

The background of the page is a dark, futuristic digital landscape. It features glowing blue and cyan light trails, circular patterns, and a grid of data points, suggesting a high-tech or cyber environment. The overall aesthetic is sleek and modern.

Bitdefender®

GravityZone

INSTALLAZIONE

Bitdefender GravityZone Installazione

Data di pubblicazione 2021.04.20

Diritto d'autore© 2021 Bitdefender

Avvertenze legali

Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza il consenso scritto di un rappresentante autorizzato di Bitdefender. L'inserimento di brevi citazioni nelle recensioni è possibile solo indicando la fonte citata. Il contenuto non può essere modificato in alcun modo.

Avvertenze e Limiti. Questo prodotto e la sua documentazione sono protetti dal diritto d'autore. Le informazioni su questo documento sono fornite «così come sono» senza alcuna garanzia. Sebbene sia stata adottata ogni precauzione nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo prodotto.

Questo manuale contiene collegamenti a siti Internet di terze parti, che non sono sotto il controllo di Bitdefender, conseguentemente Bitdefender non è responsabile per il contenuto di qualsiasi sito collegato. Se accedi a siti Internet di terze parti, menzionati in questo manuale, lo farai assumendotene tutti i rischi. Bitdefender fornisce tali collegamenti solo come risorsa, e l'inclusione dei collegamenti non implica che Bitdefender approvi o accetti alcuna responsabilità per il contenuto dei siti di terze parti.

Marchi registrati. In questo manuale potrebbero essere citati nomi e marchi registrati. Tutti i marchi registrati e non in questo documento appartengono ai rispettivi proprietari e vengono rispettosamente riconosciuti.

Avvertenze legali

Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza il consenso scritto di un rappresentante autorizzato di Bitdefender.

L'inserimento di brevi citazioni nelle recensioni è possibile solo indicando la fonte citata. Il contenuto non può essere modificato in alcun modo.

Avvertenze e Limiti. Questo prodotto e la sua documentazione sono protetti dal diritto d'autore. Le informazioni su questo documento sono fornite «così come sono» senza alcuna garanzia. Sebbene sia stata adottata ogni precauzione nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo prodotto.

responsabilità per il contenuto dei siti di terze parti.

Marchi registrati. In questo manuale potrebbero essere citati nomi e marchi registrati. Tutti i marchi registrati e non in questo documento appartengono ai rispettivi proprietari e vengono rispettosamente riconosciuti.

Indice

Prefazione	viii
1. Convenzioni usate in questo manuale	viii
1. Informazioni su GravityZone	1
2. Livelli di protezione di GravityZone	2
2.1. Antimalware	2
2.2. Advanced Threat Control	4
2.3. HyperDetect	4
2.4. Anti-exploit avanzato	4
2.5. Firewall	5
2.6. Controllo contenuti	5
2.7. Network Attack Defense	5
2.8. Patch Management	5
2.9. Controllo dispositivi	6
2.10. Full Disk Encryption	6
2.11. Security for Exchange	6
2.12. Controllo applicazioni	7
2.13. Sandbox Analyzer	7
2.14. Hypervisor Memory Introspection (HVI)	7
2.15. Network Traffic Security Analytics (NTSA)	8
2.16. Security for Storage	8
2.17. Security for Mobile	9
2.18. Disponibilità dei livelli di protezione di GravityZone	9
3. Architettura di GravityZone	10
3.1. GravityZone VA	10
3.1.1. Database di GravityZone	10
3.1.2. Server di aggiornamento di GravityZone	11
3.1.3. Server di comunicazione di GravityZone	11
3.1.4. Console web (GravityZone Control Center)	11
3.1.5. Report builder database	11
3.1.6. Rapporti processori builder	11
3.2. Security Server	11
3.3. Pacchetto supplementare HVI	12
3.4. Agenti di sicurezza	12
3.4.1. Bitdefender Endpoint Security Tools	12
3.4.2. Endpoint Security for Mac	15
3.4.3. GravityZone Mobile Client	15
3.4.4. Bitdefender Tools (vShield)	15
3.5. Architettura di Sandbox Analyzer	16
4. Requisiti	18
4.1. GravityZone Virtual Appliance	18
4.1.1. Formati supportati e piattaforme di virtualizzazione	18
4.1.2. Hardware	18
4.1.3. Connessione Internet	22

4.2. Control Center	23
4.3. Protezione degli endpoint	23
4.3.1. Hardware	24
4.3.2. Sistemi operativi supportati	27
4.3.3. File system supportati	33
4.3.4. Browser supportati	33
4.3.5. Piattaforme di virtualizzazione supportate	34
4.3.6. Security Server	37
4.3.7. Uso del traffico	39
4.4. Exchange Protection	41
4.4.1. xxx	41
4.4.2. Requisiti di sistema	41
4.4.3. Altri requisiti software	42
4.5. Sandbox Analyzer On-Premises	42
4.5.1. ESXi Hypervisor	42
4.5.2. Virtual Appliance di Sandbox Analyzer	43
4.5.3. Network Security Virtual Appliance	45
4.5.4. Requisiti host fisici e scaling hardware	45
4.5.5. Requisiti di comunicazione di Sandbox Analyzer	46
4.6. HVI	47
4.7. Full Disk Encryption	53
4.8. Protezione archiviazione	54
4.9. Protezione mobile	55
4.9.1. Piattaforme supportate	55
4.9.2. Requisiti connettività	55
4.9.3. Notifiche push	55
4.9.4. Certificati gestione iOS	55
4.10. Report Builder	56
4.10.1. Hardware	56
4.10.2. Versioni del prodotto GravityZone	57
4.11. Porte di comunicazione di GravityZone	57
5. Installare la protezione	58
5.1. Installazione e configurazione di GravityZone	58
5.1.1. Preparati per l'installazione	58
5.1.2. Implementare GravityZone	59
5.1.3. Configurazione iniziale Control Center	68
5.1.4. Configura le impostazioni della Control Center	71
5.1.5. Gestire la appliance di GravityZone	105
5.2. Amministrazione licenza	119
5.2.1. Trovare un rivenditore	119
5.2.2. Inserire i tuoi codici di licenza	120
5.2.3. Verificare i dettagli della licenza attuale	120
5.2.4. Reimpostare il conteggio utilizzo licenze	122
5.2.5. Eliminare i codici di licenza	122
5.3. Installare la protezione per endpoint	122
5.3.1. Installare Security Server	123
5.3.2. Installare gli agenti di sicurezza	133
5.4. Installare Sandbox Analyzer On-Premises	158

5.4.1. Preparati per l'installazione	158
5.4.2. Impiegare la Virtual appliance di Sandbox Analyzer	158
5.4.3. Impiegare la Network Security Virtual Appliance	164
5.5. Installare Full Disk Encryption	166
5.6. Installare la protezione di Exchange	166
5.6.1. Preparazione all'installazione	167
5.6.2. Installare la protezione sui server Exchange	167
5.7. Installare HVI	168
5.8. Installare la Protezione memorizzazione	171
5.9. Installare la protezione dei dispositivi mobile	172
5.9.1. Configura l'indirizzo esterno per il Server di comunicazione	172
5.9.2. Crea e organizza utenti personalizzati	174
5.9.3. Aggiungi dispositivi agli utenti	175
5.9.4. Installa GravityZone Mobile Client sui dispositivi	177
5.10. Installare il Report Builder	178
5.10.1. Installare il database del Report Builder	179
5.10.2. Installare Processori del Report Builder	180
5.11. Credentials Manager	181
5.11.1. Sistema operativo	182
5.11.2. Ambiente virtuale	183
5.11.3. Eliminare le credenziali dal Credentials Manager	184
6. Aggiornare GravityZone	185
6.1. Aggiornare le appliance di GravityZone	185
6.1.1. Aggiornamento Manuale	186
6.1.2. Aggiornamento automatico	187
6.2. Configurare il server di aggiornamento	188
6.3. Scaricare gli aggiornamenti del prodotto	189
6.4. Testare gli aggiornamenti	190
6.4.1. Prerequisiti	190
6.4.2. Usare la fase di test	191
6.5. Aggiornamenti del prodotto offline	198
6.5.1. Prerequisiti	198
6.5.2. Configurare l'istanza di GravityZone online	199
6.5.3. Configurare e scaricare i file di aggiornamento iniziali	199
6.5.4. Configurare l'istanza di GravityZone offline	202
6.5.5. Utilizzare gli aggiornamenti offline	205
6.5.6. Utilizzare la console web	205
7. Disinstallare la protezione	207
7.1. Disinstallare la protezione per endpoint	207
7.1.1. Disinstallare gli agenti di sicurezza	207
7.1.2. Disinstallare Security Server	209
7.2. Disinstallare HVI	210
7.3. Disinstallare la protezione di Exchange	212
7.4. Disinstallare Sandbox Analyzer On-Premises	213
7.5. Disinstallare la protezione dei dispositivi mobile	213
7.6. Disinstallare Report Builder	215
7.7. Disinstallare i ruoli della Virtual appliance di GravityZone	216



8. Ottenere aiuto	218
8.1. Centro di supporto di Bitdefender	218
8.2. Necessiti di assistenza	219
8.3. Usare lo strumento di supporto	220
8.3.1. Utilizzare lo Strumento di supporto sui sistemi operativi Windows	220
8.3.2. Utilizzare lo Strumento di supporto su sistemi operativi Linux	221
8.3.3. Utilizzare lo Strumento di supporto sui sistemi operativi Mac	223
8.4. Informazioni di contatto	224
8.4.1. Indirizzi Web	224
8.4.2. Distributori locali	225
8.4.3. Uffici di Bitdefender	225
A. Appendici	228
A.1. Tipi di file supportati	228
A.2. Oggetti Sandbox Analyzer	229
A.2.1. Estensioni e tipi di file supportati per l'invio manuale	229
A.2.2. Tipi di file supportati da Pre-filtro contenuti per l'invio automatico	229
A.2.3. Eccezioni predefinite all'invio automatico	230
A.2.4. Applicazioni consigliate per le VM di detonazione	230

Prefazione

Questa guida è rivolta agli amministratori IT responsabili dell'impiego della protezione di GravityZone nelle sedi della propria organizzazione. In questa guida, i responsabili IT in cerca di informazioni su GravityZone possono trovare i requisiti di GravityZone e i moduli di protezione disponibili.

Questo documento intende spiegare come installare e configurare la soluzione GravityZone e i suoi agenti di sicurezza su tutti i tipi di endpoint nella tua azienda.

1. Convenzioni usate in questo manuale




Convenzioni tipografiche

Questa guida utilizza diversi stili di testo per migliorare la leggibilità. Scopri maggiori dettagli sul loro aspetto e significato nella tabella sottostante.

Aspetto	Descrizione
campione	I nomi dei comandi e le sintassi, i percorsi e i nomi dei file, i percorsi dei file di configurazione e i testi inseriti vengono stampati con caratteri a spaziatura fissa.
http://www.bitdefender.com	I link URL portano a ubicazioni esterne, su server http o ftp.
gravityzone-docs@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
«Prefazione» (p. viii)	Questo è un link interno, verso una qualche posizione nel documento.
opzione	Tutte le opzioni del prodotto sono indicate in grassetto .
parola chiave	Le opzioni dell'interfaccia, le parole chiave o le scorciatoie sono evidenziate usando caratteri in grassetto .

Avvertenze

Gli avvisi appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione informazioni aggiuntive relative al paragrafo attuale.

-  **Nota**
La nota è una breve osservazione. Anche se la puoi omettere, la nota può fornire informazioni di valore come una caratteristica specifica o un link verso temi collegati.
-  **Importante**
Questa richiede attenzione, è sconsigliato saltarla. Solitamente contempla informazioni non critiche ma importanti.
-  **Avvertimento**
Questa è un'informazione critica che deve essere trattata con estrema cautela. Seguendone le indicazioni si eviteranno eventualità negative. Dovrebbe essere letta e compresa in quanto è la descrizione di qualcosa di estremamente rischioso.

1. INFORMAZIONI SU GRAVITYZONE

GravityZone è una soluzione di sicurezza aziendale sviluppata da zero per il cloud e la virtualizzazione con l'obiettivo di offrire servizi di sicurezza a endpoint fisici, dispositivi mobile e macchine virtuali in cloud pubblici e privati, oltre a mail server di Exchange.

GravityZone è un prodotto con una console di gestione unificata disponibile nel cloud, ospitata da Bitdefender o come appliance virtuale da installare nelle strutture dell'azienda, fornendo un unico punto per la distribuzione, l'applicazione e la gestione delle policy di sicurezza per qualunque numero e tipo di endpoint, in qualsiasi posizione.

GravityZone offre più livelli di sicurezza per gli endpoint e per i mail server di Microsoft Exchange: antimalware con monitoraggio comportamentale, protezione da minacce zero-day, controllo delle applicazioni e sandboxing, firewall, controllo dei dispositivi, controllo dei contenuti, anti-phishing e antispam.

2. LIVELLI DI PROTEZIONE DI GRAVITYZONE

GravityZone ti offre i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Anti-exploit avanzato
- Firewall
- Controllo contenuti
- Patch Management
- Controllo dispositivi
- Full Disk Encryption
- Security for Exchange
- Controllo applicazioni
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

Il livello di protezione antimalware è basato su scansione delle firme e analisi euristica (B-HAVE, ATC) contro virus, worm, Trojan, spyware, adware, keylogger, rootkit e altri tipi di software dannoso.

La tecnologia di scansione di Bitdefender si basa sulle seguenti tecnologie:

- Per iniziare, viene impiegato un metodo di scansione tradizionale, dove i contenuti esaminati vengono confrontati con il database delle firme. Il database delle firme include schemi di byte specifici per le minacce conosciute e viene regolarmente aggiornato da Bitdefender. Questo metodo di scansione è efficace contro le minacce confermate che sono state individuate e documentate. Tuttavia, non importa quanto il database delle firme venga aggiornato prontamente, c'è sempre una finestra di vulnerabilità tra il momento in cui la minaccia viene scoperta e quello in cui viene rilasciata una soluzione.
- Contro le nuove minacce non ancora documentate, un secondo livello di protezione viene offerto da **B-HAVE**, il motore euristico di Bitdefender. Gli algoritmi euristici rilevano i malware basati sulle caratteristiche

comportamentali. B-HAVE esegue i file sospetti in un ambiente virtuale per testarne l'impatto sul sistema e assicurarsi che non siano una minaccia. Se viene rilevata una minaccia, viene bloccata l'esecuzione del programma.

Motori di scansione

Bitdefender GravityZone è in grado di impostare automaticamente i motori di scansione quando si creano i pacchetti dell'agente di sicurezza, in base alla configurazione dell'endpoint.

L'amministratore può anche personalizzare i motori di scansione, potendo scegliere tra diverse tecnologie di scansione:

1. **Scansione locale**, quando la scansione è eseguita su un endpoint in locale. La modalità di scansione locale è adatta per macchine potenti, con il contenuto di sicurezza memorizzato localmente.
2. **Scansione ibrida con motori leggeri (cloud pubblico)**, con un'impronta media, utilizzando la scansione in-the-cloud e, in parte, il contenuto di sicurezza in locale. Questa modalità di scansione ha il vantaggio di un miglior consumo delle risorse, mentre coinvolge la scansione off-premise.
3. **Scansione centrale in cloud pubblico o privato**, con una piccola impronta che richiede un Security Server per la scansione. In questo caso, nessun contenuto di sicurezza viene memorizzato localmente e la scansione viene scaricata sul Security Server.



Nota

C'è un minimo set di motori che viene memorizzato localmente, necessario per scompattare i file compressi.

4. **Scansione centrale (scansione tramite cloud pubblico o privato con Security Server) con riserva* nella scansione locale (motori completi)**
5. **Scansione centrale (scansione tramite cloud pubblico o privato con Security Server) con riserva* nella scansione ibrida (cloud pubblico con motori leggeri)**

* Quando si usa un doppio motore di scansione, se il primo motore non è disponibile, sarà utilizzato quello di riserva. Il consumo di risorse e l'utilizzo della rete dipenderanno dai motori utilizzati.

2.2. Advanced Threat Control

Per le minacce in grado di eludere persino il motore euristico, c'è un altro livello di protezione costituito da Advanced Threat Control (ATC).

Advanced Threat Control monitora costantemente i processi in esecuzione e classifica i comportamenti sospetti come un tentativo di: mascherare il tipo di processo, eseguire il codice nello spazio di un altro processo (disattivando la memoria del processo per l'escalation dei privilegi), replicare, rilasciare file, nascondere applicazioni dall'enumerazione dei processi, ecc. Ogni comportamento sospetto aumenta la valutazione del processo. Quando viene raggiunta una determinata soglia, viene attivato un allarme.

2.3. HyperDetect

Bitdefender HyperDetect è un livello di sicurezza aggiuntivo appositamente progettato per rilevare attacchi avanzati e attività sospette in fase di pre-esecuzione. HyperDetect contiene modelli di apprendimento automatico e tecnologie di rilevamento di attacchi furtivi contro minacce come attacchi zero-day, minacce persistenti avanzate (APT), malware oscurati, attacchi privi di file (uso improprio di PowerShell, Windows Management Instrumentation, ecc.), furto di credenziali, attacchi mirati, malware personalizzati, attacchi basati su script, exploit, strumenti di hacking, traffico di rete sospetto, applicazioni potenzialmente indesiderate (PUA) e ransomware.



Nota

Questo modulo è un add-on disponibile con un codice di licenza separato.

2.4. Anti-exploit avanzato

Dotato di apprendimento automatico, l'Anti-Exploit avanzato è una nuova tecnologia proattiva che blocca gli attacchi zero-day portati da exploit evasivi. L'Anti-exploit avanzato rileva gli exploit più recenti in tempo reale e attenua le vulnerabilità in grado di danneggiare la memoria, che potrebbero altre soluzioni di sicurezza. Protegge le applicazioni più comunemente utilizzate, come i browser, Microsoft Office o Adobe Reader, e non solo. Monitora i processi del sistema e protegge da violazioni di sicurezza e dall'hijack dei processi esistenti.

2.5. Firewall

Il Firewall controlla l'accesso delle applicazioni alla rete e a Internet. L'accesso viene consentito automaticamente per un vasto database di applicazioni note e legittime. Inoltre, il firewall può proteggere il sistema da port scan, limitare ICS e avvisare quando nuovi nodi si uniscono a una connessione Wi-Fi.

2.6. Controllo contenuti

Il modulo Controllo contenuti ti aiuta a rafforzare le politiche aziendali relative a traffico consentito, accesso web, protezione dati e controllo applicazioni. Gli amministratori possono definire le opzioni e le eccezioni di scansione del traffico, programmare l'accesso al web bloccando o consentendo eventuali URL o categorie web, configurare le regole della protezione dati e definire le autorizzazioni per l'uso di determinate applicazioni.

2.7. Network Attack Defense

Il modulo Network Attack Defense si affida a una tecnologia di Bitdefender focalizzata sul rilevamento di attacchi di rete progettati per ottenere accesso agli endpoint attraverso tecniche specifiche, come attacchi di forza bruta, exploit di rete, furti di password, vettori di infezione drive-by-download, bot e Trojan.

2.8. Patch Management

Pienamente integrato in GravityZone, Gestione patch mantiene i sistemi operativi e le applicazioni software sempre aggiornati, fornendo una visione completa sullo stato delle patch per i tuoi endpoint Windows gestiti.

Il modulo Gestione patch di GravityZone include diverse funzionalità, come scansione patch a richiesta / programmata, applicazione di patch automatica / manuale o segnalazione di patch mancanti.

Puoi anche trovare maggiori informazioni su fornitori e prodotti supportati da Gestione patch di GravityZone in questo [articolo della KB](#).



Nota

Gestione patch è un add-on disponibile con un codice di licenza separato per tutti i pacchetti GravityZone disponibili.

2.9. Controllo dispositivi

Il modulo Controllo dispositivi consente di prevenire la sottrazione di dati sensibili e le infezioni di malware tramite dispositivi esterni collegati agli endpoint, applicando regole ed eccezioni di blocco tramite una policy a una vasta gamma di tipi di dispositivi (come unità flash USB, dispositivi Bluetooth, lettori CD/DVD, dispositivi di archiviazione, ecc.).

2.10. Full Disk Encryption

Questo livello di protezione ti consente di fornire una cifratura completa del disco sugli endpoint, gestendo BitLocker su Windows e FileVault e diskutil su macOS. È possibile cifrare e decifrare i volumi di avvio con pochi clic, mentre GravityZone gestisce l'intero processo con un intervento minimo da parte degli utenti. Inoltre, GravityZone memorizza i codici di ripristino necessari per sbloccare i volumi quando gli utenti dimenticano le proprie password.



Nota

Full Disk Encryption è un add-on disponibile con un codice di licenza separato per tutti i pacchetti GravityZone disponibili.

2.11. Security for Exchange

Bitdefender Security for Exchange offre funzioni antimalware, antispam, antiphishing e di filtraggio contenuti e allegati, integrate perfettamente con Microsoft Exchange Server per assicurare un ambiente di messaggistica e collaborazione protetto e aumentare la produttività. Utilizzando tecnologie antimalware e antispam pluripremiate, protegge gli utenti di Exchange dai malware più recenti e sofisticati, e da ogni tentativo di sottrarre dati sensibili e preziosi degli utenti.



Importante

Security for Exchange è stato progettato per proteggere l'intera organizzazione di Exchange a cui appartiene il server Exchange protetto. Ciò significa che protegge tutte le caselle di posta attive, incluso le caselle di posta di utente/stanza/equipaggiamento/condivise.

Oltre alla protezione di Microsoft Exchange, la licenza copre anche i moduli di protezione endpoint installati sul server.

2.12. Controllo applicazioni

Il modulo Controllo applicazioni ferma malware e attacchi zero-day, migliorando la sicurezza senza influenzare la produttività. Il Controllo applicazioni impone policy di whitelist flessibili, che identificano e impediscono l'installazione e l'esecuzione di qualsiasi applicazione indesiderata, inaffidabile o dannosa.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender. Il sandbox utilizza una vasta gamma di tecnologie Bitdefender per eseguire i payload in un ambiente virtuale contenuto, ospitato da Bitdefender o impiegato in locale, analizzare il loro comportamento e segnalare anche il minimo cambiamento del sistema, in genere un chiaro segnale di intenzioni dannose.

Sandbox Analyzer utilizza una serie di sensori per detonare i contenuti da endpoint gestiti, stream di traffico di rete, quarantena centralizzata e server ICAP.

Inoltre, Sandbox Analyzer consente l'invio manuale e tramite API del campione.

2.14. Hypervisor Memory Introspection (HVI)

È risaputo che aggressori organizzati e in cerca di facili profitti cercano vulnerabilità conosciute (vulnerabilità zero-day) o sfruttano exploit specifici (exploit zero-day) e altri strumenti. Gli aggressori utilizzano anche tecniche avanzate per ritardare e sequenziare i payload degli attacchi così da mascherare le attività dannose. Gli attacchi più recenti e guidati dal profitto vengono sviluppati per essere furtivi e superare gli strumenti di sicurezza tradizionali.

Per gli ambienti virtualizzati, ora il problema è stato risolto, in quanto HVI protegge i data center con un'elevata densità di virtual machine dalle minacce più avanzate e sofisticate che i motori basati su firme non possono scongiurare. Impone un forte isolamento, assicurando una rilevazione in tempo reale degli attacchi, bloccandoli non appena avvengono e rimuovendo subito le minacce.

Sia che la macchina protetta sia Windows o Linux, un server o un desktop, HVI fornisce un'introspezione a un livello impossibile da raggiungere dall'interno del sistema operativo guest. Proprio come l'hypervisor controlla l'accesso hardware per ciascuna virtual machine, HVI ha una conoscenza profonda sia in kernel che user mode a livello di memoria in-guest. Di conseguenza, HVI ha una visione

completa della memoria guest, e quindi un contesto completo. Allo stesso tempo, HVI è isolato dai guest protetti, proprio come lo stesso hypervisor. Operando a livello di hypervisor e sfruttandone le funzionalità, HVI supera le sfide tecniche della sicurezza tradizionale per svelare le attività dannose nei data center.

HVI identifica le tecniche di attacco piuttosto che gli schemi di attacco. In questo modo, la tecnologia è in grado di identificare, segnalare e impedire le tecniche di exploit più comuni. Il kernel è protetto dalle tecniche di hooking dei rootkit che vengono usate durante la catena d'attacco per fornire la massima furtività. Anche i processi in user mode sono protetti dall'inserimento di codice, alterazione delle funzioni ed esecuzione di codice da stack o heap.

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) è una soluzione di sicurezza di rete che analizza i flussi di traffico IPFIX per rilevare l'eventuale presenza di malware e comportamenti dannosi.

Bitdefender NTSA è progettato per agire accanto alle misure di sicurezza esistenti, come protezione complementare in grado di coprire tutti i punti ciechi che gli strumenti tradizionali non monitorano.

Gli strumenti di sicurezza di rete tradizionali in genere tentano di prevenire le infezioni malware analizzando il traffico in uscita (tramite sandbox, firewall, antivirus e così via). Bitdefender NTSA si concentra unicamente sul monitorare il traffico di rete in uscita per rilevare eventuali comportamenti dannosi.

2.16. Security for Storage

GravityZone Security for Storage offre la migliore protezione in tempo reale per i principali sistemi di condivisione di file e archiviazione in rete. Sia il sistema che gli algoritmi di rilevazione delle minacce si aggiornano automaticamente, senza richiedere alcun intervento da parte tua e interrompere l'attività dei tuoi utenti finali.

Due o più Security Server di GravityZone multiplatforma svolgono il ruolo di server ICAP fornendo servizi antimalware ai dispositivi Network-Attached Storage (NAS) e sistemi di condivisione dei file conformi al protocollo ICAP (Internet Content Adaptation Protocol, come definito in RFC 3507).

Quando un utente chiede di aprire, leggere, scrivere o chiudere un file da un portatile, una postazione di lavoro, una piattaforma mobile o un altro dispositivo, il client ICAP (un NAS o un sistema di condivisione di file) invia una richiesta di scansione

al Security Server e riceve un verdetto relativo al file. In base al risultato, il Security Server consente l'accesso, nega l'accesso o elimina il file.

Nota

Questo modulo è un add-on disponibile con un codice di licenza separato.

2.17. Security for Mobile

Unifica la sicurezza a livello aziendale con gestione e controllo di conformità di iPhone, iPad e dispositivi Android fornendo un software affidabile e una serie di aggiornamenti tramite i marketplace di Apple e Android. La soluzione è stata progettata per consentire l'adozione controllata di iniziative di bring-your-own-device (BYOD), applicando costantemente le politiche di utilizzo a tutti i dispositivi portatili. Le funzionalità di sicurezza includono blocco dello schermo, controllo dell'autenticazione, posizione del dispositivo, eliminazione remota dei contenuti, rilevazione di dispositivi con root o jailbreak e profili di sicurezza. Sui dispositivi Android, il livello di sicurezza viene migliorato con la scansione in tempo reale e la cifratura dei supporti rimovibili. Di conseguenza, i dispositivi mobile sono controllati e le importanti informazioni aziendali su di essi sono protette.

2.18. Disponibilità dei livelli di protezione di GravityZone

La disponibilità dei livelli di protezione di GravityZone varia a seconda del sistema operativo dell'endpoint. Per maggiori informazioni, fai riferimento all'articolo della KB [disponibilità dei livelli di protezione di GravityZone](#).

3. ARCHITETTURA DI GRAVITYZONE

L'architettura unica di GravityZone consente alla soluzione di adattarsi con facilità e proteggere qualsiasi numero di sistemi. GravityZone può essere configurato per utilizzare più appliance virtuali e istanze di ruoli specifici (database, server di comunicazione, server di aggiornamento e console web) per assicurare affidabilità e scalabilità.

Ogni istanza del ruolo può essere installata su una diversa appliance. I balancer del ruolo integrati assicurano che l'impiego di GravityZone protegga persino le maggiori reti aziendali senza causare rallentamenti o colli di bottiglia. Se presenti nella rete, al posto dei balancer integrati, possono essere usati anche software e hardware di bilanciamento del carico esistenti.

Fornito in un contenitore virtuale, GravityZone può essere importato per essere eseguito su qualsiasi piattaforma di virtualizzazione, tra cui VMware, Citrix, Microsoft Hyper-V, Nutanix Prism e Microsoft Azure.

L'integrazione con VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element e Microsoft Azure riduce lo sforzo di impiego della protezione per gli endpoint fisici e virtuali.

La soluzione di GravityZone include i seguenti componenti:

- GravityZone Virtual Appliance
- Security Server
- Pacchetto supplementare HVI
- Agenti di sicurezza

3.1. GravityZone VA

La soluzione in locale di GravityZone viene fornita come una appliance virtuale (VA) indurita autoconfigurante Linux Ubuntu, incorporata in un'immagine di una virtual machine, facile da installare e configurare tramite una CLI (Interfaccia a riga di comando). La virtual appliance è disponibile in diversi formati, compatibili con le principali piattaforme di virtualizzazione (OVA, XVA, VHD, OVF, RAW).

3.1.1. Database di GravityZone

La logica centrale dell'architettura di GravityZone. Bitdefender utilizza un database non relazionale MongoDB, facile da adattare e replicare.

3.1.2. Server di aggiornamento di GravityZone

Il Server di aggiornamento ha un ruolo importante: aggiornare la soluzione GravityZone e gli agenti endpoint replicando e pubblicando i pacchetti o i file d'installazione necessari.

3.1.3. Server di comunicazione di GravityZone

Il server di comunicazione è il collegamento tra gli agenti di sicurezza e il database, trasferendo policy e attività agli endpoint protetti, oltre agli eventi segnalati dagli agenti di sicurezza.

3.1.4. Console web (GravityZone Control Center)

Le soluzioni di sicurezza di Bitdefender vengono gestite da un solo punto di gestione, la console web Control Center. Ciò fornisce una gestione e un accesso semplificati all'intero stato di sicurezza, oltre che alle minacce alla sicurezza globale, e al controllo su tutti i moduli di sicurezza che proteggono desktop fisici o virtuali, server e dispositivi mobile. Basata su un'Architettura Gravity, Control Center è in grado di rispondere alle necessità persino delle maggiori aziende.

La Control Center si integra con il sistema di gestione e monitoraggio esistenti per semplificare l'applicazione automatica della protezione a workstation, server o dispositivi mobile non gestiti, che compaiono in Microsoft Active Directory, VMware vCenter, Nutanix Prism Element o Citrix XenServer, o che vengono semplicemente rilevati nella rete.

3.1.5. Report builder database

Il ruolo Report Builder Database fornisce i dati necessari per creare rapporti query-based.

3.1.6. Rapporti processori builder

Il ruolo Report Builder Processors è essenziale per creare, gestire e memorizzare in rapporti query-based che usano le informazioni dal Report Builder Database.

3.2. Security Server

Il Security Server è una macchina virtuale dedicata che deduplica e centralizza la maggior parte delle funzionalità antimalware dei relativi agenti, comportandosi come un server di scansione.

Ci sono tre versioni di Security Server, per ciascun tipo di ambiente di virtualizzazione:

- **Security Server for VMware NSX.** Questa versione si installa automaticamente su ogni host nel cluster in cui è stato impiegato Bitdefender.
- **Security Server for VMware vShield Endpoint.** Questa versione deve essere installata su ciascun host da proteggere.
- **Security Server Multi-Platform.** Questa versione è per diversi altri ambienti virtualizzati e deve essere installata su uno o più host in modo da accogliere il numero di virtual machine protette. Utilizzando HVI, un Security Server deve essere installato su ciascun host che contiene virtual machine da proteggere.

3.3. Pacchetto supplementare HVI

Il pacchetto HVI assicura il collegamento tra l'hypervisor e il Security Server su quell'host. In questo modo, il Security Server può monitorare la memoria in uso sull'host in cui è installato, in base alle policy di sicurezza di GravityZone.

3.4. Agenti di sicurezza

Per proteggere la tua rete con Bitdefender, devi installare gli appropriati agenti di sicurezza di GravityZone sugli endpoint della rete.

- [Bitdefender Endpoint Security Tools](#)
- [Endpoint Security for Mac](#)
- [GravityZone Mobile Client](#)
- [Bitdefender Tools \(vShield\)](#)

3.4.1. Bitdefender Endpoint Security Tools

GravityZone assicura la protezione di macchine Windows e Linux fisiche e virtuali con Bitdefender Endpoint Security Tools, un agente di sicurezza intelligente e consapevole, che si adatta al tipo di endpoint. Bitdefender Endpoint Security Tools può essere impiegato su qualsiasi macchina, virtuale o fisica, fornendo un sistema di scansione flessibile e diventando una scelta ideale per ambienti misti (fisici, virtuali e cloud).

Oltre a proteggere il file system, Bitdefender Endpoint Security Tools include anche una protezione del server mail per Microsoft Exchange Server.

Bitdefender Endpoint Security Tools utilizza un unico modello di policy per macchine fisiche e virtuali e una fonte per i kit di installazione per qualsiasi ambiente (fisico o virtuale) con Windows.

Livelli di protezione

Con Bitdefender Endpoint Security Tools sono disponibili i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Controllo contenuti
- Network Attack Defense
- Patch Management
- Controllo dispositivi
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Controllo applicazioni

Ruoli degli endpoint

- Utente esperto
- Relay
- Server caching patch
- Exchange Protection

Utente esperto

Gli amministratori del Control Center possono garantire diritti di Utente esperto agli utenti degli endpoint tramite le impostazioni della policy. Il modulo Utente esperto consente di garantire diritti di amministrazione a livello di utente, permettendo all'utente dell'endpoint di accedere e modificare le impostazioni di sicurezza tramite una console in locale. Control Center riceve una notifica ogni volta che un endpoint passa in modalità Utente esperto e l'amministratore di Control Center può sempre sovrascrivere le impostazioni di sicurezza locali.



Importante

Questo modulo è disponibile solo per i sistemi operativi Windows desktop e server supportati. Per maggiori informazioni, fai riferimento a «[Sistemi operativi supportati](#)» (p. 27).

Relay

Gli agenti endpoint con ruolo Bitdefender Endpoint Security Tools Relay agiscono da proxy di comunicazione e server di aggiornamento per gli altri endpoint nella rete. Gli agenti endpoint con ruolo di relay sono particolarmente richiesti in organizzazioni con reti isolate, in cui tutto il traffico passa da un singolo punto di accesso.

In aziende con grandi reti distribuite, gli agenti relay aiutano a ridurre il consumo di banda, prevenendo agli endpoint protetti e ai server di sicurezza di connettersi direttamente alla appliance di GravityZone.

Una volta che un agente Bitdefender Endpoint Security Tools Relay viene installato nella rete, altri endpoint possono essere configurati tramite la policy per comunicare con Control Center tramite l'agente relay.

Gli agenti Bitdefender Endpoint Security Tools Relay servono per i seguenti scopi:

- Scoprire tutti gli endpoint non protetti nella rete.
- Impiegare l'agente dell'endpoint nella rete locale.
- Aggiornare gli endpoint protetti nella rete.
- Assicurare la comunicazione tra Control Center e gli endpoint connessi.
- Agire come server proxy per gli endpoint protetti.
- Ottimizzare il traffico di rete durante gli aggiornamenti, gli impieghi, la scansione e le altre attività che richiedono risorse.

Server caching patch

Gli endpoint con ruolo Relay possono agire anche come Server di cache patch. Con questa regola attivata, i Relay servono per memorizzare le patch software scaricate dai siti web del fornitore e distribuirle agli endpoint di destinazione nella propria rete. Ogni volta che un endpoint connesso ha software mancante di patch, le scarica dal server e non dal sito web del fornitore, ottimizzando così il traffico generato e il carico sulla banda della rete.



Importante

Questo ruolo aggiuntivo è disponibile con un add-on di Gestione patch registrato.

Exchange Protection

Bitdefender Endpoint Security Tools con ruolo Exchange può essere installato su Microsoft Exchange Server allo scopo di proteggere gli utenti di Exchange da minacce derivanti da e-mail.

Bitdefender Endpoint Security Tools con ruolo di Exchange protegge sia la macchina server che la soluzione Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac è un agente di sicurezza progettato per proteggere workstation e portatili Macintosh basati su Intel. La tecnologia di scansione disponibile è la **Scansione locale**, con il contenuto di sicurezza memorizzato a livello locale.

Livelli di protezione

Con Endpoint Security for Mac sono disponibili i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- Controllo contenuti
- Controllo dispositivi
- Full Disk Encryption

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client estende le policy di sicurezza con facilità a qualsiasi numero di dispositivi iOS e Android, proteggendoli da un uso non autorizzato, riskware e perdita di dati personali. Le funzionalità di sicurezza includono blocco dello schermo, controllo dell'autenticazione, posizione del dispositivo, eliminazione remota dei contenuti, rilevazione di dispositivi con root o jailbreak e profili di sicurezza. Sui dispositivi Android, il livello di sicurezza viene migliorato con la scansione in tempo reale e la cifratura dei supporti rimovibili.

GravityZone Mobile Client viene distribuito in esclusiva tramite Apple App Store e Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools è un agente leggero per ambienti virtualizzati VMware che sono integrati con vShield Endpoint. L'agente di sicurezza viene installato su virtual

machine protette da Security Server per consentirti di sfruttare le funzionalità aggiuntive che fornisce:

- Ti consente di eseguire attività di scansione della memoria e dei processi sulla macchina.
- Informa l'utente sulle infezioni rilevate e le azioni intraprese su di esse.
- Aggiunge più opzioni per le eccezioni della scansione antimalware.

3.5. Architettura di Sandbox Analyzer

Bitdefender Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender.

Sandbox Analyzer è disponibile in due varianti:

- [Sandbox Analyzer Cloud](#), ospitato da Bitdefender.
- [Sandbox Analyzer On-Premises](#), disponibile come virtual appliance impiegabile in locale.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud include i seguenti componenti:

- **Portale Sandbox Analyzer** - Un server di comunicazione ospitato per la gestione delle richieste tra gli endpoint e il cluster di Bitdefender Sandbox.
- **Sandbox Analyzer Cluster** - L'infrastruttura sandbox ospitata, in cui si verifica l'analisi dei campioni. A questo livello, i file inviati vengono attivati su virtual machine con Windows 7.

GravityZone Control Center funziona come una console di gestione e reportistica, dove puoi configurare le policy di sicurezza, oltre a visualizzare notifiche e rapporti di analisi.

Bitdefender Endpoint Security Tools, l'agente di sicurezza installato sugli endpoint, che agisce come sensore di feeding per Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises viene offerto come una virtual appliance Linux Ubuntu, integrata in un'immagine di una virtual machine, facile da installare e configurare attraverso un'interfaccia a linea di comando (CLI). Sandbox Analyzer On-Premises è disponibile in formato OVA, impiegabile su VMWare ESXi.

Un'istanza di Sandbox Analyzer On-Premises include i seguenti componenti:

- **Sandbox Manager.** Questo componente è l'orchestratore sandbox. Sandbox Manager si connette all'hypervisor ESXi tramite API e utilizza le sue risorse hardware per creare ed eseguire l'ambiente di analisi dei malware.
- **Detonazione virtual machine.** Questo componente consiste di virtual machine sfruttate da Sandbox Analyzer per eseguire file e analizzarne il comportamento. Le virtual machine di detonazione può eseguire sistemi operativi Windows 7 e Windows 10 a 64 bit.

GravityZone Control Center funziona come una console di gestione e reportistica, dove puoi configurare le policy di sicurezza, oltre a visualizzare notifiche e rapporti di analisi.

Sandbox Analyzer On-Premises esegue i seguenti sensori di feeding:

- **Sensore Endpoint.** Bitdefender Endpoint Security Tools for Windows agisce come sensore di feeding installato sugli endpoint. L'agente di Bitdefender utilizza apprendimento automatico avanzato e algoritmi di rete neurali per determinare contenuti sospetti e inviarli a Sandbox Analyzer, tra cui elementi dalla quarantena centralizzata.
- **Sensore rete.** Network Security Virtual Appliance (NSVA) è una virtual appliance impiegabile nello stesso ambiente ESXi virtualizzato, come istanza di Sandbox Analyzer. Il sensore di rete estrae i contenuti dai sistemi di rete, inviandoli a Sandbox Analyzer.
- **Sensore ICAP.** Impiegato nei dispositivi network attached storage (NAS) usando il protocollo ICAP, Bitdefender Security Server supporta l'invio dei contenuti a Sandbox Analyzer.

Oltre a questi sensori, Sandbox Analyzer On-Premises supporta l'invio manuale e tramite API. Per maggiori dettagli, fai riferimento al capitolo **Utilizzare Sandbox Analyzer** della Guida per gli amministratori di GravityZone.

4. REQUISITI

Tutte le soluzioni di GravityZone sono installate e gestite tramite la Control Center.

4.1. GravityZone Virtual Appliance

4.1.1. Formati supportati e piattaforme di virtualizzazione

GravityZone viene fornito come una virtual appliance (VA). È disponibile nei seguenti formati, che supportano la maggior parte delle piattaforme di virtualizzazione più comuni:

- OVA (compatibile con VMware vSphere, View, VMware Player)
- XVA (compatibile con Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (compatibile con Microsoft Hyper-V)
- VMDK (compatibile con Nutanix Prism)
- OVF (compatibile con Red Hat Enterprise Virtualization)*
- OVF (compatibile con Oracle VM)*
- RAW (compatibile con Kernel-based Virtual Machine o KVM)*

* I pacchetti OVF e RAW vengono archiviati nel formato tar.bz2.

Per la compatibilità con la piattaforma Oracle VM VirtualBox, fai riferimento a [questo articolo della KB](#).

Il supporto per altri formati e piattaforme di virtualizzazione può essere fornito su richiesta.

4.1.2. Hardware

I requisiti hardware della virtual appliance di GravityZone variano con la dimensione della rete e con l'architettura di impiego scelta. Per reti fino a 3.000 endpoint, puoi scegliere di installare tutti i ruoli di GravityZone su una singola appliance, mentre per reti di maggiori dimensioni, devi pensare a distribuire i ruoli tra le diverse appliance. Le risorse richieste dalla appliance dipendono dai ruoli che vi hai installato e se usi oppure no il set di replica.



Nota

Il set di replica è una funzionalità MongoDB che mantiene la replica del database e garantisce elevata ridondanza e disponibilità dei dati memorizzati. Per maggiori dettagli, fai riferimento alla [documentazione di MongoDB](#) e «[Gestire la appliance di GravityZone](#)» (p. 105).

Bitdefender HVI richiede anche una notevole quantità di risorse. Se utilizzi questo servizio, controlla le tabelle con dati specifici. Per i requisiti completi del servizio, fai riferimento a «[HVI](#)» (p. 47).



Importante

Le misure sono un risultato dei test interni di Bitdefender sull'uso regolare e una configurazione base di GravityZone. I risultati possono variare in base alla configurazione della rete, il software installato, il numero di eventi generati, ecc. Per metriche di scalabilità personalizzate, contattare Bitdefender.

vCPU

La seguente tabella ti informa sul numero di vCPU per ciascun ruolo delle richieste della virtual appliance.

Ogni vCPU deve essere pari a un minimo di 2 GHz.

Componente	Numero di endpoint (fino a)							
	250	500	1000	3000	5000	10000	25000	50000
Funzionalità base di GravityZone								
Server di aggiornamento [*]					4	4	6	8
Console web ^{**}	8	12	14	16	6	10	12	12
Server di comunicazione					6	10	12	18
Database ^{***}					6	6	9	12
Totale	8	12	14	16	22	30	39	50
GravityZone con Bitdefender HVI								
Server di aggiornamento [*]	8	4	4	4	4	4	6	8
Console web ^{**}		6	8	8	10	10	12	12
Server di comunicazione		6	8	8	10	10	16	20
Database ^{***}		6	6	6	6	6	9	12



Componente	Numero di endpoint (fino a)							
	250	500	1000	3000	5000	10000	25000	50000
Totale	8	22	26	26	30	30	43	52

* Consigliato quando non vengono impiegati relay.

** Per ogni integrazione attiva, aggiungi una vCPU alla virtual appliance con il ruolo di console web.

*** In caso di installazione distribuita di ruoli, insieme al set di replica: per ogni istanza aggiuntiva del database, aggiungi il numero specificato all'ammontare totale.

RAM (GB)

Componente	Numero di endpoint (fino a)							
	250	500	1000	3000	5000	10000	25000	50000
Funzionalità base di GravityZone								
Server di aggiornamento					2	2	3	3
Console web *	16	16	18	20	8	8	12	16
Server di comunicazione					6	12	12	16
Database **					8	10	12	12
Totale	16	16	18	20	24	32	39	47
GravityZone con Bitdefender HVI								
Server di aggiornamento		2	2	2	2	2	3	3
Console web *	16	8	10	10	10	10	12	16
Server di comunicazione		8	10	10	12	12	16	20
Database **		8	8	8	8	12	12	12
Totale	16	26	30	30	32	36	43	51

* Per ogni integrazione attiva, aggiungi un GB di RAM sulla virtual appliance con il ruolo di console web.



****** In caso di installazione distribuita di ruoli, insieme al set di replica: per ogni istanza aggiuntiva del database, aggiungi il numero specificato all'ammontare totale.

Spazio libero su disco (GB)

Componente	Numero di endpoint (fino a)								
	250	250*	500	1000	3000	5000	10000	25000	50000
Funzionalità base di GravityZone									
Server di aggiornamento						80	80	80	80
Console web	120	160	160	200	200	80	80	80	80
Server di comunicazione						80	80	80	80
Database**						80	120	200	500
Totale	120	160	160	200	200	320	360	440	740
GravityZone con Bitdefender HVI									
Server di aggiornamento			80	80	80	80	80	80	80
Console web	120	160	80	80	80	80	80	80	80
Server di comunicazione			80	80	80	80	80	80	80
Database**			80	80	100	100	160	300	700
Totale	120	160	320	320	340	340	400	540	940



Importante

Si consiglia vivamente di usare unità di memoria a stato solido (SSD).

* Spazio aggiuntivo richiesto su SSD scegliendo l'installazione automatica, poiché installa anche il Security Server. Una volta terminata l'installazione, è possibile disinstallare il Security Server per liberare spazio su disco.

** In caso di installazione distribuita di ruoli, insieme al set di replica: per ogni istanza aggiuntiva del database, aggiungi il numero specificato all'ammontare totale.

4.1.3. Connessione Internet

La appliance di GravityZone richiede l'accesso a Internet.

4.2. Control Center

Per accedere alla console web Control Center, serve:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Risoluzione dello schermo consigliata: 1280x800 o superiore
- Il computer da cui ti connetti deve avere la connettività di rete alla Control Center.



Avvertimento

Control Center non funzionerà / apparirà correttamente in Internet Explorer 9+ con la funzione Visualizzazione compatibilità attivata, che equivale a utilizzare una versione del browser non supportata.

4.3. Protezione degli endpoint

Per proteggere la tua rete con Bitdefender, devi installare gli agenti di sicurezza di GravityZone negli endpoint della rete. Per una protezione ottimizzata, puoi installare anche Security Server. A tale scopo, ti serve un utente Control Center con privilegi di amministratore sui servizi che devi installare e gli endpoint di rete sotto la tua gestione.

I requisiti per l'agente di sicurezza sono diversi, in base alla presenza di eventuali ruoli server aggiuntivi, come Relay, Protezione Exchange o Patch Caching Server. Per maggiori informazioni sui ruoli dell'agente, fai riferimento a [«Agenti di sicurezza»](#) (p. 12).

4.3.1. Hardware

Agente di sicurezza senza ruoli

Usa CPU

Sistemi bersaglio	Tipo CPU	Sistemi operativi supportati (OS)
Workstation	Processori compatibili Intel® Pentium, 2 GHz o superiori	Sistemi operativi desktop di Microsoft Windows
	Intel® Core 2 Duo, 2 GHz o superiore	macOS
Dispositivi smart	Processori compatibili Intel® Pentium, 800 MHz o superiori	Sistemi operativi Microsoft Windows embedded
Server	Requisiti minimi: processori compatibili Intel® Pentium a 2,4 GHz	Sistemi operativi Microsoft Windows server e Linux
	Requisiti consigliati: processore Intel® Xeon multi-core, 1.86 GHz o superiore	



Avvertimento

Al momento i processori ARM non sono supportati.

Memoria RAM libera

All'installazione (MB)

SO	SINGOLO MOTORE					
	Scansione locale		Scansione ibrida		Scansione centralizzata	
	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	N/D	N/D	N/D	N/D

Per uso giornaliero (MB)*



SO	Antivirus (singolo motore)			Moduli di protezione			
	Locale	Ibrida	Centralizzata	Scans. comportamentale	Firewall	Controllo contenuti	Utente esperto
Windows	75	55	30	+13	+17	+41	+29
Linux	200	180	90	-	-	-	-
macOS	650	-	-	+100	-	+50	-

* I valori si riferiscono a un utilizzo del client endpoint giornaliero, senza considerare eventuali attività aggiuntive, come scansioni a richiesta o aggiornamenti del prodotto.

Spazio libero su disco rigido

All'installazione (MB)

SO	SINGOLO MOTORE						DOPPIO MOTORE			
	Scansione locale		Scansione ibrida		Scansione centralizzata		Centralizzata + Scansione locale		Centralizzata + Scansione ibrida	
	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D

Per uso giornaliero (MB)*

SO	Antivirus (singolo motore)			Moduli di protezione			
	Locale	Ibrida	Centralizzata	Scans. comportamentale	Firewall	Controllo contenuti	Utente esperto
Windows	410	190	140	+12	+5	+60	+80
Linux	500	200	110	-	-	-	-
macOS	1700	-	-	+20	-	+0	-

* I valori si riferiscono a un utilizzo del client endpoint giornaliero, senza considerare eventuali attività aggiuntive, come scansioni a richiesta o aggiornamenti del prodotto.

Agente di sicurezza con ruolo di relay

Il ruolo di relay richiede risorse hardware aggiuntive alla configurazione dell'agente di sicurezza base. Questi requisiti sono per supportare il server di aggiornamento e i pacchetti di installazione ospitati dall'endpoint:

Numero di endpoint connessi	Processore per supportare il server di aggiornamento	RAM	Spazio libero su disco per il server di aggiornamento
1-300	Minimo processore Intel® Core™ i3 o equivalente, 2 vCPU per core	1,0 GB	10 GB
300-1000	Minimo processore Intel® Core™ i5 o equivalente, 4 vCPU per core	1,0 GB	10 GB



Avvertimento

- Al momento i processori ARM non sono supportati.
- Gli agenti relay richiedono dischi SSD per supportare l'elevato ammontare di operazioni di lettura/scrittura.



Importante

- Se vuoi salvare i pacchetti di installazione e gli aggiornamenti per un'altra partizione rispetto a quella in cui è stato installato l'agente, assicurati che entrambe le partizioni abbiano sufficiente spazio libero sul disco (10 GB), altrimenti l'agente annullerà l'installazione. Ciò è richiesto solo all'installazione.
- Sugli endpoint Windows, è necessario attivare i collegamenti simbolici da locale a locale.

Agente di sicurezza con ruolo di protezione Exchange

La quarantena per Exchange Server richiede spazio su disco aggiuntivo nella partizione in cui l'agente di sicurezza viene installato.

Lo spazio della quarantena dipende dal numero di oggetti memorizzati e dalla loro dimensione.

Di norma, l'agente viene installato sulla partizione del sistema.

Agente di sicurezza con ruolo Patch Caching Server

L'agente con ruolo Patch Caching Server deve soddisfare i seguenti requisiti cumulativi:

- Tutti i requisiti hardware dell'agente di sicurezza semplice (senza ruoli)
- Tutti i requisiti hardware del ruolo relay
- In aggiunta 100 GB di spazio libero su disco per memorizzare le patch scaricate



Importante

Se vuoi salvare le patch per un'altra partizione rispetto a quella in cui è stato installato l'agente, assicurati che entrambe le partizioni abbiano sufficiente spazio libero sul disco (100 GB), altrimenti l'agente annullerà l'installazione. Ciò è richiesto solo all'installazione.

Requisiti per gli ambienti VMware vShield

Questi sono i requisiti di Bitdefender Tools e l'impronta per i sistemi integrati negli ambienti VMware con vShield Endpoint.

Piattaforma	RAM	Spazio su disco
Windows	6-16* MB (circa 10 MB per la GUI)	24 MB
Linux	9-10 MB	10-11 MB

* 5 MB in caso di attivazione dell'opzione Modalità silenziosa e 10 MB quando viene disattivata. Quando la Modalità silenziosa è attivata, l'interfaccia grafica di Bitdefender Tools (GUI) non viene caricata automaticamente all'avvio del sistema, liberando le risorse associate.

4.3.2. Sistemi operativi supportati

Windows Desktop

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)

- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1⁽¹⁾⁽²⁾
- Windows 8⁽³⁾
- Windows 7



Avvertimento

(1) Piattaforma VMware vShield (versione agentless) - Il supporto per Windows 8.1 (32/64 bit) è disponibile a partire da VMware vSphere 5.5 - ESXi build 1892794 e superiore.

(2) In VMware NSX, la versione del sistema operativo è supportata a partire da vSphere 5.5 Patch 2.

(3) In VMware NSX, la versione del sistema operativo è supportata a partire da vSphere 5.5.



Avvertimento

Bitdefender non supporta build del Programma Windows Insider.

Windows Tablet e Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Server

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2⁽¹⁾⁽²⁾
- Windows Server 2012⁽³⁾⁽⁴⁾
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2⁽⁴⁾



Avvertimento

(3) Piattaforma VMware vShield (versione agentless) - Il supporto per Windows Server 2012 R2 (64 bit) è disponibile a partire da VMware vSphere 5.5 - ESXi build 1892794 e superiore.

(2) In VMware NSX, la versione del sistema operativo è supportata a partire da vSphere 5.5 Patch 2.

(3) In VMware NSX, la versione del sistema operativo è supportata a partire da vSphere 5.5.

(4) VMware NSX non supporta le versioni a 32 bit di Windows 2012 e Windows Server 2008 R2.

Linux



Importante

Gli endpoint Linux usano set di licenze provenienti dai pool di licenze per sistemi operativi dei server.

- Ubuntu 14.04 LTS o superiore
- Red Hat Enterprise Linux / CentOS 6.0 o superiore⁽²⁾
- SUSE Linux Enterprise Server 11 SP4 o superiore
- OpenSUSE Leap 42.x
- Fedora 25 o superiore⁽¹⁾
- Debian 8.0 o superiore
- Oracle Linux 6.3 o più recente
- Amazon Linux AMI 2016.09 o superiore
- Amazon Linux 2



Avvertimento

(1) Su Fedora 28 e versioni successive, Bitdefender Endpoint Security Tools richiede l'installazione manuale del pacchetto `libnsl`, eseguendo il seguente comando:

```
sudo dnf install libnsl -y
```

(2) Per le installazioni minime di CentOS, Bitdefender Endpoint Security Tools richiede l'installazione manuale del pacchetto `libnsl`, eseguendo il seguente comando:

```
sudo yum install libnsl
```

Prerequisiti Active Directory

Integrando gli endpoint Linux con un dominio Active Directory tramite il System Security Services Daemon (SSSD), assicurati che gli strumenti **ldbsearch**, **krb5-user** e **krb5-config** siano installati e che kerberos sia configurato correttamente.

```
/etc/krb5.conf

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    default_realm = DOMAIN.NAME
    dns_lookup_realm = true
    dns_lookup_kdc = true
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    fcc-mit-ticketflags = true
    default_keytab_name = FILE:/etc/krb5.keytab

[realms]
    DOMAIN.NAME = {
        kdc = dc1.domain.name
```

```
        kdc = dc2.domain.name
        admin_server = dc.domain.com
        default_domain = domain.com
    }

[domain_realm]
domain.name = DOMAIN.NAME
.domain.name = DOMAIN.NAME

[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```



Nota

Tutti i valori sono sensibili alle lettere maiuscole/minuscole.

Supporto scansione a richiesta

La scansione a richiesta è disponibile per tutti i sistemi operativi guest supportati. Nei sistemi Linux, il supporto per la scansione a richiesta viene fornito nelle seguenti situazioni:

Versioni kernel	Distribuzioni Linux	Requisiti all'accesso
2.6.38 o superiore*	Red Hat Enterprise Linux / CentOS 6.0 o superiore Ubuntu 14.04 o superiore SUSE Linux Enterprise Server 11 SP4 o superiore OpenSUSE Leap 42.x Fedora 25 o superiore Debian 9.0 o superiore	Fanotify (opzione kernel) deve essere attivata.




Versioni kernel	Distribuzioni Linux	Requisiti all'accesso
	Oracle Linux 6.3 o più recente Amazon Linux AMI 2016.09 o superiore	
2.6.38 o superiore	Debian 8	Fanotify deve essere attivata e impostata in modalità enforcing. Inoltre, il pacchetto del kernel deve essere ricostruito. Per maggiori dettagli, fai riferimento a questo articolo della KB .
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender fornisce supporto via DazukoFS con moduli kernel predefiniti.
Tutti gli altri kernel	Tutti gli altri sistemi supportati	Il modulo DazukoFS deve essere compilato manualmente. Per maggiori dettagli, fai riferimento a « Compila manualmente il modulo DazukoFS » (p. 152).

* Con determinate limitazioni descritte in basso.

Limitazioni scansione all'accesso

Versioni kernel	Distribuzioni Linux	Dettagli
2.6.38 o superiore	Tutti i sistemi supportati	La scansione a richiesta monitora le condivisioni di rete installate solo in queste condizioni: <ul style="list-style-type: none"> ● Fanotify è attivato sia su sistemi locali che remoti. ● La condivisione è basata sui file system CIFS e NFS.

Versioni kernel	Distribuzioni Linux	Dettagli
		 Nota La scansione a richiesta non esamina le condivisioni di rete installate utilizzando SSH o FTP.
Tutti i kernel	Tutti i sistemi supportati	La scansione all'accesso non è supportata su sistemi con DazukoFS per condivisioni di rete montate su percorsi già protetti dal modulo All'accesso.

macOS


- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Controllo contenuti non è supportato in macOS Big Sur (11.0).

4.3.3. File system supportati

Bitdefender si installa e protegge i seguenti file system:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

 **Nota**
 Il supporto per la scansione a richiesta non è fornito per NFS e CIFS/SMB.

4.3.4. Browser supportati

La sicurezza per i browser degli endpoint risulta funzionante con i seguenti browser:

- Internet Explorer 8+
- Mozilla Firefox 30+

- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.3.5. Piattaforme di virtualizzazione supportate

Security for Virtualized Environments ti fornisce un supporto fuori dagli schemi per le seguenti piattaforme di virtualizzazione:

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0



Nota

La funzionalità Workload Management in vSphere 7.0 non è supportata.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (incluso Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 o Windows Server 2008 R2, 2012, 2012 R2 (incluso Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (incluso KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

 **Nota**

Il supporto per altre piattaforme di virtualizzazione può essere fornito su richiesta.

Integrazione con requisiti VMware NSX-V

- ESXi 5.5 o superiore per ciascun server
- vCenter Server 5.5 o successivo
- NSX Manager 6.2.4 o successivo
- VMware Tools 9.1.0 o superiore, con agente di Guest Introspection.
 - Per Virtual Machine Windows fare riferimento al seguente [articolo di VMware Docs](#).
 - Per Virtual Machine Linux fare riferimento al seguente [articolo di VMware Docs](#).

 **Nota**

VMware consiglia di utilizzare le seguenti versioni di VMware Tools:

- 10.0.8 o superiore, per risolvere il problema di lentezza delle VM dopo l'upgrade a VMware Tools in NSX / vCloud Networking and Security ([Knowledge Base di VMware - Articolo 2144236](#)).
- 10.0.9 e superiore per il supporto di Windows 10.

 **Importante**

Si consiglia di mantenere tutti i prodotti VMware aggiornati con la patch più recente.

Integrazione con requisiti VMware NSX-T Data Center

- VMware NSX-T Manager 2.4, 2.5 o 3.0
- ESXi compatibile con la versione di NSX-T Manager
- vCenter Server & vSphere compatibili con la versione di NSX-T Manager
- VMware Tools con agente leggero di Guest Introspection, compatibile con la versione di NSX-T Manager

Per maggiori dettagli sulla compatibilità, fai riferimento alle seguenti pagine web di VMware:

- [Guida alla compatibilità di VMware](#) – GravityZone contro NSX-T Manager

- [Matrici di interoperabilità dei prodotti VMware - NSX-T Data Center](#) contro VMware vCenter e VMware Tools

Requisiti dell'integrazione con Nutanix Prism Element

- Credenziali di un utente Nutanix Prism Element con privilegi di amministratore (Cluster Admin o User Admin)
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

Piattaforme cloud supportate

Oltre agli ambienti di virtualizzazione in locale, GravityZone può anche integrarsi con le seguenti piattaforme cloud:

- **Amazon EC2**

Come cliente di Amazon EC2, puoi integrare l'inventario delle istanze EC2 raggruppate per regione e zone di disponibilità con l'inventario di rete di GravityZone.

- **Microsoft Azure**

Come cliente di Microsoft Azure, puoi integrare l'inventario delle virtual machine di Microsoft Azure raggruppate per regione e zone di disponibilità con l'inventario di rete di GravityZone.

Compatibilità con le tecnologie di virtualizzazione di desktop e applicazioni

GravityZone è compatibile con le seguenti tecnologie di virtualizzazione, a partire dalla versione 6.6.16.226 di Bitdefender Endpoint Security Tools:

- **VMware:**

VMware V-App (stessa versione con vCenter Server)

VMware ThinApp 5.2.6

VMware AppVolumes 2.180

**Importante**

Si consiglia di non installare in stack di applicazioni o volumi scrivibili.

● Microsoft:

Microsoft App-V 5.0, 5.1

Microsoft FSLogix 2.9.7237

● Citrix:

Citrix App Layering 19.10

Citrix Appdisks 7.12

**Importante**

Assegna policy basate sulle regole per l'utente in modo che Controllo dispositivi non impedisca la creazione di livelli di sistema operativo e piattaforma.

Potrebbe essere necessario configurare le regole del firewall di GravityZone per consentire il traffico di rete per ognuna di queste applicazioni. Per maggiori informazioni, fai riferimento alla [Documentazione del prodotto Citrix App Layering](#).

Strumenti gestione virtualizzazione supportati

Attualmente Control Center si integra con i seguenti strumenti di gestione della virtualizzazione:

- Server VMware vCenter
- Citrix XenServer
- Nutanix Prism Element

Per configurare l'integrazione, devi fornire il nome utente e la password di un amministratore.

4.3.6. Security Server

Il Security Server è una macchina virtuale preconfigurata che funziona su un Server Ubuntu con le seguenti versioni:

- 16.04 (VMware NSX e Multi-Platform)
- 12.04 LTS (VMware vShield)

Memoria e CPU

L'assegnazione delle risorse di memoria e CPU per il Security Server dipende dal numero e dal tipo di VM in esecuzione sull'host. La seguente tabella elenca le risorse consigliate da assegnare:

Numero di VM protette	RAM	CPU
1-50 VM	2 GB	2 CPU
51-100 VM	2 GB	4 CPU
101-200 VM	4 GB	6 CPU

Security Server for NSX viene fornito con una configurazione hardware predefinita (Processore e RAM), che è possibile impostare nel VMware vSphere Web Client disattivando la macchina, modificando le sue impostazioni e riattivandola. Per informazioni dettagliate, fai riferimento a [«Installare Security Server for VMware NSX»](#) (p. 123).

Spazio su disco rigido

Ambiente	Provisioning dello spazio su disco rigido
VMware NSX-V / NSX-T	40 GB
VMware con vShield Endpoint	40 GB
Altro	16 GB

Distribuzione di Security Server su host

Ambiente	Security Server vs. host
VMware NSX-V / NSX-T	Il Security Server viene installato automaticamente su ciascun host ESXi nel cluster da proteggere, al momento dell'impiego del servizio di Bitdefender.
VMware con vShield Endpoint	Il Security Server deve essere installato su ciascun host ESXi da proteggere.
Altro	Anche se non è obbligatorio, Bitdefender consiglia di installare Security Server su ogni host fisico per ottenere prestazioni migliori.

Latenza di rete

La latenza delle comunicazioni tra Security Server e gli endpoint protetti deve essere inferiore a 50 ms.

Carico di Protezione archiviazione

L'impatto della Protezione archiviazione sul Security Server durante la scansione di 20 GB è il seguente:

Stato Protezione archiviazione	Risorse del Security Server	Caricamento Security Server	Tempo di trasferimento (mm:ss)
Disattivato (riferimento)	N/A	N/A	10:10
Attivato	4 vCPU 4 GB RAM	Normale	10:30
Attivato	2 vCPU 2 GB RAM	Pesante	11:23

Nota

Questi risultati sono stati ottenuti con un campione di diversi tipi di file (.exe, .txt, .doc, .eml, .pdf, .zip etc.), che spaziano da 10 KB a 200 MB. La durata del trasferimento corrisponde a 20 GB di dati contenuti in 46.500 file.

4.3.7. Uso del traffico

● **Traffico dell'aggiornamento dei prodotti tra il client endpoint e il server di aggiornamento**

Ogni aggiornamento periodico del prodotto Bitdefender Endpoint Security Tools genera il seguente traffico di download in ciascun client endpoint:

- Su SO Windows: ~20 MB
- Su SO Linux: ~26 MB
- Su macOS: ~25 MB

● **Traffico degli aggiornamenti del contenuto di sicurezza scaricati tra il client endpoint e il server di aggiornamento (MB / giorno)**

Tipo di server di aggiornamento	Tipo di motore di scansione		
	Locale	Ibrida	Centralizzata
Relay	65	58	55
Server di aggiornamento pubblico di Bitdefender	3	3.5	3

● **Traffico della scansione centralizzata tra il client endpoint e Security Server**

Oggetti esaminati	Tipo di traffico		Download (MB)	Upload (MB)
File*	Prima scansione		27	841
	Scansione nella cache		13	382
Siti web**	Prima scansione	Traffico web	621	N/A
		Security Server	54	1050
	Scansione nella cache	Traffico web	654	N/A
		Security Server	0.2	0.5

* I dati forniti sono stati misurati per file di 3,49 GB (6.658 file) di cui 1,16 GB sono file Portable Executable (PE).

** I dati forniti sono stati misurati per i migliori 500 siti web.

● **Traffico della scansione ibrida tra il client endpoint e i servizi cloud di Bitdefender**

Oggetti esaminati	Tipo di traffico	Download (MB)	Upload (MB)
File*	Prima scansione	1.7	0.6
	Scansione nella cache	0.6	0.3
Traffico web**	Traffico web	650	N/A
	Servizi Cloud di Bitdefender	2.6	2.7

* I dati forniti sono stati misurati per file di 3,49 GB (6.658 file) di cui 1,16 GB sono file Portable Executable (PE).

** I dati forniti sono stati misurati per i migliori 500 siti web.

- **Traffico tra i client Bitdefender Endpoint Security Tools Relay e il server di aggiornamento per il download del contenuto di sicurezza**

I client con ruolo Bitdefender Endpoint Security Tools Relay scaricano circa 16 MB / giorno* dal server di aggiornamento.

* Disponibile con client Bitdefender Endpoint Security Tools a partire dalla versione 6.2.3.569.

- **Traffico tra i client endpoint e la console web Control Center**

Tra i client endpoint e la console web Control Center viene generato un traffico medio di 618 KB / giorno.

4.4. Exchange Protection

Security for Exchange viene fornito attraverso Bitdefender Endpoint Security Tools, che è in grado di proteggere sia il file system che il mail server di Microsoft Exchange.

4.4.1. xxx

Security for Exchange supporta i seguenti ruoli e le seguenti versioni di Microsoft Exchange:

- Exchange Server 2019 con ruolo Edge Transport o mailbox
- Exchange Server 2016 con ruolo Edge Transport o mailbox
- Exchange Server 2013 con Edge Transport o ruolo Mailbox
- Exchange Server 2010 con ruolo Edge Transport, Hub Transport o mailbox
- Exchange Server 2007 con ruolo Edge Transport, Hub Transport o mailbox

Security for Exchange è compatibile con Microsoft Exchange Database Availability Groups (DAGs).

4.4.2. Requisiti di sistema

Security for Exchange è compatibile con ogni server fisico o virtuale a 64 bit (Intel o AMD) che esegue un ruolo o una versione supportata di Microsoft Exchange Server. Per maggiori dettagli sui requisiti di sistema di Bitdefender Endpoint Security Tools, fai riferimento a «[Agente di sicurezza senza ruoli](#)» (p. 24).

Disponibilità risorse server consigliato:

- Memoria RAM libera: 1 GB
- Spazio libero su disco rigido: 1 GB

4.4.3. Altri requisiti software

- Per Microsoft Exchange Server 2013 con Service Pack 1: [KB2938053](#) di Microsoft.
- Per Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 o superiore

4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises ha determinati requisiti:

- [ESXi Hypervisor](#) (la piattaforma di virtualizzazione che eseguirà l'ambiente).
- [Sandbox Analyzer Virtual Appliance](#) (la appliance di gestione che controllerà le virtual machine di detonazione).
- [Network Security Virtual Appliance](#) (una VM che include un sensore di rete in grado di estrarre il carico dal traffico di rete).
- Connettività a un GravityZone Control Center esistente utilizzato per la gestione ad alto livello dell'ambiente sandbox.
- Una connessione a Internet per il download della Virtual Appliance di Sandbox Analyzer, con una larghezza di banda minima di 5 MBps.



Importante

Assicuratevi che non ci siano altri processi o applicazioni che potrebbero bloccare la connessione a Internet durante il download e l'installazione di Sandbox Analyzer.

4.5.1. ESXi Hypervisor

Sandbox Analyzer Virtual Appliance è disponibile in formato OVA, impiegabile su un singolo host fisico che esegue l'hypervisor VMware ESXi (versione 6.5 o 6.7).

Requisiti hardware per l'host fisico

- CPU: il numero totale di core delle CPU (considerando l'hyperthreading) può essere extrapolato utilizzando il calcolo presentato nella sezione «[Requisiti host fisici e scaling hardware](#)» (p. 45).

- RAM: la quantità totale di RAM necessaria per l'host fisico può essere estrapolata utilizzando il calcolo presentato nella sezione «[Requisiti host fisici e scaling hardware](#)» (p. 45).
- Spazio su disco: almeno 1 TB di archiviazione SSD (adeguato per l'ambiente di detonazione di 8-VM, scalabile con almeno 50 GB per ogni VM di detonazione aggiuntiva).
- Rete: una scheda di interfaccia di rete fisica dedicata (NIC).
Questa NIC può essere divisa in due NIC virtuali, con la seguente mappatura:
 - Una NIC per l'interfaccia di gestione.
 - Una NIC per la rete di detonazione.

**Nota**

Si consiglia di utilizzare NIC fisiche dedicate con le stesse mapping come le vNIC sopra indicate, se la configurazione hardware lo consente.

Requisiti Software

Versioni supportate di ESXi server: 6.5 o superiore, VMFS versione 5.

Configurazione aggiuntiva su host ESXi:

- SSH attivato all'avvio.
- Servizio NTP configurato e attivo.
- L'opzione **avvia/ferma con host** attivata.

**Nota**

Sandbox Analyzer è compatibile con la versione di prova di VMWare ESXi. Tuttavia, per impieghi produttivi, si consiglia di eseguire una versione con licenza di ESXi.

4.5.2. Virtual Appliance di Sandbox Analyzer

La Virtual appliance di Sandbox Analyzer fornisce una flessibilità virtualmente illimitata, purché siano disponibili le risorse hardware sottostanti.

Della quantità totale di risorse ESXi disponibili, Sandbox Analyzer condivide CPU e RAM tra Sandbox Manager e le virtual machine di detonazione.

Requisiti di sistema minimi di Sandbox Manager

- 6 vCPU
- 20 GB di RAM
- 600 GB di spazio su disco

Sandbox Manager ha tre NIC virtuali interne assegnate come segue:

- Una NIC per la comunicazione con la console di gestione (GravityZone Control Center).
- Una NIC per la connettività a Internet.
- Una NIC per la comunicazione con le VM di detonazione.

Nota

Per consentire la comunicazione, sia la vNIC di gestione ESXi che la vNIC di gestione di Sandbox Manager devono essere nella stessa rete.

Virtual machine di detonazione

Requisiti di sistema

- 4 vCPU (sovradimensionate nel rapporto 4:1, fai riferimento a [«Requisiti host fisici e scaling hardware»](#) (p. 45))
- 3 GB di RAM
- 50 GB di spazio su disco

Sandbox Analyzer On-Premises fornisce supporto per immagini di virtual machine personalizzate. Ciò consente la detonazione del campione in un ambiente runtime che imita un ambiente produttivo realistico.

La creazione di un'immagine di una virtual machine richiede le seguenti condizioni:

- L'immagine della virtual machine è in formato VMDK, versione 5.0.
- I sistemi operativi supportati per creare virtual machine di detonazione:
 - Windows 7 64 bit (qualsiasi livello di patch)
 - Windows 10 64 bit (qualsiasi livello di patch)

! Importante

- Il sistema operativo deve essere installato sulla seconda partizione nella tabella delle partizioni e montato sull'unità C: (configurazione di installazione di Windows predefinita)
- L'account "Amministratore" locale deve essere attivato e avere una stringa della password vuota (disattivazione password).
- Prima di esportare l'immagine della VM, è necessario disporre della licenza corretta del sistema operativo e di tutto il software installato nell'immagine della virtual machine.

Immagine software Virtual machine

Sandbox Analyzer supporta la detonazione di una vasta gamma di formati e tipi di file. Per maggiori dettagli, fai riferimento a [«Oggetti Sandbox Analyzer»](#) (p. 229).

Per rapporti conclusivi, assicurati di aver installato nell'immagine personalizzata il software in grado di aprire un particolare tipo di file che desideri detonare. Per maggiori dettagli, fai riferimento a [«Applicazioni consigliate per le VM di detonazione»](#) (p. 230).

4.5.3. Network Security Virtual Appliance

Network Security Virtual Appliance gestisce il sensore di rete, in grado di estrarre i carichi dai flussi di rete e inviarli a Sandbox Analyzer. I requisiti minimi hardware sono:

- 4 vCPU
- 4 GB di RAM
- 1 TB di spazio su disco
- 2 vNIC

4.5.4. Requisiti host fisici e scaling hardware

L'algoritmo di scaling dell'ambiente Sandbox Analyzer considera la seguente formula, dove "K" sta per il numero di slot di detonazione (o le VM di detonazione):

- $\text{Sandbox Analyzer VA vCPU} = 6 \text{ vCPU} + K \times 1 \text{ vCPU}$
- $\text{Sandbox Analyzer VA RAM} = 20 \text{ GB RAM} + K \times 2 \text{ GB}$

Analogamente, l'algoritmo di scaling per l'host è il seguente:

- ESXi Host vCPU = 6 vCPU + K x 2 vCPU
- ESXi Host RAM = 20 GB RAM + K x 5 GB

Le differenze principali tra la VA di Sandbox Analyzer e le risorse di ESXi sono date dalle risorse assegnate a ciascuna VM di detonazione.

Inoltre, un tipico ambiente di detonazione (8VM) avrebbe i seguenti requisiti:

- Sandbox Analyzer VA vCPU = 6 vCPU + 8 x 1vCPU = 14 vCPU
- Sandbox Analyzer VA RAM = 20 GB RAM + 8 x 2 GB = 36 GB RAM
- ESXi Host vCPU = 6 vCPU + 8 x 2 vCPU = 22 vCPU

**Nota**

Ogni VM di detonazione richiede 1 vCPU allocata per la VA di Sandbox Analyzer e 1 vCPU per la VM di detonazione. La VM di detonazione sarà fornita con 4 vCPU, ma verrà eseguito un overprovisioning in un rapporto di 4:1, risultando necessaria solo 1 vCPU per l'host ESXi.

- ESXi Host RAM = 20 GB RAM + 8 x 5 GB = 60 GB RAM

**Nota**

La RAM viene usata in un rapporto 1:1 tra la VM di Sandbox Analyzer, le VM di detonazione e l'host ESXi. Inoltre, ogni VM di detonazione richiederà 5 GB di RAM dall'host ESXi, di cui 2 GB saranno assegnati alla VA di Sandbox Analyzer e 3 GB alla VM di detonazione stessa.

L'host fisico risultante richiede, nel suddetto scenario, almeno 22 core di CPU (incluso l'hyperthreading) e almeno 60 GB di RAM, con un ulteriore 10-20% della RAM riservata per l'hypervisor stesso.

Generalmente, la detonazione di un campione richiede nove minuti per l'esecuzione e la generazione del rapporto di detonazione, e utilizza tutte le risorse fornite. Si consiglia di progettare il proprio ambiente sandbox partendo dalla capacità di detonazione (file/ora) e poi trasformare tale parametro nelle risorse necessarie a livello di host e VM.

4.5.5. Requisiti di comunicazione di Sandbox Analyzer

Le componenti di Sandbox Analyzer On-Premises utilizzano determinate porte di comunicazione vincolate a particolari interfacce di rete, così da comunicare tra loro e/o con server pubblici di Bitdefender

L'ambiente di sandbox richiede tre interfacce di rete:

- **eth0 – Interfaccia di gestione di rete.** Si connette a GravityZone e all'host ESXi. Si consiglia di connettere eth0 alla stessa rete dell'interfaccia di gestione ESXi. Si consiglia anche di mapparla a un adattatore fisico dedicato.

La seguente tabella descrive i requisiti di comunicazione della rete per eth0:

Direzione	Porte di comunicazione (su TCP)	Origine/destinazione
In uscita	8443	Server di comunicazione di GravityZone
	443	GravityZone Virtual Appliance
	80	GravityZone Virtual Appliance
	22	Host ESXi
	443	API host ESXi
In entrata	8443	Qualsiasi

- **eth1 – Rete di detonazione.** Non richiede alcuna configurazione. Il processo di installazione crea le necessarie risorse virtuali.
- **eth2 – Rete di accesso a Internet.** Si consiglia di avere una connessione a Internet non limitata e filtrata.

Si consiglia di assegnare la rete di gestione e la rete di accesso a Internet a sottoreti diverse.

La GravityZone Virtual Appliance richiede accesso alla Sandbox Analyzer Virtual Appliance sulla porta 443 (su TCP) per visualizzare e scaricare i rapporti di Sandbox Analyzer.

La GravityZone Virtual Appliance richiede la connettività con la Sandbox Analyzer Virtual Appliance sulla porta 443 (su TCP) per richiedere lo stato dei campioni detonati.

4.6. HVI

HVI funziona con l'aiuto di due componenti: Security Server e Pacchetto supplementare di HVI. Questi prodotti devono essere installati sugli host nel tuo ambiente virtualizzato, dove hai le virtual machine che intendi proteggere.

Prima di impiegare HVI sugli host, assicurati che i seguenti requisiti siano soddisfatti:

Piattaforme di virtualizzazione supportate

- Citrix XenServer 7.1 Enterprise Edition o superiore, con le ultime patch



Importante

Per ogni XenServer a partire dalla versione 7.1 che ha raggiunto EOL Bitdefender fornisce supporto HVI per due mesi aggiuntivi. Dopo tale periodo, ti consigliamo di passare a una versione di XenServer supportata da Citrix. Per maggiori informazioni, fare riferimento alle documentazioni [Citrix Legacy Products Matrix](#) e [Citrix Product Matrix](#).

- Citrix Hypervisor 8.0 Enterprise Edition o superiore, con le patch più recenti



Avvertimento

Per Citrix Hypervisor 8.0, devi installare la patch [XS80E004](#).

Virtual machine guest supportate

Le virtual machine che intendi proteggere con HVI devono soddisfare i seguenti requisiti:

1. Le macchine sono in modalità di virtualizzazione HVM, il che significa che sono interamente virtualizzate.
2. Le macchine devono avere un sistema operativo supportato:
 - **Sistemi operativi Windows Desktop (32 e 64 bit)**
 - Windows 10 May 2020 Update (20H1)
 - Windows 10 November 2019 Update (19H2)
 - Windows 10 May 2019 Update (19H1)
 - Windows 10 October 2018 Update (Redstone 5)
 - Windows 10 April 2018 Update (Redstone 4)
 - Windows 10 Fall Creators Update (Redstone 3)
 - Windows 10 Creators Update (Redstone 2)



- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

- **Sistemi operativi Windows Server (64 bit)**

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012/ Windows Server 2012 R2
- Windows Server 2008 R2

- **Sistemi operativi Linux (64 bit)**

Distribuzione	Versione	Versione Kernel
Debian	10	4.19
Debian	9	4.9
Debian	8	3.16
Ubuntu	20.04 LTS	5.4
Ubuntu	18.04 LTS	4.15
Ubuntu	16.04 LTS	4.4
Ubuntu	14.04 LTS	3.13.139 e successivo
CentOS	8.2	4.18
CentOS	8	4.18
CentOS	7	3.10
Red Hat Enterprise Linux	8.2	4.18
Red Hat Enterprise Linux	8	4.18
Red Hat Enterprise Linux	7	3.10
Red Hat Enterprise Linux	6.8 / 6.9 / 6.10	2.36.32



Distribuzione	Versione	Versione Kernel
SUSE Linux Enterprise Server	15 SP1	4.12
SUSE Linux Enterprise Server	12 SP4	4.12
SUSE Linux Enterprise Server	12 SP3	4.4
SUSE Linux Enterprise Server	12 SP2	4.4
SUSE Linux Enterprise Server	12 SP1	3.12
Oracle Linux	Precedente alla versione 7.5	4.1 (UEK/RHCK)
Oracle Linux	7.5 e successivo	4.14 (UEK/RHCK)

Requisiti hardware della VA di GravityZone

- vCPU richiesta**

La seguente tabella ti informa sul numero di vCPU per ciascun ruolo delle richieste della virtual appliance.

Ogni vCPU deve essere pari a un minimo di 2 GHz.

Componente	Numero di endpoint (fino a)							
	250	500	1000	3000	5000	10000	25000	50000
Server di aggiornamento *	8	4	4	4	4	4	6	8
Console web **		6	8	8	10	10	12	12
Server di comunicazione		6	8	8	10	10	16	20
Database ***		6	6	6	6	6	9	12
Totale	8	22	26	26	30	30	43	52

* Consigliato quando non vengono impiegati relay.

** Per ogni integrazione attiva, aggiungi una vCPU alla virtual appliance con il ruolo di console web.

*** In caso di installazione distribuita di ruoli, insieme al set di replica: per ogni istanza aggiuntiva del database, aggiungi il numero specificato all'ammontare totale.

- RAM richiesta (GB)**

Componente	Numero di endpoint (fino a)							
	250	500	1000	3000	5000	10000	25000	50000
Server di aggiornamento		2	2	2	2	2	3	3
Console web *	16	8	10	10	10	10	12	16
Server di comunicazione		8	10	10	12	12	16	20
Database **		8	8	8	8	12	12	12
Totale	16	26	30	30	32	36	43	51

* Per ogni integrazione attiva, aggiungi un GB di RAM sulla virtual appliance con il ruolo di console web.

** In caso di installazione distribuita di ruoli, insieme al set di replica: per ogni istanza aggiuntiva del database, aggiungi il numero specificato all'ammontare totale.

● **Spazio su disco richiesto (GB)**

Server di aggiornamento			80	80	80	80	80	80	80
Console web	120	160	80	80	80	80	80	80	80
Server di comunicazione			80	80	80	80	80	80	80
Database **			80	80	100	100	160	300	700
Totale	120	160	320	320	340	340	400	540	940

* Spazio aggiuntivo richiesto su SSD scegliendo l'installazione automatica, poiché installa anche il Security Server. Una volta terminata l'installazione, è possibile disinstallare il Security Server per liberare spazio su disco.

** In caso di installazione distribuita di ruoli, insieme al set di replica: per ogni istanza aggiuntiva del database, aggiungi il numero specificato all'ammontare totale.

Requisiti hardware per gli host

● **Microarchitettura CPU:**

- Qualsiasi processore Intel® Sandy Bridge o successivo, con supporto per la tecnologia di virtualizzazione Intel®.
- Le estensioni VT-x o VT-d devono essere attivate nel BIOS.

- **Spazio libero su disco rigido:** oltre allo spazio richiesto dal Security Server, HVI richiede altri 9 MB per il Pacchetto supplementare su ogni host.

Requisiti di Security Server

L'assegnazione delle risorse di memoria e CPU per il Security Server dipende dal numero e dal tipo di VM in esecuzione sull'host. La seguente tabella elenca le risorse consigliate da assegnare:

Numero di VM protette	RAM	CPU
1-50 VM	6 GB	4 CPU
51-100 VM	8 GB	6 CPU
101-200 VM	16 GB	8 CPU

Spazio libero su disco rigido: servono 8 GB di spazio libero su ogni host per il Security Server.

Per una prestazione ottimale in un ambiente XenAPP, suddividi le risorse del Security Server in base alla tua configurazione, come segue:

Numero di VDA di XenApp	VDA		Security Server	
	CPU	RAM (GB)	CPU	RAM (GB)
1 VDA	4 / 8	12 / 24	2	4
2 VDA	4 / 8	12 / 24	2	8
4 VDA	8	24	2	16
8 VDA	4	12	4	16

Requisiti virtual machine guest

In una classica configurazione dell'ambiente, per prestazioni e tasso di consolidamento ottimali della VM, si consiglia di avere la seguente configurazione hardware minima per le virtual machine guest:

- **vCPU:** 2 x vCPU
- **RAM:** 3 GB

4.7. Full Disk Encryption

GravityZone Full Disk Encryption ti consente di usare BitLocker su endpoint Windows e FileVault e l'utility con linea di comando diskutil su endpoint macOS tramite Control Center.

Per garantire la protezione dei dati, questo modulo fornisce una crittografia completa del disco per volumi di avvio e non su dischi fissi, e memorizza le chiavi di recupero nel caso gli utenti dimenticassero le proprie password.

Il modulo Cifratura utilizza le risorse hardware esistenti nel tuo ambiente di GravityZone.

Da un punto di vista software, i requisiti sono quasi gli stessi di BitLocker, FileVault e l'utility con linea di comando diskutil, e la maggior parte delle limitazioni si riferisce a questi strumenti.

Su Windows

GravityZone Encryption supporta BitLocker, a partire dalla versione 1.2 su macchine con e senza un chip Trusted Platform Module (TPM).

GravityZone supporta BitLocker sugli endpoint con i seguenti sistemi operativi:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (con TPM)
- Windows 7 Enterprise (con TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*

- Windows Server 2008 R2* (con TPM)

*BitLocker non è incluso sui seguenti sistemi operativi e deve essere installato separatamente. Per maggiori informazioni sull'impiego di BitLocker su Windows Server, fai riferimento a questi articoli della KB forniti da Microsoft:

- <https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server>
- [https://technet.microsoft.com/en-us/library/cc732725\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx)



Importante

GravityZone non supporta la cifratura su Windows 7 e Windows 2008 R2 senza TPM.

Per i requisiti dettagliati di BitLocker, fai riferimento a questo articolo della KB fornito da Microsoft: [https://technet.microsoft.com/en-us/library/cc766200\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

Su Mac

GravityZone supporta FileVault e diskutil su endpoint macOS con i seguenti sistemi operativi:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.8. Protezione archiviazione

Soluzioni di archiviazione e condivisione file supportate:

- Sistemi ICAP-compatible network-attached storage (NAS) e storage-area network (SAN) di Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle® e altri
- Nutanix® Files 3.x fino al 3.6.2
- Citrix® ShareFile

4.9. Protezione mobile

4.9.1. Piattaforme supportate

Security for Mobile supporta le seguenti tipologie di dispositivi e sistemi operativi mobile:

- iPhone e iPad di Apple (iOS 8.1+)
- Smartphone e tablet Google Android (4.2+)

4.9.2. Requisiti connettività

I dispositivi mobile devono avere una connessione dati mobile o Wi-Fi attiva e una connettività con il Server di comunicazione.

4.9.3. Notifiche push

Security for Mobile utilizza le notifiche push per avvisare i clienti mobile quando sono disponibili attività e aggiornamenti della policy. Le notifiche push vengono inviate dal Server di comunicazione tramite il servizio fornito dal produttore del sistema operativo:

- Il servizio Firebase Cloud Messaging (FCM) per dispositivi Android. Affinché FCM funzioni, sono necessari i seguenti requisiti:
 - Deve essere installato Google Play Store.
 - Dispositivi con Android 4.2 o superiore.
 - Per inviare notifiche push, deve essere aperto [un certo numero di porte](#).
- Il servizio Apple Push Notifications (APN) per dispositivi iOS. Per maggiori informazioni, fai riferimento a questo [articolo della KB dedicato ad Apple](#).

Puoi verificare quali notifiche push mobile stanno funzionando correttamente nella sezione **Verifica notifiche push mobile** in **Configurazione > Varie**.

Per maggiori informazioni sui processi lavorativi di GravityZone Mobile Device Management, fai riferimento a [questo articolo della KB](#).

4.9.4. Certificati gestione iOS

Per configurare l'infrastruttura per la gestione dei dispositivi mobile iOS, devi fornire un certo numero di certificati di sicurezza.

Per maggiori informazioni, fai riferimento a [«Certificati» \(p. 98\)](#).

4.10. Report Builder

I ruoli Report Builder devono funzionare su istanze separate della Virtual Appliance di GravityZone: la prima virtual appliance deve avere il ruolo Report Builder Database installato, il secondo deve avere il ruolo Report Builder Processors installato.

4.10.1. Hardware

I ruoli Report Builder richiedono le seguenti risorse hardware:

Processore richiesto

Virtual appliance	Numero di endpoint (fino a)					
	250	1000	5000	10000	25000	50000
Base di dati	4	4	4	4	6	8
Processori	6	6	6	6	6	6

RAM (GB)

Virtual appliance	Numero di endpoint					
	250	1000	5000	10000	25000	50000
Base di dati	8	8	8	8	16	16
Processori	8	8	8	8	8	8

Spazio su disco rigido libero (GB)

Virtual appliance	Numero di endpoint					
	250	1000	5000	10000	25000	50000
Database*	15	20	50	90	210	400
Processori**	50	200	1000	1950	4800	9500

* L'utilizzo del disco della Report Builder Database virtual appliance indica gli eventi memorizzati per un anno.

** L'utilizzo del disco della Report Builder Database virtual appliance viene inviato considerando 10 rapporti al mese in media, con un sottoinsieme di 15 colonne

ciascuna. La virtual appliance Report Builder Processors richiede più spazio perché memorizza tutti i rapporti creati con i dati dal Report Builder Database.

4.10.2. Versioni del prodotto GravityZone

A partire dalla versione 6.5.5-1 di GravityZone, i ruoli Report Builder vengono offerti con la Virtual Appliance di GravityZone.

Prima di questa versione, i ruoli Report Builder erano offerti come una virtual appliance virtuale compatibile con la versione 6.1.27-537 o successiva di Bitdefender GravityZone.

4.11. Porte di comunicazione di GravityZone

GravityZone è una soluzione distribuita, in altre parole i suoi componenti comunicano tra loro attraverso l'utilizzo della rete locale o Internet. Ogni componente utilizza una serie di porte per comunicare con gli altri. Devi assicurarti che queste porte siano aperte per GravityZone.

Per maggiori informazioni sulle porte di GravityZone, fai riferimento a [questo articolo della KB](#).

5. INSTALLARE LA PROTEZIONE

GravityZone è una soluzione client-server. Per proteggere la tua rete con Bitdefender, devi implementare i ruoli server di GravityZone, registrare la tua licenza, configurare i pacchetti di installazione e implementarli tramite gli agenti di sicurezza sugli endpoint. Alcuni livelli di sicurezza richiedono l'installazione e la configurazione di componenti aggiuntivi.

5.1. Installazione e configurazione di GravityZone

Per assicurarsi che l'installazione avvenga correttamente, segui questi passaggi:

1. [Prepararsi all'installazione](#)
2. [Implementare e impostare GravityZone](#)
3. [Connetti alla Control Center e configura il primo account utente](#)
4. [Configura le impostazioni della Control Center](#)

5.1.1. Preparati per l'installazione

Per l'installazione, ti serve un'immagine della virtual appliance di GravityZone. Dopo aver impiegato e configurato la appliance di GravityZone, puoi installare in remoto il client o scaricare i pacchetti di installazione necessari per tutti i componenti dei servizi di sicurezza dall'interfaccia web della Control Center.

L'immagine della appliance di GravityZone è disponibile in diversi formati, compatibile con le principali piattaforme di virtualizzazione. Puoi ottenere i link di download registrandoti per una versione di prova sul [sito web di Bitdefender](#).

Per l'installazione e la configurazione iniziale, devi avere a portata di mano:

- I nomi dei DNS o gli indirizzi IP fissi (sia tramite configurazione statica o tramite una prenotazione DHCP) per le appliance di GravityZone
- Nome utente e password di un amministratore del dominio
- Dettagli vCenter Server, vShield Manager, XenServer (nome host o indirizzo IP, porta di comunicazione, nome utente e password amministratore)
- Codici di licenza (controlla l'e-mail dell'acquisto o della registrazione della versione di prova)
- Impostazioni server di posta in uscita

- Se necessario, impostazioni server proxy
- Certificati di sicurezza

5.1.2. Implementare GravityZone

Un'implementazione di GravityZone include una o più appliance che eseguono i ruoli server. Il numero di appliance può dipendere da vari criteri, come la dimensione e l'architettura della tua infrastruttura di rete o le funzionalità di GravityZone che intendi utilizzare. I ruoli server possono essere di tre tipi: base, ausiliario o opzionale.



Importante

Il ruolo ausiliario e quello opzionale sono disponibili solo per determinate soluzioni di GravityZone.

Ruolo di GravityZone	Tipo di ruolo	Installa
Server base di dati Update Server Console web Server di comunicazione	Base (richiesto)	Almeno un'istanza per ciascun ruolo. Un'appliance di GravityZone può eseguire uno o più di questi ruoli (anche tutti).
Report builder database Rapporti processor builder	Ausiliario	Una appliance per ciascun ruolo
Security Server	Opzionale	Consigliato solo per reti di piccole dimensioni o in caso di risorse ridotte. In caso contrario, implementa un Security Server stand-alone da Control Center, una volta completata l'implementazione di GravityZone.

A seconda di come distribuisce i ruoli di GravityZone, dovrai implementare una o più appliance di GravityZone (almeno tre appliance se usi Report Builder). Il Server database è il primo a essere installato.

In uno scenario con più appliance di GravityZone, installerai il ruolo server del database nella prima appliance e configurerai tutte le altre appliance per connetterti all'istanza del database esistente.

Puoi implementare più istanze dei ruoli di Server database, Console web e Server di comunicazione. In questo caso utilizzerai un set di replica per il Server database e balancer del carico per Console web e Server di comunicazione sulle appliance di GravityZone.

È consigliabile installare i ruoli di Report Builder dopo aver impostato GravityZone, ovvero dopo aver installato i ruoli base di GravityZone, configurato la Control Center, aggiornato GravityZone e implementato la protezione sugli endpoint. Inoltre, è necessario prima installare il ruolo Report Builder Database, poi il ruolo Report Builder Processors. Per maggiori dettagli, fai riferimento a [«Installare il Report Builder»](#) (p. 178).

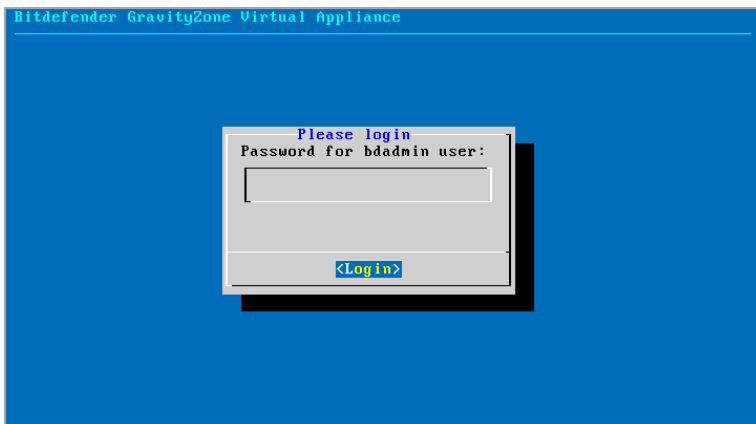
Per implementare e impostare GravityZone:

1. Scarica l'immagine dell'appliance virtuale di GravityZone dal sito web di Bitdefender (link incluso nell'e-mail di registrazione o di acquisto).
2. Importa l'immagine della appliance virtuale di GravityZone nel tuo ambiente virtualizzato.
3. Alimenta la appliance.
4. Dal tuo strumento di gestione della virtualizzazione, accedi all'interfaccia della console della appliance di GravityZone.
5. Configura la password per `bdadmin`, l'amministratore di sistema integrato.



Interfaccia console appliance: inserire una nuova password

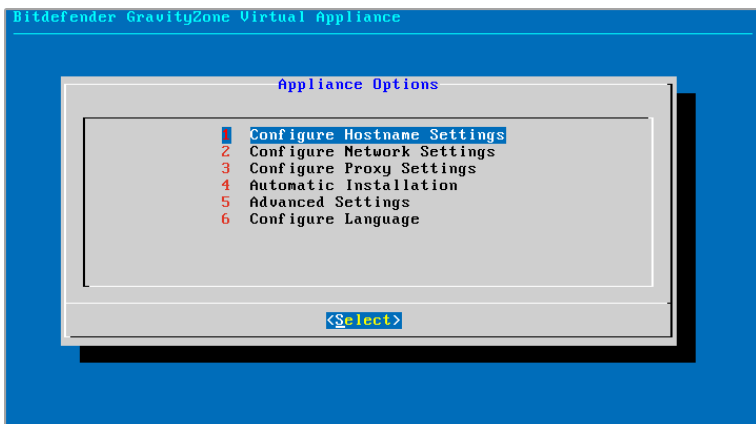
6. Accedi con la password che hai appena impostato.



Interfaccia console appliance: accedere

Accederai all'interfaccia di configurazione della appliance.

Usa i tasti freccia e il tasto Tab per spostarti nei menu e nelle opzioni. Premi Invio per selezionare un'opzione specifica.



Interfaccia console appliance: menu principale

7. Se desideri modificare la lingua dell'interfaccia, seleziona l'opzione **Configura lingua**. Per informazioni dettagliate sulla configurazione, fai riferimento a [«Configura lingua»](#) (p. 68).
8. [Configura il nome dell'host dell'appliance](#).
9. [Configura le impostazioni di rete](#).
10. [Configura le impostazioni proxy](#). (se necessario)
11. Installa i ruoli del server GravityZone. Hai due opzioni:
 - [Installazione automatica](#). Seleziona questa opzione se devi implementare una sola appliance di GravityZone sulla tua rete.
 - [Impostazioni avanzate](#). Seleziona questa opzione se devi implementare GravityZone manualmente o in un'architettura distribuita.

Dopo aver impiegato e configurato la appliance di GravityZone, puoi modificare in qualsiasi momento le impostazioni della appliance, utilizzando l'interfaccia di configurazione. Per maggiori informazioni sulla configurazione della appliance di GravityZone, fai riferimento a [«Gestire la appliance di GravityZone»](#) (p. 105).

Configura impostazioni nome host

La comunicazione con i ruoli di GravityZone viene eseguita utilizzando l'indirizzo IP o il nome del DNS della appliance su cui sono stati installati. Per impostazione predefinita, i componenti di GravityZone comunicano usando gli indirizzi IP. Se vuoi attivare la comunicazione tramite i nomi DNS, devi configurare le appliance di GravityZone con un nome DNS e assicurarti che ci sia corrispondenza con l'indirizzo IP configurato della appliance.

Prerequisiti:

- Configura il valore DNS nel server DNS.
- Il nome DNS deve corrispondere correttamente all'indirizzo IP configurato della appliance. Inoltre, devi assicurarti che la appliance sia configurata con il corretto indirizzo IP.

Per configurare le impostazioni dell'hostname:

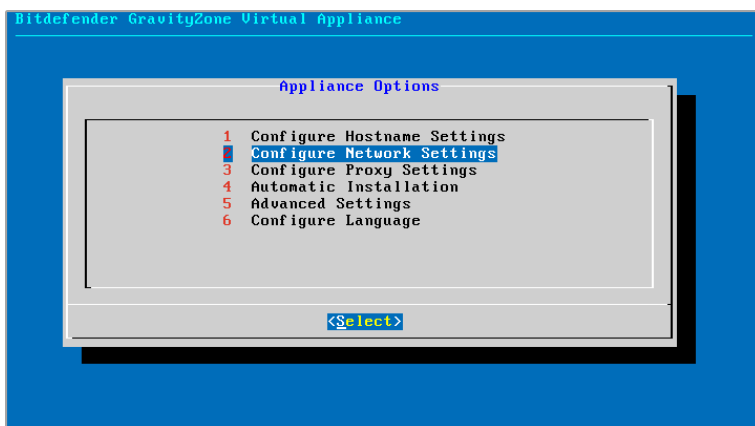
1. Dal menu principale, seleziona **Configura impostazioni hostname**.
2. Inserire l'hostname della appliance e il nome del dominio di Active Directory (se necessario).

3. Seleziona **OK** per salvare le modifiche.

Configura impostazioni rete

Puoi configurare la appliance per ottenere automaticamente le impostazioni di rete dal server DHCP oppure puoi configurare le impostazioni di rete manualmente. Se scegli di utilizzare DHCP, devi configurare il server DHCP per riservare un indirizzo IP specifico per la appliance.

1. Dal menu principale, seleziona **Configura impostazioni di rete**.

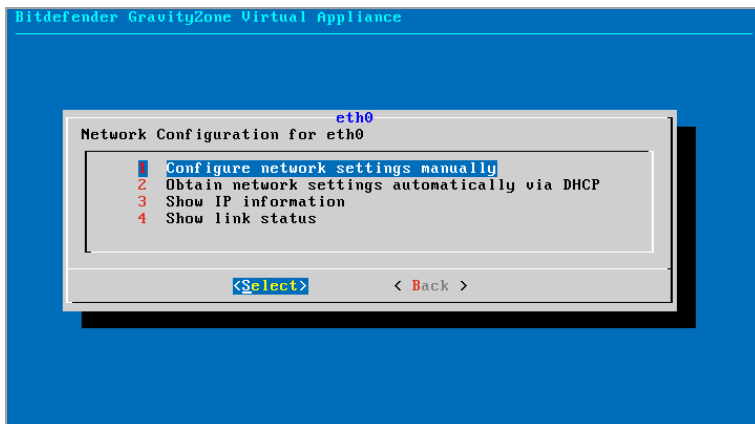


Interfaccia console appliance: opzione impostazioni di rete

2. Seleziona l'interfaccia di rete.

3. Seleziona il metodo di configurazione:

- **Configura manualmente le impostazioni di rete.** Devi specificare l'indirizzo IP, la maschera di rete, l'indirizzo del gateway e gli indirizzi del server DNS.
- **Otteni automaticamente le impostazioni di rete tramite DHCP.** Usa questa opzione se hai configurato il server DHCP per riservare un indirizzo IP specifico per la appliance.



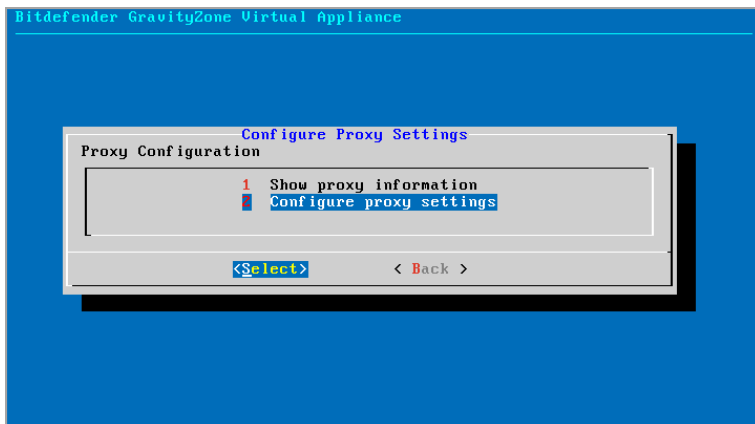
Interfaccia console appliance: configurazione di rete

4. Puoi controllare i dettagli della configurazione IP attuale o lo stato del collegamento, selezionando le opzioni corrispondenti.

Configura le impostazioni proxy

Se vuoi che la appliance si connetta a Internet tramite un server proxy, devi configurare le impostazioni del proxy.

1. Dal menu principale, seleziona **Configura impostazioni proxy**.
2. Seleziona **Mostra informazioni proxy** per verificare se il proxy è attivo.
3. Seleziona **OK** per ritornare alla schermata precedente.
4. Seleziona di nuovo **Configura impostazioni proxy**.



Interfaccia console appliance: configurare impostazioni proxy

5. Inserisci l'indirizzo del server proxy. Usa la seguente sintassi:

- Se il server proxy non richiede l'autenticazione:

```
http(s)://<IP/hostname>:<port>
```

- Se il server proxy richiede l'autenticazione:

```
http(s)://<username>:<password>@<IP/hostname>:<port>
```

6. Seleziona **OK** per salvare le modifiche.

Installazione automatica

Durante l'installazione automatica tutti i ruoli base si installano sulla stessa appliance. Per un'implementazione distribuita di GravityZone, fai riferimento a [«Avanzate» \(p. 66\)](#).

Importante

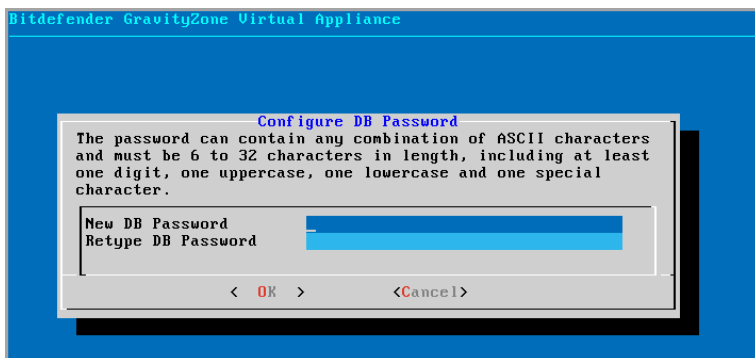
L'implementazione automatica installerà anche il Security Server, integrato nell'appliance di GravityZone. Per informazioni su Security Server, fai riferimento a [«Architettura di GravityZone» \(p. 10\)](#).

L'opzione di installazione automatica dei ruoli è disponibile solo durante la configurazione iniziale di GravityZone.

Per installare i ruoli automaticamente:

1. Dal menu principale, seleziona **Installazione automatica**.
2. Leggi e accetta l'Accordo di licenza con l'utente finale per continuare.
3. Conferma i ruoli da installare.
4. Imposta la password per il Server database.

La password può contenere una qualsiasi combinazione di caratteri ASCII e dev'essere compresa tra i 6 e i 32 caratteri, tra cui almeno un numero, un carattere maiuscolo, uno minuscolo e uno speciale.



Interfaccia console appliance: configurare la password del database

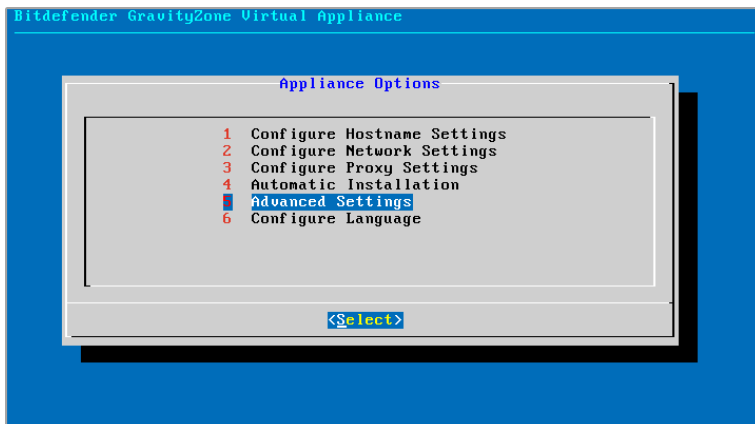
5. Attendi il completamento del processo di installazione.

Avanzate

Usa questa opzione per installare una parte o tutti i ruoli di GravityZone, singolarmente, o per espandere la tua infrastruttura GravityZone. Puoi installare i ruoli su una o più appliance. Questo metodo di installazione è richiesto per testare gli aggiornamenti o in architetture GravityZone distribuite, per scalare GravityZone su reti di grandi dimensioni e garantire una disponibilità elevata dei servizi di GravityZone.

Per installare i ruoli individualmente:

1. Dal menu principale, seleziona **Impostazioni avanzate**.



Interfaccia console appliance: installare i ruoli

2. Seleziona **Installa/Disinstalla ruoli** per installare la appliance in un ambiente GravityZone con un solo server database.



Nota

Le altre opzioni sono per estendere l'impiego di GravityZone a un'architettura distribuita. Per maggiori informazioni, fai riferimento a «[Connetti a base di dati esistente](#)» (p. 116) o «[Connetti a database esistente \(Cluster VPN sicuro\)](#)» (p. 117).

3. Seleziona **Aggiungi o rimuovi i ruoli**. Apparirà un messaggio di conferma.
4. Premi **Invio** per continuare.
5. Premi la **barra spaziatrice** e poi il tasto **Invio** per installare il ruolo Server database. Devi confermare la tua scelta, premendo ancora **Invio**.
6. Imposta la password del database.
La password può contenere una qualsiasi combinazione di caratteri ASCII e dev'essere compresa tra i 6 e i 32 caratteri, tra cui almeno un numero, un carattere maiuscolo, uno minuscolo e uno speciale.
7. Premi **Invio** e attendi il completamento dell'installazione.
8. Installa gli altri ruoli scegliendo **Aggiungi o rimuovi ruoli** dal menu **Installa/Disinstalla ruoli** e poi i ruoli da installare.

- a. Scegli **Aggiungi o rimuovi ruoli** dal menu **Installa/Disinstalla ruoli**.
- b. Leggi l'accordo di licenza con l'utente finale. Premi **Invio** per accettare e continuare.

**Nota**

Questa azione è necessaria solo dopo aver installato il Server database.

- c. Seleziona i ruoli da installare. Premi la **Barra spaziatrice** per selezionare un ruolo e **Invio** per continuare.
- d. Premi **Invio** per confermare e attendi il completamento dell'installazione.

**Nota**

Ogni ruolo di norma viene installato in pochi minuti. Durante l'installazione, i file richiesti vengono scaricati da Internet. Di conseguenza, l'installazione richiede più tempo se la connessione a Internet è lenta. Se l'installazione si blocca, ripeti la procedura con la appliance.

Configura lingua

Inizialmente, l'interfaccia di configurazione della appliance è in inglese.

Per cambiare la lingua dell'interfaccia:

1. Seleziona **Configura lingua** dal menu principale.
2. Seleziona la lingua dalle opzioni disponibili. Apparirà un messaggio di conferma.

**Nota**

Potresti dover scorrere verso il basso per visualizzare la tua lingua.

3. Seleziona **OK** per salvare le modifiche.

5.1.3. Configurazione iniziale Control Center

Dopo aver impiegato e configurato la appliance di GravityZone, devi accedere all'interfaccia web della Control Center e configurare il tuo account di Amministratore aziendale.

1. Nella barra dell'indirizzo del tuo browser web, inserisci l'indirizzo IP o il DNS hostname della appliance della Control Center (usando il prefisso `https://`) Comparirà la procedura guidata per la configurazione.
2. Inserisci i codici di licenza richiesti per convalidare i servizi di sicurezza di GravityZone acquistati. Puoi anche fornire un qualsiasi codice add-on di GravityZone che possiedi.

Controlla l'e-mail di acquisto o registrazione della versione di prova per trovare i tuoi codici di licenza.

- a. Clicca sul pulsante **+** **Aggiungi** nel lato superiore della tabella. Apparirà la finestra di configurazione.
- b. Seleziona il tipo di registrazione della licenza (online oppure offline).
- c. Inserisci il codice di licenza nella voce **Codice di licenza**. Per la registrazione offline, devi inserire anche il codice di registrazione.
- d. Attendi che il codice di licenza venga convalidato. Clicca su **Aggiungi** per finire.

Il codice di licenza comparirà nella tabella licenza. Puoi anche visualizzare il servizio di sicurezza, lo stato, la data di scadenza e l'utilizzo attuale di ciascun codice di licenza nelle colonne corrispondenti.



Nota

- Durante la configurazione iniziale, deve essere fornito almeno un codice di licenza per iniziare a utilizzare GravityZone. In seguito puoi aggiungere altri codici di licenza e add-on, o modificare quelli esistenti.
- Puoi utilizzare gli add-on finché viene fornita una licenza base valida. Diversamente, potrai visualizzare le funzionalità, ma non potrai utilizzarle.

Product Registration

English

MyBitdefender Account

License key

Create Accounts

Enter License Keys

+ Add Refresh

Key	Service	Expiry Date
-----	---------	-------------

Next

Configurazione iniziale - Inserisci i codici di licenza

3. Clicca su **Avanti** per continuare.
4. Inserisci le tue informazioni aziendali, come nome dell'azienda, indirizzo e numero di telefono.
5. Puoi modificare il logo mostrato nella Control Center e anche nei rapporti e nelle notifiche e-mail dell'azienda, come segue:
 - Clicca su **Cambia** per cercare l'immagine da usare come logo sul tuo computer. L'immagine dev'essere in formato .png o .jpg, mentre la dimensione deve essere di 200x30 pixel.
 - Clicca su **Predefinita** per eliminare l'immagine e passare all'immagine fornita da Bitdefender.
6. Indica i dettagli richiesti per il tuo account di amministratore aziendale: nome utente, indirizzo e-mail e password. La password deve contenere almeno un carattere maiuscolo, uno minuscolo e un numero o un carattere speciale.

Product Registration

English

MyBitdefender Account

License key


Create Accounts

Enter Company Details

Company Name:

Address:

Phone:

Logo:  The logo needs to have the size 200x30 px, and needs to be in png or jpg format

[Change](#) [Default](#)

Enter Company Administrator Account Details

Username:

Email:

Full Name:

Password:

Confirm password:

[Create account](#)

Configurazione iniziale - Configura il tuo account

7. Clicca su **Crea account**.

Sarà creato l'account di amministratore aziendale e accederai automaticamente con il nuovo account alla Control Center di Bitdefender.

5.1.4. Configura le impostazioni della Control Center

Dopo la configurazione iniziale, devi configurare le impostazioni della Control Center. Come Amministratore aziendale, puoi fare quanto segue:

- Configurare altre impostazioni generali oltre a quelle relative a posta e proxy.
- Eseguire o programmare un backup del database della Control Center.
- Imposta l'integrazione con Active Directory e gli strumenti di gestione della virtualizzazione (vCenter Server, XenServer).
- Installare i certificati di sicurezza.

The screenshot shows the Bitdefender GravityZone web interface. The top navigation bar includes 'Mail Server', 'Proxy', 'Miscellaneous', 'Backup', 'Active Directory', 'Virtualization', and 'Certificates'. The left sidebar lists various system components, with 'Configuration' highlighted. The main content area is titled 'Mail Server Settings' and contains the following fields:

- Mail server (SMTP): *** Input field containing 'mail.comp.com'
- Port: *** Input field containing '25'
- Encryption type:** Dropdown menu set to 'None'
- From email: *** Input field containing 'noreply@comp.com'
- Use authentication**
- Username: *** Input field (empty)

Impostazioni mail server

Server e-mail

Control Center richiede un server mail esterno per inviare comunicazioni via e-mail.



Nota

Si consiglia di creare un account di posta dedicato da utilizzare con la Control Center.

Per consentire alla Control Center di inviare le e-mail:

1. Vai alla pagina **Configurazione**.
2. Seleziona la scheda **Server mail**.
3. Seleziona **Impostazioni server e-mail** e configura le impostazioni richieste:
 - **Server mail (SMTP)**. Inserisci l'indirizzo IP o l'hostname del server mail che invierà le e-mail.
 - **Porta**. Inserisci la porta usata per connettersi al server mail.
 - **Tipo di crittografia**. Se il server mail richiede una connessione cifrata, seleziona il tipo appropriato nel menu (SSL, TLS o STARTTLS).
 - **Da e-mail**. Inserisci l'indirizzo e-mail che vuoi che compaia nel campo Da dell'e-mail (indirizzo e-mail del mittente).

- **Usa autenticazione.** Seleziona questa casella se il server mail richiede un'autenticazione. Devi specificare un nome utente / indirizzo e-mail e password validi.

4. Clicca su **Salva**.

Control Center convalida automaticamente le impostazioni della posta quando le salvi. Se le impostazioni fornite non possono essere convalidate, un messaggio d'errore ti informerà dell'impostazione errata. Correggi l'impostazione e riprova.

proxy

Se la tua azienda si connette a Internet tramite un server proxy, devi configurare le impostazioni del proxy:

1. Vai alla pagina **Configurazione**.
2. Seleziona la scheda **Proxy**.
3. Seleziona **Usa impostazioni proxy** e configura le impostazioni richieste:
 - **Indirizzo** - Inserisci l'indirizzo IP del server proxy.
 - **Porta** - Inserisci la porta usata per connettersi al server proxy.
 - **Nome utente** - inserisci un nome utente riconosciuto dal proxy.
 - **Password** - inserisci la password dell'utente già specificato in precedenza.
4. Clicca su **Salva**.

Funzioni varie

Dalla pagina **Configurazione** e dalla scheda **Varie**, puoi configurare le seguenti preferenze generali:

- **Quando è necessaria un'immagine del Security Server non disponibile.** La appliance di GravityZone non include in modo predefinito le immagini della macchina virtuale del Security Server. Se un amministratore prova a scaricare un'immagine del Security Server o a eseguire un'attività di installazione del Security Server, l'azione fallirà. Puoi configurare un'azione automatica per questa situazione, selezionando una delle seguenti opzioni:
 - **Scarica l'immagine automaticamente**
 - **Avvisa l'amministratore e non scaricare**



Nota

Per evitare ogni interferenza con il lavoro dell'amministratore, puoi scaricare manualmente i pacchetti del Security Server necessari dalla pagina **Aggiornamento** nella scheda **Aggiornamento prodotto**. Per maggiori informazioni, fai riferimento a [«Scaricare gli aggiornamenti del prodotto»](#) (p. 189).

- **Quando è necessario un kit non disponibile** . Puoi configurare un'azione automatica per questa situazione, selezionando una delle seguenti opzioni:
 - **Scarica il pacchetto automaticamente**
 - **Avvisa l'amministratore e non scaricare**
- **Impieghi contemporanei**. Gli amministratori possono impiegare in remoto le componenti di sicurezza, eseguendo le attività di installazione. Usa questa opzione per specificare il numero massimo di impieghi simultanei che possono essere eseguiti alla volta.

Per esempio, se il numero massimo di impieghi contemporanei è impostato su 10 e un'attività di installazione remota del client viene assegnata a 100 computer, la Control Center inizialmente invierà 10 pacchetti di installazione nella rete. In questo caso, l'installazione del client viene eseguita contemporaneamente su un numero massimo di 10 computer, mentre tutte le altre sotto-attività resteranno in sospeso. Non appena una sotto-attività viene completata, viene inviato un altro pacchetto di installazione e così via.

- **Applica autenticazione a due fattori per tutti gli account**. L'autenticazione a due fattori (2FA) aggiunge un ulteriore livello di sicurezza agli account GravityZone, richiedendo un codice di autenticazione oltre alle credenziali della Control Center. Questa funzionalità richiede il download e l'installazione di Google Authenticator, Microsoft Authenticator o un altro autenticatore a due fattori compatibile TOTP (Time-Based One-Time Password Algorithm) con lo standard RFC6238 sul dispositivo mobile dell'utente, per poi collegare la app all'account di GravityZone e utilizzarla con ogni accesso a Control Center. La app di autenticazione genera un codice di sei cifre ogni 30 secondi. Per completare l'accesso a Control Center, dopo aver inserito la password, l'utente dovrà fornire anche il codice di autenticazione a sei cifre.

L'autenticazione a due fattori viene attivata per impostazione predefinita quando si crea un profilo aziendale. Successivamente, all'accesso, una finestra di configurazione chiederà agli utenti di attivare tale funzionalità. Gli utenti avranno la possibilità di saltare l'attivazione della 2FA solo per tre volte. Al quarto

tentativo di accesso, non sarà più possibile saltare la configurazione della 2FA e l'utente non potrà più effettuare l'accesso.

Se vuoi disattivare l'applicazione della 2FA per tutti gli account di GravityZone nella tua azienda, deselezioni l'opzione. Prima di attivare le modifiche ti sarà presentato un messaggio di conferma. Da questo punto in poi, gli utenti potranno avere la 2FA ancora attivata, ma potranno disattivarla dalle impostazioni del proprio account.



Nota

- Puoi visualizzare lo stato della 2FA per un account utente nella pagina **Account**.
- Se un utente con la 2FA attivata non può accedere a GravityZone (per via di un nuovo dispositivo o di un codice segreto smarrito), è possibile reimpostare la sua autenticazione a due fattori dalla pagina dell'account utente, nella sezione **Autenticazione a due fattori**. Per maggiori dettagli, fai riferimento al capitolo **Account utente > Gestire l'autenticazione a due fattori** della Guida dell'amministratore.

- **Impostazioni server NTP.** Il server NTP viene usato per sincronizzare il tempo tra tutte le appliance di GravityZone. Viene fornito un indirizzo del server NTP predefinito, che puoi modificare nella voce **Indirizzo server NTP**.



Nota

Affinché le appliance di GravityZone possano comunicare con il server NTP, la porta 123 (UDP) deve essere aperta.

- **Attiva Syslog.** Attivando questa funzione, consenti a GravityZone di inviare le notifiche a un server di logging che utilizza il protocollo Syslog. In questo modo, hai la possibilità di monitorare meglio gli eventi di GravityZone.

Per visualizzare o configurare la lista delle notifiche inviate al server di Syslog, fai riferimento al capitolo **Notifiche** nella Guida per gli amministratori di GravityZone.

Per consentire il logging a un server di Syslog remoto:

1. Seleziona la casella **Attiva Syslog**.
2. Inserisci il nome del server o l'IP, il protocollo preferito e la porta Syslog.
3. Seleziona il formato con cui inviare i dati al server Syslog:

- **Formato JSON.** JSON è un formato di scambio dei dati piuttosto leggero e completamente indipendente da qualsiasi linguaggio di programmazione. JSON rappresenta i dati in un formato di testo leggibile. Nel formato JSON, i dettagli di ogni evento sono strutturati in oggetti, con ciascun oggetto costituito da una coppia nome/valore.

Per esempio:

```
{
  "name": "Login from new device",
  "created": "YYYY-MM-DDThh:mm:ss+hh:ss",
  "company_name": "companyname",
  "user_name": "username",
  "os": "osname",
  "browser_version": "browserversion",
  "browser_name": "browsername",
  "request_time": "DD MMM YYYY, hh:mm:ss +hh:ss",
  "device_ip": "computerip"
}
```

Per maggiori informazioni, fai riferimento a www.json.org.

Questo è il formato predefinito in GravityZone.

- **Common Event Format (CEF).** CEF è un formato aperto standard sviluppato da ArcSight, che semplifica la gestione dei rapporti.

Per esempio:

```
CEF:0|Bitdefender|GZ|<GZ version>|NNNNN|Login from new
device|3|start=MMM DD YYYY hh:mm:ss+hh:mm
BitdefenderGZCompanyName=companyname suser=username
BitdefenderGZLoginOS=osname
BitdefenderGZAuthenticationBrowserName=browsername
BitdefenderGZAuthenticationBrowserVersion=browserversion
dvchost=computerip
```

Per maggiori informazioni, fai riferimento a [ArcSight Common Event Format \(CEF\) Implementation Standard](#).

Nel capitolo **Notifiche** della Guida per gli amministratori, puoi visualizzare i tipi di notifiche disponibili per ciascun formato.

4. Clicca sul pulsante **+** **Aggiungi** nella colonna **Azione**.

Clicca su **Salva** per applicare le modifiche.

Backup

Per assicurarti che tutti i tuoi dati della Control Center siano sicuri, puoi fare un backup del database di GravityZone. Puoi eseguire quanti backup del database desideri, oppure puoi programmare dei backup periodici in modo che vengano eseguiti automaticamente negli intervalli di tempo stabiliti.

Ogni comando di backup del database crea un file `tgz` (file di archivio Tar compresso GZIP) nella posizione indicata nelle impostazioni di backup.

Quando diversi amministratori devono gestire privilegi sulle impostazioni della Control Center, puoi anche configurare le **Impostazioni di notifica** per avisarti ogni volta che viene completato un backup del database. Per maggiori informazioni, fai riferimento al capitolo **Notifiche** nella Guida per gli amministratori di GravityZone.

Creazione dei backup dei database

Per eseguire un database del backup:

1. Vai alla pagina **Configurazione** nella Control Center e clicca sulla scheda **Backup**.
2. Clicca sul pulsante **Fai il backup ora** nel lato superiore della tabella. Apparirà la finestra di configurazione.
3. Seleziona il tipo di posizione in cui l'archivio del backup sarà salvato:

- **Locale**, per salvare l'archivio di backup nella appliance di GravityZone. In questo caso, devi specificare il percorso per la cartella della appliance di GravityZone in cui l'archivio sarà salvato.

La appliance di GravityZone ha una struttura delle cartelle pari a Linux. Per esempio, puoi scegliere di creare il backup nella cartella `tmp`. In questo caso, inserisci `tmp` nel campo **Percorso**.

- **FTP**, per salvare l'archivio del backup in un server FTP. In questo caso, inserisci i dettagli dell'FTP nei seguenti campi.
- **Rete**, per salvare l'archivio del backup in una rete condivisa. In questo caso, inserisci il percorso della posizione di rete che desideri (per esempio, `\\computer\cartella`), il nome del dominio e le credenziali dell'utente del dominio.

4. Clicca sul pulsante **Testa impostazioni**. Una notifica testuale ti informerà se le impostazioni indicate sono valide oppure no.

Per creare un backup, tutte le impostazioni devono essere valide.


5. Clicca su **Genera**. Sarà mostrata la pagina **Backup**. Una nuova voce di backup sarà aggiunta alla lista. Verifica lo **Stato** del nuovo backup. Una volta completato il backup, troverai l'archivio `tgz` nella posizione indicata.



Nota

L'elenco disponibile nella pagina **Backup** contiene i registri di tutti i backup creati. Questi registri non forniscono l'accesso agli archivi di backup, ma mostrano soltanto alcuni dettagli dei backup creati.

Per programmare un backup del database:

1. Vai alla pagina **Configurazione** nella Control Center e clicca sulla scheda **Backup**.
2. Clicca sul pulsante  **Impostazioni backup** nel lato superiore della tabella. Apparirà la finestra di configurazione.
3. Seleziona **Backup programmato**.
4. Configura l'intervallo del backup (giornaliero, settimanale o mensile) e l'ora di inizio.

Per esempio, puoi programmare i backup per essere eseguiti a cadenza settimanale, ogni venerdì, a partire dalle 22:00.

5. Configura la posizione del backup programmato.
6. Seleziona il tipo di posizione in cui l'archivio del backup sarà salvato:
 - **Locale**, per salvare l'archivio di backup nella appliance di GravityZone. In questo caso, devi specificare il percorso per la cartella della appliance di GravityZone in cui l'archivio sarà salvato.

La appliance di GravityZone ha una struttura delle cartelle pari a Linux. Per esempio, puoi scegliere di creare il backup nella cartella `tmp`. In questo caso, inserisci `tmp` nel campo **Percorso**.

- **FTP**, per salvare l'archivio del backup in un server FTP. In questo caso, inserisci i dettagli dell'FTP nei seguenti campi.
- **Rete**, per salvare l'archivio del backup in una rete condivisa. In questo caso, inserisci il percorso della posizione di rete che desideri (per esempio,

\\computer\cartella), il nome del dominio e le credenziali dell'utente del dominio.

7. Clicca sul pulsante **Testa impostazioni**. Una notifica testuale ti informerà se le impostazioni indicate sono valide oppure no.

Per creare un backup, tutte le impostazioni devono essere valide.

8. Clicca su **Salva** per creare il backup programmato.

Ripristinare un backup del database

Quando per vari motivi la tua istanza di GravityZone non funziona regolarmente (aggiornamenti falliti, problemi con l'interfaccia, file danneggiati, errori, ecc.), puoi ripristinare il database di GravityZone da una copia di backup, utilizzando:

- [La stessa appliance](#)
- [Una nuova immagine di GravityZone](#)
- [La funzionalità set di replica](#)

Seleziona l'opzione che si adatta meglio alla tua situazione e continua con la procedura di ripristino solo dopo aver letto attentamente i prerequisiti descritti di seguito.

Ripristinare il database nella stessa VA di GravityZone

Prerequisiti

- Una connessione SSH all'appliance di GravityZone, utilizzando i privilegi di **root**. Puoi utilizzare le credenziali **putty** e **bdadmin** per connetterti alla appliance tramite SSH, poi esegui il comando `sudo su` per passare all'account di **root**.
- L'infrastruttura di GravityZone non è cambiata dal backup.
- Il backup è più recente del 30 aprile 2017 e la versione di GravityZone è superiore alla 6.2.1-30. Altrimenti, contatta il team del Supporto tecnico.
- Nelle architetture distribuite, GravityZone non è stato configurato per usare la replica del database (set di replica).

Per verificare la configurazione, segui questi passaggi:

1. Apri il file `/etc/mongodb.conf`.
2. Controlla che `replSet` non sia stato configurato, come nell'esempio sottostante:


```
# replSet = setname
```



Nota

Per ripristinare il database quando il set di replica è attivato, fai riferimento a «Ripristinare il database in un ambiente di un set di replica» (p. 84).

- Nessun processo CLI è in esecuzione.

Per assicurarti che tutti i processi CLI siano stati fermati, esegui il seguente comando:

```
# killall -9 perl
```

- Il pacchetto **mongoconsole** è stato installato nella appliance.

Per verificare che la condizione sia soddisfatta, esegui questo comando:

```
# /opt/bitdefender/bin/mongoshellrestore --version
```

Il comando non dovrebbe restituire alcun errore, altrimenti eseguire:

```
# apt-get update  
# apt-get install --upgrade mongoconsole
```

Ripristinare il database

1. Vai alla posizione contenente l'archivio del database:

```
# cd /cartella-con-backup
```

, dove **directory-with-backup** è il percorso della posizione dei file di backup.

Per esempio:

```
# cd /tmp/backup
```

2. Ripristina il database.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password  
--authenticationDatabase admin --gzip --drop --archive < \  
gz-backup-$$$AMMGGtimestamp
```



Importante

Assicurati di sostituire `GZ_db_password` con la password effettiva del Server database di GravityZone e le variabili del timestamp nel nome dell'archivio con la data corrente.

Ad esempio, la data corrente avrà un aspetto simile a questo:

```
gz-backup-2019-05-17 (1495004926) .tar.gz
```

3. Riavvia le appliance.

Ora il ripristino del database è stato completato.

Ripristinare il database da una VA di GravityZone disattivata

Prerequisiti

- Una nuova installazione di una VA di GravityZone:
 - Con lo stesso IP come la vecchia appliance
 - Avendo installato SOLO il ruolo Server database.Puoi scaricare l'immagine della VA di GravityZone da [qui](#).
- Una connessione SSH all'appliance virtuale di GravityZone, utilizzando i privilegi di **root**.
- L'infrastruttura di GravityZone non è cambiata da quando è stato fatto il backup.
- Il backup è più recente del 30 aprile 2017.
- Nelle architetture distribuite, GravityZone non è stato configurato per usare la replica del database (set di replica).
Se usi un set di replica nel tuo ambiente di GravityZone, puoi anche avere installato il ruolo di server database su altre istanze di appliance.

Per ripristinare il database quando il set di replica è attivato, fai riferimento a [«Ripristinare il database in un ambiente di un set di replica»](#) (p. 84).

Ripristinare il database

1. Connettiti all'appliance di GravityZone tramite SSH e passa a **root**.
2. Ferma VASync:

```
# stop vasync
```

3. Ferma CLI:

```
# # killall -9 perl
```

4. Vai alla posizione in cui si trova il backup:

```
# cd /cartella-con-backup
```

,dove `directory-with-backup` è il percorso della posizione dei file di backup.

Per esempio:

```
# cd /tmp/backup
```

5. Ripristina il database.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password  
--authenticationDatabase=admin --gzip --drop \  
--archive='/home/bdadmin/gz-backup-$AAAAMGGtimestamp
```



Importante

Assicurati di sostituire `GZ_db_password` con la password effettiva del Server database di GravityZone e le variabili del timestamp nel nome dell'archivio con la data corrente.

Ad esempio, la data corrente avrà un aspetto simile a questo:

```
gz-backup-2019-05-17 (1495004926) .tar.gz
```

6. Ripristina l'ID precedente della appliance:

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ-db_password  
--eval print(db.applianceInstalls.findOne({name:'db'}).\  
applianceId)" --quiet > /opt/bitdefender/etc/applianceid
```



Importante

Assicurati di sostituire `GZ_db_password` con la password effettiva del Server database di GravityZone.

7. Rimuovi il riferimento dai vecchi ruoli.

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ_db_password  
'db.applianceInstalls.remove({ip:db.applianceInstalls.findOne(  
{name:"db"}).ip,name:{"$ne": "db"}});' --quiet devdb
```



Importante

Assicurati di sostituire `GZ_db_password` con la password effettiva del Server database di GravityZone.

8. Avvia VASync:

```
# start vasync
```

9. Avvia CLI:

```
# /opt/bitdefender/eltiw/installer
```

10. Installa gli altri ruoli.

```
# dpkg -l gz*
```

Verifica di aver fatto l'upgrade all'ultima versione dello schema del database

```
> db.settings.findOne().database
{
  "previousVersion" : "000-002-009",
  "ranCleanUpVersions" : {
    "b0469c84f5bf0bec0b989ae37161b986" : "000-002-008"
  },
  "updateInProgress" : false,
  "updateTimestamp" : 1456825625581,
  "version" : "000-002-011"
}
```

11. Riavvia l'appliance.

Ora il ripristino del database è stato completato.

Ripristinare il database in un ambiente di un set di replica

Se hai impiegato il database in un ambiente di un set di replica, puoi trovare la procedura ufficiale di ripristino nel [manuale online di mongoDB](#) (solo in inglese).

Nota

La procedura richiede abilità tecniche avanzate e deve essere fatta solo un ingegnere qualificato. In caso di difficoltà, contatta il nostro [Supporto tecnico](#) per ricevere assistenza nel ripristinare il database.

Active Directory

Tramite l'integrazione con Active Directory, puoi importare nella Control Center l'inventario esistente dalle installazioni in locale di Active Directory e da Active Directory ospitato in Microsoft Azure, semplificando l'impiego, la gestione, il monitoraggio e la reportistica della sicurezza. Inoltre, gli utenti di Active Directory possono essere assegnati a diversi ruoli utente nella Control Center.

Per integrare e sincronizzare GravityZone con un dominio di Active Directory:

1. Vai in **Configurazione > Active Directory > Domini** e clicca su **+ Aggiungi**.
2. Configura le impostazioni richieste:
 - Intervallo di sincronizzazione (in ore)
 - Nome dominio Active Directory (incluso l'estensione del dominio)
 - Nome utente e password di un amministratore del dominio

- Posizione nell'Inventario di rete in cui mostrare gli endpoint AD:
 - Mantieni la struttura AD e ignora le unità operative vuote
 - Ignora la struttura AD, importa in Gruppi personalizzati
 - Mantieni la struttura AD solo con le unità operative selezionate
- I Domain Controller con cui la Control Center si sta sincronizzando. Espandi la sezione **Richiedi Domain Controller** e seleziona i controller dalla tabella.

3. Clicca su **Salva**.



Importante

Ogni volta che viene cambiata la password utente, ricordati di aggiornarla anche nella Control Center.

Permessi di accesso

Con i permessi d'accesso puoi garantire accesso a GravityZone Control Center agli utenti di Active Directory (AD), in base alle regole di accesso. Per integrare e sincronizzare i domini AD, fai riferimento ad [Active Directory](#). Per maggiori informazioni sulla gestione degli account utente tramite le regole di accesso, fai riferimento al capitolo **Account utente** della Guida di installazione di GravityZone.

Fornitori di servizi di virtualizzazione

Attualmente GravityZone può integrarsi con VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 e Microsoft Azure.

- [«Integrazione con vCenter Server» \(p. 86\)](#)
- [«Integrazione con XenServer» \(p. 89\)](#)
- [«Integrazione con Nutanix Prism Element» \(p. 89\)](#)
- [«Integrazione con Amazon EC2» \(p. 91\)](#)
- [«Integrazione con Microsoft Azure» \(p. 92\)](#)
- [«Gestire le integrazioni della piattaforma» \(p. 93\)](#)



Importante

Se imposti una nuova integrazione con un altro sistema vCenter Server, XenServer, Nutanix Prism Element e Microsoft Azure, ricordati anche di rivedere e aggiornare i privilegi di accesso per gli utenti esistenti.

Integrazione con vCenter Server

Puoi integrare GravityZone con uno o più sistemi vCenter Server. I sistemi vCenter Server in modalità Linked devono essere aggiunti separatamente alla Control Center.

Per configurare l'integrazione con un vCenter Server:

1. Vai alla pagina **Configurazione** in Control Center e raggiungi **Fornitori di virtualizzazione > Piattaforme di gestione**.
2. Clicca sul pulsante **+** **Aggiungi** nel lato superiore della tabella e seleziona **vCenter Server** nel menu. Apparirà la finestra di configurazione.
3. Specifica i dettagli del vCenter Server.
 - Dai un nome al sistema vCenter Server nella Control Center
 - Nome dell'host o indirizzo IP del sistema vCenter Server
 - Porta vCenter Server (predefinita 443)
4. Specifica le credenziali da usare per autenticarti con il vCenter Server. Puoi scegliere di usare le credenziali fornite per l'integrazione con Active Directory o un diverso set di credenziali. L'utente di cui vengono fornite le credenziali deve avere permessi di root o amministratore sul vCenter Server.
5. Scegli la piattaforma VMware installata nel tuo ambiente e configura le impostazioni di conseguenza:
 - **Nessuna**. Seleziona questa opzione per NSX-T o nel caso non ci fosse alcuna piattaforma VMware specifica installata, e clicca su **Salva**. Accettare il certificato di sicurezza auto-firmato è necessario per l'integrazione.
Per configurare l'integrazione di NSX-T Manager e applicare la protezione per endpoint alle tue VM tramite la policy di GravityZone Guest Introspection, fai riferimento al seguente [articolo della KB](#).
 - **vShield**. Specifica i dettagli del sistema vShield Manager integrato con il vCenter Server.
 - Nome dell'host o indirizzo IP del sistema vShield Manager
 - Porta vShield Manager (predefinita 443)
 - **NSX-V**. Specifica i dettagli del sistema NSX Manager integrato con il vCenter Server.

**Nota**

Per fare l'upgrade da VMware vShield a NSX, fai riferimento a questo [articolo della KB](#).

- Nome dell'host o indirizzo IP del NSX Manager
- Porta NSX Manager (predefinita 443)
- Nome utente e password utilizzati per l'autenticazione in NSX Manager. Queste credenziali saranno salvate sull'entità protetta, non nel Credentials Manager.
- Selezione la casella **Metti un tag in caso di virus** per usare i tag di sicurezza predefiniti di NSX quando viene rilevato un malware sulla virtual machine.

Una macchina può essere taggata con tre diversi tag di sicurezza, in base al livello di rischio della minaccia:

- `ANTI_VIRUS.VirusFound.threat=low`, si applica sulla macchina quando Bitdefender trova un malware poco rischioso, che può essere eliminato.
- `ANTI_VIRUS.VirusFound.threat=medium`, si applica sulla macchina quando Bitdefender non può eliminare i file infetti, ma li disinfetta.
- `ANTI_VIRUS.VirusFound.threat=high`, si applica sulla macchina quando Bitdefender non può eliminare o disinfettare i file infetti, ma ne blocca l'accesso.

Quando vengono rilevate minacce di diversi livelli di rischio sulla stessa macchina, saranno applicati tutti i tag associati. Per esempio, una macchina su cui sono stati rilevati malware ad alto e basso rischio, avrà entrambi i tag di sicurezza.

**Nota**


Puoi trovare i tag di sicurezza in VMware vSphere, nella scheda **Rete e sicurezza > NSX Manager > NSX Manager > Manage > Tag di sicurezza**. Anche se puoi creare quanti tag desideri, solo i tre tag indicati funzioneranno con Bitdefender.

6. **Limita l'assegnazione della policy dalla visione della rete.** Usa questa opzione per controllare l'autorizzazione degli amministratori di rete di cambiare le policy

delle virtual machine tramite la schermata **Computer e Virtual Machine** nella pagina **Rete**. Quando viene selezionata questa opzione, gli amministratori possono cambiare le policy delle virtual machine solo dalla schermata **Virtual Machine** dell'inventario della rete.

7. Clicca su **Salva**. Ti sarà chiesto di accettare i certificati di sicurezza per vCenter Server e NSX Manager. Questi certificati assicurano una comunicazione sicura tra GravityZone e i componenti di VMware, prevenendo il rischio di attacchi man in the middle.

Puoi verificare se sono stati installati i certificati corretti controllando le informazioni del sito sul browser per ciascun componente di VMware rispetto alle informazioni del certificato mostrate nella Control Center.

8. Seleziona le caselle per accettare l'uso dei certificati.
9. Clicca su **Salva**. Potrai visualizzare il vCenter Server nell'elenco delle integrazioni attive.
10. Se usi la piattaforma NSX-V:
 - a. Vai alla scheda **Aggiornamento > Componenti**.
 - b. Scarica e pubblica il pacchetto **Security Server (VMware con NSX)** Per maggiori informazioni su come aggiornare i componenti di GravityZone, fai riferimento a «[Aggiornare GravityZone](#)» (p. 185).
 - c. Vai alla scheda **Configurazione > Fornitori di virtualizzazione**.
 - d. Nella colonna **Azione**, clicca sul pulsante  **Registra** corrispondente al vCenter integrato con NSX per registrare il servizio di Bitdefender con VMware NSX Manager.



Avvertimento

Quando il certificato di sicurezza è scaduto e il vCenter prova a sincronizzarsi, una finestra pop-up ti avviserà di aggiornarlo. Accedi alla finestra di configurazione dell'integrazione di vCenter Server, clicca su **Salva**, accetta i nuovi certificati e clicca di nuovo su **Salva**.

Dopo la registrazione, Bitdefender si aggiunge alla console di VMware vSphere:

- Servizio di Bitdefender
- Gestore servizio di Bitdefender
- Tre nuovi profili predefiniti del servizio per una modalità di scansione permissiva, normale e aggressiva.



Nota

Puoi visualizzare questi profili del servizio anche nella pagina **Policy** della Control Center. Clicca sul pulsante **Colonne** in alto a destra del riquadro destro per visualizzare maggiori informazioni.

Alla fine, potrai effettivamente assistere alla sincronizzazione del vCenter Server. Attendi un paio di minuti fino al completamento della sincronizzazione.

Integrazione con XenServer

Puoi integrare GravityZone con uno o più sistemi XenServer.


Per configurare l'integrazione con un XenServer:

1. Vai alla pagina **Configurazione** nella Control Center e clicca sulla scheda **Fornitori di virtualizzazione**.
2. Clicca sul pulsante **+ Aggiungi** nel lato superiore della tabella e seleziona **XenServer** nel menu. Apparirà la finestra di configurazione.
3. Specifica i dettagli del XenServer.
 - Dai un nome al sistema XenServer nella Control Center
 - Nome dell'host o indirizzo IP del sistema XenServer
 - Porta XenServer (predefinita 443)
4. Specifica le credenziali da usare per autenticarti con il XenServer. Puoi scegliere di usare le credenziali fornite per l'integrazione con Active Directory o un diverso set di credenziali.
5. **Limita l'assegnazione della policy dalla visione della rete.** Usa questa opzione per controllare l'autorizzazione degli amministratori di rete di cambiare le policy delle virtual machine tramite la schermata **Computer e Virtual Machine** nella pagina **Rete**. Quando viene selezionata questa opzione, gli amministratori possono cambiare le policy delle virtual machine solo dalla schermata **Virtual Machine** dell'inventario della rete.
6. Clicca su **Salva**. Potrai visualizzare il vCenter Server nell'elenco delle integrazioni attive e che sta effettuando la sincronizzazione. Attendi un paio di minuti fino al completamento della sincronizzazione.

Integrazione con Nutanix Prism Element

Puoi integrare GravityZone con uno o più cluster di Nutanix Prism Element, che siano registrati a Nutanix Prism Central oppure no.

Per configurare l'integrazione con Nutanix Prism Element:

1. Vai alla pagina **Configurazione** nella Control Center e clicca sulla scheda **Fornitori di virtualizzazione**.
2. Clicca sul pulsante  **Aggiungi** nel lato superiore della tabella e seleziona **Nutanix Prism Element** nel menu. Apparirà la finestra di configurazione.
3. Specifica i dettagli del Nutanix Prism Element:
 - Il nome del Nutanix Prism Element nella Control Center.
 - L'indirizzo IP di una Controller Virtual Machine (CVM) dal cluster di Nutanix Prism Element o l'indirizzo IP del Cluster Virtual IP.
 - Porta di Nutanix Prism Element (predefinita 9440).
4. Specifica le credenziali da usare per autenticarti con Nutanix Prism Element.



Importante

L'utente di cui si forniscono le credenziali deve disporre dei privilegi di amministratore cluster o amministratore utente in Nutanix Prism Element.

5. **Limita l'assegnazione della policy dalla visione della rete.** Usa questa opzione per controllare l'autorizzazione degli amministratori di rete di cambiare le policy delle virtual machine tramite la schermata **Computer e Virtual Machine** nella pagina **Rete**. Quando viene selezionata questa opzione, gli amministratori possono cambiare le policy delle virtual machine solo dalla schermata Virtual Machine dell'inventario della rete.
6. Clicca su **Salva**. Ti verrà chiesto di accettare i certificati di sicurezza per Nutanix Prism. Questi certificati assicurano una comunicazione sicura tra GravityZone e Nutanix Prism Element, prevedono il rischio di attacchi man-in-the-middle.
Puoi verificare se sono stati installati i certificati corretti controllando le informazioni del sito sul browser per ciascun cluster di Nutanix Prism Element o CVM rispetto alle informazioni del certificato mostrate nella Control Center.
7. Seleziona le caselle per accettare l'uso dei certificati.
8. Clicca su **Salva**.

Se inserisci un IP CVM per configurare l'integrazione, ti sarà chiesto in una nuova finestra se vuoi usare il Cluster Virtual IP al posto del CVM IP:

- a. Clicca su **Sì** per usare il Cluster Virtual IP per l'integrazione. Il Cluster Virtual IP sostituirà il CVM IP nei dettagli del Nutanix Prism Element.
- b. Clicca su **No** per utilizzare ulteriormente il CVM IP.

i **Nota**

Come miglior pratica, si consiglia di usare il Cluster Virtual IP piuttosto che il CVM IP. In questo modo, l'integrazione resta attiva anche quando un particolare host diventa indisponibile.

- c. Nella finestra **Aggiungi Nutanix Prism Element**, clicca su **Salva**.

Potrai visualizzare il Nutanix Prism Element nell'elenco delle integrazioni attive. Attendi un paio di minuti fino al completamento della sincronizzazione.

Integrazione con Amazon EC2

Puoi integrare GravityZone con il tuo inventario Amazon EC2 e proteggere le tue istanze EC2 ospitate nel cloud Amazon.

Prerequisiti:

- I codici segreti e di accesso di un account AWS valido
- L'account AWS deve avere i seguenti permessi:
 - IAMReadOnlyAccess
 - AmazonEC2ReadOnly per tutte le regioni AWS

Puoi creare diverse integrazioni con Amazon EC2. Per ciascuna integrazione, devi fornire un valido account utente AWS.

i **Nota**

Non è possibile aggiungere più integrazioni usando le credenziali dei ruoli IAM create per lo stesso account AWS.

Per configurare l'integrazione con Amazon EC2:

1. Vai alla pagina **Configurazione** nella Control Center e clicca sulla scheda **Fornitori di virtualizzazione**.
2. Clicca sul pulsante **+** **Aggiungi** nel lato superiore della tabella e seleziona **Integrazione Amazon EC2** nel menu. Apparirà la finestra di configurazione.
3. Specifica i dettagli dell'integrazione con Amazon EC2:

- Il nome dell'integrazione. Aggiungendo diverse integrazioni di Amazon EC2, puoi identificarle per nome.
 - I codici segreti e di accesso dell'account utente AWS.
4. **Limita l'assegnazione della policy dalla visione della rete.** Usa questa opzione per controllare l'autorizzazione degli amministratori di rete di cambiare le policy delle virtual machine tramite la schermata **Computer e Virtual Machine** nella pagina **Rete**. Quando viene selezionata questa opzione, gli amministratori possono cambiare le policy delle virtual machine solo dalla schermata **Virtual Machine** dell'inventario della rete.
 5. Clicca su **Salva**. Se le credenziali fornite sono valide, l'integrazione sarà creata e aggiunta alla griglia.

Attendi qualche istante mentre GravityZone si sincronizza con l'inventario di Amazon EC2.

Integrazione con Microsoft Azure

Puoi integrare GravityZone con Microsoft Azure e proteggere le tue virtual machine ospitate nel Microsoft Cloud.

Prerequisiti:

- Applicazione Azure con permesso di lettura
- ID Active Directory
- ID applicazione
- Application Secret

Per dettagli su come ottenere le credenziali richieste e impostare l'applicazione Azure, fai riferimento a questo [articolo della KB](#).

Puoi creare diverse integrazioni con Microsoft Azure. Per ciascuna integrazione, devi avere un valido ID di Active Directory.

Per configurare l'integrazione con Microsoft Azure:


1. Vai alla pagina **Configurazione** nella Control Center e clicca sulla scheda **Fornitori di virtualizzazione**.
2. Clicca sul pulsante **+ Aggiungi** nel lato superiore della tabella e seleziona **Integrazione Azure** nel menu. Apparirà la finestra di configurazione.
3. Specifica i dettagli dell'integrazione con Azure:

- **Il nome dell'integrazione.** Aggiungendo diverse integrazioni di Azure, puoi identificarle per nome.
 - **ID Active Directory.** Ogni istanza di Azure Active Directory ha un identificatore unico disponibile nei dettagli dell'account di Microsoft Azure.
 - **ID applicazione.** Ogni applicazione Azure ha un identificatore unico disponibile nei dettagli dell'applicazione.
 - **Application Secret.** L'Application Secret è il valore mostrato quando si salva un codice nelle impostazioni dell'applicazione Azure.
4. Seleziona l'opzione **Limita l'assegnazione della policy dalla visuale di rete** per modificare la policy solo dalla visuale **Virtual Machine**. Se deselezionato, puoi modificare la policy dalla visuale **Computer e virtual machine**.
 5. Clicca su **Salva**. Se le credenziali fornite sono valide, l'integrazione sarà creata e aggiunta alla griglia.


Attendi qualche istante mentre GravityZone si sincronizza con l'inventario di Microsoft Azure.


Gestire le integrazioni della piattaforma

Per modificare o aggiornare un'integrazione della piattaforma:


1. Nella Control Center, vai alla scheda **Configurazione > Fornitori di virtualizzazione**.
2. Clicca sul pulsante  **Modifica** nella colonna **Azione**.
3. Configura le impostazioni della regola come necessario. Per maggiori informazioni, fai riferimento a una delle seguenti sezioni, a seconda dei casi:
 - [«Integrazione con vCenter Server» \(p. 86\)](#)
 - [«Integrazione con XenServer» \(p. 89\)](#)
 - [«Integrazione con Nutanix Prism Element» \(p. 89\)](#)
 - [«Integrazione con Amazon EC2» \(p. 91\)](#)
 - [«Integrazione con Microsoft Azure» \(p. 92\)](#)
4. Clicca su **Salva**. Attendi un paio di minuti fino alla re-sincronizzazione del server.

Le integrazioni con Nutanix Prism Element, Amazon EC2 e Microsoft Azure vengono sincronizzate automaticamente ogni 15 minuti. Puoi sincronizzare manualmente un'integrazione in qualsiasi momento, in questo modo:


1. Nella Control Center, vai alla scheda **Configurazione > Fornitori di virtualizzazione**.
2. Clicca sul pulsante  **Risincronizza l'inventario** nella colonna **Azione**.
3. Clicca su **Si** per confermare.

Il pulsante  **Risincronizza inventario** è particolarmente utile quando lo stato dell'integrazione cambia e richiede la sincronizzazione, come nelle seguenti situazioni:

- Per l'integrazione con Nutanix Prism Element:
 - L'utente non ha più privilegi di amministratore nell'inventario.
 - L'utente non è più valido (password modificata o eliminata).
 - Il certificato di sicurezza non è più valido.
 - Si è verificato un errore di connessione.
 - Un host è stato aggiunto o rimosso nel cluster di Nutanix Prism Element.
- Per l'integrazione con Microsoft Azure:
 - Un abbonamento è stato aggiunto o rimosso in Microsoft Azure.
 - Virtual machine sono state aggiunte o rimosse nell'inventario di Microsoft Azure.



Puoi anche sincronizzare l'integrazione cliccando il pulsante  **Modifica** e poi clicca su **Salva**.

Per rimuovere un'integrazione vShield, XenServer, Nutanix Prism Element, Amazon EC2 o Microsoft Azure:

1. Nella Control Center, vai alla scheda **Configurazione > Fornitori di virtualizzazione**.
2. Clicca sul pulsante  **Elimina** nella colonna **Azione** corrispondente all'integrazione da rimuovere.
3. Clicca su **Si** per confermare.

Per rimuovere un'integrazione NSX:

1. Accedi alla console di VMware vSphere ed elimina tutte le policy di Bitdefender e del Security Server.

2. Nella Control Center, vai alla scheda **Configurazione > Fornitori di virtualizzazione**.
3. Nella colonna **Azione**, corrispondente all'integrazione da rimuovere, clicca su  **Annulla registrazione** e poi  **Elimina**.
4. Clicca su **Si** per confermare.

Per assicurarsi che vengano visualizzate le informazioni più recenti, clicca sul pulsante **Aggiorna** nel lato superiore della tabella.


Fornitori di sicurezza

GravityZone Security for Virtualized Environments si integra con il VMware NSX-T Data Center tramite NSX-T Manager.

Integrazione con NSX-T Manager

NSX-T Manager è il piano di gestione dei server vCenter integrati con un NSX-T Data Center affinché l'integrazione funzioni correttamente, è necessario configurare l'integrazione per i server vCenter associati con NSX-T Manager. Per maggiori informazioni, fai riferimento a [Integrazione con vCenter Server](#).

Per configurare l'integrazione con NSX-T Manager:

1. In Control Center, vai a **Configurazione > Fornitori di virtualizzazione > Fornitori di sicurezza**.
2. Clicca sul pulsante  **Aggiungi** nel lato superiore della tabella. Apparirà la finestra di configurazione.
3. Specifica i dettagli dell'integrazione NSX-T:
 - Nome dell'integrazione NSX-T.
 - Nome dell'host o indirizzo IP del sistema vCenter Server associato.
 - Porta NSX-T (predefinita 433).
4. Specifica le credenziali per autenticarti con il vCenter Server. Puoi scegliere di usare le credenziali fornite per l'integrazione con Active Directory o un diverso set di credenziali. L'utente di cui vengono fornite le credenziali deve avere permessi di root o amministratore sul vCenter Server.
5. Clicca su **Salva**.

Ora Control Center è integrato con NSX-T. Per applicare la protezione degli endpoint alle tue VM tramite la policy di GravityZone Guest Introspection, fai

riferimento all'articolo della KB [Configura e applica la protezione degli endpoint a VM VMware NSX-T guest tramite la policy di GravityZone Guest Introspection](#).

Nota

GravityZone può essere usato solo per proteggere il vCenter Server associato.

NTSA

Con questa sezione, puoi configurare l'integrazione con Bitdefender Network Traffic Security Analytics, una soluzione di sicurezza di livello aziendale che rileva in modo accurato le violazioni e fornisce informazioni approfondite sugli attacchi avanzati tramite l'analisi del traffico di rete. Per maggiori informazioni su questa soluzione, fai riferimento alla documentazione di [Bitdefender NTSA](#).

Importante

La sezione dedicata all'integrazione di NTSA è disponibile solo dopo aver fornito un codice di licenza di NTSA valido nella pagina **Configurazione > Licenza**.

Per configurare l'integrazione con NTSA, devi avere la soluzione NTSA installata nel tuo ambiente e le credenziali per accedere alla console web di NTSA.

Durante l'integrazione, ti sarà chiesto di fornire l'indirizzo della console web di NTSA (IP o nome dell'host) e un token (codice di abbinamento) generato nella console web di NTSA, come spiegato di seguito.

Configura l'integrazione con NTSA

1. Accedi a GravityZone Control Center.
2. Vai alla pagina **Configurazione** e clicca sulla scheda NTSA.
3. Attiva l'opzione **Integra con Network Traffic Security Analytics (NTSA)**.
4. Inserisci i seguenti dati:
 - L'indirizzo della console web di NTSA (IP / Hostname).
 - La porta usata da GravityZone per comunicare con NTSA (la predefinita è 443).
 - Il codice di abbinamento (token) viene generato dalla console web di NTSA come segue:
 - a. Accedi alla tua console web di NTSA e vai alla pagina **Licenze**.
 - b. Seleziona l'opzione **Integrazione con GravityZone**.

- c. Clicca su **Genera un codice di abbinamento**. Il codice comparirà automaticamente.
 - d. Usa il pulsante **Copia negli appunti** per ottenere il codice di abbinamento.
 - e. Clicca su **OK** per confermare.
5. Verifica che l'impronta dell'host mostrata corrisponda all'hash del certificato SSL della appliance NTSA, poi attiva l'opzione **Accetto il certificato**.
 6. Clicca su **Salva**.

Una volta completata la configurazione con successo, l'integrazione sarà mostrata come **Sincronizzata**. L'integrazione di NTSA può avere i seguenti stati:

- **N.D.**: l'integrazione non è ancora stata configurata.
- **Sincronizzata**: l'integrazione è stata configurata e attivata.
- **Token non valido**: il codice di abbinamento della console web NTSA non è valido.
- **Errore di connessione**: non è stato possibile connettersi all'indirizzo della console web di NTSA specificato (IP/nome dell'host non valido).
- **Errore di certificato**: l'impronta attuale del certificato SSL della appliance di NTSA non corrisponde all'impronta accettata inizialmente.
- **Errore sconosciuto**: si è verificato un errore di comunicazione sconosciuto.

Il campo **Ultimo cambiamento stato** mostra data e ora dell'ultima modifica delle impostazioni dell'integrazione avvenuta con successo, o quando lo stato dell'integrazione è stato cambiato.

Una volta configurata l'integrazione con NTSA, puoi disattivare / attivare l'integrazione usando la casella disponibile nel lato superiore della pagina di **NTSA**.

Collegare i propri account di GravityZone e NTSA

Dopo aver configurato l'integrazione, i tuoi account di GravityZone e NTSA saranno collegati e potrai raggiungere facilmente la console web di NTSA come segue:

1. In GravityZone Control Center, clicca sul pulsante **NTSA** posizionato nell'angolo in basso a sinistra della finestra.
2. Sarai reindirizzato alla pagina di accesso della console web di NTSA. Dopo aver inserito le tue credenziali di accesso di NTSA, puoi iniziare a esplorare la console web di NTSA.

Devi inserire le tue credenziali di NTSA solo la prima volta. In seguito, otterrai l'accesso alla console web di NTSA automaticamente cliccando sul pulsante **NTSA**, senza che ti venga richiesto di accedere.

Eliminare l'integrazione di NTSA

Eliminando il codice di licenza di NTSA dalla pagina **Configurazione > Licenza**, eliminerai anche l'integrazione di NTSA.

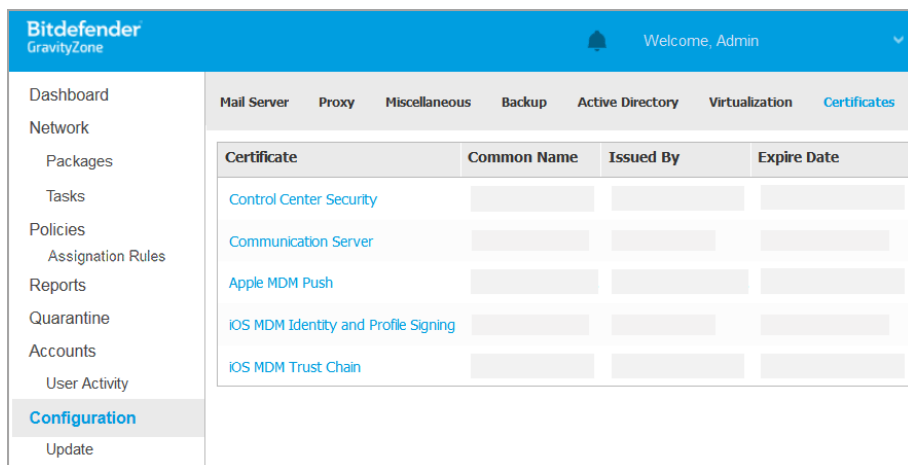
Nota

Il tuo account di NTSA e GravityZone saranno scollegati nelle seguenti situazioni:

- Il codice di licenza di NTSA è stato rimosso.
- La password di NTSA è stata modificata.
- La tua password di GravityZone è stata modificata.
- Le impostazioni dell'integrazione di NTSA è stata modificata.

Certificati

Affinché il tuo impiego di GravityZone funzioni correttamente e in modo sicuro, devi creare e aggiungere un certo numero di certificati di sicurezza nella Control Center.



The screenshot shows the Bitdefender GravityZone web console interface. The top navigation bar is blue and contains the Bitdefender GravityZone logo, a notification bell, and the text "Welcome, Admin" with a dropdown arrow. Below the navigation bar, there are several tabs: "Mail Server", "Proxy", "Miscellaneous", "Backup", "Active Directory", "Virtualization", and "Certificates". The "Certificates" tab is selected. The main content area displays a table with the following columns: "Certificate", "Common Name", "Issued By", and "Expires Date". The table contains five rows of certificate information:

Certificate	Common Name	Issued By	Expires Date
Control Center Security			
Communication Server			
Apple MDM Push			
iOS MDM Identity and Profile Signing			
iOS MDM Trust Chain			

On the left side of the console, there is a sidebar menu with the following items: Dashboard, Network, Packages, Tasks, Policies, Assignment Rules, Reports, Quarantine, Accounts, User Activity, Configuration (highlighted), and Update.

La pagina Certificati

La Control Center supporta i seguenti formati dei certificati:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)



Nota

I seguenti certificati sono richiesti esclusivamente per gestire la sicurezza sui dispositivi iOS di Apple:

- Certificato server comunicazione
- Certificato push MDM di Apple
- Certificato Identify and Profile Signing MDM iOS
- Certificato Trust Chain MDM iOS

Se non intendi disporre della gestione dei dispositivi mobile iOS, non sarà necessario fornire tali certificati.

Certificato di sicurezza Control Center

Il certificato di sicurezza della Control Center è necessario per identificare la console web della Control Center come un sito web affidabile nel browser. La Control Center utilizza di norma un certificato SSL firmato da Bitdefender. Questo certificato integrato non viene riconosciuto dai browser web e attiva degli avvisi di sicurezza. Per evitare gli avvisi di sicurezza del browser, aggiungi un certificato SSL firmato dalla tua azienda o da un'Autorità di Certificazione (CA) esterna.

Per aggiungere o sostituire il certificato della Control Center:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato.
3. Seleziona il tipo di certificato (con codice privato separato o incorporato).
4. Clicca sul pulsante **Aggiungi** accanto al campo **Certificato** e carica il certificato.
5. Per i certificati con codice privato separato, clicca sul pulsante **Aggiungi** accanto al campo **Codice privato** e carica il codice privato.
6. Se il certificato è protetto da password, inserisci la password nel campo corrispondente.

7. Clicca su **Salva**.

Endpoint - Certificato di sicurezza di comunicazione di Security Server

Questo certificato assicura una comunicazione sicura tra gli agenti di sicurezza e il Security Server (multiplatforma) che hanno assegnato.

Durante il suo impiego, il Security Server genera un certificato autofirmato predefinito. Puoi sostituire questo certificato integrato aggiungendone uno di tua scelta nella Control Center.

Per aggiungere o sostituire un Certificato di comunicazione Security Server - Endpoint:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato.
3. Seleziona il tipo di certificato (con codice privato separato o incorporato).
4. Clicca sul pulsante **Aggiungi** accanto al campo **Certificato** e carica il certificato.
5. Per i certificati con codice privato separato, clicca sul pulsante **Aggiungi** accanto al campo **Codice privato** e carica il codice privato.
6. Se il certificato è protetto da password, inserisci la password nel campo corrispondente.
7. Clicca su **Salva**. Potrebbe comparire un messaggio di avviso se il certificato è autofirmato o scaduto. Se scaduto, rinnova il tuo certificato.
8. Clicca su **Sì** per continuare a caricare il certificato. Subito dopo il completamento del caricamento, la Control Center invia il certificato di sicurezza ai Security Server.

Se necessario, puoi tornare al certificato integrato originale di ciascun Security Server, come segue:

1. Clicca sul nome del certificato nella pagina **Certificati**.
2. Scegli **Nessun certificato (usa predefinito)** come tipo di certificato.
3. Clicca su **Salva**.

Certificato server comunicazione

Il certificato server comunicazione viene utilizzato per proteggere la comunicazione tra il Server di comunicazione e i dispositivi mobile iOS.

Requisiti:

- Questo certificato SSL può essere firmato dalla tua azienda o da un'Autorità di certificazione esterna.



Avvertimento

Il certificato deve essere invalidato se non emesso da un'Autorità di certificazione affidabile/pubblica (per esempio, certificati autofirmati).

- Il nome comune del certificato deve corrispondere esattamente al nome del dominio o all'indirizzo IP utilizzato dai client mobile per connettersi al Server di comunicazione. Questo viene configurato come indirizzo MDM esterno nell'interfaccia di configurazione della console della appliance di GravityZone.
- I client mobile devono fidarsi di questo certificato. Per questo, devi aggiungere anche la [iOS MDM Trust Chain](#).

Per aggiungere o sostituire il certificato del Server di comunicazione:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato.
3. Seleziona il tipo di certificato (con codice privato separato o incorporato).
4. Clicca sul pulsante **Aggiungi** accanto al campo **Certificato** e carica il certificato.
5. Per i certificati con codice privato separato, clicca sul pulsante **Aggiungi** accanto al campo **Codice privato** e carica il codice privato.
6. Se il certificato è protetto da password, inserisci la password nel campo corrispondente.
7. Clicca su **Salva**.

Certificato push MDM di Apple

Apple richiede un certificato push MDM per assicurare una comunicazione sicura tra il Server di comunicazione e il servizio di Notifiche Push Apple (APN), quando si inviano le notifiche push. Le notifiche push vengono usate per invitare i dispositivi a connettersi al Server di comunicazione quando sono disponibili nuove attività o modifiche nelle policy.

Apple rilascia questo certificato direttamente alla tua azienda, ma richiede che la tua Certificate Signing Request (CSR) sia firmata da Bitdefender. Control Center

offre una procedura guidata per aiutarti a ottenere facilmente il tuo certificato push MDM di Apple.

Importante

- Ti serve un ID Apple per ottenere e gestire il certificato. Se non hai un ID Apple, puoi crearne uno nella pagina web [My Apple ID](#). Usa un indirizzo e-mail generico e non quello di un dipendente per registrarti per ottenere un ID Apple, in quanto ti servirà successivamente per rinnovare il certificato.
- Il sito web di Apple non funziona correttamente con Internet Explorer. Consigliamo di utilizzare le versioni più recenti di Safari o Chrome.
- Il certificato push MDM di Apple è valido solo per un anno. Quando il certificato sta per scadere, devi rinnovarlo e importare il certificato rinnovato nella Control Center. Se permetti al certificato di scadere, devi crearne uno nuovo e riattivare tutti i tuoi dispositivi.

Aggiungere un certificato push MDM di Apple

Per ottenere il certificato push MDM di Apple e importarlo nella Control Center:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato e segui la procedura guidata come descritto in basso:

Fase 1 - Ottieni una richiesta di firma del certificato firmata da Bitdefender

Seleziona l'opzione appropriata:

- **Mi serve generare una richiesta di firma del certificato firmata da Bitdefender** (Consigliato)
 - a. Inserisci il nome dell'azienda, il tuo nome completo e l'indirizzo e-mail nei campi corrispondenti.
 - b. Clicca su **Genera** per scaricare il file CSR firmato da Bitdefender.
- **Ho già una richiesta di firma del certificato e mi serve che venga firmata da Bitdefender**
 - a. Invia il file CSR e il codice privato associato cliccando sul pulsante **Aggiungi** accanto ai rispettivi campi.

Il Server di comunicazione richiede il codice privato durante l'autenticazione con i server APN.
 - b. Specifica la password che protegge il codice privato, se necessario.
 - c. Clicca sul pulsante **Firma** per scaricare il file CSR firmato da Bitdefender.

Fase 2 - Richiedi un certificato push da Apple

- a. Clicca sul link **Portale certificati push di Apple** e accedi utilizzando il tuo ID Apple e la tua password.
- b. Clicca sul pulsante **Crea un certificato** e accetta le Condizioni d'uso.
- c. Clicca su **Scegli file**, seleziona il file CSR e clicca su **Invia**.



Nota

Potresti trovare il pulsante **Scegli file** con un nome diverso, come **Scegli** o **Esplora**, in base al browser che utilizzi.

- d. Dalla pagina di conferma, clicca sul pulsante **Scarica** per ricevere il tuo certificato push MDM.
- e. Torna alla procedura guidata dalla Control Center.

Fase 3 - Importa il certificato push di Apple

Clicca sul pulsante **Aggiungi certificato** per inviare il file del certificato dal tuo computer.

Puoi controllare i dettagli del certificato nel campo sottostante.

3. Clicca su **Salva**.

Rinnovare il certificato push MDM di Apple

Per rinnovare il certificato MDM di Apple e aggiornarlo nella Control Center:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato per aprire la procedura guidata dell'importazione.
3. Ottieni una richiesta di firma del certificato firmata da Bitdefender. La procedura è la stessa per ottenere un nuovo certificato.
4. Clicca sul link **Portale certificati push di Apple** e accedi con lo stesso ID Apple utilizzato per creare il certificato.
5. Localizza il certificato push MDM per Bitdefender e clicca sul pulsante **Rinnova** corrispondente.
6. Clicca su **Scegli file**, seleziona il file CSR e clicca su **Invia**.
7. Clicca su **Scarica** per salvare il certificato sul tuo computer.
8. Torna alla Control Center e importa il nuovo certificato push di Apple.
9. Clicca su **Salva**.

Certificato Identity and Profile Signing MDM iOS

Il certificato Identity and Profile Signing MDM iOS viene utilizzato dal Server di comunicazione per firmare i certificati di identità e i profili di configurazione inviati ai dispositivi mobile.

Requisiti:

- Deve essere un certificato intermedio o End-Entity, firmato o dalla tua azienda o da un'Autorità di certificazione esterna.
- I client mobile devono fidarsi di questo certificato. Per questo, devi aggiungere anche la [iOS MDM Trust Chain](#).

Per aggiungere o sostituire il certificato Identity and Profile Signing MDM iOS:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato.
3. Seleziona il tipo di certificato (con codice privato separato o incorporato).
4. Clicca sul pulsante **Aggiungi** accanto al campo **Certificato** e carica il certificato.
5. Per i certificati con codice privato separato, clicca sul pulsante **Aggiungi** accanto al campo **Codice privato** e carica il codice privato.
6. Se il certificato è protetto da password, inserisci la password nel campo corrispondente.
7. Clicca su **Salva**.

Certificato Trust Chain MDM iOS

I certificati iOS MDM Trust Chain sono richiesti sui dispositivi mobile per assicurarsi che possano fidarsi del [certificato Server di comunicazione](#) e il [certificato Identity and Profile Signing MDM iOS](#). Il Server di comunicazione invia questo certificato ai dispositivi mobile durante l'attivazione.

L'iOS MDM Trust Chain deve includere tutti i certificati intermedi fino al certificato principale della propria azienda o il certificato intermedio emesso da un'Autorità di certificazione esterna.

Per aggiungere o sostituire i certificati iOS MDM Trust Chain:

1. Vai alla pagina **Configurazione** e clicca sulla scheda **Certificati**.
2. Clicca sul nome del certificato.

3. Clicca sul pulsante **Aggiungi** accanto al campo **Certificato** e carica il certificato.
4. Clicca su **Salva**.

Archivio

Questa scheda mostra le informazioni sugli aggiornamenti dell'agente di sicurezza, incluso le versioni del prodotto archiviate nel server di aggiornamento e le versioni disponibili nell'archivio ufficiale di Bitdefender, i ring di aggiornamento, la data e l'ora dell'aggiornamento e l'ultimo controllo per nuove versioni.

Nota

Le versioni del prodotto non sono disponibili per i server di sicurezza.

5.1.5. Gestire la appliance di GravityZone

La appliance di GravityZone è dotata di un'interfaccia di configurazione base, disponibile dallo strumento di gestione utilizzato per gestire l'ambiente virtualizzato dove hai impiegato la appliance.

Queste sono le opzioni principali disponibili dopo la prima distribuzione dell'appliance di GravityZone:

- [Configura impostazioni nome host](#)
- [Configura impostazioni rete](#)
- [Configura le impostazioni proxy](#)
- [Server comunicazione MDM](#)
- [Avanzate](#)
- [Configura lingua](#)

Usa i tasti freccia e il tasto `Tab` per spostarti nei menu e nelle opzioni. Premi `Invio` per selezionare un'opzione specifica.

Configurare hostname e impostazioni

La comunicazione con i ruoli di GravityZone viene eseguita utilizzando l'indirizzo IP o il nome del DNS della appliance su cui sono stati installati. Per impostazione predefinita, i componenti di GravityZone comunicato usando gli indirizzi IP. Se vuoi attivare la comunicazione tramite i nomi DNS, devi configurare le appliance di GravityZone con un nome DNS e assicurarti che ci sia corrispondenza con l'indirizzo IP configurato della appliance.

Prerequisiti:

- Configura il valore DNS nel server DNS.
- Il nome DNS deve corrispondere correttamente all'indirizzo IP configurato della appliance. Inoltre, devi assicurarti che la appliance sia configurata con il corretto indirizzo IP.

Per configurare le impostazioni dell'hostname:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Configura impostazioni hostname**.
3. Inserire l'hostname della appliance e il nome del dominio di Active Directory (se necessario).
4. Seleziona **OK** per salvare le modifiche.

Configura impostazioni rete

Puoi configurare la appliance per ottenere automaticamente le impostazioni di rete dal server DHCP oppure puoi configurare le impostazioni di rete manualmente. Se scegli di utilizzare DHCP, devi configurare il server DHCP per riservare un indirizzo IP specifico per la appliance.

Per configurare le impostazioni di rete:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Configura impostazioni di rete**.
3. Seleziona l'interfaccia di rete (predefinita `eth0`).
4. Seleziona il metodo di configurazione:
 - **Configura manualmente le impostazioni di rete.** Devi specificare l'indirizzo IP, la maschera di rete, l'indirizzo del gateway e gli indirizzi del server DNS.
 - **Ottieni automaticamente le impostazioni di rete tramite DHCP.** Usa questa opzione se hai configurato il server DHCP per riservare un indirizzo IP specifico per la appliance.
5. Puoi controllare i dettagli della configurazione IP attuale o lo stato del collegamento, selezionando le opzioni corrispondenti.

Configura le impostazioni proxy

Se la appliance si connette a Internet tramite un server proxy, devi configurare le impostazioni del proxy.

Nota

Le impostazioni del proxy possono essere configurate anche dalla Control Center, nella pagina **Configurazione > Proxy**. Modificando le impostazioni proxy in una posizione, automaticamente saranno aggiornate anche nell'altra posizione.

Per configurare le impostazioni proxy:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Configura impostazioni proxy**.
3. Seleziona **Configura impostazioni proxy**.
4. Inserisci l'indirizzo del server proxy. Usa la seguente sintassi:
 - Se il server proxy non richiede l'autenticazione:
`http(s)://<IP/hostname>:<port>`
 - Se il server proxy richiede l'autenticazione:
`http(s)://<username>:<password>@<IP/hostname>:<port>`
5. Seleziona **OK** per salvare le modifiche.

Seleziona **Mostra informazioni proxy** per verificare le impostazioni proxy.

Server comunicazione MDM

Nota

Questa configurazione è richiesta solo per la gestione di dispositivi mobile, se il tuo codice di licenza include il servizio Security for Mobile. L'opzione compare nel menu dopo aver installato il [ruolo Server di comunicazione](#).

Nella configurazione predefinita di GravityZone, i dispositivi mobile possono essere gestiti solo quando sono direttamente connessi alla rete aziendale (via Wi-Fi o VPN). Ciò accade perché quando si iscrivono dispositivi mobile, questi sono configurati per connettersi all'indirizzo locale della appliance del Server di comunicazione.

Per poter gestire i dispositivi mobile su Internet, indipendentemente dalla loro posizione, devi configurare il Server di comunicazione con un indirizzo pubblicamente raggiungibile.

Per poter gestire i dispositivi mobile quando non sono connessi alla rete aziendale, sono disponibili le seguenti opzioni:

- Configurare la mappatura delle porte sul gateway aziendale per la appliance che esegue il ruolo di Server di comunicazione.
- Aggiungere un adattatore di rete aggiuntivo alla appliance con il ruolo di Server di comunicazione e assegnarlo a un indirizzo IP pubblico.

In entrambi i casi, devi configurare il Server di comunicazione con l'indirizzo esterno per essere usato per la gestione dei dispositivi mobile:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Server di comunicazione MDM**.
3. Seleziona **Configura indirizzo esterno server MDM**.
4. Inserisci l'indirizzo esterno.

Usa la seguente sintassi: `https://<IP/Domain>:<Port>`.

- Se usi la mappatura della porta, devi inserire l'indirizzo IP pubblico o il nome del dominio e la porta aperta sul gateway.
 - Se utilizzi un indirizzo pubblico per il Server di comunicazione, devi inserire l'indirizzo IP pubblico o il nome del dominio e la porta del Server di comunicazione. La porta standard è 8443.
5. Seleziona **OK** per salvare le modifiche.
 6. Seleziona **Mostra indirizzo esterno del server MDM** per verificare le impostazioni.

Avanzate

Le impostazioni avanzate riguardano diverse opzioni per l'impiego manuale, l'estensione dell'ambiente e i miglioramenti alla sicurezza:

- [Installa/Disinstalla ruoli](#)
- [Installare Security Server](#)
- [Imposta nuova password del database](#)

- Server di aggiornamento
- Configura balancer ruolo
- Set di replica
- Attiva Cluster VPN sicuro
- Connetti a base di dati esistente
- Connetti a database esistente (Cluster VPN sicuro)
- Controlla Cluster VPN sicuro

La disponibilità delle opzioni varia in base ai ruoli installati e ai servizi attivati. Per esempio, se il ruolo Server database non è stato installato sulla appliance, puoi solo installare i ruoli o connetterti a un database di GravityZone distribuito nella tua rete. Una volta che il ruolo Server database è stato installato sulla appliance, le opzioni per la connessione a un altro database non saranno disponibili.

Installa/Disinstalla ruoli

L'appliance di GravityZone può eseguire uno, più o tutti i seguenti ruoli:

- **Server base di dati**
- **Server di aggiornamento**
- **Console web**
- **Server di comunicazione**
- **Server incidenti**

Un impiego di GravityZone richiede un'istanza di ciascun ruolo operativa. Di conseguenza, in base a come preferisci distribuire i ruoli di GravityZone, impiegherai da uno a quattro appliance di GravityZone. Il ruolo del server centro dati è il primo a essere installato. In uno scenario con più appliance di GravityZone, installerai il ruolo server del database nella prima appliance e configurerai tutte le altre appliance per connetterti all'istanza del database esistente.

Nota

Puoi installare istanze aggiuntive di ruoli specifici usando i balancer del ruolo. Per maggiori informazioni, fai riferimento a [«Configura balancer ruolo»](#) (p. 113).

Per installare i ruoli di GravityZone:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).

2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Seleziona **Installa/Disinstalla ruoli**.
4. Seleziona **Aggiungi o rimuovi i ruoli**.
5. Procedi in base alla situazione attuale:
 - Se questo è l'impiego iniziale della appliance di GravityZone, premi la Barra spaziatrice e poi **Invio** per installare il ruolo Server del database. Devi confermare la tua scelta, premendo ancora **Invio**. Configura la password del database e attendi il completamento dell'installazione.
 - Se hai già impiegato un'altra appliance con il ruolo di Server del database, seleziona **Annulla** e torna al menu **Aggiungi o rimuovi ruoli**. Poi devi scegliere **Configura indirizzo database** e inserire l'indirizzo del server del database. Assicurati di impostare una password del database prima di accedere a questa opzione. Se non conosci la password del database, configurane una nuova selezionando **Impostazioni avanzate e Imposta una nuova password del database** nel menu principale.

Usa la seguente sintassi: `http://<IP/Hostname>:<Port>`. La porta del database predefinita è 27017. Inserisci la password del database primario.
6. Installa gli altri ruoli scegliendo **Aggiungi o rimuovi ruoli** dal menu **Installa/Disinstalla ruoli** e poi i ruoli da installare. Per ciascun ruolo che desideri installare o disinstallare, premi la Barra spaziatrice per selezionare o deselegionare il ruolo e poi premi **Invio** per continuare. Devi confermare la tua scelta, premendo ancora **Invio**, per poi attendere il completamento dell'installazione.



Nota

Ogni ruolo di norma viene installato in pochi minuti. Durante l'installazione, i file richiesti vengono scaricati da Internet. Di conseguenza, l'installazione richiede più tempo se la connessione a Internet è lenta. Se l'installazione si blocca, ripeti la procedura con la appliance.

Puoi visualizzare i ruoli installati e i loro IP, selezionando una delle seguenti opzioni nel menu **Installa/Disinstalla ruoli**:

- **Mostra i ruoli installati in locale** per visualizzare solo i ruoli installati su quella appliance.

- **Mostra tutti i ruoli installati**, per visualizzare tutti i ruoli installati nel tuo ambiente di GravityZone.

Installare Security Server

Nota

Il Security Server sarà disponibile all'utilizzo solo se il codice di licenza lo consente.

Puoi installare il Security Server dall'interfaccia di configurazione della appliance di GravityZone, direttamente sulla appliance di GravityZone o dalla Control Center come appliance indipendente. I vantaggi di installare il Security Server dalla appliance sono:

- Adatto per le implementazioni di GravityZone con una singola appliance con tutti i ruoli.
- Puoi visualizzare e utilizzare Security Server senza dover integrare GravityZone con una piattaforma di virtualizzazione.
- Meno operazioni di impiego da eseguire.

Prerequisiti:

La appliance di GravityZone deve avere il ruolo di Server del database installato o deve essere configurata per connettersi a un database esistente.

Per installare il Security Server dall'interfaccia della appliance:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Seleziona **Installa Security Server**. Apparirà un messaggio di conferma.
4. Premi **Invio** per continuare e attendi la fine dell'installazione.

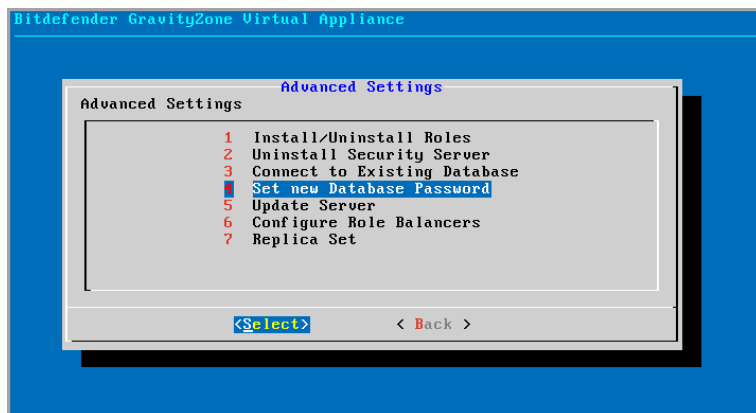
Nota

Puoi disinstallare questo Security Server solo dal menu **Impostazioni avanzate** dell'interfaccia della appliance.

Imposta nuova password del database

Installando il ruolo Server database, è necessario impostare una password per proteggere il database. Nel caso volessi modificarla, impostane una nuova

accedendo a **Impostazioni avanzate e Imposta una nuova password del database** nel menu principale.



Interfaccia console della appliance: opzione Imposta una nuova password del database

Segui le linee guida per impostare una password sicura.

Configurare il Server di aggiornamento

La appliance di GravityZone è configurata in modo predefinito per aggiornarsi da Internet. Se preferisci, puoi impostare le tue appliance installate per aggiornarsi dal server di aggiornamento locale di Bitdefender (l'appliance di GravityZone con il ruolo Server di aggiornamento installato).

Per impostare l'indirizzo del server di aggiornamento:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Seleziona **Server di aggiornamento**.
4. Seleziona **Configura indirizzo aggiornamento**.
5. Inserisci l'indirizzo IP o l'hostname della appliance che esegue il ruolo di Server di aggiornamento. La porta predefinita del Server di aggiornamento è 7074.

Configura balancer ruolo

Per assicurare affidabilità e scalabilità, puoi installare più istanze di determinati ruoli (Server di comunicazione, Console web).

Per assicurare affidabilità e scalabilità, puoi installare più istanze di determinati ruoli (Server Incidenti, Server di comunicazione, Console web).

Ogni istanza del ruolo viene installata su una diversa appliance.

Tutte le istanze di un determinato ruolo devono essere connesse agli altri ruoli tramite un balancer dei ruoli.

La appliance di GravityZone include balancer integrati che puoi installare e utilizzare. Se hai già software o hardware con funzioni di balancer nella tua rete, puoi scegliere di utilizzarli al posto dei balancer integrati.

I balancer dei ruoli integrati non possono essere installati insieme ai ruoli in una appliance di GravityZone.

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Seleziona **Configura balancer ruoli**.
4. Seleziona l'opzione desiderata:
 - **Usa balancer esterni.** Seleziona questa opzione se la tua infrastruttura di rete include già software o hardware con funzioni di balancer che puoi utilizzare. Devi inserire l'indirizzo del balancer per ciascun ruolo che vuoi equilibrare. Usa la seguente sintassi:
`http(s)://<IP/Hostname>:<Porta>`
 - **Usa balancer integrati.** Seleziona questa opzione per installare e usare il software balancer integrato.



Importante

To install multiple instances of the Incidents Server role you may only use the built-in balancer.

5. Seleziona **OK** per salvare le modifiche.

Set di replica

Con questa opzione puoi attivare l'utilizzo di un set di replica del database invece di un'istanza database con un solo server. Questo meccanismo consente di creare più istanze del database in un ambiente GravityZone distribuito, assicurando l'elevata disponibilità del database in caso di fallimento.

! Importante

La replica del database è disponibile solo per le nuove installazioni della appliance di GravityZone a partire dalla versione 5.1.17-441.

Configurare il set di replica

Per iniziare, devi attivare il set di replica sulla prima appliance di GravityZone installata. Poi, potrai aggiungere i membri del set di replica installando il ruolo database nelle altre istanze di GravityZone nello stesso ambiente.

! Importante

- Il set di replica richiede almeno tre membri per funzionare.
- Puoi aggiungere fino a sette istanze del ruolo database come membri del set di replica (limitazione MongoDB).
- Si consiglia di usare un numero dispari di istanze del database. Un numero pari di membri consumerà solo più risorse per gli stessi risultati.

Per consentire la replica del database nel tuo ambiente di GravityZone:

1. Installa il ruolo Server del database nella prima appliance di GravityZone. Per maggiori informazioni, fai riferimento a [«Installa/Disinstalla ruoli»](#) (p. 109).
2. Configura le altre appliance per connettersi alla prima istanza del database. Per maggiori informazioni, fai riferimento a [«Connetti a base di dati esistente»](#) (p. 116).
3. Vai al menu principale della prima appliance, seleziona **Impostazioni avanzate** e poi scegli **Set di replica** per consentirla. Apparirà un messaggio di conferma.
4. Seleziona **Sì** per confermare.
5. Installa il ruolo Server del database in ogni altra appliance di GravityZone.

Non appena completati i passaggi precedenti, tutte le istanze del database inizieranno a lavorare come un set di replica:

- Viene istituita un'istanza primaria, che è l'unica ad accettare operazioni di scrittura.
- L'istanza primaria riporta tutte le modifiche fatte ai suoi set di dati in un registro.
- Le istanze secondarie replicano questo registro e applicano le stesse modifiche ai rispettivi set di dati.
- Quando l'istanza primaria diventa indisponibile, il set di replica eleggerà una delle istanze secondarie come primaria.
- Quando un'istanza primaria non comunica con gli altri membri del set per più di 10 secondi, il set di replica tenterà di selezionare un altro membro per farlo diventare la nuova istanza primaria.

Rimuovere i membri del set di replica

Per rimuovere i membri del set di replica, seleziona **Installa/Disinstalla ruoli e Aggiungi o Rimuovi ruoli** dalla relativa interfaccia della console delle appliance (interfaccia basata su menu) e deseleziona **Server database**.

Nota

Puoi rimuovere un membro del set di replica solo se nella rete sono state installate almeno quattro istanze del database.

Attiva Cluster VPN sicuro

I ruoli di GravityZone hanno diversi servizi interni che comunicano esclusivamente tra loro. Per un ambiente ancora più sicuro, puoi isolare tali servizi creando un Cluster VPN per loro. Se questi servizi sono sulla stessa appliance o su più, allora comunicheranno tramite un canale sicuro.

Importante

- Questa funzionalità richiede un impiego di GravityZone standard, senza alcun strumento personalizzato installato.
- Una volta attivato il cluster, non potrai disattivarlo.

Per proteggere i servizi interni sulle appliance:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Impostazioni avanzate**.

3. Seleziona Attiva **Cluster VPN sicuro**.

Un messaggio ti informa sulle modifiche che saranno apportate.

4. Seleziona **Sì** per confermare e procedi con l'installazione della VPN.

Una volta completata, sarà visualizzato un messaggio di conferma.

D'ora in poi, tutti i ruoli nella appliance vengono installati in modalità protetta e i servizi comunicheranno attraverso l'interfaccia della VPN. Ogni nuova appliance che aggiungi all'ambiente deve aderire al Cluster VPN. Per maggiori informazioni, fai riferimento a [«Connetti a database esistente \(Cluster VPN sicuro\)»](#) (p. 117).

Connetti a base di dati esistente

In un'architettura distribuita di GravityZone, devi installare il ruolo Server database nella prima appliance e configurare tutte le altre appliance per connetterti all'istanza del database esistente. In questo modo, tutte le appliance condivideranno lo stesso database.

Importante

Si consiglia di attivare il Cluster VPN sicuro e connettersi a un database all'interno di tale cluster. Per maggiori informazioni, fai riferimento a:

- [«Attiva Cluster VPN sicuro»](#) (p. 115)
- [«Connetti a database esistente \(Cluster VPN sicuro\)»](#) (p. 117)

Per connettere la appliance a un database di GravityZone all'esterno di un Cluster VPN sicuro:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Seleziona **Connetti a database esistente**.

Nota

Assicurati di impostare una password del database prima di accedere a questa opzione. Se non conosci la password del database, impostane una nuova accedendo a **Impostazioni avanzate e Imposta una nuova password del database** nel menu principale.

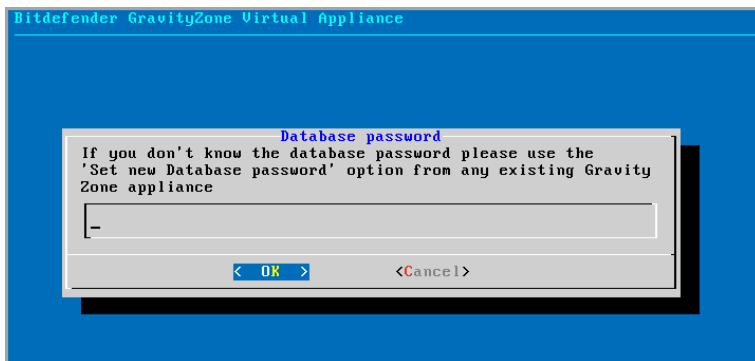
4. Seleziona **Configura indirizzo Server database**.

5. Inserisci l'indirizzo del database, utilizzando la seguente sintassi:

<IP/Hostname>:<Porta>

Specificare la porta è opzionale. La porta standard è 27017.

6. Inserisci la password del database primario.



Interfaccia console appliance: inserire la password del database

7. Seleziona **OK** per salvare le modifiche.

8. Seleziona **Mostra indirizzo Server database** per assicurarti che l'indirizzo sia stato configurato correttamente.

Connetti a database esistente (Cluster VPN sicuro)

Usa questa opzione quando devi estendere il tuo impiego di GravityZone con più appliance e un Cluster VPN sicuro è attivato. In questo modo, la nuova appliance condividerà lo stesso database con l'impiego esistente in una modalità protetta.

Per maggiori informazioni su un Cluster VPN sicuro, fai riferimento a [«Attiva Cluster VPN sicuro»](#) (p. 115).

Prerequisiti

Prima di continuare, assicurati di avere le seguenti informazioni a portata di mano:

- Indirizzo IP Server database
- La password per l'utente **bdadmin** sulla appliance con il ruolo Server database

Connettiti al database

Per connettere la appliance a un database di GravityZone in un Cluster VPN sicuro:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Seleziona **Connetti a database esistente (Cluster VPN sicuro)**.
Sarai informato dei requisiti e delle alternative, se non fossero soddisfatti.
4. Seleziona **OK** per prenderne atto e continuare.
5. Inserisci l'indirizzo IP del Server database nel Cluster VPN sicuro.
6. Inserisci la password per l'utente **bdadmin** sulla appliance con il ruolo Server database.
7. Seleziona **OK** per salvare le modifiche e continuare.

Una volta completato il processo, riceverai un messaggio di conferma. La nuova appliance diventa un membro del cluster e comunicherà con le altre appliance in modo sicuro. Tutte le appliance condivideranno lo stesso database.

Controlla lo stato del Cluster VPN sicuro

Questa opzione è disponibile solo dopo aver precedentemente attivato il Cluster VPN sicuro. Seleziona questa opzione per controllare quali appliance nel tuo impiego di GravityZone non hanno ancora protetto i loro servizi. Potrebbe essere necessario indagare ulteriormente e verificare se le appliance siano online e accessibili.

Configura lingua

Per cambiare la lingua dell'interfaccia di configurazione della appliance:

1. Seleziona **Configura lingua** dal menu principale.
2. Seleziona la lingua dalle opzioni disponibili. Apparirà un messaggio di conferma.



Nota

Potresti dover scorrere verso il basso per visualizzare la tua lingua.

3. Seleziona **OK** per salvare le modifiche.

5.2. Amministrazione licenza

I servizi di sicurezza di GravityZone sono concessi in licenza e venduti separatamente. Ciascun servizio di sicurezza di GravityZone richiede un codice di licenza base valido. Per utilizzare GravityZone deve essere fornito almeno un codice di licenza valido.

Oltre ai servizi di sicurezza base, GravityZone fornisce anche importanti funzionalità di protezione sotto forma di add-on. Ogni add-on viene concesso in licenza con un codice separato e può essere utilizzato solo insieme a una licenza base valida. Se la licenza principale non è valida, visualizzerai le impostazioni delle funzionalità, ma non potrai utilizzarle.

Puoi scegliere di testare GravityZone e decidere se è la soluzione adatta alla tua organizzazione. Per attivare il tuo periodo di valutazione, devi inserire i codici di licenza della versione di prova indicati nell'e-mail di registrazione nella Control Center.



Nota

La Control Center è fornita gratuitamente con qualsiasi servizio di sicurezza di GravityZone.

Per continuare a utilizzare un servizio di sicurezza dopo la scadenza del periodo di prova, devi acquistare un codice di licenza e usarlo per registrare il servizio.

Per acquistare una licenza, contatta un rivenditore Bitdefender o contattaci via e-mail all'indirizzo enterprisesales@bitdefender.com.

I codici di licenza di GravityZone possono essere gestiti dalla pagina **Configurazione > Licenza** nella Control Center. Quando il tuo attuale codice di licenza sta per scadere, nella console comparirà un messaggio per informarti della necessità di rinnovarlo. Per inserire un nuovo codice di licenza o visualizzare i dettagli della licenza attuale, vai alla pagina **Configurazione > Licenza**.

5.2.1. Trovare un rivenditore

I nostri rivenditori ti forniranno tutte le informazioni che ti servono, aiutandoti a scegliere la migliore opzione di licenza per te.

Per trovare un rivenditore di Bitdefender nel tuo paese:

1. Visita la pagina [Trova un partner](#) sul sito web di Bitdefender.
2. Seleziona il paese in cui risiedi per visualizzare le informazioni di contatto dei partner di Bitdefender disponibili.

3. Se non dovessi trovare un rivenditore di Bitdefender nel tuo paese, contattaci via e-mail all'indirizzo enterprisesales@bitdefender.com.

5.2.2. Inserire i tuoi codici di licenza

La registrazione della licenza di GravityZone può essere fatta online oppure offline (quando non è disponibile una connessione a Internet). In entrambi i casi, devi inserire un codice di licenza valido per ciascun servizio di sicurezza che vuoi utilizzare.

Per la registrazione offline, sarà anche necessario il codice di registrazione offline associato al codice di licenza.

Puoi inserire più codici di licenza per lo stesso servizio, ma solo l'ultimo codice inserito sarà attivo.

Per utilizzare la licenza dei servizi di sicurezza GravityZone, per modificare un codice di licenza attuale o inserire un codice separato per un add-on:

1. Accedi alla Control Center usando un account Amministratore azienda.
2. Vai alla pagina **Configurazione > Licenza**.
3. Clicca sul pulsante **+ Aggiungi** nel lato superiore della tabella.
4. Seleziona il tipo di registrazione:
 - **Online**. In questo caso, inserisci un codice di licenza valido nella voce **Codice di licenza**. Il codice di licenza sarà verificato e confermato online.
 - **Offline**, quando non è disponibile una connessione a Internet. In questo caso, devi inserire il codice di licenza e anche il codice di registrazione.

Se il codice di licenza non è valido, viene mostrato un errore di conferma come suggerimento alla voce **Codice di licenza**.

5. Clicca su **Add** (Aggiungi). Il codice di licenza sarà aggiunto alla pagina **Licenza**, dove potrai verificarne i dettagli.
6. Clicca su **Salva** per applicare le modifiche. La Control Center sarà riavviata e dovrai accedere di nuovo per visualizzare le modifiche.



Nota

Puoi utilizzare gli add-on finché esiste una licenza base compatibile e valida. Diversamente, potrai visualizzare le funzionalità, ma non potrai utilizzarle.

5.2.3. Verificare i dettagli della licenza attuale

Per visualizzare i dettagli della tua licenza:

1. Accedi alla Control Center usando un account Amministratore azienda.
2. Vai alla pagina **Configurazione > Licenza**.

Bitdefender GravityZone						
Dashboard						
+ Add ⊗ Reset - Delete ↻ Refre						
Network						
Packages	<input type="checkbox"/>	Key	Service	Status	Expiry Date	Usage
Tasks	<input type="checkbox"/>		Desktops	Active	21 May 2017, 699 ...	0/400 Desktops
Policies	<input type="checkbox"/>		Mailboxes	Active	27 Nov 2015, 158 ...	35/20 Mailboxes
Assignment Rules	<input type="checkbox"/>		Mobile Devices	Active	12 Feb 2020, 1696 ...	1/100 Devices
Reports	<input type="checkbox"/>		Virtual Machines	Active	01 Jul 2017, 740 da...	4/640 CPU cores
Quarantine	<input type="checkbox"/>		Servers	Active	04 Dec 2017, 896 ...	0/15 Servers
Accounts	<input type="checkbox"/>					
User Activity						
Configuration						
Update						
License						

La pagina Licenza

3. Nella tabella, puoi visualizzare maggiori dettagli sui codici di licenza esistenti.
 - Codice di licenza
 - Servizio di sicurezza a cui si applica il codice di licenza
 - Stato codice di licenza



Importante

Per un determinato servizio, può essere attivo un solo codice di licenza alla volta.

- Data di scadenza e periodo restante della licenza




Importante

Alla scadenza della licenza, i moduli di protezione degli agenti installati vengono disattivati. Di conseguenza, gli endpoint non saranno più protetti e non potrai eseguire alcuna attività di scansione. Ogni nuovo agente installato entrerà in un periodo di prova.

- Conteggio utilizzo licenze

5.2.4. Reimpostare il conteggio utilizzo licenze

Puoi trovare maggiori informazioni sul conteggio di utilizzo dei tuoi codici di licenza nella pagina **Licenza**, nella colonna **Utilizzo**.

Se devi aggiornare le informazioni di utilizzo, seleziona il codice di licenza desiderato e clicca sul pulsante  **Reimposta** nel lato superiore della tabella.

5.2.5. Eliminare i codici di licenza

Puoi scegliere di eliminare i codici di licenza non validi o scaduti nella pagina **Licenza**.




Avvertimento

Eliminando un codice di licenza rimuoverai il servizio di sicurezza corrispondente dalla Control Center. Non potrai installare e gestire la protezione offerta da tale servizio sugli endpoint nella tua rete. Tuttavia, gli endpoint saranno protetti finché il codice di licenza è valido.

Se inserisci un nuovo codice di licenza che include il servizio eliminato in precedenza, riattiverai tutte le funzionalità di quel servizio nella Control Center.

Per eliminare un codice di licenza:

1. Accedi alla Control Center usando un account Amministratore azienda.
2. Vai alla pagina **Configurazione > Licenza**.
3. Seleziona il codice di licenza che vuoi rimuovere e clicca sul pulsante  **Elimina** nel lato superiore della tabella.

5.3. Installare la protezione per endpoint

In base alla configurazione delle macchine e all'ambiente di rete, puoi scegliere di installare solo gli agenti di sicurezza o anche utilizzare un **Security Server**. In quest'ultimo caso, devi prima installare il Security Server e poi gli agenti di sicurezza.

Si consiglia di utilizzare il Security Server negli ambienti virtualizzati come Nutanix, VMware o Citrix Xen, o se le macchine hanno risorse hardware limitate.



Importante

Solo Bitdefender Endpoint Security Tools e Bitdefender Tools supportano la connessione al Security Server. Per maggiori informazioni, fai riferimento a [«Architettura di GravityZone»](#) (p. 10).

5.3.1. Installare Security Server

Security Server è una macchina virtuale dedicata che deduplica e centralizza la maggior parte delle funzionalità antimalware dei relativi client, comportandosi come un server di scansione.

L'impiego del Security Server è specifico per l'ambiente in cui è installato. Le procedure di installazione sono qui descritte:

- [Security Server per VMware NSX](#)
- [Security Server multipiattaforma o per VMware vShield](#)
- [Security Server per Amazon EC2](#)
- [Security Server per Microsoft Azure](#)

Installare Security Server for VMware NSX

Negli ambienti VMware NSX, devi impiegare il servizio di Bitdefender in ciascun cluster da proteggere. La appliance appositamente creata sarà impiegata automaticamente su tutti gli host nel cluster. Tutte le virtual machine in un host vengono connesse automaticamente tramite Guest Introspection all'istanza Security Server installata su tale host.

L'impiego del Security Server deve essere eseguito esclusivamente dal vSphere Web Client.

Per installare il servizio di Bitdefender:

1. Accedi al vSphere Web Client.
2. Vai in **Rete e sicurezza > Installazione** e clicca sulla scheda **Impieghi servizio**.
3. Clicca sul pulsante **Nuovo servizio di impiego** (l'icona con il segno più). Si aprirà la finestra di configurazione.
4. Seleziona **Guest Introspection** e clicca su **Continua**.
5. Seleziona il datacenter e i cluster su cui vuoi impiegare il servizio, e clicca su **Continua**.
6. Seleziona la rete di archiviazione e gestione, clicca su **Continua** e poi su **Termina**.
7. Ripeti i passaggi dal 3 al 6, questa volta scegliendo **servizio di Bitdefender**.

Prima di continuare con l'installazione, assicurati di avere una connessione di rete tra la rete selezionata e GravityZone Control Center.

Una volta installato il servizio di Bitdefender, il Security Server sarà impiegato automaticamente su tutti gli host ESXi nei cluster selezionati.



Avvertimento

Affinché i servizi funzionino correttamente, è molto importante installarli in quest'ordine: prima Guest Introspection e poi Bitdefender, e non entrambi contemporaneamente.



Nota

Per maggiori informazioni sull'aggiunta di servizi partner a NSX, fai riferimento al [VMware NSX Documentation Center](#).

Se selezioni **Specificato nell'host** per la gestione di archiviazione e rete, controlla che l'Agente VM sia impostato sugli host sia per la Guest Introspection che per i servizi di Bitdefender.

Il Security Server ha determinati requisiti che dipendono dal numero di virtual machine che deve proteggere. Per importare la configurazione hardware predefinita del Security Server:

1. Accedi al VMware vSphere Web Client.
2. Vai a **Host e Cluster**.
3. Seleziona il cluster in cui è installato Security Server, quindi la scheda **Oggetti correlati > Virtual Machine**.
4. Disattiva la appliance di **Bitdefender**.
5. Fai clic con il pulsante destro sul nome della appliance e seleziona **Modifica impostazioni...** nel menu contestuale.
6. Nella tabella **Virtual Hardware**, imposta i valori di Processore e RAM in base alle tue esigenze e clicca su **OK** per salvare le modifiche.
7. Riattiva la appliance.



Nota

Per fare l'upgrade da VMware vShield a NSX, fai riferimento a questo [articolo della KB](#).

Installare la multiplatforma del Security Server o per VMware vShield

1. [Connettiti alla piattaforma di virtualizzazione](#)

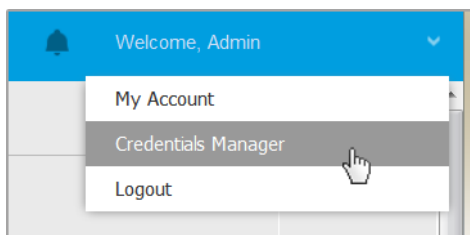
2. Installa il Security Server sugli host

Connessione alla piattaforma di virtualizzazione

Per accedere all'infrastruttura virtualizzata integrata con la Control Center, devi fornire le tue credenziali utente per ciascun sistema server di virtualizzazione disponibile. La Control Center utilizza le tue credenziali per connettersi all'infrastruttura virtualizzata, mostrando solo le risorse a cui hai accesso (come definito nel vCenter Server).

Per specificare le credenziali per connettersi ai sistemi del server di virtualizzazione:

1. Clicca sul tuo nome utente nell'angolo in alto a destra della pagina e seleziona **Credentials Manager**.



Il menu Rete > Pacchetti

2. Vai alla scheda **Ambiente virtuale**.
3. Specifica le necessarie credenziali di autenticazione.
 - a. Seleziona un server dal menu corrispondente.



Nota

Se il menu non è disponibile, non è ancora stata configurata alcuna integrazione o tutte le credenziali necessarie sono già state configurate.

- b. Inserisci il tuo nome utente e la password, oltre a una apposita descrizione.
- c. Clicca sul pulsante **+ Aggiungi**. Il nuovo set di credenziali viene visualizzato nella tabella.

i Nota

Se non hai specificato le tue credenziali di autenticazione, dovrai inserirle quando cercherai di esplorare l'inventario di ogni sistema vCenter Server. Una volta inserite le tue credenziali, saranno salvate nel tuo Credentials Manager in modo che non dovrai più reinserirle la volta successiva.

Installare il Security Server sugli host

Devi installare il Security Server sugli host come segue:

- Negli ambienti VMware con vShield Endpoint, devi installare la relativa appliance su ciascun host da proteggere. Tutte le virtual machine in un host vengono connesse automaticamente tramite vShield Endpoint all'istanza del Security Server installata su tale host.
- Negli ambienti Citrix, devi installare il Security Server su ogni host che vuoi proteggere con HVI, tramite un'attività di installazione in remoto.
- Negli ambienti Nutanix Prism Element, devi installare il Server di sicurezza su ciascun host, tramite un'attività di installazione remota.
- In tutti gli altri ambienti, devi installare il Security Server su uno o più host in modo da accogliere il numero di virtual machine da proteggere. Devi considerare il numero di macchine virtuali protette, le risorse disponibili per il Security Server sugli host, oltre alla connettività di rete tra il Security Server e le macchine virtuali protette. L'agente di sicurezza installato sulle macchine virtuali si connette al Security Server su TCP/IP, utilizzando i dettagli configurati all'installazione o tramite una policy.

Se la Control Center è integrata con vCenter Server, XenServer e Nutanix Prism Element puoi impiegare automaticamente il Security Server sugli host della Control Center. Puoi anche scaricare i pacchetti del Security Server per l'installazione indipendente dalla Control Center.

i Nota

Per gli ambienti VMware con vShield Endpoint, puoi impiegare il Security Server sugli host esclusivamente tramite attività di installazione.


Installazione locale

In tutti gli ambienti virtualizzati che non sono integrati con la Control Center, devi installare manualmente il Security Server sugli host, utilizzando un pacchetto di

installazione. Il pacchetto Security Server è disponibile al download dalla Control Center in diversi formati, compatibili con le principali piattaforme di virtualizzazione.

Scaricare i pacchetti di installazione di Security Server

Per scaricare i pacchetti di installazione di Security Server:

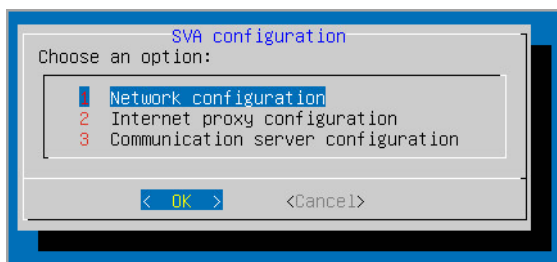
1. Vai alla pagina **Rete e Pacchetti**.
2. Seleziona il pacchetto Security Server standard.
3. Clicca sul pulsante  **Scarica** nel lato superiore della tabella e seleziona il tipo di pacchetto nel menu.
4. Salva il pacchetto selezionato nella posizione desiderata.

Impiegare i pacchetti di installazione di Security Server

Una volta ottenuto il pacchetto di installazione, impiegalo nell'host utilizzando lo strumento di impiego di virtual machine preferito.

Dopo l'impiego, configura il Security Server come segue:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client). In alternativa, puoi anche connetterti alla appliance via SSH.
2. Accedi utilizzando le credenziali predefinite.
 - Nome utente: `root`
 - Password: `sve`
3. Esegui il comando `sva-setup`. Accederai all'interfaccia di configurazione della appliance.



Interfaccia configurazione di Security Server (menu principale)

Per esplorare i menu e le opzioni, usa il tasto `Tab` e le frecce. Per selezionare un'opzione specifica, premi `Invio`.

4. Configura le impostazioni di rete.

Il Security Server utilizza il protocollo TCP/IP per comunicare con gli altri componenti di GravityZone. Puoi configurare la appliance per ottenere automaticamente le impostazioni di rete dal server DHCP oppure puoi configurare le impostazioni di rete manualmente, come descritto qui:

- a. Dal menu principale, seleziona **Configurazione di rete**.
- b. Seleziona l'interfaccia di rete.
- c. Seleziona la modalità di configurazione IP:
 - **DHCP**, se vuoi che il Security Server ottenga automaticamente le impostazioni di rete dal server DHCP.
 - **Statico**, se un server DHCP è assente o se è stata fatta una prenotazione IP da parte della appliance sul server DHCP. In questo caso, devi configurare manualmente le impostazioni di rete.
 - i. Inserisci l'hostname, l'indirizzo IP, la maschera di rete, il gateway, i server DND nei campi corrispondenti.
 - ii. Seleziona **OK** per salvare le modifiche.



Nota

Se sei connesso a una appliance tramite un client SSH, modificando le impostazioni di rete la tua sessione sarà conclusa immediatamente.

5. Configura le impostazioni del proxy.

Se nella rete viene usato un server proxy, devi fornire le sue informazioni, in modo che Security Server possa comunicare con GravityZone Control Center.



Nota

Sono supportati solo proxy con autenticazione base.

- a. Dal menu principale, seleziona **Configurazione proxy Internet**.
- b. Inserisci l'hostname, il nome utente, la password e il dominio nei campi corrispondenti.
- c. Seleziona **OK** per salvare le modifiche.

6. Configura l'indirizzo del server di comunicazione.
 - a. Dal menu principale, seleziona **Configurazione server di comunicazione**.
 - b. Inserisci l'indirizzo del Server di comunicazione, incluso il numero della porta 8443, usando il seguente formato:

```
https://Communication-Server-IP:8443
```

In alternativa, puoi usare il nome dell'host del Server di comunicazione, invece dell'indirizzo IP.
 - c. Seleziona **OK** per salvare le modifiche.

Installazione remota

La Control Center ti consente di installare in remoto il Security Server sugli host visibili, utilizzando le attività di installazione.


Per installare il Security Server in remoto su uno o più host:

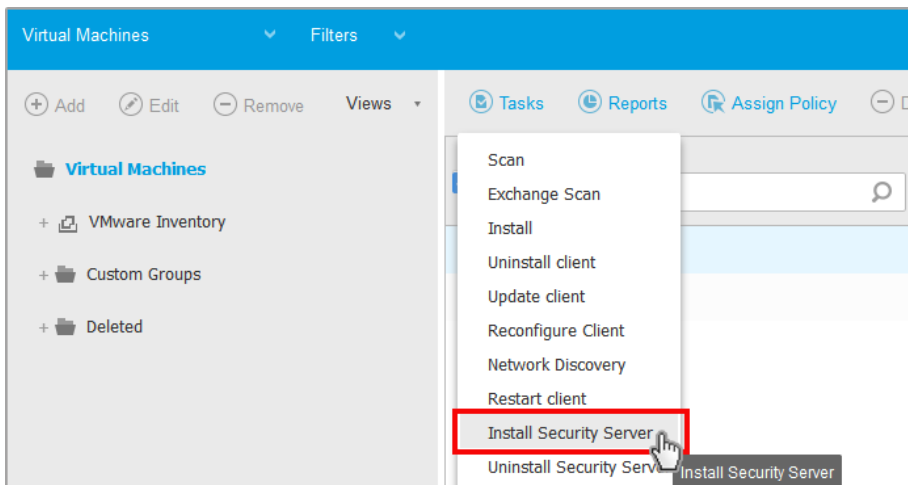
1. Vai alla pagina **Rete**.
2. Seleziona **Macchine virtuali** dal selettore del servizio.
3. Esplora l'inventario VMware, Citrix e Nutanix e seleziona le caselle corrispondenti agli host o contenitori desiderati (Nutanix Prism, vCenter Server, XenServer o data center). Per una selezione rapida, puoi selezionare direttamente il contenitore root (Nutanix Inventory, VMware Inventory o Citrix Inventory). Potrai selezionare gli host individualmente dalla procedura guidata dell'installazione.



Nota

Non puoi selezionare gli host da cartelle diverse.

4. Clicca sul pulsante  **Attività** nel lato superiore della tabella e seleziona **Installa Security Server** nel menu. Verrà mostrata la finestra **Installazione del Security Server**.



Installare il Security Server dal menu Attività

5. Seleziona gli host su cui vuoi installare le istanze del Security Server.
6. Seleziona le impostazioni di configurazione che vuoi utilizzare.



Importante

L'uso di impostazioni comuni mentre si impiegano più istanze del Security Server contemporaneamente è necessario che gli host condividano la stessa archiviazione, abbiano i propri indirizzi IP assegnati da un server DHCP e facciano parte della stessa rete.

Scegliendo di configurare ciascun Security Server in maniera differente, potrai definire le impostazioni desiderate per ciascun host nel prossimo passaggio della procedura guidata. I passaggi descritti di seguito sono validi nel caso in cui si utilizza l'opzione **Configura ogni Security Server**.

7. Clicca su **Avanti**.
8. Inserisci un nome specifico per il Security Server.
9. Per gli ambienti VMware, seleziona il contenitore in cui desideri includere il Security Server nel menu **Impiega container**.
10. Seleziona l'archivio di destinazione.

11. Seleziona il tipo di disco fornito. Si consiglia di impiegare la appliance utilizzando thick disk provisioning.



Importante

Se utilizzi thin disk provisioning e lo spazio su disco nel datastore è esaurito, il Security Server si bloccherà e, di conseguenza, l'host resterà privo di protezione.

12. Configura l'allocazione delle risorse di memoria e processore in base al tasso di consolidamento della VM sull'host. Seleziona **Basso**, **Medio** o **Alto** per caricare le impostazioni di allocazione delle risorse consigliate o **Manuale** per configurare manualmente l'allocazione delle risorse.

13. Devi impostare una password amministrativa per la console del Security Server. L'impostazione di una password amministrativa sostituisce la password principale predefinita ("sve").

14. Imposta il fuso orario della appliance.

15. Seleziona il tipo di configurazione di rete per la rete di Bitdefender. L'indirizzo IP del Security Server non deve cambiare nel tempo, in quanto viene utilizzato dagli agenti Linux per la comunicazione.

Se scegli di utilizzare DHCP, assicurati di configurare il server DHCP per riservare un indirizzo IP per la appliance.

Se scegli statico, devi inserire l'indirizzo IP, la subnet mask, il gateway e il DNS.

16. Seleziona la rete vShield e inserisci le credenziali di vShield. L'etichetta predefinita per la rete vShield è `vmervice-vshield-pg`.

17. Clicca su **Salva**.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.



Nota

Per fare l'upgrade da VMware vShield a NSX, fai riferimento a questo [articolo della KB](#).



Importante

Installare il Security Server su Nutanix tramite l'attività remota potrebbe fallire se il cluster di Prism Element viene registrato in Prism Central o a causa di un altro motivo. In queste situazioni, si consiglia di eseguire un impiego manuale del Security Server. Per maggiori dettagli, fai riferimento a questo [articolo della KB](#).

Installare Security Server for Amazon EC2

Puoi usare il Security Server per proteggere le tue istanze Amazon EC2 nel seguente modo:

- Configura il Security Server installato nella tua rete locale per comunicare con le istanze di Amazon EC2. Inoltre, potrai usare le tue risorse locali, fisiche o virtuali, per proteggere anche l'inventario Amazon EC2.
- Installa una o più istanze del Security Server nel tuo ambiente Amazon EC2, in base alle tue esigenze. In questo caso, segui la procedura descritta in questo [articolo della KB](#).



Importante

- Affinché la comunicazione fra le tue macchine EC2 e le istanze del Server di sicurezza installate nel tuo inventario Amazon EC2 funzioni, devi configurare correttamente le tue connessioni ad Amazon VPC (Virtual Private Cloud) e Amazon VPN. Per maggiori informazioni, fai riferimento alla [documentazione di Amazon VPC](#).
- Consigliamo di installare il Security Server nella stessa regione di Amazon EC2 con le istanze che vuoi proteggere.

La modalità di scansione predefinita per le istanze EC2 è la Scansione locale (tutti i contenuti di sicurezza vengono memorizzati sull'agente di sicurezza installato e la scansione viene eseguita localmente sulla macchina). Se vuoi esaminare le tue istanze EC2 con un Security Server, devi configurare il pacchetto di installazione dell'agente di sicurezza e la policy applicata di conseguenza.

Installare il Security Server per Microsoft Azure

Puoi usare il Security Server per proteggere le tue virtual machine di Microsoft Azure nel seguente modo:

- Configura il Security Server installato nella tua rete locale per comunicare con le virtual machine di Microsoft Azure. Inoltre, potrai usare le tue risorse locali, fisiche o virtuali, per proteggere anche l'inventario Microsoft Azure.
- Installa una o più istanze del Security Server nel tuo ambiente Microsoft Azure, in base alle tue esigenze. In questo caso, segui la procedura descritta in questo [articolo della KB](#).



Importante

- Affinché la comunicazione fra le tue virtual machine di Microsoft Azure e le istanze del Server di sicurezza installate nel tuo inventario Microsoft Azure funzioni, devi configurare correttamente la tua subnet/rete virtuale. Per maggiori dettagli, fai riferimento alla [documentazione di Microsoft Azure Virtual Network](#).
- Consigliamo di installare il Security Server nella stessa regione di Microsoft Azure con le virtual machine che vuoi proteggere.

La modalità di scansione predefinita per le virtual machine di Microsoft Azure è la Scansione locale (tutti contenuti di sicurezza vengono memorizzati sull'agente di sicurezza installato e la scansione viene eseguita localmente sulla macchina). Se vuoi esaminare le tue virtual machine di Microsoft Azure con un Security Server, devi configurare il pacchetto di installazione dell'agente di sicurezza e la policy applicata di conseguenza.

5.3.2. Installare gli agenti di sicurezza

Per proteggere i tuoi endpoint fisici e virtuali, devi installare un agente di sicurezza in ciascuno di loro. Oltre a gestire la protezione sull'endpoint locale, l'agente di sicurezza comunica anche con la Control Center per ricevere i comandi dell'amministratore e inviare i risultati delle sue azioni.

Per ulteriori informazioni sugli agenti di sicurezza, fai riferimento a [«Agenti di sicurezza» \(p. 12\)](#).

Su macchine Windows e Linux, l'agente di sicurezza può avere due ruoli e puoi installarlo come segue:

1. Come un semplice agente di sicurezza per i tuoi endpoint.
2. Come un [relay](#), agendo come un agente di sicurezza e anche come server di comunicazione, aggiornamento e proxy per altri endpoint nella rete.

Puoi installare gli agenti di sicurezza su endpoint fisici e virtuali [eseguendo i pacchetti di installazione in locale](#) o [eseguendo le attività di installazione in remoto](#) dalla Control Center.

È molto importante leggere e seguire con attenzione le istruzioni per preparare l'installazione.

In modalità normale, gli agenti di sicurezza hanno un'interfaccia utente minimale. Consente solo agli utenti di verificare lo stato della protezione ed eseguire attività

di sicurezza base (aggiornamenti e scansioni), senza fornire accesso alle impostazioni.

Se attivato dall'amministratore di rete tramite pacchetto di installazione e policy di sicurezza, l'agente di sicurezza può anche essere eseguito in [modalità utente esperto](#) sugli endpoint Windows, consentendo all'utente dell'endpoint di visualizzare e modificare le impostazioni della policy. Tuttavia, l'amministratore della Control Center può sempre controllare quali impostazioni della policy applicare, prevalendo sulla modalità utente esperto.

Di norma, la lingua dell'interfaccia utente sugli endpoint protetti è impostata al momento dell'installazione in base a quella del proprio account di GravityZone.

Su Mac, la lingua dell'interfaccia utente è impostata al momento dell'installazione in base a quella del sistema operativo dell'endpoint. Su Linux, l'agente di sicurezza non ha un'interfaccia utente localizzata.

Per installare l'interfaccia utente in un'altra lingua su determinati endpoint Windows, puoi creare un pacchetto di installazione e impostare la lingua preferita nelle sue opzioni di configurazione. Questa opzione non è disponibile per endpoint Mac e Linux. Per maggiori informazioni sulla creazione dei pacchetti di installazione, fai riferimento a [«Creare i pacchetti di installazione»](#) (p. 137).

Preparazione all'installazione

Prima dell'installazione, segui questi passaggi preparatori per assicurarti che tutto vada bene:

1. Assicurati che gli endpoint di destinazione soddisfino i [requisiti di sistema minimi](#). Per alcuni endpoint, potresti dover installare l'ultimo pacchetto di servizio del sistema operativo disponibile oppure liberare spazio sul disco rigido. Compila un elenco di endpoint che non soddisfano i requisiti necessari in modo da escluderli dalla gestione.
2. Disinstalla (non solo disattiva) ogni antimalware o software di sicurezza Internet esistente dagli endpoint di destinazione. Eseguire l'agente di sicurezza in contemporanea con un altro software di sicurezza su un endpoint potrebbe influenzare il suo funzionamento e causare parecchi problemi al sistema.

Molti programmi di sicurezza incompatibili vengono rilevati e rimossi automaticamente al momento dell'installazione.

Per maggiori informazioni e per controllare l'elenco dei software di sicurezza rilevati da Bitdefender Endpoint Security Tools per gli attuali sistemi operativi Windows, fai riferimento a [questo articolo della KB](#).



Importante

Se vuoi impiegare l'agente di sicurezza su un computer con Bitdefender Antivirus for Mac 5.X, devi prima rimuovere quest'ultimo manualmente. Per dei passaggi di guida, fai riferimento a [questo articolo della KB](#).

3. L'installazione richiede privilegi di amministratore e accesso a Internet. Se gli endpoint di destinazione sono nel dominio di Active Directory, devi usare le credenziali di amministratore del dominio per un'installazione in remoto. Altrimenti, assicurati di avere le credenziali necessarie a portata di mano per tutti gli endpoint.
4. Gli endpoint deve avere una connessione di rete alla appliance di GravityZone.
5. Si consiglia di usare un indirizzo IP statico per il server relay. Se non imposti un IP statico, utilizza l'hostname della macchina.
6. Impiegando l'agente tramite un relay Linux, devono essere soddisfatte le seguenti condizioni aggiuntive:
 - L'endpoint relay deve aver installato il pacchetto Samba (`smbclient`) in versione 4.1.0 o superiore, e il comando `net` binario per impiegare gli agenti Windows.



Nota

Il comando/binario `net` viene generalmente consegnato con i pacchetti `samba-client` e / o `samba-common`. In alcune distribuzioni Linux (come CentOS 7.4), il comando `net` viene installato unicamente quando si installa la suite completa di Samba (Common + Client + Server). Assicurati che il tuo endpoint relay abbia il comando `net` disponibile.

- Gli endpoint Windows bersaglio devono avere le opzioni Condivisione amministrativa e Condivisione rete attivate.
 - Gli endpoint Linux e Mac di destinazione devono avere SSH attivato.
7. A partire da macOS High Sierra (10.13), dopo aver installato Endpoint Security for Mac manualmente o in remoto, agli utenti viene chiesto di approvare le estensioni del kernel di Bitdefender sui propri computer. Fin quando l'utente non approva le estensioni del kernel di Bitdefender, alcune funzionalità di Endpoint Security for Mac non funzioneranno. Per eliminare l'intervento dell'utente, puoi pre-approvare le estensioni del kernel di Bitdefender inserendole nella whitelist usando uno strumento di Mobile Device Management.

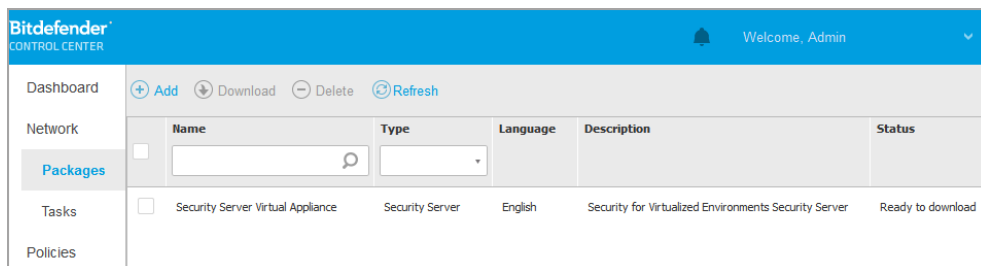
8. Impiegando l'agente in un inventario Amazon EC2, configura i gruppi di sicurezza associati con le istanze che vuoi proteggere in **Dashboard > Rete & Sicurezza** di Amazon EC2, nel seguente modo:
 - Per un'installazione remota, consenti l'accesso SSH* dall'istanza EC2.
 - Per l'installazione locale, consenti l'accesso SSH* e RDP (Remote Desktop Protocol) dal computer da cui ti connetti.

* Per un'installazione remota su istanze Linux devi consentire l'accesso SSH usando nome utente e password.
9. Quando si impiega l'agente in un inventario Microsoft Azure:
 - La virtual machine bersaglio deve essere nella stessa rete virtuale della appliance di GravityZone.
 - La virtual machine bersaglio deve essere nella stessa rete virtuale con un relay, che comunica con la appliance di GravityZone quando quest'ultima si trova in un'altra rete.

Installazione locale

Un modo per installare l'agente di sicurezza su un endpoint è eseguire localmente un pacchetto di installazione.

Puoi creare e gestire i pacchetti di installazione nella pagina **Rete > Pacchetti**.



Name	Type	Language	Description	Status
<input type="checkbox"/> [Empty field]	[Empty dropdown]	[Empty dropdown]	[Empty field]	[Empty field]
<input type="checkbox"/> Security Server Virtual Appliance	Security Server	English	Security for Virtualized Environments Security Server	Ready to download

La pagina dei pacchetti

Una volta che il primo client è stato installato, sarà utilizzato per rilevare altri endpoint nella stessa rete, basati sul meccanismo di Network Discovery. Per maggiori informazioni su Network Discovery, fai riferimento a [«Come funziona Network Discovery»](#) (p. 154).

Per installare localmente l'agente di sicurezza su un endpoint, segui questi passaggi:

1. [Crea un pacchetto di installazione](#) in base alle tue necessità.

**Nota**

Questo passaggio non è obbligatorio se nel tuo account è già stato creato un pacchetto di installazione per la rete.

2. [Scarica il pacchetto di installazione](#) sull'endpoint di destinazione.
In alternativa puoi [inviare i link per scaricare il pacchetto di installazione via e-mail](#) a diversi utenti nella tua rete.
3. [Esegui il pacchetto di installazione](#) sull'endpoint di destinazione.

Creare i pacchetti di installazione

Per creare un pacchetto di installazione:

1. Connettiti e accedi alla Control Center.
2. Vai alla pagina **Rete e Pacchetti**.
3. Clicca sul pulsante **+Aggiungi** nel lato superiore della tabella. Apparirà la finestra di configurazione.

The screenshot shows a configuration window titled "General". It contains the following elements:

- Name:** * [Empty text box]
- Description:** [Empty text box]
- Language:** English (dropdown menu)
- Modules:**
 - Antimalware
 - Advanced Threat Control
 - Advanced Anti-Exploit
 - Firewall
 - Network Protection
 - Content Control
 - Network Attack Defense
 - Device Control
 - Power User

Crea pacchetti - Opzioni

4. Inserisci un nome indicativo e una descrizione per il pacchetto di installazione che vuoi creare.
5. Dal campo **Lingua**, seleziona la lingua desiderata per l'interfaccia del client.

**Nota**

Questa opzione è disponibile solo per i sistemi operativi Windows.

6. Seleziona i moduli della protezione che desideri installare.

**Nota**

Saranno installati solo i moduli supportati per ciascun sistema operativo. Per maggiori informazioni, fai riferimento a «[Agenti di sicurezza](#)» (p. 12).

7. Seleziona il ruolo dell'endpoint di destinazione:

- **Relay**, per creare il pacchetto per un endpoint con ruolo di relay. Per maggiori informazioni, fai riferimento a «[Relay](#)» (p. 14)
- **Server cache gestione patch**, per rendere il Relay un server interno per la distribuzione delle patch dei software. Questo ruolo viene mostrato quando si seleziona il ruolo Relay. Per maggiori informazioni, fai riferimento a «[Server caching patch](#)» (p. 14)
- **Protezione Exchange**, per installare i moduli di protezione per i Microsoft Exchange Server, tra cui antimalware, antispam, filtro di contenuti e allegati per il traffico e-mail di Exchange e scansione antimalware a richiesta dei database di Exchange. Per maggiori informazioni, fai riferimento a «[Installare la protezione di Exchange](#)» (p. 166).

8. **Rimuovi concorrenti**. Si consiglia di mantenere selezionata questa casella per rimuovere automaticamente ogni software di sicurezza incompatibile mentre l'agente di Bitdefender viene installato sull'endpoint. Deselezionando questa opzione, l'agente di Bitdefender si installerà accanto alla soluzione di sicurezza esistente. Puoi rimuovere manualmente la soluzione di sicurezza installata precedentemente in un secondo momento, a tuo rischio e pericolo.

**Importante**

Eseguire l'agente di Bitdefender in contemporanea con un altro software di sicurezza su un endpoint potrebbe influenzare il suo funzionamento e causare parecchi problemi al sistema.

9. **Mod. di scansione.** Seleziona la tecnologia di scansione che si adatta meglio all'ambiente della tua rete e alle risorse dei tuoi endpoint. Puoi definire la modalità di scansione scegliendo una delle seguenti tipologie:

- **Automatica.** In questo caso, l'agente di sicurezza rileverà automaticamente la configurazione dell'endpoint e adatterà la tecnologia di scansione di conseguenza:
 - Scansione centrale nel cloud pubblico o privato (con Security Server) e fallback su scansione ibrida (motori leggeri), per computer fisici con prestazioni hardware limitate e macchine virtuali. Questo caso richiede almeno un Security Server impiegato nella rete.
 - Scansione locale (con motori completi) per computer fisici con prestazioni hardware elevate.
 - Scansione locale per istanze EC2 e virtual machine Microsoft Azure.

Nota

I computer con prestazioni limitate sono sistemi con una frequenza della CPU inferiore a 1,5 GHz o meno di 1 GB di memoria RAM.

- **Personalizzata.** In questo caso, puoi configurare la modalità di scansione scegliendo tra diverse tecnologie di scansione per macchine fisiche e virtuali:
 - Scansione centrale in cloud pubblico o privato (con Security Server), che può passare* a una scansione ibrida (con motori leggeri) o una scansione locale (con motori completi)
 - Scansione ibrida (con motori leggeri)
 - Scansione locale (con motori completi)

La modalità di scansione predefinita per le istanze EC2 è la Scansione locale (tutti contenuti di sicurezza vengono memorizzati sull'agente di sicurezza installato e la scansione viene eseguita localmente sulla macchina). Se vuoi esaminare le tue istanze EC2 con un Security Server, devi configurare il pacchetto di installazione dell'agente di sicurezza e la policy applicata di conseguenza.

La modalità di scansione predefinita per le virtual machine di Microsoft Azure è la Scansione locale (tutti contenuti di sicurezza vengono memorizzati sull'agente di sicurezza installato e la scansione viene eseguita localmente sulla macchina). Se vuoi esaminare le tue virtual machine di Microsoft Azure

con un Security Server, devi configurare il pacchetto di installazione dell'agente di sicurezza e la policy applicata di conseguenza.

* Quando si usa un doppio motore di scansione, se il primo motore non è disponibile, sarà utilizzato quello di riserva. Il consumo di risorse e l'utilizzo della rete sarà basato sui motori utilizzati.

Per maggiori informazioni sulle tecnologie di scansione disponibili, fai riferimento a «[Motori di scansione](#)» (p. 3)





10. **Impiega endpoint con vShield quando viene rilevato un ambiente VMware integrato con vShield.** Questa opzione può essere utilizzata quando il pacchetto di installazione viene impiegato su una virtual machine da un ambiente VMware integrato con vShield. In questo caso, VMware vShield Endpoint sarà installato sulla macchina bersaglio al posto dell'agente di sicurezza di Bitdefender.



Importante

Questa opzione è solo gli impieghi in remoto, non le installazioni locali. Quando si installa localmente in ambiente VMware integrato con vShield, hai la possibilità di scaricare il pacchetto integrato vShield.

11. Personalizzando i motori di scansione, usando una scansione in cloud pubblico o privato (Security Server), ti sarà richiesto di selezionare i Security Server installati in locale, se desideri usare e configurare la loro priorità nella sezione **Assegnazione Security Server**:

- a. Clicca sull'elenco Security Server) nell'intestazione della tabella. Viene mostrato l'elenco dei Security Server rilevati.
- b. Seleziona un'entità.
- c. Clicca sul pulsante  **Aggiungi** dall'intestazione della colonna **Azioni**.
Il Security Server viene aggiunto all'elenco.
- d. Segui gli stessi passaggi per aggiungere i server di sicurezza, se disponibili. In questo caso, puoi configurare la loro priorità utilizzando le frecce  su e  giù, disponibili sul lato destro di ciascuna entità. Quando il primo Security Server non è disponibile, sarà usato il successivo e così via.
- e. Per eliminare un'entità dall'elenco, clicca sul pulsante  **Elimina** corrispondente nel lato superiore della tabella.

Puoi scegliere di cifrare la connessione al Security Server selezionando l'opzione **Usa SSL**.

12. **Varie.** Puoi configurare le seguenti opzioni su diversi tipi di file dagli endpoint di destinazione:

- **Invia crash dump.** Seleziona questa opzione per inviare i file di dump della memoria ai laboratori di Bitdefender per l'analisi, se l'agente di sicurezza dovesse bloccarsi. I dump dei blocchi aiuteranno i nostri ingegneri a scoprire le cause del problema, impedendo che si verifichi nuovamente. Non sarà inviata alcuna informazione personale.
- **Invia file messi in quarantena a Bitdefender Labs ogni (ore).** Di norma, i file messi in quarantena vengono inviati automaticamente ai laboratori di Bitdefender ogni ora. Puoi modificare l'intervallo di tempo in cui vengono inviati i file messi in quarantena. I file campioni saranno analizzati dai ricercatori antimalware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.
- **Invia file eseguibili sospetti a Bitdefender.** Seleziona questa opzione per inviare ai laboratori di Bitdefender tutti i file che sembrano poco affidabili o con un comportamento sospetto per ulteriori analisi.

13. Seleziona **Esamina prima dell'installazione**, se vuoi assicurarti che le macchine siano pulite prima di installarci il client. Una scansione veloce nel cloud sarà eseguita sulle macchine bersaglio prima di iniziare l'installazione.

14. Bitdefender Endpoint Security Tools viene installato nella cartella di installazione predefinita. Seleziona **Usa percorso di installazione personalizzato**, se vuoi installare Bitdefender in un'altra posizione. Se la cartella indicata non esiste, sarà creata durante l'installazione.

- Su Windows, il percorso predefinito è `C:\Program Files\`. Per installare Bitdefender Endpoint Security Tools in un percorso personale, usa le convenzioni di Windows quando inserisci il percorso. Per esempio, `D:\folder`.
- Su Linux, Bitdefender Endpoint Security Tools viene installato in maniera predefinita nella cartella `/opt`. Per installare l'agente di Bitdefender in un percorso personale, usa le convenzioni di Linux quando inserisci il percorso. Per esempio, `/folder`.

Bitdefender Endpoint Security Tools non supporta l'installazione nei seguenti percorsi personali:

- Qualsiasi percorso che non inizia con la barra (/). L'unica eccezione è la posizione di Windows %PROGRAMFILES%, che l'agente di sicurezza interpreta come la cartella predefinita di Linux opt.
- Qualsiasi percorso che sia in /tmp o /proc.
- Qualsiasi percorso che contenga i seguenti caratteri speciali: \$, !, *, ?, ", \, ` , \, (,), [,], {, }.
- L'indicatore systemd (%).

Su Linux, l'installazione in un percorso predefinito richiede glibc 2.21 o superiore.



Importante

Nell'usare un percorso personalizzato, assicurati di avere il giusto pacchetto di installazione per ciascun sistema operativo.

15. Se lo desideri, puoi impostare una password per impedire agli utenti di rimuovere la protezione. Seleziona **Imposta password di disinstallazione** e inserisci la password desiderata nei campi corrispondenti.

16. Se gli endpoint di destinazione sono nell'inventario di rete nei **Gruppi personalizzati**, puoi scegliere di spostarli subito in una cartella specifica, subito dopo il completamento dell'impiego dell'agente di sicurezza.

Seleziona **Usa cartella personalizzata** e scegli una cartella nella tabella corrispondente.

17. Nella sezione **Gestore**, scegli l'entità a cui gli endpoint di destinazione si connettono per installare e aggiornare il client:

- **Appliance di GravityZone**, quando gli endpoint si connettono direttamente alla appliance di GravityZone.

In questo caso, puoi anche definire:

- Un Server di comunicazione personale inserendo il suo IP o nome dell'host, se necessario.
- Le impostazioni proxy, se gli endpoint di destinazione comunicano con la appliance di GravityZone tramite proxy. In questo caso, seleziona **Usa proxy per la comunicazione** e inserisci le impostazioni proxy richieste nei campi sottostanti.

- **Relay di sicurezza endpoint**, se vuoi connettere gli endpoint a un client relay installato nella tua rete. Tutte le macchine con ruolo di relay rilevate nella tua rete compariranno nella tabella mostrata sotto. Seleziona la macchina relay che desideri. Gli endpoint connessi comunicheranno con la Control Center solo tramite il relay specificato.



Importante

Per funzionare, la porta 7074 deve essere aperta per l'impiego tramite Bitdefender Endpoint Security Tools Relay.

18. Clicca su **Salva**.

Il pacchetto appena creato sarà aggiunto all'elenco dei pacchetti.




Nota

Le impostazioni configurate in un pacchetto di installazione saranno applicate agli endpoint subito dopo l'installazione. Non appena la policy viene applicata al client, le impostazioni configurate nella policy vengono applicate, sostituendo alcune impostazioni del pacchetto di installazione (come i server di comunicazione o le impostazioni del proxy).

Scaricare i pacchetti di installazione

Per scaricare i pacchetti di installazione degli agenti di sicurezza:

1. Accedi alla Control Center dall'endpoint su cui vuoi installare la protezione.
2. Vai alla pagina **Rete e Pacchetti**.
3. Seleziona il pacchetto di installazione che desideri scaricare.
4. Clicca sul pulsante  **Scarica** nel lato superiore della tabella e seleziona il tipo di installer che vuoi utilizzare. Sono disponibili due tipi di file di installazione:
 - **Downloader**. Il downloader scarica prima il kit di installazione completo dai server cloud di Bitdefender e poi avvia l'installazione. È di piccole dimensioni e può essere eseguito su sistemi a 32 e 64 bit (il che ne facilita la distribuzione). Il lato negativo, è che richiede una connessione a Internet attiva.
 - **Kit completo**. I kit di installazione completi sono di maggiori dimensioni e devono essere eseguiti su un determinato tipo di sistema operativo.
Il kit completo deve essere utilizzato per installare la protezione sugli endpoint con una connessione a Internet lenta o assente del tutto. Scarica

questo file in un endpoint connesso a Internet e poi distribuisilo sugli altri endpoint utilizzando un supporto di archiviazione esterno o una rete condivisa.

Nota

Versioni dei kit completi disponibili:

- **SO Windows:** sistemi a 32 e 64 bit
- **SO Linux:** sistemi a 32 e 64 bit
- **macOS:** solo sistemi a 64 bit

Assicurati di utilizzare la versione corretta per il sistema in cui vuoi installarlo.

5. Salva il file nell'endpoint.

Avvertimento

- L'eseguibile del downloader non deve essere rinominato, altrimenti non sarà possibile scaricare i file di installazione dal server di Bitdefender.

6. Inoltre, se hai selezionato il Downloader, puoi creare un pacchetto MSI per gli endpoint Windows. Per maggiori informazioni, fai riferimento a [questo articolo della KB](#).

Invia i link per scaricare i pacchetti di installazione via e-mail.

Potrebbe essere necessario informare rapidamente gli altri utenti che è un pacchetto di installazione è disponibile per il download. In questo caso, segui i passaggi descritti di seguito:

1. Vai alla pagina **Rete e Pacchetti**.
2. Seleziona il pacchetto di installazione che desideri.
3. Clicca sul pulsante  **Invia link di download** nel lato superiore della tabella. Apparirà la finestra di configurazione.
4. Inserisci l'e-mail di ogni utente che vuole ricevere il link per il download del pacchetto di installazione. Premi **Invio** dopo ogni indirizzo e-mail.

Assicurati che ogni indirizzo e-mail inserito sia valido.

5. Se vuoi visualizzare i link di download prima di inviarli via e-mail, clicca sul pulsante **Link di installazione**.

6. Clicca su **Invia**. A ciascun indirizzo e-mail indicato viene inviata un'e-mail contenente il link di installazione.

Eeguire i pacchetti di installazione

Affinché l'installazione funzioni, il pacchetto di installazione deve essere eseguito utilizzando i privilegi di amministratore.

Il pacchetto si installa in modo diverso su ciascun sistema operativo, come segue:

- Su sistemi operativi Windows e macOS:
 1. Sull'endpoint di destinazione, scarica il file di installazione dalla Control Center o copialo da una rete condivisa.
 2. Se hai scaricato il kit completo, estrai i file dall'archivio.
 3. Esegui il file eseguibile.
 4. Seguire le istruzioni sullo schermo.



Nota

Su macOS, dopo aver installato Endpoint Security for Mac, agli utenti viene chiesto di approvare le estensioni del kernel di Bitdefender sui propri computer. Finché gli utenti non approvano le estensioni del kernel di Bitdefender, alcune funzionalità dell'agente di sicurezza non funzioneranno. Per maggiori dettagli, fai riferimento a [questo articolo della KB](#).

- Sui sistemi operativi Linux:
 1. Connettiti e accedi alla Control Center.
 2. Scarica o copia il file di installazione sull'endpoint di destinazione.
 3. Se hai scaricato il kit completo, estrai i file dall'archivio.
 4. Ottieni privilegi di root eseguendo il comando `sudo su`.
 5. Modifica i permessi per il file di installazione in modo da eseguirlo:

```
# chmod +x installer
```

6. Lanciare il file di installazione:

```
# ./installer
```

7. Per verificare se l'agente è stato installato sull'endpoint, esegui questo comando:

```
$ service bd status
```

Una volta che l'agente di sicurezza è stato installato, l'endpoint comparirà come gestito nella Control Center (pagina **Rete**) in pochi minuti.



Importante

Utilizzando VMware Horizon View Persona Management, si consiglia di configurare Active Directory Group Policy per escludere i seguenti processi di Bitdefender (senza il percorso completo):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationsservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Queste eccezioni devono essere applicate finché l'agente di sicurezza non viene eseguito sull'endpoint. Per maggiori dettagli, fai riferimento alla [pagina della documentazione di VMware Horizon](#).

Installazione remota

La Control Center ti consente di installare in remoto l'agente di sicurezza sugli endpoint da ambienti integrati con la Control Center e su altri endpoint rilevati nella rete utilizzando le attività di installazione. Negli ambienti VMware, l'installazione remota si basa su VMware Tools, mentre negli ambienti Citrix XenServer e Nutanix Prism Element, si basa su condivisioni amministrative di Windows e SSH.

Una volta che l'agente di sicurezza è stato installato su un endpoint, potrebbero volerci alcuni minuti affinché gli altri endpoint della rete diventino visibili nella Control Center.

Bitdefender Endpoint Security Tools include un meccanismo di Network Discovery automatico che consente di rilevare gli endpoint non in Active Directory. Gli endpoint rilevati vengono mostrati come **non gestiti** nella pagina **Rete**, nella schermata

Computer, in Gruppi personalizzati. La Control Center rimuove automaticamente gli endpoint di Active Directory dall'elenco degli endpoint rilevati.

Per consentire Network Discovery, devi avere Bitdefender Endpoint Security Tools già installato su almeno un endpoint nella rete. Questo endpoint sarà utilizzato per esaminare la rete e installare Bitdefender Endpoint Security Tools sugli endpoint non protetti.

Per maggiori informazioni su Network Discovery, fai riferimento a [«Come funziona Network Discovery»](#) (p. 154).

Requisiti per l'installazione in remoto

Affinché l'installazione in remoto funzioni:

- Su Windows:
 - La condivisione amministrativa `admin$` deve essere attivata. Configura ogni workstation bersaglio per non usare la condivisione file avanzata.
 - Configura User Account Control (UAC) in base al sistema operativo in esecuzione sugli endpoint di destinazione. Se gli endpoint sono in un dominio di Active Directory, puoi usare una policy di gruppo per configurare User Account Control. Per maggiori dettagli, fai riferimento a [questo articolo della KB](#).
 - Disattiva Windows Firewall o configuralo per consentire il traffico tramite il protocollo di condivisione di file e stampanti.



Nota

L'impiego remoto funziona solo sui sistemi operativi moderni, a partire con Windows 7 / Windows Server 2008 R2, per cui Bitdefender fornisce supporto completo. Per maggiori informazioni, fai riferimento a [«Sistemi operativi supportati»](#) (p. 27).

- Su Linux: SSH deve essere attivato.
- Su macOS: l'accesso remoto e la condivisione file devono essere attivati.

Eseguire attività di installazione in remoto


Per eseguire un'attività di installazione in remoto:

1. Connettiti e accedi alla Control Center.

2. Vai alla pagina **Rete**.
3. Seleziona **Computer e Macchine Virtuali** dal selettore di visualizzazione.
4. Seleziona il gruppo desiderato dal pannello sulla sinistra. Le entità contenute nel gruppo selezionato sono mostrate nel lato destro della tabella del pannello.

**Nota**

In alternativa, puoi applicare alcuni filtri per mostrare solo gli endpoint non gestiti. Clicca sul menu **Filtri** e seleziona le seguenti opzioni: **Non gestito** dalla scheda **Sicurezza** e **Tutti gli elementi ricorsivamente** dalla scheda **Profondità**.

5. Seleziona le entità (endpoint o gruppi di endpoint) su cui vuoi installare la protezione.
6. Clicca sul pulsante  **Attività** nel lato superiore della tabella e seleziona **Installa**. Viene mostrata la procedura guidata **Installa client**.

User	Password	Description	Action
tester	*****		

Installare Bitdefender Endpoint Security Tools dal menu Attività

7. Nella sezione **Opzioni**, configura il momento dell'installazione:
 - **Ora**, per lanciare immediatamente l'impiego.
 - **Programmato**, per configurare l'intervallo di ricorrenza dell'impiego. In questo caso, seleziona l'intervallo di tempo che desideri (orario, giornaliero o settimanale) e configuralo in base alle tue necessità.

 **Nota**

Per esempio, quando determinate operazioni sono necessarie sulla macchina bersaglio prima di installare il client (come disinstallare altri software e riavviare il SO), puoi programmare l'attività di impiego per essere eseguita ogni 2 ore. L'attività inizierà su ogni macchina bersaglio ogni 2 ore fin quando l'impiego non avrà successo.

8. Se vuoi che gli endpoint di destinazione vengano riavviati automaticamente per completare l'installazione, seleziona **Riavvio automatico (se necessario)**.
9. Nella sezione **Credentials Manager**, indica le credenziali amministrative richieste per l'autenticazione remota sugli endpoint di destinazione. Puoi aggiungere le credenziali, inserendo l'utente e la password per il sistema operativo di ogni bersaglio.

 **Importante**

Per sistemi con Windows 8.1, devi fornire le credenziali dell'account da amministratore integrato o di un account amministratore del dominio. Per maggiori informazioni, fai riferimento a [questo articolo della KB](#).

Per aggiungere le credenziali SO richieste:


- a. Inserisci il nome utente e la password di un account amministratore nei campi corrispondenti dall'installazione della tabella.

Se i computer sono in un dominio, è sufficiente inserire le credenziali dell'amministratore del dominio.

Usa le convenzioni di Windows nell'inserire il nome di un account utente:

- Per le macchine Active Directory, utilizza queste sintassi: `username@domain.com` e `domain\username`. Per assicurare che le credenziali inserite funzioneranno, aggiungile in entrambi i moduli (`username@domain.com` e `domain\username`).
- Per le macchine Workgroup, è sufficiente inserire solo il nome utente senza il nome del gruppo di lavoro.

In alternativa, puoi aggiungere una descrizione che ti aiuterà a identificare ogni account più facilmente.

- b. Clicca sul pulsante  **Aggiungi**. L'account è stato aggiunto all'elenco delle credenziali.

**Nota**

Le credenziali indicate vengono salvate automaticamente nel tuo **Credentials Manager**, in modo che non dovrai inserirle le prossime volte. Per accedere al Credentials Manager, punta al tuo nome utente nell'angolo in alto a destra della console.

**Importante**

Se le credenziali fornite non sono valide, l'impiego del client sugli endpoint corrispondenti non funzionerà. Assicurati di aggiornare le credenziali SO inserite nel Credentials Manager quando queste vengono modificate negli endpoint di destinazione.

10. Seleziona le caselle corrispondenti agli account che vuoi usare.

**Nota**

Viene visualizzato un messaggio di avviso finché non viene selezionata alcuna credenziale. Questo passaggio è obbligatorio per installare in remoto l'agente di sicurezza sugli endpoint.

11. Nella sezione **Gestore**, scegli l'entità a cui gli endpoint di destinazione si connettono per installare e aggiornare il client:

- **Appliance di GravityZone**, quando gli endpoint si connettono direttamente alla appliance di GravityZone.

In questo caso, puoi anche definire:

- Un Server di comunicazione personale inserendo il suo IP o nome dell'host, se necessario.
 - Le impostazioni proxy, se gli endpoint di destinazione comunicano con la appliance di GravityZone tramite proxy. In questo caso, seleziona **Usa proxy per la comunicazione** e inserisci le impostazioni proxy richieste nei campi sottostanti.
- **Relay di sicurezza endpoint**, se vuoi connettere gli endpoint a un client relay installato nella tua rete. Tutte le macchine con ruolo di relay rilevate nella tua rete compariranno nella tabella mostrata sotto. Seleziona la macchina relay che desideri. Gli endpoint connessi comunicheranno con la Control Center solo tramite il relay specificato.



Importante

Per funzionare, la porta 7074 deve essere aperta per l'impiego tramite l'agente relay.

Deployer			
Deployer:		Endpoint Security Relay	
Name	IP	Custom Server Name/IP	Label
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
CO_SUPA	192.168.0.183		N/A
FC-WIN7-X64-01	192.168.3.80		N/A

First Page -- Page 1 of 1 -- Last Page 20 2 items

12. Usa la sezione **Bersagli aggiuntivi** se vuoi impiegare il client in determinate macchine della tua rete non mostrate nel suo inventario. Espandi la sezione e inserisci gli indirizzi IP o i nomi dell'host di tali macchine nel campo dedicato, separati da una virgola. Puoi aggiungere quanti IP ti servono.
13. Devi selezionare un pacchetto di installazione per l'impiego attuale. Clicca sull'elenco **Usa pacchetto** e seleziona il pacchetto di installazione che desideri. Qui puoi trovare tutti i pacchetti di installazione creati in precedenza per il tuo account e anche il pacchetto di installazione standard disponibile con la Control Center.
14. Se necessario, puoi modificare alcune delle impostazioni del pacchetto selezionato, cliccando sul pulsante **Personalizza** accanto al campo **Usa pacchetto**.

Le impostazioni del pacchetto di installazione compariranno in basso e potrai effettuare le modifiche necessarie. Per scoprire maggiori informazioni su come modificare i pacchetti di installazione, fai riferimento a «[Creare i pacchetti di installazione](#)» (p. 137).

Se vuoi salvare le modifiche come nuovo pacchetto, seleziona l'opzione **Salva come pacchetto** posizionata in fondo all'elenco delle impostazioni del pacchetto e inserisci un nome per il nuovo pacchetto di installazione.

15. Clicca su **Salva**. Apparirà un messaggio di conferma.
Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.



Importante

Utilizzando VMware Horizon View Persona Management, si consiglia di configurare Active Directory Group Policy per escludere i seguenti processi di Bitdefender (senza il percorso completo):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationsservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Queste eccezioni devono essere applicate finché l'agente di sicurezza non viene eseguito sull'endpoint. Per maggiori dettagli, fai riferimento alla [pagina della documentazione di VMware Horizon](#).

Preparare i sistemi Linux per la scansione all'accesso

Bitdefender Endpoint Security Tools per Linux include capacità di scansione all'accesso che funzionano con determinate distribuzioni Linux e versioni kernel. Per maggiori informazioni, fai riferimento ai [requisiti di sistema](#).

Poi scoprirai come compilare manualmente il modulo DazukoFS.

Compila manualmente il modulo DazukoFS

Segui i passaggi sottostanti per compilare DazukoFS per la versione del kernel del sistema e poi carica il modulo:

1. Scaricare le corrette intestazioni kernel.

- Sui sistemi **Ubuntu**, esegui questo comando:

```
$ sudo apt-get install linux-headers-`uname -r`
```

- Sui sistemi **RHEL/CentOS**, esegui questo comando:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. Sui sistemi **Ubuntu**, ti serve `build-essential`:

```
$ sudo apt-get install build-essential
```

3. Copia ed estrai il codice sorgente di DazukoFS in una cartella preferita:

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzvf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Compila il modulo:

```
# make
```

5. Installa e carica il modulo:

```
# make dazukofs_install
```

Requisiti per utilizzare la scansione a richiesta con DazukoFS

Affinché DazukoFS e la scansione a richiesta lavorino insieme, devono essere soddisfatte alcune condizioni. Controlla se una delle seguenti indicazioni si applica al tuo sistema Linux e segui le linee guida per evitare problemi.

- La policy SELinux deve essere disattivata o impostata su **permissivo**. Per controllare e impostare l'impostazione della policy di SELinux, modifica il file `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools è compatibile esclusivamente con la versione DazukoFS inclusa nel pacchetto di installazione. Se DazukoFS è già stato installato sul sistema, rimuovilo prima di installare Bitdefender Endpoint Security Tools.
- DazukoFS supporta determinate versioni del kernel. Se il pacchetto DazukoFS fornito con Bitdefender Endpoint Security Tools non è compatibile con la versione kernel del sistema, il modulo non potrà essere caricato. In tal caso,

puoi aggiornare il kernel alla versione supportata o ricompila il modulo DazukoFS per la tua versione del kernel. Puoi trovare il pacchetto DazukoFS nella cartella di installazione di Bitdefender Endpoint Security Tools:

`/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`

- Condividendo i file usando server dedicati come NFS, UNFSv3 o Samba, devi avviare i servizi nel seguente ordine:
 1. Attiva la scansione all'accesso tramite la policy dalla Control Center.
Per maggiori informazioni, fai riferimento alla Guida dell'amministratore di GravityZone.
 2. Avvia il servizio di condivisione della rete.

Per NFS:

```
# service nfs start
```

Per UNFSv3:

```
# service unfs3 start
```

Per Samba:

```
# service smbd start
```



Importante

Per il servizio NFS, DazukoFS è compatibile solo con NFS User Server.

Come funziona Network Discovery

Oltre all'integrazione con Active Directory, GravityZone include anche un meccanismo automatico di network discovery inteso a rilevare i computer del gruppo di lavoro.

GravityZone si basa sul servizio **Microsoft Computer Browser** e lo strumento **NBTscan** per eseguire Network Discovery.

Il servizio Computer Browser è una tecnologia di rete utilizzata da computer Windows per mantenere aggiornati gli elenchi di domini, workgroup e computer in essi e fornire tali elenchi ai computer client a richiesta. I computer rilevati nella rete dal servizio Computer Browser possono essere visualizzati eseguendo il comando **net view** in una finestra di comando.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

Il comando Net view

Lo strumento NBTscan esamina le reti dei computer utilizzando NetBIOS. Interroga ogni endpoint nella rete e recupera informazioni come indirizzo IP, nome computer NetBIOS e indirizzo MAC.

Per consentire automaticamente Network Discovery, devi avere già installato Bitdefender Endpoint Security Tools Relay su almeno un computer nella rete. Questo computer sarà utilizzato per esaminare la rete.



Importante

Control Center non usa le informazioni di rete da Active Directory o dalla funzionalità mappa di rete. La mappa di rete si affida a una diversa tecnologia di Network Discovery: il protocollo Link Layer Topology Discovery (LLTD).

Control Center non è attivamente coinvolto nell'operatività del servizio Computer Browser. Bitdefender Endpoint Security Tools interroga solo il servizio Computer Browser per l'elenco delle workstation e dei server attualmente visibili nella rete (conosciuto come elenco di navigazione) e quindi lo invia alla Control Center. Control Center elabora l'elenco di navigazione, aggiungendo i nuovi computer rilevati al suo elenco **Computer non gestiti**. I computer rilevati in precedenza non vengono eliminati dopo una nuova query di Network Discovery, quindi dovrai escludere ed eliminare direttamente i computer che non appartengono più alla rete.

La query iniziale per la lista di navigazione viene eseguita dal primo Bitdefender Endpoint Security Tools installato nella rete.

- Se il relay è installato su un computer workgroup, solo i computer di quel workgroup saranno visibili in Control Center.
- Se il relay è installato su un computer dominio, solo i computer di quel dominio saranno visibili in Control Center. I computer da altri domini possono essere rilevati se c'è un rapporto di fiducia con il dominio dove è stato installato il relay.

Le richieste successive di Network Discovery vengono eseguite regolarmente ogni ora. Per ogni nuova query, Control Center divide lo spazio dei computer gestiti in aree di visibilità e successivamente designa un relay in ciascuna area per eseguire un'attività. Un'area di visibilità è un gruppo di computer che si rilevano a vicenda. In genere, un'area di visibilità viene definita da un workgroup o un dominio, ma dipende dalla topologia e la configurazione della rete. In alcuni casi, un'area di visibilità può consistere in più domini e workgroup.

Se un relay selezionato non riesce a eseguire la query, Control Center attende per la prossima query programmata, senza selezionare un altro relay per riprovare.

Per una completa visibilità della rete, il relay deve essere installato in almeno un computer in ogni workgroup o dominio nella rete. Idealmente, Bitdefender Endpoint Security Tools deve essere installato su almeno un computer in ogni sottorete.

Maggiori informazioni sul servizio Microsoft Computer Browser

Alcune informazioni sul servizio Computer Browser:

- Funziona in modo indipendente da Active Directory.
- Funziona esclusivamente su reti IPv4 e opera autonomamente nei confini di un gruppo LAN (workgroup o dominio). Per ciascun gruppo LAN viene compilata e mantenuta una lista di navigazione.
- Utilizza tipicamente trasmissioni server senza connessione per comunicare tra i nodi.
- Utilizza NetBIOS su TCP/IP (NetBT).
- Richiede la risoluzione dei nomi NetBIOS. Si consiglia di avere un'infrastruttura Windows Internet Name Service (WINS) attiva e in esecuzione nella rete.
- Di norma non è attivata in Windows Server 2008 e 2008 R2.

Per maggiori informazioni sul servizio Computer Browser, consulta [Computer Browser Service Technical Reference](#) su Microsoft Technet.

Requisiti di Network Discovery

Per scoprire con successo tutti i computer (server e workstation) che saranno gestiti dalla Control Center, servono i seguenti requisiti:

- I computer devono essere uniti in un workgroup o un dominio e connessi tramite una rete locale IPv4. Il servizio Computer Browser non funziona su reti IPv6.
- Diversi computer in ogni gruppo LAN (workgroup o dominio) devono eseguire il servizio Computer Browser. Anche i Primary Domain Controller devono eseguire il servizio.
- NetBIOS su TCP/IP (NetBT) deve essere attivato sui computer. Il firewall locale deve consentire il traffico NetBT.
- Se si utilizza un relay Linux per scoprire altri endpoint Linux o Mac, è necessario installare Samba sugli endpoint bersaglio, oppure associarli in Active Directory e usare DHCP. In questo modo, NetBIOS sarà configurato automaticamente su di essi.
- Sui computer deve essere attiva la condivisione dei file. Il firewall locale deve consentire la condivisione dei file.
- Un'infrastruttura Windows Internet Name Service (WINS) deve essere attivata e deve funzionare correttamente.
- Network Discovery deve essere attivato (**Pannello di controllo > Centro connessioni di rete e condivisione > Modifica impostazioni di condivisione avanzate**).

Per attivare questa funzionalità, i seguenti servizi devono essere attivati:

- Client DNS
 - Function Discovery Resource Publication
 - SSDP Discovery
 - UPnP Device Host
- Negli ambienti con più domini, si consiglia di impostare relazioni affidabili tra i domini, in modo che i computer possano accedere a liste di navigazione da altri domini.

I computer da cui Bitdefender Endpoint Security Tools interroga il servizio Computer Browser devono essere in grado di risolvere i nomi NetBIOS.

i Nota

Il meccanismo di Network Discovery funziona per tutti i sistemi operativi supportati, tra cui versioni di Windows Embedded, a condizione che i requisiti siano soddisfatti.

5.4. Installare Sandbox Analyzer On-Premises

Per assicurarsi che l'installazione avvenga correttamente, segui questi passaggi:

1. [Preparati per l'installazione](#)
2. [Impiegare la Virtual appliance di Sandbox Analyzer](#)
3. [Impiegare la Network Security Virtual Appliance](#)

5.4.1. Preparati per l'installazione

Prima di installare Sandbox Analyzer On-Premises, assicurati che:

- Il VMWare ESXi hypervisor è stato installato e configurato. Per maggiori dettagli, fai riferimento alla documentazione [Installazione e configurazione di vSphere](#), sezione 2: "Installare e configurare ESXi".
- La Virtual Appliance di Bitdefender GravityZone è stata impiegata e configurata.

i Nota

Per quanto riguarda il VMWare ESXi hypervisor, assicurati che:

- La versione ESXi sia 6.5 o superiore.
- La versione di datastore VMFS sia 5.
- SSH sia attivata nella **policy di avvio** con la configurazione **Start and stop with host**.
- Il servizio NTP è attivo e configurato.

Il codice di licenza di Sandbox Analyzer On-Premises controlla il numero massimo di detonazioni contemporanee. Poiché ogni detonazione richiede un'istanza di virtual machine in esecuzione, il numero di detonazioni simultanee si riflette nel numero di virtual machine create. Per maggiori dettagli sull'aggiunta di codici di licenza in GravityZone Control Center, fai riferimento a [«Inserire i tuoi codici di licenza»](#) (p. 120).

5.4.2. Impiegare la Virtual appliance di Sandbox Analyzer

Per impiegare la Virtual Appliance di Sandbox Analyzer:

1. Accedi in GravityZone Control Center.
2. Vai alla pagina **Rete e Pacchetti**.
3. Seleziona la casella **Sandbox Analyzer** dalla tabella.
4. Clicca sul pulsante **Scarica** nell'angolo in alto a sinistra della pagina. Seleziona l'opzione **Security Appliance (ESXi standalone)**.
5. Usa il tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client) per importare il file OVA scaricato nel tuo ambiente virtuale.



Nota

Nell'impiegare il file OVA, configura le reti in questo modo:

- **Bitdefender Network** - Questa è la rete dove risiedono gli altri componenti di Bitdefender (interfaccia `eth0`). Sandbox Analyzer e l'appliance di GravityZone deve essere nella stessa rete e devono comunicare tramite `eth0`.
 - **Rete di detonazione privata** - Sandbox Analyzer utilizza questa rete per la comunicazione interna (interfaccia `eth1`). Questa rete deve essere isolata da qualsiasi altro segmento di rete.
 - **Rete di accesso a Internet** - Sandbox Analyzer usa questa rete per ottenere gli aggiornamenti più recenti (interfaccia `eth2`). L'interfaccia `eth2` non deve avere lo stesso IP o rete di `eth0`.
6. Alimenta la appliance.
 7. Dal tuo strumento di gestione della virtualizzazione, accedi all'interfaccia della Virtual Appliance di Sandbox Analyzer.
 8. Quando ti saranno chieste le credenziali, usa `root` come nome utente e `sve` come password.
 9. Accedi al menu di configurazione eseguendo il seguente comando:

```
/opt/bitdefender/bin/sandbox-setup
```

10. Nel menu **Configurazione sandbox**, effettua le seguenti impostazioni:
 - a. **Configurazione di rete**. Seleziona questa opzione per configurare la NIC di gestione. Sandbox Analyzer utilizzerà questa interfaccia di rete per comunicare con GravityZone.

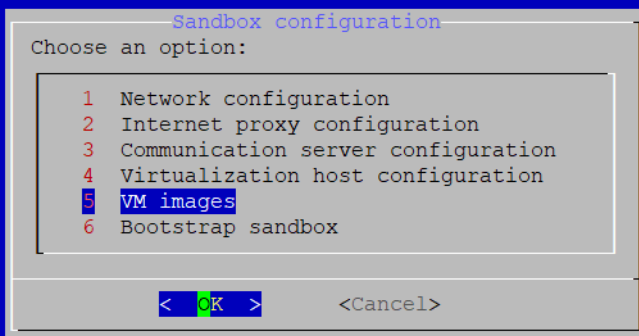
L'indirizzo IP può essere indicato manualmente o automaticamente tramite DHCP.



Nota

Se la appliance di GravityZone è in un'altra rete rispetto a `eth0`, devi aggiungere un percorso statico in **Configurazione rete > Rete BitDefender > Percorsi** per il corretto funzionamento di Sandbox Analyzer.

```
Bitdefender Security for Virtualized Environments (Sandbox) 1.0.1.8513
```



Console appliance di Sandbox Analyzer

b. **Configurazione proxy Internet.** Affinché l'installazione abbia successo, Sandbox Analyzer richiede una connessione a Internet. In tal caso, è possibile configurare Sandbox Analyzer per usare un server proxy specificando questi dettagli:

- **Host** - IP o FQDN del server proxy. Usa la seguente sintassi:
`http://<IP/Hostname>:<Port>`.
- **Utente e password** - Devi inserire la password due volte.
- **Dominio** - Il dominio Active Directory, se il caso.

- c. **Configurazione server comunicazione.** Inserisci l'indirizzo IP o l'hostname della appliance che esegue il ruolo di Server di comunicazione.

Usa la seguente sintassi: `http://<IP/Hostname>:<Port>`. La porta standard è 8443.



Nota

Una volta indicato l'indirizzo IP e l'hostname, e salvata la configurazione, l'istanza di Sandbox Analyzer diventerà visibile in GravityZone Control Center, nella pagina **Sandbox Analyzer > Infrastruttura**.

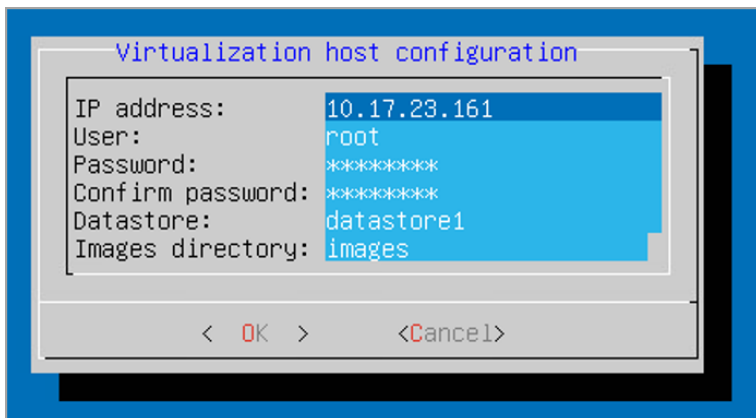
- d. **Configurazione host virtualizzata.** Sandbox Analyzer usa il server ESXi per eseguire il provisioning dell'infrastruttura di analisi dei malware. Utilizzando la **Configurazione host virtualizzata**, connetti l'appliance di Sandbox Analyzer all'host ESXi, fornendo le seguenti informazioni:

- L'indirizzo IP del server ESXi.
- Credenziali root per accedere all'host ESXi.
- Archivio di dati dedicato a Sandbox Analyzer.

Inserisci il nome dell'archivio di dati come mostrato da ESXi.

- Nome della cartella utilizzata nell'archivio di dati per l'archiviazione delle immagini di virtual machine.

Se tale cartella non esiste, devi crearla sull'archivio di dati, prima di salvare la configurazione di Sandbox Analyzer.



Console della appliance di Sandbox Analyzer

- e. **Immagini VM.** Per creare virtual machine di detonazione per Sandbox Analyzer, devi copiare i file VMDK contenenti le immagini desiderate nella cartella **Immagini** indicata nel menu **Configurazione host virtualizzata**. Per ciascuna immagine, nel menu **Immagini VM**, puoi trovare le seguenti impostazioni:
 - i. Nel menu **Configurazione immagine**, indica il nome dell'immagine (come sarà mostrato in GravityZone Control Center) e il sistema operativo.



Nota

La cartella contenente le immagini VM viene esaminata periodicamente e le nuove voci vengono segnalate a GravityZone. Queste voci sono visibili in Control Center, nella pagina **Sandbox Analyzer > Infrastruttura > Gestione immagine**.

- In alcune situazioni, utilizzando Sandbox Analyzer, puoi riscontrare problemi con le virtual machine di detonazione. Per risolvere tali problemi, devi disattivare l'opzione anti-impronte digitali. Per maggiori dettagli, fai riferimento a [«Tecniche anti-impronte digitali»](#) (p. 163).
- ii. Nel menu **host DMZ**, puoi inserire nella whitelist gli hostname richiesti da servizi e componenti di terze parti integrati nelle virtual machine per comunicare con Sandbox Manager. Per maggiori dettagli, fai riferimento a [«Host DMZ»](#) (p. 164)

- iii. Nel menu **Pulizia**, puoi rimuovere le immagini delle VM che non servono più.
- f. **Lancia sandbox**. Una volta aggiunto i dettagli della configurazione di Sandbox Analyzer, continua con l'installazione selezionando questa opzione. Lo stato dell'installazione sarà riflesso in GravityZone Control Center, nella pagina **Sandbox Analyzer > Infrastruttura**.

Tecniche anti-impronte digitali

Di norma, durante il processo di creazione dell'immagine, Sandbox Analyzer consentirà diverse tecniche anti-impronte digitali. Determinati tipi di malware sono in grado di determinare se stanno operando in un ambiente sandbox e, in tal caso, non attiveranno le proprie routine dannose.

Lo scopo delle tecniche anti-impronte digitali è simulare diverse condizioni per imitare un ambiente reale. A causa di una combinazione virtuale eliminata di software impiegato e configurazione dell'ambiente, una combinazione che non può essere prevista in anticipo o controllata, è possibile che alcune tecniche non siano compatibili con il software installato nell'immagine dorata. Puoi identificare tali rare situazioni dai seguenti sintomi:

- Errori durante la fase di creazione dell'immagine.
- Errori nel tentativo di eseguire il software nell'immagine.
- Messaggi di errore durante la detonazione dei campioni.
- Software su licenza che non funziona più a causa di codici di licenza non validi.

Un rimedio rapido a tali rare circostanza consiste nel ricreare l'immagine con le tecniche anti-impronte digitali disattivate. Per farlo, segui questi passaggi:

1. Accedi in GravityZone Control Center ed elimina l'immagine.
2. Accedi nella appliance di Sandbox Analyzer e lancia la console della appliance di Sandbox Analyzer eseguendo il seguente comando:

```
/opt/bitdefender/bin/sandbox-setup
```

3. Vai in **VM Immagini > Configurazione immagine**.
4. Seleziona l'immagine che sta causando problemi.
5. Vai all'opzione **Anti-impronte digitali**.

6. Deseleziona la casella corrispondente per disattivare le tecniche anti-impronte digitali.

Host DMZ

Durante il processo di creazione dell'immagine, un'infrastruttura virtuale sarà creata per facilitare la comunicazione tra Sandbox Manager e le virtual machine. Dalla prospettiva della rete, ciò si traduce in un ambiente di rete isolato che conterrà tutte le potenziali comunicazioni che un campione detonato potrebbe creare.

Il menu server DMZ consente di inserire nella whitelist gli hostname con i quali servizi e componenti di terze parti integrati nelle virtual machine devono comunicare per funzionare correttamente.

Un esempio di questa situazione sono i server di licenze KMS utilizzati dalle licenze di Windows, se una licenza di volume venisse applicata sulle virtual machine fornite.

5.4.3. Impiegare la Network Security Virtual Appliance

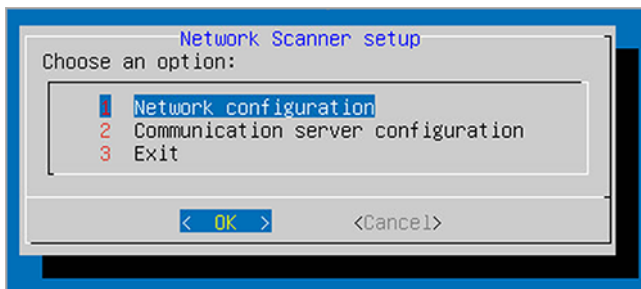
Questa sezione descrive come impiegare la Network Security Virtual Appliance, una componente di Sandbox Analyzer che cattura il traffico di rete e invia campioni sospetti all'analisi comportamentale.

Per impiegare la Network Security Virtual Appliance:

1. Accedi in GravityZone Control Center.
2. Vai alla pagina **Rete e Pacchetti**.
3. Seleziona la casella **Network Security Virtual Appliance** nella tabella.
4. Clicca sul pulsante **Scarica** nell'angolo in alto a sinistra della pagina e seleziona l'opzione (**VMware OVA**).
5. Usa il tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client) per importare il file OVA scaricato nel tuo ambiente virtuale.
6. Nella procedura guidata di impiego, seleziona la scheda di interfaccia di rete (NIC) usata per la comunicazione con GravityZone e la NIC usata per catturare il traffico.
7. Alimenta la appliance.
8. Dal tuo strumento di gestione della virtualizzazione, accedi all'interfaccia della console di GravityZone SVE SVA Network Security Virtual Appliance.

- Quando ti saranno chieste le credenziali, usa `root` come nome utente e `sve` come password.
- Accedi al menu di configurazione eseguendo il seguente comando:

```
/opt/bitdefender/bin/nsva-setup
```



Console appliance Network Security

- Vai all'opzione del menu **Configurazione server comunicazione**.
- Indica l'indirizzo IP o l'hostname, e la porta del Server di comunicazione di GravityZone.
Usa la seguente sintassi: `http://<IP/Hostname>:<Port>`. La porta standard è 8443.
- Salva la configurazione.

Configurare il sensore di rete per detonare i file pcap

Il sensore di rete può estrarre contenuti dai file acquisiti nella rete (pcap) e inviarli automaticamente per la detonazione all'istanza di Sandbox Analyzer.

Per detonare contenuti da file pcap:

- Accedi nella Network Security Virtual Appliance.
- Quando ti saranno chieste le credenziali, usa `root` come nome utente e `sve` come password.
- Esegui il seguente comando:

```
/opt/bitdefender/bin/scan-pcap <local pcap path>
```

Nel comando precedente, `<local pcap path>` rappresenta la posizione in cui il file pcap è stato caricato nella Network Security Virtual Appliance.

Per altri dettagli sull'utilizzo del sensore di rete, fai riferimento al capitolo **Policy > Sandbox Analyzer** della Guida per l'amministratore di GravityZone.

5.5. Installare Full Disk Encryption

GravityZone Full Disk Encryption viene fornito come un servizio che richiede un'attivazione basata su un codice di licenza. Per farlo, devi andare in **Configurazione > Licenza** e inserisci il codice di licenza.

Per maggiori informazioni sui codici di licenza, fai riferimento a [«Amministrazione licenza»](#) (p. 119).

Gli agenti di sicurezza di Bitdefender supportano Full Disk Encryption a partire dalla versione 6.2.22.916 su Windows e 4.0.0173876 su Mac. Per assicurarsi che gli agenti siano pienamente compatibili con questo modulo, hai due opzioni:

- Installa gli agenti di sicurezza con il modulo Cifratura incluso.
- Usa l'attività **Riconfigura**.

Per maggiori informazioni sull'utilizzo di Full Disk Encryption nella tua rete, fai riferimento al capitolo **Policy di sicurezza > Cifratura** nella Guida dell'amministratore di GravityZone.

5.6. Installare la protezione di Exchange

Security for Exchange si integra automaticamente con i server Exchange, in base al ruolo del server. Per ciascun ruolo, vengono installate solo le funzionalità compatibili, come descritto qui:

Caratteristiche	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Edge	Casella di posta	Edge	Hub	Casella di posta
Livello di Trasporto					
Filtro antimalware	x	x	x	x	
Filtro antispam	x	x	x	x	
Filtro contenuti	x	x	x	x	
Filtro allegati	x	x	x	x	
Store Exchange					
Scansione antimalware a richiesta		x			x

5.6.1. Preparazione all'installazione

Prima di installare Security for Exchange, assicurati che tutti i [requisiti](#) siano soddisfatti, altrimenti Bitdefender Endpoint Security Tools potrebbe essere installato senza il modulo Protezione Exchange.

Per far funzionare il modulo Protezione Exchange senza problemi e impedire eventuali conflitti e risultati indesiderati, rimuovere ogni agente antimalware e di filtro e-mail.

Bitdefender Endpoint Security Tools rileva e rimuove automaticamente la maggior parte dei prodotti antimalware e disattiva l'agente antimalware del Server Exchange fin dalla versione 2013. Per maggiori dettagli sulla lista dei software di sicurezza rilevati, fai riferimento a [questo articolo della FAQ](#).

Puoi riattivare manualmente l'agente antimalware di Exchange in qualsiasi momento, anche se non si consiglia di farlo.

5.6.2. Installare la protezione sui server Exchange

Per proteggere i tuoi server Exchange, devi installare Bitdefender Endpoint Security Tools con il ruolo Protezione Exchange su ciascuno di loro.

Hai diverse opzioni per impiegare Bitdefender Endpoint Security Tools sui server Exchange:

- Installazione locale, scaricando ed eseguendo il pacchetto di installazione sul server.
- Installazione remota, eseguendo un'attività di **Installazione**.
- Remota, eseguendo l'attività **Riconfigura client**, se Bitdefender Endpoint Security Tools offre già la protezione del file system sul server.

Per i passaggi dettagliati dell'installazione, fai riferimento a [«Installare gli agenti di sicurezza» \(p. 133\)](#).

5.7. Installare HVI

Per poter utilizzare HVI sulle virtual machine dai tuoi host Xen, devi eseguire questi passaggi:

1. [Verifica i prerequisiti di installazione](#)
2. [Installare Security Server](#)
3. [Installa il Pacchetto supplementare di HVI](#)

Prerequisiti

- XenServer è integrato in GravityZone.
- XenCenter è installato sulla tua macchina.

Installare Security Server

Per installare il Security Server su uno o più host:

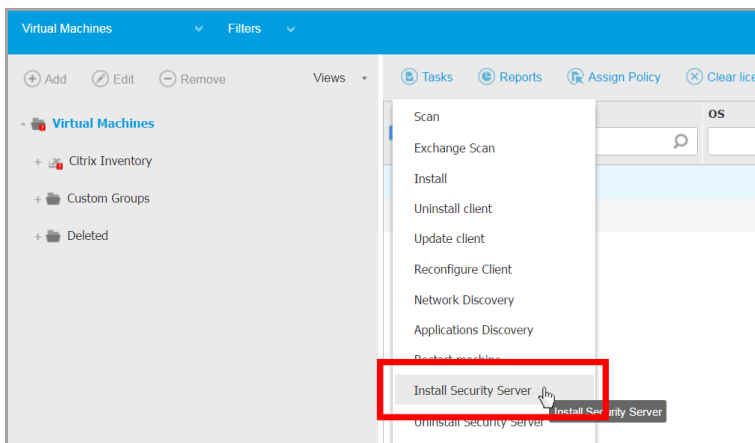
1. Vai alla pagina **Rete**.
2. Seleziona **Macchine virtuali** dal selettore del servizio.
3. Esplora l'inventario Citrix e seleziona le caselle corrispondenti agli host desiderati. Per una selezione rapida, puoi selezionare direttamente il container root (Citrix Inventory). Potrai selezionare gli host individualmente dalla procedura guidata dell'installazione.



Nota

Non puoi selezionare gli host da cartelle diverse.

4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Installa Security Server** nel menu. Verrà mostrata la finestra **Installazione del Security Server**.



Installare Security Server

5. Seleziona gli host su cui vuoi installare le istanze del Security Server.
6. Seleziona le impostazioni di configurazione che vuoi utilizzare.



Importante

L'uso di impostazioni comuni mentre si impiegano più istanze del Security Server contemporaneamente è necessario che gli host condividano la stessa archiviazione, abbiano i propri indirizzi IP assegnati da un server DHCP e facciano parte della stessa rete.

Scegliendo di configurare ciascun Security Server in maniera differente, potrai definire le impostazioni desiderate per ciascun host nel prossimo passaggio della procedura guidata. I passaggi descritti di seguito sono validi nel caso in cui si utilizza l'opzione **Configura ogni Security Server**.

7. Clicca su **Avanti**.



Nota

In base alla scelta fatta in precedenza, alcune opzioni descritte qui di seguito potrebbero non essere disponibili nella tua situazione.

8. Inserisci un nome specifico per il Security Server.
9. Seleziona il container in cui vuoi includere il Security Server nel menu **Container**.
10. Seleziona l'archivio di destinazione.
11. Seleziona il tipo di disco fornito. Si consiglia di impiegare la appliance utilizzando thick disk provisioning.



Importante

Se utilizzi thin disk provisioning e lo spazio su disco nel datastore è esaurito, il Security Server si bloccherà e, di conseguenza, l'host resterà privo di protezione.

12. Configura l'allocazione delle risorse di memoria e processore in base al tasso di consolidamento della VM sull'host. Seleziona **Basso**, **Medio** o **Alto** per caricare le impostazioni di allocazione delle risorse consigliate o **Manuale** per configurare manualmente l'allocazione delle risorse.
13. Imposta il fuso orario della appliance.
14. Imposta una password amministrativa per la console del Security Server. L'impostazione di una password amministrativa sostituisce la password principale predefinita ("sve").
15. Seleziona il tipo di configurazione di rete per la rete di Bitdefender. L'indirizzo IP del Security Server non deve cambiare nel tempo, in quanto viene utilizzato dagli agenti Linux per la comunicazione.

Se scegli di utilizzare DHCP, assicurati di configurare il server DHCP per riservare un indirizzo IP per la appliance.

Se scegli statico, devi inserire l'indirizzo IP, la subnet mask, il gateway e il DNS.
16. Clicca su **Salva**.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.

Installare il Pacchetto supplementare di HVI

1. Vai alla pagina **Configurazione > Aggiornamento**.
2. Seleziona il Pacchetto supplementare di HVI nell'elenco **Componenti** e clicca sul pulsante **Scarica** nel lato superiore della tabella.
3. Vai alla pagina **Rete** e seleziona **Virtual Machine** dal selettore di visualizzazioni.
4. Seleziona **Server** dal menu **Visualizzazioni** nel pannello a sinistra.

5. Seleziona uno o più host Xen dall'inventario della rete. Puoi facilmente visualizzare gli host disponibili selezionando l'opzione **Tipo > Host** nel menu **Filtri**.
6. Clicca sul pulsante **Attività** nel pannello a destra e seleziona **Installa il Pacchetto supplementare di HVI**. Si aprirà la finestra di installazione.
7. Programma quando eseguire l'attività di installazione. Puoi scegliere di eseguire l'attività immediatamente dopo aver salvato l'attività o in un determinato momento. Nel caso non fosse possibile completare l'installazione nel momento indicato, l'attività sarà ripetuta automaticamente in base alle impostazioni di ripetizione. Per esempio, se selezioni più host e un host non è disponibile quando si è programmato di installare il pacchetto, l'attività sarà eseguita nuovamente nel momento indicato.
8. Per applicare le modifiche e completare l'installazione, l'host deve essere riavviato. Se desideri che l'host venga riavviato in modo automatico, seleziona **Riavvia l'host automaticamente**.
9. Clicca su **Salva**. Apparirà un messaggio di conferma.
Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.

5.8. Installare la Protezione memorizzazione

Security for Storage è un servizio di Bitdefender sviluppato per proteggere i dispositivi Network-Attached Storage (NAS) e i sistemi di condivisione dei file conformi con l'Internet Content Adaptation Protocol (ICAP). Per i sistemi di condivisione dei file, fai riferimento a [«Protezione archiviazione»](#) (p. 54).

Per usare Security for Storage con la tua soluzione di GravityZone:

1. Installare e configurare almeno due Security Server nel tuo ambiente per funzionare come server ICAP. I Security Server di Bitdefender analizzano i file, inviano verdetti ai sistemi di memorizzazione e, se necessario, prendono le azioni appropriate. In caso di sovraccarico, il primo Security Server ridireziona l'eccesso di dati al secondo.



Nota

Come prassi ottimale, installa i Security Server dedicati per la protezione dell'archiviazione, separatamente dai Security Server usati per altri ruoli, come la scansione antim malware.

Per maggiori dettagli sulla procedura di installazione del Security Server, fai riferimento alla sezione **Installare Security Server** di questa guida.

2. Configura il modulo **Protezione archiviazione** dalle impostazioni della policy di GravityZone.

Per maggiori dettagli, fai riferimento al capitolo **Policy di sicurezza > Policy computer e virtual machine > Protezione archiviazione** della Guida per gli amministratori di GravityZone.

Per maggiori dettagli sulla configurazione e la gestione dei server ICAP su un determinato dispositivo NAS o sistema di condivisione dei file, fai riferimento alla documentazione per quella determinata piattaforma.

5.9. Installare la protezione dei dispositivi mobile

Security for Mobile è una soluzione di gestione dei dispositivi mobile sviluppata per iPhone, iPad e dispositivi Android. Per un elenco completo delle versioni dei sistemi operativi supportati, controlla i [requisiti di sistema](#).

Per gestire Security for Mobile dalla Control Center, devi aggiungere i dispositivi mobile ad Active Directory o agli utenti personalizzati, poi installa l'applicazione GravityZone Mobile Client sui dispositivi. Dopo aver configurato il servizio, devi eseguire le attività amministrative sui dispositivi mobile.

Prima di iniziare, assicurati di [configurare un indirizzo pubblico \(esterno\) per il Server di comunicazione](#).

Per installare Security for Mobile:

1. Se non si dispone dell'integrazione con Active Directory, è necessario [creare gli utenti per i proprietari per il dispositivo mobile](#).
2. [Aggiungi i dispositivi agli utenti](#).
3. [Installa GravityZone Mobile Client sui dispositivi e attivalo](#).

5.9.1. Configura l'indirizzo esterno per il Server di comunicazione

Nella configurazione predefinita di GravityZone, i dispositivi mobile possono essere gestiti solo quando sono direttamente connessi alla rete aziendale (via Wi-Fi o VPN). Ciò accade perché quando si iscrivono dispositivi mobile, questi sono configurati per connettersi all'indirizzo locale della appliance del Server di comunicazione.

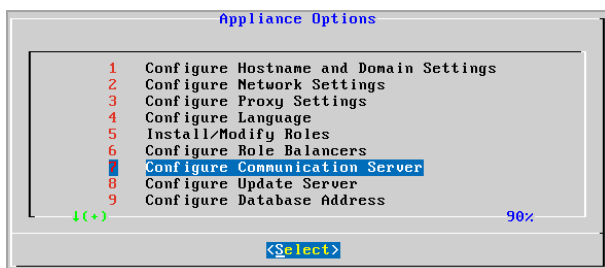
Per poter gestire i dispositivi mobile su Internet, indipendentemente dalla loro posizione, devi configurare il Server di comunicazione con un indirizzo pubblicamente raggiungibile.

Per poter gestire i dispositivi mobile quando non sono connessi alla rete aziendale, sono disponibili le seguenti opzioni:

- Configurare la mappatura delle porte sul gateway aziendale per la appliance che esegue il ruolo di Server di comunicazione.
- Aggiungere un adattatore di rete aggiuntivo alla appliance con il ruolo di Server di comunicazione e assegnarlo a un indirizzo IP pubblico.

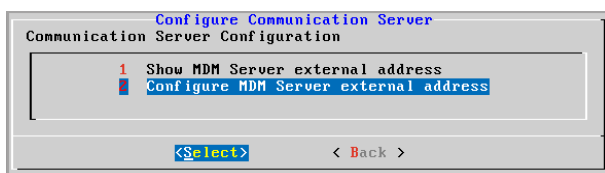
In entrambi i casi, devi configurare il Server di comunicazione con l'indirizzo esterno per essere usato per la gestione dei dispositivi mobile:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
2. Dal menu principale, seleziona **Configura Server di comunicazione**.



Finestra opzioni applicazione

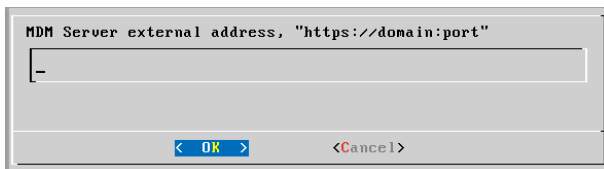
3. Seleziona **Configura indirizzo esterno server MDM**.



Configura la finestra del Server di comunicazione

4. Inserisci l'indirizzo esterno.

Usa la seguente sintassi: `https://<IP/Domain>:<Port>`.



Finestra inserimento indirizzo esterno server MDM

- Se usi la mappatura della porta, devi inserire l'indirizzo IP pubblico o il nome del dominio e la porta aperta sul gateway.
- Se utilizzi un indirizzo pubblico per il Server di comunicazione, devi inserire l'indirizzo IP pubblico o il nome del dominio e la porta del Server di comunicazione. La porta standard è 8443.


5. Seleziona **OK** per salvare le modifiche.

5.9.2. Crea e organizza utenti personalizzati

In assenza di Active Directory, devi prima creare gli utenti personalizzati per avere un mezzo per identificare i proprietari dei dispositivi mobile. Gli utenti dei dispositivi mobile specificati non sono collegati in alcun modo con Active Directory o con altri utenti definiti nella Control Center.

Creazione di utenti personalizzati

Per creare un utente personalizzato:

1. Vai alla pagina **Rete**.
2. Seleziona **Dispositivi mobile** dal selettore di visualizzazioni.
3. Nel pannello a sinistra, seleziona **Gruppi personalizzati**.
4. Clicca sull'icona  **Aggiungi utente** sulla barra degli strumenti. Apparirà la finestra di configurazione.
5. Indica i dettagli dell'utente richiesto:
 - Un nome utente specifico (per esempio, il nome dell'utente)
 - Indirizzo e-mail dell'utente




Importante

- Assicurati di fornire un indirizzo e-mail valido. L'utente riceverà le istruzioni di installazione via e-mail, quando aggiungerai un dispositivo.
- Ogni indirizzo e-mail può essere associato con un solo utente.

6. Clicca su **OK**.


Organizzare gli utenti personalizzati

Per organizzare gli utenti personalizzati:

1. Crea gruppi personalizzati.
 - a. Seleziona **Gruppi personalizzati** nel pannello a sinistra e clicca sull'icona  **Aggiungi** nella barra degli strumenti (sopra al pannello).
 - b. Inserisci un nome specifico per il gruppo e clicca su **OK**. Il nuovo gruppo viene mostrato in **Gruppi personalizzati**.
2. Sposta gli utenti personalizzati nei gruppi personalizzati appropriati.
 - a. Seleziona gli utenti nel pannello a destra.
 - b. Trascina e rilascia l'elemento selezionato sul gruppo desiderato nel pannello a sinistra.

5.9.3. Aggiungi dispositivi agli utenti

Per aggiungere un dispositivo a un utente:

1. Vai alla pagina **Rete**.
2. Seleziona **Dispositivi mobile** dal selettore di visualizzazioni.
3. Cerca l'utente nelle cartelle di Active Directory o nei Gruppi personalizzati.
4. Clicca sull'icona  **Aggiungi dispositivo** nel lato superiore della tabella della rete. Apparirà la finestra di configurazione.

Add device

Device name:

Auto-configure name

Ownership:

Show activation credentials

OK Cancel

Aggiungi un dispositivo mobile a un utente

- Inserisci un nome specifico per il dispositivo.
- Usa l'opzione **Configura nome automaticamente** se desideri che il nome del dispositivo venga generato automaticamente. Una volta aggiunto, il dispositivo ha un nome generico. Una volta che il dispositivo è attivato, viene rinominato automaticamente con le corrispondenti informazioni su produttore e modello.
- Seleziona il tipo di proprietà del dispositivo (Aziendale o personale).
- Seleziona l'opzione **Mostra credenziali di attivazione** dopo aver cliccato sul pulsante **OK**, se stai installando il GravityZone Mobile Client sul dispositivo dell'utente.
- Clicca su **OK**. All'utente viene inviata immediatamente un'e-mail con le istruzioni di installazione e i dettagli per configurare l'attivazione sul dispositivo. I dettagli per l'attivazione includono il token di attivazione e l'indirizzo del Server di comunicazione (e il corrispondente codice QR).



Nota

- Puoi visualizzare i dettagli dell'attivazione di un dispositivo in qualsiasi momento, cliccando sul suo nome nella Control Center.
- Puoi anche aggiungere i dispositivi mobile a una selezione di utenti e gruppi. In questo caso, la finestra di configurazione consentirà di definire solo la proprietà dei dispositivi. Ai dispositivi mobile creati con una selezione multipla sarà assegnato un nome generico. Non appena un dispositivo viene inserito,

il suo nome sarà modificato automaticamente, includendo le corrispondenti informazioni relative a produttore e modello.

5.9.4. Installa GravityZone Mobile Client sui dispositivi

L'applicazione GravityZone Mobile Client è distribuita esclusivamente tramite App Store di Apple e Google Play.

Per installare GravityZone Mobile Client su un dispositivo:

1. Cerca l'applicazione sul relativo store ufficiale.
 - [Link Google Play](#)
 - [Link App Store di Apple](#)
2. Scarica e installa l'applicazione sul dispositivo.
3. Avvia l'applicazione ed effettua la configurazione richiesta:
 - a. Sui dispositivi Android, tocca **Attiva** per attivare GravityZone Mobile Client come amministratore del dispositivo. Leggi attentamente le informazioni fornite.

Nota

- L'attività di blocco per dispositivi Android (7.0 o superiore) imporrà la password impostata nella console di GravityZone, solo se non vi è alcuna protezione di blocco configurata sul dispositivo. Diversamente, per proteggere il dispositivo saranno utilizzate le opzioni della schermata di blocco esistenti, come Schema, PIN, Password, Impronta digitale o Smart Lock.
 - L'attività di sblocco non è più disponibile per i dispositivi Android (7.0 o superiore).
 - A causa di limiti tecnici, le attività Elimina contenuti e Blocca non sono disponibili su Android 11.
- b. Inserisci il token di attivazione e l'indirizzo del Server di comunicazione, o, in alternativa, esamina il codice QR ricevuto via e-mail.
 - c. Tocca **Affidabile** quando ti viene chiesto di accettare il certificato del Server di comunicazione. In questo modo, GravityZone Mobile Client convalida il Server di comunicazione e accetterà solo i messaggi da esso, impedendo attacchi man-in-the-middle.

- d. Tocca **Attiva**.
- e. Nei dispositivi iOS, ti sarà chiesto di installare il profilo MDM. Se il tuo dispositivo è protetto da una password, ti sarà chiesto di fornirla. Inoltre, devi consentire a GravityZone di accedere alle impostazioni del tuo dispositivo, altrimenti il processo di installazione tornerà al passaggio precedente. Segui le istruzioni sullo schermo per completare l'installazione del profilo.

**Nota**

Affinché la funzionalità Localizza funzioni correttamente, è necessario consentire il rilevamento della posizione in background dei dispositivi, non solo mentre viene utilizzata la app.

5.10. Installare il Report Builder

Il Report Builder ti consente di creare e gestire query e rapporti dettagliati basati su query in GravityZone.

Report Builder consiste in due ruoli: Database e Processors, che sono inclusi nella Virtual Appliance di GravityZone e devono essere installati separatamente l'uno dall'altro e dagli altri ruoli di GravityZone. Dopo aver installato Report Builder, l'ambiente di GravityZone deve eseguire almeno tre istanze della Virtual Appliance di GravityZone, come segue:

- Una o più istanze della Virtual Appliance di GravityZone con tutti i ruoli installati, tranne Report Builder Database e Report Builder Processors.
- Un'istanza della Virtual Appliance di GravityZone con il ruolo Report Builder Database installato.
- Un'istanza della Virtual Appliance di GravityZone con il ruolo Report Builder Processors installato.

Per un'installazione agevole, assicurati che l'ambiente virtuale soddisfi i requisiti hardware e software. Poi, devi avere a portata di mano:

- L'immagine della Virtual Appliance di GravityZone, che userai per installare i ruoli Report Builder Database e Report Builder Processors.
- Il nome del DNS o l'indirizzo IP della Virtual Appliance di GravityZone che ha il ruolo GravityZone Database installato.
- Nome utente e password di un amministratore del dominio.

- Password per il database di GravityZone. Nel caso l'avessi dimenticata, puoi crearne un'altra nell'interfaccia della console della appliance di GravityZone.

L'installazione del Report Builder implica due passaggi:

- [Installare il database del Report Builder](#)
- [Installare Processori del Report Builder](#)

Come migliore prassi, prima installa GravityZone e configura la Control Center (se necessario), poi aggiorna GravityZone, impiega la protezione sugli endpoint e alla fine, installa i ruoli del Report Builder.

Importante

È necessario prima installare il ruolo Report Builder Database, poi il ruolo Report Builder Processors.

5.10.1. Installare il database del Report Builder

Report Builder Database è il primo ruolo che devi installare. Per installare questo ruolo:

1. Importa la Virtual Appliance di GravityZone nel tuo ambiente virtualizzato.
2. Alimenta la appliance.
3. Dal tuo strumento di gestione della virtualizzazione, accedi all'interfaccia della Virtual Appliance di GravityZone.
4. Configura la password per l'amministratore del sistema `bdadmin` integrato.
5. Accedi con la password che hai impostato per accedere all'interfaccia di configurazione della appliance. Usa i tasti freccia e il tasto `Tab` per spostarti nei menu e nelle opzioni. Premi `Invio` per selezionare un'opzione specifica.

Inizialmente, l'interfaccia della appliance è in inglese.

Per cambiare la lingua dell'interfaccia:

- a. Seleziona **Configura lingua** dal menu principale.
- b. Seleziona la lingua dalle opzioni disponibili. Apparirà un messaggio di conferma.

Nota

Potresti dover scorrere verso il basso per visualizzare la tua lingua.

- c. Seleziona **OK** per salvare le modifiche.

6. Vai alla voce **Impostazioni avanzate** e seleziona **Connetti a database esistente**.
7. Inserisci l'indirizzo IP e la password del database di GravityZone.
8. Dal menu **Impostazioni avanzate**, seleziona **Installa/Disinstalla ruoli**.
9. Vai alla voce **Aggiungi o rimuovi ruoli** e seleziona **Report Builder Database**. Premi la **Barra spaziatrice** per scegliere di installare questo ruolo e **Invio** per continuare. Premi ancora **Invio** per confermare e attendi il completamento della disinstallazione.

**Nota**

Il Database del Report Builder viene installato e funziona solamente come istanza indipendente. I backup dei set di replica non sono supportati.

5.10.2. Installare Processori del Report Builder

Report Builder Processors è il secondo ruolo che devi installare. Per installare questo ruolo:

1. Importa la Virtual Appliance di GravityZone nel tuo ambiente virtualizzato.
2. Alimenta la appliance.
3. Dal tuo strumento di gestione della virtualizzazione, accedi all'interfaccia della Virtual Appliance di GravityZone.
4. Configura la password per l'amministratore del sistema `bdadmin` integrato.
5. Accedi con la password che hai già impostato. Accederai all'interfaccia di configurazione della appliance. Usa i tasti freccia e il tasto **Tab** per spostarti nei menu e nelle opzioni. Premi **Invio** per selezionare un'opzione specifica.

Inizialmente, l'interfaccia della appliance è in inglese.

Per cambiare la lingua dell'interfaccia:

- a. Seleziona **Configura lingua** dal menu principale.
- b. Seleziona la lingua dalle opzioni disponibili. Apparirà un messaggio di conferma.

**Nota**

Potresti dover scorrere verso il basso per visualizzare la tua lingua.

- c. Seleziona **OK** per salvare le modifiche.

6. Vai alla voce **Impostazioni avanzate** e seleziona **Connetti a database esistente**.
7. Inserisci l'indirizzo IP e la password del database di GravityZone.
8. Dal menu **Impostazioni avanzate**, seleziona **Installa/Disinstalla ruoli**.
9. Vai alla voce **Aggiungi o rimuovi ruoli** e seleziona **Report Builder Processors**. Premi la **Barra spaziatrice** per scegliere di installare questo ruolo e **Invio** per continuare. Premi ancora **Invio** per confermare e attendi il completamento della disinstallazione.



Nota

Report Builder Processors viene installato e funziona solamente come istanza indipendente.

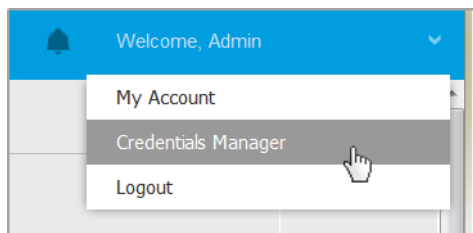
Dopo aver installato il Report Builder, verrà mostrata la nuova opzione del menu **Query** nella sezione **Rapporti** della Control Center.

I ruoli Database e Processori del Report Builder vengono visualizzati nella sezione **Infrastruttura** della pagina **Configurazione > Aggiornamento**, insieme agli altri ruoli di GravityZone.

5.11. Credentials Manager

I Credential Manager ti aiutano a definire le credenziali richieste per accedere agli inventari disponibili del vCenter Server e anche all'autenticazione remota su diversi sistemi operativi nella tua rete.

Per aprire il Credentials Manager, clicca sul tuo nome utente nell'angolo in alto a destra della pagina e seleziona **Credentials Manager**.



Il menu Credentials Manager

La finestra **Credentials Manager** contiene due schede:

- Sistema operativo
- Ambiente virtuale

5.11.1. Sistema operativo

Dalla scheda **Sistema operativo**, puoi gestire le credenziali amministrative richieste per l'autenticazione remota durante le attività di installazione inviate ai computer e alle macchine virtuali nella tua rete.

Per aggiungere un set di credenziali:

Username	Password	Description		
User	Password	Description		Action

Credentials Manager

1. Inserisci il nome utente e la password di un account da amministratore per ciascun sistema operativo bersaglio nei campi corrispondenti nella parte superiore dell'installazione della tabella. In alternativa, puoi aggiungere una descrizione che ti aiuterà a identificare ogni account più facilmente. Se i computer sono in un dominio, è sufficiente inserire le credenziali dell'amministratore del dominio.

Usa le convenzioni di Windows nell'inserire il nome di un account utente:

- Per le macchine Active Directory, utilizza queste sintassi: `username@domain.com` e `domain\username`. Per assicurare che le credenziali inserite funzioneranno, aggiungile in entrambi i moduli (`username@domain.com` e `domain\username`).
 - Per le macchine Workgroup, è sufficiente inserire solo il nome utente senza il nome del gruppo di lavoro.
2. Clicca sul pulsante **+Aggiungi** nel lato destro della tabella. Il nuovo set di credenziali viene aggiunto alla tabella.

**Nota**

Se non hai specificato le credenziali di autenticazione, ti sarà richiesto di inserirle all'esecuzione delle attività di installazione. Le credenziali indicate vengono salvate automaticamente nel tuo Credentials manager, in modo che non dovrai inserirle le prossime volte.

5.11.2. Ambiente virtuale

Dalla scheda Ambiente virtuale, puoi gestire le credenziali di autenticazione per i sistemi server virtualizzati disponibili.

Per accedere all'infrastruttura virtualizzata integrata con la Control Center, devi fornire le tue credenziali utente per ciascun sistema server virtualizzato disponibile. La Control Center utilizza le tue credenziali per connettersi all'infrastruttura virtualizzata, mostrando solo le risorse a cui hai accesso (come definito nel server virtualizzato).

Per specificare le credenziali richieste per connettersi a un server virtualizzato:

1. Seleziona il server dal menu corrispondente.

**Nota**

Se il menu non è disponibile, non è ancora stata configurata alcuna integrazione o tutte le credenziali necessarie sono già state configurate.

2. Inserisci il tuo nome utente e la password, oltre a una apposita descrizione.
3. Clicca sul pulsante **+** **Aggiungi**. Il nuovo set di credenziali viene aggiunto alla tabella.

**Nota**


Se non configuri le tue credenziali di autenticazione nel Credentials Manager, dovrai inserirle quando cercherai di esplorare l'inventario di ogni sistema server virtualizzato. Una volta inserite le tue credenziali, saranno salvate nel tuo Credentials Manager in modo che non dovrai più reinserirle la volta successiva.

**Importante**

Ogni volta che modifichi la password utente del server virtualizzato, ricordati di aggiornarla anche nel Credentials Manager.

5.11.3. Eliminare le credenziali dal Credentials Manager

Per eliminare credenziali obsolete dal Credentials Manager:

1. Cerca la riga nella tabella contenente le credenziali che vuoi eliminare.
2. Clicca sul pulsante  **Elimina** sul lato destro della corrispondente riga della tabella. L'account selezionato sarà eliminato.

6. AGGIORNARE GRAVITYZONE

Bitdefender pubblica tutti gli aggiornamenti del prodotto e del contenuto di sicurezza attraverso i server di Bitdefender su Internet. Tutti gli aggiornamenti sono cifrati e firmati digitalmente, in modo che non possano essere manomessi.

GravityZone include un ruolo di Server di aggiornamento, progettato per funzionare come punto di distribuzione degli aggiornamenti centralizzato per il tuo impiego di GravityZone. Il Server di aggiornamento verifica e scarica tutti gli aggiornamenti di GravityZone disponibili dai server di aggiornamento di Bitdefender su Internet, rendendoli disponibili alla rete locale. I componenti di GravityZone possono essere configurati per aggiornarsi automaticamente dal server di aggiornamento locale invece che da Internet.

Quando è disponibile un nuovo aggiornamento, la appliance di GravityZone, l'agente di sicurezza o il Security Server controllano la firma digitale dell'aggiornamento per verificarne l'autenticità, e i contenuti del pacchetto per l'integrità. Poi, ciascun file dell'aggiornamento viene analizzato e la sua versione verificata rispetto a quella installata. I file più nuovi vengono scaricati a livello locale e controllati nuovamente nell'hash MD5 per assicurarsi che non siano stati alterati.

Se un controllo non viene superato in qualsiasi momento, il processo di aggiornamento si blocca, fornendo un errore. Diversamente, l'aggiornamento viene considerato valido e pronto per essere installato.

Per aggiornare le appliance di GravityZone installate nel tuo ambiente e i pacchetti di installazione dei componenti di GravityZone, accedi con un account di amministratore dell'azienda e vai alla pagina **Configurazione e Aggiornamento**.

6.1. Aggiornare le appliance di GravityZone

Tramite gli aggiornamenti della appliance di GravityZone, Bitdefender rilascia nuove funzionalità e miglioramenti di quelle esistenti. Queste sono visibili in Control Center.

Prima di eseguire un aggiornamento, si consiglia di controllare le seguenti cose:

- Lo stato di aggiornamento
- Qualsiasi informazione o messaggio di avviso che può apparire.
- Il registro delle modifiche

Per controllare lo stato di aggiornamento:

1. Vai alla pagina **Configurazione > Aggiornamento > Ruoli di GravityZone**
2. Nella sezione **Stato attuale**, puoi visualizzare il messaggio che indica lo stato generale della tua implementazione. Se GravityZone richiede un aggiornamento, il pulsante **Aggiorna** diventa disponibile.
3. Nella sezione **Infrastruttura**, puoi analizzare i dettagli per ogni ruolo di GravityZone impiegato nella tua rete. Poiché i ruoli si aggiornano in modo indipendente, per ogni ruolo puoi visualizzare: il nome della appliance che lo ospita, il suo indirizzo IP, la versione attuale, la versione più recente disponibile e lo stato di aggiornamento.

Per controllare il registro delle modifiche:

1. Vai alla pagina **Configurazione > Aggiornamento > Ruoli di GravityZone**
2. Clicca sul link **Vedi registro delle modifiche**. Una finestra pop-up mostrerà un elenco con tutte le versioni e le modifiche che includono.

Le note di rilascio per ogni nuova versione del prodotto vengono anche pubblicate nel [Centro di Supporto di Bitdefender](#).

Puoi aggiornare GravityZone in due modi:

- [Manualmente](#)
- [Automaticamente](#)

6.1.1. Aggiornamento Manuale

Scegli questo metodo se vuoi avere il controllo totale di quando eseguire l'aggiornamento.

Per aggiornare GravityZone manualmente:

1. Vai alla pagina **Configurazione > Aggiornamento > Ruoli di GravityZone**
2. Clicca sul pulsante **Aggiorna** (se disponibile).

L'aggiornamento può richiedere un po' di tempo. Attendi che venga completato.

3. Svuota la cache del browser.

Durante l'aggiornamento, Control Center disconnette tutti gli utenti e li informa dei progressi dell'aggiornamento. Potrai visualizzare informazioni dettagliate sull'avanzamento del processo di aggiornamento.

Una volta completato l'aggiornamento, Control Center mostra la pagina di accesso.

6.1.2. Aggiornamento automatico

Installando gli aggiornamenti automaticamente, ti assicuri che GravityZone sia sempre aggiornato con tutte le nuove funzionalità e patch di sicurezza.

GravityZone ha due tipi di aggiornamenti automatici:

- [Aggiornamenti prodotto](#)
- [Aggiornamenti software di terze parti](#)

Aggiornamenti prodotto

Questi aggiornamenti apportano nuove funzionalità in GravityZone, risolvendo alcuni problemi derivanti da esse.

Dato che gli aggiornamenti possono essere un disturbo per gli utenti di GravityZone, sono progettati per essere eseguiti in base a un determinato programma. Puoi programmare l'aggiornamento per gli orari che preferisci. Di norma, gli aggiornamenti automatici del prodotto sono disattivati.

Per attivare e programmare gli aggiornamenti del prodotto:

1. Vai alla pagina **Configurazione > Aggiornamento > Ruoli di GravityZone**.
2. Seleziona la casella **Attiva aggiornamenti automatici prodotto GravityZone**.
3. Imposta la **Ricorrenza** su **Giornaliera**, **Settimanale** (seleziona uno o più giorni feriali) o **Mensile**.
4. Definisci un **Intervallo**. Puoi programmare un momento per iniziare il processo di aggiornamento quando è disponibile un nuovo aggiornamento.

Di norma, GravityZone mostra un messaggio di avviso a tutti gli utenti di Control Center 30 minuti prima dell'avvio dell'aggiornamento automatico. Per disattivare l'avviso, deseleziona la casella **Attiva l'avviso di inattività di 30 minuti prima dell'aggiornamento**.

Aggiornamenti software di terze parti

La virtual appliance di GravityZone integra una serie di prodotti software forniti da altri fornitori. Questo tipo di aggiornamenti mira a patchare tempestivamente tali software, riducendo i possibili rischi per la sicurezza.

Questi aggiornamenti vengono eseguiti silenziosamente e non interrompono il funzionamento di Control Center.

Di norma, questa opzione è attivata. Per disattivare questa opzione:

1. Vai alla pagina **Configurazione > Aggiornamento > Ruoli di GravityZone**.
2. Deseleziona la casella **Attiva gli aggiornamenti di sicurezza automatici per i componenti di terze parti di GravityZone**.

Le patch per i software di terze parti saranno quindi rilasciati con l'aggiornamento del prodotto GravityZone.

6.2. Configurare il server di aggiornamento

Di norma, il Server di aggiornamento scarica gli aggiornamenti da Internet ogni ora. Si consiglia di non modificare le impostazioni standard del Server di aggiornamento.

Per controllare e configurare le impostazioni del Server di aggiornamento:

1. Vai alla pagina **Aggiorna** nella Control Center e clicca sulla scheda **Componenti**.
2. Clicca sul pulsante **Impostazioni** nella parte superiore del pannello sul lato sinistro per visualizzare la finestra **Impostazioni Server di aggiornamento**.
3. In **Configurazione Server di aggiornamento**, puoi controllare e configurare le impostazioni principali.
 - **Indirizzo pacchetti**. L'indirizzo da cui i pacchetti vengono scaricati.
 - **Indirizzo aggiornamento**. Il Server di aggiornamento è configurato per controllare e scaricare gli aggiornamenti da `upgrade.bitdefender.com:80`. Si tratta di un indirizzo generico che viene automaticamente rivolto al server più vicino con gli aggiornamenti di Bitdefender nella tua regione.
 - **Porta**. Configurando i vari componenti di GravityZone per l'aggiornamento dal Server di aggiornamento, devi fornire questa porta. La porta standard è 7074.
 - **IP**. L'indirizzo IP del Server di aggiornamento.
 - **Periodo aggiornamento (ore)**. Se vuoi modificare il periodo di aggiornamento, inserisci un nuovo valore in questo campo. Il valore predefinito è 1.
4. Puoi configurare il Server di aggiornamento per scaricare automaticamente i kit del Security Server ed endpoint.

5. Il Server di aggiornamento può funzionare come gateway per l'invio dei dati dai prodotti client di Bitdefender installati nella rete per i server di Bitdefender. Questi dati possono includere rapporti anonimi sulle attività dei virus, segnalazioni sui blocchi del prodotto e dati per la registrazione online. Attivare i ruoli di gateway è utile per il controllo del traffico e nelle reti senza accesso a Internet.

**Nota**

Puoi disattivare i moduli del prodotto che inviano dati statistici o relativi a blocchi ai laboratori di Bitdefender in qualsiasi momento. Puoi utilizzare le policy per controllare in remoto queste opzioni sui computer e le virtual machine gestite dalla Control Center.

6. Clicca su **Salva**.

6.3. Scaricare gli aggiornamenti del prodotto

Puoi visualizzare informazioni sui pacchetti dei componenti di GravityZone esistenti nella scheda **Componenti**. Le informazioni disponibili includono la versione attuale, la versione dell'aggiornamento (se disponibile) e lo stato delle operazioni di aggiornamento eventualmente avviate.

Per aggiornare un componente di GravityZone:

1. Vai alla pagina **Aggiorna** nella Control Center e clicca sulla scheda **Componenti**.
2. Clicca sul componente che vuoi aggiornare nell'elenco **Prodotto**. Tutte le versioni disponibili saranno mostrate nella tabella **Pacchetti**. Seleziona la casella corrispondente alla versione che vuoi scaricare.

**Nota**

I nuovi pacchetti saranno nello stato **Non scaricato**. Una volta rilasciata una versione più aggiornata da Bitdefender, la versione più datata e non scaricata sarà rimossa dalla tabella.

3. Clicca su **Azioni** nel lato superiore della tabella e seleziona **Pubblica**. Sarà scaricata la versione selezionata e lo stato cambierà di conseguenza. Aggiorna i contenuti della tabella, cliccando sul pulsante **Aggiorna** e verifica lo stato corrispondente.

**Importante**

Di norma, la appliance di GravityZone non include i pacchetti del Security Server. Devi scaricare manualmente i pacchetti del Security Server necessari al tuo ambiente.

6.4. Testare gli aggiornamenti

La fase di prova ti consente di testare i kit o gli aggiornamenti del prodotto più recenti in un ambiente chiuso e controllato, prima di pubblicarli nella rete. L'ambiente di prova dovrebbe rispecchiare quello produttivo il più possibile, per un testing efficace. In questo modo puoi massimizzare le tue opportunità di scovare ogni problema che potrebbe verificarsi nel tuo ambiente, prima di rilasciare la versione nella fase produttiva.

La funzionalità di test ti consente anche di creare una policy per gli endpoint più importanti nell'ambiente produttivo. Puoi aggiornare questi endpoint solo dopo che gli aggiornamenti sono stati testati nello specifico ambiente e sulle macchine non fondamentali dell'ambiente produttivo. Per maggiori dettagli, fai riferimento a [«Pubblicare con i ring di aggiornamento»](#) (p. 197).

**Nota**

- Di norma, la fase di test è disattivata.
- Security Server (VMware con NSX) non supporta la fase di test.
- BEST for Windows Legacy non supporta la fase di test. Gli endpoint "legacy" in posizione di staging deve essere portati in posizione di produzione.

6.4.1. Prerequisiti

La modalità di test richiede che l'infrastruttura di GravityZone soddisfi le seguenti condizioni:

- Il Server di aggiornamento deve essere installato da solo sulla virtual appliance. Se il Server di aggiornamento è presente sulla appliance con altri ruoli, devi seguire questi passaggi:
 1. Elimina il vecchio ruolo di Server di aggiornamento.
 2. Impiega una nuova appliance di GravityZone.

**Importante**

Non è stato ancora installato alcun ruolo.

3. Connetti la nuova appliance al database di GravityZone esistente.
4. Installa il ruolo server di aggiornamento sulla nuova appliance.

Per maggiori informazioni sull'installazione dei ruoli di GravityZone, fai riferimento a «[Gestire la appliance di GravityZone](#)» (p. 105).

- La appliance del Server di aggiornamento deve essere di almeno 120 GB.
- La appliance della Console web deve essere di almeno 120 GB.

6.4.2. Usare la fase di test

Per impostare l'ambiente di test e provare gli ultimi aggiornamenti, devi:

1. [Attivare la fase di test e definire le impostazioni del Server di aggiornamento.](#)
2. [Definisci una policy di test per testare gli endpoint.](#)
3. [Installa i pacchetti nell'endpoint di test.](#)
4. [Assegna la policy della fase di test per il testing degli endpoint.](#)
5. [Aggiorna gli endpoint di test alla versione più recente e testa l'aggiornamento nello specifico ambiente.](#)
6. [Esegui un secondo test prima di aggiornare tutti gli endpoint nell'ambiente produttivo. Puoi testare l'aggiornamento prima sugli endpoint non critici.](#)

Attivare la fase di test

Per attivare la modalità di test per gli aggiornamenti di GravityZone:

1. Vai alla pagina **Configurazione > Aggiornamento** e clicca sulla tabella **Componenti**.
2. Clicca sul pulsante **Impostazioni** nella parte superiore del pannello sul lato sinistro per visualizzare la finestra **Impostazioni Server di aggiornamento**.
3. Seleziona la casella **Attiva la fase di test**.
4. In **Configurazione Server di produzione**, configura le impostazioni principali:
 - **Indirizzo pacchetti.** L'indirizzo da cui i pacchetti vengono scaricati: `download.bitdefender.com/SMB/Hydra/release`
 - **Indirizzo aggiornamento.** L'indirizzo da cui vengono scaricati gli aggiornamenti del prodotto: `upgrade.bitdefender.com:80`.

- **Porta.** La porta standard è 7074. Non puoi modificare questa voce.
 - **IP.** L'indirizzo IP del Server di aggiornamento. Non puoi modificare questa voce.
 - **Periodo aggiornamento (ore).** Se vuoi modificare il periodo di aggiornamento, inserisci un nuovo valore in questo campo. Il valore predefinito è 1.
5. Il Server di aggiornamento e di produzione può funzionare come gateway per l'invio dei dati dai prodotti client di Bitdefender installati nella rete ai server di Bitdefender. Questi dati possono includere rapporti anonimi sulle attività dei virus, segnalazioni sui blocchi del prodotto e dati per la registrazione online. Attivare i ruoli di gateway è utile per il controllo del traffico e nelle reti senza accesso a Internet.



Nota

Puoi disattivare i moduli del prodotto che inviano dati statistici o relativi a blocchi ai laboratori di Bitdefender in qualsiasi momento. Puoi utilizzare le policy per controllare in remoto queste opzioni sui computer e le virtual machine gestite dalla Control Center.

6. In **Configurazione server di test**, configura le seguenti opzioni:
- **Porta.** La porta predefinita è 7077.
 - **IP.** L'indirizzo IP del Server di aggiornamento. Non puoi modificare questa voce.
7. In **Pacchetti**, puoi configurare il Server di aggiornamento per scaricare e pubblicare automaticamente i kit del Security Server ed endpoint.

Packages

Automatically download security server kits

Automatically publish newest downloaded kit version

Security Server (VMware)

Security Server (Microsoft Hyper-V)

Security Server (Citrix XenServer)

Security Server (ESXi standalone)

Automatically download endpoint kits

Keep maximum (kits):

Pacchetti - Pubblicazione automatica

Puoi anche configurare il numero massimo di kit che puoi memorizzare nella appliance di GravityZone. Inserisci un numero tra 4 e 10 nel menu **Mantieni il massimo (kit)**.

8. In **Aggiornamento prodotti**, puoi configurare il Server di aggiornamento per scaricare automaticamente gli aggiornamenti per gli agenti di sicurezza.

Products Update

Automatically download updates

Automatically publish newest downloaded version

BEST (Windows)

BEST (Linux)

Endpoint Security for Mac

Source Ring:

Destination ring:

Keep maximum (updates):

Pacchetti - Pubblicazione automatica

Puoi scegliere anche di pubblicare automaticamente le versioni scaricate più recenti:

- a. Seleziona almeno un agente di sicurezza dall'elenco disponibile.
- b. Definisci i ring sorgente e di destinazione:
 - **Ring sorgente.** Il ring usato per inviare gli aggiornamenti nell'ambiente di test. Quando una versione viene convalidata dai suoi primi utilizzatori, sarà pubblicata nel ring lento. Questo è il valore predefinito. I nuovi aggiornamenti disponibili saranno pubblicati nel ring veloce.
 - **Ring di destinazione.** Il ring usato per pubblicare gli aggiornamenti nell'ambiente di produzione. Puoi scegliere tra lento e veloce.

Puoi anche configurare il numero massimo di aggiornamenti che puoi memorizzare nella appliance di GravityZone. Inserisci un numero tra 4 e 10 nel menu **Mantieni il massimo (aggiornamenti)**.

9. Clicca su **Salva**.

Una volta attivata la fase di test, crea il tuo ambiente di test per iniziare a testare i kit e gli aggiornamenti disponibili del prodotto.



Importante

Disattivando la fase di test eliminerai tutti i pacchetti non pubblicati e gli aggiornamenti del prodotto.

Definire la policy della fase di test

Devi definire una policy della fase di test:

1. Vai alla pagina **Policy**
2. Seleziona o crea una policy da utilizzare nell'ambiente di test.
3. Nella sezione **Generale > Aggiornamento**, inserisci l'indirizzo del Server di test nella tabella **Ubicazioni aggiornamento**.
4. Configura le altre impostazioni della policy come necessario. Per maggiori dettagli, fai riferimento al capitolo **Policy di sicurezza** della Guida per gli amministratori di GravityZone.
5. Clicca su **Salva**.

Testare i pacchetti

Per installare il pacchetto più recente negli endpoint di test:

1. Vai alla pagina **Configurazione > Aggiornamento** e seleziona la scheda **Componenti**.
2. Clicca su **Controlla disponibilità aggiornamenti** per assicurarti di visualizzare l'ultima versione rilasciata del prodotto.
3. Clicca sul componente che vuoi aggiornare nell'elenco **Prodotto**.
4. Seleziona un pacchetto disponibile nella tabella **Pacchetti**, che vuoi testare. Puoi scaricare diversi kit per ogni prodotto, fino al limite indicato nella finestra **Impostazioni Server di aggiornamento**. Una volta raggiunto il limite, la versione più vecchia viene rimossa dalla tabella.
5. Clicca su **Azioni** e seleziona **Download** per ottenere il pacchetto nella tua appliance di GravityZone.
6. Con il pacchetto selezionato, clicca su **Salva sul disco**. Viene visualizzata la finestra di configurazione del pacchetto.
7. Configura il pacchetto. Per maggiori informazioni, fai riferimento a [«Creare i pacchetti di installazione»](#) (p. 137).
8. Installa il kit sugli endpoint di test.
9. Monitora il comportamento degli endpoint.
10. Se il pacchetto è stato installato con successo e gli endpoint hanno un comportamento normale, puoi pubblicare il pacchetto nella rete di produzione. Per pubblicare un pacchetto, selezionalo nella tabella **Pacchetti**, clicca su **Azioni** nel lato superiore della tabella e seleziona **Pubblica**.




Importante

Non puoi pubblicare pacchetti più vecchi di uno già pubblicato.

11. Se riscontrassi problemi con il pacchetto, puoi creare un ticket di supporto. Per maggiori dettagli, fai riferimento a [«Ottenere aiuto»](#) (p. 218).
Per eliminare un pacchetto dalla appliance di GravityZone, clicca sul pulsante **Azione** e seleziona **Elimina dal disco**.

Assegnare le policy della fase di test

Per assegnare la policy della fase di test agli endpoint di test:

1. Vai alla pagina **Rete**.
2. Seleziona **Computer e Macchine Virtuali** dal selettore di visualizzazione.
3. Seleziona il gruppo desiderato dal pannello a sinistra. Tutti i computer del gruppo selezionato sono mostrati nella tabella a destra.
4. Seleziona la casella del computer o del gruppo che desideri. Puoi selezionare uno o più elementi dello stesso tipo solo dallo stesso livello.
5. Clicca sul pulsante  **Aggiungi policy** nel lato superiore della tabella.
6. Effettua le impostazioni necessarie nella finestra di assegnazione della policy. Per maggiori informazioni, fai riferimento al capitolo **Policy di sicurezza > Gestire le policy > Assegnare le policy agli endpoint** nella Guida per gli amministratori di GravityZone.

Testare gli aggiornamenti del prodotto

Per installare gli ultimi aggiornamenti:

1. Vai alla pagina **Configurazione > Aggiornamento** e seleziona la scheda **Componenti**.
2. Clicca su **Controlla disponibilità aggiornamenti** per assicurarti di visualizzare l'ultima versione rilasciata del prodotto.
3. Seleziona il prodotto Bitdefender desiderato nell'elenco **Prodotto**.



Nota

Puoi usare la fase di test solo con gli aggiornamenti per gli agenti di sicurezza e non per i Security Server.

4. Seleziona un aggiornamento disponibile nella tabella **Aggiornamenti**, che vuoi testare.
5. Clicca su **Azioni** e seleziona **Scarica** per ottenere l'aggiornamento della tua appliance di GravityZone.

Puoi scaricare diversi aggiornamenti per ogni prodotto, fino al limite indicato nella finestra **Impostazioni Server di aggiornamento**. Una volta raggiunto il limite, la versione più vecchia viene rimossa dalla tabella.

6. Una volta selezionato un aggiornamento, clicca su **Azioni** e seleziona **Aggiungi a fase di test**. L'aggiornamento sarà installato negli endpoint di test, in base alle impostazioni della policy. Per maggiori dettagli, fai riferimento a «[Definire la policy della fase di test](#)» (p. 194).
7. Se l'aggiornamento è stato installato con successo e gli endpoint hanno un comportamento normale, inizia a inviare l'aggiornamento alle macchine nell'ambiente produttivo. Per iniziare, aggiorna le macchine non critiche, in modo da eseguire un altro test prima di aggiornare gli endpoint critici. Per maggiori dettagli, fai riferimento a «[Pubblicare con i ring di aggiornamento](#)» (p. 197).
8. Se riscontrassi problemi con l'aggiornamento, puoi creare un ticket di supporto. Per maggiori dettagli, fai riferimento a «[Ottenere aiuto](#)» (p. 218).

Per eliminare un aggiornamento non pubblicato della appliance di GravityZone, clicca sul pulsante **Azioni** e seleziona **Elimina**. Puoi eliminare solo gli aggiornamenti non pubblicati.

Pubblicare con i ring di aggiornamento

Per testare l'aggiornamento sugli endpoint non critici dell'ambiente produttivo, devi prima modificare le policy esistenti e assegnare una policy fast ring.

Nota

Una policy slow ring viene assegnata automaticamente a tutte le policy che crei.

1. Vai alla pagina **Policy**
2. Modifica le impostazioni della policy per gli endpoint non critici nell'ambiente produttivo. Nella sezione **Ring di aggiornamento**, seleziona **Fast Ring**.

Nota

L'aggiornamento pubblicato nel fast ring non può essere antecedente a quello pubblicato nello slow ring.

3. Pubblica l'aggiornamento sul fast ring:
 - a. Vai alla pagina **Configurazione > Aggiornamento** e seleziona la scheda **Componenti**.
 - b. Seleziona l'aggiornamento nella tabella Aggiornamento, clicca sul pulsante **Azione** nel lato superiore della tabella e seleziona **Pubblica**.

- c. Seleziona l'opzione Fast Ring.

**Nota**

Quando pubblichi la prima volta un aggiornamento, sarà disponibile su fast e slow ring.

A questo punto, tutti gli endpoint con la policy Fast Ring vengono aggiornati alla versione pubblicata.

4. Monitora il comportamento degli endpoint fast ring.
5. Se l'aggiornamento è stato installato con successo e gli endpoint hanno un comportamento normale, puoi pubblicare l'aggiornamento sullo slow ring:
 - a. Vai alla pagina **Configurazione > Aggiornamento** e seleziona la scheda **Componenti**.
 - b. Seleziona l'aggiornamento nella tabella Aggiornamento, clicca sul pulsante **Azione** nel lato superiore della tabella e seleziona **Pubblica**.
 - c. Seleziona l'opzione Slow Ring.

Ora ogni endpoint dell'ambiente produttivo viene aggiornato alla versione che hai pubblicato.
6. Se riscontrassi problemi con il pacchetto, puoi creare un ticket di supporto. Per maggiori dettagli, fai riferimento a [«Ottenere aiuto»](#) (p. 218).

6.5. Aggiornamenti del prodotto offline

Di norma, GravityZone utilizza un sistema di aggiornamento connesso a Internet. Per le reti isolate, Bitdefender offre un'alternativa, rendendo gli aggiornamenti dei componenti e del contenuto di sicurezza disponibili anche online.

6.5.1. Prerequisiti

Per usare gli aggiornamenti offline, devi:

- Un'istanza di GravityZone installata in una rete con accesso a Internet ("istanza online"). L'istanza online deve avere:
 - Accesso diretto a Internet
 - Accesso alle porte 80 e 443. Per maggiori dettagli sulle porte usate da GravityZone, fai riferimento a [questo articolo della KB](#).

- Aver installato solo i ruoli Database e Server di aggiornamento
- Uno o più istanze di GravityZone installate in una rete senza accesso a Internet ("istanze offline")
- Entrambe le istanze di GravityZone devono avere la stessa versione della appliance

6.5.2. Configurare l'istanza di GravityZone online

Durante questa fase, impiegherai un'istanza di GravityZone in una rete senza accesso a Internet e poi configurarla come server di aggiornamento offline.

1. Impiega GravityZone in una macchina con connessione a Internet.
2. Installa solo i ruoli Database e Server di aggiornamento.
3. Accedi al terminale TTY della macchina nel tuo ambiente virtuale (o connessi tramite SSH).
4. Accedi con l'utente `bdadmin` e la password che hai impostato.
5. Esegui il comando `sudo su` per ottenere i privilegi di **root**.
6. Esegui i seguenti comandi per installare il pacchetto offline `gzou-mirror`:

```
# apt update # gzcli update # apt install gzou-mirror
```

Il `gzou-mirror` ha i seguenti ruoli:

- Configura il Server di aggiornamento per generare automaticamente archivi di aggiornamento offline.
- Imposta un servizio web per l'istanza online, fornendo opzioni di configurazione e download per gli archivi di aggiornamento offline.

6.5.3. Configurare e scaricare i file di aggiornamento iniziali

Durante questa fase, configurerai le impostazioni dell'archivio di aggiornamento tramite il servizio web installato sull'istanza online, creando poi i file dell'archivio richiesti per [configurare l'istanza offline](#). Poi dovrai scaricare i file di aggiornamento e posizionali in un dispositivo multimediale portatile (chiavetta USB).

1. Accedi al servizio web tramite un URL in questa forma: `https://Online-Instance-Update-Server-IP-or-Hostname`, con il nome utente `bdadmin` e la password che hai impostato.

Appliance Status

[Download archives](#) [Generate support bundle](#)

Current job: -

Next archive will be created on: Tue Aug 14 2018 17:55:07 GMT+0300 (Eastern European Summer Time) [Create...](#)

Free disk space: 86.59 GiB

Kits	Settings
<input checked="" type="checkbox"/> Bitdefender Security Tools (BEST)	Archive creation interval (in hours): <input type="text" value="2"/>
<input type="checkbox"/> Bitdefender Security Tools (BEST) Legacy	Number of FULL archives to keep on disk: <input type="text" value="1"/>
<input checked="" type="checkbox"/> Bitdefender Security Tools (BEST)	Number of LITE archives to keep on disk: <input type="text" value="1"/>
<input type="checkbox"/> Bitdefender Endpoint Security	
<input type="checkbox"/> Bitdefender Endpoint Security	
<input type="checkbox"/> Bitdefender Tools	
<input type="checkbox"/> Bitdefender Tools	

[Apply](#)

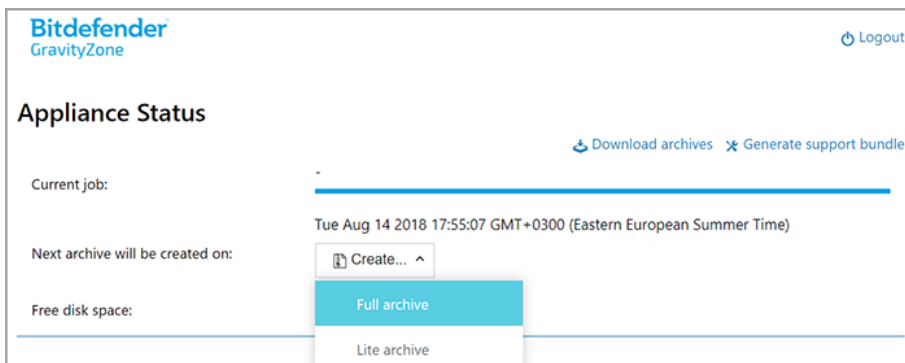
L'istanza online - Servizio web

2. Configura l'archivio di aggiornamento offline come segue:
 - In **Kit**: seleziona i kit agente endpoint che desideri includere nell'archivio di aggiornamento offline.
 - In **Impostazioni**, modifica le tue preferenze dell'archivio di aggiornamento.
Un CRON job installato sull'istanza online controllerà ogni minuto se ci sono nuovi file di aggiornamento disponibili e se lo spazio libero su disco è superiore a 10 GB. A ogni periodo impostato dall'opzione **Intervallo di creazione archivio (in ore)**, il CRON job creerà i seguenti file:
 - **Archivio completo (prodotto + contenuto di sicurezza)**, quando sono disponibili nuovi file di aggiornamento
 - **Archivio semplice** (solo contenuto di sicurezza), quando non ci sono nuovi file di aggiornamento

Gli archivi saranno creati alla seguente posizione:

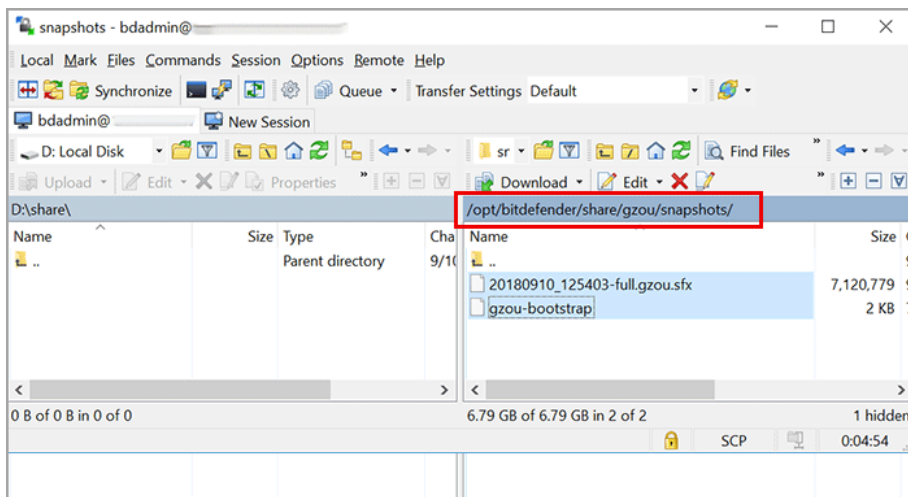
<https://Online-Instance-Update-Server-IP-or-Hostname/snapshots>

3. Clicca su **Crea > Archivio** completo per creare il primo archivio completo. Attendi che l'archivio venga creato.



L'istanza online - Servizio web: creare l'archivio

4. Scarica l'intero archivio di aggiornamento e il file `gzou-bootstrap` dall'istanza online. Hai diverse opzioni a portata di mano:
 - Tramite il servizio web: clicca su **Scarica archivi** per accedere alla pagina contenente i link per i file dell'aggiornamento. Clicca sui link dell'archivio di aggiornamento completo e del file `gzou-bootstrap` per scaricarli sul tuo endpoint.
 - Usa il tuo client SCP/SCTP preferito (per esempio WinSCP) per stabilire una connessione SCP con l'istanza online e trasferire i suddetti file in una posizione nella tua rete online. Il percorso predefinito sull'istanza online è:
`/opt/bitdefender/share/gzou/snapshots`



Trasferire i file di aggiornamento usando SCP

- Tramite condivisione SAMBA. Usa una condivisione SAMBA di sola lettura per recuperare gli archivi di aggiornamento offline dalla seguente posizione:

\\Online-Instance-Update-Server-IP-or-Hostname\gzou-snapshots



Nota

Le credenziali per accedere alla condivisione SAMBA, se richieste, sono le stesse delle credenziali dell'istanza online (utente `badmin` e password).

6.5.4. Configurare l'istanza di GravityZone offline

Durante questa fase, impiegherai e configurerai l'istanza offline per ricevere aggiornamenti tramite gli archivi generati dall'istanza online. Salvo diversamente indicato, tutti i comandi devono essere eseguiti come **root**.

1. Impiega GravityZone in una macchina da un ambiente isolato.
2. Installa solo i ruoli Database e Server di aggiornamento.
3. Trasferisci l'archivio di aggiornamento e il file `gzou-bootstrap` scaricato dall'istanza online in `/home/badmin` directory dell'istanza offline usando un dispositivo multimediale portatile (chiavetta USB).



Importante

Affinché l'aggiornamento offline funzioni, assicurati di:

- L'archivio di aggiornamento e `gzou-bootstrap` sono nella stessa cartella.
- L'archivio di aggiornamento è un archivio **completo**.

4. Esegui il file `gzou-bootstrap` come segue:

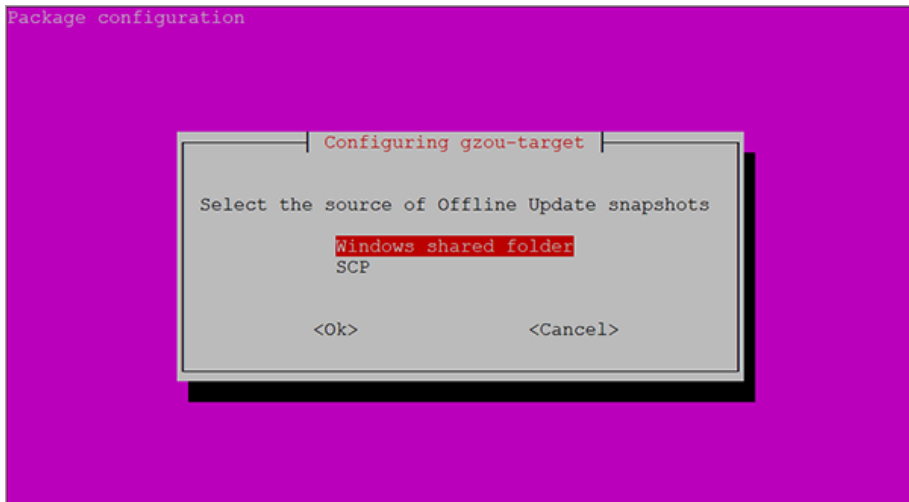
- a. Accedi al termine TTY della macchina nel tuo ambiente virtuale (o connettiti tramite SSH).
- b. Trasformare `gzou-bootstrap` in un eseguibile:

```
#  
chmod +x gzou-bootstrap
```

- c. Esegui: `./gzou-bootstrap`

5. Scegli il metodo per trasferire gli archivi di aggiornamento all'istanza offline:

- Seleziona la **cartella condivisa di Windows** (condivisione Samba). In questo caso, dovrai specificare il percorso per una condivisione Windows dalla rete isolata, in cui l'istanza offline si conetterà automaticamente per recuperare gli archivi di aggiornamento. Inserisci le credenziali richieste per accedere alla posizione indicata.
- Seleziona **SCP** se trasferirai manualmente i file nella cartella `/opt/bitdefender/share/gzou/snapshots/` dell'istanza offline tramite SCP.



Istanza offline di GravityZone - Configurare la modalità di trasferimento dei file di aggiornamenti



Nota

Se vuoi cambiare il metodo di trasferimento in un secondo momento:

- L'accesso al terminale TTY dell'istanza offline nel tuo ambiente virtuale (o connessi tramite SSH).
- Accedi con l'utente `bdadmin` e la password che hai impostato.
- Esegui il comando `sudo su` per ottenere i privilegi di root.
- Esegui:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Comparirà la finestra di configurazione, in cui potrai effettuare le modifiche che desideri.

- Passa alla linea di comando della console di GravityZone offline e installa il resto dei ruoli.
- Accedi alla console offline dal tuo browser web e inserisci il tuo codice di licenza (in modalità offline).

6.5.5. Utilizzare gli aggiornamenti offline

Una volta configurate le istanze di GravityZone, segui questi passaggi per aggiornare la tua installazione offline:

1. Scarica l'ultimo archivio di aggiornamento offline dall'istanza online nella tua condivisione di rete preferita. Per maggiori dettagli, fai riferimento a «[Configurare e scaricare i file di aggiornamento iniziali](#)» (p. 199).
2. Usa una chiavetta USB per trasferire l'archivio di aggiornamento alla condivisione Samba configurata dalla rete isolata. Per maggiori dettagli, fai riferimento a «[Configurare l'istanza di GravityZone offline](#)» (p. 202).

I file saranno automaticamente inseriti nella seguente cartella dell'istanza offline:

```
/opt/bitdefender/share/gzou/snapshots/
```

6.5.6. Utilizzare la console web

Accedi alla console web inserendo l'IP/il nome host della appliance nel browser web. Puoi modificare le opzioni disponibili:

- [Control Center](#)
- [Impostazioni generali](#)

Control Center

Lo **Stato della appliance** mostra i dettagli dell'ultima attività eseguita (tipo di archivio, data e ora), e la prossima attività programmata.

Hai la possibilità di:

- **Creare un archivio del contenuto di sicurezza**
- **Creare un archivio completo**

Nella sezione **Archivi creati**, puoi scaricare archivi del contenuto di sicurezza e archivi completi.

Seleziona l'archivio o gli archivi dall'elenco disponibile e clicca sul pulsante **Download**.

Puoi anche visualizzare lo spazio disponibile nel disco della appliance.



Impostazioni generali

Puoi definire un programma di download per i kit di GravityZone.

1. Clicca sul pulsante **Modifica impostazioni**.
2. Seleziona uno o più kit dall'elenco **Kit disponibili**.
3. Nella sezione **Pianifica** puoi stabilire un intervallo di tempo per la creazione degli archivi, oltre al numero di archivi da conservare su disco.
4. Clicca sul pulsante **Applica** per salvare le tue modifiche.

7. DISINSTALLARE LA PROTEZIONE

Puoi disinstallare e reinstallare le componenti di GravityZone quando è necessario usare un codice di licenza per un'altra macchina, correggere eventuali errori o effettuare un upgrade.

Per disinstallare correttamente la protezione di Bitdefender dagli endpoint nella tua rete, segui le istruzioni descritte in questo capitolo.

- [Disinstallare la protezione per endpoint](#)
- [Disinstallare HVI](#)
- [Disinstallare la protezione di Exchange](#)
- [Disinstallare la protezione dei dispositivi mobile](#)
- [Disinstallare Sandbox Analyzer On-Premises](#)
- [Disinstallare Report Builder](#)
- [Disinstallare ruoli server di GravityZone](#)

7.1. Disinstallare la protezione per endpoint

Per rimuovere in modo sicuro la protezione di Bitdefender, devi prima disinstallare gli agenti di sicurezza e poi Security Server, se necessario. Se vuoi disinstallare solo il Security Server, assicurati prima di connettere i suoi agenti a un altro Security Server.

- [Disinstallare gli agenti di sicurezza](#)
- [Disinstallare Security Server](#)

7.1.1. Disinstallare gli agenti di sicurezza

Hai due opzioni per disinstallare gli agenti di sicurezza:

- [In remoto](#) nella Control Center
- [Manualmente](#) nella macchina bersaglio



Avvertimento

Gli agenti di sicurezza e i server di sicurezza sono essenziali per mantenere sicuri gli endpoint da qualsiasi tipo di minaccia, perciò disinstallarli potrebbe mettere in pericolo l'intera rete.

Disinstallazione remota

Per disinstallare la protezione di Bitdefender da un endpoint gestito in remoto:

1. Vai alla pagina **Rete**.
2. Seleziona **Computer e Macchine Virtuali** dal selettore di visualizzazione.
3. Seleziona il contenitore desiderato dal pannello sulla sinistra. Tutti i computer del contenitore selezionato sono mostrati nella tabella a destra.
4. Seleziona gli endpoint da cui vuoi disinstallare l'agente di sicurezza di Bitdefender.
5. Clicca su **Attività** nel lato superiore della tabella e seleziona **Disinstalla client**. Apparirà una finestra di configurazione.
6. Nella finestra dell'attività **Disinstalla agente**, puoi selezionare se mantenere i file in quarantena nell'endpoint o eliminarli.

Per gli ambienti integrati VMware vShield, devi selezionare le credenziali richieste per ciascuna macchina, altrimenti la disinstallazione non avverrà correttamente. Seleziona **Usa credenziali per integrazione vShield** e aggiungi i dati richiesti nella tabella Credentials Manager mostrata in basso.

7. Clicca su **Salva** per creare l'attività. Apparirà un messaggio di conferma.

Puoi visualizzare e gestire l'attività in **Rete e attività**.

Se vuoi reinstallare gli agenti di sicurezza, fai riferimento a [«Installare la protezione per endpoint»](#) (p. 122).

Disinstallazione locale

Per disinstallare manualmente l'agente di sicurezza di Bitdefender da una macchina Windows:

1. In base al tuo sistema operativo:
 - In Windows 7, vai in **Start - Pannello di Controllo - Disinstalla un programma** nella categoria **Programmi e funzionalità**.
 - In Windows 8, vai in **Impostazioni - Pannello di Controllo - Disinstalla un programma** nella categoria **Programmi e funzionalità**.
 - In Windows 8.1, fai clic con il pulsante destro del mouse sul pulsante **Start**, poi seleziona **Pannello di Controllo - Programmi e funzionalità**.

- In Windows 10, vai in **Start - Impostazioni - App - App e funzionalità**.
2. Seleziona l'agente di Bitdefender dall'elenco dei programmi.
 3. Clicca su **Disinstalla**.
 4. Inserisci la password di Bitdefender, se attivata nella policy di sicurezza. Durante la disinstallazione, puoi visualizzare i progressi dell'attività.

Per disinstallare manualmente l'agente di sicurezza di Bitdefender da una macchina Linux:

1. Apri il terminale.
2. Ottieni l'accesso root usando i comandi `su` o `sudo su`.
3. Usa il comando `cd` per esplorare il seguente percorso: `/opt/BitDefender/bin`
4. Esegui lo script:

```
# ./remove-sve-client
```

5. Inserisci la password di Bitdefender per continuare, se attivata nella policy di sicurezza.

Per disinstallare manualmente l'agente di Bitdefender da un Mac:

1. Vai in **Finder - Applicazioni**.
2. Apri la cartella Bitdefender.
3. Fai doppio click su **Disinstalla Mac Uninstall**.
4. Nella finestra della configurazione, clicca sia sua **Controlla** e **Disinstalla** per continuare.

Se vuoi reinstallare gli agenti di sicurezza, fai riferimento a [«Installare la protezione per endpoint»](#) (p. 122).

7.1.2. Disinstallare Security Server

Puoi disinstallare il Security Server nello stesso modo in cui è stato installato, o dalla Control Center o dall'interfaccia organizzata su menu della appliance virtuale di GravityZone.

Per disinstallare il Security Server nella Control Center:

1. Vai alla pagina **Rete**.
2. Seleziona **Macchine virtuali** dal selettore del servizio.
3. Seleziona il data center o la cartella contenente l'host su cui è stato installato il Security Server. Gli endpoint vengono visualizzati nel pannello a destra.
4. Seleziona la casella corrispondente all'host su cui è stato installato il Security Server.
5. Nel menu **Attività**, seleziona **Disinstalla Security Server**.
6. Inserisci le credenziali di vShield (se disponibili) e clicca su **Sì** per creare l'attività.

Puoi visualizzare e gestire l'attività in **Rete e attività**.

Quando il Security Server viene installato sulla stessa virtual appliance come gli altri ruoli di GravityZone, puoi rimuoverlo utilizzando l'interfaccia a riga di comando della appliance. Segui questi passaggi:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client).
Usa i tasti freccia e il tasto **Tab** per spostarti nei menu e nelle opzioni. Premi **Invio** per selezionare un'opzione specifica.
2. Nel menu **Opzioni appliance**, vai in **Impostazioni avanzate**.
3. Seleziona **Disinstalla Server di sicurezza**. Apparirà una finestra di conferma.
4. Premi il tasto **Y** o premi **Invio** con l'opzione **Sì** selezionata, per continuare. Attendi il completamento della disinstallazione.

7.2. Disinstallare HVI

Per rimuovere HVI da un host, è sufficiente disinstallare il Pacchetto supplementare di HVI. Puoi comunque utilizzare il Security Server come server di scansione, a patto di avere un codice di licenza valido per Security for Virtualized Environments.

Se vuoi rimuovere completamente Bitdefender, devi disinstallare sia il Pacchetto supplementare di HVI sia il Security Server.

Disinstallare il Pacchetto supplementare di HVI

Hai due opzioni per rimuovere il Pacchetto Supplementare:

- In remoto dalla Control Center, eseguendo un'attività di disinstallazione.

- In remoto da XenCenter, eseguendo un paio di comandi sull'host bersaglio.

Per rimuovere il pacchetto HVI usando la Control Center:

1. Accedi al tuo account Control Center.
2. Vai alla pagina **Rete** e seleziona **Virtual Machine** dal selettore di visualizzazioni.
3. Seleziona **Server** dal menu **Visualizzazioni** nel pannello a sinistra.
4. Seleziona uno o più host Xen dall'inventario della rete. Puoi facilmente visualizzare gli host disponibili selezionando l'opzione **Tipo > Host** nel menu **Filtri**.
5. Clicca sul pulsante **Attività** nel pannello a destra e seleziona **Disinstalla il Pacchetto supplementare di HVI**. Si aprirà la finestra di configurazione.
6. Programma quando rimuovere il pacchetto. Puoi scegliere di eseguire l'attività immediatamente dopo aver salvato l'attività o in un determinato momento. Nel caso non fosse possibile completare la rimozione nel momento indicato, l'attività sarà ripetuta automaticamente in base alle impostazioni di ripetizione. Per esempio, se selezioni più host e un host non è disponibile quando si è programmato di rimuovere il pacchetto, l'attività sarà eseguita nuovamente nel momento indicato.
7. L'host deve essere riavviato per completare la rimozione. Se desideri che l'host venga riavviato in modo automatico, seleziona **Riavvia automaticamente (se necessario)**.
8. Clicca su **Salva**. Apparirà un messaggio di conferma.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.


Per rimuovere il pacchetto HVI usando XenCenter:

1. Accedi a XenCenter.
2. Apri la console dell'host Xen.
3. Inserisci la password per l'host XenServer.
4. Esegui i seguenti comandi:

```
# rpm -e bitdefender-xen-dom0 # rm -rf /etc//xensource/installed-rpms/bitdefender\;bitdefender-hvi/ # rm -rf/opt/bitdef* # servizio
```

Disinstallare Security Server

Per disinstallare il Security Server da uno o più host:

1. Accedi al tuo account Control Center.
2. Vai alla pagina **Rete**.
3. Seleziona **Macchine virtuali** dal selettore del servizio.
4. Esplora l'inventario Citrix e seleziona le caselle corrispondenti agli host desiderati. Per una selezione rapida, puoi filtrare l'inventario della rete per visualizzare solo i Security Server.
5. Clicca sul pulsante  **Attività** nel lato superiore della tabella e seleziona **Disinstalla Security Server** dal menu. Apparirà un messaggio di conferma. Clicca su **Sì** per continuare.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.

7.3. Disinstallare la protezione di Exchange

Puoi rimuovere la Protezione Exchange da qualsiasi Microsoft Exchange Server che ha Bitdefender Endpoint Security Tools installato con questo ruolo. Puoi eseguire la disinstallazione nella Control Center.

1. Vai alla pagina **Rete**.
2. Seleziona **Computer e Macchine Virtuali** dal selettore di visualizzazione.
3. Seleziona il contenitore desiderato dal pannello sulla sinistra. Le entità saranno mostrate nel pannello a destra.
4. Seleziona l'endpoint da cui vuoi disinstallare la Protezione Exchange.
5. Clicca su **Riconfigura client** nel menu **Attività** nel pannello in alto della tabella. Apparirà una finestra di configurazione.
6. Nella sezione **Generale**, deseleziona la casella **Protezione Exchange**.



Avvertimento

Nella finestra di configurazione, assicurati di aver selezionato tutti gli altri ruoli che sono attivi sull'endpoint. Diversamente, saranno anch'essi disinstallati.

7. Clicca su **Salva** per creare l'attività.

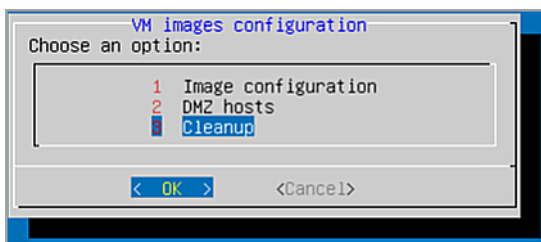
Puoi visualizzare e gestire l'attività in **Rete e attività**.

Se vuoi reinstallare la Protezione Exchange, fai riferimento a «[Installare la protezione di Exchange](#)» (p. 166).

7.4. Disinstallare Sandbox Analyzer On-Premises

Per disinstallare Sandbox Analyzer On-Premises:

1. Rimuovi le immagini della virtual machine (VM) dalla console della appliance di Sandbox Analyzer.
 - a. Accedi all'interfaccia della appliance di Sandbox Analyzer.
Usa i tasti freccia e il tasto `Tab` per spostarti nei menu e nelle opzioni.
Premi `Invio` per selezionare un'opzione specifica.
 - b. Nel menu **Configurazione sandbox**, vai all'opzione **Immagini VM**.
 - c. Nel menu **Configurazione immagine VM**, vai all'opzione **Pulizia**.



Console della appliance di Sandbox Analyzer - Configurazione sandbox - Pulizia

- d. Conferma di voler rimuovere le immagini della virtual machine installate.
Attendi il completamento di questa azione. Durante tale azione, anche i dati associati alle immagini della virtual machine saranno eliminati.
2. Elimina la Virtual Appliance di Sandbox Analyzer:
 - a. Disattiva la Virtual Appliance di Sandbox Analyzer.
 - b. Elimina la appliance dall'inventario di ESXi.

7.5. Disinstallare la protezione dei dispositivi mobile

Per rimuovere la protezione di Bitdefender da un dispositivo mobile, devi farlo sia nella Control Center che nel dispositivo.

Quando elimini un dispositivo dalla Control Center:

- GravityZone Mobile Client è stato scollegato ma non rimosso dal dispositivo.
- Tutti i registri relativi al dispositivo eliminato sono ancora disponibili.
- Le tue informazioni personali e le applicazioni non sono influenzate.
- Per i dispositivi iOS, viene rimosso il profilo MDM. Se il dispositivo non è connesso a Internet, il profilo MDM resta installato finché non sarà disponibile una nuova connessione.



Avvertimento

- Non puoi ripristinare i dispositivi mobile eliminati.
- Assicurati che il dispositivo bersaglio non sia bloccato prima dell'eliminazione. Se hai eliminato per sbaglio un dispositivo bloccato, devi riportare il dispositivo alle impostazioni di fabbrica per sbloccarlo.


1. Vai alla pagina **Rete**.
2. Seleziona **Dispositivi mobile** dal selettore di visualizzazioni.
3. Clicca su **Filtri** nel lato superiore del pannello della rete e seleziona **Dispositivi** nella categoria **Visualizza**. Clicca su **Salva**.
4. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti i dispositivi vengono mostrati nella tabella a destra.
5. Seleziona la casella del dispositivo da cui vuoi rimuovere la protezione.
6. Clicca su **⊖ Elimina** nel lato superiore della tabella.

Poi, dovrai disinstallare il software dal dispositivo.

Per disinstallare la protezione di Bitdefender da un dispositivo Android:

1. Vai in **Sicurezza > Amministratori dispositivo**.
2. Deseleziona la casella GravityZone. Apparirà una finestra di conferma.
3. Tocca **Disattiva**. Comparirà un messaggio di avviso che ti informerà del cessato funzionamento delle funzionalità antifurto, oltre all'impossibilità di accedere alle reti e ai dati aziendali.
4. Disinstalla GravityZone Mobile Client come qualsiasi altra applicazione.

Per disinstallare la protezione di Bitdefender da un dispositivo iOS:

1. Trova l'icona di Bitdefender GravityZone Mobile Client e tienila premuta per alcuni secondi.
2. Tocca il relativo cerchio  quando compare. L'applicazione è stata eliminata. Se vuoi reinstallare la protezione mobile, fai riferimento a [«Installare la protezione dei dispositivi mobile»](#) (p. 172)

7.6. Disinstallare Report Builder

Per rimuovere correttamente Report Builder dalla tua soluzione GravityZone, devi prima disinstallare il ruolo Report Builder Processors, poi il ruolo Report Builder Database.

Per disinstallare il ruolo Processori del Report Builder:

1. Accedi all'interfaccia della console Processori del Report Builder dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client). Usa i tasti freccia e il tasto `Tab` per spostarti nei menu e nelle opzioni. Premi `Invio` per selezionare un'opzione specifica.
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Vai a **Installa/Disinstalla ruoli e Aggiungi o rimuovi ruoli**.
4. Utilizzando la Barra spaziatrice, deseleziona il ruolo **Report Builder Processors** e premi `Invio`. Apparirà una finestra di conferma.
5. Seleziona **Sì** e premi `Invio` per continuare e attendere il completamento della disinstallazione.

Per disinstallare il ruolo Database del Report Builder:

1. Accedi all'interfaccia della console Database del Report Builder dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client). Usa i tasti freccia e il tasto `Tab` per spostarti nei menu e nelle opzioni. Premi `Invio` per selezionare un'opzione specifica.
2. Dal menu principale, seleziona **Impostazioni avanzate**.
3. Vai a **Installa/Disinstalla ruoli e Aggiungi o rimuovi ruoli**.
4. Utilizzando la Barra spaziatrice, deseleziona il ruolo **Report Builder Database** e premi `Invio`. Apparirà una finestra di conferma.

5. Seleziona **Sì** e premi **Invio** per continuare e attendere il completamento della disinstallazione.



Avvertimento

Se disattivi le tue appliance del Report Builder nell'ambiente di virtualizzazione senza disinstallare i ruoli Database e Processors, non potrai connetterti a GravityZone Control Center.

7.7. Disinstallare i ruoli della Virtual appliance di GravityZone

Puoi disinstallare i ruoli della appliance virtuale di GravityZone tramite l'interfaccia organizzata su menu. Anche rimuovendone uno, la tua rete è comunque protetta. Tuttavia, ti serve almeno un'istanza di ciascun ruolo affinché GravityZone funzioni correttamente.

In uno scenario con una sola appliance con tutti i ruoli di GravityZone, rimuovendo un solo ruolo, gli endpoint continueranno a essere protetti, sebbene alcune delle funzionalità della appliance non saranno disponibili, in base a ciascun ruolo.

In uno scenario con più appliance di GravityZone, puoi disinstallare in sicurezza un ruolo finché è disponibile un'altra istanza con lo stesso ruolo. Di proposito, più istanze dei ruoli Server di comunicazione e Console web possono essere installate su diverse appliance e connesse ad altri ruoli, tramite un bilanciatore di ruoli. Quindi, se disinstalli una istanza di un determinato ruolo, la sua funzione viene presa da un altro.

Se necessario, puoi disinstallare il Server di comunicazione da una appliance, assegnando la sua funzione a un'altra istanza di questo ruolo. Per una migrazione agevole, segui questi passaggi:

1. Nella Control Center, vai alla pagina **Policy**.
2. Seleziona una policy esistente o clicca su **+Aggiungi** per crearne una nuova.
3. Nella sezione **Generale**, vai in **Comunicazione**.
4. Nella tabella **Assegnazione comunicazione endpoint**, clicca sul campo **Nome**. Viene mostrato l'elenco dei server di comunicazione rilevati.
5. Seleziona il server di comunicazione che vuoi come riferimento per gli endpoint.

6. Clicca sul pulsante **+** **Aggiungi** nel lato destro della tabella. Se nell'elenco hai più di un server di comunicazione, puoi configurare la loro priorità utilizzando le frecce su e giù alla destra di ciascuna entità.
7. Clicca su **Salva** per creare la policy. Gli endpoint comunicheranno con la Control Center tramite il server di comunicazione indicato.
8. Nell'interfaccia a riga di comando di GravityZone, disinstalla il vecchio ruolo di Server di comunicazione.



Avvertimento

Disinstallando il vecchio Server di comunicazione senza prima impostarne la policy, la comunicazione sarà persa in modo permanente e sarà necessario reinstallare gli agenti di sicurezza.

Per disinstallare i ruoli della virtual appliance di GravityZone:

1. Accedi all'interfaccia della console dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client). Usa i tasti freccia e il tasto **Tab** per spostarti nei menu e nelle opzioni. Premi **Invio** per selezionare un'opzione specifica.
2. Seleziona **Impostazioni avanzate**.
3. Seleziona **Installa/Disinstalla ruoli**.
4. Vai in **Aggiungi o rimuovi i ruoli**.
5. Usando la **Barra spaziatrice**, deseleziona ogni ruolo che desideri disinstallare e premi **Invio**. Comparirà una finestra di conferma, informandoti sul ruolo che sarà rimosso.
6. Premi **Invio** per continuare e attendi il completamento della disinstallazione.

Se vuoi disinstallare un ruolo, fai riferimento a [«Installa/Disinstalla ruoli»](#) (p. 109).

8. OTTENERE AIUTO

Bitdefender si sforza di fornire ai suoi clienti un supporto veloce e preciso assolutamente senza pari. Se riscontri un problema o in caso di domande sul tuo prodotto di Bitdefender, visita il nostro [Centro di supporto online](#). Fornisce diverse risorse che puoi utilizzare per trovare rapidamente una soluzione o una risposta. O, se preferisci, puoi contattare il Servizio clienti di Bitdefender. Gli operatori del nostro supporto risponderanno alle tue domande in modo tempestivo e ti forniranno l'assistenza necessaria.



Nota

Puoi trovare informazioni sui nostri servizi e la politica di supporto nel Centro di supporto.

8.1. Centro di supporto di Bitdefender

[Centro di supporto di Bitdefender](#) è il luogo in cui troverai tutta l'assistenza necessaria con il tuo prodotto di Bitdefender.

Puoi usare varie risorse per trovare rapidamente una soluzione o una risposta:

- Articoli della Knowledge Base
- Forum supporto di Bitdefender
- Documentazione del prodotto

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

Articoli della Knowledge Base

La Knowledge Base di Bitdefender è un archivio online di informazioni sui prodotti di Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione antivirus, la gestione delle soluzioni di Bitdefender, con spiegazioni dettagliate, e molti altri articoli.

La Knowledge Base di Bitdefender è aperta al pubblico e liberamente esplorabile. Le molte informazioni contenute sono un altro mezzo per fornire ai clienti di Bitdefender le conoscenze tecniche che gli servono. Tutte le richieste di informazioni o segnalazioni di bug dai clienti di Bitdefender arrivano alla Knowledge Base di

Bitdefender, così come segnalazioni e informazioni su bug risolti o articoli tecnici per integrare i file di supporto del prodotto.

La Knowledge Base di Bitdefender per i prodotti aziendali è disponibile in qualsiasi momento presso <http://www.bitdefender.com/support/business.html>.

Forum supporto di Bitdefender

Il forum del supporto di Bitdefender fornisce agli utenti di Bitdefender un modo semplice per ottenere aiuto e aiutare gli altri. Puoi pubblicare ogni problema o domanda relativa al tuo prodotto Bitdefender.

I tecnici del supporto di Bitdefender controllano le nuove discussioni sul forum per poterti assistere. Potresti ricevere una risposta o una soluzione anche da un utente di Bitdefender più esperto.

Prima di postare il tuo problema o la tua domanda, cerca nel forum un'eventuale discussione simile o collegata.

Il forum del supporto di Bitdefender è disponibile all'indirizzo <http://forum.bitdefender.com> in 5 lingue diverse: inglese, tedesco, francese, spagnolo e rumeno. Clicca sul link **Protezione Business** per accedere alla sezione dedicata ai prodotti per utenti aziendali.

Documentazione del prodotto

La documentazione del prodotto è la fonte di informazioni più completa sul tuo prodotto.

Il modo più semplice per raggiungere la documentazione è dalla pagina **Aiuto e supporto** di Control Center. Clicca sul tuo nome utente nell'angolo in alto a destra della console, seleziona **Aiuto e Supporto** e poi il link della guida a cui sei interessato. La guida si aprirà in una nuova scheda del tuo browser.

Puoi anche consultare e scaricare la documentazione nel **Centro di supporto**, nella sezione **Documentazione** disponibile in ciascuna pagina di supporto del prodotto.

8.2. Necessiti di assistenza

Puoi chiederci assistenza attraverso il nostro Centro di supporto online. Compila il **modulo di contatto** e invialo.

8.3. Usare lo strumento di supporto

Lo Strumento di supporto di GravityZone è stato progettato per aiutare gli utenti e supportare i tecnici a ottenere facilmente le informazioni necessarie per risolvere eventuali problemi. Esegui lo Strumento di supporto nei computer interessati e invia l'archivio risultante con le informazioni sulla risoluzione dei problemi al rappresentante del supporto di Bitdefender.

8.3.1. Utilizzare lo Strumento di supporto sui sistemi operativi Windows

Eseguire l'applicazione dello strumento di supporto

Per generare il rapporto sul computer interessato, utilizza uno dei seguenti metodi:

- **Linea di comando**

Per qualsiasi altro problema con BEST, installato sul computer.

- **Problema di installazione**

Per situazioni in cui BEST non è stato installato sul computer e l'installazione non è avvenuta.

Metodo a linea di comando

Usando una linea di comando puoi ottenere i rapporti direttamente dal computer interessato. Questo metodo è utile in situazioni in cui non hai accesso a GravityZone Control Center o se il computer non comunica con la console.

1. Apri il prompt dei comandi con privilegi di amministratore.
2. Vai alla cartella di installazione del prodotto. Il percorso predefinito è:

```
C:\Programmi\Bitdefender\Endpoint Security
```

3. Raccogli e salva i registri eseguendo il seguente comando:

```
Product.Support.Tool.exe collect
```

Per impostazione predefinita, i registri vengono salvati in C:\Windows\Temp.

Facoltativamente, se desideri salvare il rapporto dello strumento di supporto in una posizione personalizzata, utilizza il percorso opzionale:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Esempio:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Mentre il comando è in esecuzione, sullo schermo apparirà una barra di avanzamento. Una volta completato il processo, vengono mostrati il nome e la posizione dell'archivio che contiene i registri.

Per inviare i rapporti al supporto aziendale di Bitdefender, accedi a `C:\Windows\Temp` o al percorso personalizzato e trova il file di archivio chiamato `ST_[computername]_[currentdate]`. Allega l'archivio al tuo ticket di supporto per ricevere ulteriore assistenza.

Problema di installazione

1. Per scaricare lo Strumento di supporto di BEST, clicca [qui](#).
2. Esegui il file eseguibile come amministratore. Comparirà una finestra.
3. Scegli una posizione per salvare l'archivio dei rapporti.

Mentre i rapporti vengono ottenuti, sullo schermo potrai visualizzare una barra indicante i progressi. Una volta completato il processo, vengono mostrati il nome e la posizione dell'archivio.

Per inviare i rapporti al Supporto aziendale di Bitdefender, accedi alla posizione selezionata e trova il file di archivio chiamato `ST_[computername]_[currentdate]`. Allega l'archivio al tuo ticket di supporto per ricevere ulteriore assistenza.

8.3.2. Utilizzare lo Strumento di supporto su sistemi operativi Linux

Per i sistemi operativi Linux, lo Strumento di supporto è integrato nell'agente di sicurezza di Bitdefender.

Per raccogliere informazioni sul sistema Linux utilizzando lo Strumento di supporto, esegui il seguente comando:

```
# /opt/BitDefender/bin/bdconfigure
```

usando le seguenti opzioni disponibili:

- `--help` per elencare tutti i comandi dello Strumento di supporto
- `enablelogs` per attivare i registri dei moduli prodotto e comunicazione (tutti i servizi saranno riavviati automaticamente)
- `disablelogs` per disattivare i registri dei moduli prodotto e comunicazione (tutti i servizi saranno riavviati automaticamente)
- `deliverall` per creare:
 - Un archivio contenente i registri dei moduli prodotto e comunicazioni, forniti alla cartella `/tmp` nel seguente formato:
`bitdefender_machineName_timeStamp.tar.gz`.

Una volta creato l'archivio:

1. Ti sarà chiesto se desideri disattivare i registri. Se necessario, i servizi vengono riavviati automaticamente.
 2. Ti sarà chiesto se desideri eliminare i registri.
- `deliverall -default` fornisce le stesse informazioni dell'opzione precedente, ma le azioni predefinite saranno prese nei registri, senza che venga chiesto nulla all'utente (i registri vengono disattivati ed eliminati).

Puoi anche eseguire il comando `/bdconfigure` direttamente dal pacchetto BEST (completo o downloader) senza aver installato il prodotto.

Per segnalare un problema di GravityZone che riguarda i tuoi sistemi Linux, segui questi passaggi, usando le opzioni descritte in precedenza:

1. Attiva i registri dei moduli prodotto e comunicazione.
2. Prova a riprodurre il problema.
3. Disattiva i registri.
4. Crea l'archivio dei registri.
5. Apri un ticket di supporto via e-mail utilizzando il modulo disponibile nella pagina **Aiuto e supporto** della Control Center, con una descrizione del problema e allegando l'archivio dei registri.

Lo Strumento di supporto per Linux fornisce le seguenti informazioni:

- Le cartelle `etc`, `var/log`, `/var/crash` (se disponibili) e `var/epag` da `/opt/BitDefender`, contenenti i registri e le impostazioni di Bitdefender.
- Il file `/var/log/BitDefender/bdinstall.log`, contenente le informazioni di installazione
- Il file `network.txt`, contenente informazioni su impostazioni di rete / connettività della macchina
- Il file `product.txt`, incluso i contenuti di tutti i file `update.txt` da `/opt/BitDefender/var/lib/scan` e un elenco completo ricorrente di tutti i file da `/opt/BitDefender`
- Il file `system.txt`, contenente informazioni generali sul sistema (distribuzione e versione del kernel, RAM disponibile e spazio libero su disco rigido)
- Il file `users.txt`, contenente le informazioni dell'utente
- Altre informazioni sul prodotto e relative al sistema, come connessioni esterne di processi e utilizzo della CPU.
- Registri di sistema

8.3.3. Utilizzare lo Strumento di supporto sui sistemi operativi Mac

Inviando una richiesta al supporto tecnico di Bitdefender, devi fornire le seguenti informazioni:

- Una descrizione dettagliata del problema che stai riscontrando.
- Un'immagine (se possibile) dell'esatto messaggio di errore che compare.
- Il registro dello Strumento di supporto.

Per raccogliere informazioni sul sistema Mac con lo Strumento di supporto:

1. Scarica [l'archivio ZIP](#) contenente lo Strumento di supporto.
2. Estrai il file **BDProfiler.tool** dall'archivio.
3. Apri una finestra del Terminale.
4. Raggiungi la posizione del file **BDProfiler.tool**.

Per esempio:

```
cd /Users/Bitdefender/Desktop;
```

5. Aggiungi i permessi di esecuzione al file:

```
chmod +x BDProfiler.tool;
```

6. Esegui lo strumento.

Per esempio:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Premi **Y** e inserisci la password quando ti verrà chiesto di indicare la password dell'amministratore.

Attendi un paio di minuti finché lo strumento non finisce di generare il registro. Troverai il file di archivio risultante (**Bitdefenderprofile_output.zip**) sul desktop.

8.4. Informazioni di contatto

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 18 anni Bitdefender ha acquisito una reputazione inestimabile superando le aspettative di clienti e partner, e sforzandosi costantemente per una comunicazione sempre più efficiente. Se hai delle domande o richieste, non esitare a contattarci.

8.4.1. Indirizzi Web

Dipartimento vendite: enterprisesales@bitdefender.com

Centro di supporto: <http://www.bitdefender.com/support/business.html>

Documentazione: gravityzone-docs@bitdefender.com

Distributori locali: <http://www.bitdefender.it/partners>

Programma partner: partners@bitdefender.com

Rapporti con i Media: pr@bitdefender.com

Invio virus: virus_submission@bitdefender.com

Invio spam: spam_submission@bitdefender.com

Segnala abuso: abuse@bitdefender.com

Sito web: <http://www.bitdefender.com>

8.4.2. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Visitare <http://www.bitdefender.it/partners>.
2. Vai a **Trova partner**.
3. Le informazioni di contatto dei distributori locali di Bitdefender dovrebbero essere visualizzate automaticamente. Se non fosse così, seleziona il paese in cui risiedi per visualizzare le informazioni.
4. Se non dovessi trovare un distributore di Bitdefender nel tuo paese, contattaci via e-mail all'indirizzo enterprisesales@bitdefender.com.

8.4.3. Uffici di Bitdefender

Gli uffici di Bitdefender sono sempre pronti a rispondere a ogni richiesta inerente le loro competenze, sia in ambito commerciale sia generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

Stati Uniti

Bitdefender, LLC

PO Box 667588

Pompano Beach, FL 33066

United States

Telefono (supporto tecnico e vendite): 1-954-776-6262

Vendite: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Centro di supporto: <http://www.bitdefender.com/support/business.html>

Francia

Bitdefender

49, Rue de la Vanne

92120 Montrouge

Fax: +33 (0)1 47 35 07 09

Telefono: +33 (0)1 47 35 72 73

E-mail: b2b@bitdefender.fr

Sito web: <http://www.bitdefender.fr>

Centro di supporto: <http://www.bitdefender.fr/support/business.html>

Spagna

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax: (+34) 93 217 91 28

Telefono (ufficio e vendite): (+34) 93 218 96 15

Telefono (supporto tecnico): (+34) 93 502 69 10

Vendite: comercial@bitdefender.es

Sito web: <http://www.bitdefender.es>

Centro di supporto: <http://www.bitdefender.es/support/business.html>

Germania

Bitdefender GmbH

Technologiezentrum Schwerte

Lohbachstrasse 12

D-58239 Schwerte

Deutschland

Telefono (ufficio e vendite): +49 (0) 2304 94 51 60

Telefono (supporto tecnico): +49 (0) 2304 99 93 004

Vendite: firmenkunden@bitdefender.de

Sito web: <http://www.bitdefender.de>

Centro di supporto: <http://www.bitdefender.de/support/business.html>

Regno Unito e Irlanda

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

UK

Telefono (supporto tecnico e vendite): (+44) 203 695 3415

E-mail: info@bitdefender.co.uk

Vendite: sales@bitdefender.co.uk

Sito web: <http://www.bitdefender.co.uk>

Centro di supporto: <http://www.bitdefender.co.uk/support/business.html>

Romania

BITDEFENDER SRL

Orhideea Towers

15A Orhideelor Street

060071 Bucharest, Sector 6

Fax: +40 21 2641799

Telefono (supporto tecnico e vendite): +40 21 2063470

Vendite: sales@bitdefender.ro

Sito web: <http://www.bitdefender.ro>

Centro di supporto: <http://www.bitdefender.ro/support/business.html>

Emirati Arabi Uniti

Bitdefender FZ-LLC

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Telefono (supporto tecnico e vendite): 00971-4-4588935 / 00971-4-4589186

Fax: 00971-4-44565047

Vendite: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Centro di supporto: <http://www.bitdefender.com/support/business.html>

A. Appendici

A.1. Tipi di file supportati

I motori di scansione antimalware inclusi nelle soluzioni di sicurezza di Bitdefender possono esaminare tutti i tipi di file che potrebbero contenere minacce. L'elenco sottostante include i tipi di file più comuni che vengono analizzati.

```
{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;
```

xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; z1?; zoo

A.2. Oggetti Sandbox Analyzer

A.2.1. Estensioni e tipi di file supportati per l'invio manuale

Le seguenti estensioni di file sono supportate e possono essere detonate manualmente in Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archivio), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, file MZ/PE (eseguibile), PDF, PEF (eseguibile), PIF (eseguibile), RTF, SCR, URL (binario), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer è in grado di rilevare i suddetti tipi di file anche se sono inclusi nei seguenti tipi di archivio: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

A.2.2. Tipi di file supportati da Pre-filtro contenuti per l'invio automatico

Pre-filtro contenuti determinerà un particolare tipo di file, attraverso una combinazione che include il contenuto e l'estensione dell'oggetto. Ciò significa che un eseguibile con estensione .tmp verrà riconosciuto come un'applicazione e, se ritenuto sospetto, verrà inviato a Sandbox Analyzer.

- Applicazioni - file in formato PE32, incluse, a titolo esemplificativo, le seguenti estensioni: exe, dll, com.
- Documenti - file in formato documento, incluse, a titolo esemplificativo, le seguenti estensioni: xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf.

- **Script:** ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- **Archivi:** zip, jar, 7z, bz, bz2, tgz, msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- **E-mail (salvate nel file system):** eml, tnef.

A.2.3. Eccezioni predefinite all'invio automatico

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, ppg, png, txt.

A.2.4. Applicazioni consigliate per le VM di detonazione

Sandbox Analyzer On-Premises richiede l'installazione di determinate applicazioni sulle virtual machine di detonazione, così da poter aprire i campioni inviati.

Applicazioni	Tipi di file
Suite di Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Predefinito di Windows	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml