# #Configurazione# Abilitare la protezione in tempo reale su Endpoint Security V6.0.2EN tramite policy di sicurezza

***Prodotto:** Endpoint Security

***Versione:** 6.0.2EN

# *1. Introduzione

## 1.1 Scenario

Tramite l'appliance Sangfor Endpoint Secure è possibile proteggere le nostre risorse windows e linux e raggrupparle assieme in gruppi specifici.

Quest'aspetto porta a diversi benefici dato che vi è la possibilità di creare altri utenti ed assegnare loro determinate risorse all'interno di specifici gruppi (nel caso si voglia rivendere la soluzione ad aziende esterne in qualità di MSP questo aspetto è essenziale, al fine di garantire un accesso amministrativo solo a gruppi specifici di risorse ai rispettivi IT Manager).

Un' ulteriore vantaggio è dato dalla possibilità di applicare determinate policy ad un gruppo specifico, al fine di permettere l'applicazione della policy a tutte le risorse facenti parte di quel gruppo. Nella seguente guida, vedremo come applicare la protezione in tempo reale a tutte le risorse di un gruppo.

## 1.2 Requisiti

1. La rete dell'utente deve avere l'appliance Endpoint Secure appliance già configurata (in locale od in un cloud pubblico).

2. Avere alcune risorse cui è già stato installato l'agent di Endpoint Secure

# *2. Configurazione

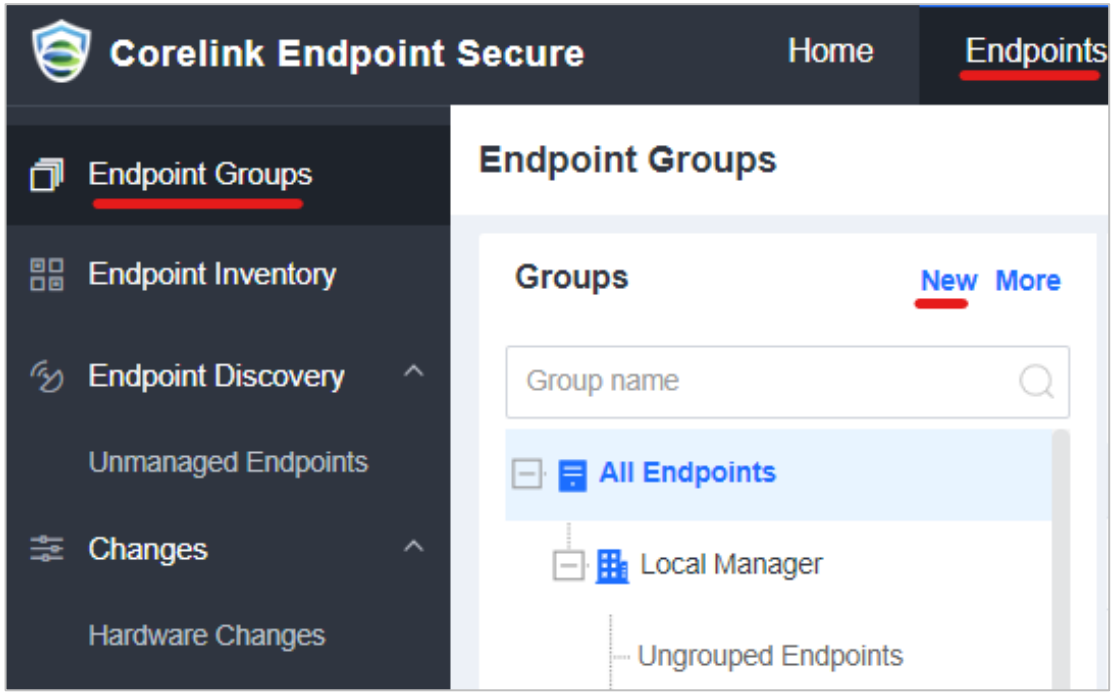
Nella seguente guida, creeremo un gruppo di test e sposteremo delle risorse al suo interno.

## 2.1 Creazione di un gruppo con delle risorse

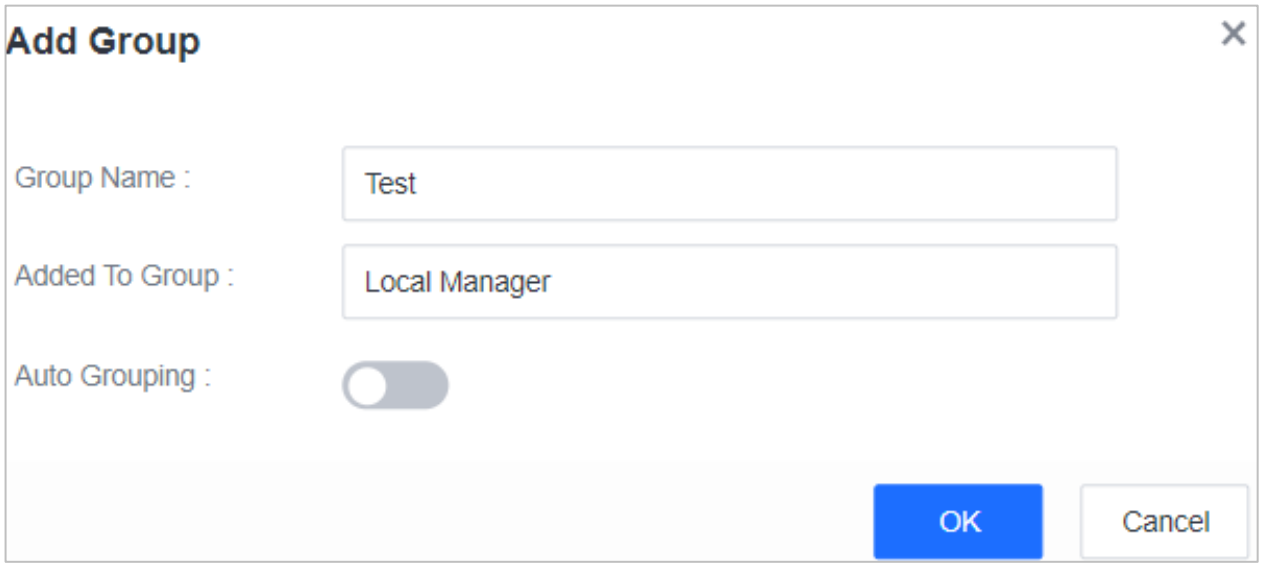
**Passo 1.** Creazione di un gruppo di test

Per creare un gruppo, dall'interfaccia web di Endpoint Secure recarsi su:

**Endpoint > Endpoint Groups > New**




Qui è possibile aggiungere un nuovo gruppo (che chiameremo test in questo esempio):

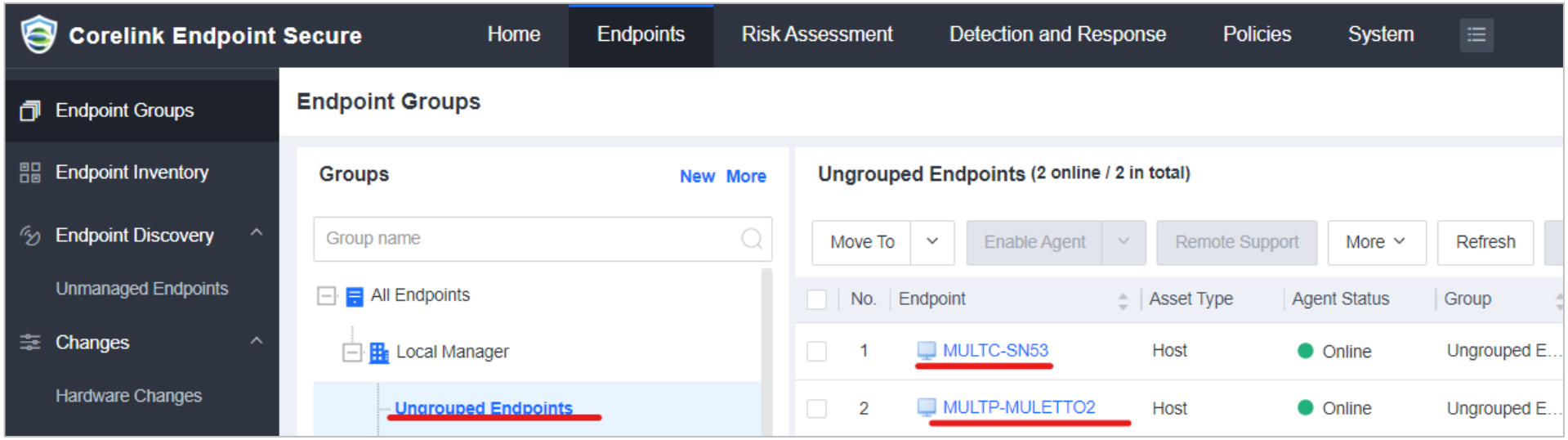



Nella schermata sopra, potete vedere che vi è un opzione per aggiungere un gruppo all'interno di un gruppo esistente.

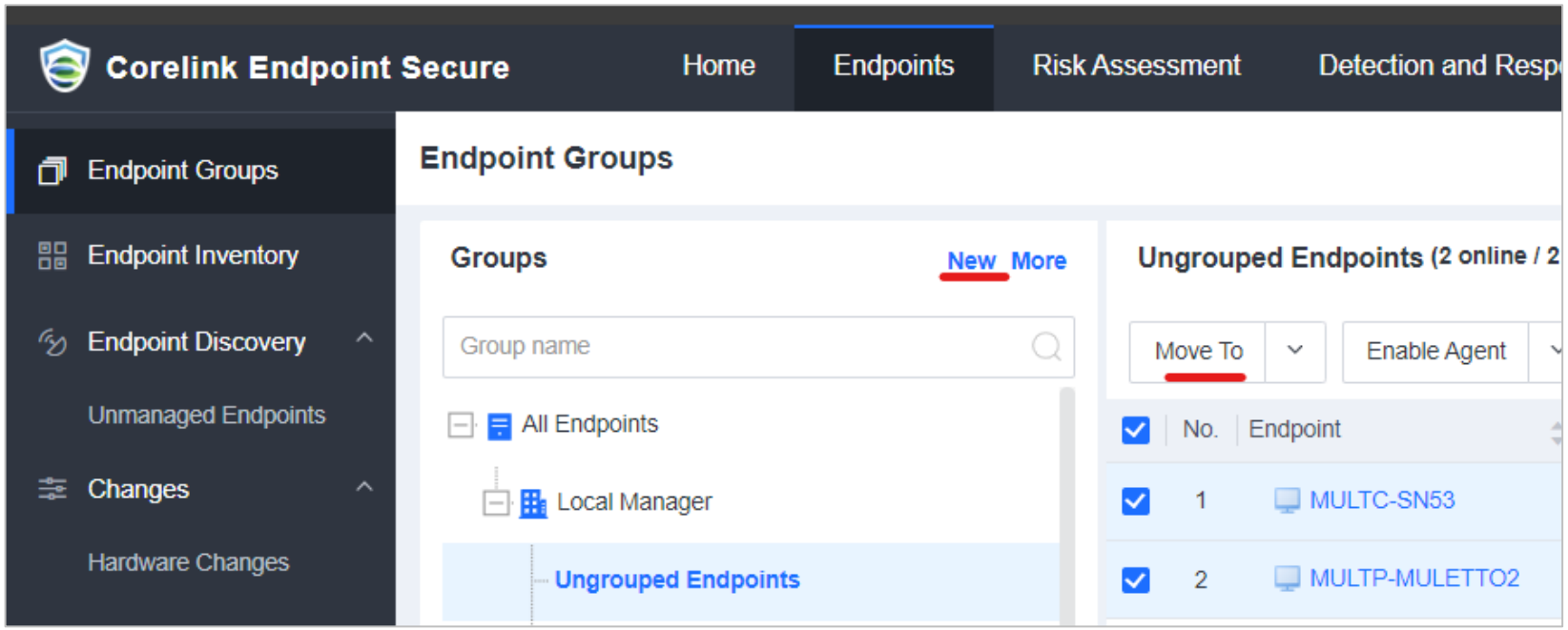
Particolare attenzione riguardo la funzionalità di raggruppamento automatico (Auto Grouping) se pianificate di dare un accesso ad un cliente esterno in quanto potrebbero avere delle sottoreti identiche a quelle già presenti (overlap) e questa funzionalità di raggruppamento automatico sposta automaticamente le risorse in base alla rete di provenienza.

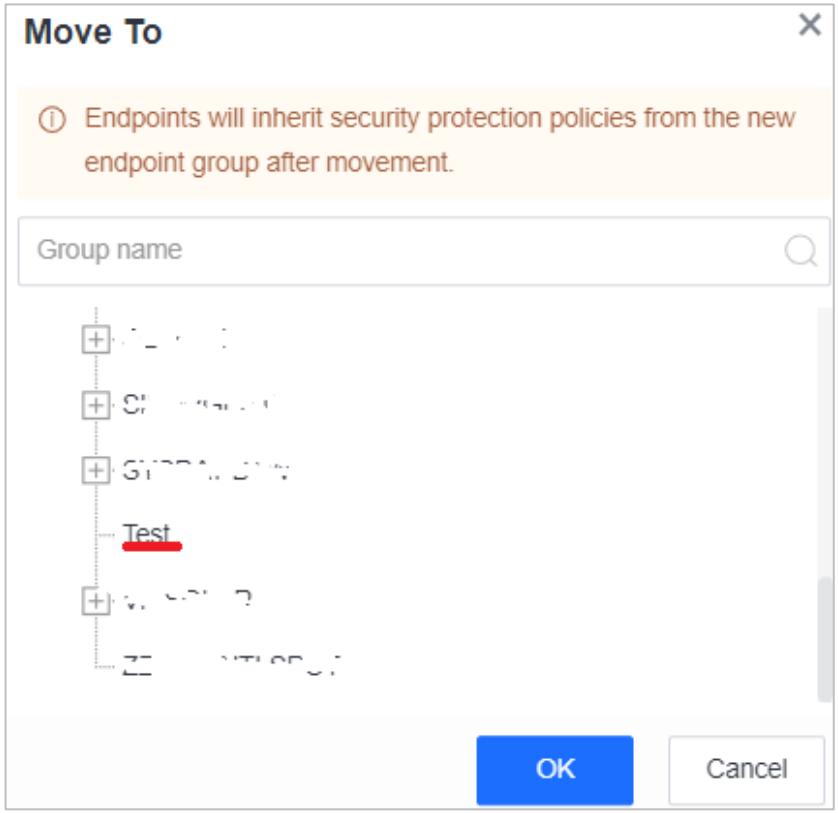
**Passo 2** Spostare risorse specifiche sul nuovo gruppo

Di default, tutti I client cui viene installato Endpoint Secure stanno su questo gruppo di default chiamato Ungrouped Endpoints




Potete selezionare le risorse ed effettuarne lo spostamento nel nuovo gruppo test:



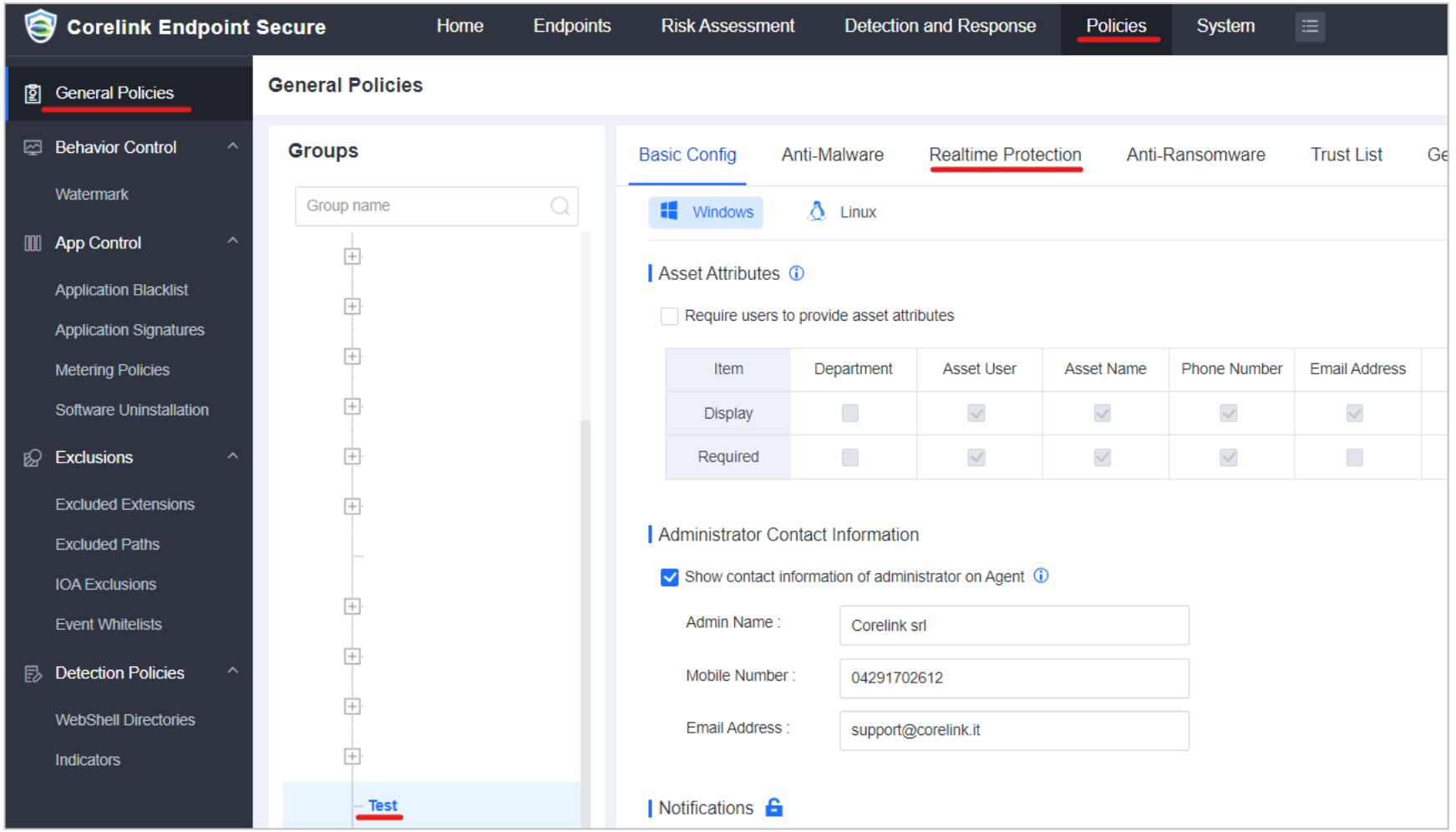



Tenere a mente che il nuovo gruppo creato eredita di default la policy applicata in cima a tutti I gruppi.

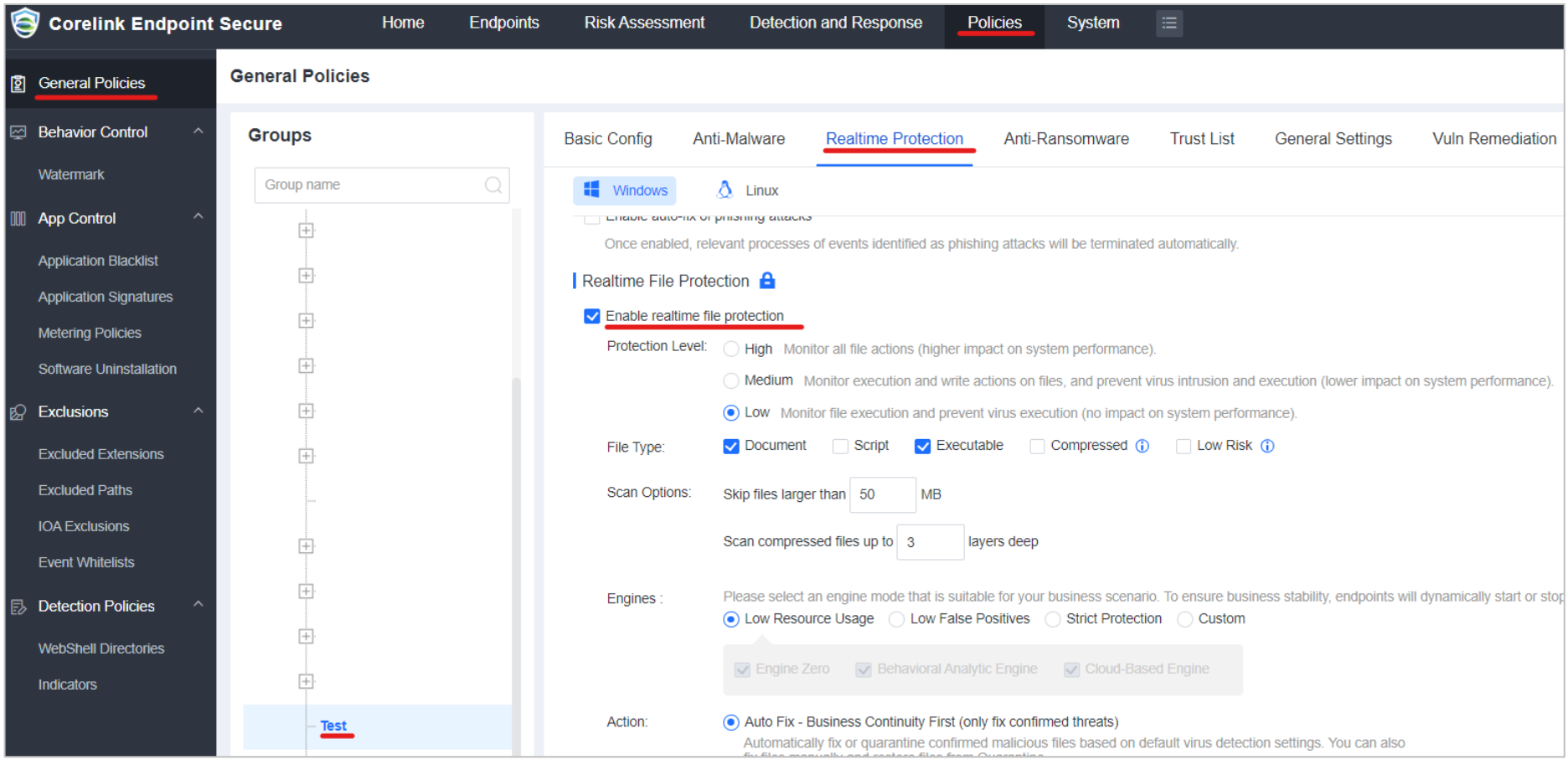
## 2.2 Configurazione Policy

**Passo 1.** A questo punto, nella sezione policies possiamo Vedere che abbiamo una policy con tutti I valori ereditati dalla policy applicate in cima a tutti I gruppi

**Policies > General Policies > Groups**



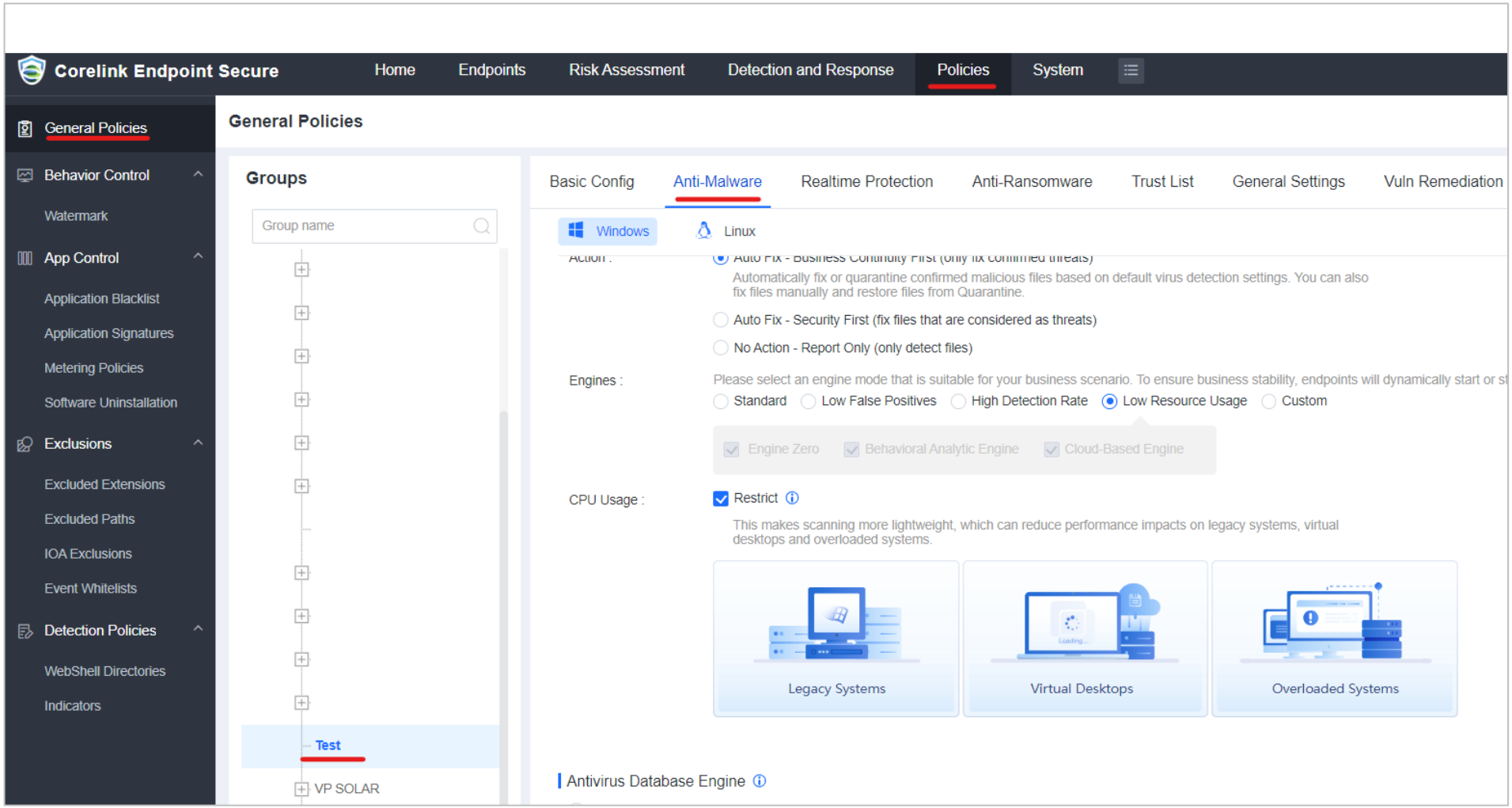

**Passo 2.** In questa sezione è possibile aprire la protezione in tempo reale ed attivare la protezione su tutte le risorse che sono nel gruppo di test:




# *3. Attenzione

1. Tenere a mente che, se avete alcuni client datati, potete raggrupparli in un sottogruppo al fine di modificarne la relativa policy.

Da prove effettuate, su queste risorse datate è meglio attivare la protezione in tempo reale con le seguenti impostazioni al fine di impostare un basso impatto sulle performance riguardo l'antivirus e non interferire con le attività giornaliere degli utenti che usano queste risorse datate.


Corelink Endpoint Secure
Home
Endpoints
Risk Assessment
Detection and Response
Policies
System
General Policies
Behavior Control
Watermark
App Control
Application Blacklist
Application Signatures
Metering Policies
Software Uninstallation
Exclusions
Excluded Extensions
Excluded Paths
IOA Exclusions
Event Whitelists
Detection Policies
WebShell Directories
Indicators
General Policies
Groups
Group name
Test
VP SOLAR
Basic Config
Anti-Malware
Realtime Protection
Anti-Ransomware
Trust List
General Settings
Vuln Remediation
Windows
Linux
Automatically fix or quarantine confirmed malicious files based on default virus detection settings. You can also fix files manually and restore files from Quarantine.
Auto Fix - Security First (fix files that are considered as threats)
No Action - Report Only (only detect files)
Engines :
Please select an engine mode that is suitable for your business scenario. To ensure business stability, endpoints will dynamically start or st
Standard
Low False Positives
High Detection Rate
Low Resource Usage
Custom
Engine Zero
Behavioral Analytic Engine
Cloud-Based Engine
CPU Usage :
Restrict
This makes scanning more lightweight, which can reduce performance impacts on legacy systems, virtual desktops and overloaded systems.
Legacy Systems
Virtual Desktops
Overloaded Systems
Antivirus Database Engine