

ABEGuardian

OT Cybersecurity made simple
Full visibility of your OT Systems in a centralized location.



ABEGuardian helps users to identify, evaluate, respond and report on software insecurities and misconfigurations of endpoints.

Identify

Centralized management solution to help manage IT and OT resources from a single interface, using a simple interface that makes your job easier

Evaluate

Find all valuable assets across the organization that could be harmed by threats in a way that can results in a monetary loss

Detect

Analyze the entirety of your plant Ecosystem to identify any malicious activities that could compromise the network or the integrity of the System

Respond

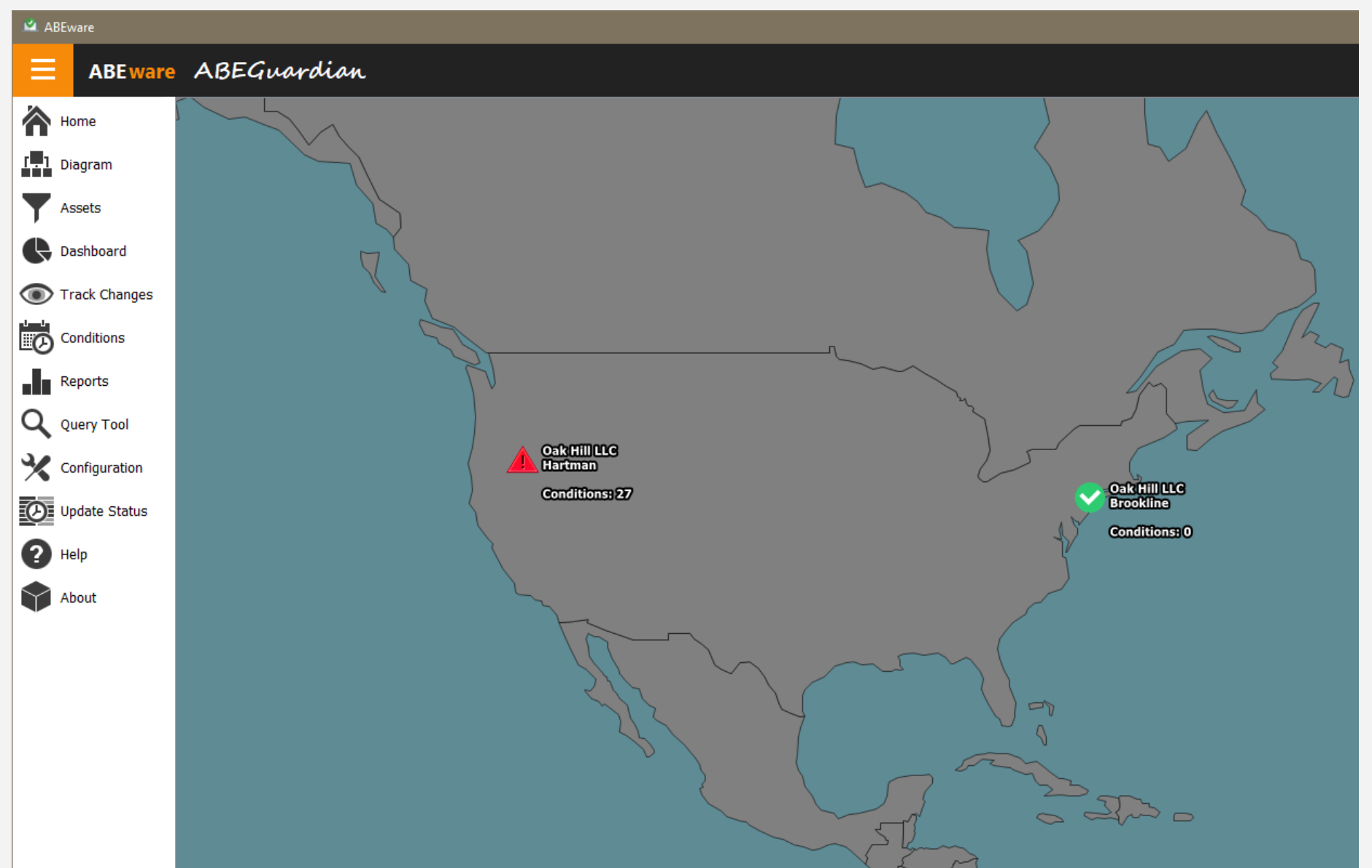
Quickly act againts detected malicious threats with the help of the an advanced Alert System

Report

Monitor all devices proactively to guarantee the best practices defined are being enforced throughout the plant

Multi Site Support

MANAGE ALL YOUR SITES FROM A SINGLE LOCATION, WITH A FULL VISUALIZATION OF YOUR ASSETS AND THREATS



Overview Diagram:

- Oak Hill LLC
 - Hartman
 - Newton Refinery
 - Honeywell DCS
 - Windows Features
 - Watchdog
 - Security
 - Hardware Monitoring
 - Authentication
 - Foxboro DCS

Active Conditions Table:

Type	Device Name	Device Type	Condition Date	Condition	Priority	Details	Category	ACK	Shelved	Ignored
Green	WIN-MIL8SLAFRNS	Computers	2021-02-25 04:24:51 EST	Process Not Running on Device	3	"Entity": "abc" "Status": "Not Running"	Windows Features	🔔	🔊	👁️
Yellow	IASERIES.local	Domains	2021-02-24 07:17:45 EST	Locked Users	2	"Entity": "krtgt" "Source": "ActiveDirectory" "Account Locked Out": "True"	Authentication	🔔	🔊	👁️
Red	LAPTOP-PSHFK182	Computers	2021-02-21 08:14:43 EST	Users with Password set to never expire	1	"Entity": "ricar" "Source": "MicrosoftAccount" "Password Expires": "1970-01-01 00:00:00" "Password Never Expires": null	Authentication	🔔	🔊	👁️
Green	WIN-MIL8SLAFRNS	Computers	2021-02-25 04:14:29 EST	Service Not Running on Device	3	"Entity": "teamviewer2" "Status": "Not Running"	Windows Features	🔔	🔊	👁️
Green	LAPTOP-PSHFK182	Computers	2021-02-24 05:37:27 EST	Devices not Synchronizing with NTP	3	"Entity": "time.nist.gov,0x9" "Root Delay": "0.0000000s" "Last Successful Sync Time": "2021-02-25 21:44:39"	Windows Features	🔔	🔊	👁️
Yellow	LAPTOP-PSHFK182	Computers	2021-02-24 08:23:16 EST	Unsafe USB Device	2	"Name": "USB Composite Device" "Type": "USBTRACK" "Entity": "USB\\VID_0451&PID_3421\\80FF599107930836" "Vendor": "Texas Instruments, Inc." "Product": "Unknown"	Hardware Monitoring	🔔	🔊	👁️
Yellow	LAPTOP-PSHFK182	Computers	2021-02-24 08:23:16 EST	Unsafe USB Device	2	"Name": "USB Composite Device" "Type": "USBTRACK" "Entity": "USB\\VID_046D&PID_C539\\583A5E17948081" "Vendor": "Logitech, Inc." "Product": "Unknown"	Hardware Monitoring	🔔	🔊	👁️

Manage all Conditions

CONDITIONS CAN BE MANAGED LIKE PROCESS ALARMS, WITH ACKNOWLEDGE, SHELVE AND IGNORE CAPABILITIES. STAY ON TOP OF ALL EVENTS AND MAKE SURE NOTHING IS LEFT BEHIND



Manage Vulnerability Exposure

DETECT AND MANAGE VULNERABILITIES APPLICABLE TO DEVICES IN THE PROCESS NETWORK BY CROSS REFERENCING NIST.GOV, MICROSOFT AND VENDOR DATABASE INFORMATION

The screenshot shows the ABEGuardian interface for asset 'LAPTOP-PSHFK182'. Key details include:

- Asset Name:** LAPTOP-PSHFK182
- OS Version:** Microsoft Windows 10 Pro (10.0.19041 N/A Build 19041)
- System Manufacturer:** LENOVO
- System Model:** 20KH02PHUS
- Serial Number:** PFI18QZC
- Processor:** Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
- Memory Usage:** 77.6%
- Vulnerabilities:** A list of 15 CVEs, including CVE-2020-17090, CVE-2020-17040, CVE-2020-0763, etc., with severity levels ranging from High to Critical.

Vulnerability Dashboard

MULTIPLE DASHBOARDS AVAILABLE TO KEEP THE VULNERABILITIES UNDER CONTROL AND FOCUS ON THE HIGHER RISK AND LOWER COMPLEXITY THREATS

The Vulnerabilities Dashboard provides the following key metrics and visualizations:

- Total Vulnerabilities:** 4407
- Vulnerabilities per Score:**
 - Critical: 69
 - High: 3027
 - Medium: 1269
 - Low: 42
- Vulnerability per Score per Day:** A line chart showing the daily count of vulnerabilities categorized by severity (Low, Medium, High, Critical) from 2/19/2021 to 2/27/2021.
- Impact Analysis (Pie Charts):**
 - Integrity Impact:** HIGH 69.93%, NONE 27.39%, LOW 2.68%
 - Confidentiality Impact:** HIGH 86.18%, NONE 9.53%, LOW 4.29%
 - Availability Impact:** HIGH 73.47%, NONE 24.94%, LOW 1.59%
 - Attack Complexity:** HIGH 22.19%, LOW 77.81%
- Attack Vector Criticality Table:**

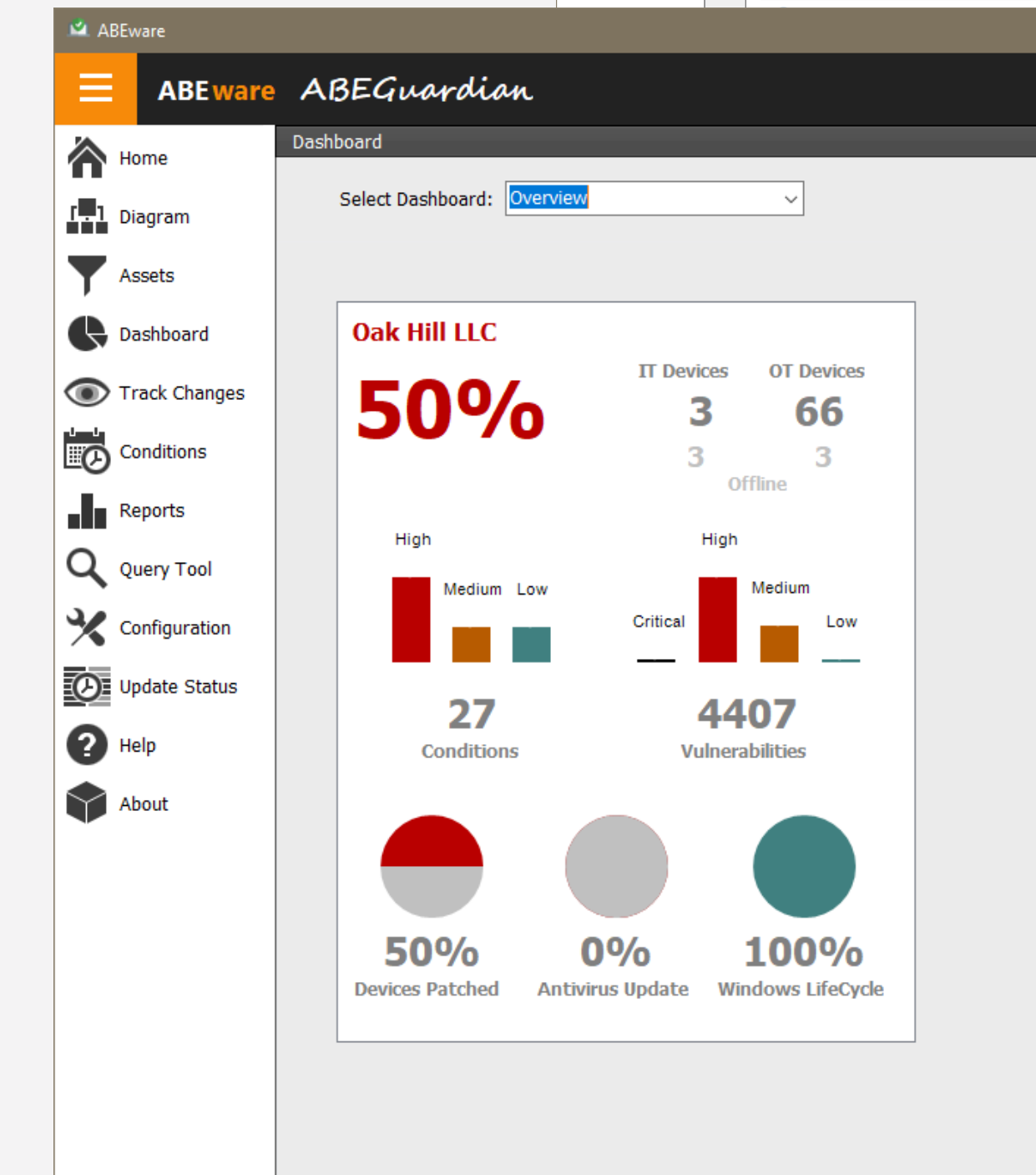
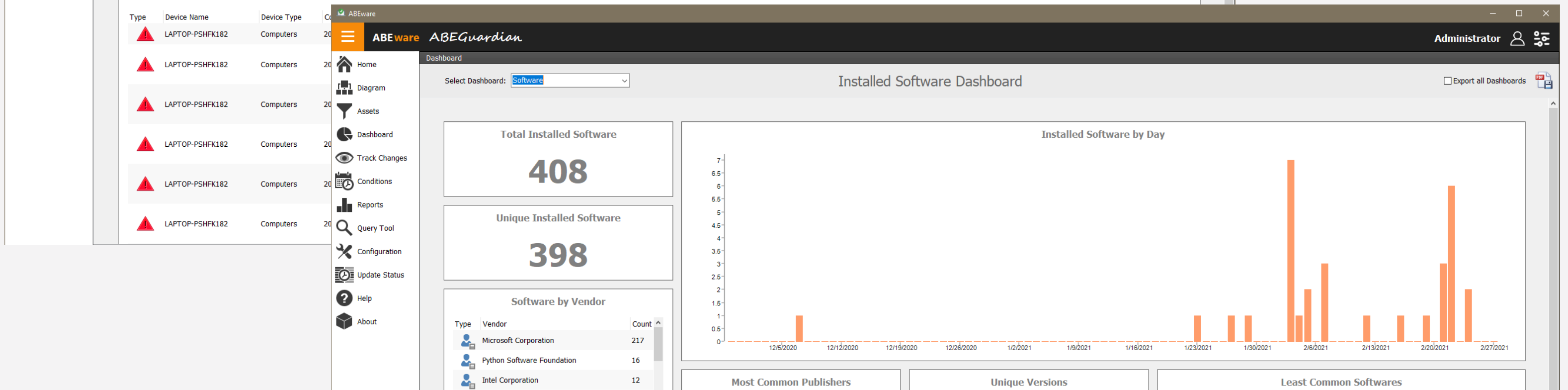
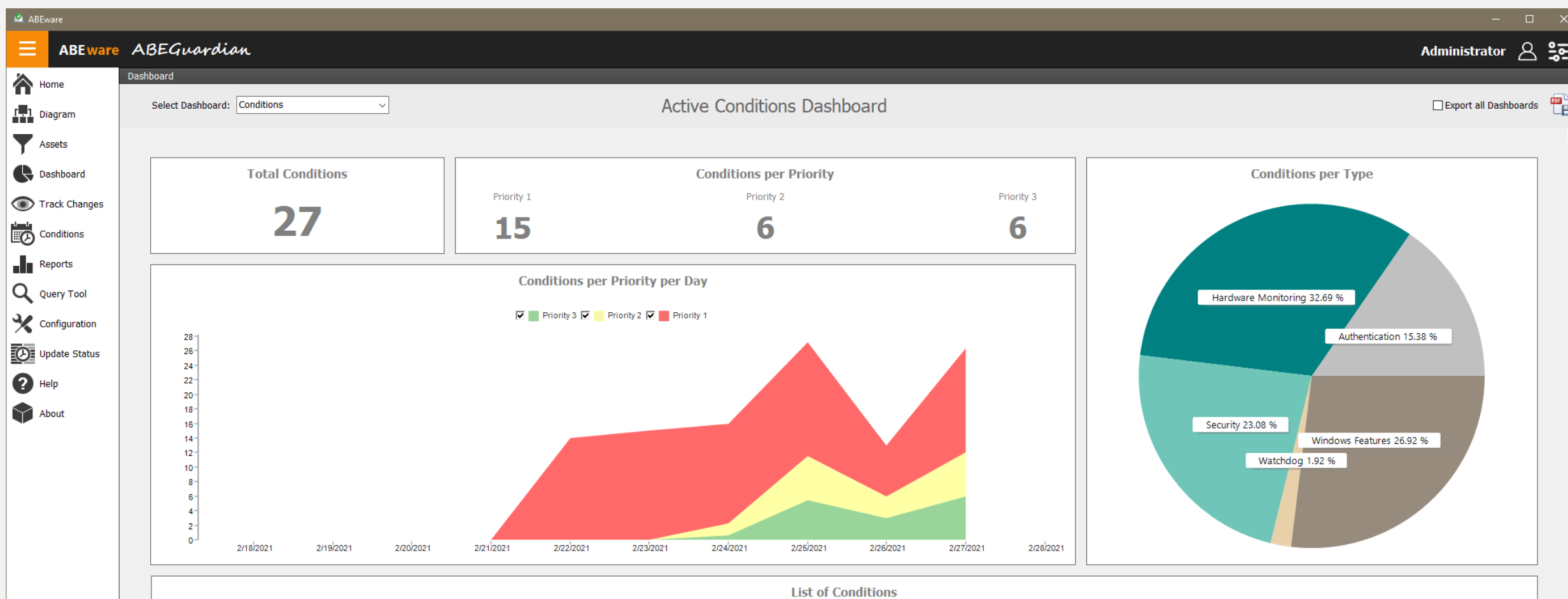
Type	Attack Vector	Severity	Count
LOCAL	LOCAL	HIGH	1912
NETWORK	NETWORK	HIGH	1068
LOCAL	LOCAL	MEDIUM	784
NETWORK	NETWORK	MEDIUM	413
NETWORK	NETWORK	CRITICAL	67
ADJACENT_NETWORK	ADJACENT_NETWORK	MEDIUM	61
ADJACENT_NETWORK	ADJACENT_NETWORK	HIGH	47
NETWORK	NETWORK	LOW	21
LOCAL	LOCAL	LOW	19
PHYSICAL	PHYSICAL	MEDIUM	11
ADJACENT_NETWORK	ADJACENT_NETWORK	LOW	2
ADJACENT_NETWORK	ADJACENT_NETWORK	CRITICAL	2
- List of Vulnerabilities Table:**

Severity	Device Name	CVE	Product	Base Score	Impact Score	Exploitability Score	Integrity	Confidentiality	Availability	Complexity	Attack Vector
Critical	LAPTOP-PSHFK182	CVE-2021-1694	Windows 10 Version 2004 for x64-based Systems	9.8	5.9	3.9	HIGH	HIGH	HIGH	LOW	NETWORK
High	LAPTOP-PSHFK182	CVE-2020-17095	Windows 10 Version 2004 for x64-based Systems	9.9	6.0	3.1	HIGH	HIGH	HIGH	LOW	NETWORK
High	LAPTOP-PSHFK182	CVE-2020-17040	Windows 10 Version 2004 for x64-based Systems	9.8	5.9	3.9	HIGH	HIGH	HIGH	LOW	NETWORK



Condition Monitoring

MONITOR ALL ACTIVE CONDITIONS, EVENTS, PATCH MANAGEMENT, ANTIVIRUS DEFINITION, INSTALLED SOFTWARES AND MUCH MORE



Compare Sites and Plants

COMPARE SITES AND PLANTS USING THE OVERVIEW CARDS. THIS INCLUDES A SUMMARY OF THE MOST IMPORTANT METRICS CALCULATED BY ABEGUARDIAN



External Devices Management

TRACK USB EXTERNAL DEVICES AND STORAGE, FLAG THEM AS SAFE OR UNSAFE AND CREATE ALERTS WHEN UNKNOWN OR UNSAFE DEVICES ARE PLUGGED IN THE NETWORK

The screenshot displays the ABEware ABEGuardian interface for USB Device Management. The main content area is divided into two sections:

Connected USB Devices:

Type	Name	Product	Vendor	Status	Description	Device ID	Secure Device
Realtek USB 3.0 Card Reader	Unknown	Realtek Semiconductor Corp.	OK	Realtek USB 3.0 Card Reader	USB\VID_08DA&PID_0328\28203008282014000		
USB Composite Device	G413 Gaming Keyboard	Logitech, Inc.	OK	USB Composite Device	USB\VID_046D&PID_C33A\028537713235		
Generic USB Hub	TUSB8041 4-Port Hub	Texas Instruments, Inc.	OK	Generic USB Hub	USB\VID_0451&PID_8142\MSFT20140100716C84		
USB Root Hub (USB 3.0)	Generic	Internal USB Root Hub	OK	USB Root Hub (USB 3.0)	USB\ROOT_HUB30\783D7FF298180		
USB Composite Device	Unknown	Acer, Inc.	OK	USB Composite Device	USB\VID_5986&PID_2115\583A5E17B4&088		

USB Activity:

Type	Operation	Datetime	Name	Product	Vendor	Status	Description	Device ID	Secure Device
Disconnected	2021-02-25 09:02:58	USB Mass Storage Device	Survivor Stealth Flash Drive	Corsair	OK	USB Mass Storage Device	USB\VID_1B1C&PID_1A0A\07083A038A1B9F43		
Disconnected	2021-02-25 09:02:58	USB Composite Device	Unknown	Texas Instruments, Inc.	OK	USB Composite Device	USB\VID_0451&PID_8142\80FF599107930836		
Disconnected	2021-02-25 09:02:58	Generic USB Hub	TUSB8041 4-Port Hub	Texas Instruments, Inc.	OK	Generic USB Hub	USB\VID_0451&PID_8142\MSFT20140100716C84		
Disconnected	2021-02-25 09:02:58	USB Composite Device	G413 Gaming Keyboard	Logitech, Inc.	OK	USB Composite Device	USB\VID_046D&PID_C33A\028537713235		
Connected	2021-02-25 09:02:42	USB Mass Storage Device	Survivor Stealth Flash Drive	Corsair	OK	USB Mass Storage Device	USB\VID_1B1C&PID_1A0A\07083A038A1B9F43		
Connected	2021-02-25 09:02:42	Generic USB Hub	TUSB8041 4-Port Hub	Texas Instruments, Inc.	OK	Generic USB Hub	USB\VID_0451&PID_8142\MSFT20140100716C84		
Connected	2021-02-25 09:02:42	USB Composite Device	G413 Gaming Keyboard	Logitech, Inc.	OK	USB Composite Device	USB\VID_046D&PID_C33A\028537713235		
Connected	2021-02-25 09:02:42	USB Composite Device	Unknown	Texas Instruments, Inc.	OK	USB Composite Device	USB\VID_0451&PID_3421\80FF599107930836		
Connected	2021-02-25 09:02:38	Generic USB Hub	TUSB8041 4-Port Hub	Texas Instruments, Inc.	OK	Generic USB Hub	USB\VID_0451&PID_8142\MSFT20140100716C84		
Connected	2021-02-25 09:02:38	USB Composite Device	G413 Gaming Keyboard	Logitech, Inc.	OK	USB Composite Device	USB\VID_046D&PID_C33A\028537713235		
Connected	2021-02-25 09:02:38	USB Composite Device	Unknown	Texas Instruments, Inc.	OK	USB Composite Device	USB\VID_0451&PID_3421\80FF599107930836		
Connected	2021-02-25 09:02:38	USB Mass Storage Device	Survivor Stealth Flash Drive	Corsair	OK	USB Mass Storage Device	USB\VID_1B1C&PID_1A0A\07083A038A1B9F43		

GPO Monitoring

MAKE SURE ALL MACHINES ARE UP TO DATE WITH GROUP POLICIES AND TRACK ANY CHANGES TO THE POLICIES AS THEY HAPPEN TO AVOID MALICIOUS ACTIONS GO UNNOTICED FOR TOO LONG

The screenshot displays the ABEware ABEGuardian interface for GPO Monitoring. The main content area is divided into two sections:

GPO Details:

Type	GPO Name	Group	Owner	Filter Name	Filter Description	User Enabled	Computer E
	Default Domain Policy	IASERIES\Domain Admins	IASERIES\Domain Admins			true	true
	Default Domain Controllers Policy	IASERIES\Domain Admins	IASERIES\Domain Admins			true	true
	TestGPO	IASERIES\Domain Admins	IASERIES\Domain Admins			true	true

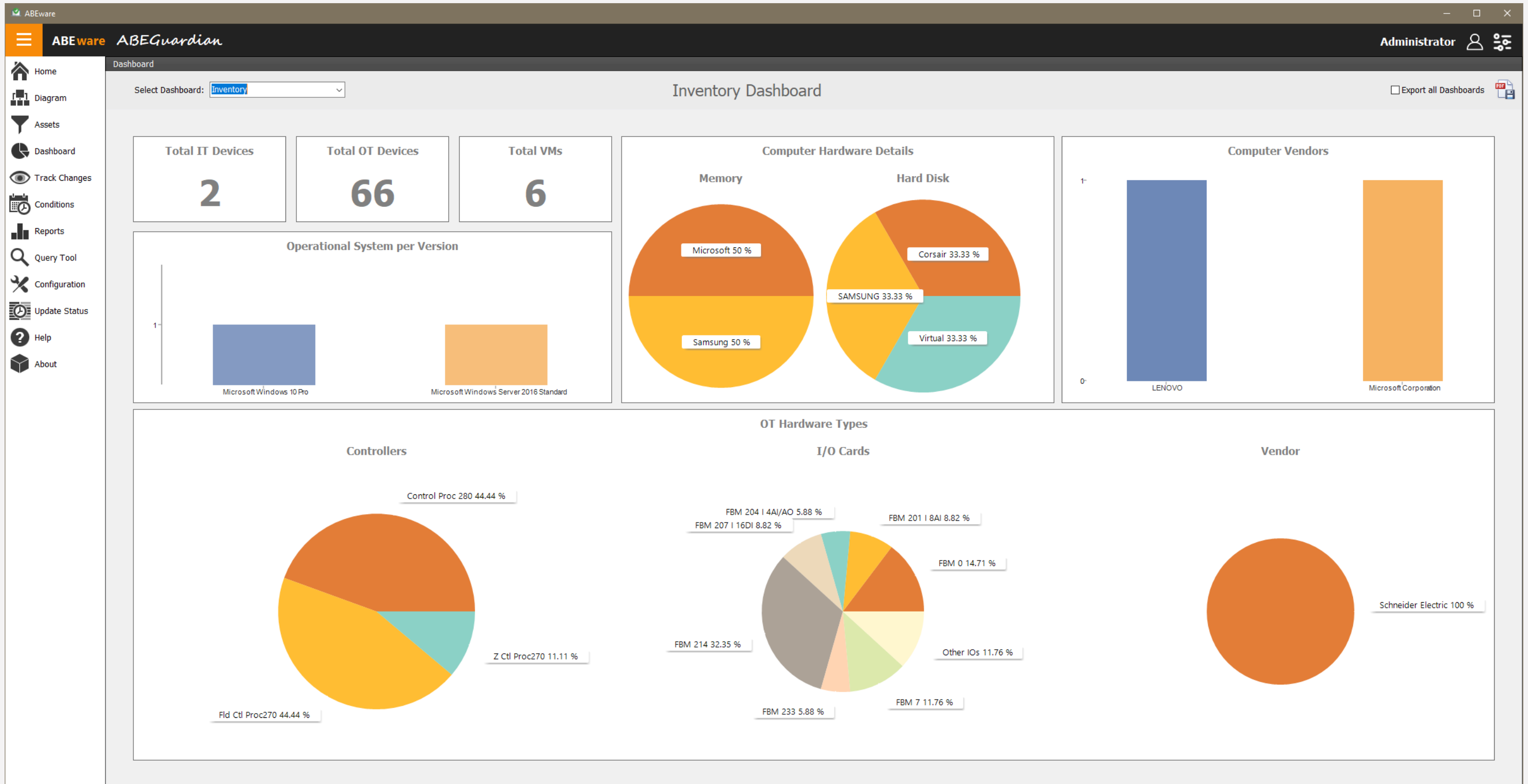
GPO Policies:

Type	Policy Sub Type	Policy Item	Policy Details
GPO Name : Default Domain Controllers Policy (Count = 32)			
GPO Name : Default Domain Policy (Count = 21)			
Scope : Computer (Count = 21)			
Policy Type : Permissions (Count = 3)			
Policy Type : Public Key (Count = 3)			
Policy Type : Security (Count = 15)			
GPO Name : TestGPO (Count = 10)			
Scope : Computer (Count = 9)			
Policy Type : Permissions (Count = 7)			
Policy Type : Security (Count = 2)			
	Event.Log	"AuditLogRetentionPeriod"	"Log": "Security" "Name": "AuditLogRetentionPeriod" "SettingNumber": "1"
	Event.Log	"RetentionDays"	"Log": "Security" "Name": "RetentionDays" "SettingNumber": "7"
Scope : User (Count = 1)			
Policy Type : Registry (Count = 1)			



Inventory Management

DISCOVER AVAILABLE IT AND OT DEVICES, VENDOR, MODEL, FIRMWARE, REVISION AND STATUS. DETECT DEVICES NOT RUNNING PROPERLY AND WITH PENDING UPDATES



The screenshot shows the 'Asset Details' view for a specific device. The table below lists the assets:

Logo	Vendor	Device Name	Type	Model	Status Main	Status Backup	Firmware
	Schneider Electric	ASHLEY	Controller	Control Proc 280	Off	Off	
	Schneider Electric	BROOKE	Controller	Control Proc 280	Off	Off	11
	Schneider Electric	ELOISE	Controller	Control Proc 280	Off	Off	11
	Schneider Electric	FARRAH	Controller	Control Proc 280	On	Off	092028
	Schneider Electric	ALEXIS	Controller	Fld Ctl Proc270	Off	Off	
	Schneider Electric	JASMIN	Controller	Fld Ctl Proc270	On	Off	920041
	Schneider Electric	ROXANN	Controller	Fld Ctl Proc270	Off	Off	20111
	Schneider Electric	SERENA	Controller	Fld Ctl Proc270	Off	Off	20111

Below the table, the details for the selected device 'FARRAH' (Control Proc 280) are shown:

Parameter	Value
@HOST STATION	FARRAH
@SYSTEM NAME	ISMON1
ALARMING STATE	Enabled
CABLE STATE	Both Cables Okay
DIAG STATE	Not Active
DOWNLOAD STATE	Not Downloading
EE UPDATE STATE	Not Updating
FAIL ACK STATE	Acknowledged
FAIL DEV ACK	Acknowledged
FAIL DEV ATT	Yes
FAIL STATE	Not Failed
FT STATE	Operational
MT REPORT STATE	Sync_Not_Config
PRIM EEPROM REV	092028
PRIM HARD DATE	1434
PRIM HARD PART	RH924YA
PRIM HARD REV	CF
PRIM ROM ADDRESS	00006C2E1398
PRIMARY MODE	Married Prim
RUN MODE	On Line
SELF HOSTING	Not Enabled
SHAD EEPROM REV	092028
SHAD HARD DATE	1430
SHAD HARD PART	RH924YA
SHAD HARD REV	CE
SHAD MODE	Married Shad
SHAD ROM ADDRESS	00006C2E063F
SM REPORT STATE	Report All
STATION ADDRESS	00006CC008A

Multi Vendor Support

ABEGUARDIAN SUPPORTS SCHNEIDER FOXBORO, HONEYWELL EXPERION AND EMERSON DELTA-V SYSTEMS, BESIDES MANY MORE OT SYSTEMS.



Other features:

Credential Monitoring

Monitor all logins, log outs, failed login attempts, current users logged in, all credential properties, locked accounts and expired passwords

File Tracking

Select folders and file types to track. Monitor changes, deleted and created files on chosen devices

Services and Process Monitoring

Monitor and Track changes in Windows Services and Processes to detect unwanted changes and unauthorized processes running

Hardware Management

Monitor CPUs, Motherboard, Memory, Hard disk of all Assets and detect unusual behaviors

Query Tool

Create queries across the whole system in a centralized location. This allows users to expand the capabilities of ABEGuardian beyond existing features (secure RESTfull API available for sharing data to other applications)

Security Monitoring

Track Firewall Settings and rules as well as Antivirus configuration (including Windows Defender), detected threats and much more

ABEGuardian

OT Cybersecurity made simple
Full visibility of your OT Systems in a centralized
location.

TALK TO US

+1 281 945 8900

www.sas-web.com

info@sas-web.com

