Enhancing Security & Compliance in Windows Workspaces with ProfileUnity™

Whitepaper

Introduction

This Whitepaper and guide has been authored by experts at Liquidware in order to provide information and guidance concerning the use of ProfileUnity to enhance security and compliance in Windows Workspaces.

Information in this document is subject to change without notice. No part of this publication may be reproduced in whole or in part, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any external use by any person or entity without Liquidware's express prior written consent.

Liquidware
3600 Mansell Road
Suite 200
Alpharetta, Georgia 30022
U.S.A.
Phone: 678-397-0450
www.liquidware.com

Contents

Overview

As the leader in user and application management for modern Windows workspaces, ProfileUnity™ and FlexApp™ provide enterprises with the security, flexibility, and control needed to protect users, applications, and data — without compromising productivity.

A key advantage of ProfileUnity and FlexApp is that they are developed and supported by a USA-based company with USA-based developers. Liquidware has many years of experience working with high-security federal environments, ensuring our solutions meet the stringent cybersecurity and compliance standards required by government agencies and contractors.

IT teams face increasing challenges in securing Windows environments — balancing workspace lockdown, compliance, and access control while ensuring a seamless user experience. Traditional security measures, such as granting local administrator privileges or enforcing restrictive policies, often lead to operational inefficiencies and increased security risks.

ProfileUnity addresses these challenges by offering secure profile management, workspace lockdown, application rights management, secure privilege elevation, and context-aware settings, among other security capabilities. These features help IT teams enforce security policies at a granular level, ensuring that users operate within controlled environments while maintaining productivity.

FlexApp enhances security further by delivering applications dynamically while leveraging technologies like OAuth authentication and other access controls to ensure that only authorized users can open and use an application. By decoupling applications from the base OS, organizations can reduce attack surfaces and streamline application management without adding administrative overhead.

Together, ProfileUnity and FlexApp empower organizations to create a secure, compliant, and efficient Windows workspace that meets the needs of modern workforces, including federal agencies and highly regulated environments.

The Need for Securing Modern Windows Workspaces

Modern IT environments face evolving security threats, requiring adaptive, proactive security measures to protect user data, applications, and system integrity. Some of the primary risks include:

- Insider Threats: Unauthorized privilege escalation and application misuse by internal users.
- Application Security: Persistent software installations increase attack surfaces.
- Compliance Requirements: Federal agencies and enterprises must adhere to strict regulations, such as CISA & NIST for high security and zero trust.

To address these risks, organizations require solutions that deliver dynamic, policy-driven security without disrupting user experience or IT operations.

How ProfileUnity and FlexApp Provide Flexible Security Solutions

ProfileUnity and FlexApp deliver comprehensive security across three critical layers:

- User Environment Security: Secure profile management, role-based access control (RBAC), and session-aware security policies.
- Application Security: Secure dynamic application delivery, blocking unauthorized access while maintaining flexibility.
- Zero Trust Security & Compliance: Granular access control, immutable audit logs, and adaptive security policies aligned with federal cybersecurity best practices.

These capabilities ensure that organizations can enforce strong security policies while maintaining operational flexibility.

Data Sovereignty & Ownership

Liquidware does not store or manage client data. Organizations using ProfileUnity and FlexApp retain complete control over their data, profiles, and configurations, ensuring compliance with federal data security policies.

Insider Threat Protection

Unlike SaaS-based or cloud-hosted solutions, ProfileUnity and FlexApp run entirely within an organization's infrastructure, ensuring that federal agencies and high-security environments maintain complete control over their data and configurations. Even if the administration console is offline, ProfileUnity and FlexApp continue to operate seamlessly, enforcing policies, managing profiles, and delivering applications dynamically.

Additionally, ProfileUnity fully supports Windows Access Control Lists (ACLs) and does not require open 'Everyone' access, as some competing solutions or profile disks do. This ensures fine-grained security and compliance for highly regulated environments.

Securing ProfileUnity: Best Practices for Permissions, Audit Logging, and Access Control

Properly securing the ProfileUnity infrastructure itself is critical to maintaining the overall security posture of your Windows workspace environment. This section outlines best practices for securing ProfileUnity configuration files, shares, and management interfaces.

ProfileUnity File Share Security

a) Read and Write Permissions for ProfileUnity Administrators: The ProfileUnity configuration files should be stored in a secured network share where ProfileUnity administrators have read and write permissions to modify configurations. End users should only have read-only access to configuration files. No write or modify permissions should be granted to non-administrative users.

b) Profile Storage Folder Permissions: Typically, the folder where user profiles are stored should have: Creator Owner permission: Each user should only have access to their own profile data. ProfileUnity administrators should have read and write access for backup and recovery purposes. No blanket 'Everyone' or unrestricted access.

Additional Best Practices for Securing ProfileUnity

a) Limit ProfileUnity Console access to ensure only ProfileUnity administrators have access to the ProfileUnity Management Console.

b) Verify Folder Share Security Policies and optionally enable NTFS permissions auditing on the ProfileUnity file share to log unauthorized access attempts.

c) Ensure the file server hosting ProfileUnity shares follows industry-standard security hardening.

d) Protect ProfileUnity Executables & Scripts by regularly updating ProfileUnity to the latest version to patch security vulnerabilities.

e) Implement secure profile management practices to maintain integrity of user profiles. Enforce strong encryption for sensitive profile data.

By implementing these security best practices for ProfileUnity infrastructure, organizations can significantly reduce the risk of unauthorized access to configuration settings, profiles, and ensure the integrity of their ProfileUnity deployment.

Secure Profile Management

User profiles contain critical data, settings, and application configurations, making them a key security concern for IT administrators.

Profiles remain in your environment or cloud — never third-party storage

ProfileUnity ensures that user profiles remain within an organization's controlled environment — whether on-premises or in a private or public cloud — without being stored in third-party locations outside of IT's oversight.

By keeping profile data within the organization's infrastructure, ProfileUnity helps IT teams enhance security without disrupting user access or introducing unnecessary complexity.

Context-Aware Security Policies & Workspace Lockdown

Securing Windows workspaces requires adaptive policies that adjust dynamically based on user roles, devices, network environments, and session conditions. ProfileUnity provides flexible, context-aware security policies that enable IT teams to enforce workspace lockdown settings, restrict application access, and control Windows features in real time — ensuring a secure environment without disrupting productivity.

Adaptive security based on user role, device, network, and authentication

ProfileUnity enables IT administrators to apply security policies dynamically, adjusting access levels based on:

- User Identity & Role – Different policies for employees, contractors, and guest users.
- Device Type – Restricting access on BYOD devices while allowing full functionality on corporate-managed endpoints.
- Network Connection – Adjusting security policies if a user moves from a trusted internal network to an external or public network.
- Authentication Method – Enforcing additional security measures based on how users authenticate.
- Session Changes (Trigger Points) – Automatically enabling or disabling access to applications and Windows features based on real-time session events.

Locking down Windows features with secure policy enforcement

ProfileUnity effectively locks down workspaces by leveraging secure HKLM registry enforcement, ensuring that standard users cannot modify critical system settings. IT can enforce (by ProU controlling your custom HKLM registry settings):

- Control Panel & System Settings Restrictions – Preventing users from making unauthorized changes.
- Task Manager & Command Prompt Lockdown – Blocking access to tools that could be misused for privilege escalation.
- Registry Editor Restrictions – Ensuring that critical system settings remain intact.
- Application Access Controls – Dynamically hiding or blocking applications based on user policies.

Effectively creating a security perimeter with dynamic access control

While ProfileUnity does not track global locations, it effectively creates a security perimeter by restricting application access and Windows settings based on network and session conditions. Organizations can: Dynamically enable or restrict application access when users move between network environments. Prevent unauthorized application launches based on changing session conditions (e.g., automatically restricting access if a VPN disconnects).

Trigger Points to automatically adjust settings mid-session

By combining workspace lockdown with context-aware registry or config file settings, ProfileUnity helps IT:

- Reduce the attack surface by preventing unauthorized system changes.
- Ensure security policies adapt dynamically to changing conditions.
- Support compliance initiatives by enforcing granular access controls.
- Minimize IT burden by automating security adjustments instead of relying on manual intervention.

With ProfileUnity's adaptive security policies and Trigger Points, organizations can secure Windows workspaces dynamically, ensuring compliance and reducing risk — all without impacting user productivity.

Application Rights Management & Restrictions

Controlling which applications users can access and execute is a critical component of securing Windows workspaces. ProfileUnity provides flexible application rights management that allows IT to enforce security policies without the need for complex configurations or unnecessary administrative privileges.

Application blacklisting and whitelisting

ProfileUnity enables IT administrators to dynamically enforce application restrictions based on user identity, device type, network location, and other context-aware conditions. This includes Application Blacklisting & Whitelisting to prevent unauthorized applications from running while ensuring approved applications remain accessible.

Application cloaking to hide unauthorized apps

Application Cloaking hides specific applications from users who are not authorized to see or launch them.

Blocking specific executables to prevent unauthorized access

Blocking Specific Executables to prevent users from launching unauthorized or potentially harmful applications.

One of the most common security pitfalls is granting local administrator privileges just so users can run certain applications. ProfileUnity eliminates this risk by providing secure privilege elevation, allowing users to run applications with admin-level rights only when necessary and without granting full system-wide administrative access.

Organizations can apply dynamic security policies to control who can access which applications and under what conditions. Policies can be enforced based on:

- User Role – Different application rights for employees, contractors, and guest accounts.
- Device Type – Enforcing stricter policies on BYOD and personal devices.
- Network Location – Restricting applications based on whether users are inside a corporate network, connected via VPN, or using a public connection.

By enforcing application controls dynamically, ProfileUnity helps organizations:

- Reduce attack surfaces by limiting unnecessary application access.
- Ensure compliance with security frameworks that require strict access controls.
- Prevent privilege escalation attacks by restricting admin-level execution to only approved applications.

With ProfileUnity's application rights management, organizations gain better control over software access, reduce security risks, and eliminate the need for unnecessary administrative privileges—all while maintaining user productivity.

Limiting Admin Privileges

One of the most common security risks in Windows environments is granting local administrator privileges to users who need elevated access for specific applications. This practice increases the risk of malware execution, unauthorized system changes, and compliance violations. ProfileUnity eliminates this risk by enabling basic privilege elevation—allowing applications to run with admin-level permissions without requiring users to be full system administrators.

Enabling application-level admin rights without full system admin access

ProfileUnity enables IT to elevate application permissions dynamically based on context-aware rules rather than granting blanket administrative access. This allows:

- Selective privilege elevation for specific applications that require admin rights. No need to grant full local admin access to end users.
- Dynamic enforcement based on security policies rather than manual IT intervention.

Context-aware elevation based on user, device, and session conditions

Privilege elevation in ProfileUnity is not a one-size-fits-all solution; it is applied based on security rules that adapt to user needs and risk levels. IT administrators can define privilege elevation policies based on:

- User Role – Ensuring only designated users receive elevated rights.
- Application Type – Limiting elevation to business-critical applications while blocking risky executables.
- Device & Network Context – Restricting privilege elevation on unmanaged or off-network devices.

By enabling applications to run with elevated rights instead of users, ProfileUnity:

- Eliminates the need for local admin rights, reducing security vulnerabilities.
- Prevents privilege escalation attacks that exploit admin-level permissions.
- Allows IT to maintain a principle of least privilege while supporting end-user productivity.

With ProfileUnity's secure privilege elevation, organizations can enforce stronger security policies without interrupting users or requiring excessive IT involvement.

Secure Application Delivery with FlexApp

Traditional application deployment methods often introduce security challenges, such as permanent application installs, excessive administrative privileges, and increased attack surfaces. FlexApp eliminates these risks by delivering applications dynamically, ensuring they are only available when authorized and under the right conditions.

Reducing attack surfaces with dynamic application delivery

Unlike traditional software installations, FlexApp applications are not permanently installed on the endpoint. Instead, they are attached dynamically at login or on demand, providing several security advantages:

- Applications only exist when needed – reducing the risk of persistent vulnerabilities.
- No need for full admin rights – applications can be assigned without requiring users to install or modify system settings.
- Automatic detachment – applications can be removed cleanly without leaving behind system modifications or potential attack vectors.

Controlling app availability based on user identity, device, and network conditions

FlexApp ensures that applications are only available under authorized conditions, helping IT enforce security policies while maintaining user productivity. Application delivery can be controlled based on:

- User Identity & Group Membership – Only authorized users can access specific applications.
- Device Type & Compliance Status – Applications can be restricted on unmanaged or non-compliant devices.
- Network & Session Conditions – Applications can be dynamically enabled or disabled based on whether a user is on a secure corporate network or connected through a VPN.

OAuth authentication and access controls to restrict unauthorized application usage

FlexApp One enhances security with OAuth-based authentication and other access control mechanisms, ensuring that:

- Only approved users can open an application, even if it is delivered to their session.
- Access to applications can be revoked instantly without modifying the base image or uninstalling software.
- IT can enforce security policies on a per-application basis, ensuring compliance with internal access control standards.

By dynamically delivering applications only when needed and under the right conditions, FlexApp helps organizations:

- Reduce security risks by keeping applications detached when not in use.
- Limit user privileges while still providing necessary software access.
- Streamline compliance efforts with controlled application delivery and access logging.

With FlexApp, organizations gain a powerful way to secure application delivery without locking users into restrictive environments — ensuring both security and flexibility in modern Windows workspaces.

Secure Administration, Auditing, and Compliance

Managing security for Windows workspaces requires centralized control over administrative actions and visibility into system changes to ensure compliance. The Liquidware Management Console provides Role-Based Access Control (RBAC), auditing, and summary reporting, helping organizations enforce security policies while maintaining a clear record of administrative activity.

Role-Based Access Control (RBAC) for ProfileUnity and FlexApp

RBAC ensures that administrative access is restricted based on role, reducing security risks associated with overprivileged accounts. Within the Liquidware Management Console, IT administrators can:

- Assign different permission levels to administrators, support staff, and auditors.
- Limit access to ProfileUnity and FlexApp configurations based on user roles.
- Enforce separation of duties by restricting who can modify security-sensitive settings.

Microsoft Active Directory integration for centralized authentication

The Liquidware Management Console integrates with Active Directory, allowing organizations to centrally manage access controls using existing AD roles and security groups. This provides:

- Seamless authentication using corporate credentials.
- Automatic permission updates when AD roles change.
- A consistent, organization-wide security policy.

Auditing and summary reports for compliance and security tracking

To support security and compliance efforts, ProfileUnity and FlexApp provide administrative activity reports that offer insights into:

- Profile and application configuration changes – Tracking modifications to settings and security policies.
- Application access policies – Showing how application rights are assigned and enforced.
- Administrative actions – Logging updates made within the management console for accountability.

These reports help organizations meet compliance requirements for security audits, internal governance, and industry regulations. IT teams can use them to track policy enforcement, maintain records for audits, and demonstrate adherence to security best practices.

By combining RBAC, auditing, and reporting in a single, streamlined platform, ProfileUnity and FlexApp provide centralized security controls while ensuring that administrative activities are documented for compliance and accountability.

Federal Security & Compliance Enhancements

Part of a Multi-Layered process to CISA and NIST Compliance

ProfileUnity, when used with FlexApp One, helps meet compliance for Zero Trust security architecture, aligning with federal cybersecurity best practices.

Offline & Air-Gapped Security

Unlike cloud-reliant solutions, ProfileUnity's configuration console can operate entirely offline, ensuring that federal agencies maintain full operational capability even in air-gapped networks.

Zero Trust Security Model

ProfileUnity and FlexApp ensure that user data and profiles remain securely within the enterprise infrastructure, never stored in the cloud or a SaaS environment, ensuring full administrative control.

Granular Role-Based Access & Auditing

RBAC ensures only authorized personnel can modify security settings. Comprehensive, immutable audit logs support compliance mandates & forensic security reviews.

Privacy, Security, and Compliance Policies

Privacy Policy

Liquidware respects the privacy of our customers, business partners, and other visitors to our websites. We do not collect, process, or store customer data — organizations using Liquidware solutions retain full control over their data and configurations.

For full privacy policy details, visit: Liquidware Privacy Policy
https://www.liquidware.com/disclosures#privacy-policy

Security Standards

Liquidware adheres to industry-leading security frameworks, including: SOC 2 Type II Compliance ISO/IEC 27001:2022 Certified PCI-DSS Compliant Regular Penetration Testing & Security Audits

For full security policy details, visit: Liquidware Security Policy
https://www.liquidware.com/disclosures#security

Regulatory Compliance

Liquidware solutions are part of a multi-layered approach to align with federal and industry security regulations, including: CISA & NIST Zero Trust Framework GDPR & Data Protection Regulations HIPAA & Healthcare Security Standards.

Liquidware Corporate Security

Supply Chain Security

Liquidware only works with vendors that meet strict security and compliance requirements. Our supply chain is highly scrutinized, ensuring that all partners align with industry-leading security practices.

Insider Threat Protection

All Liquidware employees undergo comprehensive background checks before being granted access to source code or sensitive systems. We enforce strict access controls, ensuring that only authorized personnel can interact with mission-critical components.

Corporate compliance details, visit: Liquidware Compliance Page
https://www.liquidware.com/disclosures#compliance

Conclusion

Securing Windows workspaces requires a comprehensive approach that balances strong security controls with user productivity. ProfileUnity and FlexApp provide IT teams with flexible, context-aware security solutions that help organizations lock down workspaces, enforce access controls, and deliver applications securely—all without introducing unnecessary complexity.

By leveraging features such as secure profile management, application rights management, privilege elevation, and context-aware security policies, ProfileUnity ensures that users operate within a controlled, compliant environment. Meanwhile, FlexApp enhances security by delivering applications dynamically, ensuring that only authorized users can access them.

With role-based access control (RBAC), administrative auditing, and compliance reporting, the Liquidware Management Console provides visibility and accountability, enabling IT to manage security policies effectively. Organizations can enforce least-privilege access, prevent unauthorized system changes, and meet compliance requirements with confidence.

By integrating ProfileUnity and FlexApp One, federal agencies gain a hardened, compliant, and highly secure environment that supports:

- Zero Trust practices and application enforcement Granular role-based access & session-based security controls Air-gapped, offline-capable operation
- Adaptive security measures that dynamically adjust based on risk factors.

Contact Information

For more information about Liquidware's Digital Workspace Management solutions, please contact sales@liquidware.com or visit www.liquidware.com.