MD-102 AUDIO BOOK NOTES

SECTIONS

Section 1.1: Choosing an Appropriate Device Join Type

- **Importance**: Join type defines how devices access organizational resources and how much control IT has.
- **Types**:
    1. **Entra ID Join** – Cloud-only; best for fully cloud-based environments (e.g., startups using Microsoft 365 only).
    2. **Hybrid Entra ID Join** – Connects to both cloud and on-prem AD; best for organizations in transition (e.g., large enterprises with local servers + cloud).
    3. **Entra ID Registration** – Lightweight, BYOD; best for personal devices needing limited access (e.g., email on personal phone).

- **Decision Factors**: Cloud vs hybrid, company-owned vs personal, level of management needed.

Section 1.2: Joining Devices to Microsoft Entra ID

- **Purpose**: Provides secure, centralized device authentication and management.
- **Methods**:
    1. **Self-Service Join** – User-driven process in Windows settings.
    2. **Bulk Enrollment with Autopilot** – Pre-configures many devices to auto-join during setup.
    3. **Group Policy for Hybrid Join** – Automates join for devices in hybrid environments.
- **Key Considerations**:
    - Ensure proper permissions.
    - Device join limits (default: 15 per user).
    - Supports Conditional Access policies.

Section 1.3: Registering Devices to Microsoft Entra ID

- **Purpose**: Allows secure access from personal/BYOD devices without full management.
- **Process**: User initiates registration → Device authenticates → Gains access to resources.
- **Best Scenarios**:
    - Work email/calendar on personal phone.
    - Contractors with temporary access.
- **Benefits**: Quick setup, light IT involvement, protects user privacy, applies basic security controls.
- **Limitations**: Not full management; subject to device limits and Conditional Access.

Section 1.4: Planning and Implementing Groups for Devices

- **Purpose**: Organizes devices, simplifies management, and applies policies efficiently.
- **Group Types**:
    1. **Assigned Groups** – Manual membership; best for static, small environments (e.g., shared conference room devices).
    2. **Dynamic Groups** – Automatic membership based on rules/attributes; best for large, changing environments (e.g., all Windows laptops).
- **Planning Considerations**:
    - Define purpose (security, apps, compliance).
    - Balance group size and flexibility.
    - Prevent policy overlap (last writer wins in conflicts).
- **Implementation Steps**: Create group → Define membership → Apply policies.
- **Example**: Sales (mobile policies) vs Engineering (firewall + updates).

Section 2.1: Configure Enrollment Settings

Purpose

- Enrollment settings define **who can enroll devices**, **what device types are permitted**, and **how secure the enrollment process must be**.
- They act as the *first line of control* over your Intune environment.

Core Configuration Elements

1. **User Scope**
    - Determines which users or groups are allowed to enroll devices.
    - *Example:* Limit enrollment to only Sales and Marketing departments.
2. **Device Type Restrictions**
    - Control allowed operating systems, manufacturers, and models.
    - Ensures standardization (e.g., only Windows and iOS devices permitted).
3. **Device Ownership**

    - Classify devices as **corporate-owned** or **personal/BYOD**.
    - Ownership affects what level of IT control applies.
4. **Require Multi-Factor Authentication (MFA)**
    - Adds identity verification during enrollment.
    - Enhances security by preventing unauthorized enrollment.
5. **Enrollment Limits**
    - Set a maximum number of devices a user can enroll (default is 5–15 depending on tenant).

Customizing the Enrollment Experience

- **Branding:** Add company logos, support links—improves user trust and engagement.
- **Terms and Conditions:** Require acceptance to enforce compliance expectations.

Key Considerations

- Educate users on requirements (like MFA or OS version).
- Balance **security vs user convenience**.
- Regularly review and update enrollment settings.

Bottom Line: Enrollment settings protect your Intune environment by controlling access before devices even join the system.

Section 2.2: Configure Automatic Enrollment (Windows) & Bulk Enrollment (iOS/Android)

Automatic Enrollment for Windows Client Devices

- Windows devices can automatically enroll into Intune when users sign in with their Entra ID account.
- Enabled through **Microsoft Entra ID** settings and Intune enrollment configurations.

How It Works

1. Admin enables automatic enrollment in Entra ID.
2. Enrollment policies define *who* is eligible.

3. User signs in → device automatically enrolls and receives policies.

Real-world benefit: Zero-touch onboarding for Windows laptops—ideal for remote workers or bulk deployments.

Bulk Enrollment for iOS & Android

- Designed for rolling out many company-owned devices quickly (like store tablets or field devices).

Methods

- **iOS:** Uses **Apple Business Manager (ABM)** integrated with Intune.
- **Android:** Uses **Android Enterprise** (zero-touch enrollment, QR code, Knox Mobile Enrollment, etc.)

Benefits

- Devices enroll automatically on first boot.
- Policies, apps, and security settings are applied instantly.
- Great for shared or corporate-owned devices.

Key Considerations

- Ensure only eligible devices are automatically enrolled.
- Use **Conditional Access + MFA** to secure enrollment.
- Clearly communicate instructions to users.

Bottom Line: These methods streamline large-scale deployments and deliver instant compliance with minimal IT effort.

Section 2.3: Configure Enrollment Profiles for Android Devices

Purpose

Enrollment profiles control how Android devices are managed, based on use case and ownership. They define the *level of control* and *privacy*.

Types of Android Enrollment Profiles

Profile Type	Ownership	Use Case	Control Level
Fully Managed	Corporate-owned	Work-only devices	Full IT control
Dedicated	Corporate-owned	Single-purpose devices (kiosks, POS, digital signage)	Locked to specific apps
COPE (Corporate-Owned Personally Enabled)	Corporate-owned	One device for both work and personal use	Separate work/personal profiles
Work Profile	Personal/BYOD	Personal devices with work needs	Only work apps/data are managed

Key Benefits & Scenarios

- **Fully Managed:** Field employees using a device only for business.
- **Dedicated:** Retail kiosk or inventory tablet.
- **COPE:** Executive using one phone for both personal and work.
- **Work Profile:** Employee checking email on a personal phone.

Configuration Steps

1. Go to **Intune Admin Center → Device Enrollment → Android Enrollment**
2. Select enrollment type
3. Configure policies, apps, restrictions
4. Assign to user or device groups

Important Considerations

- Choose profile based on **device ownership and intended usage**.
- Communicate clearly with end-users regarding privacy (especially BYOD and COPE).
- Balance usability with security requirements.

Bottom Line: Enrollment profiles ensure Android devices receive the exact level of security and control needed—nothing more, nothing less.

Section 3.1: Manage Roles in Intune

Purpose

Roles control access in Intune and ensure that each administrator or support person only has the permissions needed for their responsibilities. This improves security and operational control.

Key Built-in Roles

Role	Purpose	Real-World Analogy
Intune Administrator	Full access to Intune features and settings	IT Director with full system control
Policy and Profile Manager	Manages device configuration and compliance policies	Technician configuring devices
Application Manager	Manages app deployment and assignment	Librarian selecting and distributing applications
Help Desk Operator	Troubleshoots devices and performs limited actions	Front-line support staff

Best Practices

- Follow the principle of least privilege.
- Assign roles to groups, not individuals.
- Review role assignments regularly.
- Create custom roles for specialized scenarios.

Summary: Role-based access ensures security, delegation, and administrative efficiency.

Section 3.2: Implement Compliance Policies

Purpose

Compliance policies define security requirements that devices must meet before being allowed to access company resources.

Key Compliance Policy Controls

- Password requirements (length, complexity, expiration)
- Operating system version restrictions
- Encryption requirements
- Device health checks (antivirus, firewall, secure boot)
- Jailbreak/root detection

Outcome

Devices are marked compliant or noncompliant. Noncompliant devices can be blocked or required to remediate.

Summary: Compliance policies enforce baseline security across all device platforms.

Section 3.3: Implement Conditional Access Requiring Compliance

Purpose

Conditional Access controls access to apps and resources based on conditions, such as device compliance, user identity, and sign-in risk.

Key Functionalities

- Requires compliant devices for access
- Supports multi-factor authentication
- Can restrict access based on location or application sensitivity

Best Practices

- Test policies using report-only mode before enforcing
- Educate users on compliance requirements
- Review policies as threats evolve

Summary: Conditional Access enforces compliance and provides intelligent access control for cloud resources.

Section 3.4: Configure Windows Hello for Business

Purpose

Windows Hello for Business replaces passwords with stronger authentication methods such as biometrics and PINs.

Key Features

- Biometric authentication (fingerprint, facial recognition)
- Device-specific PIN known only to the user and valid only on one device
- Can be used with multi-factor authentication
- Integrated with Microsoft Entra ID for passwordless access to cloud resources

Benefits

- Reduces password-based security risks
- Provides a faster login experience
- Supports modern authentication

Summary: Windows Hello for Business provides secure and user-friendly authentication without traditional passwords.

Section 3.5: Implement and Manage LAPS (Local Administrator Password Solution)

Purpose

Microsoft LAPS secures local administrator passwords by automatically generating, storing, and rotating unique passwords per device.

Key Features

- Automatic password rotation
- Unique password per device
- Secure password storage in Microsoft Entra ID
- Access restricted to authorized IT personnel

Benefits

- Prevents password reuse across devices
- Enhances security by limiting lateral movement

- Simplifies administrative password management

Summary: LAPS ensures each device has a secure, unique, rotating local administrator password.

Section 3.6: Manage Local Group Membership Using Intune

Purpose

Local groups control what users can do on a Windows device. Managing these groups in Intune ensures that only approved users have administrative or special access.

Common Local Groups

Group	Purpose
Administrators	Full control over device settings
Power Users	Elevated permissions with restrictions
Remote Desktop Users	Allowed to connect remotely to device
Guests	Minimal access for temporary users

Management with Intune

- Create configuration profiles to manage membership
- Automatically add or remove users from local groups
- Assign policies to device groups for consistency

Best Practices

- Use least privilege
- Regularly review group membership
- Automate changes through Intune

Summary: Managing local group membership through Intune centralizes control and secures access on Windows devices.

Section 4.1: Choose Between Windows Autopilot and Provisioning Packages

Purpose

Understand the two main deployment methods for Windows devices: **Windows Autopilot** (cloud-based, large scale) and **Provisioning Packages** (offline, customizable).

Windows Autopilot

- Cloud-based deployment managed through Intune.
- Best for large enterprises or remote users.
- Devices configure automatically as soon as they connect to the internet.
- Supports zero-touch setup, automatic enrollment, policy deployment, and easy device resets.

Provisioning Packages

- Configuration files applied directly to devices (often via USB).
- Best for small-scale or offline deployments.
- Ideal when internet access is limited or when you need custom one-time configurations.

Key Decision Factors

- Scale: Autopilot for large-scale; provisioning packages for smaller or offline environments.
- Connectivity: Autopilot requires internet; provisioning packages can be used without it.
- Management: Autopilot integrates with Intune for full lifecycle management.

Summary: Use Autopilot for cloud-first organizations. Use provisioning packages when flexibility or offline deployment is needed.

Section 4.2: Choose a Windows Autopilot Deployment Mode

Deployment Modes

1. **User-Driven Mode**
    - For users setting up their own devices with minimal IT help.
    - Devices configured when user signs in.

2. **Self-Deploying Mode**
    - No user credentials required during setup.
    - Best for kiosks, shared devices, digital signage.
3. **Pre-Provisioning (White Glove) Mode**
    - IT pre-configures devices before handing them to users.
    - Users perform only final sign-in steps.
4. **Windows Autopilot for Pre-Provisioned Deployments**
    - Similar to White Glove but for more complex scenarios.
    - Supports extensive pre-configuration by IT before delivery.

Choosing the Right Mode

- Use **User-Driven** when users can handle setup.
- Use **Self-Deploying** for unattended or shared devices.
- Use **Pre-Provisioning** for pre-configured user-ready experiences.
- Consider configuration complexity when selecting Pre-Provisioned vs standard White Glove.

Section 4.3: Apply a Device Name Template

Purpose

Standardize device names during deployment to improve organization and management.

Benefits

- Enables easy identification by location, user, or department.
- Improves troubleshooting and inventory tracking.
- Ensures naming consistency during Autopilot deployments.

Best Practices

- Keep names short and meaningful.
- Use variables such as %SERIAL%, %USERNAME%, %RAND% for unique identifiers.

- Test templates before production rollout.

Example Template: NYC-%SERIAL% or SALES-%RAND:4%

Section 4.4: Implement Windows Client Device Deployment Using Windows Autopilot

Purpose

Automate deployment of Windows devices through the cloud, enabling remote, zero-touch provisioning.

Key Benefits

- Minimizes IT involvement.
- Ensures consistent policy, security, and app deployment.
- Supports remote workers and distributed teams.
- Integrates with Intune for ongoing management.

Important Considerations

- Requires internet connectivity.
- Deployment profiles must be tested.
- Vendor support can assist with hardware ID registration.

Summary: Autopilot makes large-scale, remote deployment efficient and secure.

Section 4.5: Create an Enrollment Status Page (ESP)

Purpose

Control the user experience during Autopilot deployment and enforce that required apps and policies are installed before allowing access to the desktop.

Benefits

- Displays real-time deployment progress.
- Ensures compliance before device use.
- Prevents incomplete or insecure setups.
- Assists troubleshooting with visible status and error reporting.

Best Practices

- Include only essential apps to avoid delays.
- Communicate expectations to users.
- Set timeouts and monitor performance.

Summary: ESP ensures devices are fully configured and secure before users begin working.

Section 4.6: Plan and Implement Provisioning Packages

Purpose

Configure devices offline using a provisioning file created with the Windows Configuration Designer.

Common Uses

- Offline or low-connectivity environments.
- One-time configuration scenarios.
- Temporary or department-specific setups.

Key Components

- Wi-Fi and network settings
- Security policies
- Applications
- Custom scripts

Benefits

- Fast deployment without internet
- Flexible customization
- Easy distribution using USB or network drives

Best Practices: Test packages, secure sensitive data, document configurations.

Section 4.7: Plan and Implement Device Upgrades for Windows 11

Purpose

Use Intune to upgrade devices to Windows 11 in a controlled and secure manner.

Key Planning Steps

- Assess hardware and application compatibility.
- Pilot test the upgrade.
- Use phased rollout strategies.
- Schedule upgrades during non-business hours.

Benefits of Windows 11

- Enhanced security with TPM and Secure Boot.
- Improved productivity features (Snap Layouts, virtual desktops).
- Modern, consistent user experience.
- Long-term support lifecycle.

Considerations

- Provide user training.
- Monitor upgrade status through Intune.
- Ensure backup plans are in place.

Summary: A strategic Windows 11 upgrade improves security and productivity while maintaining continuity.

Section 4.8: Implement a Windows 365 Cloud PC Deployment

Purpose

Deploy cloud-hosted Windows desktops accessible from any device.

Benefits

- Enables secure remote work.
- Provides a consistent user experience.
- Scalable performance based on user needs.

- Integrated with Intune for management.

Use Cases

- Remote employees
- Temporary/contract workers
- Bring-your-own-device environments

Key Considerations

- Choose appropriate performance tiers.
- Configure Conditional Access and security policies.
- Monitor cost based on licensing and resource use.
- Provide user onboarding instructions.

Summary: Windows 365 Cloud PCs provide flexible, secure, cloud-based desktops for modern workforces.

Section 5.1: Create Device Configuration Profiles for Windows Devices (Including Importing ADMX Files)

Purpose

Create standardized settings for Windows devices using Intune configuration profiles. Importing ADMX files allows you to configure advanced Group Policy-style settings that are not included in Intune by default.

Why It Matters

- Ensures consistent security configuration across all devices.
- Reduces manual setup and risk of misconfiguration.
- ADMX import enables granular control similar to on-premises Group Policy.

Common Settings in Windows Configuration Profiles

1. **Security Policies** – Password complexity, BitLocker encryption, Defender settings.
2. **Wi-Fi Profiles** – Automatically connect devices to corporate Wi-Fi.
3. **Update Policies** – Control Windows Update behavior to maintain security.

4. **Privacy Controls** – Manage telemetry and diagnostic data collection.

Benefits

- Standardization across all Windows devices.
- Advanced customization with ADMX templates.
- Remote deployment and scalability.

Key Considerations

- Test profiles before wide rollout.
- Use clear naming conventions.
- Watch for conflicts between multiple profiles.
- Regularly update ADMX files to align with new policies.

Summary: Configuration profiles create a secure, standardized environment. ADMX files extend Intune's capabilities to include Group Policy-level control.

Section 5.2: Create Device Configuration Profiles for Android Devices

Purpose

Apply consistent settings across Android devices for security, productivity, and compliance.

Common Settings

1. **Password and Security Policies** – Require PIN, biometrics, prevent device wipe.
2. **Wi-Fi Settings** – Automatically configure network access.
3. **VPN Configuration** – Enforce secure access to internal resources.
4. **App Restrictions** – Allow or block applications.
5. **Compliance Rules** – Enforce device encryption, OS version, and health checks.

Benefits

- Protects company data on Android devices.
- Ensures consistent access and user experience.
- Supports both BYOD and fully managed corporate devices.

Considerations

- Always test policies.
- Avoid profile conflicts.
- Use separate profiles for corporate-owned vs BYOD devices.

Summary: Android configuration profiles enforce security and connectivity settings across devices consistently using Intune.

Section 5.3: Create Device Configuration Profiles for iOS Devices

Purpose

Provide secure, consistent configurations for iPhones and iPads using Intune.

Common Settings

1. **Password Requirements** – Enforce strong passcodes or biometrics.
2. **Wi-Fi Profiles** – Preconfigure secure wireless access.
3. **VPN Rules** – Enable secure access to internal systems.
4. **Email and Calendar Auto-Setup** – Ensure productivity from day one.
5. **App Restrictions** – Limit app usage to approved business apps.

Benefits

- Ensures compliance with corporate standards.
- Enables secure remote work.
- Protects sensitive data through encryption and policy enforcement.

Considerations

- Test before deployment.
- Name profiles clearly.
- Avoid conflicting settings across multiple profiles.

Summary: iOS configuration profiles in Intune ensure security, connectivity, and compliance across Apple devices in the organization.

Section 5.4: Create Device Configuration Profiles for macOS Devices

Purpose

Manage Mac computers using standardized policies similar to Windows configuration profiles.

Common macOS Settings

1. **Security Policies** – Password enforcement, screen lock timers.
2. **Wi-Fi and VPN** – Preconfigure secure connectivity.
3. **Application Restrictions** – Allow only approved apps.
4. **FileVault Encryption** – Enforce disk encryption to protect data.

Benefits

- Provides centralized control over Mac environments.
- Protects corporate data.
- Ensures consistent user experience.

Considerations

- Test before wide rollout.
- Keep profiles updated as macOS features evolve.

Summary: Intune profiles for macOS enable centralized, secure management of Apple desktops in enterprise environments.

Section 5.5: Create Device Configuration Profiles for Enterprise Multi-Session Devices

Purpose

Manage virtual environments such as Azure Virtual Desktop (AVD), where multiple users share the same Windows session host.

Common Settings

1. **Session Timeout Policies** – Automatically sign out inactive users.
2. **Application Control** – Limit access to only required applications.
3. **Security Requirements** – Password rules and antivirus enforcement.

4. **User Profile Management** – Optimize storage by deleting inactive profiles.
5. **VPN and Network Access** – Secure remote connections.

Benefits

- Consistent settings for every session.
- Prevents performance issues from user misuse.
- Ensures security across shared environments.

Considerations

- Pilot test in a limited environment.
- Monitor resource usage and adjust policies as necessary.

Summary: Multi-session configuration profiles ensure consistent performance and security across shared cloud or virtual desktops.

Section 5.6: Target a Profile by Using Filters

Purpose

Filters provide granular control over which devices a profile applies to, using criteria such as OS version, device type, or ownership.

When to Use Filters

1. Apply different policies to **corporate vs personal (BYOD)** devices.
2. Target specific **operating systems** (e.g., Windows only).
3. Configure devices based on **hardware model or manufacturer**.
4. Apply special settings to **remote vs on-premises devices**.

Benefits

- Precise targeting without creating many separate groups.
- Reduces policy conflicts.
- Supports complex deployment scenarios with ease.

Considerations

- Always verify filter logic.

- Monitor policy results to ensure devices are correctly targeted.

Summary: Filters allow you to assign configuration profiles based on dynamic device attributes, increasing accuracy and reducing administrative work.

Section 6.1: Configure Endpoint Privilege Management (EPM)

Purpose

Endpoint Privilege Management in Intune allows you to control administrative privileges on devices. Rather than giving users full admin access, EPM lets you grant elevated rights only when needed, reducing risk while maintaining productivity.

Why It Matters

If every user has local admin rights, they can unintentionally install unapproved software, disable security settings, or expose the organization to malware. EPM ensures users have only the permissions required for their role, protecting devices from misuse while still enabling them to perform their work.

Key Components

1. **Just-in-Time Access** – Grants elevation only when required, for a limited period.
2. **Role-Based Access Control (RBAC)** – Assigns privileges based on job role rather than individual users.
3. **Auditing and Logging** – Tracks all elevation activities to maintain accountability.
4. **Approval Workflows** – Requires IT approval before admin rights are granted.

Benefits

- Reduces attack surface
- Supports compliance requirements
- Protects critical system settings
- Allows secure flexibility for advanced users

Important Considerations

- Use least privilege as a guiding principle
- Enable temporary elevation over permanent admin roles

- Monitor audit logs regularly
- Train users on how to request elevation properly

Summary: Endpoint Privilege Management ensures users get only the access they need, when they need it, creating a secure and controlled device environment.

Section 6.2: Manage Applications Using the Enterprise App Catalog

Purpose

The Enterprise App Catalog is a centralized location in Intune that allows organizations to securely distribute and manage applications across devices.

Why It Matters

Without centralized control, users may download unapproved or insecure apps. The Enterprise App Catalog ensures employees only use trusted applications while also making it easy for them to install what they need.

Key Features

1. **Centralized Deployment** – IT can push apps to devices or make them available for self-service installation.
2. **Self-Service Experience** – Users can install approved apps without helpdesk involvement.
3. **Automatic Updates** – Keeps applications current and secure.
4. **Role-Based Access** – Controls app availability based on department or job role.
5. **Version Management** – Supports multiple app versions for pilot groups and phased rollouts.

Benefits

- Enhances productivity by giving users quick access to tools
- Improves security by restricting app choices
- Reduces IT workload
- Ensures version consistency across the organization

Important Considerations

- Keep applications updated
- Use assignments wisely to target the right users
- Monitor usage and remove outdated apps
- Align catalog apps with compliance policies

Summary: The Enterprise App Catalog acts as the organization's secure app store, balancing usability with IT control.

Section 6.3: Implement Microsoft Intune Advanced Analytics

Purpose

Advanced Analytics in Intune provides insights into device health, compliance, and security posture to help IT make informed decisions.

Why It Matters

Without analytics, IT is reactive rather than proactive. Advanced Analytics identifies trends, signals risk, and helps IT optimize performance and security across the device fleet.

Key Capabilities

1. **Device Health Monitoring** – Tracks performance, battery life, and hardware issues.
2. **Security Posture Insights** – Identifies devices that are out of compliance.
3. **Application Usage Reports** – Shows which apps are actively being used.
4. **Compliance and Risk Reporting** – Enables proactive enforcement of policies.
5. **Troubleshooting Tools** – Provides diagnostics to resolve issues faster.

Benefits

- Improves operational efficiency
- Helps allocate resources wisely
- Reduces downtime
- Supports data-driven decision-making

Important Considerations

- Focus on metrics aligned with business needs

- Monitor high-risk devices regularly
- Use analytics to guide policy adjustments
- Ensure compliance with privacy and regulatory requirements

Summary: Intune Advanced Analytics turns raw data into actionable intelligence for better device management and security.

Section 6.4: Configure Microsoft Intune Remote Help

Purpose

Remote Help enables IT to securely assist users in real-time by remotely viewing or controlling their devices, reducing downtime and improving support efficiency.

Why It Matters

With remote work on the rise, IT needs tools to assist users from anywhere. Remote Help enables fast troubleshooting without requiring physical access to devices.

Key Features

1. **Secure Remote Sessions** – Encrypted connections protect data during help sessions.
2. **View or Control Options** – IT can watch or interact with the device.
3. **Session Logging** – Records activity for auditing and compliance.
4. **RBAC Integration** – Limits access to authorized support technicians.
5. **User Consent** – Ensures transparency and privacy.

Benefits

- Increases IT support efficiency
- Improves user experience
- Supports compliance requirements
- Reduces time to resolution

Important Considerations

- Clearly define who has access to Remote Help

- Train both IT and end users
- Monitor session activity logs
- Implement policies to protect sensitive environments

Summary: Remote Help is a secure, cloud-based support tool that empowers IT teams to resolve issues rapidly while maintaining user trust and organizational control.

Section 6.5: Identify Use Cases for Cloud PKI

Purpose

Cloud PKI (Public Key Infrastructure) provides cloud-based management of digital certificates used for encryption, authentication, and secure communications.

Why It Matters

As organizations adopt zero-trust models and remote work, validating device and user identity becomes critical. Cloud PKI enables this without the complexity of on-premises certificate infrastructure.

Common Use Cases

1. **Device Authentication** – Ensures only trusted devices connect to the network.
2. **User Authentication** – Certificate-based authentication replaces passwords.
3. **VPN Access** – Secures VPN connections with certificates rather than credentials.
4. **Email and Document Signing** – Ensures authenticity and integrity of communications.
5. **IoT Device Security** – Protects communication between IoT devices and backend systems.
6. **Data Encryption** – Protects sensitive data in transit and at rest.

Benefits

- Enhances zero-trust security
- Scales easily across global environments
- Simplifies certificate management
- Reduces password dependency

Important Considerations

- Choose a compliant PKI provider
- Monitor certificate expiration and revocation
- Educate users on certificate-based access
- Align certificate policies with business requirements

Summary: Cloud PKI enables secure authentication and encryption across devices, users, and applications, supporting modern cloud-first security strategies.

Section 6.6: Implement Microsoft Tunnel for Mobile Application Management (MAM)

Purpose

Microsoft Tunnel provides a secure VPN connection for mobile applications without requiring full device management. It is designed for BYOD and mobile-first environments.

Why It Matters

Users often access corporate data from personal devices. Microsoft Tunnel ensures only approved apps can securely connect to corporate resources—without IT controlling the entire device.

Key Features

1. **Per-App VPN** – Only managed apps use the secure tunnel.
2. **Data Separation** – Corporate data is isolated from personal data.
3. **Conditional Access Enforcement** – Blocks access from non-compliant devices.
4. **Split Tunneling** – Optimizes performance by routing only corporate traffic through VPN.
5. **Cross-Platform Support** – Works with both iOS and Android.

Benefits

- Supports secure BYOD
- Protects corporate data without invading user privacy
- Reduces attack surface

- Enables secure mobile productivity

Important Considerations

- Clearly communicate privacy protections to users
- Ensure infrastructure can support tunnel capacity
- Use Conditional Access to enforce compliance
- Regularly monitor tunnel usage and performance

Summary: Microsoft Tunnel for MAM delivers secure, app-specific VPN access for mobile devices, supporting modern flexible work while protecting organizational data.

Section 7.1: Sync, Restart, Retire, or Wipe Devices

Purpose

Remote device actions in Intune allow IT to manage devices from anywhere, enforce compliance, troubleshoot issues, and protect corporate data.

Why It Matters

In a modern environment with remote and hybrid users, IT needs the ability to act quickly without physical access to devices. These remote actions ensure security, maintain control, and minimize downtime.

Key Remote Actions

1. Sync

- Forces the device to immediately check in with Intune
- Ensures policies, configuration changes, and app deployments apply without delays

2. Restart

- Remotely reboots a device to resolve performance issues or complete updates
- Reduces the need for user intervention

3. Retire

- Removes corporate data, apps, and profiles while preserving personal data
- Ideal for BYOD or when a user leaves the organization

4. Wipe

- Restores the device to factory settings, erasing all data (corporate and personal)
- Used if a device is lost, stolen, or permanently decommissioned

Real-World Application

If an employee loses their laptop, IT can issue a wipe command to ensure no data is exposed. If a policy update is urgently required, a sync is triggered to apply it immediately.

Key Benefits

- Immediate policy enforcement
- Reduced support time
- Strong data protection
- Seamless user transitions

Important Considerations

- Use *wipe* only when full data erasure is required
- Notify users before triggering restarts or syncs if possible
- Always verify that retired devices lose access to corporate resources
- Document actions for compliance and auditing

Section 7.2: Perform Bulk Remote Actions

Purpose

Bulk actions allow administrators to perform remote management tasks across multiple devices simultaneously.

Why It Matters

Managing devices one by one is time-consuming and inefficient. Bulk actions help ensure consistency and reduce administrative effort, especially in large environments.

Common Bulk Actions

- **Bulk Sync** – Applies policies or app deployments to many devices at once

- **Bulk Restart** – Reboots multiple devices to complete updates or improve performance
- **Bulk Retire** – Removes corporate data from multiple BYOD or offboarded user devices
- **Bulk Wipe** – Factory resets multiple devices (commonly used in device turnover or decommissioning)
- **Bulk Security Updates** – Enforces new policies or security settings across the fleet

Real-World Application

At the end of a school semester, an education institution retires hundreds of student tablets in bulk, removing all school data so they can be reassigned. A bulk sync is also run to apply new profiles for the incoming class.

Benefits

- Saves time and reduces manual effort
- Ensures consistency across devices
- Improves compliance and security responsiveness
- Enables large-scale deployments and transitions smoothly

Important Considerations

- Double-check device selection before running retire or wipe
- Communicate with users to minimize disruptions
- Monitor completion status through the Intune console
- Use dynamic groups and filters for precise targeting

Section 7.3: Update Windows Defender Security Intelligence

Purpose

Windows Defender Security Intelligence provides the latest threat definitions to detect and block malware. Keeping this updated is critical for endpoint protection.

Why It Matters

Cyber threats evolve daily. Outdated threat definitions leave devices exposed to new malware variants, ransomware attacks, and phishing attempts.

Core Components

1. **Threat Definitions** – Identifies known viruses and malware
2. **Cloud-Based Protection** – Delivers real-time threat detection using Microsoft's global intelligence network
3. **Behavioral Monitoring** – Detects suspicious activity even without a known signature
4. **Automatic Sample Submission** – Sends suspicious files to Microsoft for rapid analysis

Benefits

- Provides real-time protection against emerging threats
- Reduces vulnerability windows
- Ensures compliance with security policies
- Centralizes and automates update management through Intune

Important Considerations

- Increase update frequency in high-security environments
- Enable cloud-based protection for zero-day threat coverage
- Use Intune reports to verify update compliance
- Ensure devices stay online to receive frequent updates

Section 7.4: Rotate BitLocker Recovery Keys

Purpose

Rotating BitLocker recovery keys is a proactive security measure to protect encrypted devices from unauthorized access.

Why It Matters

If a recovery key becomes known or exposed, the encrypted drive can be unlocked. Key rotation ensures that only the most recent key is valid.

Key Benefits

- Protects against compromised credentials
- Meets compliance standards requiring periodic encryption key changes
- Allows secure remote rotation via Intune
- Enhances protection in lost or stolen device scenarios

Real-World Example

A company suspects that a former contractor may have recorded a BitLocker recovery key. IT rotates the keys across all contractor devices using Intune to ensure previous keys can no longer be used.

Important Considerations

- Ensure rotated keys sync successfully back to Intune
- Notify users if recovery prompts may occur
- Audit key rotation as part of compliance requirements

Section 7.5: Run a Device Query Using KQL (Kusto Query Language)

Purpose

KQL queries allow administrators to extract device information, detect compliance issues, and analyze the status of devices managed through Intune.

Why It Matters

Standard reports sometimes lack granularity. KQL provides deep visibility into device health, software versions, security posture, and policy compliance.

Common Use Cases

- Identify devices missing a critical update
- Check compliance status across a department
- Generate software inventory reports
- Discover devices with failed deployments
- Monitor security vulnerabilities

Benefits

- Enables proactive device management
- Supports audit and compliance requirements
- Reduces troubleshooting time by isolating issues quickly
- Enhances decision-making with real-time insights

Real-World Example

Before a cybersecurity audit, IT uses a KQL query to identify all devices missing encryption or antivirus coverage and quickly addresses the gaps before the inspection.

Section 8.1: Prepare Applications for Deployment by Using Intune

Purpose

Preparing applications ensures they install correctly, meet organizational requirements, and provide a consistent user experience.

Why Preparation Matters

Without proper preparation, applications may fail to install or cause compatibility or security issues. Preparation allows IT to define installation behavior, configure prerequisites, and test compatibility before deployment.

Key Benefits

1. Reduced deployment failures
2. Streamlined app management using structured packaging
3. Targeted delivery to specific users or device groups
4. Improved user experience with minimal post-deployment troubleshooting

Real-World Application

An organization packages a Win32 app using the Microsoft Win32 Content Prep Tool, defines device requirements, creates custom install and uninstall commands, and sets detection rules to verify successful installation. This preparation prevents faulty installs and ensures only supported devices receive the app.

Important Considerations

- Always test the application in a pilot group
- Use detection rules to avoid duplicate installations
- Document installation commands for future maintenance
- Monitor post-deployment logs to verify success

Conclusion

Preparation is essential for a seamless deployment experience. Proper planning reduces IT workload and ensures apps deploy successfully and consistently across managed devices.

Section 8.2: Deploy Apps by Using Intune

Purpose

App deployment with Intune enables centralized, remote installation across Windows, Android, iOS, and macOS devices.

Why It Matters

Without centralized deployment, IT would manually install apps on each device, which is inefficient and error-prone. Intune automates this process and ensures consistency.

Key Benefits

1. Consistent app versions across all devices
2. Improved security through controlled deployment
3. Time savings with remote, automated delivery
4. Flexibility through required or available app assignments

Real-World Application

An organization schedules deployment of a secure collaboration app outside working hours using Intune. Devices receive the app automatically, and IT monitors installation results through the console to ensure compliance.

Important Considerations

- Use groups to target only relevant users
- Monitor deployment status and resolve failures

- Plan for app updates and maintenance
- Provide instructions to users for installing available apps

Conclusion

Intune simplifies app deployment, allowing IT to control distribution, ensure compliance, and support productivity across all devices.

Section 8.3: Deploy Microsoft 365 Apps by Using Intune

Purpose

Deploying Microsoft 365 apps through Intune ensures users have access to essential productivity tools like Word, Outlook, and Teams.

Why It Matters

Manual deployment leads to inconsistent versions and increased IT workload. Automated deployment ensures every user receives the latest version with secure and compliant configurations.

Key Benefits

1. Centralized configuration and control
2. Automatic updates with version management
3. Consistent user experience
4. Improved security and compliance

Real-World Application

An organization deploys Microsoft 365 apps through Intune across all corporate laptops, ensuring each user receives the same configuration and enabling automatic updates via the Monthly Enterprise Channel.

Conclusion

Deploying Microsoft 365 apps using Intune delivers a consistent, secure, and managed experience, reducing IT effort and improving user productivity.

Section 8.4: Configure Policies for Office Apps

Purpose

Policies control how Microsoft Office apps behave, ensuring data is protected and the user experience is consistent.

Why It Matters

Office apps often handle sensitive data. Policies help enforce security controls, limit risky actions, and standardize app behavior across devices.

Key Policy Categories

1. Security and privacy controls
2. File storage restrictions
3. User interface customization
4. Automatic updates
5. Add-in management

Real-World Application

A law firm configures policies that disable macros and restrict file saving to OneDrive for Business, ensuring secure storage and preventing malware attacks.

Conclusion

By configuring Office app policies through Intune, IT can enforce compliance, improve security, and deliver a consistent user experience.

Section 8.5: Deploy Microsoft 365 Apps as Part of a Windows Autopilot Deployment (Using ODT or OCT)

Purpose

Combining Microsoft 365 app deployment with Windows Autopilot enables devices to be provisioned with productivity apps during initial setup.

Why It Matters

Employees receive fully configured devices on first login without IT involvement, accelerating onboarding and maintaining configuration consistency.

Key Tools

- **Office Deployment Tool (ODT):** Used to create detailed XML files that control app configuration
- **Office Customization Tool (OCT):** A web interface for customizing and generating configuration files

Key Benefits

1. Streamlined provisioning process
2. Automated app installation during device setup
3. Standardized configurations across new devices
4. Reduced IT workload

Real-World Application

New hires receive laptops provisioned with Autopilot. During setup, Microsoft 365 apps are automatically installed based on the OCT configuration, enabling productivity immediately upon sign-in.

Conclusion

Using ODT or OCT with Windows Autopilot accelerates device readiness and ensures consistent application deployment organization-wide.

Section 8.6: Manage Microsoft 365 Apps by Using the Microsoft 365 Apps Admin Center

Purpose

The Apps Admin Center provides centralized management of Microsoft 365 apps, including updates, health monitoring, and usage analytics.

Why It Matters

Without centralized management, devices may become outdated or misconfigured, leading to security and compatibility risks.

Key Capabilities

1. Update channel control
2. Device inventory and app health insights

3. Application configuration policies
4. Security and compliance monitoring
5. Usage analytics for license optimization

Real-World Application

An organization uses deployment rings to test Office updates with a pilot group before broader rollout, ensuring application stability and reducing disruption.

Conclusion

The Apps Admin Center allows IT to manage app lifecycle, enforce standards, and optimize licensing from a single, centralized interface.

Section 8.7: Deploy Apps from Platform-Specific App Stores by Using Intune

Purpose

Deploying apps directly from official app stores ensures security, compatibility, and ease of access on all supported platforms.

Why It Matters

Store apps are vetted, automatically updated, and optimized for their respective platforms, reducing risk and management overhead.

Key Benefits

1. Simplified deployment through a single console
2. Automatic updates through the app store
3. Improved security with vetted applications
4. Unified user experience across platforms

Real-World Application

A field services organization deploys apps from the Microsoft Store, Google Play, and Apple App Store using Intune. This ensures employees receive trusted, automatically updated apps on Windows, Android, and iOS devices.

Conclusion

Deploying store-based apps with Intune streamlines cross-platform management while improving security and user experience.

Section 9.1: Plan and Implement App Protection Policies

Purpose

App protection policies secure corporate data within applications, especially in environments where users access organizational data from personal (BYOD) devices.

Why App Protection Policies Matter

Without app protection, corporate data could be saved to unapproved locations, shared through unsecured apps, or accessed if a device is lost or compromised. App protection policies apply controls directly to applications rather than the entire device, making them ideal for securing data while preserving user privacy.

Key Components

1. **Data Relocation Controls**
   Restrict data transfer to only managed apps or storage locations.
   Example: Allow Outlook to share data only with Teams or OneDrive.
2. **Access Requirements**
   Require app-level authentication such as a PIN or biometric sign-in.
   Example: Enforce a PIN when opening corporate apps on mobile devices.
3. **Data Encryption**
   Encrypt data saved within managed applications to prevent unauthorized access.
4. **Selective Wipe**
   Remove only corporate data from devices while preserving personal content.
5. **Conditional Access Integration**
   Combine with policies that require devices to meet compliance standards before accessing corporate apps.

Real-World Example

A consultant accesses Outlook and Teams from a personal phone. App protection policies encrypt corporate data, require PIN authentication, and restrict data sharing to only approved apps. When the consultant leaves the company, the corporate data is selectively wiped from the device without affecting personal data.

Conclusion

App protection policies offer strong security for both managed and unmanaged devices by securing data at the application level. They enable organizations to support BYOD while maintaining control over corporate information.

Section 9.2: Implement Conditional Access Policies for App Protection Policies

Purpose

Conditional access policies ensure that only trusted users and secure devices are allowed to access corporate apps and data. When paired with app protection policies, they create a layered defense system.

Why Conditional Access Is Important

While app protection controls data within the app, conditional access prevents unauthorized or high-risk access before it happens. It enforces requirements such as device compliance, MFA, or geographic restrictions before granting access.

Key Components

1. **Device Compliance Requirements**
   Ensure only compliant devices (encrypted, up-to-date, and secured) are allowed access.
2. **User and Group Targeting**
   Apply different policies to departments based on their role and data sensitivity.
3. **Location-Based Restrictions**
   Limit access from high-risk geographic regions.
4. **Risk-Based Sign-In**
   Evaluate login attempts and apply MFA for risky sign-ins.
5. **Access Controls**
   Decide whether to allow, block, or require remediation steps before granting access.

Real-World Example

A financial institution creates a conditional access policy that only allows employees with compliant devices to access Outlook. If a user signs in from an unknown location, MFA is required. Access is blocked entirely if the device does not meet compliance standards.

Conclusion

Conditional access combined with app protection ensures that data is protected both at the point of access and within applications. This layered approach greatly reduces unauthorized access risks.

Section 9.3: Plan and Implement App Configuration Policies for Managed Apps and Managed Devices

Purpose

App configuration policies pre-configure applications with required settings, ensuring that apps function consistently and securely without requiring user setup.

Why App Configuration Is Necessary

Without configuration policies, each user might configure apps differently—or incorrectly—leading to data leaks, compliance failures, or poor user experience. App configuration automates setup, enforces security, and improves productivity.

Key Components

1. **Pre-Configured App Settings**
   Automatically apply default server addresses or sign-in preferences.
2. **Security and Data Controls**
   Prevent data sharing with unmanaged applications or storage.
3. **Interface Customization**
   Simplify the application interface by hiding unnecessary features.
4. **Compliance and Monitoring Settings**
   Enforce settings that support auditing, reporting, or regulatory requirements.
5. **Conditional Access Integration**
   Ensure apps check device compliance before allowing access.

Real-World Example

A healthcare provider deploys Microsoft Teams with app configuration policies that disable external chat, enforce encryption, and preconfigure logging for compliance. All new users receive the same secure and compliant Teams setup automatically.

Conclusion

App configuration policies standardize how apps behave across users and devices, improving both security and the user experience. They eliminate setup errors, enforce policy compliance, and support rapid onboarding.

Section 10.1: Create Antivirus Policies

Purpose

Antivirus policies in Microsoft Intune enforce protection across all managed devices to defend against malware, ransomware, and other cyber threats.

Why Antivirus Policies Matter

Without centralized antivirus management, devices may run outdated or inconsistent protection, increasing risk of data breaches. Antivirus policies ensure real-time scanning, automated updates, and standardized configurations throughout the organization.

Key Components

1. **Real-Time Protection** – Continuously scans files and processes to block threats as they occur.
2. **Scheduled Scans** – Ensures recurring malware checks across all devices.
3. **Cloud-Delivered Protection** – Uses Microsoft's threat intelligence to detect emerging threats quickly.
4. **Automatic Sample Submission** – Sends suspicious files to Microsoft for analysis.
5. **Exclusions** – Allows critical or trusted applications to bypass scans to avoid disruption.

Real-World Example

A financial firm enables real-time protection and weekly scans, while excluding folders used by secure financial applications to ensure uninterrupted workflows.

Key Benefits

- Consistent protection across all devices
- Latest threat intelligence through cloud services
- Reduced manual management
- Targeted deployment by device group

Important Considerations

- Balance scan frequency with performance needs
- Review threat and compliance reports regularly
- Use exclusions cautiously
- Inform users about scheduled scans

Conclusion

Creating antivirus policies in Intune ensures every device remains protected with the latest security standards, reinforcing an organization-wide defense against cyber threats.

Section 10.2: Create Disk Encryption Policies

Purpose

Disk encryption policies protect data at rest by encrypting device storage, ensuring that data cannot be accessed if a device is lost or stolen.

Why Disk Encryption Matters

Without encryption, sensitive information stored on devices is vulnerable to unauthorized access. Intune disk encryption policies automate encryption deployment using BitLocker for Windows and FileVault for macOS.

Key Components

1. **Encryption Method Selection** – Choose between XTS-AES 128-bit or 256-bit.
2. **BitLocker/FileVault Configuration** – Automates encryption activation.
3. **Startup Authentication** – Adds PINs or passwords for additional protection.
4. **Recovery Key Management** – Secures recovery keys in Entra ID.
5. **Compliance Monitoring** – Ensures devices remain encrypted and report status to Intune.

Real-World Example

A healthcare organization enables BitLocker with 256-bit encryption and stores recovery keys in Entra ID to protect patient data and meet regulatory requirements.

Key Benefits

- Strong protection of data at rest
- Automated compliance enforcement
- Secure key management
- Support for regulatory mandates

Important Considerations

- Prioritize stronger encryption for sensitive departments
- Treat recovery keys as critical security assets
- Balance security with user experience
- Monitor policy compliance consistently

Conclusion

Disk encryption policies in Intune are foundational for data protection and regulatory compliance, ensuring that sensitive information remains secure even when devices are compromised.

Section 10.3: Create Firewall Policies

Purpose

Firewall policies protect devices by controlling network traffic and blocking unauthorized access attempts.

Why Firewall Policies Matter

Devices frequently connect to public or unsecured networks. Firewall policies enforce protective barriers that prevent malicious network traffic from reaching the device.

Key Components

1. **Inbound and Outbound Rules** – Control allowed and blocked network traffic.
2. **Port and Protocol Restrictions** – Limit exposure by blocking unused or vulnerable ports.
3. **Application Rules** – Allow or deny connectivity for specific applications.
4. **Domain/IP Filtering** – Restrict access to approved network locations.

5. **Logging** – Monitor network traffic for suspicious activity.

Real-World Example

A legal firm blocks traffic from public networks and restricts access to only approved IP addresses when users work remotely.

Key Benefits

- Consistent network protection
- Reduced exposure to attacks
- Application-level control
- Visibility through logs and reports

Important Considerations

- Customize by department needs
- Balance security with accessibility
- Regularly review firewall logs
- Educate users on access limitations

Conclusion

Firewall policies in Intune provide a strong first line of network defense, ensuring devices remain protected against unauthorized access regardless of location.

Section 10.4: Configure Attack Surface Reduction (ASR) Policies

Purpose

Attack Surface Reduction policies proactively block behaviors commonly exploited by malware.

Why ASR Policies Matter

Common tools like Office macros and scripts are frequently used to launch attacks. ASR policies reduce these risks by blocking suspicious actions before they cause harm.

Key Components

1. **Block Office Apps from Creating Child Processes**

2. **Block Executables in Email and Webmail**
3. **Block Untrusted or Unsigned Applications**
4. **Controlled Folder Access** to prevent ransomware attacks
5. **Script Blocking** for JavaScript and VBScript
6. **Credential Theft Protection**

Real-World Example

A bank uses ASR to block macros from launching PowerShell and restrict access to protected folders, stopping ransomware attempts.

Key Benefits

- Proactive threat prevention
- Minimizes malware entry points
- Protects sensitive folders from unauthorized access
- Hardens the environment against phishing and fileless attacks

Important Considerations

- Test in audit mode before enforcement
- Apply varying policies based on department risk
- Monitor alerts and adjust settings as needed

Conclusion

ASR policies significantly reduce the attack surface by restricting high-risk behaviors, providing proactive and targeted protection against emerging threats.

Section 10.5: Plan and Implement Security Baselines

Purpose

Security baselines provide pre-configured security settings based on best practices and industry standards.

Why Security Baselines Matter

Without standardized settings, devices may become misconfigured or vulnerable. Security baselines ensure all devices meet a minimum level of protection.

Key Components

1. **Baseline Templates** from Microsoft
2. **Configuration Profiles** enforcing key settings
3. **Device Compliance Policies**
4. **Group Assignments** for different departments
5. **Monitoring and Reporting Tools**

Real-World Example

A healthcare provider applies the Windows security baseline to all administrative staff devices, enforcing encryption, passwords, and automatic updates for compliance.

Key Benefits

- Fast deployment of best practices
- Consistent security across the organization
- Easier regulatory compliance
- Centralized monitoring

Important Considerations

- Customize baselines for organizational needs
- Test before full rollout
- Keep baselines updated over time
- Communicate changes to users

Conclusion

Security baselines simplify security management, ensure consistent protection, and reduce configuration errors through automated, policy-driven enforcement.

Section 10.6: Integrate Intune with Microsoft Defender for Endpoint

Purpose

Integration combines Intune's management capabilities with Defender's advanced threat detection and response.

Why Integration Matters

On its own, Intune manages device compliance, while Defender identifies active threats. Together, they enable automated remediation and conditional access based on threat level.

Key Components

1. **Threat-Based Compliance Policies**
2. **Real-Time Monitoring**
3. **Automated Remediation**
4. **Threat Analytics**
5. **Conditional Access Integration**

Real-World Example

When Defender flags a device as high-risk, Intune automatically marks it non-compliant and restricts access until remediation is complete.

Key Benefits

- Unified management and security
- Automated response to threats
- Reduced exposure window
- Enhanced visibility and reporting

Important Considerations

- Define acceptable risk levels
- Monitor remediation logs
- Educate users on restricted access
- Review threat analytics regularly

Conclusion

Integrating Intune with Defender for Endpoint creates an intelligent, automated security ecosystem capable of detecting, isolating, and remediating threats in real time.

Section 10.7: Onboard Devices into Microsoft Defender for Endpoint

Purpose

Onboarding brings devices under Defender's protection for real-time monitoring, threat detection, and incident response.

Why Onboarding Matters

Devices not onboarded into Defender remain unmonitored and vulnerable. Onboarding ensures visibility, centralized control, and automated threat response.

Key Components

1. **Device Enrollment** into Defender
2. **Security Configuration Settings**
3. **Endpoint Detection and Response (EDR)**
4. **Compliance and Conditional Access Integration**
5. **Automated Remediation**

Real-World Example

A retail company enrolls all Windows devices into Defender via Intune. When malware is detected, Defender automatically quarantines it and notifies IT.

Key Benefits

- Enhanced threat visibility
- Centralized security telemetry
- Automated response to attacks
- Enforcement of compliance at the device level

Important Considerations

- Confirm compatibility before enrollment
- Monitor compliance status regularly

- Inform users of onboarding requirements
- Use reporting to identify risks

Conclusion

Onboarding devices into Defender for Endpoint is essential for enabling continuous threat monitoring, automated remediation, and strong endpoint protection across the organization.

Section 11.1: Plan for Device Updates

Purpose

Planning device updates ensures all managed devices receive the latest features, performance improvements, and security patches in a controlled, efficient manner.

Why This Matters

Without a structured update strategy, devices may fall behind on critical patches, leading to security risks, incompatibility issues, and unpredictable performance. A proactive update plan ensures consistency, compliance, and minimal disruption to users.

Key Components

1. **Update Frequency** – Determines how often updates are checked and installed.
2. **Device Group Targeting** – Enables phased deployment based on department, role, or risk level.
3. **Update Rings and Channels** – Controls who receives updates first and allows staged testing.
4. **User Notification and Scheduling** – Helps minimize disruption by allowing users to schedule installations.
5. **Monitoring and Compliance Reporting** – Tracks the update status of devices to identify non-compliance.

Real-World Example

An organization deploys critical updates first to executive devices, followed by IT pilot groups, and then the general workforce. This staged approach allows testing before large-scale rollout, minimizing risk.

Benefits

- Improved security posture
- Reduced update-related downtime
- Streamlined management
- Consistent user experience

Important Considerations

- Balance security requirements with user productivity.
- Monitor devices that miss update deadlines.
- Communicate update expectations clearly to end users.

Conclusion

Effective update planning ensures devices remain secure and reliable while minimizing disruption. Intune provides the tools necessary to automate, monitor, and control this process with precision.

Section 11.2: Create and Manage Update Rings Using Intune

Purpose

Update rings allow staged deployment of Windows updates to manage risk, test compatibility, and control update timing.

Why Update Rings Matter

Staged deployment helps organizations avoid widespread issues that may result from deploying untested updates to all users at once.

Key Components

1. **Active Hours** – Prevents automatic restarts during working hours.
2. **Automatic Update Behavior** – Determines how and when updates install.
3. **Deferral Periods** – Delays feature or quality updates for controlled rollout.
4. **Update Channels** – Assign devices to specific service channels (e.g., Pilot vs Broad).

5. **User Notifications** – Notifies users of required restarts or upcoming installations.

Real-World Example

A tech company sets a Pilot ring for a test group, a Broad ring for the majority of employees, and a Critical ring with stricter enforcement for devices handling sensitive data.

Benefits

- Reduced risk during update deployment
- Controlled rollout with early testing
- Improved reliability and user satisfaction
- Enhanced compliance monitoring

Important Considerations

- Test in the Pilot ring before broad deployment.
- Monitor update behavior and user feedback.
- Adjust rings based on update performance data.

Conclusion

Update rings provide a strategic approach to deploying Windows updates, allowing organizations to control timing, test compatibility, and manage risk effectively.

Section 11.3: Create and Manage Update Policies Using Intune

Purpose

Update policies define how updates are handled across Windows, macOS, and mobile operating systems to ensure consistency and compliance.

Why Update Policies Matter

Devices left unmanaged may miss critical patches, introducing vulnerabilities. Update policies enforce standardized OS update behavior across the environment.

Key Components

1. **Update Timing and Scheduling** – Reduces disruption by setting installation windows.

2. **OS Version Control** – Ensures compatibility and stability by controlling version levels.
3. **Automatic vs Manual Updates** – Defines the degree of user control.
4. **Device Targeting** – Applies policies based on device roles or departments.
5. **User Notifications** – Keeps users informed of upcoming changes and restarts.

Real-World Example

A retail company enforces automatic overnight updates for macOS and Windows devices, while allowing manual updates for executive devices that require flexibility.

Benefits

- Improved security compliance
- Reduced IT workload through automation
- Enhanced user experience
- Standardized update management across platforms

Important Considerations

- Test policies with a pilot group.
- Balance enforcement with flexibility.
- Monitor compliance reports regularly.

Conclusion

Update policies in Intune offer a unified solution to keep devices across operating systems secure, compliant, and consistently updated.

Section 11.4: Manage Android Updates Using Configuration Profiles or FOTA Deployments

Purpose

This section outlines how to control Android OS updates using Intune through configuration profiles or Firmware-Over-The-Air (FOTA) deployments.

Why It Matters

Without centralized control, Android devices may run outdated versions, creating vulnerabilities and inconsistent user experiences.

Key Components

1. **Configuration Profiles** – Enable automatic system updates and define update settings.
2. **FOTA Deployments** – Leverages manufacturer integration to push firmware updates.
3. **Scheduling Controls** – Ensures updates occur during non-working hours.
4. **Device Group Targeting** – Allows different update strategies for various roles or departments.
5. **Monitoring and Compliance Reporting** – Tracks whether devices are updated successfully.

Real-World Example

A healthcare provider uses FOTA to push urgent firmware updates to Android tablets used in patient care, ensuring full compliance with data protection regulations.

Benefits

- Consistent update experience across Android fleet
- Reduced security risk
- Automated, remote delivery of updates
- Improved regulatory compliance

Important Considerations

- Confirm device compatibility with FOTA.
- Schedule updates to minimize disruption.
- Monitor devices that fall behind on updates.

Conclusion

Managing Android updates through Intune ensures that all devices remain secure, optimized, and compliant using automation and centralized control.

Section 11.5: Configure Windows Client Delivery Optimization Using Intune

Purpose

Delivery Optimization improves update efficiency by enabling peer-to-peer content sharing, reducing bandwidth consumption.

Why It Matters

Large scale update deployments can overwhelm network resources. Delivery Optimization minimizes internet usage and speeds up distribution.

Key Components

1. **Download Mode** – Determines whether devices use Microsoft's CDN or peer devices.
2. **Bandwidth Limits** – Controls network impact during business hours.
3. **Cache Size and Retention** – Manages local storage used for shared content.
4. **Peer Grouping** – Defines how devices discover each other to share content.
5. **Monitoring Tools** – Provides visibility into bandwidth savings and performance.

Real-World Example

A retail chain enables peer sharing in each store. Devices share updates locally, reducing the amount of data downloaded from the cloud.

Benefits

- Significant bandwidth reduction
- Faster update delivery
- Optimized use of local networks
- Centralized management and monitoring

Important Considerations

- Group devices appropriately for peer sharing.
- Monitor cache usage.
- Configure bandwidth limits during peak hours.

Conclusion

Delivery Optimization is a cost-effective strategy that accelerates update delivery while reducing network impact across Windows client devices.

Section 11.6: Monitor Updates

Purpose

Monitoring updates allows IT to verify that devices are receiving and installing updates according to policy.

Why It Matters

Incomplete or failed updates can leave devices vulnerable. Ongoing monitoring ensures compliance and allows proactive remediation.

Key Components

1. **Update Compliance Reports** – Summarize update status across devices.
2. **Device Update Status** – Provides detailed insight per device.
3. **Policy Compliance Tracking** – Ensures adherence to assigned update rings and policies.
4. **Alerts and Notifications** – Notify IT when devices fall out of compliance.
5. **Troubleshooting Tools** – Help quickly resolve update failures.

Real-World Example

A hospital's IT department monitors update compliance daily and receives alerts when devices miss critical patches, allowing immediate remediation to maintain regulatory compliance.

Benefits

- Stronger security posture
- Automatic identification of non-compliant devices
- Faster troubleshooting
- Improved reporting for audits and regulation

Important Considerations

- Set compliance thresholds.

- Review reports regularly.
- Adjust update strategies based on trends.
- Use alerts proactively to reduce exposure.

Conclusion

Monitoring device updates is critical for ensuring ongoing security and compliance. Intune's reporting and alerting features provide full visibility and control across all managed devices.

Acronyms of Note

- **AD (Active Directory)**: A Microsoft directory service for managing users, devices, and resources on a network, supporting authentication and authorization.
- **ADMX (Administrative Template XML)**: A file format used to define group policy settings, often imported into Intune to configure device policies.
- **ASR (Attack Surface Reduction)**: Security policies in Microsoft Defender that reduce the attack surface by restricting risky behaviors on devices.
- **AVD (Azure Virtual Desktop)**: A cloud-based service providing virtual desktops and applications, allowing remote access from various devices.
- **BYOD (Bring Your Own Device)**: A policy allowing employees to use their personal devices for work purposes, often managed with app and data protection policies.
- **CA (Conditional Access)**: Policies that restrict access to resources based on conditions like user location, device compliance, and risk level.
- **CCNA (Cisco Certified Network Associate)**: An entry-level certification by Cisco, validating skills in networking and IT infrastructure.
- **CNAME (Canonical Name Record)**: A DNS record that maps one domain name to another, useful in web and email configurations.
- **DAG (Database Availability Group)**: A feature in Exchange Server that provides high availability and disaster recovery for Exchange databases.
- **DEM (Device Enrollment Manager)**: A role in Intune that allows an account to enroll multiple devices, typically used for shared or kiosk devices.

- **DNS (Domain Name System)**: The system that translates domain names into IP addresses, allowing users to access websites by entering URLs.
- **ESP (Enrollment Status Page)**: A page displayed during Windows Autopilot setup, tracking the progress of device configurations and policies.
- **FOTA (Firmware-Over-The-Air)**: Technology that allows firmware updates to be deployed remotely, keeping devices secure and up-to-date.
- **GPO (Group Policy Object)**: A feature in Windows that controls user and computer settings across a network, managed through Active Directory.
- **IAM (Identity and Access Management)**: A framework of policies and technologies for managing user identities and access to resources.
- **KQL (Kusto Query Language)**: A query language used to analyze large datasets in Microsoft services, particularly useful for troubleshooting and reporting.
- **LAPS (Local Administrator Password Solution)**: A tool that manages and rotates passwords for local administrator accounts on Windows devices to improve security.
- **MAM (Mobile Application Management)**: Policies that control data and security within specific apps on mobile devices, without requiring full device management.
- **MDM (Mobile Device Management)**: A solution that allows IT administrators to manage, configure, and secure mobile devices remotely.
- **MDT (Microsoft Deployment Toolkit)**: A free Microsoft tool that automates the deployment of Windows operating systems, often used in conjunction with SCCM.
- **NTP (Network Time Protocol)**: A protocol that synchronizes the clocks of computers to a standard time source, critical for network security and operation.
- **ODT (Office Deployment Tool)**: A tool that helps IT professionals deploy Microsoft Office apps with customized configurations.
- **OS (Operating System)**: Software that manages computer hardware and software resources and provides common services for computer programs.
- **PKI (Public Key Infrastructure)**: A framework that enables secure communication and data exchange by managing digital certificates and encryption keys.

- **SCCM (System Center Configuration Manager)**: A Microsoft solution for managing large groups of Windows computers, including software distribution and patch management.
- **SID (Security Identifier)**: A unique identifier assigned to each user, group, and computer in a Windows environment for security purposes.
- **SMS MFA (Short Message Service Multi-Factor Authentication)**: A form of two-factor authentication that uses text messages to provide a second layer of security.
- **SPF (Sender Policy Framework)**: An email authentication method that helps prevent spoofing by verifying sender IP addresses.
- **SSO (Single Sign-On)**: A system that allows users to log in once and gain access to multiple applications without re-authenticating.
- **TLS (Transport Layer Security)**: A protocol that secures communications over a network, often used in email and web applications.
- **UPN (User Principal Name)**: The format for user logins in Microsoft Entra ID (formerly Azure AD), typically in the form of an email address.
- **URL (Uniform Resource Locator)**: The address used to access resources on the internet, such as websites.
- **VPN (Virtual Private Network)**: A tool that creates a secure connection to a network over the internet, protecting data and user privacy.
- **WDS (Windows Deployment Services)**: A Microsoft tool for network-based installation of Windows operating systems.
- **WIP (Windows Information Protection)**: A feature in Intune that helps separate and protect work and personal data on Windows devices.
- **WSUS (Windows Server Update Services)**: A Microsoft tool that manages and distributes software updates to computers in a corporate environment.

Glossary of Terms

- **Active Directory (AD)**: Microsoft's directory service for managing users, devices, and resources on a network. AD supports authentication, authorization, and group policies.
- **ADMX (Administrative Template XML)**: A file format used to define group policy settings for Windows. ADMX files are often imported into Intune for configuring device policies.
- **App Configuration Policy**: A set of rules used to manage app settings and configurations on managed devices to enhance productivity and security by pre-setting configurations for users.
- **App Protection Policy**: Policies designed to secure corporate data within applications, particularly on personal or unmanaged devices. These policies control how data is accessed, shared, and stored within specific applications.
- **Attack Surface Reduction (ASR)**: A set of security policies in Microsoft Defender for Endpoint designed to reduce the attack surface on devices by restricting certain behaviors.
- **Autopilot**: A deployment technology used to preconfigure new devices, allowing IT to customize devices with settings, apps, and policies before delivering them to users.
- **Azure Virtual Desktop (AVD)**: A cloud-based service by Microsoft that provides virtual desktops and applications hosted on Azure, accessible from various devices.
- **BitLocker Key Rotation**: A process of renewing the encryption key for BitLocker-protected drives, which helps prevent unauthorized access in case of compromised keys.
- **Cloud PKI (Public Key Infrastructure)**: A cloud-based system for managing digital certificates and cryptographic keys, supporting secure access and data protection.
- **Compliance Policy**: A set of Intune rules that define conditions for devices to access organizational resources, ensuring security and regulatory compliance.
- **Conditional Access**: A security feature that enforces access policies based on a user's identity, device compliance, and risk, determining access based on who, what device, and under what conditions users connect to resources.

- **Corporate-Owned Device**: Devices purchased and managed by an organization, configured with security and usage policies for business purposes.
- **Delivery Optimization**: A feature that manages bandwidth use during updates by allowing devices on the same network to share downloaded content, reducing redundant downloads.
- **Device Compliance Status**: The status assigned to a device based on its adherence to the compliance policies set by an organization. Devices can be compliant, non-compliant, or not evaluated.
- **Device Query Language (KQL)**: A query language used to retrieve and analyze data in Microsoft services, including Intune, helping administrators filter, sort, and analyze data for reporting and troubleshooting.
- **Device Restriction Profile**: Configuration settings in Intune used to restrict specific device functions or behaviors, such as camera access or app installations.
- **Enrollment Profile**: A profile in Intune used for enrolling devices with specific configurations, such as fully managed, corporate-owned, or work profile setups.
- **Enterprise App Catalog**: A feature in Intune that provides a catalog of approved applications for users, allowing IT to manage app deployment and updates.
- **Endpoint Analytics**: A tool in Microsoft Intune that provides insights on device performance, software use, and potential configuration issues, helping organizations optimize device health and user experience.
- **Endpoint Privilege Management**: A feature in Intune that allows organizations to manage and control privileged access on endpoints, reducing risks from excessive permissions.
- **ESP (Enrollment Status Page)**: A screen displayed during Windows Autopilot enrollment, tracking progress as configurations, apps, and policies are applied to the device.
- **FOTA (Firmware-Over-The-Air)**: Technology that allows firmware updates to be deployed remotely to devices, ensuring they remain secure and up-to-date without manual intervention.
- **Group Policy**: A feature in Windows that allows IT administrators to control user and computer settings within an Active Directory environment.

- **Just-in-Time Access**: A security measure that grants temporary administrative privileges to users, enabling them to perform specific tasks with controlled access, enhancing security by reducing permanent admin rights.
- **Kusto Query Language (KQL)**: A read-only request language used for querying large datasets in Microsoft services like Intune. KQL supports detailed queries to filter and analyze data for reporting.
- **Local Admin Account**: A user account on a Windows device with full administrative privileges, typically managed for security through solutions like LAPS.
- **LAPS (Local Administrative Password Solution)**: A tool that manages and rotates passwords for local administrator accounts on Windows devices, enhancing security.
- **Managed App**: Applications configured through Intune with security policies to control access and data handling, ensuring compliance with corporate standards.
- **Microsoft Intune Suite**: A collection of advanced device management tools and capabilities in Intune, offering features like Endpoint Privilege Management and analytics.
- **Mobile Application Management (MAM)**: Policies applied to apps on mobile devices to control access and security, even on devices not enrolled in Intune.
- **Multi-Session Device**: A device or virtual machine in Windows that allows multiple users to sign in simultaneously, commonly used in virtual desktop environments like AVD.
- **Patch Compliance**: The level to which devices meet an organization's patching policies, ensuring they have the latest security updates and reducing vulnerabilities.
- **Pilot Ring**: A testing group within an update ring where updates are deployed first, allowing IT to identify any issues before rolling updates out to all users.
- **Remote Help**: An Intune feature that enables IT support to provide remote assistance to end-users on managed devices, enhancing troubleshooting and support capabilities.
- **Security Baseline**: A predefined set of security policies from Microsoft that can be deployed via Intune, ensuring devices meet recommended security standards.

- **Selective Wipe**: A feature in Intune that removes corporate data from an app or device while leaving personal data intact. This is useful when a user leaves the organization or loses their device.
- **Shared Device Mode**: A configuration in Intune for devices used by multiple users, often deployed in retail or healthcare environments where users log in with unique credentials.
- **Targeting Filter**: Filters in Intune used to apply specific policies to devices based on criteria such as device type, OS, or enrollment status, enhancing policy precision.
- **Update Compliance**: A report in Intune that shows the update status of all managed devices, helping IT ensure that devices are current with patches and updates.
- **Update Policy**: Rules defined in Intune that control when and how updates are applied to devices, ensuring consistency across the organization.
- **User-Driven Mode**: A Windows Autopilot deployment mode where users start the enrollment process, designed for organizations that want to minimize IT involvement during setup.
- **Windows Defender**: Microsoft's built-in antivirus and anti-malware tool for Windows devices, providing endpoint protection and security threat mitigation.
- **Windows Hello for Business**: A passwordless login solution for Windows devices that uses biometrics or a PIN, enhancing security and user experience.
- **Windows Information Protection (WIP)**: A feature in Intune that helps protect enterprise data on both managed and unmanaged devices by separating work and personal data.
- **Windows Update Rings**: A feature in Intune used to configure and manage update schedules for Windows devices, controlling when and how updates are installed.
- **Zero Trust Security Model**: A security approach that requires verification for every device and user accessing a network, assuming no implicit trust.