

System Center EndPoint Protection

LA Mission College uses Microsoft System Center Configuration Manager and System Center EndPoint Protection to manage computers (inventory, software updates/upgrades) and to manage malware. Antimalware policies such as schedule scans, default actions (when malware is found), and protection settings are managed centrally from the server. Settings are updated to all computers.

The screenshot displays the System Center Configuration Manager interface. The main window shows the 'Antimalware Policies' section under 'Endpoint Protection'. A table lists the 'Default Client Antimalware Policy' with a Type of 'Default', Order of 10000, and 0 Deployments. The description states: 'Settings that apply to all clients in the hierarchy, and'. A dialog box titled 'Default Antimalware Policy' is open, showing the configuration for 'Scheduled scans'. The settings are as follows:

Setting	Value
Run a scheduled scan on client computers:	Yes
Scan type:	Full Scan
Scan day:	Friday
Scan time:	4:30 PM
Run a daily quick scan on client computers:	Yes
Daily quick scan schedule time:	7:00 PM
Check for the latest definition updates before running a scan:	Yes
Start a scheduled scan only when the computer is idle:	Yes
Force a scan of the selected scan type if client computer is offline during two or more scheduled scans:	Yes
Limit CPU usage during scans to (%):	30

The server also provides reports, including identification of infected computers, and the remediation status. IT Staff can go directly to a user's computer if remediation failed.

Monitoring > Overview > Endpoint Protection Status > Malware Detected > All Systems

Monitoring > All Systems 23 items

Search

Collection	Threat Name	Severity	Threat Category	Collection Member Count	Computers Infected	Computers Remediated	Remediation Pending	Remediation Failed
All Syste...	HackTool:Win32/Keygen	Moder...	Tool	471	1	0	0	1
All Syste...	PWS:HTML/Bankfraud	Severe	Password Stealer	471	1	1	0	0
All Syste...	PWS:Win32/Zbot!CI	Severe	Password Stealer	471	1	1	0	0
All Syste...	Ransom:HTML/Tescript.D	Severe	Trojan	471	1	1	0	0
All Syste...	SoftwareBundler:Win32/Mizenota	High	Software Bundler	471	2	2	0	0
All Syste...	SoftwareBundler:Win32/OutBrowse	High	Software Bundler	471	1	1	0	0
All Syste...	Trojan:JS/BlacoleRef.CZ	Severe	Trojan	471	1	0	0	1
All Syste...	Trojan:JS/BlacoleRef.W	Severe	Trojan	471	1	0	0	1
All Syste...	Trojan:JS/Redirector.FV	Severe	Trojan	471	1	0	0	1
All Syste...	Trojan:Win32/Dynamerlac	Severe	Trojan	471	1	1	0	0
All Syste...	Trojan:Win32/Glod.B	Severe	Trojan	471	1	1	0	0
All Syste...	Trojan:Win32/Oficla.AE	Severe	Trojan	471	1	0	0	1
All Syste...	Trojan:Win32/Togalrfm	Severe	Trojan	471	1	0	0	1
All Syste...	TrojanDownloader:JS/Swabfex.A	Severe	Trojan Downloa...	471	1	1	0	0
All Syste...	TrojanDownloader:JS/Swabfex.E	Severe	Trojan Downloa...	471	1	1	0	0
All Syste...	TrojanDownloader:O97M/Adnel	Severe	Trojan Downloa...	471	1	1	0	0
All Syste...	TrojanDownloader:Win32/Cutwail.P	Severe	Trojan Downloa...	471	1	0	0	1
All Syste...	TrojanDownloader:Win32/Cutwail.R	Severe	Trojan Downloa...	471	1	0	0	1
All Syste...	TrojanSpy:JS/Paylap.A	Severe	Trojan Monitorin...	471	1	1	0	0
All Syste...	TrojanSpy:JS/Phish.K	Severe	Trojan Monitorin...	471	1	1	0	0
All Syste...	VirTool:JS/Obfuscator.HE	Severe	Tool	471	2	2	0	0
All Syste...	Worm:Win32/Cridex.E	Severe	Worm	471	1	0	0	1
All Syste...	Worm:Win32/Mydoom.A@mm	Severe	Worm	471	1	0	0	1