Managing the Configuration Manager Client in SCCM

Managing the SCCM client involves key operational areas to ensure proper communication and functionality:

1.Discovery & Deployment:

- Detect unmanaged devices via discovery methods.
- Deploy the client using methods like Client Push, Group Policy, manual install, or OS image integration.

2.Client Settings Configuration:

- Configure default or custom settings through the Client Settings node in the Administration workspace.
- Adjust behaviors for software updates, activity monitoring, and compliance checks.

3.Client Cache Management:

- Stores installation files for apps/updates.
- Configure size and location via the client control panel and clean up with “Delete Files”.

4.Client Status Monitoring:

- View client health in the Monitoring workspace.
- Use alerts and reports to track activity and compliance.

5.Troubleshooting Tools:

- Use Software Center for app installations and updates.
- Use ConfigMgr client applet for configuration and diagnostics.
- Launch client control panel via Control smscfgrc for detailed inspection.

This structured approach ensures clients are properly installed, configured, monitored, and supported across the SCCM environment.

Configure software metering

Software Metering in SCCM allows you to track and report how often specific applications are used across client devices. This helps in understanding software usage and optimizing license costs.

Steps to Configure Software Metering:

1.Enable Software Metering in Client Settings

- Go to the SCCM console.
- Navigate:
  Administration → Client Settings
- Right-click Default Client Settings (or create a new custom one) → Properties
- Select Software Metering from the left pane.
- Set "Enable software metering on clients" to Yes.
- Click OK to apply.

2. Create Software Metering Rules

Go to:

Assets and Compliance → Software Metering

Right-click in the right pane → Create Software Metering Rule

Fill in the rule details:

- Name: Friendly name for the rule.
- File Name: Exact .exe name of the application to track (e.g., winword.exe).
- Original File Name, Version, Language, etc. (Optional filters).

Click Next and Finish.

3. Monitor Software Metering Usage

1.Go to:

Monitoring → Reporting → Software Metering Reports

2.Use built-in reports like:

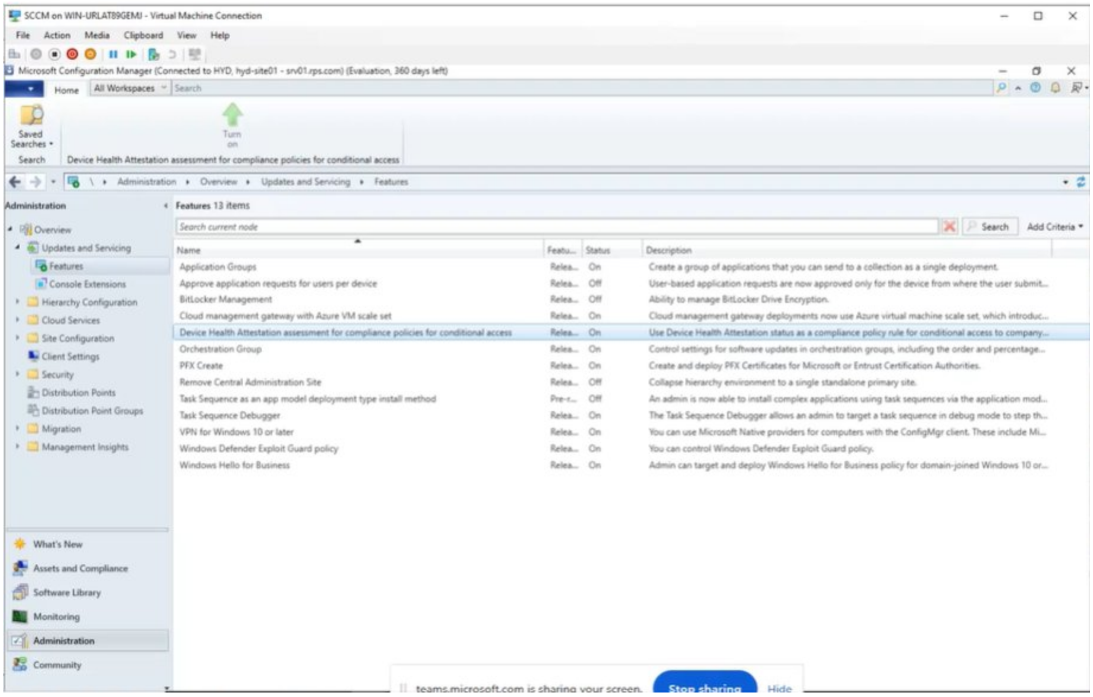
"Software metering usage summary report"

"Total usage trend analysis"

"Monthly usage summary per user"

Features

This feature allows SCCM to use Device Health Attestation (DHA) data to determine if a device meets compliance policies (e.g., BitLocker enabled, Secure Boot on). It is particularly useful when integrating with Conditional Access in Microsoft Intune or Azure AD — ensuring that only healthy, compliant devices can access corporate resources.



Name	Featu...	Status	Description
Application Groups	Relea...	On	Create a group of applications that you can send to a collection as a single deployment.
Approve application requests for users per device	Relea...	Off	User-based application requests are now approved only for the device from where the user submit...
BitLocker Management	Relea...	Off	Ability to manage BitLocker Drive Encryption.
Cloud management gateway with Azure VM scale set	Relea...	On	Cloud management gateway deployments now use Azure virtual machine scale set, which introduc...
Device Health Attestation assessment for compliance policies for conditional access	Relea...	On	Use Device Health Attestation status as a compliance policy rule for conditional access to company...
Orchestration Group	Relea...	On	Control settings for software updates in orchestration groups, including the order and percentage...
PFX Create	Relea...	On	Create and deploy PFX Certificates for Microsoft or Entrust Certification Authorities.
Remove Central Administration Site	Relea...	Off	Collapse hierarchy environment to a single standalone primary site.
Task Sequence as an app model deployment type install method	Pre-r...	Off	An admin is now able to install complex applications using task sequences via the application mod...
Task Sequence Debugger	Relea...	On	The Task Sequence Debugger allows an admin to target a task sequence in debug mode to step th...
VPN for Windows 10 or later	Relea...	On	You can use Microsoft Native providers for computers with the ConfigMgr client. These include Mi...
Windows Defender Exploit Guard policy	Relea...	On	You can control Windows Defender Exploit Guard policy.
Windows Hello for Business	Relea...	On	Admin can target and deploy Windows Hello for Business policy for domain-joined Windows 10 or...

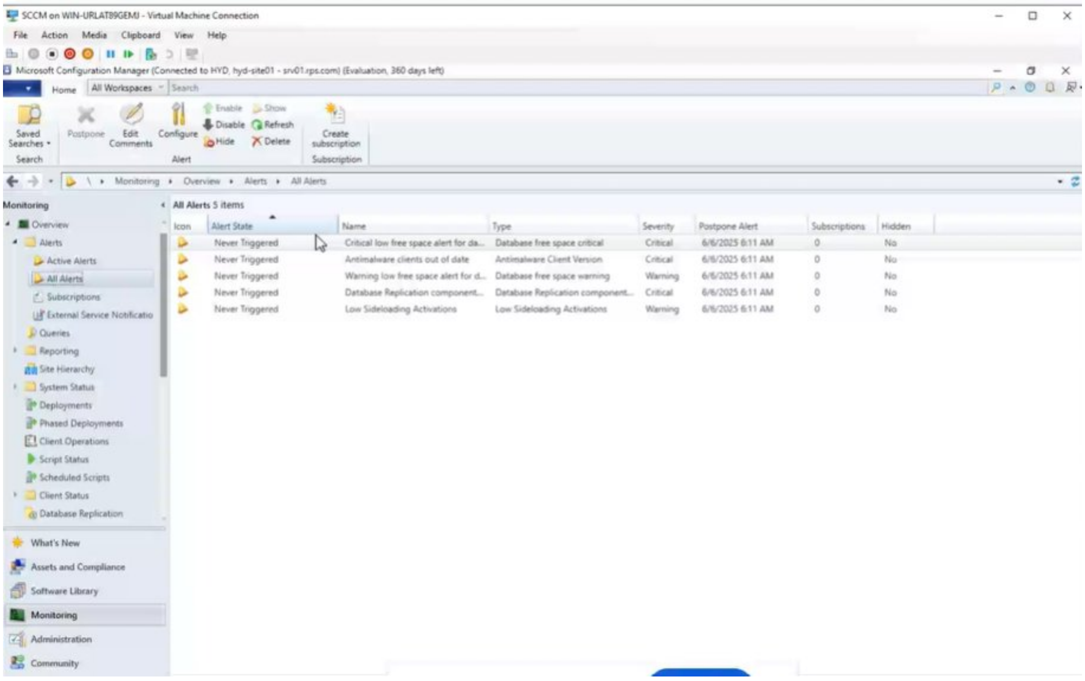
Alerts section in the **Monitoring**

The alert dashboard displays **5 system alerts**.

These alerts are categorized by:

- **Alert State**: All are currently **"Never Triggered"**, meaning the conditions haven't been met yet.
- **Name & Type**: Includes alerts for **low disk space**, **outdated client versions**, and **replication issues**.
- **Severity**: Ranges from **Critical** (e.g., low free space, outdated client version) to **Warning** (e.g., low sideloading activations).

No subscriptions are set for automatic email or system notifications.



SCCM on WIN-URLAT89GEMJ - Virtual Machine Connection

Microsoft Configuration Manager (Connected to HYD, hyd-site01 - srv01.rps.com) (Evaluation, 360 days left)

All Alerts 5 items

Icon	Alert State	Name	Type	Severity	Postpone Alert	Subscriptions	Hidden
	Never Triggered	Critical low free space alert for da...	Database free space critical	Critical	6/6/2025 6:11 AM	0	No
	Never Triggered	Antimalware clients out of date	Antimalware Client Version	Critical	6/6/2025 6:11 AM	0	No
	Never Triggered	Warning low free space alert for d...	Database free space warning	Warning	6/6/2025 6:11 AM	0	No
	Never Triggered	Database Replication component...	Database Replication component...	Critical	6/6/2025 6:11 AM	0	No
	Never Triggered	Low Sideloading Activations	Low Sideloading Activations	Warning	6/6/2025 6:11 AM	0	No

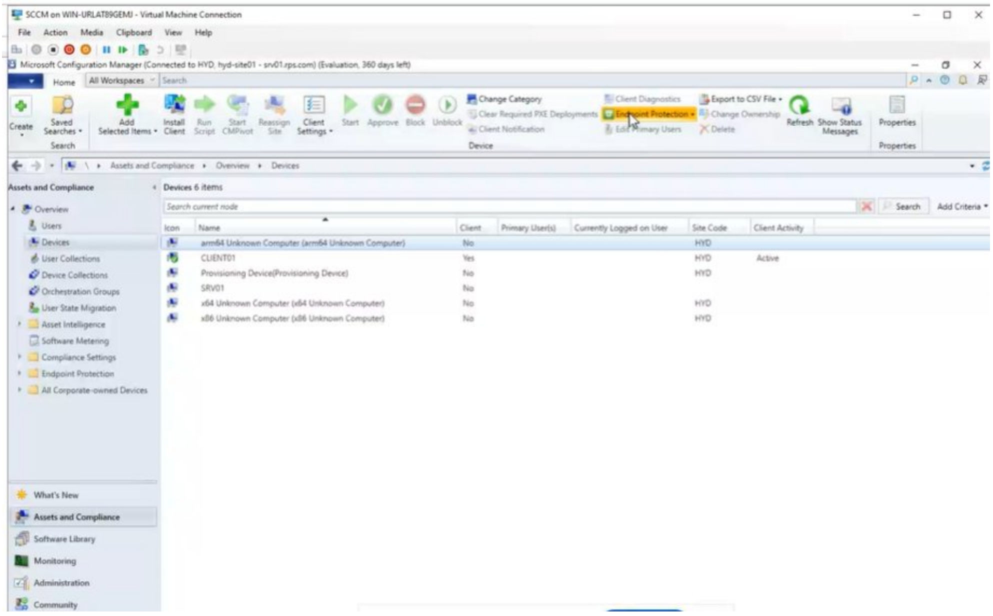
List of Devices

This section is essential for managing and monitoring all devices registered or discovered in SCCM.

This view shows a list of **devices (computers)** that SCCM is aware of.

Each row represents a device, including:

- **Name**: Device hostname or "Unknown Computer" if not fully identified.
- **Client**: Indicates whether the **SCCM client agent** is installed (Yes/No).
- **Primary User** and **Currently Logged On User**: User association and session info.
- **Site Code**: The site managing the device (e.g., HYD).
- **Client Activity**: Shows if the client is active.



SCCM on WIN-URLAT89GEMJ - Virtual Machine Connection

Microsoft Configuration Manager (Connected to HYD, hyd-site01 - srv01.rps.com) (Evaluation, 360 days left)

Devices 6 items

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity
	arm64 Unknown Computer (arm64 Unknown Computer)	No			HYD	
	CLIENT01	Yes			HYD	Active
	Provisioning Device(Provisioning Device)	No			HYD	
	SRV01	No				
	x64 Unknown Computer (x64 Unknown Computer)	No			HYD	
	x86 Unknown Computer (x86 Unknown Computer)	No			HYD	

Create Custom Client Device Settings

This window is used to create custom client settings for specific collections of devices.

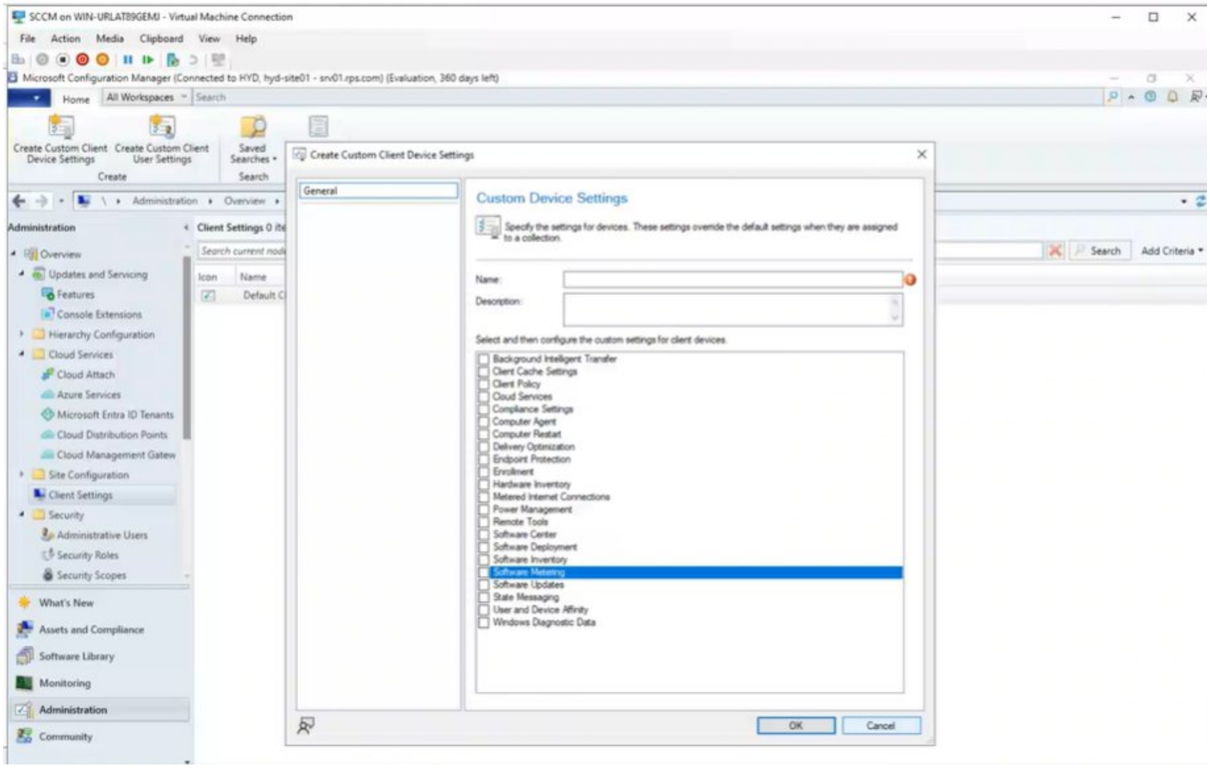
These settings override the default settings when assigned to a collection.

You can choose which components to configure, such as:

- Software Updates
- Software Inventory
- Power Management
- Client Policy
- Hardware Inventory, etc.

After selecting the required settings, you can configure detailed options for each.

This allows administrators to apply granular client configurations to specific device groups, improving management and compliance flexibility.



Create Custom Client Device Settings

General

Custom Device Settings

Specify the settings for devices. These settings override the default settings when they are assigned to a collection.

Name:

Description:

Select and then configure the custom settings for client devices.

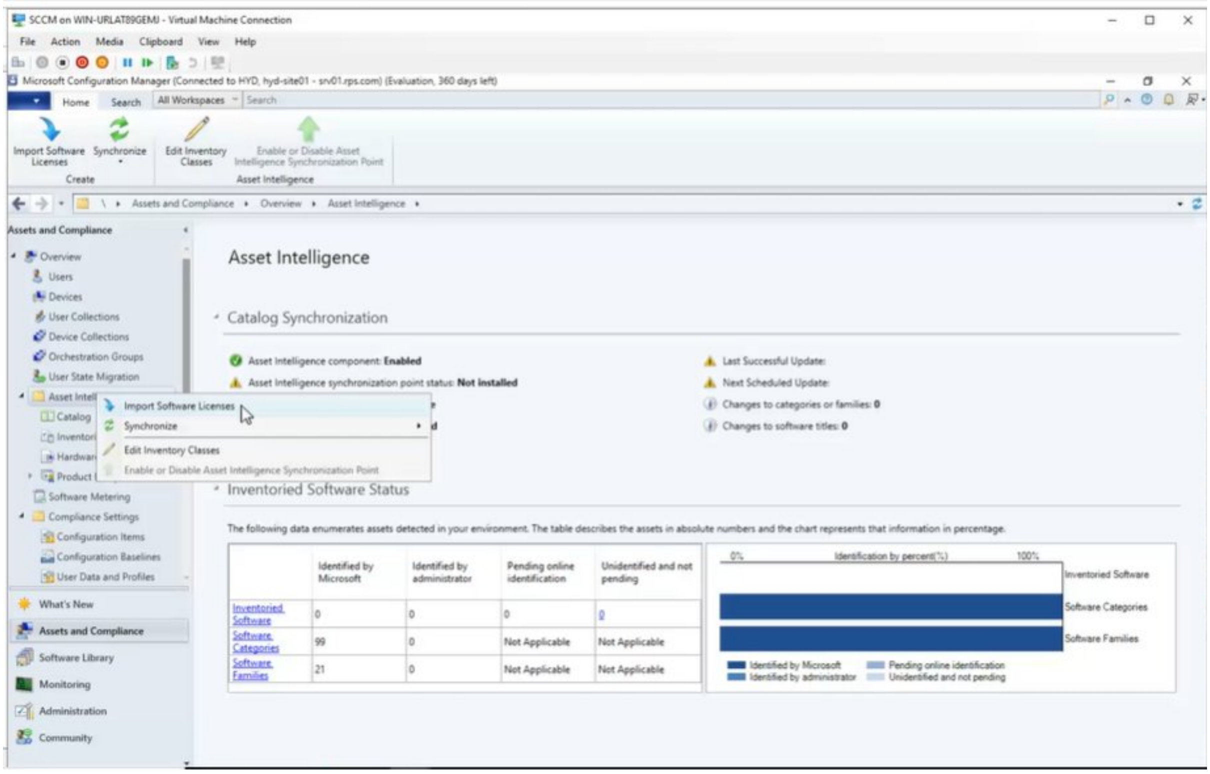
- □ Background Intelligent Transfer
- □ Client Cache Settings
- □ Client Policy
- □ Cloud Services
- □ Compliance Settings
- □ Computer Agent
- □ Computer Restart
- □ Delivery Optimization
- □ Endpoint Protection
- □ Enrollment
- □ Hardware Inventory
- □ Metered Internet Connections
- □ Power Management
- □ Remote Tools
- □ Software Center
- □ Software Deployment
- □ Software Inventory
- □ Software Metering
- □ Software Updates
- □ State Messaging
- □ User and Device Affinity
- □ Windows Diagnostic Data

OK Cancel

Asset Intelligence dashboard

Asset Intelligence helps organizations collect, analyze, and report on software inventory data from managed systems.

The Asset Intelligence dashboard gives a quick overview of software inventory and licensing status. It helps in software compliance, license tracking, and IT asset management.



Asset Intelligence

Catalog Synchronization

Asset Intelligence component: **Enabled**

Asset Intelligence synchronization point status: **Not installed**

Last Successful Update:

Next Scheduled Update:

Changes to categories or families: **0**

Changes to software titles: **0**

Inventoried Software Status

The following data enumerates assets detected in your environment. The table describes the assets in absolute numbers and the chart represents that information in percentage.

	Identified by Microsoft	Identified by administrator	Pending online identification	Unidentified and not pending
Inventoried Software	0	0	0	0
Software Categories	99	0	Not Applicable	Not Applicable
Software Families	21	0	Not Applicable	Not Applicable

NOIDMIF and **IDMIF**

The **NOIDMIF** and **IDMIF** files are used in SCCM (System Center Configuration Manager) to **extend hardware inventory** by adding custom data that SCCM clients do not automatically report.

<u>IDMIF (Intermediate MIF)</u>

Purpose: Adds information about a new object that is not part of the SCCM client inventory, such as printers, monitors, or other non-managed assets.

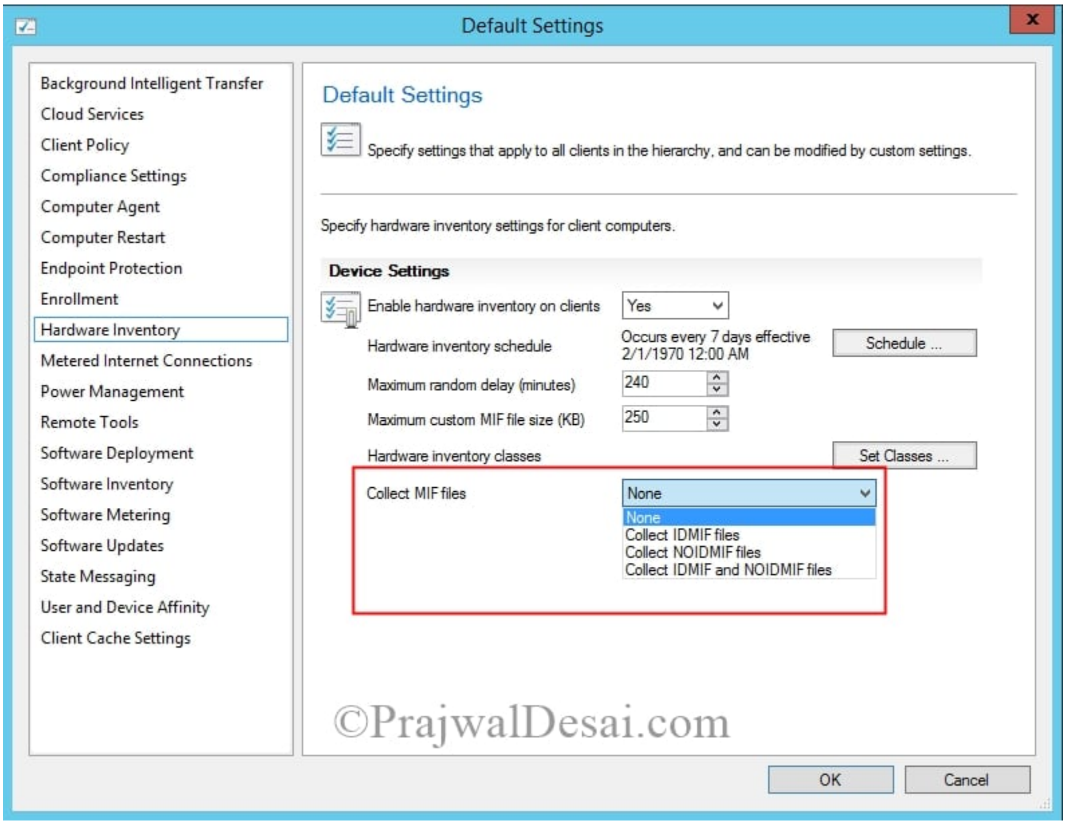
Use Case: Useful when you want to add **external inventory items** not installed on the client (e.g., peripherals).

Stored As: Separate records in the SCCM database (not tied to a specific client).

Example: Adding a projector that isn't connected to a PC.

NOIDMIF (No ID MIF)

- Purpose: Adds extra information to an existing client device’s inventory.
- Use Case: Used when you want to extend the inventory of the current SCCM client, like adding custom fields (e.g., Asset Tag, Owner Name).
- Stored As: Part of the client's inventory in SCCM.
- Example: Adding a custom field like "Floor Number" or "Location" to a specific computer.



Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify hardware inventory settings for client computers.

Device Settings

Enable hardware inventory on clients	Yes
Hardware inventory schedule	Occurs every 7 days effective 2/1/1970 12:00 AM
Maximum random delay (minutes)	240
Maximum custom MIF file size (KB)	250
Hardware inventory classes	
Collect MIF files	None

None
Collect IDMIF files
Collect NOIDMIF files
Collect IDMIF and NOIDMIF files