

kod szkolenia: MS 55399 / PL AA 3d

Implement and Manage Microsoft Intune

Zobacz film: <https://youtu.be/gmUE0GQu3ao>



Przeznaczenie szkolenia

Ten trzydniowy kurs jest skierowany do profesjonalistów zajmujących się nowoczesnym zarządzaniem urządzeniami oraz którzy chcą zarządzać urządzeniami za pomocą Microsoft Intune. Kurs obejmuje rejestrację, zarządzanie aplikacjami, bezpieczeństwo końcówek oraz Windows Autopilot, a także warunkowy dostęp i ochronę tożsamości w Azure Active Directory.



Korzyści wynikające z ukończenia szkolenia

Uczestnicy dowiedzą się, jak rejestrować urządzenia, wdrażać aplikacje i zarządzać nimi, aby maksymalizować produktywność użytkowników i bezpieczeństwo urządzeń.



Oczekiwane przygotowanie słuchaczy

Po zapisaniu się na szkolenie prosimy o zapoznanie się z instrukcją zakładania tenantu :

https://www.altkomakademia.pl/app/uploads/2024/09/MS_TENANT_PL.pdf

Tenant musi zostać założony min. 4 dni przed pierwszym dniem szkolenia.

- podstawowe zrozumienie koncepcji sieci komputerowych i sprzętu.
- podstawowe zrozumienie koncepcji systemu operacyjnego i aplikacji.
- doświadczenie w korzystaniu z systemu operacyjnego Windows.

- dobra znajomość administracji Windows 10/11
- podstawowa wiedza o Microsoft Azure (min. poziom z AZ-900) lub praktyczne doświadczenie w administracji Office 365



Język szkolenia

- Szkolenie: polski
- Materiały: angielski



Szkolenie obejmuje

* dostęp do portalu słuchacza Altkom Akademii



Czas trwania

3 dni / 21 godzin

Agenda szkolenia

1. Wprowadzenie do Microsoft Intune

- *Zarządzanie urządzeniami mobilnymi (Mobile Device Management)
- *Microsoft Intune
- *Azure Active Directory (AAD)
- *Ochrona tożsamości w AAD (AAD Identity Protection)
- *Warunkowy dostęp w AAD (AAD Conditional Access)

2. Zarządzanie urządzeniami w Microsoft Intune

- *Rejestracja urządzeń (Enrolling Devices)
- *Zgodność urządzenia (Device Compliance)
- *Profile urządzeń (Device Profiles)
- *Aktualizacje urządzeń (Device Updates)

3. Zarządzanie aplikacjami w Microsoft Intune

- *Zarządzanie aplikacjami (Application Management)
- *Wdrażanie aplikacji (Deploying Applications)
- *Konfiguracja aplikacji (Application Configuration)
- *Zarządzanie aplikacjami (Managing Applications)
- *Zestawy polityk i prowadzone scenariusze (Policy Sets and Guided Scenarios)

4. Bezpieczeństwo końcówek w Microsoft Intune

- *Podstawowe linie bezpieczeństwa i zadania (Security Baselines and tasks)
- *Antywirus
- *Szyfrowanie dysku (Disk Encryption)
- *Zapora sieciowa (Firewall)
- *Redukcja powierzchni ataku (Attack Surface Reduction)
- *Wykrywanie i reagowanie na końcówki (Endpoint Detection and Response)
- *Ochrona konta (Account Protection)

5. Wdrażanie systemu Windows za pomocą Windows Autopilot

- *Przegląd Windows Autopilot
- *Przygotowanie do wdrożenia Windows Autopilot
- *Wdrażanie systemu Windows 11 za pomocą Windows Autopilot

6. Dodatkowe i Premium funkcje Microsoft Intune

- *Pomoc zdalna (Remote Help)
- *Tunel do zarządzania aplikacjami mobilnymi (Tunnel for Mobile Application Management)
- *Zarządzanie przywilejami na końcówce (Endpoint Privilege Management)
- *Zaawansowana analiza końcówek (Advanced Endpoint Analytics)