

Deploy - How to

| Versione | Data | Redattore | Descrizione |
|-----------------|-------------|------------------|--|
| 0.6 | 18/07/2025 | Davide Marin | Continuo stesura capitoli vecchi, aggiunto “Gestione dei Report” |
| 0.5 | 17/07/2025 | Davide Marin | Continuo stesura capitoli 2, 3, 4 e 5 |
| 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 |
| 1.3.1. Installazione da remoto | 5 |
| 1.4. Integrazione di Active Directory | 6 |
| 2. Guida alla creazione delle politiche di protezione | 8 |
| 2.1. General | 8 |
| 2.1.1. Policy | 8 |
| 2.1.2. Agent | 9 |
| 2.1.3. Relay | 11 |
| 2.2. Protection & Monitoring | 11 |
| 2.2.1. Antimalware | 11 |
| 2.2.2. Sandbox Analyzer | 12 |
| 2.2.3. Firewall | 13 |
| 2.2.4. Network Protection | 13 |
| 2.2.5. Patch Management | 14 |
| 2.2.6. Device Control | 14 |
| 2.2.7. Incident Sensor | 14 |
| 2.2.8. Risk Management | 15 |
| 2.2.9. Blocklist | 15 |
| 2.2.10. Live Search | 16 |
| 3. Guida alla gestione dei tag | 17 |
| 3.1. Creazione del tag | 17 |
| 3.2. Associazione di tag e policy | 17 |
| 4. Guida al patch management | 19 |
| 5. Gestione dei Report | 20 |
| 5.1. Creazione di Report | 20 |
| 5.2. Creazione report per singoli endpoint o gruppi | 20 |
| 5.3. Best Practices | 21 |
| 6. Altre funzionalità | 22 |
| 6.1. Creazione Installation Packages | 22 |
| 6.2. Best Practices | 22 |
| 6.3. Creazione Maintenance Windows | 22 |
| 6.3.1. Best Practices | 23 |
| 6.4. Creazione Web Access Control Scheduler | 23 |
| 6.4.1. Best Practices | 24 |
| 6.5. Creazione liste di esclusioni | 24 |
| 6.6. Creazione delle Blocklist | 24 |

Lista delle immagini

| | | |
|-----------|--|----|
| Figure 1 | Installazione Agent Remoto - prima parte | 6 |
| Figure 2 | Installazione Agent Remoto - seconda parte | 6 |
| Figure 3 | Aggiungi nuova politica di protezione | 8 |
| Figure 4 | Aggiungi ereditarietà di un modulo | 9 |
| Figure 5 | Impostare il power user | 10 |
| Figure 6 | Esempio notifiche Agent | 11 |
| Figure 7 | Impostazioni di scansione | 12 |
| Figure 8 | Device Control | 14 |
| Figure 9 | Configurazione Risk Management | 15 |
| Figure 10 | Configurazione Blocklist | 16 |
| Figure 11 | Creazione Tag | 17 |
| Figure 12 | Creazione Assignment Rule | 18 |
| Figure 13 | Patch Inventory | 19 |
| Figure 14 | Report Schedule | 20 |
| Figure 15 | Report Singolo Endpoint | 21 |
| Figure 16 | Maintenance Window | 23 |
| Figure 17 | Patch Caching Server | 23 |
| Figure 18 | Creazione Web Access Control Scheduler | 24 |

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 sarà necessario creare almeno un pacchetto di installazione per i nostri agent che dovremo installare sugli endpoint, per vedere come creare un pacchetto di installazione, fare riferimento al paragrafo “[6.1 Creazione Installation Packages](#)”.

1.2. Installare Security Server (solo per endpoint con poche risorse)

Security server può 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, alleggerendo il carico sulle macchine.

Per installarlo, innanzitutto scaricare il pacchetto di installazione di Security Server di default (per vedere come creare un pacchetto di installazione, fare riferimento al paragrafo “[6.1 Creazione 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 ufficiale dettagliata disponibile [qui](#), oppure tramite “sva-setup command”, con guida ufficiale 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:** Si scarica il pacchetto di installazione e si installa manualmente sugli endpoint, per vedere come creare un pacchetto di installazione, fare riferimento al paragrafo “[6.1 Creazione Installation Packages](#)”.
- **Installazione da remoto:** Modalità in cui mi concentrerò in questa guida.

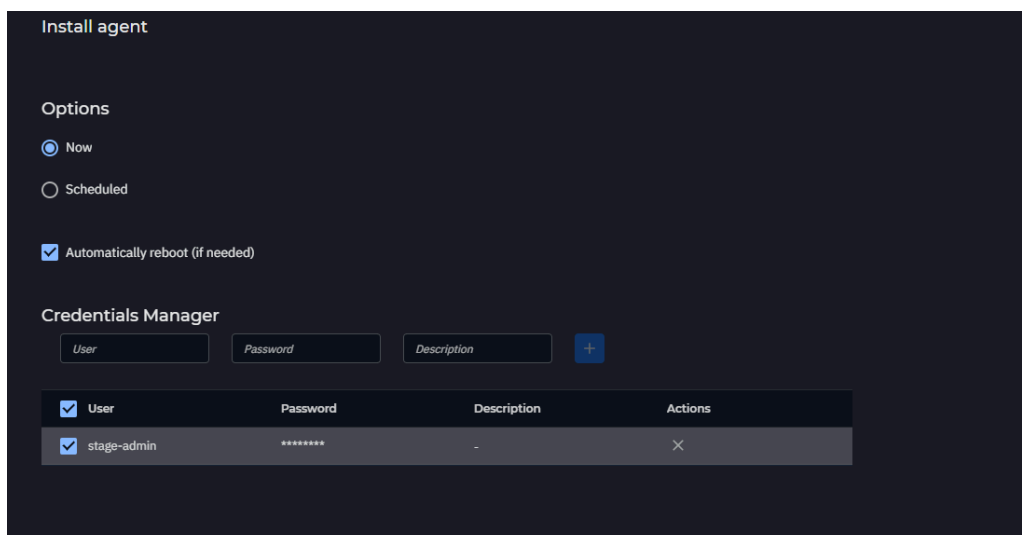
1.3.1. Installazione da remoto

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, per vedere come creare un pacchetto di installazione, fare riferimento al paragrafo “[6.1 Creazione Installation Packages](#)”. 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 e creato un pacchetto di installazione per gli altri endpoint. sarà possibile installare gli agenti sugli altri endpoint da remoto; per farlo,

andare nella pagina “Network”, selezionare dalla lista tutti gli endpoint sui quali si vuole installare l’agente, a questo punto 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.



Install agent

Options

☒ Now

☐ Scheduled

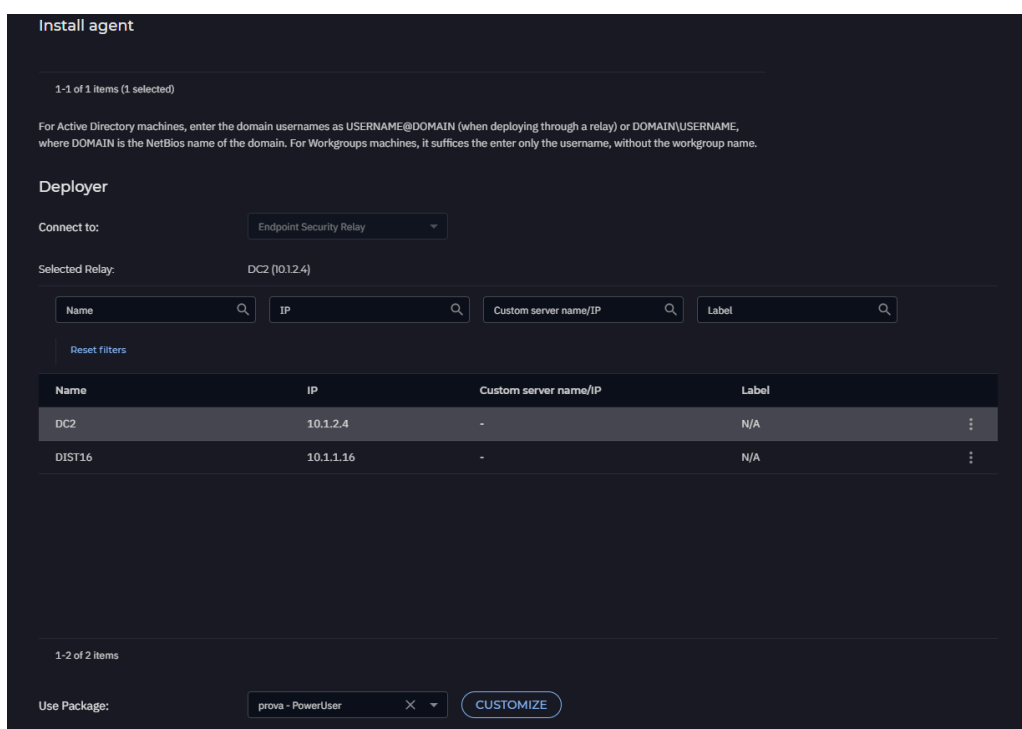
☒ Automatically reboot (if needed)

Credentials Manager

User Password Description +

| <input checked="" type="checkbox"/> User | Password | Description | Actions |
|---|----------|-------------|---------|
| <input checked="" type="checkbox"/> stage-admin | ***** | - | × |

Figure 1: Installazione Agent Remoto - prima parte



Install agent

1-1 of 1 items (1 selected)

For Active Directory machines, enter the domain usernames as USERNAME@DOMAIN (when deploying through a relay) or DOMAIN\USERNAME, where DOMAIN is the NetBios name of the domain. For Workgroups machines, it suffices to enter only the username, without the workgroup name.

Deployer

Connect to: Endpoint Security Relay

Selected Relay: DC2 [10.12.4]

| Name | IP | Custom server name/IP | Label |
|--------|-----------|-----------------------|-------|
| DC2 | 10.1.2.4 | - | N/A |
| DIST16 | 10.1.1.16 | - | N/A |

1-2 of 2 items

Use Package: prova - PowerUser CUSTOMIZE

Figure 2: Installazione Agent Remoto - seconda parte

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”.

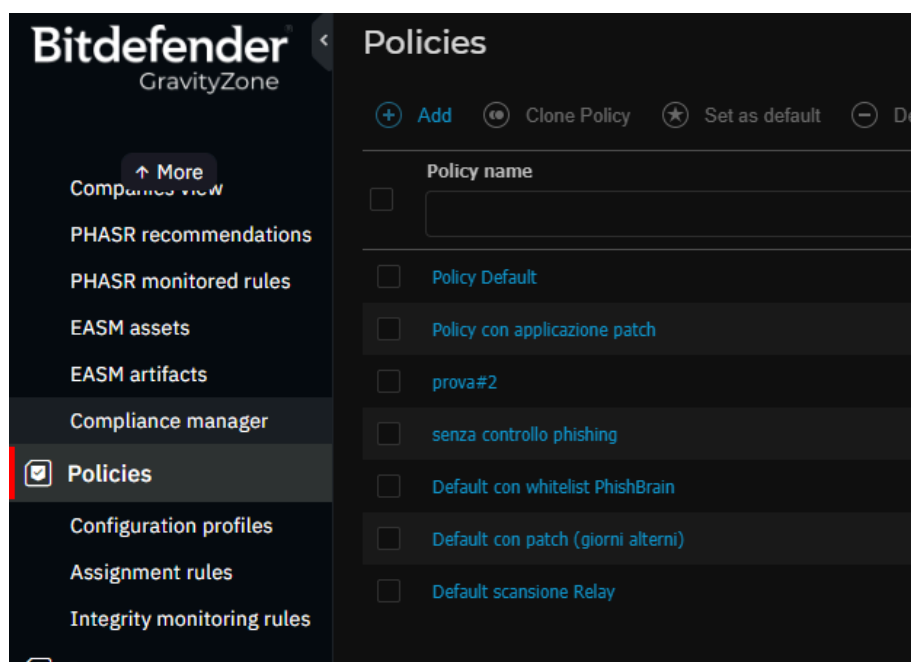


Figure 3: Aggiungi nuova politica di protezione

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.

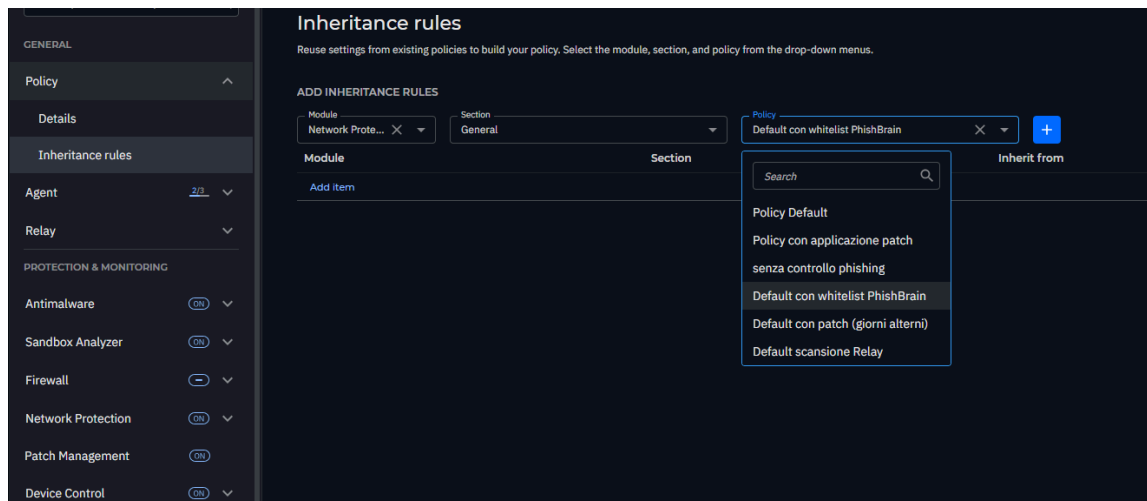


Figure 4: Aggiungi ereditarietà di un modulo

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.

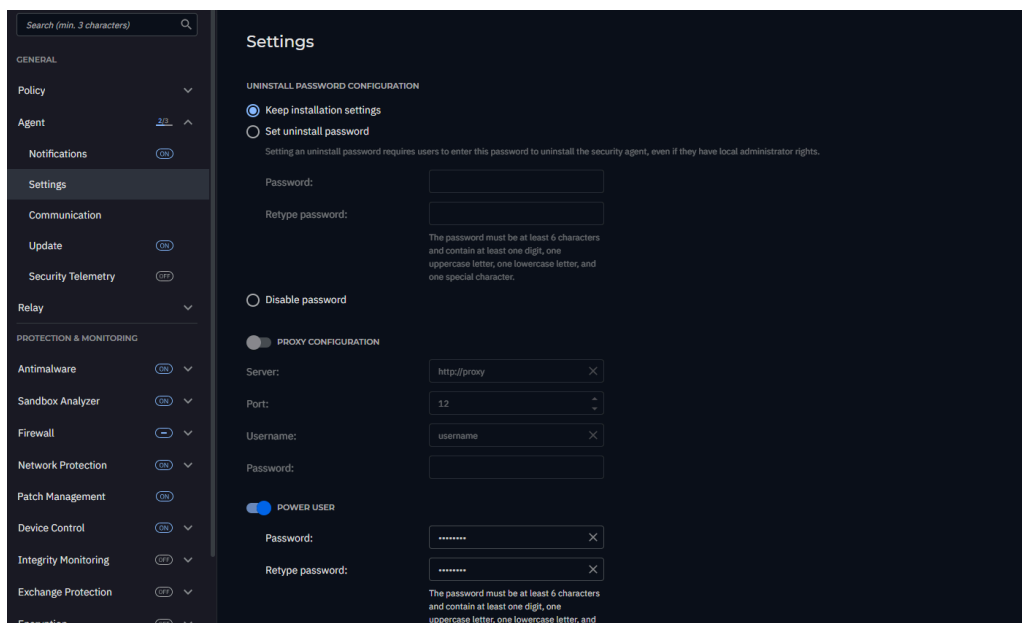


Figure 5: Impostare il power user

- **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.*

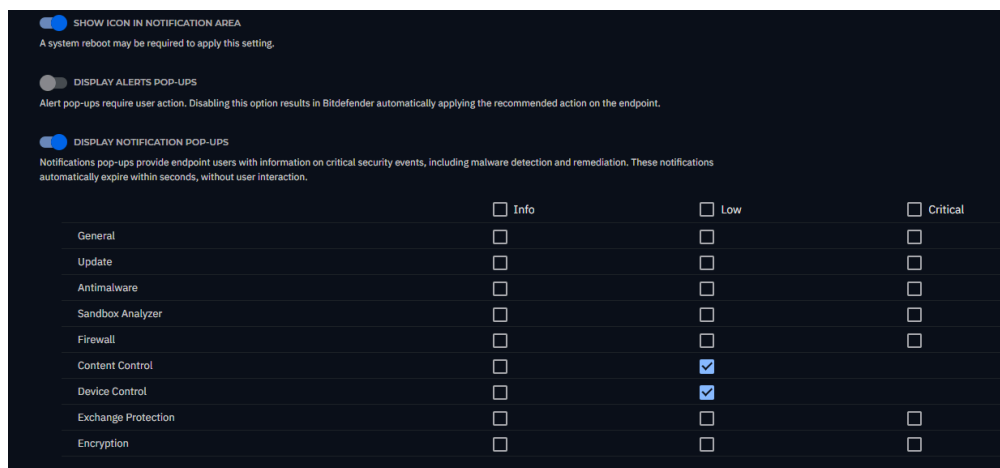


Figure 6: Esempio notifiche Agent

- **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

Qui è possibile vedere le impostazioni relative agli endpoint con ruolo relay, in particolare è possibile impostare i server di proxy e le location di update (che normalmente è il cloud di bitdefender).

2.1.3.1. Best Practices

Il consiglio, per quanto riguarda la sezione relay, è quello di mantenere le impostazioni di default, andando ad aggiungere i server di proxy, se disponibili, nella sezione Relay -> Communication.

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, ecc.). 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 7: 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:** Qui è possibile associare un security server alla policy, per farlo è sufficiente selezionare il Security Server desiderato dal menu a scomparsa e premere “+”.
- **Settings:** Qui sono disponibili alcune opzioni aggiuntive per la policy, in particolare relativi alla quarantena dei file.
- **Exclusions:** Qui è possibile creare delle esclusioni per determinati file ,applicazioni o processi, oppure è possibile associare una lista di esclusioni precedentemente creata, per vedere come crearne una, fare riferimento al paragrafo “6.4 Creazione liste di esclusioni”

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:** Qui è possibile attivare il firewall e decidere se controllare anche le connessioni wi-fi e lo scanning delle porte inserendo anche eventuali esclusioni.
- **Settings:** Qui è possibile creare diverse categorie di rete (ufficio, casa, fidata, ecc.) per poi potergli affidare diverse regole di controllo.
- **Rules:** Qui è possibile creare le regole di controllo e assegnarle alle varie categorie di rete.

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. Creare le categorie desiderate in Firewall -> Settings e 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 “6.3 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 “6.3 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 “6.2 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”.

| CUSTOM PERMISSIONS | | |
|--------------------|----------------------------------|----------------------------------|
| | <input type="radio"/> Allowed | <input type="radio"/> Blocked |
| Firewire | <input checked="" type="radio"/> | <input type="radio"/> |
| ISA Plug & Play | <input checked="" type="radio"/> | <input type="radio"/> |
| PCI | <input checked="" type="radio"/> | <input type="radio"/> |
| PCMCIA | <input checked="" type="radio"/> | <input type="radio"/> |
| SCSI | <input checked="" type="radio"/> | <input type="radio"/> |
| SD Card | <input checked="" type="radio"/> | <input type="radio"/> |
| USB | <input type="radio"/> | <input checked="" type="radio"/> |
| Other | <input checked="" type="radio"/> | <input type="radio"/> |

Figure 8: Device Control

- **Exclusions:** Qui è possibile aggiungere determinati dispositivi “fidati” che potranno essere utilizzati nonostante 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

Collegare prima i dispositivi fidati e dopo attivare il blocco, in questo modo sarà possibile aggiungerli nelle esclusioni direttamente da “from discovered devices”.

2.2.7. Incident Sensor

Questo modulo è fondamentale per poter utilizzare la funzionalità di rilevamento incidenti, e relativa pagina “Incidents” nel menu a sinistra.

2.2.8. Risk Management

Questa pagina permette di configurare la regola di scansione dei rischi, queste scansioni individuano vulnerabilità date da impostazioni delle applicazioni o da registri di sistema inutilizzati, inoltre individuano anche il rischio associato ad ogni utente. Sempre in questa schermata è possibile abilitare il PHASR, sistema di machine learning che, dopo un periodo di training (circa 30 giorni), fornisce consigli su che modifiche applicare ai vari utenti per migliorarne la sicurezza.

2.2.8.1. Best Practices

Impostare la scansione anche ogni giorno, meglio in orari dove il computer non è utilizzato, ma è una scansione più leggera rispetto ad una full scan. Consigliato è anche attivare il PHASR, impostando tutto su “Direct Control”, in questo modo non verranno applicate le misure individuate automaticamente, ma saranno solo consigliate e attenderanno approvazione.

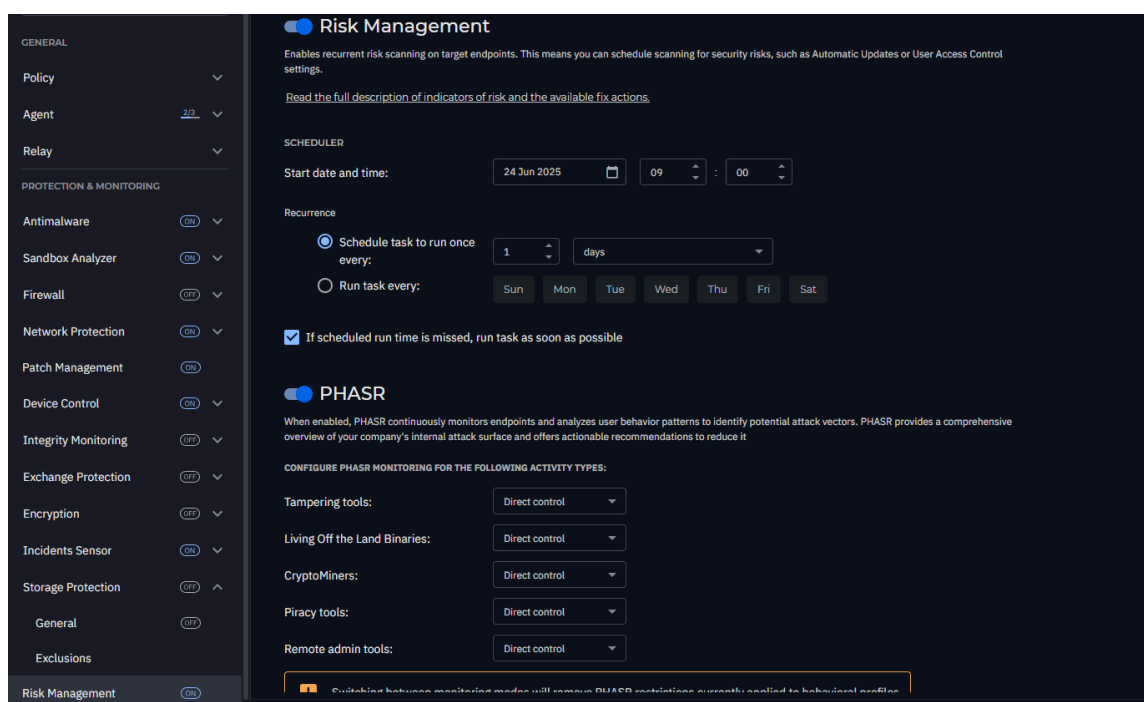


Figure 9: Configurazione Risk Management

2.2.9. Blocklist

Nella pagina blocklist è possibile configurare quali controlli saranno efficaci su questa policy. Disattivando “Application path” ad esempio, se fossero presenti delle applicazioni inserite tramite path nella blocklist, esse non sarebbero bloccate per gli utenti con questa policy.

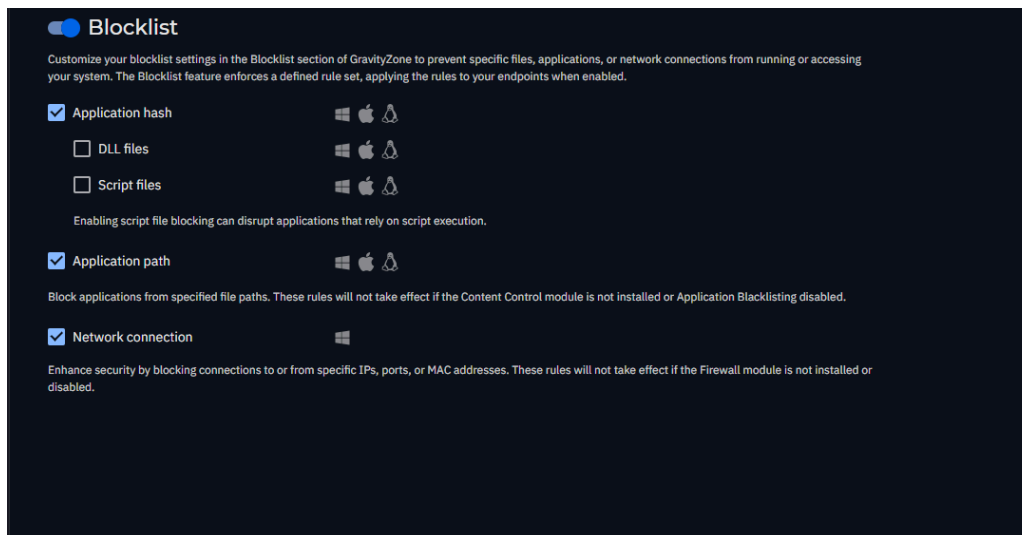


Figure 10: Configurazione Blocklist

2.2.9.1. Best Practices

Spuntare tutte le tipologie di controllo, tranne DLL files e Script files per non causare problemi durante l'esecuzione delle applicazioni. Ricordarsi che alcuni di questi controlli dipendono anche dall'attivazione del modulo della rispettiva categoria (es. Network connection non funzionerà se il firewall è disattivato).

2.2.10. Live Search

Attivando la live search si rende possibile effettuare delle query per ottenere informazioni sugli endpoint. Le informazioni possono essere utili per la diagnostica in caso di incidenti nella rete. Per effettuare le ricerche in tempo reale è necessario creare le query nella pagina "Incidents -> Search" nel menu a sinistra.

2.2.10.1. Best Practices

Si consiglia di attivarla, in quanto non comporta nessun carico extra finché non vengono eseguite delle query dalla schermata apposita.

3. Guida alla gestione dei tag

3.1. Creazione del tag

I tag sono uno strumento utile che permette di raggruppare gli endpoint per diversi criteri, per poi assegnare le policy di protezione direttamente ai gruppi risparmiando tempo e semplificando l'operazione.

Per creare un tag, andare in “Network -> Tags management” dal menu a sinistra, a questo punto premere su “Add tag”. Nella schermata che si apre è possibile creare un tag in modalità custom, ovvero sarà necessario poi scegliere manualmente a quali endpoint assegnarlo, oppure in modalità automatica, ovvero il tag sarà assegnato automaticamente in base ai filtri inseriti di seguito.

Selezionando “Automatic”, sarà possibile inserire i filtri per nome (anche con wildcard), IP, sistema operativo e tipologia di endpoint (workstation/server/ecc.). Inserendo più filtri, il tag si applicherà agli endpoint che li rispettano tutti.

Figure 11: Creazione Tag

Se si è creato un tag “Custom” invece, sarà necessario andare nella sezione “Network” e selezionare dalla lista degli endpoint tutti quelli a cui vogliamo assegnare il tag, una volta selezionati premere “Action -> Assign tags” e selezionare il tag desiderato.

3.2. Associazione di tag e policy

Per associare il tag alla policy desiderata sarà sufficiente andare nella sezione “Policy -> Assignment Rules”, in questa schermata premere su “Add -> Endpoint tag rule”. Nella finestra che si è aperta, compilare i campi in base alla policy e al tag che si vuole associare

Assignment rules

[Back](#) | [Add Tag Rule](#)

Details

Name: *

Description:

Priority:

Policy:

Tag

*

| Tag type | Tag name | Actions |
|-----------|----------|----------------------------------|
| Automatic | Server | <input type="button" value="X"/> |

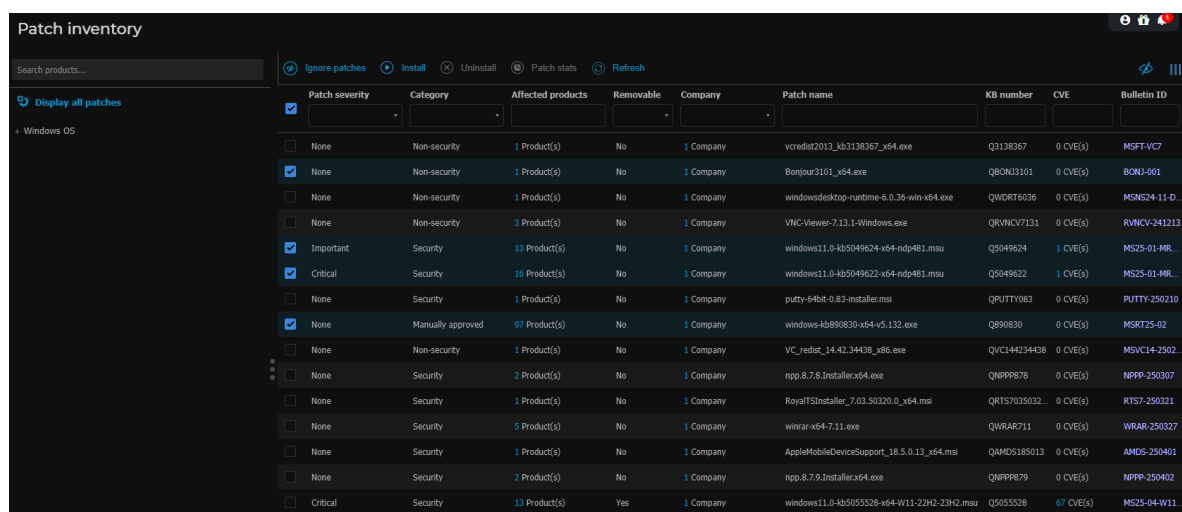
Figure 12: Creazione Assignment Rule

4. Guida al patch management

La funzione di patch management di GravityZone trova bug, errori di configurazione e obsolescenze che possono essere sfruttati per degli attacchi, e ne ricerca le patch, permettendo poi di installarle in automatico.

GravityZone mette a disposizione uno strumento per eseguire scansioni delle patch disponibili per le proprie macchine, è possibile avviarle manualmente (on-demand) selezionando la macchina desiderata nella sezione “Network” e premendo su “Action -> Patch Scan”, oppure è possibile farle eseguire automaticamente creando prima una “Maintenance Window” e poi assegnandola alla policy, per vedere come crearla, far riferimento al paragrafo “[6.2 Creazione Maintenance Window](#)”.

Una volta che gli endpoint eseguiranno le scansioni patch, sarà possibile visualizzare la lista di tutte quelle trovate nella sezione “Network -> Patch Inventory” del menu a sinistra. Direttamente in questa schermata, sarà possibile spuntare le patch desiderate e poi premere su “Install” per installarle su tutti gli endpoint che le richiedono. Se nella maintenance window si è spuntata l’opzione “Patch Install”, questa operazione sarà necessaria solo per alcune patch che richiedono approvazione manuale.



| Patch severity | Category | Affected products | Removable | Company | Patch name | KB number | CVE | Bulletin ID |
|---|-------------------|-------------------|-----------|-----------|---|----------------|-----------|----------------|
| <input type="checkbox"/> None | Non-security | 1 Product(s) | No | 1 Company | vcredist2013_kb3138367_x64.exe | Q3138367 | 0 CVE(s) | MSFT-VC7 |
| <input checked="" type="checkbox"/> None | Non-security | 1 Product(s) | No | 1 Company | Bonjour3101_x64.exe | QBONJ3101 | 0 CVE(s) | BONJ-001 |
| <input type="checkbox"/> None | Non-security | 1 Product(s) | No | 1 Company | windowsdesktop-runtime-6.0.36-win-x64.exe | QWDRT6036 | 0 CVE(s) | MSNS24-11-D... |
| <input type="checkbox"/> None | Non-security | 3 Product(s) | No | 1 Company | VNC-Viewer-7.13.1-Windows.exe | QRVNCV7131 | 0 CVE(s) | RVNCV-241213 |
| <input checked="" type="checkbox"/> Important | Security | 13 Product(s) | No | 1 Company | windows11.0-kb5049624-x64-ndp481.msu | Q5049624 | 1 CVE(s) | MS25-01-MR... |
| <input checked="" type="checkbox"/> Critical | Security | 16 Product(s) | No | 1 Company | windows11.0-kb5049622-x64-ndp481.msu | Q5049622 | 1 CVE(s) | MS25-01-MR... |
| <input type="checkbox"/> None | Security | 1 Product(s) | No | 1 Company | putty-64bit-0.83-installer.msi | QPUTTY083 | 0 CVE(s) | PUTTY-250210 |
| <input checked="" type="checkbox"/> None | Manually approved | 97 Product(s) | No | 1 Company | windows-kb890830-x64-v5.132.exe | Q890830 | 0 CVE(s) | MSRT25-02 |
| <input type="checkbox"/> None | Non-security | 1 Product(s) | No | 1 Company | VC_redist_14.42.34438_x86.exe | QVC144234438 | 0 CVE(s) | MSVC14-2502... |
| <input type="checkbox"/> None | Security | 2 Product(s) | No | 1 Company | npp.8.7.8.Installer.x64.exe | QNPP878 | 0 CVE(s) | NPPP-250307 |
| <input type="checkbox"/> None | Security | 1 Product(s) | No | 1 Company | RoyalTSInstaller_7.03.50320_0_x64.msi | QRTS7035032... | 0 CVE(s) | RTS7-250321 |
| <input type="checkbox"/> None | Security | 5 Product(s) | No | 1 Company | winsar-x64-7.11.exe | QWRAR711 | 0 CVE(s) | WRAR-250327 |
| <input type="checkbox"/> None | Security | 1 Product(s) | No | 1 Company | AppleMobileDeviceSupport_18.5.0.13_x64.msi | QAMD5185013 | 0 CVE(s) | AMDS-250401 |
| <input type="checkbox"/> None | Security | 2 Product(s) | No | 1 Company | npp.8.7.9.Installer.x64.exe | QNPP879 | 0 CVE(s) | NPPP-250402 |
| <input type="checkbox"/> Critical | Security | 13 Product(s) | Yes | 1 Company | windows11.0-kb5055328-x64-W11-22H2-23H2.msu | Q5055328 | 67 CVE(s) | MS25-04-W11... |

Figure 13: Patch Inventory

Per avere una panoramica dello stato delle patch su ogni endpoint, è possibile creare un report apposito chiamato “Network Patch Status”, per vedere come creare un report, fare riferimento al paragrafo “[5 Gestione dei Report](#)”

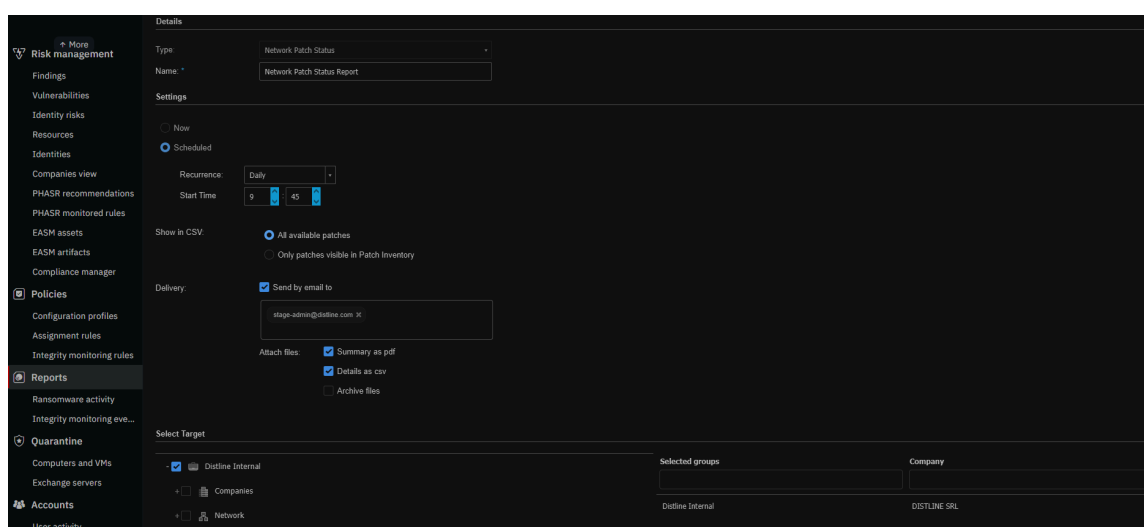
5. Gestione dei Report

GravityZone permette di controllare lo stato degli endpoint, della rete e anche del servizio attraverso un grande numero di report.

5.1. Creazione di Report

È possibile creare un report andando nella sezione “Reports” del menu a sinistra, nella pagina che si apre premere “Add”. Nella schermata che si apre, selezionare il tipo di report desiderato dalla lista proposta, per alcuni tipi di report saranno disponibili ulteriori filtri una volta selezionati.

A questo punto è possibile scegliere se generare un report rapido, che sarà visualizzato direttamente in questa pagina, oppure aggiungere una schedule e inviarlo per mail agli indirizzi desiderati con ricorrenza e orari a piacere.



The screenshot shows the 'Details' configuration page for a 'Network Patch Status Report'. The left sidebar contains a navigation menu with categories like Risk management, Findings, Vulnerabilities, and Reports (which is highlighted). The main panel is divided into 'Settings' and 'Select Target' sections. In the 'Settings' section, the 'Type' is 'Network Patch Status' and the 'Name' is 'Network Patch Status Report'. Under 'Recurrence', 'Scheduled' is selected with a 'Daily' frequency and a start time of 9:45. The 'Show in CSV' section has 'All available patches' selected. The 'Delivery' section has 'Send by email to' checked, with the email address 'stage-admin@distline.com.it' entered. The 'Attach files' section has 'Summary as pdf' and 'Details as csv' checked, while 'Archive files' is unchecked. The 'Select Target' section shows 'Distline Internal' selected under 'Selected groups' and 'Company' under 'Company'. At the bottom, there are input fields for 'Distline Internal' and 'DISTLINE URL'.

Figure 14: Report Schedule

5.2. Creazione report per singoli endpoint o gruppi

Questi report però, saranno solo per l'intera rete aziendale, se si volesse creare un report per uno specifico endpoint o un gruppo, ad esempio, è possibile farlo dalla sezione “Network” del menu a sinistra. Una volta che si visualizza la lista degli endpoint, è possibile selezionare gli endpoint desiderati e poi premere su “Reports”.

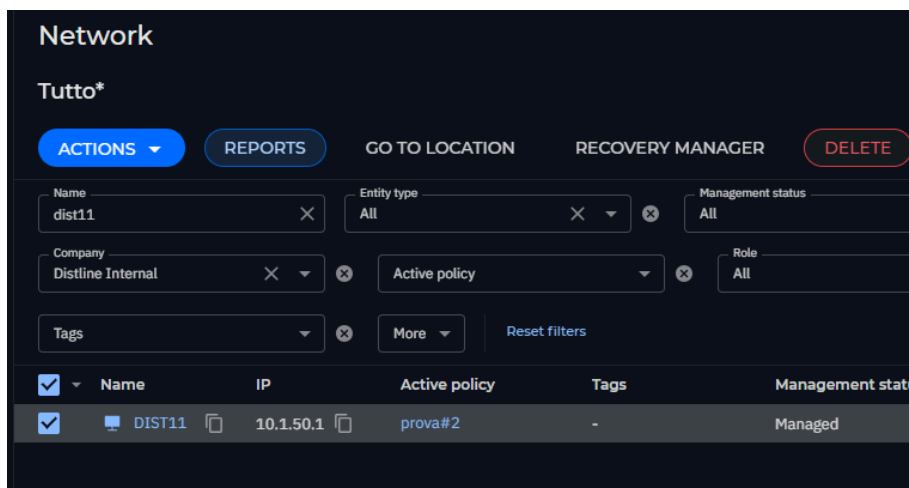


Figure 15: Report Singolo Endpoint

Attenzione, in questo caso i report saranno solo di tipo rapido, non è possibile infatti creare schedule di report per singoli endpoint o gruppi.

5.3. Best Practices

Nella creazione di report con schedule, il file PDF solitamente ha una panoramica molto riassuntiva dei dati del report, se si volessero numeri e dati precisi (spesso suddivisi anche per endpoint), è consigliato allegare anche il file CSV.

6. Altre funzionalità

6.1. Creazione Installation Packages

I pacchetti di installazione definiscono quali moduli ed eventuali privilegi saranno attribuiti agli endpoint.

Per creare un pacchetto, andare nella sezione “Network -> Installation Packages” del menu a sinistra, nella finestra che si apre, premere su “Create”. A questo punto, nella schermata aperta, sarà possibile inserire il nome del pacchetto e selezionare tutti i moduli desiderati da essere installati. È inoltre possibile settare altre impostazioni, come richiedere una password per la disinstallazione dell’agent, se installare il pacchetto in un percorso specifico, se utilizzare un server di proxy per comunicare con il Control Center.

6.2. Best Practices

Per la creazione dei pacchetti, si consiglia di selezionare tutti i moduli disponibili, tranne “Power User”, in modo da rendere più agevole la gestione degli endpoint e la creazione delle policy, senza dare inutilmente privilegi agli utenti.

È consigliato impostare una password per la disinstallazione dell’agent e di spuntare “remove competitors”.

6.3. Creazione Maintenance Windows

La maintenance window definisce la politica di scansione e applicazione delle patch, una volta creata è possibile associarla alle policy desiderate direttamente nella sezione “Patch Management” all’interno della policy.

Per creare una maintenance window andare 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 le impostazioni di ricorrenza e orario di esecuzione.

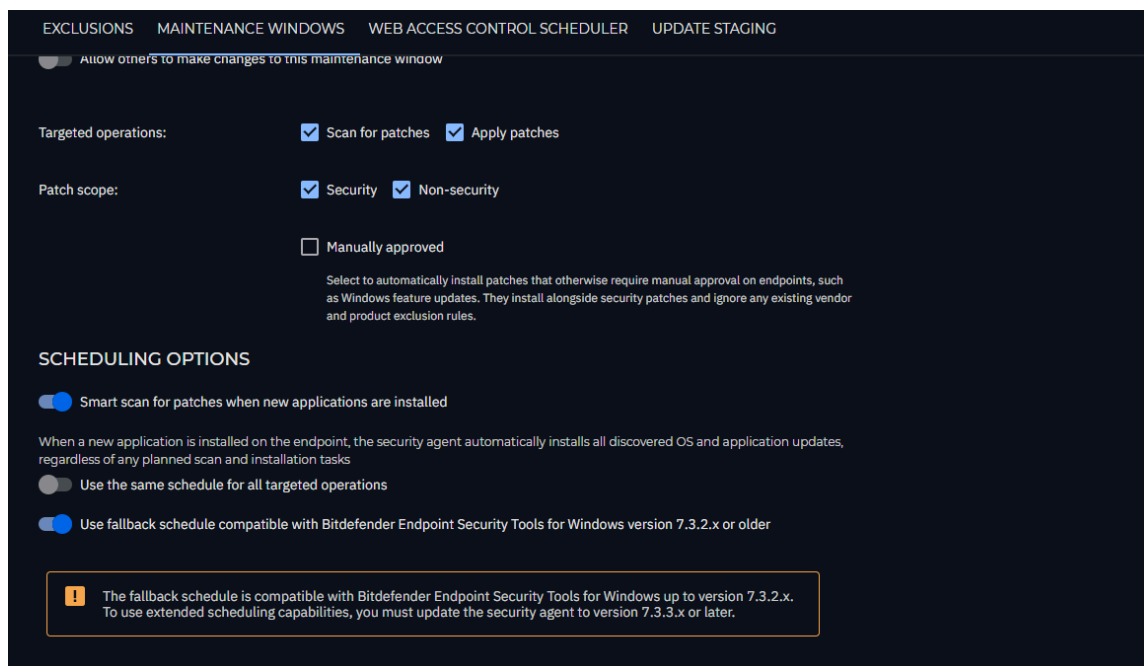


Figure 16: Maintenance Window

6.3.1. 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.

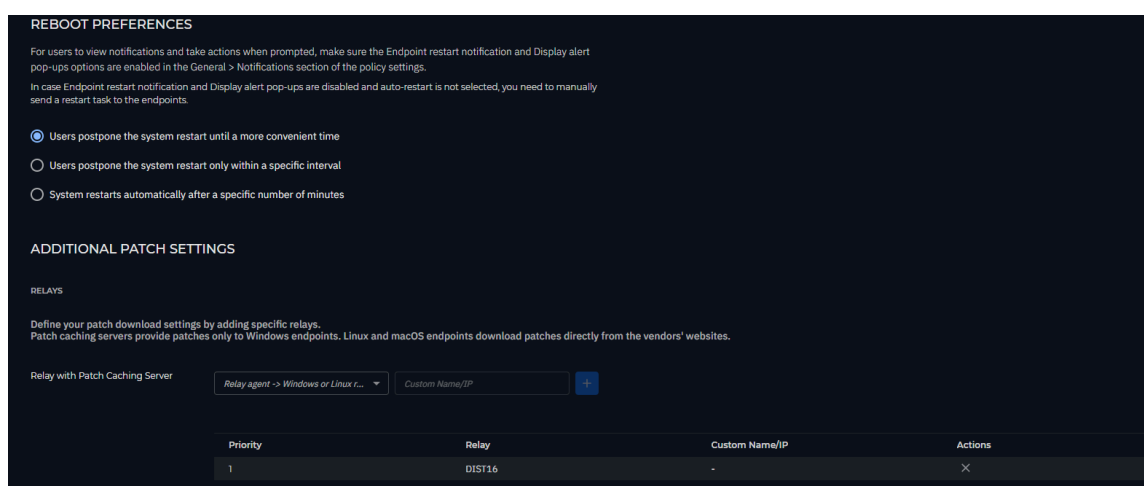


Figure 17: Patch Caching Server

6.4. Creazione Web Access Control Scheduler

È possibile creare un Web Access Control Scheduler nella sezione "Policies -> Configuration Profiles -> Web Access Control Scheduler".

Nella schermata che si apre, è possibile creare una o più regole di controllo, il sistema propone categorie di siti selezionabili per il controllo (come social network, gioco d'azzardo, shopping ecc.). Per ogni regola è possibile selezionare gli intervalli di tempo per cui essa sarà in vigore e anche se bloccare completamente le pagine oppure mostrare solo un warning all'utente.

| Priority | Name | Categories | Time Range | Actions |
|----------|---------|---------------------------------------|---------------|---------|
| 1 | prova#2 | Food, Gambling, Hate, Social Networks | 00:00 - 23:59 | |

Figure 18: Creazione Web Access Control Scheduler

6.4.1. Best Practices

Perché la schedule funzioni a dovere, è necessario aver attivato la scansione HTTPS in Network Protection -> General.

6.5. Creazione liste di esclusioni

Tramite le liste di esclusioni, è possibile creare dei gruppi di esclusioni, in modo da poterle aggiungere a più policy in maniera rapida e semplice. Innanzitutto, andare alla sezione "Policy -> Configuration Profiles -> Exclusions". Se non si ha già una lista, premere su "New List", a questo punto inserire un nome e tutte le esclusioni che vogliamo.

Altrimenti, è anche possibile creare direttamente un'esclusione tramite pulsante "Add Exclusion", e poi assegnarla a tutte le liste che vogliamo selezionandola dall'elenco e premendo su "Assign to Lists".

6.6. Creazione delle Blocklist

Le blocklist permettono di avere delle liste di applicazioni o processi bloccati "prestabilite" da poter essere incluse in tutte le policy che vogliamo, senza doverle ricreare in ogni policy.

Per creare una regola, andare nella sezione "Incidents -> Blocklist" nel menu a sinistra e, nella finestra che si apre, premere "Add rule". Una volta premuto "Add Rule" ci verrà richiesto di scegliere quale tipo di blocco vogliamo creare, e poi i dettagli riguardanti all'elemento da bloccare (Percorso app, IP, ecc.).

Una volta creati i blocchi, essi saranno automaticamente aggiunti a tutte le policy che hanno attivi i corrispondenti moduli.