Deploy - How to

Versione	Data	Redattore	Descrizione
0.3	14/07/2025	Davide Marin	Aggiunto e iniziato a redigere capitolo “Guida alla creazione delle politiche di protezione”
0.2	27/06/2025	Davide Marin	Stesura sezioni “Installare Security Server” e “Guida all’integrazione di Active Directory”
0.1	26/06/2025	Davide Marin	Creazione documento e inizio stesura

Indice

Lista delle immagini

1. Guida al deploy di GravityZone

Questa guida ha lo scopo di essere più diretta e semplice possibile, per permettere un'installazione semplice e veloce di GravityZone. La guida ufficiale e completa è invece disponibile **qui**.

1.1. GravityZone Control Center

Questa è la parte più semplice, ma fondamentale. Collegarsi alla pagina di login di GravityZone, e inserire le credenziali relative al proprio account, impostare il 2FA o SSO e continuare.

A questo punto ci verrà richiesto di creare almeno un pacchetto di installazione per i nostri agent che dovremmo installare sugli endpoint.

1.2. Installare Security Server (per ambienti con macchine virtuali)

Security server è necessario da essere installato su uno o più host, in base a quante macchine virtuali di devono gestire. L'host con security server installato centralizza la maggior parte delle attività anti-malware, e si comporta come un server per scansionare le macchine virtuali.

Innanzitutto, scaricare il pacchetto di installazione di Security Server di default (disponibile in Network -> Installation Packages), poi, installarlo sul endpoint che si vuole utilizzare come Security Server.

Successivamente è richiesto di configurare il Security Server si può fare tramite interfaccia locale, guida dettagliata disponibile **qui**, oppure tramite "sva-setup command", con guida dettagliata disponibile **qui**

1.3. Installare gli agenti

Per garantire la sicurezza degli endpoint (fisici e virtuali), è necessario installare l'agente di sicurezza su ciascun dispositivo. GravityZone offre diversi metodi per l'installazione degli agenti:

- **Installazione locale**
- **Installazione da remoto**: modalità in cui mi concentrerò in questa guida.

È importante che al primo endpoint sul quale andiamo ad installare l'agente venga assegnato il ruolo di Relay, questo per poter installare da remoto gli agenti sugli altri endpoint. Inoltre, l'endpoint che ha il ruolo di Relay deve essere sempre acceso e connesso alla rete per permettere agli altri endpoint di comunicare con il Control Center.

Una volta installato l'agente con ruolo Relay, sarà possibile, tramite la finestra all'interno della sezione "Network", installare gli agenti sugli altri endpoint da remoto. Per farlo, bisogna prima creare un pacchetto di installazione, operazione possibile nella finestra che si apre selezionando "Installation packages" nel menu a sinistra.

Sulla finestra che si apre, cliccare su "Create", compilare i campi e prestare attenzione a selezionare tutti i moduli che si vogliono utilizzare sugli endpoint (è comunque possibile modificare i moduli in seguito, per ogni endpoint), e salvare.

Una volta creato il pacchetto, andare nella pagina “Network”, selezionare tutti gli endpoint sui quali si vuole installare l’agente e cliccare “Action” e poi “install agent”. Nella finestra che si apre, bisogna inserire le credenziali di amministratore dell’endpoint (se si ha selezionato un gruppo di endpoint sotto ad un DC, inserire le credenziali del domain administrator), selezionare il Relay a cui fare “affidamento” ed infine il pacchetto di installazione desiderato. Questo installerà l’agente su tutti gli endpoint selezionati.

2. Guida all’integrazione di Active Directory

Per integrare Active Directory con GravityZone, è sufficiente accedere a GravityZone Control Center, andare nella sezione “Network” e selezionare l’endpoint che si vuole utilizzare come integratore di Active Directory. Una volta selezionato, cliccare su “Action” e poi “Set as Active Directory Integrator”.

Ora GravityZone si sincronizzerà con Active Directory ogni ora.

Per indicazioni aggiuntive e troubleshooting, è possibile consultare la guida ufficiale **qui**.

3. Guida alla creazione delle politiche di protezione

Il primo passo, è andare nella sezione “Policies” dal menu a sinistra e cliccare su “Add”.

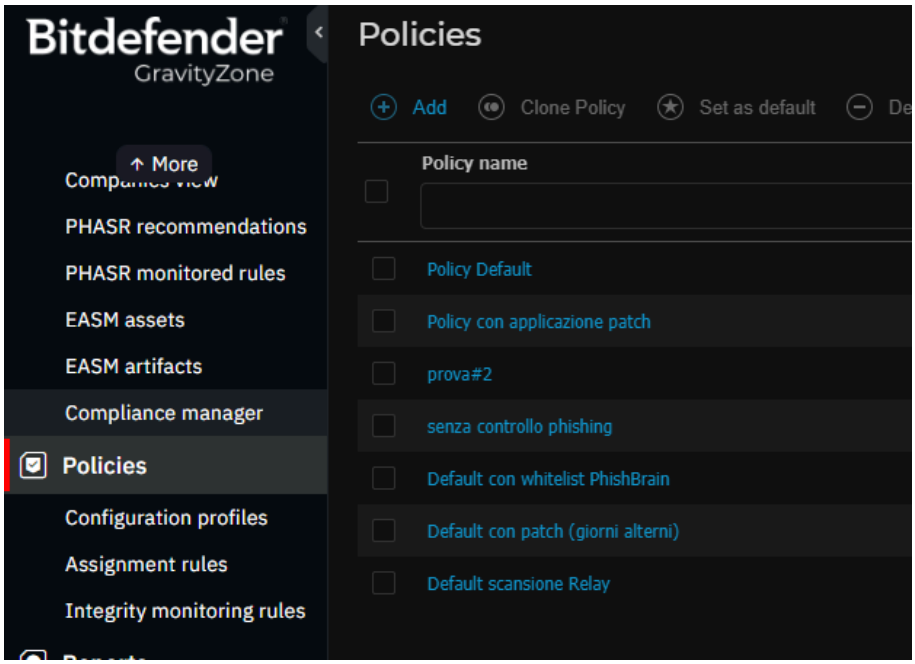

Figure 1: Aggiungi nuova politica di protezione

Dalla finestra che si apre, è possibile definire nello specifico la policy, esploriamo le varie sezioni, che si suddividono in due gruppi principali: “General” e “Protection & Monitoring”.

3.1. General

Sotto a “General” è possibile definire le impostazioni relative alla policy e agli agenti.

3.1.1. Policy

Nella sezione “policy” è possibile definire le informazioni base della policy.

3.1.1.1. Details

Qui è possibile definire il nome della politica e se essa è collaborativa o meno. È inoltre possibile inserire i contatti del supporto tecnico visualizzati dagli utenti sui loro endpoint, che di base sono quelli del supporto ufficiale di Bitdefender.

3.1.1.2. Inheritance Rules

In questa pagina è possibile scegliere se “ereditare” la configurazione di un determinato modulo da un’altra policy. Attenzione, scegliendo di ereditare le regole da un’altra policy, si andrà a creare “un puntatore” alla policy da cui si ereditano le regole, e non una copia delle regole; modificando la policy da cui si ereditano le regole quindi, le modifiche verranno applicate anche a quella corrente.

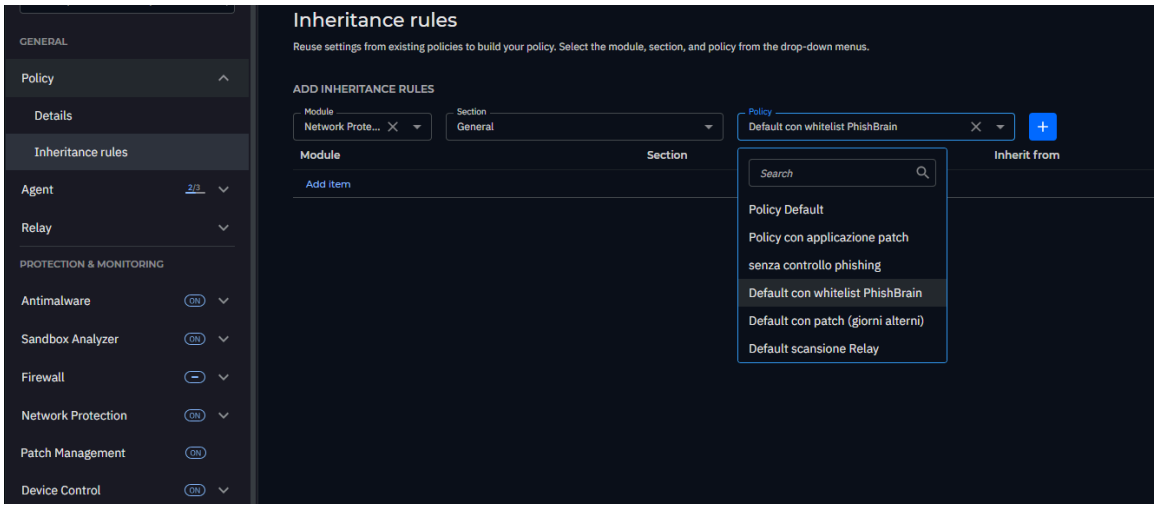

Figure 2: Aggiungi ereditarietà di un modulo

3.1.1.3. Best Practices

Per la configurazione della voce "Policy", si consiglia di non aggiungere regole di ereditarietà, a meno che non si sia sicuri che le possibili modifiche apportate al modulo della policy "madre" vadano bene anche per la policy corrente; in tutti gli altri casi, è consigliato clonare la policy madre per poter lavorare sulle due politiche indipendentemente.

3.1.2. Agent

Nella sezione "Agent" è possibile definire le impostazioni relative agli agenti che utilizzeranno questa policy.

3.1.2.1. Notifications

In questa pagina si possono scegliere quali notifiche vedranno gli utenti sui loro endpoint; è possibile scegliere sia la tipologia di notifica, sia per quali eventi mostrarle.

3.1.2.2. Settings

In questa pagina è possibile definire alcune impostazioni riguardanti l'installazione e i permessi dell'agente. È possibile infatti inserire impostare una password per limitare la disinstallazione dell'agente, impostare il server di proxy se presente, e rendere o meno l'agente un "Power User". Il Power User è un utente che, tramite console, può gestire le proprie impostazioni della policy.

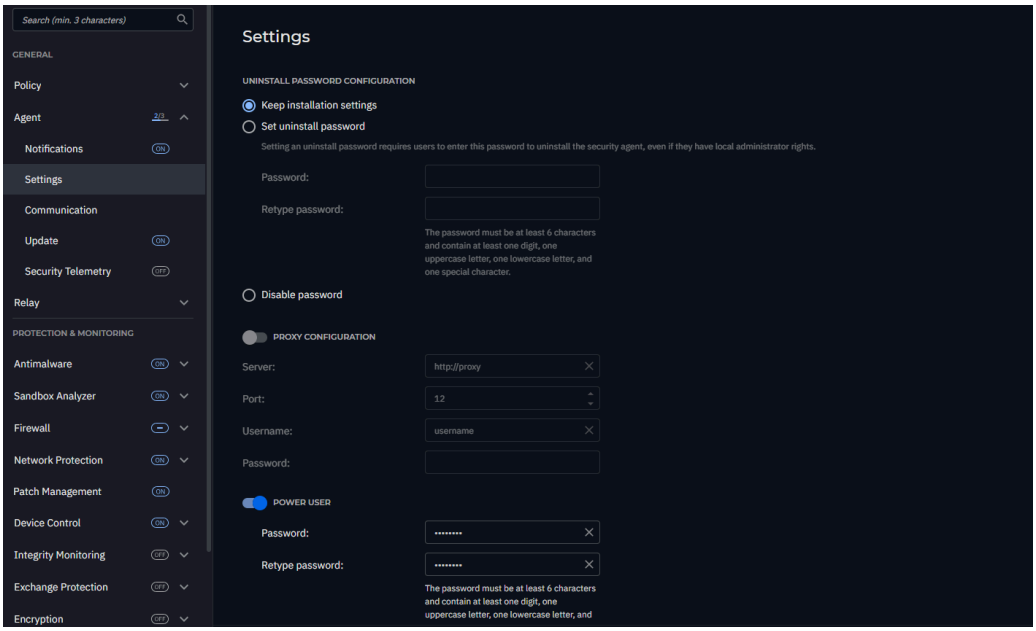

Figure 3: Impostare il power user

3.1.2.3. Communication

Qui è possibile impostare con quale endpoint con ruolo “Relay” comunicare, e impostare diverse priorità in caso ci fossero più Relay. Impostare la comunicazione con il relay aiuta ad alleggerire il carico di lavoro sugli endpoint, delegando la comunicazione con il Control Center al relay.

3.1.2.4. Update

In questa pagina è possibile definire le impostazioni relative agli aggiornamenti degli agenti, come ad esempio la frequenza di aggiornamento del prodotto e dei sistemi di sicurezza.

3.1.2.5. Security Telemetry

In caso si disponesse di un server SIEM (soluzione di gestione delle informazioni e degli eventi di sicurezza), è possibile configurare la comunicazione con quest’ultimo in questa pagina.

3.1.2.6. Best Practices

3.1.3. Relay

3.2. Protection & Monitoring

3.2.1. Antimalware

3.2.2. Sandbox Analyzer

3.2.3. Firewall

3.2.4. Network Protection

3.2.5. Patch Management

3.2.6. Device Control

3.2.7. Incident Sensori

3.2.8. Risk Management

3.2.9. Blocklist

3.2.10. Live Search

4. Guida al patch management

5. Altre funzionalità