

#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

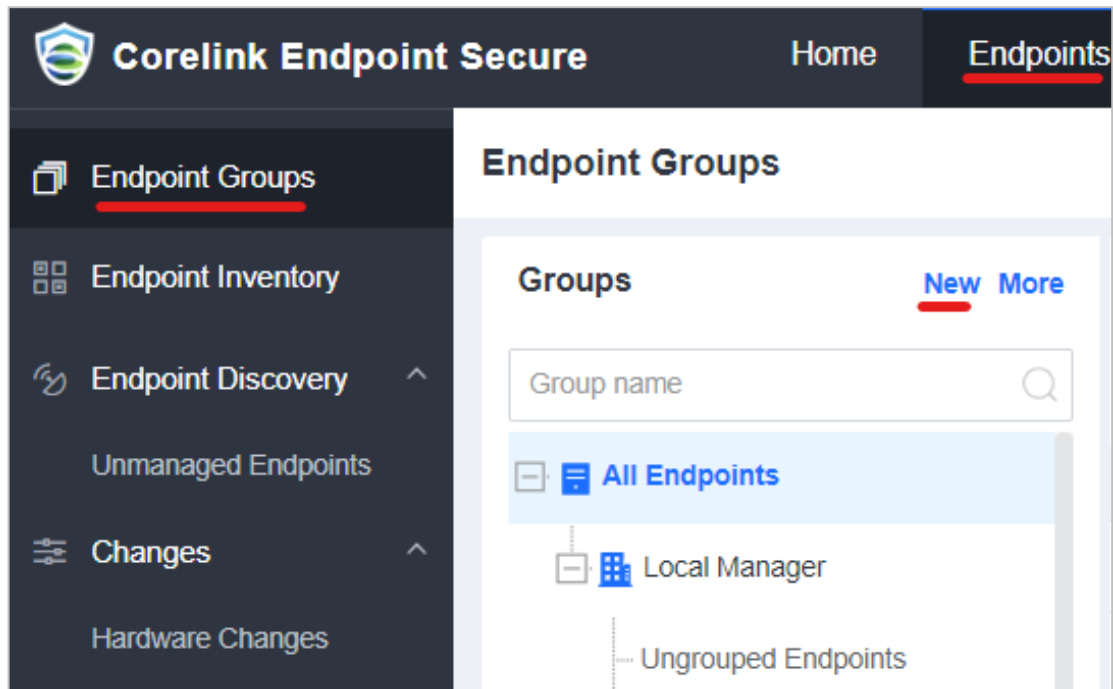
Nella seguente guida, creeremo un gruppo di test e sposteremo delle risorse al suo interno.

2.1 Creazione di un gruppo con delle risorse

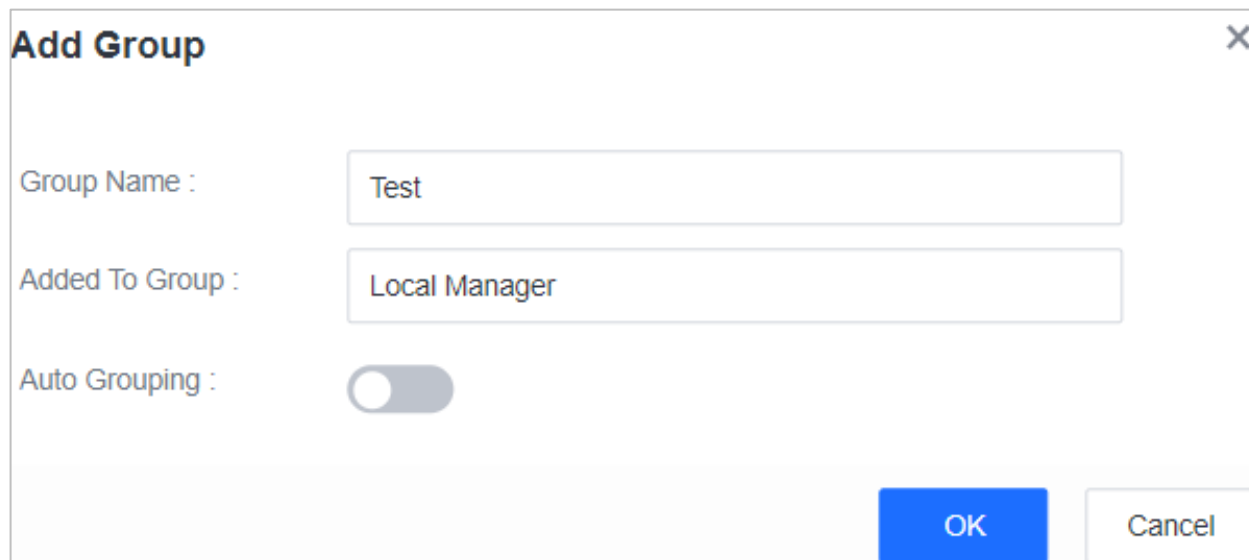
Passo 1. Creazione di un gruppo di test

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):



Add Group [X]

Group Name :

Added To Group :

Auto Grouping : ☐


OK Cancel

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

Corelink Endpoint Secure

HomeEndpointsRisk AssessmentDetection and ResponsePoliciesSystem

Endpoint Groups

Endpoint Inventory

Endpoint Discovery

Unmanaged Endpoints

Changes

Hardware Changes

Endpoint Groups

Groups

NewMore

Group name

All Endpoints

Local Manager


Unarouped Endpoints

Ungrouped Endpoints (2 online / 2 in total)

Move ToEnable AgentRemote SupportMoreRefresh

No.	Endpoint	Asset Type	Agent Status	Group
1	MULTC-SN53	Host	Online	Ungrouped E...
2	MULTP-MULETTO2	Host	Online	Ungrouped E...

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

Corelink Endpoint Secure

HomeEndpointsRisk AssessmentDetection and Respo

Endpoint Groups

Endpoint Inventory

Endpoint Discovery

Unmanaged Endpoints

Changes

Hardware Changes

Endpoint Groups

Groups

NewMore

Group name

All Endpoints

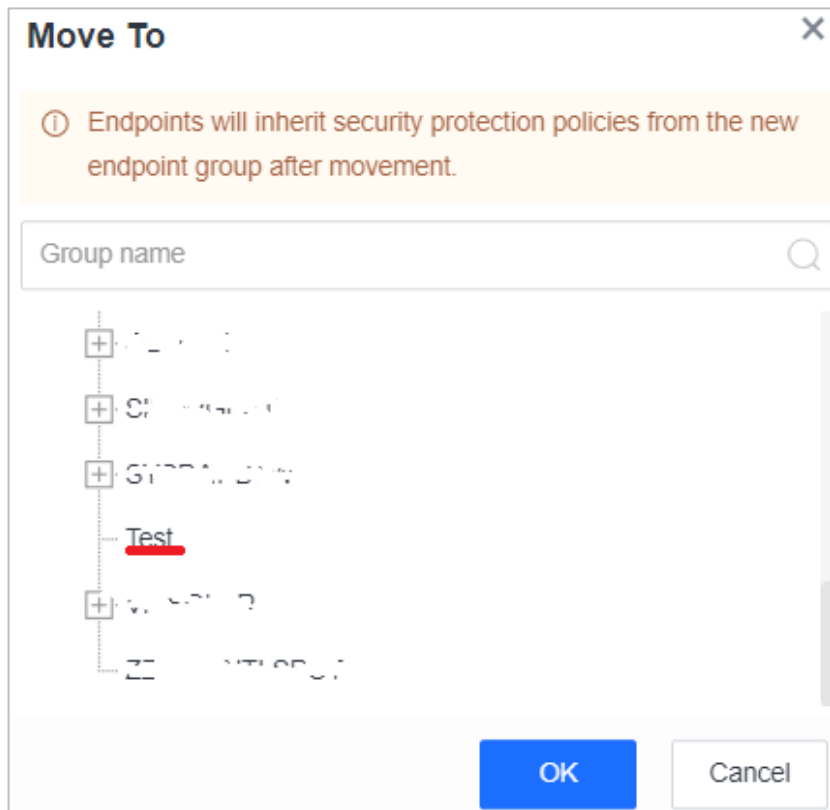
Local Manager

Ungrouped Endpoints

Ungrouped Endpoints (2 online / 2

Move ToEnable Agent

No.	Endpoint
1	MULTC-SN53
2	MULTP-MULETTO2

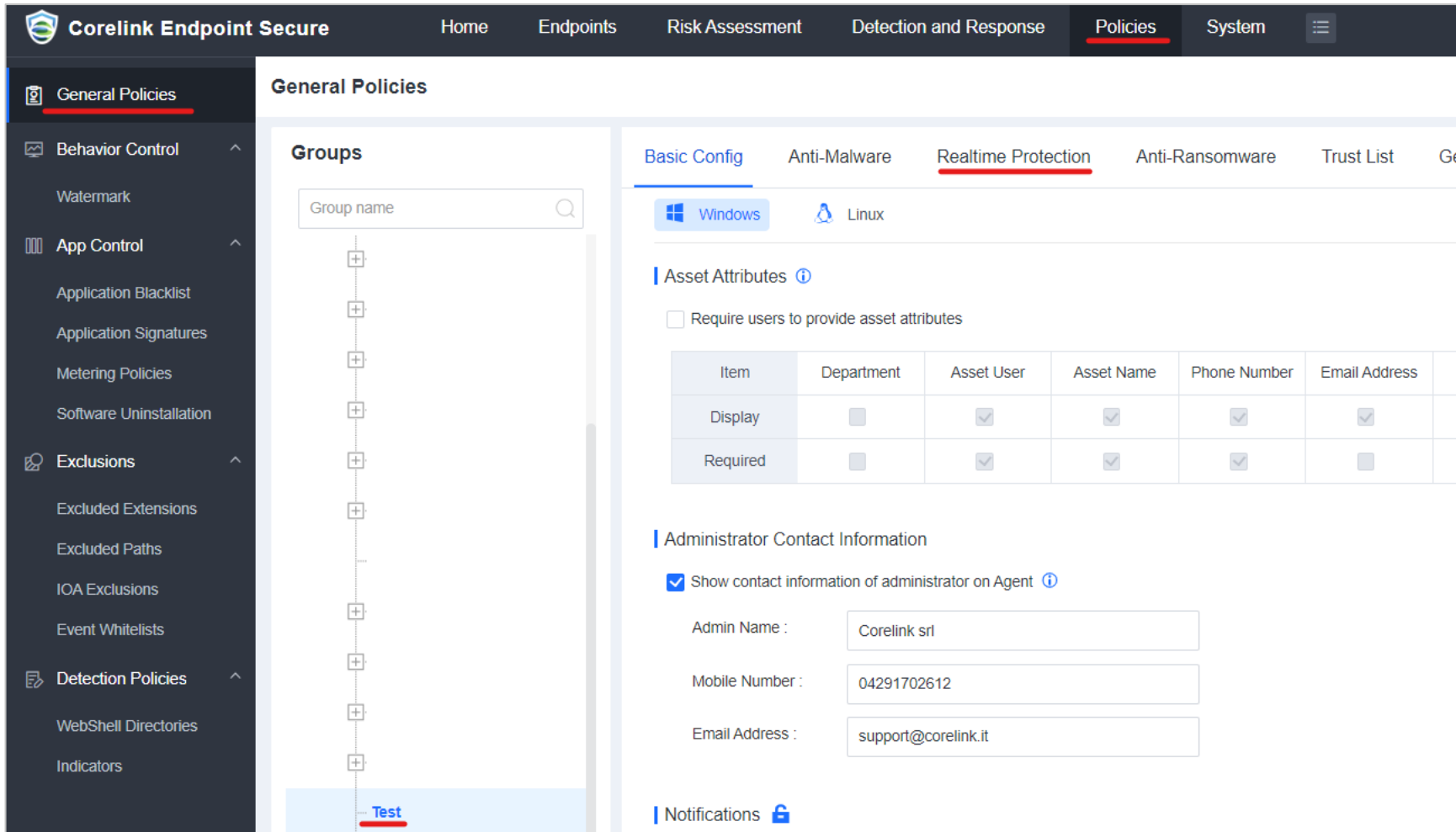


Tenere a mente che il nuovo gruppo creato eredita di default la policy applicata in cima a tutti I gruppi.

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:

The screenshot displays the 'Corelink Endpoint Secure' management console. The top navigation bar includes 'Home', 'Endpoints', 'Risk Assessment', 'Detection and Response', 'Policies' (highlighted), and 'System'. The left sidebar lists various policy categories: 'General Policies' (selected), 'Behavior Control', 'App Control', 'Exclusions', 'Detection Policies', and 'Indicators'. The main content area is titled 'General Policies' and contains a 'Groups' list on the left and a configuration panel on the right. The 'Groups' list has a search bar and a vertical stack of group icons, with a 'Test' button at the bottom. The configuration panel has tabs for 'Basic Config', 'Anti-Malware', 'Realtime Protection' (selected), 'Anti-Ransomware', 'Trust List', 'General Settings', and 'Vuln Remediation'. Under 'Realtime Protection', the 'Windows' tab is active. The 'Enable auto-fix or phishing attacks' checkbox is unchecked. The 'Realtime File Protection' section has 'Enable realtime file protection' checked. The 'Protection Level' is set to 'Low'. The 'File Type' settings include 'Document' and 'Executable' checked. The 'Scan Options' show 'Skip files larger than 50 MB' and 'Scan compressed files up to 3 layers deep'. The 'Engines' section shows 'Low Resource Usage' selected, with 'Engine Zero', 'Behavioral Analytic Engine', and 'Cloud-Based Engine' all checked. The 'Action' is set to 'Auto Fix - Business Continuity First (only fix confirmed threats)'.

*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.



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

Action :

☒ Auto Fix - Business Continuity First (only fix confirmed threats)

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 stop engines based on the selected mode.

☐ 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