Microsoft Intune

Article • 09/21/2023

Microsoft Intune is the cloud-based mobile device management (MDM) and mobile app management (MAM) provider for apps and devices. Each customer has their own unique environment. Assistance is based on specific mobile device and mobile app management needs.

FastTrack provides remote guidance for:

- Licensing your end users
- Configuring identities used by Intune by leveraging either on-premises Active Directory or cloud identities (Microsoft Entra ID).
- Adding users to your Microsoft Intune subscription, defining IT admin roles, and creating user and device groups.
- Configuring MDM authority, based on management needs, including setting Intune as your MDM authority when Intune is the only MDM solution.
- Providing MDM guidance for:
  - Configuring tests groups to be used to validate MDM management policies.
  - Configuring MDM management policies and services including:
    - App deployment for each supported platform through web links or deep links.
    - Conditional Access policies.
    - Deployment of email, wireless networks, VPN profiles for existing certificate authority, wireless network, or VPN infrastructure in the organization.
    - Connecting to the Intune Data Warehouse.
    - Integrating Intune with:
      - Team Viewer for remote assistance (a Team Viewer subscription is required).
      - Mobile Threat Defense (MTD) partner solutions (an MTD subscription is required).
      - A telecom expense management solution (a telecom expense management solution subscription is required).
  - Enrolling devices of each supported platform to Intune.
- Providing app protection guidance on:
- Configuring app protection policies for each supported platform.
- Configuring Conditional Access policies for managed apps.
- Targeting the appropriate user groups with the previously mentioned MAM policies.
- Using managed-apps usage reports.
- Providing migration guidance from legacy PC management to Intune MDM.

Certificate delivery

FastTrack provides remote guidance for:

- Simple Certificate Enrollment Protocol (SCEP) and the Network Device Enrollment Service (NDES).
  - Configuring Enterprise Certificate Authority-related items.
  - Creating and issuing a SCEP certificate template.
  - Installing and configuring NDES.
  - Installing and configuring the Microsoft Intune Connector for SCEP.
  - Installing and configuring Microsoft Entra ID Application Proxy and Microsoft Entra ID Application connectors.
  - Creating and assigning a trusted certificate device configuration profile in Microsoft Endpoint Manager.
  - Creating and assigning a SCEP certificate device configuration profile on Microsoft Endpoint Manager.
- Public-Key Cryptography Standards (PKCS) and PFX (PKCS#12) certificates.
  - Configuring enterprise Certificate Authority-related items.
  - Creating and issuing a PKCS certificate template.
  - Installing and configuring a PFX certificate connector.
  - Creating and assigning a trusted certificate device configuration profile in Microsoft Endpoint Manager.
  - Creating and assigning a PKCS certificate device configuration profile in Microsoft Endpoint Manager.

Out of scope

- Assistance with public key infrastructure (PKI) certificates or enterprise Certificate Authority.
  - Supporting advanced scenarios, including:
    - Placing the NDES server in the customer's DMZ.
    - Configuring or using a Web Application Proxy server to publish the NDES URL externally to the corporate network. We recommend and provide guidance for using the Microsoft Entra ID Application Proxy to accomplish this.
    - Using imported PKCS certificates.
    - Configuring Intune certification deployment using a hardware security module (HSM).

Cloud-attach

FastTrack provides remote guidance to customers to cloud-attach existing Configuration Manager environments with Intune.

This includes:

- Licensing end users.
- Configuring identities to be used by Intune by leveraging on-premises Active Directory and cloud identities.
- Adding users to your Intune subscription, defining IT admin roles, and creating user and device groups.
- Providing guidance setting up hybrid Microsoft Entra ID join.
- Providing guidance on setting up Microsoft Entra ID for MDM auto-enrollment.
- Providing guidance on how to set up cloud management gateway when used as a solution for co-management of remote internet-based device management.
- Configuring supported workloads to switch to Intune.
- Installing the Configuration Manager client on Intune-enrolled devices.

Deploy Outlook mobile for iOS and Android securely

FastTrack provides remote guidance to customers to deploy Outlook mobile for iOS and Android securely to ensure users have all required apps installed.

This includes:

- Downloading Outlook for iOS and Android, Microsoft Authenticator, and Intune Company Portal apps through the Apple App Store or Google Play Store.
- Setting up:
  - The Outlook for iOS and Android, Microsoft Authenticator, and Intune Company Portal apps deployment with Intune.
  - App protection policies.
  - Conditional Access policies.
  - App configuration policies.

Endpoint analytics

FastTrack provides remote guidance to customers to enable Endpoint analytics.

This includes:

- Confirming the licenses for your endpoints and users.
- Confirming your organizational environments meet the prerequisites for Endpoint analytics features.
- Configuring endpoints with correct policies to enable Endpoint analytics features.
- Setting organizational baselines to track progress.
- Providing guidance on using Remediation within Endpoint analytics, including:
  - Using Microsoft-authored remediation scripts.
  - Creating custom remediation scripts.

Out of scope

- Setting up or configuring Certificate Authorities, wireless networks, VPN infrastructures, or Apple MDM push certificates for Intune.
- Setting up or upgrading either the Configuration Manager site server or Configuration Manager client to the minimum requirements needed to support cloud-attach.
- Integrating Intune with Microsoft Defender for Endpoint and creating device compliance policies based on its Windows** 10** risk level assessment. FastTrack doesn't assist with purchasing, licensing, or activation.

Contact a Microsoft Partner for assistance with any out-of-scope services.

Source environment expectations

- IT admins must have existing Certificate Authority, wireless network, and VPN infrastructures enabled in their production environments in order to deploy wireless network and VPN profiles with Intune.
- The customer environment should have an existing healthy PKI before enabling PKCS and SCEP certificate delivery with Intune.
- Endpoint devices must be managed by Intune.
- IT admins are responsible for registering the devices to the organization by either having the hardware vendor upload the hardware IDs for uploading it themselves into the Windows Autopilot service.

Microsoft advanced deployment guides

Microsoft provides customers with technology and guidance to assist with deploying your Microsoft 365, Microsoft Viva, and security services. We encourage our customers to start their deployment journey with these offerings.

For non-IT admins, see Microsoft 365 Setup .