Deploy - How to

Versione	Data	Redattore	Descrizione
0.4	16/07/2025	Davide Marin	Continuo stesura capitoli 2 e 5
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

1. Guida al deploy di GravityZone 5
   1.1. Accedere a GravityZone Control Center 5
   1.2. Installare Security Server (solo per endpoint con poche risorse) 5
   1.3. Installare gli agenti 5
   1.4. Integrazione di Active Directory 6
2. Guida alla creazione delle politiche di protezione 7
   2.1. General 7
      2.1.1. Policy 7
      2.1.2. Agent 8
      2.1.3. Relay 10
   2.2. Protection & Monitoring 10
      2.2.1. Antimalware 10
      2.2.2. Sandbox Analyzer 11
      2.2.3. Firewall 12
      2.2.4. Network Protection 12
      2.2.5. Patch Management 12
      2.2.6. Device Control 13
      2.2.7. Incident Sensor 13
      2.2.8. Risk Management 13
      2.2.9. Blocklist 13
      2.2.10. Live Search 13
3. Guida alla gestione dei tag 14
4. Guida al patch management 15
5. Altre funzionalità 16
   5.1. Creazione Maintenance Windows 16
      5.1.1. Best Practices 16
   5.2. Creazione Web Access Control Scheduler 17
   5.3. Creazione liste di esclusioni 17

Lista delle immagini

Figure 1 Aggiungi nuova politica di protezione 7
Figure 2 Aggiungi ereditarietà di un modulo 8
Figure 3 Impostare il power user 9
Figure 4 Esempio notifiche Agent 10
Figure 5 Impostazioni di scansione 11
Figure 6 Maintenance Window 16
Figure 7 Patch Caching Server 17

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. Accedere a 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 (solo per endpoint con poche risorse)

Security server è necessario da essere installato su uno o più host, in base a quante macchine si 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.

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.

1.4. 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**.

2. Guida alla creazione delle politiche di protezione

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

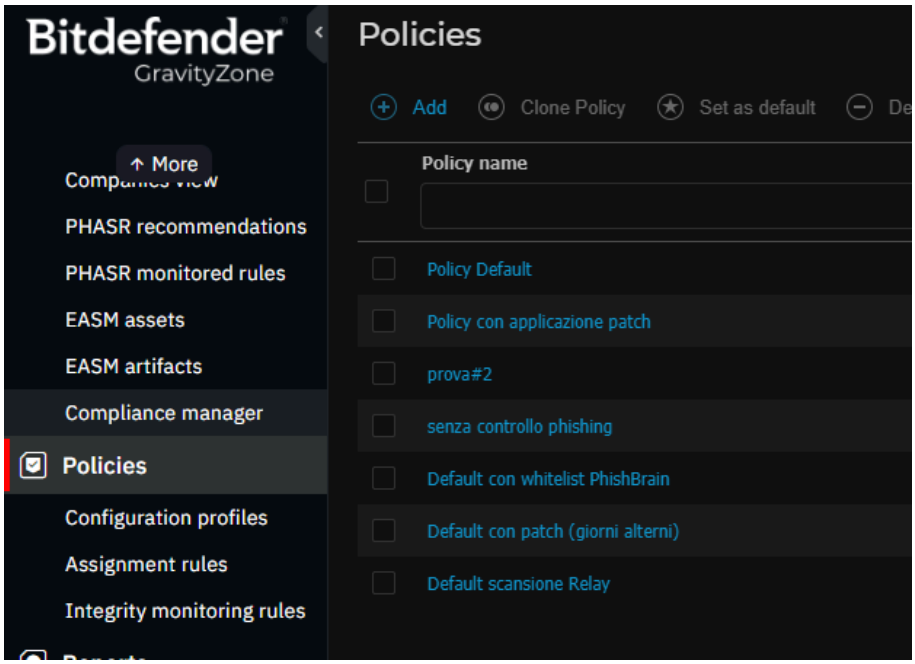

Figure 1: Aggiungi nuova politica di protezione

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”.

2.1. General

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

2.1.1. Policy

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

- **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.
- **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.

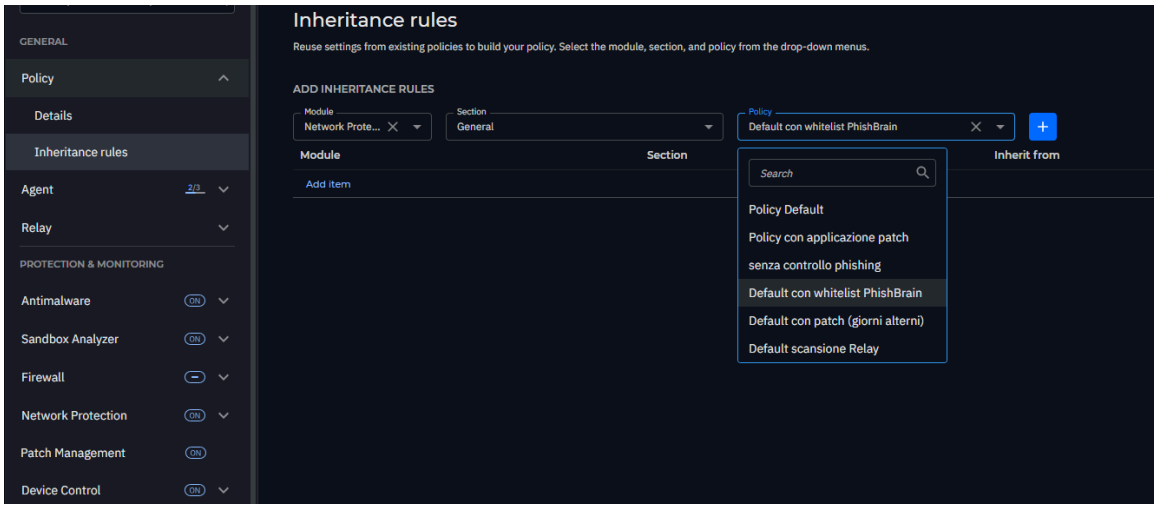

Figure 2: Aggiungi ereditarietà di un modulo

2.1.1.1. 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 in futuro 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.

2.1.2. Agent

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

- **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.
- **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.

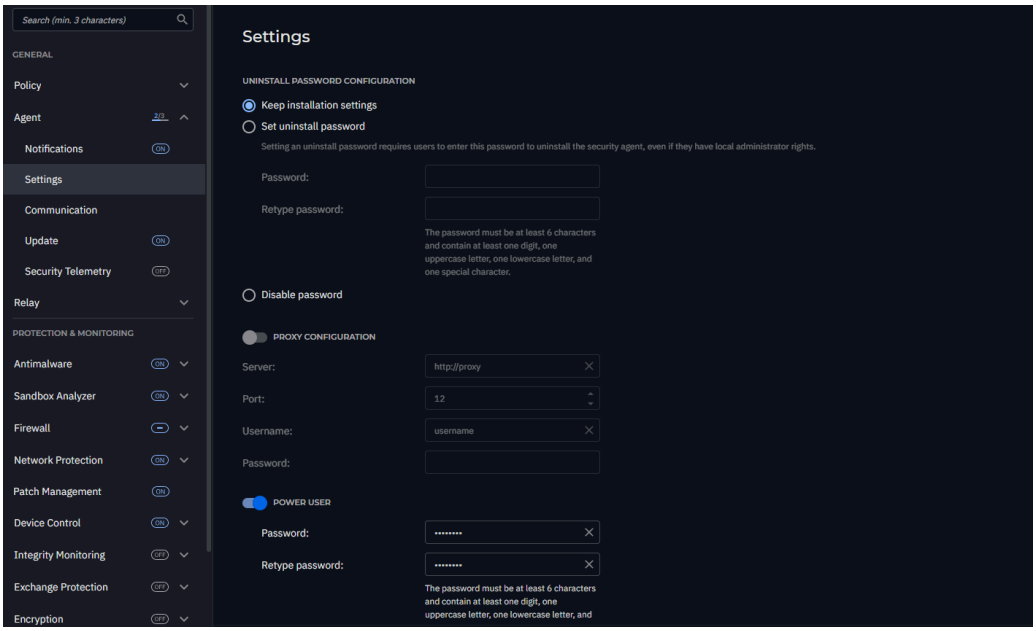

Figure 3: Impostare il power user

- **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.
- **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.
- **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.

2.1.2.1. Best Practices

Per quanto riguarda la sezione "Agent", si consiglia per i diversi punti:

- ***Notifications:** impostare solo di tipo "notification pop-up" (non richiedono input utente) e solo per gli eventi che interessano direttamente l'utente (es. blocco applicazione o dispositivo), lasciare invece il controllo degli incidenti malware al team di sicurezza tramite Control Center, per non allarmare inutilmente gli utenti in caso di falsi positivi. Disattivare le notifiche dei moduli che non si vogliono utilizzare.*

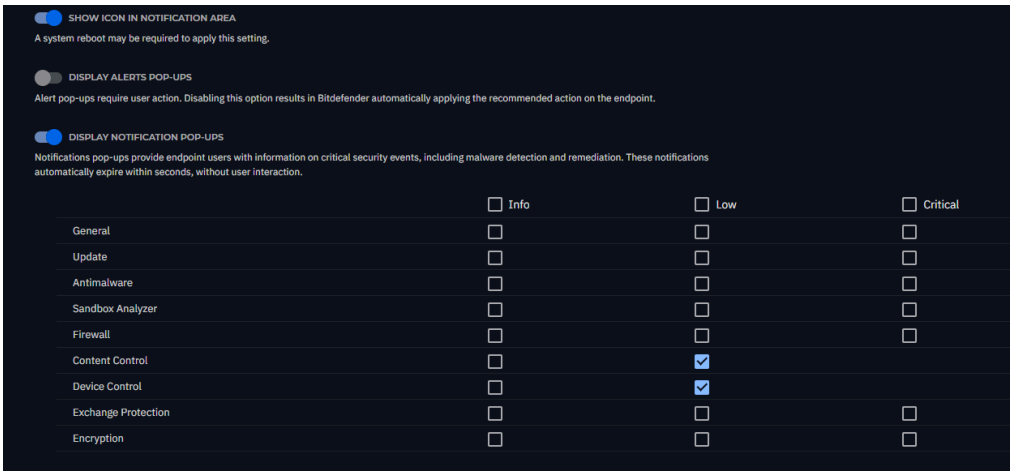

Figure 4: Esempio notifiche Agent

- ***Settings:*** *impostare la password di disinstallazione. A meno di casi particolari, non impostare l'agente come Power User.*
- ***Communication:*** *impostare tutti i Relay come endpoint di comunicazione, assegnandogli la stessa priorità, in modo da far scegliere a Bitdefender quale Relay utilizzare in base alla disponibilità.*
- ***Update:*** *lasciare le impostazioni di default.*

2.1.3. Relay

2.2. Protection & Monitoring

In questa sezione viene definita la politica vera e propria, che è composta da diversi moduli:

2.2.1. Antimalware

Il modulo antimalware è molto completo, e diviso in diverse sezioni:

- **On-Access:** In questa sezione è definito il livello di aggressività della scansione che avviene al momento dell'accesso ai file.
- **On-Execute:** In questa sezione è definito il livello di aggressività della scansione che avviene al momento dell'esecuzione dei file eseguibili. Inoltre è possibile attivare o disattivare alcuni tipi di controlli, come quello per gli attacchi fileless o ransomware.
- **On-Demand:** Qui è possibile creare una regola di scansione, sono disponibili delle tipologie predefinite, come quick o full scan, oppure è possibile crearla custom, per personalizzare più a fondo la scansione (scegliere su quali cartelle effettuarla, la profondità e minutezza...). In questa schermata inoltre, premendo su "Edit" all'interno del paragrafo "Contextual Scan", si possono personalizzare le impostazioni di scansione per le cartelle locali e quelle di dispositivi esterni.

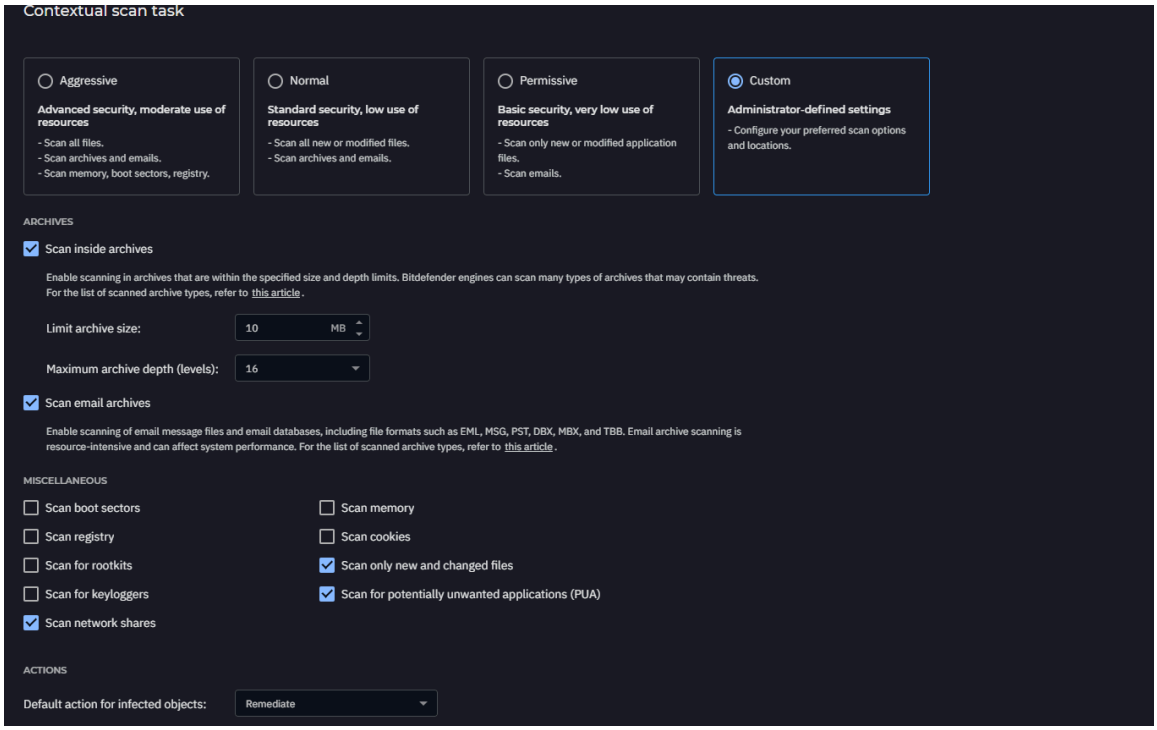

Figure 5: Impostazioni di scansione

- **Anti Tampering:** Qui è possibile attivare o disattivare i controlli anti-tampering, in particolare sui driver sensibili e sulle call-back evasion.
- **Hyper Detect:** In questa pagina è possibile attivare e configurare per quali minacce utilizzare Hyper Detect, un sistema di analisi di Bitdefender basato su machine learning.
- **Advanced Anti-exploit:** Qui si possono gestire i controlli su diversi tipi di exploit,
- **Security Servers**:
- **Settings:**
- **Exclusions:**

2.2.1.1. Best Practices

Per quanto riguarda il modulo antimalware, il consiglio è quello di attivare tutti i controlli disponibili (di default dovrebbero tutti essere attivi tranne la mitigazione ransomware all'interno di "On-Execute"). Per quanto riguarda lo scan On-Demand, è consigliato impostare una full scan, magari a giorni alterni, in un momento in cui le macchine sono accese ma non utilizzate (la scansione NON impedisce nessuna operazione sulla macchina, ma potrebbe appesantirne il carico di lavoro).

2.2.2. Sandbox Analyzer

Il sandbox analyzer permette di analizzare i file sospetti in un ambiente sicuro, attivando la funzione, verranno inviati automaticamente al sandbox i file individuati.

2.2.2.1. Best Practices

Si consiglia di attivare la funzione, mantenendo però la "analysis mode" su "Monitoring" e la default action "report only", in questo modo non verranno mai bloccati file senza motivazioni certe.

2.2.3. Firewall

Il firewall di bitdefender permette di controllare le connessioni in entrata e in uscita direttamente sul endpoint.

- **General:**
- **Settings:**
- **Rules:**

2.2.3.1. Best Practices

Per quanto riguarda il firewall, in caso il cliente disponesse già di un firewall esterno è possibile anche disattivare il modulo, ricordandosi di deselezionare la spunta "Firewall" all'interno della sezione Agent -> Notifications. In caso si volesse mantenere il firewall invece, lasciare le impostazioni di default ricordandosi di aggiungere le porte da escludere in Firewall -> General.

Inserire poi tutte le regole necessarie in FIrewall -> Rules.

2.2.4. Network Protection

Il modulo Network Protection permetta di applicare filtri e controlli su web e applicazioni.

- **General:** Qui si imposta se controllare o meno anche il traffico criptato e di quale tipo, e si aggiungo le eventuali esclusioni ai controlli (sia URL o IP sia applicazioni)
- **Content Control:** Nella schermata content control è possibile attivare il controllo web, selezionando una regola precedentemente creata, per farlo seguire la guida al paragrafo "5.2 Creazione Web Access Control Scheduler". È anche possibile creare una blacklist di applicazioni per impedirne l'esecuzione. Infine, è possibile inserire una lista di dati sensibili, questa lista bloccherà l'invio di questi dati scansionando tutte le tipologie di traffico spuntate nella sezione Network Protection -> General, in caso di blocco l'utente visualizzerà un alert.
- **Web Protection:** Qui è possibile attivare il controllo phishing, il controllo web in real time e la scansione email.
- **Network Attacks:** Qui è possibile attivare e impostare la difesa dagli attacchi web. È possibile scegliere per ogni tipologia di attacco se bloccarne l'accesso o creare solamente un alert nel Control Center.

2.2.4.1. Best Practices

- ***General:** Attivare la scansione del traffico criptato e anche il controllo https. Aggiungere alle esclusioni siti e applicazioni utilizzati frequentemente e/o sensibili (es. banca, gestionali, ecc.).*
- ***Content Control:** se presente, assegnare al web access control la schedule creata precedentemente come spiegato nel paragrafo "5.2 Creazione Web Access Control Scheduler". In caso si volessero aggiungere dei dati sensibili al Data Protection, si consiglia di non aggiungere, ad esempio, una password per intero, ma piuttosto una sua parte univoca (es. con password "Psd!23@" inserire "!23@").*
- ***Web Protection:** Mantenere le impostazioni di default, ovvero tutto attivo tranne il controllo mail (senza exchange protection configurato non ha alcun effetto).*
- ***Network Attacks:** Attivare RDP traffic e settare tutti i controlli su "block".*

2.2.5. Patch Management

Qui è possibile associare alla policy una maintenance window creata precedentemente, per crearne una fare riferimento al paragrafo "5.1 Creazione Maintenance Windows"

2.2.6. Device Control

- **Rules:** Nella schermata rules è possibile bloccare determinati tipi di dispositivi divisi per categorie, in caso non si volesse bloccare un'intera categoria ma una specifica tipologia di dispositivo per quella categoria, è possibile selezionare la categoria, premere su custom, e settare su "block" solo quella tipologia. Ad esempio, per bloccare le chiavette USB, selezionare "External Storage" e settare solo "USB" su "block".
- **Exclusions:** Qui è possibile aggiungere determinati dispositivi "fidati" che potranno esssere utilizzati nonstante le regole di blocco, nel caso delle USB si possono inserire da dispositivi già conosciuti, oppure manualmente tramite ID.

2.2.6.1. Best Practices

2.2.7. Incident Sensor

2.2.8. Risk Management

2.2.9. Blocklist

2.2.10. Live Search

3. Guida alla gestione dei tag

4. Guida al patch management

5. Altre funzionalità

5.1. Creazione Maintenance Windows

È possibile creare una maintenance window nella sezione “Policies -> Configuration Profiles -> Maintenance Windows” del menu a sinistra. Nella schermata che si apre premere “Add Window”. A questo punto sarà possibile decidere se solo scansionare o anche applicare le patch trovate. Per entrambe le operazioni sono disponibili diverse impostazioni.

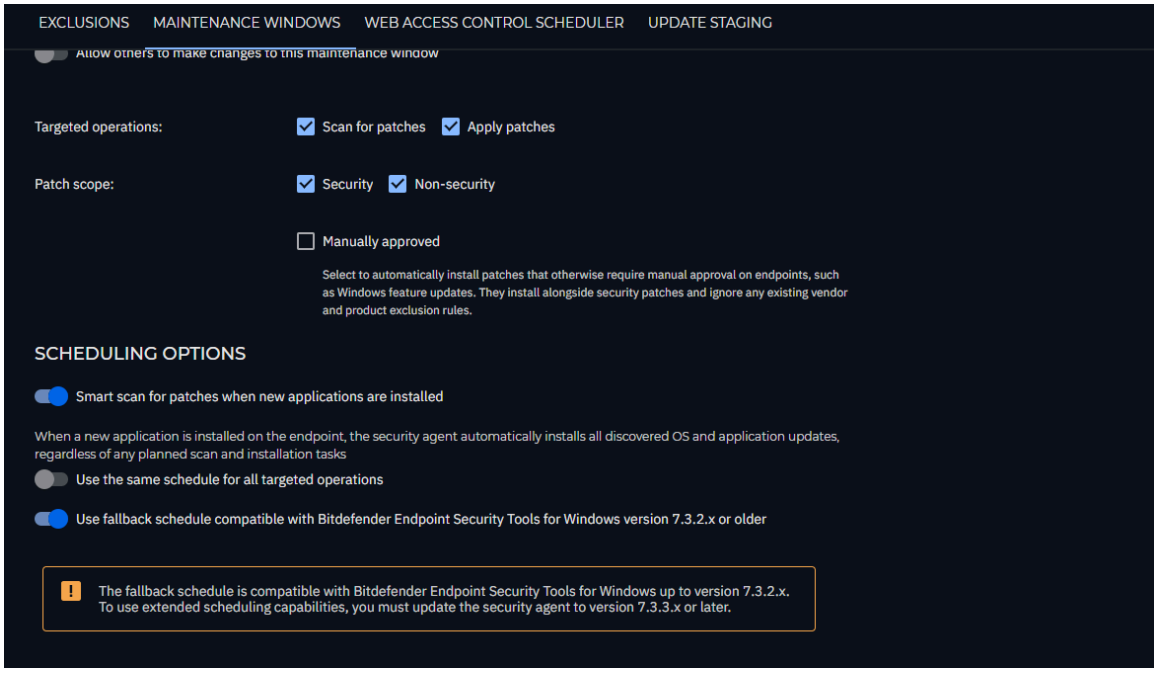

Figure 6: Maintenance Window

5.1.1. Best Practices

Si consiglia di attivare sia la scansione sia l’applicazione delle patch, e di spuntare sia “Security” che “Non-security”. Attivare anche la fallback schedule, che permette di ripristinare i prodotti alla versione precedente in caso di problemi in seguito all’applicazione patch.

Per quanto riguarda la ricorrenza, è consigliato effettuare la scansione abbastanza spesso, ad esempio una volta ogni 2 giorni e in orari in cui le macchine sono accese (in ogni caso lasciare spuntata l’opzione “if missed run ASAP”).

Se si è impostato un endpoint come server di cache per le patch qui è possibile assegnarlo alla window, in questo modo le patch saranno scaricate dal server di patch e non dal sito del vendor.

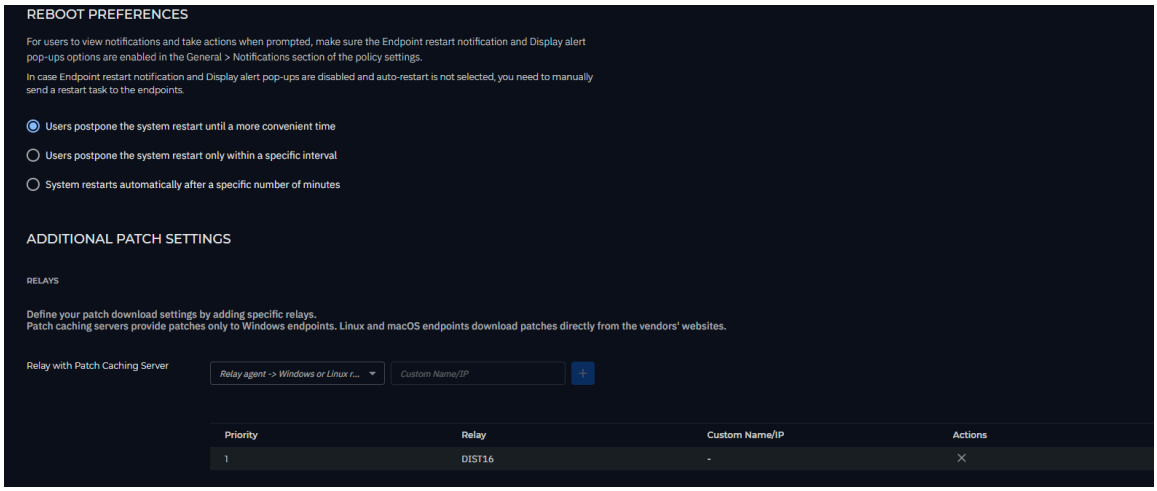

Figure 7: Patch Caching Server

5.2. Creazione Web Access Control Scheduler

5.3. Creazione liste di esclusioni