CyberQP

Why MSPs Need Just-in-Time Accounts

Table of Contents

Key Findings

Managing Privileged Access Is A Top Concern for MSPs: Many small and medium-sized businesses (SMBs) are asking their Managed Service Providers (MSPs) how they are protecting key client accounts and data, as more security breaches and supply chain attacks make headlines in the news cycle.

Cyber Insurance and Compliance Requirements Remain Top-of-Mind: As identity-centric attacks continue to spike for SMBs and enterprises alike, cybersecurity insurance firms are taking notice and beginning to ask MSPs if they are implementing safety measures and tools designed to combat these threats. Today, MSPs are looking for security-focused partners and solutions that can help them align with best practices and attain or maintain their cyber insurance eligibility with a robust cybersecurity program.

Remote and Hybrid Work Creates New Security Concerns: Traditionally shared admin accounts are not enough anymore. In today's Work-From-Anywhere landscape, MSPs need robust privileged access management controls to minimize their cyber risk and manage growing attack surfaces. In order to address risks created by employee turnover or bringing in temporary contractors, MSPs need a dynamic solution that ensures they can grant privileged access strictly for a necessary period of time to minimize vulnerability windows and exposure of sensitive data and accounts.

It's clear that MSPs need a security-first partner and platform that integrates across their technology stack to automate help desk technician workflows and streamline the management of privileged, local, and service accounts.

Following Best Practices with Your MSP's Privileged Accounts

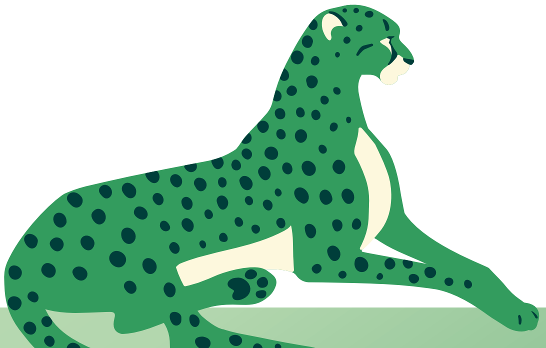
As MSPs' attack surfaces continue to grow with their client base, protecting their privileged accounts becomes a key line of defense to prevent threat actors from exfiltrating sensitive data through privilege escalation or lateral movement attempts.

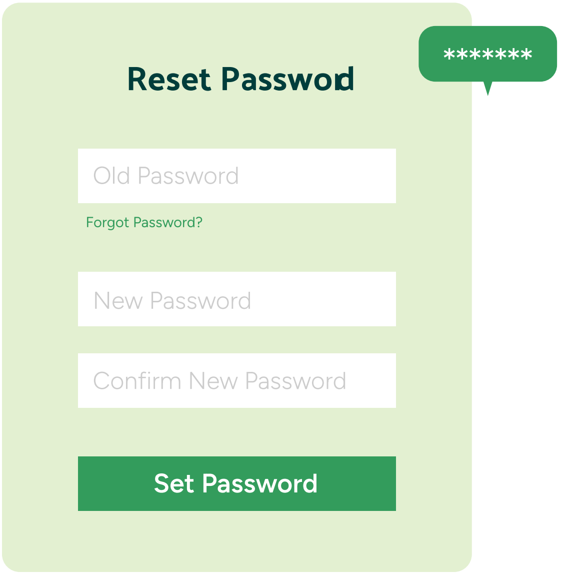
Text BoxAs cyber criminals start using tactics that target privileged accounts and identities, cybersecurity insurance providers and policy makers are outlining compliance frameworks and requiring that MSPs adopt Privileged Access Management tooling with robust features (including Just-in-Time access) that mitigate MSP and SMB risks by closing visibility or security gaps.

Passwords per Person

The average person has around **100 passwords**. That's a **25% increase** in the average number of passwords per person from 2021.

(Source: NordPass)





Following Best Practices with Your MSP's Privileged Accounts

As MSPs' attack surfaces continue to grow with their client base, protecting their privileged accounts becomes a key line of defense to prevent threat actors from exfiltrating sensitive data through privilege escalation or lateral movement attempts.

As cyber criminals start using tactics that target privilege accounts and identities, cybersecurity insurance providers and policy makers are outlining compliance frameworks and requiring that MSPs adopt features (including Just-in-Time access) that mitigate MSP and SMB risks by closing visibility or security gaps.

Rapid Attack Surface Growth

133% Year-Over-Year Growth in **Number of Security Assets**

Achieve Zero Standing Privilege with Just-in-Time Accounts

Just-in-Time (JIT) privileged accounts offer MSPs a scalable and secure way of maintaining momentum without sacrificing security. By offering temporary access, MSPs can minimize standing privilege and risk associated with technicians having 24/7 access to privileged accounts.

PAM tools with robust JIT creation minimize vulnerability windows by:

Dynamically Limiting Access

to sensitive resources on an as-needed basis.

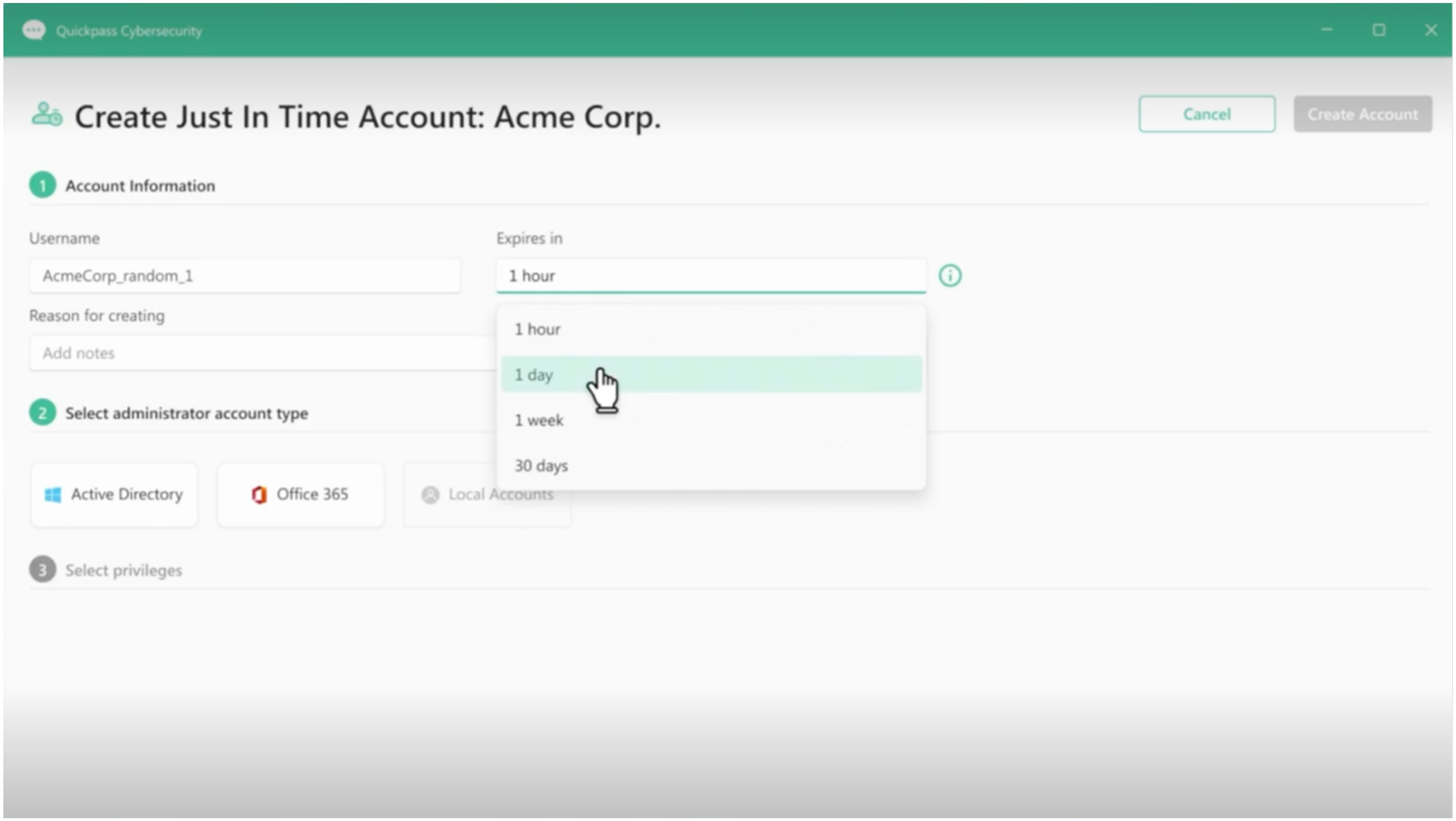
Mitigating Insider Threats

by automating administrative controls and revoke access at will.

Complying With Best Practices

by generating comprehensive audit logs and clean dashboards, for better visibility and accountability.

The Principle of Least Privilege requires a security architecture that grants the minimum number of permissions or resources that a technician needs for their workflow.



Create Just In Time Account: Acme Corp.

1 Account Information

Username: AcmeCorp_random_1

Expires in: 1 hour

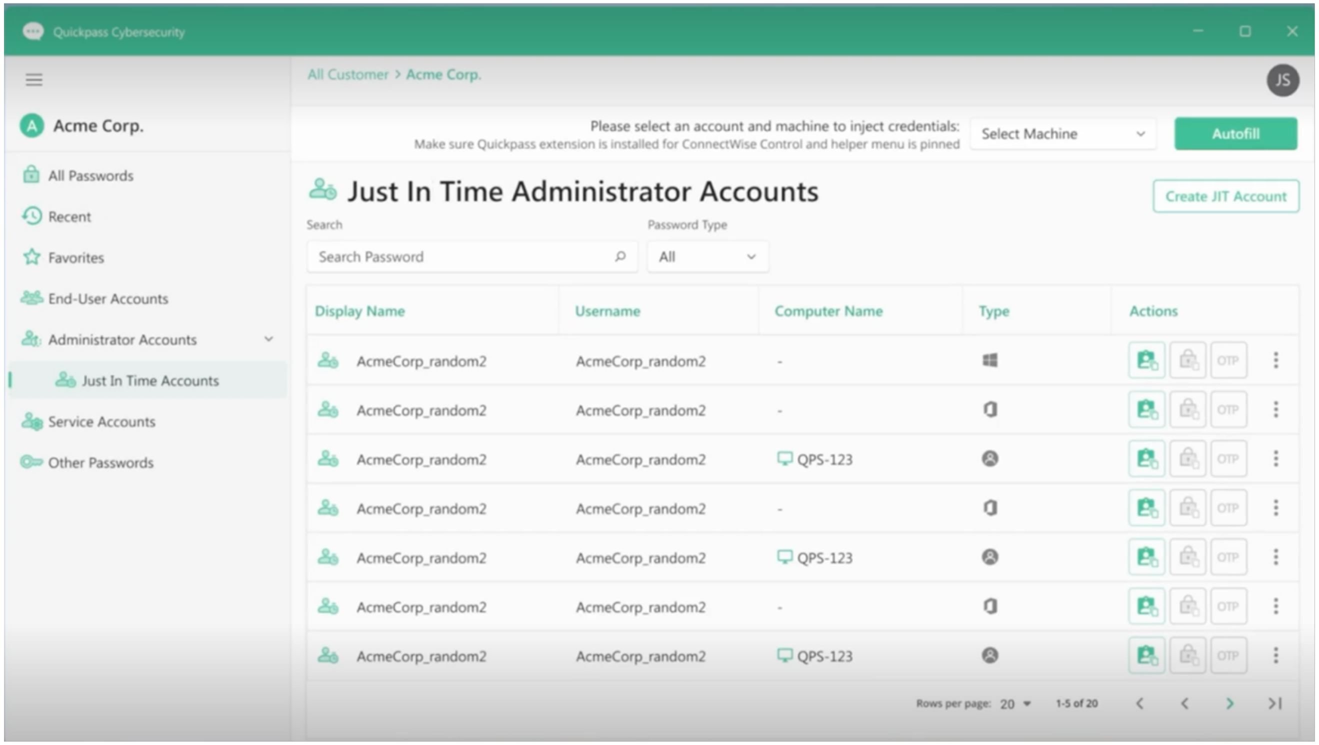
Reason for creating: Add notes

2 Select administrator account type

3 Select privileges

Streamline and Secure Co-Managed IT Agreements with On-Demand Account Creation

MSPs clearly need Privileged Access Management tooling that is purpose-built for all types of client environments.



Please select an account and machine to inject credentials:
Make sure Quickpass extension is installed for ConnectWise Control and helper menu is pinned

Just In Time Administrator Accounts

Display Name	Username	Computer Name	Type	Actions
AcmeCorp_random2	AcmeCorp_random2	-	⊞	OTP ⋮
AcmeCorp_random2	AcmeCorp_random2	-	▯	OTP ⋮
AcmeCorp_random2	AcmeCorp_random2	QPS-123	●	OTP ⋮
AcmeCorp_random2	AcmeCorp_random2	-	▯	OTP ⋮
AcmeCorp_random2	AcmeCorp_random2	QPS-123	●	OTP ⋮
AcmeCorp_random2	AcmeCorp_random2	-	▯	OTP ⋮
AcmeCorp_random2	AcmeCorp_random2	QPS-123	●	OTP ⋮

CyberQP enables MSPs with Just-in-Time account creation designed for both conventional managed service agreements and co-managed IT offerings. MSPs can invite a client's key IT or security managers to CyberQP's platform and offer them the exact level of access they need with temporary admin accounts.

Conclusion

Just-in-Time (JIT) privileged accounts offer MSPs a scalable and secure way of maintaining momentum without sacrificing security. By offering temporary access, MSPs can minimize standing privilege and risk associated with technicians having 24/7 access to privileged accounts.

PAM tools with robust JIT creation minimize vulnerability windows by:

On-demand Account Creation

Empower technicians to create new, temporary accounts on demand to give users access to what they need for a specific period of time.

Zero Standing Privilege

Minimize the risk of security breaches, stoled credentials, and privilege abuse by only activating privileged accounts when thy are being used.

Safeguard Access

Increase your MSP's security by limiting the number of people who have access to sensitive information at all times.

Compliance & Cyber Insurance

Make it easier to stay in compliance and adhere to cyber insurance requirements by minimizing the number of users who have ongoing access to privileged information and systems.

By implementing just-in-time account creation into your MSP's workflows, you can both close internal gaps in your MSP's security gaps, and enable technicians or contractors to get and use privileged access for limited amounts of time and complete work that matters to you and your company.

MSPs partner with CyberQP to protect the information and accounts that matter to them. With QGuard, you can deploy a complete Privileged Access Management solution as part of your cybersecurity program to discover, monitor, and manage privileged accounts across your client base and security estate, and align with cyber insurance eligibility requirements or best practices in line with compliance frameworks like NIST and CIS in the process.

To learn more about how CyberQP can help you keep your business secure and eliminate operational costs to maximize value for your customers, you can book a demo **here** or visit us on our **website**.