TELTONIKA Accelerated Password Management with RMS User Guide

TELTONIKA

Networks

USE CASE // ENTERPRISE
ACCELERATED PASSWORD
MANAGEMENT WITH RMS

Contents

1 HIGHLIGHTS
2 THE CHALLENGE – CYBERATTACKS ARE NO JOKE
3 TOPOLOGY
4 THE SOLUTION – AUTOMATING FOR A TRIPLE-WIN
5 Documents / Resources
6 Related Posts

HIGHLIGHTS

✓ Manual password-changing in networks consisting of thousands of connectivity devices is costly, inefficient, and prone to human error. Luckily, there is a simple way to expedite this process.

✓ Using the streamlined password management function of our Remote Management System (RMS) allows changing the password of thousands of devices to be accomplished in a matter of seconds.

✓ Additional features like device monitoring, performance analysis, and full control over updates and configurations further help RMS reduce human error potential and save time and money.

THE CHALLENGE – CYBERATTACKS ARE NO JOKE

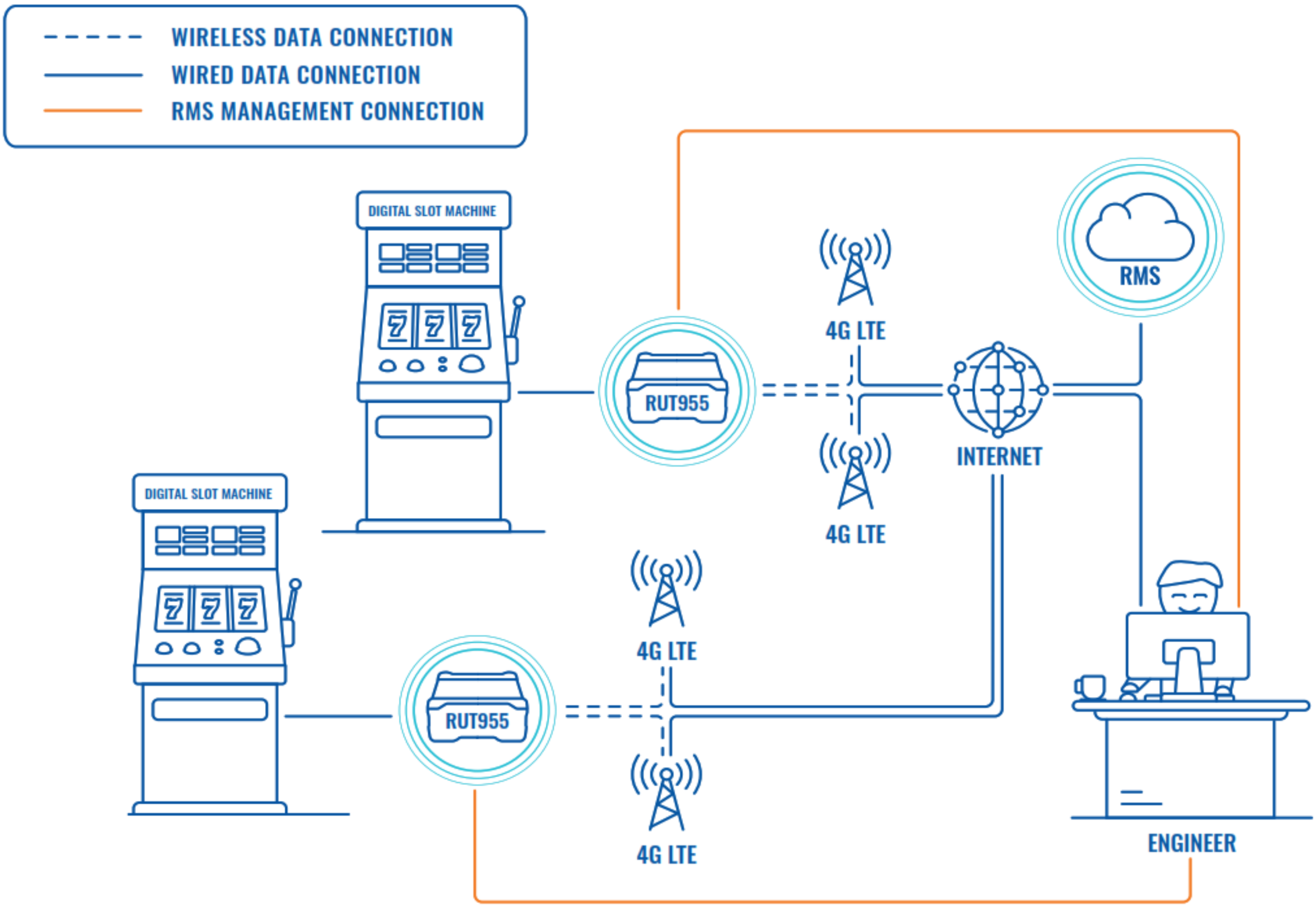
Nowadays, precautions against cyberattacks are a must, and you would think that would reduce the number of possible threats – but the opposite is true. Hackers are always getting sneakier, and their attempts to hijack your precious data are becoming more insidious. The wiser thing to do is to take extra security steps rather than being sorry when your personal information gets leaked or stolen. But it looks like there are still people who want to live on the edge.

There are numerous cybersecurity steps you can take, yet the one we believe matters most starts at the early point of network connectivity provision: networking devices. Any connected solution of a given company must be secure and protected from cyberattacks, especially when hijacking even one device could take a heavy monetary and reputational toll. The best way to ensure device security is periodically changing the system passwords of all devices in the solution. That’s not so easy when the fleet consists of thousands of devices that demand the same task, which cannot be completed over non-encrypted Internet connectivity tunnels.

Sigh

Changing passwords manually usually requires SMS services and a highly-skilled engineer. This can quickly ramp up the expenses and still leave the potential for human error. So, what would be a quicker and more resource-efficient way to achieve this?

TOPOLOGY



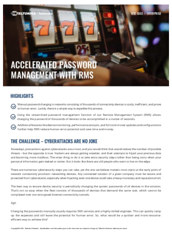
THE SOLUTION – AUTOMATING FOR A TRIPLE-WIN

The best way to avoid cyberattacks without spending a lot of money or time is to automate it with our RMS. Using RMS, you can easily manage your entire fleet's system passwords and automatically assign a unique, random password to each device – turning an otherwise tedious process into an incredibly quick and simple one without making any security compromises!
Sigh (this time of relief) Turning lengthy tasks into brief ones is only one of the ways RMS saves your time and money, but it packs quite a few more! RMS opens a whole new world of control and management of networking devices. You can monitor thousands of devices at once, analyze their performance, update their firmware, and reconfigure them. Our RMS accelerates the password-changing process of your fleet and immensely reduces the costs and human errors associated with it. RMS makes this not just a win-win but a triple-win solution.

https://teltonika-networks.com/product/rms/

Specifications and information given in this document are subject to change by Teltonika Networks without prior notice.

Documents / Resources



TELTONIKA | Networks

USE CASE // ENTERPRISE

ACCELERATED PASSWORD MANAGEMENT WITH RMS

HIGHLIGHTS

- Manual password-changing in networks consisting of thousands of connectivity devices is costly, inefficient, and prone to human error. Luckily, there is a simple way to expedite this process.
- Using the streamlined password management function of our Remote Management System (RMS) allows changing the password of thousands of devices to be accomplished in a matter of seconds.
- Additional features like device monitoring, performance analysis, and full control over updates and configurations further help RMS reduce human error potential and save time and money.

THE CHALLENGE – CYBERATTACKS ARE NO JOKE

Nowadays, precautions against cyberattacks are a must, and you would think that would reduce the number of possible threats – but the opposite is true. Hackers are always getting sneakier, and their attempts to hijack your precious data are becoming more insidious. The wiser thing to do is to take extra security steps rather than being sorry when your personal information gets leaked or stolen. But it looks like there are still people who want to live on the edge.

There are numerous cybersecurity steps you can take, yet the one we believe matters most starts at the early point of network connectivity provision: networking devices. Any connected solution of a given company must be secure and protected from cyberattacks, especially when hijacking even one device could take a heavy monetary and reputational toll.

The best way to ensure device security is periodically changing the system passwords of all devices in the solution. That's not so easy when the fleet consists of thousands of devices that demand the same task, which cannot be completed over non-encrypted Internet connectivity tunnels.

Sigh

Changing the passwords manually usually requires SMS services and a highly-skilled engineer. This can quickly ramp up the expenses and still leave the potential for human error. So, what would be a quicker and more resource-efficient way to achieve this?

TELTONIKA Accelerated Password Management with RMS [pdf] User Guide
Accelerated Password Management with RMS, Accelerated Password Management, APM with RMS

Manuals+,