Digital Signing and Implementation, Troubleshooting Tools, SCCM Its Configuration Manager Client and its Inventory For PC’s.

GROUP C

What is Digital Signing?

- Digital Signing is the process of adding a certificate-based signature to a file (like an MSIX package)
- It verifies the authenticity (trusted source) and integrity (no tampering) of the package.
- Why Digital Signing in MSIX?
- Ensures safe installation of apps.
- Builds user trust by verifying publisher identity.
- Protects against tampered or malicious software.
- Allows apps to be accepted in Microsoft Store & enterprise environments.

Requirement of Digital Signing in MSIX

- ✔ Mandatory – MSIX packages cannot install without a valid signature.
- ✔ Authenticity – Verifies the publisher’s identity.
- ✔ Integrity – Confirms the package has not been altered.
- ✔ Security – Protects against malware or tampered apps.
- ✔ Deployment – Required for Microsoft Store, Intune, and SCCM.
- ✔ Trust – Builds user and enterprise confidence.

Implementation Steps

- Obtain Code Signing Certificate (CA or self-signed for testing)
- Build MSIX package (MSIX Packaging Tool / Visual Studio)
- Sign package (SignTool.exe / Visual Studio / MSIX Tool)
- Distribute package (Microsoft Store, Intune, SCCM, App Installer, sideloading)
- Validate signature during installation

Benefits

- Ensures security and integrity
- Confirms authenticity of publisher
- Required for Microsoft Store submission
- Builds user trust & professionalism
- Enterprise control over allowed apps
- Timestamping keeps signatures valid

Most used troubleshooting tools for MSIX Packages

- Event viewer
- Powershell cmdlets
- MSIX packages tool
- Process moniter (Procmon)
- Process explorer
- Dependency walker / dependency tool
- WinDbg (windows Debugger)
- App installer logs
- Event tracking for windows (ETW)
- Fiddler / network monitors

Introduction to SCCM

- System Center Configuration Manager (SCCM)
- Microsoft solution for centralized device and system management.
- Supports desktops, laptops, and servers.
- Key functions:
- Software deployment, OS installation, patch management, compliance, and reporting.

Preparing the Management Infrastructure

- Assess current IT environment and hardware resources.
- Ensure Active Directory (AD) structure is ready for integration.
- Configure network prerequisites (DNS, DHCP, firewall rules).
- Plan site hierarchy (Central Administration Site, Primary Site, Secondary Sites).

SCCM Components Setup

- Site Server – central management point.
- Management Points – client communication.
- Distribution Points – deliver software, updates, OS images.
- SQL Server Database – stores configuration and client data.
- Integration with Windows Server Update Services (WSUS).

Benefits of Prepared Infrastructure

- Centralized control of desktop devices.
- Automated OS & software deployment.
- Secure patching & compliance enforcement.
- Improved IT efficiency & reduced downtime.
- Scalability for future growth.

Managing Inventory for PCs &Applications

- **Why It Matters:**
- Track assets efficiently
- Reduce costs
- Ensure software compliance
- Improve security & planning

What to Manage

- PCs, laptops, monitors
- Operating systems
- Installed software
- Software licenses
- Cloud apps & services

Key Tools

- Microsoft Intune / SCCM
- Lansweeper / PDQ Inventory
- ManageEngine
- Excel (basic tracking)
- ITSM tools (e.g., ServiceNow)

Data to Track

- Device name, user, location
- OS & hardware specs
- Installed apps
- License keys & expiration
- Usage stats

Best Practices

- Automate inventory updates
- Tag all assets
- Audit regularly
- Track license usage
- Set renewal alerts

Challenges

- Shadow IT
- Outdated records
- Unused software
- License violations

Benefits

- Save costs
- Reduce risks
- Faster support
- Better forecasting
- Stay audit-ready

What is the SCCM Client?

- The SCCM client is a small program installed on computers.
- It allows the computer to:
- Receive software updates
- Install applications
- Get configuration settings
- Report its status to the SCCM server

Installing the Client

- The SCCM client is usually:
- Automatically installed by the SCCM server (called “client push”)
- Installed during Windows setup (task sequence)
- Or installed manually by an IT technician
- Once installed, the client starts talking to the SCCM server.

Repairing the Client and Uninstalling the Client

- If the SCCM client isn't working (e.g., not getting updates or showing offline), it can be repaired.
- Repairing makes the client try to reconnect to the server and fix missing or broken parts.
- Sometimes the client might need to be removed (uninstalled), like when a computer is being re-imaged, repurposed, or removed from SCCM management.

Checking If It’s Working

- You can check the client’s status in:
- The Control Panel (Configuration Manager icon)
- The SCCM console (shows client health)
- Or by checking if software and updates are arriving correctly

Logs for Troubleshooting

- The client creates log files that show what it’s doing.
- IT staff use these logs to:
- Check if the client installed correctly
- Find out why it’s not working
- See what updates or apps were deployed
- Forcing the Client to Check In:
- If a client seems slow to respond, it can be told to “check in now” — this means:
- It will talk to the SCCM server
- Download any new policies, apps, or updates