Multi-Factor Authentication

What Is Multi-Factor Authentication (MFA)?

Use of 2 or more authentication factors, from:

- Something you know (password, PIN)
- Something you have (token, mobile phone)
- Something you are (fingerprint, face)

AuthPoint factors:

1. Your password
2. Approval on your mobile authenticator
3. Correct mobile phone DNA
4. A fingerprint to access (with certain phone model)

itro's Multi-Factor Authentication

How confident are you with passwords?
What about passwords shared across your team? Would they stop hackers?

Passwords are annoying, so most of us pick something easy to remember.
Which is why freelance cyber security journalist Kate O'Flaherty, writing about the worst passwords of 2018 for Forbes, discovered:

'...23.2 million [hacks] worldwide [exploited] the password '123456'.' (NB It was also the most hacked password in 2017!)

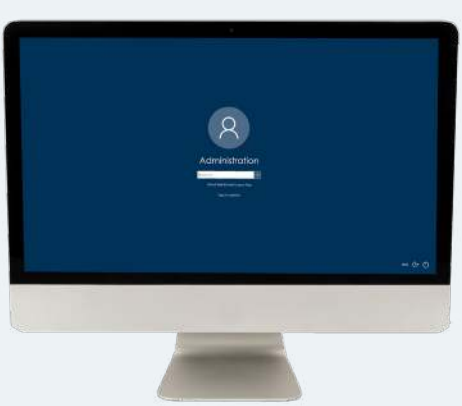
BUT.. this is a problem easily solved!
Instead of worrying, get your individual and team passwords automated and managed from the Cloud using itro's Multi-Factor Authentication ('MFA').

Our unique multi-factor authentication (MFA) solution not only reduces network disruptions and data breaches arising from weak or stolen credentials, but we deliver this important capability entirely from the Cloud for easy set-up and management.

Ultimately, itro's AuthPoint is the right solution at the right time to make MFA a reality for businesses who desperately need it to block attacks.

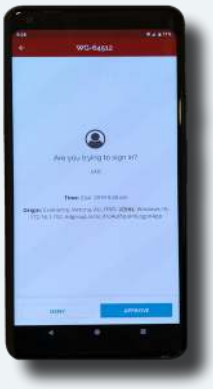
Using MFA Is Easy!

Follow these 4 simple steps to use MFA



Step 1:
Log into your computer and enter your password

Step 2:
Your phone recieves a notification to approve the login



Step 3:
Await approval in the back end

Step 4:
You are automatically sent to the home page on your phone and are successfully logged in on your computer