MD-102: Manage and secure Microsoft 365 endpoints by using Intune

Microsoft

Promoção: **Curso com 15% de desconto**Aproveite já!

Live Training (também disponível em presencial)

- **Localidade:**
- **Data:** 02 Jul 2025
- **Preço:** 2010 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 9h00 às 17h00
- **Nível:** Intermédio
- **Duração:** 35h

Sobre o curso

Aprende a planear e executar uma estratégia de implementação, configuração e gestão de endpoints utilizando o Microsoft Intune como plataforma unificada de gestão de endpoints.

Neste curso irás abordar a preparação da infraestrutura de identidade e dispositivos com Microsoft Entra ID, o enrollment e a configuração de dispositivos, a gestão de aplicações e a proteção de endpoints e dados. Irás também explorar a automação com PowerShell e Microsoft Graph, a gestão assistida por AI com Microsoft Security Copilot, as capacidades avançadas do Microsoft Intune Suite e a disponibilização de desktops na cloud com Windows 365 e Azure Virtual Desktop.

Entre as tecnologias abordadas incluem-se Microsoft Intune, Microsoft Entra ID, Windows Autopilot, Microsoft Defender for Endpoint, Microsoft Tunnel, Microsoft Cloud PKI, Microsoft Intune Suite, Windows 365 e Azure Virtual Desktop.

Destinatários

- Administradores de sistemas e de endpoints que pretendam implementar, configurar e gerir dispositivos com Microsoft Intune.
- Profissionais de IT responsáveis pela administração de ambientes Microsoft 365 e Microsoft Entra ID.
- Endpoint Administrators e Workplace Administrators que pretendam aprofundar competências em gestão moderna de dispositivos Windows, macOS, iOS/iPadOS e Android.
- Técnicos de suporte e administradores de postos de trabalho que pretendam evoluir para funções de gestão e administração de endpoints.

- Profissionais envolvidos na implementação de Windows Autopilot, Windows 365, Azure Virtual Desktop e Microsoft Intune Suite.
- Profissionais que pretendam preparar-se para a certificação Microsoft 365 Certified: Endpoint Administrator Associate.

Objetivos

- Planear e implementar uma estratégia moderna de gestão de endpoints utilizando Microsoft Intune e Microsoft Entra ID.
- Configurar, implementar e gerir dispositivos Windows, macOS, iOS/iPadOS e Android, incluindo cenários de deployment com Windows Autopilot.
- Gerir aplicações, políticas, atualizações e conformidade para garantir a segurança e a produtividade dos utilizadores.
- Proteger dispositivos e dados através de Microsoft Defender, Conditional Access, Microsoft Tunnel e Microsoft Cloud PKI.
- Automatizar tarefas de administração e otimizar a gestão de endpoints utilizando PowerShell, Microsoft Graph e Microsoft Security Copilot.
- Preparar candidatos para o exame de certificação Microsoft 365 Certified: Endpoint Administrator Associate (MD-102).

Condições

Para particulares

• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.

• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes do início do curso.

• Possibilidade de pagamento faseado.

• Isenção de IVA para particulares.

Para empresas

• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).

• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

- Conhecimentos básicos dos conceitos de administração do Microsoft 365.
- Familiaridade com Microsoft Entra ID e gestão de utilizadores e grupos.

Programa

- Preparar a infraestrutura para dispositivos com Microsoft Intune e Microsoft Entra ID

- Gerir e manter dispositivos com Microsoft Intune
- Gerir aplicações com Microsoft Intune
- Proteger dispositivos com Microsoft Intune
- Automatizar e otimizar a gestão de endpoints com Microsoft Intune
- Suportar excelência operacional e preparação com Microsoft Intune
- Expandir capacidades de endpoints com Microsoft Intune Suite
- Disponibilizar desktops alojados na cloud com Azure Virtual Desktop e Windows 365

Preparar a infraestrutura para dispositivos com Microsoft Intune e Microsoft Entra ID

Neste módulo, vais aprender a criar a infraestrutura de identidade e enrollment que suporta a gestão de endpoints baseada em cloud com Microsoft Intune e Microsoft Entra ID. Começas por explorar o papel do Intune na gestão moderna de endpoints e os modelos de gestão disponíveis, configurando depois o Microsoft Entra ID para suportar a segmentação de políticas através de utilizadores, grupos, funções e definições de registo de dispositivos. Aprofundas ainda a identidade e autenticação de dispositivos, compreendendo como os tipos de adesão e modelos de confiança afetam a gestão de dispositivos e o Conditional Access. A partir daí, vais planear e implementar o enrollment de dispositivos Windows, iOS/iPadOS, macOS e Android, configurar restrições de enrollment e resolver falhas comuns. O módulo termina com Windows Autopilot, onde vais registar dispositivos, configurar perfis de deployment, pré-aprovisionar hardware e monitorizar e resolver problemas em deployments.

- Compreender estratégias de gestão de endpoints e Microsoft Intune
- Configurar Microsoft Entra ID para gestão de dispositivos e políticas
- Administrar identidade e autenticação de dispositivos com Microsoft Entra ID
- Planear e implementar enrollment de dispositivos com Microsoft Intune
- Implementar dispositivos Windows com Windows Autopilot

Gerir e manter dispositivos com Microsoft Intune

Neste módulo, vais aprender a configurar e gerir dispositivos após o enrollment com Microsoft Intune. Começas por criar e atribuir perfis de configuração de dispositivos e políticas de conformidade, utilizando grupos e filtros para uma segmentação precisa, e migrando definições de Group Policy on-premises para a cloud. Depois, exploras a gestão de atualizações do Windows, configurando update rings, políticas de atualização de funcionalidades, Hotpatch e Windows Autopatch para manter os dispositivos atualizados e seguros. Em seguida, aprendes a monitorizar o estado dos dispositivos e das políticas com Endpoint Analytics, Proactive Remediations e relatórios do Intune para manter visibilidade e promover ações corretivas à escala. O módulo termina com uma abordagem estruturada à resolução de problemas, abrangendo falhas de enrollment e conformidade, conflitos de políticas, ferramentas de diagnóstico, o painel de Troubleshooting do Intune e a resolução automatizada de problemas com scripts de remediação.

- Configurar perfis de dispositivos e gestão de políticas com Microsoft Intune
- Monitorizar e manter dispositivos com Microsoft Intune
- Gerir atualizações e ciclo de vida do Windows com Microsoft Intune
- Resolver problemas de dispositivos e políticas com Microsoft Intune

Gerir aplicações com Microsoft Intune

Neste módulo, vais aprender a disponibilizar e governar aplicações em endpoints geridos com Microsoft Intune.

Começas por implementar aplicações line-of-business, store, web e Microsoft 365 para utilizadores e dispositivos, implementando depois políticas de proteção de aplicações (APP) e políticas de configuração de aplicações para proteger dados corporativos em dispositivos móveis e BYOD. Exploras todo o ciclo de vida das aplicações, incluindo atribuição, atualizações, supersedence, retirada e desinstalação, e aprendes a monitorizar o sucesso das instalações, resolver falhas de entrega e otimizar o desempenho à escala. O módulo termina com o Enterprise App Catalog, onde aprendes a publicar, configurar e atualizar aplicações Win32 pré-empacotadas com esforço mínimo de reempacotamento.

- Implementar e gerir aplicações com Microsoft Intune
- Implementar proteção e segurança de aplicações com Microsoft Intune
- Gerir o ciclo de vida das aplicações e a experiência de utilizador com Microsoft Intune
- Monitorizar e otimizar o desempenho das aplicações com Microsoft Intune
- Gerir aplicações do Enterprise App Catalog

Proteger dispositivos com Microsoft Intune

Neste módulo, vais aprender a aplicar proteção por camadas a endpoints geridos com Microsoft Intune e o conjunto mais amplo de soluções Microsoft Defender. Começas por integrar Microsoft Defender for Endpoint com Intune, implementando depois encriptação de dispositivos (BitLocker, FileVault e personal data encryption) para proteger dados em repouso. Exploras cenários avançados de proteção contra ameaças, incluindo attack surface reduction rules, endpoint detection and response e Conditional Access baseado no risco. A partir daí, crias e aplicas políticas de conformidade, promoves a remediação através de Conditional Access e monitorizas a postura de conformidade à escala. O módulo termina com dois cenários especializados: disponibilização de acesso móvel seguro com Microsoft Tunnel e emissão e gestão de certificados de dispositivos com Microsoft Cloud PKI.

- Implementar segurança de endpoints com Microsoft Defender e Microsoft Intune
- Implementar encriptação de dispositivos e políticas de segurança com Microsoft Intune
- Implementar proteção avançada contra ameaças com Microsoft Intune e Microsoft Defender
- Aplicar conformidade e corrigir problemas de segurança com Microsoft Intune
- Proteger o acesso móvel com Microsoft Tunnel
- Implementar Microsoft Cloud PKI

Automatizar e otimizar a gestão de endpoints com Microsoft Intune

Neste módulo, vais aprender a escalar, automatizar e otimizar a gestão diária de endpoints com Microsoft Intune, PowerShell, Microsoft Graph e Copilot. Começas por automatizar tarefas repetitivas do Intune, como consultas de dispositivos, alterações de configuração em massa, relatórios e provisionamento de políticas, utilizando o Microsoft Graph PowerShell SDK e o Graph Explorer. Depois, exploras como a AI e o Microsoft Copilot no Intune ajudam os administradores a obter recomendações, criar políticas, investigar problemas de dispositivos e acelerar a resolução de problemas. O módulo termina com a gestão end-to-end do desempenho de endpoints com Endpoint Analytics, Proactive Remediations e performance baselines para identificar e resolver, à escala, problemas de arranque lento, início de sessão lento, fiabilidade de aplicações e estado da bateria.

- Automatizar a gestão de endpoints com PowerShell e Microsoft Graph
- Otimizar a gestão de dispositivos com AI e ferramentas Copilot
- Monitorizar e otimizar o desempenho de endpoints com Microsoft Intune

Suportar excelência operacional e preparação com Microsoft Intune

Neste módulo, vais aprender a operar o Microsoft Intune como um serviço operacionalmente saudável, no qual outras equipas podem confiar. Começas por implementar reporting e visibilidade de dados, escolhendo os relatórios operacionais, organizacionais, históricos e especializados adequados, exportando dados através da Reports API e apresentando insights em dashboards Power BI. Depois, desenhas e aplicas role-based access control (RBAC), incluindo funções incorporadas e personalizadas, scope tags e padrões de delegação administrativa alinhados com princípios de least privilege. O módulo termina com práticas de saúde do tenant, incluindo monitorização do estado do serviço, audit logs, higiene de licenças e ciclo de vida do tenant, bem como rotinas que mantêm um tenant Intune preparado para produção.

- Implementar reporting e visibilidade de dados com Microsoft Intune
- Aplicar RBAC e delegação administrativa no Microsoft Intune
- Manter a saúde do tenant e a preparação do suporte

Expandir capacidades de endpoints com Microsoft Intune Suite

Neste módulo, vais aprender a expandir o Microsoft Intune com as capacidades premium disponibilizadas através do Microsoft Intune Suite. Começas com uma visão geral do portefólio Intune Suite, incluindo o que está incluído, como é licenciado e que cenários cada componente foi desenhado para responder. Depois, implementas Remote Help para disponibilizar assistência remota segura e auditada a dispositivos geridos, e utilizas Advanced Endpoint Analytics para apresentar sinais mais detalhados de dispositivos e aplicações, incluindo deteção de anomalias, analytics segmentados e reporting de desempenho mais rico. O módulo termina com Endpoint Privilege Management (EPM), onde vais avaliar políticas que permitem a utilizadores standard executar ações aprovadas com privilégios elevados, reduzindo a dispersão de administradores locais sem comprometer a produtividade.

- Explorar capacidades do Microsoft Intune Suite
- Implementar cenários de Remote Help com Microsoft Intune
- Analisar sinais avançados de dispositivos com Microsoft Intune Suite
- Avaliar Endpoint Privilege Management com Microsoft Intune

Disponibilizar desktops alojados na cloud com Azure Virtual Desktop e Windows 365

Neste módulo, vais aprender a disponibilizar desktops Windows alojados na cloud aos utilizadores com Windows 365 e Azure Virtual Desktop, e a gerir esses desktops em conjunto com endpoints físicos através do Microsoft Intune. Começas por explorar edições do Windows 365 Cloud PC, licenciamento, provisionamento e experiência do utilizador final, configurando e gerindo depois Cloud PCs diretamente a partir do centro de administração do Intune, incluindo gestão de imagens, configuração de rede, atribuição de utilizadores e monitorização contínua do estado. Exploras a arquitetura do Azure Virtual Desktop, host pools, application groups, perfis FSLogix e gestão de session hosts, e comparas Azure Virtual Desktop com Windows 365 para escolher a plataforma de cloud desktop mais adequada a cada workload. O módulo termina com a integração de session hosts do Azure Virtual Desktop com Microsoft Intune para uma gestão unificada de políticas, aplicações e segurança em todos os endpoints Windows, físicos e virtuais.

- Explorar Windows 365 para deployment de Cloud PCs
- Configurar e gerir Windows 365 com Microsoft Intune
- Explorar Azure Virtual Desktop

- Integrar Azure Virtual Desktop com Microsoft Intune