

Ako (ne)ohroziť firemnú bezpečnosť pomocou tlačiarňí

Michael Grafnetter



X @MGrafnetter  www.dsinternals.com

Print Infrastructure Security Often Neglected

This site is asking you to sign in.

Username

Password

TOP Print Infrastructure Security Concerns

- Confidential documents being printed / stolen
- Employee-owned printers
 - Post-COVID remote work
- Maintaining HW/SW security of MFPs
 - Majority of orgs have multi-vendor print fleets
 - Shadow purchasing widens security gaps
 - Lack of automated patch management
 - Zero trust approach and micro-segmentation rarely used
- Ensuring security of print management SW
 - Some orgs move print management to the cloud
- Zero-day attacks using the print infrastructure
- Monitoring print activity

Identity & Pull Printing



Demo: Card ID Cloning

The screenshot shows the Director V4.50.1 software interface. At the top, it displays 'Port: USB', 'Baud Rate: 9600', and 'Status: Connected to USB (COM3)'. Below this are tabs for 'Simple Test', 'Function Test', and 'Settings'. The 'Result' section contains a large green box with the text 'ID: 785707877' and 'Tag Type: ISO14443A/MIFARE (32 Bit)'. Below the result box are controls for 'Select Tag Types', 'ID Format' (set to 'decimal'), 'Cycle (16)', 'Search Tag', 'Sound Beep With PC', and 'Sound Beep With TWN4'. At the bottom, a log window shows a list of search results for 'SearchTag (32)', with the target ID '785707877' highlighted in green.

Director V4.50.1

Port: USB Baud Rate: 9600 Disconnect Status: Connected to USB (COM3)

Simple Test Function Test Settings

Result

ID: 785707877
Tag Type: ISO14443A/MIFARE (32 Bit)

Select Tag Types ID Format Cycle (16) Sound Beep With PC
 decimal Display New ID only Search Tag Sound Beep With TWN4

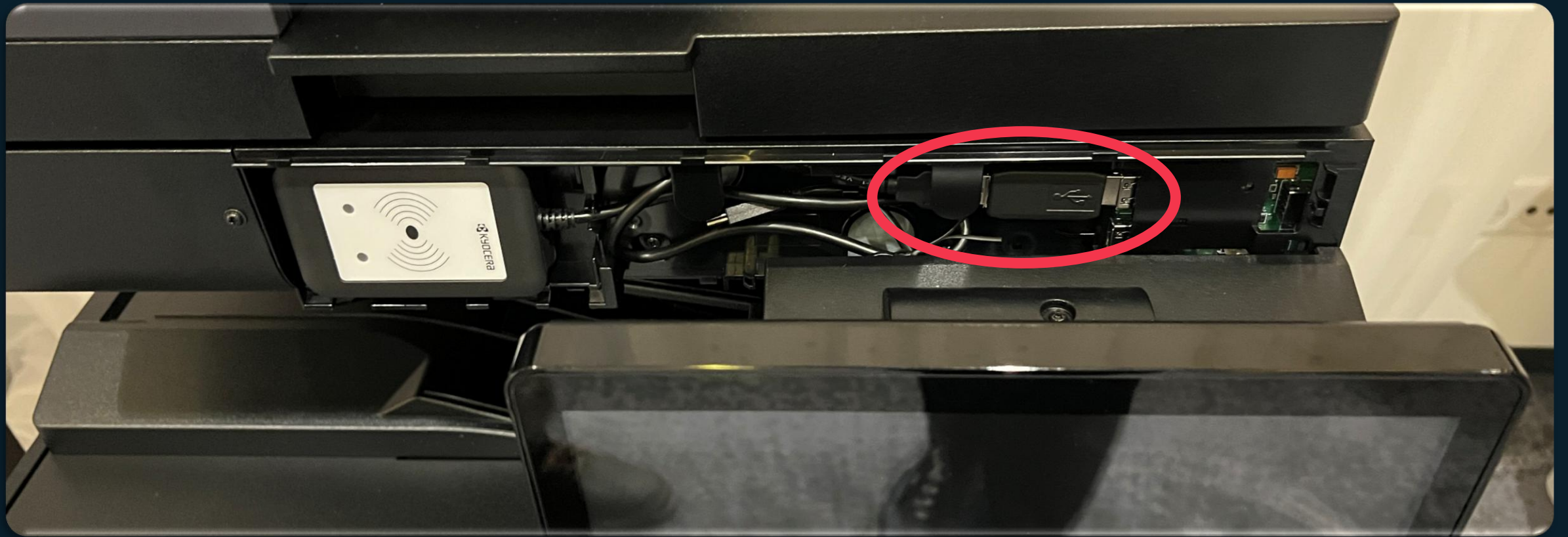
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 2ED4F365
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 2ED4F365
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 2ED4F365
SearchTag (32)	Result: No Tag
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 2ED4F365
SearchTag (32)	Result: No Tag
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 2ED4F365
SearchTag (32)	Result: No Tag
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 2ED4F365
SearchTag (32)	Result: No Tag
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 785707877
SearchTag (32)	Result: No Tag
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 785707877
SearchTag (32)	Result: No Tag
SearchTag (32)	Result: true TagType: ISO14443A/MIFARE IDBitCount: 32 ID: 785707877

Show Raw Data

Card ID Sniffing



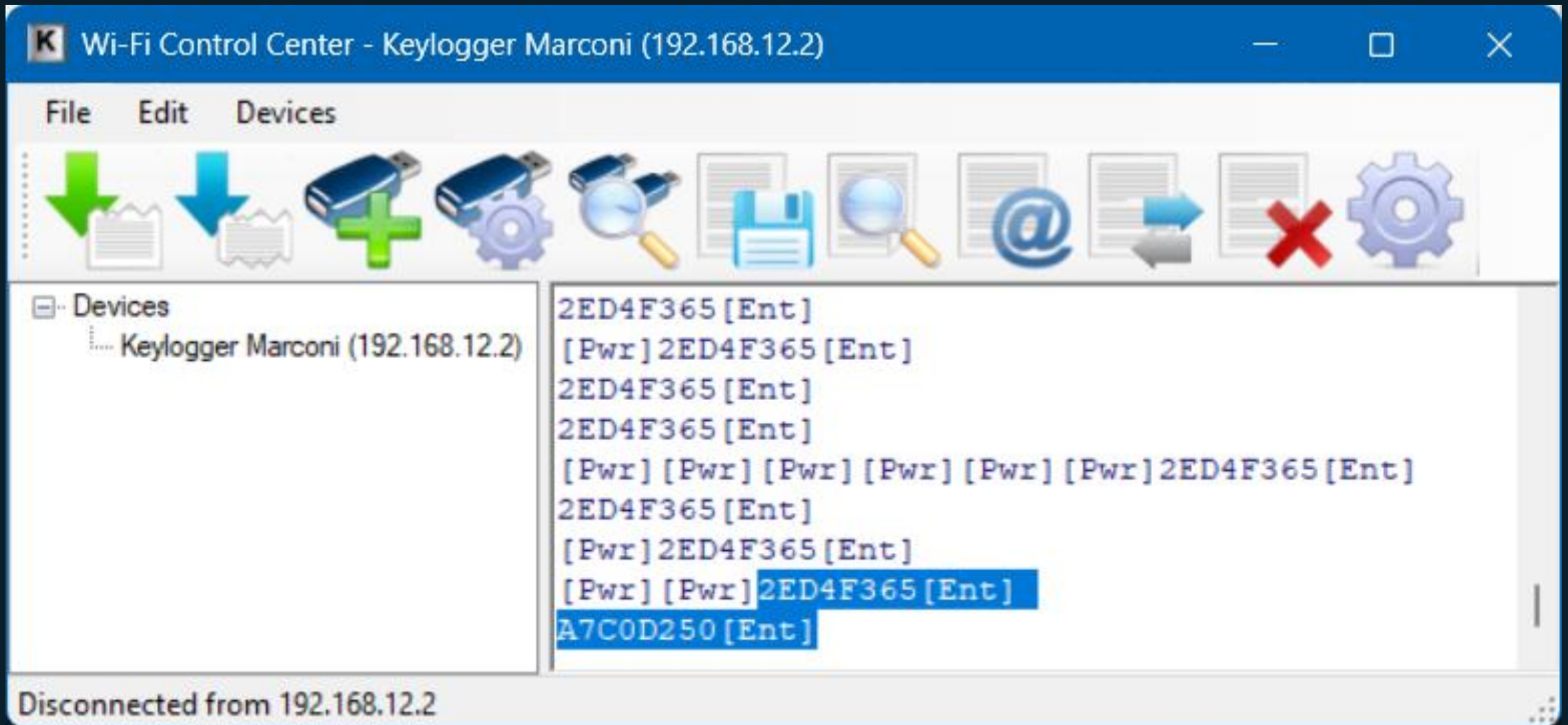
Card ID Sniffing



Demo: Card ID Sniffing



Demo: Card ID Sniffing



Possible Solutions

Configuration Profile: Default

General Terminal Printers

Terminal type: Embedded

Install terminal package

Login methods:

- Simple
 - PIN
 - ID Card
 - User name and password/PIN
 - ID Card and PIN
 - ID Card and password/PIN

Copier operation panel idle time: 90 seconds

Automatic configuration: Automatically configure the device and install the terminal during printer activation. If unchecked, you must do the steps manually.


Set MyQ as device SMTP server: When enabled, email communication from the device is routed via the MyQ server. This might be required for some functionality such as Scan to Me from the native device panel.

> Guest Account

Save Cancel



User Synchronization From Active Directory / Entra ID

 **User Synchronization: Microsoft Entra ID** ✕

General **Users** Groups

Users to import: All users
 Users from selected groups

▼ Properties

Full name: * ▼

Personal number: ▼

Email: ▼

Notes: ▼

Language: ▼

Department: ▼

Alias: ▼

Card: ▼

PIN: ▼

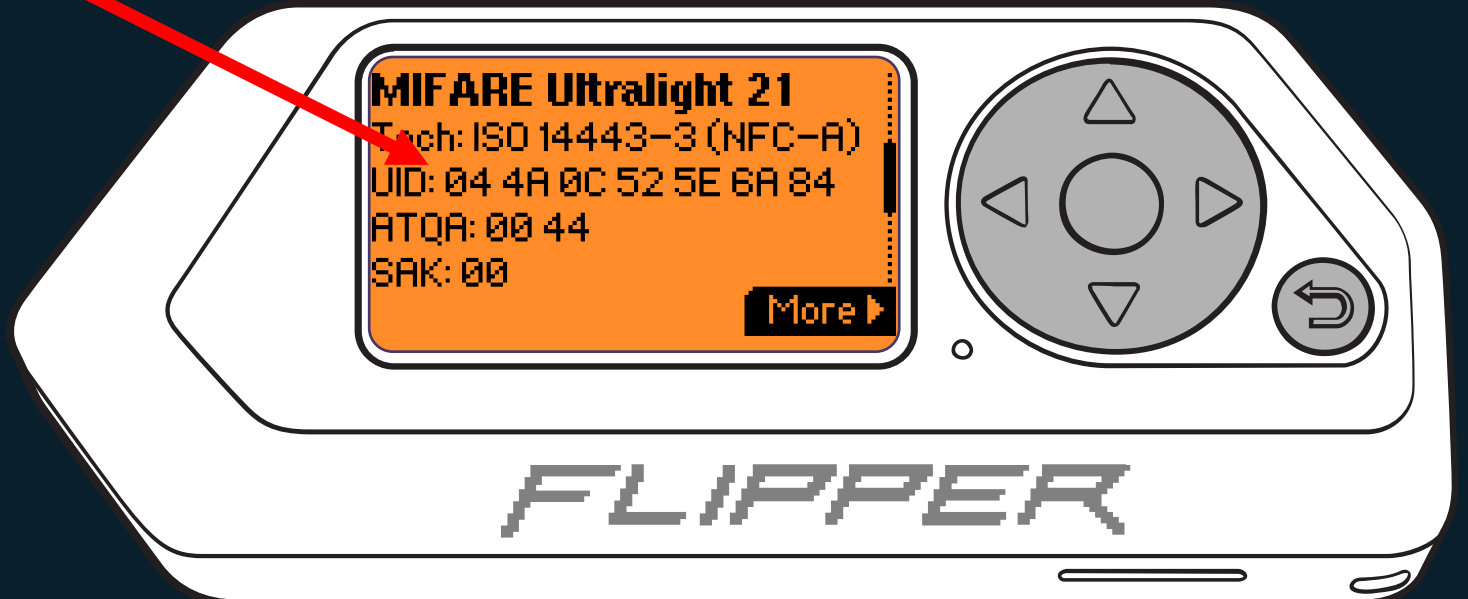
Custom (1): ▼

Activate Windows
Go to Settings to activate Windows.

Misusing Read-Only Address Book Access

```
powershell in C:\  
C:\> Get-Recipient | Format-Table -Property Name,CustomAttribute1,CustomAttribute2
```

Name	CustomAttribute1	CustomAttribute2
AdeleV	044A0C525E6A84	1234
AlexW	04ED6ECAF76A80	4321
DiegoS	049D26DADC5E27	1111



Building Access Control Systems



Possible Solution

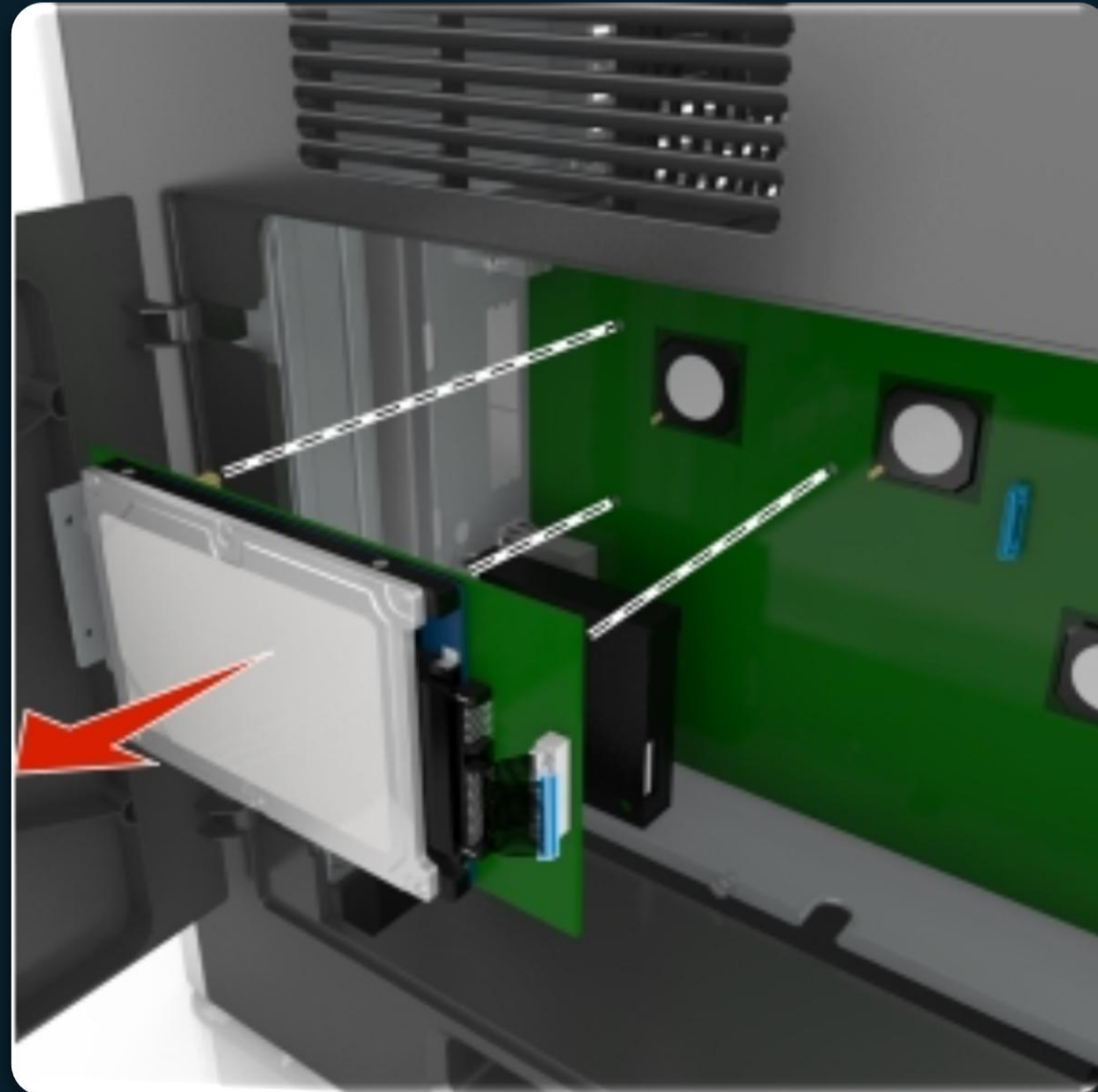


Print Job and Log Storage

The screenshot shows a software interface with a blue header bar labeled 'Status'. Below the header, there are two tabs: 'Status' and 'Log'. The 'Log' tab is selected and highlighted with a red box. Under the 'Log' tab, there is a 'Job Type' dropdown menu set to 'All'. Below the dropdown is a table with the following columns: Job No., End Date, Type, Job Name, User Name, and Result. The table contains five rows of data, all with a 'Completed' status. To the right of the table is a vertical scrollbar with a '1/20' indicator. Below the table is a 'Detail' button. At the bottom of the interface, there is a navigation bar with five buttons: 'Printing Jobs', 'Sending Jobs', 'Storing Jobs', 'Device/Communicate', and 'Paper/Supplies'. The 'Printing Jobs' button is highlighted with a red box. To the right of these buttons is a 'Close' button with a back arrow icon.

Job No.	End Date	Type	Job Name	User Name	Result
003606	07/29 11:22		Sample3.docx 130729 112059	Yoshida, Toshin...	Completed <input type="button" value="OK"/>
003605	07/29 11:22		Sample2.docx 130729 112051	Yoshida, Toshin...	Completed <input type="button" value="OK"/>
003604	07/29 11:22		Sample1.docx 130729 112044	Yoshida, Toshin...	Completed <input type="button" value="OK"/>
003603	07/29 11:21		outbind://8-000 130729 111...	Kuramae, Yosh...	Completed <input type="button" value="OK"/>
003602	07/29 11:02		MarketingWP_Dra 130726 20...	Kuramae, Yosh...	Completed <input type="button" value="OK"/>

Print Job and Log Storage



Optional Security Settings

User: Application Administrator , MyQ Terminal.admin 13:56

Copy Send | Status/Job Cancel Device Information System Menu Numeric Keypad Application Ad... Logout

Identification/Wired Network
Supplies/Paper
USB/NFC/Bluetooth
Option/Application
Capability/Version
Security
Report
Remote Ope. Status

Security

DataEncrypt./Overwrite	Disabled
Trusted Platform Module Specification Version	2.0
Manufacturer Name	IFX
Manufacturer Version	1.16
Secure Boot	Enabled
Runtime Integrity Check	Enabled
Allowlisting	Disabled

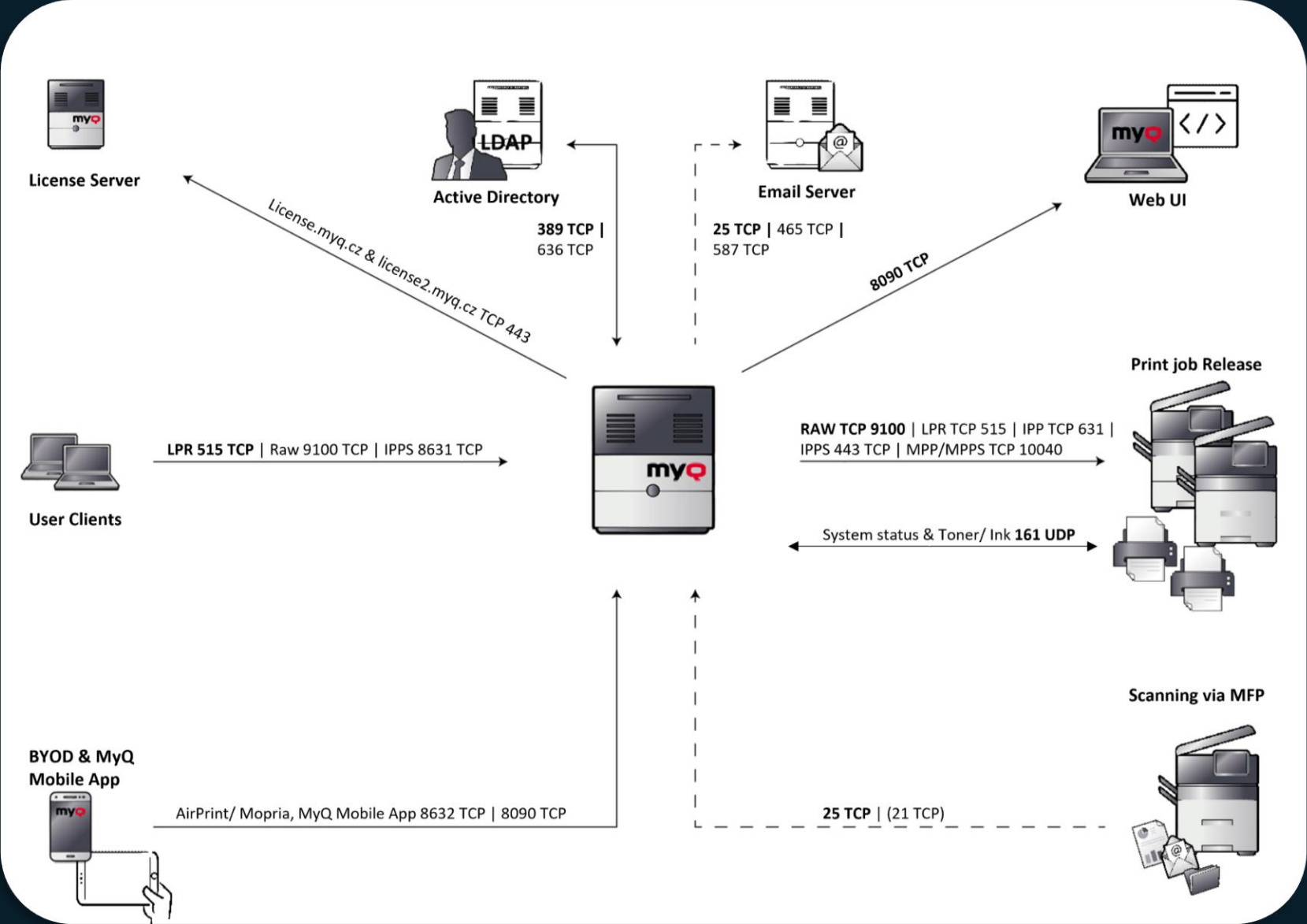
Energy Saver
Reset

Close

Network Security



Communication Diagram



Wiretapping



Printing Protocols

*LPD :	<input checked="" type="checkbox"/>	On
*FTP Server (Reception) :	<input checked="" type="checkbox"/>	On
*IPP :	<input checked="" type="checkbox"/>	On
*Port Number :	<input type="text" value="631"/>	(1 - 32767)
*IPP over SSL :	<input checked="" type="checkbox"/>	On
	Note : To use these settings, enable SSL. Network Security	
*Port Number :	<input type="text" value="443"/>	(1 - 32767)
*IPP over SSL Certificate :	Device Certificate 1	
	<input type="button" value="Settings"/>	
IPP Authentication :	<input type="checkbox"/>	Off
*Raw :	<input checked="" type="checkbox"/>	On
*WSD Print :	<input type="checkbox"/>	Off

Scanning Protocols

SMTP (E-mail TX) : On

Note :
For more settings, click here. [E-mail Settings](#)

SMTP Security :

Note :
To use these settings, enable SSL. [Network Security](#)

Certificate Auto Verification :
 Validity Period Server Identity
 Chain Revocation

Revocation Check Type :

Hash :
 SHA1 SHA2(256/384)

S/MIME :

FTP Client (Transmission) : On

Port Number : (1 - 65535)

FTP Encryption TX : On

Note :
To use these settings, enable SSL. [Network Security](#)

Certificate Auto Verification :
 Validity Period Server Identity
 Chain Revocation

Folder ✕

Folder :


Protocol : SMB FTP

Host Name :

Port Number : (1 - 65535)

Path :

Login User Name :

Login Password : 

Connection Test :

Connection Test (Encrypted TX) :

Address Book Access

↑ External Address Book 1 Settings

External Address Book Name :


LDAP Server

LDAP Server Name :

LDAP Port Number : (1 - 65535)

Search Timeout : seconds

Login User Name :

Login Password : 

Max Search Results :

Search Base :

LDAP Security : Off

Note :
Make settings here. [Protocol](#)

Authentication Type : ▼

Connection Test :

Active Directory Authentication (LDAP)

The image shows a Wireshark network traffic capture of an LDAP authentication session. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. The main display area is divided into three sections: a packet list, a packet details pane, and a packet bytes pane.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
102	19:54:19.557075	10.220.0.4	10.220.0.3	LDAP	68	bindRequest(1) "<ROOT>" simple
103	19:54:19.557437	10.220.0.3	10.220.0.4	LDAP	76	bindResponse(1) success
104	19:54:19.564350	10.220.0.4	10.220.0.3	LDAP	61	unbindRequest(2)
168	19:56:50.819182	10.220.0.4	10.220.0.3	LDAP	102	bindRequest(1) "svc_myq_print2@contoso.com" simple
169	19:56:50.820993	10.220.0.3	10.220.0.4	LDAP	76	bindResponse(1) success
171	19:56:53.434836	10.220.0.4	10.220.0.3	LDAP	61	unbindRequest(2)

Packet Details (Frame 168):

- Frame 168: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{05D9E828-50E1-415E-9...}
- Ethernet II, Src: Fa_00:00:04 (00:17:fb:00:00:04), Dst: Fa_00:00:03 (00:17:fb:00:00:03)
- Internet Protocol Version 4, Src: 10.220.0.4, Dst: 10.220.0.3
- Transmission Control Protocol, Src Port: 53733, Dst Port: 389, Seq: 1, Ack: 1, Len: 48
- Lightweight Directory Access Protocol
 - LDAPMessage bindRequest(1) "svc_myq_print2@contoso.com" simple
 - messageID: 1
 - protocolOp: bindRequest (0)
 - bindRequest
 - version: 3
 - name: svc_myq_print2@contoso.com
 - authentication: simple (0)
 - simple: Pa\$\$w0rd

Packet Bytes:

0000	00	17
0010	00	58
0020	00	03
0030	04	02
0040	04	1a
0050	40	63
0060	24	24

Management Protocols

Other Protocols

*SNMPv1/v2c : On

Note :
For more settings, click here. [SNMP Settings](#)

*SNMPv3 : Off

Note :
For more settings, click here. [SNMP Settings](#)

*HTTP : On

*HTTPS : On

Note :
To use these settings, enable SSL. [Network Security](#)

*HTTPS Certificate : Device Certificate 1

HTTP (Clientside) :

Certificate Auto Verification : Validity Period Server Identity
 Chain Revocation

Revocation Check Type : OCSPP

Hash : SHA1 SHA2(256/384)

↑ **Management Settings : SNMP**

SNMPv1/v2c

*SNMPv1/v2c : On

Note :
Make settings here. [Protocol](#)

*Read Community : public

*Write Community : public

Simple Network Management Protocol (SNMP)

*2 interfaces

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

snmp

No.	Time	Source	Destination	Protocol	community	Info
608	13:21:41.044904	10.14.253.56	10.14.4.11	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
610	13:21:41.046819	10.14.253.56	10.14.4.11	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
692	13:21:44.952879	fe80::9725:45bd:ffa5:c2b3	KM260DD2.local	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
693	13:21:44.953438	KM260DD2.local	fe80::9725:45b...	SNMP	public	get-response 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
803	13:21:51.601775	10.14.253.56	10.14.4.11	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
805	13:21:51.602035	10.14.253.56	10.14.4.11	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
1041	13:22:01.630502	10.14.253.56	10.14.4.11	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
1043	13:22:01.631238	10.14.253.56	10.14.4.11	SNMP	public	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.2.1.5.1
1079	13:22:03.402247	10.15.2.5	KM260DD2.local	SNMP	public	get-request 1.3.6.1.2.1.2.2.1.6.1
1080	13:22:03.410540	KM260DD2.local	10.15.2.5	SNMP	public	get-response 1.3.6.1.2.1.2.2.1.6.1
1081	13:22:03.446657	KM260DD2.local	10.15.2.5	SNMP	public	get-response 1.3.6.1.2.1.2.2.1.6.2
1082	13:22:03.446343	10.15.2.5	KM260DD2.local	SNMP	public	get-request 1.3.6.1.2.1.2.2.1.6.2
1084	13:22:03.482045	KM260DD2.local	10.15.2.5	SNMP	public	get-response 1.3.6.1.2.1.43.18.1.1.2.1.3
1085	13:22:03.481680	10.15.2.5	KM260DD2.local	SNMP	public	get-next-request 1.3.6.1.2.1.43.18.1.1.2
1086	13:22:03.517724	10.15.2.5	KM260DD2.local	SNMP	public	get-next-request 1.3.6.1.2.1.43.18.1.1.2.1.3
1087	13:22:03.518059	KM260DD2.local	10.15.2.5	SNMP	public	get-response 1.3.6.1.2.1.43.18.1.1.2.1.83
1088	13:22:03.553586	10.15.2.5	KM260DD2.local	SNMP	public	get-next-request 1.3.6.1.2.1.43.18.1.1.2.1.83
1089	13:22:03.553979	KM260DD2.local	10.15.2.5	SNMP	public	get-response 1.3.6.1.2.1.43.18.1.1.2.1.92

Simple Network Management Protocol (SNMP)

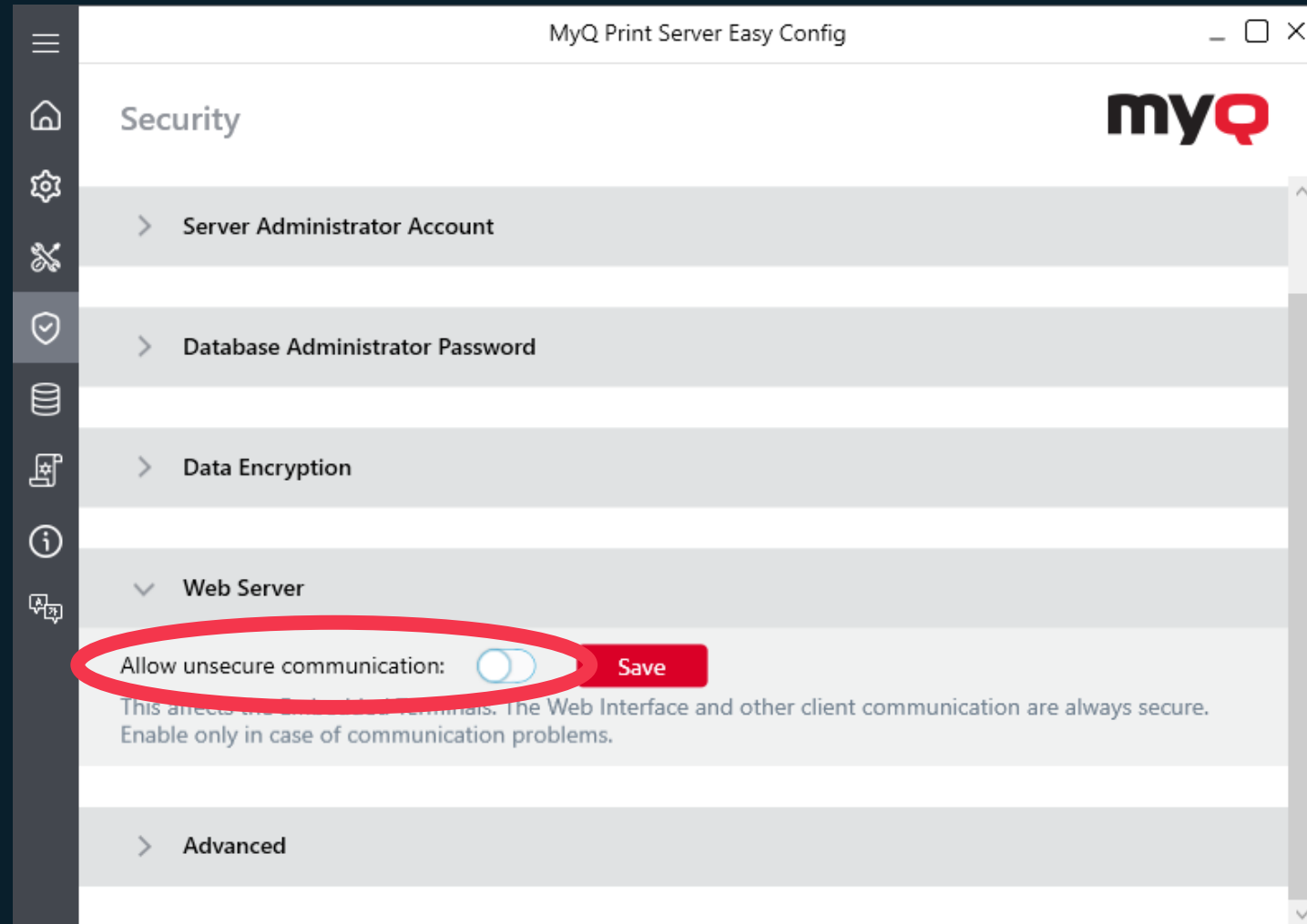
The screenshot shows the MyQ Settings: SNMP interface. The left sidebar contains a navigation menu with the following items: Settings, Server Type, License, General, Personalization, Task Scheduler, Network, Connections, **SNMP**, Authentication Servers, Printers & Terminals, and Configuration Profiles. The main content area is titled 'Network > SNMP' and contains a table with the following data:

Default	Name	SNMP version	Parameters
<input checked="" type="checkbox"/>	SNMP v1	v1	SNMP read community: ***** SNMP write community: ***** SNMP port: 161
<input type="checkbox"/>	SNMP v2c	v2c	SNMP read community: ***** SNMP write community: ***** SNMP port: 161
<input type="checkbox"/>	SNMP v3	v3	Security name: MyQ Authentication protocol: MD5 Authentication password: ***** SNMP port: 161 Privacy protocol: AES128 Privacy password: ***** Context:

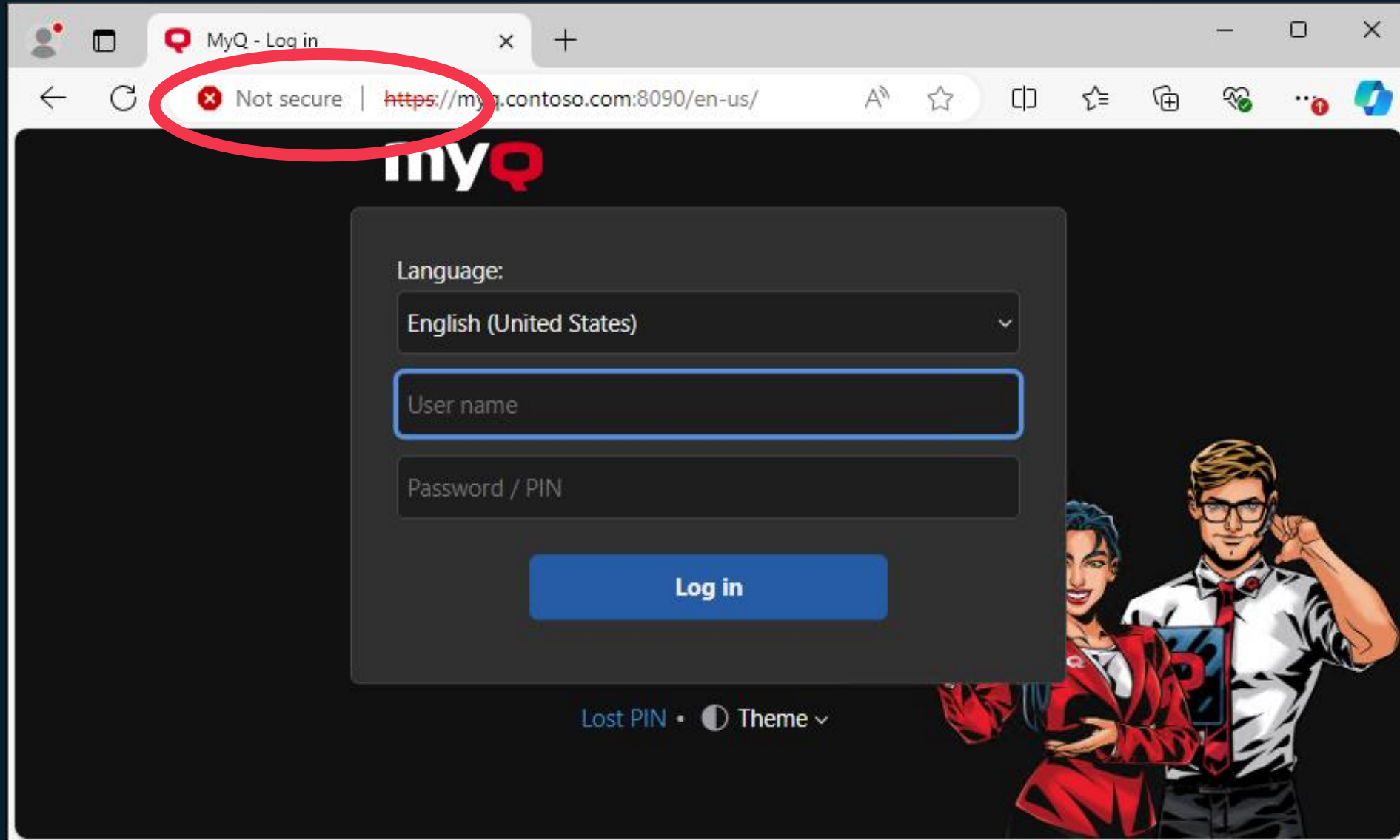
Problem: Legacy Devices



Problem: Legacy Devices



Social Engineering



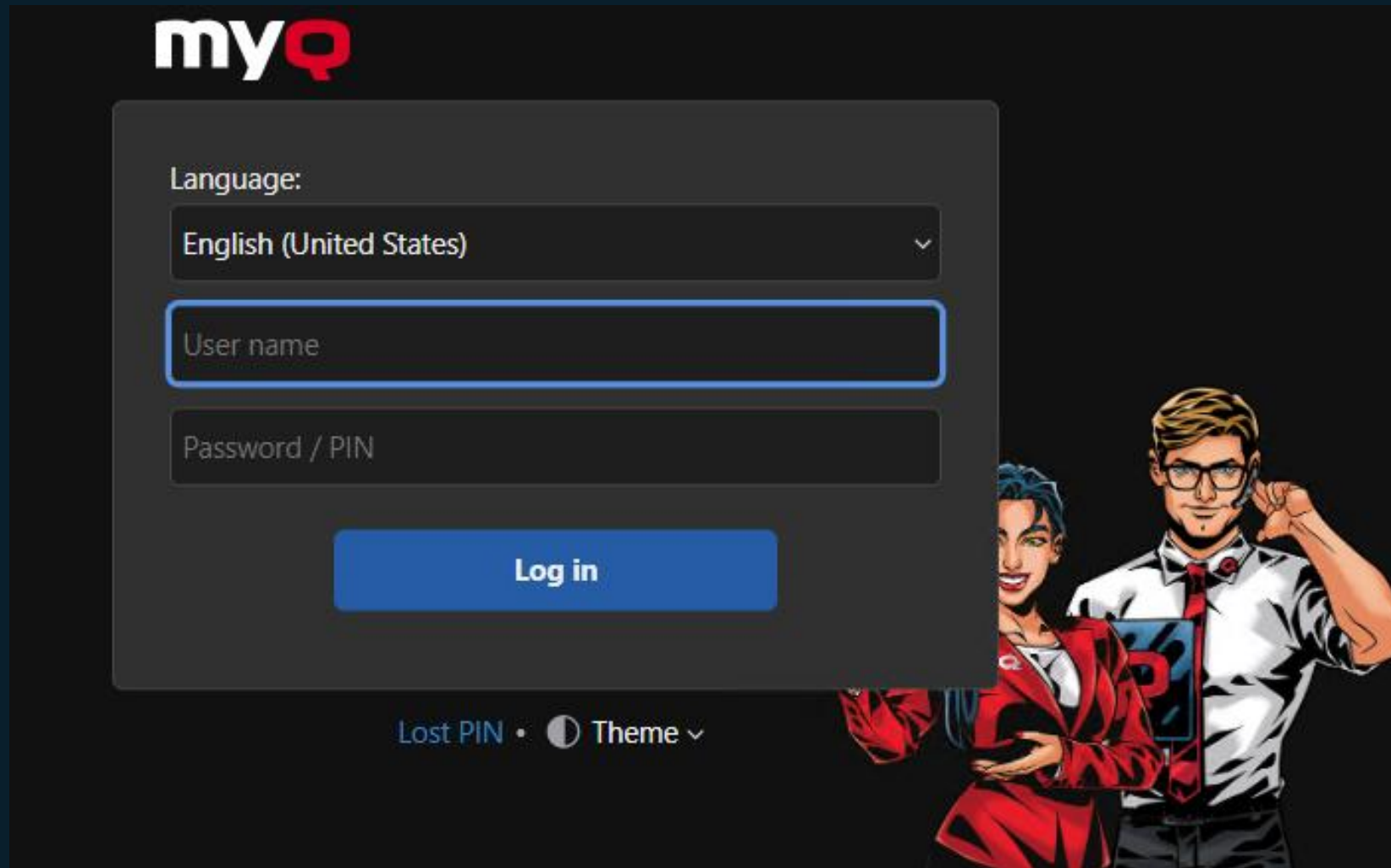
Active Directory Authentication (LDAP)

The screenshot shows the MyQ Settings interface for Authentication Servers. The browser address bar indicates the URL is localhost:8090/en-us/app/#{"r":"authservers"}. The page title is "Settings: Authentication S...". The left sidebar contains various settings categories: Settings, General, Personalization, Task Scheduler, Network, and Printers & Terminals. The main content area is titled "Network > Authentication Servers" and contains a table with the following data:

Type	Domain/Name	Server	Security
Active Directory	contoso.com	Autodiscover	None
Active Directory	adatum.com	Autodiscover	TLS

The "Security" column for the second server (adatum.com) is circled in red. The "Add..." and "Actions" buttons are visible in the top right corner of the table area.

Demo: Server-Side Authentication Traffic Sniffing



The image shows a login interface for 'myQ'. At the top left is the 'myQ' logo. Below it is a language selection dropdown menu currently set to 'English (United States)'. There are two input fields: 'User name' and 'Password / PIN'. A blue 'Log in' button is positioned below the input fields. At the bottom of the form area, there are links for 'Lost PIN' and a 'Theme' selector. The background features a stylized illustration of a man in a white shirt and red tie, and a woman in a red suit.

myQ

Language:
English (United States) ▾

User name

Password / PIN













Log in

Lost PIN • Theme ▾

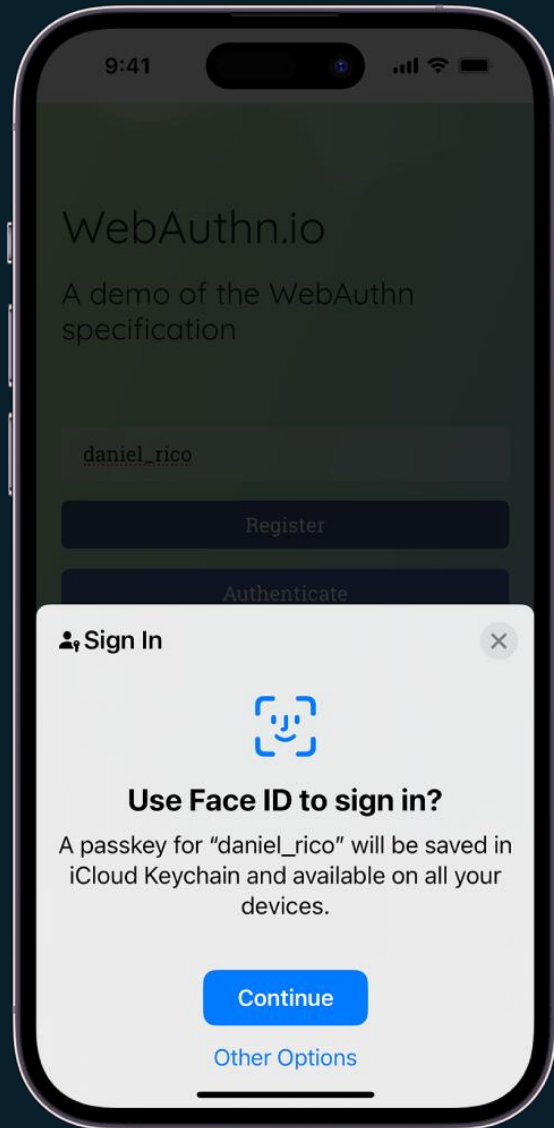
Delegated Authentication and Single Sign-On (SSO)

The image shows a login interface for 'myQ'. At the top left is the 'myQ' logo. Below it is a 'Language:' dropdown menu set to 'English (United States)'. There are input fields for 'User name' and 'Password / PIN', followed by a blue 'Log in' button. Below the 'Log in' button is the text 'OR'. Two buttons are listed: 'Continue with Microsoft' and 'Continue with Windows Authentication'. These two buttons are circled in red. At the bottom left, there are links for 'Lost PIN' and 'Theme'. On the right side of the page, there is a stylized illustration of a woman with blue hair in a red suit and a man with blonde hair and glasses in a white shirt and tie, holding a tablet.

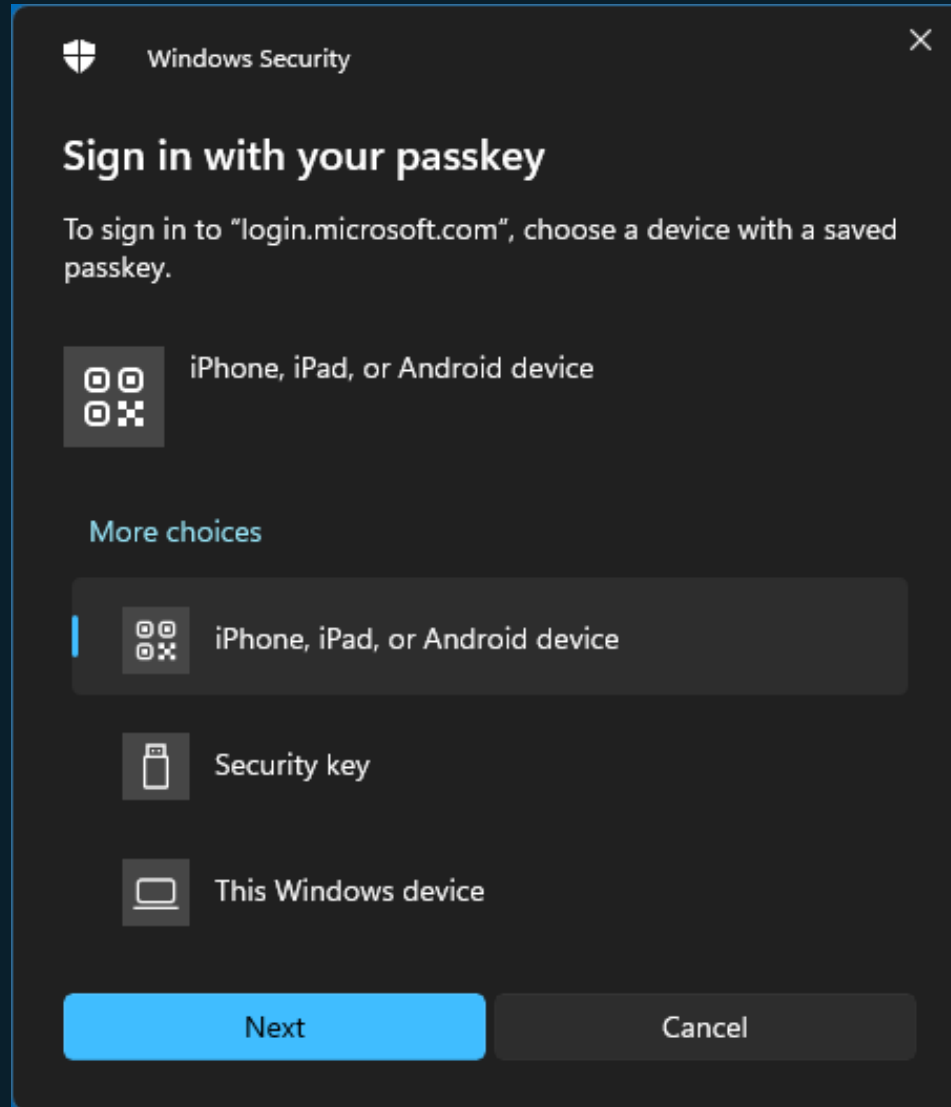
Authentication Method Strength

Bad  Password (Only)	Good  Password +	Better  Password +	Best Passwordless 
123456	 SMS	 Authenticator (Push notifications)	 Windows Hello
qwerty	 Voice	 Software Tokens OTP	 Authenticator (Phone Sign-in)
password		 Hardware Tokens OTP (Preview)	 FIDO2 security key
lloveyou			
Password1			

Passkeys (FIDO2)



Demo: Cross-Device Passkey Authentication



Server-Side Job Archive

▼ Job archiving

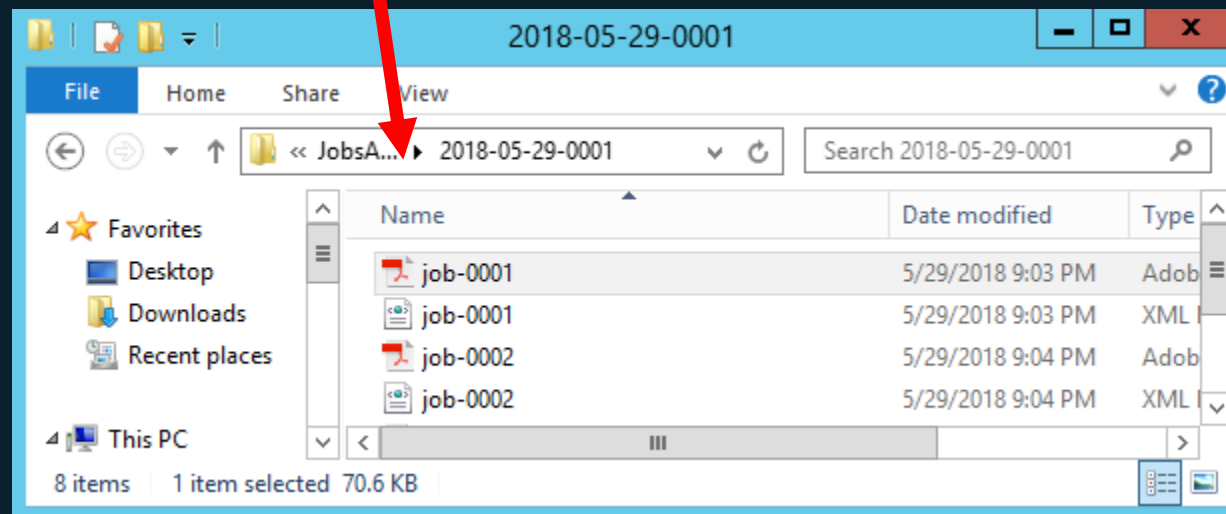
The job archiving feature stores all print/copy/scan/fax jobs and their metadata in the archive folder.

Enabled:

Archive folder:
%app% is the M...Q data folder

Resolution: DPI

Page range:



Critical Security Vulnerabilities

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

WORST FIT EVER —

Nasty bug with very simple exploit hits PHP just in time for the weekend

With PoC code available and active Internet scans, speed is of the essence.

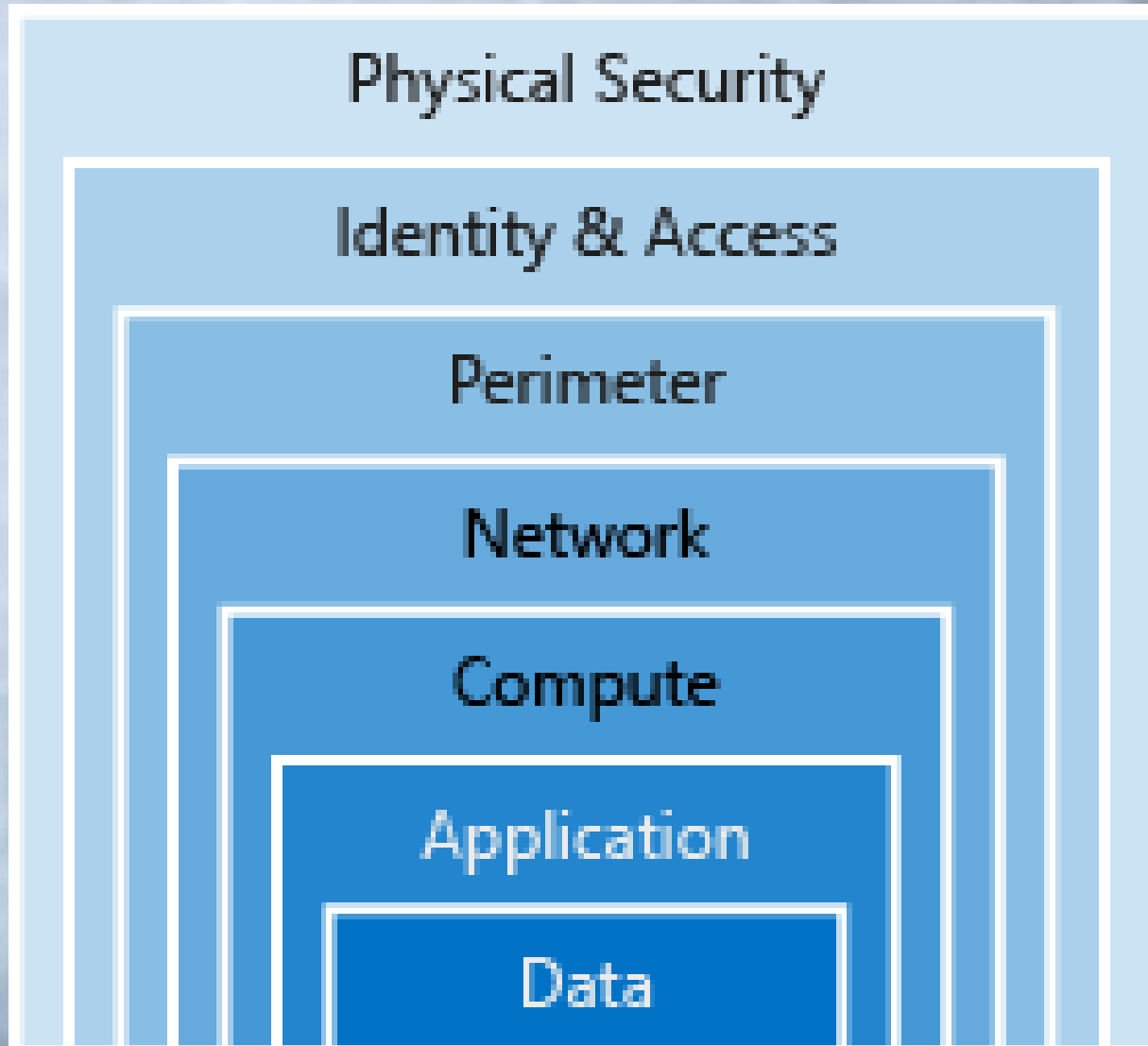
DAN GOODIN - 6/8/2024, 5:57 AM



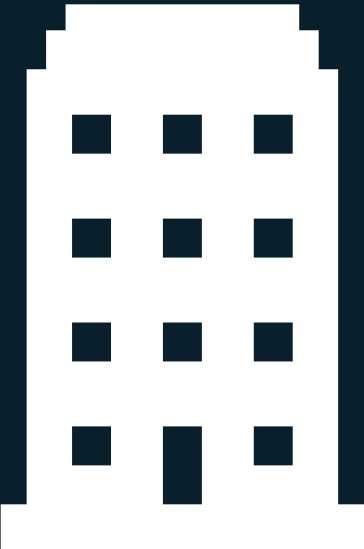
[Enlarge](#)

81 A critical vulnerability in the PHP programming language can be trivially exploited to execute malicious code on Windows devices, security researchers warned as they urged those affected to take action before the weekend starts.

Security = Shared Responsibility



On-Premise vs. Cloud



myQ X



myQ roger