Inventory Management

This document summarizes the data that is collected from managed devices by different components of Miradore (usually by Miradore clients or 3rd party connectors). Each section explains in detail what data is collected, how often the data is updated, and which component is used to collect the data. At the end, it is also explained how Miradore can be configured to collect custom inventory data.

This document was last reviewed on May 18, 2020. No changes after that are included.

Table of Contents

1. Inventory Data Gathered by Miradore Clients ... 2
1.1 Linux ... 2
1.2 macOS / OS X ... 4
1.3 Windows ... 6
1.4 Hardware Change Logging (all client platforms) ... 8
1.5 Software Change Logging (all client platforms) ... 9
2. Inventory Data Gathered by Miradore Connectors ... 10
2.1 3 Step IT ... 10
2.2 Blancco Management Console ... 11
2.3 F-Secure Policy Manager ... 12
2.4 F-Secure Protection Service for Business (PSB) ... 13
2.5 Kroll Ontrack Eraser ... 14
2.6 McAfee ePolicy Orchestrator ... 15
2.8 Microsoft Active Directory ... 16
2.9 Microsoft Exchange ActiveSync ... 17
2.10 Microsoft System Center Configuration Manager ... 19
2.11 Microsoft Windows Server Update Services (WSUS) ... 20
2.12 Miradore Online ... 21
2.13 Sampo ... 22
2.14 Symantec Antivirus ... 23
2.15 Symantec Endpoint Protection ... 24
2.16 Trend Micro OfficeScan ... 25
3. Inventory Data Gathered by Other Components ... 26
3.1 SNMP Scanner ... 26
3.2 Network Discovery ... 27
4. Custom Inventory ... 28

1. Inventory Data Gathered by Miradore Clients

This chapter describes what inventory data Miradore clients (or management agents) gather from managed devices on different operating system platforms, how often the data is updated, and whether there are restrictions to the data collection.

1.1 Linux

Inventory interval & Restrictions	
Default interval	Hardware information: 12 hours File scan: 7 days Package manager scan: 12 hours
Restrictions	Miradore client for Linux is compatible with the following Linux distributions: CENTOS 6 - 7, Debian 6 - 9, Fedora 15 – 19, Open SUSE 11.4 - 12.3, Red Hat Enterprise Linux 6 - 7, SUSE Enterprise Linux 11, Ubuntu 10.04 LTS - 13.04

Data to collect	
Basic information	Status, Full name, Computer description, OS, OS installed, Logged in user (Full name, User ID, Last logon date, Logon count) Last logged in user, Last seen, Reboot date
Miradore Client	Status, Last seen, Version, Public IP, Local IP Device identity (Computer name, Serial number, MAC address(es), Domain)
Hardware	Manufacturer, Model, Serial number Processors (Description, Cores, Speed, Data width, L2 cache size) System type, BIOS (Release date, Serial number, SMBIOS version, Software identification, Version) RAM memory (Memory location, Description, Manufacturer, Capacity, Part number, Serial number, Form factor, Data width, Total width) Physical disks (Model, Interface type, Size (GB), Partitions, Firmware version, Serial number, SMART Health status, SMART Reallocated sector count, SMART uncorrectable error count, SMART HDD Temperature, SMART Media wearout indicator) Logical disks (Capacity, Free space, Used space, Daily history graph, Monthly history graph) Network adapter (Full name, MAC address, IPv4 address, IPv6 address, Subnet mask, Gateway address)

	Video controller (Description, Adapter RAM) Battery information (Description, Name, Manufacturer, Location, Serial number, Battery status [Discharging / Running on AC power / Fully charged / Low / Critical / Charging / Charging and High / Charging and Low/Charging and Critical / Undefined / Partially charged], Estimated Charge remaining [%], Estimated run time [in minutes], Health status [information about battery health e.g. "Normal"], Full charge capacity [Wh, the current battery capacity when the battery is fully charged], Designed capacity [Wh], Designed voltage [V], Chemistry)
Monitors	Description, Model, Serial number
Printers	Name, Port, Form name, Paper size
PnP devices and drivers	Manufacturer, Name, Status (Driver not installed, Newer driver available, No driver available)
File scan	By default, Miradore client scans the system drive for executable files. Some locations, such as the Recycle/Trash bin are excluded from the scan. The retrieved file attributes are: File name, File size, Fingerprint, File path, Inventory date
Package manager	Category, Description, Inventory date, Package name, Version
Custom inventory	Custom inventory can be used to collect customer-configured data about the managed assets. The custom inventory is performed by the Miradore client according to a script file provided by the customer.

1.2 macOS / OS X

Inventory interval & Restrictions	
Default interval	Hardware information: 12 hours File scan: 7 days Installed applications scan: 12 hours
Restrictions	Miradore OS X client is compatible with the following Mac OS X / macOS versions: 10.6 – 10.13

Data to collect	
Basic information	Status, Full name, Computer description, OS, OS installed Logged in user (Full name, User ID, Last logon date, Logon count) Last logged in user, Last seen, Reboot date
Miradore Client	Status, Last seen, Version, Public IP, Local IP Device identity (Computer name, Serial number, MAC address(es), Domain)
Hardware	Manufacturer, Model, Serial number Processors (Description, Cores, Speed, Data width, L2 cache size) System type, Boot ROM version, SMC version RAM memory (Memory location, Description, Manufacturer, Capacity, Part number, Serial number) Physical disks (Model, Interface type, Size (GB), Partitions, Firmware version, Serial number, SMART Health status, SMART Reallocated sector count, SMART uncorrectable error count, SMART HDD Temperature, SMART Media wearout indicator) Logical disks (Capacity, Free space, Used space, Daily history graph, Monthly history graph) Network adapters (Full name, MAC address, IPv4 address, IPv6 address, Subnet mask, Gateway address) Batteries (Device ID, Description, Name, Manufacturer, Serial number, Battery status [Discharging / Running on AC power / Fully charged / Low / Critical / Charging / Charging and High / Charging and Low / Charging and Critical / Undefined / Partially charged], Estimated charge remaining [%], Estimated run time [minutes or empty when running on AC power], Health status [Normal / Replace Soon / Replace Now / Service Battery], Designed voltage [V], Designed capacity [Wh], Full charge capacity [Wh, the current battery capacity when the battery is fully charged], Estimated remaining capacity [%] Video controller (Description, Adapter RAM)

Monitors	Description, Model, Serial number
File scan	By default, Miradore client scans the system drive for executable files. Some locations, such as the Recycle/Trash bin are excluded from the scan. The retrieved file attributes are: File name, File size, Fingerprint, File path, Inventory date
Installed applications	64-Bit (Intel), Application name, Get info string, Inventory date, Kind, Last modified, Location, Version
Custom inventory	Custom inventory can be used to collect customer-configured data about the managed assets. The custom inventory is performed by the Miradore client according to a script file provided by the customer.

1.3 Windows

Inventory interval & Restrictions	
Default interval	Hardware information: 12 hours Boot duration: 7 days File scan: 7 days Add/Remove programs scan: 12 hours Software usage: 12 hours Device power state: 24 hours Local administrators scan: 12 hours
Restrictions	Miradore client for Windows is compatible with the following versions: Windows XP (32/64-bit), Windows Embedded POSReady 2009, Windows Server 2003 (32/64-bit), Windows Vista (32/64-bit), Windows Server 2008 (32/64-bit), Windows Server 2008 R2, Windows 7 (32/64-bit), Windows Embedded POSReady 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Data to collect	
Basic information	Status, Full name, Computer description, OS, OS installed Logged in user (Full name, User ID, Last logon date, Logon count) Last logged in user, Last seen, Reboot date, Windows stability score (The system stability index or reliability score is a number between 1 (least stable) to 10 (most stable) and it is calculated based on the number of failures over a rolling historical period. Recent failures have bigger impact to the score than past failures.)
Boot duration	Last boot date, Last boot duration, Fastest boot duration, Slowest boot duration, Average boot duration, Average boot duration (main phase), Average boot duration (post phase), Oldest recorded boot date, Boot frequency in days
Miradore Client	Status, Last seen, Version, Public IP, Local IP Device identity (Computer name, Serial number, MAC address(es), Domain)
Power information	Daily report of device power states (Power off, Low power, Power on – computer locked, Power on – computer unlocked) Estimate of power consumption in kWh and electricity costs.
Hardware	Manufacturer, Model, Serial number Processors (Description, Cores, Speed, Data width, L2 cache size) System type BIOS (Release date, Serial number, SMBIOS version, Software identification, UEFI version, UEFI architecture, UEFI secure boot, Version)

	RAM memory (Memory location, Description, Manufacturer, Capacity, Part number, Serial number, Form factor, Data width, Total width) Display, Keyboard layout Physical disks (Model, Interface type, Description, Size (GB), Partitions, Firmware version, Serial number, SMART Health status, SMART Reallocated sector count, SMART uncorrectable error count, SMART HDD Temperature, SMART Media wearout indicator) Logical disks (Capacity, Free space, Used space, Daily history graph, Monthly history graph) Network adapters (Full name, MAC address, IPv4 address, IPv6 address, Subnet mask, Gateway address) Video controller (Description, Adapter RAM, Driver date, Driver version, Resolution) Batteries (Description, Manufacturer, Name, Location, Serial number, Battery status [Discharging / Running on AC power / Fully charged / Low / Critical / Charging / Charging and High / Charging and Low / Charging and Critical / Undefined / Partially charged], Estimated charge remaining [%], Estimated run time [minutes or empty when running on AC power], Health status [OK / Error / Degraded / Unknown / Pred Fail / Starting / Stopping / Service / Stressed / NonRecover / No contact / Lost comm], Full charge capacity [Wh, the current battery capacity when the battery is fully charged], Designed capacity [Wh], Designed voltage [V], Chemistry [Other / Lead Acid / Nickel Cadium / Nickel Metal Hybride / Lithium-ion / Zinc Air / Lithium Polymer], Last error code, Error description)
Monitors	Description, Model, Serial number
Printers	Name, Port, Color, Duplex, Paper size
PnP devices and drivers	Manufacturer, Name, Status (Driver not installed, Newer driver available, No driver available)
Local administrators	Local administrator's user name
File scan	By default, Miradore client scans the system drive for executable files. Some locations, such as the Recycle/Trash bin are excluded from the scan. The retrieved file attributes are: File name, File size, Company, Product name, File version, File path, Inventory date
Add/remove programs	Name, Version, Display version, Uninstall string, Product code, Publisher, Install source, Install location, Estimated size, Install date, Inventory date
Software catalog	Category, Manufacturer, Name, Version, Suite (Yes/No), Is a partial match (Yes/No)
Managed software	Software name, Status, Usage frequency, License status, Software category, Quality index rule, Package names, Description, Identified by file scan (Yes/No), Identified by Add/remove programs (Yes/No), Identified by software catalog (Yes/No), Identified month, Identified date,
Windows event logs	Application crashes (Category, CategoryString, EventCode, EventType, InvDate, Logfile, Message, Param1 [executable], Param2 [lexecutable path], Param3 [executable version], Param4 [execption], RecordNumber, SourceName, TimeWritten) OS crashes (Category, CategoryString, EventCode, EventType, InvDate, Logfile, Message, Param1 [Bugcheck parameters], Param2 [memory dumb

	location], Param3 [report ID], Param4, RecordNumber, SourceName, TimeWritten)
Windows-provided security information	Type (Antivirus/Antispyware/Firewall), Name, Status (enabled/disabled), Up-to-date (Yes/No/””, for type “Firewall” this data is not available), Timestamp
Security patch status	Category (Critical/Recommended), Release date, Status change date, Info, Approval, Name, Patch installation status (Failed, Installed, Installed by superseding, Not installed)
Custom inventory	Custom inventory can be used to collect customer-configured data about the managed assets. The custom inventory is performed by the Miradore client according to a script file provided by the customer.

1.4 Hardware Change Logging (all client platforms)

Miradore clients run hardware inventory scans and send collected inventory information to Miradore server at regular, configurable intervals. The inventory interval can be set for each client platform separately in the system settings of Miradore. The collected data may vary between different client platforms.

About hardware change logging

If Asset inventory change logging is enabled at "System settings > Main > Event log settings > Asset inventory change log" in Miradore, then Miradore compares the newest hardware inventory scan results with the previous scan result to detect changes in the devices hardware configurations. If a change is detected, it is logged and shown in *Hardware inventory change log* report. At the system settings, it is also possible to define how long information of the changes is stored in Miradore.

Logged hardware change types

Table below describes the types of hardware changes that are recorded by Miradore.

Changed item		**Monitored attributes**
	Hard disk	Description, Model, Name, Size, Idx, Firmware revision, Serial number, Interface type
	RAM	Capacity, Description, Manufacturer, Part number, Serial number, Device locator, Form factor, Speed, Data width, Total width
	BIOS	Manufacturer, Serial number, Release date, BIOS version, Software element ID, Version
CPU	Processor	Architecture, Data width, L2 cache size, Manufacturer, Max clock speed, Name, Number of cores, Number of logical processors, Description

	Video controller	Adapter RAM, Description, Name
	Mobile devices *	IMSI & Firmware, Logical disks *

* Notice that management of mobile devices is carried out with Miradore Online, but the asset information regarding mobile devices can be imported to Miradore Management Suite using the Miradore connector for Miradore Online.

Icons designed by Freepik and Those Icons from Flaticon

1.5 Software Change Logging (all client platforms)

Miradore clients run software inventory scans and send collected inventory information to Miradore Management Suite server at regular, configurable intervals. The inventory interval can be set for each client platform separately in the system settings of Miradore Management Suite. The collected data may vary between different client platforms.

About software change logging

If the Asset inventory change logging is enabled at "System settings > Main > Event log settings > Asset inventory change log" in Miradore Management Suite, then the system compares the newest software inventory scan results with the previous scan result to detect if there has happened any changes in the devices' software configurations. If a change is detected, it is logged and shown in *Software inventory change log* report. At the system settings, it is also possible to define how long information of the changes is stored in Miradore Management Suite.

Logged software change types

Miradore tracks software installations and writes a log if software is installed or removed to/from a managed device. Table below describes the software inventory information sources on different platforms.

Platform	Software inventory source
Windows	Add/Remove programs scan
Linux	Package manager scan
OS X	Installed applications scan

2. Inventory Data Gathered by Miradore Connectors

Miradore connectors are ready-made integration components that can be used to integrate Miradore Management Suite with third-party information systems. The connectors are typically used to automatically import data into Miradore Management Suite from another information system, or vice versa, to export data from Miradore database to the external information system.

2.1 3 Step IT

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	3 Step IT Asset Management NG

What data can be imported
All available attributes from 3 Step IT Asset Management are imported to Miradore database. **The following attributes will be shown in the asset inventory:** Id number, Contract number, Product group, Serial number, Cost center, Device rent, Lease length, Lease start date, Financial type, Lease end date, Order reference, Ending option, Ending option info, Location, Pickup location, User name, Device model, Hard disk, Memory, Processor, Extra info, Other, Change date

What data can be exported
Asset notice, Asset status, Asset tag, Company name, Cost center, Cost center (full name), Cost center 2, Cost center 2 (full name), Detailed location, Device name, Device role, Ending option, Hardware category, Hardware model, Location, Location (full name), Logged on user (firstname + middle + lastname), Logged on user (lastname + firstname + middle), Organisation, Organisation (full name), Pickup location, Responsible person (firstname + middle + lastname), Responsible person (Lastname + Firstname + middle), Responsible person’s email, Responsible person’s employee ID, Responsible person’s user ID, Static text: ‘Miradore’

What data can be updated in the export
Company product group, Cost center, Cost center 2, Ending option, Extra info 1, Extra info 2, Extra info 3, Extra info 4, Extra info 5, Extra number 1, Extra number 2, Extra number 3, Extra number 4, Extra number 5, Extra text 1, Extra text 2, Extra text 3, Extra text 4, Extra text 5, Id number, Location, PickupLocation, Project, Username, Version

2.2 Blancco Management Console

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Blancco Management Console 2.x – 4.0.3

What data can be imported	
All erasure reports since the last run of the connector.	
Erasure information	All erasure reports since the last run. The field in the report are: Report id, Asset serial number, Asset MAC address, Erasure end time, Duration, Overwrites, Pattern, Verify, Software version
Erased media	Model, Serial number, Size, Block size, Status

2.3 F-Secure Policy Manager

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	F-Secure Policy Manager 10.x – 12.2

What data can be imported	
Connector sends a full report on every run. Items in the report can be limited by defining F-Secure policy domain groups to be read. **Fields in the report are:**	
Antivirus	Product name, Product version, Definition date, Definition version, Last seen, Last scanned, Parent server, Server group, Client group
Firewall	Product name, Product version, Settings name, Settings updated, Server

2.4 WithSecure Elements Endpoint Protection (previously F-Secure PSB)

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	WithSecure Elements Endpoint Protection

What data can be imported
Connector sends a full report on every run. **Fields in the report are:**
CurrentProfileName, FirewallState, Id, IpAddress, Label, LastConnectionTimestamp, LastStatusUpdateTimestamp, Name, Product, ProductVersion, RealTimeScanningState, SerialNumber, SubscriptionKey, VirusDbUpdateTimestamp, VirsuDbVersion, VirusProtectionState, WinsName

What data can be exported
None.

2.5 Kroll Ontrack Eraser

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Kroll Ontrack Eraser 3.x

What data can be imported	
All erasure reports since the last run of the connector.	
Erasure information	All erasure reports since the last run. The fields in the report are: Report id, Asset serial number, Asset MAC address, Erasure end time, Duration, Overwrites, Pattern, Verify, Software version
Erased media	Model, Serial number, Size, Block size, Status

2.6 McAfee ePolicy Orchestrator

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	McAfee ePolicy Orchestrator 3.x or 4.x

What data can be imported	
Connector sends a full report on every run. The report contains information about McAfee antivirus and firewall products on computers managed by ePolicy Orchestrator.	
Antivirus	Computer name, Client group (computer node path), Server, Client IP address, Last check-in time, Virus definition date, Virus definition version, Product version, Hotfix
Firewall	Computer name, Server, Product version, Hotfix, Last check-in time

2.8 Microsoft Active Directory

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Microsoft Active Directory on Microsoft Windows Server 2003 or later

What data can be imported	
Connector sends a full report on every run. Items in the report can be limited by defining one more LDAP paths where from the users and computers are read.	
Groups	DistinguishedName, SAMAccountName, Email, GroupType, Description, MemberOf
Users	DistinguishedName, SAMAccountname, Description, UserAccountControl, WhenCreated, WhenChanged, GivenName, Initials, Sn, DisplayName, ScriptPath, LogonCount, PwdLastSet, Department, Manager, Mail, TelephoneNumber, AccountExpires, MemberOf, LastLogonTimeStamp, EmployeeID
Computers	DistinguishedName, MemberOf, SAMAccountName, Description, WhenCreated, WhenChanged, OperatingSystem, OperatingSystemServicePack, OperatingSystemVersion, Location, LastLogonTimeStamp

2.9 Microsoft Exchange ActiveSync

Inventory interval & Restrictions	
Default interval	24 hours for all Exchange inventory data types.
Supported systems	Microsoft Exchange Server 2010 Microsoft Office 365 / Exchange Online

What data can be imported	
Device information	Device ID, Device type, Device access state, Exchange server, Friendly name, First sync time, GUID, Identity, IMEI, Last policy update time, Last successful sync, Last sync attempt time, Mobile operator, Model, OS, OS language, Telephone number, User agent, User display name, When changed (UTC), When created (UTC)
Mailbox policy information	**General:** Allow non-provisionable devices, Device policy refresh interval, Distinguished name, Exchange server, GUID, Identity, Is default policy **Password:** Require password, Require alphanumeric password, Minimum number of character sets, Enable password recovery, Device encryption enabled, Require encryption on device, Require encryption on storage card, Allow simple password, Number of failed attempts allowed, Minimum password length, Password expiration (days), Enforce password history **Synchronisation settings:** Include past calendar items, Include past e-mail items, Limit e-mail size to (KB), Maximum e-mail HTML body truncation size, Require manual sync when roaming, Allow HTML-formatted e-mail, Allow downloading of attachments, Maximum attachment size (KB), Require signed S/MIME messages, Require encrypted S/MIME messages, Allow S/MIME soft certs, Require signed S/MIME algorithm, Require encryption S/MIME algorithm, Allow S/MIME encryption algorithm negotiation **Device:** Allow removable storage, Allow camera, Allow Wi-Fi, Allow infrared, Allow Internet sharing from device, Allow remote desktop from device, Allow desktop synchronisation, Allow bluetooth, Mobile OTA update mode, Allow mobile OTA update, Allow external device management, IRM enabled **Device applications:** Allow browser, Allow consumer e-mail, Allow unsigned applications, Allow unsigned installation packages, Allow text messaging, Allow POP/IMAP e-mail **Other:** Blocked applications, Allowed applications, WSS access enabled, UNC access enabled

User information	Exchange server, Distinguished name, Mailbox username, Primary address, Assigned policy

2.10 Microsoft System Center Configuration Manager

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Microsoft SCCM 2007 and 2012.

What data can be imported	
Inventory data about computers which belong to defined SCCM collection.	
System	Name, SMBIOS_GUID
PC BIOS	Name, Manufacturer, SerialNumber, ReleaseDate, SMBIOSVersion, SoftwareElementID, Version
Computer system	Name, Domain, Manufacturer, Model, SystemType, UserName
Operating system	Caption, CSDVersion, Locale, OSLanguage, RegisteredUser, InstallDate, LastBootUpTime, WindowsDirectory, CSDVersion, Version
Device display	VerticalResolution, HorizontalResolution
Keyboard device	Layout
Logical disk	Name, FreeSpace, Size, Description, DriveType
Network adapter	DeviceID, MACAddress, Name, PNPDeviceID
Network adapter configuration	Index, DefaultIPGateway, DHCPEnabled, DHCPServer, DNSDomain, IPAddress, IPEnabled, IPSubnet
Disk	Description, InterfaceType, Index, Model, Name, Partition, Size
Physical memory	Capacity, DataWidth, Description, DeviceLocator, FormFactor, Manufacturer, PartNumber, SerialNumber, Speed, TotalWidth
Processor	CurrentClockSpeed, DataWidth, Version, Manufacturer, MaxClockSpeed, Name
Video controller	AdapterRAM, CurrentBitsPerPixel, CurrentHorizontalResolution, CurrentNumberOfColors, CurrentRefreshRate, CurrentVerticalResolution, Description, DriverDate, DriverVersion, Name
Desktop monitor	DeviceID, Description
PNP device driver	ClassGuid, DeviceID, Manufacturer, Name

2.11 Microsoft Windows Server Update Services (WSUS)

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Microsoft Windows Server Update Services (WSUS) 3.0

What data can be imported
Connector uses public WSUS database views or SCCM database tables to read the data. If the connector, is configured to read security update information, it sends full reports of available security updates on every time the connector is run. If the connector is configured to read computer information, it sends report of computers reported since the last run. To make sure that Miradore has correct information about computers, the connector sends a full report of computers on every 10th run time. **Fields in the report are:** DefaultTitle, SecurityBulletin, KnowledgebaseArticle, UpdateId, CreationDate, MsrcSeverity Action ComputerTargetId, Name, LastReportedStatusTime UpdateID, State

2.12 Miradore Online

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Miradore Online & Miradore Management Suite 3.8.0 or later

What data can be imported	
The connector reads the below mentioned data attributes from Miradore Online through the Miradore Online API and imports the data into Miradore Management Suite where it is attached to assets.	
Hardware inventory	**Device info (iOS):** Device name, IMEI, IMSI, ICCID, UDID, Serial number, Phone number, Manufacturer, Model, Product name, Software version, Operating system, Logical disk (size/free) **Device info (Android):** IMEI, IMSI, ICCID, Serial number, Serial number (Samsung KNOX), Phone number, Manufacturer, Model, Product name, Firmware, Operating system, Logical disk (size/free) **Network (iOS):** Operator, Cell ID, Current country, Current network, Home country, Home network, Location area, Roaming state, Roaming allowed **Network (Android):** Operator, Cell ID, Current country, Current network, Home country, Home network, Location area **Network interfaces:** Name, Mode, Status, MAC
Software inventory	**Installed applications (iOS):** Package name, Name, Version, App size (MB), Data size (MB) **Installed applications (Android):** Package name, Name, Version
User (responsible person)	The user must exist in Miradore Management Suite. If the user does not exist, the imported asset is left in *AutoGenerated* status.
Location	The location must exist in Miradore Management Suite. If the location does not exist, the imported asset is left in *AutoGenerated* status.

2.13 Sampo

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Sampo Finance EfecteLiira interface spec 0.7

What data can be imported
All available attributes from Sampo Finance asset system are imported to Miradore. **The following attributes will be shown in the asset inventory:** Id number, Contract number, Product group, Serial number, Cost center, Device rent, Lease length, Lease start date, Lease end date, Order reference, Ending option, Location, Pickup location, User name, Device model, Hard disk, Memory, Processor, Extra info, Other, Change date

2.14 Symantec Antivirus

Inventory Interval & Restrictions	
Default interval	24 hours
Supported systems	Symantec Antivirus 8.x – 10.x

What data can be imported	
Connector sends a full report on every run. Report contains information about antivirus and firewall products on computers managed by Symantec Antivirus server.	
Antivirus	Computer name, IP address, Server, Server group, Product version, Virus definition date, Virus definition version, Last check-in time, Client group, Last scan time
Firewall	Computer name, Server, Product version, Policy update time, Policy file name

2.15 Symantec Endpoint Protection

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Symantec Symantec Endpoint Protection 11.x – 12.x

What data can be imported	
The connector sends a full reports on every run. The report contains information about Symantec Endpoint Protection antivirus and firewall products on computers managed by Symantec Endpoint Protection server.	
Antivirus	Computer name, Server, Server group (last site), Last check-in time, Last scan time, Client group (last group), Virus pattern date, Virus pattern version
Firewall	Computer name, Server Agent version, Last check-in time, Firewall status

2.16 Trend Micro OfficeScan

Inventory interval & Restrictions	
Default interval	24 hours
Supported systems	Trend Micro OfficeScan 7.x – 10.x

What data can be imported	
The connector sends a full report on every run. The report contains information about products on computers managed by Trend Micro OfficeScan server. The data is exported from OfficeScan web management console like the CSV reports exported using a web browser.	
Antivirus	Computer name, IP address, Server name, Client version, Virus pattern version, Client domain group, Last scan time, Product name

3. Inventory Data Gathered by Other Components

3.1 SNMP Scanner

Inventory interval & Restrictions	
Default interval	The interval depends on the Windows Task Scheduler configurations made during the installation of SNMP Scanner.
Supported systems	The target device(s) must have an asset configuration item in Miradore Management Suite and it must have an IP address.

Data to collect	
CPU	LineCardIndex, LineCardDesc, Utilization
Interface	Index, Description, Status, Usage, InErrors, OutErrors, InOctets, OutOctets, LastChange, MACAddress, ConnectingDeviceMAC, IPAddress
Memory	LineCardIndex, LineCardDescription, LineCardPhysicalDescription, MemoryType, TotalMemory, MemoryPoolUsed, MemoryPoolFree, MemoryPoolLargestFree, Utilization, Fragmentation
Physical	Index, PartNumber, SerialNumber, Description, DiskSize, FreeDiskSpace
Printer	PrintedPagesTotal, PrintedPagesBW, PrintedPagesColour, PrintedPagesTotal_Counter, PrintedPagesBW_Counter, PrintedPagesColour_Counter, RemainingToner
System	Description, Uptime, Contact, Name, Location, Software version, Software image

3.2 Network Discovery

Inventory interval & Restrictions	
Default interval	1 hour
Supported systems	Subnets that have the network discovery enabled

Data to collect
Miradore network discovery is a utility that scan organization’s subnets for network connected devices. During the scan, a preselected discovery device pings each IP address within the subnet(s) and waits for a response. The network discovery gathers the following data attributes from the scanned devices: Device name, IP address, Location, Miradore asset created, Miradore client installed, Network address, Operating system, Scan date, Subnet mask

4. Custom Inventory

Custom inventory can be used to collect custom data of managed devices and enter the data into the configuration management database of Miradore. The custom inventory is performed by Miradore clients according to a script file, provided by the customer. The script file defines the data that should be collected from the managed assets and generates an output file which is automatically imported to Miradore after the custom inventory has been run successfully. The results of the custom inventory are shown on *Asset custom inventory view* and on Asset configuration item form at *Inventory report > Custom inventory* tab.

When an asset is removed from Miradore, the custom inventory data concerning the asset is automatically cleared.

Step-by-step guide to implementing custom inventory

Step	Task	How to...
1	Enable custom inventory	1. Navigate to Administration > System settings > Main > Miradore features. 2. Enable the "Custom inventory" feature.
2	Define data to be collected	1. Go to System settings > Main > Custom inventory 2. Define the name, display name, and data type of the attributes that you wish to collect from the managed devices. An attribute is a single characteristic or property of an asset (e.g. Serial number). 3. Define new classes and categorize the attributes into the classes. A class is a logical collection of attributes that are somehow related to each other (e.g. Disk drive). For example, the "disk drive" class may consist of "serial number" and "disk size" attributes. Names of the attributes and classes are used to determine which attributes or classes are allowed when processing incoming custom inventory files.
3	Create a script for data collection	The easiest way to create a new custom inventory script is to copy the provided sample script from the support site of Miradore and customize it according to your needs. Download the sample script from here: https://support.miradore.com/WebSites/Authenticated/sp_Downloads.aspx?id=154 **Notice** If the script generates an output file, the output file name must contain the device name of the computer that runs the scheduled task.

4	Upload and schedule the script to be executed	1. Go to System settings > Clients > General. 2. Create a new custom scheduled task from the "Custom scheduled tasks" table. 3. Enter a name for the custom scheduled task item, configure the running interval of the task, and upload the script that was made in step 3 as a task file to the scheduled tasks item in Miradore. Alternatively, you can write the script file directly to the editor that is shown on the task file popup window. The task file is the file which is performed by Miradore client when the custom inventory is ran. See Custom scheduled task item attributes for scheduled task item form field descriptions. 4. Control the running of built-in scheduled tasks and custom scheduled tasks in assets with the help of scheduled task profile items. With the scheduled task profile items, it is possible to configure the running settings of the scheduled tasks on an asset level, or according to the device role, device usage, location, organisation, or subcategory of operating system that has been installed to the device. See scheduled task profile item attributes for more information.
5	Check data import results	1. Go to System settings > System tasks and click "Show log" hyperlink on the task named "Import asset inventory information". 2. Filter log rows by entering "custominv" to the Output column´s quick filter.
6	Examine custom inventory data	1. Asset custom inventory view at Operations > Asset management > Inventory reports > Custom inventory on Miradore management console shows all data that has been gathered with the custom inventories. 2. The data, gathered by the custom inventories is also displayed on the particular asset configuration item in Miradore. To see the data produced by the custom inventories, go to Asset configuration item > Inventory report > Custom inventory.