EPASS
SOFTWARE

User Conference 2024

System Migrations
&
IT Security

System Migrations

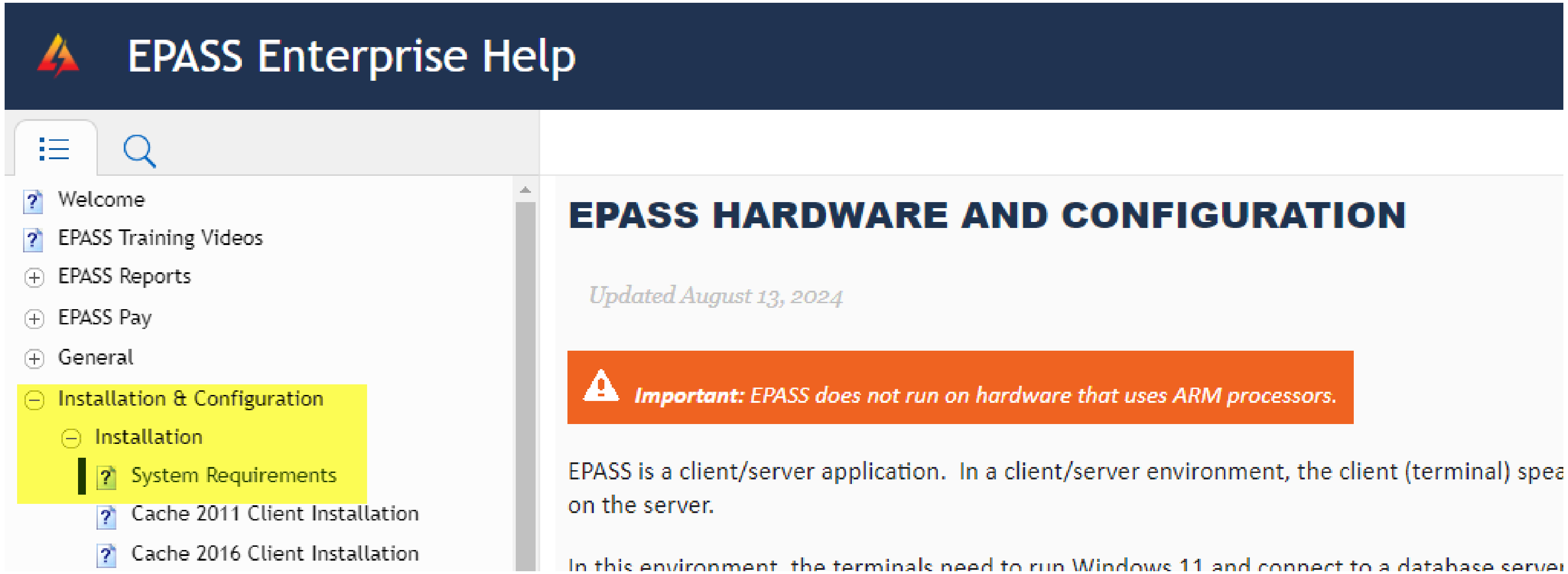
Why this topic?

- Something all EPASS users will encounter eventually
  - Microsoft depreciates their operating systems every 7-10 years
- Migrations must be carefully planned, tested, and executed
- Clarify scope of the project and tasks / responsibilities involved – it’s a team effort

System Requirements

The latest requirements are always available at:

help.epass.software



EPASS HARDWARE AND CONFIGURATION

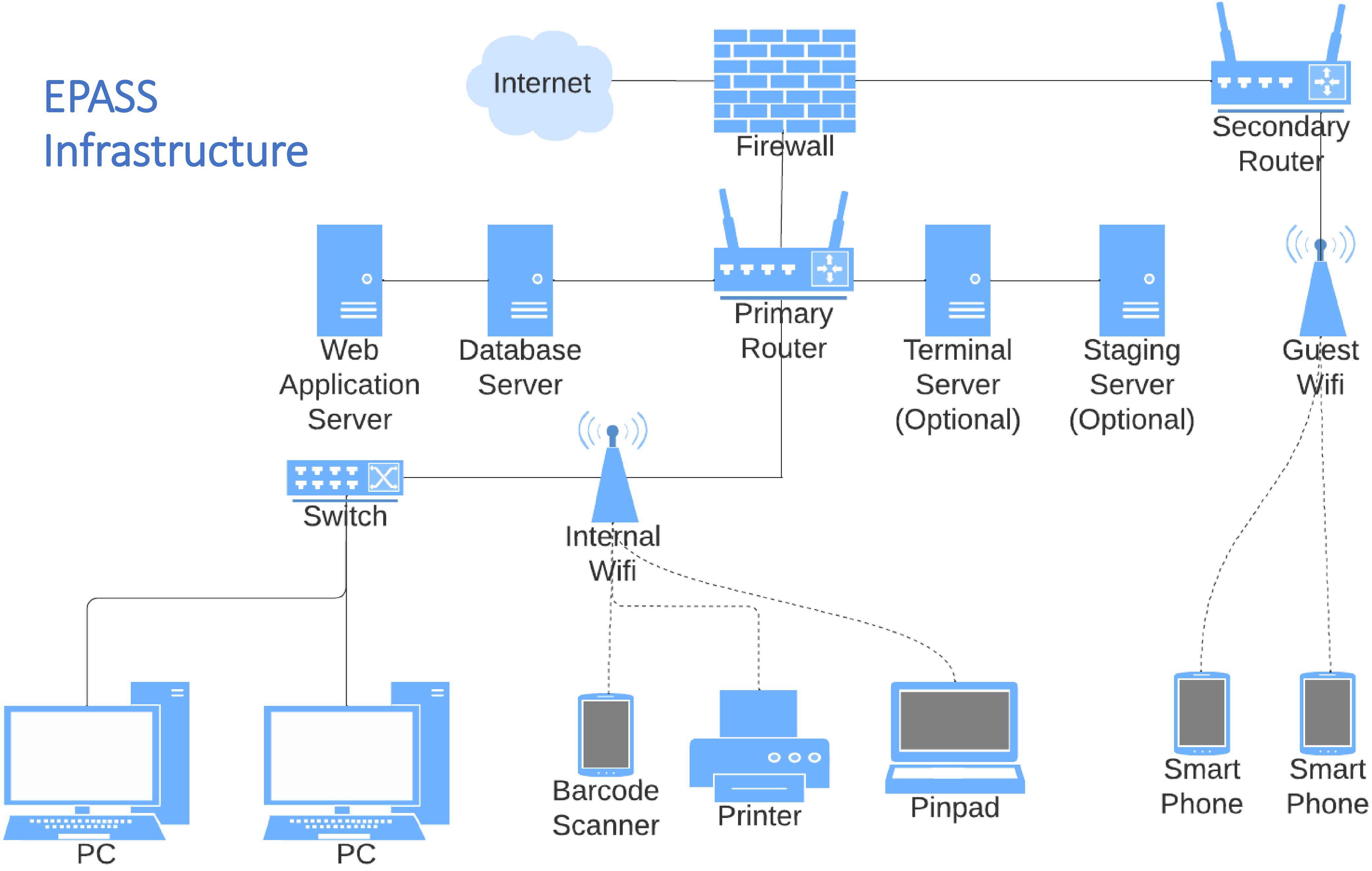
Updated August 13, 2024

⚠ ***Important:** EPASS does not run on hardware that uses ARM processors.*

EPASS is a client/server application. In a client/server environment, the client (terminal) spea on the server.

In this environment, the terminals need to run Windows 11 and connect to a database server

EPASS Infrastructure



Specs for 20 Users

Database Server

- Xeon E5/i7+ processor with minimum of 8 cores
- MS Windows Server 2016/2019/2022 64-bit
- 32GB RAM available to EPASS; 64GB recommended
- 1TB of hard disk space available for EPASS
- MS Excel must be installed

Specs for 20 Users

Web Application Server

- Xeon E5/i7+ processor with minimum of 4 cores; 8 cores is recommended
- MS Windows Server 2016/2019/2022 64-bit
- 16GB RAM available to EPASS; 32GB recommended
- 100GB of hard disk space available for EPASS applications
- Internet Information Services (IIS)

Specs for 20 Users

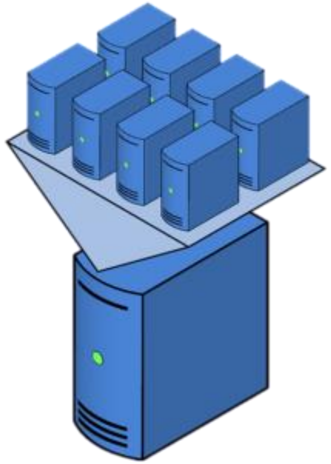
Terminal Servers (Optional)

- Requirements are dependent upon:
  - How many users?
  - Are the users running other apps aside from EPASS?
  - Are the users logged into EPASS in a desktop environment or a remote app?
  - Heavy or light EPASS usage?
- In general, budget 1 CPU core per user & 2-4 to run the OS
- MS Windows Server 2016/2019/2022 64-bit
- Minimum of 32GB RAM
- Must support IP Virtualization

Virtual Servers

Advantages:

- Scalability & Performance
- Reduce hardware costs
- Improved disaster recovery
- Increased uptime
- Instant provisioning
- Save physical space
- Cloud-ready
- Security
- Energy savings



Cloud Hosted Servers

Considerations:

- Reduce up-front hardware costs vs subscription model
- Reduce administrative burden
- No risk to on-site systems
- Latency compared to a local network

Migration Planning

Essential steps in a **Migration Plan**:

1. Hardware & Software Inventory

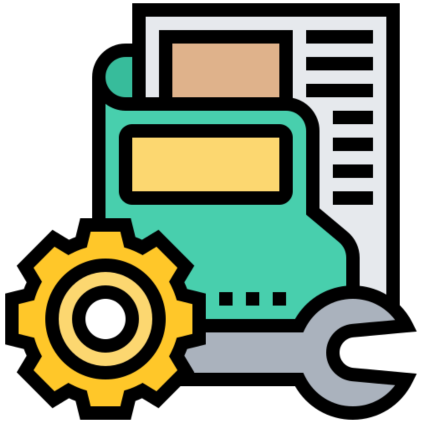
   - Document all hardware and software on the old server, including integrations and non-EPASS systems

   - Ensure that the new hardware meets your requirements, and your network infrastructure is ready to support the new server

Migration Planning

2. Configuration

- Server setup by EPASS Support
- Server name planning
- Prepare for testing



Migration Planning

3. Testing

- Set up key individuals with access to the server so they can test their job actions & devices (printers, scanners, etc)

- Verify scheduled tasks are running

- If there are any changes for users, provide training and documentation

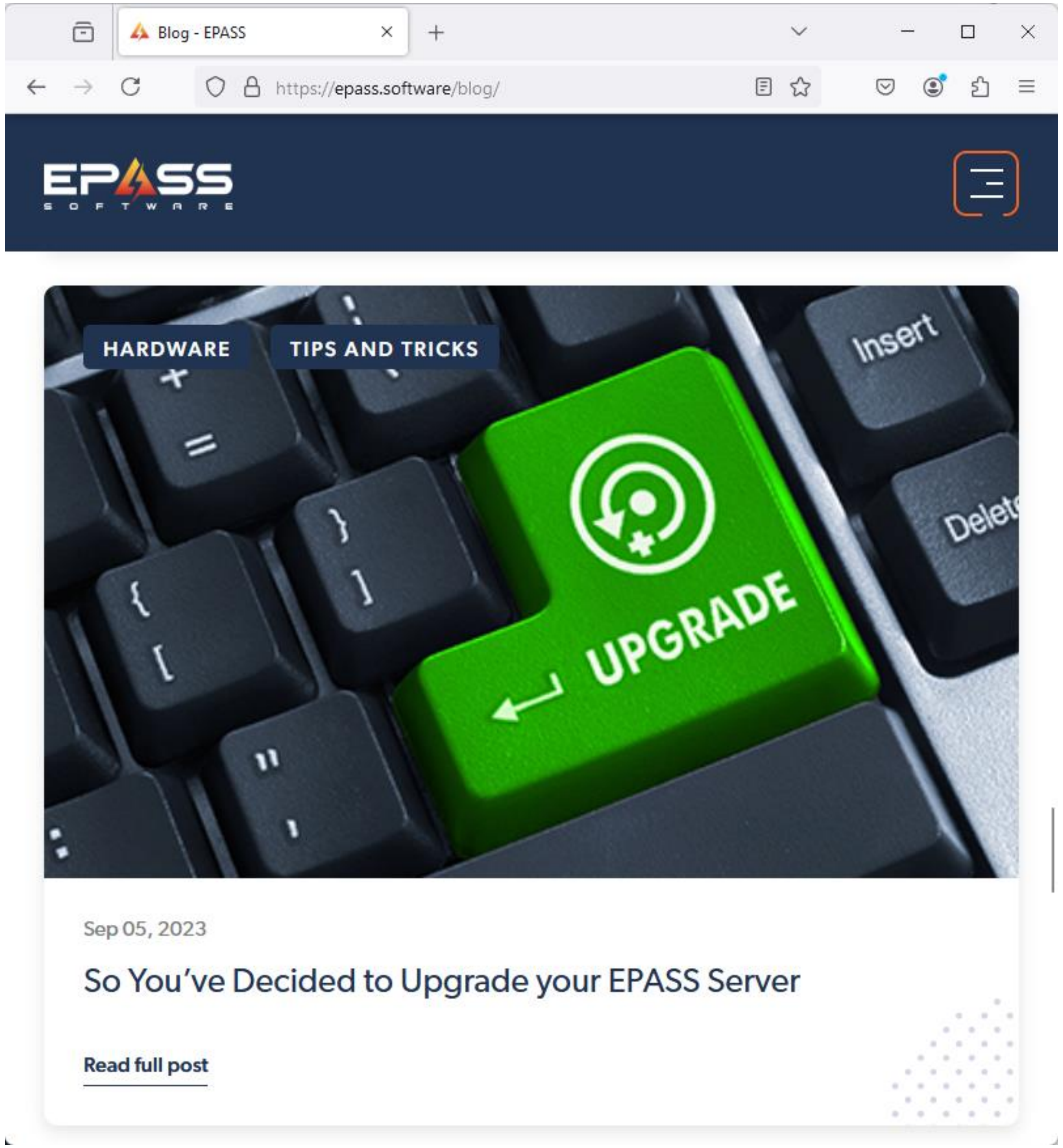
Migration Planning

4. Going live

- The database cut-over must be performed by EPASS Support and should be scheduled with 2 weeks’ notice
- Determine the best time to perform the switch-over to the new server to minimize disruption to your operations and communicate the plan to your team
- Have a rollback plan

Next Steps

See post on **epass.software/blog**: *So You’ve Decided to Upgrade Your EPASS Server*



Sep 05, 2023

So You’ve Decided to Upgrade your EPASS Server

Read full post

Moving Along…

Next topic is: **IT Security**

IT Security

What are the risks?

- **Financial loss**
- **Downtime**
- **Operational disruptions**
- **Data theft**
- **Damage to reputation**

IT Security

What are the threats?

Malware

- Can effect system performance
- May steal, delete, or encrypt your data
- Your email or website may become compromised
- Opens back doors for more serious threats

IT Security

What are the threats?

Ransomware

- Attacker will encrypt your system and demand that you pay a ransom to unlock it
- Your system is down until the ransom is paid or you rebuild it from a backup
- Be prepared to pay if you do not have off-site backups
- System will need to be rebuilt to eliminate the back door

IT Security

What are the threats?

Social Engineering / Phishing

- Scammers will attempt to deceive your team into revealing sensitive information, installing malware, or transferring funds
- Can range from emails enticing recipients to click a link to sophisticated targeted attempts including phone calls and impersonation
- Awareness is key; look for red flags like a sense of urgency, poor spelling, or anything related to sending gift cards. Online safety courses are available to help with training your team.

IT Security

What are the threats?

Damage / Theft / Hardware Failure

- Ensure your servers are physically secure with limited access
- Be prepared with spare parts on hand; waiting for replacements could take weeks
- You must have off site backups for recovery
- Plan for downtime while systems are rebuilt

Protect Yourself

What can you do?

Put someone in charge

- Someone on your team should be responsible for IT Security for your business and implementing best practices
- Build an IT Security policy – enforce strong passwords, ban USB storage drives, set up role based user access, etc.
- Consult with an IT Security Specialist to perform audits, penetration testing, and address weaknesses in security

Protect Yourself

What can you do?

Proactive Monitoring

- Set up detectors to alert you to problems with heat or moisture
- Automate notifications for issues with hard drive space, CPU & disk usage, intrusion detections, etc.
- Set up surveillance cameras to keep an eye on mission critical systems

Protect Yourself

What can you do?

Virtualize

- Set up virtual servers that can be:
  - Restored from a backup in minutes
  - Scaled to meet changing business needs
  - Used to set up test/play environments
- Consider migrating to a Cloud-based hosting platform:
  - Eliminate physical threats
  - Centralize management & simplify maintenance

Protect Yourself

What can you do?

Create an Incident Response Plan

- Outline the steps you will take in the event of a security incident or system outage
- Include communication protocols and containment measures
- Document processes to be followed during an outage and train your team

Q&A