Assignment -
1. Experience-Based Practical and Learning Approach

Scenario:

**You start a new role at a company using both JAMF and Intune to manage a rapidly increasing
number of remote Apple and Windows devices. There have been frequent compliance failures
and security incidents on newly onboarded devices**.

Task:

Outline the step-by-step actions you would take in your first two weeks to audit, standardize, and secure the onboarding process for all devices.

Answer:

In my first two weeks, I would focus on understanding the current setup and then standardizing the onboarding process for both Apple and Windows devices.

Step 1: Audit the existing environment

I will review JAMF and Intune policies that are already in place for macOS, iOS, and Windows.
Then I will check current compliance policies, configuration profiles, and security baselines.
I will identify gaps, for example, devices that are not checking in properly, missing encryption, or outdated OS versions.

Step 2: Understand the onboarding workflow

I will go through how new devices are currently enrolled (Apple Business Manager + JAMF, Windows Autopilot + Intune).
I will note where failures are happening. For example, users skipping steps, profiles not applying.
I will connect with the support team to gather feedback on frequent issues during device setup.

Step 3: Standardize enrollment

For Apple devices: I will make sure all devices are linked with Apple Business Manager and auto-enrolled into JAMF with the right profiles.

For Windows devices: I will review Autopilot configuration in Intune and apply standard baseline profiles.
I ensure that all onboarding steps are consistent and well-documented for IT and end users.

Step 4: Strengthen security & compliance

I will apply conditional access policies so only compliant devices can access company resources and check FileVault for macOSand BitLocker for Windows encryption enforcement.
I validate that antivirus/EDR is deployed on all devices and push OS and app updates via JAMF/Intune to close patch gaps.

Step 5: Communication & Documentation

I will document the new onboarding process with clear steps for IT and employees and provide short training or knowledge articles to the support team.
I will set up reporting to track compliance status daily and highlight non-compliant devices quickly.

By the end of two weeks, the goal is to have a clear, repeatable onboarding process where every device is auto-enrolled, compliant policies are applied immediately, and security checks like encryption, updates are enforced from day one.

Specify which new knowledge resources, documentation, or communities you would consult or join to quickly adapt to the company's unique setup.

Answer:

To adapt quickly to the company's setup, I would use a mix of official documentation and community resources.

1. Microsoft Learn & Intune Documentation - This is used to understand how current Intune policies and Autopilot enrollment are designed.

2. Jamf Learning Hub & Jamf Nation Community - This is very useful for troubleshooting macOS/iOS issues and learning best practices from other admins.

3. Apple Business Manager & Deployment Guides - This is used to review how Apple devices are linked with JAMF.

4. Internal IT Documentation - any existing KB's or setup guides created by the company's IT team.

5. Tech Communities & Forums - like Microsoft Tech Community, Reddit r/macsysadmin, and LinkedIn groups for Intune/Jamf admins to learn real-world fixes.

6. Vendor Support - I will directly reach out to Microsoft and Jamf support when hitting product-specific issues.

Mention specific automations or compliance policies you would prioritize deploying for maximum early impact.

Answer:

For quick impact, I would focus on automations and compliance policies that cover the basics of security and standardization:

1. For Device Encryption I will enforce FileVault on macOS and BitLocker on Windows.

2. For OS & Patch updates, I will automate updates through JAMF policies and Intune update rings.

3. With the help of Conditional Access policies I can block non-compliant devices from accessing company apps or data.

4. For App Deployment, I will push required apps automatically during onboarding.

5. To Password and Lock Policies, I will enforce strong password rules and automatic screen lock.

6. For Compliance Alerts, I would set automated alerts for non-compliant devices so IT can act fast.

2**. Psychological / Persona Question**

Task:

Describe a time when you faced an unexpected technical issue that disrupted employee productivity.

How did you manage stress—both yours and that of the affected users?

I remember facing a case where several new Mac devices enrolled in Intune were failing compliance right after setup. Users were frustrated because they couldn't access Teams, Outlook, or SharePoint on their first day due to conditional access blocking non-compliant devices. Instead of panicking, I kept calm and first checked Intune compliance policies for macOS. I quickly found that FileVault encryption and OS version requirements were not being applied properly during enrollment. While working on the fix, I kept users updated and gave them temporary web access to email so they could continue their work. I then corrected the compliance policy order in Intune, pushed the FileVault requirement properly, and verified encryption status through the Intune portal. Once everything applied correctly, the Macs moved to a compliant state and users regained full access. This experience taught me the importance of validating policies on a test Mac before rolling them out to everyone.

Which personal strengths helped you deliver a positive outcome, and how did the experience shape your support approach?

When the new Macs in Intune were failing compliance, the personal strength that helped me most was staying calm and communicating clearly. Instead of letting the pressure get to me, I patiently explained to users what was happening and gave them temporary workarounds so they could still get some work done. At the same time, I focused step by step on fixing the FileVault and OS compliance issues. This experience shaped my support approach by showing me that users value transparency as much as a quick fix. Now, whenever I handle Mac or Intune issues, I make sure to combine technical troubleshooting with regular user updates to keep everyone confident while the problem is being resolved.

3. **Critical Thinking and Practical Approach**

Scenario:

A major system update is scheduled, but users are spread across time zones and some use
personally-owned, lightly managed devices. Last-minute, your team discovers a critical security patch has to be installed on all devices immediately.

● Questions:

How would you design and execute a remote patch deployment, balancing compliance and user disruption?

When dealing with Windows devices across different time zones, my goal would be to install the critical patch quickly while still giving users enough flexibility to avoid major disruption. In Intune, I'd configure an update ring that forces installation of the patch as a required update with a short compliance deadline, but I'd also enable a restart grace period so users can save their work before reboot.

For users on personally-owned Windows devices, I would rely on conditional access in Intune - meaning their access to company apps like Outlook or Teams would be blocked until the patch is installed. At the same time, I'd send clear communication about the urgency, with simple instructions on how to trigger the update manually if needed.

This mix of automated patch enforcement, compliance policies, and clear user communication would ensure all devices get secured quickly, no matter the time zone, without causing unnecessary downtime.

What steps would you take if some devices fail to update or end users do not respond?

If some devices failed to update or users didn't respond, I would first check Intune reports to identify which devices were non-compliant.

For corporate-owned Macs and Windows devices, I would try a forced redeployment of the patch or push the update again with a shorter deadline. If that still failed, I would investigate common causes like low disk space, encryption issues, or network problems.

For personally-owned devices, I would tighten conditional access, so users can't access company apps until they complete the update. To handle unresponsive users, I would send direct reminders and, if needed, escalate to their manager so the urgency is clear.

This way, I ensure every device eventually gets updated,either through technical enforcement or by making compliance a requirement for work.

Propose a communication and fallback plan to ensure no vulnerable devices are left unpatched.

My first step would be to send a clear communication to all users explaining the urgency of the patch, the deadline for installation, and simple instructions for both Mac and Windows devices. I would also schedule reminder emails and Teams messages so users don't miss it, especially across different time zones.

As a fallback, if some devices still don't patch on time, I would enforce conditional access in Intune so those devices cannot access company apps or data until they are updated. For corporate-owned devices that repeatedly fail, IT would step in with remote support or re-image if needed. This way, users are well informed, but we also have a safety net to make sure no device is left vulnerable.

4. AI Tools Detection-Style Follow-up

Instructions:

Your responses will be checked for personal authenticity, unique reasoning, and real insight—not just correctness.

Follow-up Task:

For Question 1, highlight how your approach draws from your actual experience at Allianz or Vodafone and not just generic MDM procedures.

At Allianz, when I joined, I noticed that many new Mac devices were not getting FileVault enabled properly through Intune during onboarding. Instead of just following standard MDM procedures, I worked with the team to test encryption policies on a pilot group of Macs first, so we could confirm compliance before wider rollout. I also created a simple checklist for the support team to follow during device handover, which reduced missed steps.

One detail from my experience that wouldn't appear in a textbook is how we had to deal with network latency during first-time setup for remote employees. Some users had slow internet at home, which caused Intune policies to apply late, leading to non-compliance flags. To handle this, I advised those users to keep their device on power and connected overnight so the encryption and updates could complete. This practical workaround came from direct experience, not from documentation.

Point out a detail or technique from your work that would not likely appear in an AI-generated or textbook answer.

One detail from my work that wouldn't appear in a textbook is how I handled first-day device setups for remote employees who had unstable internet connections. During onboarding at Allianz, some users struggled because Intune policies and app deployments timed out on weak home Wi-Fi. Instead of telling them to "retry," I guided them to connect their Mac overnight with power plugged in, so encryption, policy sync, and app installs could finish without interruption. I also scheduled follow-ups the next morning to confirm compliance.

This kind of workaround -based on real user behavior and network conditions - is something I learned on the job, not from documentation.