Cyber Protect Cloud

23.02

Manuale dell'amministratore di partner

REVISIONE: 28/02/2023

Sommario

Informazioni sul documento **5**
Informazioni su Cyber Protect **6**
Servizi Cyber Protect 6
Modalità di fatturazione per Cyber Protect 7
Passaggio tra edizioni e modalità di fatturazione 9
Offerta di elementi e gestione delle quote 12
Servizi ed elementi dell'offerta 12
Utilizzo del portale di gestione **25**
Browser Web supportati 25
Attivare l'account di amministrazione 25
Requisiti per la password 25
Accesso al portale di gestione 26
Configurazione dei contatti nella procedura guidata Profilo azienda 26
Accesso alla console di Cyber Protection dal portale di gestione 27
Navigazione nel portale di gestione 27
Limitazione dell'accesso all'interfaccia Web 28
Accesso ai servizi 29
Scheda Panoramica 29
Scheda Clienti 30
Barra Cronologia a 7 giorni 31
Account utente e tenant 31
Gestione dei tenant 34
Creazione di un tenant 34
Modalità Sicurezza avanzata 37
Selezione dei servizi per un tenant 38
Configurazione degli elementi dell'offerta per un tenant 38
Abilitazione dei servizi per più tenant esistenti 39
Abilitazione delle Notifiche sulla manutenzione 41
Configurazione del profilo cliente autogestito 42
Configurazione dei contatti aziendali 42
Aggiornamento dei dati di utilizzo per un tenant 44
Disabilitazione e abilitazione di un tenant 45
Spostamento di un tenant in un altro tenant 45
Conversione di un tenant partner in un tenant cartella e viceversa 47
Limitazione dell'accesso al tenant 47

Eliminazione di un tenant 48
Gestione degli utenti 48
Creazione di un account utente 48
Ruoli utente disponibili per ogni servizio 51
Modifica delle impostazioni di notifica per un utente 56
Disabilitazione e abilitazione di un account utente 58
Eliminazione di un account utente 58
Trasferimento della titolarità di un account utente 59
Configurazione dell'autenticazione a due fattori 59
Come funziona 60
Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant 61
Configurazione dell'autenticazione a due fattori per il tenant 62
Gestione dell'autenticazione a due fattori per gli utenti 63
Ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore 65
Protezione da attacchi di forza bruta 65
Configurazione di scenari di upselling per i clienti 66
Elementi di upselling mostrati al cliente 67
Gestione di posizioni e archivi 67
Posizioni 68
Gestione dell'archiviazione 69
Configurazione dell'archivio immutabile 70
Configurazione del branding e del marchio personalizzabile 72
Applicazione del branding 73
Configurazione del branding 76
Ripristino delle impostazioni predefinite di branding 76
Disabilitare il branding 76
Personalizzazione 77
Configurazione degli URL delle interfacce web personalizzate 77
Aggiornamento automatico degli agenti 78
Per aggiornare gli agenti automaticamente 79
Per monitorare gli aggiornamenti degli agenti 80
Monitoraggio 80
Utilizzo 80
Operazioni 81
Elaborazione di rapporti 100
Utilizzo 100
Report Operazioni 102

Riepilogo esecutivo ... 107
Fusi orari nei report ... 119
Dati inseriti nel report in base al tipo di widget ... 120
Registro controllo ... 122
Campi del registro controllo ... 123
Filtri e ricerca ... 124
Pacchetti Advanced Protection ... 125
Funzionalità e pacchetti Advanced inclusi nei servizi Cyber Protect ... 126
Funzionalità incluse e avanzate nel servizio Protection ... 126
Funzionalità a consumo e avanzate del servizio Cyber Protection ... 129
Advanced Data Loss Prevention ... 130
Abilitazione di Advanced Data Loss Prevention ... 130
Advanced Security + EDR ... 131
Abilitazione di Advanced Security + EDR ... 131
Advanced Disaster Recovery ... 132
Advanced Email Security ... 133
Integrazioni ... 134
Integrazione con sistemi di terze parti ... 134
Configurazione di un'integrazione per Cyber Protect Cloud ... 134
Gestione dei clienti API ... 134
Riferimenti per l'integrazione ... 137
Integrazione con VMware Cloud Director ... 139
Limitazioni ... 140
Requisiti software ... 140
Configurazione del broker dei messaggi di RabbitMQ ... 141
Installazione del plug-in per VMware Cloud Director ... 141
Installazione di un agente di gestione ... 142
Installazione degli agenti di backup ... 144
Aggiornamento degli agenti ... 146
Accesso alla console web di Cyber Protection ... 146
Creazione di un amministratore di backup ... 147
Report di sistema, file di registro e file di configurazione ... 148
Rimozione dell'integrazione con VMware Cloud Director ... 149
Impostazioni di privacy ... 150
Indice ... 151

Informazioni sul documento

Questo documento è rivolto agli amministratori di partner che desiderano utilizzare Cyber Protect Cloud per offrire servizi ai propri clienti.

Il documento descrive come configurare e gestire i servizi disponibili in Cyber Protect Cloud utilizzando il portale di gestione.

Informazioni su Cyber Protect

Cyber Protect è una piattaforma cloud che consente a service provider, rivenditori e distributori di offrire servizi di protezione dati ai propri partner e clienti.

I servizi vengono forniti a livello di partner, fino al livello di azienda cliente e di utente finale.

I servizi offerti possono essere gestiti mediante applicazioni web, denominate **console del servizio**. La gestione del tenant e degli account utente avviene tramite un'applicazione web denominata **portale di gestione**.

Il portale di gestione consente agli amministratori di:

- Monitorare l'utilizzo dei servizi e l'accesso alle console dei servizi
- Gestire i tenant
- Gestire gli account utente
- Configurare i servizi e le quote dei tenant
- Gestire gli archivi
- Gestire il branding
- Generare report relativi all'utilizzo del servizio

Servizi Cyber Protect

Questa sezione descrive gli insiemi di funzionalità introdotti nel marzo 2021 con il nuovo modello di fatturazione. Scopri di più sui vantaggi del nuovo modello di fatturazione nella scheda informativa di Cyber Protect.

In Cyber Protect Cloud sono disponibili i seguenti servizi e insiemi di funzionalità:

- **Cyber Protect**
  - **Protezione** - Il prodotto base include Cyber Protection completa con funzionalità di sicurezza e gestione; disaster recovery, backup e ripristino, automazione e sicurezza e-mail sono disponibili come funzionalità a consumo. Questa funzionalità può essere estesa con pacchetti di protezione Advanced soggetti a costi aggiuntivi.
    I pacchetti di protezione Advanced sono insiemi di funzionalità uniche che soddisfano esigenze di utilizzo più complesse in aree funzionali specifiche, ad esempio Advanced Backup, Advanced Security e altri. Questi pacchetti estendono le funzionalità disponibili nel servizio Cyber Protect standard.
    Per ulteriori informazioni sui pacchetti Advanced Protection, vedere "Pacchetti Advanced Protection" (pag. 125).
  - **File Sync & Share** - una soluzione per la condivisione sicura dei contenuti aziendali da qualsiasi luogo, in qualsiasi momento il su qualsiasi dispositivo.
  - **Physical Data Shipping** - una soluzione che aiuta a risparmiare tempo e traffico di rete inviando i dati al data center nel cloud su un'unità disco rigido.

- **Notary** - una soluzione basata su blockchain che garantisce l'autenticità dei contenuti condivisi.

- **SPLA di Acronis Cyber Infrastructure**

Nel portale di gestione è possibile selezionare i servizi e gli insiemi di funzionalità che saranno disponibili ai tenant. La configurazione viene eseguita per tenant, al momento del provisioning o della modifica di un tenant, come descritto in Creazione di un tenant.

Modalità di fatturazione per Cyber Protect

Una modalità di fatturazione è lo schema per la registrazione e la fatturazione dell'uso dei servizi e delle loro funzionalità. La modalità di fatturazione scelta determina quali unità verranno utilizzate come base per calcolare i prezzi. Le modalità di fatturazione possono essere impostate dai partner a livello di cliente.

Il motore di licensing acquisisce automaticamente gli elementi dell'offerta in base alle funzionalità richieste nei piani di protezione. Gli utenti possono ottimizzare il livello di protezione e costo personalizzando i propri piani di protezione.

Nota
È possibile utilizzare solo un modello di fatturazione per ogni tenant cliente.

Modalità di fatturazione del componente Protezione

In Protezione sono disponibili due modalità di fatturazione:

- Per carico di lavoro
- Per gigabyte

Le funzionalità di entrambe le modalità di fatturazione sono identiche.

In entrambe le modalità di fatturazione, il servizio Protection include funzionalità di protezione standard che coprono la maggior parte dei rischi di Cyber Security. Gli utenti possono avvalersene senza costi aggiuntivi. L'utilizzo delle funzionalità incluse verrà registrato, ma non fatturato. Per un elenco completo degli elementi inclusi nell'offerta e fatturabili, vedere "Servizi Cyber Protect" (pag. 6).

Anche se un Advanced Pack è abilitato per un cliente, la fatturazione inizia solo quando il cliente utilizza le funzionalità di quel pacchetto contenute in un piano di protezione. Quando una funzionalità avanzata viene applicata a un piano di protezione, il motore di licensing assegna automaticamente la licenza necessaria al workload protetto.

Quando la funzionalità avanzata non è più in uso, la licenza viene revocata e la fatturazione si interrompe. Il motore di licensing assegna automaticamente la licenza che riflette l'utilizzo effettivo delle funzionalità.

È possibile assegnare licenze solo per le funzionalità del servizio Cyber Protect standard. Le funzionalità avanzate vengono fatturate in base al loro utilizzo e non è possibile modificare

manualmente le licenze. È infatti il motore di licensing che automaticamente assegna o annulla l'assegnazione delle licenze. È possibile modificare manualmente il tipo di licenza di un workload, ma questa verrà riassegnata quando il piano di protezione per quel workload viene modificato da un utente.

Nota
La fatturazione delle funzionalità di protezione avanzata non ha inizio quando le funzionalità vengono abilitate. La fatturazione inizia solo dopo che un cliente inizia a utilizzare le funzionalità avanzate contenute in un piano di protezione. L'insieme di funzionalità abilitate verrà registrato e incluso nei report di utilizzo, ma non verrà fatturato a meno che tali funzionalità non siano utilizzate.

Modalità di fatturazione della funzionalità File Sync & Share

Per la funzionalità File Sync & Share sono disponibili due modalità di fatturazione:

- Per utente
- Per gigabyte

È inoltre possibile applicare le regole di fatturazione dell'edizione File Sync & Share Legacy.

Nota
La fatturazione di Advanced File Sync & Share non ha inizio al momento della sua attivazione, ma solo dopo che un cliente inizia a utilizzare le funzionalità avanzate. L'insieme di funzionalità abilitate verrà contabilizzato e incluso nei report di utilizzo, ma non verrà fatturato a meno che tali funzionalità non siano utilizzate.

Fatturazione del servizio Physical Data Shipping

La fatturazione del servizio Physical Data Shipping avviene in base a un modello a consumo.

Fatturazione del servizio Notary

La fatturazione del servizio Notary avviene in base a un modello a consumo.

Utilizzo delle modalità di fatturazione con le edizioni Legacy

Se non è ancora stata eseguita la migrazione al modello di fatturazione corrente, utilizzare gli elementi dell'offerta avvalendosi di una delle modalità di fatturazione per sostituire le edizioni legacy. Il motore di licensing ottimizza automaticamente le licenze assegnate al cliente per ridurre al minimo l'importo fatturabile.

Nota
Non è possibile combinare le edizioni e le modalità di fatturazione.

Passaggio dalle edizioni legacy al modello di fatturazione corrente

È possibile trasferire manualmente gli elementi dell'offerta dei tenant modificando i rispettivi profili e selezionando gli elementi come appropriato. Per ulteriori informazioni sulle procedure di passaggio, fare riferimento a "Passaggio tra edizioni e modalità di fatturazione" (pag. 9).

Per trasferire più clienti dalle edizioni alle modalità di fatturazione, vedere Trasferimento di massa dall'edizione per più clienti (67942).

Passaggio tra edizioni e modalità di fatturazione

Nel portale di gestione è possibile modificare un account tenant per trasferire gli elementi in offerta tra le modalità di fatturazione (da per workload a per gigabyte e viceversa) e tra le edizioni legacy e le modalità di fatturazione.

Per informazioni sul passaggio di massa dei tenant, vedere Trasferimento di massa dall'edizione per più clienti (67942).

La procedura di trasferimento prevede i seguenti passaggi.

1. Eseguire il provisioning dei nuovi elementi dell'offerta in un tenant cliente (abilitazione degli elementi dell'offerta e configurazione delle quote) per far sì che corrispondano alle funzionalità che erano disponibili nell'elemento dell'offerta originale.
2. Annullare l'assegnazione degli elementi dell'offerta inutilizzati e assegnare gli elementi dell'offerta ai workload in base alle funzionalità utilizzate nei piani di protezione (riconciliazione dell'utilizzo).

La tabella seguente illustra il processo in entrambe le direzioni.

	Direzione del passaggio	
	Edizione > Modalità di fatturazione	**Modalità di fatturazione > Modalità di fatturazione**
Passaggio degli elementi dell'offerta	Abilitare gli elementi dell'offerta che corrispondono alle funzionalità che erano disponibili nell'edizione di origine.	Verrà abilitato lo stesso insieme degli elementi dell'offerta.
Passaggio di quote	La quota verrà replicata dall'elemento dell'offerta di origine agli elementi dell'offerta di destinazione. Origine Standard → prodotto Standard di destinazione. Origine Standard → pacchetti di destinazione. **Nota** Se si esegue il passaggio da un'edizione con edizioni secondarie (ad esempio "Cyber Protect (per workload)"), le quote verranno sommate.	Le quote verranno replicate dall'elemento dell'offerta di origine agli elementi dell'offerta di destinazione.

	Direzione del passaggio	
	Edizione > Modalità di fatturazione	**Modalità di fatturazione > Modalità di fatturazione**
Passaggio dell'utilizzo	Gli elementi dell'offerta verranno riassegnati ai workload in base alle funzionalità richieste nei piani di protezione assegnati a tali workload.	

Esempio: Passaggio dell'edizione Cyber Protect Advanced alla fatturazione per workload

Questo scenario ipotizza un tenant cliente con l'edizione Cyber Protect Advanced utilizzata su 8 workstation, e una quota impostata su 10 workload. Nei rispettivi piani di protezione, 3 delle workstation utilizzano le funzionalità di inventario software e patch management, in 2 delle workstation è abilitato il filtraggio degli URL, e 1 dei sistemi utilizza la protezione continua dei dati. La tabella seguente illustra la conversione dell'edizione ai nuovi elementi dell'offerta.

Elementi dell'offerta di origine - utilizzo/quota	Elementi dell'offerta di destinazione - utilizzo/quota
Cyber Protect Advanced Workstation - 8/10	• Workstation - 8/10 • Advanced Security - 2/10 • Advanced Backup Workstation - 1/10 • Advanced Management - 3/10

Durante il trasferimento sono stati eseguiti i passaggi seguenti:

1. Gli elementi dell'offerta che coprono le funzionalità disponibili nell'edizione di origine sono stati abilitati automaticamente.
2. La quota è stata replicata nei nuovi elementi dell'offerta.
3. L'utilizzo è stato riconciliato in base all'utilizzo corrente nei piani di protezione: 3 workload utilizzano le funzionalità del pacchetto Advanced Management, 2 utilizzano le funzionalità del pacchetto Advanced Security e 1 utilizza le funzionalità del pacchetto Advanced Backup.

Passaggio dell'edizione Cyber Protect per workload alla fatturazione per workload

Questo esempio ipotizza che il cliente disponga di più edizioni assegnate ai workload. A ogni workload può essere assegnata solo un'edizione o una modalità di fatturazione.

Elementi dell'offerta di origine - utilizzo/quota	Elementi dell'offerta di destinazione - utilizzo/quota
Cyber Protect Essentials Workstation - 6/12	• Workstation - 14/42 • Advanced Backup Workstation - 2/42 • Advanced Security - 13/42

Elementi dell'offerta di origine - utilizzo/quota	Elementi dell'offerta di destinazione - utilizzo/quota
	• Advanced Management - 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standard Workstation - 1/10	

Durante il trasferimento sono stati eseguiti i passaggi seguenti:

1. Gli elementi in offerta che coprono le funzionalità disponibili in tutte le edizioni di origine sono stati abilitati automaticamente. Con le modalità di fatturazione, è possibile assegnare più elementi dell'offerta a un workload, come necessario.
2. Le quote sono state sommate e replicate.
3. L'utilizzo è stato riconciliato in base ai piani di protezione.

Modifica della modalità di fatturazione di un tenant partner

Per modificare la modalità di fatturazione di un tenant partner

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il tenant partner di cui si desidera modificare la modalità di fatturazione, fare clic sull'icona dei puntini di sospensione , quindi fare clic su **Configura**.
3. Nella scheda **Cyber Protect**, selezionare il servizio per il quale si desidera modificare la modalità di fatturazione e fare clic su **Modifica**.
4. Selezionare la modalità di fatturazione desiderata e abilitare o disabilitare gli elementi in offerta come necessario.
5. Fare clic su **Salva**.

Modifica della modalità di fatturazione di un tenant cliente

Le azioni seguenti consentono di modificare la modalità di fatturazione di un tenant cliente:

- Modifica della modalità di fatturazione originale abilitando o disabilitando gli elementi in offerta.
- Passaggio a una modalità di fatturazione completamente nuova.

Per altre informazioni su come modificare gli elementi in offerta disponibili, fare riferimento a Abilitazione o disabilitazione degli elementi in offerta.

Per modificare la modalità di fatturazione di un tenant cliente

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il tenant cliente di cui si desidera modificare l'edizione, fare clic sull'icona dei puntini di sospensione , quindi fare clic su **Configura**.

3. Nella scheda **Configura**, in **Servizio**, selezionare la nuova modalità di fatturazione.
   Viene visualizzata una finestra di dialogo che informa sulle conseguenze del passaggio alla nuova modalità di fatturazione.
4. Immettere il nome utente per confermare la scelta effettuata.

Nota
Questa modifica può richiedere fino a 10 minuti per poter essere completata.

Offerta di elementi e gestione delle quote

In questa sezione viene descritto quanto segue:

- Cosa sono i servizi e gli elementi dell'offerta?
- Come vengono abilitati o disabilitati gli elementi dell'offerta?
- Cosa sono le modalità di fatturazione?
- Cosa sono i pacchetti di protezione Advanced?
- Cosa sono le edizioni legacy e le edizioni secondarie?
- Cosa sono le quote flessibili e rigide?
- Quando è possibile superare una quota rigida?
- In cosa consiste la trasformazione di una quota di backup?
- In che modo la disponibilità di un elemento dell'offerta può influenzare la disponibilità del programma di installazione nella console del servizio?

Servizi ed elementi dell'offerta

Servizi

Un servizio cloud è un insieme di funzionalità ospitate da un partner o nel cloud privato di un cliente finale. In genere, i servizi vengono venduti come abbonamenti o con un modello di pagamento a consumo.

Il servizio Cyber Protect integra Cyber Security, protezione dati e gestione per proteggere endpoint, sistemi e dati dalle minacce informatiche più recenti. Il servizio Cyber Protect è costituito da diversi componenti: Protezione, File Sync & Share, Notary e Physical Data Shipping. Alcuni di questi possono essere estesi con le funzionalità aggiuntive dei pacchetti di protezione Advanced. Per informazioni dettagliate sulle funzionalità avanzate e incluse, vedere "Servizi Cyber Protect" (pag. 6).

Elementi dell’offerta

Un elemento dell'offerta è un insieme di funzionalità di un servizio raggruppate per specifici tipi di workload o di funzionalità, ad esempio: storage, infrastruttura di disaster recovery e altri. Abilitando elementi dell'offerta specifici, è possibile determinare quali workload è possibile proteggere, quanti workload è possibile proteggere (impostando le quote), e il livello di protezione che sarà disponibile

ai partner, ai clienti e ai rispettivi utenti finali (abilitando o disabilitando i pacchetti di protezione avanzata).

La funzionalità non abilitata non sarà visibile a clienti e utenti, a meno che non venga configurato uno scenario di upselling. Per ulteriori informazioni sugli scenario di upselling, vedere "Configurazione di scenari di upselling per i clienti" (pag. 66).

L'utilizzo della funzionalità viene monitorato dai servizi e si riflette negli elementi dell'offerta, che viene utilizzata nei report e per la fatturazione.

Modalità di fatturazione ed edizioni

Le edizioni Legacy consentono di abilitare solo un elemento dell'offerta per workload. Con le modalità di fatturazione, la funzionalità è suddivisa; è così possibile abilitare più elementi dell'offerta (funzionalità del servizio e pacchetti Advanced) per workload, per meglio rispondere alle esigenze del cliente e applicare una fatturazione più precisa che tiene conto soltanto delle funzionalità effettivamente utilizzate dai clienti.

Per ulteriori informazioni sulle modalità di fatturazione di Cyber Protect, vedere "Modalità di fatturazione per Cyber Protect" (pag. 7).

È possibile utilizzare le modalità di fatturazione o le edizioni per configurare i servizi disponibili ai tenant. È possibile selezionare un modello di fatturazione o un'edizione per ogni tenant cliente. Per applicare diversi modelli di fatturazione per diverse funzionalità del servizio, è quindi necessario creare più tenant per un cliente. Se, ad esempio, un cliente desidera avere le caselle di posta di Microsoft 365 in modalità di fatturazione per gigabyte, e Microsoft Teams in modalità di fatturazione per workload, per questo cliente sarà necessario creare due diversi tenant cliente.

Per limitare l'utilizzo dei servizi in un elemento dell'offerta, è possibile definire le quote relative all'elemento. Vedere "Quote flessibili e rigide" (pag. 14).

Abilitazione o disabilitazione degli elementi dell'offerta

È possibile abilitare tutti gli elementi dell'offerta disponibili per una specifica edizione o modalità di fatturazione, come descritto in Creazione di un tenant.

Nota
La disabilitazione di tutti gli elementi dell'offerta non disabilita automaticamente il servizio.

Non sempre è possibile disabilitare gli elementi dell'offerta. Le limitazioni sono elencate nella tabella seguente.

Elemento dell'offerta	Disabilitazione	Risultato
Archiviazione di backup	Può essere disabilitato quando il consumo è pari a zero.	L'archivio di backup non è più disponibile come destinazione dei backup di un tenant cliente.

Backup locale	Può essere disabilitato quando il consumo è pari a zero.	L'archivio locale non è più disponibile come destinazione dei backup di un tenant cliente.
Origini dei dati (incluso Microsoft 365 e Google Workspace)	Può essere disabilitato quando il consumo è pari a zero.	Il backup e il ripristino delle origini dei dati (incluso Microsoft 365 e Google Workspace) non è più disponibile per il tenant cliente.
Tutti gli elementi dell'offerta Disaster Recovery	Può essere disabilitato quando il consumo è pari a zero.	Per ulteriori dettagli, vedere "Quote flessibili e rigide".
Tutti gli elementi dell'offerta Notary	Può essere disabilitato quando il consumo è pari a zero.	Il servizio Notary non è più disponibile per il tenant cliente.
Tutti gli elementi dell'offerta File Sync & Share	Non è possibile abilitare o disabilitare gli elementi dell'offerta separatamente.	Il servizio File Sync & Share non è più disponibile per il tenant cliente.
Tutti gli elementi dell'offerta Consegna fisica dei dati	Può essere disabilitato quando il consumo è pari a zero.	Il servizio Consegna fisica dei dati non è più disponibile per il tenant cliente.

Nel caso di un elemento dell'offerta che non è possibile disabilitare quando il consumo è superiore a zero, rimuovere manualmente il consumo e quindi disabilitare l'elemento dell'offerta corrispondente.

Quote flessibili e rigide

Le **quote** consentono di limitare la capacità di un tenant di utilizzare il servizio. Per impostare le quote, selezionare il cliente nella scheda **Clienti**, selezionare la scheda del servizio e quindi fare clic su **Modifica**.

Quando la quota viene superata, viene inviata una notifica all'indirizzo e-mail dell'utente. Se non viene impostato un surplus della quota, la quota viene considerata "**flessibile.**" Ciò significa che non vengono applicati limiti relativi all'utilizzo del servizio Cyber Protection.

Se viene specificato il surplus della quota, la quota è considerata "**rigida.**" Il **surplus della quota** consente all'utente di superare la quota del valore specificato. Quando si supera surplus della quota, vengono applicati i limiti definiti per l'uso del servizio.

Esempio

Quota flessibile: È stata impostata una quota per workstation pari a 20. Quando il numero delle workstation protette del cliente raggiunge 20, il cliente riceve una notifica via e-mail, ma il servizio Cyber Protection rimane disponibile.

Quota rigida: Se è stata impostata una quota per workstation pari a 20 e un surplus della quota di 5, il cliente riceve una notifica via e-mail quando il numero delle workstation protette raggiunge 20 e il servizio Cyber Protection viene disabilitato quando il numero raggiunge 25.

Quando viene raggiunta una quota fissa, il servizio viene limitato: non sarà possibile proteggere un altro workload o utilizzare più storage. Quando viene superata una quota fissa, il sistema invia una notifica all'indirizzo e-mail dell'utente.

Livelli nei quali è possibile definire le quote

La tabella seguente elenca i livelli in cui è possibile configurare le quote.

Tenant/Utente	Quota flessibile (solo quota)	Quota rigida (quota e surplus della quota)
Partner	sì	no
Cartella	sì	no
Cliente	sì	sì
Unità	no	no
Utente	sì	sì

È possibile configurare le quote flessibili a livello di partner e cartella. Non è possibile configurare le quote a livello di unità. È possibile configurare le quote rigide a livello di cliente e utente.

La quantità totale di quote rigide configurate a livello di utente non può superare la quota rigida del cliente correlato.

Impostazione di quote variabili e fisse

Per impostare le quote dei clienti

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il cliente per il quale impostare le quote.
3. Selezionare la scheda **Protezione**, quindi fare clic su **Modifica**.
4. Selezionare il tipo di quota da impostare. Ad esempio, selezionare **Workstation** o **Server**.
5. Fare clic sul link **Illimitata** a destra per aprire la finestra **Modifica quota**.
   - Se si desidera informare il cliente sul livello della quota senza limitare la capacità del cliente di utilizzare il servizio, impostare il valore della quota nel campo **Quota variabile**.
     Al raggiungimento della quota indicata, il cliente riceverà una notifica e-mail, ma il servizio Cyber Protection sarà ancora disponibile.
   - Se si desidera limitare l'utilizzo del servizio da parte del cliente, selezionare **Quota fissa** e impostare il valore della quota nel campo al di sotto di **Quota fissa**.
     Al raggiungimento della quota indicata, il cliente riceverà una notifica e il servizio Cyber

Protection verrà disabilitato.

6. Nella finestra **Modifica quota**, fare clic su **Fine**, quindi su **Salva**.

Quote del servizio Backup

È possibile specificare la quota di archiviazione nel cloud, la quota per il backup locale e il numero massimo di sistemi/dispositivi/siti web che un utente è autorizzato a proteggere. Sono disponibili le quote seguenti:

Quote per dispositivi

- **Workstation**
- **Server**
- **Macchine virtuali**
- **Dispositivi mobili**
- **Server di web hosting** (server virtuali e fisici Linux che eseguono i pannelli di controllo di Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager)
- **Siti Web**

Un sistema/dispositivo/sito web è considerato protetto finché risulta associato ad almeno un piano di protezione. Un dispositivo mobile diventa protetto dopo il primo backup.

Quando il surplus della quota viene superato per più dispositivi, l'utente non può applicare il piano di protezione ad altri dispositivi.

Quote per origini dati nel cloud

- **Utenze di Microsoft 365**
  Questa quota è applicata dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare la quota e l'utilizzo nel portale di gestione.
  Il licensing delle utenze di Microsoft 365 dipende dalla modalità di fatturazione selezionata per Cyber Protection.
  Nella modalità di fatturazione **Per workload**, la quota delle **utenze di Microsoft 365** viene conteggiata per i singoli utenti. È considerato singolo utente un utente che ha almeno:
  - Casella di posta protetta
  - OneDrive protetto
  - Accesso ad almeno una risorsa protetta a livello aziendale: Sito di Microsoft 365 SharePoint Online o Microsoft 365 Teams.
    Per maggiori informazioni su come controllare il numero di membri di un sito di Microsoft 365 SharePoint o Teams, fare riferimento a questo articolo della Knowledge Base.

Nota

Gli utenti bloccati di Microsoft 365 che non dispongono di una casella di posta personale protetta o di OneDrive, e possono accedere solo alle risorse condivise (caselle di posta condivise, siti SharePoint e Microsoft Teams), non riceveranno alcun addebito.

Per utente bloccato si intende l'utente che non dispone di credenziali valide e che non può accedere ai servizi di Microsoft 365. Per scoprire come bloccare tutti gli utenti senza licenza in un'organizzazione di Microsoft 365, fare riferimento a "Impedire l'accesso agli utenti di Microsoft 365 senza licenza" (pag. 19).

Le utenze di Microsoft 365 seguenti non vengono addebitate e non richiedono una licenza per utenza:

- Caselle di posta condivise
- Sale e attrezzatura
- Utenti esterni con accesso ai siti SharePoint e/o Microsoft Teams oggetto di backup

Per ulteriori informazioni sulle opzioni di licenza disponibili con la modalità di fatturazione per gigabyte, fare riferimento alla documentazione di Cyber Protect Cloud relativa al licensing per GB di Microsoft 365.

Per ulteriori informazioni sulle opzioni di licenza disponibili con la modalità di fatturazione per workload, fare riferimento alla documentazione di Cyber Protect Cloud relativa alle modifiche di pricing e licensing per Microsoft 365.

- **Microsoft 365 Teams**

  Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere i team di Microsoft 365 e definisce il numero massimo di team che è possibile proteggere. Per la protezione di un team, indipendentemente dal numero di membri o di canali che lo costituiscono, è necessaria una quota. Gli amministratori dell'azienda possono visualizzare la quota e l'utilizzo nel portale di gestione.

- **Microsoft 365 SharePoint Online**

  Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere i siti di SharePoint Online e definisce il numero massimo di raccolte dei siti e siti di gruppo che è possibile proteggere.

  Gli amministratori dell'azienda possono visualizzare la quota nel portale di gestione. La quota può inoltre essere visualizzata, insieme alla quantità di archivio occupato dai backup di SharePoint Online nei report di utilizzo.

- **Utenze di Google Workspace**

  Questa quota è applicata dal service provider per l'intera azienda. L'azienda può proteggere caselle di posta di **Gmail** (incluso calendario e contatti), file di **Google Drive** o entrambi. Gli amministratori dell'azienda possono visualizzare la quota e l'utilizzo nel portale di gestione.

- **Google Workspace Shared Drive**

  Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere le unità condivise di Google Workspace Shared Drive. Se la

quota è abilitata, è possibile proteggere un numero illimitato di unità condivise. Gli amministratori dell'azienda non possono visualizzare la quota nel portale di gestione, ma possono visualizzare la quantità di archivio occupato dai backup delle unità condivise nei report di utilizzo.

Il backup delle unità condivise di Google Workspace è disponibile solo ai clienti che dispongono di almeno una quota di utenze di Google Workspace aggiuntiva. Tale quota viene solo verificata e non sarà utilizzata.

Un'utenza di Microsoft 365 è considerata protetta finché almeno un piano di protezione è applicato alla casella di posta o al OneDrive dell'utente. Un'utenza di Google Workspace è considerata protetta finché almeno un piano di protezione è applicato alla casella di posta o al Google Drive dell'utente.

Quando il surplus della quota viene superato per più utenze, l'amministratore dell'azienda non può applicare il piano di protezione ad altre utenze.

Quote per archivio

- **Backup locale**

  La quota **Backup locale** limita la dimensione totale dei backup locali creati utilizzando l'infrastruttura cloud. Non è possibile definire un surplus per questa quota.
- **Risorse cloud**

  La quota **Risorse cloud** combina la quota per l'archivio di backup e le quote per il disaster recovery. La quota di archiviazione di backup limita la dimensione totale dei backup posizionati nell'archivio cloud. Quando si supera il surplus della quota, i backup non vanno a buon fine.

Superamento della quota per l'archivio di backup

La quota di archiviazione del backup non può essere superata. Il certificato dell'agente di protezione prevede una quota tecnica che equivale alla quota di backup del tenant più il surplus della quota. Se la quota viene superata, il backup non verrà avviato. Se la quota nel certificato viene raggiunta durante la creazione del backup, ma il surplus della quota non viene superato, il backup avrà esito positivo. Se il surplus della quota viene raggiunto durante la creazione del backup, il backup avrà esito negativo.

Esempio:

Un tenant utente ha 1 TB di spazio disponibile della quota, e il surplus configurato per questo utente è pari a 5 TB. L'utente avvia un backup. Se la dimensione del backup creato è, ad esempio 3 TB, il backup verrà completato con esito positivo perché il surplus della quota non è stato superato. Se la dimensione del backup supera i 6 TB, il backup si interromperà al superamento del surplus della quota.

Trasformazione di una quota di backup

Ecco come funziona in linea di massima l'acquisizione di una quota di backup e il mapping di un elemento dell'offerta al tipo di risorsa: il sistema confronta gli elementi dell'offerta disponibili con il

tipo di risorsa, e quindi acquisisce la quota per l'elemento dell'offerta corrispondente.

È anche possibile assegnare un'altra quota all'elemento dell'offerta, anche se non corrisponde esattamente al tipo di risorsa. È questa la cosiddetta **trasformazione della quota di backup**. Se non è presente un elemento dell'offerta corrispondente, il sistema tenta di trovare una quota appropriata più costosa per il tipo di risorsa (trasformazione automatica della quota di backup). Se non viene individuato nulla di adeguato, è possibile assegnare manualmente la quota di servizio al tipo di risorsa nella console del servizio.

Esempio

Si desidera eseguire il backup di una macchina virtuale (workstation, con agente).

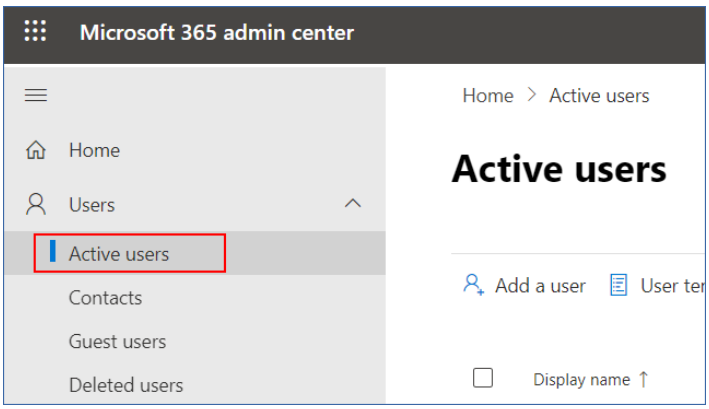
In primo luogo, il sistema controlla se è presente una quota **Macchine virtuali** allocata. Se non viene individuata, il sistema tenta automaticamente di acquisire la quota **Workstation**. Se non viene trovata neanche questa, l'altra quota non verrà acquisita automaticamente. Se è disponibile una quota sufficiente più costosa rispetto alla quota **Macchine virtuali** e se questa è applicabile a una macchina virtuale, sarà possibile accedere alla console del servizio e assegnare manualmente la quota **Server**.

Impedire l'accesso agli utenti di Microsoft 365 senza licenza

È possibile impedire di accedere a tutti gli utenti senza licenza presenti nell'organizzazione Microsoft 365 modificando il relativo stato di accesso.

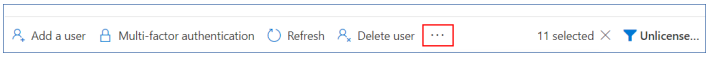
Per impedire l'accesso agli utenti senza licenza

1. Accedere al centro di amministrazione di Microsoft 365 (https://admin.microsoft.com) con un ruolo di amministratore globale.
2. Nel menu di navigazione, passare a **Utenti** > **Utenti attivi**.



3. Fare clic su **Filtro** e quindi selezionare **Utenti senza licenza**.

4. Selezionare le caselle di controllo accanto ai nomi degli utenti, quindi fare clic sull'icona dei puntini di sospensione (...).



5. Nel menu, selezionare **Modifica stato di accesso**.
6. Selezionare la casella di controllo **Blocca l'accesso degli utenti** e fare clic su **Salva**.

Quote del servizio Disaster Recovery

Nota
Gli elementi dell'offerta Disaster Recovery sono disponibili solo con il componente aggiuntivo Disaster Recovery.

Queste quote sono applicate dal service provider per l'intera azienda. Gli amministratori dell'azienda possono visualizzare le quote e l'utilizzo nel portale di gestione, ma non possono definire le quote per un utente.

- **Archivio di disaster recovery**
  Lo storage Disaster Recovery mostra la dimensione dello storage ad accesso infrequente dei server protetti con Disaster Recovery. Tale storage è calcolato a partire dal momento in cui viene creato un server di ripristino, a prescindere dal fatto che il server sia attualmente in esecuzione oppure no. Se il surplus per questa quota viene raggiunto, non sarà possibile creare server primari e di ripristino o aggiungere/estendere dischi ai server primari esistenti. Se il surplus per questa quota viene superato, non sarà possibile avviare un failover o semplicemente avviare un server arrestato. I server in esecuzione non verranno arrestati.
- **Punti di calcolo**
  Questa quota limita le risorse di CPU e RAM che vengono consumate dai server primari e di ripristino nell'arco di un periodo di fatturazione. Se il surplus per questa quota viene raggiunto, tutti i server primari e di ripristino verranno spenti. Non sarà possibile utilizzare questi server fino all'inizio del successivo periodo di fatturazione. Per impostazione predefinita, il periodo di fatturazione corrisponde a un mese di calendario.
  Se la quota è disabilitata, non è possibile utilizzare i server, indipendentemente dal periodo di fatturazione.
- **Indirizzi IP pubblici**
  Questa quota limita il numero di indirizzi IP pubblici che è possibile assegnare ai server primari e di ripristino. Se il surplus per questa quota viene raggiunto, non sarà possibile abilitare indirizzi IP pubblici per altri server. È possibile impedire a un server di utilizzare un indirizzo IP pubblico deselezionando la casella di controllo **Indirizzo IP pubblico** nelle impostazioni del server. Successivamente, è possibile consentire a un altro server di utilizzare un indirizzo IP pubblico, che in genere non sarà lo stesso.
  Quando la quota è disabilitata, nessun server utilizza gli indirizzi IP pubblici e pertanto non sarà raggiungibile da Internet.
- **Server cloud**
  Questa quota limita il numero totale di server primari e di ripristino. Se il surplus per questa quota viene raggiunto, non sarà possibile creare server primari o di ripristino.

Se la quota è disabilitata, i server sono visibili solo nella console del servizio, ma l'unica operazione disponibile è **Elimina**.

- **Accesso Internet**

  Questa quota abilita o disabilita l'accesso a Internet dai server primari o di ripristino.

  Se la quota è disabilitata, i server primari e di ripristino non saranno in grado di connettersi a Internet.

Quote del servizio File Sync & Share

È possibile definire le seguenti quote del servizio File Sync & Share per un tenant:

- **Utenti**

  Questa quota consente di configurare il numero di utenti che possono accedere al servizio.

  Gli account Amministratore non vengono conteggiati come parte della quota.
- **Archiviazione nel cloud**

  Un archivio nel cloud nel quale archiviare i file degli utenti. Questa quota definisce lo spazio allocato per un tenant nell'archiviazione nel cloud.

Quote del servizio Consegna fisica dei dati

Il consumo delle quote del servizio Consegna fisica dei dati viene considerato per unità. È possibile salvare i backup iniziali di più sistemi su un solo disco rigido.

È possibile definire le seguenti quote del servizio Consegna fisica dei dati per un tenant:

- **Nel cloud**

  Consente di inviare un backup iniziale al datacenter cloud utilizzando un'unità disco rigido. Questa quota definisce il numero massimo di unità che possono essere trasferite al datacenter cloud.

Quote del servizio Notary

È possibile definire le seguenti quote del servizio Notary per un tenant:

- **Archivio Notary**

  L'Archivio Notary è l'archivio cloud del servizio di autenticazione nel quale vengono memorizzati i file autenticati, i file firmati e i file di cui è in corso il processo di autenticazione o di firma. Questa quota definisce lo spazio massimo che può essere occupato dai file in questione.

  Per diminuire l'utilizzo della quota, è possibile eliminare i file già autenticati o firmati dall'archivio.
- **Autenticazioni**

  Questa quota definisce il numero massimo di file autenticabili tramite il servizio di autenticazione. Un file viene considerato autenticato non appena viene caricato nell'archivio di autenticazione e il relativo stato di autenticazione cambia in In corso.

  Se lo stesso file viene autenticato più volte, ogni autenticazione vale come una nuova.
- **eSignature**

Questa quota definisce il numero massimo di file che possono essere firmati tramite il servizio di autenticazione. Un file viene considerato firmato non appena viene inviato alla firma.

Modifica della quota di servizio dei sistemi

Il livello di protezione di un sistema è definito dalla quota di servizio ad esso applicata. Le quote di servizio si riferiscono agli elementi dell'offerta disponibili per il tenant in cui è registrato il sistema.

Una quota di servizio viene automaticamente assegnata quando un piano di protezione viene applicato per la prima volta a un sistema.

Viene assegnata la quota più appropriata in funzione del tipo di sistema protetto, del suo sistema operativo, del livello di protezione richiesto e di disponibilità della quota. Se nell'organizzazione non è disponibile una quota appropriata, verrà assegnata la seconda migliore quota disponibile. Se, ad esempio, la quota più appropriata è **Server di web hosting** ma questa non è disponibile, verrà assegnata la quota **Server**.

Esempi di assegnazione delle quote:

- A un sistema fisico che esegue un server Windows o un sistema operativo Linux viene assegnata la quota **Server**.
- A un sistema fisico che esegue un sistema operativo Windows desktop viene assegnata la quota **Workstation**.
- A un sistema fisico che esegue il sistema operativo Windows 10 con un ruolo di Hyper-V abilitato, viene assegnata la quota **Workstation**.
- A un sistema desktop che viene eseguito su un'infrastruttura desktop virtuale e il cui agente di protezione è installato nel sistema operativo guest (ad esempio, Agente per Windows), viene assegnata la quota **Virtual machine**. Questo tipo di sistema può inoltre utilizzare la quota **Workstation** se la quota **Virtual machine** non è disponibile.
- A un sistema desktop che viene eseguito su un'infrastruttura desktop virtuale e il cui backup viene eseguito in modalità agentless (ad esempio, Agente per VMware o Agente per Hyper-V), viene assegnata la quota **Virtual machine**.
- A un server Hyper-V o vSphere viene assegnata la quota **Server**.
- A un server con cPanel o Plesk viene assegnata la quota **Server di web hosting**. Questo tipo di sistema può inoltre utilizzare la quota **Virtual machine** o la quota **Server**, a seconda del tipo di sistema sul quale viene eseguito il server web, se la quota **Server di web hosting** non è disponibile.
- Il backup application-aware richiede la quota **Server** anche per una workstation.

È possibile modificare manualmente l'assegnazione originaria in un secondo momento. Ad esempio, per applicare un piano di protezione più avanzato allo stesso sistema, potrebbe essere necessario aggiornare la quota di servizio del sistema. Se le funzionalità richieste dal piano di protezione in questione non sono supportate dalla quota di servizio correntemente assegnata, il piano di protezione non avrà esito positivo.

In alternativa, è possibile modificare la quota di servizio se si acquistano quote più appropriate dopo l'assegnazione di quella originaria. Ad esempio, la quota **Workstation** viene assegnata a una virtual machine. Dopo aver acquistato una quota **Virtual machine**, è possibile assegnarla manualmente al sistema al posto della quota **Workstation** originaria.

È inoltre possibile rilasciare la quota di servizio attualmente assegnata e quindi assegnarla a un altro sistema.

È possibile modificare la quota di servizio di un singolo sistema o di un gruppo di sistemi.

Per modificare la quota di servizio di un singolo sistema

1. Nella console del servizio Cyber Protection, passare a **Dispositivi**.
2. Selezionare il sistema desiderato e fare clic su **Dettagli**.
3. Nella sezione **Quota di servizio**, fare clic su **Modifica**.
4. Nella finestra **Cambia licenza**, selezionare la quota di servizio desiderata o la voce **Nessuna quota**, quindi fare clic su **Modifica**.

Per modificare la quota di servizio di un gruppo di sistemi

1. Nella console del servizio Cyber Protection, passare a **Dispositivi**.
2. Selezionare più di un sistema, quindi fare clic su **Assegna quota**.
3. Nella finestra **Cambia licenza**, selezionare la quota di servizio desiderata o la voce **Nessuna quota**, quindi fare clic su **Modifica**.

Dipendenza del programma di installazione dell'agente dagli elementi dell'offerta

In base agli elementi dell'offerta consentiti, il programma di installazione dell'agente corrispondente sarà disponibile nella sezione **Aggiungi dispositivi** della console del servizio. La tabella seguente mostra i programmi di installazione degli agenti e la loro disponibilità nella console del servizio in base agli elementi dell'offerta abilitati.

Elementi dell'offerta abilitati **Programma di installazione dell'agente**	**Server**	**Workstation**	**Macchine virtuali**	**Utenze di Microsoft 365**	**Utenze di Google Workspace**	**Dispositivi mobili**	**Server di hosting su Web**	**Siti Web**
Workstation – Agente per Windows		+	+					+

Workstation – Agente per Mac OS X		+	+					+
Server – Agente per Windows	+		+				+	+
Server – Agente per Linux	+		+				+	+
Agente per Hyper-V			+					
Agente per VMware			+					
Agente per Virtuozzo			+					
Agente per SQL	+		+					
Agente per Exchange	+		+					
Agente per Active Directory	+		+					
Agente per Microsoft 365				+				
Agente per Google Workspace					+			
Programma di installazione completo per Windows	+	+	+				+	+
Mobile (iOS e Android)						+		

Utilizzo del portale di gestione

I seguenti passaggi guideranno l'utente nelle attività di base del portale di gestione.

Browser Web supportati

L'interfaccia Web supporta i seguenti browser:

- Google Chrome 29 o versione successiva
- Mozilla Firefox 23 o versione successiva
- Opera 16 o versione successiva
- Microsoft Edge 25 o versioni successive
- Safari 8 o versioni successive in esecuzione nei sistemi operativi macOS e iOS

In altri browser Web (inclusi browser Safari eseguiti in altri sistemi operativi), l'interfaccia utente potrebbe essere visualizzata in modo non corretto o alcune funzioni potrebbero non essere disponibili.

Attivare l'account di amministrazione

Dopo aver firmato l'accordo di partnership, l'utente riceverà un messaggio e-mail contenente le seguenti informazioni:

- **Dati di login.** Il nome utente utilizzato per accedere. I dati di login vengono visualizzati anche nella pagina di attivazione dell'account.
- Pulsante **Attiva account**. Fare clic sul pulsante e impostare la password per l'account. Verificare che la password sia lunga almeno nove caratteri. Per ulteriori informazioni sulla password, fare riferimento a "Requisiti per la password" (pag. 25).

Requisiti per la password

La password di un account utente deve essere lunga almeno 9 caratteri. Viene inoltre effettuato un controllo sulla complessità delle password, dopo il quale le password vengono collocate in una delle seguenti categorie:

- Vulnerabile
- Medio
- Complessa

Non è possibile salvare una password vulnerabile, anche se contiene 9 caratteri o più. Le password che ripetono il nome utente, il login, l'e-mail dell'utente o il nome del tenant al quale appartiene l'account utente sono considerate vulnerabili. Anche le password più comuni sono considerate vulnerabili.

Per rafforzare una password, aggiungere più caratteri. L'uso di più caratteri, come numeri, lettere maiuscole e minuscole e caratteri speciali non è obbligatorio, ma consente di creare password più complesse e anche più corte.

Accesso al portale di gestione

1. Passare alla pagina di accesso al servizio.
   L'indirizzo della pagina di accesso era incluso nel messaggio e-mail di attivazione ricevuto dall'utente.
2. Digitare il login e quindi fare clic su **Avanti**.
3. Digitare la password e quindi fare clic su **Avanti**.

   Nota
   Per impedire attacchi di forza bruta ad Cyber Protect Cloud, il portale blocca l'utente dopo 10 tentativi di accesso non riusciti. La durata del blocco è di 5 minuti. Il numero di tentativi di accesso non riusciti viene ripristinato dopo 15 minuti.

4. Utilizzare il menu a destra per spostarsi nel portale di gestione.

Il periodo di timeout per il portale di gestione è di 24 ore per le sessioni attive e di un'ora per le sessioni inattive.

Alcuni servizi prevedono la possibilità di passare al portale di gestione dalla console del servizio.

Configurazione dei contatti nella procedura guidata Profilo azienda

È possibile configurare le informazioni di contatto per la tua azienda. Ai contatti forniti verranno inviati gli aggiornamenti sulle nuove funzionalità e altre importanti modifiche apportate alla piattaforma.

Quando si accede al portale di gestione per la prima volta, la procedura guidata Profilo azienda guida l'utente attraverso i passaggi per fornire le informazioni di base sull'azienda e sui contatti.

È possibile creare contatti dagli utenti presenti nella piattaforma Cyber Protect o aggiungere le informazioni di contatto di persone che non hanno accesso al servizio.

Per configurare i contatti utilizzando la procedura guidata Profilo azienda

1. Nella sezione **Informazioni sull'azienda**, specificare i dettagli seguenti relativi all'azienda:
   - **Nome società ufficiale (legale)**
   - **Indirizzo legale dell'azienda (indirizzo sede principale)**
     - **Paese**
     - **Codice postale**
2. Fare clic su **Avanti**.

3. Nella sezione **Contatti aziendali**, configurare i contatti per le finalità seguenti:
   - **Contatto per fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.
   - **Contatto Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.
   - **Contatto tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.

   È possibile utilizzare un contatto per più di una finalità.

   Selezionare un'opzione per creare il contatto.
   - **Crea da utente esistente**. Selezionare un utente dall'elenco a discesa.
   - **Crea nuovo contatto**. Fornire le informazioni di contatto seguenti:
     - **Nome** - Nome del contatto. Questo campo è obbligatorio.
     - **Cognome** - Cognome del contatto. Questo campo è obbligatorio.
     - **Indirizzo e-mail aziendale** - Indirizzo e-mail aziendale del contatto. Questo campo è obbligatorio.
     - **Telefono aziendale** - Campo facoltativo.
     - **Posizione professionale** - Campo facoltativo.
4. Se si intende utilizzare il contatto di fatturazione come contatto aziendale o contatto tecnico, selezionare i flag corrispondenti nella sezione **Contatto Fatturazione**:
   - **Utilizza lo stesso contatto del contatto Business**
   - **Utilizza lo stesso contatto del contatto Tecnico**
5. Fare clic su **Fine**.

   I contatti vengono creati. È possibile modificare le informazioni e configurare altri contatti nella sezione **Gestione azienda > Profilo azienda** della console di gestione, come descritto in Configurazione dei contatti aziendali.

Accesso alla console di Cyber Protection dal portale di gestione

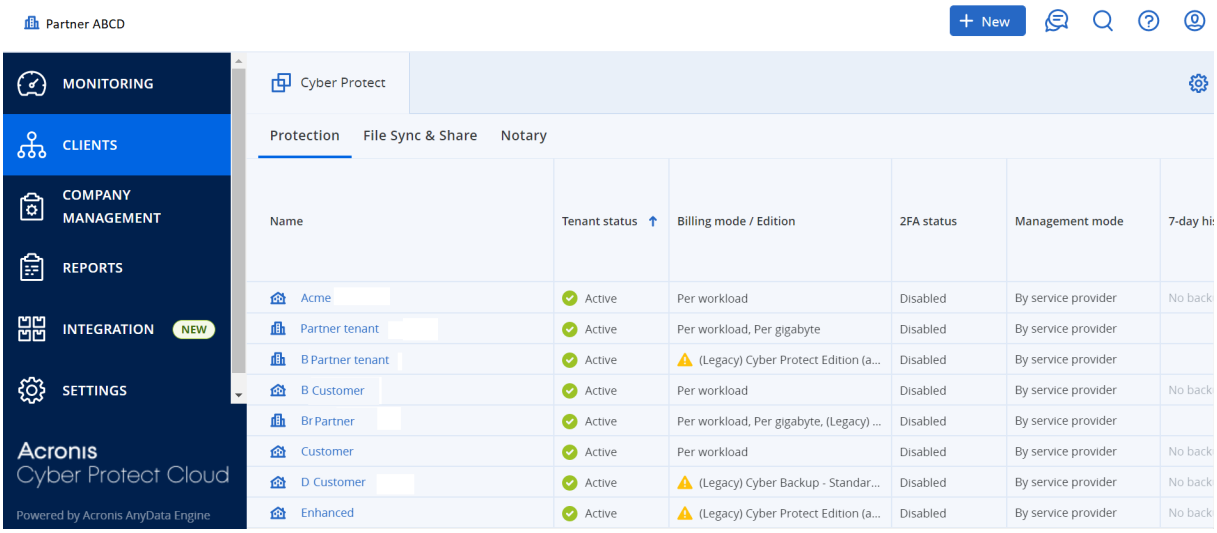
1. Nel portale di gestione passare a **Monitoraggio** > **Utilizzo**.
2. In **Cyber Protect**, selezionare **Protezione** quindi fare clic su **Gestisci servizio**.
   In alternativa, in **Clienti**, selezionare un cliente e quindi fare clic su **Gestisci servizio**.

L'utente viene reindirizzato alla console di Cyber Protection.

Navigazione nel portale di gestione

Quando si usa il portale di gestione, in qualsiasi momento si lavora con un tenant. Il nome di questo tenant viene indicato nell'angolo in alto a sinistra.

Per impostazione predefinita, è selezionato il livello gerarchico più elevato disponibile all'utente. Fare clic sul nome del tenant nell'elenco per esaminare in dettaglio la gerarchia. Per tornare a un livello superiore, fare clic sul nome del livello nell'angolo in alto a sinistra.



Vengono visualizzate tutte le sezioni dell'interfaccia utente, relative solo al tenant nel quale si sta lavorando. Per esempio:

- La scheda **Clienti** visualizza solo i tenant che sono figli diretti del tenant nel quale si sta lavorando.
- La scheda **Gestione azienda** visualizza il profilo dell'azienda e gli account utente esistenti nel tenant nel quale si sta lavorando.
- Il pulsante **Nuovo** consente di creare un tenant o un nuovo account utente solo nel tenant nel quale si sta lavorando.

Limitazione dell'accesso all'interfaccia Web

Gli amministratori possono limitare l'accesso all'interfaccia Web specificando un elenco di indirizzi IP da cui i membri di un tenant possono eseguire l'accesso.

Questa limitazione si applica anche all'accesso al portale di gestione tramite l'API.

Questa limitazione è valida solo per il livello in cui è impostata. *Non* si applica ai membri dei tenant figlio.

Per limitare l'accesso all'interfaccia Web

1. Accedere al portale di gestione.
2. Passare al tenant per il quale si desidera limitare l'accesso.
3. Fare clic su **Impostazioni** > **Sicurezza**.
4. Abilitare l'interruttore **Controllo accesso**.
5. In **Indirizzi IP consentiti**, specificare gli indirizzi IP consentiti.

È possibile immettere i seguenti parametri, separati da un punto e virgola.

- Indirizzi IP, ad esempio: 192.0.2.0
- Intervalli IP, ad esempio: 192.0.2.0-192.0.2.255
- Sottoreti, ad esempio: 192.0.2.0/24

6. Fare clic su **Salva**.

Nota
Per i service provider che utilizzano Cyber Infrastructure (modello ibrido):

Se l'opzione **Controllo accesso** è abilitata nel portale di gestione, in **Impostazioni** > **Sicurezza**, aggiungere l'indirizzo IP pubblico esterno dei nodi di Cyber Infrastructure all'elenco degli **indirizzi IP consentiti**.

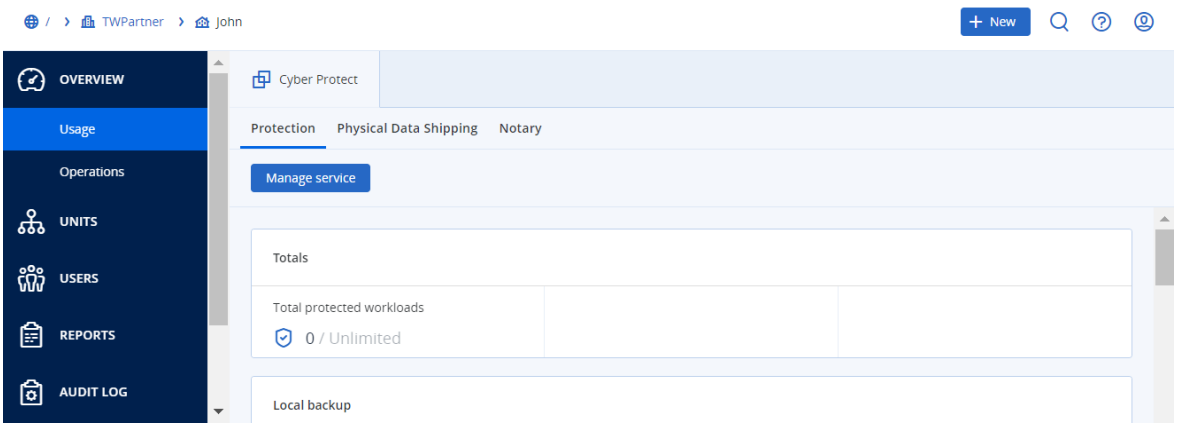
Accesso ai servizi

Scheda Panoramica

La sezione **Panoramica** > **Utilizzo** fornisce una panoramica dell'utilizzo del servizio e consente di accedere ai servizi inclusi nel tenant nel quale si sta lavorando.

Per gestire un servizio per un tenant utilizzando la scheda Panoramica

1. Passare al tenant per il quale si desidera gestire il servizio e quindi fare clic su **Panoramica** > **Utilizzo**.
   Tenere presente che alcuni servizi possono essere gestiti a livello di tenant partner e ai livelli dei tenant cliente, mentre altri servizi possono essere gestiti solo a livello di tenant cliente.
2. Fare clic sul nome del servizio che si desidera gestire e quindi fare clic su **Gestisci servizio** o su **Configura servizio**.
   Per informazioni sull'uso dei servizi, fare riferimento ai manuali dell'utente disponibili nelle console dei servizi.

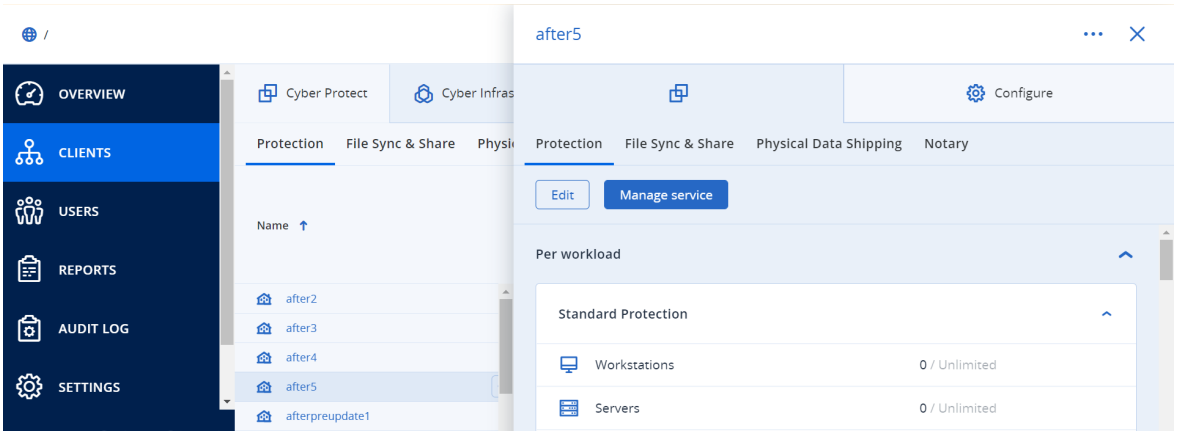


Scheda Clienti

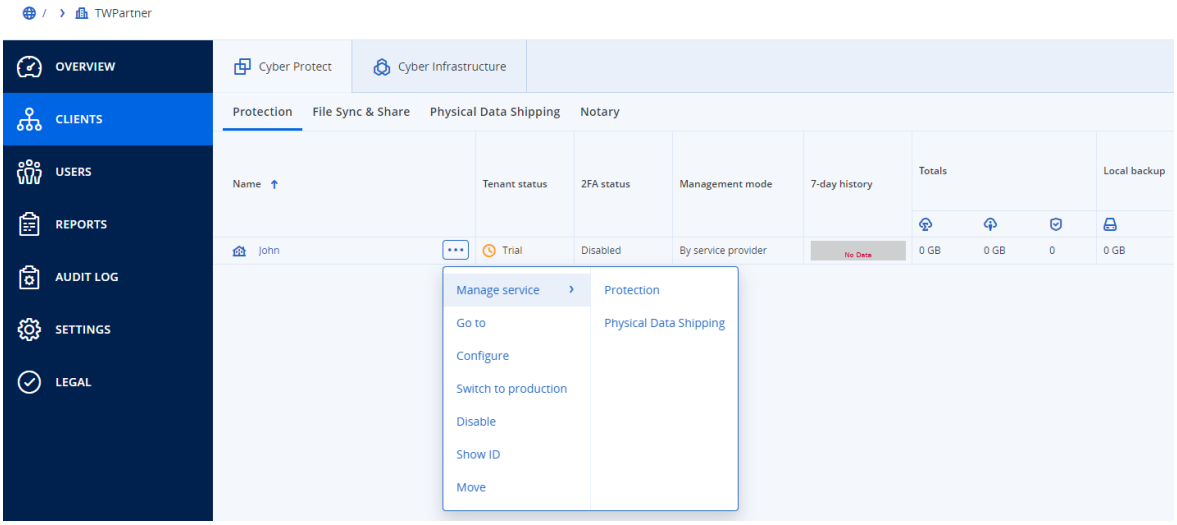
La scheda **Clienti** visualizza i tenant figlio del tenant nel quale si sta lavorando e consente di accedere ai servizi che questi contengono.

Per gestire un servizio per un tenant utilizzando la scheda Clienti

1. Eseguire una delle seguenti operazioni:
   - Fare clic su **Clienti**, selezionare il tenant per il quale gestire il servizio, fare clic sul nome o sull'icona del servizio che si desidera gestire fare clic su **Gestisci servizio** o su **Configura servizio**.



   - Fare clic su **Clienti** quindi sull'icona dei puntini di sospensione accanto al nome del tenant per il quale gestire il servizio, fare clic su **Gestisci servizio** e quindi selezionare il servizio da gestire.



Tenere presente che alcuni servizi possono essere gestiti a livello di tenant partner e ai livelli dei tenant cliente, mentre altri servizi possono essere gestiti solo a livello di tenant cliente.

Per informazioni sull'uso dei servizi, fare riferimento ai manuali dell'utente disponibili nelle console dei servizi.

Barra Cronologia a 7 giorni

Nella schermata **Clienti**, la barra **Cronologia a 7 giorni** mostra lo stato dei backup dei workload per ogni tenant cliente per gli ultimi sette giorni. La barra è divisa in 168 linee colorate. Ogni linea rappresenta un intervallo di un'ora e mostra lo stato peggiore di un backup nel corrispondente intervallo.

La tabella seguente fornisce informazioni sul significato di ogni colore delle linee.

Colore	Descrizione
rosso	durante il periodo di un'ora, almeno uno dei backup non è riuscito
arancio	durante il periodo di un'ora, almeno uno dei backup è stato completato con un avviso, ma senza errori di backup
verde	durante il periodo di un'ora, almeno uno dei backup ha avuto esito positivo, senza avvisi né errori di backup
grigio	durante il periodo di un'ora, non è stato completato alcun backup

La barra **Cronologia a 7 giorni** indicherà "Nessun backup" fino a quando non verrà acquisita la statistica corrispondente.

Per i tenant partner, la barra **Cronologia a 7 giorni** è vuota, poiché non sono supportate le statistiche aggregate.

Account utente e tenant

Esistono due tipi di account utente: account amministratore e account utente.

- Gli **amministratori** possono accedere al portale di gestione. Dispongono del ruolo di amministratore in tutti i servizi.
- Gli **utenti** non possono accedere al portale di gestione. Il loro accesso ai servizi e il loro ruolo nei servizi viene definito da un amministratore.

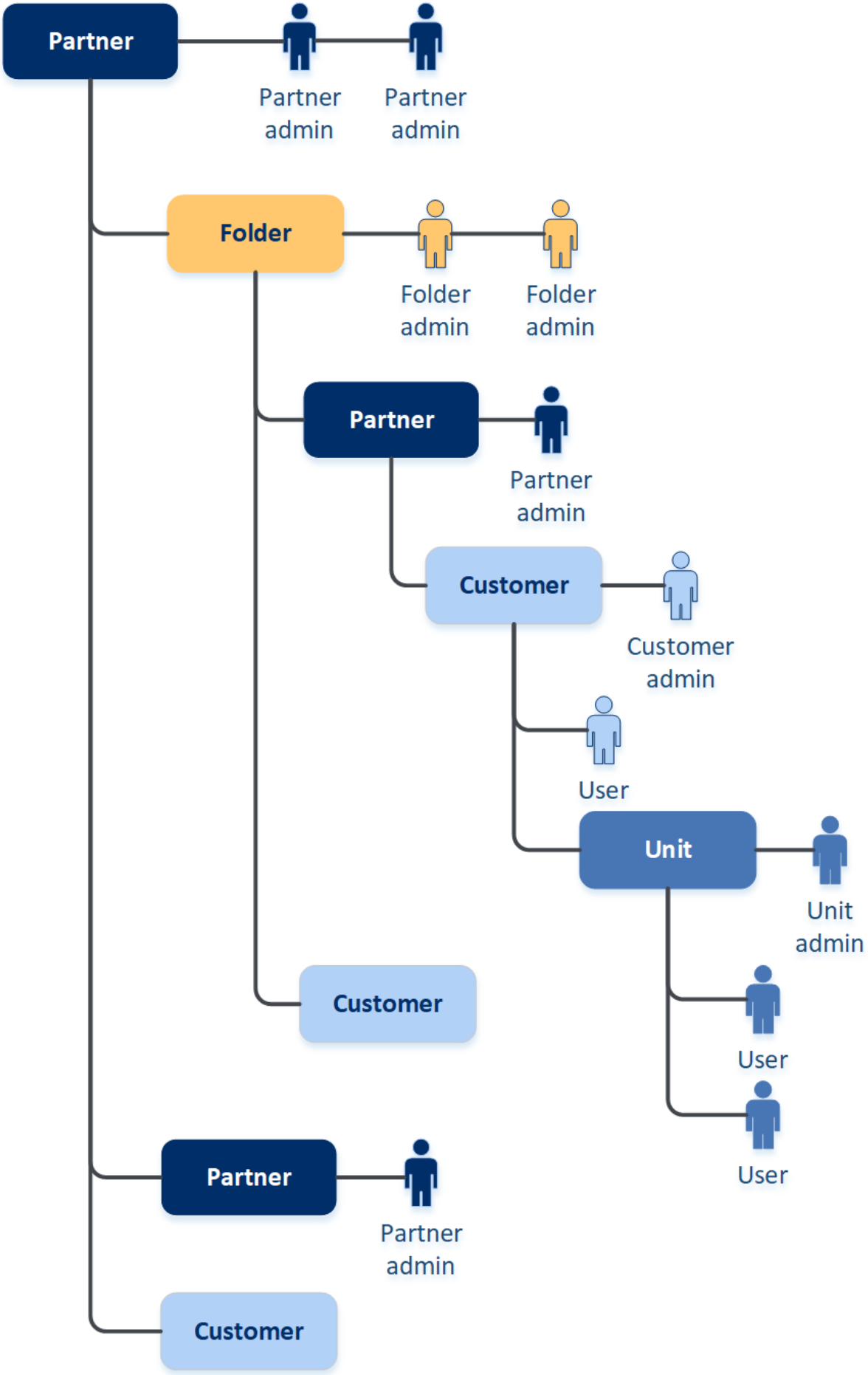
Ogni account appartiene a un tenant. Un tenant è un componente delle risorse del portale di gestione (come gli account utente e i tenant figlio) e delle offerte di servizi (servizi abilitati ed elementi offerti che questi contengono) dedicati a un partner o a un cliente. La gerarchia del tenant dovrebbe corrispondere alla relazione cliente/fornitore tra gli utenti e i fornitori del servizio.

- Il tenant di tipo **Partner** corrisponde in genere ai service provider che rivendono i servizi.
- Il tenant di tipo **Cartella** è un tenant aggiuntivo che viene usato in genere dagli amministratori dei partner per raggruppare partner e clienti per i quali configurare offerte distinte e/o branding differenti.
- Il tenant di tipo **Cliente** corrisponde in genere alle organizzazioni che utilizzano i servizi.
- Il tenant di tipo **Unità** corrisponde in genere alle unità o ai reparti dell'organizzazione.

Un amministratore può creare e gestire tenant, account amministratore e account utente nel proprio livello di gerarchia o a un livello inferiore.

L'amministratore di un tenant padre di tipo **Partner** può agire come amministratore di livello inferiore nei tenant di tipo **Cliente** o **Partner**, la cui modalità di gestione è impostata su **Gestito dal service provider**. Pertanto, l'amministratore a livello di partner può, ad esempio, gestire account utente e servizi o accedere a backup e altre risorse nel tenant figlio. Tuttavia, gli amministratori al livello inferiore possono limitare l'accesso ai propri tenant per gli amministratori di livello superiore.

La figura seguente illustra una gerarchia di esempio dei tenant partner, cartella, cliente e unità.


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

La seguente tabella riassume le operazioni che possono essere eseguite dagli amministratori e dagli utenti.

Operazione	Utenti	Amministratori di clienti e unità	Amministratori di partner e cartelle
Creazione di tenant	No	Sì	Sì
Creazione di account	No	Sì	Sì
Download e installazione del software	Sì	Sì	No*
Gestione servizi	Sì	Sì	Sì
Creazione di report sull'utilizzo del servizio	No	Sì	Sì
Configurazione del branding	No	No	Sì

*Un amministratore di partner che abbia necessità di eseguire queste operazioni può creare un account di amministratore o utente del cliente per proprio conto.

Gestione dei tenant

In Cyber Protect sono disponibili i seguenti tenant:

- Normalmente viene creato un tenant **Partner** per ciascun partner che firma l'accordo di partnership.
- Un tenant **Cartella** viene creato per raggruppare partner e clienti per i quali configurare offerte distinte e/o branding differenti.
- Il tenant **Cliente** viene creato di solito per ciascuna organizzazione che si registra per il servizio.
- Un nuovo tenant **Unità** viene creato all'interno di un tenant cliente per espandere il servizio a una nuova unità organizzativa.

I passaggi per la creazione e la configurazione di un tenant variano a seconda del tenant creato, ma in generale il processo prevede i seguenti passaggi:

1. Creazione del tenant.
2. Selezione dei servizi per il tenant.
3. Configurazione degli elementi dell'offerta per il tenant.

Creazione di un tenant

1. Accedere al portale di gestione.
2. Passare al tenant nel quale si desidera creare un tenant.

3. Nell'angolo in alto a destra, fare clic su **Nuovo** e quindi su una delle seguenti opzioni, a seconda del tipo di tenant che si desidera creare:
   - Normalmente viene creato un tenant **Partner** per ciascun partner che firma l'accordo di partnership.
   - Un tenant **Cartella** viene creato per raggruppare partner e clienti per i quali configurare offerte distinte e/o branding differenti.
   - Il tenant **Cliente** viene creato di solito per ciascuna organizzazione che si registra per il servizio.
   - Un nuovo tenant **Unità** viene creato all'interno di un tenant cliente per espandere il servizio a una nuova unità organizzativa.
4. In **Nome**, specificare un nome per il nuovo tenant.
5. [Solo durante la creazione di un tenant partner] Inserire il **Nome società ufficiale (legale)** (obbligatorio) e il **Numero IVA/Codice fiscale/Codice di registrazione dell'azienda** (facoltativo).
6. [Solo durante la creazione di un tenant cliente] In **Modalità**, indicare se il tenant utilizza i servizi in modalità trial o in modalità di produzione. I report mensili sull'uso del servizio non includono i dati sull'utilizzo per i tenant in modalità trial.

   Importante
   Se si passa dalla modalità di prova alla modalità produzione alla metà del mese, l'intero mese verrà incluso nel report mensile sull'utilizzo del servizio. Per questo motivo, si consiglia di cambiare modalità il primo giorno del mese. La modalità viene automaticamente impostata su produzione quando un tenant permane in modalità di prova per un mese intero.
   Vi sono due possibili situazioni nelle quali effettuare automaticamente il passaggio del tenant dalla modalità di prova a quella di produzione:
   - A metà del mese, perché in questo caso anche l'intero mese ***successivo*** viene incluso nel report mensile sull'utilizzo del servizio.
   - [Opzione consigliata] Il primo giorno del mese, perché in questo caso viene conteggiato solo il mese corrente.

7. In **Modalità di gestione**, selezionare una delle modalità seguenti per gestire l'accesso al tenant:
   - **Self-service** - Questa modalità limita l'accesso a questo tenant agli amministratori del tenant padre, che potranno soltanto modificare le proprietà del tenant, ma non potranno accedere o gestire nessun elemento che questo contiene (ad esempio tenant, utenti, servizi, backup e altre risorse).
   - **Gestito dal service provider** - Questa modalità garantisce l'accesso completo al tenant agli amministratori del tenant padre a che potranno modificare le proprietà; gestire tenant, utenti e servizi; accedere ai backup e ad altre risorse.

   Solo l'amministratore del tenant creato dall'utente potrà modificare la modalità di gestione se questa è configurata come **Self-service**. Per farlo, l'amministratore del tenant creato deve aprire la scheda **Impostazioni** > **Sicurezza** e configurare l'opzione **Accesso al supporto**.
   Per verificare la modalità di gestione selezionata per i tenant figlio, aprire la scheda **Clienti**.

8. In **Sicurezza**, abilitare o disabilitare l'autenticazione a due fattori per il tenant.
   Se l'opzione è abilitata, tutti gli utenti del tenant sono tenuti a configurare l'autenticazione a due fattori per i propri account, per un accesso più sicuro. Gli utenti devono installare l'applicazione di autenticazione nei propri dispositivi di secondo fattore; per accedere alla console, dovranno utilizzare il codice TOTP temporaneo generato e le credenziali tradizionali (login e password). Per ulteriori informazioni, consultare "Configurazione dell'autenticazione a due fattori". Per visualizzare lo stato dell'autenticazione a due fattori per i clienti, passare a **Clienti**.
9. [Solo durante la creazione di un tenant cliente in modalità Sicurezza avanzata] In **Sicurezza**, selezionare la casella di controllo **Modalità Sicurezza avanzata**.
   Questa modalità consente solo i backup crittografati La password di crittografia deve essere impostata sul dispositivo protetto; senza password, la creazione dei backup non avrà esito positivo. Non sono disponibili le operazioni che richiedono la fornitura di una password di crittografia a un servizio cloud. Per ulteriori informazioni, fare riferimento a "Modalità Sicurezza avanzata" (pag. 37).

   Importante
   Non è possibile disabilitare la modalità Sicurezza avanzata dopo la creazione del tenant.

10. In **Crea amministratore**, configurare un account amministratore.

    Nota
    La creazione di un amministratore è obbligatoria per i tenant cliente e per i tenant partner la cui **Modalità di gestione** è impostata su **Self-service**.

    a. Inserire un nome di accesso e l'e-mail dell'account dell'amministratore. I campi rimanenti sono facoltativi, ma è bene fornire più canali di comunicazione nel caso sia necessario contattare l'amministratore.
    b. Selezionare la lingua.
       Se non viene selezionata alcuna lingua, viene utilizzata la lingua inglese per impostazione predefinita.
    c. Specificare i contatti aziendali.
       - **Fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.
       - **Tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.
       - **Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.
         È possibile assegnare più di un contatto aziendale a un utente.
11. In **Lingua**, modificare la lingua predefinita che verrà utilizzata da questo tenant per le notifiche, i report e il software.
12. Eseguire una delle seguenti operazioni:
    - Per completare la creazione del tenant, fare clic su **Salva e chiudi**. In questo caso tutti i servizi verranno attivati per il tenant. La modalità di fatturazione del servizio Protezione verrà

impostata per workload.

- Per selezionare i servizi per il tenant, fare clic su **Avanti**. Vedere "Selezione dei servizi per un tenant" (pag. 38).

Modalità Sicurezza avanzata

La modalità Sicurezza avanzata offre impostazioni speciali ai clienti con esigenze di sicurezza aumentate. Tale modalità richiede la crittografia obbligatoria di tutti i backup e consente soltanto l'uso di password di crittografia impostate a livello locale.

Un amministratore di partner può abilitare la modalità Sicurezza avanzata solo durante la creazione di un nuovo tenant cliente, e non può disabilitare questa modalità in un secondo momento. Non è possibile abilitare la modalità Sicurezza avanzata per tenant già esistenti.

Nella modalità Sicurezza avanzata, tutti i backup creati in un tenant cliente e nelle rispettive unità vengono crittografati automaticamente con l'algoritmo AES e la chiave a 256 bit. Gli utenti possono impostare le proprie password di crittografia soltanto nei dispositivi protetti, e non possono impostarle nei piani di protezione.

I servizi cloud non possono accedere alle password di crittografia. A causa di questa limitazione, le funzionalità seguenti non sono disponibili ai tenant in modalità Sicurezza avanzata.

- Ripristino mediante la console del servizio
- Esplorazione dei backup a livello di file mediante la console del servizio
- Backup da cloud a cloud
- Backup di siti web
- Backup applicazione
- Backup di dispositivi mobili
- Scansione anti-malware dei backup
- Ripristino sicuro
- Creazione automatica di whitelist aziendali
- Mappa di protezione dati
- Disaster recovery
- Report e dashboard correlati alle funzionalità non disponibili

Limitazioni

- La modalità Sicurezza avanzata è compatibile solo con gli agenti la cui versione è 15.0.26390 o superiore.
- La modalità Sicurezza avanzata non è disponibile per i dispositivi che eseguono Red Hat Enterprise Linux 4.x o 5.x, e i loro derivati.

Selezione dei servizi per un tenant

Per impostazione predefinita, quando si crea un nuovo tenant tutti i servizi vengono abilitati. È possibile selezionare quali servizi saranno disponibili agli utenti del tenant e dei tenant figlio.

È inoltre possibile selezionare e abilitare i servizi per più tenant esistenti. Per ulteriori informazioni, consultare "Abilitazione dei servizi per più tenant esistenti" (pag. 39).

Questa procedura non è applicabile a un tenant unità.

Per selezionare i servizi per un tenant

1. Nella sezione **Seleziona servizi** della finestra di dialogo di creazione/modifica del tenant, selezionare una modalità di fatturazione o un'edizione.
   - Selezionare la modalità di fatturazione **Per workload** o **Per gigabyte**, quindi deselezionare le caselle di controllo corrispondenti ai servizi da disabilitare per il tenant.
     L'insieme di servizi è identico per entrambe le modalità di fatturazione.

     Per Advanced Disaster Recovery, se nell'account dell'utente è stata registrata una posizione di disaster recovery proprietaria, sarà possibile sceglierla dall'elenco a discesa.
   - Per utilizzare un'edizione legacy, selezionare il pulsante di opzione **Edizioni Legacy** e selezionare un'edizione dall'elenco a discesa.

   I servizi disabilitati non saranno visibili agli utenti del tenant e dei tenant figlio.
2. Eseguire una delle seguenti operazioni:
   - Per completare la creazione del tenant, fare clic su **Salva e chiudi**. In questo caso, tutti gli elementi dell'offerta per i servizi selezionati verranno attivati per il tenant, senza limiti di quota.
   - Per configurare gli elementi dell'offerta per il tenant, fare clic su **Avanti**. Vedere "Configurazione degli elementi dell'offerta per un tenant" (pag. 38).

Configurazione degli elementi dell'offerta per un tenant

Quando si crea un nuovo tenant, vengono abilitati tutti gli elementi dell'offerta dei servizi selezionati. È possibile selezionare quali elementi dell'offerta saranno disponibili agli utenti del tenant e dei tenant figlio, e impostarne le relative quote.

Questa procedura non è applicabile a un tenant unità.

Per configurare gli elementi dell'offerta per un tenant

1. Nella sezione **Configura servizi** della finestra di dialogo per la creazione/modifica del tenant, in ogni scheda del servizio deselezionare le caselle di controllo corrispondenti agli elementi dell'offerta da disabilitare.
   La funzionalità che corrisponde agli elementi dell'offerta disabilitati non sarà disponibile agli utenti del tenant e dei tenant figlio.

Nota
È possibile disabilitare elementi dell'offerta correlati alla funzionalità di protezione avanzata, ma questi verranno automaticamente riabilitati quando un utente attiva una funzionalità avanzata inclusa in un piano di protezione.

2. Alcuni servizi consentono di selezionare gli archivi che saranno disponibili al nuovo tenant. Gli archivi sono raggruppati per posizioni. È possibile selezionarli dall'elenco di posizioni e archivi disponibili per i tenant dell'utente.
   - Durante la creazione di un tenant partner/cartella, è possibile selezionare più posizioni e archivi per ciascun servizio.
   - Durante la creazione di un tenant cliente, è necessario selezionare una posizione e quindi un archivio per servizio in tale posizione. Gli archivi assegnati al cliente possono essere modificati successivamente, ma solo se il loro utilizzo è pari a 0 GB, ovvero prima che il cliente inizi a utilizzare l'archivio o dopo che il cliente ha rimosso tutti i backup da questo storage. Le informazioni relative all'utilizzo dello spazio di archiviazione non sono aggiornate in tempo reale. Per l'aggiornamento delle informazioni possono essere necessarie fino a 24 ore.

   Per informazioni sugli archivi, fare riferimento a "Gestione di posizioni e archivi".
3. Per specificare la quota per un elemento, fare clic sul link **Illimitata** accanto all'elemento dell'offerta.
   Le suddette quote sono "flessibili". Il superamento di uno qualsiasi di questi valori causa l'invio di una notifica e-mail agli amministratori del tenant e agli amministratori del tenant parent. Non vengono applicati limiti relativi all'utilizzo dei servizi. Per un tenant partner si prevede che l'utilizzo degli elementi dell'offerta possa eccedere il surplus della quota perché non è possibile impostare il surplus durante la creazione del tenant partner.
4. [Facoltativo, solo durante la creazione di un tenant cliente] Specificare il surplus della quota.
   Il surplus della quota consente a un tenant cliente di superare la quota del valore specificato. Quando si supera il surplus della quota, vengono applicati i limiti relativi all'uso del servizio corrispondente.
5. Fare clic su **Salva e chiudi**.

Il tenant appena creato viene visualizzato nella scheda **Clienti** della console di gestione.

Per modificare le impostazioni del tenant o cambiare l'amministratore, selezionare il tenant nella scheda **Clienti**, quindi fare clic sull'icona a forma di matita nella sezione che si desidera modificare.

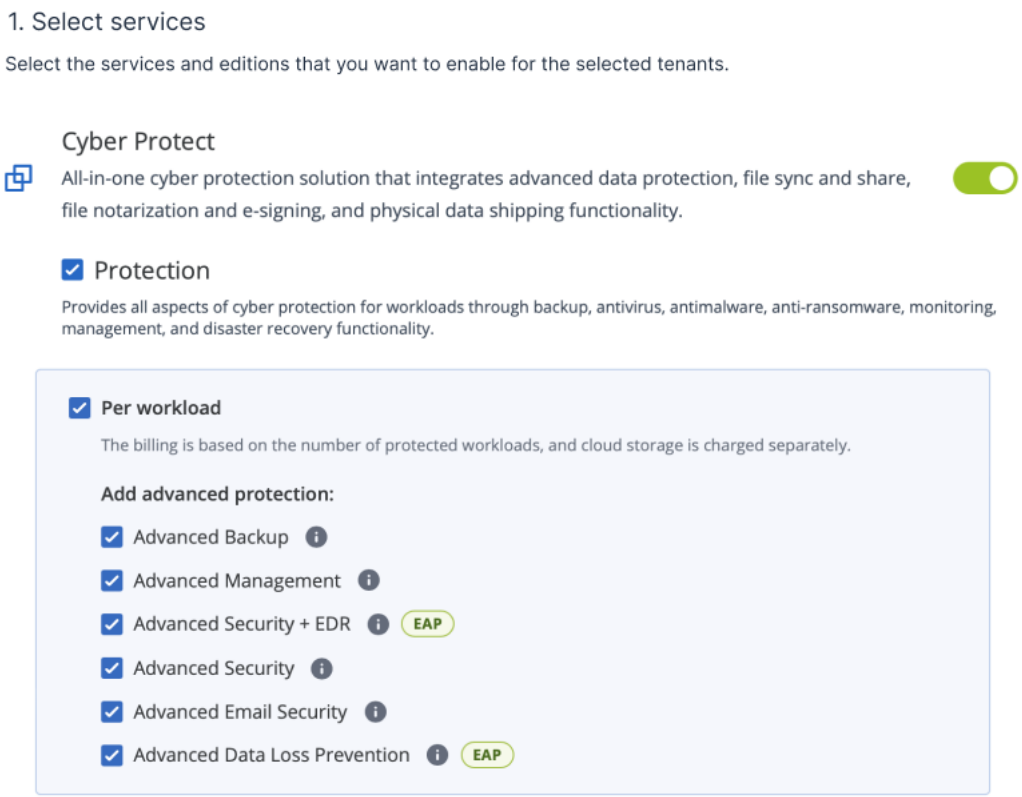
Abilitazione dei servizi per più tenant esistenti

È possibile abilitare in blocco servizi, edizioni, pacchetti ed elementi in offerta per più tenant (fino a un massimo di 100 tenant in una sessione).

Questa procedura è applicabile a tenant radice secondaria, partner, cartella e cliente. È possibile selezionare simultaneamente anche tenant di tipo diverso.

Per abilitare i servizi per più tenant

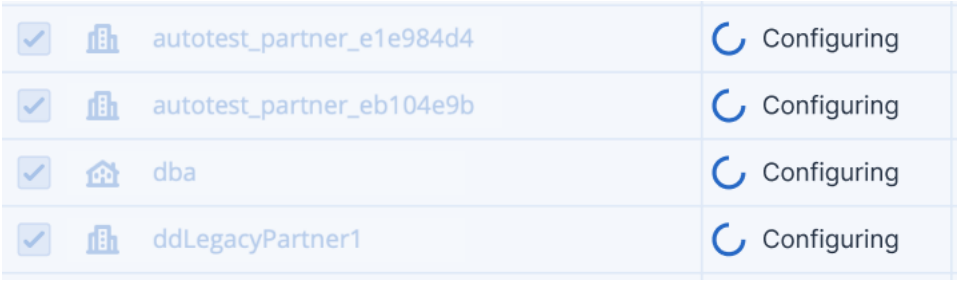
1. Nel portale di gestione, andare a **Clienti**.
2. Nell'angolo in alto a destra, fare clic su **Configura servizi**.
3. Selezionare ogni tenant per il quale abilitare i servizi attivando la casella di controllo accanto al nome del tenant, quindi fare clic su **Avanti**.
4. Nella sezione **Seleziona servizi**, selezionare i servizi pertinenti da applicare a tutti i tenant selezionati, quindi fare clic su **Avanti**.



Nota
In questa schermata non è possibile disabilitare un servizio abilitato in precedenza. Tutti i servizi, le edizioni e gli elementi in offerta selezionati prima di questa procedura resteranno abilitati.

5. Nella sezione **Configura servizi**, selezionare le funzionalità dei servizi e gli elementi in offerta da abilitare per i tenant selezionati, quindi fare clic su **Avanti**.
6. Nella sezione **Riepilogo**, rivedere le modifiche che verranno applicate ai tenant selezionati.

   Fare clic su **Espandi tutto** per visualizzare tutti i servizi e gli elementi in offerta selezionati che verranno applicati. In alternativa, espandere ogni tenant per visualizzare i servizi e gli elementi in offerta selezionati specificamente per il tenant.
7. Fare clic su **Applica modifiche**. Durante la configurazione dei servizi di ciascun tenant, il tenant è disabilitato e la colonna **Stato tenant** indica i servizi e gli elementi in offerta in corso di configurazione, come indicato di seguito.



8. Una volta applicata correttamente la configurazione dei servizi e degli elementi in offerta ai tenant selezionati, viene visualizzato un messaggio di conferma.
   Se per qualsiasi motivo non è stato possibile applicare i servizi e gli elementi in offerta a un tenant, nella colonna **Stato tenant** viene visualizzato lo stato **Non applicato**. Fare clic su **Riprova** per rivedere la configurazione dei tenant selezionati.

Abilitazione delle Notifiche sulla manutenzione

Gli utenti Partner possono consentire ai tenant figlio (partner e clienti) di ricevere le notifiche e-mail sulla manutenzione direttamente dal data center di Cyber Protect, e di ricevere notifiche sulla manutenzione nel prodotto nel portale di gestione. Ciò aiuta a ridurre il numero di chiamate relative alla manutenzione effettuate al supporto.

Nota
Le e-mail di notifica sulla manutenzione riportano il brand del data center. Il branding personalizzato non è supportato per queste notifiche.

Per abilitare le notifiche sulla manutenzione per partner o clienti figlio

1. Accedere al portale di gestione come utente Partner, fare clic su **Clienti**, quindi sul nome di un tenant partner o cliente per il quale abilitare le notifiche di manutenzione.
2. Fare clic su **Configura**.
3. Nella scheda **Impostazioni generali**, individuare e abilitare l'opzione **Notifiche sulla manutenzione**.
   Se l'opzione **Notifiche sulla manutenzione** non è visibile, contattare il service provider.

Nota
Le notifiche sulla manutenzione sono abilitate, ma non vengono inviate fino a quando il tenant selezionato non le abilita per i propri utenti o non propaga ulteriormente questa opzione ai partner o ai clienti figlio per abilitare le notifiche ai rispettivi utenti.

Per abilitare le notifiche sulla manutenzione per un utente

1. Accedere al portale di gestione come Utente partner o Amministratore aziendale.
   Un Partner può accedere agli utenti di tutti i tenant che gestisce.
2. Passare a **Gestione azienda** > **utenti**, quindi fare clic sul nome dell'utente per il quale abilitare le notifiche di manutenzione.

3. Nella scheda **Servizi**, nella sezione **Impostazioni**, fare clic sulla matita per modificare le opzioni.
4. Selezionare la casella di controllo **Notifiche sulla manutenzione** e fare clic su **Fatto**.

L'utente selezionato riceverà le notifiche sulle imminenti attività di manutenzione previste nel data center.

Configurazione del profilo cliente autogestito

I Partner possono configurare i profili dei clienti autogestiti per i tenant che gestiscono. Questa opzione consente di controllare la visibilità del profilo dei tenant e le informazioni di contatto per ogni cliente.

Per configurare il profilo cliente autogestito

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il cliente di cui configurare il profilo cliente autogestito.
3. Selezionare la scheda **Configurazione**, quindi la scheda **Impostazioni generali**.
4. Abilitare o disabilitare l'opzione **Abilita profilo cliente autogestito**.

Se il profilo cliente autogestito è abilitato, questo cliente visualizzerà la sezione **Profilo azienda** nel menu di navigazione e i campi relativi al contatto nella procedura guidata di creazione dell'utente (**Telefono aziendale**, **Contatto aziendale** e **Posizione professionale**).

Se il profilo cliente autogestito è disabilitato, la sezione **Profilo azienda** nel menu di navigazione e i campi relativi al contatto nella procedura guidata di creazione dell'utente saranno nascosti.

Configurazione dei contatti aziendali

I Partner possono configurare le informazioni di contatto per l'azienda e per i tenant che gestiscono. Ai contatti di questo elenco verranno inviati gli aggiornamenti sulle nuove funzionalità e altre importanti modifiche apportate alla piattaforma.

È possibile aggiungere più contatti e assegnare contatti aziendali, in funzione del ruolo utente. È possibile creare contatti dagli utenti presenti nella piattaforma Cyber Protect o aggiungere le informazioni di contatto di persone che non hanno accesso al servizio.

Per configurare i contatti per l'azienda

1. Nella console di gestione, passare a **Gestione azienda** > **Profilo azienda**.
2. Nella sezione **Contatti**, fare clic su **+**.
3. Selezionare un'opzione per creare il contatto.
   - **Crea da utente esistente**
     - Selezionare un utente dall'elenco a discesa.
     - Selezionare un contatto aziendale.
       - **Fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.

        - **Tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.
        - **Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.

          È possibile assegnare più di un contatto aziendale a un utente.

        Se si elimina un contatto associato a un utente dall'elenco dei contatti nel profilo dell'azienda, l'utente non verrà eliminato. Il sistema annullerà l'assegnazione di tutti i contatti aziendali dell'utente, che non verranno più visualizzati nella colonna **Contatti aziendali** dell'elenco **Utenti**.

        Se si modifica l'indirizzo e-mail del contatto associato all'utente, il sistema chiede di verificare il nuovo indirizzo indicato. Viene inviato un messaggio e-mail a tale indirizzo e l'utente che lo riceve deve confermare la modifica.
- **Crea nuovo contatto**
  - Fornire le informazioni di contatto.
    - **Nome** - Nome del contatto. Campo obbligatorio.
    - **Cognome** - Cognome del contatto. Campo obbligatorio.
    - **Indirizzo e-mail aziendale** - Indirizzo e-mail aziendale del contatto. Campo obbligatorio.
    - **Telefono aziendale** - Campo facoltativo.
    - **Posizione professionale** - Campo facoltativo.
  - Selezionare la scheda **Contatti aziendali**.
    - **Fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.
    - **Tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.
    - **Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.

      È possibile assegnare più di un contatto aziendale a un utente.
4. Fare clic su **Aggiungi**.

Per configurare i contatti per un tenant

Nota
Se si modificano le informazioni di contatto per un tenant figlio, le modifiche saranno visibili nel tenant.

1. Nel portale di gestione, andare a **Clienti**.
2. Fare clic sul tenant, quindi su **Configura**.
3. Nella sezione **Contatti**, fare clic su **+**.
4. Selezionare un'opzione per creare il contatto.

- **Crea da utente esistente**
  - Selezionare un utente dall'elenco a discesa.
  - Selezionare un contatto aziendale.
    - **Fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.
    - **Tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.
    - **Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.

      È possibile assegnare più di un contatto aziendale a un utente.

    Se si elimina un contatto associato a un utente dall'elenco dei contatti nel profilo dell'azienda, l'utente non verrà eliminato. Il sistema annullerà l'assegnazione di tutti i contatti aziendali dell'utente, che non verranno più visualizzati nella colonna **Contatti aziendali** dell'elenco **Utenti**.

    Se si modifica l'indirizzo e-mail del contatto associato all'utente, il sistema chiede di verificare il nuovo indirizzo indicato. Viene inviato un messaggio e-mail a tale indirizzo e l'utente che lo riceve deve confermare la modifica.
- **Crea nuovo contatto**
  - Fornire le informazioni di contatto.
    - **Nome** - Nome del contatto. Campo obbligatorio.
    - **Cognome** - Cognome del contatto. Campo obbligatorio.
    - **Indirizzo e-mail aziendale** - Indirizzo e-mail aziendale del contatto. Campo obbligatorio.
    - **Telefono aziendale** - Campo facoltativo.
    - **Posizione professionale** - Campo facoltativo.
  - Selezionare la scheda **Contatti aziendali**.
    - **Fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.
    - **Tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.
    - **Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.

      È possibile assegnare più di un contatto aziendale a un utente.
5. Fare clic su **Aggiungi**.

Aggiornamento dei dati di utilizzo per un tenant

Per impostazione predefinita, i dati di utilizzo vengono aggiornati a intervalli prestabiliti. È possibile aggiornare i dati di utilizzo di un tenant manualmente.

1. Nella console di gestione, passare a **Clienti**.
2. Fare clic sul tenant, quindi sui puntini di sospensione nella riga del tenant.

3. Selezionare **Aggiorna utilizzo**.

   Nota
   Il recupero dei dati può richiedere fino a 10 minuti.

4. Ricaricare la pagina per visualizzare i dati aggiornati.

Disabilitazione e abilitazione di un tenant

Potrebbe rendersi necessaria la disabilitazione temporanea di un tenant. Un esempio è il caso di un tenant con debiti per l'uso dei servizi.

Come disabilitare un tenant

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il tenant da disabilitare, quindi fare clic sull'icona dei puntini di sospensione > **Disabilita**.
3. Confermare l'operazione facendo clic su **Disabilita**.

Di conseguenza:

- Il tenant e tutti i suoi tenant secondari verranno disabilitati e i relativi servizi verranno interrotti.
- La fatturazione nei confronti del tenant e dei suoi tenant secondari proseguirà, poiché i loro dati verranno preservati e archiviati su Cyber Protect Cloud.
- Tutti i client API nell'ambito del tenant e dei relativi tenant secondari verranno disabilitati e tutte le integrazioni che utilizzano tali client verranno disattivate.

Per abilitare un tenant, selezionarlo dall'elenco e fare clic sull'icona dei puntini di sospensione > **Abilita**.

Spostamento di un tenant in un altro tenant

Il portale di gestione consente di spostare un tenant da un tenant parent a un altro tenant parent. Questa operazione si rivela utile se si desidera trasferire un cliente da un partner a un altro, oppure se è stato creato un tenant cartella per organizzare i clienti e si desidera spostarne alcuni nel nuovo tenant cartella appena creato.

Tipi di tenant che è possibile spostare

Tipo di tenant	Può essere spostato	Tenant di destinazione
Partner	Sì	Partner o Cartella
Cartella	Sì	Partner o Cartella
Cliente	Sì	Partner o Cartella
Unità	No	Nessuno

Requisiti e limitazioni

- È possibile spostare un tenant solo se il tenant padre di destinazione dispone di un set di servizi e di elementi in offerta di dimensioni pari o maggiori rispetto al tenant padre di origine.
- Quando si sposta un tenant cliente, tutti gli archivi assegnati al tenant cliente nel tenant parent di origine devono esistere nel tenant parent di destinazione. Questa limitazione è necessaria poiché non è possibile spostare i dati correlati al servizio del cliente da uno storage a un altro storage.
- Nei tenant cliente gestiti da service provider, possono essere presenti piani che vengono applicati ai workload di clienti dal livello del service provider (ad esempio piani di scripting).

  Quando si sposta questo tipo di tenant cliente, i piani del service provider verranno revocati dai workload del cliente e tutti i servizi associati a tali piani verranno bloccati per questo cliente.
- È possibile spostare i tenant all'interno della gerarchia dell'account partner. È anche possibile spostare alcuni tenant cliente in un tenant di destinazione esterno alla gerarchia dell'account partner. Per capire se l'operazione è possibile, contattare l'account manager di riferimento in .
- Solo gli amministratori (ad esempio, nel portale di gestione o l'amministrazione della società) possono spostare i tenant in tenant padre diversi.

Come spostare un tenant

1. Accedere al portale di gestione.
2. Individuare e copiare l'**ID interno** del partner di destinazione o del tenant cartella nel quale spostare un tenant. Eseguire le seguenti operazioni:
   a. Nella scheda **Clienti**, selezionare il tenant di destinazione nel quale si desidera spostare il tenant.
   b. Nel riquadro delle proprietà del tenant, fare clic sull'icona dei puntini di sospensione in verticale, quindi su **Visualizza ID**.
   c. Copiare la stringa di testo visualizzata nel campo **ID interno** e quindi fare clic su **Annulla**.
3. Selezionare il tenant da spostare, quindi spostarlo nella cartella/partner di destinazione. Eseguire le seguenti operazioni:
   a. Nella scheda **Clienti**, selezionare il tenant da spostare.
   b. Nel riquadro delle proprietà del tenant, fare clic sull'icona dei puntini di sospensione in verticale, e quindi su **Sposta**.
   c. Incollare il codice di identificazione interno del tenant di destinazione e quindi fare clic su **Sposta**.

L'operazione inizia immediatamente e può richiedere fino a 10 minuti.

Se il tenant che si intende spostare dispone di tenant figlio (se, ad esempio, si tratta di un tenant partner o di un tenant cartella con un tenant cliente al suo interno), tutta la sotto struttura del tenant verrà spostata nel tenant di destinazione.

Conversione di un tenant partner in un tenant cartella e viceversa

Il portale di gestione consente di convertire un tenant partner in un tenant cartella.

Questa funzione può rivelarsi utile se si è utilizzato un tenant partner per finalità di raggruppamento e ora si desidera organizzare l'infrastruttura dei tenant in modo più adeguato. Si rivela utile anche per far sì che il pannello di controllo operativo includa informazioni aggregate relative al tenant.

È inoltre possibile convertire un tenant cartella in un tenant partner.

Nota
La conversione è un'operazione sicura che non ha conseguenze sugli utenti inclusi nel tenant né sui dati relativi al servizio.

Per convertire un tenant

1. Accedere al portale di gestione.
2. Nella scheda **Clienti**, selezionare il tenant da convertire.
3. Eseguire una delle seguenti operazioni:
   - Fare clic sull'icona dei puntini di sospensione accanto al nome del tenant.
   - Selezionare il tenant, quindi fare clic sull'icona dei puntini di sospensione nel riquadro delle proprietà del tenant.
4. Fare clic su **Converti in cartella** o **Converti in partner**.
5. Confermare la propria decisione.

Limitazione dell'accesso al tenant

Gli amministratori a livello cliente e superiore possono limitare l'accesso ai propri tenant per gli amministratori di livello superiore.

Se l'accesso al tenant è limitato, gli amministratori dei tenant parent possono solo modificare le proprietà del tenant. Non saranno in grado di vedere gli account e i tenant figlio.

Per impedire agli amministratori di livello superiore di accedere al tenant dell'utente

1. Accedere al portale di gestione.
2. Passare a **Impostazioni** > **Sicurezza**.
3. Disabilitare l'interruttore **Accesso al supporto**.

Gli amministratori dei tenant padre avranno accesso limitato al tenant. Potranno soltanto modificare le proprietà del tenant, ma non potranno accedere o gestire nessun elemento che questo contiene (ad esempio tenant, utenti, servizi, backup e altre risorse).

Se è abilitata l'opzione **Accesso al supporto**, gli amministratori dei tenant padre avranno accesso completo al tenant. Potranno quindi effettuare le operazioni seguenti: modifica delle proprietà; gestione di tenant, utenti e servizi; accesso ai backup e altre risorse.

Eliminazione di un tenant

Potrebbe essere necessario eliminare un tenant per liberare le risorse che utilizza. Le statistiche di utilizzo verranno aggiornate entro un giorno dall'eliminazione. L'eliminazione di tenant di grandi dimensioni potrebbe richiedere più tempo.

Prima di eliminare un tenant, è necessario disabilitarlo. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Disabilitazione e abilitazione di un tenant".

Importante
L'eliminazione di un tenant è un processo irreversibile!

Per eliminare un tenant

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il tenant disabilitato da eliminare, quindi fare clic sull'icona dei puntini di sospensione > **Elimina**.
3. Per confermare l'azione, immettere il login e fare clic su **Elimina**.

Di conseguenza:

- Il tenant e i relativi tenant secondari verranno eliminati.
- Tutti i servizi abilitati nel tenant e nei relativi tenant secondari verranno arrestati.
- Tutti gli utenti in questo tenant e nei relativi tenant secondari verranno eliminati.
- Verrà annullata la registrazione di tutti i sistemi in questo tenant e nei relativi tenant secondari.
- Tutti i dati relativi al servizio (ad esempio backup, file sincronizzati) del tenant e dei relativi tenant secondari verranno eliminati.
- Tutti i client API nell'ambito del tenant e dei relativi tenant secondari verranno eliminati e tutte le integrazioni che utilizzano tali client verranno disattivate.

Gestione degli utenti

Gli amministratori del partner, dei clienti e delle unità possono configurare e gestire gli account utente nei tenant a loro accessibili.

Creazione di un account utente

È possibile creare account aggiuntivi nei casi seguenti:

- Account amministratore partner/cartella — per condividere le attività di gestione dei servizi con altre persone.

- Account amministratore cliente/potenziale cliente/unità — per delegare la gestione del servizio ad altre persone le cui autorizzazioni di accesso saranno strettamente limitate al cliente, al potenziale cliente o all'unità corrispondente.
- Account utente nel cliente o in un tenant unità — per consentire agli utenti di accedere esclusivamente a un sottoinsieme dei servizi.

Tenere presente che non è possibile trasferire gli account esistenti da un tenant a un altro. È quindi necessario innanzitutto creare un tenant che verrà poi popolato con gli account.

Per creare un account utente

1. Accedere al portale di gestione.
2. Passare al tenant nel quale si desidera creare un account utente. Vedere "Navigazione nel portale di gestione" (pag. 27).
3. Nell'angolo in alto a destra fare clic su **Nuovo** > **Utente**.
   In alternativa, passare a **Gestione azienda > Utenti** e fare clic su **Nuovo**.
4. Specificare le seguenti informazioni di contatto per l'account:
   - **Accedi**

     Importante
     Ciascun account deve disporre di un unico login

   - **E-mail**

     Importante
     Se l'utente è registrato nel servizio File Sync & Share, fornire l'e-mail che è stata utilizzata per la registrazione di File Sync & Share.
     Tenere presente che ciascun account utente del cliente deve disporre di un indirizzo e-mail esclusivo.

   - **Nome**
   - **Cognome**
   - [Facoltativo] **Telefono aziendale**

     Nota
     I campi come **Telefono aziendale**, **Posizione professionale** e **Contatto aziendale** vengono visualizzati nella procedura guidata di creazione dell'utente solo se il partner padre ha abilitato l'opzione **Abilita profilo cliente autogestito** per il tenant cliente. Altrimenti, questi campi non vengono visualizzati.

   - [Facoltativo] **Posizione professionale**
   - In **Lingua**, modificare la lingua predefinita che verrà utilizzata per questo account per le notifiche, i report e il software.

5. [Facoltativo] Selezionare i contatti aziendali.
   - **Fatturazione**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative ai report sull'utilizzo.
   - **Tecnico**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative agli aspetti tecnici.
   - **Business**. Questo contatto riceverà aggiornamenti sulle modifiche apportate alla piattaforma e relative all'azienda.

     È possibile assegnare più di un contatto aziendale a un utente.

   È possibile visualizzare i contatti aziendali assegnati a un utente nell'elenco **Utenti**, nella colonna **Contatti aziendali**, e modificare l'account utente per cambiare i tipi di contatto se necessario.
6. [Opzione non disponibile quando si crea un account in un tenant partner/cartella] Selezionare i servizi ai quali l'utente potrà accedere e i ruoli in ciascun servizio.

   I servizi disponibili dipendono dai servizi abilitati per il tenant nel quale viene creato l'account utente.
   - Se la casella di controllo **Amministratore società** è selezionata, l'utente potrà accedere al portale di gestione e al ruolo di amministratore in tutti i servizi attualmente abilitati per il tenant. L'utente potrà accedere anche al ruolo di amministratore in tutti i servizi che verranno abilitati per il tenant in futuro.
   - Se la casella di controllo **Amministratore unità** è selezionata, l'utente potrà accedere al portale di gestione, ma potrà disporre o meno del ruolo di amministratore del servizio, a seconda del servizio.
   - Altrimenti, l'utente potrà disporre dei ruoli selezionati nei servizi selezionati.
7. Fare clic su **Crea**.

L'account utente appena creato viene visualizzato nella scheda **Utenti** in **Gestione azienda**.

Per modificare le impostazioni dell'utente o specificare le impostazioni di notifica e le quote per l'utente (non disponibile per amministratori di partner/cartelle), selezionare l'utente nella scheda **Utenti**, quindi fare clic sull'icona a forma di matita nella sezione che si desidera modificare.

Per reimpostare la password di un utente

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Selezionare l'utente di cui si desidera reimpostare la password, quindi fare clic sull'icona dei puntini di sospensione > **Reimposta password**.
3. Confermare l'operazione facendo clic su **Reimposta**.

L'utente può completare il processo di reimpostazione seguendo le istruzioni nell'e-mail ricevuta.

Per i servizi che non supportano l'autenticazione a due fattori (ad esempio la registrazione a Cyber Infrastructure), potrebbe essere necessario convertire un account utente in un *Account di servizio*, ovvero un account che non richiede l'autenticazione a due fattori.

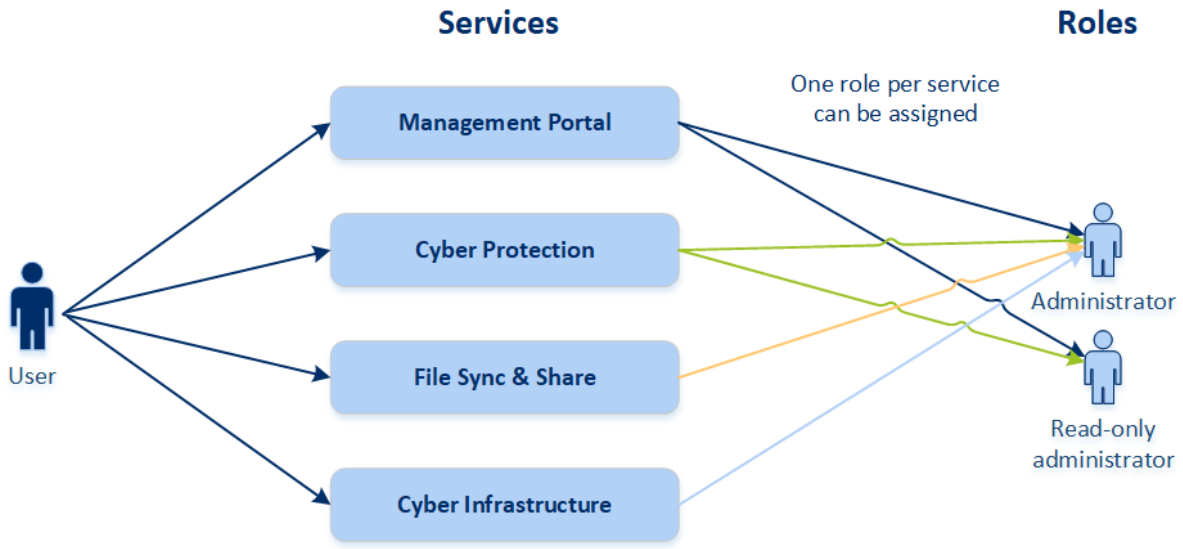
Per convertire un account utente nel tipo di account di servizio

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Selezionare l'utente il cui account si desidera convertire nel tipo di account di servizio, quindi fare clic sull'icona dei puntini di sospensione > **Contrassegna come account di servizio**.
3. Nella finestra di conferma, immettere il codice di autenticazione a due fattori e confermare l'azione.

Ora l'account può essere utilizzato per i servizi che non supportano l'autenticazione a due fattori.

Ruoli utente disponibili per ogni servizio

Un utente può disporre di diversi ruoli, ma di un solo ruolo per ogni servizio.



Per ogni servizio è possibile definire quale ruolo verrà assegnato a un utente.

Servizio	Ruolo	Descrizione
n/d	Amministratore società	Questo ruolo concede diritti di amministratore completi per tutti i servizi. Questo ruolo consente l'accesso alla whitelist aziendale. Se per l'azienda è abilitato l'add-on Disaster Recovery del servizio Cyber Protection, questo ruolo consente anche l'accesso alla funzionalità Disaster Recovery.
Portale di gestione	Amministratore	Questo ruolo consente l'accesso al portale di gestione dal quale l'amministratore può gestire gli utenti dell'intera organizzazione.
	Amministratore di sola lettura Livello del partner	Questo ruolo consente l'accesso di sola lettura a tutti gli oggetti nel portale di gestione del partner e nel portale di gestione di tutti i clienti di questo partner. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura.

	Amministratore di sola lettura Livello del cliente	Questo ruolo consente l'accesso di sola lettura a tutti gli oggetti nel portale di gestione dell'intera azienda. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura.
	Amministratore di sola lettura Livello dell'unità	Questo ruolo consente l'accesso di sola lettura a tutti gli oggetti nel portale di gestione dell'unità e delle sotto unità dell'azienda. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura.
Cyber Protection	Amministratore Cyber	Oltre ai diritti del ruolo Amministratore, questo ruolo consente la configurazione e la gestione del servizio Cyber Protection e l'approvazione delle azioni in Cyber Scripting. Il ruolo di Amministratore Cyber è disponibile solo nei tenant in cui è abilitato il pacchetto Advanced Management.
	Amministratore	Questo ruolo consente la configurazione e la gestione di Cyber Protection per i clienti. Il ruolo è necessario per configurare e gestire la funzionalità Disaster Recovery e la whitelist aziendale.
	Amministratore di sola lettura	Il ruolo consente l'accesso di sola lettura a tutti gli oggetti del servizio Cyber Protection. Gli utenti con questo ruolo possono accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura. L'amministratore di sola lettura non può configurare né gestire la funzionalità Disaster Recovery o la whitelist aziendale.
	Ripristina operatore	Il ruolo consente di accedere ai backup delle organizzazioni Microsoft 365 e Google Workspace e ne permette il ripristino, limitando l'accesso ai contenuti riservati.
File Sync & Share	Amministratore	Questo ruolo consente la configurazione e la gestione di File Sync & Share per gli utenti.
Cyber Infrastructure	Amministratore	Questo ruolo consente la configurazione e la gestione di Cyber Infrastructure per gli utenti.

Ruolo Amministratore di sola lettura

Un account con questo ruolo dispone dell'accesso di sola lettura alla console web di Cyber Protection ed è in grado di:

- Acquisire dati di diagnostica, come i report di sistema.
- Visualizzare i punti di ripristino di un backup; non può invece esplorare i dettagli del contenuto di backup e non può visualizzare file, cartelle o messaggi e-mail.

Un amministratore di sola lettura non può:

- Avviare o arrestare attività.

  Ad esempio, un amministratore di sola lettura non può avviare un ripristino o arrestare un backup in esecuzione.
- Accedere al file system su sistemi di origine o destinazione.

  Ad esempio, un amministratore di sola lettura non può visualizzare file, cartelle o messaggi e-mail di un sistema oggetto di backup.
- Modificare le impostazioni.

  Ad esempio, un amministratore di sola lettura non può creare un piano di protezione o modificarne le impostazioni.
- Creare, aggiornare o eliminare dati.

  Ad esempio, un amministratore di sola lettura non può eliminare i backup.

Tutti gli elementi dell'interfaccia utente che non sono accessibili a un amministratore di sola lettura sono nascosti, ad eccezione delle impostazioni predefinite del piano di protezione. Queste impostazioni sono visibili, ma il pulsante **Salva** non è attivo.

Qualsiasi modifica relativa agli account e ai ruoli viene visualizzata nella scheda **Attività** con le informazioni seguenti:

- Elementi modificati
- Esecutore delle modifiche
- Data e ora di esecuzione delle modifiche

Ruolo di operatore di ripristino

Questo ruolo è disponibile solo nel servizio Cyber Protection ed è limitato ai backup di Microsoft 365 e Google Workspace.

Un operatore di ripristino può eseguire le seguenti operazioni:

- Visualizzare avvisi e attività.
- Scorrere e aggiornare l'elenco dei backup.
- Sfogliare i backup senza accedere al loro contenuto. L'operatore di ripristino può visualizzare i nomi dei file e gli oggetti e i mittenti delle e-mail di cui è stato eseguito il backup.
- Ricerca nei backup (non è supportata la ricerca full text).
- Ripristino di backup cloud-to-cloud nella posizione originale nell'organizzazione Microsoft 365 o Google Workspace di origine.

Un operatore di ripristino non può eseguire le seguenti operazioni:

- Eliminare avvisi.
- Aggiungere o eliminare organizzazioni Microsoft 365 o Google Workspace.
- Aggiungere, eliminare o rinominare posizioni di backup.
- Eliminare o rinominare i backup.

- Creare, eliminare o rinominare le cartelle quando si ripristina un backup in una posizione personalizzata.
- Applicare un piano di backup o eseguire un backup.
- Accedere ai file o al contenuto delle e-mail di cui è stato eseguito il backup.
- Eseguire il download di file di cui è stato eseguito il backup o di allegati e-mail.
- Inviare come e-mail risorse cloud di cui è stato eseguito il backup, come e-mail o elementi del calendario.
- Visualizzare o ripristinare le conversazioni di Microsoft 365 Teams.
- Ripristino di backup cloud-to-cloud su posizioni non originali quali una casella di posta differente, OneDrive, Google Drive o Microsoft 365 Team.

Ruoli utente e diritti di Cyber Scripting

Le azioni disponibili con gli script e i piani di scripting dipendono dallo stato dello script e dal ruolo dell'utente.

Gli amministratori possono gestire oggetti nei propri tenant e nei rispettivi tenant figlio. Non possono visualizzare o accedere agli oggetti a un livello di amministrazione superiore, se presente.

Gli amministratori di livello più basso possono accedere esclusivamente in sola lettura ai piani di scripting applicati ai propri workload da un amministratore di livello superiore.

I ruoli seguenti forniscono diritti per Cyber Scripting:

- Amministratore società

  Questo ruolo concede diritti di amministratore completi per tutti i servizi. Per quanto riguarda Cyber Scripting, garantisce gli stessi diritti del ruolo Amministratore Cyber.
- Amministratore Cyber

  Questo ruolo garantisce autorizzazioni complete, inclusa l'autorizzazione degli script che possono essere utilizzati nel tenant e la possibilità di eseguire script con lo stato **Prova in corso**.
- Amministratore

  Questo ruolo garantisce autorizzazioni parziali, con la possibilità di eseguire script approvati e di creare ed eseguire piani di scripting che utilizzano script approvati.
- Amministratore di sola lettura

  Questo ruolo garantisce autorizzazioni limitate, con la possibilità di visualizzare gli script e i piani di protezione utilizzati nel tenant.
- Utente

  Questo ruolo garantisce autorizzazioni parziali, con la possibilità di eseguire script approvati e di creare ed eseguire piani di scripting che utilizzano script approvati, esclusivamente sul sistema dell'utente.

La tabella seguente riepiloga le azioni disponibili in base allo stato dello script e al ruolo dell'utente.

Ruolo	Oggetto	Stato dello script		
		Bozza	**Prova in corso**	**Approvato**
Amministratore Cyber Amministratore società	Piano di scripting	Modifica (rimozione di una bozza di script da un piano) Elimina Revoca Disabilita Arresta	Crea Modifica Applica Abilita Esegui Elimina Revoca Disabilita Arresta	Crea Modifica Applica Abilita Esegui Elimina Revoca Disabilita Arresta
	Script	Crea Modifica Modifica stato Clona Elimina Annulla esecuzione	Crea Modifica Modifica stato Esegui Clona Elimina Annulla esecuzione	Crea Modifica Modifica stato Esegui Clona Elimina Annulla esecuzione
Amministratore Utente (per i propri workload)	Piano di scripting	Visualizzazione Revoca Disabilita Arresta	Visualizzazione Annulla esecuzione	Crea Modifica Applica Abilita Esegui Elimina Revoca Disabilita Arresta
	Script	Crea Modifica Clona	Visualizzazione Clona Annulla	Esegui Clona Annulla

		Elimina Annulla esecuzione	esecuzione	esecuzione
Amministratore di sola lettura	Piano di scripting	Visualizzazione	Visualizzazione	Visualizzazione
	Script	Visualizzazione	Visualizzazione	Visualizzazione

Modifica delle impostazioni di notifica per un utente

Per modificare le impostazioni di notifica per un utente, passare a **Gestione azienda** > **Utenti**. Selezionare l'utente per il quale configurare le notifiche, quindi fare clic sull'icona a forma di matita nella sezione **Impostazioni**. Le seguenti impostazioni di notifica sono disponibili se il servizio Cyber Protection è stato attivato per il tenant nel quale è stato creato l'utente:

- **Notifiche relative al superamento delle quote** (abilitata per impostazione predefinita)
  Notifiche relative al superamento delle quote.
- **Report di utilizzo pianificati** (abilitata per impostazione predefinita)
  I report di utilizzo che vengono inviati il primo giorno di ogni mese.
- **Notifiche relative al branding dell'URL** (disabilitate per impostazione predefinita)
  Notifiche sull'imminente scadenza del certificato utilizzato per l'URL personalizzato dei servizi Cyber Protect Cloud. Le notifiche vengono inviate a tutti gli amministratori del tenant selezionato 30, 15, 7, 3 e 1 giorno prima della scadenza del certificato.
- **Notifiche di errore**, **Notifiche di attenzione** e **Notifiche di esito positivo** (disabilitate per impostazione predefinita)
  Notifiche relative ai risultati dell'esecuzione dei piani di protezione e ai risultati delle operazioni di ripristino per ogni dispositivo.
- **Riepilogo giornaliero degli avvisi attivi** (abilitata per impostazione predefinita)
  Il riepilogo giornaliero viene generato in base all'elenco degli avvisi attivi presenti nella console del servizio al momento della creazione del riepilogo. Il riepilogo viene generato e inviato una volta al giorno, tra le 10:00 e le 23:59 del fuso UTC. L'orario di generazione e invio del report dipende dal carico di lavoro nel data center. Se non sono presenti avvisi attivi entro tale ora, il riepilogo non viene inviato. Il riepilogo non include informazioni relative agli avvisi passati non più attivi. Se, ad esempio, un utente individua un backup non riuscito ed elimina l'avviso, oppure se un backup viene eseguito di nuovo con esito positivo prima della generazione del riepilogo, l'avviso non sarà più presente nella console e quindi non verrà inserito nel riepilogo.
- **Notifiche di Controllo dispositivo** (disabilitate per impostazione predefinita)
  Notifiche sui tentativi di utilizzo delle porte e dei dispositivi periferici a cui sono associate restrizioni nei piani di protezione con il modulo Controllo dispositivo abilitato.
- **Notifiche relative al ripristino** (disabilitate per impostazione predefinita)

Notifiche relative alle azioni di ripristino delle risorse seguenti: messaggi e-mail e intera casella di posta dell'utente, cartelle pubbliche, OneDrive/GoogleDrive: OneDrive completo e file o cartelle, file di SharePoint, Teams: Canali, intero Team, messaggi e-mail, sito del Team.

Nell'ambito di queste notifiche, le azioni seguenti sono considerate azioni di ripristino: invio come e-mail, download, o avvio di un'operazione di ripristino.

- **Notifiche di Prevenzione della perdita di dati** (disabilitate per impostazione predefinita)
  Notifiche sugli avvisi di Prevenzione della perdita di dati relative all'attività di questo utente sulla rete.
- **Notifiche relative ai problemi di sicurezza** (disabilitate per impostazione predefinita)
  Notifiche relative al malware rilevato durante l'accesso, l'esecuzione e le scansioni su richiesta e ai rilevamenti provenienti dal motore comportamentale e dal motore di filtro degli URL.

  Sono disponibili due opzioni: **Mitigato** e **Non mitigato**. Queste opzioni si riferiscono agli avvisi relativi ai problemi di Endpoint Detection and Response (EDR), agli avvisi EDR dai feed delle minacce e a singoli avvisi (per i workload sui quali non è attivata la funzionalità EDR).

  Simultaneamente alla creazione di un avviso EDR, viene inviata un'e-mail all'utente interessato. Se lo stato della minaccia relativa al problema cambia, viene inviata una nuova e-mail. Le e-mail includono pulsanti di azione che consentono all'utente di visualizzare i dettagli del problema (se è stato mitigato) oppure di indagare e correggere quanto accaduto (se non è stato mitigato).
- **Notifiche relative all'infrastruttura** (disabilitate per impostazione predefinita)
  Notifiche relative all'infrastruttura di Disaster Recovery: quando questa non è disponibile o quando non sono disponibili i tunnel VPN.

Tutte le notifiche vengono inviate all'indirizzo e-mail dell'utente.

Notifiche ricevute in base al ruolo dell'utente

Le notifiche inviate da Cyber Protection dipendono dal ruolo dell'utente.

Tipo di notifica\Ruolo utente	Utente	Amministratore di clienti
Notifiche relative ai propri dispositivi	Sì	Sì
Notifiche relative a tutti i dispositivi dell'organizzazione	n/d	Sì (ad eccezione di **Notifiche relative ai problemi di sicurezza**)
Notifiche relative ai backup di Microsoft 365, Google Workspace e altri backup basati su cloud	n/d	Sì

Tipo di notifica\Ruolo utente	Utente	Amministratori di clienti e unità	Amministratori di partner e cartelle
Notifiche relative ai propri dispositivi	Sì	Sì	n/d*
Notifiche relative a tutti i dispositivi dei tenant figlio	n/d	Sì	Sì
Notifiche relative ai backup di Microsoft 365, Google Workspace e altri backup basati su cloud	n/d	Sì	Sì

* Gli amministratori dei partner non possono registrare i propri dispositivi, ma possono creare i propri account di amministratore dei clienti e utilizzarli per aggiungere i propri dispositivi. Vedere Account utente e tenant.

Disabilitazione e abilitazione di un account utente

Potrebbe essere necessario disabilitare un account utente per limitare temporaneamente il suo accesso alla piattaforma cloud.

Per disabilitare un account utente

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'account utente da disabilitare, quindi fare clic sull'icona dei puntini di sospensione > **Disabilita**.
3. Confermare l'operazione facendo clic su **Disabilita**.

L'utente non sarà in grado di utilizzare la piattaforma cloud né di ricevere alcuna notifica.

Per abilitare un account utente disabilitato, selezionarlo dall'elenco degli utenti e fare clic sull'icona dei puntini di sospensione > **Abilita**.

Eliminazione di un account utente

Potrebbe essere necessario eliminare permanentemente un account utente per liberare le risorse che utilizza, ad esempio spazio di archiviazione o licenza. Le statistiche di utilizzo verranno aggiornate entro un giorno dall'eliminazione. Se l'account contiene più dati, potrebbe richiedere più tempo.

Prima di eliminare un account utente, è necessario disabilitarlo. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Disabilitazione e abilitazione di un account utente".

Importante
L'eliminazione di un account utente è un processo irreversibile!

Per eliminare un account utente

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'account utente disabilitato, quindi fare clic sull'icona dei puntini di sospensione > **Elimina**.
3. Per confermare l'azione, immettere il login e fare clic su **Elimina**.

Di conseguenza:

- Questo account utente verrà eliminato.
- Tutti i dati che appartengono a questo account utente verranno eliminati.

- Verrà annullata la registrazione di tutti i sistemi associati a questo account utente.

Trasferimento della titolarità di un account utente

Potrebbe essere necessario trasferire la titolarità a un account utente se si desidera mantenere l'accesso ai dati di un utente con privilegi limitati.

Importante
Non è possibile riassegnare il contenuto di un account eliminato.

Per trasferire la titolarità di un account utente:

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'account utente di cui si desidera trasferire la titolarità, quindi fare clic sull'icona a forma di matita nella sezione **Informazioni generali**.
3. Sostituire l'e-mail esistente con l'e-mail del futuro proprietario dell'account, quindi fare clic su **Fatto**.
4. Confermare l'operazione facendo clic su **Sì**.
5. Il futuro proprietario dell'account dovrà verificare il proprio indirizzo e-mail seguendo le istruzioni che gli verranno inviate.
6. Selezionare l'account utente di cui si sta trasferendo la titolarità, quindi fare clic sull'icona dei puntini di sospensione > **Ripristina password**.
7. Confermare l'operazione facendo clic su **Reimposta**.
8. Il futuro proprietario dell'account dovrà reimpostare la password seguendo le istruzioni che verranno inviate al suo indirizzo e-mail.

A questo punto il nuovo proprietario potrà accedere all'account.

Configurazione dell'autenticazione a due fattori

L'**autenticazione a due fattori (2FA)** è una tipologia di autenticazione multifattoriale che verifica l'identità di un utente combinando due fattori differenti:

- Un elemento noto all'utente (PIN o password)
- Un elemento a disposizione dell'utente (token)
- Un elemento che consente di riconoscere fisicamente l'utente (biometria)

L'autenticazione a due fattori fornisce una protezione aggiuntiva contro l'accesso non autorizzato all'account.

La piattaforma supporta l'autenticazione **TOTP (Time-based One-Time Password)**. Quando è abilitata l'autenticazione TOTP, per accedere al sistema gli utenti devono immettere la password tradizionale e un codice TOTP temporaneo. In altre parole, l'utente immette la password (il primo fattore) e il codice TOTP (il secondo fattore). Il codice TOTP viene generato dall'applicazione di

autenticazione installata nel dispositivo di secondo fattore dell'utente, in base all'orario attuale e al segreto (codice QR o codice alfanumerico) fornito dalla piattaforma.

Come funziona

1. L'autenticazione a due fattori viene abilitata a livello di organizzazione.
2. Tutti gli utenti dell'organizzazione devono installare l'applicazione di autenticazione sui propri dispositivi di secondo fattore (smartphone, laptop, desktop o tablet). Tale applicazione viene utilizzata per generare codici TOTP temporanei. Sono consigliati gli autenticatori seguenti:
   - Google Authenticator
     Versione app iOS (https://apps.apple.com/app/google-authenticator/id388497605)
     Versione Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     Versione app iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Versione Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Importante
   Gli utenti devono accertarsi che l'orario sul dispositivo nel quale è installata l'applicazione di autenticazione sia impostato in modo corretto e corrisponda all'orario corrente.

3. Gli utenti dell'organizzazione devono accedere nuovamente al sistema.
4. Dopo aver inserito login e password, verrà loro richiesto di configurare l'autenticazione a due fattori per i propri account utente.
5. A tal fine dovranno scansionare il codice QR utilizzando l'applicazione di autenticazione. Se non è possibile scansionare il codice QR potranno utilizzare il segreto TOTP visualizzato al di sotto del codice QR e aggiungerlo manualmente all'applicazione di autenticazione.

   Importante
   È consigliabile salvare queste informazioni stampando il codice QR, annotando il segreto TOTP o utilizzando un'applicazione che consente il backup dei codici in un cloud). Il segreto TOTP è necessario per ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore.

6. Il codice TOTP temporaneo viene generato nell'applicazione di autenticazione. Viene automaticamente rigenerato ogni 30 secondi.
7. Deve essere inserito nella schermata "Configura autenticazione a due fattori" visualizzata dopo aver immesso la password.
8. Viene così configurata l'autenticazione a due fattori per gli utenti.

Quando gli utenti accedono al sistema verrà richiesto loro di fornire login, password e il codice TOTP temporaneo generato nell'applicazione di autenticazione. Gli utenti possono contrassegnare il

browser come attendibile quando accedono al sistema, evitando così che il codice TOTP venga richiesto nei login successivi eseguiti con lo stesso browser.

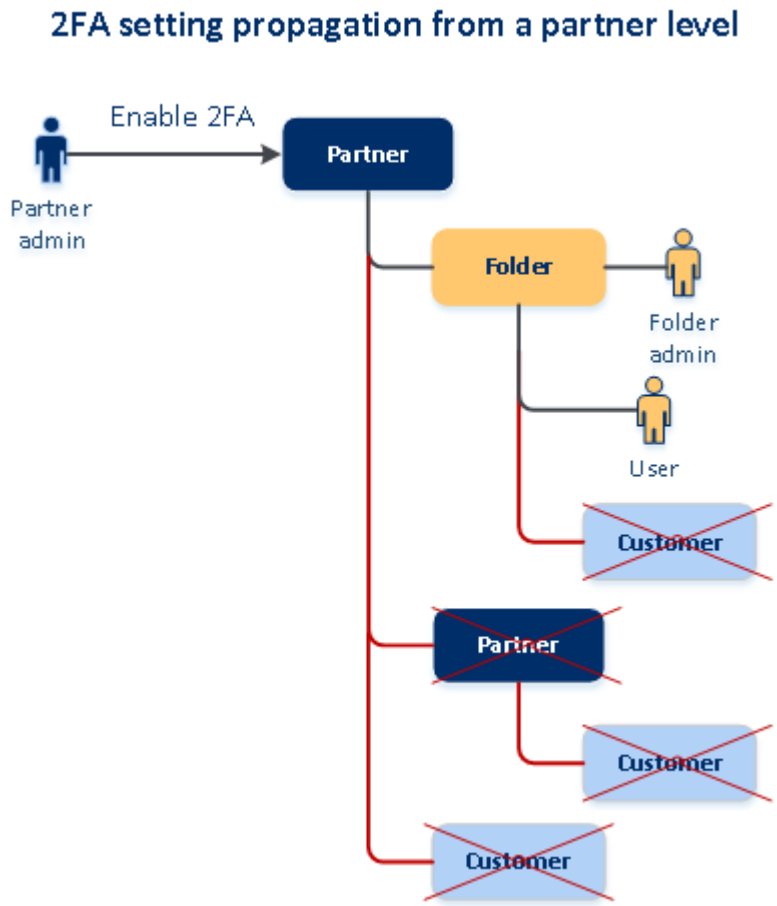
Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant

L'autenticazione a due fattori viene configurata a livello di **organizzazione**. È possibile disabilitare l'autenticazione a due fattori:

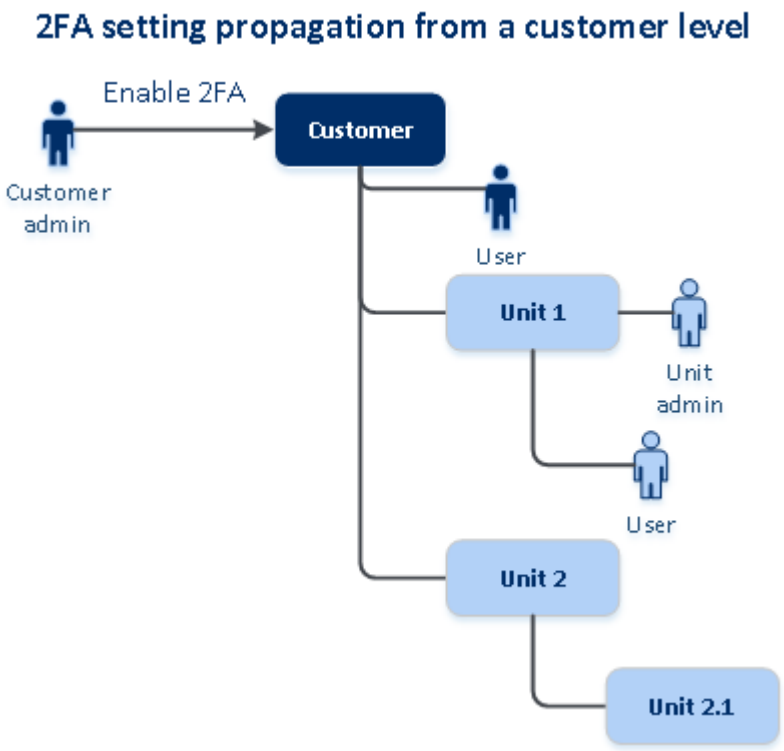
- Per la propria organizzazione.
- Per il proprio tenant figlio (solo nel caso in cui l'opzione di **Accesso al supporto** sia abilitata per tale tenant figlio).

Le impostazioni dell'autenticazione a due fattori vengono propagate ai livelli dei tenant come indicato di seguito.

- Le cartelle ereditano automaticamente le impostazioni dell'autenticazione a due fattori dall'organizzazione partner. Nello schema seguente, le linee rosse indicano che la propagazione delle impostazioni dell'autenticazione a due fattori non è possibile.



- Le unità ereditano automaticamente le impostazioni dell'autenticazione a due fattori dall'organizzazione cliente.



Nota

1. È possibile abilitare o disabilitare l'autenticazione a due fattori per le proprie organizzazioni figlio solo nel caso in cui l'opzione di **Accesso al supporto** sia abilitata per tale organizzazione figlio.
2. È possibile gestire le impostazioni dell'autenticazione a due fattori per gli utenti delle organizzazioni figlio solo nel caso in cui l'opzione di **Accesso al supporto** sia abilitata per tale organizzazione figlio.
3. Non è possibile configurare l'autenticazione a due fattori a livello di cartella o unità.
4. È possibile configurare l'impostazione dell'autenticazione a due fattori anche se tale impostazione non è abilitata nell'organizzazione padre.

Configurazione dell'autenticazione a due fattori per il tenant

L'amministratore può abilitare l'autenticazione a due fattori per l'organizzazione.

Per configurare l'autenticazione a due fattori per il tenant

1. Nel Portale di Gestione passare a **Impostazioni** > **Sicurezza**.
2. Far scorrere l'interruttore **Autenticazione a due fattori,** quindi fare clic su **Abilita**.

A questo punto, tutti gli utenti dell'organizzazione devono configurare l'autenticazione a due fattori per i propri account. Riceveranno un messaggio che indica loro di procedere alla configurazione al prossimo accesso o alla scadenza della sessione corrente.

La barra di stato al di sotto dell'interruttore mostra il numero di utenti che hanno configurato l'autenticazione a due fattori per i propri account. Per controllare quali utenti hanno configurato i

propri account, passare alla scheda **Gestione azienda** > **Utenti** e controllare la colonna **Stato 2FA**. Lo stato 2FA degli utenti che non hanno ancora configurato l'autenticazione a due fattori per i propri account è **Impostazione richiesta**.

Dopo aver eseguito la configurazione dell'autenticazione a due fattori, gli utenti dovranno inserire il login, la password e un codice TOTP ogni volta che accedono alla console del servizio.

Per disabilitare l'autenticazione a due fattori per il tenant

1. Nel Portale di Gestione passare a **Impostazioni** > **Sicurezza**.
2. Per disabilitare l'autenticazione a due fattori, disattivare l'indicatore scorrevole e quindi fare clic su **Disabilita**.
3. [Se almeno un utente ha configurato l'autenticazione a due fattori all'interno dell'organizzazione] Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo mobile.

L'autenticazione a due fattori viene disabilitata per l'organizzazione, tutti i segreti vengono cancellati e tutti i browser attendibili vengono dimenticati. Tutti gli utenti accederanno al sistema utilizzando solo il login e la password personale. Nella scheda **Gestione azienda** > **Utenti** la colonna **Stato 2FA** viene nascosta.

Gestione dell'autenticazione a due fattori per gli utenti

È possibile monitorare le impostazioni dell'autenticazione a due fattori per tutti gli utenti e ripristinare le impostazioni nella scheda **Gestione azienda** > **Utenti** del portale di gestione.

Monitoraggio

Nel portale di gestione, in **Gestione azienda** > **Utenti**, viene visualizzato un elenco di tutti gli utenti dell'organizzazione. Lo **Stato 2FA** indica se l'autenticazione a due fattori è impostata per un utente.

Per ripristinare l'autenticazione a due fattori per un utente

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Ripristina autenticazione a due fattori**.
4. Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo di secondo fattore e quindi fare clic su **Ripristina**.

L'utente potrà di nuovo configurare l'autenticazione a due fattori.

Per ripristinare il browser attendibile per un utente

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.

3. Fare clic su **Ripristina tutti i browser attendibili**.
4. Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo di secondo fattore e quindi fare clic su **Ripristina**.

Al prossimo accesso, l'utente per il quale sono stati ripristinati tutti i browser attendibili dovrà fornire il codice TOTP.

Gli utenti possono resettare da sé tutti i browser attendibili e le impostazioni di autenticazione a due fattori. Per farlo, effettuare il login nel sistema, fare clic sul link corrispondente, quindi inserire il codice TOTP per confermare l'operazione.

Per disabilitare l'autenticazione a due fattori per un utente

Non è consigliabile disabilitare l'autenticazione a due fattori perché ciò può generare potenziali vulnerabilità nella sicurezza del tenant.

Come eccezione, è possibile disabilitare l'autenticazione a due fattori per un utente e mantenere la funzionalità per tutti gli altri utenti del tenant. Questa soluzione alternativa può rivelarsi funzionale quando l'autenticazione a due fattori è abilitata in un tenant nel quale è configurata l'integrazione cloud e tale integrazione autorizza l'accesso alla piattaforma tramite l'account utente (password di accesso). Per continuare a utilizzare l'integrazione, come soluzione temporanea, è possibile convertire l'utente in un account di servizio per il quale l'autenticazione a due fattori non è applicabile.

Importante
La conversione regolare degli utenti in account di servizio, finalizzata a disabilitare l'autenticazione a due fattori, non è consigliabile perché genera rischi per la sicurezza del tenant.

La soluzione consigliata per utilizzare le integrazioni cloud senza disabilitare l'autenticazione a due fattori per i tenant è di creare i client API e configurare le integrazioni cloud in modo che lavorino con questi.

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Contrassegna come account di servizio**. Un utente ottiene uno stato speciale di autenticazione a due fattori definito **Account di servizio.**
4. [Se per almeno un utente di un tenant è stata configurata l'autenticazione a due fattori] Immettere il codice TOTP generato nell'applicazione di autenticazione del dispositivo di secondo fattore per confermare la disabilitazione.

Per abilitare l'autenticazione a due fattori per un utente

In alcuni casi è necessario abilitare l'autenticazione a due fattori per un utente per il quale l'impostazione è stata precedentemente disabilitata.

1. Nel portale di gestione, passare a **Gestione azienda** > **Utenti**.
2. Nella scheda **Utenti**, individuare l'utente per il quale modificare le impostazioni e quindi fare clic sull'icona con i puntini di sospensione.
3. Fare clic su **Contrassegna come account normale**. L'utente deve configurare l'autenticazione a due fattori o fornire il codice TOTP quando accede al sistema.

Ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore

Per ripristinare l'accesso all'account in caso di perdita del dispositivo di secondo fattore, procedere come indicato in uno degli approcci suggeriti:

- Ripristinare il segreto TOTP (codice QR o codice alfanumerico) da un backup.
  Utilizzare un dispositivo di secondo fattore e aggiungere il segreto TOTP nell'applicazione di autenticazione installata nel dispositivo.
- Chiedere all'amministratore di ripristinare l'autenticazione a due fattori.

Protezione da attacchi di forza bruta

Si definisce attacco di forza bruta quando un intruso tenta di accedere al sistema inserendo una molteplicità di password nella speranza di individuare quella corretta.

Il meccanismo di protezione da attacchi di forza bruta della piattaforma si basa sui cookie di dispositivo.

Le impostazioni per la protezione da attacchi di forza bruta utilizzate dalla piattaforma sono predefinite:

Parametro	Inserire la password	Inserire il codice TOTP
Limite di tentativi	10	5
Tempo limite per tentativi (il limite si resetta dopo ogni timeout)	15 min (900 sec)	15 min (900 sec)
Il blocco sarà attivato fra	Limite di tentativi + 1 (11° tentativo)	Limite di tentativi
Tempo di blocco	5 min (300 sec)	5 min (300 sec)

Se l'autenticazione a due fattori è abilitata, viene emesso un cookie di dispositivo verso un client (browser) solo dopo che l'autenticazione avviene con successo utilizzando entrambi i fattori (password e codice TOTP).

Per i browser attendibili, il cookie di dispositivo viene emesso dopo l'avvenuta autenticazione con un solo fattore (password).

I tentativi di inserimento del codice TOTP vengono registrati per utente, non per dispositivo. Questo significa che, anche qualora un utente tenti di inserire il codice TOTP usando dispositivi diversi, verrà comunque bloccato.

Configurazione di scenari di upselling per i clienti

L'upselling è una tecnica di vendita per suggerire ai clienti di acquistare funzionalità aggiuntive.

Cyber Protection è disponibile in numerose edizioni legacy, che differiscono tra loro in termini di funzionalità e prezzo. Il fornitore può promuovere l'acquisto di edizioni più costose e con funzioni avanzate presso i clienti esistenti che stanno utilizzando edizioni di base.

È possibile abilitare o disabilitare l'opzione di upselling per ogni cliente. Per impostazione predefinita, l'opzione di upselling è disabilitata. Se si abilita l'upselling, al cliente saranno visibili funzionalità aggiuntive che non saranno disponibili fino a quando il cliente non acquisterà l'edizione proposta. Le funzionalità aggiuntive sono contrassegnate con etichette che riportano il nome o le icone dell'edizione proposta, evidenziate in arancione. Questi elementi di upselling vengono mostrati al cliente per motivarlo all'acquisto di un'edizione più costosa. Facendo clic sull'elemento di upselling, il cliente visualizzerà una finestra di dialogo che consiglia l'acquisto dell'edizione più costosa per abilitare la funzione desiderata.

L'elemento di azione visualizzato dipende dal tipo di utente a cui corrisponde il cliente. Le tipologie di utenti (acquirenti o non acquirenti) possono essere configurate mediante l'API della piattaforma. Per ulteriori dettagli, consultare la documentazione relativa all'API. Per altre informazioni sugli elementi di azioni mostrati a clienti, fare riferimento alla seguente tabella:

Tipi di utente nel tenant cliente	Elemento di azione
Amministratore; acquirente	Nell'interfaccia utente viene visualizzato il pulsante **Acquista ora**.*
Amministratore; non acquirente	Nell'interfaccia utente viene visualizzato il messaggio "Per aggiornare l'edizione, contattare il partner".
Utente; acquirente	Nell'interfaccia utente viene visualizzato il messaggio "Per aggiornare l'edizione, contattare il partner".
Utente; non acquirente	Nell'interfaccia utente viene visualizzato il messaggio "Per aggiornare l'edizione, contattare il partner".

* Il collegamento al pulsante **Acquista ora**, che reindirizza un cliente al sito web per l'acquisto di un'edizione più avanzata, è configurabile in **Impostazioni** > **Branding**. Nella sezione upselling **Upsell** è possibile specificare l'**URL Acquista**. Le impostazioni di branding verranno applicate a tutti i partner/cartelle figlio e ai clienti, diretti e indiretti, del tenant in cui il branding è configurato.

Per abilitare o disabilitare l'opzione di upselling per un cliente

1. Nel portale di gestione, andare a **Clienti**.
2. Selezionare il cliente, passare al pannello a destra e quindi fare clic sulla scheda **Configura**.
3. Nella sezione **Upsell**, eseguire le seguenti operazioni:
   - Abilitare l'opzione **Promuovi edizioni più avanzate** per attivare lo scenario di upselling per i clienti.
   - Disabilitare l'opzione **Promuovi edizioni più avanzate** per disattivare lo scenario di upselling per i clienti.

Elementi di upselling mostrati al cliente

Elenco delle vulnerabilità

Nella console del servizio, l'elenco delle vulnerabilità è reperibile in **Gestione software** > **Vulnerabilità**. Quando l'utente fa clic sull'icona in evidenza, si apre la finestra di dialogo che promuove l'edizione e invita il cliente ad acquistare quella più costosa.

Creare o modificare un piano di protezione

Nella console del servizio, la scheda per la modifica o creazione del piano è reperibile in **Piani** > **Protezione**. Fare clic su **Crea piano**. Nelle edizioni Cyber Backup sono abilitati solo i moduli **Backup** e **Vulnerabilità**; i moduli rimanenti sono disponibili sono nelle edizioni Cyber Protect. Il cliente potrà abilitare tutti i moduli dopo aver acquistato una delle edizioni di Cyber Protect.

Individuazione automatica guidata

Nella console del servizio, la scheda di questa procedura guidata è reperibile in **Dispositivi** > **Tutti i dispositivi**. Il cliente deve avviare l'individuazione automatica guidata facendo clic su **Aggiungi**, passando alla sezione **Più dispositivi** e quindi facendo clic su **Solo per Windows**. I metodi di individuazione automatica dei sistemi sono disponibili solo nelle edizioni Advanced.

Azioni nell'elenco Dispositivi

Nella console del servizio, questo elenco è reperibile in **Dispositivi** > **Tutti i dispositivi**. Quando il cliente seleziona il sistema, nel riquadro di destra verranno visualizzate due opzioni aggiuntive:

- **Connetti tramite client HTML5**
- **Patch**

Queste opzioni saranno disponibili solo se il cliente acquista un'edizione più costosa di quella esistente.

Gestione di posizioni e archivi

La sezione **Impostazioni** > **Posizioni** mostra gli archivi cloud e le infrastrutture di disaster recovery che è possibile utilizzare per fornire i servizi **Cyber Protection** e **File Sync & Share** a partner e

clienti.

Gli archivi configurati per gli altri servizi verranno visualizzati nella scheda **Posizioni** nelle versioni future.

Posizioni

Una posizione è un contenitore che consente di raggruppare in modo pratico gli archivi cloud e le infrastrutture di disaster recovery. Può rappresentare qualsiasi elemento scelto dall'utente, ad esempio uno specifico data center o una posizione geografica dei componenti dell'infrastruttura.

È possibile creare un numero qualsiasi di posizioni e inserirvi archivi di backup, infrastrutture di disaster recovery e archivi per la **File Sync & Share**. Una posizione può contenere più archivi cloud ma una sola infrastruttura di disaster recovery.

Per informazioni su come lavorare con gli archivi, fare riferimento a "Gestione dell'archiviazione".

Selezione di posizioni e archivi per partner e clienti

Durante la creazione di un tenant partner/cartella, è possibile selezionare le diverse posizioni e i diversi archivi che saranno disponibili nel nuovo tenant per ciascun servizio.

Durante la creazione di un tenant cliente, è necessario selezionare una posizione e quindi un archivio per servizio in tale posizione. Gli archivi assegnati al cliente possono essere modificati successivamente, ma solo se il loro utilizzo è pari a 0 GB, ovvero prima che il cliente inizi a utilizzare l'archivio o dopo che il cliente ha rimosso tutti i backup da questo storage.

Le informazioni relative agli archivi assegnati a un tenant cliente vengono visualizzate nel riquadro delle informazioni cliente quando il tenant viene selezionato nella scheda **Clienti**. Le informazioni relative all'utilizzo dello spazio di archiviazione non sono aggiornate in tempo reale. Per l'aggiornamento delle informazioni possono essere necessarie fino a 24 ore.

Operazioni sulle posizioni

Per creare una nuova posizione fare clic su **Aggiungi posizione**, quindi specificare una nome per la posizione.

Per spostare un archivio o un'infrastruttura di disaster recovery in un'altra posizione, selezionare l'archivio o l'infrastruttura, fare clic sull'icona a forma di matita nel campo **Posizione** e quindi selezionare la posizione di destinazione.

Per rinominare una posizione, fare clic sull'icona con i puntini di sospensione accanto al nome della posizione, fare clic su **Rinomina** e quindi specificare il nuovo nome della posizione.

Per eliminare una posizione, fare clic sull'icona con i puntini di sospensione accanto al nome della posizione, fare clic su **Elimina** e quindi confermare l'operazione. È possibile eliminare solo le posizioni vuote.

Gestione dell'archiviazione

Aggiunta di nuovi archivi

- Servizio **Cyber Protection** :
  - Per impostazione predefinita, gli archivi di backup si trovano nei data center di .
  - Se l'elemento dell'offerta **Archivio di backup di proprietà del partner** è abilitato per un tenant partner da un amministratore di livello superiore, gli amministratori del partner possono organizzare l'archivio nel data center di proprietà del partner, utilizzando il software Cyber Infrastructure. Fare clic su **Aggiungi archivio di backup** nella sezione **Posizioni** per trovare informazioni sull'organizzazione di un archivio di backup nel proprio data center.
  - Se l'**infrastruttura di disaster recovery di proprietà del partner** che offre l'elemento è abilitata per un tenant partner da un amministratore di livello superiore, gli amministratori del partner possono organizzare l'infrastruttura di disaster recovery nel data center di proprietà del partner. Per informazioni sull'aggiunta di un'infrastruttura di disaster recovery, contattare il supporto tecnico.

Nota
Non è possibile convalidare il backup con sistemi di archiviazione degli oggetti in cloud pubblici quali Amazon S3, Microsoft Azure, Google Cloud Storage e Wasabi, utilizzati dai data center di . È invece possibile eseguire la convalida del backup con sistemi di archiviazione degli oggetti in cloud pubblici utilizzati da partner di . Tuttavia, l'abilitazione della funzionalità non è raccomandata, perché le operazioni di convalida aumentano in modo significativo il traffico in uscita dai sistemi di archiviazione degli oggetti pubblici e possono comportare un netto aumento dei costi.

- Per informazioni sull'aggiunta di archivi che verranno utilizzati da altri servizi, contattare il supporto tecnico.

Eliminazione degli archivi

È possibile eliminare gli archivi aggiunti dall'utente o dai propri tenant figlio.

Se l'archivio è assegnato a un qualsiasi tenant cliente, è necessario disabilitare il servizio che utilizza l'archivio per tutti i tenant cliente prima di eliminare l'archivio stesso.

Per eliminare un archivio

1. Accedere al portale di gestione.
2. Passare al tenant nel quale è stato aggiunto l'archivio.
3. Fare clic su **Impostazioni** > **Posizioni**.
4. Selezionare l'archivio che si desidera eliminare.

5. Nel riquadro delle proprietà dell'archivio, fare clic sull'icona dei puntini di sospensione, e quindi su **Elimina archivio**.
6. Confermare la propria decisione.

Configurazione dell'archivio immutabile

È possibile configurare l'archivio immutabile a livello del partner e a livello del cliente.

Per i tenant partner, non è possibile selezionare modalità per l'archivio immutabile. Un amministratore può disabilitare e riabilitare l'archivio immutabile e modificarne la modalità e il periodo di conservazione.

Per i tenant cliente, l'archivio immutabile è disponibile nelle modalità seguenti:

- **Modalità Governance**
  Questa modalità consente a un amministratore di disabilitare e riabilitare l'archivio immutabile e di modificarne la modalità e il periodo di conservazione.
- **Modalità Conformità**
  Dopo aver selezionato questa modalità, l'archivio immutabile non potrà essere disabilitato, né sarà possibile modificarne la modalità o il periodo di conservazione.

Se non vengono applicate impostazioni personalizzate al tenant figlio, questo eredita quelle applicate al tenant padre.

È possibile configurare le impostazioni per l'archivio immutabile solo se è stata abilitata l'autenticazione a due fattori per il tenant al quale appartiene l'account amministratore.

I backup eliminati nell'archivio immutabile utilizzano comunque uno spazio di storage, il cui consumo viene addebitato.

Nota
A partire dalla release 21.12, nei nuovi tenant partner è abilitato per impostazione predefinita un archivio immutabile con un periodo di conservazione di 14 giorni. Per i tenant esistenti è necessario abilitare l'archivio immutabile in modo manuale.

Per abilitare l'archivio immutabile per un tenant partner

1. Accedere al portale di gestione come amministratore, quindi passare a **Impostazioni** > **Sicurezza**.
2. Abilitare l'opzione **Archivio immutabile**.
3. Specificare un periodo di conservazione in un intervallo compreso tra 14 e 999 giorni.
   Il periodo di conservazione predefinito è di 14 giorni. Un periodo di conservazione più lungo può risultare in un maggiore utilizzo dell'archivio.
4. Fare clic su **Salva**.

Per disabilitare l'archivio immutabile per un tenant Partner

1. Accedere al portale di gestione come amministratore, quindi passare a **Impostazioni** > **Sicurezza**.
2. Disabilitare l'opzione **Archivio immutabile**.

Attenzione!
Questa modifica verrà ereditata da tutti i tenant figlio che non utilizzano impostazioni personalizzate per l'archivio immutabile. Tutti i backup cancellati verranno eliminati definitivamente. Inoltre, anche l'eliminazione dei nuovi backup sarà permanente.

3. Confermare la selezione facendo clic su **Disabilita**.

Per abilitare l'archivio immutabile per un tenant cliente

1. Accedere al portale di gestione come amministratore, quindi passare a **Clienti**.
2. Per modificare le impostazioni per un tenant cliente, fare clic su nome del tenant.
3. Nel menu di navigazione, passare a **Impostazioni** > **Sicurezza**.
4. Abilitare l'opzione **Archivio immutabile**.
5. Specificare un periodo di conservazione in un intervallo compreso tra 14 e 999 giorni.
   Il periodo di conservazione predefinito è di 14 giorni. Un periodo di conservazione più lungo può risultare in un maggiore utilizzo dell'archivio.
6. Selezionare la modalità Archivio immutabile.

Attenzione!
La selezione della **Modalità Conformità** è irreversibile. Non sarà più possibile disabilitare l'archivio immutabile e non sarà possibile modificare la relativa modalità né il periodo di conservazione.

7. Fare clic su **Salva**.

Per disabilitare l'archivio immutabile per un tenant cliente

1. Accedere al portale di gestione come amministratore, quindi passare a **Clienti**.
2. Per modificare le impostazioni per un tenant cliente, fare clic su nome del tenant.
3. Nel menu di navigazione, passare a **Impostazioni** > **Sicurezza**.
4. Disabilitare l'opzione **Archivio immutabile**.

Nota
È possibile disabilitare l'archivio immutabile solo in modalità Governance.

Attenzione!
Se si disabilita l'archivio immutabile, tutti i backup cancellati verranno eliminati definitivamente. Inoltre, anche l'eliminazione dei nuovi backup sarà permanente.

5. Confermare la selezione facendo clic su **Disabilita**.

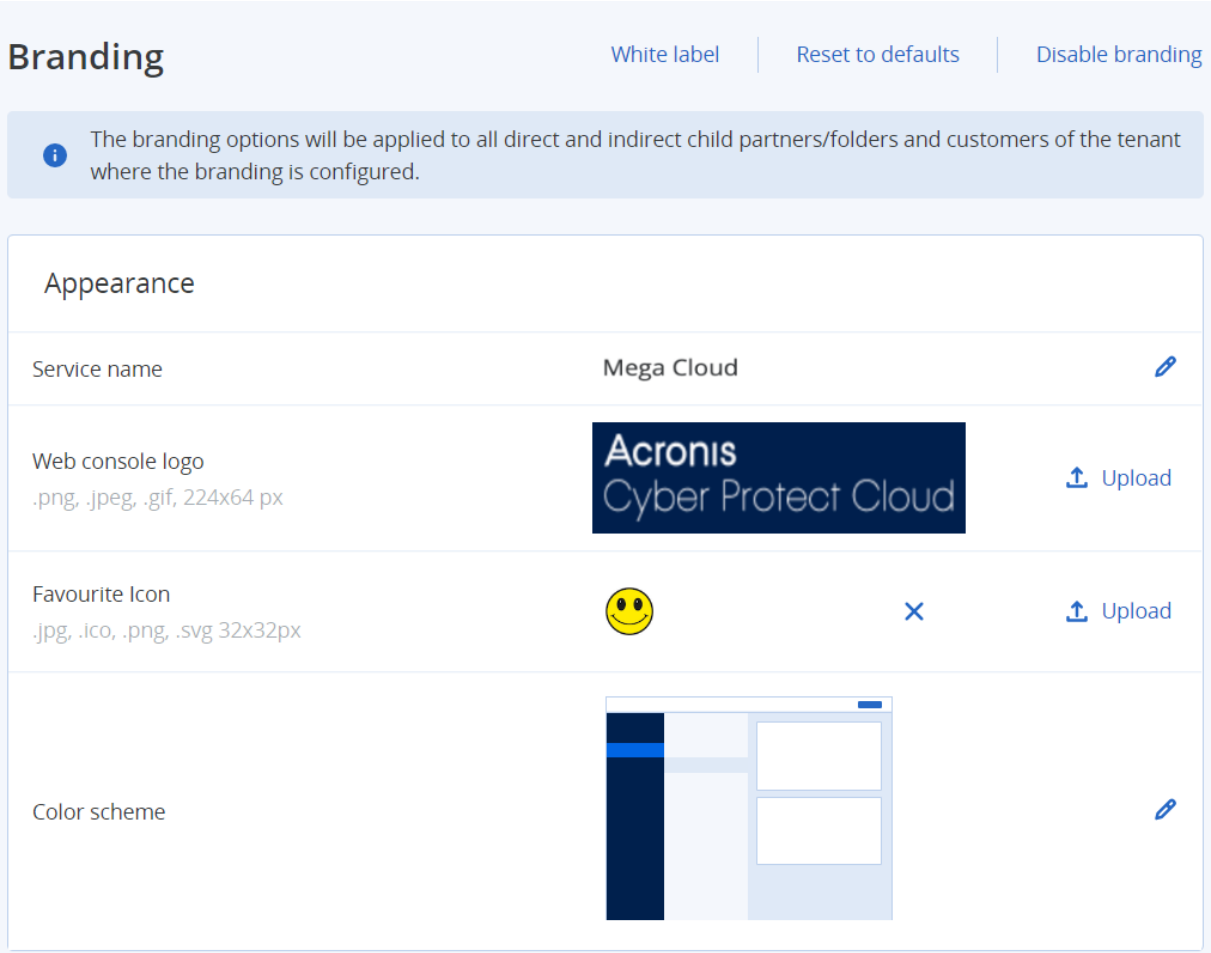
Limitazioni

- L'archivio immutabile è disponibile per archiviazioni su host Acronis o del partner che utilizzano Acronis Cyber Infrastructure versione 4.7.1 o successive.

  L'archivio immutabile richiede che la porta TCP 40440 sia aperta per il servizio Backup Gateway in Acronis Cyber Infrastructure. Nella versione 4.7.1 e successive, la porta TCP 40440 è aperta automaticamente in presenza del tipo di traffico **Backup (ABGW) public**. Per ulteriori informazioni sui tipi di traffico, fare riferimento alla documentazione di Acronis Cyber Infrastructure.
- L'archivio immutabile richiede un agente di protezione versione 21.12 (build 15.0.28532) o successive.
- Sono supportati solo i backup TIBX (Versione 12).

Configurazione del branding e del marchio personalizzabile

La sezione **Impostazioni** > **Branding** consente agli amministratori dei partner di personalizzare l'interfaccia utente del portale di gestione e il servizio **Cyber Protection** per rimuovere qualsiasi associazione con il partner di livello superiore.



È possibile configurare il branding a livello di partner e cartella. Le opzioni di branding verranno applicate a tutti i partner/cartelle figlio e ai clienti, diretti e indiretti, del tenant in cui il branding è configurato.

Altri servizi offrono capacità di branding separate nelle rispettive console del servizio. Per ulteriori informazioni, fare riferimento al Manuale utente dei servizi corrispondenti.

Applicazione del branding

Aspetto

- **Nome del servizio**. Questo nome viene utilizzato in tutti i messaggi e-mail inviati dai servizi cloud e dal portale di gestione (messaggi di attivazione dell'account, messaggi e-mail con notifiche sul servizio), nella **schermata iniziale** dopo il primo accesso e come nome della scheda del browser del portale di gestione.
- **Logo della console web**. Il logo viene visualizzato nel portale di gestione e nei servizi. Fare clic su **Carica** per caricare un file di immagine.
- **Icona Preferiti** [Disponibile solo se è stato configurato un URL personalizzato]. L'icona dei preferiti viene visualizzata accanto al titolo della pagina, nella scheda del browser. Fare clic su **Carica** per caricare un file di immagine.

- **Schema colori**. Lo schema colori definisce la combinazione di colori utilizzata per tutti gli elementi dell'interfaccia utente.

  Nota
  Fare clic su **Anteprima schema in una nuova scheda** per un'anteprima dell'interfaccia che verrà visualizzata ai tenant figlio. Il branding non viene applicato fino a quando non si fa clic sul pulsante **Chiudi** nella pagina **Seleziona schema colori**.

Branding dell'agente e del programma di installazione

È possibile personalizzare il branding dei file di installazione dell'agente e di Tray Monitor per Windows e macOS.

Nota
Per abilitare questa funzionalità di branding, è necessario aggiornare gli agenti Cyber Protection alla versione 15.0.28816 (Release 22.01) o successive.

- **Nome file del programma di installazione dell'agente**. Il nome del file di installazione che viene scaricato nei workload protetti.
- **Logo del programma di installazione dell'agente**. Il logo visualizzato nell'Installazione guidata durante l'installazione dell'agente. Fare clic su **Carica** per caricare un file di immagine.
- **Nome agente**. Il nome visualizzato nell'Installazione guidata durante l'installazione dell'agente.
- **Nome Tray Monitor**. Il nome visualizzato nella parte alta della finestra Tray Monitor.

Documentazione e supporto

- **URL home**. Questa pagina viene visualizzata quando l'utente fa clic sul nome dell'azienda nel riquadro **Informazioni su**.
- **URL supporto** Questa pagina viene visualizzata quando l'utente fa clic sul collegamento **Contatta il supporto** nel riquadro **Informazioni su** o in un messaggio e-mail inviato dal portale di gestione.
- **Telefono supporto**. Questo numero di telefono viene visualizzato nel riquadro **Informazioni su**.
- **URL della Knowledge Base** Questa pagina viene visualizzata quando l'utente fa clic sul collegamento **Knowledge Base** in un messaggio di errore.
- **Guida dell'amministratore del Portale di gestione**. Questa pagina viene visualizzata quando un utente fa clic sull'icona del punto interrogativo nell'angolo in alto a destra dell'interfaccia utente del portale di amministrazione e quindi su **Informazioni su** > **Manuale per l'amministratore**.
- **Guida in linea dell'amministratore del Portale di gestione**. Questa pagina viene visualizzata quando un utente fa clic sull'icona del punto interrogativo nell'angolo in alto a destra dell'interfaccia utente del portale di amministrazione e quindi su **Guida in linea**.

URL per i servizi Cyber Protect Cloud

È possibile rendere disponibili i servizi Cyber Protect Cloud dal dominio personalizzato dell'utente. Fare clic su **Configura** per impostare l'URL personalizzato per la prima volta, oppure fare clic su **Riconfigura** per modificare l'URL esistente. Per utilizzare l'URL predefinito (https://cloud.acronis.com), fare clic su **Ripristina valori predefiniti**. Per ulteriori informazioni sugli URL personalizzati, fare riferimento a "Configurazione degli URL delle interfacce web personalizzate".

Impostazioni documento legale

- **URL Contratto di licenza per l'utente finale**. Questa pagina viene visualizzata quando l'utente fa clic sul collegamento **Contratto di licenza per l'utente finale** nel riquadro **Informazioni su**, nella **schermata iniziale** visualizzata al primo accesso e nelle landing page della richiesta di caricamento di File Sync & Share.
- **URL Termini piattaforma** Questa pagina viene visualizzata quando un amministratore del partner fa clic sul collegamento **Termini piattaforma** nel riquadro **Informazioni su** o nella **schermata iniziale** visualizzata al primo accesso.
- **URL Informativa sulla privacy**. Questa pagina viene visualizzata quando l'utente fa clic sul collegamento **Informativa sulla privacy** nella **schermata iniziale** visualizzata al primo accesso, e nelle landing page della richiesta di caricamento di File Sync & Share.

Importante
Per non visualizzare un documento nella schermata iniziale, non immettere l'URL del documento.

Nota
Per ulteriori informazioni sulle richieste di caricamento di File Sync & Share, consultare il Manuale dell'utente di Cyber Files Cloud.

Upsell

- **URL Acquista**. Questa pagina viene visualizzata quando un utente fa clic su **Acquista ora** per passare a un'edizione più avanzata del servizio Cyber Protection. Per altre informazioni sugli scenari di upselling, fare riferimento a "Configurazione di scenari di upselling per i clienti".

App per dispositivo mobile

- **App Store**. Questa pagina viene visualizzata quando un utente fa clic su **Aggiungi** > **iOS** nel servizio **Cyber Protection** .
- **Google Play**. Questa pagina viene visualizzata quando un utente fa clic su **Aggiungi** > **Android** nel servizio **Cyber Protection** .

Impostazioni server e-mail

È possibile specificare un server e-mail personalizzato che verrà utilizzato per inviare notifiche e-mail dal portare di gestione e dai servizi. Per specificare un server e-mail personalizzato, fare clic su **Personalizza**, quindi specificare le impostazioni seguenti:

- Nel campo **Da**, inserire il nome che verrà visualizzato nel campo **Da** delle notifiche e-mail.
- Nel campo **SMTP**, immettere il nome del server della posta in uscita (SMTP).
- Nel campo **Porta**, inserire la porta del server di posta in uscita. Per impostazione predefinita, è impostata la porta 25.
- Nel campo **Crittografia** scegliere se utilizzare la crittografia TLS o SSL. Selezionare **Nessuno** per disabilitare la crittografia.
- Nei campi **Nome utente** e **Password**, specificare le credenziali dell'account che verrà utilizzato per l'invio dei messaggi.

Configurazione del branding

1. Accedere al portale di gestione.
2. Passare al tenant nel quale si desidera configurare il branding.
3. Fare clic su **Impostazioni** > **Branding**.
4. [Se il branding non è ancora stato abilitato] Fare clic su **Abilita branding**.
5. Configurare le opzioni di branding descritte sopra.

Ripristino delle impostazioni predefinite di branding

È possibile ripristinare tutti gli elementi di branding ai valori predefiniti.

1. Accedere al portale di gestione.
2. Passare al tenant nel quale si desidera ripristinare il branding.
3. Fare clic su **Impostazioni** > **Branding**.
4. In alto a destra, fare clic su **Ripristina predefiniti**.

Disabilitare il branding

È possibile disabilitare il branding per il proprio account e per tutti i tenant figlio.

1. Accedere al portale di gestione.
2. Passare al tenant nel quale si desidera disabilitare il branding.
3. Fare clic su **Impostazioni** > **Branding**.
4. In alto a destra, fare clic su **Disabilita branding**.

Personalizzazione

Questa opzione consente di definire per tutti i clienti e i partner figlio se l'agente Cyber Protection (per Windows, macOS e Linux) e Cyber Protection Monitor (per Windows, macOS e Linux) saranno dotati di marchio o saranno personalizzabili. Abilitando l'opzione, sarà possibile personalizzare l'agente e Tray Monitor. L'opzione ha effetto sui nomi e sui logo utilizzati nel programma di installazione e in Cyber Protection Monitor.

Applicazione della personalizzazione

1. Accedere al portale di gestione.
2. Passare al tenant nel quale si desidera applicare la personalizzazione.
3. Fare clic su **Impostazioni** > **Branding**.
4. Nell'area superiore della finestra, fare clic su **Personalizzazione** per annullare tutti gli elementi di branding, ad eccezione di **Nome del servizio**, **URL Contratto di licenza per l'utente finale**, **Manuale dell'amministratore del portale di gestione**, **Guida in linea dell'amministratore del portale di gestione** e **Impostazioni del server e-mail**.

Configurazione degli URL delle interfacce web personalizzate

Nota
Un URL personalizzato punta a un indirizzo IP diverso rispetto all'URL predefinito. Questo aspetto va tenuto presente quando si configurano le policy per il firewall.

Per configurare l'URL dell'interfaccia web dei servizi Cyber Protect Cloud

1. Nel portale di gestione, fare clic su **Impostazioni** > **Branding**.
2. Nella sezione **URL per i servizi Cyber Protect Cloud**:
   - Fare clic su **Configura** per impostare l'URL personalizzato per la prima volta.
   - Fare clic su **Riconfigura** per modificare l'URL personalizzato esistente.
3. Nel passaggio **Impostazioni del dominio**, preparare il dominio e un record CNAME.

   Per utilizzare un URL personalizzato è necessario disporre di un nome di dominio attivo e di un record CNAME configurato per puntare al data center in cui si trova l'account dell'utente. La configurazione del record CNAME viene eseguita dal registrar DNS e la sua propagazione può richiedere fino a 48 ore.

   Per individuare il nome di dominio del data center e richiedere la configurazione del record CNAME, consultare l'articolo della Knowledge Base Branding Web Console URL (58275).
4. Nel passaggio **Controllare l'URL**, verificare di poter accedere all'URL personalizzato e che il record CNAME sia configurato correttamente. A tal fine, inserire il nome dell'URL principale e fare clic su **Controlla**. Se si utilizza un certificato SSL jolly, è possibile aggiungere fino a dieci

nomi di dominio alternativi. Se si utilizza un certificato "Let's Encrypt", i nomi di dominio alternativi verranno ignorati.

5. Nel passaggio **Certificato SSL**, eseguire una delle seguenti operazioni:
   - Creare un certificato "Let's Encrypt". A tal fine, fare clic su **Certificato SSL gratuito con "Let's Encrypt"**. Questa opzione utilizza i certificati "Let's Encrypt" emessi da una terza parte. Il service provider non è responsabile di eventuali problemi causati dall'utilizzo di certificati gratuiti. Per ulteriori informazioni sulle condizioni di utilizzo di "Let's Encrypt", fare riferimento a https://letsencrypt.org/repository/.
   - Caricare il certificato jolly. A tal fine, fare clic su **Carica certificato jolly**, quindi fornire un certificato jolly e una chiave privata.
6. Fare clic su **Invia** per applicare le modifiche.

Per ripristinare l'URL personalizzato alle impostazioni predefinite

1. Nel portale di gestione, fare clic su **Impostazioni** > **Branding**.
2. Nella sezione **URL per i servizi Acronis Cyber Protect Cloud**, fare clic su **Ripristina valori predefiniti** per utilizzare l'URL predefinito (https://cloud.acronis.com).

Aggiornamento automatico degli agenti

Cyber Protect dispone di tre tipi di agenti che possono essere installati nei sistemi protetti: Agente per Windows, Agente per Linux e Agente per Mac.

Cyber Files Cloud è disponibile in una versione per Windows e in una per MacOS dell'Agente Desktop per File Sync & Share, che consente la sincronizzazione di file e cartelle tra un sistema e un'area di cloud storage dell'utente di File Sync & Share per incentivare il lavoro offline e le procedure lavorative WFH (Work From Home) e BYOD (Bring Your Own Device).

Per semplificare la gestione di più workload, è possibile configurare (e disabilitare) gli aggiornamenti automatici e senza intervento dell'utente di tutti gli agenti su tutti i sistemi.

Importante
Al momento, possono accedere alla funzionalità di gestione dell'aggiornamento dell'agente solo i partner e i clienti per i quali è abilitato Protezione.

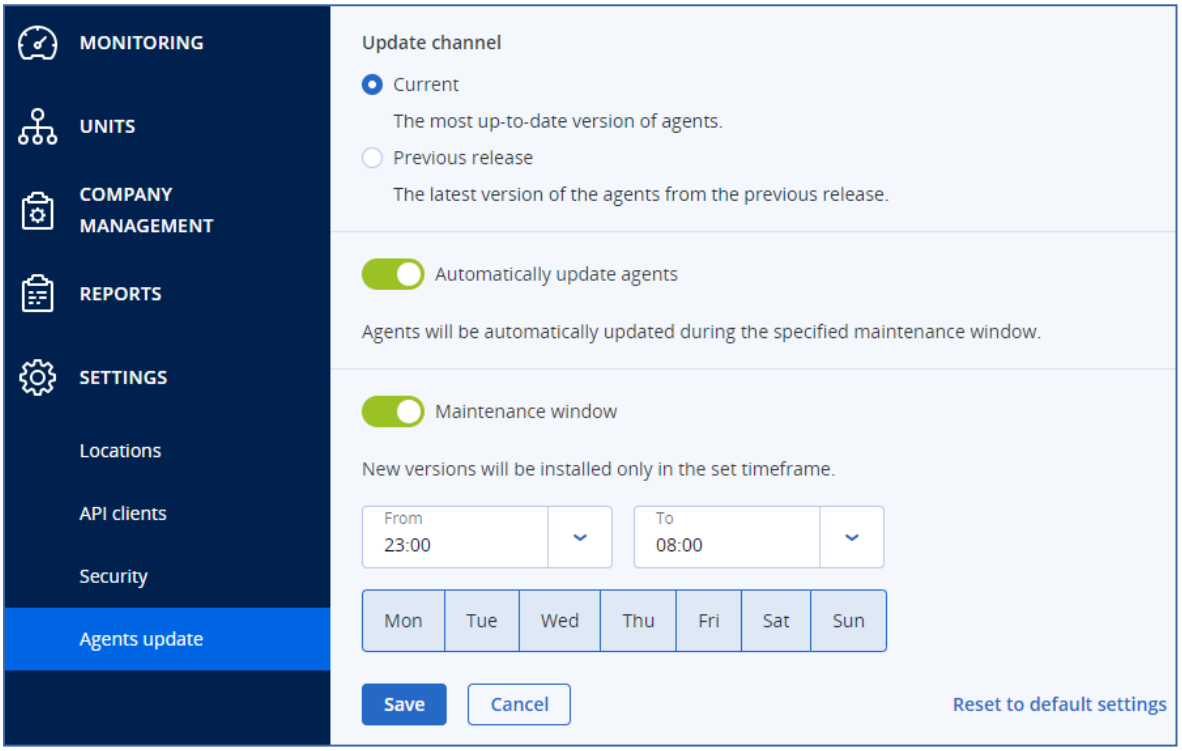
Nota
Per gestire gli agenti sui singoli sistemi e personalizzare le impostazioni di aggiornamento automatico, consultare la sezione della Guida per l'utente di Cyber Protect su come aggiornare gli agenti.

Per aggiornare gli agenti automaticamente

Nota
Le impostazioni per l'aggiornamento automatico dell'Agente per File Sync & Share sono ereditate da partner e clienti per i quali non è stata abilitata alcuna protezione.

Per mostrare l'aggiornamento automatico degli agenti dalla pagina iniziale del portale di gestione

1. Selezionare **Impostazioni > Aggiornamento agenti**.



2. Selezionare quale versione individuare per gli aggiornamenti automatici: **Attuale** o **Release precedente**.
   (L'impostazione predefinita è **Attuale**.)
3. Attivare l'opzione **Aggiorna automaticamente gli agenti**.
   (L'impostazione predefinita è **On**.)
4. Impostare l'intervallo di manutenzione.
   (L'impostazione predefinita è 23:00 - 08:00.)

   Nota
   Benché i processi di aggiornamento degli agenti siano progettati per essere rapidi e semplici, consigliamo sempre di scegliere un intervallo che causi un'interruzione operativa minima agli utenti, perché questi non possono prevenire o posticipare gli aggiornamenti automatici.

5. [Facoltativo] Selezionare i giorni specifici in cui eseguire gli aggiornamenti automatici.
6. Selezionare **Salva.**

Nota
Gli aggiornamenti automatici sono disponibili solo per:

- Agenti Cyber Protect, versione 15.0.26986 (rilasciata a maggio 2021) o successive.
- Agente Desktop per File Sync & Share, versione 15.0.30370 o successive.

Prima che possano avere effetto gli aggiornamenti automatici, gli agenti meno recenti devono essere aggiornati manualmente alla versione più recente.

Per monitorare gli aggiornamenti degli agenti

Importante
Gli aggiornamenti degli agenti possono essere monitorati solo da amministratori di partner e clienti che hanno abilitato il modulo di protezione.

Per monitorare gli aggiornamenti degli agenti, consultare le sezioni relative agli avvisi e alle attività della Guida per l'utente di Cyber Protect.

Monitoraggio

Per accedere alle informazioni sull'utilizzo dei servizi e sulle operazioni, fare clic su **Monitoraggio**.

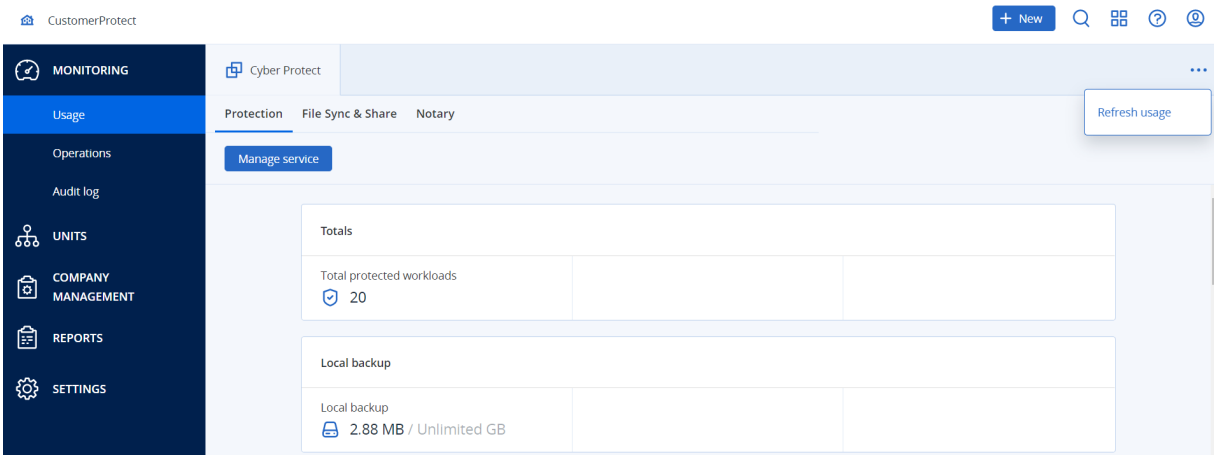
Utilizzo

La scheda **Utilizzo** fornisce una panoramica dell'utilizzo del servizio e consente di accedere ai servizi inclusi nel tenant nel quale si sta lavorando.

I dati di utilizzo includono i dati delle funzionalità incluse come standard e delle funzionalità avanzate.

Per aggiornare i dati di utilizzo visualizzati sulla scheda, fare clic sui puntini di sospensione nell'angolo in alto a destra dello schermo e selezionare **Aggiorna utilizzo**.

Nota
Il recupero dei dati può richiedere fino a 10 minuti. Ricaricare la pagina per visualizzare i dati aggiornati.



Operazioni

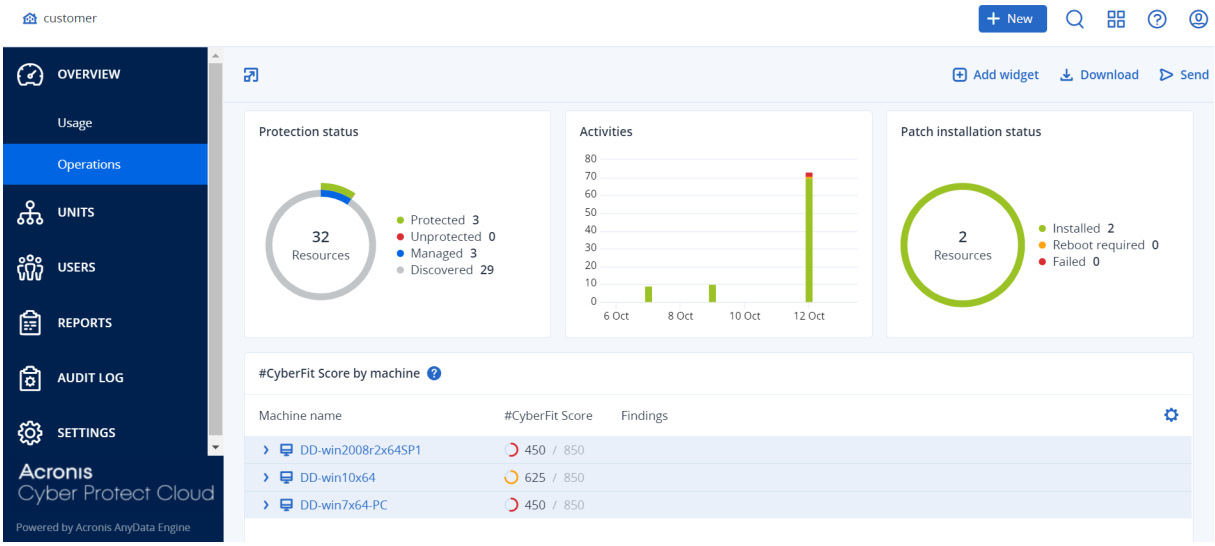
Il pannello di controllo **Operazioni** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al servizio Cyber Protection. I widget di altri servizi saranno disponibili nelle release future.

Per impostazione predefinita, i dati vengono visualizzati per il tenant nel quale si sta operando. È possibile cambiare il tenant visualizzato per ogni singolo widget modificandolo. Vengono inoltre visualizzate le informazioni aggregate sui tenant cliente figlio diretti del tenant selezionato, inclusi quelli che si trovano nelle cartelle. Nel pannello di controllo *non* vengono visualizzate informazioni sui partner figlio e sui relativi tenant figlio; è necessario esaminare in dettaglio il partner specifico per visualizzare il relativo pannello di controllo. Se, tuttavia, si converte un tenant partner figlio in un tenant cartella, le informazioni relative ai clienti figlio di tale tenant verranno visualizzate nel pannello di controllo del tenant padre.

I widget sono aggiornati ogni due minuti. I widget presentano elementi cliccabili che consentono di indagare e risolvere i problemi. È possibile scaricare lo stato corrente del pannello di controllo in formato .pdf e/o .xlsx, oppure inviarlo tramite e-mail a qualsiasi indirizzo, inclusi destinatari esterni.

È possibile scegliere tra numerosi widget, presentati come tabelle, grafici a torta, a barre e mappe ad albero. È possibile aggiungere numerosi widget dello stesso tipo per tenant diversi o con filtri

diversi.



Per riorganizzare i widget nel pannello di controllo

Trascinare e rilasciare i widget facendo clic sui rispettivi nomi.

Per modificare un widget

Fare clic sull'icona a forma di matita accanto al nome del widget. La modifica del widget consente all'utente di rinominarlo, modificare l'intervallo temporale, selezionare il tenant per il quale vengono visualizzati i dati e impostare i filtri.

Per aggiungere un widget

Fare clic su **Aggiungi widget** e quindi eseguire una delle seguenti operazioni:

- Fare clic sul widget che si desidera aggiungere. Il widget verrà aggiunto con le impostazioni predefinite.
- Per modificare il widget prima di aggiungerlo, fare clic sull'icona a forma di ingranaggio visualizzata quando il widget è selezionato. Dopo aver modificato il widget, fare clic su **Chiudi**.

Per rimuovere un widget

Fare clic sul simbolo X accanto al nome del widget.

Stato protezione

Stato protezione

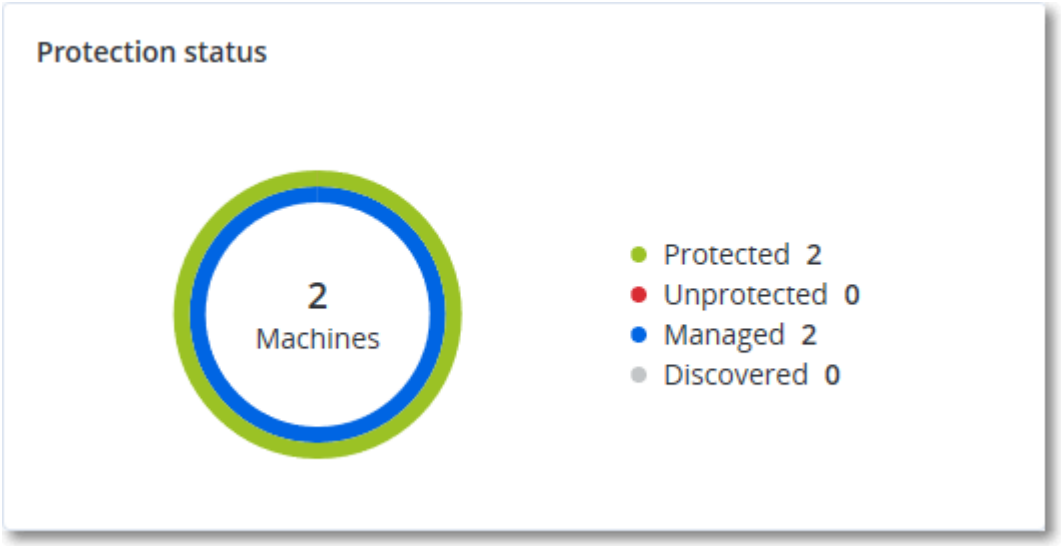
Questo widget mostra lo stato della protezione corrente di tutti i sistemi.

Un sistema può trovarsi in uno dei seguenti stati:

- **Protetto**: per tutti i sistemi con un piano di protezione applicato.
- **Non protetto**: per tutti i sistemi senza un piano di protezione applicato. Sono inclusi i sistemi individuati e quelli gestiti ai quali non è applicato un piano di protezione.

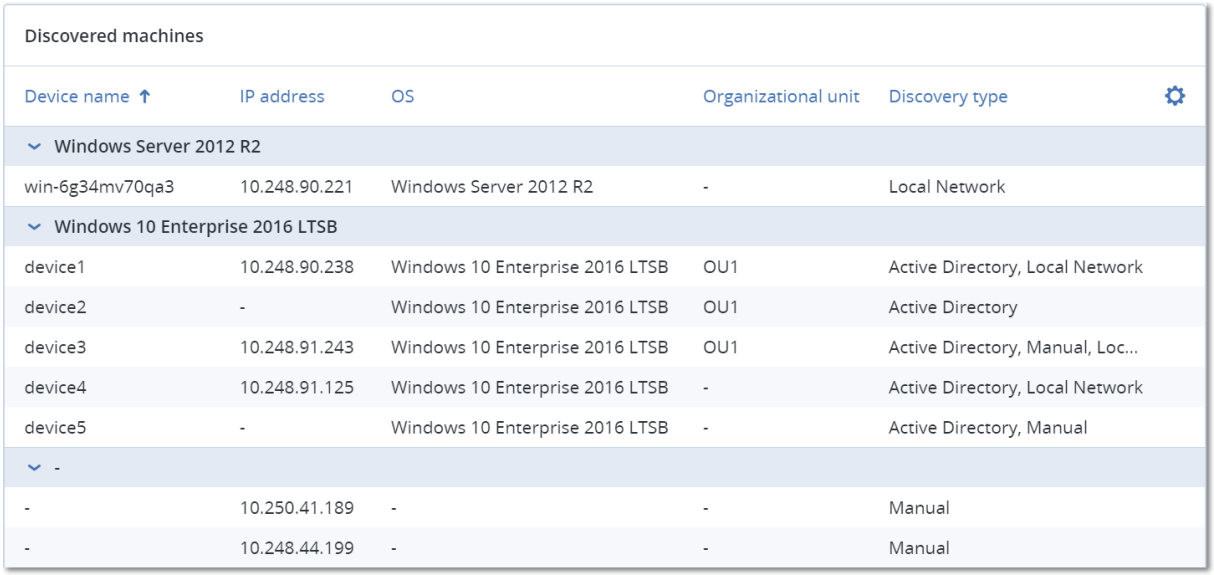
- **Gestito**: per tutti i sistemi con l'agente di protezione installato.
- **Individuato** : per tutti i sistemi senza l'agente di protezione installato.

Facendo clic sullo stato, si verrà reindirizzati all'elenco dei sistemi che presentano tale stato, per maggiori informazioni.



Macchine individuate

Questo widget mostra l'elenco dei sistemi rilevati durante l'intervallo di tempo specificato.



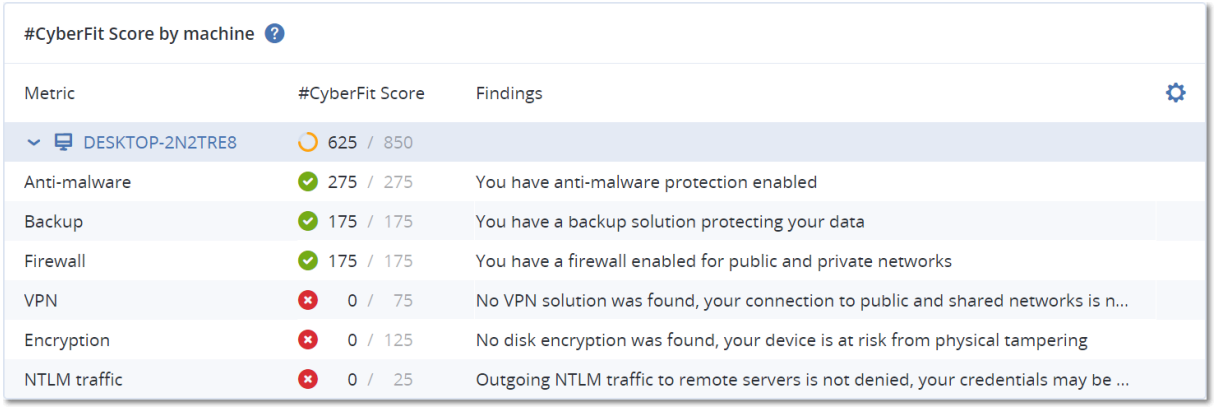
#CyberFit Score per sistema

Questo widget mostra, per ogni sistema, il #CyberFit Score totale, i punteggi che lo compongono e i risultati ottenuti per ogni metrica valutata:

- Anti-malware
- Backup
- Firewall
- VPN
- Crittografia
- Traffico NTLM

Per migliorare il punteggio di ogni metrica è possibile visualizzare le raccomandazioni disponibili nel report.

Per ulteriori informazioni sul #CyberFit Score, consultare "#CyberFit Score dei sistemi".



Widget di Endpoint Detection and Response (EDR)

Importante
Si tratta di una versione con Accesso prioritario alla documentazione EDR. Alcune delle funzionalità e delle descrizioni potrebbero essere incomplete.

Endpoint Detection and Response (EDR) include una serie di widget a cui è possibile accedere dalla dashboard **Operazioni**.

I widget disponibili sono:

- Distribuzione dei principali problemi per workload
- MTTR del problema
- Burndown dei problemi di sicurezza
- Stato della rete dei workload

Distribuzione dei principali problemi per workload

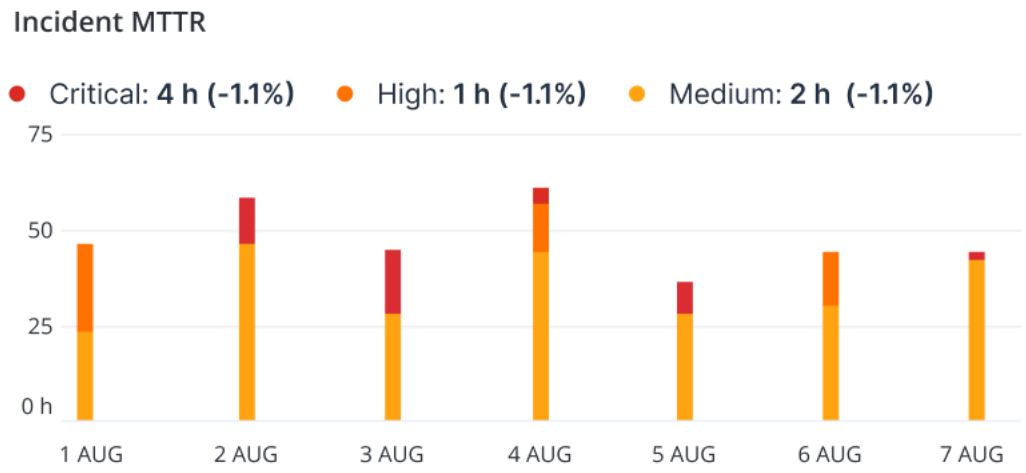
Questo widget mostra i primi cinque workload con il maggior numero di problemi (fare clic su **Mostra tutto** per essere reindirizzati all'elenco dei problemi filtrato in base alle impostazioni del widget).

Passare il mouse su una riga del workload per visualizzare i dettagli dello stato corrente delle indagini sui problemi; i possibili stati dell'indagine sono **Non avviata**, **Indagine in corso**, **Chiusa** e **Falso positivo**. Fare quindi clic sul workload che si desidera analizzare ulteriormente e selezionare il cliente di interesse nella finestra popup visualizzata; l'elenco dei problemi viene aggiornato in base alle impostazioni del widget.

MTTR del problema

Questo widget mostra il tempo medio di risoluzione dei problemi di sicurezza. Indica la rapidità con la quale i problemi vengono analizzati e risolti.

Fare clic su una colonna per visualizzare in dettaglio i problemi in base al livello di gravità (**Critica**, **Elevata** e **Media**) e un'indicazione del tempo impiegato per risolverli in base ai diversi livelli di gravità. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.

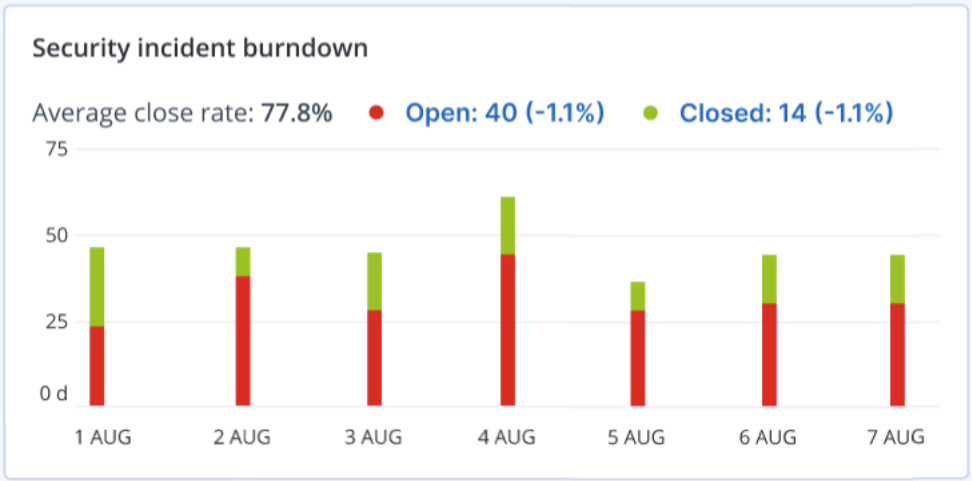


Burndown dei problemi di sicurezza

Questo widget indica il tasso di efficienza nella risoluzione dei problemi; il numero di problemi aperti viene misurato a fronte del numero di problemi chiusi in un determinato periodo di tempo.

Passare il mouse su una colonna per visualizzare in dettaglio i problemi chiusi o aperti per il giorno selezionato. Se si fa clic sul valore Aperto, viene visualizzata una finestra popup nella quale è possibile selezionare il tenant di interesse; viene visualizzato l'elenco dei problemi filtrati relativi al tenant, dal quale è possibile osservare i problemi attualmente aperti (con lo stato **Indagine in corso** o **Non avviata**). Se si fa clic sul valore Chiuso, viene visualizzato l'elenco dei problemi per il tenant selezionato, filtrato per visualizzare i problemi non più aperti (con lo stato **Chiuso** o **Falso positivo**).

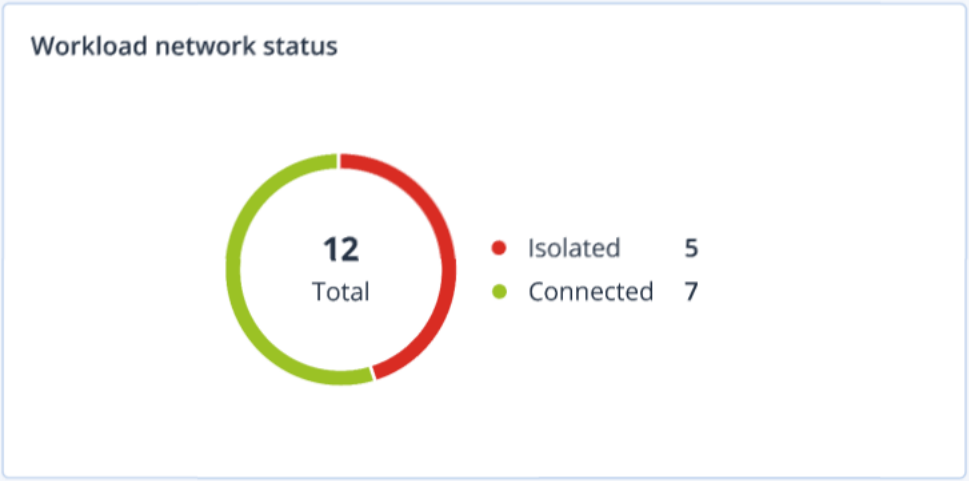
Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.



Stato della rete dei workload

Questo widget mostra lo stato corrente della rete dei workload e indica il numero di workload isolati e connessi.

Fare clic sul valore Isolato; viene visualizzata una finestra popup nella quale selezionare il tenant di interesse. La vista del workload visualizzata viene filtrata per mostrare i workload isolati. Fare clic sul valore Connesso per visualizzare l'elenco Workload con agenti filtrato per mostrare i workload connessi (per il tenant selezionato).



Monitoraggio integrità del disco

Il monitoraggio dell'integrità del disco fornisce informazioni sullo stato corrente del disco e su quello prevedibile, così da prevenire perdite di dati che potrebbero essere correlate a un guasto del disco. La funzione supporta dischi HDD e SSD.

Limitazioni

- La previsione dell'integrità del disco è supportata solo per i sistemi che eseguono Windows.
- È possibile monitorare solo i dischi dei sistemi fisici. Non è possibile monitorare e mostrare nel widget dell'integrità del disco i dischi delle virtual machine.
- Non sono supportate le configurazioni RAID.
- Nelle unità NVMe, il monitoraggio dell'integrità del disco è supportato solo per le unità in grado di comunicare i dati SMART tramite l'API Windows. Il monitoraggio dell'integrità del disco non è supportato nelle unità NVMe che richiedono la lettura dei dati SMART direttamente dall'unità.

L'integrità del disco è rappresentata da uno dei seguenti stati:

- **OK**
  L'integrità del disco è compresa tra il 70 e il 100%.
- **Attenzione**
  L'integrità del disco è compresa tra il 30 e il 70%.
- **Attenzione**
  L'integrità del disco è compresa tra lo 0 e il 30%.
- **Calcolo dei dati del disco in corso**
  È in corso il calcolo dello stato corrente del disco e delle previsioni.

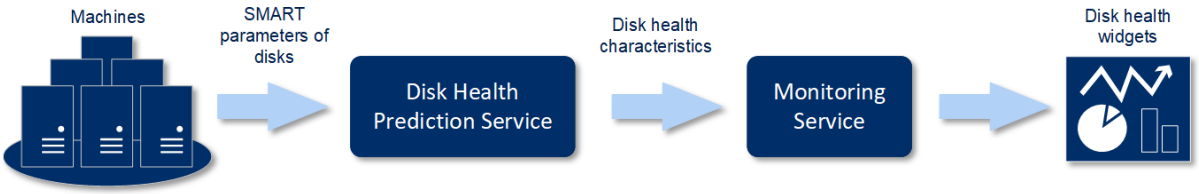
Come funziona

Il servizio Previsione dell'integrità del disco utilizza un modello di previsione basato su intelligenza artificiale.

1. L'agente di protezione acquisisce i parametri SMART dei dischi e invia i dati raccolti al servizio Previsione dell'integrità del disco:
   - SMART 5 – Conteggio dei settori riallocati.
   - SMART 9 – Ore di attività.
   - SMART 187 – Errori non correggibili segnalati.
   - SMART 188 – Timeout comando.
   - SMART 197 – Conteggio settori attualmente in sospeso.
   - SMART 198 – Conteggio settori non correggibili offline.
   - SMART 200 – Frequenza errori di scrittura.

2. Il servizio Previsione dell'integrità del disco elabora i parametri SMART ricevuti, effettua le previsioni e fornisce quindi le informazioni seguenti sull'integrità del disco:
   - Stato corrente di integrità del disco: OK, Attenzione, Critico.
   - Previsione dell'integrità del disco: negativa, stabile, positiva.
   - Probabilità della previsione dell'integrità del disco in percentuale.

   Il periodo di previsione è un mese.
3. Il Servizio di monitoraggio riceve queste informazioni e quindi mostra le informazioni pertinenti nei widget di integrità del disco nella console del servizio.



Widget di integrità del disco

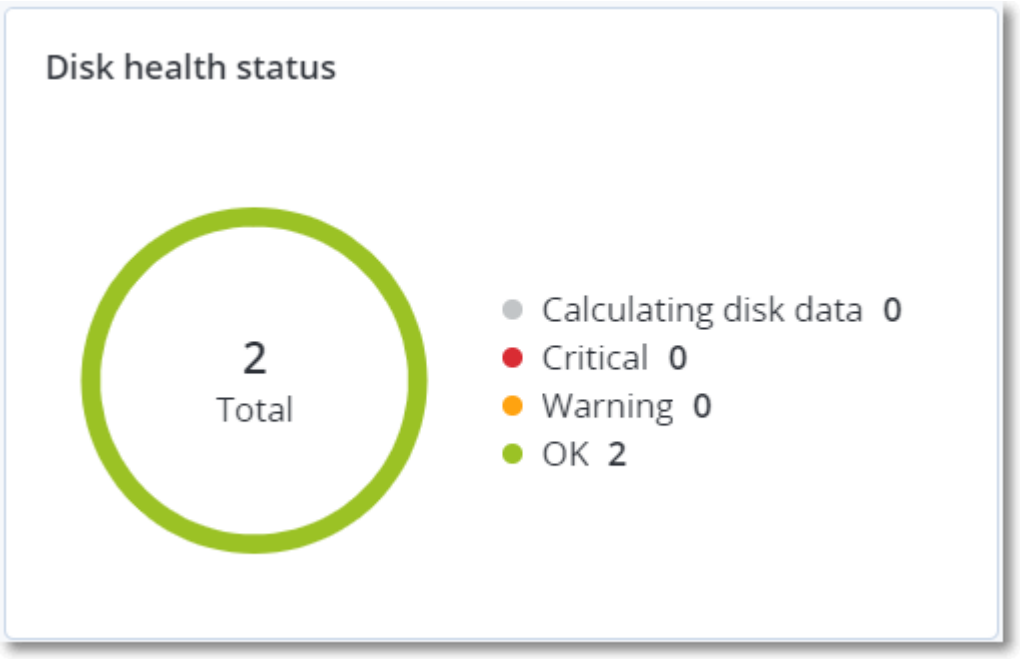
I risultati del monitoraggio dell'integrità del disco vengono presentati nei widget seguenti, disponibili nella console del servizio.

- **Panoramica dell'integrità del disco** è un widget con struttura ad albero dotata di due livelli di dettaglio, visualizzabili eseguendo il drill down:
  - Livello del sistema
    Mostra informazioni di riepilogo sullo stato dell'integrità del disco di sistemi selezionati del cliente. Vengono mostrati solo gli stati del disco critici. Gli altri stati vengono mostrati nei suggerimenti visualizzati quando si passa il mouse su uno specifico blocco. La dimensione del blocco del sistema dipende dalla dimensione totale di tutti i dischi del sistema. Il colore del blocco del sistema dipende dallo stato del disco con maggiore criticità individuato.

- Livello del disco
  Mostra lo stato corrente dell'integrità del disco di tutti i dischi del sistema selezionato. Ogni blocco disco mostra una delle seguenti previsioni di integrità del disco e la sua probabilità, espressa in percentuale:
  - Verrà danneggiato
  - Resterà stabile

- Verrà migliorato

- **Stato di integrità del disco** è un widget con grafico a torta che mostra il numero di dischi per ogni stato.



Avvisi di stato dell'integrità del disco

Il controllo dell'integrità del disco viene eseguito ogni 30 minuti, mentre l'avviso corrispondente viene generato una volta al giorno. Viene sempre generato un avviso quando lo stato di integrità del disco passa da **Attenzione** a **Critico**.

Nome avviso	Gravità	Stato integrità del disco	Descrizione
È possibile che il disco sia stato danneggiato	Avviso	(30 – 70)	Il disco <nome disco> di questo sistema potrebbe subire un guasto nel prossimo futuro. Eseguire il backup dell'immagine completa del disco il più presto possibile, sostituirlo e quindi ripristinare l'immagine sul nuovo disco.
Il guasto del disco è imminente	Critico	(0 – 30)	Il disco <nome disco> in questo sistema è in condizioni critiche e potrebbe subire un danno nell'immediato futuro. Con queste condizioni il backup dell'immagine del disco non è consigliata, perché il lavoro aggiuntivo richiesto potrebbe causare il guasto del disco. Eseguire immediatamente il backup dei file più importanti presenti sul disco, e sostituirlo.

Mappa di protezione dati

La funzione Mappa di protezione dati consente di esaminare tutti i dati ritenuti importanti e di ottenere informazioni dettagliate su numero, dimensione, posizione, stato della protezione di tutti i file rilevanti, in una vista scalabile con mappa ad albero.

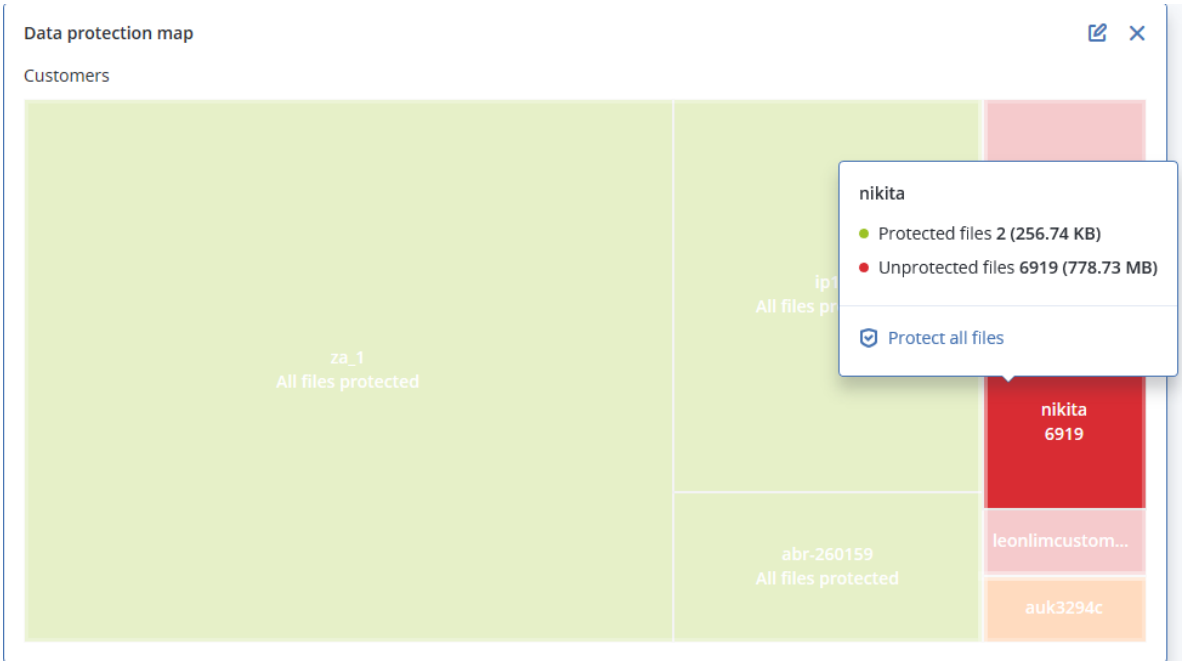
Ogni dimensione del blocco dipende dal numero/dimensione totale di tutti i file importanti che appartengono a un cliente/sistema.

I file possono presentare uno dei seguenti stati di protezione:

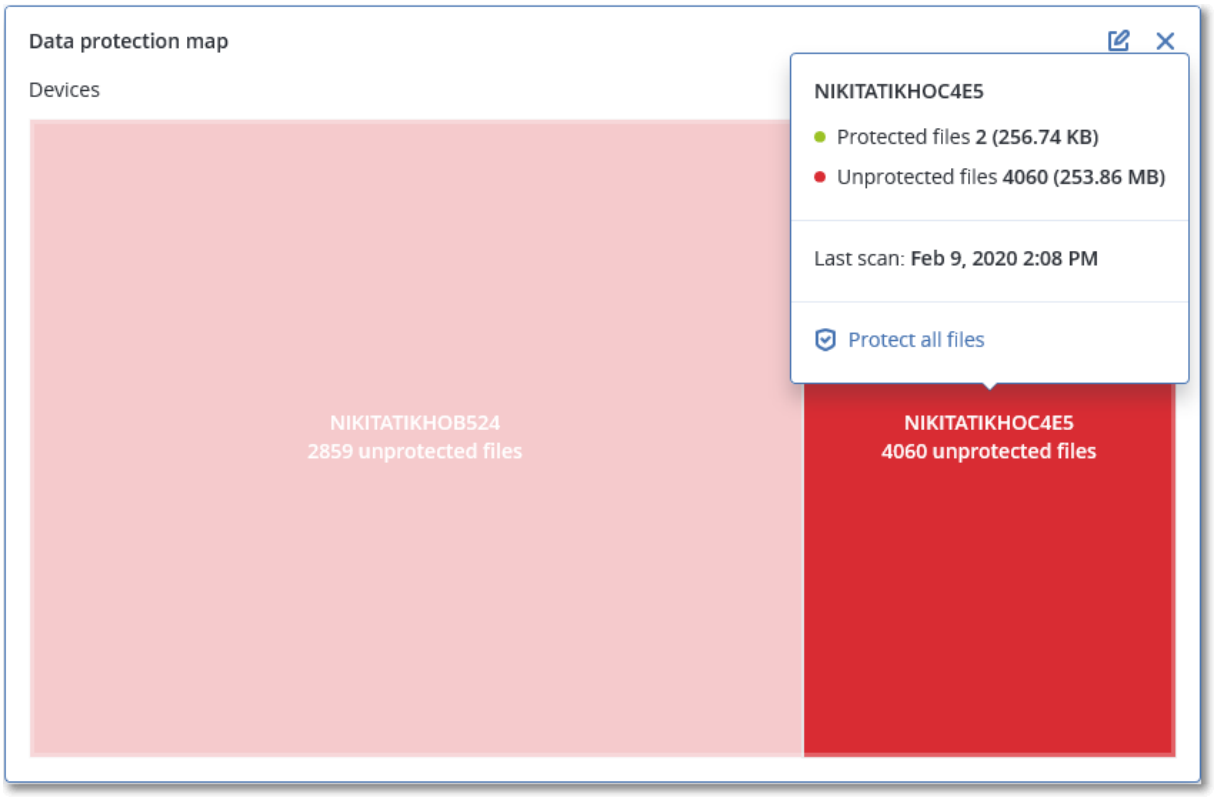
- **Critico** – è presente una percentuale compresa tra il 51 e il 100% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup per il tenant/il sistema/la posizione del cliente selezionato.
- **Basso** – è presente una percentuale compresa tra il 21 e il 50% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup per il tenant/il sistema/la posizione del cliente selezionato.
- **Medio** – è presente una percentuale compresa tra l'1 e il 20% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup per il tenant/il sistema/la posizione del cliente selezionato.
- **Elevato** – tutti i file con le estensioni specificate dall'utente sono protetti (viene eseguito il backup) per il tenant/il sistema/la posizione del cliente selezionato.

I risultati dell'analisi della protezione dati sono disponibili nel pannello di controllo del widget Mappa di protezione dati, una mappa ad albero dotata di due livelli di dettaglio, visualizzabili eseguendo il drill down:

- Livello del tenant cliente – mostra informazioni di riepilogo sullo stato di protezione dei file importanti dei clienti selezionati.



- Livello del sistema – mostra informazioni di riepilogo sullo stato di protezione dei file importanti dei clienti selezionati.



Per proteggere file che non sono protetti, passare il mouse sul blocco e fare clic su **Proteggi tutti i file**. Nella finestra di dialogo sono reperibili informazioni sul numero di file non protetti e sulla loro posizione. Per proteggerli, fare clic su **Proteggi tutti i file**.

È inoltre possibile scaricare un rapporto dettagliato in formato CSV.

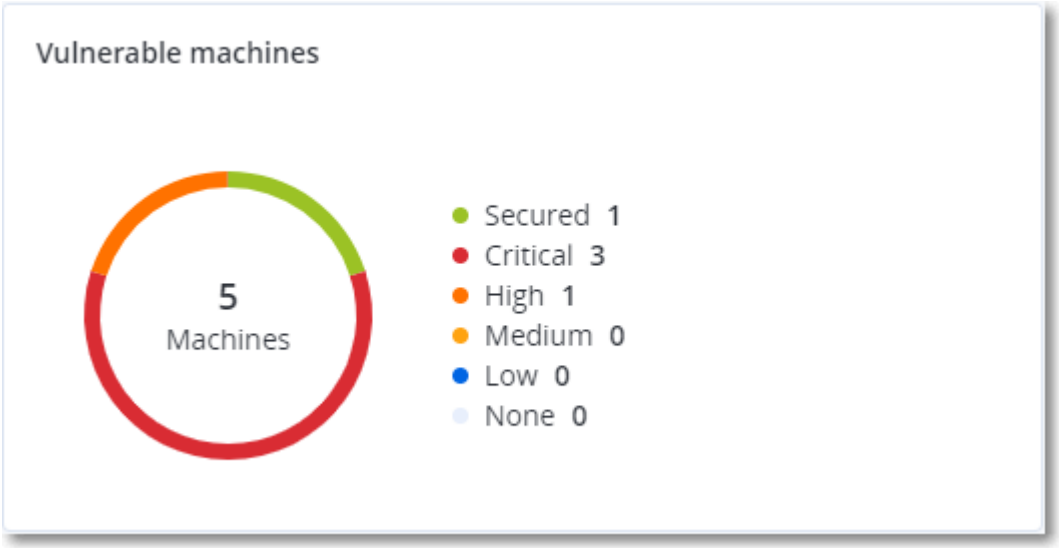
Widget di valutazione delle vulnerabilità

Sistemi vulnerabili

Questo widget mostra i sistemi vulnerabili ordinati in base alla gravità della vulnerabilità.

Conformemente al sistema CVSS (Common Vulnerability Scoring System) v3.0, la vulnerabilità individuata può presentare uno dei seguenti livelli di gravità:

- Protetto: non sono state individuate vulnerabilità
- Critico: 9.0 - 10.0 CVSS
- Elevato: 7.0 - 8.9 CVSS
- Medio: 4.0 - 6.9 CVSS
- Basso: 0.1 - 3.9 CVSS
- Nessuno: 0.0 CVSS



Vulnerabilità esistenti

Questo widget mostra le vulnerabilità attualmente esistenti sui sistemi. Nel widget **Vulnerabilità esistenti** sono presenti due colonne che mostrano gli indicatori data e ora:

- **Individuata per la prima volta** – la data e l'ora della prima individuazione della vulnerabilità nel sistema.
- **Individuata l'ultima volta** – la data e l'ora dell'ultima individuazione della vulnerabilità nel sistema.

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

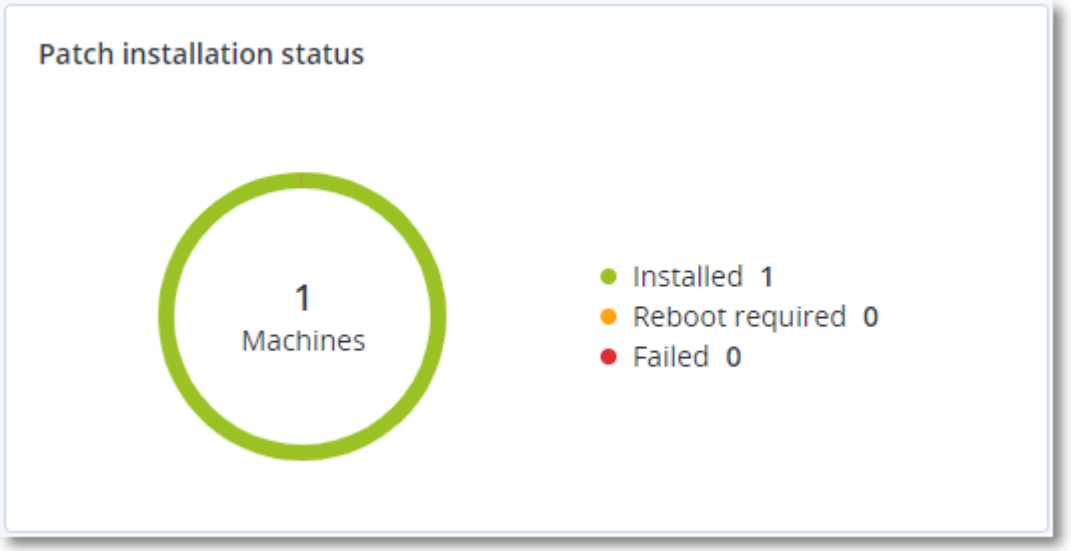
Widget di installazione patch

Sono disponibili quattro widget correlati alla funzionalità di gestione delle patch.

Stato di installazione patch

Questo widget mostra il numero di sistemi raggruppati in base allo stato di installazione delle patch.

- **Installate** – tutte le patch disponibili sono installate in un sistema
- **Riavvio necessario** – dopo l'installazione della patch, è richiesto il riavvio di un sistema
- **Non riuscita** – l'installazione di una patch non è riuscita in un sistema



Riepilogo di installazione patch

Questo widget mostra il riepilogo delle patch presenti nei sistemi, in base allo stato di installazione delle patch.

Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

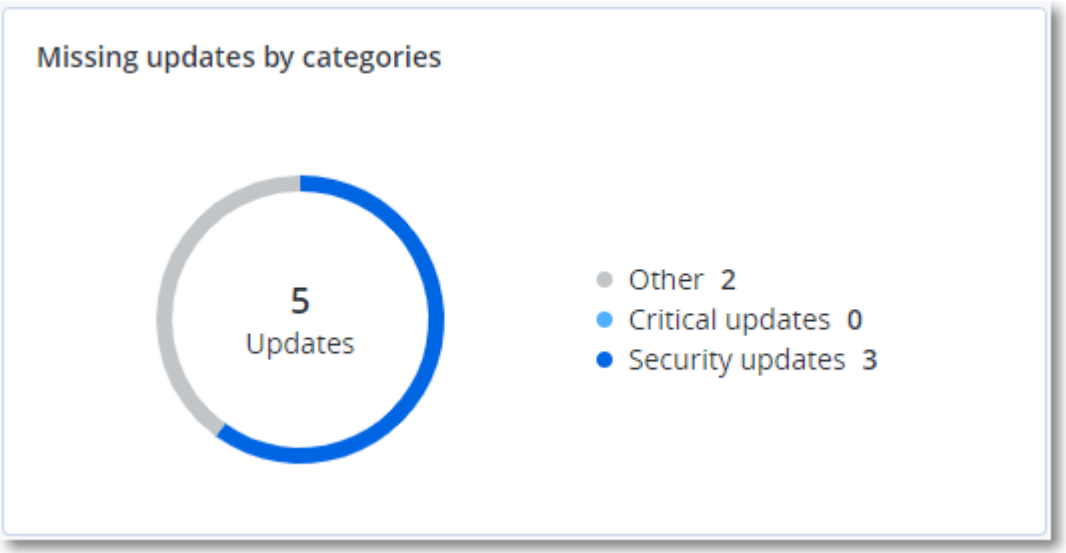
Cronologia di installazione patch

Questo widget mostra informazioni dettagliate sulle patch installate nei sistemi.

Aggiornamenti non effettuati per categorie

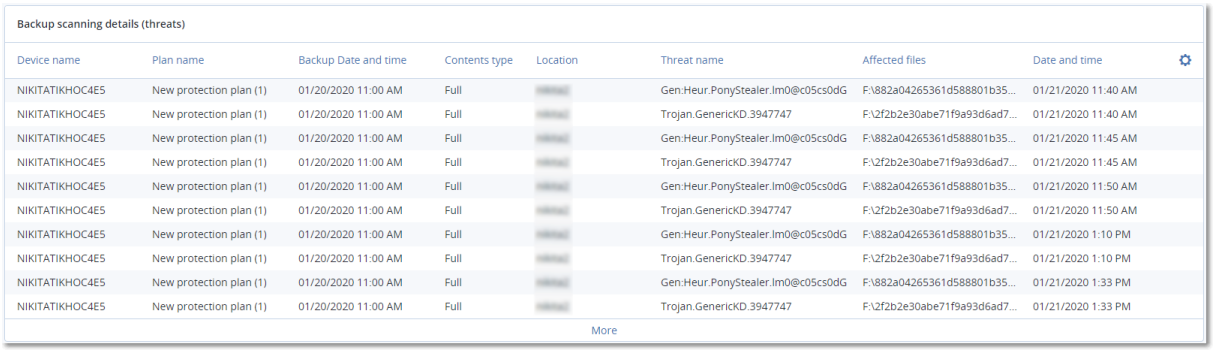
Questo widget mostra il numero di aggiornamenti non effettuati, per categoria. Vengono mostrate le seguenti categorie:

- Aggiornamenti di sicurezza
- Aggiornamenti critici
- Altro



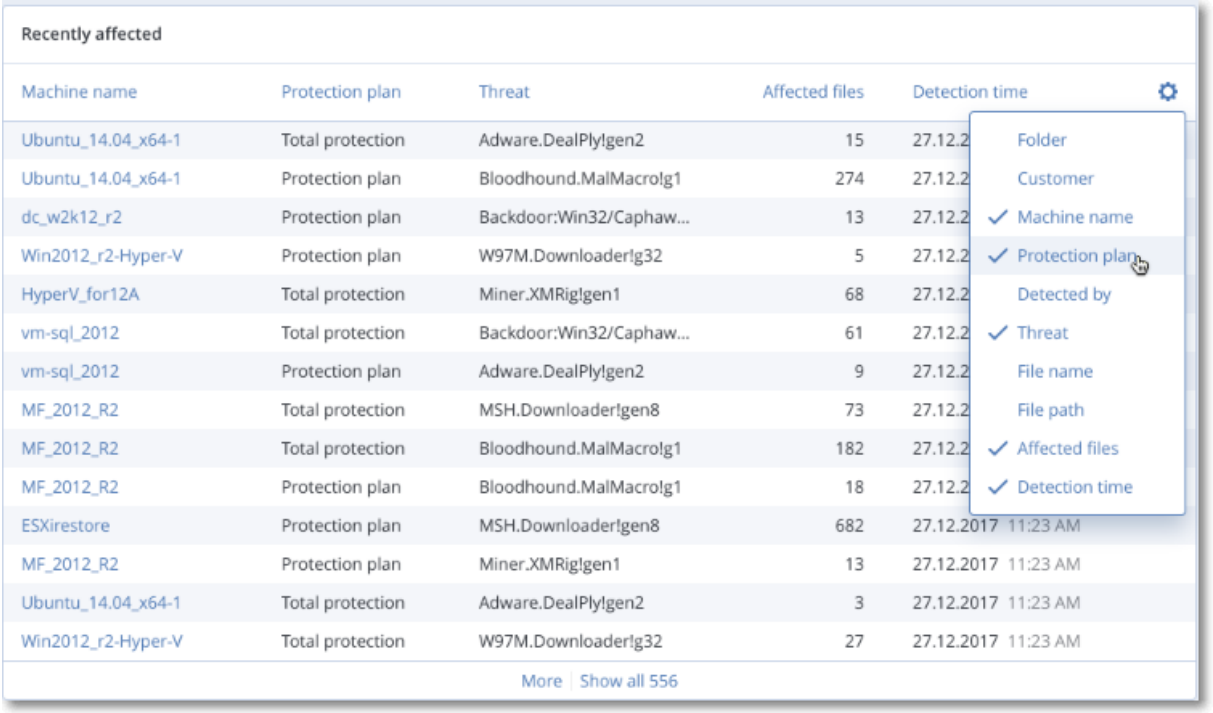
Informazioni sulla scansione del backup

Questo widget mostra informazioni dettagliate sulle minacce individuate nei backup.



Recentemente interessato

Questo widget mostra informazioni dettagliate sui workload recentemente interessati da minacce quali virus, malware e ramsomware. Lo strumento rende disponibili informazioni sulle minacce individuate, l'orario di individuazione e il numero di file infettati.



Download dei dati relativi ai workload recentemente interessati

È possibile scaricare i dati relativi ai workload recentemente interessati, generare un file CSV e inviarlo ai destinatari specificati.

Per scaricare i dati relativi ai workload recentemente interessati

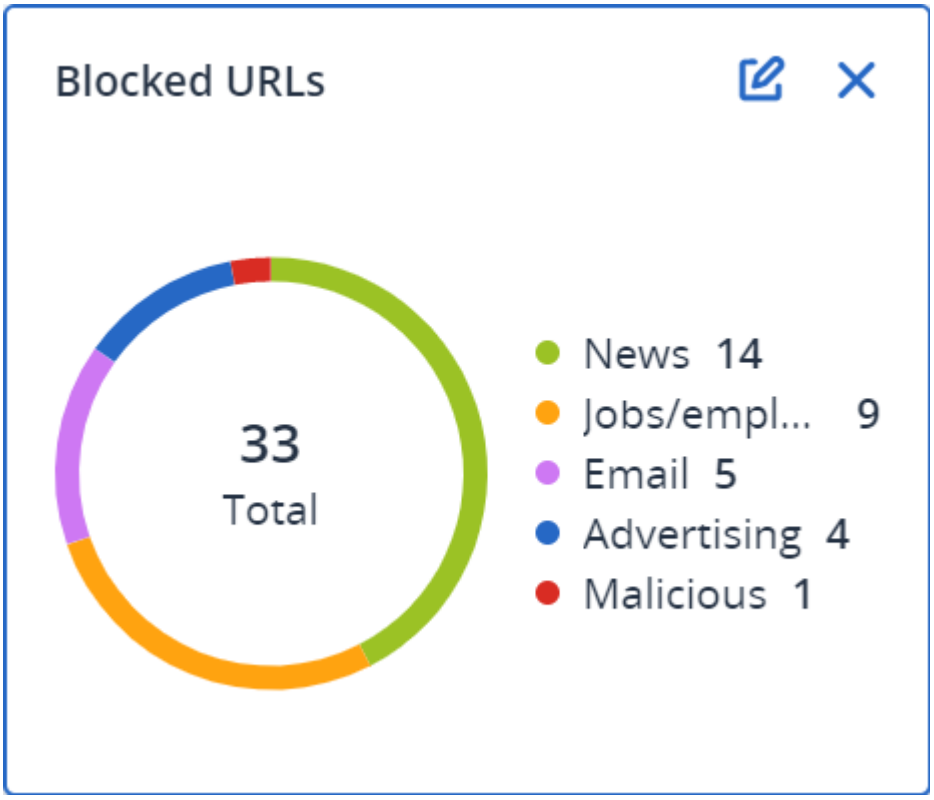
1. Nel widget **Recentemente interessati** fare clic su **Scarica dati**.
2. Nel campo **Periodo di tempo**, inserire il numero di giorni per i quali scaricare i dati. Il numero massimo di giorni che è possibile inserire è 200.
3. Nel campo **Destinatari**, immettere gli indirizzi e-mail di tutte le persone che riceveranno un'e-mail con il link per scaricare il file CSV.

4. Fare clic su **Download**.

   Il sistema avvia la generazione del file CSV contenente i dati relativi ai workload interessati per il periodo di tempo specificato. Una volta completato il file CSV, il sistema invia un'e-mail ai destinatari. Ogni destinatario potrà quindi scaricare il file CSV.

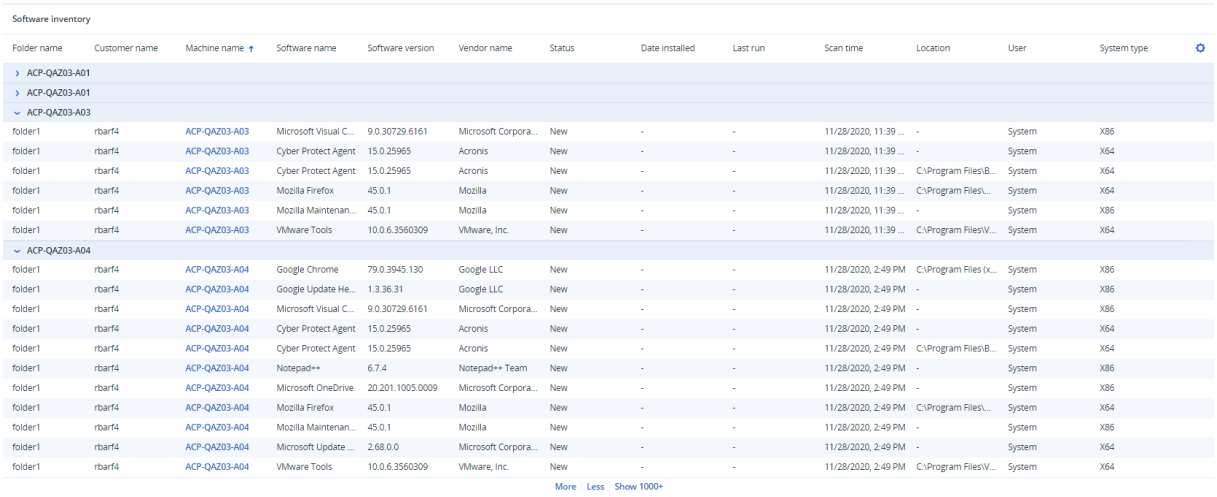
URL bloccati

Il widget mostra le statistiche degli URL bloccati per categoria. Per ulteriori informazioni sui filtri URL e la divisione in categorie, consultare il manuale utente del servizio Cyber Protection.

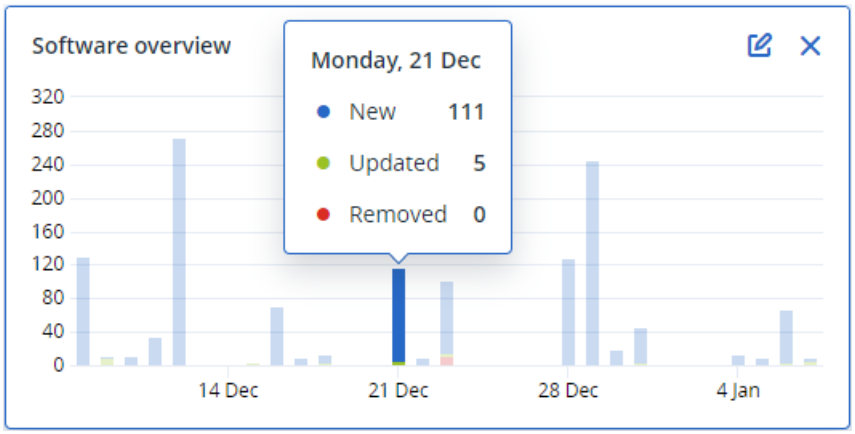


Widget Inventario software

Il widget di tabella **Inventario software** mostra informazioni dettagliate su tutti i componenti software installati nei sistemi Windows e macOS dell'organizzazione del cliente.



Il widget **Panoramica software** mostra il numero di applicazioni nuove, aggiornate ed eliminate sui sistemi Windows e macOS dell'organizzazione del cliente per il periodo di tempo specificato (7 giorni, 30 giorni o mese corrente).



Quando si passa il mouse su una determinata barra del grafico, viene visualizzato un suggerimento che mostra le informazioni seguenti:

Nuove - il numero di nuove applicazioni installate.

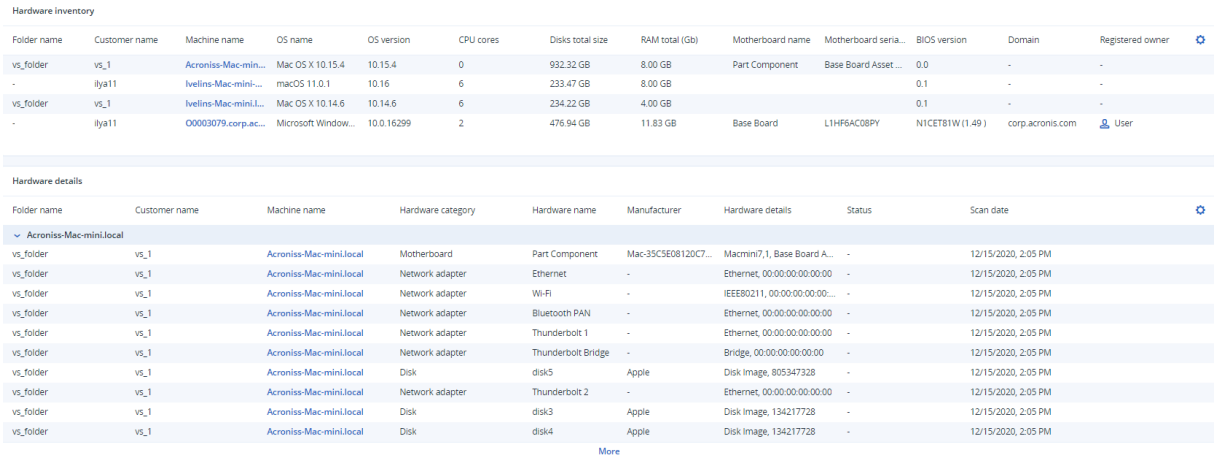
Aggiornate - il numero di applicazioni aggiornate.

Rimosse - il numero di applicazioni rimosse.

Facendo clic sulla parte di barra corrispondente a un determinato stato, viene visualizzata una finestra pop-up, che elenca tutti i clienti che hanno dispositivi con applicazioni nello stato selezionato nella data selezionata. Selezionando un cliente dall'elenco e quindi facendo clic su **Passa al cliente**, l'utente viene reindirizzato alla pagina **Gestione software** -> **Inventario software** nella console del servizio del cliente. Le informazioni presenti nella pagina sono filtrate in base alla data e allo stato corrispondenti.

Widget Inventario hardware

I widget di tabella **Inventario hardware** e **Informazioni hardware** mostrano informazioni su tutti i componenti hardware installati sui dispositivi Windows e macOS fisici e virtuali dell'organizzazione del cliente.



Hardware inventory

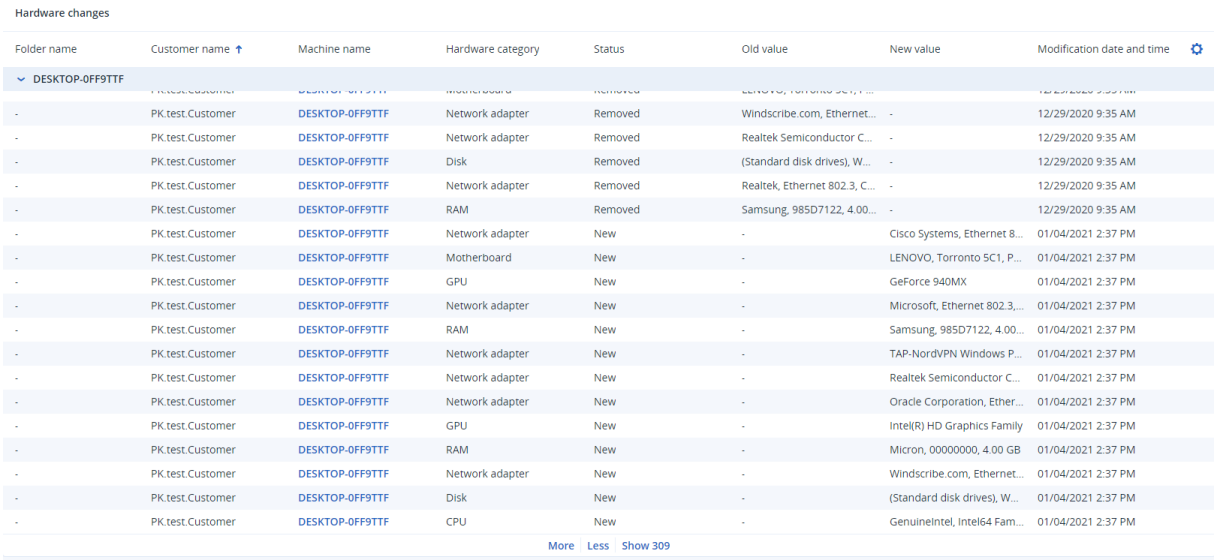
Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

More

Il widget di tabella **Modifiche hardware** mostra informazioni su tutti i componenti hardware aggiunti, eliminati e modificati sui sistemi Windows e macOS fisici e virtuali dell'organizzazione del cliente per il periodo di tempo specificato (7 giorni, 30 giorni o mese corrente).



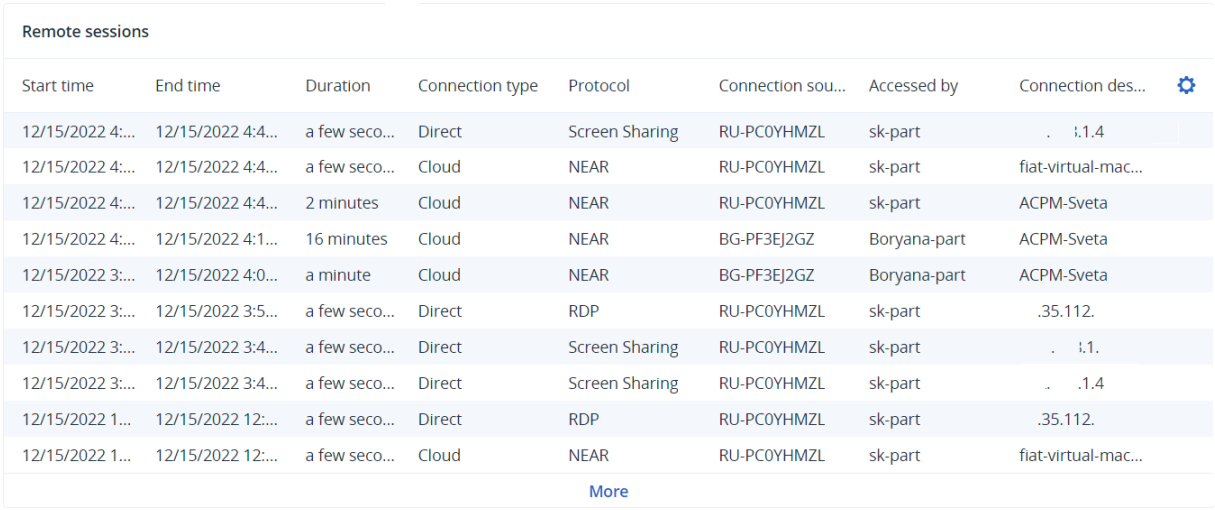
Hardware changes

Folder name	Customer name	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

More | Less | Show 309

Cronologia della sessione

Il widget mostra informazioni dettagliate sulle sessioni di desktop remoto e di trasferimento di file eseguite nell'organizzazione del cliente in un intervallo di tempo specificato.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

Elaborazione di rapporti

Per creare i report sull'utilizzo dei servizi e sulle operazioni, fare clic su **Report**.

Utilizzo

I report sull'utilizzo forniscono dati cronologici relativi all'utilizzo dei servizi. I report di utilizzo sono disponibili nei formati CSV e HTML.

Tipo di rapporto

È possibile selezionare uno dei seguenti tipi di report:

- **Utilizzo corrente**

  Il rapporto contiene le metriche di utilizzo correnti del servizio.

  Le statistiche di utilizzo sono calcolate per ciascuno dei periodi di fatturazione dei tenant figlio. Se i tenant inclusi nel report presentano periodi di fatturazione differenti, l'utilizzo del tenant padre può essere differente dalla somma degli utilizzi dei tenant figlio.
- **Distribuzione utilizzo corrente**

  Questo report è disponibile solo per i tenant parent gestiti da un sistema di provisioning esterno. Questo rapporto è utile quando i periodi di fatturazione dei tenant figlio non corrispondono al periodo di fatturazione del tenant parent. Il rapporto contiene le metriche di utilizzo del servizio relative ai tenant figlio calcolate nel periodo di fatturazione corrente del tenant parent. L'utilizzo del tenant parent deve essere uguale alla somma degli utilizzi dei tenant figlio.
- **Riepilogo per il periodo**

  Il rapporto contiene le metriche di utilizzo del servizio relative al termine del periodo specificato e la differenza tra le metriche all'inizio e alla fine del periodo specificato.
- **Giorno per giorno per il periodo**

  Il rapporto contiene le metriche di utilizzo correnti del servizio e le relative modifiche per ogni giorno del periodo specificato.

Ambito del report

È possibile selezionare l'ambito del report tra i seguenti valori:

- **Tutti i clienti e i partner diretti**
  Il report conterrà le statistiche di utilizzo del servizio relative solo ai tenant figlio diretti del tenant nel quale si sta lavorando.
- **Tutti i clienti e i partner**
  Il report conterrà le statistiche di utilizzo del servizio relative a tutti i tenant figlio del tenant nel quale si sta lavorando.
- **Tutti i clienti e i partner (includendo i dettagli utente)**
  Il report conterrà le statistiche di utilizzo del servizio relative a tutti i tenant figlio del tenant nel quale si sta lavorando e di tutti gli utenti inclusi nel tenant.

Metriche con utilizzo pari a zero

È possibile ridurre il numero di righe contenute nel report mostrando informazioni sulle metriche che hanno un utilizzo diverso da zero e nascondendo quelle con un utilizzo pari a zero.

Configurazione di report di utilizzo pianificati

Un report pianificato fornisce le statistiche di utilizzo del servizio per l'ultimo mese di calendario. I report sono generati alle ore 23:59:59 del fuso orario UTC il primo giorno del mese e vengono inviati il secondo giorno dello stesso mese. I report vengono inviati a tutti gli amministratori del tenant che hanno selezionato la casella **Report di utilizzo pianificati** nelle impostazioni utente.

Per abilitare o disabilitare un report pianificato

1. Accedere al portale di gestione.
2. Assicurarsi di operare nel primo tenant di livello superiore disponibile.
3. Fare clic su **Report** > **Utilizzo**.
4. Fare clic su **Pianificati**.
5. Selezionare o deselezionare la casella di controllo **Invia un report di riepilogo mensile** del report.
6. In **Livello di dettaglio**, selezionare l'ambito del report.
7. [Facoltativo] Selezionare **Nascondi metriche con utilizzo pari a zero** per escludere dal report le metriche con utilizzo pari a zero.

Configurazione di report di utilizzo personalizzati

Questo tipo di report può essere generato a richiesta e non può essere pianificato. Il report verrà inviato all'indirizzo e-mail dell'utente.

Per generare un report personalizzato

1. Accedere al portale di gestione.
2. Passare al tenant per il quale si desidera creare un report.
3. Fare clic su **Report** > **Utilizzo**.
4. Selezionare la scheda **Personalizzato**.
5. In **Tipo**, selezionare il tipo di report come descritto sopra:
6. [Non disponibile per il tipo di report **Utilizzo corrente**] In **Periodo**, selezionare il periodo di report:
   - **Mese di calendario corrente**
   - **Mese di calendario precedente**
   - **Personalizzato**
7. [Non disponibile per il tipo di report **Utilizzo corrente**] Se si desidera specificare un periodo di report personalizzato, selezionare le date di inizio e di fine. Altrimenti, ignorare questo passaggio.
8. In **Livello di dettaglio** selezionare l'ambito del report come descritto sopra.
9. [Facoltativo] Selezionare **Nascondi metriche con utilizzo pari a zero** per escludere dal report le metriche con utilizzo pari a zero.
10. Per generare il report, fare clic su **Genera e invia**.

Report Operazioni

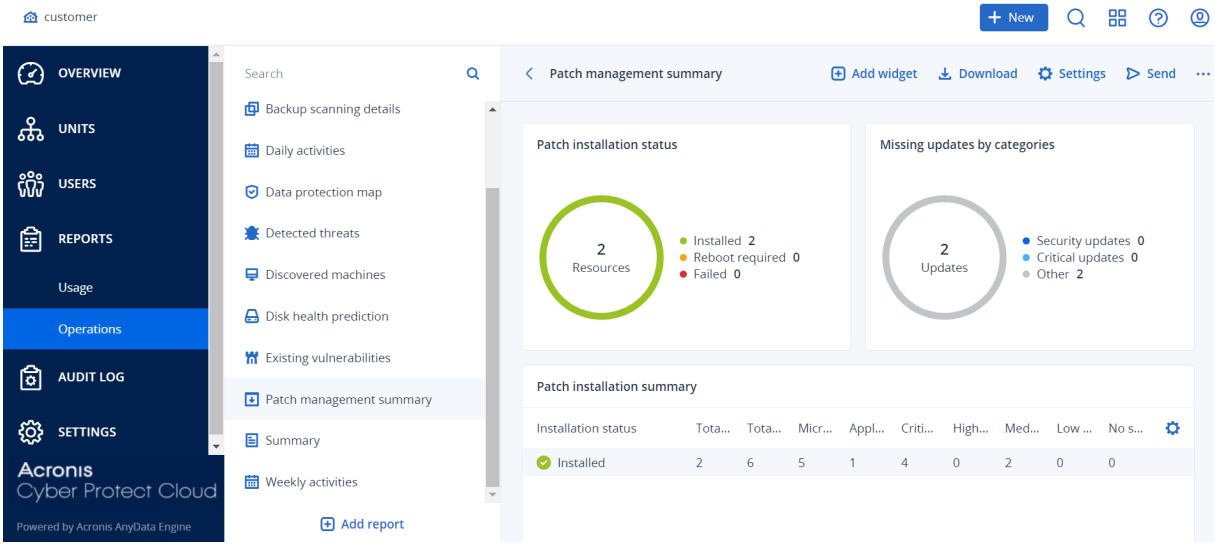
Un report relativo alle operazioni può includere qualsiasi insieme di widget del pannello di controllo **Operazioni**. Per impostazione predefinita, tutti i widget mostrano le informazioni di riepilogo per il tenant in cui si sta operando. È possibile cambiare il tenant visualizzato per ogni widget modificandolo, o per tutti i widget nelle impostazioni del report.

A seconda del tipo di widget, il report include i dati relativi a un intervallo di tempo o al momento in cui il report è stato esplorato o generato. Vedere "Dati inseriti nel report in base al tipo di widget" (pag. 120).

Tutti i widget cronologici mostrano i dati per lo stesso intervallo di tempo. È possibile modificare questo intervallo nelle impostazioni del report.

È possibile utilizzare i report predefiniti o crearne uno personalizzato.

È possibile scaricare un report sulle operazioni o inviarlo via e-mail in formato Excel (XLSX) o PDF.



I report predefiniti sono elencati di seguito:

Nome report	Descrizione
#CyberFit Score per sistema	Mostra il #CyberFit Score, basato sulla valutazione delle metriche di sicurezza e delle configurazioni per ogni sistema, nonché i miglioramenti consigliati.
Avvisi	Mostra gli avvisi generati durante un periodo di tempo specificato.
Informazioni sulla scansione del backup	Mostra informazioni dettagliate sulle minacce individuate nei backup.
Attività giornaliere	Mostra informazioni di riepilogo sulle attività eseguite durante un periodo di tempo specificato.
Mappa di protezione dati	Mostra informazioni dettagliate su numero, dimensione, posizione, stato della protezione di tutti i file importanti sui sistemi.
Minacce rilevate	Mostra informazioni relative ai sistemi interessati per numero di minacce bloccate e di sistemi integri e vulnerabili.
Macchine individuate	Mostra tutti i sistemi individuati nella rete dell'organizzazione.
Previsione dell'integrità del disco	Mostra le previsioni circa i guasti di HDD/SSD e lo stato attuale dei dischi.
Vulnerabilità esistenti	Mostra le vulnerabilità esistenti per i sistemi operativi e le applicazioni dell'organizzazione. Visualizza inoltre le informazioni sui sistemi interessati nella rete per ogni prodotto in elenco.
Riepilogo di gestione patch	Mostra il numero di patch mancanti, patch installate e patch applicabili. È possibile esplorare i report per ottenere le informazioni sulle patch installate e/o mancanti e ulteriori dettagli su tutti i sistemi.

Riepilogo	Mostra informazioni di riepilogo sui dispositivi protetti per un periodo di tempo specificato.
Attività settimanali	Mostra informazioni di riepilogo sulle attività eseguite durante un periodo di tempo specificato.
Inventario software	Mostra informazioni dettagliate su tutti i componenti software installati nei sistemi Windows e macOS dell'organizzazione del cliente.
Inventario hardware	Mostra informazioni dettagliate su tutti i componenti hardware disponibili nei sistemi Windows e macOS fisici e virtuali dell'organizzazione del cliente.
Sessioni remote	Mostra informazioni dettagliate sulle sessioni di desktop remoto e di trasferimento di file eseguite nell'organizzazione del cliente in un intervallo di tempo specificato.

Per visualizzare un report, fare clic sul relativo nome.

Per accedere alle operazioni in un report, fare clic sull'icona dei puntini di sospensione verticali nella riga del report. Le stesse operazioni sono disponibili anche all'interno del report.

Aggiunta di un report

1. Fare clic su **Aggiungi report**.
2. Eseguire una delle seguenti operazioni:
   - Per aggiungere un report predefinito, fare clic sul relativo nome.
   - Per aggiungere un report personalizzato, fare clic su **Personalizzato**, quindi sul nome del report (i nomi assegnati per impostazione predefinita vengono visualizzati come **Personalizzato(1)**), e quindi aggiungere i widget al report.
3. [Facoltativo] Trascinare e rilasciare i widget per riorganizzarli.
4. [Facoltativo] Modificare il report come descritto di seguito.

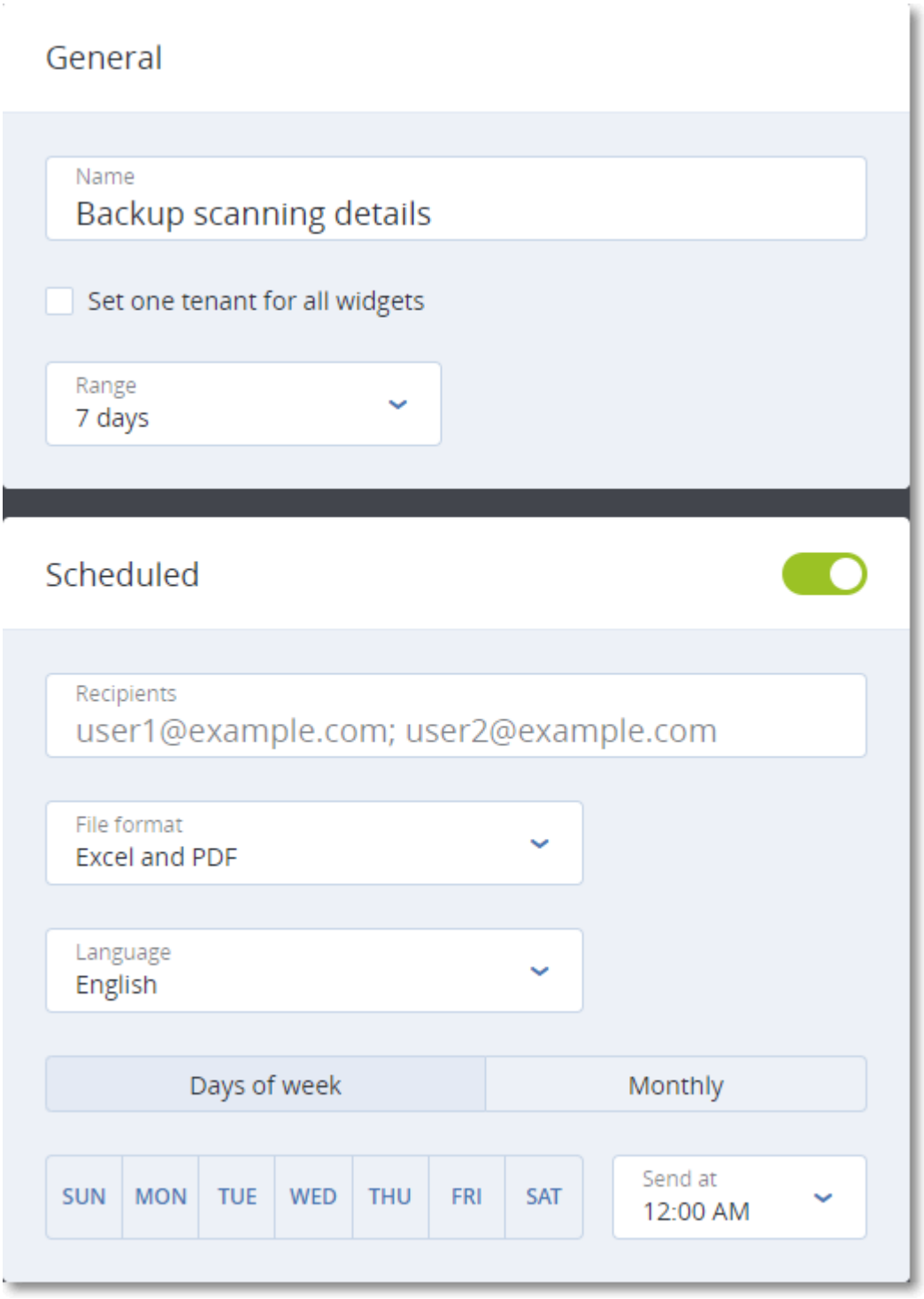
Modifica delle impostazioni del report

Per modificare un report, selezionare il relativo nome e quindi fare clic su **Impostazioni**. Quando si modifica un report, è possibile:

- Rinominare il report
- Modificare il widget visualizzato di tutti i widget inclusi nel report

  Se sono presenti tenant figlio, all'utente è disponibile l'opzione **Impostare un tenant per tutti i widget**. Tale opzione consente di filtrare i dati in tutti i widget del report in base al tenant selezionato. Se l'opzione non è selezionata, i widget mostreranno i dati di tutti i tenant figlio del tenant corrente.

- Modificare l'intervallo di tempo di tutti i widget inclusi nel report
- Pianificare l'invio del report tramite e-mail in formato PDF e/o Excel.



Pianificazione di un report

1. Fare clic sul nome del report, quindi su **Impostazioni**.
2. Attivare il commutatore **Pianificato**.

3. Specificare gli indirizzi e-mail dei destinatari.
4. Selezionare il formato di report: PDF, Excel o entrambi.
5. Selezionare i giorni e l'ora in cui il report verrà inviato.
6. Fare clic su **Salva** nell'angolo in alto a destra.

Esportazione e importazione della struttura del report

È possibile esportare e importare la struttura del report (l'insieme di widget e le impostazioni del report) in e da un file JSON. Questa operazione può rivelarsi utile per copiare la struttura del report da un tenant a un altro.

Per esportare la struttura del report, selezionare il nome del report, quindi fare clic sull'icona dei puntini di sospensione in verticale nell'angolo in alto a destra e quindi su **Esporta**.

Per importare la struttura del report, selezionare **Aggiungi report**, quindi fare clic su **Importa**.

Download di un report

Per eseguire il download di un report, fare clic su **Scarica** e selezionare i formati richiesti:

- Excel e PDF
- Excel
- PDF

Dumping dei dati del report

È possibile inviare un dump dei dati del report in un file CSV tramite e-mail. Il dump include tutti i dati del report (senza filtri) per un intervallo di tempo personalizzato. Gli indicatori data e ora nei report CSV sono indicati nel formato UTC mentre nei report Excel e PDF sono indicati nel fuso orario del sistema in uso.

Il software genera il dump dei dati al volo. Se si specifica un periodo prolungato, questa azione potrebbe richiedere molto tempo.

Per effettuare il dumping dei dati del report

1. Fare clic sul nome del report.
2. Fare clic sull'icona dei puntini di sospensione in verticale nell'angolo in alto a destra, quindi fare clic su **Dump dati**.
3. Specificare gli indirizzi e-mail dei destinatari.
4. In **Intervallo di tempo** specificare l'intervallo di tempo.
5. Fare clic su **Invia**.

Riepilogo esecutivo

Il report Riepilogo esecutivo offre una panoramica dello stato della protezione degli ambienti e dei dispositivi protetti dei clienti, per un intervallo di date specificato.

Il report Riepilogo esecutivo include sezioni con widget dinamici che mostrano le metriche prestazionali chiave relative all'utilizzo da parte dei clienti dei seguenti servizi cloud: Backup, Protezione antimalware, Vulnerability assessment, Patch management, Prevenzione della perdita di dati, Notary, Disaster Recovery, Files Sync & Share.

È possibile personalizzare il report in diversi modi.

- Aggiungere o eliminare sezioni.
- Modificare l'ordine delle sezioni.
- Rinominare le sezioni.
- Spostare i widget da una sezione a un'altra.
- Modificare l'ordine dei widget in ogni sezione.
- Aggiungere o rimuovere widget.
- Personalizzare i widget.

È possibile generare i report Riepilogo esecutivo in formato PDF ed Excel, e quindi inviarli alle parti interessate o ai titolari delle organizzazioni dei clienti, in modo che possano visualizzare con facilità il valore tecnico e aziendale dei servizi forniti.

Gli amministratori dei partner possono generare e inviare i report Riepilogo esecutivo solo ai clienti diretti. In presenza di una gerarchia di tenant più complessa che prevede partner secondari, saranno i partner secondari a dover generare il report.

Widget del report Riepilogo esecutivo

È possibile aggiungere o rimuovere sezioni e widget dal report Riepilogo esecutivo in modo da controllare le informazioni da includervi.

Widget Panoramica dei workload

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Panoramica dei workload**.

Widget	Descrizione
Stato della protezione dei workload cloud	Questo widget mostra il numero di workload cloud protetti e non protetti per tipo al momento della generazione del report. È considerato protetto un workload cloud al quale è applicato almeno un piano di backup. È considerato non protetto un workload cloud al quale non è applicato alcun piano di backup. Nel diagramma sono mostrati i tipi di workload cloud elencati di seguito (in ordine alfabetico dalla A alla Z):

Widget	Descrizione
	• Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Caselle di posta di Exchange ospitato • Caselle di posta di Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Siti Web Per alcuni tipi di workload, vengono utilizzati i seguenti gruppi di workload: • Microsoft 365: Utenti, Gruppi, Cartelle pubbliche, Team e Raccolte di siti • Google Workspace: Utenti e unità condivise • Exchange ospitato: Utenti Se in un gruppo di workload sono presenti più di 10.000 workload, il widget non mostra alcun dato per i workload corrispondenti. Se, ad esempio, il cliente dispone di un account di Microsoft 365 con 10.000 caselle di posta e di un servizio OneDrive per 500 utenti, tutti appartengono al gruppo dei workload utente. La somma di questi workload è pari a 10.500, che supera il limite di 10.000 unità per un gruppo di workload. Pertanto, il widget nasconderà i tipi di workload corrispondenti: Caselle di posta di Microsoft 365 e Microsoft 365 OneDrive.
Riepilogo di Cyber Protection	Questo widget mostra le metriche principali delle prestazioni di Cyber Protection per il periodo di tempo specificato. **Dati di cui è stato eseguito il backup** - Dimensione totale degli archivi creati negli storage cloud e locale. **Minacce mitigate** - Il numero totale di malware bloccati su tutti i dispositivi. **URL dannosi bloccati**- Il numero totale di URL bloccati su tutti i dispositivi. **Vulnerabilità con patch applicate** - Il numero totale di vulnerabilità corrette tramite l'installazione di patch software su tutti i dispositivi. **Patch installate**- Il numero totale di patch installate su tutti i dispositivi. **Server protetti da Disaster Recovery** - Il numero totale dei server protetti da Disaster Recovery. **Utenti di File Sync & Share** - Il numero totale di utenti e di utenti guest che utilizzano Cyber Files. **File autenticati** - Il numero totale di file autenticati. **Documenti con firma elettronica** - Il numero totale di documenti con firma elettronica.

Widget	Descrizione
	Dispositivi periferici bloccati - Il numero totale di dispositivi periferici bloccati.
Stato della rete dei workload	Questo widget mostra il numero di workload isolati e di quelli connessi (questo è lo stato normale dei workload). Selezionare il cliente di interesse; la vista del workload visualizzata viene filtrata per mostrare i workload isolati. Fare clic sul valore Connesso per visualizzare l'elenco Workload con agenti filtrato per mostrare i workload connessi (per il cliente selezionato).
Stato di protezione dei workload	Il widget mostra i workload protetti e non protetti per tipo al momento della generazione del report. È considerato protetto un workload al quale è applicato almeno un piano di backup o di protezione. Un workload non protetto è un workload al quale non è applicato alcun piano di backup o di protezione. Vengono calcolati i seguenti workload: **Server** - Server fisici e server Controller di dominio. **Workstation** - Workstation fisiche. **Virtual machine** - Virtual machine con e senza agente. **Server di web hosting** - Server virtuali o fisici sui quali è installato cPanel o Plesk. **Dispositivi mobili** - Dispositivi mobile fisici. Un workload può appartenere a più di una categoria. Ad esempio, un server di web hosting viene conteggiato in due categorie - **Server** e **Server di web hosting**.
Stato della protezione dei workload cloud	**Stato della protezione dei workload cloud** Il widget mostra il numero di workload cloud protetti e non protetti per tipo al momento della generazione del report. È considerato protetto un workload cloud al quale è applicato almeno un piano di backup. È considerato non protetto un workload cloud al quale non è applicato alcun piano di backup. Nel diagramma sono mostrati i tipi di workload cloud elencati di seguito (in ordine alfabetico dalla A alla Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Caselle di posta di Exchange ospitato • Caselle di posta di Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Siti Web Per alcuni tipi di workload, vengono utilizzati i seguenti gruppi di workload:

Widget	Descrizione
	• Microsoft 365: Utenti, Gruppi, Cartelle pubbliche, Team e Raccolte di siti • Google Workspace: Utenti e unità condivise • Exchange ospitato: Utenti Se in un gruppo di workload sono presenti più di 10.000 workload, il widget non mostra alcun dato per i workload corrispondenti. Se, ad esempio, il cliente dispone di un account di Microsoft 365 con 10.000 caselle di posta e di un servizio OneDrive per 500 utenti, tutti appartengono al gruppo dei workload utente. La somma di questi workload è pari a 10.500, che supera il limite di 10.000 unità per un gruppo di workload. Pertanto, il widget nasconderà i tipi di workload corrispondenti: Caselle di posta di Microsoft 365 e Microsoft 365 OneDrive.

Widget di Protezione antimalware

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Difesa dalle minacce**.

Widget	Descrizione
Scansione antimalware dei file	Il widget mostra i risultati della scansione antimalware su richiesta effettuata sui dispositivi, per l'intervallo di date specificato. **File** - Il numero totale di file scansionati **Pulito** - Il numero totale di file puliti **Rilevato, in quarantena** - Il numero totale di file infetti messi in quarantena **Rilevato, non in quarantena** - Il numero totale di file infetti non messi in quarantena **Dispositivi protetti** - Il numero totale di dispositivi ai quali è applicata una policy di protezione antimalware **Numero totale di dispositivi registrati** - Il numero totale di dispositivi registrati al momento della generazione del report
Scansione antimalware dei backup	Il widget mostra i risultati della scansione antimalware effettuata sui backup, per l'intervallo di date specificato, utilizzando le metriche seguenti: • Numero totale di punti di ripristino scansionati • Numero di punti di ripristino puliti • Numero di punti di ripristino puliti con partizioni non supportate • Numero di punti di ripristino infetti. Questa metrica include il numero di punti di ripristino infetti con partizioni non supportate.
URL bloccati	Il widget mostra il numero di URL bloccati, raggruppati per categoria di sito web, per l'intervallo di date specificato. Il widget elenca le sette categorie di siti web che presentano il numero più

Widget	Descrizione
	elevato di URL bloccati, e combina le categorie di siti web rimanenti nella voce **Altro**. Per ulteriori informazioni sulle categorie di siti web, consultare l'argomento relativo al filtraggio degli URL in Cyber Protection.
Burndown dei problemi di sicurezza	Questo widget indica il tasso di efficienza nella risoluzione dei problemi di sicurezza per l'azienda selezionata; il numero di problemi aperti viene misurato a fronte del numero di problemi chiusi in un determinato periodo di tempo. Passare il mouse su una colonna per visualizzare in dettaglio i problemi chiusi o aperti per il giorno selezionato. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.
MTTR del problema	Questo widget mostra il tempo medio di risoluzione dei problemi di sicurezza. Indica la rapidità con la quale i problemi vengono analizzati e risolti. Fare clic su una colonna per visualizzare in dettaglio i problemi in base al livello di gravità (**Critica**, **Elevata** e **Media**) e un'indicazione del tempo impiegato per risolverli in base ai diversi livelli di gravità. Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.
Stato minaccia	Questo widget mostra lo stato corrente della minaccia per i workload dell'azienda (indipendentemente dal numero dei workload); evidenzia il numero attuale di problemi non mitigati che devono essere analizzati. Il widget indica anche il numero di problemi mitigati (manualmente e/o automaticamente dal sistema).
Minacce rilevate per tecnologia di protezione	Per l'intervallo di date specificato, il widget mostra il numero di minacce rilevate, raggruppate in base alle tecnologie di protezione seguenti: • Scansione antimalware • Motore comportamentale • Protezione dal mining di criptovalute • Prevenzione degli exploit • Protezione attiva contro il ransomware • Protezione in tempo reale • Filtro URL

Widget di Backup

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Backup**.

Widget	Descrizione
Workload con backup eseguito	Il widget mostra il numero totale dei workload registrati per stato di backup. **Backup eseguito** - Numero di workload di cui è stato eseguito il backup (con almeno un backup riuscito) durante l'intervallo di date del report. **Backup non eseguito** - Numero di workload di cui non è stato eseguito il backup (senza alcun backup riuscito) durante l'intervallo di date del report.
Stato integrità del disco per dispositivo fisici	Il widget mostra lo stato di integrità complessivo dei dispositivi fisici in base agli stati di integrità dei rispettivi dischi. **OK** - Questo stato di integrità del disco è correlato ai valori [70-100]. Lo stato del dispositivo corrisponde a **OK** quando tutti i relativi dischi sono nello stato **OK**. **Attenzione** - Questo stato di integrità del disco è correlato ai valori [30-70]. Lo stato del dispositivo corrisponde a **Attenzione** quando lo stato di almeno uno dei suoi dispositivi corrisponde a **Attenzione** e quando non sono presenti dischi nello stato **Errore**. **Errore** - Questo stato di integrità del disco è correlato ai valori [0-30]. Lo stato del dispositivo corrisponde a **Errore** quando lo stato di almeno uno dei suoi dispositivi corrisponde a **Errore**. **Calcolo dei dati del disco** - Lo stato del dispositivo corrisponde a **Calcolo dei dati del disco** quando gli stati dei relativi dischi non sono ancora stati calcolati.
Utilizzo dell'archivio di backup	Per l'intervallo di date specificato, il widget mostra il numero totale e la dimensione totale dei backup archiviati nel cloud e in locale.

Widget Valutazione della vulnerabilità e gestione patch

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Valutazione della vulnerabilità e gestione patch**.

Widget	Descrizione
Vulnerabilità con patch applicate	Il widget mostra i risultati delle prestazioni di valutazione delle vulnerabilità per l'intervallo di date specificato. **Totale**- Il numero totale di vulnerabilità con patch applicate. **Vulnerabilità del software Microsoft** - Il numero totale di vulnerabilità di Microsoft corrette su tutti i dispositivi Windows. **Vulnerabilità del software Windows di terze parti** - Il numero totale di vulnerabilità del software Windows di terze parti corrette, su tutti i dispositivi Windows. **Workload scansionati** - Il numero totale di dispositivi analizzati alla ricerca

Widget	Descrizione
	di vulnerabilità almeno una volta durante l'intervallo di date specificato.
Patch installate	Il widget mostra i risultati delle prestazioni della gestione delle patch per l'intervallo di date specificato. **Installate**- Il numero totale di patch applicate installate su tutti i dispositivi. **Patch del software Microsoft**- Il numero totale di patch del software Microsoft installate su tutti i dispositivi Windows. **Patch del software Windows di terze parti**- Il numero totale di patch del software Windows di terze parti installate su tutti i dispositivi Windows. **Workload con patch applicata** - Il numero totale di dispositivi con patch applicata (almeno una patch installata durante l'intervallo di date specificato).

Widget di Disaster Recovery

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Disaster Recovery**.

Widget	Descrizione
Statistiche di Disaster Recovery	Il widget mostra le metriche KPI di Disaster Recovery per l'intervallo di date specificato. **Failover di produzione** - Il numero di operazioni di failover di produzione per l'intervallo di tempo specificato. **Failover di prova** - Il numero di operazioni di failover di prova eseguite durante l'intervallo di tempo specificato. **Server primari** - Il numero totale di server primari al momento della generazione del report. **Server di ripristino** - Il numero totale di server di ripristino al momento della generazione del report. **IP pubblici** - Il numero totale di indirizzi IP pubblici al momento della generazione del report. **Punti di calcolo totali consumati** - Il numero totale di punti di calcolo consumati durante l'intervallo di tempo specificato.
Server di Disaster Recovery testati	Il widget mostra informazioni sui server protetti da Disaster Recovery e testati tramite failover di prova. Il widget mostra le metriche seguenti: **Server di ripristino** - Il numero totale di server protetti da Disaster Recovery (server dotati di almeno un server di ripristino) al momento della generazione del report.

Widget	Descrizione
	Testati - Il numero di server protetti da Disaster Recovery che sono stati testati usando il failover di prova durante l'intervallo di tempo selezionato, sul totale dei server protetti da Disaster Recovery. **Non testati** - Il numero di server protetti da Disaster Recovery che non sono stati testati usando il failover di prova durante l'intervallo di tempo selezionato, sul totale dei server protetti da Disaster Recovery. Il widget mostra anche la dimensione dello storage di Disaster Recovery (in GB) al momento della generazione del report. È la somma delle dimensioni di backup dei server cloud.
Server protetti con Disaster Recovery	Il widget mostra informazioni sui server protetti da Disaster Recovery e sui server non protetti. Il widget mostra le metriche seguenti: Il numero totale di server registrati nel tenant cliente al momento della generazione del report. **Protetti** - Il numero di server protetti da Disaster Recovery (server dotati di almeno un server di ripristino e di un backup del server completo), sul totale di tutti i server registrati al momento della generazione del report. **Non protetti** - Il numero totale di server non protetti, sul totale di tutti i server registrati al momento della generazione del report.

Widget Prevenzione della perdita di dati

L'argomento seguente fornisce maggiori informazioni sulle periferiche bloccate nella sezione **Prevenzione della perdita di dati**.

Il widget mostra il numero totale di dispositivi bloccati e il numero totale di dispositivi bloccati per tipo di dispositivo e per l'intervallo di date specificato.

- Archivio rimovibile
- Rimovibile crittografato
- Stampanti
- Appunti - Include i tipi di dispositivo per gli appunti e l'acquisizione di screenshot.
- Dispositivi mobili
- Bluetooth
- Unità ottiche
- Unità floppy
- USB - Include i tipi di dispositivo Porta USB e Porta USB reindirizzata.
- FireWire

- Unità mappate
- Appunti reindirizzati - Include i tipi di dispositivi Appunti reindirizzati in entrata e Appunti reindirizzati in uscita.

Il widget mostra i primi sette tipi di dispositivo che presentano il numero più alto di dispositivi bloccati e combina i tipi di dispositivo rimanenti nel tipo di dispositivo **Altro**.

Widget di File Sync & Share

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **File Sync & Share**.

Widget	Descrizione
Statistiche di File Sync & Share	Il widget mostra le metriche seguenti: **Archiviazione totale nel cloud utilizzata** - L'utilizzo dello storage totale di tutti gli utenti. **Utenti finali** - Il numero totale di utenti finali. **Spazio di archiviazione utilizzato in media per utente** - lo spazio di storage medio utilizzato da ogni utente finale. **Utenti guest** - Il numero totale di utenti guest.
Utilizzo dell'archivio di File Sync & Share per utente finale	Il widget mostra il numero totale di utenti finali del servizio File Sync & Share con un utilizzo dello storage compreso negli intervalli seguenti: • 0 – 1 GB • 1 – 5 GB • 5 – 10 GB • 10 – 50 GB • 50 – 100 GB • 100 – 500 GB • 500 – 1 TB • 1+ TB

Widget del servizio Notary

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Notary**.

Widget	Descrizione
Statistiche di Cyber Notary	Il widget mostra le metriche seguenti del servizio Notary: **Archivio cloud Notary utilizzato** - La dimensione totale dello storage utilizzato per i servizi Notary. **File autenticati** - Il numero totale di file autenticati. **Documenti con firma elettronica** - Il numero totale di documenti e

Widget	Descrizione
	file con firma elettronica.
File autenticati dagli utenti finali	Mostra il numero totale dei file autenticati per tutti gli utenti finali. Gli utenti vengono raggruppati in base al numero di file autenticati di cui dispongono. • Fino a 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file
Documenti con firma elettronica degli utenti finali	Il widget mostra il numero totale di documenti e file con firma elettronica per tutti gli utenti finali. Gli utenti vengono raggruppati in base al numero di file e documenti con firma elettronica di cui dispongono. • Fino a 10 file • 11 - 100 file • 101 - 500 file • 501 - 1000 file • 1000+ file

Configurazione delle impostazioni del report Riepilogo esecutivo

È possibile aggiornare le impostazioni del report Riepilogo esecutivo che sono state configurate durante la creazione del report.

Per aggiornare le impostazioni del report Riepilogo esecutivo

1. Nella console di gestione, passare a **Report**>**Riepilogo esecutivo**.
2. Fare clic sul nome del report Riepilogo esecutivo da aggiornare.
3. Fare clic su **Impostazioni**.
4. Modificare i valori nei campi come necessario.
5. Fare clic su **Salva**.

Creazione di un report Riepilogo esecutivo

È possibile creare un report Riepilogo esecutivo, visualizzare un'anteprima del contenuto, configurare i destinatari del report e pianificarne l'invio automatico.

Per creare un report Riepilogo esecutivo

1. Nella console di gestione, passare a **Report**>**Riepilogo esecutivo**.
2. Fare clic su **Crea report Riepilogo esecutivo**.

3. In **Nome report**, immettere il nome del report.
4. Selezionare i destinatari del report.
   - Per inviare il report a tutti i clienti diretti, selezionare **Invia a tutti i clienti diretti**.
   - Per inviare il report a clienti specifici
     a. Deselezionare la casella **Invia a tutti i clienti diretti**.
     b. Fare clic su **Seleziona contatti**.
     c. Selezionare i clienti specifici. Per individuare con facilità un contatto specifico, è possibile utilizzare la funzione Cerca.
     d. Fare clic su **Seleziona**.
5. Selezionare l'intervallo: **30 giorni** o **Questo mese**
6. Selezionare il formato del file: **PDF**, **Excel** oppure **Excel e PDF**.
7. Configurare le impostazioni di pianificazione.
   - Per inviare il report ai destinatari in una data e ora specifica:
     a. Abilitare l'opzione **Pianificato**.
     b. Fare clic sul campo **Giorno del mese**, cancellare il contenuto del campo Ultimo giorno e fare clic sulla data da impostare.
     c. Nel campo **Ora** inserire l'ora da impostare.
     d. Fare clic su **Applica**.
   - Per creare il report senza inviarlo ai destinatari, disabilitare l'opzione **Pianificato**.
8. Fare clic su **Salva**.

Personalizzazione del report Riepilogo esecutivo

È possibile definire le informazioni da includere nel report Riepilogo esecutivo. È possibile aggiungere o eliminare sezioni, aggiungere o eliminare widget, rinominare sezioni, personalizzare widget e trascinare e rilasciare widget e sezioni per modificare l'ordine con cui le informazioni vengono visualizzate nel report stesso.

Per aggiungere una sezione

1. Fare clic su **Aggiungi elemento** > **Aggiungi sezione**.
2. Nella finestra **Aggiungi sezione**, digitare un nome per la sezione o utilizzare quello predefinito.
3. Fare clic su **Aggiungi al report**.

Per rinominare una sezione

1. Nella sezione che si desidera rinominare, fare clic su **Modifica**.
2. Nella finestra **Modifica sezione**, digitare il nuovo nome.

3. Fare clic su **Salva**.

Per eliminare una sezione

1. Nella sezione che si desidera eliminare, fare clic su **Elimina sezione**.
2. Nella finestra di conferma **Elimina sezione**, fare clic su **Elimina**.

Per aggiungere un widget con impostazioni predefinite a una sezione

1. Nella sezione alla quale si desidera aggiungere il widget, fare clic su **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere.

Per aggiungere un widget personalizzato a una sezione

1. Nella sezione alla quale si desidera aggiungere il widget, fare clic su **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere e quindi su **Personalizza**.
3. Configurare i campi come necessario.
4. Fare clic su **Aggiungi widget**.

Per aggiungere un widget con impostazioni predefinite al report

1. Fare clic su **Aggiungi elemento** > **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere.

Per aggiungere un widget personalizzato al report

1. Fare clic su **Aggiungi widget**.
2. Nella finestra **Aggiungi widget** fare clic sul widget da aggiungere e quindi su **Personalizza**.
3. Configurare i campi come necessario.
4. Fare clic su **Aggiungi widget**.

Per ripristinare le impostazioni predefinite di un widget

1. Nel widget che si desidera personalizzare, fare clic su **Modifica**.
2. Fare clic su **Ripristina valori predefiniti**.
3. Fare clic su **Fine**.

Per personalizzare un widget

1. Nel widget che si desidera personalizzare, fare clic su **Modifica**.
2. Modificare i campi come necessario.
3. Fare clic su **Fine**.

Invio dei report Riepilogo esecutivo

È possibile inviare un report Riepilogo esecutivo su richiesta. In questo caso, l'impostazione **Pianificato** viene ignorata e il report è inviato immediatamente. Per l'invio del report, il sistema utilizza i valori relativi a Destinatari, Intervallo e Formato file configurati nelle **Impostazioni**. Prima di inviare il report è possibile modificare manualmente tali impostazioni. Per ulteriori informazioni, consultare "Configurazione delle impostazioni del report Riepilogo esecutivo" (pag. 116).

Per inviare un report Riepilogo esecutivo

1. Nel portale di gestione, passare a **Report**>**Riepilogo esecutivo**.
2. Fare clic sul nome del report Riepilogo esecutivo da inviare.
3. Fare clic su **Invia ora**.
   Il sistema invia il report Riepilogo esecutivo ai destinatari selezionati.

Fusi orari nei report

I fusi orari utilizzati nei report variano in funzione del tipo di report. La tabella seguente contiene informazioni da utilizzare come riferimento.

Tipo e posizione del report	Fuso orario utilizzato nel report
Portale di gestione > Panoramica > Operazioni (widget)	L'orario di generazione del report è indicato con il fuso orario del sistema in cui viene eseguito il browser.
Portale di gestione > Panoramica > Operazioni (esportato in PDF o xslx)	• L'indicatore data e ora del report esportato è indicato nel fuso orario del sistema utilizzato per esportare il report. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report > Utilizzo > Report pianificati	• Il report è generato alle ore 23:59:59 del fuso orario UTC il primo giorno del mese. • Viene inviato il secondo giorno del mese.
Portale di gestione > Report > Utilizzo > Report personalizzati	La data e il fuso orario del report sono indicati con il fuso UTC.
Portale di gestione > Report > Operazioni (widget)	• L'orario di generazione del report è indicato con il fuso orario del sistema in cui viene eseguito il browser. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report > Operazioni (esportato in PDF o xslx)	• L'indicatore data e ora del report esportato è indicato nel fuso orario del sistema utilizzato per esportare il report. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report >	• Il fuso orario della distribuzione del report è il fuso UTC.

Operazioni (distribuzione pianificata)	• Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Utenti > Riepilogo giornaliero degli avvisi attivi	• Il report viene inviato una volta al giorno tra le 10:00 e le 23:59 del fuso UTC. L'orario di invio del report dipende dal carico di lavoro nel data center. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Utenti > Notifiche sullo stato del servizio Cyber Protection	• Il report viene inviato al completamento di un'attività. **Nota** A seconda del carico di lavoro del data center, l'invio di alcuni report potrebbe subire ritardi. • Il fuso orario dell'attività visualizzata nel report è il fuso UTC.

Dati inseriti nel report in base al tipo di widget

In base all'intervallo di dati che visualizzano, i widget nella dashboard sono di due tipi:

- Widget che visualizzano i dati correnti nel momento in cui il report viene sfogliato o generato.
- Widget che visualizzano dati cronologici.

Quando si configura un intervallo di dati nelle impostazioni del report, per eseguire il dump relativo a un determinato periodo, l'intervallo di tempo selezionato verrà applicato solo ai widget che visualizzano dati cronologici. Il parametro dell'intervallo di tempo non è applicabile ai widget che visualizzano i dati correnti nel momento in cui il report viene sfogliato.

La tabella seguente elenca i widget disponibili e i relativi intervalli di dati.

Nome widget	Dati visualizzati nel widget e nei report
#CyberFit Score per sistema	Correnti
5 avvisi più recenti	Correnti
Dettagli sugli avvisi attivi	Correnti
Riepilogo avvisi attivi	Correnti
Attività	Cronologici
Elenco attività	Cronologici
Cronologia avvisi	Cronologici
Scansione anti-malware dei backup	Cronologici
Scansione antimalware dei file	Cronologici
Informazioni sulla scansione del backup	Cronologici

(minacce)	
Stato backup	Cronologici - nelle colonne **Esecuzioni totali** e **Numero di esecuzioni riuscite** Correnti - in tutte le altre colonne
Utilizzo dell'archivio di backup	Cronologici
Dispositivi periferici bloccati	Cronologici
URL bloccati	Correnti
Applicazioni cloud	Correnti
Stato della protezione dei workload cloud	Correnti
Cyber protection	Correnti
Riepilogo di Cyber Protection	Cronologici
Mappa di protezione dati	Cronologici
Dispositivi	Correnti
Server di Disaster Recovery sottoposti a test	Cronologici
Statistiche di Disaster Recovery	Cronologici
Macchine individuate	Correnti
Panoramica dell'integrità del disco	Correnti
Stato integrità del disco	Correnti
Stato integrità del disco per dispositivi fisici	Correnti
Documenti con firma elettronica degli utenti finali	Correnti
Vulnerabilità esistenti	Cronologici
Statistiche di File Sync & Share	Correnti
Utilizzo dell'archivio di File Sync & Share per utente finale	Correnti
Modifiche hardware	Cronologici
Dettagli hardware	Correnti
Inventario hardware	Correnti
Riepilogo avvisi cronologici	Cronologici

Riepilogo posizioni	Correnti
Aggiornamenti non effettuati per categorie	Correnti
Non protetto	Correnti
File autenticati dagli utenti finali	Correnti
Statistiche Notary	Correnti
Cronologia di installazione patch	Cronologici
Stato di installazione patch	Cronologici
Riepilogo di installazione patch	Cronologici
Vulnerabilità con patch applicate	Cronologici
Patch installate	Cronologici
Stato protezione	Correnti
Recentemente interessato	Cronologici
Sessioni remote	Cronologici
Burndown dei problemi di sicurezza	Cronologici
MTTR dei problemi di sicurezza	Cronologici
Server protetti con Disaster Recovery	Correnti
Inventario software	Correnti
Panoramica software	Cronologici
Stato minaccia	Correnti
Minacce rilevate per tecnologia di protezione	Cronologici
Distribuzione dei principali problemi per workload	Correnti
Sistemi vulnerabili	Correnti
Stato della rete dei workload	Correnti
Workload con backup eseguito	Cronologici
Stato di protezione dei workload	Correnti

Registro controllo

Per visualizzare il registro controllo, fare clic su **Registro controllo**.

Il registro controllo contiene una registrazione cronologica degli eventi seguenti:

- Operazioni eseguite dagli utenti nel portale di gestione
- Operazioni con risorse cloud-to-cloud eseguite dagli utenti nella console del servizio Cyber Protection
- Operazioni di Cyber Scripting eseguite dagli utenti nella console del servizio Cyber Protection
- Messaggi di sistema relativi a consumo di quote e quote raggiunte

Il registro visualizza gli eventi del tenant che si sta utilizzando e i relativi tenant figlio. È possibile fare clic su un evento per visualizzare ulteriori informazioni.

I registri di audit sono archiviati nei data center e la loro disponibilità non può essere influenzata dai problemi sui sistemi degli utenti finali.

La pulizia del registro avviene giornalmente. Gli eventi vengono rimossi dopo 180 giorni.

Campi del registro controllo

Per ogni evento il registro visualizza i campi seguenti:

- **Evento**
  Breve descrizione dell'evento. Ad esempio: **Tenant creato**, **Tenant eliminato**, **Utente creato**, **Utente eliminato**, **Quota raggiunta**, **Contenuto di backup esaminato**, **Script modificato**.
- **Gravità**
  Una tra le seguenti:
  - **Errore**
    Indica un errore.
  - **Attenzione**
    Indica un'azione potenzialmente negativa. Ad esempio: **Tenant eliminato**, **Utente eliminato**, **Quota raggiunta**.
  - **Avviso**
    Indica un evento che potrebbe richiedere attenzione. Ad esempio: **Tenant aggiornato**, **Utente aggiornato**.
  - **Informazione**
    Indica una modifica o un'azione informativa neutrale. Ad esempio: **Tenant creato**, **Utente creato**, **Quota aggiornata**, **Piano di scripting eliminato**.
- **Data**
  Data e ora in cui si è verificato l'evento.
- **Nome oggetto**
  L'oggetto sul quale è stata eseguita l'operazione. Ad esempio, l'oggetto dell'evento **Utente aggiornato** è l'utente di cui sono state modificate le proprietà. Per gli eventi correlati a una quota, l'oggetto è la quota.
- **Tenant**
  Il nome del tenant a cui appartiene l'oggetto.

- **Iniziatore**

  Il login dell'utente che ha avviato l'evento. Per i messaggi di sistema e gli eventi avviati da amministratori di livello superiore, l'iniziatore viene visualizzato come **Sistema**.
- **Tenant dell'iniziatore**

  Il nome del tenant a cui appartiene l'iniziatore. Per i messaggi di sistema e gli eventi avviati da amministratori di livello superiore, il campo è vuoto.
- **Metodo**

  Mostra se l'evento è stato avviato tramite l'interfaccia Web o tramite l'API.
- **IP**

  L'indirizzo IP della macchina dalla quale è stato avviato l'evento.

Filtri e ricerca

È possibile filtrare gli eventi in base a tipo, gravità o data. È inoltre possibile eseguire una ricerca tra gli eventi in base a nome, oggetto, tenant, iniziatore e tenant dell'iniziatore.

Pacchetti Advanced Protection

I pacchetti Advanced Protection possono essere abilitati in aggiunta al servizio Protezione e sono soggetti a un costo aggiuntivo. Forniscono funzionalità esclusive che non si sovrappongono all'insieme di funzionalità standard e agli altri pacchetti Advanced. I clienti possono proteggere i propri workload con uno, con diversi o con tutti i pacchetti Advanced. I pacchetti di protezione Advanced sono disponibili per entrambe le modalità di fatturazione del servizio Protezione - per workload e per gigabyte.

Le funzionalità di Advanced File Sync & Share possono essere abilitate con il servizio File Sync & Share. È disponibile in entrambe le modalità di fatturazione: per gigabyte e per utente.

È possibile abilitare i seguenti pacchetti di protezione Advanced:

- Advanced Backup
- Advanced Management
- Advanced Security
- Advanced Security + EDR
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share

Nota
I pacchetti Advanced possono essere utilizzati soltanto se la funzionalità che estendono è abilitata. Gli utenti non possono utilizzare le funzionalità Advanced quando la funzionalità del servizio standard è disabilitata. Ad esempio, gli utenti non possono utilizzare le funzionalità del pacchetto Advanced Backup se la funzionalità Protezione è disabitata.

Se è stato abilitato un pacchetto di protezione Advanced, le relative funzionalità verranno visualizzate nel piano di protezione e contrassegnate con l'icona della funzionalità Advanced  . Quando gli utenti tentano di abilitare la funzionalità, viene visualizzato un messaggio che segnala l'applicazione di una fatturazione aggiuntiva.

Se non è stato abilitato alcun pacchetto Advanced ma l'upselling è attivato, le funzionalità di protezione avanzate verranno visualizzate nel piano di protezione, ma non saranno accessibili all'utente. Accanto al nome della funzionalità viene visualizzata l'icona seguente . Verrà inoltre visualizzato un messaggio che chiede all'utente di contattare l'amministratore per abilitare l'insieme di funzionalità Advanced richiesto.

Se non è stato abilitato alcun pacchetto di protezione Advanced e l'upselling è disattivato, i clienti non potranno visualizzare le funzionalità avanzate nei propri piani di protezione.

Funzionalità e pacchetti Advanced inclusi nei servizi Cyber Protect

Quando si abilita un servizio o un insieme di funzionalità in Cyber Protect, viene abilitato il numero di funzionalità incluse e disponibili per impostazione predefinita. Inoltre, è possibile abilitare i pacchetti di protezione Advanced.

Le sezioni seguenti contengono una panoramica dettagliata delle funzionalità e dei pacchetti Advanced del servizio Cyber Protect. Per un elenco completo delle offerte, consultare la Guida al licensing di Cyber Protect.

Funzionalità incluse e avanzate nel servizio Protection

Funzionalità incluse e avanzate nel servizio Protection

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
Sicurezza	• #CyberFit score • Valutazione delle vulnerabilità • Protezione anti-ransomware: Active Protection • Protezione antivirus e antimalware: Rilevamento di file basato su firme nel cloud (senza protezione in tempo reale, solo scansioni pianificate)* • Protezione antivirus e antimalware: Analisi pre-esecuzione basata su intelligenza artificiale, motore di analisi comportamentale • Gestione di Microsoft Defender *Per individuare gli attacchi zero day, Cyber Protect utilizza regole di scansione euristiche e algoritmi che rivelano i comandi pericolosi.	Sono disponibili due pacchetti per la protezione avanzata: **Advanced Security** e **Advanced Security + EDR**. Il pacchetto Advanced Security include: • Protezione antivirus e antimalware in tempo reale con individuazione basata sulle firme in locale (con protezione in tempo reale) • Prevenzione degli exploit • Filtro URL • Gestione firewall degli endpoint • Backup con dati forensi, scansione dei backup alla ricerca del malware, ripristino sicuro, whitelist aziendale • Piani di protezione smart (integrazione con gli avvisi dei CPOC) • Scansione centralizzata del backup alla ricerca del malware • Cancellazione remota Il pacchetto di protezione Advanced Security + EDR include tutte le funzionalità sopra elencate e le seguenti capacità EDR per l'identificazione delle minacce avanzate o degli attacchi in corso:

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
		• Gestione dei problemi in una pagina centralizzata • Visualizzare ambito e impatto dei problemi • Consigli e raccomandazioni di correzione • Verificare gli attacchi resi pubblici ai workload utilizzando i Feed minacce • Archiviare gli eventi di sicurezza per 180 giorni Per informazioni su come abilitare Advanced Security + EDR, consultare "Abilitazione di Advanced Security + EDR" (pag. 131).
Prevenzione della perdita di dati	• Controllo dispositivo	• Prevenzione sensibile al contesto della perdita di dati dai workload tramite dispositivi periferici e comunicazioni di rete • Rilevamento automatico integrato di Informazioni che consentono l'identificazione personale dell'utente (PII), Informazioni sanitarie protette (PHI) e Dati soggetti allo standard Payment Card Industry Data Security Standard, oltre a documenti della categoria “Contrassegnato come Riservato” • Creazione di policy automatiche per la prevenzione della perdita di dati con assistenza facoltativa all'utente finale • Applicazione adattativa della prevenzione della perdita di dati con adeguamento automatico delle policy basato sull'apprendimento • Registrazione centralizzata di audit, avvisi e notifiche agli utenti finali basata su cloud
Gestione	• Gestione di gruppo dei workload • Gestione centralizzata dei piani di protezione • Inventario hardware	• Gestione patch • Integrità del disco • Inventario software • Applicazione sicura delle patch

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
	• Controllo da remoto • Azioni remote • Connessioni simultanee per tecnico • Protocollo di connessione remota: RDP	• Cyber Scripting • Assistenza remota • Trasferimento e condivisione di file • Selezionare una sessione a cui connettersi • Osservazione dei workload su più visualizzazioni • Modalità di connessione: controllo, osservazione e tenda • Connessione tramite applicazione Quick Assist • Protocolli di connessione remota: NEAR e Condivisione schermo • Sessione di registrazione per connessioni NEAR • Trasmissione screenshot • Report della cronologia della sessione
Sicurezza e-mail	Nessuno	Protezione in tempo reale delle caselle di posta di Microsoft 365 e Gmail: • Antimalware Antispam • Scansione degli URL nelle e-mail • Analisi DMARC • Antiphishing • Protezione dagli attacchi di imitazione delle identità • Scansione degli allegati • Neutralizzazione e ricostruzione di contenuti • Grafico di attendibilità Vedere la guida alla configurazione.
Cyber Disaster Recovery Cloud	È possibile utilizzare le funzionalità standard di Disaster Recovery per sottoporre a test gli scenari di Disaster Recovery dei workload. Considerare le funzionalità standard di Disaster Recovery disponibili, e i loro limiti: • Failover di prova in un ambiente di rete isolato. Limitato a 32 punti di	È possibile abilitare il pacchetto Advanced Disaster Recovery e proteggere i workload utilizzando la funzionalità Disaster Recovery completa. Considerare le funzionalità avanzate di Disaster Recovery disponibili: • Failover di produzione • Failover di prova in un ambiente di rete isolato.

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
	calcolo al mese, e a un massimo di 5 failover di prova contemporanei. • Configurazioni del server di ripristino: 1 CPU e 2 GB RAM, 1 CPU e 4 GB RAM, 2 CPU e 8 GB RAM. • Numero di punti di ripristino disponibili per il failover: soltanto l'ultimo punto di ripristino disponibile subito dopo un backup. • Modalità di connessione disponibili: Solo cloud e da punto a sito. • Disponibilità del gateway VPN: Il gateway VPN verrà temporaneamente sospeso se resta inattivo per 4 ore dopo il completamento dell'ultimo failover di prova, e verrà distribuito di nuovo all'avvio del failover di prova. • Numero di reti cloud: 1. • Accesso Internet • Operazioni con i runbook: creazione e modifica.	• Numero di punti di ripristino disponibili per il failover: tutti i punti di ripristino che sono disponibili dopo la creazione del server di ripristino. • Server primari • Configurazioni del server di ripristino/primario: Nessun limite • Modalità di connessione disponibili: Solo cloud, Da punto a sito, Open VPN da sito a sito e VPN IPsec multisito. • Disponibilità del gateway VPN: sempre disponibile. • Numero di reti cloud: 23. • Indirizzi IP pubblici • Accesso Internet • Operazioni con i runbook: creazione, modifica ed esecuzione.

Funzionalità a consumo e avanzate del servizio Cyber Protection

Funzionalità a consumo e avanzate nel servizio Cyber Protection

Gruppo di funzionalità	Funzionalità a consumo	Caratteristiche avanzate
Backup	• Backup di file • Backup di immagine • Backup di applicazioni • Backup su condivisioni di rete • Backup su archivio cloud • Backup su archivio locale **Nota** Si applicano tariffe per l'utilizzo dell'archivio cloud.	• Cluster di Microsoft SQL Server e Microsoft Exchange • Oracle DB • SAP HANA • Mappa della protezione dati • Protezione continua dei dati • Piani di elaborazione dei dati esternamente all'host • Autenticazione dei backup • Utenze di Microsoft 365 • Utenze di Google Workspace
File Sync & Share	• Archiviazione di contenuto crittografato basato su file	• Autenticazione e firma elettronica • Modelli di documento*

Gruppo di funzionalità	Funzionalità a consumo	Caratteristiche avanzate
	• Sincronizzazione di file tra dispositivi designati • Condivisione di file e cartelle con persone e sistemi designati	*Backup di file con sincronizzazione e condivisione
Consegna fisica dei dati	Funzionalità del servizio Consegna fisica dei dati	N/D
Servizio di autenticazione	• Autenticazione dei file • Firma elettronica dei file • Modelli di documento	N/D

Nota
Non è possibile abilitare i pacchetti di protezione Advanced senza abilitare la funzionalità di protezione standard che estendono. Se si disabilita una funzionalità, verranno automaticamente disabilitati i relativi pacchetti Advanced e revocati i piani di protezione che li utilizzano. Ad esempio, se si disabilita la funzionalità Protection, verranno automaticamente disabilitati i relativi pacchetti Advanced e revocati tutti i piani di protezione che la utilizzano.

Gli utenti non possono utilizzare i pacchetti di protezione Advanced senza la protezione Standard, ma possono utilizzare soltanto le funzionalità incluse nella protezione standard insieme ai pacchetti Advanced per specifici workload. In questo caso, verrà loro addebitato solo il costo dei pacchetti Advanced che utilizzano.

Per informazioni sulla fatturazione, vedere "Modalità di fatturazione per Cyber Protect" (pag. 7).

Advanced Data Loss Prevention

Il modulo Advanced Data Loss Prevention previene la sottrazione di informazioni sensibili da workstation, server e virtual machine ispezionando il contenuto dei dati trasferiti tramite canali locali e di rete e applicando le regole delle policy di flusso dei dati specifiche dell'organizzazione.

Prima di iniziare a utilizzare il modulo Advanced Data Loss Prevention, accertarsi di aver letto e compreso i concetti di base e la logica di gestione della funzionalità descritti nella Guida ai concetti di base.

Può inoltre essere utile leggere il documento Specifiche tecniche.

Abilitazione di Advanced Data Loss Prevention

Per impostazione predefinita, la funzionalità Advanced Data Loss Prevention viene abilitata durante la configurazione dei nuovi tenant. Se la funzionalità è stata disabilitata durante la procedura di creazione del tenant, gli amministratori del Partner potranno abilitarla in un secondo momento.

Per abilitare Advanced Data Loss Prevention

1. Nella console di gestione Cyber Protect Cloud, andare a **Clienti**.
2. Selezionare il tenant da modificare.
3. Nella sezione **Seleziona servizi**, scorrere fino a **Protezione** e nella modalità di fatturazione applicata selezionare **Advanced Data Loss Prevention**.
4. In Configura servizi, scorrere fino a **Advanced Data Loss Prevention** e configurare le quote. Per impostazione predefinita, ogni quota è impostata su Illimitata.
5. Salvare le impostazioni.

Advanced Security + EDR

Endpoint Detection and Response (EDR) rileva le attività sospette a livello di workload, inclusi gli attacchi passati inosservati, e genera un elenco di problemi. Le descrizioni dei problemi forniscono una panoramica passo per passo di ogni attacco e aiutano a comprendere come si è verificato l'evento e come impedire che accada di nuovo. Grazie alla possibilità di interpretare in modo semplice ogni fase dell'attacco, il tempo dedicato all'indagine può ridursi a pochi minuti.

Abilitazione di Advanced Security + EDR

L'amministratore del Partner può abilitare il pacchetto di protezione Advanced Security + EDR per includere la funzionalità EDR nei piani di protezione del cliente.

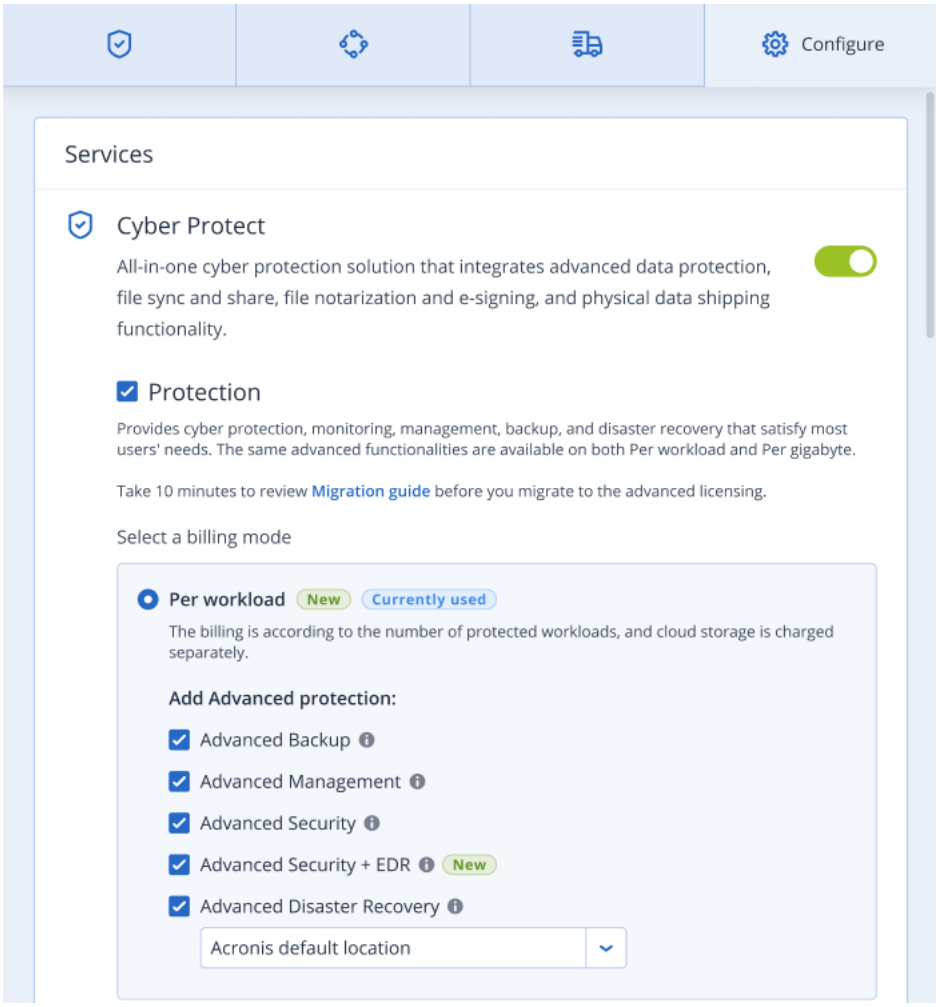
Per abilitare il pacchetto Advanced Security + EDR

1. Accedere al portale di gestione.

   Nota
   Se richiesto, selezionare i clienti ai quali applicare il pacchetto di protezione Advanced Security + EDR, quindi fare clic su **Abilita**.

2. Nel riquadro di navigazione a sinistra, fare clic su **CLIENTI**.
3. In Cyber Protect, fare clic sulla scheda **Protezione**.
   Viene visualizzato l'elenco dei clienti esistenti che hanno sottoscritto il servizio di protezione.
4. Fare clic sul cliente da aggiungere al pacchetto di protezione Advanced Security + EDR.
   Nella sezione Protezione della scheda **Configura**, verificare che la casella di controllo **Advanced**

Security + EDR sia selezionata.



Advanced Disaster Recovery

È possibile abilitare il pacchetto Advanced Disaster Recovery e proteggere i workload utilizzando la funzionalità Disaster Recovery completa.

Sono disponibili le seguenti funzionalità di Disaster Recovery:

- Failover di produzione
- Failover di prova in un ambiente di rete isolato.
- Numero di punti di ripristino disponibili per il failover: tutti i punti di ripristino che sono disponibili dopo la creazione del server di ripristino.
- Server primari
- Configurazioni del server di ripristino/primario: Nessun limite
- Modalità di connessione disponibili: Solo cloud, Da punto a sito, Open VPN da sito a sito e VPN IPsec multisito.
- Disponibilità del gateway VPN: sempre disponibile.

- Numero di reti cloud: 23.
- Indirizzi IP pubblici
- Accesso Internet
- Operazioni con i runbook: creazione, modifica ed esecuzione.

Advanced Email Security

Il pacchetto Advanced Email Security offre protezione in tempo reale delle caselle di posta di Microsoft 365, Google Workspace o Open-Xchange:

- Anti-malware e anti-spam
- Scansione degli URL nelle e-mail
- Analisi DMARC
- Antiphishing
- Protezione dagli attacchi di imitazione delle identità
- Scansione degli allegati
- Neutralizzazione e ricostruzione di contenuti
- Grafico di attendibilità

Per ulteriori informazioni sul modulo Advanced Email Security, leggere la relativa scheda informativa.

Per istruzioni sulla configurazione, vedere Advanced Email Security con Perception Point.

Integrazioni

Integrazione con sistemi di terze parti

Un service provider può integrare Cyber Protect Cloud con un sistema di terze parti come indicato di seguito:

- Configurando un'estensione della piattaforma in questo sistema.
  La pagina **Integrazione** del portale di gestione elenca le estensioni disponibili per i sistemi più diffusi di PSA (Professional Services Automations) e RMM (Remote Monitoring and Management).
  È la modalità consigliata per l'integrazione della piattaforma.
- Creando un'API client per il sistema e quindi abilitando il sistema all'accesso alle API della piattaforma e ai relativi servizi. I client API sono parte integrante della struttura di autorizzazione OAuth 2.0 della piattaforma. Per ulteriori informazioni su OAuth 2.0, consultare https://tools.ietf.org/html/rfc6749.
  È una modalità di basso livello inferiore per l'integrazione della piattaforma, che richiede competenze di programmazione. Questa scelta è consigliata quando non sono disponibili estensioni della piattaforma per il sistema in uso o quando il sistema deve essere personalizzato, nei casi in cui la gestione della piattaforma e dei servizi non sono coperti dall'estensione disponibile.

Configurazione di un'integrazione per Cyber Protect Cloud

1. Accedere al portale di gestione.
2. Passare a **Integrazioni** nel menu di navigazione principale.
3. Fare clic sul nome del sistema di terze parti per il quale abilitare l'integrazione.
4. Seguire le istruzioni a video.

Ulteriori informazioni sulle integrazioni con sistemi di terze parti disponibili, inclusa la documentazione passo per passo, sono disponibili all'indirizzo https://solutions.acronis.com.

Gestione dei clienti API

È possibile integrare sistemi di terze parti in Cyber Protect Cloud usando le relative interfacce di programmazione API. L'accesso a queste API è abilitato tramite i client API, parte integrante della struttura di autorizzazione OAuth 2.0 della piattaforma.

Cosa è un client API?

Un client API è uno speciale account di piattaforma che rappresenta un sistema di terze parti che deve essere autenticato e autorizzato per accedere ai dati nelle API della piattaforma e ai suoi servizi.

L'accesso al client è limitato a un tenant, nel quale un amministratore crea il client e i relativi tenant secondari.

Quando viene creato, il client eredita i ruoli di servizio dell'account di amministrazione, ruoli che non possono essere modificati in un secondo momento. La modifica o la disabilitazione dei ruoli dell'account amministratore non ha effetto sul client.

Le credenziali del client sono costituite dall'identificatore univoco e dal valore segreto. Le credenziali non hanno scadenza e non possono essere utilizzate per accedere al portale di gestione o a qualsiasi console del servizio. Il valore del segreto può essere ripristinato.

Non è possibile abilitare l'autenticazione a due fattori per il client.

Procedura di integrazione tipica

1. Un amministratore crea un client API in un tenant che viene gestito da un sistema di terze parti.
2. L'amministratore abilita il flusso di credenziali del client OAuth 2.0 nel sistema di terzi.
   In base a questo flusso, prima di accedere al tenant e ai relativi servizi tramite l'API, il sistema deve inviare le credenziali del client creato alla piattaforma, utilizzando l'autorizzazione API. La piattaforma genera e restituisce un token di sicurezza, una stringa crittografata univoca assegnata a questo client specifico. Il sistema deve aggiungere questo token a tutte le richieste API.
   Un token di sicurezza evita di dover passare le credenziali del client tramite le richieste API. Per ulteriore sicurezza, il token scade dopo due ore. Al termine delle due ore, tutte le richieste API con il token scaduto non avranno esito positivo e il sistema dovrà richiedere un nuovo token alla piattaforma.

Per ulteriori informazioni sull'uso delle API di autorizzazione e di piattaforma, fare riferimento alla guida dello sviluppatore all'indirizzo https://developer.acronis.com/doc/account-management/v2/guide/index.

Creazione di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API** > **Crea client API**.
3. Inserire un nome per il client API.
4. Fare clic su **Avanti**.
   Al momento della creazione, per il client API è impostato lo stato predefinito **Attivo**.
5. Copiare e salvare l'ID e il valore del segreto del client e l'URL del data center. Saranno necessari durante l'abilitazione del flusso di credenziali del client OAuth 2.0 in un sistema di terzi.

   Importante
   Per ragioni di sicurezza, il valore segreto viene visualizzato solo una volta. In caso di perdita, non

sarà possibile recuperare questo valore ma solo eseguirne il ripristino.

6. Fare clic su **Fine**.

Reimpostazione del valore segreto di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su e quindi su **Reimposta segreto**.
5. Confermare la decisione facendo clic su **Avanti**.
   Viene generato un nuovo valore del segreto. L'ID del client e l'URL del data center non vengono modificati.
   Tutti i token di sicurezza assegnati a questo client scadranno immediatamente e le richieste API con tali token non avranno esito positivo.
6. Copiare e salvare il nuovo valore del segreto del client.

   Importante
   Per ragioni di sicurezza, il valore segreto viene visualizzato solo una volta. In caso di perdita, non sarà possibile recuperare questo valore ma solo eseguirne il ripristino.

7. Fare clic su **Fine**.

Disabilitazione di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su , quindi su **Disabilita**.
5. Confermare la propria decisione.
   Lo stato del client cambia in **Disabilitato**.
   Le richieste API con token di sicurezza assegnate a questo client non avranno esito positivo, ma i token non scadranno immediatamente. La disabilitazione del client non ha effetto sulla scadenza dei token.
   Sarà possibile riabilitare il client in qualsiasi momento.

Abilitazione di un client API disabilitato

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.

3. Individuare il client richiesto nell'elenco.
4. Fare clic su , quindi su **Abilita**.

   Lo stato del client cambia in **Attivo**.

   Le richieste API con token di sicurezza assegnate a questo client avranno esito positivo se i token non sono ancora scaduti.

Eliminazione di un client API

1. Accedere al portale di gestione.
2. Fare clic su **Impostazioni** > **Client API**.
3. Individuare il client richiesto nell'elenco.
4. Fare clic su , quindi su **Elimina**.
5. Confermare la propria decisione.

   Tutti i token di sicurezza assegnati a questo client scadranno immediatamente e le richieste API con tali token non avranno esito positivo.

   Importante
   Non è possibile recuperare un client eliminato.

Riferimenti per l'integrazione

La tabella seguente elenca le integrazioni implementate con terze parti e fornisce i link alla rispettiva documentazione.

NOME INTEGRAZIONE	Visualizza online	Apri PDF
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf

NOME INTEGRAZIONE	Visualizza online	Apri PDF
Connect Wise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
Connect Wise Control	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf
Connect Wise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableNsightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentati	https://dl.acronis.com/u/pdf/AcronisPRTG

NOME INTEGRAZIONE	Visualizza online	Apri PDF
	on/PRTG/	Plugin_userguide_en-US.pdf
ServiceNow	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

Integrazione con VMware Cloud Director

Un Service Provider può integrare VMware Cloud Director (già noto come VMware vCloud Director) con Cyber Protect Cloud e fornire ai propri clienti una soluzione di backup pronta all'uso per le loro virtual machine.

La procedura di integrazione prevede i seguenti passaggi:

1. Configurazione del broker dei messaggi di RabbitMQ per l'ambiente VMware Cloud Director.
   RabbitMQ consente la sincronizzazione delle modifiche nell'ambiente VMware Cloud Director con Cyber Protect Cloud.
2. Installazione del plug-in per VMware Cloud Director.
   Questo plug-in aggiunge Cyber Protectionall'interfaccia utente di VMware Cloud Director.
3. Distribuzione di un agente di gestione.
   L'agente di gestione associa automaticamente le organizzazioni VMware Cloud Director ai tenant cliente in Cyber Protect Cloud, e gli amministratori delle organizzazioni agli amministratori del tenant cliente. Per ulteriori informazioni sulle organizzazioni, consultare l'articolo relativo alla creazione di un'organizzazione in VMware Cloud Director nella Knowledge Base di VMware.
   I tenant cliente vengono creati all'interno del tenant partner per il quale è configurata l'integrazione VMware Cloud Director. Questi nuovi tenant cliente sono in modalità **bloccata** e non possono essere gestiti dagli amministratori dei partner in Cyber Protect Cloud.

   Nota
   Soltanto gli amministratori delle organizzazioni con indirizzi e-mail univoci in VMware Cloud Director sono associati a Cyber Protect Cloud.

4. Distribuzione di uno o più agenti di backup.

   L'agente di backup fornisce funzionalità dei backup e ripristino per le virtual machine nell'ambiente VMware Cloud Director.

Per disabilitare l'integrazione tra VMware Cloud Director e Cyber Protect Cloud, contattare il team di supporto tecnico.

Limitazioni

- L'integrazione con VMware Cloud Director è possibile solo per i tenant partner in modalità di gestione **Gestito dal service provider**, il cui tenant parent (se esistente) è altresì impostato sulla modalità di gestione **Gestito dal service provider**. Per ulteriori informazioni sulle tipologie di tenant e sulle rispettive modalità di gestione, consultare "Creazione di un tenant" (pag. 34).

  Tutti i partner diretti esistenti possono configurare l'integrazione con VMware Cloud Director. Gli amministratori dei partner possono abilitare questa opzione anche per i tenant secondari, selezionando la casella di controllo **Infrastruttura di VMware Cloud Director di proprietà del partner** al momento della creazione di un tenant partner figlio.
- Nel tenant partner nel quale è configurata l'integrazione con VMware Cloud Director è necessario disabilitare l'autenticazione a due fattori.
- Un amministratore che ricopre il ruolo di amministratore dell'organizzazione in più organizzazioni di VMware Cloud Director può gestire il backup e il ripristino per un solo tenant cliente in Cyber Protection.
- La console web di Cyber Protection viene visualizzata in una nuova scheda.

Requisiti software

Versioni di VMware Cloud Director supportate

- VMware Cloud Director 10.0, 10.1, 10.2, 10.3, 10.4, 10.4.1

Browser Web supportati

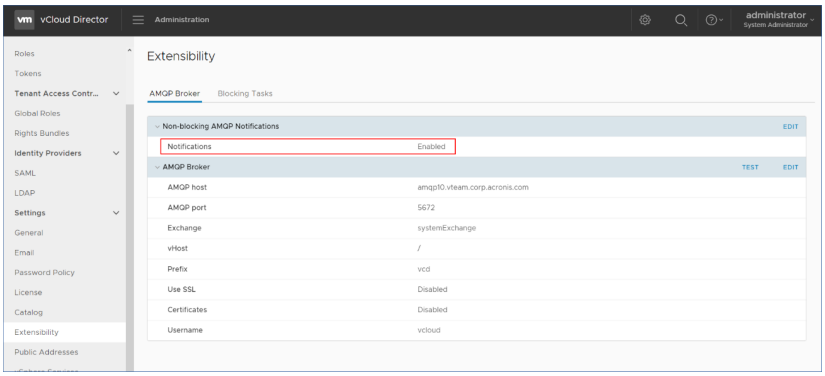
- Google Chrome 29 o versione successiva
- Mozilla Firefox 23 o versione successiva
- Opera 16 o versione successiva
- Microsoft Edge 25 o versioni successive
- Safari 8 o versioni successive in esecuzione nei sistemi operativi macOS e iOS

In altri browser Web (inclusi browser Safari eseguiti in altri sistemi operativi), l'interfaccia utente potrebbe essere visualizzata in modo non corretto o alcune funzioni potrebbero non essere disponibili.

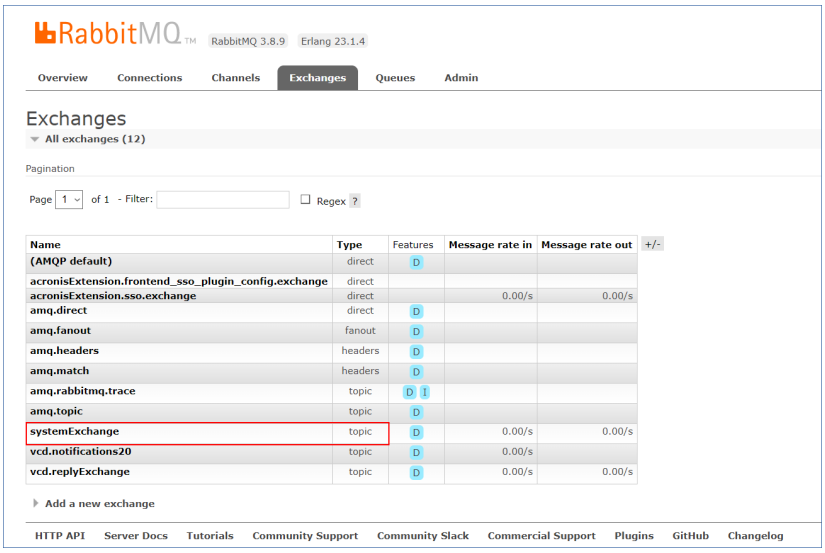
Configurazione del broker dei messaggi di RabbitMQ

1. Installare un broker RabbitMQ AMQP per l'ambiente VMware Cloud Director.

   Per ulteriori informazioni su come installare RabbitMQ, consultare la documentazione di VMware: Installare e configurare un broker RabbitMQ AMQP.
2. Accedere al portale del provider VMware Cloud Director come amministratore di sistema.
3. Passare a **Administration** > **Extensibility**, e quindi verificare che in **Non-blocking AMQP Notifications**, sia abilitata l'opzione **Notifications**.



4. Accedere alla console di gestione di RabbitMQ come amministratore.
5. Nella scheda **Exchanges**, verificare che lo scambio (per impostazione predefinita, sotto al nome **SystemExchange**) sia stato creato, e che corrisponda al tipo **topic**.



Installazione del plug-in per VMware Cloud Director

1. Fare clic sul link seguente per scaricare il file **vCDPlugin.zip**: https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Accedere al portale del provider VMware Cloud Director come amministratore di sistema.
3. Nel menu di navigazione, selezionare **Customize Portal**.
4. Nella scheda **Manage Plugins**, fare clic su **Upload**.

Viene visualizzata la procedura guidata **Upload Plugin**.

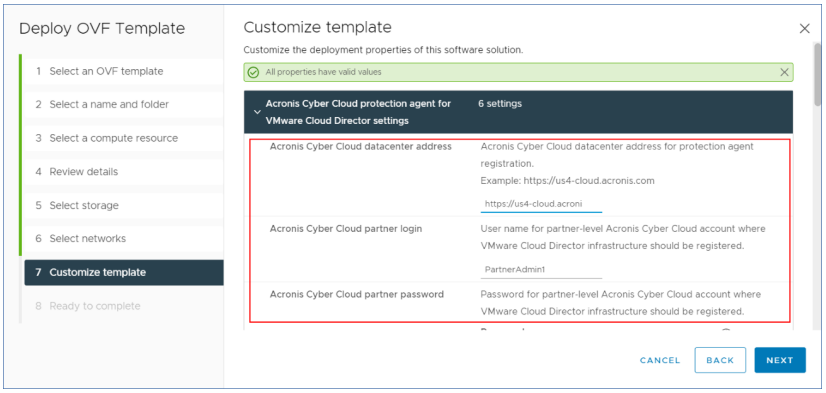
5. Fare clic su **Select Plugin File** e quindi selezionare il file **vCDPlugin.zip**.
6. Fare clic su **Avanti**.
7. Configurare l'ambito e la pubblicazione:
   a. Nella sezione **Scope to**, selezionare solo la casella di controllo **Tenant**.
   b. Nella sezione **Publish to**, selezionare **All tenants** per abilitare il plug-in per tutti i tenant esistenti e futuri, o selezionare i singoli tenant per i quali abilitare il plug-in.
8. Fare clic su **Avanti**.
9. Ricontrollare le impostazioni, quindi fare clic su **Fine**.

Installazione di un agente di gestione

1. Accedere al portale di gestione di Cyber Protect Cloud come amministratore del partner.
2. Passare a **Impostazioni** > **Posizione**, quindi fare clic su **Aggiungi VMware Cloud Director**.
3. Fare clic sul link **Agente di gestione** e scaricare il file ZIP.
4. Estrarre il file del modello dell'agente di gestione `vCDManagementAgent.ovf` e il file del disco rigido virtuale `vCDManagementAgent-disk1.vmdk`.
5. Nel client vSphere, distribuire il modello OVF dell'agente di gestione in un host ESXi in un'istanza di vCenter che sia gestita da VMware Cloud Director.

   Importante
   Installare un solo agente di gestione per ogni ambiente VMware Cloud Director.

6. Nella procedura guidata **Deploy OVF Template**, configurare l'agente di gestione impostando quanto segue:



   a. URL del data center Cyber Protect Cloud. Ad esempio, `https://us5-cloud.esempio.com`.
   b. Login e password dell'amministratore del partner.
   c. ID dello storage di backup per le virtual machine nell'ambiente VMware Cloud Director. Questo storage di backup può essere solo di proprietà del partner. Per ulteriori informazioni sugli storage, fare riferimento a "Gestione di posizioni e archivi" (pag. 67).

Per verificare l'ID, nel portale di gestione passare a **Impostazioni** > **Posizioni**, e quindi selezionare lo storage desiderato. L'ID relativo è visualizzato dopo la parte **uuid=** dell'URL.

d. Modalità di fatturazione di Cyber Protect Cloud: **Per gigabyte** o **Per workload**.

> **Nota**
> La modalità di fatturazione selezionata verrà applicata a tutti i nuovi tenant cliente che verranno creati.

e. Parametri di VMware Cloud Director: indirizzo dell'infrastruttura, login dell'amministratore di sistema e password.

f. Parametri di RabbitMQ: indirizzo del server, porta, nome dell'host virtuale, login dell'amministratore e password.

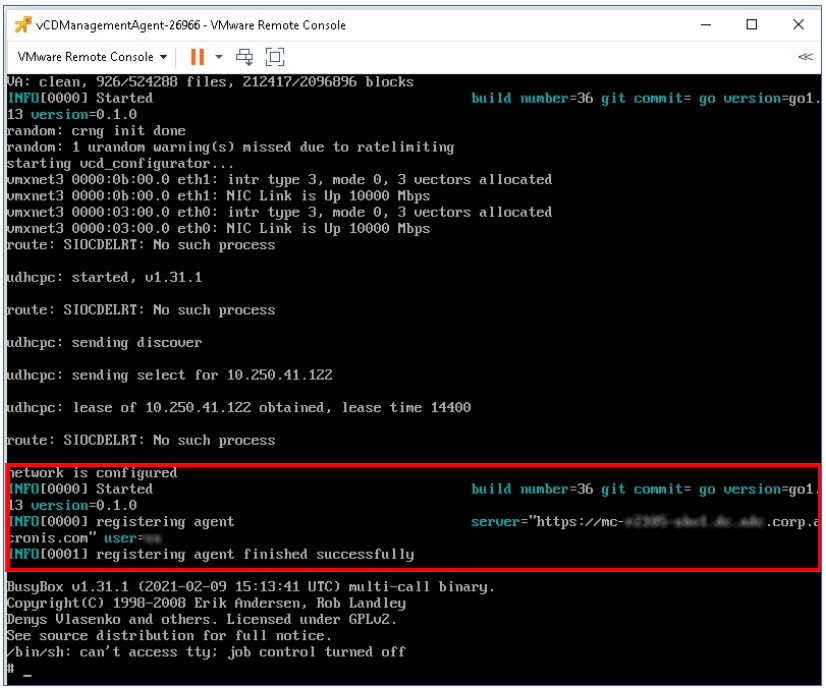
g. Parametri della rete: Indirizzo IP, subnet mask, gateway predefinito, DNS, suffisso DNS.

Per impostazione predefinita, è attivata una sola interfaccia di rete. Per abilitare una seconda interfaccia di rete selezionare la casella di controllo accanto a **Enable eth1**.

> **Nota**
> Verificare che le impostazioni di rete consentano all'agente di gestione di accedere sia all'ambiente VMware Cloud Director sia al data center Cyber Protect Cloud.

Dopo il deployment iniziale, sarà inoltre possibile configurare i le impostazioni dell'agente di gestione. Nel client vSphere, spegnere la virtual machine con l'agente di gestione, quindi fare clic su **Configure** > **Settings** > **vApp Options**. Applicare le impostazioni desiderate, quindi accendere la virtual machine con l'agente di gestione.

7. [Facoltativo] Nel client vSphere, aprire la console della virtual machine con l'agente di gestione e verificare la configurazione.

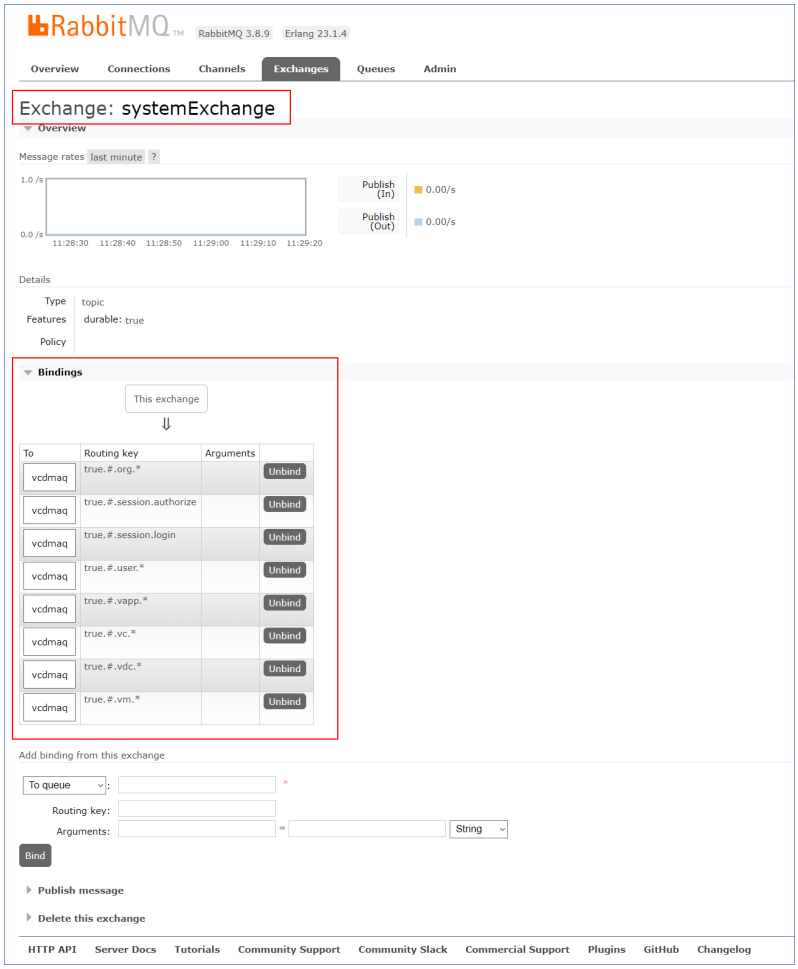


8. Verificare la connessione RabbitMQ.

a. Accedere alla console di gestione di RabbitMQ come amministratore.

b. Nella scheda **Exchanges**, selezionare lo scambio impostato durante l'installazione di RabbitMQ. Per impostazione predefinita, tale scambio è denominato **systemExchange**.

c. Verificare le associazioni alla coda **vcdmaq**.



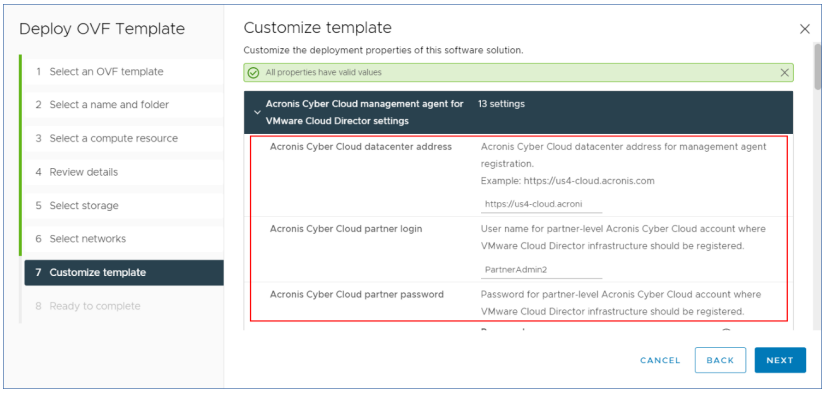
Installazione degli agenti di backup

1. Accedere al portale di gestione come amministratore del partner.
2. Passare a **Impostazioni** > **Posizione**, quindi fare clic su **Aggiungi VMware Cloud Director**.
3. Fare clic sul link **Agente di backup** e scaricare il file ZIP.
4. Estrarre il file del modello dell'agente di backup `vCDCyberProtectAgent.ovf` e il file del disco rigido virtuale `vCDCyberProtectAgent-disk1.vmdk`.
5. Nel client vSphere, distribuire il modello dell'agente di backup nell'host ESXi desiderato.

   È necessario almeno un agente di backup per host. Per impostazione predefinita, all'agente di backup sono assegnati 8 GB di RAM e 2 vCPU; è in grado di eseguire fino a 10 backup o attività di ripristino contemporaneamente. Per elaborare più attività o distribuire il traffico di backup e ripristino, è necessario distribuire agenti aggiuntivi nello stesso host.

Nota
Il backup di virtual machine su host ESXi nei quali non è installato alcun agente di backup non avrà esito positivo e genererà l'errore "Timeout dell'attività scaduto".

6. Nella procedura guidata **Deploy OVF Template**, configurare l'agente di backup impostando quanto segue:



   a. URL del data center Cyber Protect Cloud. Ad esempio, `https://us5-cloud.esempio.com`.

   b. Login e password dell'amministratore del partner.

   c. Parametri di VMware vCenter: indirizzo del server, login e password.

      L'agente utilizzerà queste credenziali per la connessione al vCenter Server. Si consiglia di utilizzare un account a cui è assegnato il ruolo **Amministratore**. Altrimenti, fornire un account con i privilegi necessari in vCenter Server.

   d. Parametri della rete: Indirizzo IP, subnet mask, gateway predefinito, DNS, suffisso DNS.

      Per impostazione predefinita, è attivata una sola interfaccia di rete. Per abilitare una seconda interfaccia di rete selezionare la casella di controllo accanto a **Enable eth1**.

      Nota
      Verificare che le impostazioni di rete consentano all'agente di backup di accedere sia al vCenter Server sia al data center Cyber Protect Cloud.

   e. Limite di download: la velocità massima di download (in Kbps), che definisce la velocità di lettura dell'archivio di backup durante un'operazione di ripristino. Il valore predefinito è 0 - Senza limiti.

   f. Limite di upload: la velocità massima di upload (in Kbps), che definisce la velocità di scrittura dell'archivio di backup durante un'operazione di backup. Il valore predefinito è 0 - Senza limiti.

   Dopo il deployment iniziale, sarà inoltre possibile configurare i parametri di impostazione dell'agente di backup. Nel client vSphere, spegnere la virtual machine con l'agente di backup, quindi fare clic su **Configure** > **Settings** > **vApp Options**. Applicare le impostazioni desiderate, quindi accendere la virtual machine con l'agente di backup.

7. Nel client vSphere, verificare che le opzioni **Host** e **Storage vMotion** siano disabitate per la virtual machine con l'agente di backup.

Aggiornamento degli agenti

Per aggiornare un agente di gestione

1. Accedere al portale di gestione di Cyber Protect Cloud come amministratore del partner.
2. Passare a **Impostazioni** > **Posizione**, quindi fare clic su **Aggiungi VMware Cloud Director**.
3. Fare clic sul link **Agente di gestione** e scaricare il file ZIP con l'agente più aggiornato.
4. Estrarre il file del modello dell'agente di gestione `vCDManagementAgent.ovf` e il file del disco rigido virtuale `vCDManagementAgent-disk1.vmdk`.
5. Nel client vSphere, spegnere la virtual machine con l'agente di gestione corrente.
6. Distribuire una virtual machine con il nuovo agente di gestione utilizzando i file `vCDManagementAgent.ovf` e `vCDManagementAgent-disk1.vmdk` più recenti.
7. Configurare l'agente di gestione utilizzando le stesse impostazioni dell'agente precedente.
8. [Facoltativo] Eliminare la virtual machine con l'agente di gestione obsoleto.

Importante
Deve essere presente un solo agente di gestione attivo per ogni ambiente VMware Cloud Director.

Per aggiornare un agente di backup

1. Accedere al portale di gestione di Cyber Protect Cloud come amministratore del partner.
2. Passare a **Impostazioni** > **Posizione**, quindi fare clic su **Aggiungi VMware Cloud Director**.
3. Fare clic sul link **Agente di backup** e scaricare il file ZIP con l'agente più recente.
4. Estrarre il file del modello dell'agente di gestione `vCDCyberProtectAgent.ovf` e il file del disco rigido virtuale `vCDCyberProtectAgent-disk1.vmdk`.
5. Nel client vSphere, spegnere la virtual machine con l'agente di backup corrente.
   Tutte le attività di backup e ripristino in esecuzione verranno interrotte. Per verificare la presenza di attività in esecuzione, nel client vSphere aprire la console della virtual machine con l'agente di backup ed eseguire il seguente comando: `ps | grep esx_worker`. Verificare che non siano presenti processi `esx_worker` attivi.
6. Distribuire una virtual machine con il nuovo agente di backup utilizzando i file `vCDCyberProtectAgent.ovf` e `vCDCyberProtectAgent-disk1.vmdk` più recenti.
7. Configurare l'agente di backup utilizzando le stesse impostazioni dell'agente precedente.
8. [Facoltativo] Eliminare la virtual machine con l'agente di backup obsoleto.

Accesso alla console web di Cyber Protection

I seguenti amministratori possono gestire il backup di virtual machine nelle organizzazioni di VMware Cloud Director:

- Amministratori dell'organizzazione
- Assegnato specificamente agli amministratori di backup
  Per ulteriori informazioni su come creare questo tipo di amministratore, fare riferimento a "Creazione di un amministratore di backup" (pag. 147).

Gli amministratori possono accedere alla console web Cyber Protection personalizzata facendo clic su **Cyber Protection** nel menu di navigazione del portale del tenant VMware Cloud Director.

Nota
L'accesso single sign-on è disponibile solo agli amministratori dell'organizzazione e non è supportato per gli amministratori di sistema che utilizzano il portale del tenant VMware Cloud Director.

Nella console web di Cyber Protection, gli amministratori possono accedere solo agli elementi della propria organizzazione VMware Cloud Director: data center virtuali, vApp e singole virtual machine. Possono gestire il backup e il ripristino delle risorse dell'organizzazione VMware Cloud Director.

Gli amministratori dei partner possono accedere alle console web di Cyber Protection dei tenant dei propri clienti e gestire le attività di backup e ripristino per loro conto.

Limitazioni

L'elenco delle limitazioni è soggetto a modifica nelle prossime versioni di Cyber Protect Cloud.

Backup

- È supportato soltanto il backup dell'intero sistema. Il filtraggio dei file o la selezione di dischi o volumi non sono disponibili.
- Come posizione di backup è supportato soltanto il cloud storage. Lo storage viene configurato nelle impostazioni dell'agente di gestione e non è modificabile dagli utenti nel piano di protezione.
- Non sono supportati i gruppi dinamici.
- Sono supportati i seguenti schemi di backup: **Sempre incrementale (file singolo)**, **Sempre completo** e **Settimanale completo, Giornaliero incrementale**.
- È supportata la pulizia solo dopo il backup.

Ripristino

- È supportato il ripristino solo sulla virtual machine originale. La virtual machine originale deve essere già esistente nell'ambiente VMware Cloud Director.
- Non è supportato il ripristino a livello di file.

Creazione di un amministratore di backup

Gli Amministratori dell'organizzazione possono delegare la gestione del backup ad amministratori di backup specificamente assegnati al ruolo.

Per creare un amministratore di backup

1. Nel portale del tenant VMware Cloud Director, fare clic su **Amministrazione** > **Ruoli** > **Nuovo**.
2. Nella finestra **Aggiungi ruolo**, specificare un nome e una descrizione per il nuovo ruolo.
3. Scorrere l'elenco delle autorizzazioni e quindi, in **Altro**, selezionare **Operatore di backup self-service di VM**.

   Nota
   L'autorizzazione **Operatore di backup self-service di VM** diventa disponibile dopo aver installato il plug-in per VMware Cloud Director. Per ulteriori informazioni su come eseguire questa operazione, fare riferimento a "Installazione del plug-in per VMware Cloud Director" (pag. 141).

4. Nel portale del tenant VMware Cloud Director, fare clic su **Utenti**.
5. Selezionare un utente, quindi fare clic su **Modifica**.
6. Assegnare questo utente al nuovo ruolo creato.

L'utente selezionato potrà gestire i backup delle virtual machine in questa organizzazione.

Nota
Gli amministratori di sistema dell'ambiente VMware Cloud Director possono definire un ruolo globale con l'autorizzazione **Operatore di backup self-service di VM** abilitata e quindi pubblicare tale ruolo nei tenant. A questo punto, gli Amministratori dell'organizzazione dovranno solo assegnare il ruolo a un utente.

Report di sistema, file di registro e file di configurazione

Per le finalità di soluzione dei problemi, può essere necessario creare un record di sistema utilizzando lo strumento `sysinfo` oppure controllare i file di registro e configurazione in una virtual machine con un agente.

È possibile accedere alla virtual machine direttamente, aprendo la relativa console nel client vSphere oppure da remoto, tramite un client SSH. Per accedere alla virtual machine tramite client SSH, è necessario innanzitutto abilitare la connessione SSH su tale virtual machine.

Per abilitare una connessione SSH in una virtual machine

1. Nel client vSphere, aprire la console della virtual machine con l'agente.
2. Nel prompt dei comandi, eseguire il comando `/bin/sshd` per avviare il daemon SSH.

Sarà possibile connettersi a questa virtual machine utilizzando un client SSH, come ad esempio WinSCP.

Per eseguire lo strumento `sysinfo`

1. Accedere alla virtual machine con l'agente.
   - Per accedere direttamente all'agente, nel client vSphere aprire la console della virtual machine.
   - Per accedere all'agente da remoto, connettersi alla virtual machine tramite un client SSH. Utilizzare la seguente combinazione predefinita di login:password: `root`:`root`.
2. Passare alla directory `/bin` e quindi eseguire lo strumento `sysinfo`.

   ```
   # cd /bin/
   # ./sysinfo
   ```

   Il file del report di sistema verrà salvato nella directory predefinita: `/var/lib/Acronis/sysinfo`.
   È possibile specificare un'altra directory eseguendo lo strumento `sysinfo` con l'opzione `--target_dir`.

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```

3. Scaricare il report di sistema generato utilizzando un client SSH.

Per accedere a un file di registro o di configurazione

1. Connettersi alla virtual machine tramite un client SSH.
   Utilizzare la seguente combinazione predefinita di login:password: `root`:`root`.
2. Scaricare il file desiderato.
   È possibile individuare i file di registro nelle seguenti posizioni:
   - Agente di backup: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Agente di gestione: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   È possibile individuare i file di configurazione nelle seguenti posizioni:
   - Agente di backup: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Agente di gestione: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Rimozione dell'integrazione con VMware Cloud Director

Ripristinare la configurazione e annullare la registrazione dell'istanza VMware Cloud Director da Cyber Protect Cloud è una procedura complessa. Contattare il referente del supporto.

Impostazioni di privacy

Le impostazioni di privacy aiutano a indicare se si è fornito o meno il consenso alla raccolta, all'uso e alla diffusione delle proprie informazioni personali.

A seconda del paese in cui si utilizza Cyber Protect e il data center Cyber Protect Cloud che fornisce servizi all'utente, all'avvio iniziale di Cyber Protect può essere chiesto di confermare se si accetta l'uso di Google Analytics in Cyber Protect.

Google Analytics ci aiuta a comprendere meglio i comportamenti degli utenti e a migliorare l'esperienza utente con Cyber Protect raccogliendo dati presentati con l'uso di pseudonimi.

Se nell'interfaccia di Cyber Protect non è visibile il consenso e il menu di Google Analytics, è probabile che il prodotto non è usato nel paese dell'utente.

Se Google Analytics è stato abilitato o rifiutato durante l'avvio iniziale di Cyber Protect, l'utente potrà modificare la decisione in un momento successivo.

Per abilitare o disabilitare Google Analytics

1. Nella console di Cyber Protect, fare clic sull'icona dell'account nell'angolo in alto a destra.
2. Selezionare **Impostazioni di privacy personali**.
3. Nella sezione **Acquisizione dati da Google Analytics** selezionare uno dei seguenti pulsanti:
   - **On** per abilitare Google Analytics
   - **Off** per disabilitare Google Analytics

Indice

#

#CyberFit Score per sistema 83

A

Abilitazione dei servizi per più tenant esistenti 39

Abilitazione delle Notifiche sulla manutenzione 41

Abilitazione di Advanced Data Loss Prevention 130

Abilitazione di Advanced Security + EDR 131

Abilitazione di un client API disabilitato 136

Abilitazione o disabilitazione degli elementi dell'offerta 13

Accesso ai servizi 29

Accesso al portale di gestione 26

Accesso alla console di Cyber Protection dal portale di gestione 27

Accesso alla console web di Cyber Protection 146

Account utente e tenant 31

Advanced Data Loss Prevention 130

Advanced Disaster Recovery 132

Advanced Email Security 133

Advanced Security + EDR 131

Aggiornamenti non effettuati per categorie 95

Aggiornamento automatico degli agenti 78

Aggiornamento degli agenti 146

Aggiornamento dei dati di utilizzo per un tenant 44

Aggiunta di nuovi archivi 69

Aggiunta di un report 104

Ambito del report 101

App per dispositivo mobile 75

Applicazione del branding 73

Applicazione della personalizzazione 77

Aspetto 73

Attivare l'account di amministrazione 25

Avvisi di stato dell'integrità del disco 91

Azioni nell'elenco Dispositivi 67

B

Backup 147

Barra Cronologia a 7 giorni 31

Branding dell'agente e del programma di installazione 74

Browser Web supportati 25, 140

Burndown dei problemi di sicurezza 85

C

Campi del registro controllo 123

Come funziona 60, 87

Come spostare un tenant 46

Configurazione degli elementi dell'offerta per un tenant 38

Configurazione degli URL delle interfacce web personalizzate 77

Configurazione dei contatti aziendali 42

Configurazione dei contatti nella procedura guidata Profilo azienda 26

Configurazione del branding 76

Configurazione del branding e del marchio personalizzabile 72

Configurazione del broker dei messaggi di RabbitMQ 141

Configurazione del profilo cliente autogestito 42

Configurazione dell'archivio immutabile 70

Configurazione dell'autenticazione a due fattori 59

Configurazione dell'autenticazione a due fattori per il tenant 62

Configurazione delle impostazioni del report Riepilogo esecutivo 116

Configurazione di report di utilizzo personalizzati 101

Configurazione di report di utilizzo pianificati 101

Configurazione di scenari di upselling per i clienti 66

Configurazione di un'integrazione per Cyber Protect Cloud 134

Conversione di un tenant partner in un tenant cartella e viceversa 47

Cosa è un client API? 134

Creare o modificare un piano di protezione 67

Creazione di un account utente 48

Creazione di un amministratore di backup 147

Creazione di un client API 135

Creazione di un report Riepilogo esecutivo 116

Creazione di un tenant 34

Cronologia della sessione 99

Cronologia di installazione patch 95

D

Dati inseriti nel report in base al tipo di widget 120

Dipendenza del programma di installazione dell'agente dagli elementi dell'offerta 23

Disabilitare il branding 76

Disabilitazione di un client API 136

Disabilitazione e abilitazione di un account utente 58

Disabilitazione e abilitazione di un tenant 45

Distribuzione dei principali problemi per workload 84

Documentazione e supporto 74

Download dei dati relativi ai workload recentemente interessati 96

Download di un report 106

Dumping dei dati del report 106

E

Elaborazione di rapporti 100

Elementi dell’offerta 12

Elementi di upselling mostrati al cliente 67

Elenco delle vulnerabilità 67

Eliminazione degli archivi 69

Eliminazione di un account utente 58

Eliminazione di un client API 137

Eliminazione di un tenant 48

Esempio

- Passaggio dell'edizione Cyber Protect Advanced alla fatturazione per workload 10

Esportazione e importazione della struttura del

report 106

F

Fatturazione del servizio Notary 8

Fatturazione del servizio Physical Data Shipping 8

Filtri e ricerca 124

Funzionalità a consumo e avanzate del servizio Cyber Protection 129

Funzionalità e pacchetti Advanced inclusi nei servizi Cyber Protect 126

Funzionalità incluse e avanzate nel servizio Protection 126

Fusi orari nei report 119

G

Gestione degli utenti 48

Gestione dei clienti API 134

Gestione dei tenant 34

Gestione dell'archiviazione 69

Gestione dell'autenticazione a due fattori per gli utenti 63

Gestione di posizioni e archivi 67

I

Impedire l'accesso agli utenti di Microsoft 365 senza licenza 19

Impostazione di quote variabili e fisse 15

Impostazioni di privacy 150

Impostazioni documento legale 75

Impostazioni server e-mail 76

Individuazione automatica guidata 67

Informazioni su Cyber Protect 6

Informazioni sul documento 5

Informazioni sulla scansione del backup 95

Installazione degli agenti di backup 144

Installazione del plug-in per VMware Cloud Director 141

Installazione di un agente di gestione 142

Integrazione con sistemi di terze parti 134

Integrazione con VMware Cloud Director 139

Integrazioni 134

Invio dei report Riepilogo esecutivo 119

L

Limitazione dell'accesso al tenant 47

Limitazione dell'accesso all'interfaccia Web 28

Limitazioni 37, 87, 140, 147

Livelli nei quali è possibile definire le quote 15

M

Macchine individuate 83

Mappa di protezione dati 91

Metriche con utilizzo pari a zero 101

Modalità di fatturazione del componente Protezione 7

Modalità di fatturazione della funzionalità File Sync & Share 8

Modalità di fatturazione ed edizioni 13

Modalità di fatturazione per Cyber Protect 7

Modalità Sicurezza avanzata 37

Modifica della modalità di fatturazione di un tenant cliente 11

Modifica della modalità di fatturazione di un tenant partner 11

Modifica della quota di servizio dei sistemi 22

Modifica delle impostazioni del report 104

Modifica delle impostazioni di notifica per un utente 56

Monitoraggio 63, 80

Monitoraggio integrità del disco 87

MTTR del problema 85

N

Navigazione nel portale di gestione 27

Notifiche ricevute in base al ruolo dell'utente 57

O

Offerta di elementi e gestione delle quote 12

Operazioni 81

Operazioni sulle posizioni 68

P

Pacchetti Advanced Protection 125

Passaggio dalle edizioni legacy al modello di fatturazione corrente 9

Passaggio dell'edizione Cyber Protect per workload alla fatturazione per workload 10

Passaggio tra edizioni e modalità di fatturazione 9

Per abilitare l'autenticazione a due fattori per un utente 64

Per aggiornare gli agenti automaticamente 79

Per configurare l'autenticazione a due fattori per il tenant 62

Per disabilitare l'autenticazione a due fattori per il tenant 63

Per disabilitare l'autenticazione a due fattori per un utente 64

Per monitorare gli aggiornamenti degli agenti 80

Per ripristinare il browser attendibile per un utente 63

Per ripristinare l'autenticazione a due fattori per un utente 63

Personalizzazione 77

Personalizzazione del report Riepilogo esecutivo 117

Pianificazione di un report 105

Posizioni 68

Procedura di integrazione tipica 135

Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant 61

Protezione da attacchi di forza bruta 65

Q

Quote del servizio Backup 16

Quote del servizio Consegna fisica dei dati 21

Quote del servizio Disaster Recovery 20

Quote del servizio File Sync & Share 21

Quote del servizio Notary 21

Quote flessibili e rigide 14

Quote per archivio 18

Quote per origini dati nel cloud 16

R

Recentemente interessato 96

Registro controllo 122

Reimpostazione del valore segreto di un client API 136

Report di sistema, file di registro e file di configurazione 148

Report Operazioni 102

Requisiti e limitazioni 46

Requisiti per la password 25

Requisiti software 140

Riepilogo di installazione patch 94

Riepilogo esecutivo 107

Riferimenti per l'integrazione 137

Rimozione dell'integrazione con VMware Cloud Director 149

Ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore 65

Ripristino 147

Ripristino delle impostazioni predefinite di branding 76

Ruoli utente disponibili per ogni servizio 51

Ruoli utente e diritti di Cyber Scripting 54

S

Scheda Clienti 30

Scheda Panoramica 29

Selezione dei servizi per un tenant 38

Selezione di posizioni e archivi per partner e clienti 68

Servizi 12

Servizi Cyber Protect 6

Servizi ed elementi dell'offerta 12

Sistemi vulnerabili 93

Spostamento di un tenant in un altro tenant 45

Stato della rete dei workload 86

Stato di installazione patch 94

Stato protezione 82

Superamento della quota per l'archivio di backup 18

T

Tipi di tenant che è possibile spostare 45

Tipo di rapporto 100

Trasferimento della titolarità di un account utente 59

Trasformazione di una quota di backup 18

U

Upsell 75

URL bloccati 97

URL per i servizi Cyber Protect Cloud 75

Utilizzo 80, 100

Utilizzo del portale di gestione 25

Utilizzo delle modalità di fatturazione con le edizioni Legacy 8

V

Versioni di VMware Cloud Director supportate 140

Vulnerabilità esistenti 93

W

Widget del report Riepilogo esecutivo 107

Widget del servizio Notary 115

Widget di Backup 111

Widget di Disaster Recovery 113

Widget di Endpoint Detection and Response (EDR) 84

Widget di File Sync & Share 115

Widget di installazione patch 94

Widget di integrità del disco 88

Widget di Protezione antimalware 110

Widget di valutazione delle vulnerabilità 93

Widget Inventario hardware 99

Widget Inventario software 97

Widget Panoramica dei workload 107

Widget Prevenzione della perdita di dati 114

Widget Valutazione della vulnerabilità e gestione patch 112