Quickpass

ITGlue

# Security Best Practices for Protecting IT Glue Passwords

## Contents

# 1 The State of Passwords

MSPs use IT Glue because it is the most powerful documentation platform designed for MSPs. An integral part of IT Glue's documentation platform is their password manager. Their password manager is easy to use and the best part about it is you can link passwords to other records in your documentation such as servers, network devices and applications to name of few. All of this valuable information is available in one place. IT Glue also does a great job at keeping your documentation secure by being SOC 2 compliant, encrypting your passwords at rest and proving substantial security auditing and reporting capabilities. Nonetheless, there are security challenges and risks that IT Glue customers face with their passwords.

2

# Security Best Practices

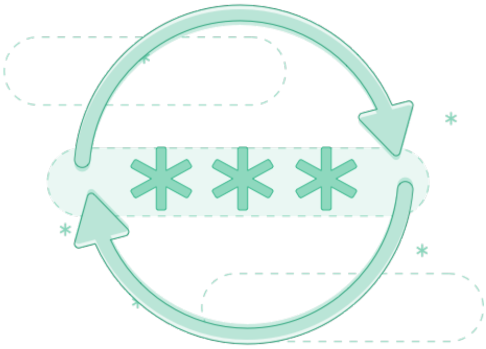
The following is a list of the top areas that IT Glue customers must deal with to ensure they are following security best practices.

## Critical administrator and service account passwords

Avoid using common passwords or previously breached passwords

- Minimum **12-15 characters** in length
- Use **passphrases** instead of completely random complex passwords as they are easier to remember and more difficult to crack
- Use a **password generator** if possible
- Remember 10 **password history**
- **Lockout policy** 3 attempts
- Use **MFA** where available
- Limit the number of accounts that have Domain or Enterprise Admins group privileges in Active Directory
- Secure the built-in Administrator account
  - Enable the Account is sensitive and cannot be delegated
  - Enable the smart card is required for interactive logon
  - Deny access to this computer from the network
  - Deny logon as batch job
  - Deny log on as a service
  - Deny log on through RDP

- Limit the accounts that can login to Active Directory domain controllers and leverage remote tools to manage common user management tasks.
- Avoid using common passwords or previously breached passwords
- Do not use the same password that you use personally, for other online services or any variation of the same
- **Rotate** on a recurring basis and/or when technicians turnover especially if MFA is not available
- Password formulas consistent across all customers should be avoided
- Do not use the same password at each customer



Rotate Password on recurring basis

## Local administrator account passwords on end-user workstations

- Minimum **12-15 characters** in length
- Use **passphrases** instead of completely random complex passwords as they are easier to remember and more difficult to crack
- Use a **password generator** if possible
- Do not use the same password that you use personally, for other online services or any variation of the same
- Rotate on a recurring basis and/or when technicians turnover
- Password formulas used at all customers should be avoided

- Never use the same password at each customer
- Disable the default local administrator account on all end-user workstations

## End-User Passwords

Use MFA if available

- Minimum **12-15 characters** in length
- Use **passphrases** instead of completely random complex passwords as they are easier to remember and more difficult to crack
- Use **MFA** where available
- Remember 10 **password history**
- **Lockout polic**y 3 attempts
- Avoid using common passwords or previously breached passwords
- Do not use the same password that you use personally, for other online services or any variation of the same
- Accessing end-user workstation or email passwords to perform maintenance and support when they are out of the office

## Preventing Help Desk Social Engineering Attacks

- Have a system in place to verify customer identities
- Provide a procedure to your customers that allows them to **confirm the identity of your MSP** technicians when they receive a call

3

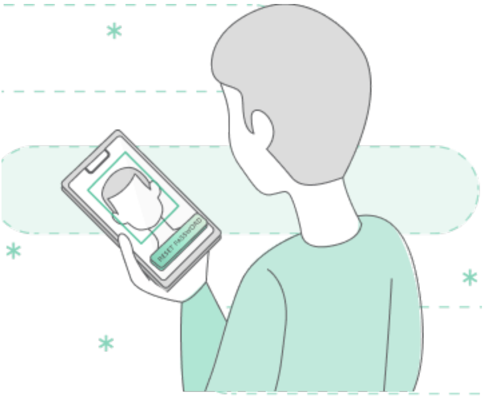
## Challenges

Adhering to the guidelines above is good in theory for an MSP but many of these guidelines can be difficult to implement, enforce and consistently follow. **The greatest asset of an MSP is time.** Time for an MSP is at the best of times very limited. Any task that requires redundant manual effort is highly likely to be done incorrectly or not done at all. In a perfect world all your customers would all be standardized and running the latest hardware, software and operating systems. The truth is a lot of MSPs must deal with a wide variety of systems and applications and implementing the latest and greatest technologies is not always feasible. User adoption can also be challenging. The result is MSPs need solutions that fit with their current realities and constraints.

Time is limited, frustration of technician of doing things manually

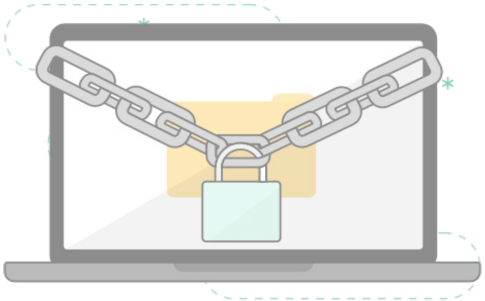
Using passphrases instead of standard complex passwords is a great way to increase the security of your account. Although Microsoft recommends only 8 characters these can be easily hacked meanwhile longer passphrases are much more difficult. According to ZDNet, *"The idea behind the FBI's advice is that a longer password, even if relying on simpler words and no special characters, will take longer to crack and require more computational resources."* There are several different opinions on the recommended minimum length for passphrases such as 12, 15 or more but you must balance this with what your customers can realistically follow. Choose what works for your MSP. You can check out passphrase generators such as https://www.useapassphrase.com/ or https://untroubled.org/pwgen/pwgen.cgi for more information.

Implementing MFA for all your accounts is one of the best ways to secure them. However, this is not always possible with customer Active Directory systems due to dated versions of Windows server, cost and user adoption. MFA is also not immune to hacking. According to Secureworld, "*The MFA attack known as Network Session Hijacking has compromised millions of accounts.*" Microsoft does offer great tools including AD Connect and Microsoft Authenticator but MSPs can often find these more geared to the Enterprise and challenging to deploy and manage across all their customers. Microsoft also currently recommends not changing or rotating your administrator passwords. Although this may be feasible with MFA on all your accounts this does not consider that technicians can quit and be fired and can still get access to your customer systems with malicious intent if you never change the passwords. According to Huntress Labs, *"MSPs need to closely audit admin accounts after employees depart"*, after covering a story about a former MSP technician who was fired tried to sell all the MSPs passwords on the dark web. Also, never changing the password does not address the risk of key logging malware that may infect a technician's computer giving a hacker access to both the username and password to your customers critical administrator account. In an article by ZDNet, PyXie RAT keylogging malware is *"used to steal usernames, passwords and any other information in the system"* which leave MSP customers quite vulnerable if a technicians computer used to login to their servers is infected.



MFA for all your accounts is one of the best ways to secure them.

Subsequently, MSPs are forced to address the need to rotate critical administrator passwords on customer servers. Rotating these passwords manually can be a huge task whether on a recurring basis or when a technician quits or is let go. Consequently, MSPs can fall into the trap of using a formula for their passwords that is used at all their clients, simply using the same password across clients and/or never changing the password because they just don't have the time or the resources to do it.

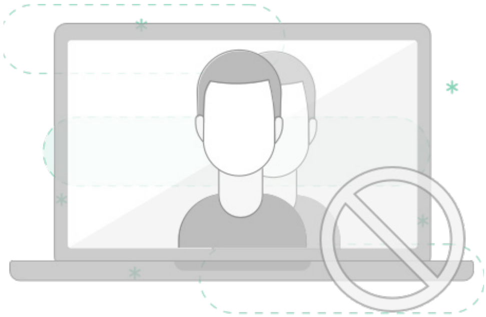


Hackers infecting technicians computers with key-logging malware

Another challenge for MSPs relate to local administrator accounts on PC's. PC's that are joined to an Active Directory domain can sometimes lose their trust relationship and subsequently locking users out of their machines in addition to Active Directory administrator accounts. To address this problem most MSP's will create a local administrator account that is a back door to the end-user workstation in the event the PC loses its trust relationship with Active Directory or is offline and can't connect to Active Directory. A common tactic is to use the same username and password at all their clients leaving a significant back door to all their customer PCs if someone were to hack their username and password or more likely a previous technician. According to Virtual Administrator on local administrator passwords, *"If you are like many MSPs that password is the same across ALL your clients...Maybe you are better than most, and actually create a separate password for each client".*

Ideally each computer would have a separate password on each PC and to do this MSPs need to implement a solution such as Microsoft Local Administrator Password Solution (LAPS) Otherwise, MSPs require very persistent documenting of these passwords in your password manager and the time required to manually rotate these passwords on all client PC's is an impossible task for most MSPs.

Many small business clients of MSPs are also very busy and do not allow technicians to connect to their machines for support or maintenance during working hours. When it's time to connect to end-user machines the users are generally not available to provide their password and technicians are then not able to do their job. Security best practices preach that MSPs should not record end-user passwords however this is often not feasible to get around this challenge. MSPs are then forced to record the end-user passwords in their password manager and then consequently set their end-user passwords to never expire so they do not need to constantly update the password in their password manager.



Hackers calling MSPs and impersonating customers

Finally, hackers have recently started targeting MSPs with social engineering attacks. This is where a hacker will contact an MSP help desk and pretend to be an employee at one of their clients or vice-versa. They may ask if the technician can reset their email or computer password so they can get access to their email or PC to initiate a phishing campaign.

Alternatively, if the hacker is impersonating an MSP technician, they may try to convince an end-user to give them remote control over the PC so they can install a malware payload as a pre-cursor to a ransomware attack. According to Channel Pro UK, *"Security software vendor Barracuda conducted research in June 2019 that shows the channel is increasingly falling victim to brand impersonation attacks. A third (35%) said criminals have impersonated them to target their customers, and almost half of the customers fell for it. Conversely, 57% have had criminals impersonating their customers, although only 9% of those were taken in by the ruse."* Without any tool to easily verify the client calling are who they say they are MSPs and their customers are susceptible of these types of attacks which are a substantial security risk.

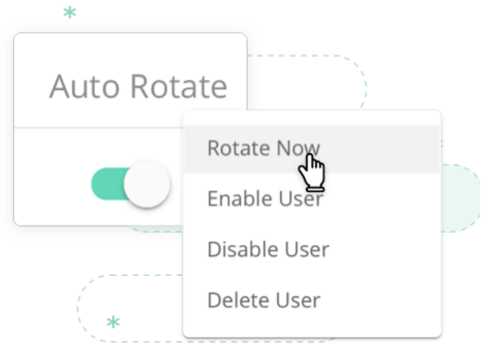
Hackers impersonating MSP technicians try to convice end-users to give them remote access

3

# The Solution You Need

At Quickpass our goal is to provide MSPs with solutions to the above issues that leverage automation and self-serve capabilities that empower end-users to solve the most basic redundant support issues.

## Administrator and Service Accounts



Set rotations to be automatic or rotate instantly.

- Automatically rotate and update your IT Glue password entries for your critical Active Directory and Office 365 administrator passwords on a regular basis

INTERNAL CUSTOMER

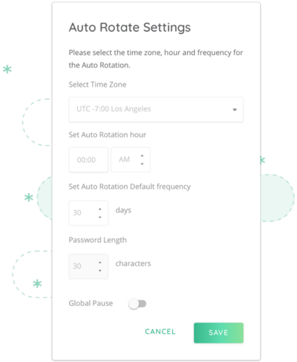
- Use longer random complex passwords or passphrases
- Rotate and update your IT Glue password entries on demand for your critical passwords when a technician quits or is fired

INTERNAL CUSTOMER

## PC Local Administrator Accounts

*Coming Soon*

- Use Quickpass to automatically rotate your local administrator account password on end-user workstations and update your IT Glue password entry on a regular basis.



Auto Rotate Settings

Please select the time zone, hour and frequency for the Auto Rotation.

Select Time Zone: UTC -7:00 Los Angeles

Set Auto Rotation hour: 00:00 AM

Set Auto Rotation Default frequency: 30 days

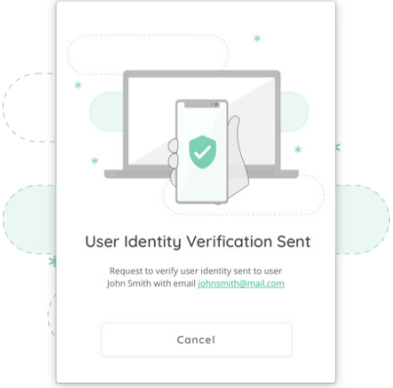
Password Length: 30 characters

Global Pause

Set rotation frequency and password length

## Customer Identity Verification

- Easily verify your customers identities when they call by sending a push notification to the Quickpass mobile app and allowing your customers to click Approve to confirm their identity. This also allows your customers to confirm they are speaking with their IT Service provider by receiving and approving the verification request.



User Identity Verification Sent

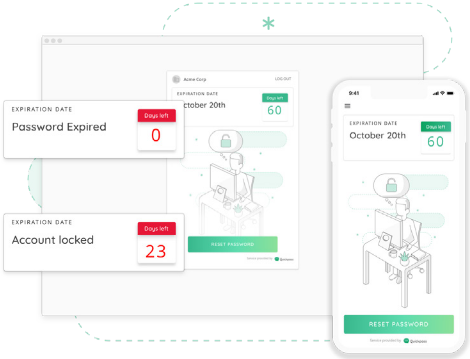
Request to verify user identity sent to user John Smith with email johnsmith@mail.com

Verify your customer’s Identity

## Self-Serve

- Empower end-users to reset their passwords and unlock their own accounts instead of calling the IT help desk.

- Save end-user passwords as embedded passwords in IT Glue contact records and have them update automatically whenever an end-user resets their password. You can now enforce a password policy on your clients, have them reset on their own and get access to their passwords for remote sessions in the evening when the end-user is not available.



Self-serve mobile and web app available for password resets and account unlocking

# References

- FBI recommends passphrases over password complexity: https://www.zdnet.com/article/fbi-recommends-passphrases-over-password-complexity/

- Top 25 Active Directory Security Best Practices: https://activedirectorypro.com/active-directory-security-best-practices/

- Microsoft Password policy recommendations: https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

- Adversary Exposed: How One Criminal Attempted to Sell an MSP on the Dark Web (Disgruntled ex-employee of the MSP): https://blog.huntresslabs.com/adversary-exposed-how-one-criminal-attempted-to-sell-an-msp-on-the-dark-web-d707a5464669

- Does Social Engineering Threaten MSPs?: https://www.channelfutures.com/from-the-industry/does-social-engineering-threaten-msps

- MSPs in cybercriminals' crosshairs: https://www.channelpro.co.uk/advice/11483/msps-in-cybercriminals-crosshairs

- Managing Local Admin passwords with Kaseya: https://virtualadministrator.com/managing-local-admin-passwords-with-kaseya/

- 12 Ways to Hack Multi-Factor Authentication: https://www.secureworldexpo.com/industry-news/12-ways-how-to-hack-multi-factor-authentication-mfa

- This trojan malware is being used to steal passwords and spread ransomware: https://www.zdnet.com/article/this-trojan-malware-is-being-used-to-steal-passwords-and-spread-ransomware/

Learn how Quickpass
helps protect your MSP at
getquickpass.com
or call us at
+1 (888) 384-0566