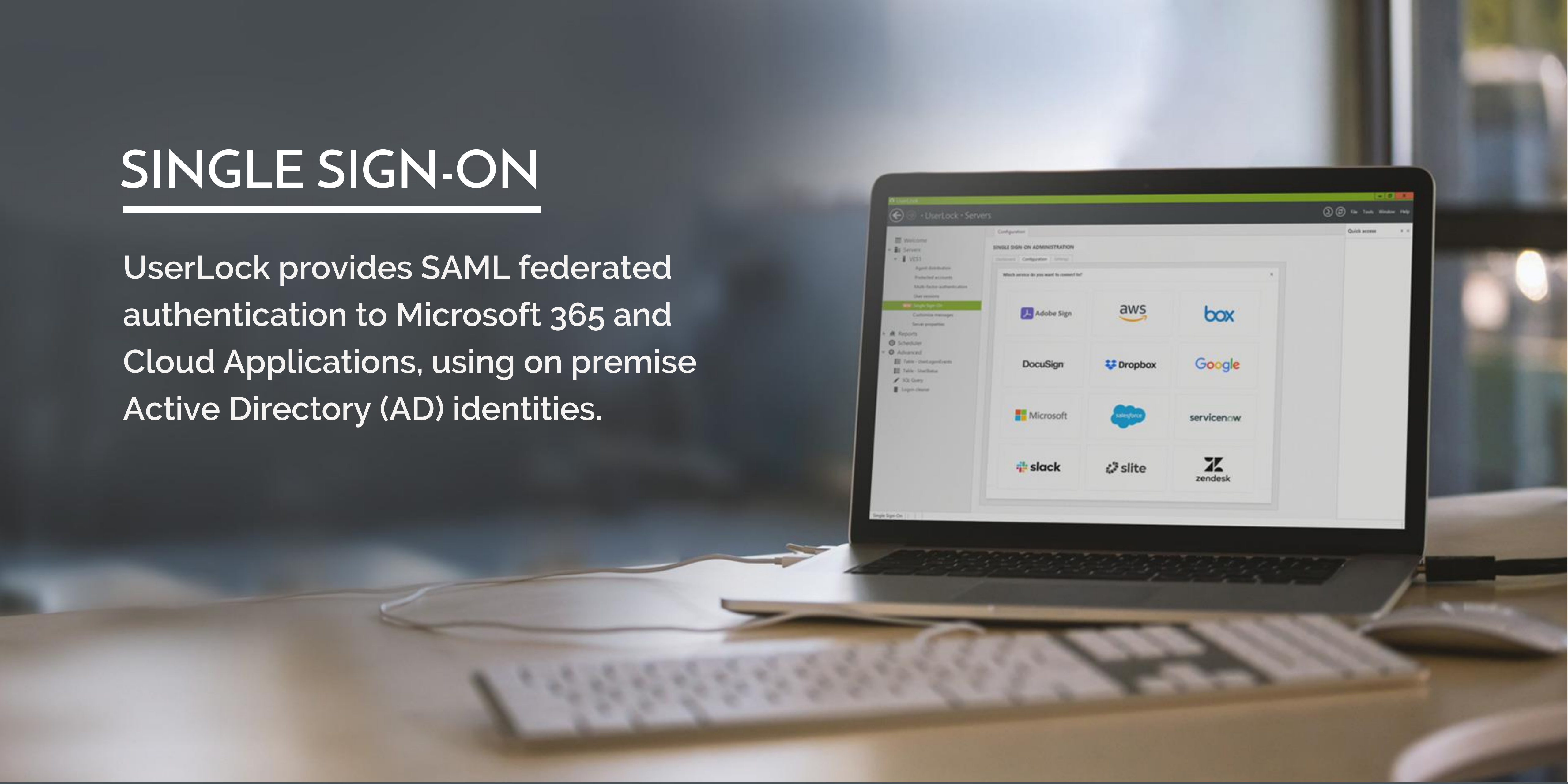
OFFLINE MFA

With secure on-premise hosting, UserLock MFA needs no internet connection on-site.
An agent can also protect a remote machine with MFA when no internet connection.



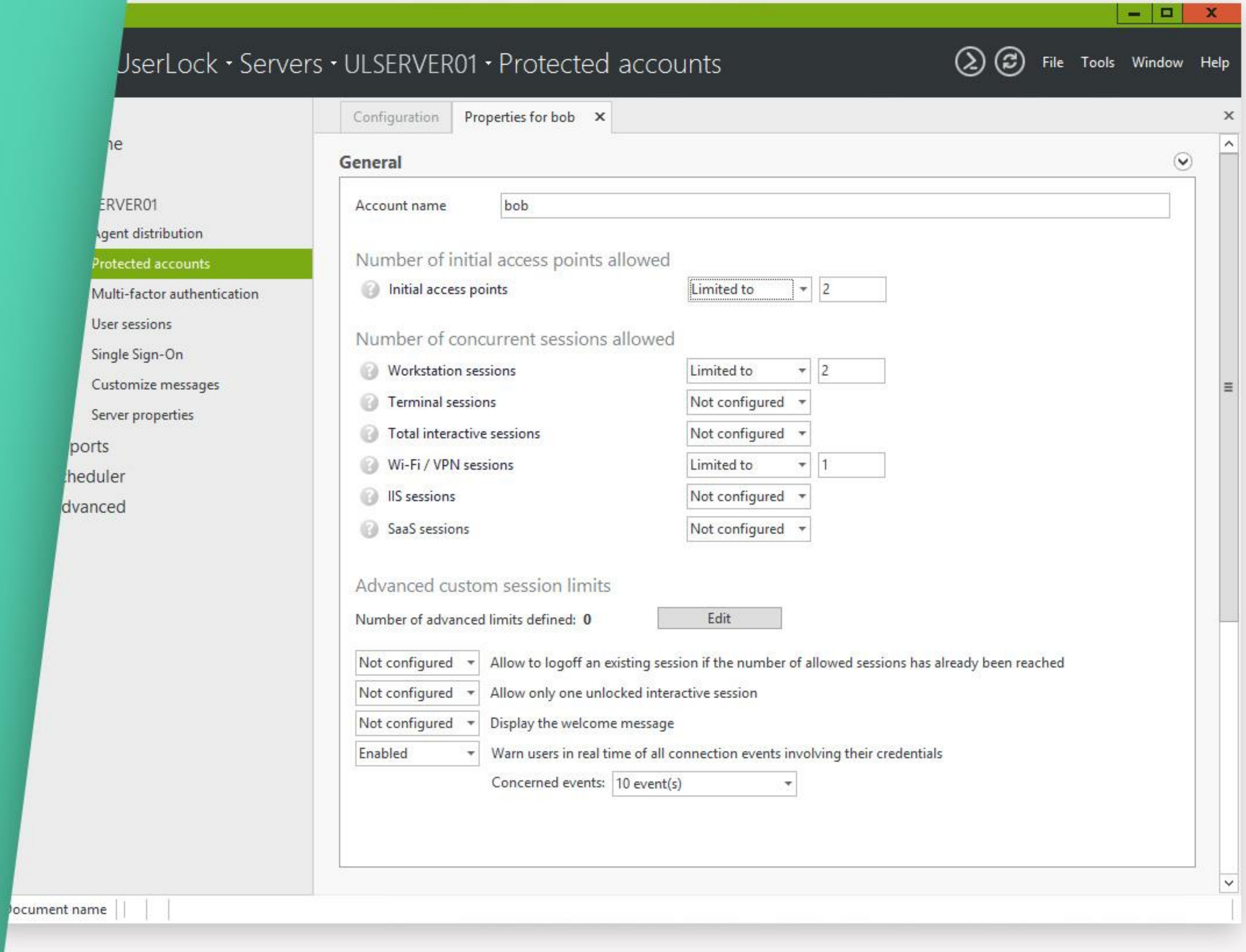
SINGLE SIGN-ON

UserLock provides SAML federated authentication to Microsoft 365 and Cloud Applications, using on premise Active Directory (AD) identities.



CONTEXTUAL ACCESS CONTROLS

Reduce the risk of inappropriate access. Limit who can logon when, from where, for how long, and how frequent, and restrict specific combinations of logon types.



General

Account name: bob

Number of initial access points allowed

Initial access points: Limited to 2

Number of concurrent sessions allowed

Workstation sessions: Limited to 2

Terminal sessions: Not configured

Total interactive sessions: Not configured

Wi-Fi / VPN sessions: Limited to 1

IIS sessions: Not configured

SaaS sessions: Not configured

Advanced custom session limits

Number of advanced limits defined: **0**

Not configured — Allow to logoff an existing session if the number of allowed sessions has already been reached

Not configured — Allow only one unlocked interactive session

Not configured — Display the welcome message

Enabled — Warn users in real time of all connection events involving their credentials

Concerned events: 10 event(s)

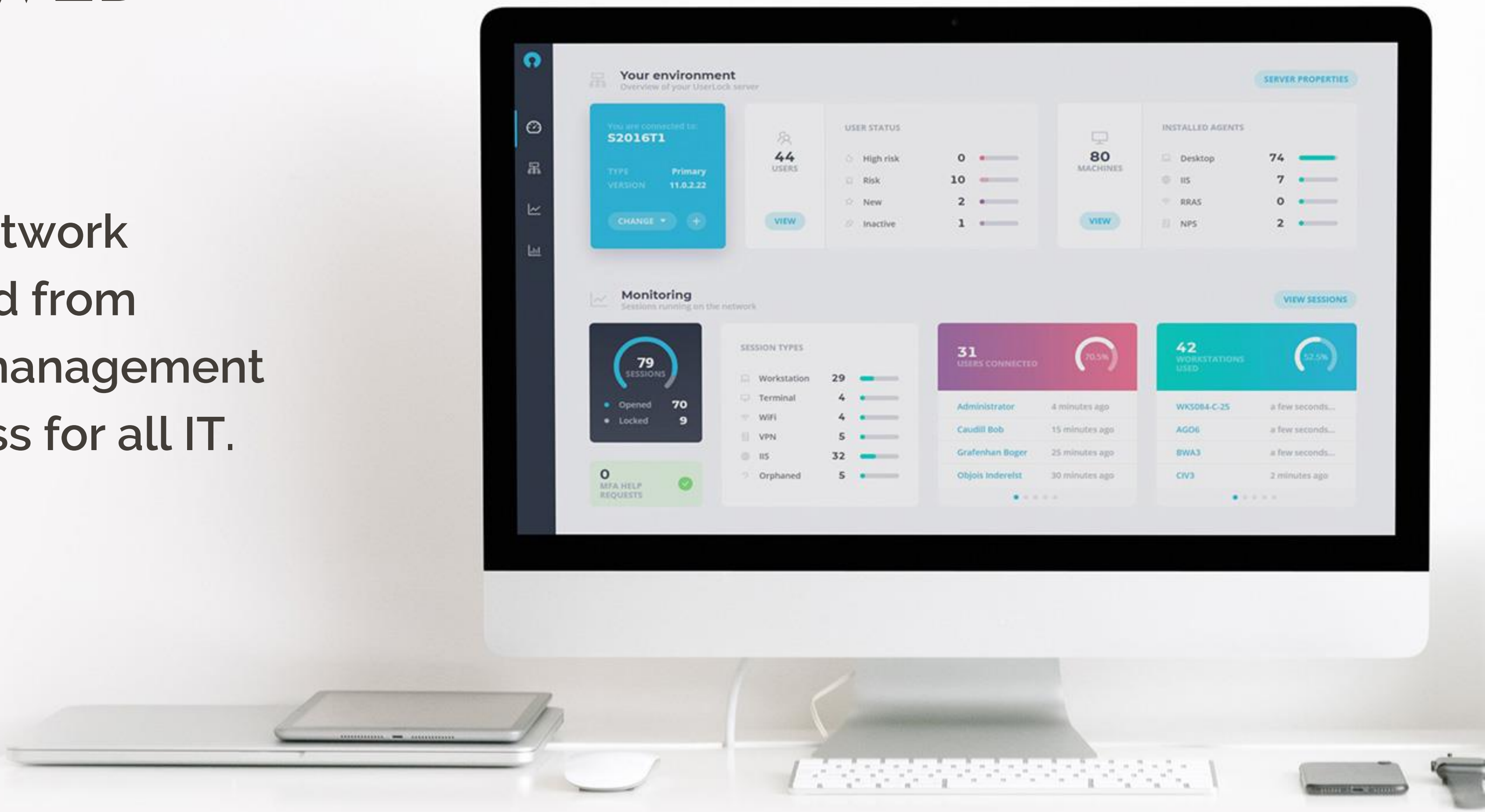
SESSIONS MANAGEMENT

Real-time visibility serves as the basis for enforcing policy, alerting and interacting on any access events.

A centralized audit provides detailed reports to support forensics and prove regulatory compliance

THE USERLOCK WEB APPLICATION

Monitor and respond to network sessions quickly, easily and from anywhere. Simplify daily management and widen UserLock access for all IT.



Your environment
Overview of your UserLock server

You are connected to:
S2016T1

TYPE	Primary
VERSION	11.0.2.22

44 USERS

USER STATUS	
High risk	0
Risk	10
New	2
Inactive	1

80 MACHINES

INSTALLED AGENTS	
Desktop	74
IIS	7
RRAS	0
NPS	2

Monitoring
Sessions running on the network

79 SESSIONS

Opened	70
Locked	9

0 MFA HELP REQUESTS

SESSION TYPES	
Workstation	29
Terminal	4
WiFi	4
VPN	5
IIS	32
Orphaned	5

31 USERS CONNECTED 70.5%

Administrator	4 minutes ago
Caudill Bob	15 minutes ago
Grafenhan Boger	25 minutes ago
Objois Inderelst	30 minutes ago

42 WORKSTATIONS USED 52.5%

WKS084-C-25	a few seconds...
AGO6	a few seconds...
BWA3	a few seconds...
CIV3	2 minutes ago

UserLock

USE CASES

How UserLock helps Active Directory environments of all sizes and sectors achieve their objectives.

COMBINING SSO WITH MFA TO PROTECT ALL ACCESS

SYMTA Pièces was looking to enable single sign-on (SSO) and multi-factor authentication (MFA) for Office 365 using on-premises Active Directory (AD) credentials.

UserLock SSO now streamlines login to various Office 365 apps, and reduces the burden on employees of entering complex passwords multiple times a day. The IT team can choose how often to prompt for MFA at a granular level – setting a lower frequency for on-site access, but asking for MFA at each connection for remote access.

MFA WITH YUBIKEY FOR QUEBEC POLICE

The City of Trois-Rivières is required to use MFA in order to comply with government regulations.

UserLock matched the need of supporting YubiKey on both on-site and RDP connections. It also offered easy user enrollment, a centralized console and detailed reports on all access and access attempts.

Thanks to UserLock, the Police Directorate were able to comply with regulations and simplify the day-to-day work of the IT team.

MSP CHOOSES USERLOCK FOR INSURANCE-APPROVED, ON PREMISE MFA

A Minnesota-based MSP that served small and large enterprises needed an Insurance-approved MFA solution.

The solution needed to work without an internet connection, handle all access attempts to the network, support both **YubiKey** and mobile phone authentication, and be customizable for different user access policies.

Hosted on-premises and linked directly to Active Directory, UserLock was found to be easy to implement, lightweight for users, and secured access without impeding employee productivity.

ACTIVE DIRECTORY MFA FOR US CITY FOLLOWING A **RANSOMWARE** ATTACK

The City of Keizer needed to strengthen their access security after being hit by a ransomware attack.

To comply, the Department had implemented Duo 2FA, but they didn't find it to be very easy to set up or user friendly. So, they sought a new solution that they could easily deploy across all user and administrative accounts, from all departments.

According to the City, UserLock is an IT managers' dream: the deployment and implementation were flawless, zero complaints from end-users, easy-to-use, affordable and it integrates simply with Active Directory.

ARTICLE

How Does MFA Help Prevent Ransomware

MEETING THE CENTRAL BANK OF KUWAIT'S **COMPLIANCE POLICY**

Following an audit by the CBK, an emerging bank was found not to have a solution in place to restrict active directory concurrent sessions.

With UserLock, IT administrators can set and enforce access rules that restrict from where, when and how long an authenticated Active Directory user may logon.

The complete UserLock set up was done in a single day and the team was able to easily integrate it into the bank's system. With compliance now achieved for concurrent sessions, the bank is looking at implementing MFA and other contextual access restrictions to secure employee's access.

MANAGING ACCESS FOR HUNDREDS OF USERS
AT A LEADING REAL ESTATE COMPANY

The IT Team at Orange Coast Title Company needed to be able to remotely manage users' sessions and comply with many regulations around multi factor authentication..

UserLock's real-time visibility and reporting into all users' sessions gave administrators the overview they were looking for, and the ability to quickly review and respond to any incident or event.

UserLock's MFA proved to be a game-changer for the IT team as it represents one of the functionalities most demanded by many regulations.

OFFLINE MFA FOR REMOTE WORKING

DOBBS PETERBILT

Dobbs Peterbilt needed to be sure that their senior employees who worked remotely and travelled extensively were secured as much as possible.

IT required MFA at login on all remote connections, even when offline. UserLock MFA requires no internet connection and can prompt users for a second authentication factor when connecting via RDP or VPN.

With MFA in place wherever remote users are working, access is secured and auditors are satisfied.

EASY TO INSTALL MFA FOR A LARGE ENTERPRISE

With over 2000 employees working remotely, MFA protection was needed, with or without a secure network connection.

UserLock proved easy for the IT Team to install and configure across multiple sites to protect on-site and remote access. Opting to use Google Authentication App , users found the self-enrollment process quick and simple.

With MFA in place wherever remote users are working, access is secured, even for offline access.

OUR CLIENTS

Trusted by over 3000 organizations, UserLock scales easily across organizations of any size, including some of the world's most regulated and security-conscious.

PROVEN ACROSS DIFFERENT SECTORS

HIGH POINT NETWORKS
matrix IT SUPPORT
EuskoData Soluciones Tecnológicas
angliss HONG KONG
ZOODFOOD
COASTAL Housing Group
MICHIGAN STATE UNIVERSITY
City School District of ALBANY
NORTHERN LIGHTS
DEPARTMENT OF JUSTICE
Ministerie van Defensie
TURKISH AEROSPACE
trois-rivières
KEIZER SINCE 1982
LA MAYENNE Le Département
NEW YORK CITY COLLEGE OF TECHNOLOGY CITY TECH
University of Kent
CAMDEN CITY SCHOOL DISTRICT NEW JERSEY
Oklahoma City PUBLIC SCHOOLS
Santander
FIS
بنك بوبيان Boubyan Bank
Star Union Dai-ichi LIFE INSURANCE
MOORE CAPITAL
First Flight FEDERAL CREDIT UNION
arnold IMMOBILIEN
LINEMASTER
Peterbilt DOBBS PETERBILT
EUROCONTROLLI
MRIoA
Clemson Eye
NHS
ANEW
DUBAI LONDON CLINIC
sabin MEDICINA DIAGNÓSTICA
DP WORLD
OTOLIFT MONTE-ESCALIERS
Rieckermann Machinery &amp; Industrial Solutions

> *We wanted to add multi-factor authentication for RDP and local on-site connections. The installation only took a few minutes and the initial setup was very easy. The low cost of the solution, the ease of implementation, the quality of the documentation and the 30 day free trial convinced me.*

Mathieu Vandal
System Administrator, City of Trois-Rivières, Quebec

> *We wanted a multi-factor authentication solution to secure access to jump servers and meet local audit requirements. The technology had to be provided by a system that was hosted locally (on-premise) and worked with corporate AD credentials. We found UserLock very easy to implement and will recommend to other branches within the bank.*

IT Officer
Multinational Banking Group, Hong Kong.

“

UserLock is a great software that has simplified our working day. Employees work in large, open-space offices, where no user has their own machine. UserLock allows us to verify that the user who authenticates is who they say they are. We also found the reports to be an extremely useful tool. The visibility on all user connection events provides us a central audit across the whole network. With this they could easily view the start and end of a session opened on the network to spot any anomalies or suspicious behavior.

José Miguel Villafuerte
IT Infastructure Manager, Teleperformance, Mexico

All in all, the UserLock solution allows you to do what it says it will do—control all aspects of user login activity. The beauty of the solution is that you can do this in a granular way, and it is highly customizable. The auditing and reporting are very detailed and provide great visibility into activities around user login activity.

Brandon Lee
4sysops.com

Relatively simple to deploy via UserLock, the implementation of MFA on an infrastructure significantly enhances security, especially with the current trend and the boom in remote working.

Florian Burnel
IT-CONNECT.FR

It was very easy to add two factor authentication for our in-house AD users with UserLock. This was a huge compliance requirement in our organization. The real-time insight regarding user logons gives administrators the best way to know if any unauthorized login is happening. Also with the help of limiting number of sessions for the elevated users, this tool helps to manage secure elevated access.

5 Star Review on Gartner Peer Insights
Senior System Administrator, United States

> *UserLock was love at first sight!*
>
> *It is the perfect combination – easy to use software, with good support. I've never seen MFA implement so easily before.*

Cameron Rezvani
Senior Systems Engineer, Orange Coast Title, United States

> *In this digital age, computer access is essential for students and teachers alike, but this access needs to be managed properly as it can lead to significant misuse. UserLock is the ideal solution that helps us meet our network access objectives effectively.*

Don Manning
Server Administrator, Albany City School District, United States

> *Great product and best price/value on the market. The product was very easy to setup and use for our organization. The features included were exactly what we were looking for to meet compliance regulations and improve risk management.*

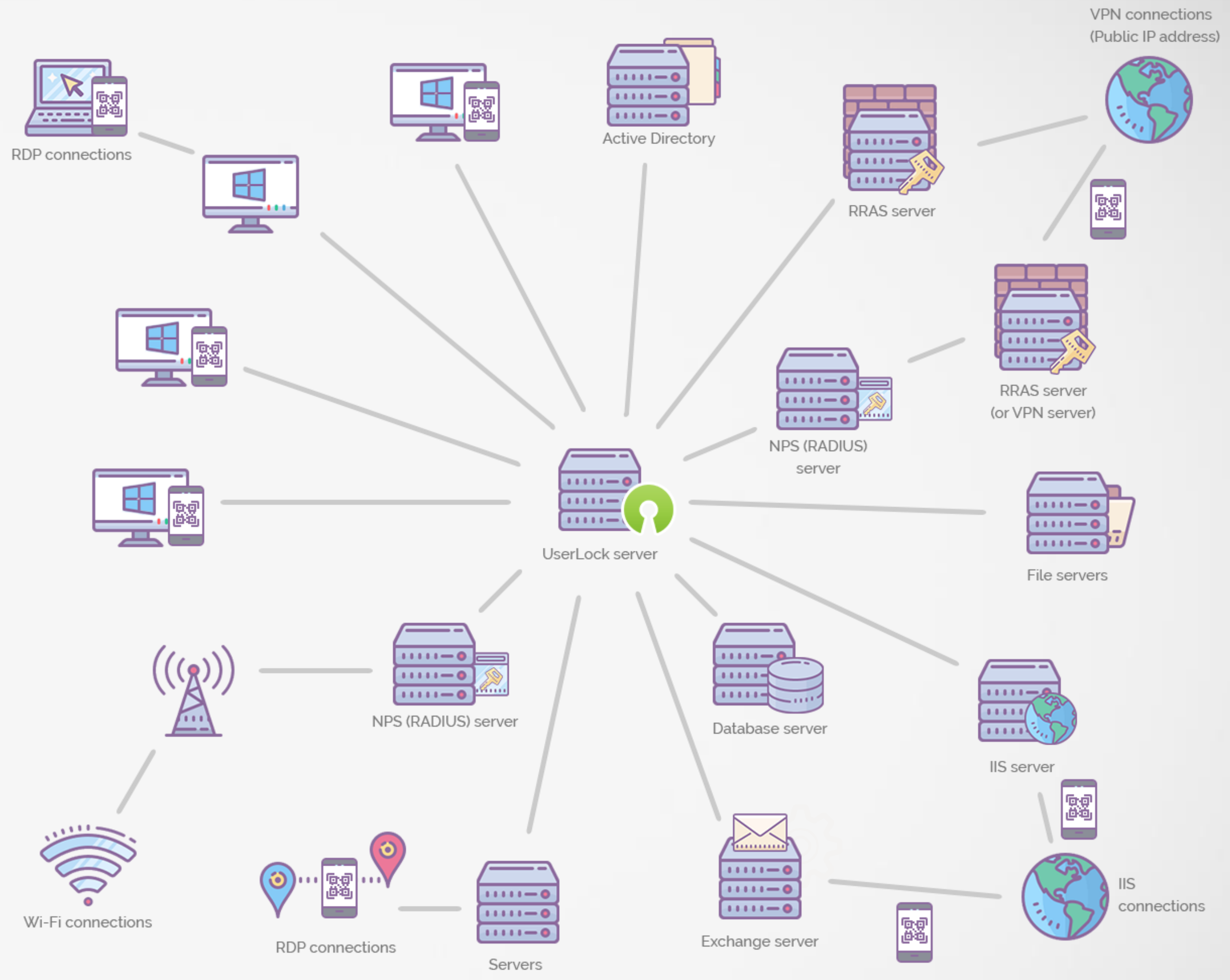
5 Star Review on Gartner Peer Insights
Senior IT Project Manager in Professional Services, United States

« The perfect access security partner for Windows Active Directory environments. »

IT SECURITY GURU
THE SITE FOR OUR COMMUNITY

INFRASTRUCTURE

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

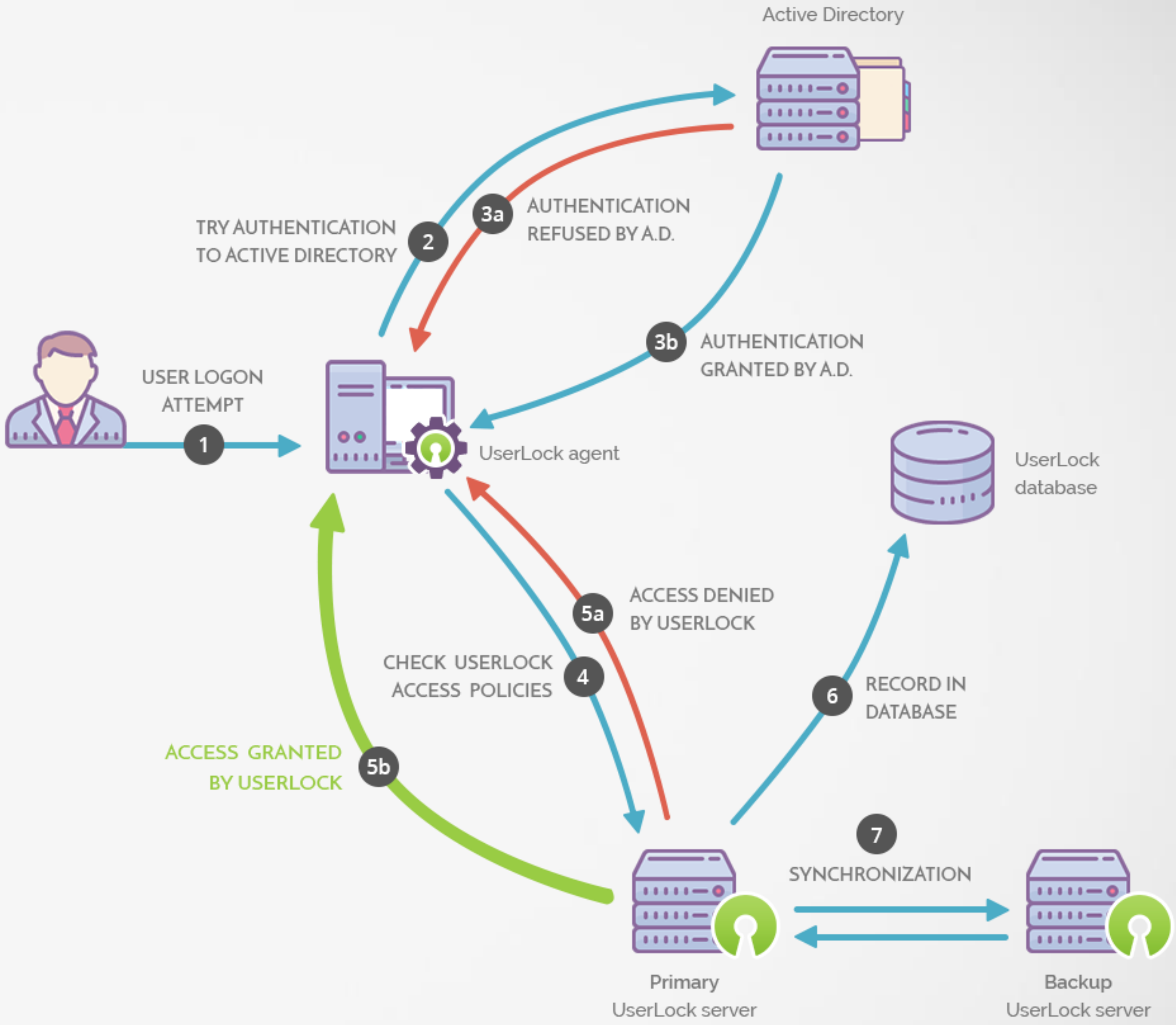


HOW **USERLOCK** WORKS

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.

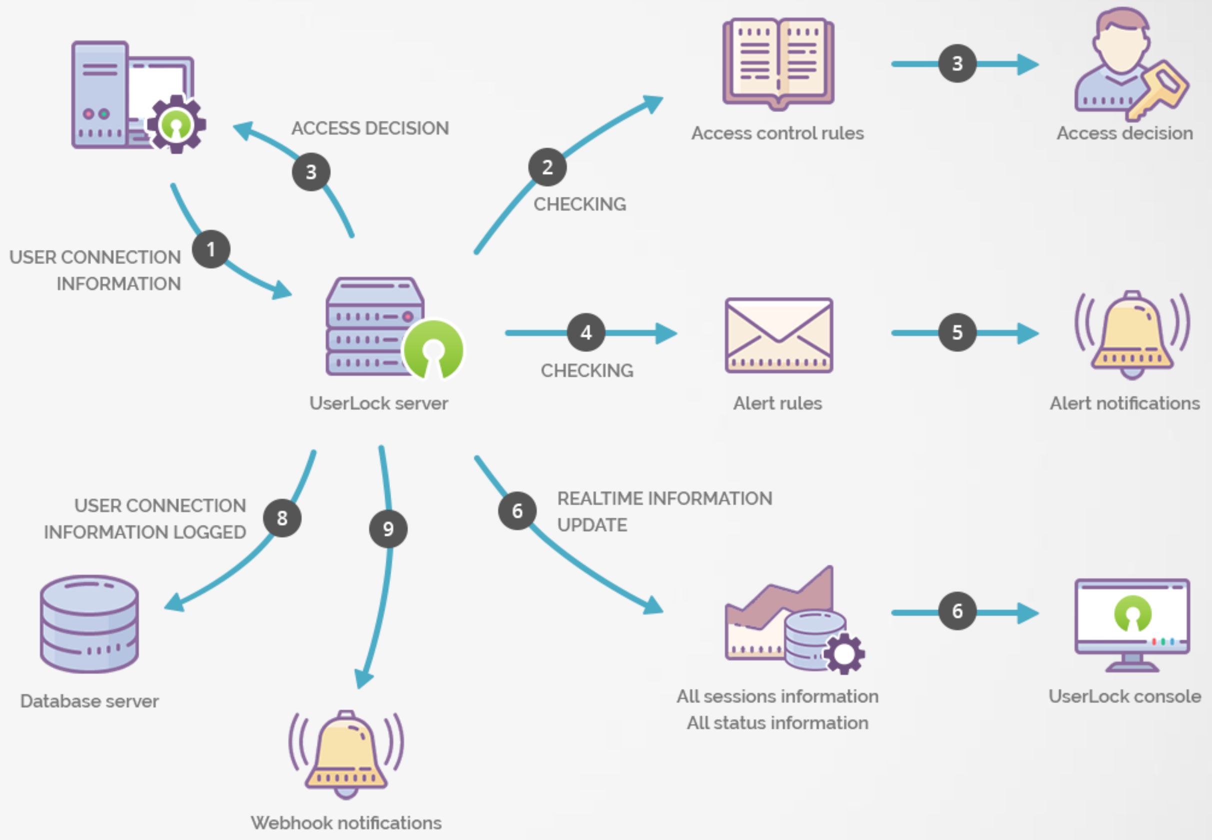


Active Directory
2 TRY AUTHENTICATION TO ACTIVE DIRECTORY
3a AUTHENTICATION REFUSED BY A.D.
3b AUTHENTICATION GRANTED BY A.D.
1 USER LOGON ATTEMPT
UserLock agent
UserLock database
5a ACCESS DENIED BY USERLOCK
4 CHECK USERLOCK ACCESS POLICIES
6 RECORD IN DATABASE
5b ACCESS GRANTED BY USERLOCK
7 SYNCHRONIZATION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

HOW **USERLOCK** WORKS

GENERAL PROCESS DESCRIPTION (2/2)

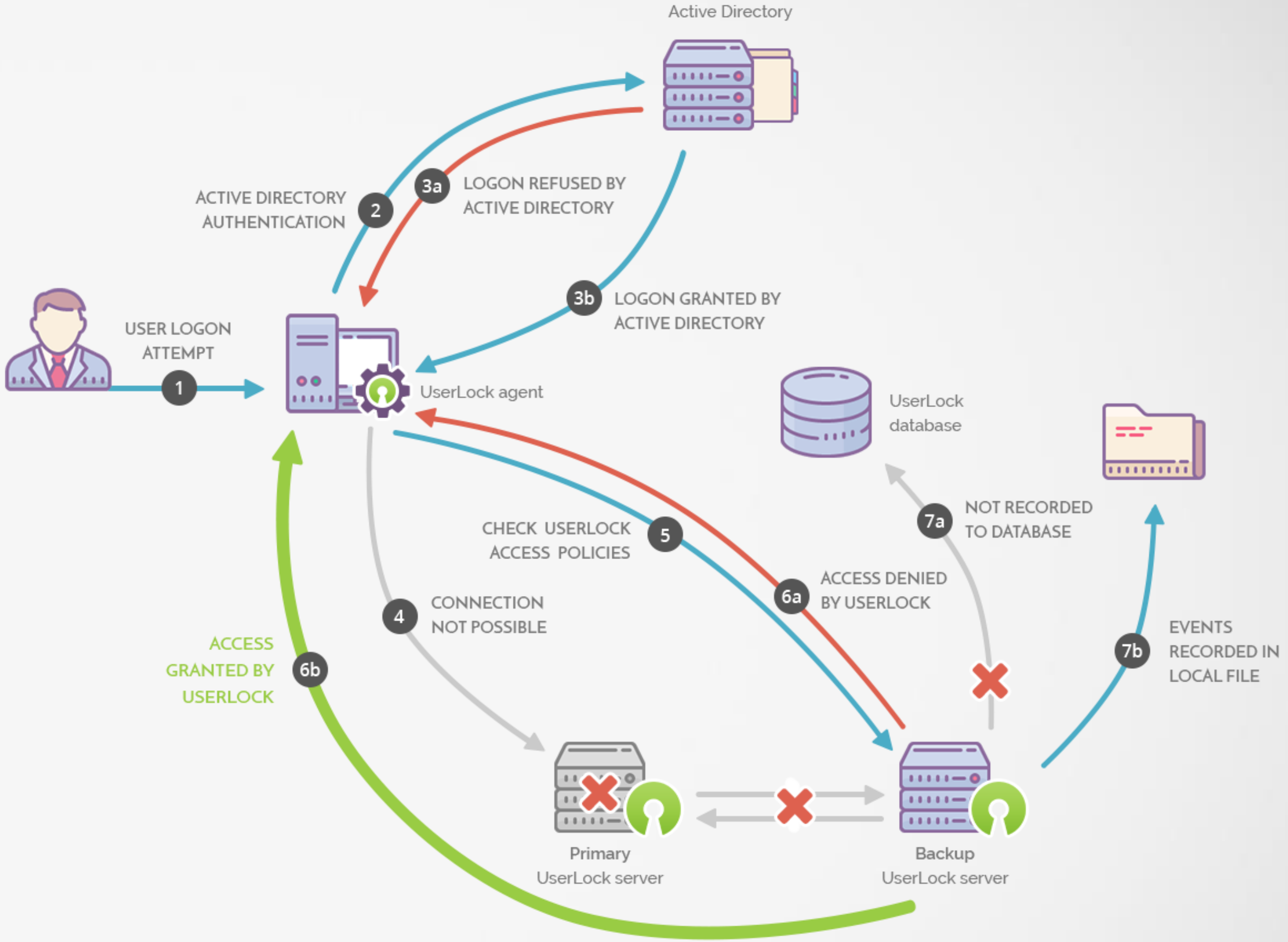
If the **authentication is successful**, the UserLock agent will transmit to the UserLock server all information about the **context of the connection** requested. The UserLock server will then **process and analyze the data** transmitted by the agent to check access control rules, trigger any alerts, 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.



HOW **USERLOCK** WORKS IN HIGH AVAILABILITY

USERLOCK BACKUP SERVER

The **UserLock Backup server** regularly synchronizes its configuration and its sessions database with the Primary server. If the Primary server has an issue, then the Backup server will automatically maintain the sessions activity monitoring and control of the network protected zone.


Active Directory
ACTIVE DIRECTORY AUTHENTICATION
2
3a
LOGON REFUSED BY ACTIVE DIRECTORY
3b
LOGON GRANTED BY ACTIVE DIRECTORY
USER LOGON ATTEMPT
1
UserLock agent
UserLock database
CHECK USERLOCK ACCESS POLICIES
5
7a
NOT RECORDED TO DATABASE
6a
ACCESS DENIED BY USERLOCK
4
CONNECTION NOT POSSIBLE
ACCESS GRANTED BY USERLOCK
6b
7b
EVENTS RECORDED IN LOCAL FILE
Primary UserLock server
Backup UserLock server

HOW **USERLOCK** WORKS ACROSS MULTIPLE SITES

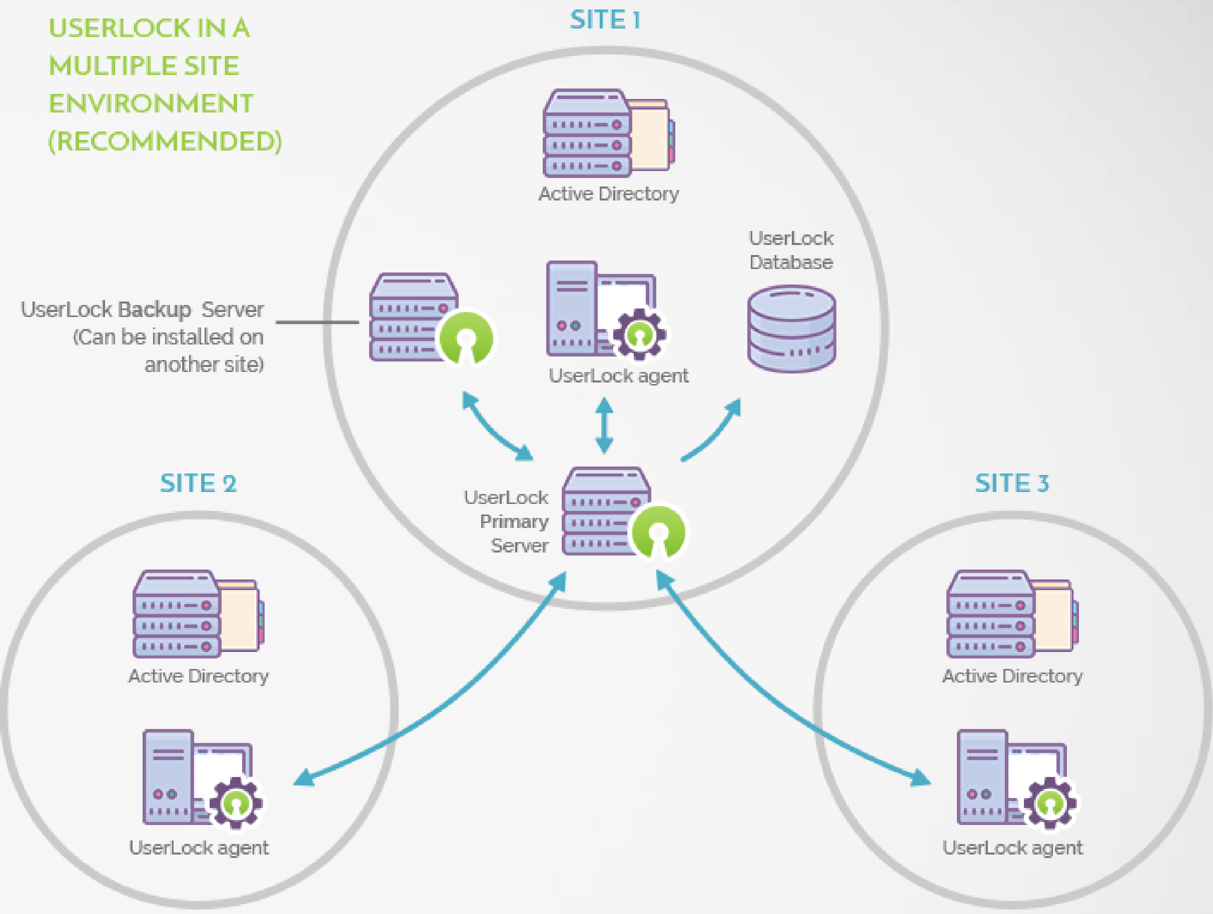
It is possible to install UserLock to monitor multiple sites. The diagram shows how the agents installed on workstations will all contact the same UserLock service to allow for a centralized management.

UserLock service will contact the first available DC at the time of the user login.

If you would like to force the UserLock service to contact a specific DC, you can configure this in the advanced setting

DcToContactForServerMember:

USERLOCK IN A MULTIPLE SITE ENVIRONMENT (RECOMMENDED)



Recommended: Install the service on one server, and deploy the agent to end clients on all sites. This will allow you to manage all users in one centralized console.

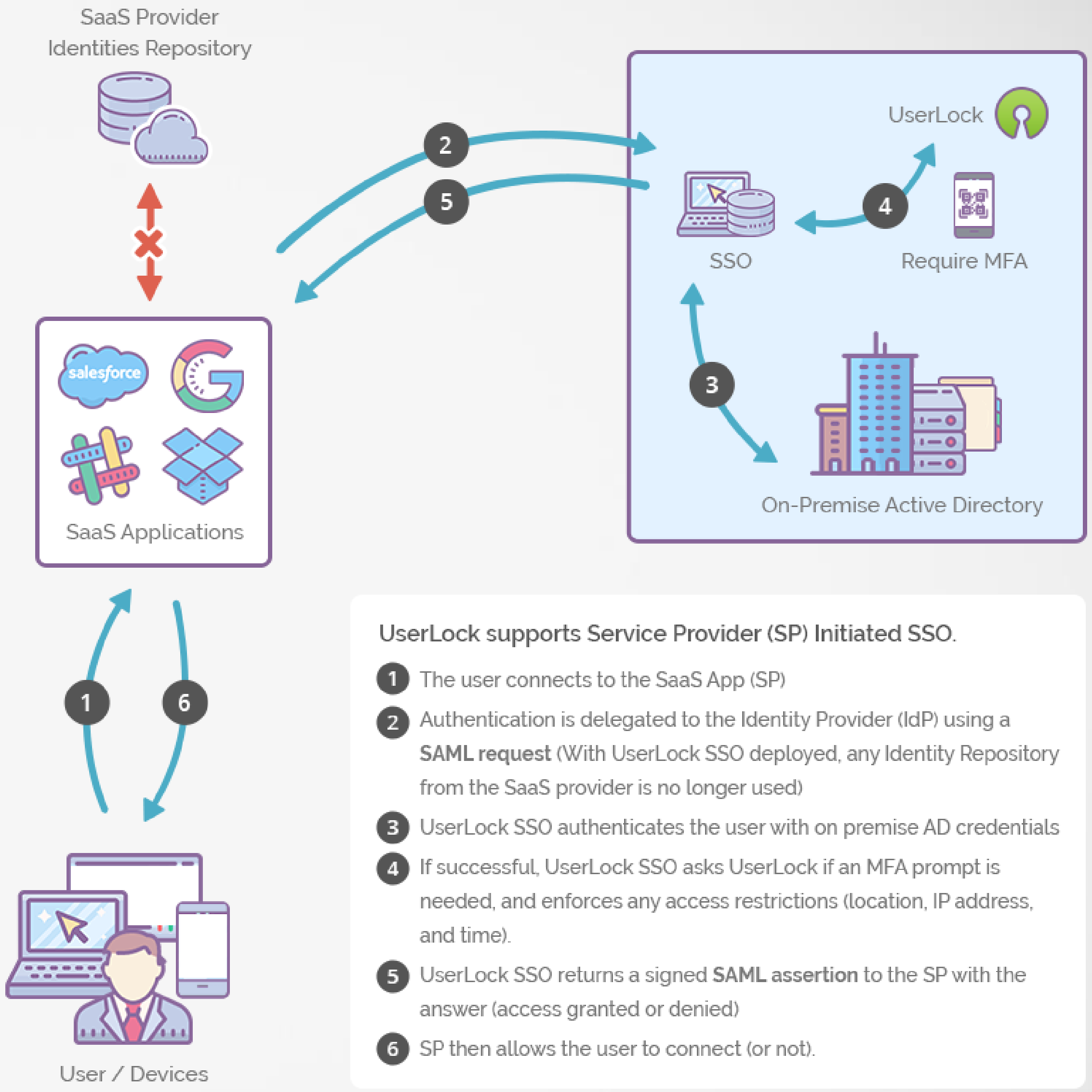
HOW **USERLOCK** SINGLE SIGN-ON WORKS

USERLOCK SSO FOR SAAS APPLICATIONS

UserLock SSO is hosted on premise and **retains Active Directory as the authoritative Identity Provider**.

For access to SaaS Applications, the user is authenticated with their **existing on premise credentials**.

Users may be prompted for **Two-Factor Authentication**, depending on the conditions that are set.



UserLock supports Service Provider (SP) Initiated SSO.

1. The user connects to the SaaS App (SP)
2. Authentication is delegated to the Identity Provider (IdP) using a **SAML request** (With UserLock SSO deployed, any Identity Repository from the SaaS provider is no longer used)
3. UserLock SSO authenticates the user with on premise AD credentials
4. If successful, UserLock SSO asks UserLock if an MFA prompt is needed, and enforces any access restrictions (location, IP address, and time).
5. UserLock SSO returns a signed **SAML assertion** to the SP with the answer (access granted or denied)
6. SP then allows the user to connect (or not).

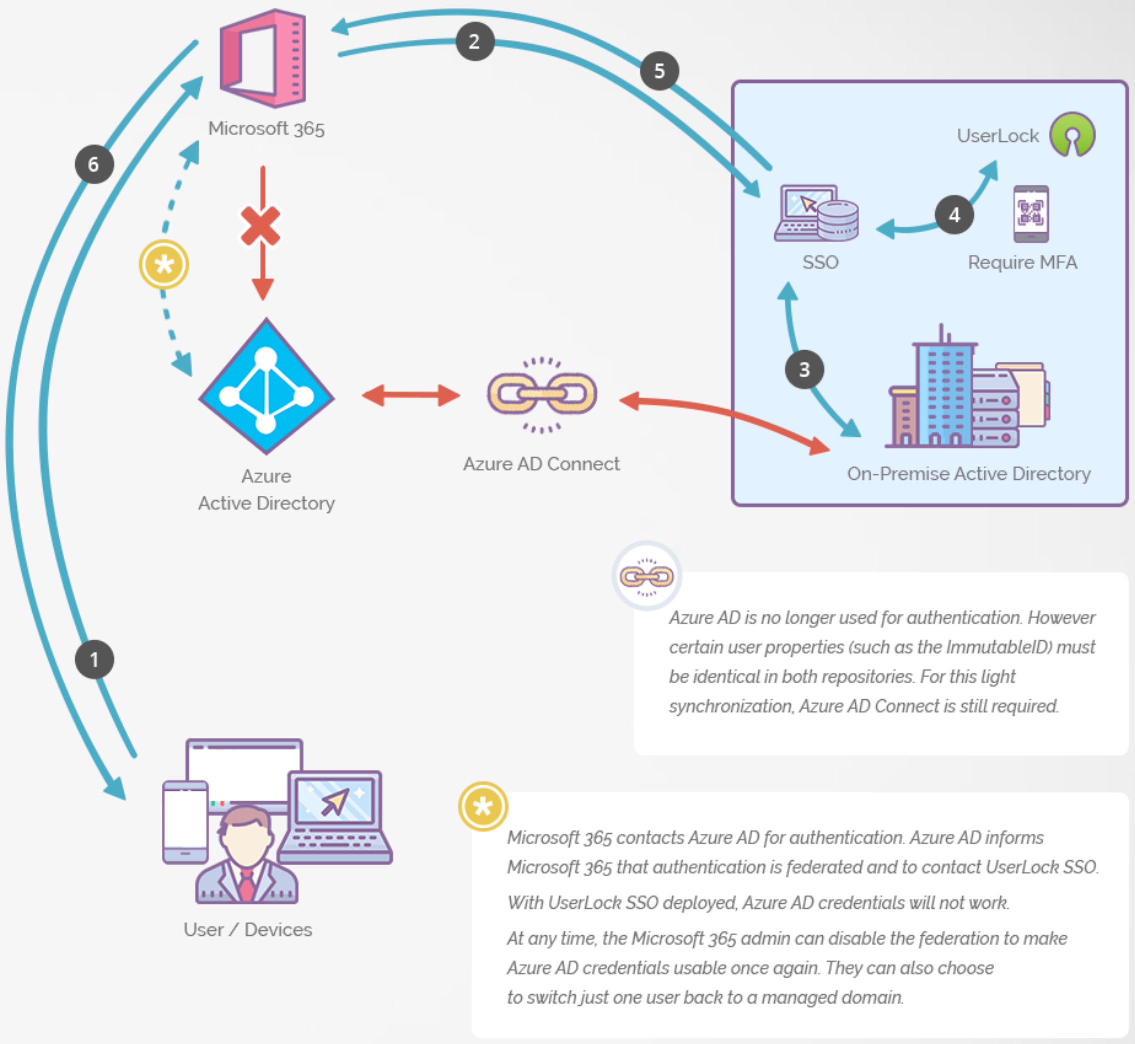
HOW **USERLOCK** SINGLE SIGN-ON WORKS

USERLOCK SSO FOR MICROSOFT 365

UserLock SSO is hosted on premise and **retains Active Directory as the authoritative Identity Provider**.

For access to Microsoft 365, the user is authenticated with their **existing on premise credentials**.

Users may be prompted for **Two-Factor Authentication**, depending on the conditions that are set.



Azure AD is no longer used for authentication. However certain user properties (such as the ImmutableID) must be identical in both repositories. For this light synchronization, Azure AD Connect is still required.

Microsoft 365 contacts Azure AD for authentication. Azure AD informs Microsoft 365 that authentication is federated and to contact UserLock SSO.

With UserLock SSO deployed, Azure AD credentials will not work.

At any time, the Microsoft 365 admin can disable the federation to make Azure AD credentials usable once again. They can also choose to switch just one user back to a managed domain.

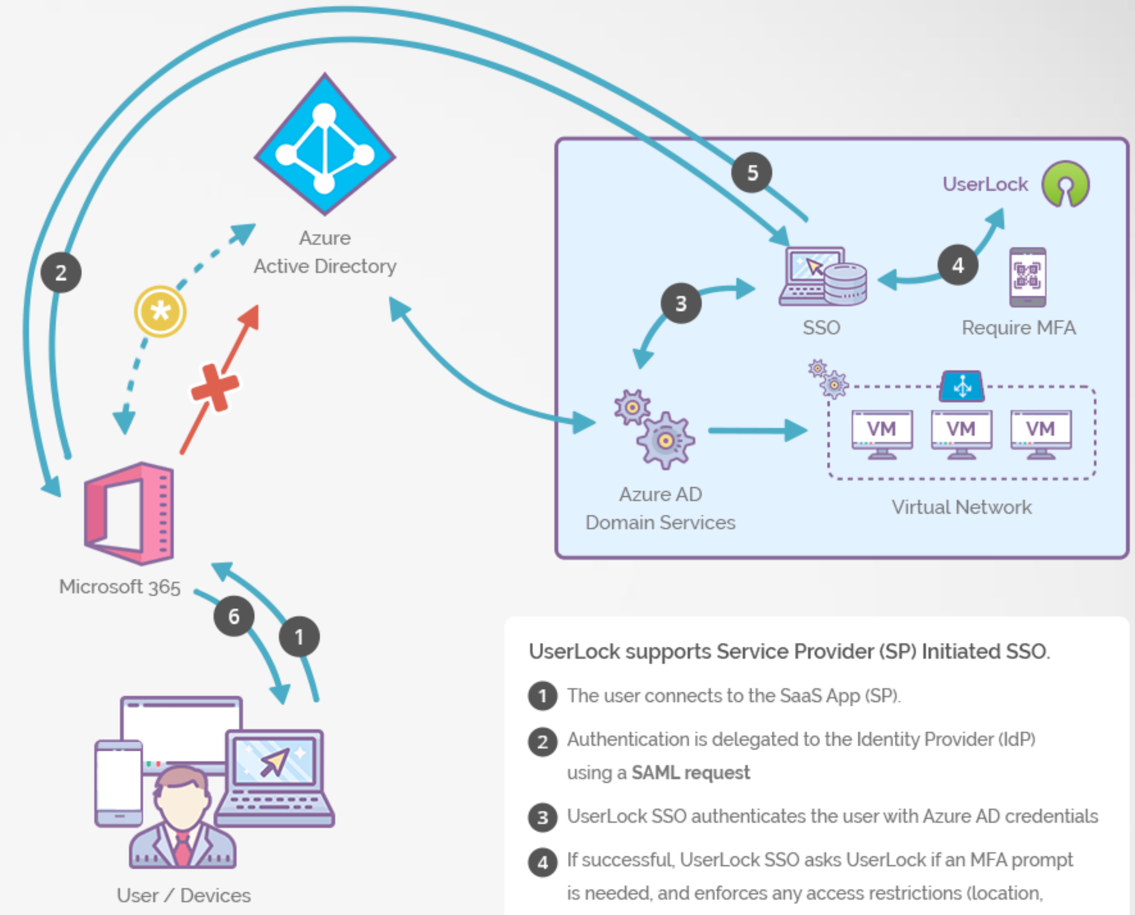
HOW **USERLOCK** SINGLE SIGN-ON WORKS

USERLOCK SSO FOR MICROSOFT 365 WITH AZURE AD DOMAIN SERVICES

UserLock SSO can be hosted on a virtual network and **use Azure Active Directory as the authoritative Identity Provider**.

For access to SaaS Applications, the user is authenticated with their **Azure AD credentials**.

Users may be prompted for **Two-Factor Authentication**, depending on the conditions that are set.



Microsoft 365 contacts Azure AD for authentication. Azure AD informs that authentication is federated and to contact UserLock SSO.

UserLock supports Service Provider (SP) Initiated SSO.

1. The user connects to the SaaS App (SP).
2. Authentication is delegated to the Identity Provider (IdP) using a **SAML request**
3. UserLock SSO authenticates the user with Azure AD credentials
4. If successful, UserLock SSO asks UserLock if an MFA prompt is needed, and enforces any access restrictions (location, IP address, and time).
5. UserLock SSO returns a signed **SAML assertion** to the SP with the answer (access granted or denied)
6. SP then allows the user to connect (or not).

OUR INTERNATIONAL TEAM

Since 2000, IS Decisions has worked to develop security software that can bolster your defense against unauthorized and unwanted access.

Whether helping partners at international events, writing for leading security publications or speaking at events, the industry respects our people for their access management know-how.

IS Decisions®

www.isdecisions.com

info@isdecisions.com