Lab 7

Brandon P Trinkle

Arizona State University

Course Number: IFT 220

Professor Betty J. Lauer

April 16, 2024

Lab 7

For this lab I will create a fictional company called TechCorp to better illustrate the use of Intune. TechCorp is a leading technology solutions provider with 500 employees distributed across multiple locations. The workforce includes software developers, product managers, sales and marketing professionals, and support staff. TechCorp has a mix of in-office and remote employees, with a variety of devices, including Windows laptops, macOS computers, iOS devices, and Android smartphones. The company promotes a Bring Your Own Device (BYOD) culture, allowing employees to use their personal devices for work, which presents unique challenges for device management and security. Given the diverse device landscape and flexible work arrangements, TechCorp's IT department is tasked with implementing an endpoint management solution to streamline device management, control application deployment, and ensure security and compliance. Microsoft Intune has been chosen to centralize these efforts, offering the flexibility and cloud-based functionality required by TechCorp's dynamic work environment.

Microsoft Intune is designed to help organizations manage devices and apps in a flexible and secure manner. It is particularly valuable in environments with a diverse range of devices, including mobile phones, tablets, and laptops. Intune offers several features that streamline the management of endpoints while ensuring security and compliance. One of Intune's key strengths is its cloud-based nature, allowing administrators to manage devices remotely. This feature is crucial in a world where remote work and Bring Your Own Device (BYOD) policies are increasingly common. Additionally, Intune integrates seamlessly with other Microsoft products, such as Azure Active Directory, Microsoft 365, and Microsoft Defender, offering a comprehensive suite for endpoint management.

To control end-user management and maintain security across TechCorp's device landscape, the following steps outline an installation and implementation plan for Microsoft Intune:

*Step 1: Establish Enrollment Policies*

The first step in implementing Intune for end-user management is to define device enrollment policies. TechCorp's IT team must create a set of rules that govern how devices are enrolled into Intune. This includes:

* **Authorized Devices**: Specify which device types and operating systems are allowed to enroll in Intune. This should cover Windows, macOS, iOS, and Android.
* **BYOD Guidelines**: Define rules for personal devices used in a work context. This may include restrictions on jailbroken/rooted devices and requirements for device security features like encryption.
* **Enrollment Authentication**: Set up authentication methods to ensure only authorized users can enroll their devices. This might include integration with Azure Active Directory (Azure AD) for single sign-on (SSO).

*Step 2: Implement Device Configuration Policies*

Once enrollment policies are established, TechCorp's IT team must create device configuration policies to control end-user management. This involves:

* **Device Settings**: Define configurations for device settings, such as Wi-Fi connections, email accounts, and VPN settings. This allows IT to ensure consistent setup across all devices.
* **Security Policies**: Implement security policies, such as password requirements, device encryption, and automatic screen lock. These policies help protect sensitive data and ensure compliance with industry regulations.
* **Compliance Rules**: Set up compliance rules to monitor device health and ensure adherence to company policies. This may include checking for the latest operating system updates and verifying the presence of security software.

*Step 3: Set Up Application Management*

Application management is a critical aspect of end-user control. TechCorp's IT team should configure application deployment policies to manage software across enrolled devices. This includes:

* **Approved Applications**: Define a list of approved applications that can be installed on company devices. This list should cover productivity software, communication tools, and any specialized applications required for TechCorp's operations.
* **Application Deployment**: Create policies for deploying applications to specific groups or departments. This allows IT to tailor application sets to different user roles.
* **Application Compliance**: Implement rules to restrict unauthorized applications and monitor application usage. This helps prevent security risks from unapproved software.

*Step 4: Integrate Security and Compliance Features*

To ensure comprehensive security, TechCorp's IT team should integrate Intune's security and compliance features into the end-user management process. This involves:

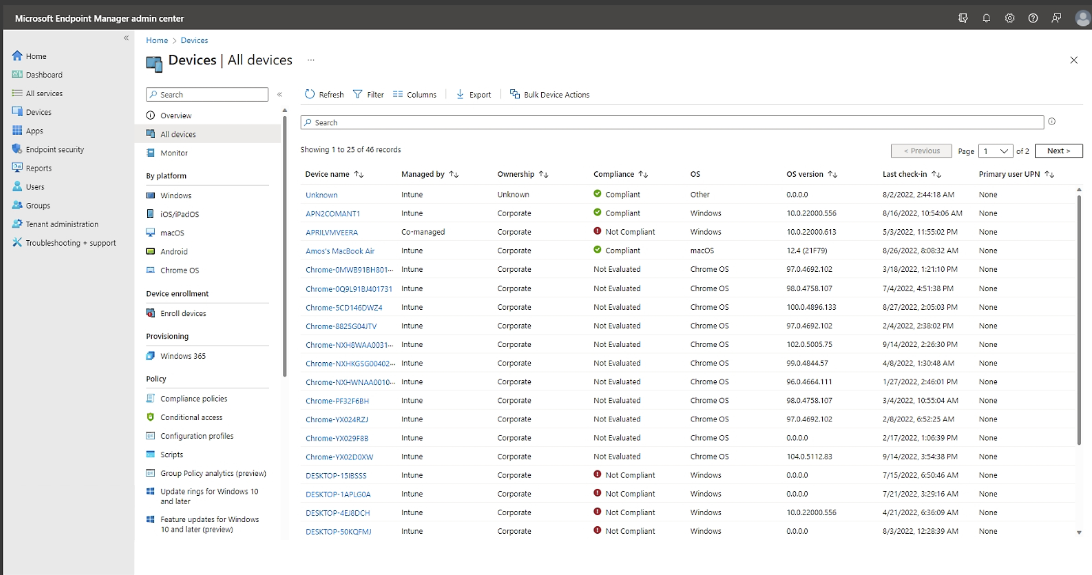
* **Conditional Access:** Configure conditional access policies that restrict access to sensitive data based on device compliance. This feature ensures that only secure devices can access critical resources.
* **Remote Wipe Capabilities**: Set up remote wipe policies to protect sensitive data in case of device loss or theft. This feature allows IT to erase data remotely to prevent unauthorized access.
* **Security Monitoring:** Integrate Intune with Microsoft Defender to monitor security threats and detect potential vulnerabilities. This integration provides an additional layer of protection for TechCorp's endpoints.

*Step 5: Establish User Support and Communication*

The final step in the installation plan is to establish user support and communication strategies. TechCorp's IT team should:

Provide User Training: Offer training sessions to educate employees about Intune's features and the new device management policies. This helps ensure user compliance and reduces the risk of security incidents.

* **Create a Support System**: Set up a helpdesk or support system to assist users with any issues related to Intune. This includes troubleshooting device enrollment problems, addressing application deployment issues, and handling security concerns.
* **Communicate Policy Changes:** Maintain clear communication with employees regarding any changes to device management policies. This helps prevent confusion and ensures everyone is aware of their responsibilities.



(Microsoft, 2024)

# References

Microsoft. (2024, April 22). *Microsoft Intune core capabilities*. Retrieved from Microsoft: https://www.microsoft.com/en-us/security/business/endpoint-management/microsoft-intune