

Cybersecurity for (Nearly) Zero Dollars

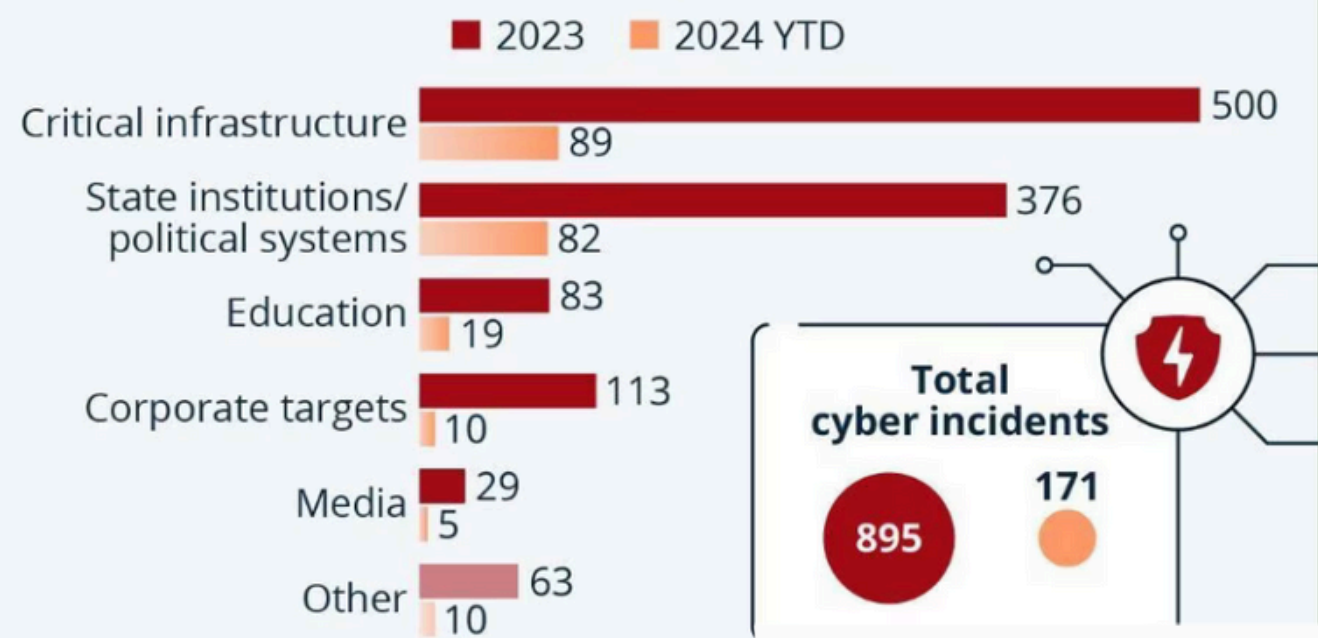
Joshua Martin

“System Administrator” – Philomath School District

HVAC Server

- On Facilities Manager's Desk
- Open Door
- 2010 Hardware
- Windows Server 2008
- No Disk Encryption
- Not Domain Joined
- HVAC\Administrator
- Password: 1234
- No Antivirus/EDR
- Not Domain Joined
- No System Monitor/Alerts
- No backups
- 24/7 3rd-Party Remote Access
- No Network Isolation

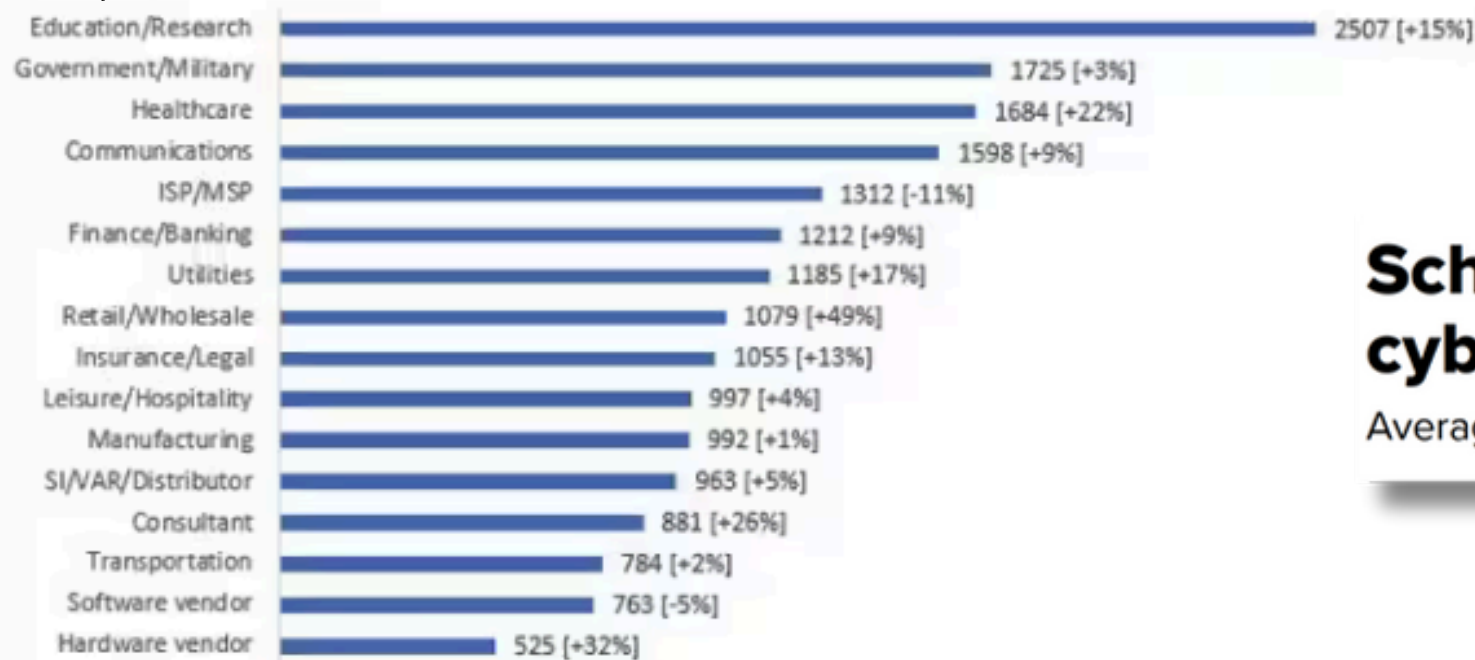




As of Mar. 26, 2024
 * One incident may target more than one sector. Initial malevolent actors may not always coincide with report
 Source: European Repository of Cyber Incidents



Global Avg. Weekly Cyber Attacks Per Industry
 (2022 Q1 Compare to 2023 Q1)



9. Education: Hubs of Knowledge and Innovation

Educational institutions, particularly universities, are increasingly targeted for their intellectual property, personal data, and operational vulnerabilities. Attackers often aim to disrupt operations or monetize stolen data on the **dark web**.

Major Threats:

- **Dark Web Exploitation:** Selling stolen academic research and personal data.
- **DDoS Attacks:** Crippling online learning platforms and administrative systems.

Mitigation Strategies:

Implement robust cybersecurity frameworks, including identity and access management, regular security awareness training. Strong network segmentation and encryption can also help reduce exposure to **cyber threats**.

Schools and colleges are top targets of cybercriminals in 2024

Average weekly attacks on educational institutions are up 37% so far this year.

Three industries stand out as key targets in the first half of 2023: technology, energy and education, according to recent [analysis](#) by Gatewatcher.

Gatewatcher CEO Jacques de la Riviere tells *ITPro* that schools and universities “suffer from a significant and recurring lack of resources, investment, and staff – and they offer criminals a lot of return”.

“There is access to a database of student and teacher accounts, confidential information that could be resold and technological and engineering data at research establishments.”

Education

Why Education Is a Prime Target

Educational institutions, from schools to universities, have become prime targets for cybercriminals due to the vast amount of personal data they store. Students' personal information, academic records, and financial details are valuable to attackers, particularly those seeking to exploit vulnerabilities in legacy systems or unsecured networks.

Higher education institutions are often targeted by Ransomware and phishing attacks, with the disruption of research and academic resources being a significant concern. Moreover, the decentralised nature of many educational systems means that security may be inconsistent across departments.

Impact of Cyberattacks on Education

Internal Vulnerability Scan
For
Philomath School District

November 7th, 2023

Page 35 of 35



Detailed Findings and Recommended Mitigations by Vulnerability

This section presents detailed scan results from the network mapping and vulnerability scans. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

Vulnerability	Severity	CVSS	Recommendation
Microsoft SQL Server Unsupported Version Detection (remote check)	Critical	10	Upgrade to a version of Microsoft SQL Server that is currently supported.
Vulnerability	Severity	CVSS	Recommendation
Mozilla Foundation Unsupported Application Detection	Critical	10	Upgrade to a version that is currently supported.
Vulnerability	Severity	CVSS	Recommendation
Unsupported Web Server Detection	Critical	10	Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.
Vulnerability	Severity	CVSS	Recommendation
Apache Log4j SEoL (<= 1.x)	Critical	10	Upgrade to a version of Apache Log4j that is currently supported.
Vulnerability	Severity	CVSS	Recommendation
Microsoft .NET Core SEoL	Critical	10	Upgrade to a version of Microsoft .NET Core that is currently supported.
Vulnerability	Severity	CVSS	Recommendation
ASP.NET Core SEoL	Critical	10	Upgrade to a version of ASP.NET Core that is currently supported.
Vulnerability	Severity	CVSS	Recommendation
Unsupported Windows OS (remote)	Critical	10	Upgrade to a supported service pack or operating system
Vulnerability	Severity	CVSS	Recommendation
SSL Version 2 and 3 Protocol Detection	Critical	9.8	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.
Vulnerability	Severity	CVSS	Recommendation
Google Chrome < 119.0.6045.105 Multiple Vulnerabilities	Critical	9.8	Upgrade to Google Chrome version 119.0.6045.105 or later.
Vulnerability	Severity	CVSS	Recommendation

Mozilla Firef

Vulnerability
Curl 7.69 < 8
Buffer Overf

Vulnerability
KB5031364:
2022 / Azure
22H2 Securit
(October 202

Vulnerability
Mozilla Firef

Vulnerability
Microsoft Me
Queuing RC
21554, Queu

Vulnerability
Apache Log4
Vulnerabilitie



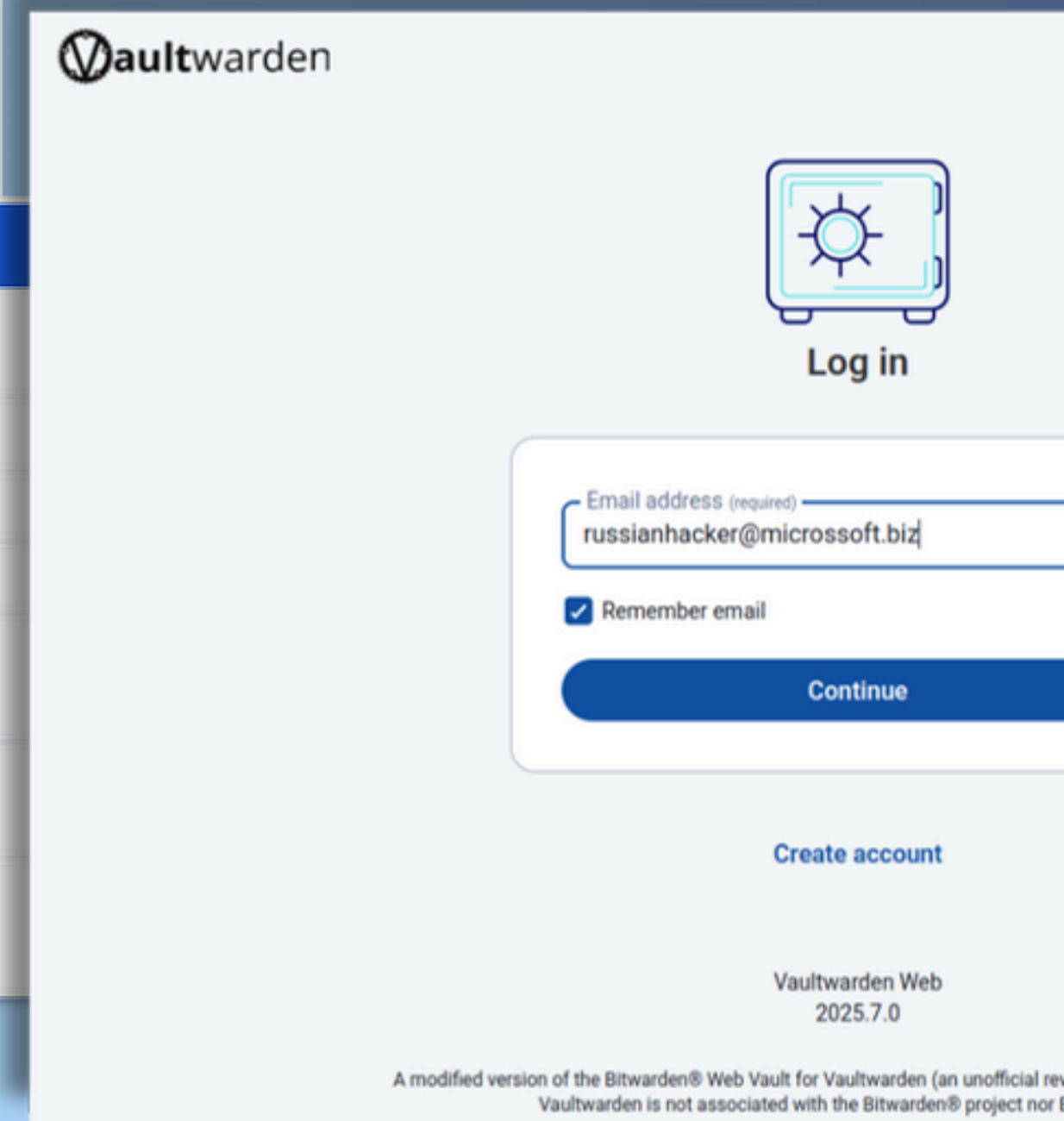
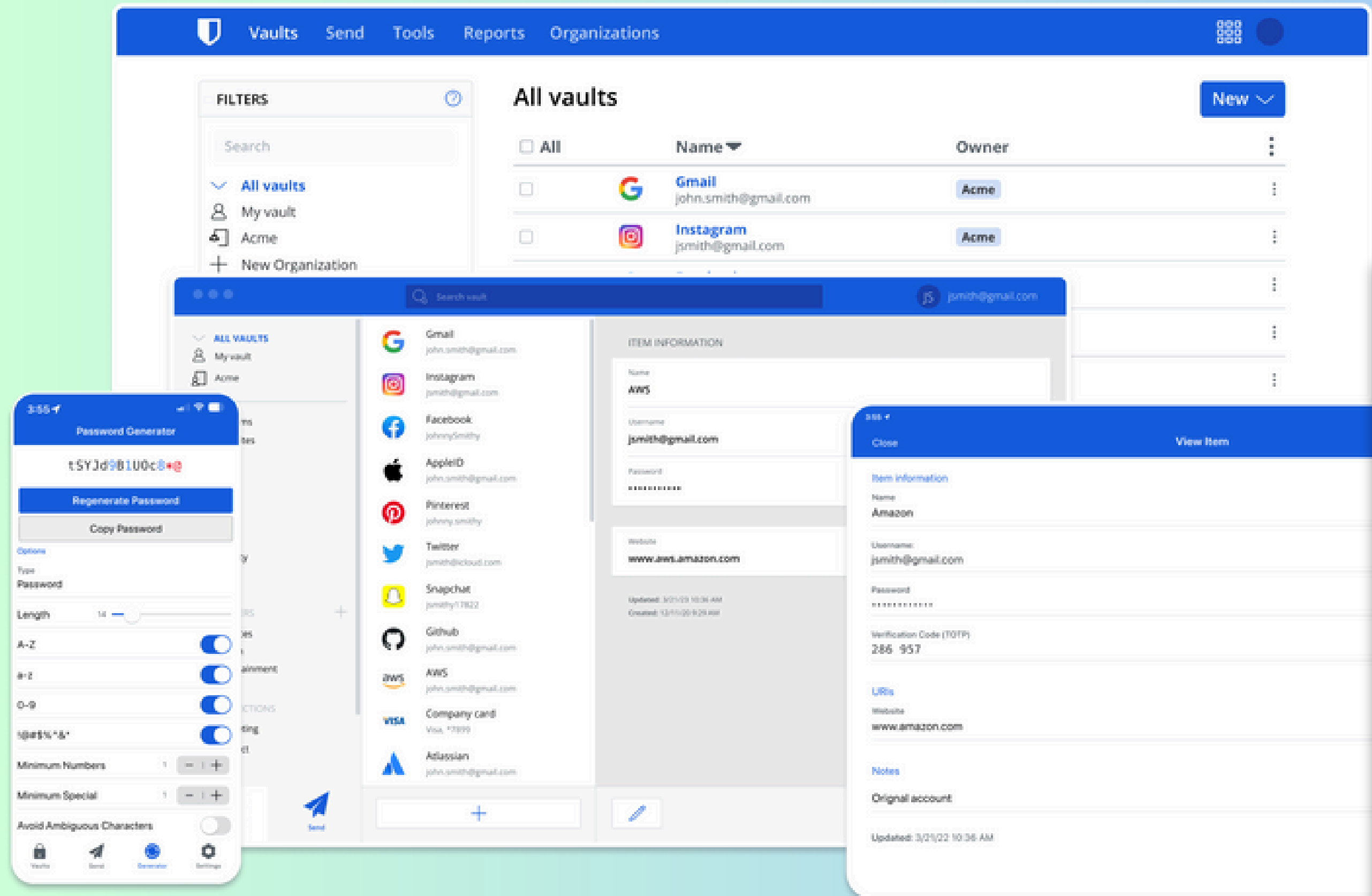
LBL

LINN BENTON LINCOLN
EDUCATION SERVICE DISTRICT

to <https://logging.apache.org/log4j/2.x/security.html> for the latest versions.

Get your st together

- IT Logins/Passwords/Credentials
 - Service Accounts
 - Tech Accounts
 - Generic Superadmin
 - Generic/Shared Accounts
- Apps & Services





Account Goals

1. Generic SuperAdmin for All the things!
2. One account per thing.
3. MFA All the things!
4. Obvious names
5. SSO for everyone else!
6. Strong passphrase/password
7. Least-privilege
8. No shared staff accounts

Account Type	Permissions	Generic?	Provisioned?	SSO?	MFA?
Service	?	Yes	No	No	Yes
SuperAdmin	A	Yes	No	No	Yes
Tech Admin	B	Maybe	Maybe	Maybe	Yes
School Admin	C	No	Yes	Yes	Yes
Specialized Staff	D	No	Yes	Yes	Yes
Staff	E	No	Yes	Yes	Yes
Students	F	No	Yes	Yes	No

SuperAdmin (Web Apps)

- Email: BingBong.Admin@philomath.k12.or.us
- Username: BingBongAdmin
- Password: Mulled-Reptile3-Strobe-Sandblast-Machine



SSO



MFA (TOTP)



Login credentials

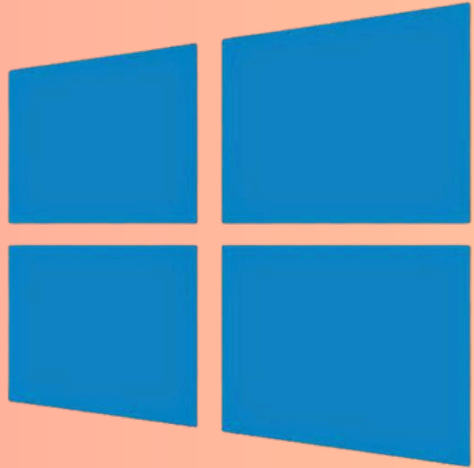
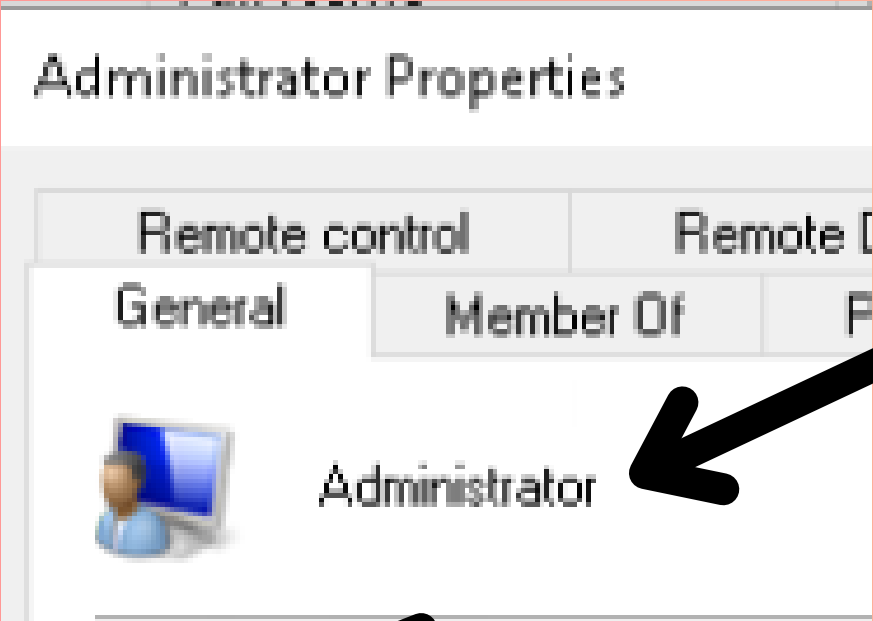
Username

Password

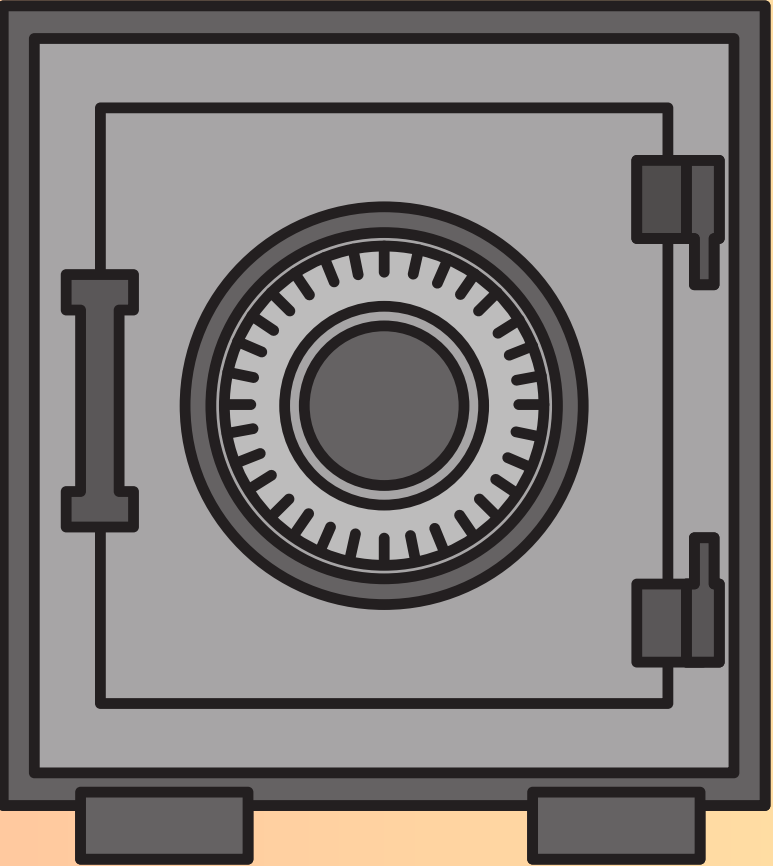
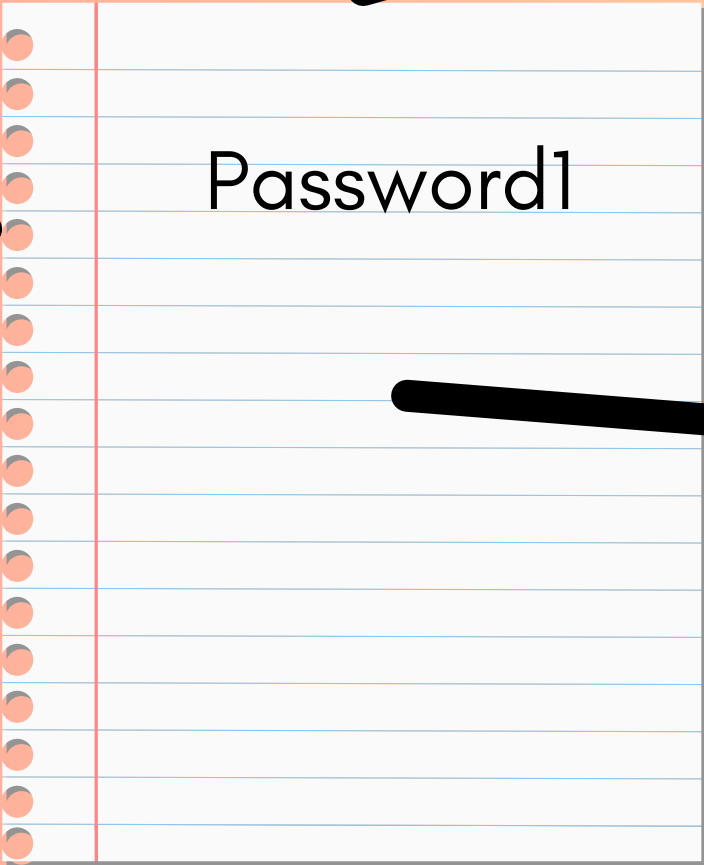
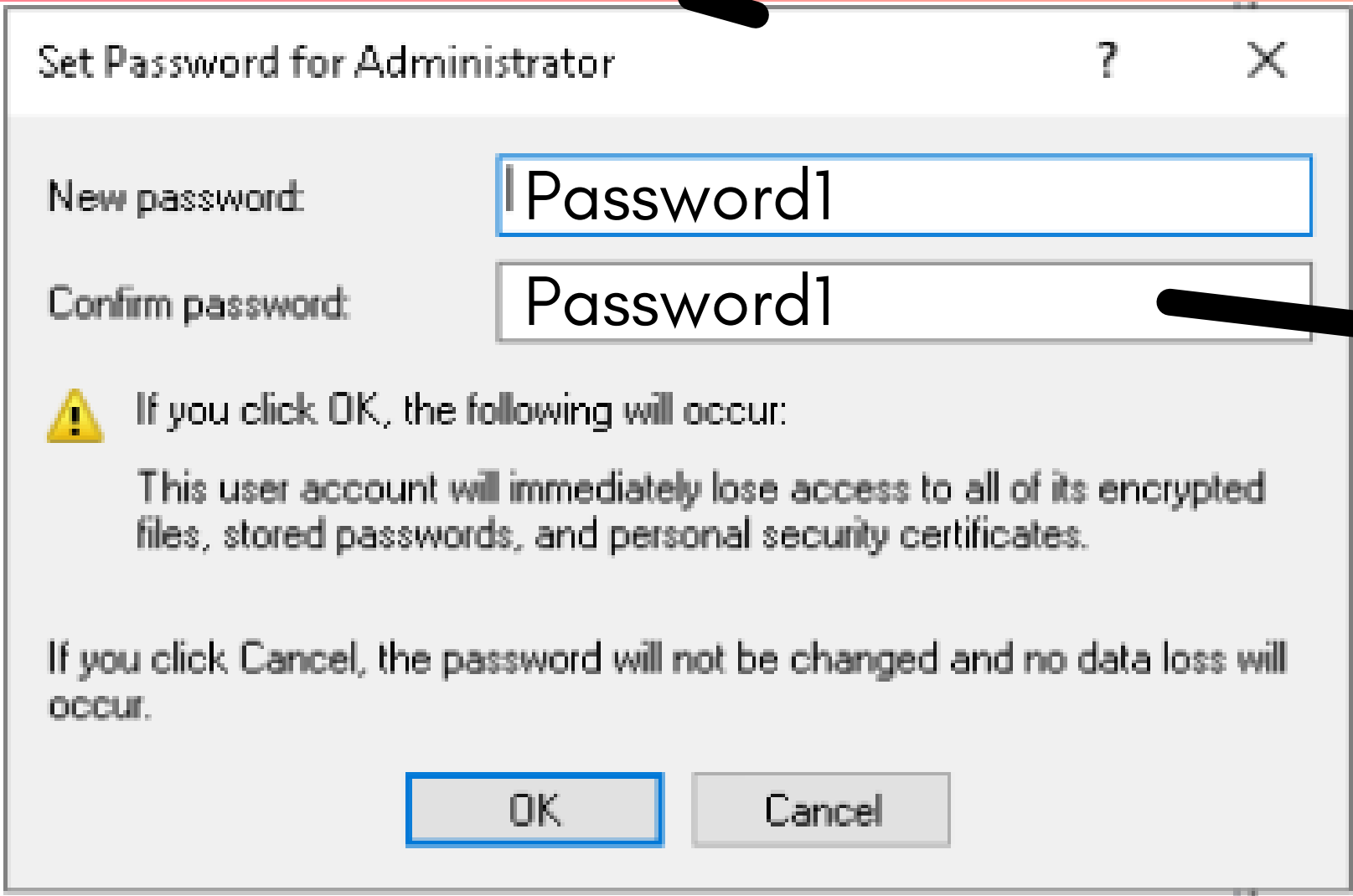
Use the generator to create a strong unique password

Authenticator key

Local Admin (Servers)



```
root@pve:~# passwd
New password:Password1
Retype new password:Password1
passwd: password updated successfully
root@pve:~#
```



"SuperAdmin" (Workstations)



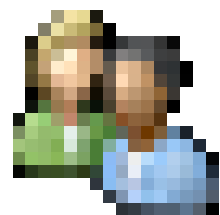
Microsoft LAPS: Install and Setup Guide

Step 1: Install Microsoft LAPS Software on Management Computers

[Learn](#) / [Windows Server](#) / [Identity and access](#) /



What is Windows LAPS?



LAPS Admins

PESLIBPC Properties

Location	Managed By	Dial-in	BitLocker Recovery
General	Operating System	Member Of	Delegation

Local Administrator Password Solution

Current LAPS password expiration:

16 October, 2025 08:03

Set new LAPS password expiration:

Thursday , October 16, 2025 8:03 AM

LAPS local admin account name:

localadmin

LAPS local admin account password:

Password1

LAPS (Workstations)

Scope Details Settings Delegation Status

Delegation

Computer Configuration (Enabled)

Policies

Administrative Templates

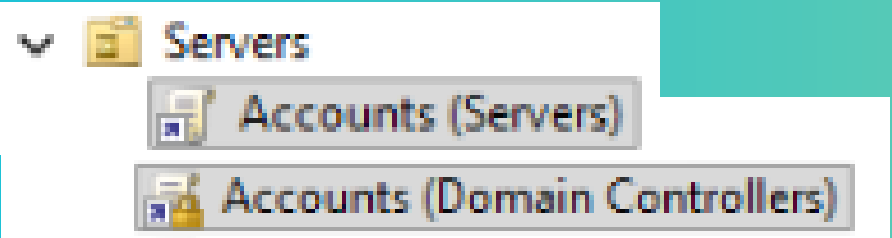
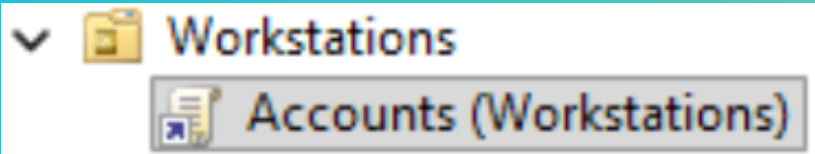
Policy definitions (ADMX files) retrieved from the central store.

System/LAPS

Policy	Setting
Configure authorized password decryptors	Enabled
Authorized password decryptor	
Configure password backup directory	Enabled
Backup directory	
Configure size of encrypted password history	Enabled
Encrypted password history size	
Enable password backup for DSRM accounts	Enabled
Enable password encryption	Enabled
Name of administrator account to manage	Enabled
Administrator account name	
Password Settings	Enabled
Password Complexity	
Password Length	
Password Age (Days)	
Passphrase Length (words)	
Post-authentication actions	Enabled
Grace period (hours):	
Actions:	

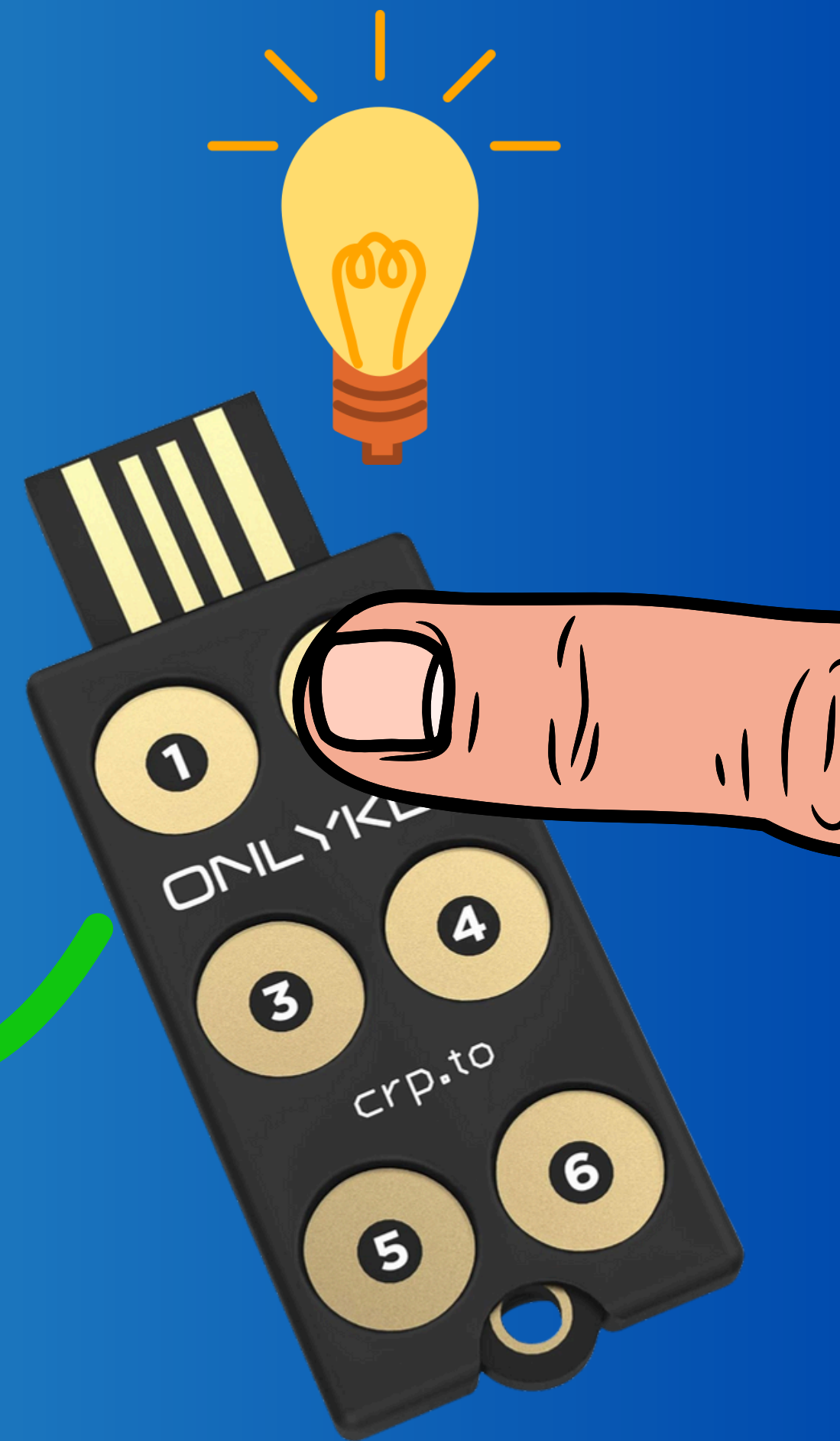
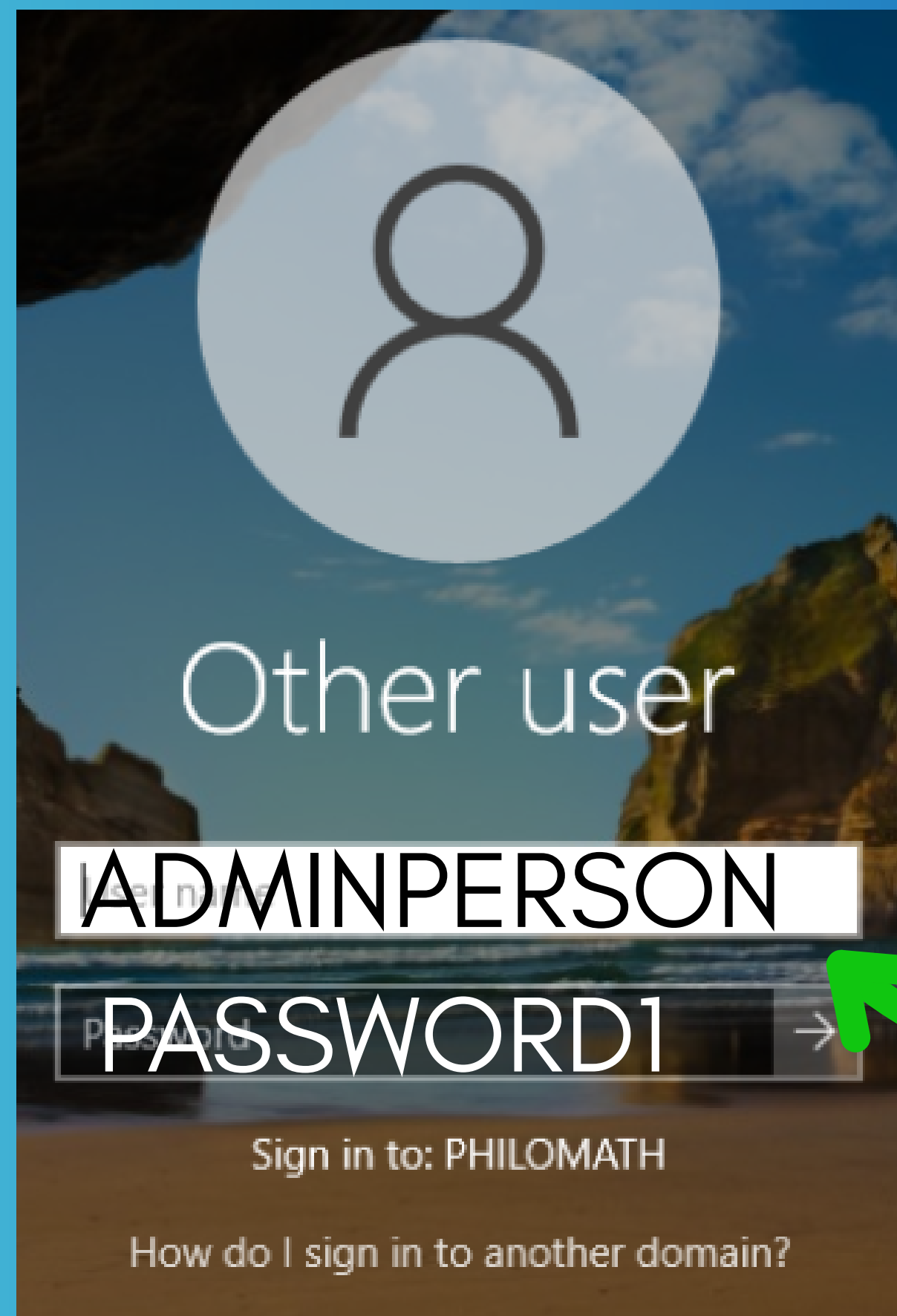
IT Admin Accounts

- Domain Admin
- Server Admin
- Workstation Admin
- Entra Admin
- Google Workspace Admin



Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Local Policies/User Rights Assignment	
Policy	Setting
Deny log on as a batch job	PHILOMATH\Workstation Admins, PHILOMATH\Enterprise Admins, PHILOMATH\Domain Admins
Deny log on as a service	PHILOMATH\Workstation Admins, PHILOMATH\Enterprise Admins, PHILOMATH\Domain Admins
Deny log on locally	PHILOMATH\Domain Admins, PHILOMATH\Enterprise Admins, PHILOMATH\Workstation Admins
Deny log on through Terminal Services	NT AUTHORITY\Local account, PHILOMATH\Domain Admins, PHILOMATH\Enterprise Admins, PHILOMATH\Workstation Admins

- Domain Admins
- Server Admins
- Workstation Admins



Service Accounts

Remote Desktop Services Profile COM+ Attribute Editor

Attributes:

Attribute	Value
ipPhone	<not set>
isCriticalSystemObject	<not set>
isDeleted	<not set>
isRecycled	<not set>
jpegPhoto	<not set>
	<not set>
labeledURI	<not set>
lastKnownParent	<not set>
lastLogoff	<not set>
lastLogon	<not set>
lastLogonTimestamp	2025-09-26 16:14:04 Pacific Daylight Time
legacyExchangeDN	<not set>
lmPwdHistory	<not set>

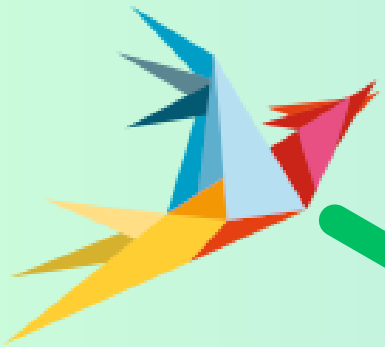
Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [DC.philomath.k12.or.us]

- > Saved Queries
- > philomath.k12.or.us
 - > Builtin
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipals
 - > Managed Service Accounts
 - > PSD17J
 - > Users
 - > Security Groups
 - > Data Groups
 - > Entra Groups
 - > Filter Groups
 - > Main Groups
 - > Manual Groups
 - > Override Groups
 - > Override Main
 - > Override Student Services
 - > Override Union
 - > Print Groups
 - > Student Services Groups
 - > Tech Groups
 - > Union Group
 - > Zammad Groups
 - > Service
 - > Staff

Name	Type
Meraki	User
Scanne	User
Service	User
Service	User
service	User
Service	User
Service	User
Service	User
Service	User
Service	User
Service	User
Service	User
Service	User
Service	User



Zammad


Bind User

PHILOMATH

Service.Zammad

Generic Account Emails





Adobe Admin

Active
Last sign in: A month ago
Created: Mar 28, 2023

Organizational unit

philomath.k12.or.us > **Service**



● Default

Google SAML

PROTOCOL

SAML

CERTIFICATE TYPE

SHA-256

AUTO-ACCOUNT CREATION

● Enabled

CREATED AT

Sep 1, 2020

UPDATE STRATEGY

Always Update

Test

Edit

● Active

Google OIDC

PROTOCOL

OIDC

CERTIFICATE TYPE

SHA-256

AUTO-ACCOUNT CREATION

● Enabled

CREATED AT

Oct 18, 2021

UPDATE STRATEGY

Always Update

Test

Set default



[Parent of a Canvas User?](#)
[Click Here For an Account](#)

Login

such.admin@philomath.k12.or.us

Password

.....

☐ Stay signed in

[Forgot Password?](#)

Log In

[Help](#) [Privacy Policy](#) [Cookie Notice](#) [Acceptable Use Policy](#)

[Facebook](#) [X.com](#)



Meet the Instructure Learning Platform:

[Canvas LMS](#) [Mastery Connect](#) [Elevate Analytics](#) [Impact](#)

Google Group *Alias*:

SERVICE - IT Admin (0)

 philomath.k12.or.us

- Up to date

RENAME GROUP

EDIT MEMBERSHIP QUERY

ACCESS SETTINGS

INSPECT GROUP

DELETE GROUP

Group labels

Access type: Custom Mailing Dynamic

Group information

Group details

Group email

philomath.k12.or.us

Group description

[Add a group description](#)

Aliases

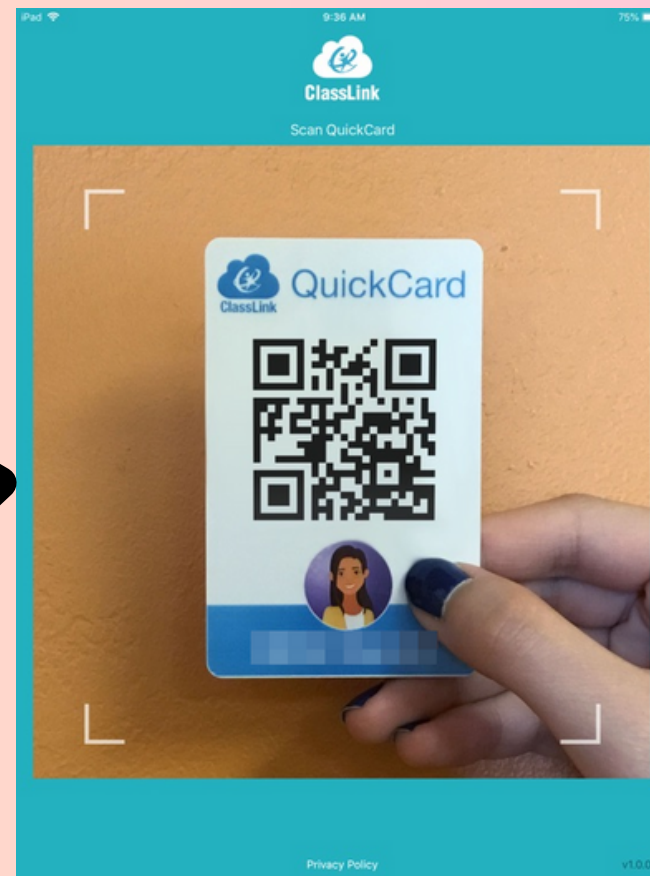
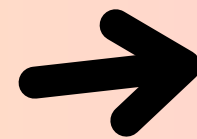
Alias

[ilomath.k12.or.us](#)
[k12.or.us](#)
[ilomath.k12.or.us](#)
[k12.or.us](#)
[h.k12.or.us](#)
[ath.k12.or.us](#)
[ath.k12.or.us](#)
[or.us](#)
[k12.or.us](#)
[.or.us](#)
[xmath.k12.or.us](#)
[math.k12.or.us](#)
[lomath.k12.or.us](#)
[nath.k12.or.us](#)
[ath.k12.or.us](#)
[philomath.k12.or.](#)

Generic Staff Accounts

- Substitutes
- Student Teachers
- Volunteers

K-2 Students



First.Last@sub.domain



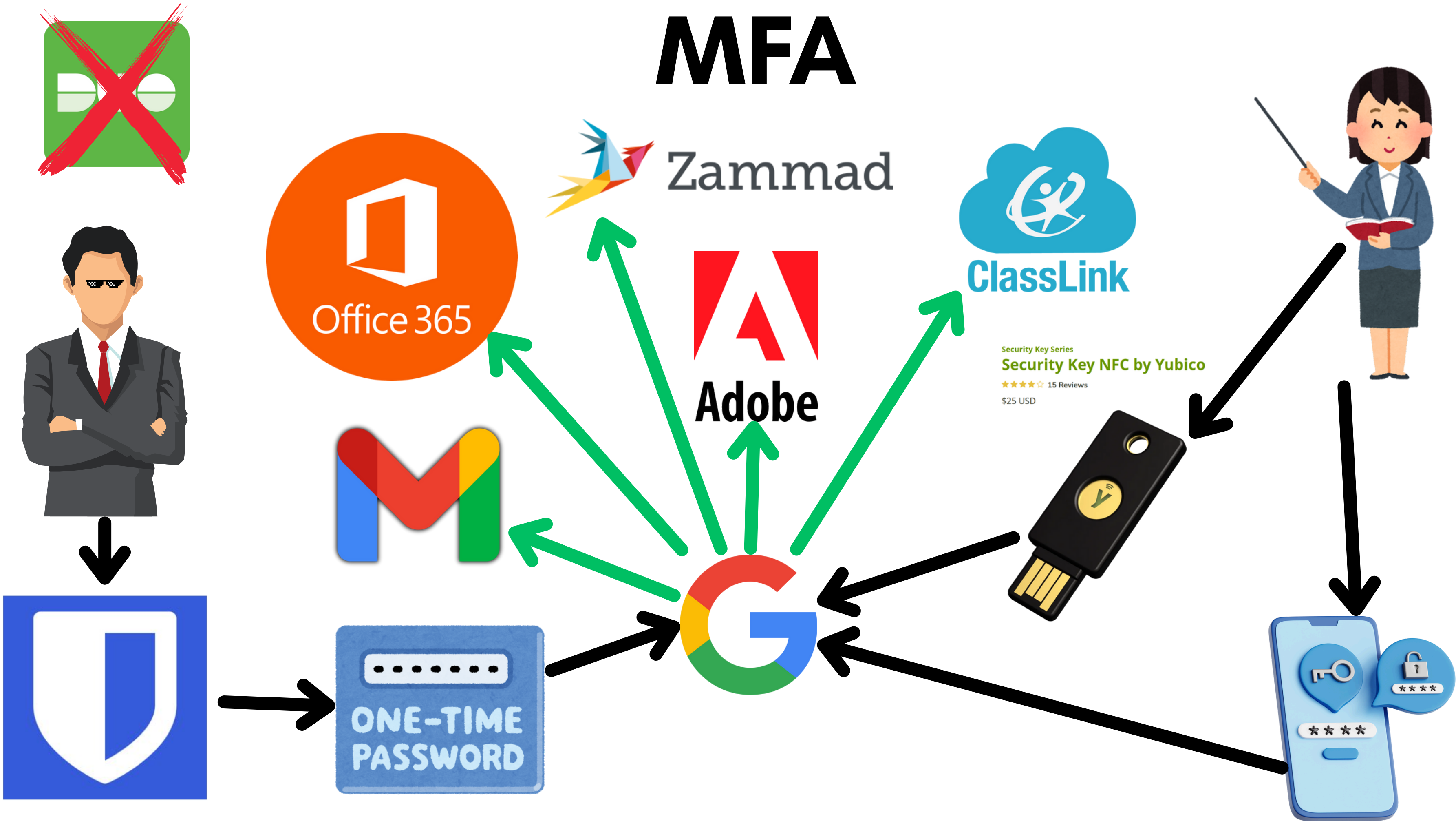
First.Last@student.domain

Scream Test!

- *Mostly* a last resort
- Mind your timing
- Disable, don't delete
- Have a backout plan



MFA





Joshua Martin <joshua.martin@philomath.k12.or.us>

to All

Thu, Sep 21, 2023, 11:55 AM



Hello Philomath!!

Josh here with the Tech Department.

Today I would like to talk about **Two-Factor Authentication**. (Also known as **2FA**, **Multi-Factor**, or **MFA**.)

You may have heard whispers about it, and to some it may seem like a big scary monster, but *here's the truth*:

Most of you are using 2FA already somewhere, whether you know it or not.

In it's simplest form, after you enter your password, you will receive a text message with a code. Enter that code and you will be logged in.

Many banks and other institutions have required it for years now, and with good reason...

Two-Factor Authentication:

- Takes a whopping **90 seconds** to set up. (aka Google)
- Reduces the likelihood of your account being compromised ("hacked") by **over 90%**
- Will soon be **mandatory** for all staff to maintain PACE insurance compliance.

I **highly** recommend you get ahead of the curve and enable it now, **before** it becomes mandatory.

[Here is the setup Guide!](#)
(5 steps, 90 Seconds.)

[Warning: The following contains my opinion. This is not intended to diagnose, treat, or cure any virus in humans or computers.]

I'm gonna be real with you about phones...

I know some folks have a lot of reservations about the phone situation. While I understand the initial skepticism, these concerns are largely unfounded.

In fact it's ironic that anyone is distressed about using SMS to their phone, since it's technically a slightly less secure option (but still plenty for our purposes.)

We elected allow the use of personal phones for everyone's convenience.

There are dozens of other districts who have run into these same hurdles, and they all had the same experience; They enforce two-factor, but no one wants to use their phone, either on principle or because they have misunderstandings about the technology, so the district spends a ton of money on physical security keys, and a month later everyone flips to using their phone because it is so much more convenient with zero downsides. From the numbers I know about, if you choose to use a security key, the likelihood that you'll still be using it 90 days from now is less than 1%.

Do with that information what you will.

Personally, I don't really care what people choose. It's not my money, and physical security keys are super secure, they're just inconvenient.

I use one, but I'm a security nut, and admittedly sometimes it is super annoying.

[Non-Warning: The following does not contain my opinion.]

Having said all that, we strongly recommend using your personal phone for Two-Factor for a number of reasons:

Philomath SD17J Knowledge Base > Google & Gmail > How do I enable 2FA? (Two-Factor Authentication)

How do I enable 2FA? (Two-Factor Authentication)

I'm sure you've all heard by now the need for Two-Factor Authentication, but as a refresher 2FA:

- Reduces the likelihood of your account being compromised by over 90%
- Is now mandatory for all staff to maintain PACE insurance compliance.
- Takes about 90 seconds to set up.

There are multiple forms of 2FA. We highly recommend just doing "Phone Number" and getting a text message. It's the most convenient, you might get 3 or 4 texts a year, your phone number isn't used for advertising, it's not sold to anyone, the tech department can't see anything you're doing on your phone, and Google doesn't get any additional access to your phone.

Here are the steps to enable 2FA:

1) From Gmail or Google Drive, click your little profile icon in the top-right and click "Manage your Google Account"



My Devices

Select All Group Action Filter All ☐ OS Filter

Webcams [Add Device](#)

<input type="checkbox"/> ops-cam	<input type="checkbox"/> noc-cam
----------------------------------	----------------------------------

Linux (Agent) [Add Agent](#) [Index](#)

<input type="checkbox"/> gods Agent, Powered	
---	--

Linux (Only) [Add Device](#)

<input type="checkbox"/> cubebackup-google	<input type="checkbox"/> cubebackup-ms365
<input type="checkbox"/> helpdesk	<input type="checkbox"/> meshcentral
<input type="checkbox"/> truenas	<input type="checkbox"/> truenas-backup

Linux Workstations [Add Agent](#) [Index](#)

<input type="checkbox"/> NOODIRLXS Agent, Powered	
--	--

Windows [Add Device](#)

<input type="checkbox"/> GHOST	<input type="checkbox"/> linewiz
<input type="checkbox"/> SMOKE	<input type="checkbox"/> SNAIL

iPhone [Add Device](#)

<input type="checkbox"/> cisco-voice-gateway	<input type="checkbox"/> freepbx
--	----------------------------------

PIXELLOR [Add Agent](#) [Index](#)

<input type="checkbox"/> Pixellor PHS Pool IDF	<input type="checkbox"/> Pixellor Stadium
--	---

Philomath

MeshCentral

Welcome Administrator. [Logout](#)

General Desktop Terminal Files Events Details Console

Desktop - HVAC

Disconnect Connected Actions Settings...

Press Ctrl+Alt+Delete to unlock

12:59
Wednesday, October 8

Alt + Ctrl + Del Send Clipboard Type ☒ Input 2 ms 00:00:10 Tools

[Terms & Privacy](#)

Proxmox

Proxmox VE Login

Second login factor required

WebAuthn TOTP App Recovery Key

Please enter your TOTP verification code:

Confirm Second Factor

Philomath MeshCentral

Token

Log In

☐ Remember this device for 30 days.

[Back to login](#)

Linux

```
administrator@noc-josh:~$ ssh truenas_admin@truenas-backup.philomath.k12.or.us -i truenas-backup-key-ecdsa
Enter passphrase for key 'truenas-backup-key-ecdsa':
```


Group Info

Non-School Locations:

- DO (District Office)
- SSO (Student Services Office)
- FO (Facilities Office)
- TO (Technology Office)
- CCP (Clemens Community Pool)

School Locations:

- CPS (Clemens Primary School)
- PA (Philomath Academy)
- PES (Philomath Elementary School)
- PMS (Philomath Middle School)
- PHS (Philomath High School)
- KVCS (Kings Valley Charter School)

Staff Positions:

- Admin
- Teacher
 - Counselor
- Instructional Assistant
- Custodian
- Media (Library)
- Office
- Kitchen
- Manager
- Nurse

Non-Staff Positions:

- Student
- Coach
- Substitute
- Student Teacher
- Board Members
- Volunteers
- External (Usually ESD)

Student Services:

- SpEd (Special Education)
 - SpEd Case Managers
 - SpEd IAs
- SLP (Speech/Language Pathology)
- ELL (English Language Learners)
- MTSS (Multi-Tiered System of Support)
 - Formerly RTII

Union/Contract:

- Licensed (PEA Members)
- Classified (OSEA Members)
- Admin
- Confidential
- Extra Duty

Special Cases:

- District Media
- District Kitchen
- PEA Leadership
- OSEA Leadership
- Registrars
- Campus Stewards

Account Creation

```
PS C:\Windows\system32> C:\scripts\CREATE-ACCOUNT-STAFF.PS1
First Name?: Potato
Potato
Middle Initial (Optional)? :
Last Name?: Potato
|Teacher|Coach|Counselor|Custodian|Instructional Assistant|Kitchen|Media|Nurse|Student Teacher|Admin|Off
Position?: Nurse
Valid Locations for this position: | BES | CPS | KVCS | PA | PES | PHS | PMS |
Location?: BES
Potato
Potato

Please Review:
Full Name:      Potato Potato
UserPrincipalName: potato.potato@philomath.k12.or.us
sAMAccountName: potapota
Mail:          potato.potato@philomath.k12.or.us
OU:            OU=BES,OU=Staff,OU=Users,OU=PSD17J,DC=philomath,DC=k12,DC=or,DC=us
DistinguishedName: CN=Potato Potato,OU=BES,OU=Staff,OU=Users,OU=PSD17J,DC=philomath,DC=k12,DC=or,DC=us
Home Directory: \\truenas.philomath.k12.or.us\staff\potapota
Press Enter to Verify User:
```

Union

employeeNumber	101538
employeeType	Classified

Student Services

Office:	SpEd
---------	------

Populate Groups

```
PRE-GCDS-AD-SCRIPT.PS1 X CREATE-ACCOUNT-STAFF.PS1
947
948 if ($True) {
949     Start-Transcript -Path $global:LOGFILE -Force
950     Delete-DisabledStaff
951     Delete-DisabledStudents
952     Clear-PersonalData
953     Check-TitleOffice
954     Set-BasicInfo
955     Check-BasicInfo
956     Set-IPhone
957     Fix-StaffUserAccountControl
958     Set-StaffUnion
959
960     Set-EntraGroupMembers
961     Set-StaffFilterGroup
962     Set-StaffDataGroup
963     Clear-MainGroupMembers
964     Clear-SSGroupMembers
965     Clear-UnionGroupMembers
966
967     Set-SSGroupMembers
968     Set-MainGroupMembers
969     Set-UnionGroupMembers
970     Fix-UnionConflict
971     Set-OverrideGroups
972     Set-MetaGroupMembers
973
974     Suspend-InactiveComputers
975     Move-StagedComputers
976     repadmin /syncall /A /e
977     if ($UNATTENDED) {
978         Archive-StudentFolders
979         Create-StudentFolders
980         Archive-StaffFolders
981         Create-StaffFolders
982         Fix-ShareFolders
983     }
984     Stop-Transcript
985     Send-SMTPReport
986 }
```

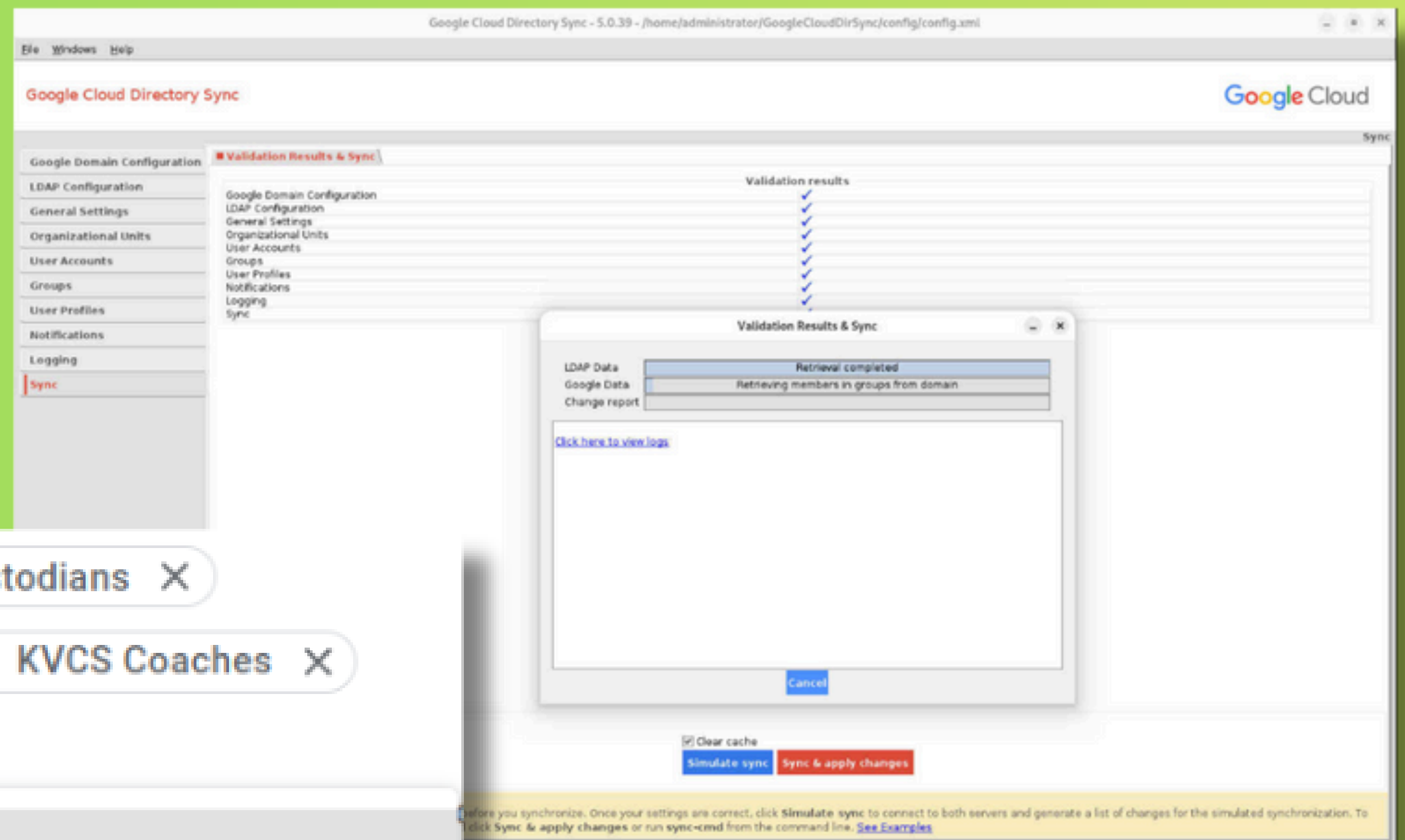
Location

- Staff
 - BES
 - CCP
 - CPS
 - DO
 - External
 - FO
 - Generic
 - KVCS
 - PA
 - PES
 - PHS
 - PMS
 - SSO
 - Substitute
 - TO

Position

Joshua Martin Properties				
Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop	Services Profile	COM+	Attribute Editor	
General	Class	Account	Profile	Telephones
General	Class	Account	Profile	Telephones
Job Title:	Manager			
Department:	TO			
Company:	Philomath SD17J			

GCDS



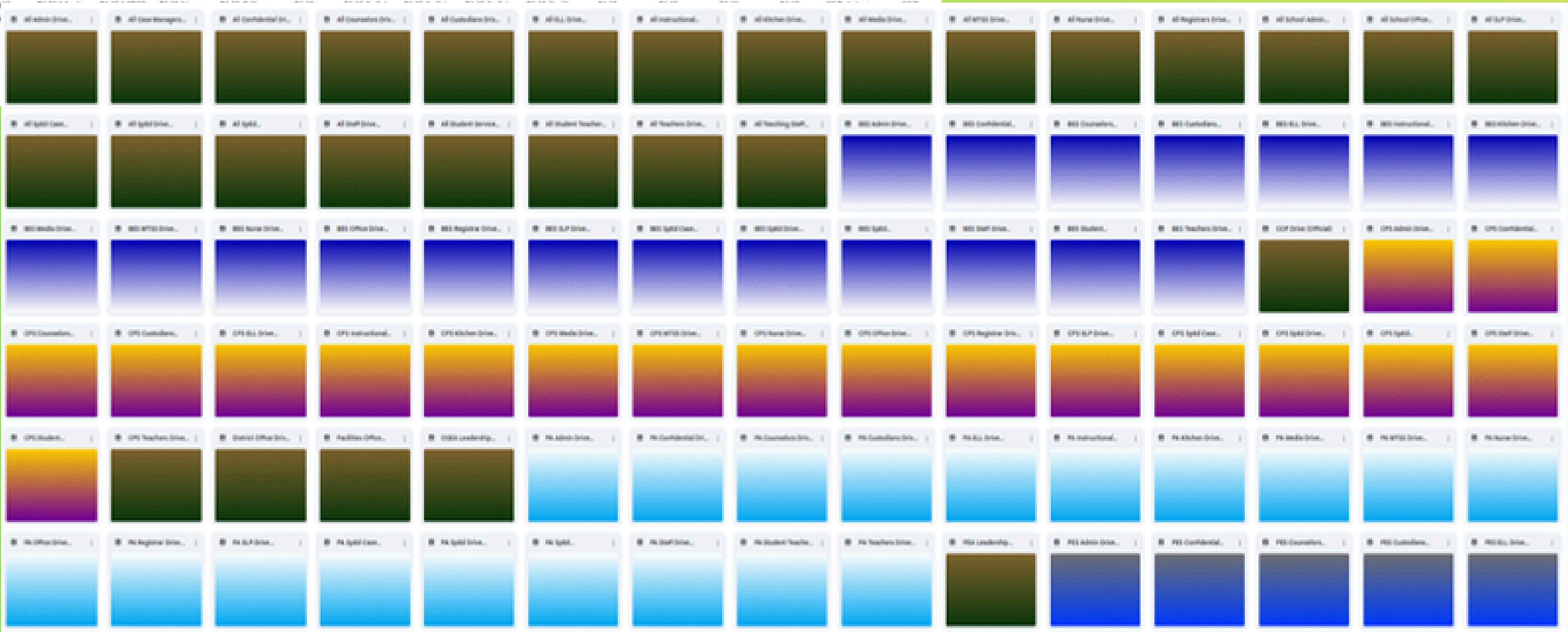
To P PES SpEd Case Managers X P PMS Custodians X
C CCP Licensed Staff (PEA Members) X K KVCS Coaches X
P PMS Office Staff X cps

Subject

Classification

- C **CPS Staff**
cps.staff@philomath.k12.or.us
- C **CPS Admin Mail**
cps.admin@philomath.k12.or.us
- C **CPS Teachers Mail**
cps.teachers@philomath.k12.or.us
- P **PSD CPS All Staff**
psdcpsallstaff@philomath.k12.or.us





User Manager

What is User Manager

Users Groups Directories Settings UCP Templates Call Activity Groups

Group Priorities can be changed by clicking and dragging groups around in the order you'd like. Groups with a lower number are higher priority.

Add Delete All Directories

Directory	Group Name	Description
<input type="checkbox"/> Philomath Active Directory	All Staff	
<input type="checkbox"/> PBX Internal Directory	All Generics	Rule C
<input type="checkbox"/> Philomath Active Directory	TO Office	
<input type="checkbox"/> Philomath Active Directory	DO Office	
<input type="checkbox"/> Philomath Active Directory	FO Office	
<input type="checkbox"/> Philomath Active Directory	All Substitute	
<input type="checkbox"/> Philomath Active Directory	BES Coach	
<input type="checkbox"/> Philomath Active Directory	CPS Coach	
<input type="checkbox"/> Philomath Active Directory	All Coach	
<input type="checkbox"/> Philomath Active Directory	PMS Coach	
<input type="checkbox"/> Philomath Active Directory	PHS Coach	
<input type="checkbox"/> Philomath Active Directory	PES Coach	
<input type="checkbox"/> Philomath Active Directory	PA Coach	
<input type="checkbox"/> Philomath Active Directory	KVCS Coach	
<input type="checkbox"/> Philomath Active Directory	SSO Office	
<input type="checkbox"/> Philomath Active Directory	PA Staff	
<input type="checkbox"/> Philomath Active Directory	PHS Staff	
<input type="checkbox"/> Philomath Active Directory	PMS Staff	
<input type="checkbox"/> Philomath Active Directory	PES Staff	
<input type="checkbox"/> Philomath Active Directory	BES Staff	
<input type="checkbox"/> Philomath Active Directory	CPS Staff	
<input type="checkbox"/> Philomath Active Directory	All Nurse	
<input type="checkbox"/> Philomath Active Directory	All Campus Steward	Campus Steward (General Administration)
<input type="checkbox"/> PBX Internal Directory	DO Generics	14
<input type="checkbox"/> PBX Internal Directory	Tech Generics	15



admin

Access points Cardholders Keys Monitoring Tools System

User access levels

NAME	DESCRIPTION	PARTITION
<input type="checkbox"/> All Admin	Synced from Active Directory	General
<input type="checkbox"/> All Campus Steward	Synced from Active Directory	General
<input checked="" type="checkbox"/> All Classified	Synced from Active Directory	General
<input type="checkbox"/> All Coach	Synced from Active Directory	General
<input type="checkbox"/> All Confidential	Synced from Active Directory	General
<input type="checkbox"/> All Counselor	Synced from Active Directory	General
<input type="checkbox"/> All Custodian	Synced from Active Directory	General
<input type="checkbox"/> All Instructional Assistant	Synced from Active Directory	General
<input type="checkbox"/> All Kitchen	Synced from Active Directory	General
<input type="checkbox"/> All Licensed	Synced from Active Directory	General
<input type="checkbox"/> All Manager	Synced from Active Directory	General
<input type="checkbox"/> All Monitor	Synced from Active Directory	General
<input type="checkbox"/> All Nurse	Synced from Active Directory	General
<input type="checkbox"/> All Office Admin	Synced from Active Directory	General
<input type="checkbox"/> All Office	Synced from Active Directory	General
<input type="checkbox"/> All Parent Teacher	Synced from Active Directory	General
<input type="checkbox"/> All Substitute	Synced from Active Directory	General

ITEMS: 1 - 20 Total: 163

Page: 1 / 9

~~GAM~~ → **GAM7** ← ~~GAMADV-XT3~~

How to Install GAM7

Ross Scroggs edited this page on Dec 7, 2024 · [3 revisions](#)

Installing GAM7

Use these steps if you have never used any version of GAM in your domain. They will create your GAM project and all necessary authentications.

- [Downloads-Installs](#)
- [Linux and MacOS and Google Cloud Shell](#)
- [Windows](#)
- [GAM Configuration](#)

Things we do with GAM:

- Sync ImmutableID for MS365 SSO
- Take ownership of all Calendars
- Take ownership of all Shared drives
- Unshare all files owned by suspended users →
- Enforce Drive Sharing Settings
- "Hide" Groups and Users

```
#!/bin/bash
gam="/home/administrator/bin/gam7/gam"
dir="/unshare-suspended-staff-files"
mkdir $dir
cd $dir

# Empty list of users, Give it the correct headers
echo "primaryEmail" > ./users.csv
# Get a list of all suspended users in the "Staff" OU and below.
$gam config csv_output_header_force "primaryEmail" redirect csv ./users.csv

# Empty list of files, Give it the correct headers
echo "Owner,id" > ./files.csv
# Create a list of all files owned by all users in the list
$gam config csv_output_header_force "Owner,id" csv ./users.csv gam

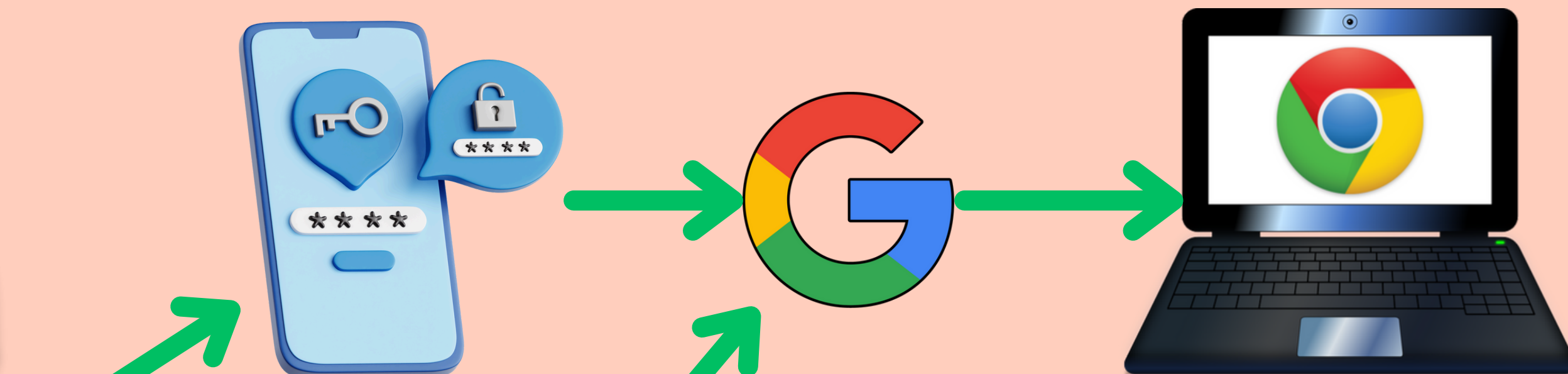
# Empty list of permissions, Give it the correct headers
echo "Owner,id,permission.role,permission.id" > ./permissions.csv
# Create a list of all permissions (ACLs Entries) for all the files
$gam config csv_output_header_force "Owner,id,permission.role,permission.id" gam

# Delete all permissions other than owner/organizer (All share permissions)
$gam config csv_input_row_drop_filter "permission.role:repan:(owner,organizer)"

# Remove user from all groups
$gam csv ./users.csv gam user "-primaryEmail" delete group

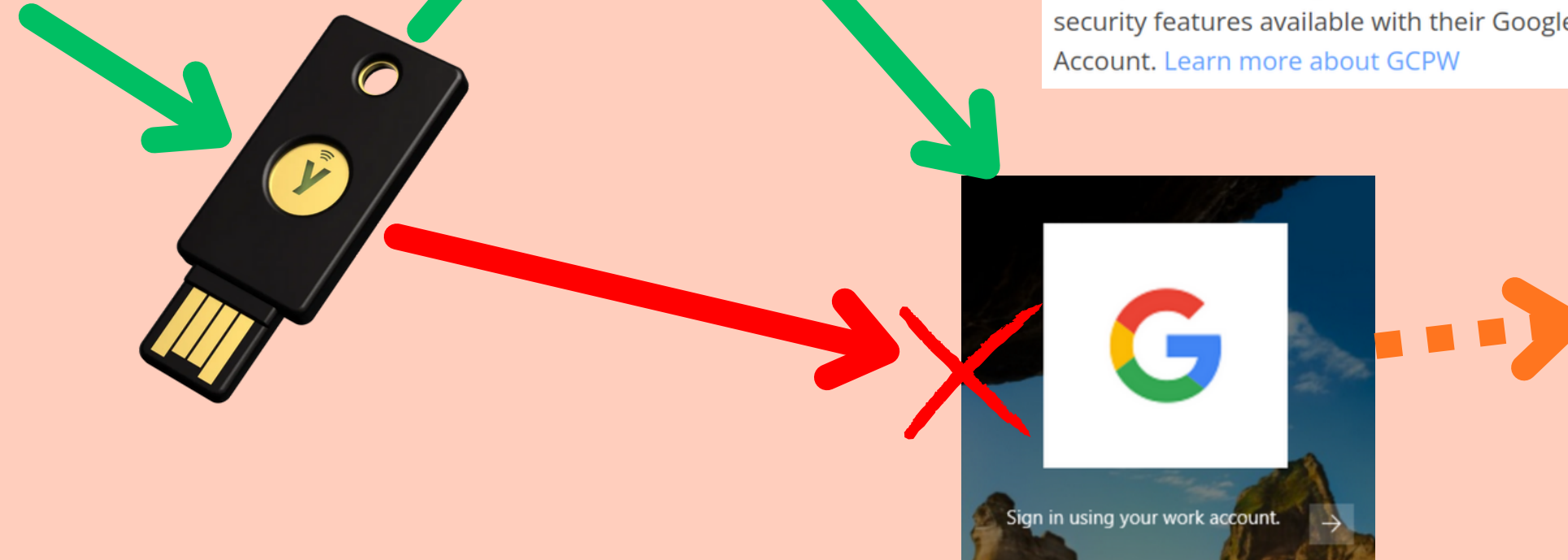
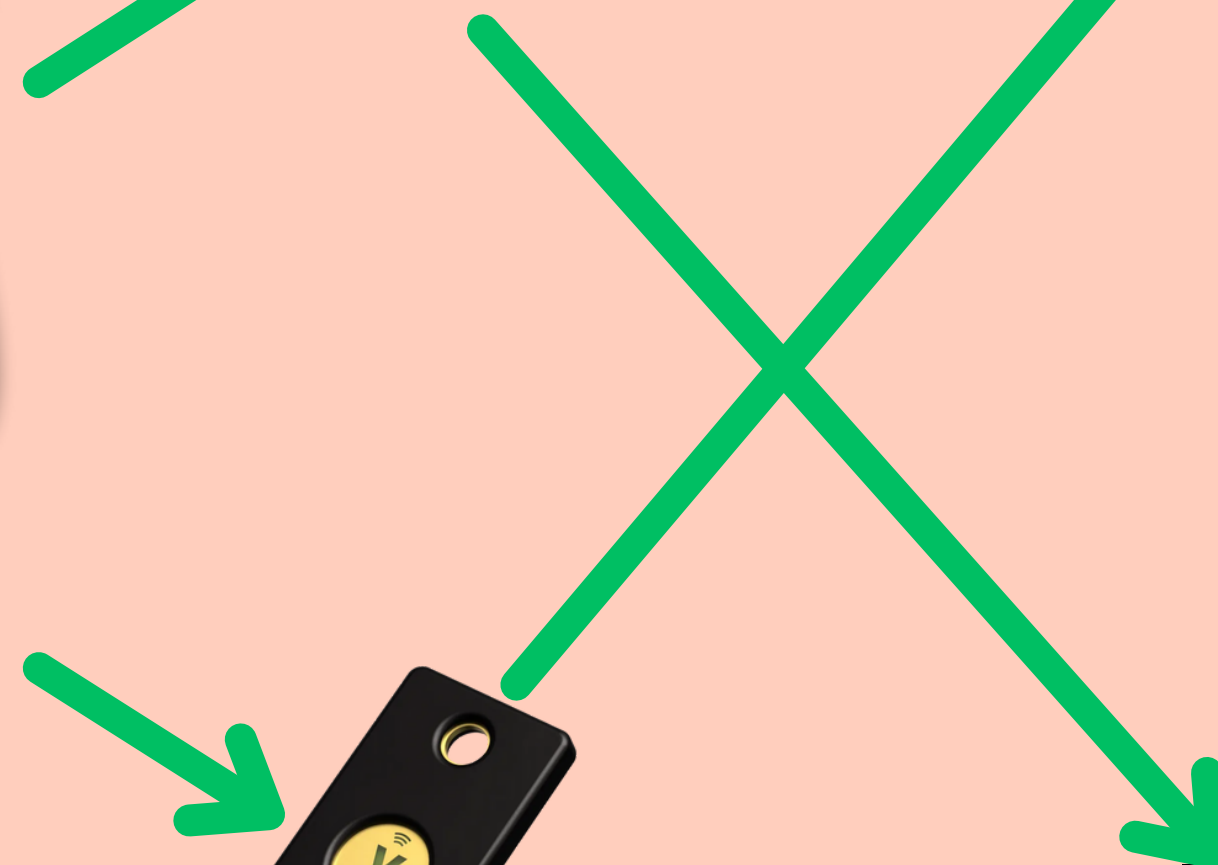
# Move users to the archive OU
$gam csv ./users.csv gam update user "-primaryEmail" org "/Staff Archive"
```

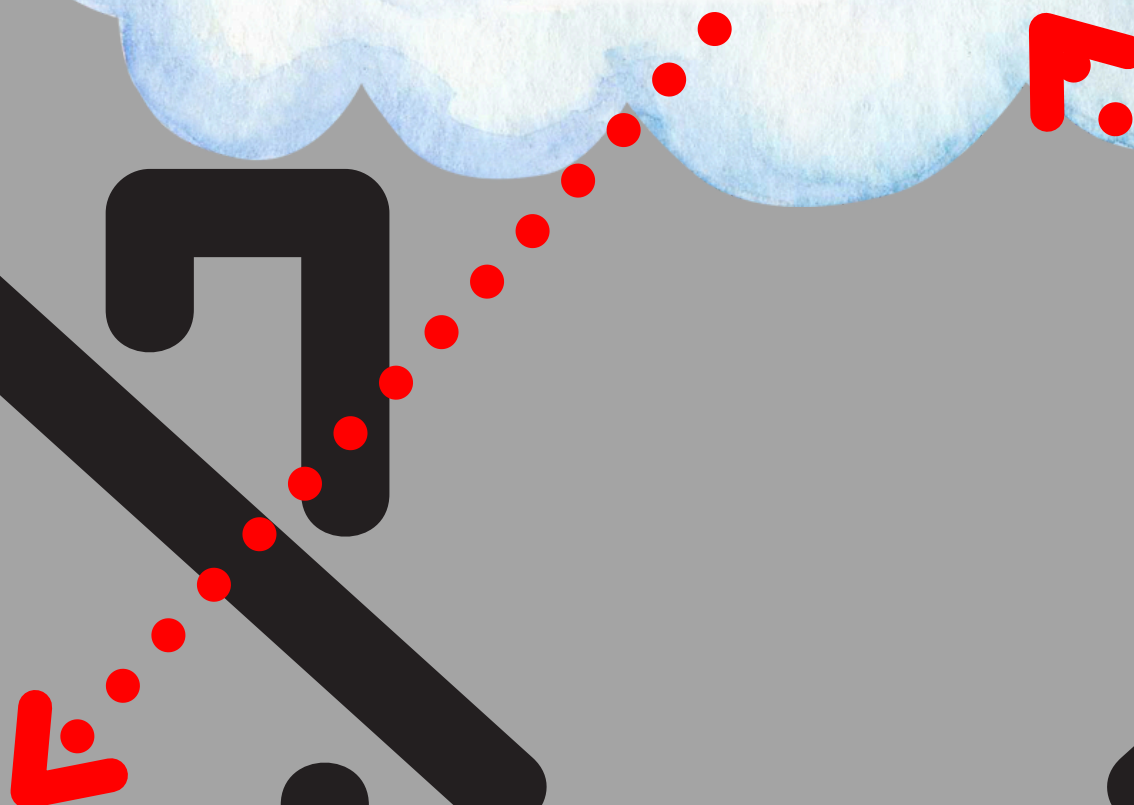
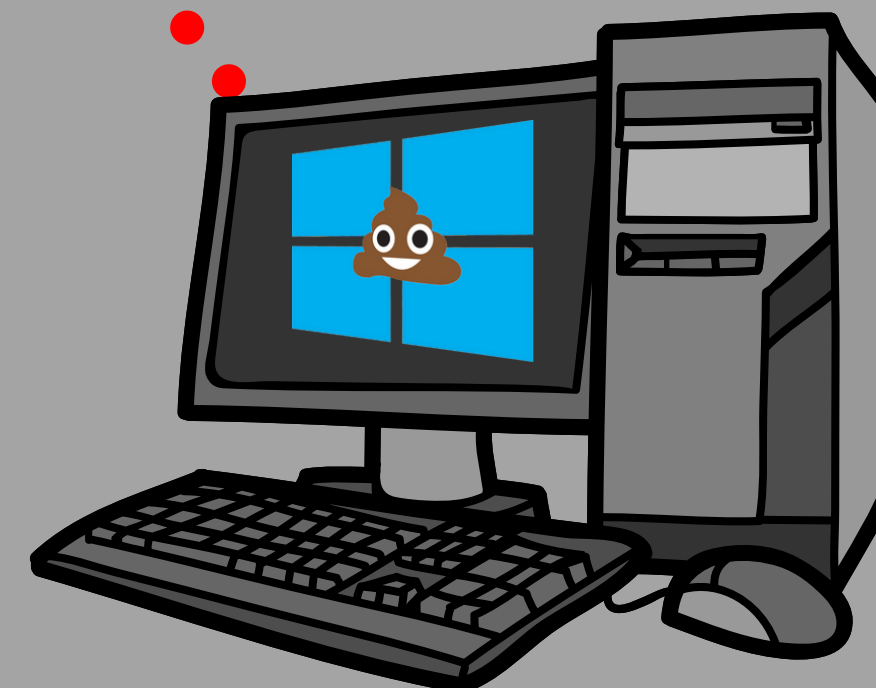
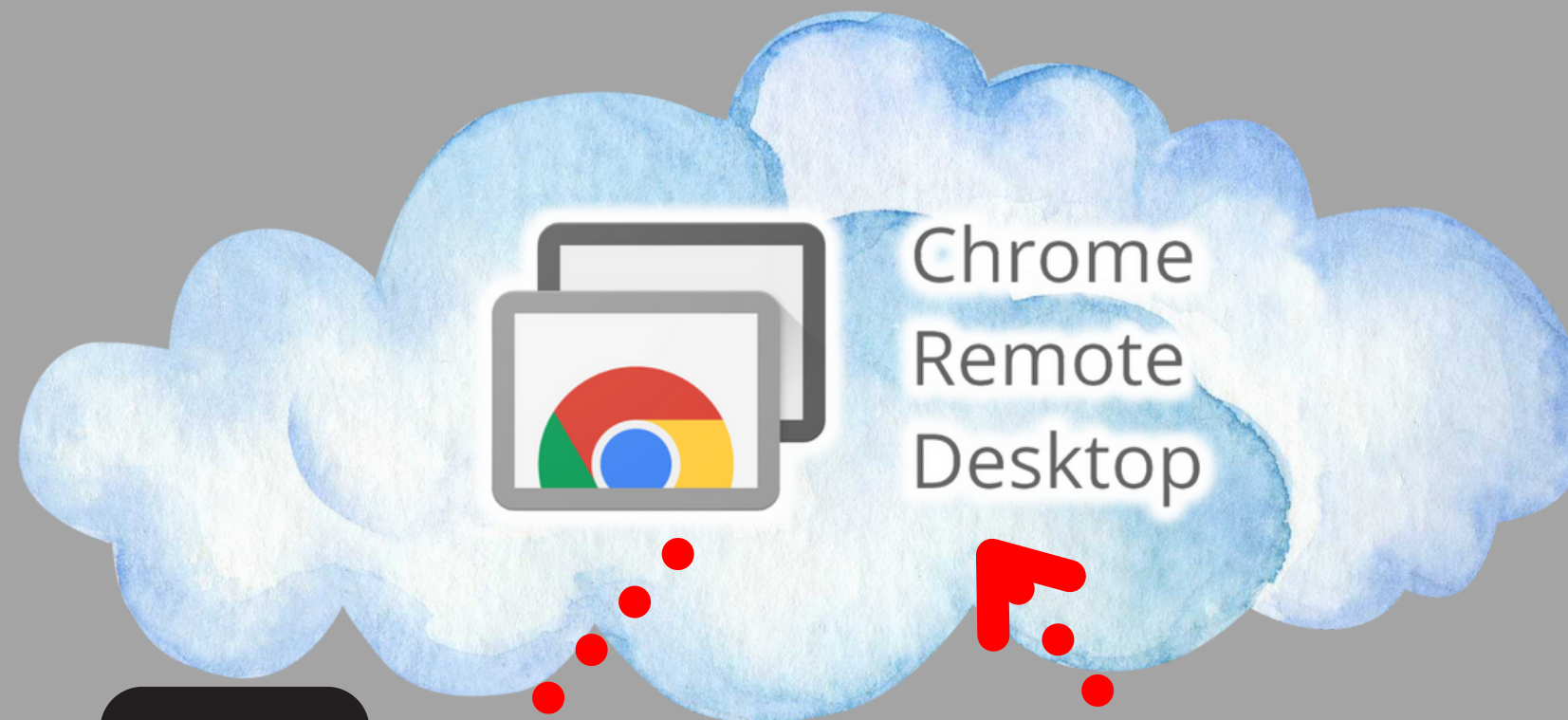
HARDWARE



Google Credential Provider for Windows®

Google Credential Provider for Windows® (GCPW) lets users sign in to Windows® devices with the Google Account they use for work. GCPW provides users with a single sign-on experience to Google services and all the security features available with their Google Account. [Learn more about GCPW](#)







Network Changes



✓ 1. IP Schema

a. 167.x.x.x → 10.x.x.x

✓ 2. VLANs

a. 30 → 200+



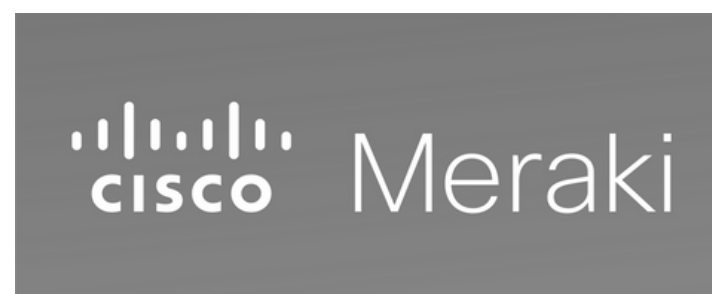
✓ 3. Internet Filter

a. iBoss → Linewize



⌚ 4. Network Switches

a. Cisco → Unifi



⌚ 5. Firewall

a. Meraki → OPNsense



Network

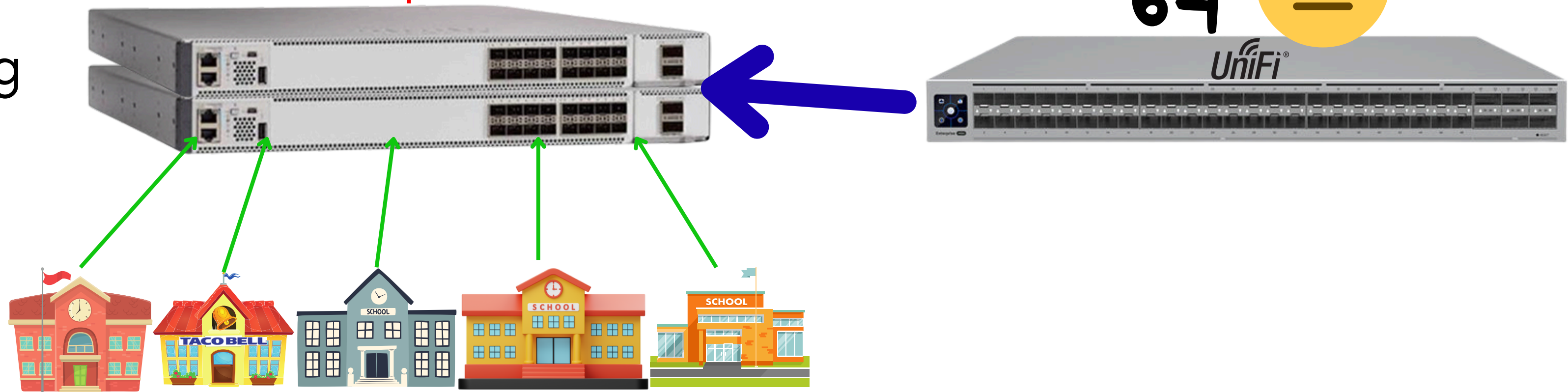
Firewall

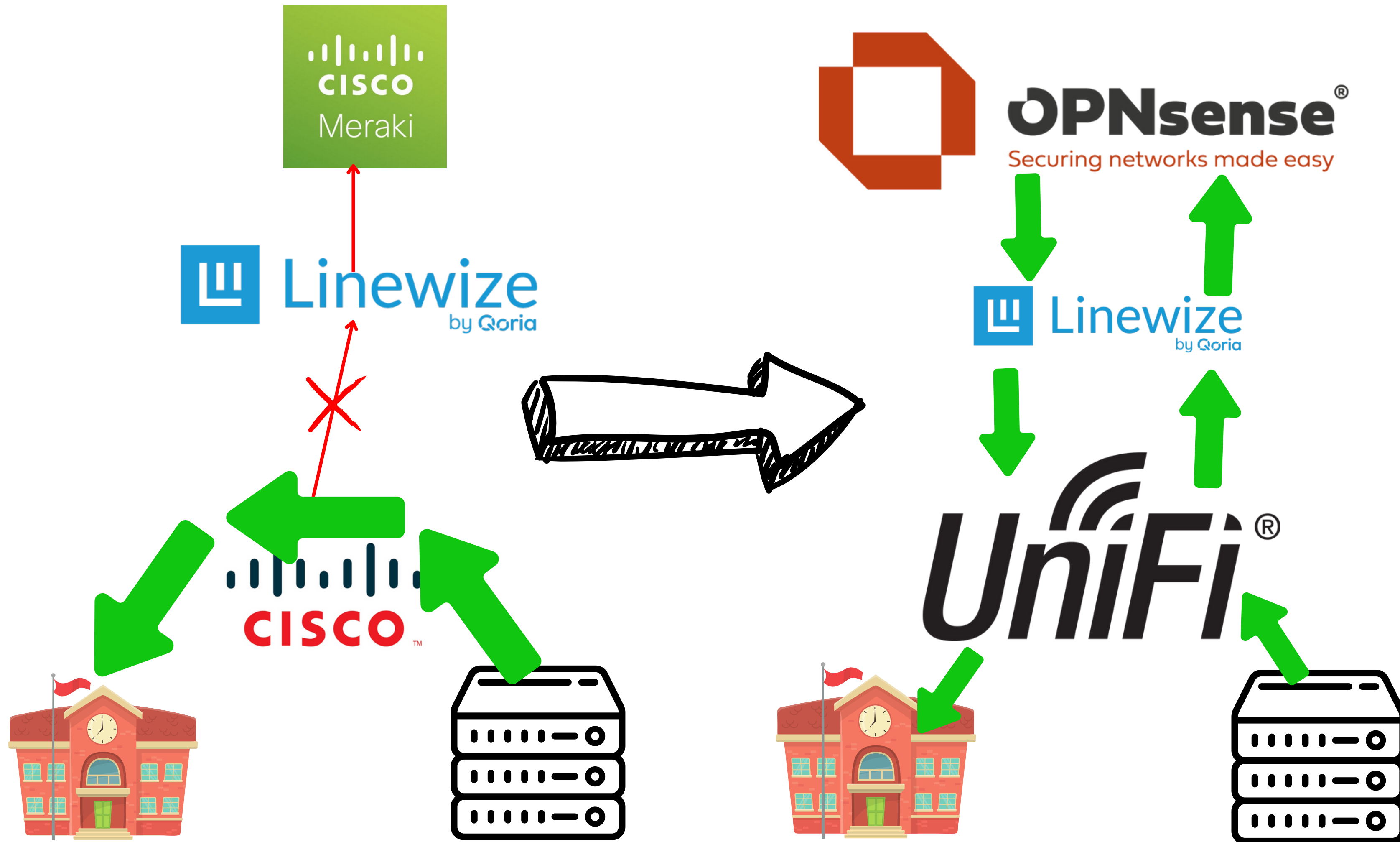


Filter



Switching





- Cheap

- 2 Mini PCs
- 1 Raspberry Pi
- 2x Dumb Switch

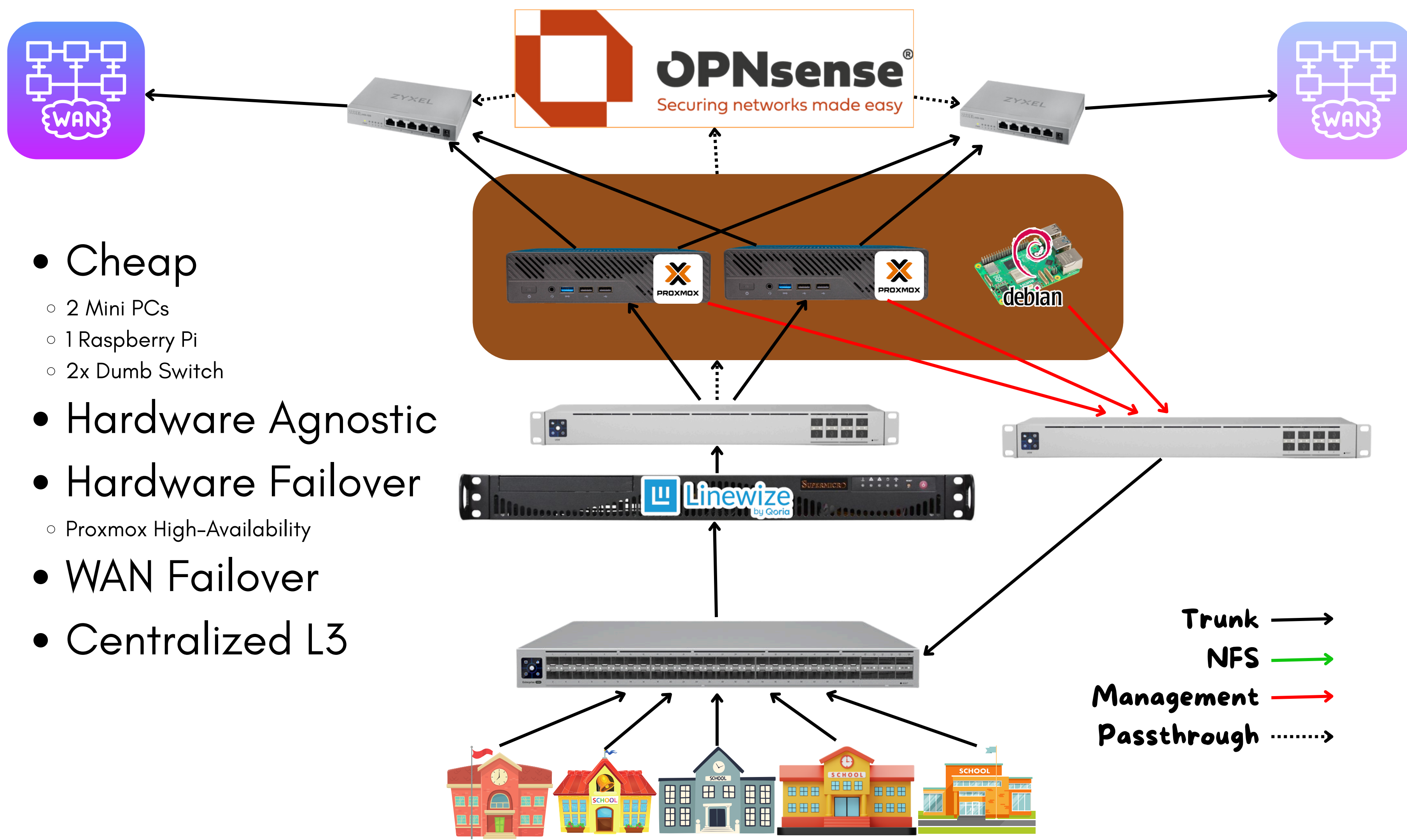
- Hardware Agnostic

- Hardware Failover

- Proxmox High-Availability

- WAN Failover

- Centralized L3





Standard Stuff:

- Firewall
- NAT
- VLANs
- Traffic Shaping / QOS
- DHCP
- DNS
- Web UI + MFA + SSO

Bonus:

- Multi-WAN
- VPN
 - WireGuard
 - OpenVPN
 - IPSec
- DDNS
- ACME / CA
- NTP
- **IDS/IPS**
 - **Suricata**
 - **Crowdsec**
- Reverse Proxy
- Load Balancing

Integrations:

- Kerberos
- LDAP
- Radius
- Zabbix
- XEN
- VMWare
- NetData
- Wazuh
- Virtualbox
- QEMU
- Puppet
- NUT
- Nextcloud
- GIT
- Google Drive/Cloud
- Tailscale / ZeroTier
- Tor



SURICATA

OPNsense

Lobby

Reporting

System

Interfaces

Firewall

VPN

Services

ACME Client

Captive Portal

CrowdSec

DHCRelay

Dnsmasq DNS & DHCP

Intrusion Detection

ISC DHCPv4

ISC DHCPv6

Kea DHCP

Monit

Network Time

Nginx

OpenDNS

Unbound DNS

Power

Help

Services: Intrusion Detection: Administration

SettingsDownloadRulesUser definedAlertsSchedule

advanced mode

General Settings

Enabled☒

IPS mode☒

Promiscuous mode☐

Interfaces

WAN

Clear AllSelect All

Detection

Pattern matcher

Default

Logging

Enable syslog alerts☒

Enable eve syslog output☐

Rotate log

Weekly

Save logs

4

Apply



Security Stack

Search for anything...

SC

Organizations

SC

Try the new Enterprise offer!

Engines

Alerts

Decisions

Remediation Metrics

Hub

Service API

Notification settings

Allowlists

Enroll command

How to install Security Engine?

Monthly alert quota exhausted

500 / 500 alerts received

Recover 34812 missing alerts

Search by name, tag or id

AllActiveInactive

Show only archived

Enroll date (newest)

Security Engine Troubleshooting

Get an overview of your Security Engines' status and identify Engines that require immediate attention.

OPNsense

1.00k Alerts

7 Scenarios

0 Remediation component

1 Blocklist

IP

Enroll date: Mar 24, 13:11:43

Last activity: today at 4:08 AM

Back to the default design

Feedback



- Hypervisor
 - VMWare → Free DELL Server + **Proxmox**
 - \$15k Savings/yr



- NAS
 - Tegile → Daktech Server + **TrueNAS**
 - \$100k+ Savings
 - Use whatever drives



- Phones
 - Cisco CUCM → Sangoma Phones + **FreePBX**
 - \$100k+ Savings
 - Use whatever phones



- Cameras
 - Dahua → Old Servers + **ZoneMinder**
 - Multiple Dollars! in savings
 - Use whatever cameras





debian

- Hypervisor
- NAS
- Phones
- Cameras

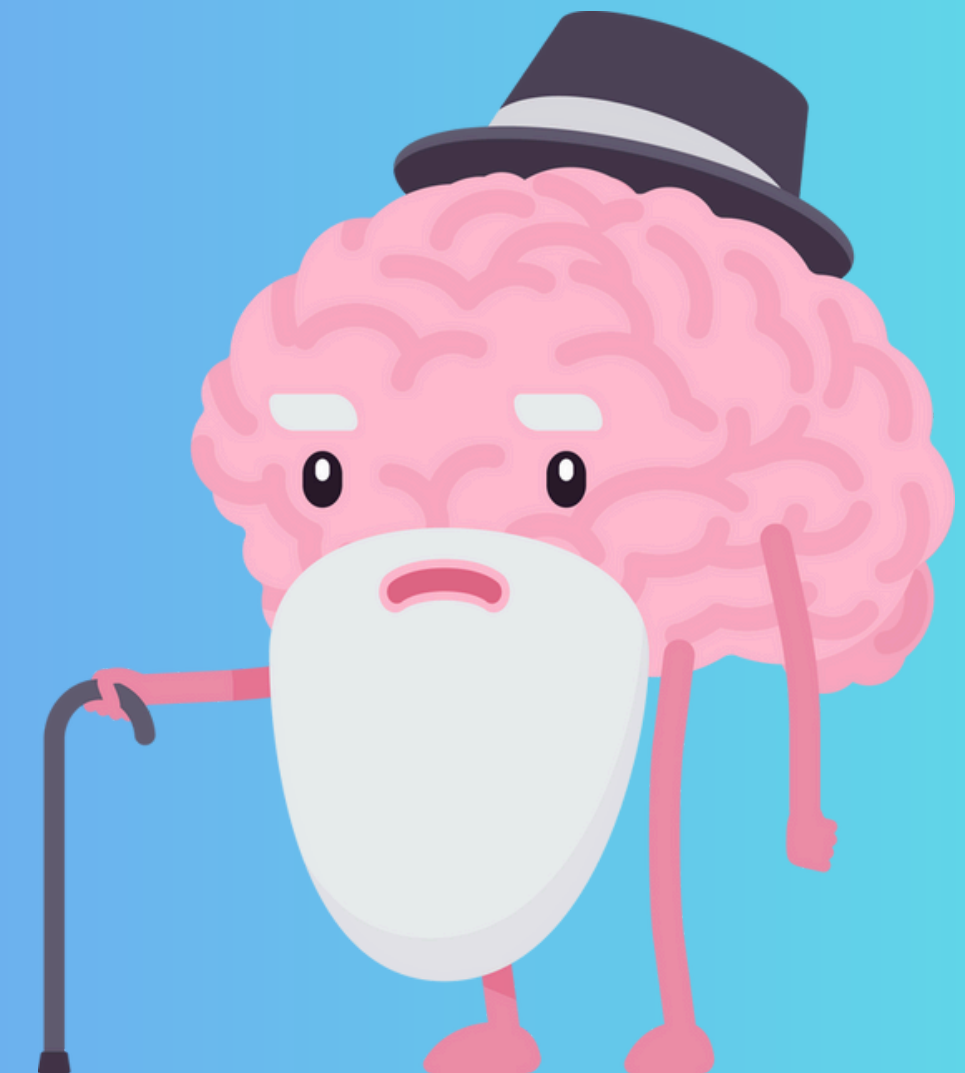
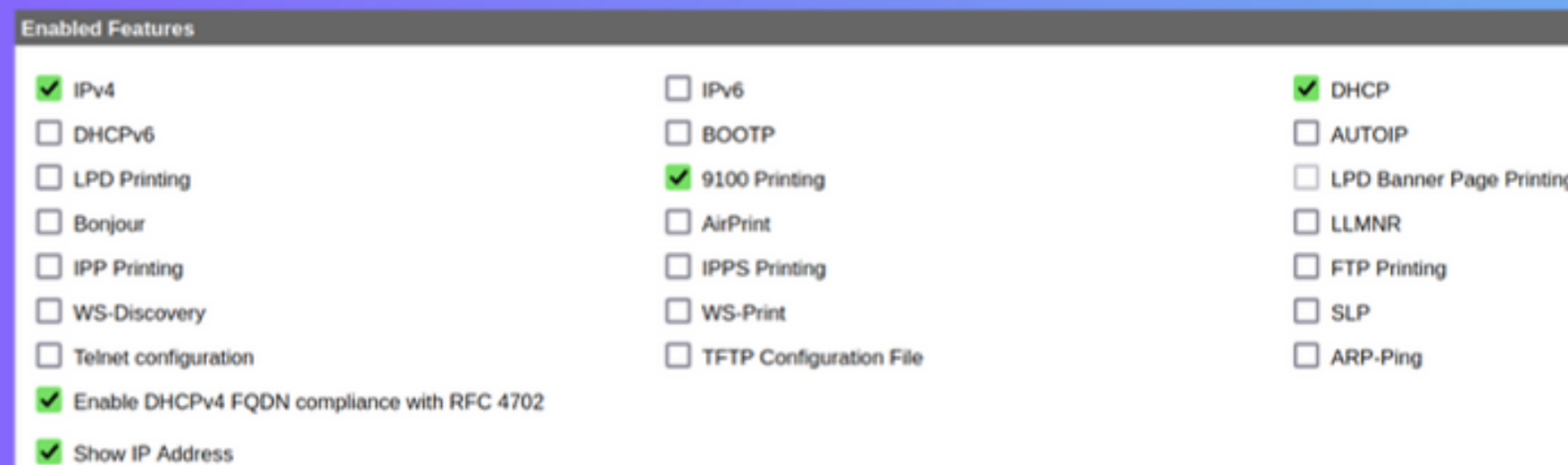


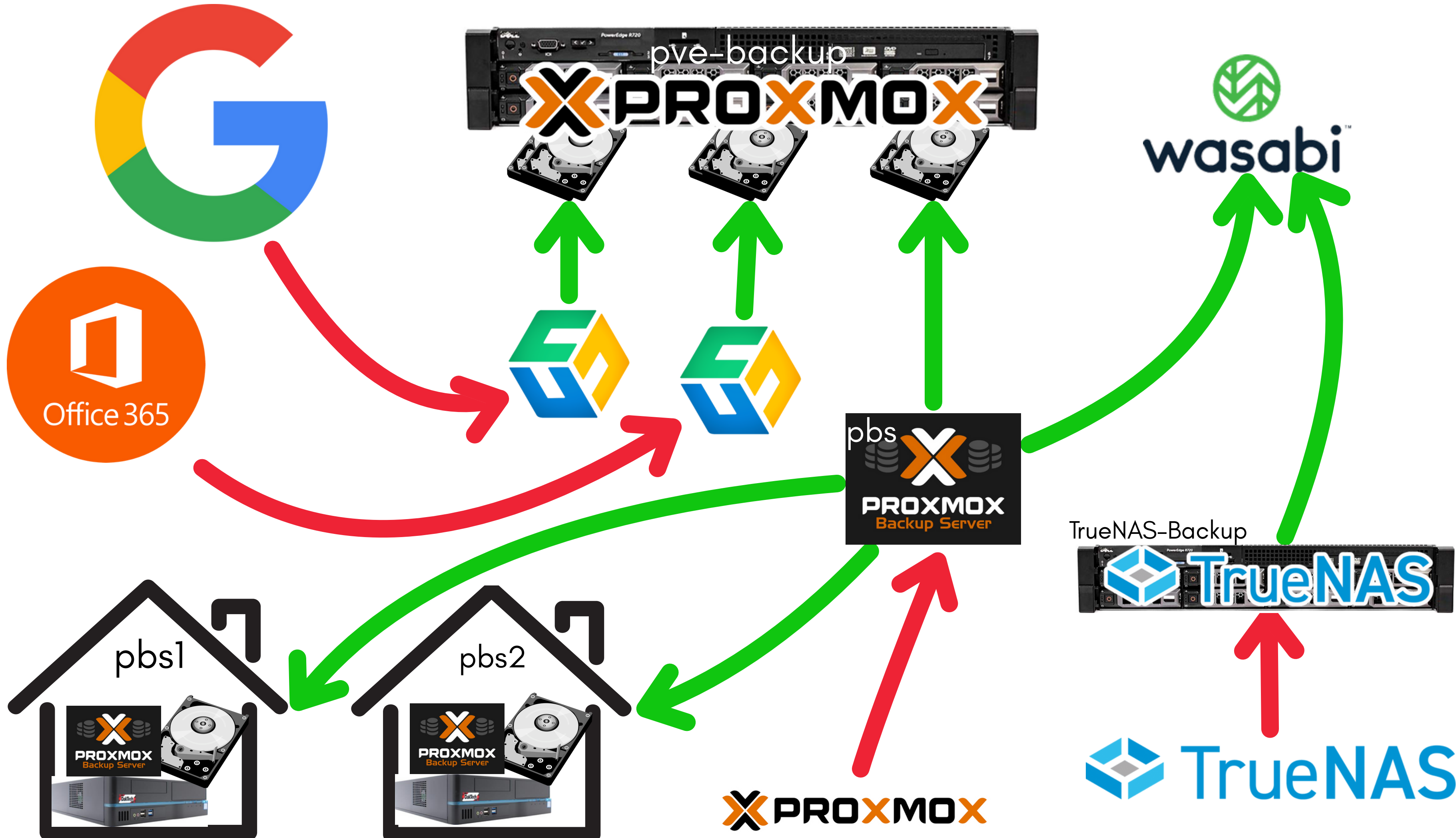
Also:

- Fail2Ban
- UFW (Uncomplicated Firewall)
- Zabbix/CheckMK Agent
- Key-Only SSH
- ZFS
- LUKS Encryption
- Unattended-Upgrades

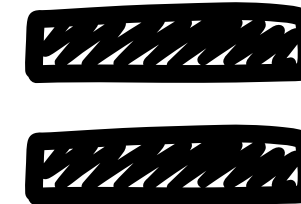
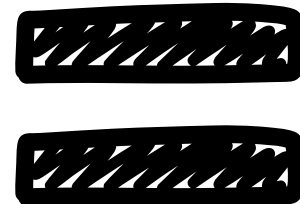
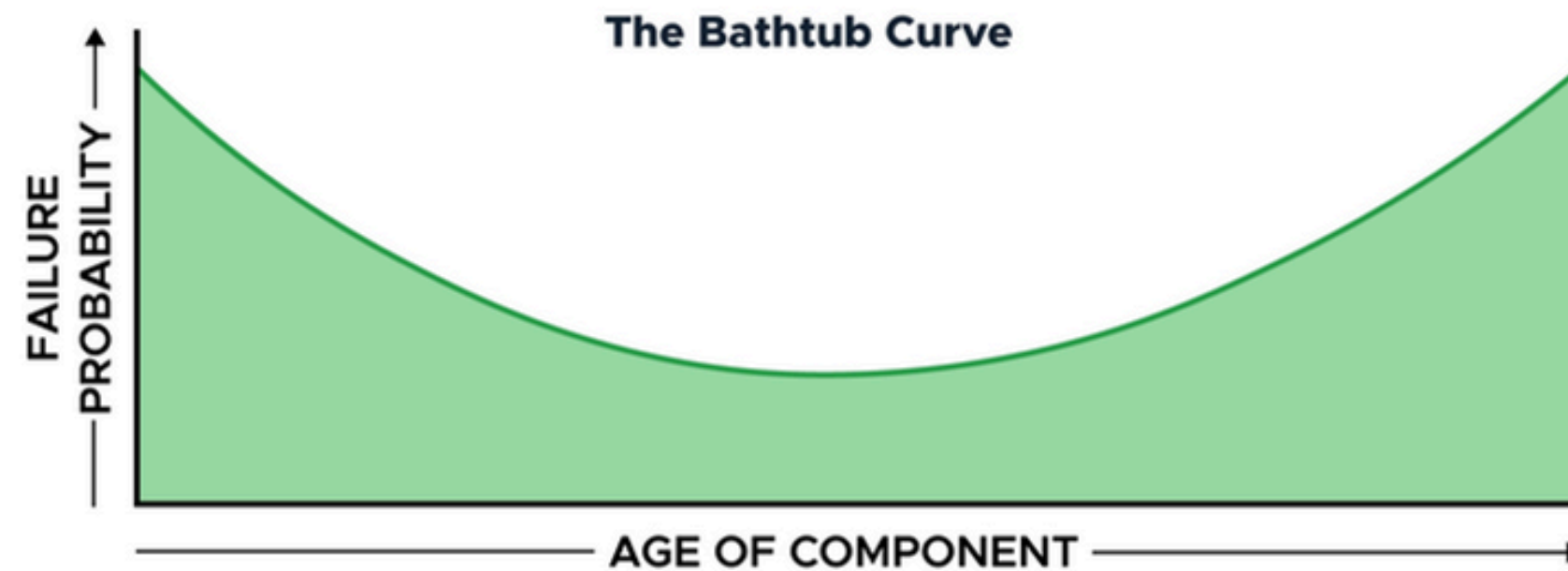
Old Hardware

- Upgrade Firmware
- Reset BIOS
- Set BIOS Passwords
- Assign RM to Dedicated NIC
- Disable RM
- Disable Unused Protocols
- Apply OS-Level Mitigations
- Disable Hyperthreading





Backups – Drives



\$0 • 1x Backup Server

\$1800 ○ 6x 20TB Drives (Refurb)

\$0 • 1x TrueNAS-Backup (Old R720)

\$180 ○ 8x 6TB Drives (Refurb)

\$0 • 2x PBS Backup Servers (Old Desktop)

\$1000 ○ 4x 20TB Drives (Refurb)

\$700 • CubeBackup Annual Subscription (Google)

\$700 • CubeBackup Annual Subscription (MS365)

\$3000 • Wasabi Fees

Fun? Stuff

Group Policy

1.

Default Domain Controllers Policy



Default Domain Policy

2.

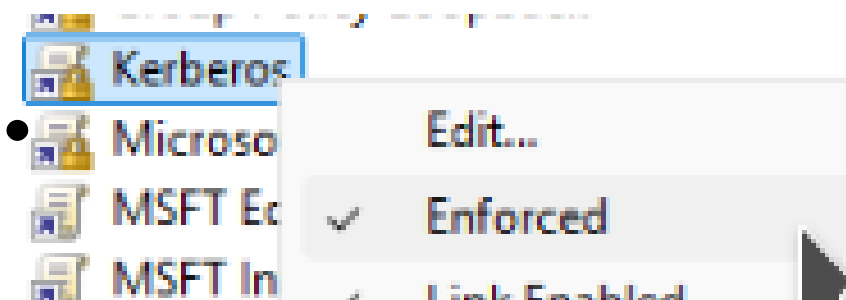
```
PowerShell 7 (x64)
PowerShell 7.5.3
PS C:\Users\[redacted] > dcgpofix /target:dc
```

```
PowerShell 7 (x64)
PowerShell 7.5.3
PS C:\Users\[redacted] > dcgpofix /target:Domain
```

3. Edit policy setting

Requirements:
Windows Server 2003 only

4.



5?

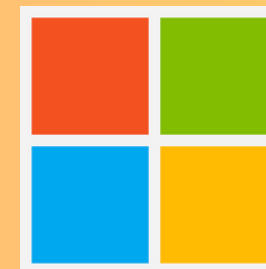
Group Policy Loopback

Computer Configuration (Enabled)	
Policies	
Administrative Templates	
Policy definitions (ADMX files) retrieved from the central store.	
System/Group Policy	
Policy	Setting
Configure user Group Policy loopback processing mode	Enabled
Mode:	

- Account Lockout Policy
- Accounts (Domain Controllers)
- Accounts (Pearson)
- Accounts (Servers)
- Accounts (Staging)
- Accounts (Workstations)
- Annoyances
- Auditing
- Autoenroll Certificates
- AzureAdConnect Fix (DCs)
- Bitlocker (Workstations)
- Chrome (All Users)
- Chrome (Generic)
- Chrome (Students)
- Chrome (Tech)
- Chrome (Workstations)
- Chrome Settings (Staff)
- Datetime Format
- Default Domain Controllers Policy
- Default Domain Policy
- Disable Firewall (Staging)
- Disable Remote UAC for PDQ (Workstations)
- Edge
- Firewall (Servers)
- Folder Redirection
- Group Policy Loopback
- Group Policy Processing (Workstations)
- Hibernation (Workstations)
- Kerberos
- LAPS (Workstations)
- M Drive (PHS111)
- M Drive (PHS506)
- Map V Drive (Staff)
- Microsoft Accounts (Disable)



Security Baselines



Microsoft Security Compliance Toolkit 1.0

This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.

Version:

1.0

File Name:

Windows 11 v23H2 Security Baseline.zip

Microsoft 365 Apps for Enterprise 2412.zip

Windows Server 2022 Security Baseline.zip

Windows 11 v24H2 Security Baseline.zip

Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip

Windows 10 Update Baseline.zip

SetObjectSecurity.zip

Windows Server 2025 Security Baseline - 2506.zip

Windows 10 Version 20H2 and Windows Server Version 20H2 Security Baseline.zip

LGPO.zip

Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip

Windows 11 version 22H2 Security Baseline.zip

PolicyAnalyzer.zip

Microsoft Edge v139 Security Baseline.zip

Windows 10 version 22H2 Security Baseline.zip

Windows 11 v25H2 Security Baseline.zip

Change the complete page content to that language.

Download



- MSFT Edge Version 128 - Computer
- MSFT Internet Explorer 11 - Computer
- MSFT Internet Explorer 11 - User
- MSFT Microsoft 365 Apps v2412 - Computer
- MSFT Microsoft 365 Apps v2412 - DDE Block - User
- MSFT Microsoft 365 Apps v2412 - Legacy File Block - User
- MSFT Microsoft 365 Apps v2412 - Legacy File Block - User (OVERRIDE)
- MSFT Microsoft 365 Apps v2412 - Legacy JScript Block - Computer
- MSFT Microsoft 365 Apps v2412 - Require Macro Signing - User
- MSFT Microsoft 365 Apps v2412 - User
- MSFT Windows 11 24H2 - BitLocker
- MSFT Windows 11 24H2 - Computer
- MSFT Windows 11 24H2 - Credential Guard
- MSFT Windows 11 24H2 - Defender Antivirus
- MSFT Windows 11 24H2 - Domain Security
- MSFT Windows 11 24H2 - User
- MSFT Windows Server 2022 - Defender Antivirus
- MSFT Windows Server 2022 - Domain Controller
- MSFT Windows Server 2022 - Domain Controller Virtualization Based Security
- MSFT Windows Server 2022 - Domain Security
- MSFT Windows Server 2022 - Member Server
- MSFT Windows Server 2022 - Member Server Credential Guard
- MSFT Windows Server 2025 v2506 - Defender Antivirus
- MSFT Windows Server 2025 v2506 - Domain Controller
- MSFT Windows Server 2025 v2506 - Domain Controller Virtualization Based Security
- MSFT Windows Server 2025 v2506 - Domain Security
- MSFT Windows Server 2025 v2506 - Member Server
- MSFT Windows Server 2025 v2506 - Member Server Credential Guard

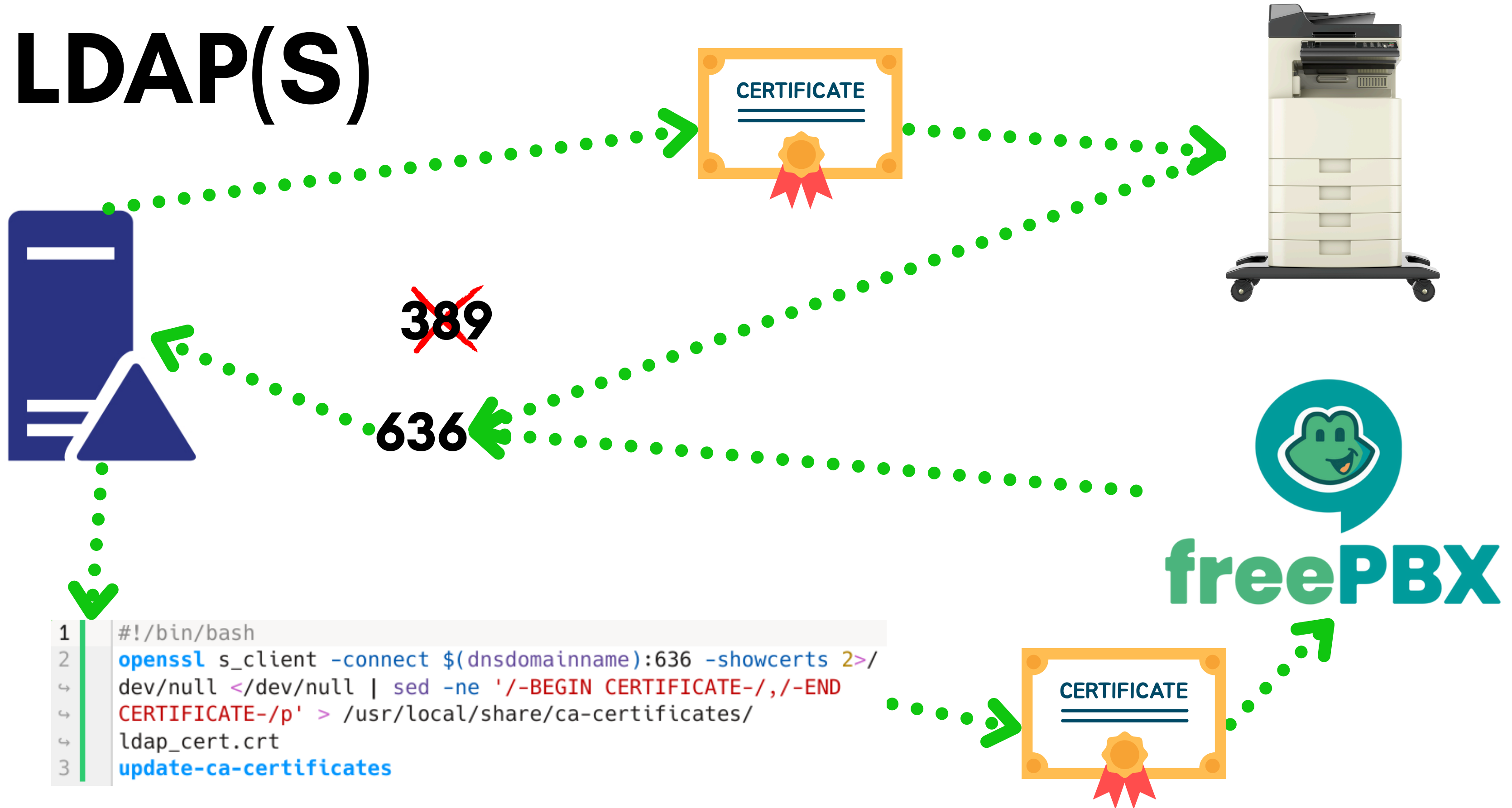
Kill Old Stuff

- **LLMNR**
- **mDNS**
- **WINS**
- **NetBIOS**
- **LLDP***
- **LM (LDAP)**
- **NTLM (LDAP)**
- **RC4 (Kerberos)**
- **SSL 3.0**
- **TLS 1.0**
- **TLS 1.1**

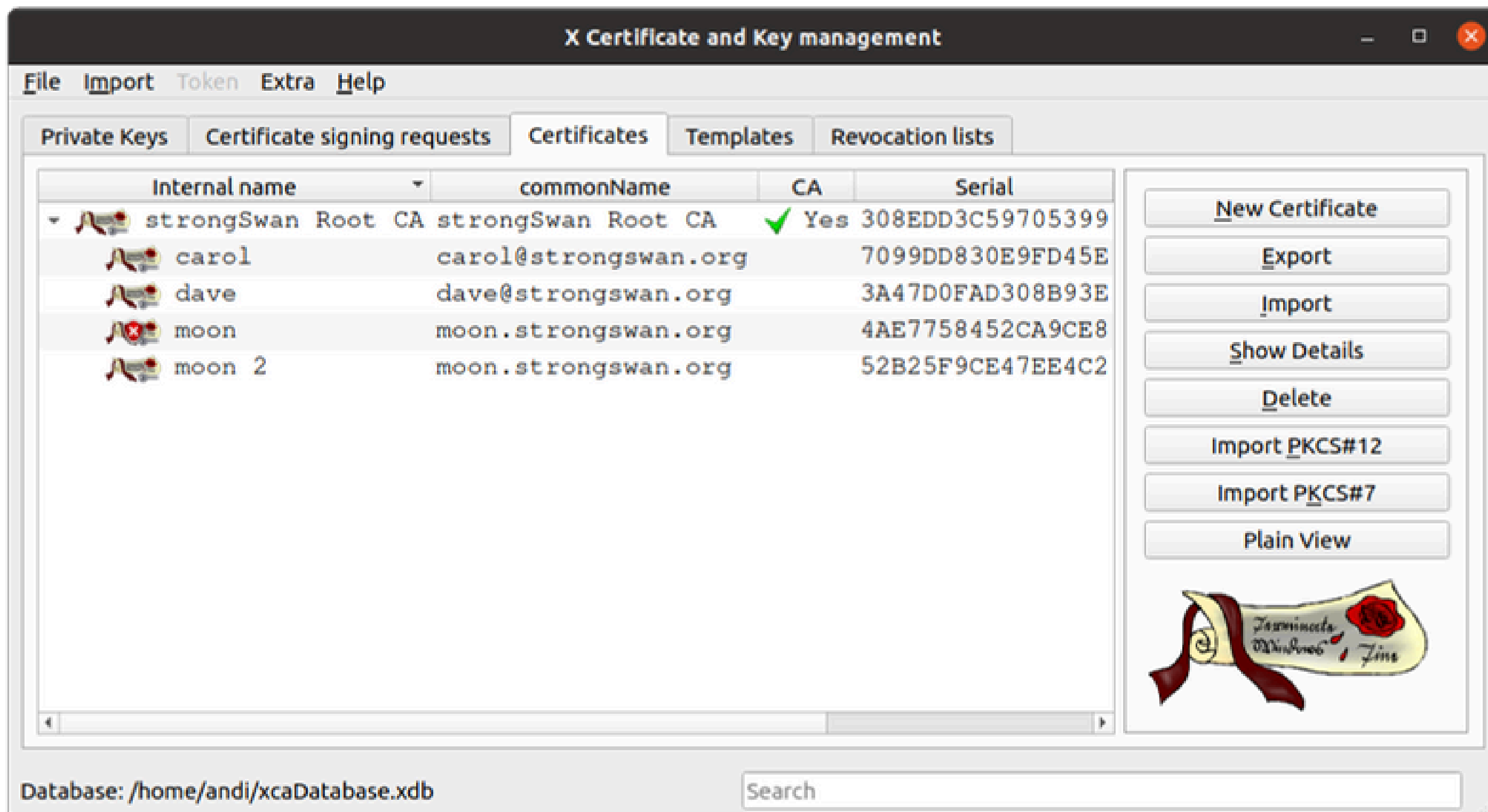
Encrypt Stuff

- **LDAPS Only**
- **HTTPS Only**
- **LDAP Signing**
- **LDAP Channel Binding**
- **SMB Signing**
- **SMB Encryption**
- **UNC Hardening**

LDAP(S)

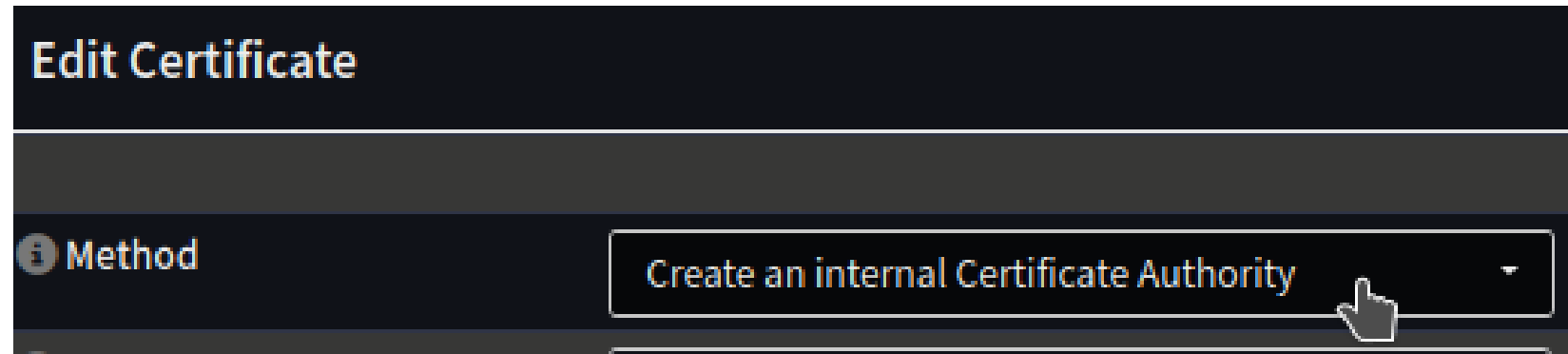


XCA

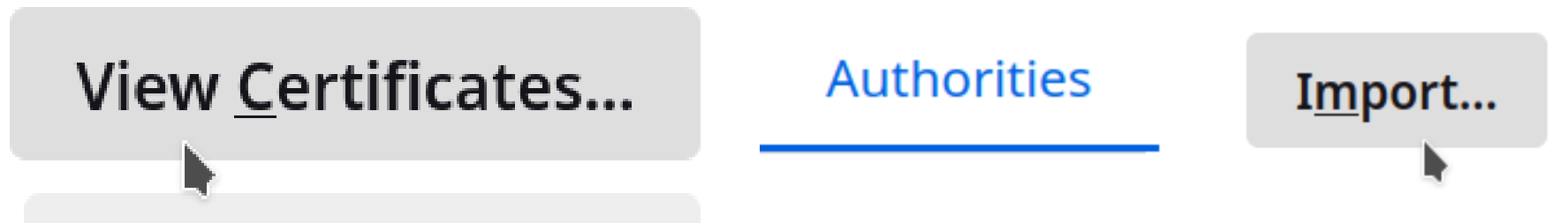


HTTP(S)

1.



2.



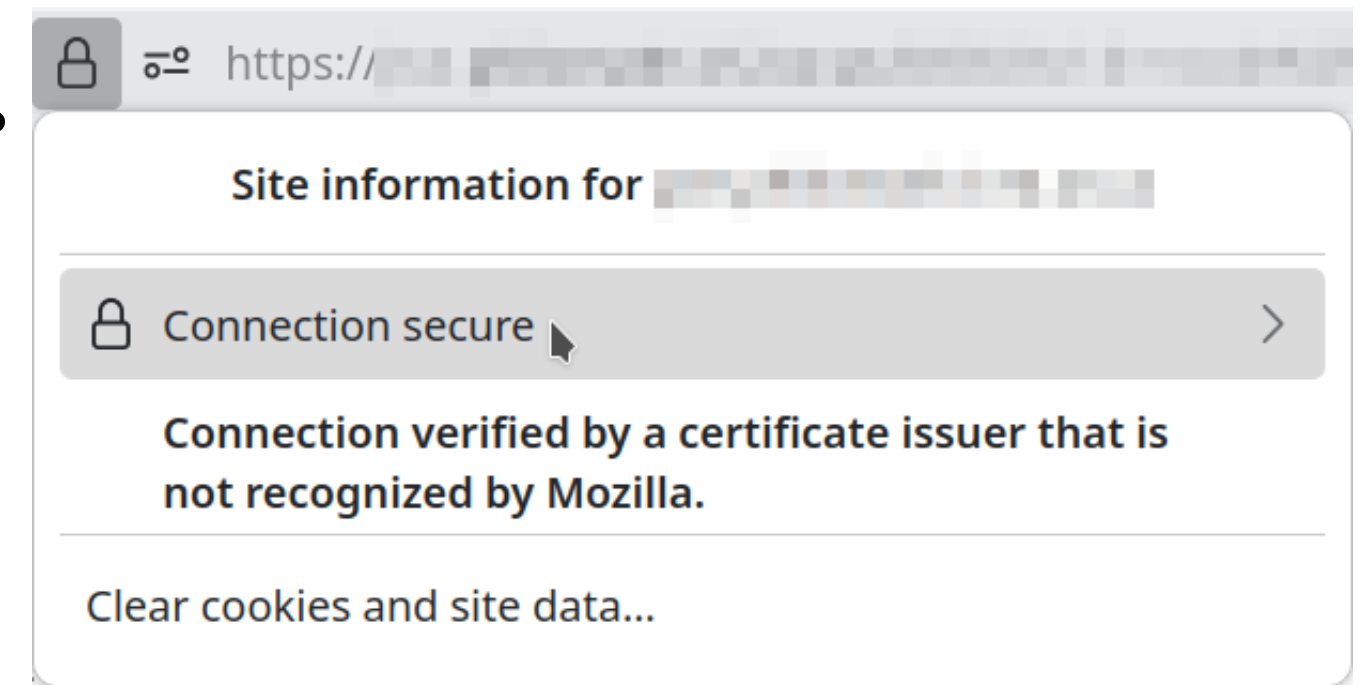
3.



4.



5.



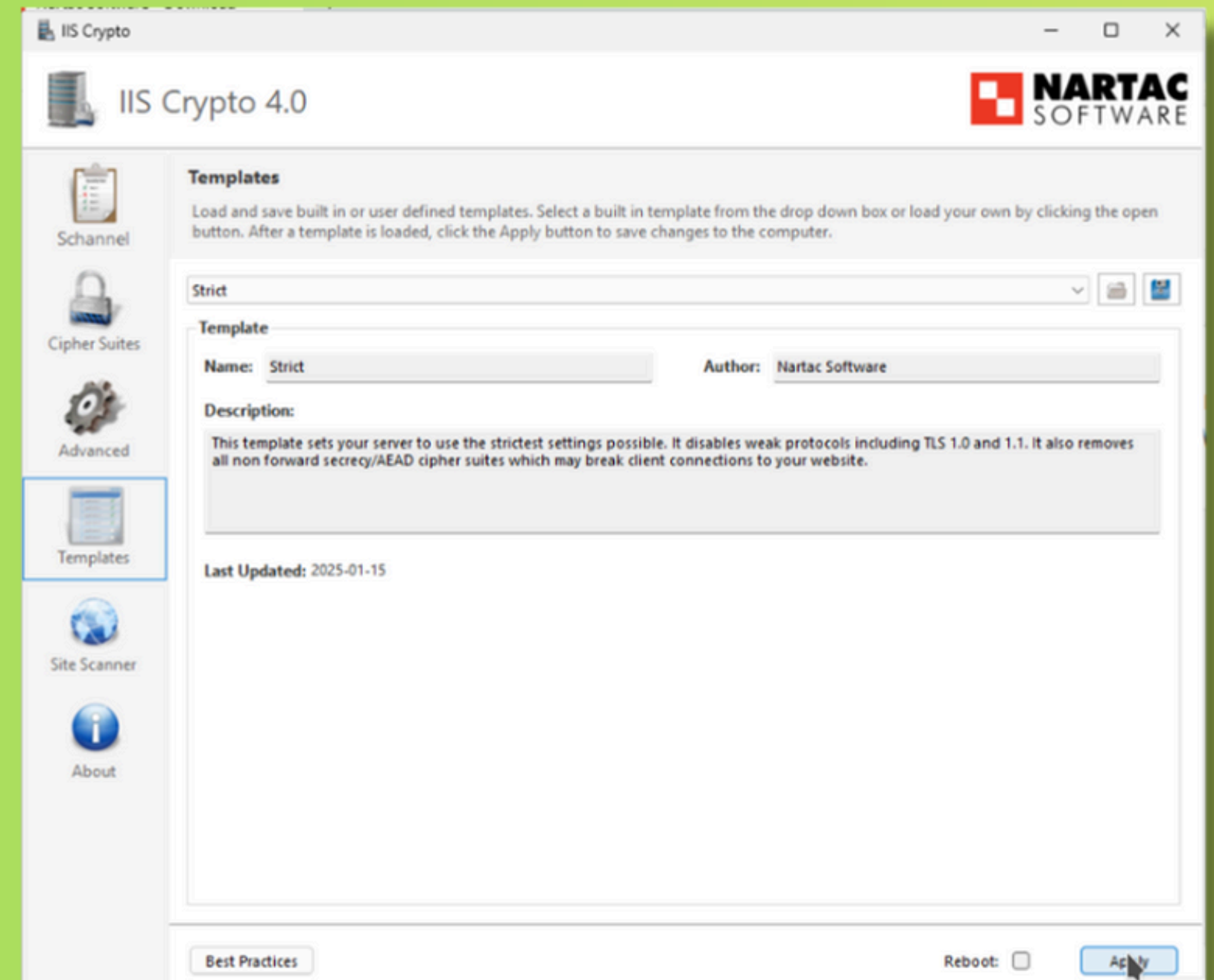
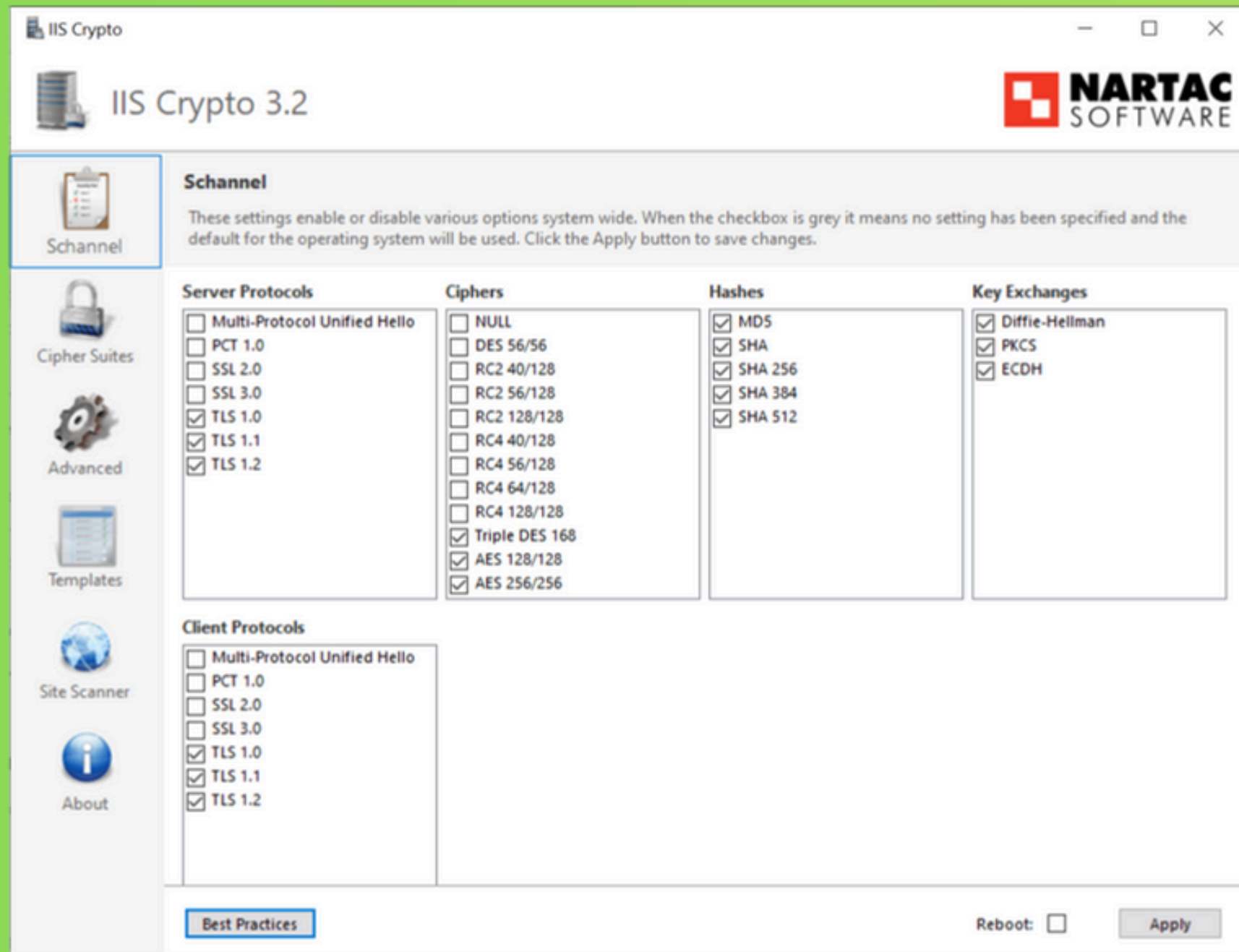
Your connection is not private

Attackers might be trying to steal your information from **truenas.philomath.k12.or** (for example, passwords, messages, or credit cards).

[Learn more about this warning](#)

NET::ERR_CERT_AUTHORITY_INVALID

IIS Crypto





purple knight

powered by  semperis

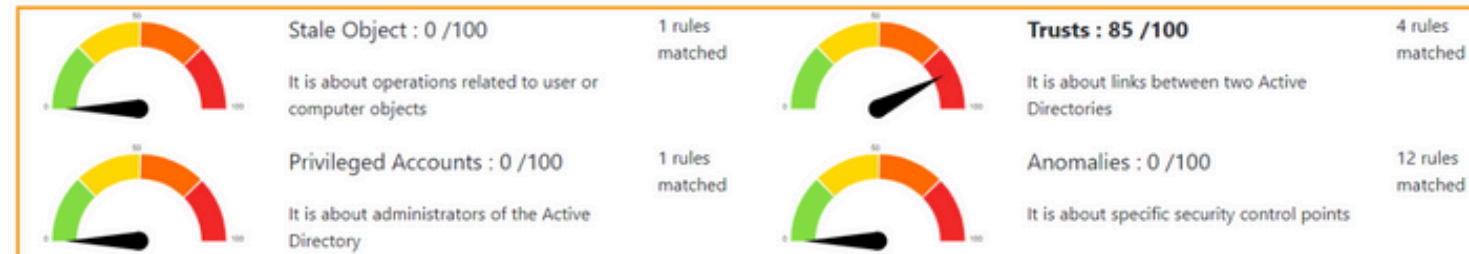
Active Directory Indicators

Indicators



Domain Risk Level: 85 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better



CA\PingCastle_2.5.1.0\ad_hc_ndsedv.de.html

ndsedv.de 2018-09-28

Risk model

Staled Objects	Privileged accounts	Trusts	Anomalies
inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			Temporary admins
			Weak password

Legend:
score is 0 - no risk identified but some improvements detected

SECURITY ASSESSMENT REPORT

Security Posture Overview

Indicators of Exposure

Indicators Failed to Run

AD Results

Account Security

AD Delegation

AD Infrastructure Security

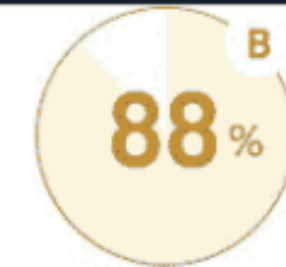
Group Policy Security

Kerberos Security

Appendix 1 – Domains list

Appendix 2 – Scoring Method

Appendix 3 – ANSSI Scorecard

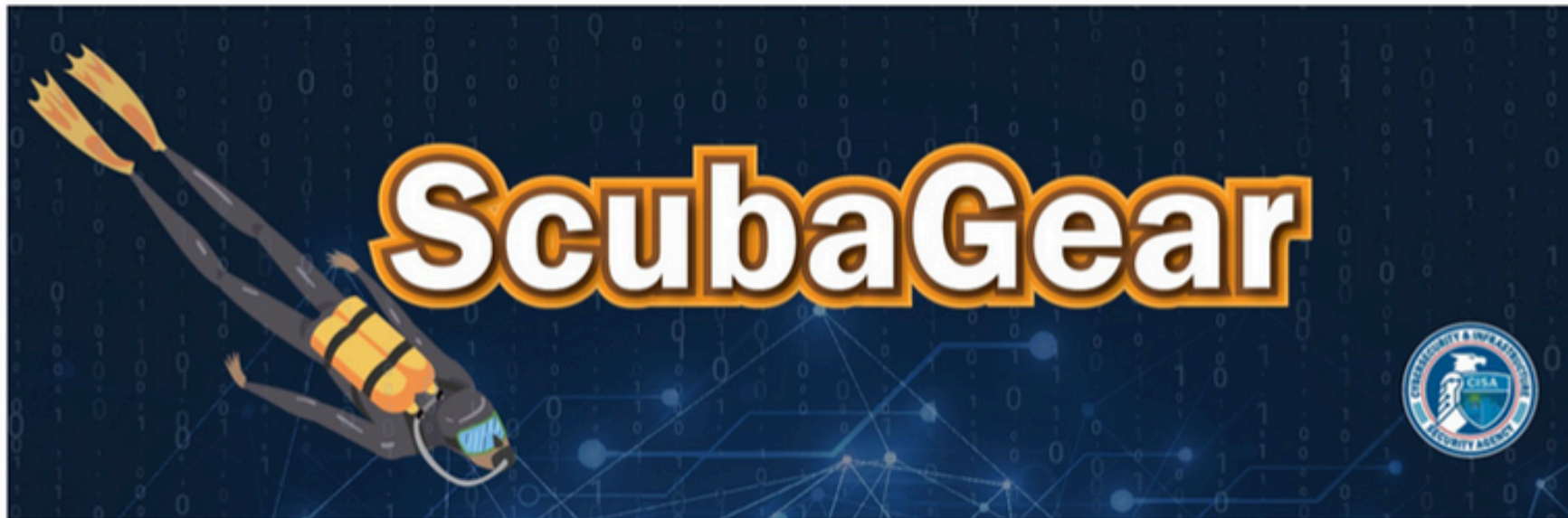


ACTIVE DIRECTORY

Forest	it-connect.local
No. of Domains	1
Duration	00:01:01
Run by	IT-CONNECT\Ad...

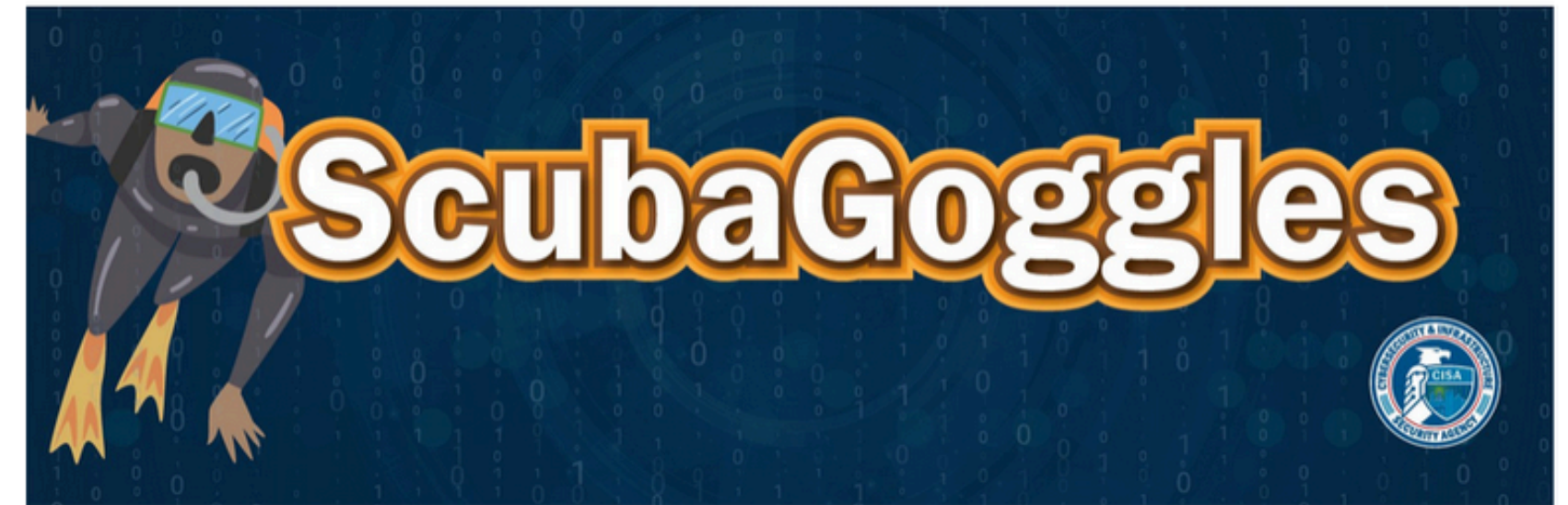
Indicators

Evaluated	97
Not selected	1
IOEs found	15
Passed	82
Failed to run	1
Not Relevant	0
Canceled	0



GitHub v1.6.0 PSGallery v1.6.0 CI Pipeline passing Functional Tests failing license CC0-1.0 downloads 14k
downloads 137k issues 185 open

ScubaGear is an assessment tool that verifies that a Microsoft 365 (M365) tenant's configuration conforms to the policies described in the Secure Cloud Business Applications ([SCuBA](#)) Secure Configuration Baseline [documents](#).



GitHub v0.5.0 PyPI v0.5.0 GitHub downloads 5.8k PyPI downloads 322/month license CC0-1.0

Developed by CISA, ScubaGoggles is an assessment tool that verifies a Google Workspace (GWS) organization's configuration conforms to the policies described in the Secure Cloud Business Applications ([SCuBA](#)) Secure Configuration Baseline [documents](#).

For the Microsoft 365 (M365) rendition of this tool, see [ScubaGear](#).

Automations

History

REAL-TIME REPORTS & ALERTS

Custom Reports

Built-in Reports

Scheduled Reports

Alerts

CONFIGURATION

Software Repository

Agent Deployment

Script Library

Advanced

Subscription

Organizations

Users & API Credentials

Roles New

Data Sources

Dashboard

a few seconds ago



Overview



134
Endpoints



422
Installed software



581
Vulnerabilities



224
Missing updates

Endpoint Summary



19
Last seen 31+ days ago



0
Last seen within 7 days



115
Last seen 8-30 days ago



14
Reboot required

Vulnerability Remediation Compliance



540
need attention

Overdue: 538

Due soon: 2

Service-Level Agreement:

Critical in 7 day(s)

High in 15 day(s)

Medium in 30 day(s)

Low in 60 day(s)

Vulnerability Remediation Deadlines

	Overdue	1-7 days	8-30 days	31+ days
Critical	16	0	0	0
High	355	1	6	0
Medium	151	1	29	0
Low	16	0	0	0

Update Deployment Compliance



170
need attention

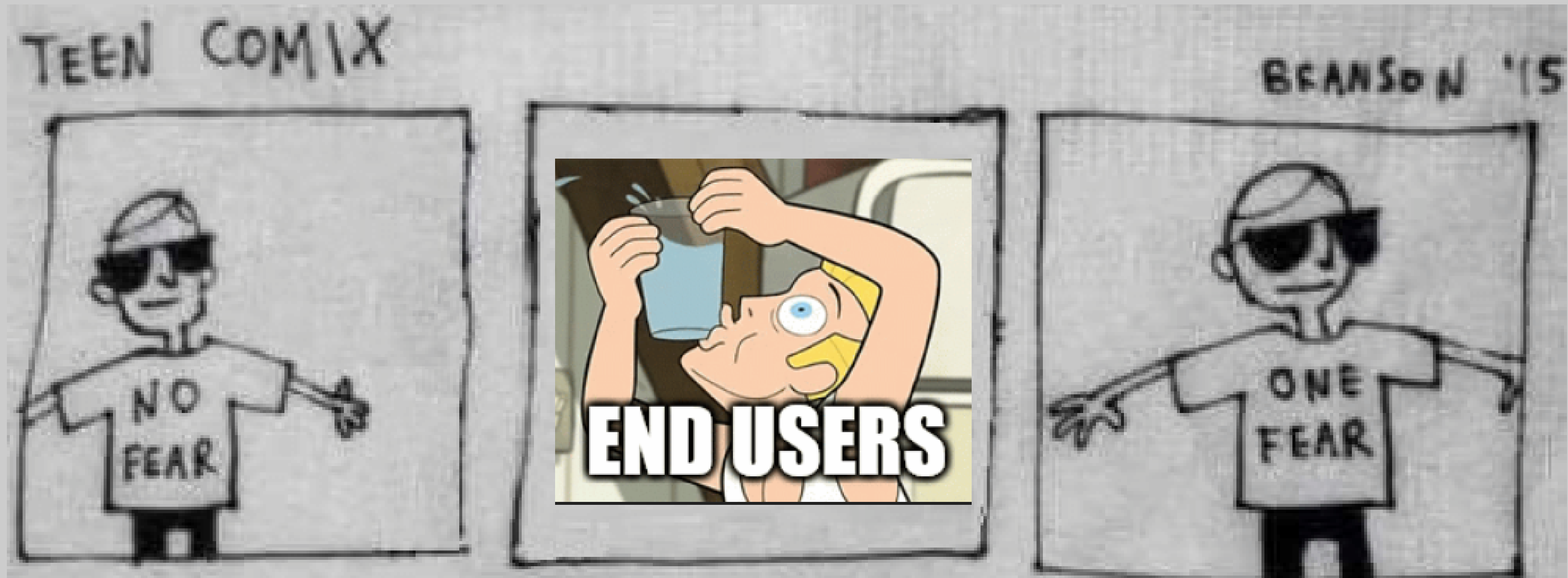
Service-Level Agreement:

Critical in 7 day(s)

Update Deployment Deadlines

	Overdue	1-7 days	8-30 days	31+ days
Critical	11	0	0	0

People...





C.I.A.

- Confidentiality
 - Info -> wrong place
- Integrity
 - Thing "works", but lies
- Availability
 - Thing broke



- Identification, Authentication, Authorization
 - Principle of Least-Privilege
- Redundancy
- Backups
- Encryption
- Network Segmentation
- Disaster Recovery Plans

People

- External (Null)
 - Delegated (Third-Party)
- Internal (Access)
- Admin (Access + Privilege)

People Problems

- Clueless
- Lone Wolves
- Fat Finger
- Eager Beavers
- Actual bad guys

Trust

Legend:

 No Trust Violation

 Questionable

 Trust Violation

Internal (Staff)

 Clueless

 Lone Wolves

 Fat Finger

 Eager Beavers

 Actual bad guys

Admin (IT)

 Clueless

 Lone Wolves

 Fat Finger

 Eager Beavers

 Actual bad guys

*External (Public)

 Clueless

 Lone Wolves

 Fat Finger

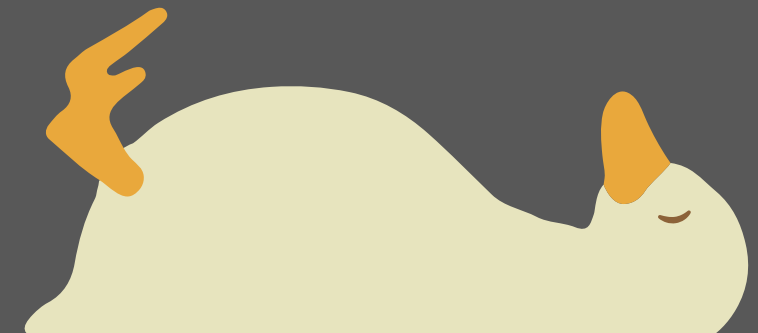
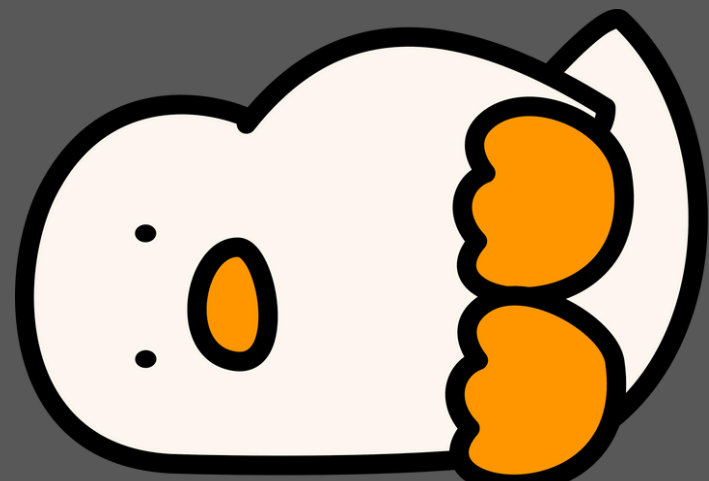
 Eager Beavers


 Actual bad guys

How can I fuck it up?



1. No foul allowed ever.
2. No harm, no foul.
3. Much harm, much foul.
4. LARPing





Good = Easy



Dashboard

Overviews

Knowledge Base

My Stats

First Steps

Activity Stream

WAITING TIME TODAY

0

My handling time: 0 minut
Average: 11 minutes

MOOD

CHANNEL DISTRIBUTION

ASSIGNED

Tickets assigned to me: 11 of
Average: 0.8

New Ticket

TITLE *
Can't log in to Destiny

TEXT
I can't log in to Destiny and my pants are on fire.
select attachment...

WHAT BUILDING ARE YOU IN? (OPTIONAL)
Technology Office

WHAT ROOM ARE YOU IN? (OPTIONAL)
Room #999

WHEN ARE YOU AVAILABLE? *
Any time today

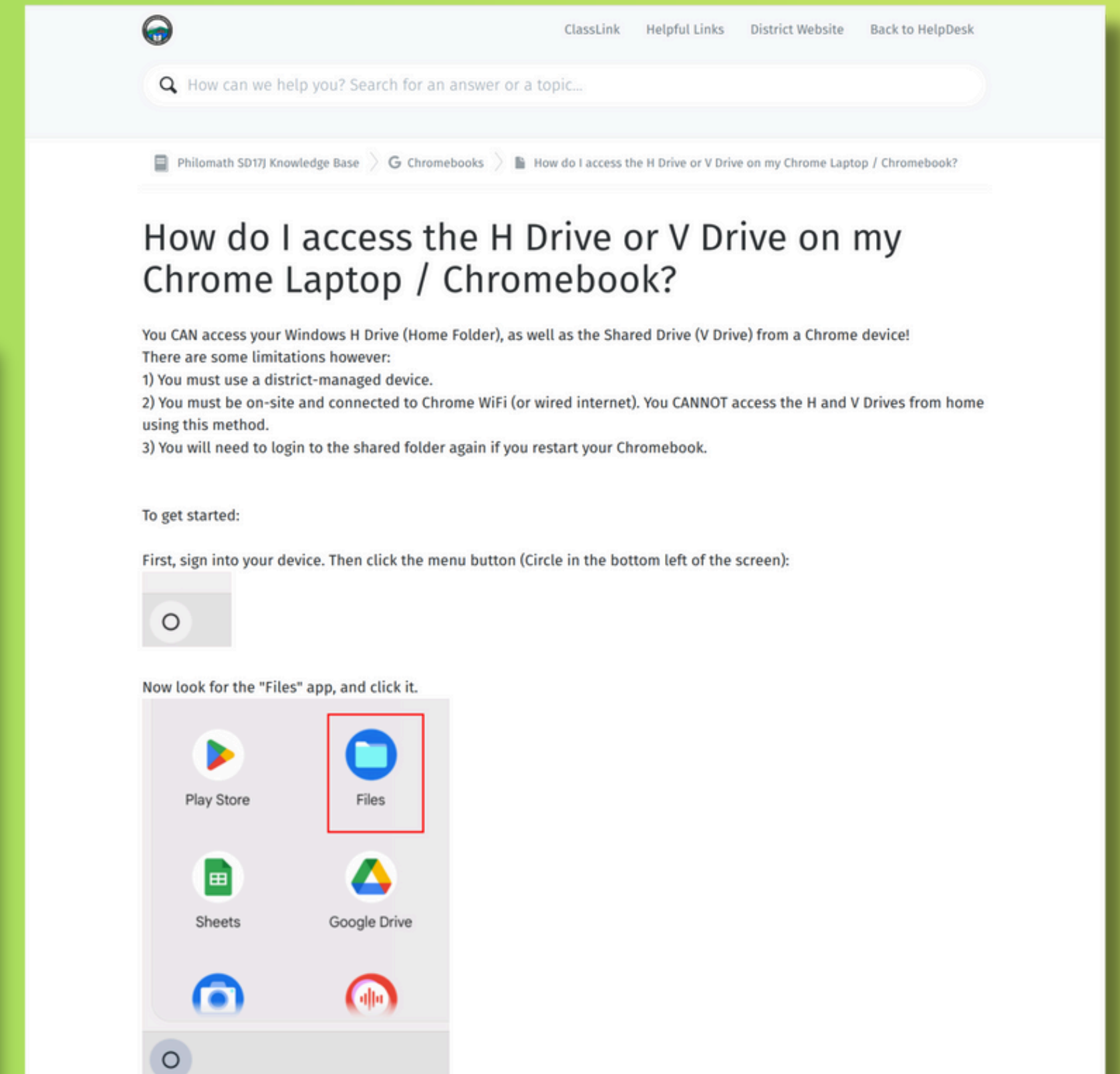
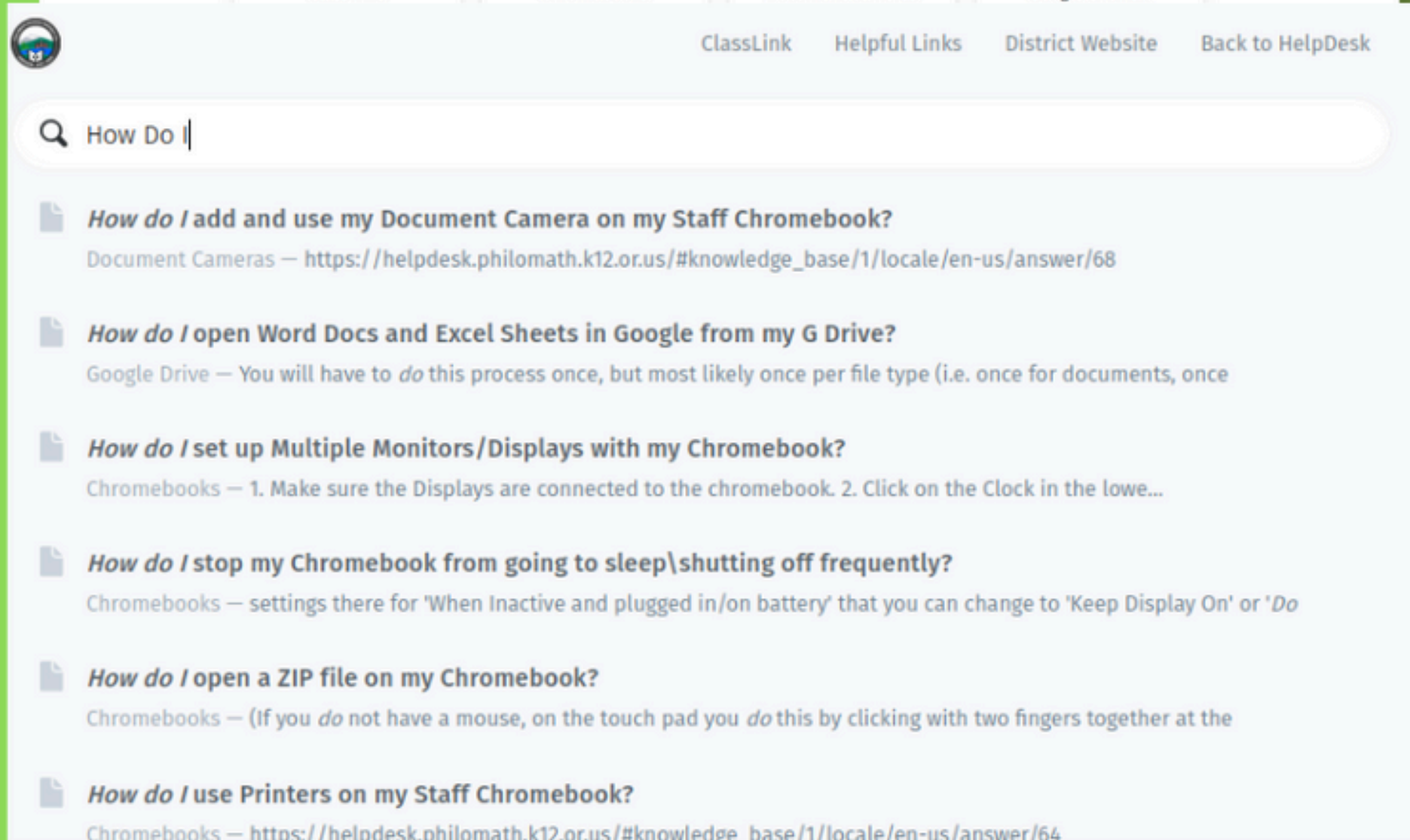
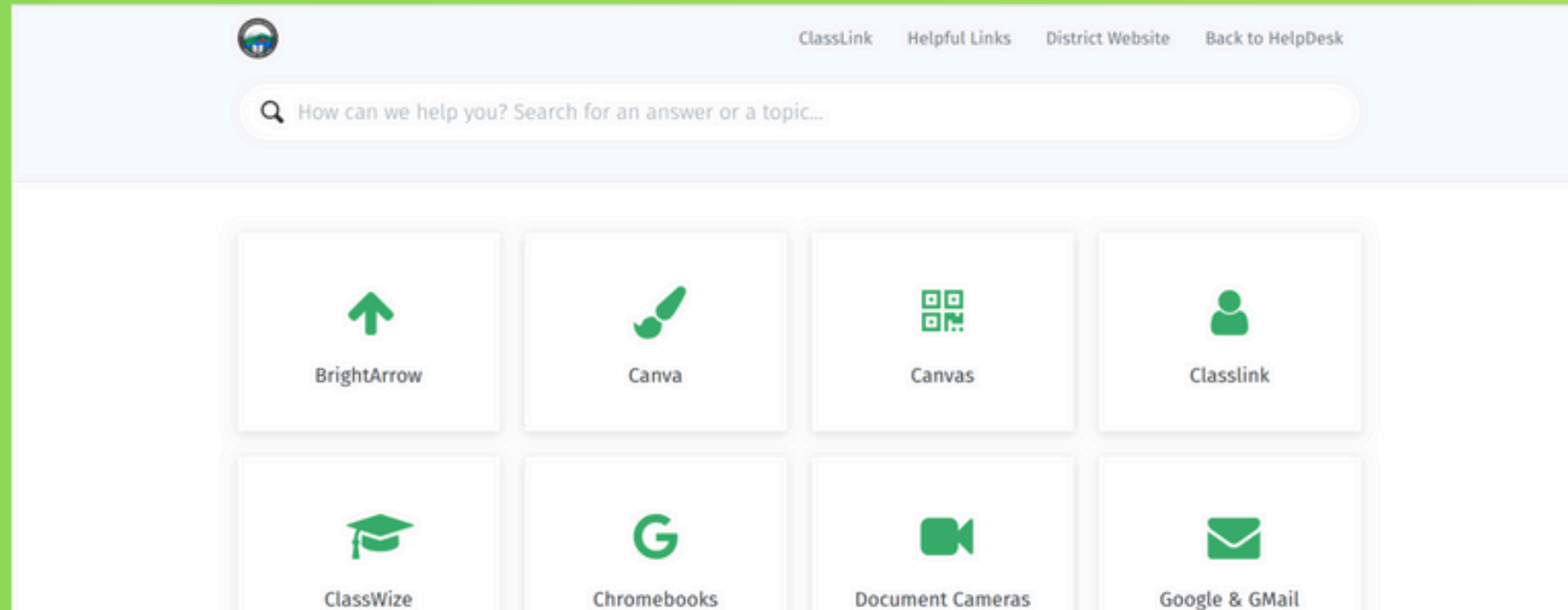
CATEGORY *
Technology

WHAT'S THE PROBLEM? *
Can't log in.

WHICH APP/WEBSITE? *
Destiny

Cancel & Go Back

Create



My Recent Drafts

New Page

My Most Viewed Favourites

New Debian Server - First Steps

During Install: Use All Files in One Partition formatting option. Generate a super long root ...

[View All](#)

My Recently Viewed

Security 0 Completed Projects

Archive

Security - AD

Technology

New Debian Server - First Steps

Shelves



Anthias

Headwind

VMWare

Zoom

Impero



Activate Learning (Ed.Link)

Amplify Learning

Boardmaker

Classlink

Archive

Technology

Sort

Name



Actions

New Shelf



Back

Editing Page 1

Set Changelog

Save Page

Verify Account Info is Correct

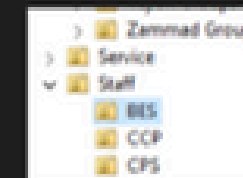


Paragraph



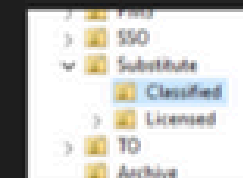
Open Active Directory Users and Computers on a Domain controller. There are only a few fields that must be correct.

First, verify the user in question is in the correct OU:



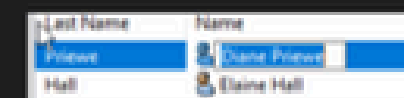
OU is used to populate the "Department" field & "Description" field. Department field is used to determine group membership.

just because someone is a sub for a school, does not mean they should be in the OU for that school! Substitutes need to be placed in either the Classified or Licensed OU under the Substitute OU. This does NOT mean they are union members, it just means they substitute either for classified staff or licensed staff.

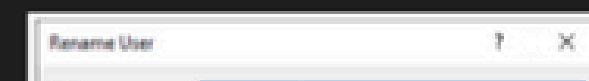


AD stores the name in like 15 different fields. To properly Rename a user or verify name is correct, always do the following:

In Active Directory, Right-Click the user and choose "Rename".



After you type the new name and hit enter, this will appear.



Stuff you 100% have to pay for



- Antivirus



- Web Filter



Label Things



The image shows a grey and black DYMO LetraTag handheld label maker. To its left is a red and yellow 'BONUS!' sticker that says '3 LABELS INCLUDED ETIQUETTES INCLUSES' and 'PERSONALIZE & ORGANIZE PERSONNALISER & ORGANISER PERSONALISIEREN & ORGANISIEREN PERSONALISEREN & ORGANISIEREN'. Below the sticker are three rolls of DYMO tape. To the left of the sticker is a vertical strip of icons and text: '3 VIDEOS'.

DYMO Label Maker Machine with Tape - 100H LetraTag Handheld, Comes with 3 LT label tapes. Great for Home & Office Organization

[Visit the DYMO Store](#)

4.6 ★★★★★ (44,051) | [Search or ask](#)

Amazon's Choice

3K+ bought in past month

Limited time deal

-32% \$33.82

List Price: \$49.99

FREE Returns

Available at a lower price from [other sellers](#) that may not offer free Prime shipping.

Style: **Machine + 3 Tapes**

Machine + 3 Tapes	Pink Machine + ...	Machine + 2 Tapes
\$33.82 \$49.99	\$25.29 \$29.99	\$24.99 \$44.99

Brand: DYMO

S2Score	Last Snapshot	New Snapshot
Overall Score	596	774 (+178)
Administrative	<div> <div>S2SCORE® Scale</div> <div> The S2SCORE® is calculated in a range from 300 to 850. The lower the score, the higher the risk, and vice versa. </div> <div> </div> <div> The applicable ranges for a S2SCORE® are: <div> <div>Excellent: 780.00 – 850.00</div> <div>Poor: 500.00 – 599.99</div> <div>Good: 660.00 – 779.00</div> <div>Very Poor: 300.00 – 499.99</div> <div>Fair: 600.00 – 659.99</div> </div> </div> </div>	
Physical		
Internal Technical		
External Technical		
New scan (Y/N)	-	No
Number of response changes	-	67

Thank you