Portale di gestione

25.05

Manuale dell'amministratore di partner

REVISIONE: 06/06/2025

Sommario

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 un'area funzionale specifica, ad esempio Advanced Backup, Advanced Security + XDR e altri. Questi pacchetti estendono le funzionalità disponibili con il servizio Cyber Protect standard.
    Per ulteriori informazioni sui pacchetti Advanced Protection, vedere "Pacchetti Advanced Protection" (pag. 172).
  - **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. 8).

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. 11).

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 gestione patch, in 2 delle workstation è abilitato il filtro 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 + XDR - 2/10 • Advanced Backup Workstation - 1/10 • Advanced Management (RMM) - 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 (RMM), 2 utilizzano le funzionalità del pacchetto Advanced Security + XDR 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

Elementi dell'offerta di origine - utilizzo/quota	Elementi dell'offerta di destinazione - utilizzo/quota
	• Advanced Security + XDR - 13/42 • Advanced Management (RMM) - 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, passare 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, passare 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 in offerta può influenzare la disponibilità del tipo di workload nella console di Cyber Protect?

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. 8).

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. 85).

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. 9).

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. 17).

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
Storage di backup	Può essere disabilitato quando il	Il cloud storage non è più disponibile come destinazione dei backup di un tenant cliente.

	consumo è pari a zero.	
Backup locale	Può essere disabilitato quando il consumo è pari a zero.	Lo storage locale diventerà non disponibile come destinazione per i backup all'interno di un tenant cliente. Disabilitando la quota di backup locale si disabiliteranno i backup su dischi locali, condivisioni di rete e cloud pubblici, come S3 compatibile, Azure, AWS, Wasabi e Impossible Cloud.
Origini dei dati (incluso Microsoft 365 e Google Workspace)*	Può essere disabilitato quando il consumo è pari a zero.	La protezione delle origini dei dati disabilitate (incluse Microsoft 365 e Google Workspace) non sarà più disponibile per il tenant cliente, come indicato di seguito:
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.

* Gli elementi in offerta sono relativi ai workload che è possibile aggiungere nella console di Cyber Protect. Per ulteriori informazioni, fare riferimento a "Dipendenza del workload dagli elementi in offerta" (pag. 29). La tabella seguente riepiloga quali tipi di workload non saranno disponibili se un elemento in offerta, una combinazione di elementi in offerta o un Advanced Pack non sono abilitati nel portale di gestione.

Se i seguenti elementi in offerta o Advanced Pack vengono disabilitati	Non sarà possibile aggiungere questi tipi di workload
La seguente combinazione: • Utenze di Microsoft 365 • Microsoft 365 SharePoint online • Microsoft 365 Teams	Microsoft 365 Business
La seguente combinazione: • Google Workspace • Google Workspace Shared Drive	Google Workspace
La seguente combinazione: • Server • Virtual machine	• Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory
L'elemento in offerta seguente: • NAS	Synology
L'elemento in offerta seguente: • Mobile	• Dispositivi iOS • Dispositivi Android
L'Advanced Pack seguente: • Advanced Backup	Database Oracle
La seguente combinazione: • Utenze di archiviazione e-mail • Storage di archiviazione	Server di posta

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 rigida, il servizio viene limitato: non sarà possibile proteggere un altro workload o utilizzare più storage. Quando viene superata una quota rigida, 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 rigide

Per impostare le quote dei clienti

1. Nel portale di gestione, passare 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 flessibile**.
     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 rigida** e impostare il valore della quota nel campo al di sotto di **Quota rigida**.
  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**.

Importante
I valori di utilizzo dello storage visualizzati nell'interfaccia utente del prodotto sono espressi in unità di byte binari: mebibyte (MiB), gibibyte (GiB) e tebibyte (TiB), anche se le rispettive etichette visualizzano MB, GB e TB. Ad esempio, se l'utilizzo effettivo è di 3105886629888 byte, il valore nell'interfaccia utente viene visualizzato correttamente come 2,82, ma l'etichetta riporta TB invece che TiB.

Quote del servizio Backup

È possibile specificare la quota di cloud storage, 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**
- **Virtual machine**
- **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**
  Questo limite viene applicato dal service provider all'intera azienda. Gli amministratori dell'azienda possono visualizzare la quota e il suo utilizzo nel portale di gestione. Quando la quota fissa viene superata, non è possibile applicare i piani di backup alle nuove utenze.
  La fatturazione di questa quota dipende dalla modalità di fatturazione selezionata per Cyber Protection.

- Nella modalità di fatturazione **Per gigabyte**, la fatturazione si basa solo sull'utilizzo dello storage e le utenze non vengono conteggiate.
- Nella modalità di fatturazione **Per workload**, la fatturazione si basa sul numero di utenze Microsoft 365 protette. L'utilizzo dello storage viene fatturato solo per le utenze non protette.

  La tabella seguente riassume la modalità di fatturazione **Per workload**.

	Posizione del backup	
	Storage su host Acronis* Storage su host del Partner	**Storage Microsoft Azure Storage Google**
Utenza protetta	La fatturazione è calcolata in base al numero di utenze protette. Lo spazio di storage utilizzato dai backup delle utenze protette non viene fatturato.	Vengono fatturati sia le utenze protette che lo storage utilizzato.
Utenza non protetta	Le utenze non protette non vengono fatturate. Lo spazio di storage utilizzato dai backup delle utenze non protette viene fatturato.	Le utenze non protette non vengono fatturate. Lo spazio di storage utilizzato dai backup delle utenze non protette viene fatturato.

  * Si applica la Politica sul Fair Usage per Acronis Storage. I termini e le condizioni sono disponibili all'indirizzo https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage.

Un'utenza è considerata protetta quando un utente di Microsoft 365 dispone di uno qualsiasi tra i seguenti elementi:

- Casella di posta a cui è applicato un piano di backup
- OneDrive a cui è applicato un piano di backup
- 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, consultare questo articolo della Knowledge Base.

Un'utenza può perdere la protezione nei casi seguenti:

- A un utente viene revocato l'accesso a una risorsa protetta a livello aziendale, ad esempio un sito di Microsoft 365 SharePoint Online o Microsoft 365 Teams.
- Tutti i piani di backup vengono revocati dalla casella di posta o dal OneDrive di un utente.
- Un utente viene eliminato dall'organizzazione Microsoft 365.

Le risorse 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.

Nota
Gli utenti Microsoft 365 bloccati che non dispongono di una casella di posta personale o di OneDrive protetti e possono accedere solo a risorse condivise (caselle di posta condivise, siti SharePoint e Microsoft Teams) non riceveranno alcun addebito. Gli utenti bloccati sono quelli che non dispongono di un accesso valido e non possono accedere ai servizi Microsoft 365. Per sapere come bloccare tutti gli utenti senza licenza in un'organizzazione Microsoft 365, consultare "Impedire l'accesso agli utenti di Microsoft 365 senza licenza" (pag. 24).

Importante
L'agente locale e l'agente cloud consumano quote distinte. Se si esegue il backup degli stessi workload utilizzando entrambi gli agenti, l'addebito avviene due volte. Per esempio:
- Se si esegue il backup delle caselle di posta di 120 utenti tramite l'agente locale e si esegue il backup dei file di OneDrive degli stessi utenti tramite l'agente cloud, verranno addebitate 240 utenze di Microsoft 365.
- Se si esegue il backup delle caselle di posta di 120 utenti tramite l'agente locale e si esegue il backup delle stesse caselle di posta anche tramite l'agente cloud, verranno addebitate 240 utenze di Microsoft 365.

Per consultare le domande frequenti sul licensing delle utente di Microsoft 365, consultare Cyber Protect Cloud: Licensing per GB di Microsoft 365 e Cyber Protect Cloud: Modifiche di pricing e licensing per Microsoft 365.

- **Microsoft 365 SharePoint Online**

  Questa quota è applicata dal service provider all'intera azienda. La quota abilita la protezione dei 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 nei report di utilizzo, insieme alla quantità di storage occupato dai backup di SharePoint Online.
- **Microsoft 365 Teams**

  Questa quota è applicata dal service provider per l'intera azienda. Questa quota abilita o disabilita la possibilità di proteggere Microsoft 365 Teams 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.
- **Utenze di archiviazione e-mail di Microsoft 365**

  La quota **Utenze di archiviazione e-mail di Microsoft 365** abilita o disabilita la possibilità di creare un archivio e-mail per i server Microsoft 365 e imposta il numero massimo di caselle di posta che possono essere aggiunte all'archivio.
- **Utenze di archiviazione e-mail (obsolete)**

Questa quota è obsoleta e non è possibile abilitarla durante la creazione di nuovi tenant nel portale di gestione.

Per i tenant esistenti, è possibile disabilitare la quota solo se è già stata abilitata, ma non è più possibile abilitarla.

Importante

Quando si creano nuovi tenant cliente, utilizzare la quota di **Utenze di archiviazione di Microsoft 365**.

Per i clienti esistenti, la quota **Utenze di archiviazione e-mail (obsolete)** verrà sostituita automaticamente dalla quota **Utenze di archiviazione di Microsoft 365**. Qualsiasi utilizzo esistente sotto **Utenze di archiviazione e-mail (obsolete)** verrà trasferito a **Utenze di archiviazione di Microsoft 365**.

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.

Un'utenza di Google Workspace è considerata protetta se almeno un piano di backup è applicato alla casella di posta o al Google Drive dell'utente.

Quando la quota fissa viene superata, un amministratore dell'azienda non può applicare un piano di backup alle nuove utenze.

- **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.

Quote per archivio

Importante

I valori di utilizzo dello storage visualizzati nell'interfaccia utente del prodotto sono espressi in unità di byte binari: mebibyte (MiB), gibibyte (GiB) e tebibyte (TiB), anche se le rispettive etichette visualizzano MB, GB e TB. Ad esempio, se l'utilizzo effettivo è di 3105886629888 byte, il valore nell'interfaccia utente viene visualizzato correttamente come 2,82, ma l'etichetta riporta TB invece che TiB.

- **Risorse cloud**
  - **Storage di backup**
    - **Storage di backup**

      Questa quota limita la dimensione totale dei backup che si trovano nel cloud storage. Quando la quota fissa dello storage di backup viene superata, l'operazione di backup non viene avviata.

      In modalità di fatturazione **Per workload**, questa quota si applica solo ai backup di workload diversi da Microsoft 365 e Google Workspace.

      Lo storage di backup per i workload di Microsoft 365 e Google Workspace è illimitato*. Se una quota di licenze, come **licenze di Microsoft 365** o **licenze di Google Workspace**, viene rimossa da un workload, lo storage di backup rimane illimitato, ma il suo utilizzo sarà a pagamento.

      Con la modalità di fatturazione **Per gigabyte**, questa quota si applica a tutti i backup, inclusi i backup dei workload Microsoft 365 e Google Workspace.

      * Si applica la Politica sul Fair Usage per Acronis Storage. I termini e le condizioni sono disponibili all'indirizzo https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage.
    - **Storage di archiviazione**

      Questa quota limita la dimensione totale dell'archivio e-mail nell'infrastruttura cloud.
  - **Advanced Disaster Recovery**

    Questa sezione contiene le quote relative al disaster recovery.
- **Risorse locali**
  - **Backup locale**

    La quota di **Backup locale** limita la dimensione totale dei backup su dischi locali, condivisioni di rete e cloud pubblici, come S3 compatible, Azure, AWS, Wasabi e Impossible Cloud.
    - Non è possibile definire un extra per questa quota.
    - Ai backup locali non può essere applicata una quota fissa.

    Nota
    Disattivando la quota di **Backup locale**, verranno disattivati i backup locali, i backup nelle condivisioni di rete e i backup nei cloud pubblici.

Superamento della quota per lo storage di backup

La quota di storage di 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.

Importante
I valori di utilizzo dello storage visualizzati nell'interfaccia utente del prodotto sono espressi in unità di byte binari: mebibyte (MiB), gibibyte (GiB) e tebibyte (TiB), anche se le rispettive etichette visualizzano MB, GB e TB. Ad esempio, se l'utilizzo effettivo è di 3105886629888 byte, il valore nell'interfaccia utente viene visualizzato correttamente come 2,82, ma l'etichetta riporta TB invece che TiB.

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 di Cyber Protect.

Esempio

Si desidera eseguire il backup di una virtual machine (workstation, con agente).

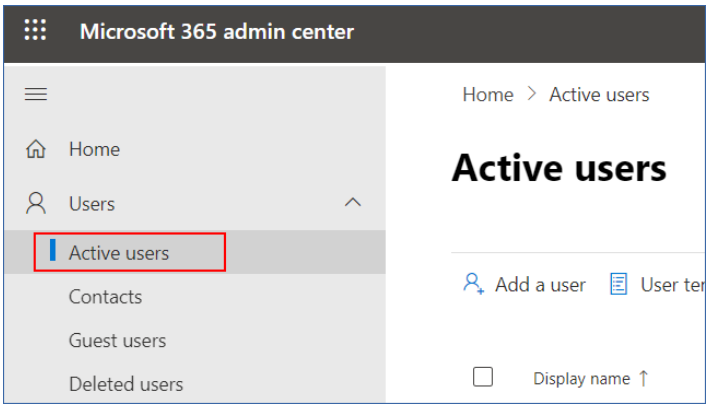
In primo luogo, il sistema controlla se è presente una quota **Virtual machine** allocata. Se non viene individuata, il sistema tenta automaticamente di acquisire la quota **Workstation**. Se non viene trovata neanche questa, l'altra quota non verrà acquisita automaticamente. Se è disponibile una quota sufficiente più costosa rispetto alla quota **Virtual machine** e se questa è applicabile a una virtual machine, è possibile accedere alla console di Cyber Protect 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.

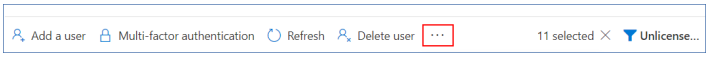
Per impedire l'accesso agli utenti senza licenza

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 di backup dei server protetti con Disaster Recovery. L'uso dello storage di disaster recovery equivale all'uso dello storage di backup dei workload protetti con i server di 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. 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 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 nella console di Cyber Protect, 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**

  Definisce il limite al numero di utenti di File Sync & Share.

  Nota
  Alla composizione di questa quota partecipano solo i ruoli Utente e Utente più Amministratore. I ruoli Amministratore e Guest sono esclusi dalla quota.

- **Cloud storage**

  Definisce il limite del cloud storage allocato per il tenant.

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 macchine 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**

  Definisce lo spazio massimo di cloud storage per i file autenticati, i file firmati e i file di cui è in corso il processo di autenticazione o di firma.

  Per diminuire l'utilizzo di questa quota, è possibile eliminare dallo storage i file già autenticati o firmati.
- **Autenticazioni**

  Definisce il numero massimo di file autenticabili tramite il servizio di autenticazione.
  Un file viene considerato autenticato non appena viene caricato nello storage 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**

  Definisce il numero massimo di firme elettroniche.

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 di Cyber Protect, 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 **Modifica quota**, selezionare la quota di servizio o la voce **Nessuna quota**, quindi fare clic su **Modifica**.

Per modificare la quota di servizio di un gruppo di sistemi

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

Dipendenza del workload dagli elementi in offerta

In base agli elementi in offerta abilitati, nel pannello **Aggiungi dispositivi** nella console di Cyber Protect verranno visualizzati diversi tipi di workload. La tabella seguente riepiloga quali tipi di workload saranno disponibili con i diversi elementi in offerta.

Tipo di workload (Programma di installazione dell'agente)	**Elementi in offerta abilitati**										
	Server	**Workstation**	**Virtual machine**	**Utenze di Microsoft 365**	**Utenze di Google Workspace**	**Dispositivi mobili**	**Server di web hosting**	**Siti Web**	**NAS**	**Utenze di archiviazione e-mail**	**Storage di archiviazione**
Workstation – Agente per Windows		+	+					+			
Workstation – Agente per macOS		+	+					+			
Server – Agente per Windows	+		+				+	+			
Server – Agente per Linux	+		+				+	+			
Agente per Hyper-V			+								
Agente per VMware			+								
Agente per Virtuozzo			+								

Tipo di workload (Programma di installazione dell'agente)	Elementi in offerta abilitati										
	Server	Workstation	Virtual machine	Utenze di Microsoft 365	Utenze di Google Workspace	Dispositivi mobili	Server di web hosting	Siti Web	NAS	Utenze di archiviazione e-mail	Storage di archiviazione
Agente per SQL	+		+								
Agente per Exchange	+		+								
Agente per Active Directory	+		+								
Agente per Synology									+		
Workload di Microsoft 365 Business				+							
Workload di Google Workspace					+						
Server di posta										+	+
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, consultare "Requisiti per la password" (pag. 31).

Requisiti per la password

La complessità delle password viene controllata durante la registrazione dell'utente; le password vengono classificate secondo le seguenti categorie:

- Vulnerabile
- Medio
- Complessa

Non è possibile salvare una password vulnerabile, anche se la sua lunghezza è corretta. 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.

Nota
I requisiti della password sono soggetti a modifiche.

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

Dopo aver attivato l'account amministratore, è possibile accedere al portale di gestione utilizzando le credenziali di accesso e la password impostate.

Per accedere al portale di gestione per la prima volta

1. Passare alla pagina di accesso al servizio.
   L'indirizzo della pagina di login era incluso nell'e-mail di attivazione ricevuta 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. Completare il questionario di onboarding.
   Per ulteriori informazioni sulle opzioni di onboarding, consultare "Questionario di onboarding" (pag. 32).
5. 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.

Questionario di onboarding

Il questionario di onboarding deve essere completato dal primo amministratore partner del tenant al primo accesso al portale di gestione. Questo questionario si adatta dinamicamente in base alle risposte dell'amministratore riguardo agli interessi primari, al modello di business e alle dimensioni dell'azienda. Personalizzando l'esperienza di onboarding in base alle esigenze e agli interessi dell'azienda, il processo diventa più rilevante ed efficiente.

Il questionario non può essere saltato o chiuso. Tutte le domande sono obbligatorie.

Configurazione dei contatti nella procedura guidata Profilo dell’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 dell’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 dell’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 **La mia azienda > Profilo dell'azienda** della console di gestione, come descritto in Configurazione dei contatti aziendali.

Accesso alla console di Cyber Protect 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**.

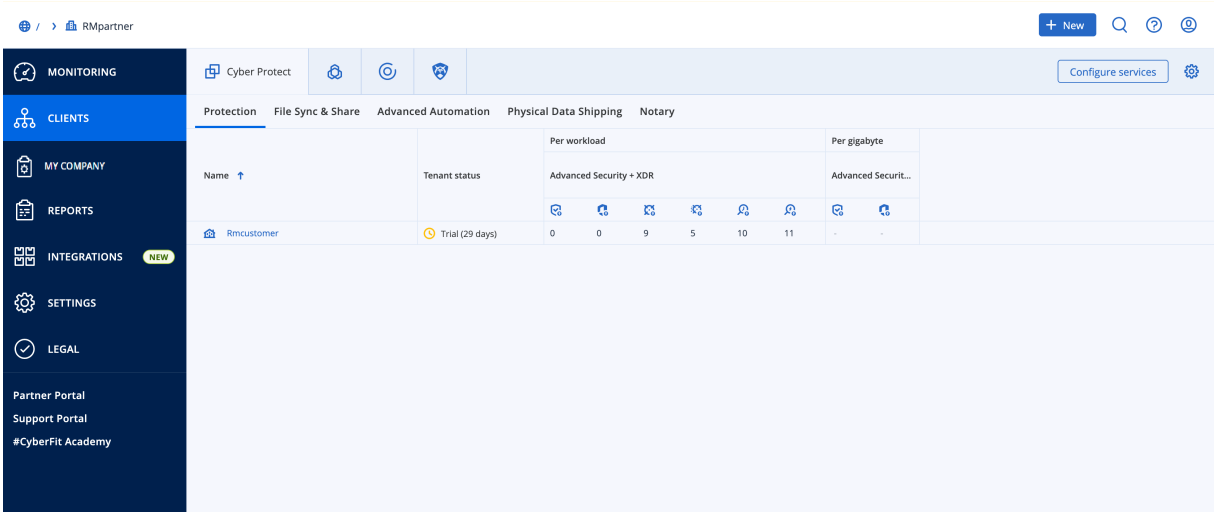
L'utente viene reindirizzato alla console di Cyber Protect.

Importante
Se per il cliente è attiva la modalità di gestione **Self-service**, non sarà possibile gestire i servizi per suo conto. Solo gli amministratori del cliente possono modificare la modalità in **Gestito dal service provider** e a questo punto gestirne i servizi.

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 oggetti figlio diretti del tenant nel quale si sta lavorando.
- La scheda **La mia azienda** visualizza il profilo dell'azienda e gli account utente esistenti nel tenant nel quale si sta lavorando.
- La scheda **Monitoraggio** visualizza informazioni sull'utilizzo e sulle operazioni degli oggetti figlio diretti del tenant nel quale si sta operando.

  Nota
  In questa scheda possono essere disponibili opzioni aggiuntive, a seconda dei servizi sottoscritti.

- Il pulsante **Nuovo** consente di creare un tenant o un nuovo account utente solo nel tenant nel quale si sta lavorando.

  Nota
  Nel menu possono essere disponibili ulteriori opzioni, a seconda dei servizi sottoscritti. Ad esempio, se è stato attivato Advanced Automation (PSA), è anche possibile creare nuovi ticket e registrazioni orarie.

Casella di posta in arrivo personale

La pagina Casella di posta in arrivo personale è stata progettata per ottimizzare la comunicazione all'interno dell'applicazione. Le indicazioni di questa guida consentono di gestire i messaggi in modo efficace e organizzato e di incrementare la produttività. La casella di posta del prodotto è il punto centrale in cui ricevere e gestire le comunicazioni nell'applicazione, e consente di ricevere aggiornamenti, messaggi e avvisi importanti correlati al proprio flusso di lavoro.

Panoramica

La scheda **Casella di posta in arrivo personale** include un contatore delle notifiche che visualizza il numero di notifiche non lette. Facendo clic sul contatore vengono visualizzate le notifiche non lette, così da tenere traccia delle voci in sospeso. Inoltre, i contatori accanto a ogni filtro (categoria, importanza, azione) mostrano il numero di notifiche disponibili per lo specifico filtro, facilitando la visualizzazione del numero di notifiche appartenenti a ogni categoria.

Nella posta in arrivo personale l'utente riceve varie notifiche, ognuna progettata per una finalità specifica in base alle impostazioni e al contesto dell'account utente: annunci di nuove funzionalità, nuovi corsi di formazione disponibili, inviti a eventi e webinar, promemoria sulla scadenza dei certificati, promozioni, avvisi di manutenzione, sondaggi e altro.

Controllo delle notifiche

Controllo della sezione notifiche

1. Accedere alla console di Cyber Protect Cloud.
2. Nel riquadro di navigazione, selezionare la voce di menu **Casella di posta in arrivo personale**.

Ricerca nella Casella di posta in arrivo personale

Per cercare i messaggi non letti

1. Fare clic sulla voce di menu **Casella di posta in arrivo personale**.
2. Nell'angolo in alto a destra, attivare l'opzione **Mostra solo non letti**.

Per cercare informazioni importanti nella posta in arrivo personale

1. Accedere alla **Casella di posta in arrivo personale** dalla dashboard di Cyber Protect Cloud.
2. Nella visualizzazione della posta in arrivo, individuare la barra **Cerca** nella parte superiore.
3. Inserire parole chiave o nomi dei mittenti per filtrare i messaggi.
4. Premere **Invio** per visualizzare i risultati della ricerca.

I risultati mostrano tutte le notifiche che corrispondono ai criteri di ricerca.

Novità del portale di gestione

Quando vengono rilasciate le nuove funzionalità di Cyber Protect Cloud, all'accesso al portale di gestione viene visualizzata una finestra popup con una breve descrizione delle novità.

La descrizione delle nuove funzionalità è inoltre visualizzabile facendo clic sul link **Novità** nell'angolo in basso a sinistra della finestra principale del portale di gestione.

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.

Importante
L'attivazione del controllo degli accessi impedisce il ripristino dal cloud storage utilizzando supporti di avvio non registrati. Consultare questo articolo della Knowledge Base.

Nota
- Questa limitazione si applica anche all'accesso al portale di gestione tramite API.
- Questa limitazione è valida solo per il livello in cui è impostata. Non si applica ai membri dei tenant figli.

Per limitare l'accesso all'interfaccia Web

1. Passare al tenant per il quale si desidera limitare l'accesso.
2. Fare clic su **Impostazioni** > **Sicurezza**.

3. Abilitare l'interruttore **Controllo accesso**.
4. 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
5. 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**.

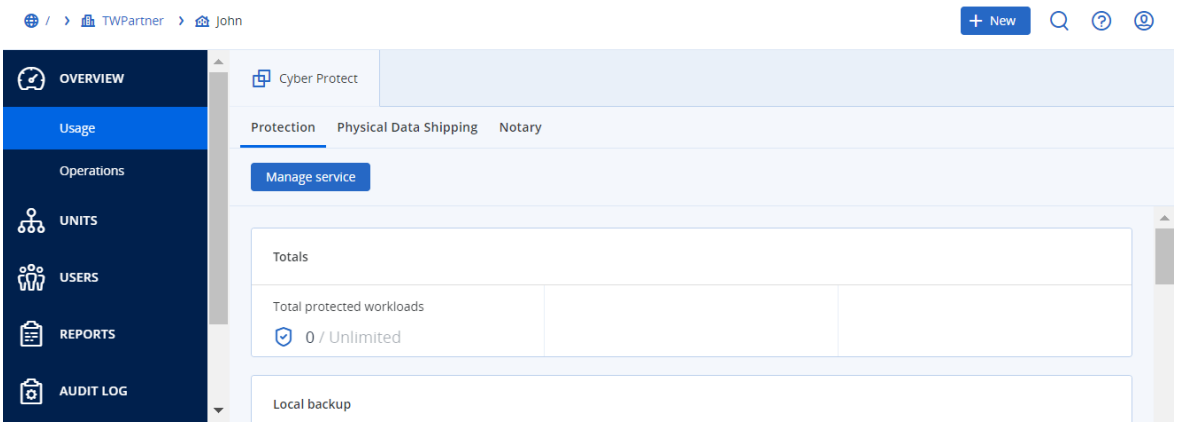
Accesso ai servizi

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.

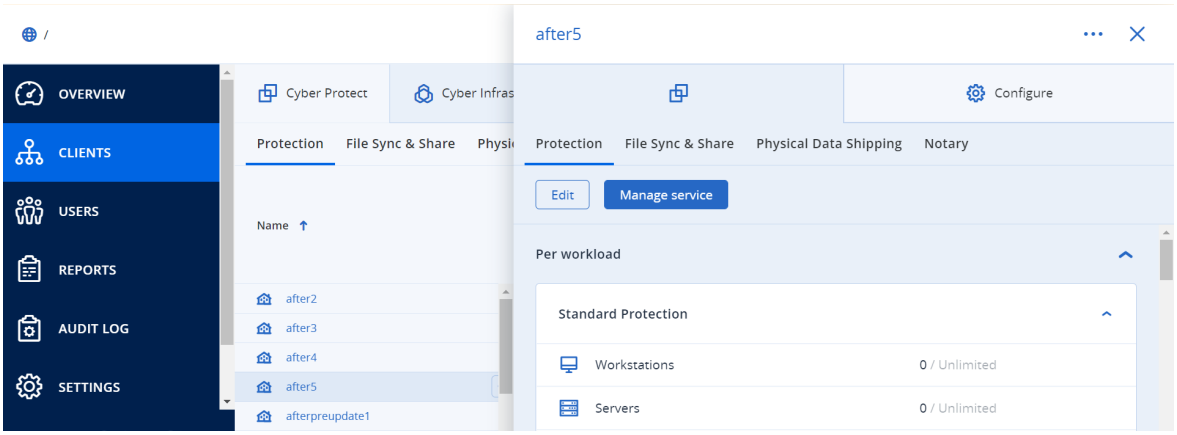


Scheda Clienti

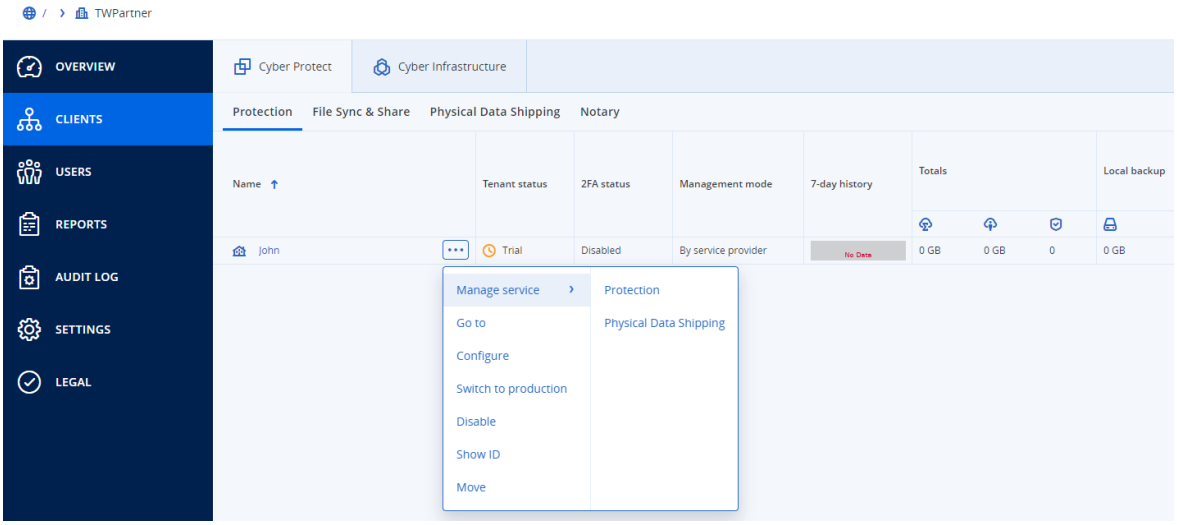
La scheda **Clienti** visualizza i tenant figlio del tenant nel quale si sta lavorando e consente di accedere ai servizi che questi contengono.

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.

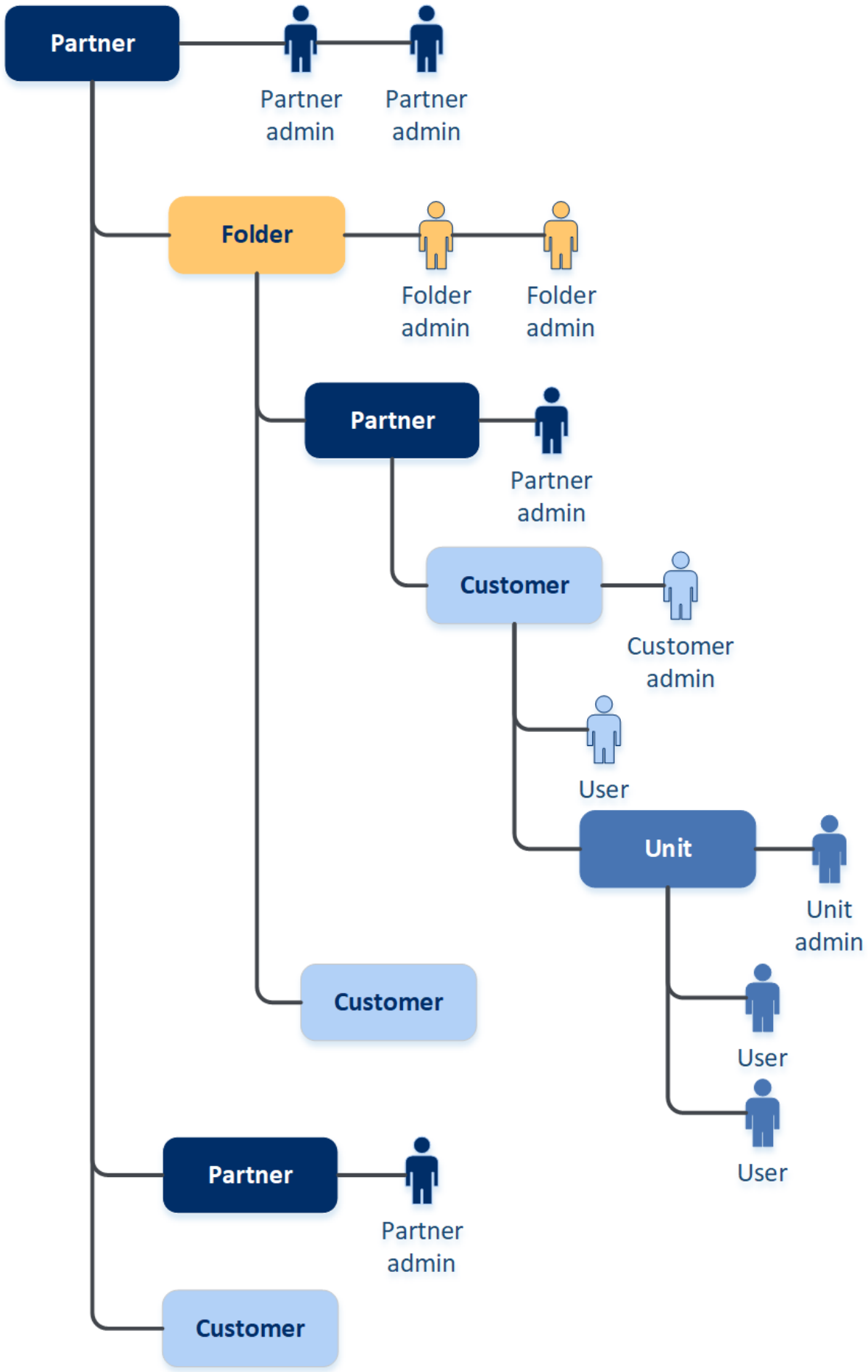
Ogni account appartiene a un tenant. Un tenant è un componente delle risorse del portale di gestione (come gli account utente e i tenant figlio) e delle offerte di servizi (servizi abilitati ed elementi offerti che questi contengono) dedicati a un partner o a un cliente. La gerarchia del tenant dovrebbe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

Nota

- È possibile creare un utente da qualsiasi tipo di tenant; potrà avere un indirizzo e-mail condiviso a condizione che la creazione avvenga dal tenant con più privilegi a quello con meno privilegi. Ad esempio, da un tenant Partner è possibile creare un tenant Cartella, Cliente e Unità, mentre un tenant Cliente non consente la creazione di un tenant Cartella.
- Gli amministratori dell'unità non possono creare, modificare o applicare i piani di protezione Disaster Recovery.

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.

   I tipi disponibili dipendono dal tipo di tenant parent. Se il servizio Advanced Automation (PSA) è abilitato, è anche possibile selezionare il tipo di tenant pertinente nella sezione **Dati di fatturazione** (consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47)).
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]
   a. In **Modalità operativa**, indicare se il tenant utilizza i servizi in modalità di prova o in modalità di produzione. I report mensili sull'utilizzo del servizio includono i dati sul consumo dei tenant in entrambe le modalità.

      Importante
      La modalità di prova offre un periodo di valutazione di 30 giorni con accesso completo al prodotto. Tenere presente che quando per il cliente viene attivata la modalità di produzione, l'utilizzo viene incluso automaticamente nel ciclo di fatturazione più vicino.
      È possibile passare alla modalità di produzione in qualsiasi momento. Non è possibile tornare dalla modalità di produzione a quella di prova.
      Se si decide di annullare la versione di prova di un cliente, è necessario cancellare anche il tenant cliente corrispondente. In caso contrario, allo scadere dei 30 giorni di prova viene automaticamente attivata la modalità di produzione e l'utilizzo corrispondente viene incluso nel ciclo di fatturazione più vicino. Per ulteriori informazioni, consultare questo articolo della Knowledge Base.

b. In **Impostazioni avanzate**, selezionare la modalità di gestione per il tenant.
   - **Gestito dal service provider**: questa modalità concede l'accesso completo al cliente agli amministratori del tenant padre e consente loro di modificare le proprietà, gestire i tenant, gli utenti, i servizi; accedere ai backup e ad altre risorse. Questa modalità è selezionata per impostazione predefinita.
   - **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, unità, servizi, backup e altre risorse).

   Nota
   Se si seleziona **Self-service**, solo l'amministratore del tenant cliente potrà modificare la modalità di gestione. A tal fine, l'amministratore del cliente deve passare a **Impostazioni** > **Sicurezza** e abilitare l'opzione **Accesso al supporto**.

Per verificare la modalità di gestione selezionata per i tenant figlio, aprire la scheda **Clienti**.

7. [Solo durante la creazione di un tenant partner] In **Impostazioni avanzate**, selezionare una delle modalità seguenti per la gestione dell'accesso al tenant:
   - **Accesso completo**: questa modalità concede l'accesso completo al tenant agli amministratori del tenant padre e consente loro di gestire le quote, gli utenti e le proprietà del Partner, accedere ai clienti del Partner e ottenere i report sull'utilizzo del Partner e dei suoi clienti. Questa modalità è selezionata per impostazione predefinita.
   - **Accesso limitato**: questa modalità limita l'accesso a questo tenant partner agli amministratori del tenant padre e consente loro di modificare le proprietà e le quote del tenant e di ottenere i report sull'utilizzo per il Partner; non potranno accedere o gestire nulla di quanto contenuto nel tenant (ad esempio tenant, utenti, servizi, backup e altre risorse del Partner) né richiedere i report sull'utilizzo per i clienti del Partner.

   Nota
   Se si seleziona **Accesso limitato**, solo l'amministratore del tenant può modificare la modalità di gestione. A tal fine, l'amministratore deve passare a **Impostazioni** > **Sicurezza** e abilitare 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 (2FA) per il tenant.
   Se l'autenticazione 2FA è abilitata, tutti gli utenti del tenant sono tenuti a configurarla 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 Conformità] In **Sicurezza**, selezionare la casella di controllo **Modalità Conformità**.

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, consultare "Modalità Conformità" (pag. 46).

Importante
Non è possibile disabilitare la modalità Conformità 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 l'indirizzo l'e-mail dell'account dell'amministratore. Questo indirizzo e-mail viene utilizzato anche per il login.
b. Se si preferisce utilizzare un indirizzo di login diverso dall'e-mail, selezionare la casella di controllo **Usa un login diverso dall'e-mail**, quindi inserire un nome di login e l'indirizzo 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.
c. Selezionare la lingua.
   Se non viene selezionata alcuna lingua, viene utilizzata la lingua inglese per impostazione predefinita.
d. 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. 48).

13. [Se Advanced Automation (PSA) è attivato] Inserire le informazioni di fatturazione per il cliente. Per ulteriori informazioni, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47).

Modalità Conformità

La modalità Conformità è progettata per clienti con esigenze di sicurezza più elevate. Tale modalità richiede la crittografia obbligatoria di tutti i backup e consente soltanto l'uso di password di crittografia impostate a livello locale.

In modalità Conformità, tutti i backup creati in un tenant cliente e nelle relative unità vengono crittografati automaticamente con l'algoritmo AES e una 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.

Importante
Un amministratore del Partner può abilitare la modalità Conformità 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 Conformità per tenant già esistenti.

Limitazioni

- La modalità Conformità è compatibile solo con gli agenti la cui versione è 15.0.26390 o superiore.
- La modalità Conformità non è disponibile per i dispositivi che eseguono Red Hat Enterprise Linux 4.x o 5.x e i loro derivati.
- I servizi cloud non possono accedere alle password di crittografia. A causa di questa limitazione, alcune funzionalità non sono disponibili ai tenant in modalità Conformità.

Funzionalità non supportate

Le funzionalità seguenti non sono disponibili ai tenant in modalità Conformità:

- Ripristino mediante la console di Cyber Protect
- Esplorazione dei backup a livello di file mediante la console di Cyber Protect
- Accesso alla console Web Restore
- Backup da cloud a cloud
- Backup di siti web
- Backup di applicazioni
- Backup di dispositivi mobili
- Scansione anti-malware dei backup
- Ripristino sicuro
- Creazione automatica di elenchi degli elementi consentiti aziendali

- Mappa di protezione dati
- Disaster Recovery
- Report e dashboard correlati alle funzionalità non disponibili

Definizione delle informazioni di fatturazione per un tenant

Se Advanced Automation (PSA) è attivato per il tenant, è necessario definire le informazioni di fatturazione per il cliente che viene creato. Le informazioni di fatturazione garantiscono la corretta fatturazione dei servizi e dei prodotti forniti.

Nota
Se le informazioni di fatturazione non vengono definite in questa fase, verrà richiesto di inserire i dati pertinenti prima di poter utilizzare determinate funzionalità di Advanced Automation (PSA), ad esempio l'approvazione delle registrazioni orario o la creazione di contratti o articoli di vendita. Per ulteriori informazioni, consultare "Onboarding di clienti esistenti" (pag. 209).

Per definire le informazioni di fatturazione

1. Nella sezione **Dati di fatturazione** della finestra di dialogo di creazione/modifica del tenant, definire i campi seguenti:
   - **Nome azienda**: il nome dell'azienda del tenant; è preselezionato come nome del tenant cliente.
   - **Tipo**: il tipo di tenant di Advanced Automation (PSA) (selezionare tra **Partner**, **Cliente**, **Potenziale cliente**).
   - **E-mail**: L'indirizzo e-mail del tenant predefinito con l'indirizzo e-mail dell'amministratore utilizzato nella sezione **Informazioni generali**.
   - **Lingua**: selezionare la lingua pertinente al tenant.
   - **Paese**: selezionare il paese pertinente al tenant.
   - **Imposta vendite**: selezionare l'imposta di vendita per il tenant. Se non viene selezionata alcuna imposta di vendita, viene applicata l'aliquota imposta predefinita. È anche possibile selezionare la casella di controllo **Esente da imposte** se per il tenant è in vigore un'esenzione dalle imposte.
2. [Facoltativo] Fare clic su **Impostazioni avanzate** per definire ulteriori informazioni di fatturazione. Alcuni campi di questa sezione sono facoltativi e alcuni sono preimpostati dal sistema.
   - **ID esterno**: il codice cliente utilizzato nei sistemi di terze parti, ad esempio i software di contabilità.
   - **Sito web**: il sito web del tenant.
   - **Arrotondamento registrazione orario (minuti)**: Impostare l'orario in minuti dell'arrotondamento della registrazione orario. Quando il lavoro sul ticket viene approvato per la fatturazione, le ore totali fatturabili verranno arrotondate in base a questo valore. Ad esempio, se si imposta il valore dell'arrotondamento su 15 minuti, se vengono svolti 7 minuti

di lavoro sul ticket, questi verranno arrotondati a 15 minuti prima della fatturazione. Allo stesso modo, 21 minuti vengono arrotondati a 30, 36 minuti a 45 e così via. Il valore predefinito è **10**.

- **Termini di pagamento (giorni)**: definire il numero di giorni entro i quali il cliente deve effettuare il pagamento.
- **Invia fatture tramite**: selezionare il metodo (**E-mail** o **Posta**) per l'invio delle fatture per questo cliente. Questa impostazione annulla l'impostazione di fatturazione predefinita. Per ulteriori informazioni, consultare "Definizione delle impostazioni di fatturazione predefinite" (pag. 336).
- **Metodo di pagamento**: scegliere **Pagamento manuale** o **Addebito diretto** per definire l'opzione di pagamento della fattura predefinita per il cliente. Questa opzione può essere adattata nei preventivi, nei contratti e negli articoli di vendita, come necessario. Se si seleziona **Addebito diretto**:
  - I clienti potranno saldare le fatture tramite bonifico o utilizzando una delle integrazioni con i sistemi di pagamento (PayPal, Stripe) disponibili.
  - I clienti potranno inviare le fatture ai rispettivi istituti bancari per l'elaborazione dell'addebito diretto.
- **Crea subtotali in fattura**: selezionare la casella di controllo, se necessario.
- **Conto bancario**: inserire il numero di conto bancario per il tenant.
- **Partita IVA/Codice fiscale**: il numero di partita Iva o codice fiscale pertinente.
- **Sede principale**: selezionare la società capogruppo dall'elenco.

3. Nella sezione **Indirizzo**, compilare i campi indirizzo pertinenti.
4. Per configurare i servizi per il tenant, fare clic su **Avanti**. Vedere "Selezione dei servizi per un tenant" (pag. 48).

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. 50).

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. 49).

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.
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).

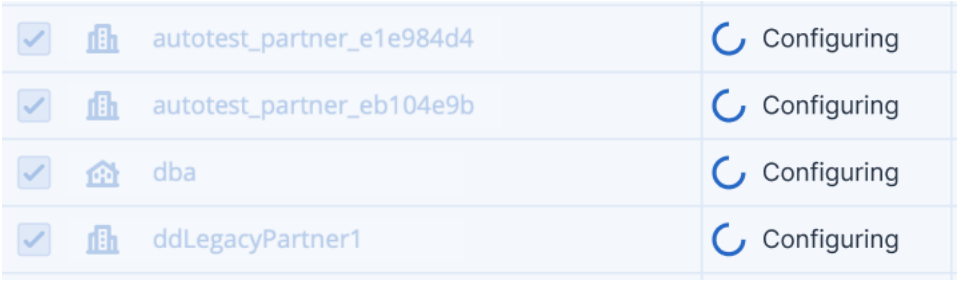
Questa procedura è applicabile a tenant radice secondaria, partner, cartella e cliente. È possibile selezionare simultaneamente anche tenant di tipo diverso.

Per abilitare i servizi per più tenant

1. Nel portale di gestione, passare 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 le 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.

Visualizzazione e aggiornamento della configurazione di un tenant

Dopo aver creato e configurato un tenant, è possibile visualizzare e aggiornare i servizi e le offerte configurate per tale tenant come e quando necessario.

Per visualizzare e aggiornare la configurazione di un tenant

1. Nel portale di gestione, passare a **Clienti**.
2. Fare clic sull'icona dei puntini di sospensione relativa al tenant da visualizzare o aggiornare e quindi selezionare **Configura**.
3. Nel riquadro a destra è possibile:
   - Aggiornare le impostazioni dei servizi disponibili facendo clic sulla scheda del servizio pertinente. Ad esempio, fare clic sulla scheda **Protezione** per aggiornare e gestire questo servizio.
   - Fare clic sulla scheda **Configura** per visualizzare e aggiornare le sezioni nella configurazione del tenant, incluso:
     - **Servizio**: Abilitare e disabilitare i servizi, come necessario.
     - **Profilo dell'azienda**: aggiornare il profilo dell'azienda e aggiungere o rimuovere i contatti aziendali, come necessario.
     - **Impostazioni generali**: aggiornare le informazioni generiche sull'azienda, incluso il nome, il paese, la lingua e lo stato della modalità Conformità.
     - **Dati di fatturazione**: disponibile solo per il servizio Advanced Automation (PSA) attivato, consente di aggiornare le informazioni per la fatturazione e gli indirizzi del tenant. Per ulteriori informazioni, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47).
     - **Contabilità**: (Sola lettura) Disponibile solo per il servizio Advanced Automation (PSA) attivato, è possibile visualizzare solo una serie di metriche chiave, incluso il valore corrente dei contratti e degli articoli di vendita da fatturare e il numero di utenti finali a cui vengono forniti i servizi.

- **Ticket**: (Sola lettura) Disponibile solo per il servizio Advanced Automation (PSA) attivato, è possibile visualizzare alcune metriche chiave, incluso i ticket aperti, le violazioni degli SLA e i ticket con assegnazione annullata. È anche possibile visualizzare un elenco dei ticket attualmente aperti.
- **Service Desk**: Disponibile solo per il servizio Advanced Automation (PSA) attivato, è possibile aggiornare le impostazioni predefinite del tenant.

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.
- Le notifiche di manutenzione non sono supportate per gli utenti VMware Cloud Director.

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 **La mia 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 **Fine**.

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

Abilitazione delle notifiche relative ai dispositivi individuati

È possibile abilitare le notifiche sui dispositivi appena individuati per gli account utente Partner e Cliente a cui è assegnato uno dei ruoli seguenti:

- Amministratore del portale di gestione.
- Amministratore o Amministratore Cyber della console di Protezione.

In questo caso, il lunedì e il giovedì il sistema invia notifiche e-mail che includono le informazioni seguenti:

- Per gli amministratori del cliente: il numero di dispositivi, raggruppati per tipo di dispositivo, che sono stati individuati dopo l'ultimo controllo.
- Per gli amministratori del partner: il numero di dispositivi individuati di recente per ogni cliente.

Per abilitare le notifiche per i dispositivi individuati

1. Accedere al portale di gestione come Utente partner o Amministratore dell'azienda.
2. Passare a **Gestione azienda** > **Utenti**, quindi fare clic sul nome dell'utente per il quale abilitare le notifiche.
3. Nella scheda **Servizi**, nella sezione **Impostazioni**, fare clic sull'icona a matita.
4. Selezionare **Notifiche sui nuovi dispositivi individuati** e fare clic su **Fine**.

L'utente selezionato riceverà notifiche via e-mail sui dispositivi appena individuati nella rete aziendale.

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, passare a **Clienti**.
2. Selezionare il cliente di cui configurare il profilo cliente autogestito.
3. Selezionare la scheda **Configura**, 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 dell'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 dell'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 **La mia azienda** > **Profilo dell'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. 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.

- 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, passare 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. 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.
    - 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, passare 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.

- Solo gli amministratori (ad esempio, l'amministratore nel portale di gestione o l'amministratore dell'azienda) 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 la dashboard operativa 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 non è limitato, gli amministratori dei tenant padre avranno accesso completo al tenant dell'utente e potranno eseguire le operazioni seguenti:

- Modificare le proprietà del tenant
- Gestire tenant, utenti e servizi per il proprio tenant
- Accedere ai backup e ad altre risorse nel tenant
- Ottenere report sull'utilizzo per il tenant, i tenant figlio e tutti i clienti.

Se l'accesso al tenant è limitato, gli amministratori dei tenant padre potranno eseguire le operazioni seguenti:

- Modificare le proprietà del tenant
- Ottenere report sull'utilizzo per il tenant, i tenant figlio e tutti i clienti.

Per limitare l'accesso degli amministratori di livello superiore al tenant

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

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".

Nota
Benché Cyber Protect offra un'opportunità per il ripristino dei tenant, tenere presente che il ripristino non è supportato per il servizio File Sync & Share.

Per eliminare un tenant

1. Nel portale di gestione, passare 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.
- Lo **stato del tenant** è visualizzato come **Eliminato**. Quando si passa il mouse sullo stato **Eliminato**, viene visualizzata la data di eliminazione del tenant.

Nota
È possibile ripristinare tutti i dati e le impostazioni pertinenti entro 30 giorni dalla data di eliminazione indicata.

Ripristino di un tenant

Nel caso in cui un tenant venga eliminato accidentalmente, Cyber Protect consente di ripristinarlo entro 30 giorni.

Ad esempio, potrebbe essere necessario ripristinare un tenant nei seguenti casi:

- Il Partner ha eliminato accidentalmente i propri tenant.
- Il team di sviluppo del Partner ha eliminato accidentalmente una parte o l'intera gerarchia dei tenant durante la fase di test dell'integrazione.
- L'integrazione del Partner ha eseguito involontariamente il deprovisioning dell'applicazione anziché passare alla nuova edizione, ed è quindi necessario ripristinare i dati.
- Il Partner ha disabilitato involontariamente l'applicazione durante il passaggio al nuovo modello di licensing, ed è quindi necessario ripristinare i dati nell'applicazione disabilitata.

Per ripristinare un tenant

1. Nel portale di gestione, passare a **Clienti**.
2. Nella scheda **Cyber Protect**, selezionare il tenant da ripristinare. Il relativo stato viene visualizzato come **Eliminato**.

3. Passare il mouse sul tenant, quindi fare clic sull'icona dei puntini di sospensione .
4. Fare clic su **Ripristina**.

   Verrà visualizzata una finestra di conferma che indica che il tenant verrà ripristinato allo stato in cui era prima dell'eliminazione, e che verrà disabilitato per impostazione predefinita.
5. [Facoltativo] Se è necessario abilitare il tenant, selezionare la casella di controllo **Desidero abilitare il tenant**. Sarà possibile abilitare il tenant in qualsiasi momento successivo.
6. Fare clic su **Ripristina**.

Di conseguenza:

- Il tenant e i relativi tenant secondari verranno ripristinati.
- Tutti i servizi abilitati nel tenant e nei relativi tenant secondari verranno riavviati.

  Nota
  Il ripristino non è supportato per il servizio File Sync & Share.

- Tutti gli utenti in questo tenant e nei relativi tenant secondari verranno ripristinati.
- Verrà eseguita una nuova registrazione di tutti i sistemi in questo tenant e nei relativi tenant secondari.
- Tutti i dati relativi al servizio, ad esempio i backup, nel tenant e nei relativi tenant secondari verranno ripristinati.
- Tutti i client API nel tenant e nei relativi tenant secondari verranno ripristinati e tutte le integrazioni che utilizzano tali client saranno di nuovo operative.
- Lo **Stato del tenant** verrà visualizzato come **Attivo** se il tenant è stato abilitato o come **Disabilitato** se il tenant non è ancora stato abilitato.

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.
- Cliente/Cliente potenziale — per delegare la gestione del servizio ad altre persone, le cui autorizzazioni di accesso saranno strettamente limitate al cliente o potenziale cliente 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. 34).
3. Nell'angolo in alto a destra fare clic su **Nuovo** > **Utente**.
   In alternativa, passare a **La mia azienda** > **Utenti** e fare clic su **+ Nuovo**.
4. Specificare le seguenti informazioni di contatto per l'account:
   - **E-mail**: questo indirizzo e-mail viene utilizzato anche per il login. Se si preferisce utilizzare un indirizzo di login diverso dall'e-mail, selezionare la casella di controllo **Utilizza un login diverso dall'e-mail**, quindi inserire **Login** ed **E-mail**.

     Importante
     Ciascun account deve disporre di un unico login

   - **Nome**: questo campo è obbligatorio per la creazione di account utente e per la creazione di utenti all'interno di una cartella.
   - **Cognome**: questo campo è obbligatorio per la creazione di account utente e per la creazione di utenti all'interno di una cartella.
   - [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**
   - Nel campo **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 dell'azienda** 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 assegnati nei servizi abilitati per tale utente.
7. Fare clic su **Crea**.

L'account utente appena creato viene visualizzato nella scheda **Utenti** in **La mia 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 **La mia 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 ad 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.

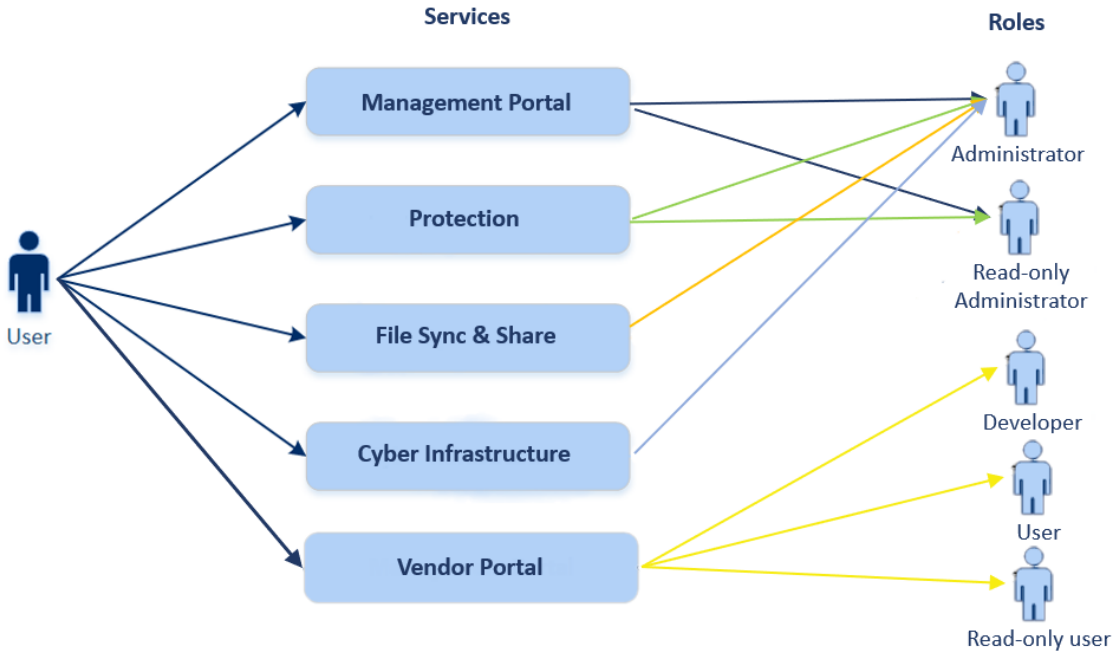
Per convertire un account utente in un account di servizio

1. Nel portale di gestione, passare a **La mia 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.

Nota

I servizi disponibili sono configurati dal service provider.

Servizio	Ruolo	Descrizione
n/d	Amministratore dell'azienda	Questo ruolo concede diritti di amministratore completi per tutti i servizi. Questo ruolo consente l'accesso all'elenco degli elementi consentiti aziendale. Se per l'azienda è abilitato l'add-on Disaster Recovery del servizio Protezione, questo ruolo consente anche l'accesso alla funzionalità Disaster Recovery.
	Amministratore unità Livello dell'unità	Questo ruolo concede i permessi massimi a tutti i servizi applicabili nell'unità. Il ruolo non fornisce 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	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

	Livello del partner	i clienti di questo partner. Consultare "Ruolo Amministratore di sola lettura" (pag. 67).
	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. Consultare "Ruolo Amministratore di sola lettura" (pag. 67).
	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. Consultare "Ruolo Amministratore di sola lettura" (pag. 67).
Vendor Portal	Sviluppatore	Questo ruolo consente l'accesso completo al Vendor Portal. Gli sviluppatori possono creare e gestire CyberApp, CyberApp Descriptions e CyberApp Versions. Possono inoltre inviare richieste di deployment e monitorare le metriche delle CyberApp.
	Utente	Questo ruolo consente all'utente di creare, gestire e richiedere le approvazioni delle CyberApp Descriptions.
	Utente di sola lettura	Questo ruolo consente l'accesso di sola lettura al Vendor Portal.

Protezione	Amministratore	Questo ruolo consente la configurazione e la gestione del servizio Protezione per i clienti. Questo ruolo è richiesto per: • configurare e gestire la funzionalità di Disaster Recovery; • configurare e gestire l'elenco degli elementi consentiti aziendale; • eseguire l'autorilevamento dei dispositivi; • eseguire tutte le azioni relative al deployment del software con DeployPilot (lavorare con i piani di deployment software, repository software, pacchetti software ed esecuzione di azioni di deployment rapido).
	Amministratore Cyber	Oltre ai diritti del ruolo Amministratore, questo ruolo consente la configurazione e la gestione del servizio Protezione 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 (RMM).
	Amministratore di sola lettura	Questo ruolo consente l'accesso di sola lettura a tutti gli oggetti del servizio di protezione. Consultare "Ruolo Amministratore di sola lettura" (pag. 67).
	Utente	Questo ruolo abilita l'utilizzo del servizio di protezione senza i privilegi di amministrazione. È consentito l'accesso a funzionalità quali Endpoint Detection and Response, ma gli utenti a cui questo ruolo è assegnato non possono accedere ai dati di altri utenti dell'organizzazione.
	Operatore di ripristino	Applicabile alle organizzazioni Microsoft 365 e Google Workspace, il ruolo fornisce l'accesso ai backup e consente il loro ripristino, limitando l'accesso ai contenuti sensibili all'interno dei backup. Vedere "Ruolo di operatore di ripristino" (pag. 68).
	Analista della sicurezza	Il ruolo può essere assegnato solo nei tenant cliente per i quali è abilitato il pacchetto Advanced Security + EDR o Advanced Security + XDR. Il ruolo fornisce l'accesso alla console Cyber Protection e consente all'utente di gestire i problemi EDR e di eseguire le azioni di risposta.
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.
Advanced Automation (PSA)	Agli utenti di Advanced Automation (PSA) possono essere assegnati numerosi ruoli. Per ulteriori informazioni, consultare "Ruoli di Advanced Automation (PSA)" (pag. 216).	

Partner Portal	Agli utenti del Partner Portal possono essere assegnati numerosi ruoli. Per ulteriori informazioni, consultare "Ruoli del Partner Portal" (pag. 403).	
Notary	Amministratore	Questo ruolo consente la configurazione e la gestione del Servizio Notary per gli utenti.
	Utente	Questo ruolo consente l'utilizzo del Servizio Notary senza i privilegi di amministrazione. Gli utenti con questo ruolo non possono accedere ai dati di altri utenti dell'organizzazione.

Nota
Il Vendor Portal è disponibile ai Partner tecnologici che hanno effettuato la registrazione al sito web Acronis Technology Ecosystem dopo il 4 ottobre 2023.
Gli utenti che intendono realizzare un'integrazione con e richiedono l'accesso al Vendor Portal e a un ambiente sandbox dedicato, possono consultare il capitolo relativo alle integrazioni.

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 Amministratore di sola lettura

Un account con questo ruolo dispone dell'accesso di sola lettura alla console di Cyber Protect 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.
- Se Advanced Security + XDR è abilitato, gli amministratori di sola lettura possono accedere alla scheda Azioni di risposta nella schermata degli incidenti EDR, ma non possono eseguire alcuna azione.
- Accedere ai dati di altri utenti dell'organizzazione in modalità di sola lettura.

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.
- Configurare e gestire la funzionalità di Disaster Recovery o l'elenco degli elementi consentiti aziendale e ha accesso in sola lettura ai piani di deployment software, ai repository software e ai pacchetti software.
- 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.

Nota
Nel portale di gestione, gli amministratori di sola lettura possono avviare la creazione di nuovi tenant figlio e configurarne tutte le proprietà a scopo dimostrativo, ma non possono salvarle.

- Salvare eventuali modifiche ai piani di scripting, ai piani di monitoraggio o ai piani dell'agente.

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.

Ruolo di operatore di ripristino

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

Un operatore di ripristino può eseguire le seguenti operazioni:

- Visualizzare avvisi e attività.
- Visualizzare e aggiornare l'elenco dei backup.
- Visualizzare l'elenco dei punti di ripristino.
- Sfogliare i backup senza accedere al loro contenuto.

Nota
Gli operatori di ripristino possono 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).
- Ripristinare i backup cloud-to-cloud solo 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.
- 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.
- Ripristinare 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 dell'azienda**
  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 dell'azienda**	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 Modifica 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

È possibile configurare quali notifiche un utente riceverà via e-mail, se il servizio Cyber Protection è abilitato per il tenant in cui è stato creato l'utente.

Per configurare le notifiche per un utente

1. Passare a **La mia azienda** > **Utenti**.
2. Fare clic sull'utente per il quale si desidera configurare le notifiche e quindi, nella scheda **Servizi**, nella sezione **Notifiche e-mail**, fare clic sull'icona della matita.
3. Selezionare le caselle di controllo delle e-mail di notifica che si desidera abilitare.

Notifiche	Descrizione
Notifiche sulla manutenzione	Notifiche inviate per informare gli utenti Partner, i tenant figlio (partner e clienti) e i singoli utenti riguardo alle prossime attività di manutenzione per il data center Cyber Protect. Queste notifiche possono essere abilitate dagli utenti Partner per i loro tenant figlio, e dagli utenti Partner o dagli amministratori dell'azienda per i singoli utenti all'interno della loro organizzazione.
Notifiche relative al superamento delle quote	Notifiche relative al superamento delle quote.
Report di utilizzo pianificati	I report di utilizzo che vengono inviati il primo giorno di ogni mese.
Notifiche sul branding dell'URL	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.
Conto alla rovescia delle notifiche di passaggio in produzione	Notifiche sull'imminente scadenza della prova del cliente che verranno inviate 10 giorni prima della scadenza della prova e 3 giorni prima della scadenza della prova.
Notifica di	Notifiche sull'attivazione della modalità di produzione.

Notifiche	Descrizione
attivazione della modalità di produzione	
Notifiche di errore	Notifiche relative ai risultati dell'esecuzione dei piani di protezione e ai risultati delle operazioni di ripristino per ogni dispositivo.
Notifiche di attenzione	Notifiche relative ai risultati dell'esecuzione dei piani di protezione e ai risultati delle operazioni di ripristino per ogni dispositivo.
Notifiche di esito positivo	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	Il riepilogo giornaliero viene generato in base all'elenco degli avvisi attivi presenti nella console di Cyber Protect 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	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 sui nuovi dispositivi rilevati	Notifiche sui dispositivi appena rilevati. Queste notifiche vengono inviate ogni lunedì e giovedì.
Notifiche di ripristino	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	Notifiche sugli avvisi di Prevenzione della perdita di dati relative all'attività di questo utente sulla rete.
Notifiche relative ai problemi di	Notifiche relative al malware rilevato durante l'accesso, l'esecuzione e le scansioni su richiesta e ai rilevamenti provenienti dal motore

Notifiche	Descrizione
sicurezza	comportamentale e dal motore del filtro 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 ai 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 dell'infrastruttura	Notifiche relative all'infrastruttura di Disaster Recovery: quando questa non è disponibile o quando non sono disponibili i tunnel VPN.

Nota
Gli utenti VMware Cloud Director possono ricevere le seguenti notifiche: notifiche relative al superamento delle quote, report di utilizzo pianificati (se tali report sono configurati per l'organizzazione) e riepilogo giornaliero degli avvisi attivi.

Impostazioni predefinite delle notifiche abilitate per tipo di notifica e ruolo utente

Le notifiche abilitate o disabilitate per impostazione predefinita dipendono dal tipo di notifica e dal ruolo utente.

Tipo di notifica\Ruolo utente	Partner, amministratori di cartelle	Cliente, amministratori di unità (self-service)	Cliente, amministratori di unità (gestito dal service provider)
Notifiche sulla manutenzione	Sì (attivato per impostazione predefinita per gli utenti di Partner diretti, disattivato per i Partner indiretti)	No	No
Notifiche relative al superamento delle quote	Sì	Sì	No
Notifiche dei report di utilizzo pianificati	Sì	Sì	No

Notifiche sul branding dell'URL	No	No	No
Notifiche di errore	No	No	No
Notifiche di attenzione	No	No	No
Notifiche di esito positivo	No	No	No
Riepilogo giornaliero degli avvisi attivi	No	Sì	No
Notifiche di Controllo dispositivo	No	No	No
Notifiche di ripristino	No	No	No
Notifiche di Prevenzione della perdita di dati	No	No	No
Notifiche relative ai problemi di sicurezza: Mitigato	No	No	No
Notifiche relative ai problemi di sicurezza: Non mitigato	No	No	No
Notifiche dell'infrastruttura	No	No	No

Notifiche abilitate per impostazione predefinita per tipo di dispositivo e ruolo utente

Tipo di dispositivo\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.

Nota
Tutti i dispositivi associati all'utente disabilitato non saranno più protetti perché non verrà applicata loro alcuna quota. Per continuare a proteggere questi dispositivi, riassegnali a un utente attivo.

Per abilitare un account utente disabilitato

1. Nel portale di gestione passare a **Utenti**.
2. Selezionare l'utente disabilitato nell'elenco utenti e quindi 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.

Nota
È possibile riutilizzare il login di un utente che è stato eliminato.

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".

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:

- Tutte le notifiche configurate per questo account verranno disabilitate.
- Tutti i dati che appartengono a questo account utente verranno eliminati.
- L'amministratore non potrà accedere al portale di gestione.
- Tutti i backup dei workload associati a questo utente verranno eliminati.
- Verrà annullata la registrazione di tutti i sistemi associati a questo account utente.
- Tutti i piani di protezione verranno revocati da tutti i workload associati a questo utente.
- Tutti i dati di File Sync & Share che appartengono a questo utente (ad esempio file e cartelle) verranno eliminati.
- I dati Notary che appartengono a questo utente (ad esempio file autenticati, file firmati elettronicamente) verranno eliminati.
- Lo **Stato** dell'utente viene visualizzato come **Eliminato**. Passando il mouse sullo stato **Eliminato** viene visualizzata la data di eliminazione dell'utente e una nota che indica la possibilità di recuperare tutti i dati e le impostazioni pertinenti entro 30 giorni dalla data di eliminazione indicata.

Ripristino di un account utente

Poiché la cancellazione di un account utente può essere accidentale, Cyber Protection offre l'opportunità di ripristinare gli account utente.

Ad esempio, potrebbe essere necessario ripristinare un account utente nel seguente caso: l'amministratore dell'azienda ha eliminato un utente che ha lasciato la società, ma tutte le risorse registrate nell'account dell'ex dipendente sono ancora necessarie.

Per ripristinare un account utente

1. Nel portale di gestione, passare a **La mia azienda** > **Utenti**.
2. Nella scheda **Utenti**, selezionare l'account utente da ripristinare. Il relativo stato viene visualizzato come **Eliminato**.
3. Passare il mouse sull'account utente, quindi fare clic sull'icona dei puntini di sospensione .
4. Fare clic su **Ripristina**.

   Verrà visualizzata una finestra di conferma che indica che l'account utente verrà ripristinato allo stato in cui era prima dell'eliminazione, e che verrà disabilitato per impostazione predefinita.
5. [Facoltativo] Se è necessario abilitare l'account utente, selezionare la casella di controllo **Desidero abilitare l'utente**. Sarà possibile abilitare l'account utente in qualsiasi momento successivo.
6. Fare clic su **Ripristina**.

Di conseguenza:

- Questo account utente verrà ripristinato.
- Tutti i dati che appartengono a questo account utente verranno ripristinati.
- Verrà eseguita una nuova registrazione di tutti i sistemi associati a questo account utente.
- Lo Stato dell'utente verrà visualizzato come **Attivo** se l'account utente è stato abilitato o come **Disabilitato** se l'account utente non è ancora stato abilitato.

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 **Fine**.
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 > **Reimposta 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.

Nota
Per i tenant Partner in modalità Produzione, l'autenticazione a due fattori è abilitata per impostazione predefinita e non può essere disabilitata.

Per i tenant cliente, l'autenticazione a due fattori è facoltativa e può essere disabilitata.

Gli account di amministratore del Partner utilizzati da un'integrazione devono essere convertiti in account di servizio. In caso contrario, le integrazioni non potranno autenticarsi su Cyber Protect Cloud. Ad esempio, gli account utilizzati da un'integrazione sono gli account per l'agente di gestione e l'agente di backup nell'integrazione VMware Cloud Director. Per ulteriori informazioni su come creare un account di servizio, consultare "Per convertire un account utente in un account di servizio" (pag. 63).

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, è possibile utilizzare codice a 32 cifre visualizzato al di sotto del codice QR e aggiungerlo manualmente all'applicazione di autenticazione.

Importante
È consigliabile salvare queste informazioni: stampare il codice QR, annotare il segreto TOTP (password temporanea), utilizzare un'applicazione che supporti il backup dei codici in un cloud. Il codice TOTP della password temporanea è necessario per ripristinare l'autenticazione a due fattori in caso di perdita del dispositivo di secondo fattore.

6. Il codice TOTP della password temporanea viene generato nell'applicazione di autenticazione. Viene automaticamente rigenerato ogni 30 secondi.
7. L'utente deve inserire il codice TOTP nella finestra **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.

Per ripristinare l'autenticazione a due fattori su un nuovo dispositivo

Se è possibile accedere all'app di autenticazione mobile precedentemente installata:

1. Installare un'app di autenticazione sul nuovo dispositivo.
2. Utilizzare il file PDF salvato al momento dell'impostazione dell'autenticazione 2FA nel dispositivo. Questo file contiene il codice a 32 cifre che deve essere inserito nell'app di autenticazione per collegarla di nuovo all'account Acronis.

Importante
Se il codice è corretto ma non funziona, accertarsi di aver sincronizzato l'orario nell'app di autenticazione mobile.

3. Se al momento dell'impostazione non è stato salvato il file PDF:

a. *Fare clic su **Reimposta l'autenticazione 2FA** e inserire la password temporanea mostrata nell'app di autenticazione mobile precedentemente installata.*
b. Seguire le istruzioni a video.

Se non è possibile accedere all'app di autenticazione mobile precedentemente installata:

1. Prendere un nuovo dispositivo mobile.
2. Utilizzare il file PDF archiviato per collegare un nuovo dispositivo (il nome predefinito del file è `cyberprotect-2fa-backupcode.pdf`).
3. Ripristinare l'accesso all'account dal backup. Verificare che l'app mobile supporti i backup.
4. Aprire l'app con lo stesso account da un altro dispositivo mobile se è supportato dall'app.

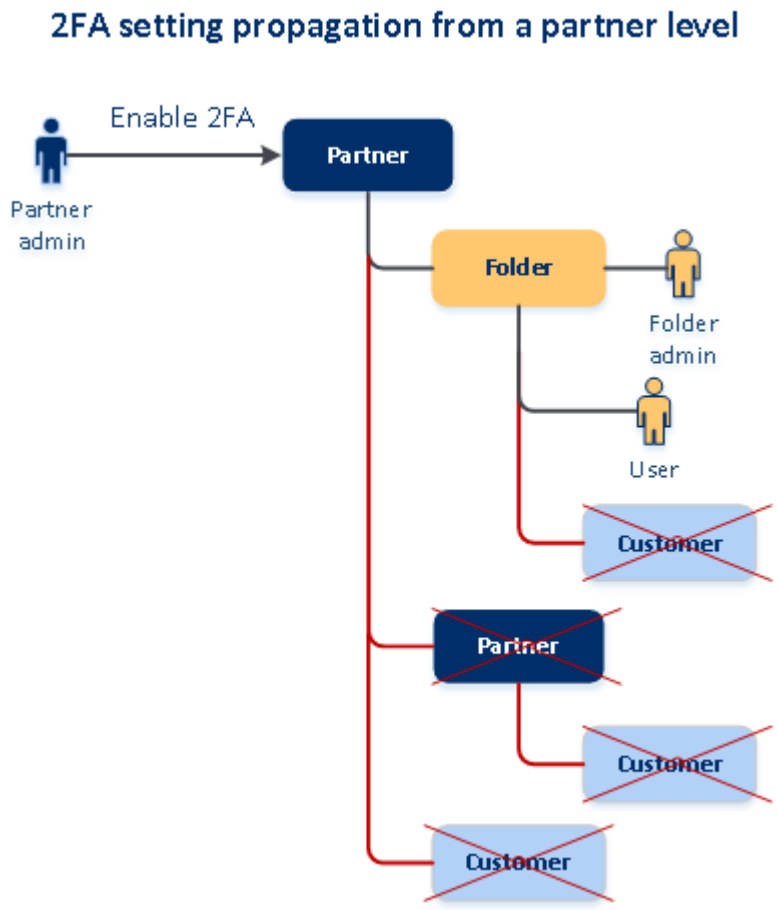
Propagazione delle impostazioni dell'autenticazione a due fattori a tutti i livelli dei tenant

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

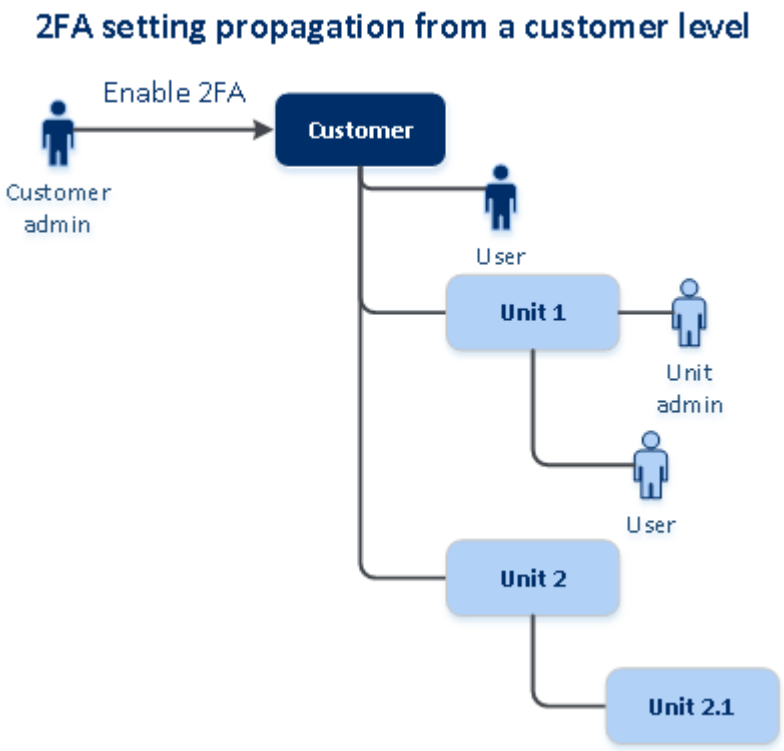
- Per la propria organizzazione.
- Per il proprio tenant figlio (solo nel caso in cui l'opzione di **Accesso al supporto** sia abilitata per tale tenant figlio).

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 i tenant

A partire dalla versione 24.09, l'autenticazione a due fattori (2FA) è abilitata per impostazione predefinita per tutti i tenant Partner (diretti e indiretti) in modalità di produzione e non può essere disabilitata.

Per i Partner in prova, l'attivazione automatica della 2FA avviene solo quando il loro account passa alla modalità di produzione.

Il supporto per gli account di servizio (utenti con 2FA disabilitata) non viene interrotto. Un amministratore del Partner può ancora disabilitare temporaneamente la 2FA per un utente, convertendolo in un account di servizio. Gli account di servizio esistenti rimangono invariati, il che è importante per le integrazioni personalizzate che utilizzano l'autenticazione di base, in quanto non è compatibile con la 2FA. La soluzione consigliata per tali integrazioni è la loro migrazione ai client API.

La 2FA non è obbligatoria per i tenant cliente, ma la sua attivazione è fortemente consigliata. Un amministratore del Partner può impersonare un amministratore del cliente e abilitare la 2FA per i clienti che gestisce.

Per abilitare l'autenticazione a due fattori

Ruolo richiesto: amministratore del Partner

1. Accedere al portale di gestione.
2. Passare a **Clienti** e selezionare il tenant cliente per il quale abilitare l'autenticazione a due fattori.
3. Passare a **Impostazioni** > **Sicurezza**.
4. 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'opzione 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 **La mia 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

Ruolo richiesto: amministratore del Partner

1. Accedere al portale di gestione.
2. Passare a **Clienti** e selezionare il tenant cliente per il quale disabilitare l'autenticazione a due fattori.
3. Passare a **Impostazioni** > **Sicurezza**.
4. Per disabilitare l'autenticazione a due fattori, disattivare l'indicatore scorrevole e quindi fare clic su **Disabilita**.
5. [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 potranno accedere al sistema utilizzando solo il login e la password personale. Nella scheda **La mia 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 **La mia azienda** > **Utenti** del portale di gestione.

Monitoraggio

Nel portale di gestione, in **La mia 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 **La mia 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 **La mia 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 **La mia 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 **La mia 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.

È possibile promuovere l'acquisto di funzionalità avanzate presso i clienti esistenti che stanno utilizzando le funzionalità standard di Cyber Protect.

È possibile abilitare o disabilitare la funzionalità di upselling per ogni cliente. Per impostazione predefinita, l'opzione di upselling è abilitata. I clienti visualizzano le funzionalità aggiuntive non disponibili fino al momento dell'acquisto. Queste funzionalità aggiuntive sono contrassegnate da etichette che ne mostrano il nome o le icone del pacchetto Advanced promosso, in verde. Se un cliente seleziona un articolo di upselling, un messaggio suggerisce di abilitare il pacchetto Advanced richiesto. Se il cliente fa clic sul collegamento **Abilita gli Advanced Pack richiesti**, viene visualizzato

un messaggio di conferma. Se il cliente fa clic sul pulsante **Abilita** e l'URL di acquisto è configurato a livello del Partner, il cliente viene reindirizzato a tale URL.

Per configurare il link di acquisto

È possibile configurare il link del pulsante **Abilita**, che reindirizzerà i clienti al sito web per l'acquisto di servizi avanzati.

1. Nel menu di navigazione del portale di gestione, selezionare **Impostazioni** > **Branding**.
2. Nella sezione **Upsell**, modificare il valore della stringa **URL Acquista**.

Nota
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.

Per disabilitare l'opzione di upselling per un cliente

1. Nel portale di gestione, passare a **Clienti**.
2. Selezionare il cliente, passare al pannello di destra, fare clic sulla scheda **Configura** e quindi fare clic su **Impostazioni generali**.
3. Nella sezione **Upsell**, disabilitare **Promuovi le opzioni di protezione avanzata** per disattivare lo scenario di upselling per il cliente selezionato.

Elementi di upselling mostrati al cliente

Elenco degli elementi consentiti

Il menu **Elenco degli elementi consentiti** viene aggiunto in **Protezione** > **Anti-malware**.

Quando un'azienda dispone di applicazioni aziendali specifiche che possono essere riconosciute e individuate come falsi positivi dai programmi antivirus, aggiungere manualmente le applicazioni attendibili all'elenco degli elementi consentiti è un'attività che potrebbe richiede tempo. L'elenco può rendere automatica l'aggiunta di tali applicazioni all'elenco degli elementi consentiti. Il modulo Protezione antivirus e anti-malware scansiona i backup e i dati acquisiti vengono analizzati per inserire queste applicazioni tra gli elementi consentiti e prevenire l'individuazione di falsi positivi.

Questo elemento di upselling promuove il pacchetto Advanced Security.

Creare o modificare un piano di protezione

I clienti possono visualizzare le funzionalità avanzate dei pacchetti seguenti durante la creazione o la modifica di piani di protezione.

- Advanced Backup
- Advanced Management (RMM)
- Advanced Data Loss Prevention

- Protezione antivirus e anti-malware
- Advanced Security + XDR

Prevenzione della perdita di dati

L'elemento di upselling **Prevenzione della perdita di dati** si trova nella console di Cyber Protection, alla voce di menu **Protezione**.

Questo elemento di upselling promuove il pacchetto Advanced Data Loss Prevention.

Gestione di posizioni e archivi

La sezione **Impostazioni** > **Posizioni** mostra i cloud storage 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 i cloud storage 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 storage di backup, infrastrutture di disaster recovery e archivi per la **File Sync & Share**. Una posizione può contenere più cloud storage ma una sola infrastruttura di disaster recovery.

Per informazioni sulle operazioni con gli storage, consultare "Gestione dell'archiviazione" (pag. 88).

Selezione di posizioni e storage 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.

Per informazioni sulla geo-ridondanza, consultare "Storage con geo-ridondanza" (pag. 94).

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 storage di backup si trovano nei data center di .
  - Se l'elemento dell'offerta **Storage 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 storage di backup** nella sezione **Posizioni** per trovare informazioni sull'organizzazione di un storage 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 lo storage è assegnato a qualsiasi tenant cliente, è necessario disabilitare il servizio che utilizza lo storage per tutti i tenant cliente prima di eliminarlo. È possibile eliminare uno storage solo se il suo utilizzo è pari a zero.

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.

Storage immutabile

Lo storage immutabile è un tipo di archiviazione dei dati che, per un periodo stabilito, impedisce di apportare modifiche, alterazioni o eliminazioni ai backup. Garantisce che i dati rimangano protetti e non vengano compromessi, fornendo un livello di protezione aggiuntivo contro modifiche non autorizzate o involontarie o attacchi ransomware. Lo storage immutabile è disponibile per tutti i backup cloud archiviati in un'istanza di cloud storage supportata. Consultare "Storage e agenti supportati" (pag. 90).

Lo storage immutabile consente di accedere ai backup eliminati durante un periodo di conservazione specificato. Sarà possibile ripristinare il contenuto da questi backup, ma non modificarli, spostarli o eliminarli. Al termine del periodo di conservazione, i backup eliminati vengono eliminati definitivamente.

Lo storage immutabile contiene i backup seguenti:

- Backup eliminati manualmente.
- Backup eliminati automaticamente in base alle impostazioni indicate nella sezione **Tempo di conservazione** di un piano di protezione o della sezione **Regole di conservazione** di un piano di pulizia.

I backup eliminati nello storage immutabile utilizzano comunque uno spazio di storage il cui consumo viene addebitato.

Lo spazio di storage utilizzato dai tenant eliminati, incluso quello per lo storage immutabile, non viene addebitato.

Modalità dello storage immutabile

Per i tenant Partner non è prevista la possibilità di scegliere modalità di storage immutabile. Un Partner può disabilitare o riabilitare lo storage immutabile per un altro tenant Partner o Cliente e impostare il periodo di conservazione.

Un amministratore del cliente può disabilitare e riabilitare lo storage immutabile e modificarne la modalità e il periodo di conservazione.

Lo storage immutabile è disponibile nelle modalità seguenti:

- **Modalità Governance**
  Questa modalità consente di disabilitare e abilitare di nuovo lo storage immutabile, modificare il periodo di conservazione o passare alla modalità Conformità.

  Nota
  A partire da settembre 2024, la modalità Governance dello storage immutabile con periodo di conservazione di 14 giorni è abilitata per impostazione predefinita in tutti gli storage in hosting Acronis per tutti i tenant cliente e Partner. Per ulteriori informazioni, consultare questo articolo della Knowledge Base.

- **Modalità Conformità**

  Attenzione!
  La selezione della modalità Conformità è irreversibile.

  Non è possibile disabilitare lo storage immutabile né modificare il periodo di conservazione e non è possibile tornare alla modalità Governance.

Storage e agenti supportati

- Lo storage immutabile è supportato solo nel cloud storage.
  - Lo storage immutabile è disponibile per i cloud storage in hosting Acronis e dei Partner che utilizzano Cyber Infrastructure versione 4.7.1 o successiva.
  - Sono supportati tutti gli storage che possono essere utilizzati con Cyber Infrastructure Backup Gateway, ad esempio lo storage Cyber Infrastructure, lo storage Amazon S3 ed EC2 e lo storage Microsoft Azure.
  - Lo storage immutabile richiede che la porta TCP 40440 sia aperta per il servizio Backup Gateway in Cyber Infrastructure. Nella versione 4.7.1 e successive, la porta TCP 40440 è aperta automaticamente in caso di traffico del tipo **Backup (ABGW) public**. Per ulteriori informazioni sui tipi di traffico, consultare la documentazione di Acronis Cyber Infrastructure.
- Lo storage immutabile richiede un agente di protezione versione 21.12 (build 15.0.28532) o successive.
- Sono supportati solo i backup TIBX (Versione 12).

Configurazione dello storage immutabile

Dopo settembre 2024, lo storage immutabile in modalità Governance è abilitato per impostazione predefinita, con un periodo di conservazione di 14 giorni, per tutti i tenant Partner e cliente.

Nota
Per consentire l'accesso ai backup eliminati, la porta 40440 dello storage di backup deve essere abilitata per le connessioni in entrata.

Per disabilitare lo storage immutabile

In un tenant partner

1. Accedere al portale di gestione come amministratore, quindi passare a **Impostazioni** > **Sicurezza**.
2. Verificare che l'opzione **Storage immutabile** sia attiva.
3. Specificare un periodo di conservazione in un intervallo compreso tra 14 e 3650 giorni.
   Il periodo di conservazione predefinito è di 14 giorni. Un periodo di conservazione più lungo implica un maggiore utilizzo dello storage.
4. Fare clic su **Salva**.

In 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 sul nome del tenant.
3. Nel menu di navigazione, passare a **Impostazioni** > **Sicurezza**.
4. Verificare che l'opzione **Storage immutabile** sia attiva.
5. Specificare un periodo di conservazione in un intervallo compreso tra 14 e 3650 giorni.
   Il periodo di conservazione predefinito è di 14 giorni. Un periodo di conservazione più lungo implica un maggiore utilizzo dello storage.
6. Selezionare la modalità di storage immutabile e, se richiesto, confermare la scelta.
   - **Modalità Governance**
     Questo modalità garantisce che ransomware o altre minacce possano alterare o cancellare i dati di backup, perché tutti i backup eliminati vengono conservati nello storage immutabile per il periodo di conservazione specificato. Garantisce inoltre l'integrità dei dati di backup, un aspetto critico per il disaster recovery.
     Questa modalità consente di disabilitare e abilitare di nuovo lo storage immutabile, modificare il periodo di conservazione o passare alla modalità Conformità.
   - **Modalità Conformità**
     Oltre ai vantaggi della modalità Governance, la modalità Conformità facilita il rispetto dei requisiti normativi relativi alla conservazione e alla protezione dei dati, prevenendone la compromissione.

Attenzione!
La selezione della modalità Conformità è irreversibile. Dopo aver selezionato questa modalità, non è possibile disabilitare lo storage immutabile, modificare il periodo di conservazione o tornare alla modalità Governance.

7. Fare clic su **Salva**.
8. Per aggiungere un archivio esistente allo storage immutabile, creare un nuovo backup in tale archivio eseguendo il piano di protezione corrispondente in modalità manuale o in base a una pianificazione.

Attenzione!
Se si elimina un backup prima che l'archivio venga aggiunto allo storage immutabile, tale backup viene cancellato definitivamente.

Per disabilitare lo storage immutabile

In un tenant partner

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

Importante
Questa modifica viene ereditata solo dai tenant figlio in cui lo storage immutabile non è abilitato per impostazione predefinita e le relative impostazioni non sono state modificate a livello di cliente.

A partire dalla versione 24.09, lo storage immutabile è abilitato per impostazione predefinita nei tenant cliente. Per verificare lo stato di abilitazione nei data center, consultare questo articolo della Knowledge Base. La disabilitazione dello storage immutabile a livello di Partner non ha alcun effetto su questi tenant. Per disabilitare lo storage immutabile, accedere al tenant cliente.

Attenzione!
La disattivazione dello storage immutabile non ha effetto immediato. Durante un grace period di 14 giorni (336 ore), è possibile accedere ai backup eliminati in base al loro periodo di conservazione originale.

Al termine del grace period, tutti i backup nello storage immutabile vengono eliminati in modo permanente. Ad esempio, se si disabilita lo storage immutabile il 1° ottobre alle 10:00, tutti i backup che si trovano ancora nello storage immutabile il 15 ottobre alle 10:00 vengono eliminati in modo permanente.

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

In 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 sul nome del tenant.
3. Nel menu di navigazione, passare a **Impostazioni** > **Sicurezza**.
4. Disabilitare l'opzione **Storage immutabile**.

   Nota
   È possibile disabilitare lo storage immutabile solo in Modalità Governance.

   Attenzione!
   La disattivazione dello storage immutabile non ha effetto immediato. Durante un grace period di 14 giorni (336 ore), è possibile accedere ai backup eliminati in base al loro periodo di conservazione originale.
   Al termine del grace period, tutti i backup nello storage immutabile vengono eliminati in modo permanente. Ad esempio, se si disabilita lo storage immutabile il 1° ottobre alle 10:00, tutti i backup che si trovano ancora nello storage immutabile il 15 ottobre alle 10:00 vengono eliminati in modo permanente.
5. Confermare la selezione facendo clic su **Disabilita**.

Visualizzazione dell'utilizzo dello storage immutabile

È possibile visualizzare lo spazio utilizzato dallo storage immutabile nella console di Cyber Protect o nel Report **Utilizzo corrente**, generato nel portale di gestione.

Limitazioni

- Il valore riportato include la dimensione totale di tutti i backup eliminati e i metadati degli archivi di backup presenti nello storage. I metadati possono raggiungere il 10% del valore riportato.
- Il valore mostra l'utilizzo fino a 24 ore prima della generazione del report.
- Se l'utilizzo effettivo è inferiore a 0,01 GB, viene visualizzato come 0,0 GB.

Per visualizzare l'utilizzo dello storage immutabile

Nella console di Cyber Protect

1. Accedere alla console di Cyber Protect.
2. Passare a **Storage di backup** > **Backup**, quindi selezionare una posizione di cloud storage che supporti lo storage immutabile.
3. Controllare la colonna **Storage immutabile e metadati**.

Nel report Utilizzo corrente

1. Accedere al portale di gestione come amministratore.
2. Passare a **Report** > **Utilizzo**.
3. Selezionare **Ad hoc**.

4. Selezionare **Utilizzo corrente** e fare clic su **Genera e invia**.
   Un report nei formati CSV e HTML viene inviato all'indirizzo e-mail dell'utente.
   Il file HTML è incluso in un archivio ZIP.
5. Nel report, controllare la colonna **Nome metrica**.
   È possibile visualizzare l'utilizzo dello storage immutabile nella riga **Cloud storage - Immutabile**.

Esempio di fatturazione per lo storage immutabile

L'esempio seguente mostra un backup eliminato che viene trasferito nello storage immutabile per 14 giorni, ovvero il periodo di conservazione predefinito. Durante questo periodo, il backup eliminato utilizza uno spazio di storage. Al termine del periodo di conservazione, il backup eliminato viene cancellato definitivamente e l'utilizzo dello storage diminuisce. Ogni mese, il costo dell'utilizzo dello storage viene fatturato in funzione del variare delle situazioni sopra delineate.

Data	Backup	Utilizzo archiviazione	Fatturazione
1 aprile	Viene creato il Backup A (10 GB) Viene creato il Backup B (1 GB)	10 GB + 1 GB = 11 GB	
20 aprile	Il Backup B viene cancellato e trasferito nello Storage immutabile (con un periodo di conservazione di 14 giorni)	10 GB + 1 GB = 11 GB	
30 aprile			Vengono fatturati 11 GB per il mese di aprile
4 maggio	Il Backup B viene eliminato definitivamente, perché è terminato il periodo di conservazione	11 GB - 1 GB = 10 GB	
31 maggio			Vengono fatturati 10 GB per il mese di maggio

Storage con geo-ridondanza

Con lo storage con geo-ridondanza, i dati di backup vengono copiati in modo asincrono in una posizione di replica geograficamente distante dalla posizione di backup primaria. Pertanto, i dati diventano duraturi e sono accessibili anche nel caso in cui la posizione primaria non sia disponibile.

I dati replicati utilizzano la stessa quantità di spazio di storage dei dati originari.

Limitazioni

- Lo storage con geo-ridondanza potrebbe non essere disponibile in tutti i data center.
- La geo-ridondanza è supportata solo dal cloud storage. Non è supportata dagli storage di terze parti, come lo storage in hosting del partner o i cloud storage pubblici.
- La posizione dei dati replicati dipende dal datacenter dell'utente. Per ulteriori informazioni, consultare questo articolo della Knowledge Base.
- Si applicano limitazioni aggiuntive quando si utilizza lo storage con geo-ridondanza con Disaster Recovery.

  Per ulteriori informazioni, consultare la documentazione di Cyber Protect Cloud.

Provisioning dello storage con geo-ridondanza

Lo storage con geo-ridondanza è disponibile in un tenant cliente dopo che è stato effettuato il provisioning del tenant nel portale di gestione.

Per eseguire il provisioning dello storage con geo-ridondanza

1. Accedere al portale di gestione come amministratore.
2. In **Clienti**, accanto al nome del tenant, fare clic sul pulsante dei puntini di sospensione > **Configura**.
3. Nella scheda **Protezione**, fare clic su **Modifica**.
4. In **Risorse cloud**, individuare lo storage per il quale abilitare la geo-ridondanza.
5. Accanto a **Geo-ridondanza**, fare clic su **Abilita**.
6. Fare clic su **Salva**.

Il cloud storage con geo-ridondanza diventa disponibile in questo tenant cliente, ma non è abilitato automaticamente. Per utilizzare lo storage con geo-ridondanza, abilitarlo nella console di Cyber Protect. Consultare "Abilitazione dello storage con geo-ridondanza" (pag. 95).

Per ulteriori informazioni sul provisioning dello storage con geo-ridondanza in più tenant, consultare "Abilitazione dei servizi per più tenant esistenti" (pag. 50).

Abilitazione dello storage con geo-ridondanza

Prerequisiti

- A tenant cliente viene assegnato uno storage che supporta la geo-ridondanza. Consultare "Selezione di posizioni e storage per partner e clienti" (pag. 87).
- Il provisioninig dello storage con geo-ridondanza per il tenant cliente viene eseguito nel portale di gestione. Consultare "Provisioning dello storage con geo-ridondanza" (pag. 95).

  Non è possibile eseguire il provisioning dello storage con geo-ridondanza se viene assegnato uno storage non compatibile, come ad esempio lo storage in hosting di un partner.

È possibile abilitare lo storage con geo-ridondanza nella schermata principale della console di Cyber Protect o nella scheda **Impostazioni**. Il risultato di entrambe le procedure è lo stesso.

Per abilitare lo storage con geo-ridondanza

Nella schermata principale

1. Accedere alla console di Cyber Protect come amministratore.
   Nella parte superiore della console di Cyber Protect viene visualizzato un messaggio di avviso.
2. Nella messaggio di avviso, fare clic su **Abilita Geo-redundant Cloud Storage**.
3. Per confermare di aver compreso le posizioni e i costi delle repliche e le relative spese, selezionare la casella di controllo.
4. Per confermare la scelta, fare clic su **Abilita**.

Lo storage con geo-ridondanza viene abilitato e i dati di backup vengono copiati nella posizione di replica.

Nella scheda Impostazioni

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Impostazioni** > **Impostazioni di sistema**.
3. Comprimere l'elenco delle opzioni di backup predefinite, quindi fare clic su **Geo-redundant Cloud Storage**.
4. Abilitare l'opzione **Geo-redundant Cloud Storage**.
5. Fare clic su **Salva**.
6. Per confermare di aver compreso le posizioni e i costi delle repliche e le relative spese, selezionare la casella di controllo.
7. Per confermare la scelta, fare clic su **Abilita**.

Lo storage con geo-ridondanza viene abilitato e i dati di backup vengono copiati nella posizione di replica.

Disabilitazione dello storage con geo-ridondanza

È possibile disabilitare lo storage con geo-ridondanza dalla console di Cyber Protect o eseguirne il deprovisioning nel portale di gestione.

Per disabilitare lo storage con geo-ridondanza

1. Accedere alla console di Cyber Protect come amministratore.
2. Passare a **Impostazioni** > **Impostazioni di sistema**.
3. Comprimere l'elenco delle opzioni di backup predefinite, quindi fare clic su **Geo-redundant Cloud Storage**.
4. Disabilitare l'opzione **Geo-redundant Cloud Storage**.

5. Fare clic su **Salva**.
6. Per confermare la scelta, fare clic su **Disabilita** e quindi su **Disabilita**.

Lo storage con geo-ridondanza è disabilitato. I dati replicati vengono eliminati entro un giorno.

Per eseguire il deprovisioning dello storage con geo-ridondanza

1. Accedere al portale di gestione come amministratore.
2. Nella sezione **Clienti**, accanto al nome del tenant cliente, fare clic sul pulsante con i puntini di sospensione e su > **Configura**.
3. Nella scheda **Protezione**, fare clic su **Modifica**.
4. In **Risorse cloud**, deselezionare la casella di controllo **Geo-ridondanza** al di sotto del nome dello storage.
5. Fare clic su **Salva**.

Lo storage con geo-ridondanza è disabilitato per il tenant cliente e non può essere abilitato nella console di Cyber Protect. I dati replicati vengono eliminati entro un giorno.

Visualizzazione dello stato della geo-replica

Lo stato della geo-replica indica se i dati dalla posizione di backup primaria vengono copiati nella posizione di replica.

Sono possibili gli stati seguenti:

- **Sincronizzata**: i dati sono stati copiati nella posizione di replica.
- **Sincronizzazione in corso**: è in corso la copia dei dati nella posizione di replica. La durata di questa operazione dipende dalla dimensione dei dati.
- **In attesa**: la replica dei dati è stata temporaneamente sospesa.
- **Disabilitata**: la replica dei dati è disabilitata.

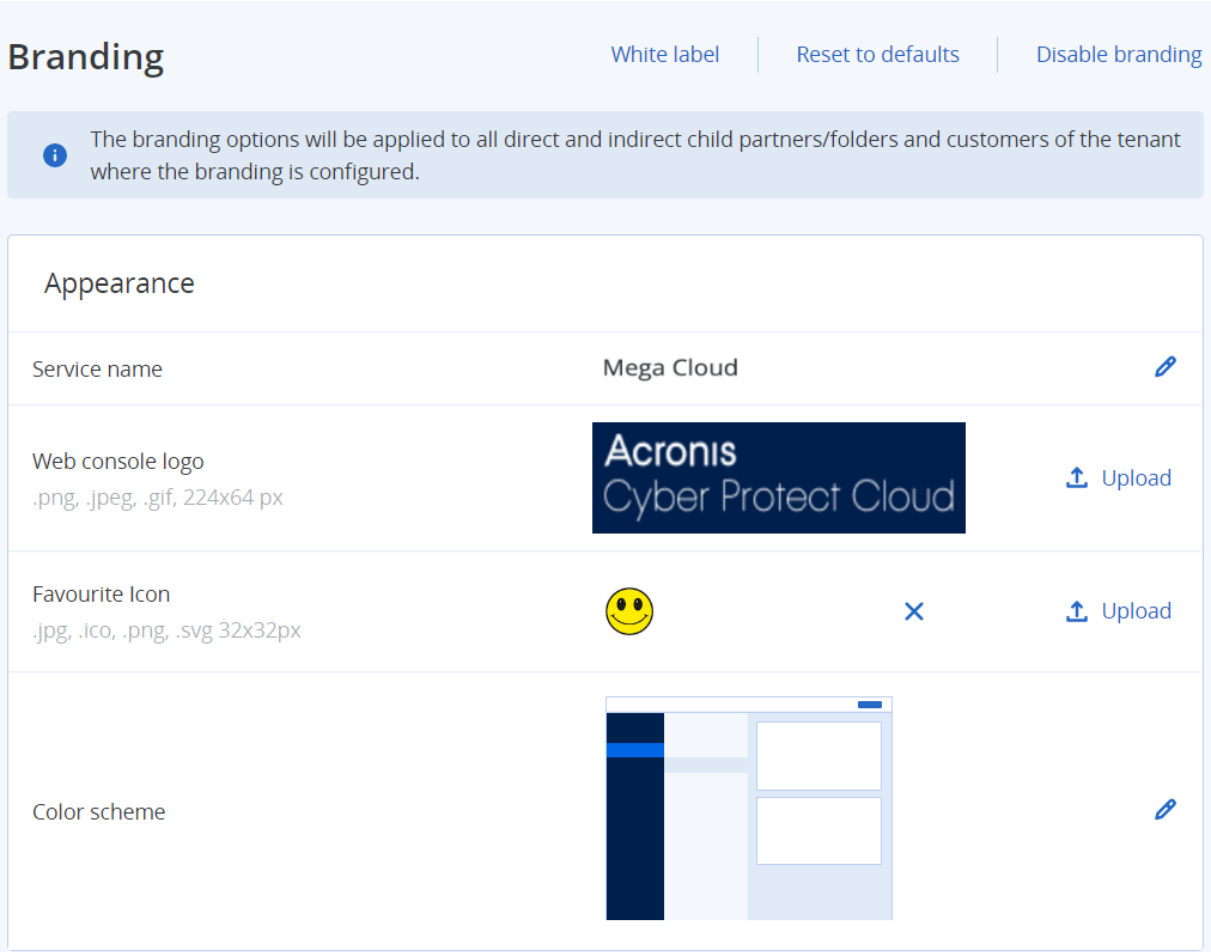
Per controllare lo stato della replica

1. Accedere alla console di Cyber Protect.
2. Nella scheda **Storage di backup**, selezionare la posizione di backup e quindi l'archivio.
3. Fare clic su **Dettagli**, quindi controllare lo stato nella sezione **Stato della geo-replica**.

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 i tenant figlio e rimuovere qualsiasi associazione con i partner di livello superiore.

Nota
Le impostazioni di branding vengono applicate a tutti i tenant figlio, diretti e indiretti. Le impostazioni di branding per il proprio tenant sono configurate dal service provider.



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 **Fine** 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 **Riconfigurazione** per modificare l'URL esistente. Per utilizzare l'URL predefinito (https://cloud.acronis.com), fare clic su **Ripristina allo stato predefinito**. 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), Cyber Protection Monitor (per Windows, macOS e Linux) e Connect Client saranno dotati di marchio o saranno personalizzabili. Abilitando l'opzione di white label, sarà possibile personalizzare l'agente, Connect Client 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 **Riconfigurazione** 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 Acronis Cyber Protect Cloud: Come definire un record CNAME.
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.

     Nota
     Può venire visualizzato un errore di convalida del certificato con il seguente messaggio di errore: "Impossibile verificare il certificato: x509: certificato firmato da un'autorità sconosciuta". Il messaggio indica in genere l'assenza di alcuni certificati intermedi. Per correggere la struttura del certificato e caricare la catena di certificati completa, utilizzare un resolver di catena di certificati.

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 allo stato predefinito** per utilizzare l'URL predefinito (https://cloud.acronis.com).

Configurazione degli aggiornamenti dell'agente Cyber Protection

Importante
È possibile accedere alla funzionalità di gestione dell'aggiornamento dell'agente se il servizio Protezione è abilitato.

Questa procedura si applica agli aggiornamenti dei seguenti agenti Cyber Protection: Agente per Windows, Agente per Linux, Agente per Mac e Agente di Cyber Files Cloud per File Sync & Share.

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 gli aggiornamenti manuali, automatici e senza intervento dell'utente di tutti gli agenti su tutti i sistemi o su sistemi singoli.

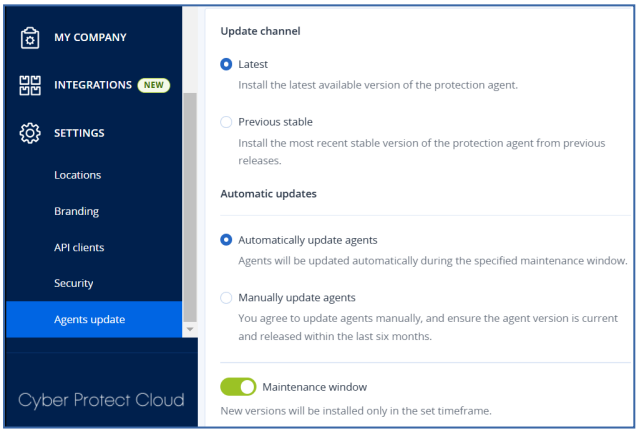
Nota
Per gestire gli agenti sui singoli sistemi e personalizzare le impostazioni di aggiornamento automatico dalla console di Cyber Protect, vedere la sezione Aggiornamento degli agenti nel Manuale dell'utente di Cyber Protect.

Aggiornamenti automatici

Nota
I Partner e i clienti che non hanno abilitato il servizio di protezione ereditano le impostazioni per gli aggiornamenti automatici dell'Agente per File Sync & Share dal proprio service provider.

Per configurare le impostazioni predefinite per gli aggiornamenti automatici degli agenti nel portale di gestione

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



2. In **Canale di aggiornamento**, selezionare la versione da utilizzare per gli aggiornamenti automatici.

Opzione	Descrizione
Più recente (selezionata per impostazione predefinita)	Installa l'ultima versione disponibile dell'agente Cyber Protection.
Versione stabile precedente	Installa la versione più recente e stabile dell'agente Cyber Protection dalle versioni precedenti.

3. Verificare che l'opzione **Aggiorna automaticamente gli agenti** sia selezionata.

Nota
Gli aggiornamenti automatici sono disponibili solo per i seguenti agenti:

- Agente Cyber Protect, versione 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.

4. [Facoltativo] Impostare la finestra di manutenzione.
   La finestra predefinita è giornaliera, dalle 23:00 alle 08:00 sul sistema in cui è installato l'agente.

   Nota
   Benché gli aggiornamenti degli agenti siano 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. Fare clic su **Salva**.

Aggiornamenti manuali

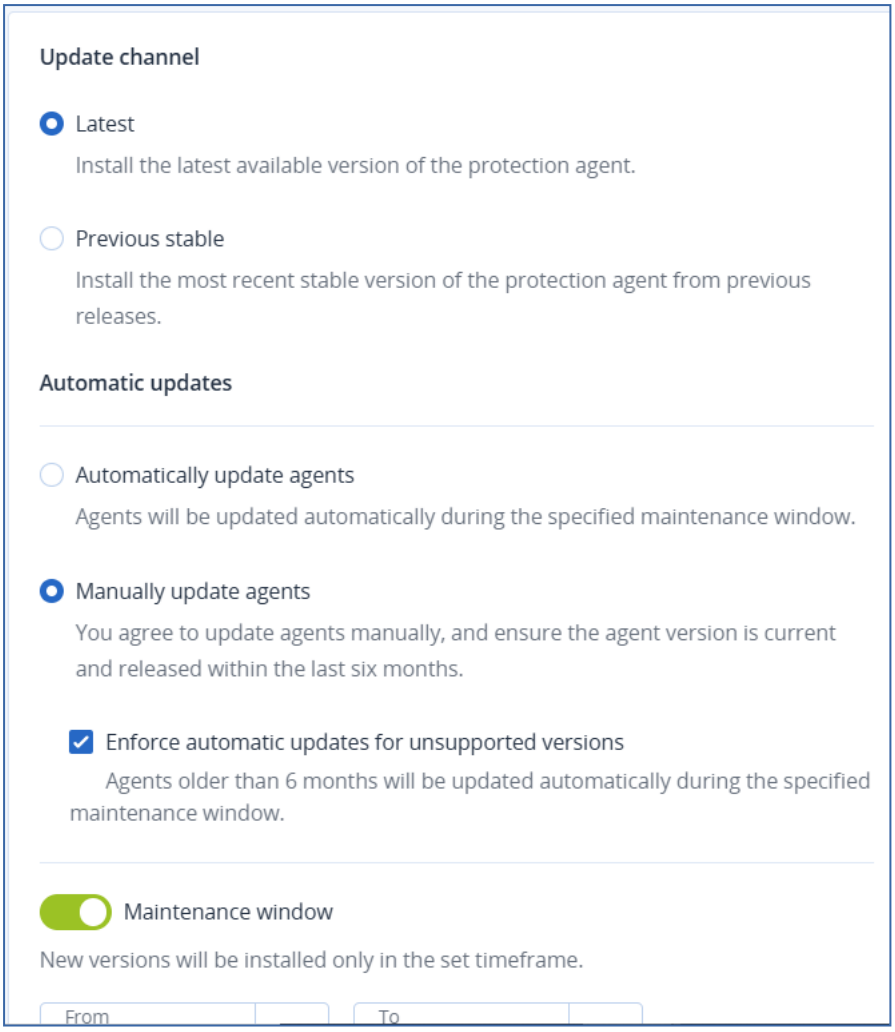
Importante
Si consiglia di abilitare gli aggiornamenti automatici per gli agenti. Gli aggiornamenti regolari consentono di mantenere gli agenti aggiornati, ottenere prestazioni migliori, risolvere i bug e disporre delle più recenti funzionalità di protezione e sicurezza.

Per configurare le impostazioni predefinite per gli aggiornamenti manuali degli agenti nel portale di gestione

1. Passare a **Impostazioni** > **Aggiornamento agenti**.
2. In **Canale di aggiornamento**, selezionare la versione da utilizzare per gli aggiornamenti automatici.

Opzione	Descrizione
Più recente (selezionata per impostazione predefinita)	Installa l'ultima versione disponibile dell'agente Cyber Protection.
Versione stabile precedente	Installa la versione più recente e stabile dell'agente Cyber Protection dalle versioni precedenti.

3. Selezionare **Aggiorna manualmente gli agenti**.



4. [Facoltativo] Per prevenire i rischi per la sicurezza, garantire l'accesso alle ultime funzionalità e ridurre al minimo i problemi tecnici causati da agenti particolarmente obsoleti, abilitare gli aggiornamenti automatici degli agenti più vecchi di 6 mesi.
   a. Selezionare **Forza gli aggiornamenti automatici per le versioni non supportate**.

      Importante
      Se gli aggiornamenti automatici degli agenti non sono stati abilitati prima del rilascio della versione C25.02, l'opzione viene abilitata automaticamente per tutti i tenant dell'ambiente.

   b. [Facoltativo] Impostare la finestra di manutenzione.
      La finestra di manutenzione predefinita è giornaliera, dalle 23:00 alle 08:00 sul sistema in cui è installato l'agente.

      Nota
      Benché gli aggiornamenti degli agenti siano 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. Fare clic su **Salva**.

Monitoraggio degli aggiornamenti dell'agente

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, vedere le sezioni Avvisi e Attività del Manuale dell'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.

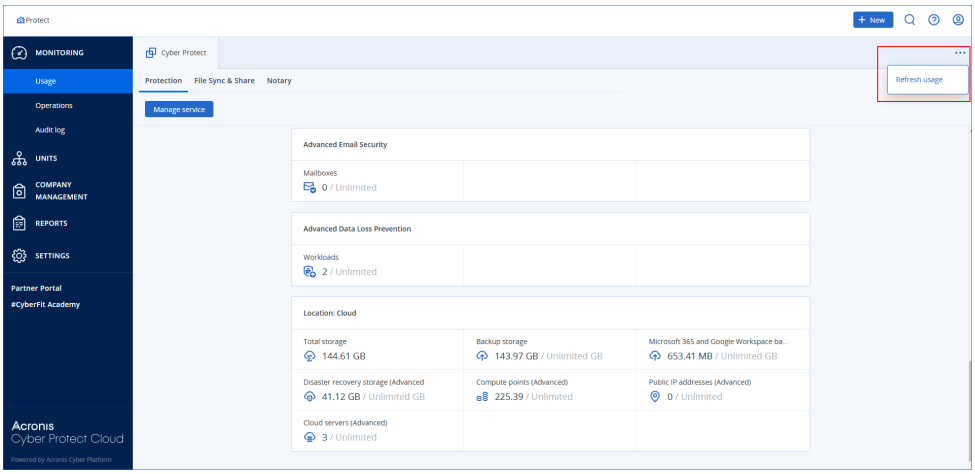
I dati di utilizzo includono i dati delle funzionalità incluse come standard e delle funzionalità avanzate.

Importante
I valori di utilizzo dello storage visualizzati nell'interfaccia utente del prodotto sono espressi in unità di byte binari: mebibyte (MiB), gibibyte (GiB) e tebibyte (TiB), anche se le rispettive etichette visualizzano MB, GB e TB. Ad esempio, se l'utilizzo effettivo è di 3105886629888 byte, il valore nell'interfaccia utente viene visualizzato correttamente come 2,82, ma l'etichetta riporta TB invece che TiB.

L'utilizzo dello storage per i workload di Microsoft 365 e Google Workspace viene riportato separatamente dallo storage di backup generale: è mostrato nella sezione **Backup di Microsoft 365 e Google Workspace**.

Per aggiornare i dati di utilizzo visualizzati sulla scheda, fare clic sull'icona dei 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

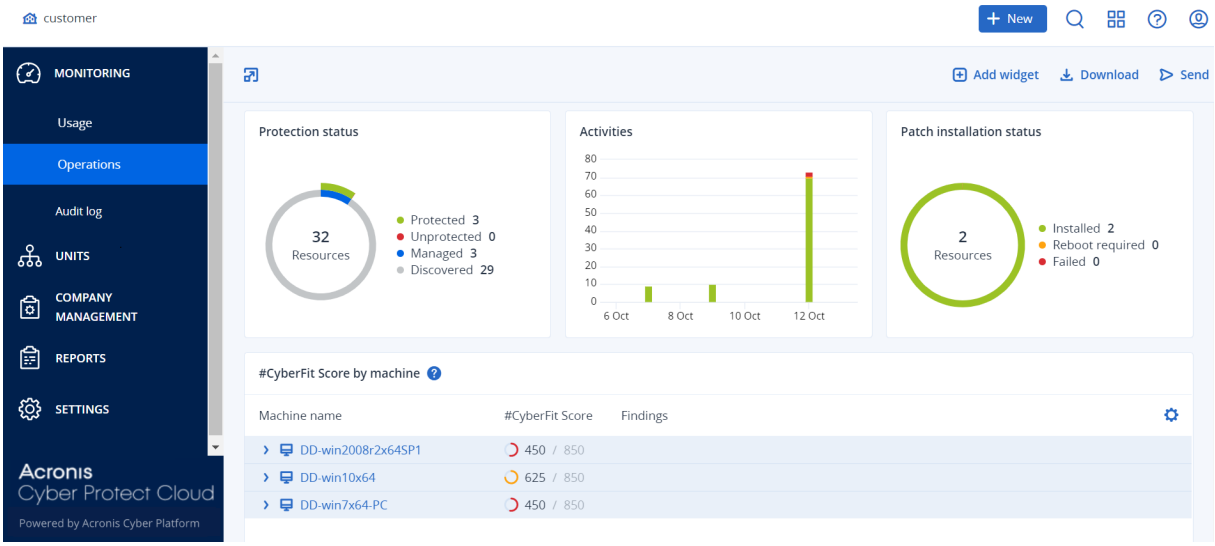
La dashboard **Operazioni** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al servizio Cyber Protection. I widget di altri servizi saranno disponibili nelle release future.

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. Nella dashboard *non* vengono visualizzate informazioni sui partner figlio e sui relativi tenant figlio; è necessario esaminare in dettaglio il partner specifico per visualizzare la relativa dashboard. Se, tuttavia, si converte un tenant partner figlio in un tenant cartella, le informazioni relative ai clienti figlio di tale tenant verranno visualizzate nella dashboard 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 della dashboard 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 nella dashboard

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 **Fine**.

Per rimuovere un widget

Fare clic sul simbolo X accanto al nome del widget.

Stato protezione

Stato protezione

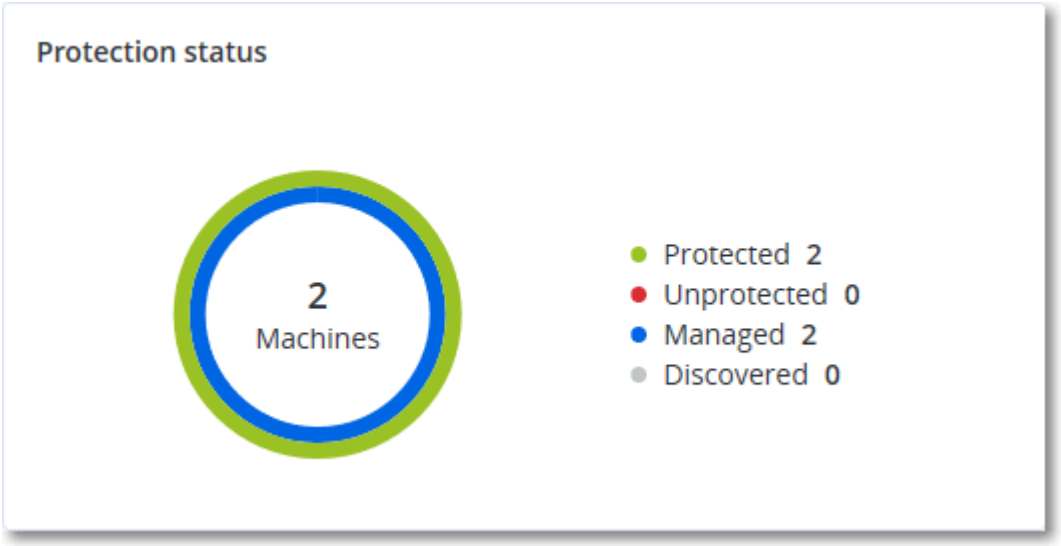
Questo widget mostra lo stato della protezione corrente di tutti i sistemi.

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.

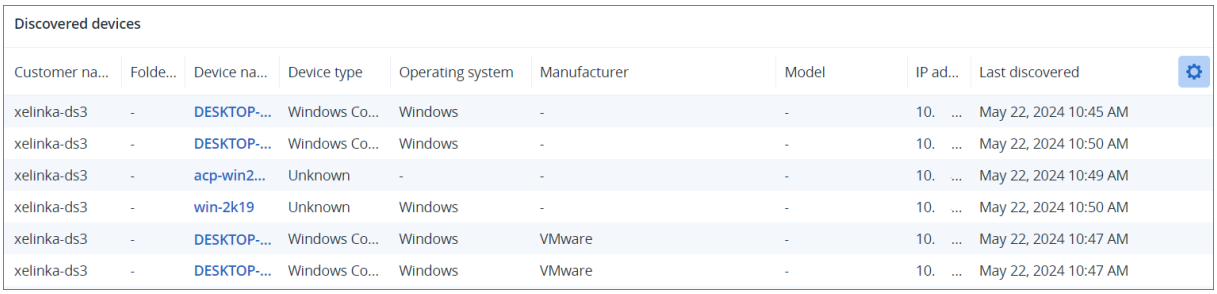
- **Gestito**: per tutti i sistemi con l'agente di protezione installato.
- **Individuato** : per tutti i sistemi senza l'agente di protezione installato.

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



Dispositivi individuati

Questo widget mostra informazioni dettagliate sui dispositivi individuati nelle reti dei clienti. Le informazioni sui dispositivi includono il tipo di dispositivo, il produttore, il sistema operativo, l'indirizzo IP, l'indirizzo MAC, la data di individuazione e altro.



#CyberFit Score per sistema

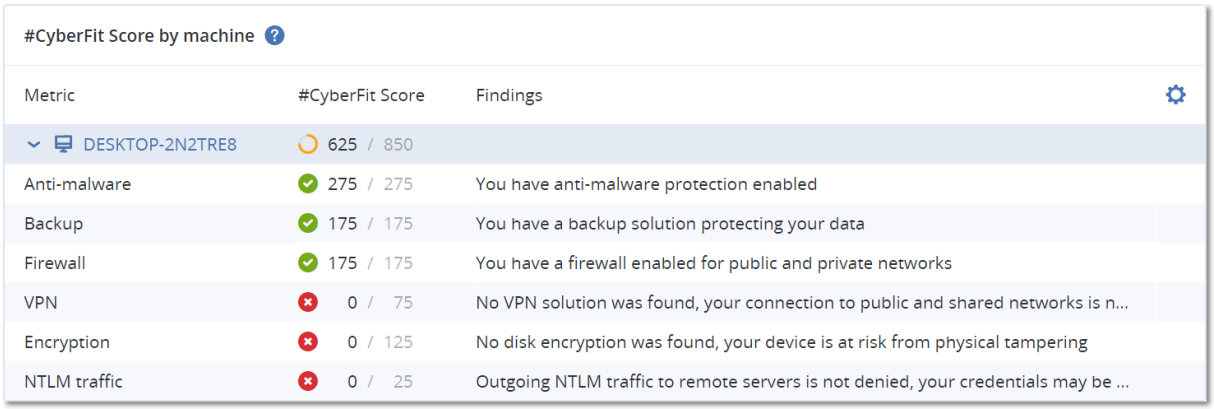
Questo widget mostra, per ogni sistema, il #CyberFit Score totale, i punteggi che lo compongono e i risultati ottenuti per ogni metrica valutata:

- 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)

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 del workload

Distribuzione dei principali problemi per workload

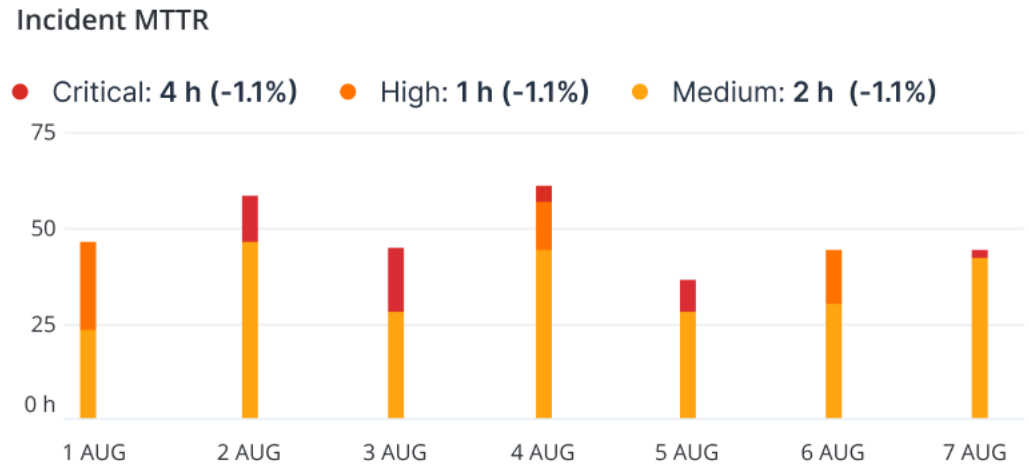
Questo widget mostra i primi cinque workload con il maggior numero di problemi (fare clic su **Mostra tutto** per essere reindirizzati all'elenco dei problemi filtrato in base alle impostazioni del widget).

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 (**Critico**, **Alto** e **Medio**) 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.



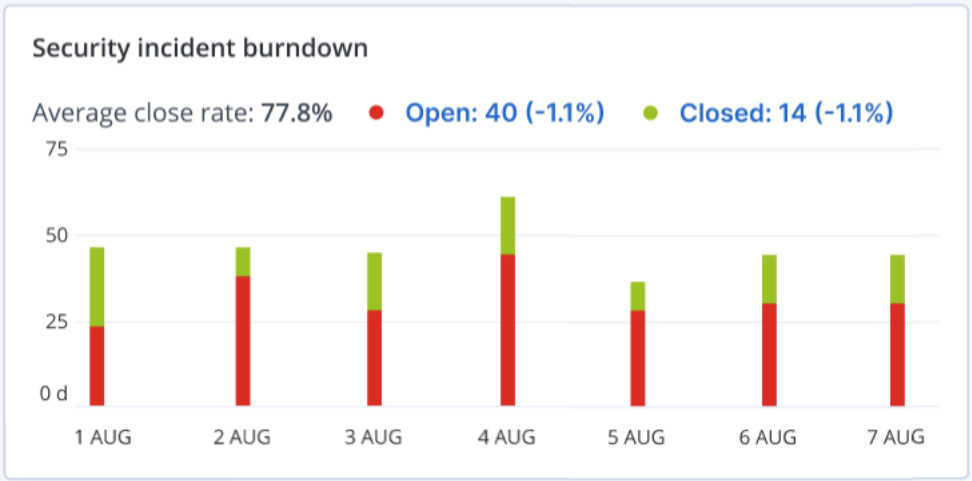
Burndown dei problemi di sicurezza

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**).

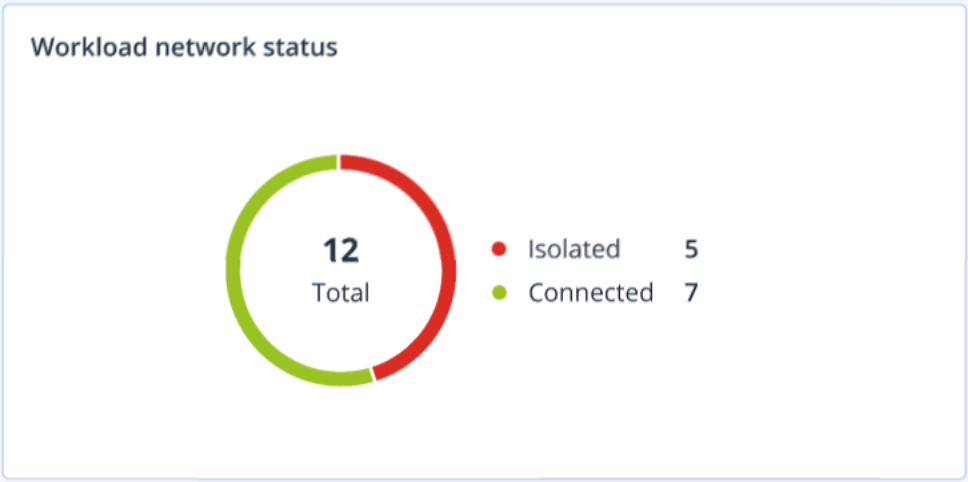
Il valore in percentuale (%) mostrato tra parentesi indica l'aumento o la diminuzione rispetto al periodo di tempo precedente.



Stato della rete del 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. I widget di integrità del disco non includono informazioni sui sistemi in cui è implementato RAID.
- Le unità SSD NVMe non sono supportate.
- I dispositivi di storage esterni non sono supportati.

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%.
- **Critico**
  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.

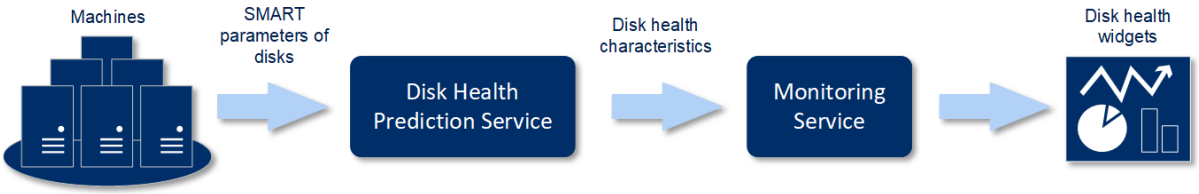
Come funziona

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 caratteristiche e quindi mostra le informazioni pertinenti nei widget di integrità del disco nella console di Cyber Protect.



Widget di integrità del disco

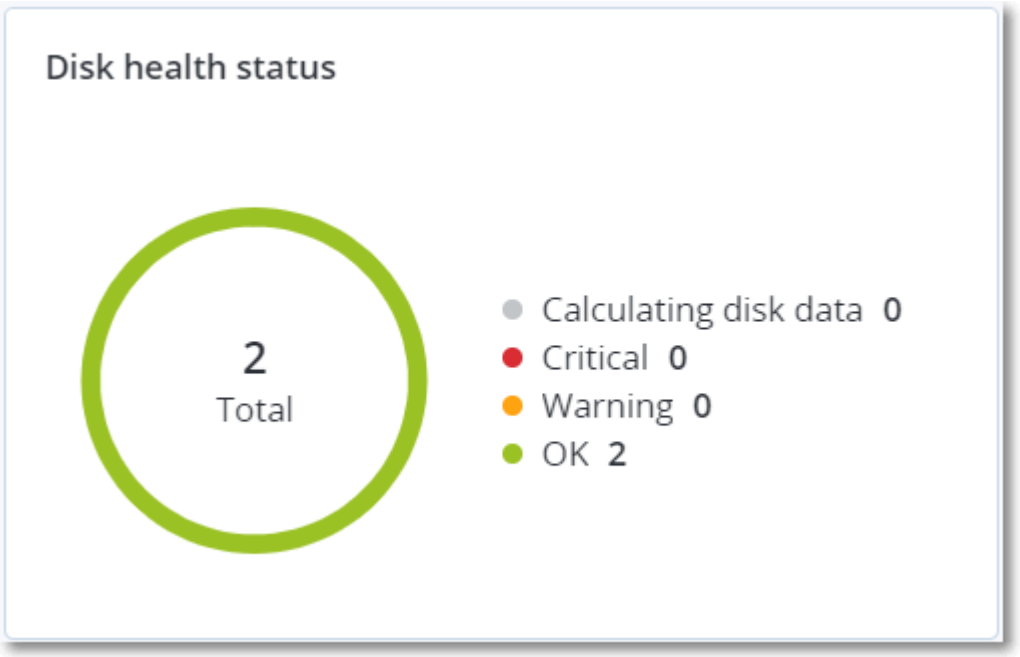
I risultati del monitoraggio dell'integrità del disco vengono presentati nei widget seguenti, disponibili nella console di Cyber Protect.

- **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	Attenzione	(30 – 70)	Il disco <disk name> 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 <disk name> 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 consigliato, 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.

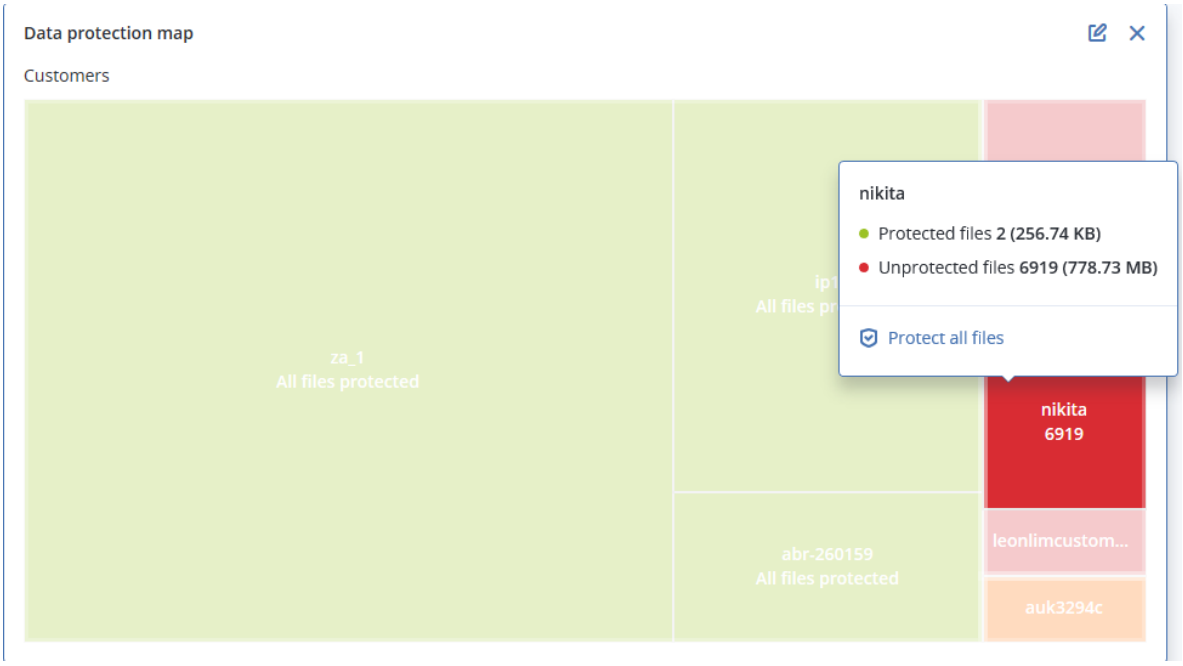
Ogni dimensione del blocco dipende dal numero/dimensione totale di tutti i file importanti che appartengono a un cliente/sistema.

I file possono presentare uno dei seguenti stati di protezione:

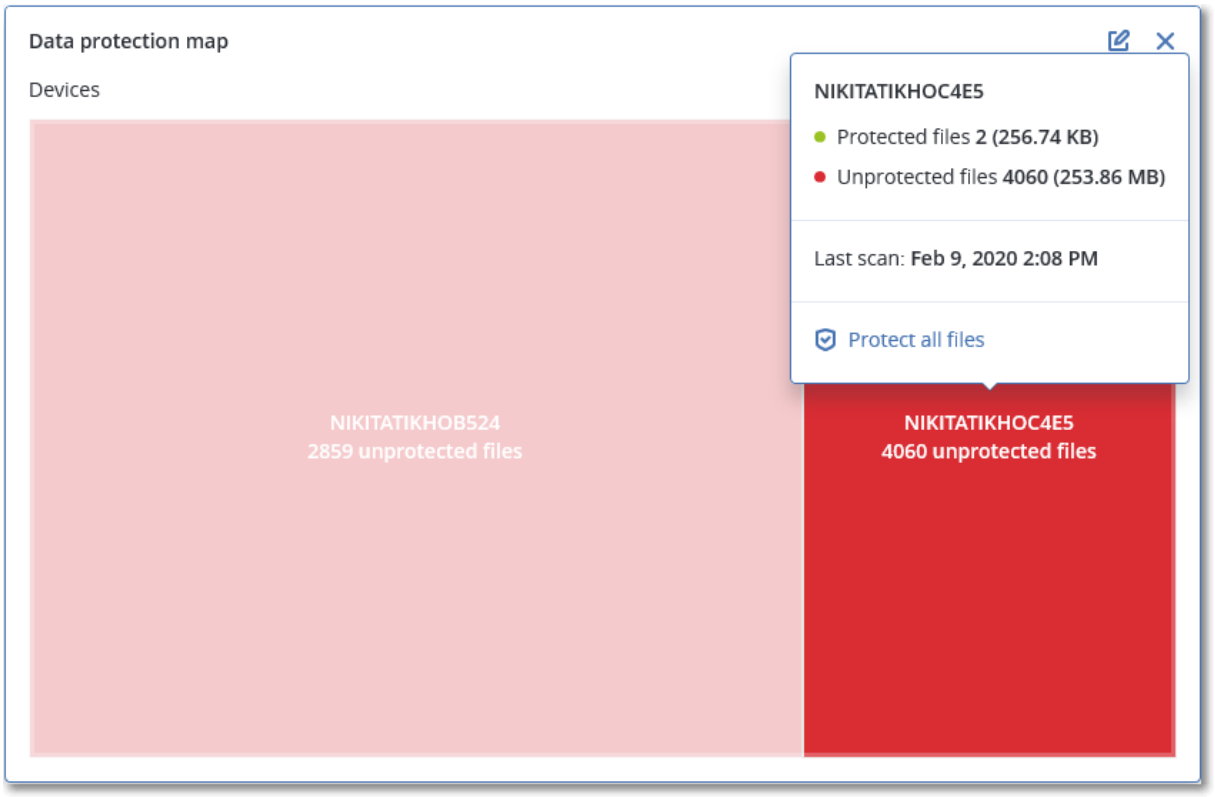
- **Critico** – è presente una percentuale compresa tra il 51 e il 100% di file non protetti con le estensioni specificate dall'utente di cui non viene eseguito il backup per il tenant/il sistema/la posizione del cliente selezionato.
- **Basso** – è presente una percentuale compresa tra il 21 e il 50% 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.
- **Alto** – 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 nella dashboard 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.

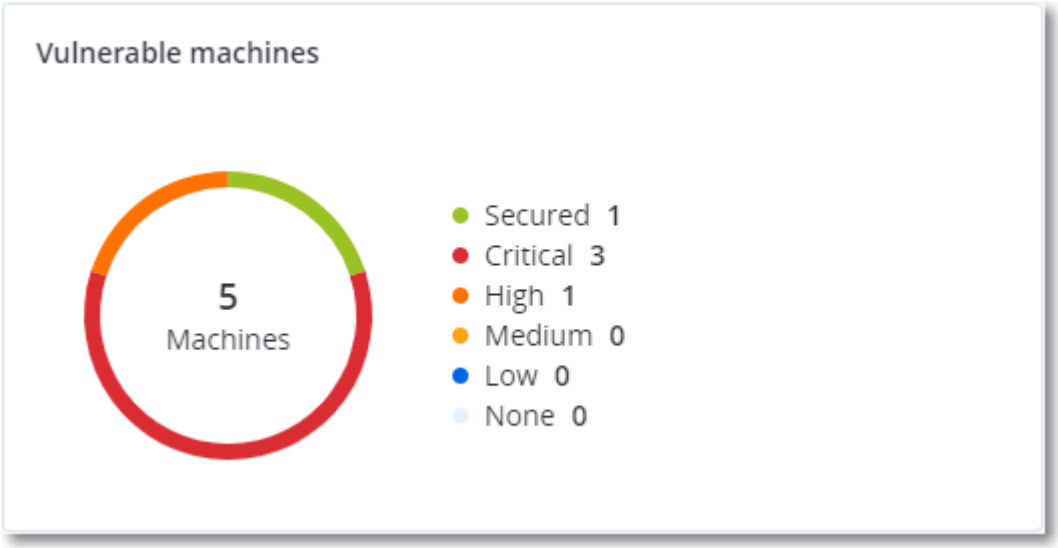
Widget di Vulnerability assessment

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
- Alto: 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

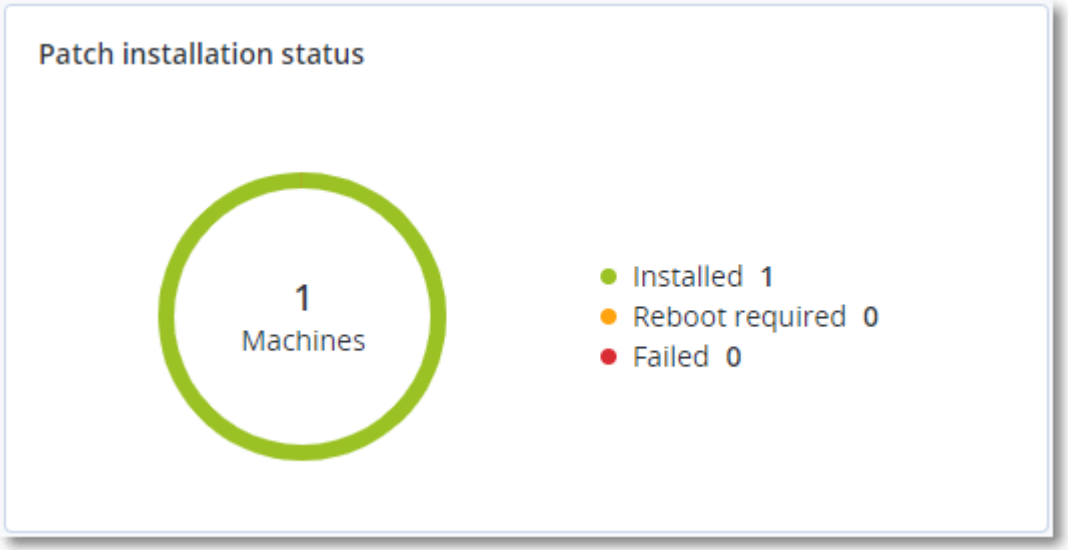
Widget di installazione patch

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

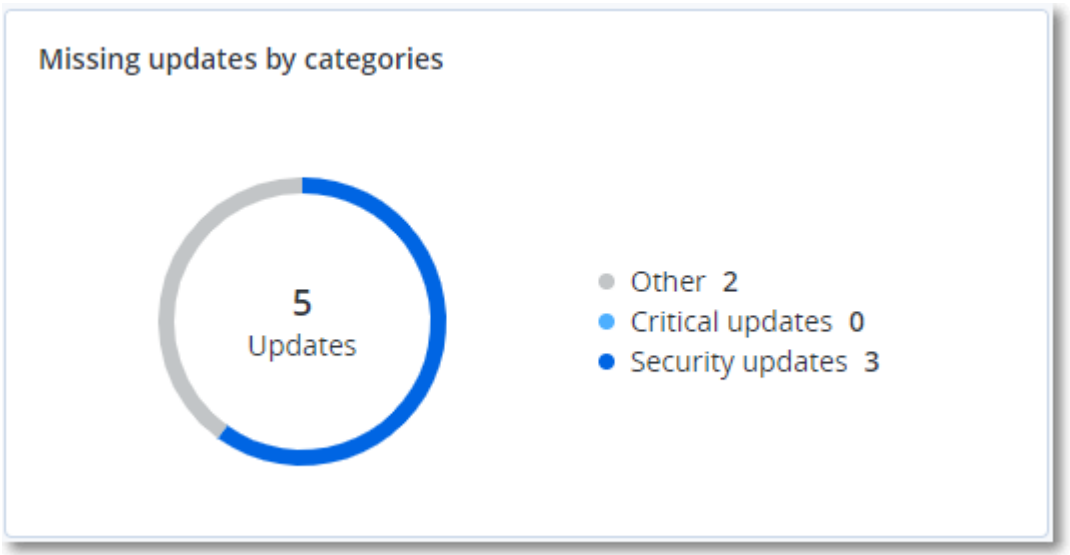
Cronologia di installazione patch

Questo widget mostra informazioni dettagliate sulle patch installate nei sistemi.

Aggiornamenti non effettuati per categorie

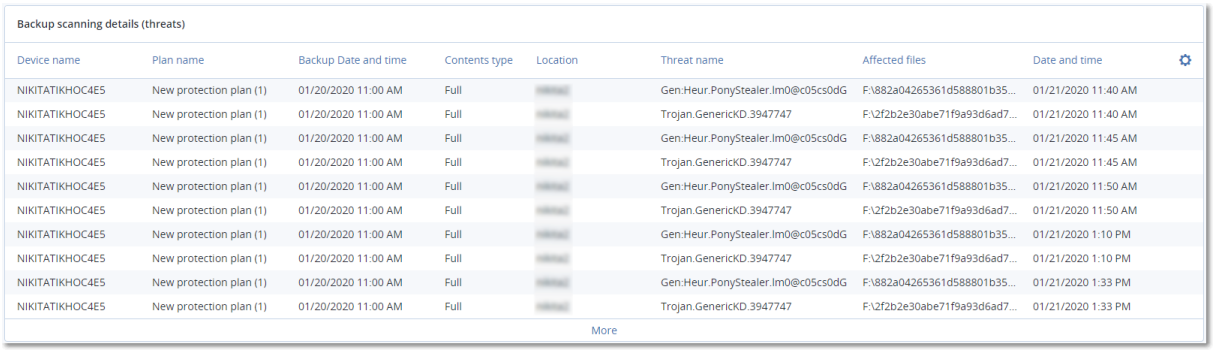
Questo widget mostra il numero di aggiornamenti non effettuati, per categoria. Vengono mostrate le seguenti categorie:

- Aggiornamenti di sicurezza
- Aggiornamenti critici
- Altro



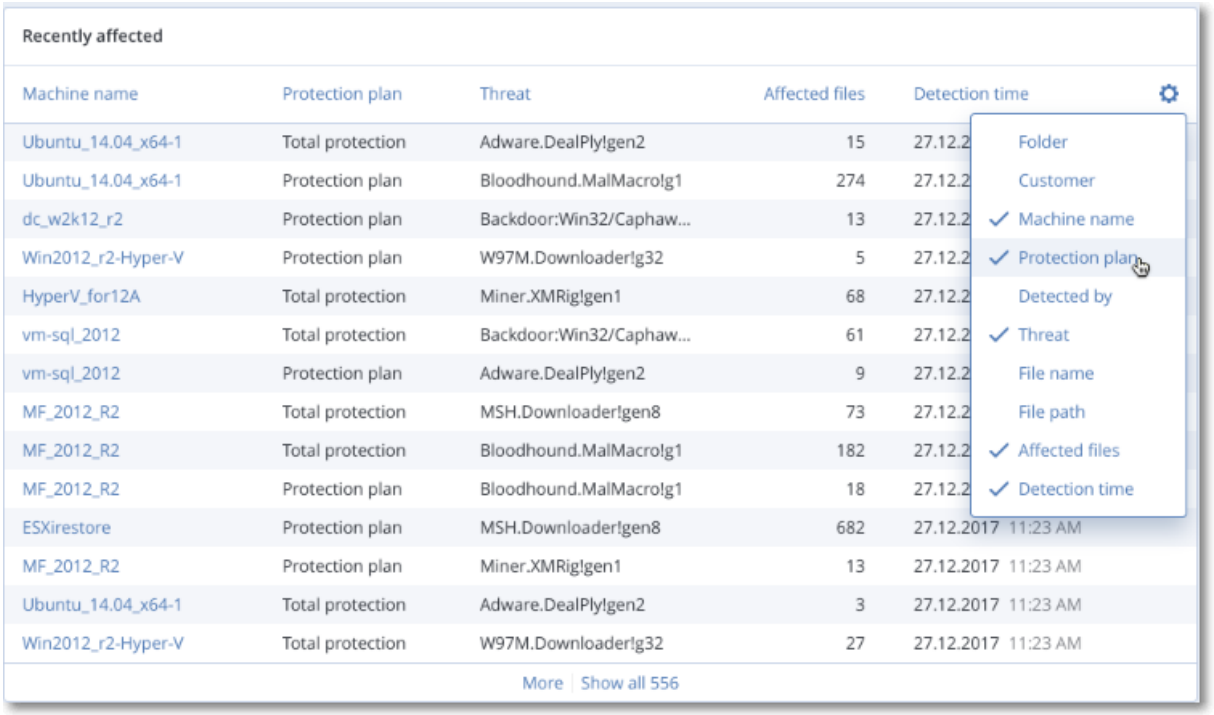
Informazioni sulla scansione del backup

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

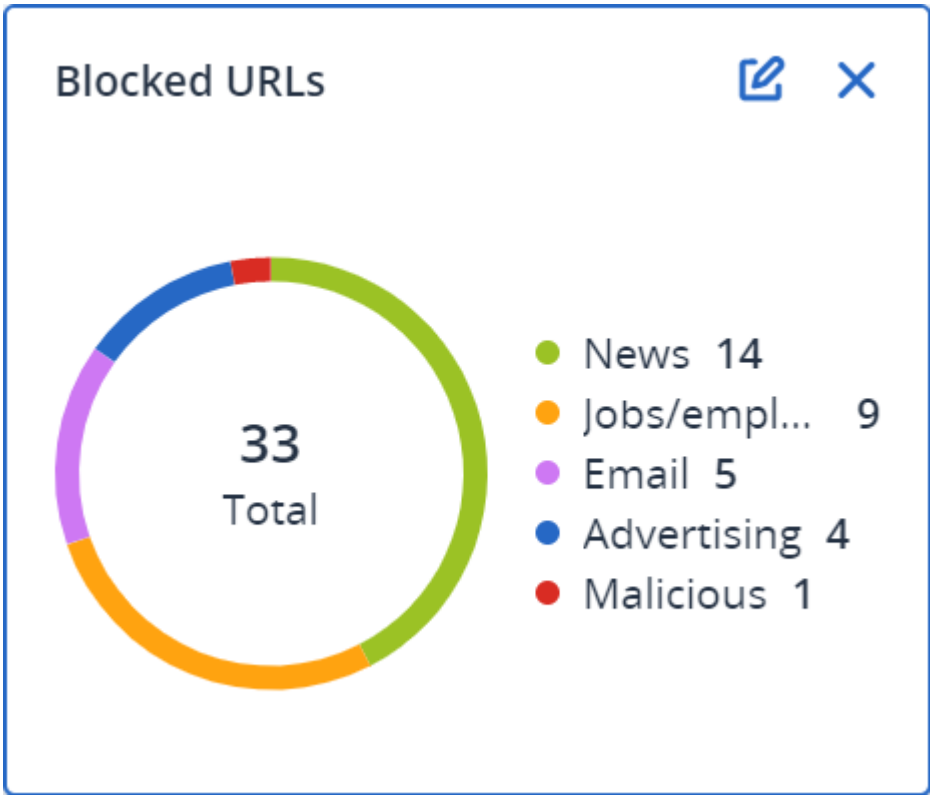
1. Nel widget **Recentemente interessati** fare clic su **Scarica dati**.
2. Nel campo **Periodo di tempo**, inserire il numero di giorni per i quali scaricare i dati. Il numero massimo di giorni che è possibile inserire è 200.
3. Nel campo **Destinatari**, immettere gli indirizzi e-mail di tutte le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

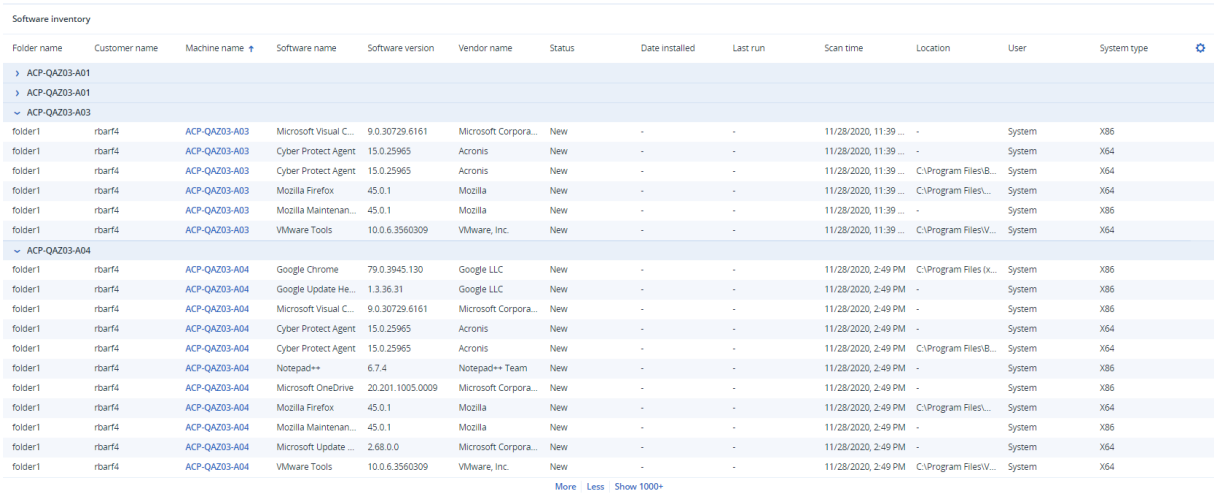
URL bloccati

Il widget mostra le statistiche degli URL bloccati per categoria. Per ulteriori informazioni sul filtro URL e sulla 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.

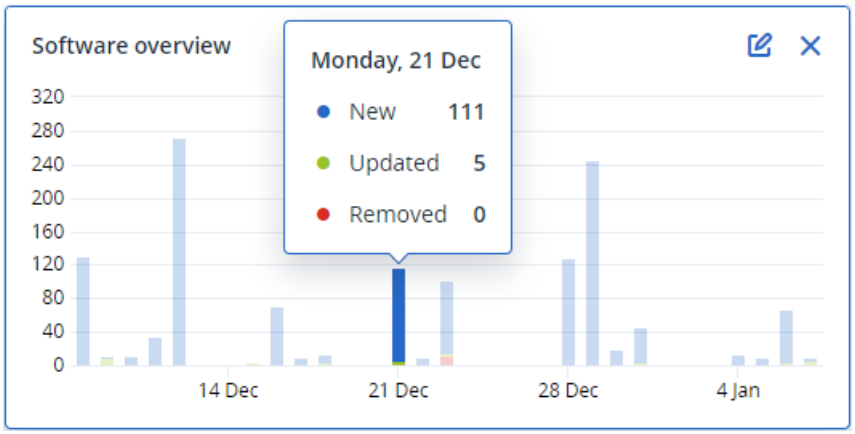


Software inventory

Folder name	Customer name	Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
ACP-QAZ03-A01												
ACP-QAZ03-A01												
ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

More | Less | Show 1000+

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.

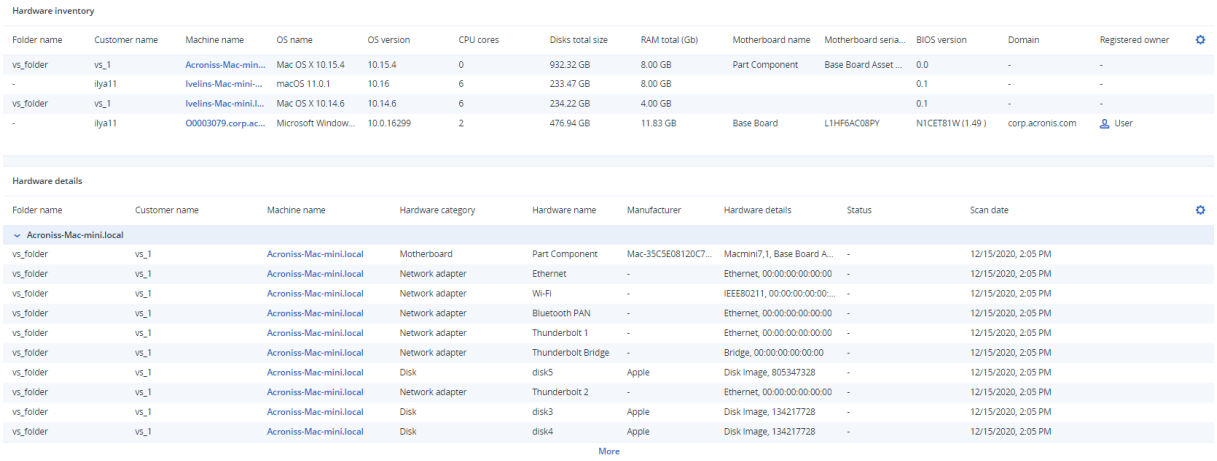
Aggiornate - il numero di applicazioni aggiornate.

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 di Cyber Protect 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 **Dettagli hardware** mostrano informazioni su tutti i componenti hardware installati sui dispositivi Windows e macOS fisici e virtuali dell'organizzazione del cliente.



Hardware inventory

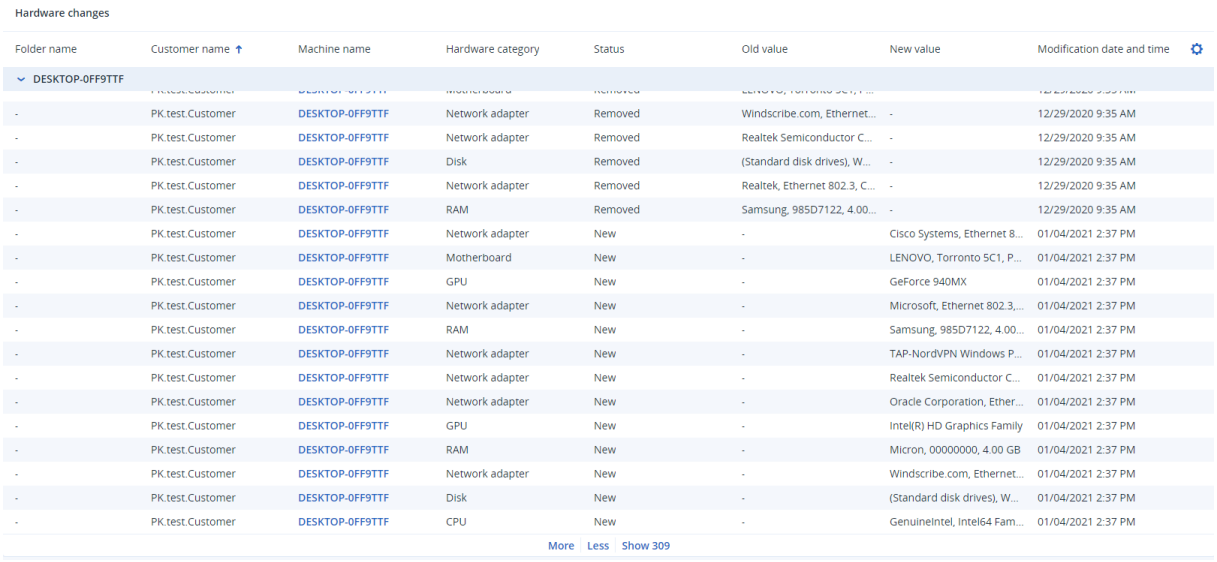
Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	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).



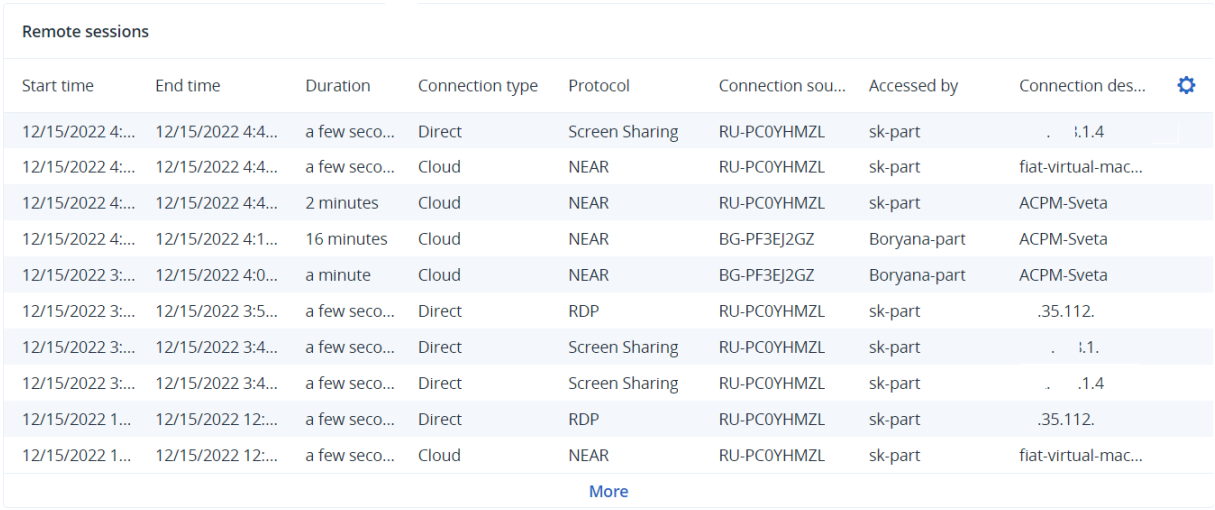
Hardware changes

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.



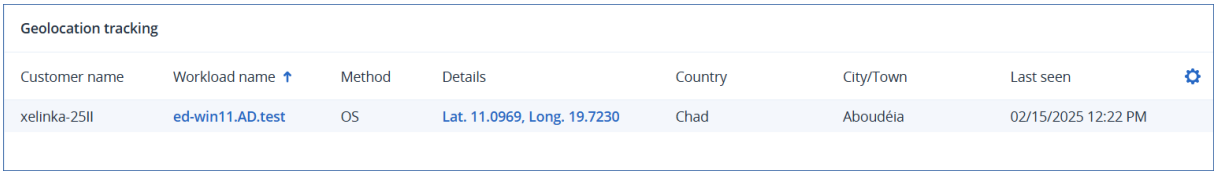
Remote sessions

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

Widget Tracciamento della geolocalizzazione

Nel widget **Tracciamento della geolocalizzazione** è possibile visualizzare i dettagli sulla posizione dei workload nelle organizzazioni dei clienti, come paese, città, coordinate, ora dell'ultimo accesso e metodo di tracciamento della geolocalizzazione.

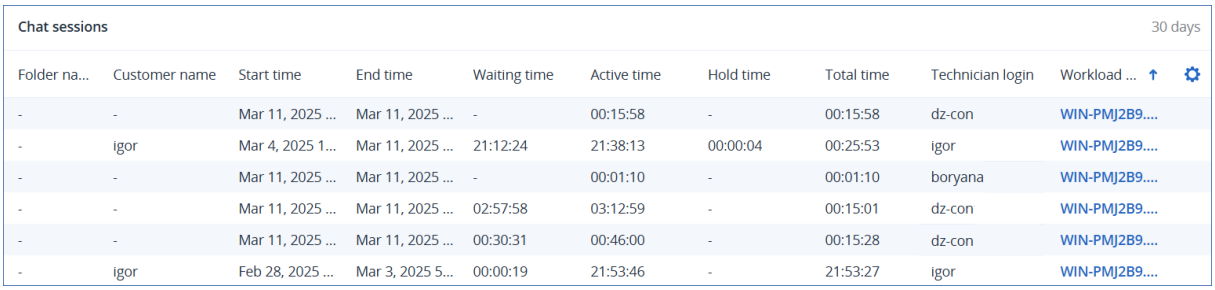


Geolocation tracking

Customer name	Workload name	Method	Details	Country	City/Town	Last seen
xelinka-25ll	ed-win11.AD.test	OS	Lat. 11.0969, Long. 19.7230	Chad	Aboudéia	02/15/2025 12:22 PM

Widget Sessioni di chat

Nel widget **Sessioni di chat**, puoi visualizzare i dettagli delle sessioni di chat remote nelle organizzazioni dei tuoi clienti per un periodo specificato.

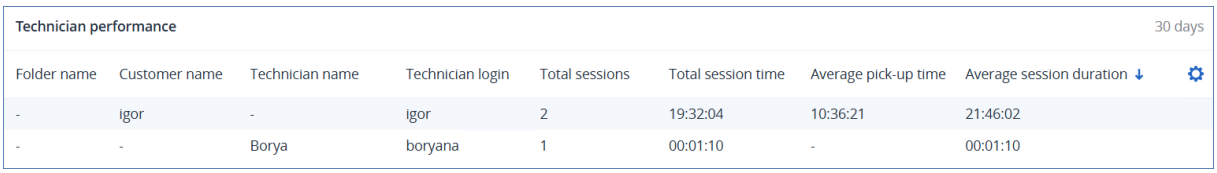


Chat sessions — 30 days

Folder na...	Customer name	Start time	End time	Waiting time	Active time	Hold time	Total time	Technician login	Workload ...
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:15:58	-	00:15:58	dz-con	WIN-PMJ2B9....
-	igor	Mar 4, 2025 1...	Mar 11, 2025 ...	21:12:24	21:38:13	00:00:04	00:25:53	igor	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:01:10	-	00:01:10	boryana	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	02:57:58	03:12:59	-	00:15:01	dz-con	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	00:30:31	00:46:00	-	00:15:28	dz-con	WIN-PMJ2B9....
-	igor	Feb 28, 2025 ...	Mar 3, 2025 5...	00:00:19	21:53:46	-	21:53:27	igor	WIN-PMJ2B9....

Widget Prestazione del tecnico

Nel widget **Prestazione del tecnico**, è possibile visualizzare i dettagli delle prestazioni di ciascun tecnico delle organizzazioni dei clienti per un periodo specificato.



Technician performance — 30 days

Folder name	Customer name	Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration
-	igor	-	igor	2	19:32:04	10:36:21	21:46:02
-	-	Borya	boryana	1	00:01:10	-	00:01:10

Vendite e fatturazione

La dashboard **Vendite e fatturazione** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al servizio Advanced Automation (PSA).

Per impostazione predefinita, i dati vengono visualizzati per il tenant nel quale si sta operando, a condizione che il servizio Advanced Automation (PSA) sia stato attivato.

I widget presentano elementi cliccabili che consentono di indagare e risolvere i problemi. È inoltre possibile scaricare lo stato corrente del dashboard in formato PDF, oppure inviarlo tramite e-mail a qualsiasi indirizzo, inclusi destinatari esterni.

Per riorganizzare i widget nella dashboard

Trascinare e rilasciare un widget facendo clic sul nome.

Per modificare un widget

Fare clic su sull'icona a matita nell'angolo in alto a destra del widget. La modifica del widget consente all'utente di rinominarlo.

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 su **Personalizza** quando il widget è selezionato. Dopo aver modificato il widget, fare clic su **Fine**.

Per rimuovere un widget

Fare clic sul simbolo X accanto al nome del widget.

Widget di Vendite e fatturazione

Questo dashboard mostra le metriche principali correlate alla fatturazione e alle vendite correnti, e include:

- **Contratti da fatturare**: questa sezione mostra l'importo totale di tutte le voci del contratto corrente che non sono state fatturate.
- **Articoli di vendita da fatturare**: questa sezione mostra l'importo totale di tutte le voci delle vendite correnti non ancora fatturate, comprese quelle in stato **Bozza**. È possibile passare alla schermata Fatture e avviare un nuovo ciclo di fatturazione per queste voci facendo clic su **Avvia ciclo di fatturazione**.
- **Numero utenti finali serviti**: questa sezione mostra il numero totale di utenti e contatti del cliente finale che vengono serviti (inclusi tutti gli utenti e i contatti attivi e inattivi).

- **Fatturato mensile dai servizi per utente**: questa sezione mostra l'importo del valore fatturato come rapporto tra *Contratti da fatturare* diviso per il *Numero di utenti finali che vengono serviti*. È possibile passare alla schermata dei Clienti facendo clic su **Vai a Clienti**.
- **Nuovo utile mensile ricorrente netto**: questo grafico mostra tre metriche principali: la perdita rispetto all'utile ricorrente mensile, l'incremento rispetto all'utile mensile ricorrente e il nuovo utile mensile ricorrente netto. Per impostazione predefinita, le tre metriche vengono visualizzate insieme ma possono essere mostrate separatamente facendo clic sul nome della metrica pertinente.
- **Tutti gli utili riferiti a elementi di vendita**: questo grafico mostra due metriche principali: tutti gli utili riferiti a elementi di vendita fatturati e tutti i nuovi utili riferiti a elementi di vendita. Per impostazione predefinita, le due metriche vengono visualizzate insieme ma possono essere mostrate separatamente facendo clic sul nome della metrica pertinente.
- **Workload**: questa sezione mostra il numero di workload che vengono gestiti e il numero di workload inclusi come parte di un contratto.

Service Desk

La dashboard **Service Desk** fornisce una serie di widget personalizzabili che offrono un'anteprima delle operazioni relative al Service Desk e correlate ad Advanced Automation (PSA).

Per impostazione predefinita, i dati vengono visualizzati per il tenant nel quale si sta operando, a condizione che il servizio Advanced Automation (PSA) sia stato attivato.

I widget presentano elementi cliccabili che consentono di indagare e risolvere i problemi. È inoltre possibile scaricare lo stato corrente del dashboard in formato PDF, oppure inviarlo tramite e-mail a qualsiasi indirizzo, inclusi destinatari esterni.

Per riorganizzare i widget nella dashboard

Trascinare e rilasciare un widget facendo clic sul nome.

Per modificare un widget

Fare clic su sull'icona a matita nell'angolo in alto a destra del widget. La modifica del widget consente all'utente di rinominarlo.

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 su **Personalizza** quando il widget è selezionato. Dopo aver modificato il widget, fare clic su **Fine**.

Per rimuovere un widget

Fare clic sul simbolo X accanto al nome del widget.

Widget del Service Desk

Grazie a una serie di widget, la dashboard Service Desk mostra le principali metriche relative alle operazioni svolte con i ticket. La dashboard visualizza le metriche relative ai ticket del Service Desk e dei preventivi, ma non ai ticket del progetto.

La dashboard include:

- **Service Desk**: questo widget viene visualizzato nella parte superiore della pagina e include diverse metriche principali:
  - **Ticket aperti**: visualizza il numero totale di ticket correnti che non sono nello stato **Chiuso** o **Risolto**.
  - **Violazioni degli SLA**: visualizza il numero totale di ticket correnti che non sono nello stato **Chiuso** o **Risolto** e che violano gli SLA. Fare clic su **Visualizza tutte le violazioni degli SLA** per visualizzare i ticket pertinenti.
  - **Ticket non assegnati**: visualizza il numero totale di ticket correnti che non sono stati assegnati a un tecnico.
  - **Ticket in scadenza oggi**: visualizza il numero totale di ticket correnti in scadenza nella giornata in corso. Fare clic su **Passa ai ticket in scadenza oggi** per visualizzare i ticket pertinenti.
  - **Prossimi interventi in sede**: visualizza il numero totale di interventi in sede pianificati. Fare clic su **Passa ai prossimi interventi in sede** per visualizzare i ticket pertinenti.
- **Ticket chiusi**: visualizza il numero totale di ticket chiusi, suddiviso in ticket odierni, del mese e dell'anno. Le metriche vengono visualizzate in due widget, uno per l'utente corrente e uno per i gruppi di cui l'utente è membro.
- **Net Promoter Score**: visualizza il punteggio NPS per il mese corrente. Le metriche vengono visualizzate in due widget, uno per l'utente corrente e uno per i gruppi di cui l'utente è membro.
- **Tipi di ticket**: visualizza un grafico a torta e la suddivisione in valori percentuali di tutti i ticket attualmente aperti, per tipo di ticket. Le metriche vengono visualizzate in due widget, uno per l'utente corrente e uno per i gruppi di cui l'utente è membro.
- **Statistiche ticket**: visualizza il numero totale di tutti i ticket chiusi rispetto ai ticket con violazioni degli SLA degli ultimi sette giorni. Le metriche vengono mostrate in due widget, uno per l'utente corrente e uno per i gruppi di cui l'utente è membro.
- **Percentuale di occupazione**: visualizza la percentuale di media di occupazione dei tecnici dell'organizzazione degli ultimi sette giorni. Le metriche vengono visualizzate in due widget, uno per l'utente corrente e uno per i gruppi di cui l'utente è membro.

Registro di audit

Il registro di audit 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 di Cyber Protect

- Operazioni di Cyber Scripting eseguite dagli utenti nella console di Cyber Protect
- Operazioni relative all'archiviazione di e-mail
- 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 di audit

Per ogni evento il registro visualizza i campi seguenti:

- **Evento**
  Breve descrizione dell'evento. Ad esempio: **Tenant creato**, **Tenant eliminato**, **L'utente è stato creato**, **L'utente è stato eliminato**, **La quota è stata raggiunta**, **Il contenuto di backup è stato esaminato**, **Script modificato**.
- **Gravità**
  Una tra le seguenti:
  - **Errore**
    Indica un errore.
  - **Attenzione**
    Indica un'azione potenzialmente negativa. Ad esempio: **Tenant eliminato**, **L'utente è stato eliminato**, **La quota è stata raggiunta**.
  - **Avviso**
    Indica un evento che potrebbe richiedere attenzione. Ad esempio: **Tenant aggiornato**, **L'utente è stato aggiornato**.
  - **Informativo**
    Indica una modifica o un'azione informativa neutrale. Ad esempio: **Tenant creato**, **L'utente è stato creato**, **La quota è stata 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 **L'utente è stato 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.

Raccolta dei dati sulle prestazioni per gli agenti Cyber Protection

Per i sistemi Windows protetti nell'ambiente dell'utente, è possibile acquisire i registri delle prestazioni manualmente o abilitare l'acquisizione automatica dei dati diagnostici se le prestazioni del sistema scendono al di sotto delle soglie definite nelle configurazioni di fabbrica. Consultare "Soglie delle prestazioni per l'acquisizione dei dati ETL" (pag. 134).

I registri acquisiti vengono anonimizzati prima di essere inviati per l'analisi al fornitore. I seguenti dati verranno eliminati da tutti i registri, messaggi, avvisi e messaggi di errore:

- Account utente
- Nome società
- Nome del workload protetto

Come amministratore Partner, è possibile abilitare l'acquisizione automatica dei registri per agenti selezionati casualmente nei tenant figli o per agenti specifici in un'organizzazione che si gestisce.

Come amministratore dell'azienda, è possibile abilitare l'acquisizione automatica dei registri per agenti selezionati casualmente o per agenti specifici nella propria organizzazione.

Nota

- L'acquisizione automatizzata dei dati sui singoli workload è supportata sull'agente di Cyber Protection per Windows versione 24.4.37758 o successiva.
- L'acquisizione dei dati sulle prestazioni a livello di tenant è supportata sull'agente di Cyber Protection per Windows versione 25.03.XXXXX o successiva.

Affinché le nostre raccomandazioni di supporto siano aggiornate, acquisiamo dati da circa il 10% degli agenti nell'ambiente per l'analisi.

Questa impostazione non annulla le impostazioni sui workload individuali. Ad esempio, se l'acquisizione automatizzata dei dati è disabilitata su un workload specifico, quel workload non verrà incluso nell'acquisizione di dati in blocco.

Acquisizione automatizzata per più agenti

Per abilitare l'acquisizione automatica dei dati sulle prestazioni per più agenti in un tenant

Ruolo richiesto: Amministratore del Partner, Amministratore di clienti

1. Nella console di Cyber Protect Cloud, passare a **Impostazioni** > **Agenti**.
2. Nel menu **Azioni** a destra, fare clic su **Modifica le impostazioni di monitoraggio delle prestazioni**.
3. Nella sezione **Monitor delle prestazioni**, attivare l'interruttore **Acquisizione e caricamento automatici dei registri delle prestazioni**.

I dati acquisiti automaticamente vengono archiviati nei dischi locali dei sistemi protetti, nella cartella `C:\ProgramData\Acronis\ETLTool\ETL\`, anonimizzati e inviati al service provider per l'analisi.

Nota
Il limite per l'invio dei registri ETL al cloud è di 3 volte in 24 ore.

Acquisizione automatica per un singolo agente

Per abilitare l,acquisizione automatica dei dati sulle prestazioni per un agente specifico

1. A livello aziendale nella console di Cyber Protect Cloud, passare a **Impostazioni** > **Agenti**.
2. Nell'elenco **Agenti**, selezionare l'agente per il quale abilitare il monitoraggio delle prestazioni.
3. Nel menu **Azioni** a destra, fare clic su **Dettagli**.
4. Scorrere verso il basso fino alla sezione **Monitor delle prestazioni** e attivare l'interruttore **Consenti a questo agente di acquisire automaticamente i registri delle prestazioni**.

I dati acquisiti automaticamente vengono archiviati nel disco locale del sistema protetto, nella cartella `C:\ProgramData\Acronis\ETLTool\ETL\`.

Acquisizione manuale

Per acquisire manualmente i dati sulle prestazioni

È possibile acquisire i dati sulle prestazioni su richiesta. In questo caso, non è necessario abilitare il monitoraggio delle prestazioni e l'acquisizione automatica dei dati sulle prestazioni.

1. Accedere al sistema protetto come utente amministratore.
2. Nel prompt dei comandi, eseguire uno dei seguenti comandi:
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o`
     La raccolta di tracce ETL viene eseguita fino a quando non si preme il tasto `S` sulla tastiera o fino a quando non scade il limite di tempo massimo di 3600 secondi.

- `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X`
  Dove X è il limite di tempo per la raccolta dei dati espresso in secondi; il valore massimo è 3600. È possibile arrestare la raccolta in qualsiasi momento premendo il tasto `S` sulla tastiera.

I dati raccolti manualmente vengono archiviati nel disco locale del sistema protetto, nella cartella `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`

Per acquisire i registri delle prestazioni

1. Accedere al sistema protetto come utente amministratore.
2. Individuare i dati richiesti:
   - I dati sulle prestazioni raccolti automaticamente si trovano nella cartella `C:\ProgramData\Acronis\ETLTool\ETL\`
   - I dati sulle prestazioni raccolti su richiesta si trovano nella cartella `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`

Le tracce ETL sono incluse anche nel pacchetto `sysinfo`.

Soglie delle prestazioni per l'acquisizione dei dati ETL

È possibile abilitare l'acquisizione automatica dei dati sulle prestazioni dei sistemi Windows protetti nel proprio ambiente. Il monitoraggio è configurato nella console di Cyber Protect Cloud per agente, e abilita la raccolta automatica dei dati di diagnostica se le prestazioni del sistema scendono al di sotto delle soglie predefinite.

L'acquisizione automatizzata dei dati inizia quando viene superata una delle soglie.

Soglie predefinite per l'acquisizione dei dati ETL

La tabella seguente descrive le soglie che attivano l'acquisizione automatica dei dati ETL.

Parametro	Descrizione	Valore predefinito
"process-memory-consumption"	Soglia per l'utilizzo elevato della memoria	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	Soglia per l'utilizzo elevato dell'I/O del disco	
"maximum-operations-number"		10000
"maximum-transferred-bytes"		100000000

Parametro	Descrizione	Valore predefinito
"estimation-period-seconds"		5
"process-file-io"	Soglia per l'utilizzo elevato dell'I/O del file	
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	Soglia per l'utilizzo elevato della CPU	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	Prestazioni dei componenti dell'agente di protezione	
"behavioral-engine"	Soglia per il motore comportamentale	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	Soglia per il componente Protezione antivirus e anti-malware	
"average-scan-duration-seconds"	Durata media massima della scansione	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	Durata massima di una singola scansione	5

Elaborazione di rapporti

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

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.

Importante
I valori di utilizzo dello storage visualizzati nell'interfaccia utente del prodotto sono espressi in unità di byte binari: mebibyte (MiB), gibibyte (GiB) e tebibyte (TiB), anche se le rispettive etichette visualizzano MB, GB e TB. Ad esempio, se l'utilizzo effettivo è di 3105886629888 byte, il valore nell'interfaccia utente viene visualizzato correttamente come 2,82, ma l'etichetta riporta TB invece che TiB.

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.

  Nota
  I dati sull'utilizzo dello storage locale vengono riportati solo ai livelli di unità e tenant cliente. I report sintetici inviati agli utenti non contengono informazioni sull'utilizzo dello storage locale.

- **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:

- **Clienti e 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.

Nota
Il filtraggio per data viene eseguito in base al timestamp corrispondente all'invio dell'evento al cloud, e non all'orario di avvio o completamento dell'attività. Pertanto, se la connessione al server è stata interrotta, il report giornaliero potrebbe contenere i dati relativi a più di una sola giornata.

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**.

Vendite e fatturazione

Il componente Vendite e fatturazione di Advanced Automation (PSA) include una serie di report ai quali è possibile accedere dal menu **Report** > **Vendite e fatturazione**.

Nota
I report Vendite e fatturazione sono disponibili agli utenti con i ruoli seguenti: Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità, Risorse umane.

Ogni report Vendite e fatturazione include informazioni relative a un intervallo di tempo specificato, che può essere modificato come necessario.

I report Vendite e fatturazione separano anche l'importo di un servizio "venduto" (visualizzato nella colonna **Quantità venduta**, se pertinente) in base alla configurazione della fatturazione e all'importo del servizio effettivamente "utilizzato" (visualizzato nella colonna **Quantità utilizzata**, se pertinente). In questo modo le spese vengono calcolate con esattezza, così come la redditività delle vendite e le spese. Ad esempio, se si utilizzano contratti con impegni minimi e si vende a un cliente 1 TB di storage (configurato tramite la quantità minima di prodotto fatturabile del contratto), ma nel mese il cliente utilizza solo 600 GB di storage, il report visualizza:

- **Quantità venduta** = 1 TB
- **Quantità utilizzata** = 600 GB

Poiché l'utilizzo effettivo è stato di soli 600 GB e non di 1 TB, il report mostrerà il profitto corretto per il mese.

I report Vendite e fatturazione disponibili sono:

- Utile cliente
- Spese
- "Redditività previsionale" (pag. 141)
- Profitto lordo per cliente
- Riepilogo profitto lordo

Creazione di un nuovo report

È possibile creare un nuovo report a partire da uno dei report disponibili.

1. Fare clic su **Crea nuovo report**.
2. Selezionare il report pertinente.
   Viene creato automaticamente un nuovo report con lo stesso nome (con l'aggiunta del suffisso (1)).
3. [Facoltativo] Per aggiornare il nome del report, fare clic su **Impostazioni**, inserire il nuovo nome e quindi fare clic su **Salva**.
   È inoltre possibile clonare ed eliminare il report, se necessario.

Download di un report

È possibile scaricare qualsiasi report facendo clic sull'icona dei puntini di sospensione accanto al selettore dell'intervallo di tempo e selezionando il formato richiesto:

- **PDF**
- **Excel e PDF** (disponibile solo per il report Spese)
- **Excel** (disponibile solo per il report Spese)

Utile cliente

Il report Utile cliente permette di tenere traccia delle principali metriche di vendita per ogni cliente, incluse informazioni su:

- Tutti i clienti, selezionati uno alla volta.
- Un intervallo di tempo specificato.

Per generare il report Utile cliente, passare a **Report** > **Vendite e fatturazione** e selezionare **Utile cliente**. Quindi selezionare il cliente e l'intervallo di tempo desiderati; per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Vendite e fatturazione" (pag. 138).

Il report generato include i widget seguenti:

- Spesa cliente, incluso:
  - Importo totale ricorrente
  - Importo totale non ricorrente
  - Importo totale VAR
  - Importo totale
- Tariffa oraria media cliente, che mostra la tariffa oraria media per i ticket e i progetti per il periodo selezionato.
- Tempo cliente trascorso, incluso:
  - Tempo trascorso in base al prezzo fisso.
  - Tempo trascorso in base a calcoli successivi.
  - Tempo trascorso sui progetti.
  - Tempo trascorso in base ad altro, non fatturabile.
- Sezione di un contratto relativa agli endpoint, che mostra il numero totale di endpoint che fanno parte dei contratti con il cliente.
- Endpoint totali gestiti, che mostra il numero totale di endpoint del cliente affidati in gestione.
- Numero utenti finali serviti, che mostra il numero totale di utenti del cliente che vengono serviti.
- Contratti da fatturare, che mostra l'importo totale di tutte le voci del contratto corrente.
- Fatturato mensile dai servizi per utente, che mostra l'importo totale dei contratti da fatturare diviso per il numero di utenti finali che vengono serviti.
- Elementi del contratto, che visualizza un elenco degli elementi dei contratti includendo il valore per l'intero anno.

Spese

Il report Spese mostra informazioni sul costo dei prodotti e dei servizi forniti ai clienti e include:

- Vendite e voci di contratto che rientrano nel periodo specificato per il report.
- Articoli fatturati o non ancora fatturati (compresi gli articoli di vendita con stato **In sospeso** e **Bozza**).
- Informazioni specifiche per un cliente o un report per tutti i clienti.
- Informazioni specifiche per un prodotto o un report per tutti i prodotti.

Per generare il report Spese, passare a **Report > Vendite e fatturazione** e selezionare **Spese**. Quindi selezionare il cliente, il prodotto, il tipo di spesa e il periodo di tempo desiderati; per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Vendite e fatturazione" (pag. 138).

Il report generato include:

- Una sezione di riepilogo generale.
- Una sezione per il cliente, ovvero un riepilogo riga per riga dei nomi dei prodotti o dei servizi forniti a un cliente.

Redditività previsionale

Il report Redditività previsionale mostra informazioni sulla redditività futura, che vengono elaborate a partire dalle informazioni seguenti:

- Contratti attuali e periodi di contratti attivi.
- Voci dei contratti attivi attuali e periodi definiti per tali voci.
- Cronologia delle attività basate sui ticket.
- Cronologia degli articoli di vendita.
- Prezzi e costi attuali dei prodotti e dei servizi.

Per generare il report Redditività previsionale, passare a **Report > Vendite e fatturazione**, quindi selezionare **Redditività previsionale**. Quindi selezionare il cliente, il prodotto e il periodo di tempo pertinenti; per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Vendite e fatturazione" (pag. 138).

Il report generato include:

- Una sezione di riepilogo generale.
- Una sezione di riepilogo mensile, che include le percentuali di crescita su base mensile e annuale.
- Un riepilogo degli ultimi sei mesi.
- Una sezione per il cliente, ovvero un riepilogo riga per riga dei nomi dei prodotti o dei servizi forniti a un cliente.

Nota
Gli articoli di vendita con stato **In sospeso** o **Bozza** sono inclusi nel riepilogo per mese e cliente. Vengono calcolati anche come parte delle voci **Costo totale**, **Entrate totali** e **Profitto totale**.

Profitto lordo per cliente

Il report Profitto lordo per cliente permette di tenere traccia dei profitti e dei costi relativi a specifici clienti, incluse le informazioni seguenti:

- Tutti i clienti, selezionati uno alla volta.
- Un intervallo di tempo specificato.

Per generare il report Profitto lordo per cliente, passare a **Report > Vendite e fatturazione** e selezionare **Profitto lordo per cliente**. Quindi selezionare il cliente e il periodo di tempo desiderati; per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Vendite e fatturazione" (pag. 138).

Il report generato include:

- Una sezione di riepilogo.
- La suddivisione di ogni contratto relativo al cliente selezionato.
- Una panoramica sulla redditività dei contratti, degli articoli di vendita dei progetti e del costo del lavoro del cliente.

Riepilogo profitto lordo

Il report Riepilogo profitto lordo offre un'analisi dei profitti e dei costi, incluse le informazioni seguenti relative a:

- Tutti i clienti, con un riepilogo su un'unica riga per ciascun cliente.
- Un intervallo di tempo specificato.
- Un periodo di aggregazione specificato (mese/trimestre/anno).

Per generare il report Riepilogo profitto lordo, passare a **Report > Vendite e fatturazione** e selezionare **Riepilogo profitto lordo**. Selezionare quindi le date pertinenti nel campo **Periodo**; per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Vendite e fatturazione" (pag. 138).

Il report include una sezione di riepilogo principale relativa a tutti i clienti e al periodo di tempo indicato; nella sezione il profitto totale per un cliente viene calcolato come la differenza tra profitto e costi.

Service Desk

Il componente Service Desk di Advanced Automation (PSA) include una serie di report ai quali è possibile accedere dal menu **Report** > **Service Desk**.

Nota
I report del componente Service Desk sono disponibili agli utenti con i ruoli seguenti: Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità, Risorse umane

Ogni report Service Desk include informazioni relative a un intervallo di tempo specificato, che può essere modificato come necessario.

I report del Service Desk disponibili sono:

- "Riepilogo dei ticket del cliente" (pag. 143)
- Durata dei ticket completati
- "Rilevamento NPS" (pag. 144)
- Numero di aggiornamenti nel ticket
- Riepilogo SLA
- "Pianificazione delle capacità dei tecnici" (pag. 146)
- Metriche di prestazione dei tecnici

- Statistiche ticket
- Ticket con stato specifico
- "Schede attività" (pag. 147)

Creazione di un nuovo report

È possibile creare un nuovo report a partire da uno dei report disponibili.

1. Fare clic su **Crea nuovo report**.
2. Selezionare il report pertinente.
   Viene creato automaticamente un nuovo report con lo stesso nome (con l'aggiunta del suffisso (1)).
3. [Facoltativo] Per aggiornare il nome del report, fare clic su **Impostazioni**, inserire il nuovo nome e quindi fare clic su **Salva**.
   È inoltre possibile clonare ed eliminare il report, se necessario.

Download di un report

È possibile scaricare qualsiasi report facendo clic sull'icona dei puntini di sospensione accanto al selettore dell'intervallo di tempo e selezionando il formato richiesto:

- **PDF**
- **Excel e PDF** (disponibile solo per il report sintetico Ticket del cliente)
- **Excel** (disponibile solo per il report sintetico Ticket del cliente)

Riepilogo dei ticket del cliente

Il report sintetico Ticket del cliente fornisce un elenco dei ticket di un cliente specifico e le relative statistiche per un periodo definito, tra cui:

- Ticket creati durante il periodo. Nel report sono inclusi tutti i ticket del Service Desk. I ticket relativi a preventivi, progetti e ordini di acquisto sono esclusi dal report.
  L'anteprima del report visualizza inizialmente fino a 100 ticket nei dettagli del ticket. Fare clic su **Altro** per visualizzare più ticket.
- Statistiche generali per il periodo, tra cui il numero di ticket aperti, chiusi e con violazione dello SLA, nonché i tipi e le categorie di ticket.
- Dettagli del ticket, tra cui il numero, il titolo, la categoria, la priorità, l'utente finale, l'agente, lo SLA e il tempo dedicato al ticket (tempo fatturabile, non fatturabile o fatturato).

Per generare il report sintetico Ticket dei clienti, passare a **Report** > **Service Desk** e selezionare **Riepilogo dei ticket del cliente**. Selezionare quindi il cliente e l'intervallo di tempo pertinenti nei campi **Cliente** e **Periodo**.

Per filtrare e personalizzare l'elenco visualizzato in base alle esigenze, è anche possibile utilizzare lo strumento **Filtro**. È ad esempio possibile mostrare o nascondere le colonne visualizzate nel report, come quelle riferite al tempo effettivamente dedicato a un ticket o alle violazioni degli SLA.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Durata dei ticket completati

Il report Durata dei ticket completati fornisce informazioni sui tempi di risoluzione dei ticket, in particolare il numero di giorni trascorsi tra la creazione e la chiusura del ticket. Questi dati consentono di individuare eventuali tempi eccessivi, per gestirli in modo più efficiente.

Per generare il report Durata dei ticket completati, passare a **Report > Service Desk** e selezionare **Durata dei ticket completati**. Selezionare quindi le date pertinenti nel campo **Periodo**.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Rilevamento NPS

Il report Rilevamento NPS (Net Promoter Score) visualizza i punteggi dei ticket in base ai feedback ricevuti dall'utente finale. Quando un ticket viene chiuso, agli utenti viene automaticamente inviata un'e-mail tramite la quale possono valutare il servizio.

Il report consente di tenere traccia di una serie di metriche chiave del cliente, tra cui:

- Rapporto percentuale tra tutti i promoter e tutti gli intervistati.
- Numero di intervistati del promoter (utenti finali) che hanno valutato i ticket con voti tra 9 e 10.
- Rapporto percentuale tra tutti i promoter e tutti gli intervistati neutrali.
- Numero di intervistati neutrali (utenti finali) che hanno valutato i ticket con voti tra 7 e 8.
- Rapporto percentuale tra tutti i detrattori e tutti gli intervistati.
- Numero di intervistati detrattori (utenti finali) che hanno valutato i ticket con voti tra 0 e 6.
- Valore NPS, che viene calcolato come punteggio medio tra tutti gli intervistati.

Per generare il report Rilevamento NPS, passare a **Report** > **Service Desk**, quindi selezionare **Rilevamento NPS**. Selezionare le date pertinenti nel campo **Periodo**; è inoltre possibile selezionare un cliente, un utente finale del cliente, un agente del supporto o un gruppo di supporto specifici per ottimizzare ulteriormente il report.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Numero di aggiornamenti nel ticket

Il report Numero di aggiornamenti nel ticket fornisce informazioni su quanti aggiornamenti sono stati apportati ai ticket in un periodo di tempo specificato e consente di individuare i ticket che

causano problemi e non vengono risolti tempestivamente. Ad esempio, molti aggiornamenti possono indicare una mancanza di conoscenze del tecnico che genera aggiornamenti da parte del tecnico e dell'utente finale, nel tentativo di risolvere il problema.

Per generare il report Numero di aggiornamenti nel ticket, passare a **Report > Service Desk**, quindi selezionare **Numero di aggiornamenti nel ticket**. Selezionare quindi le date pertinenti nel campo **Periodo**.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Riepilogo SLA

Il report Riepilogo SLA consente di esaminare le principali metriche degli SLA in base all'azienda, al gruppo e al tecnico.

Nel report, è possibile tenere traccia delle tre metriche relative allo SLA indicate di seguito:

- SLA prima risposta
- Tempo della risposta successiva
- Tempo di risoluzione

Per generare il report Riepilogo SLA, passare a **Report > Service Desk**, quindi selezionare **Riepilogo SLA**. Selezionare le date pertinenti nel campo **Periodo**; è inoltre possibile selezionare un utente e un gruppo di utenti specifici per ottimizzare ulteriormente il report.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Metriche di prestazione dei tecnici

Il report Metriche di prestazione dei tecnici consente di tenere traccia delle principali metriche relative alle prestazioni dei tecnici, tra cui:

- Orario di copertura, inclusi gli orari di lavoro disponibili e l'orario di lavoro effettivo registrato.
- Sistema di contabilità, incluso il costo del lavoro calcolato moltiplicando il numero di ore lavorate per il costo di tali ore.
- Copertura lavorativa per ticket, inclusi i ticket assegnati e lavorati dal tecnico selezionato, oltre ai primi tre ticket con il lead time più alto.
- Copertura lavorativa per progetti, inclusi i progetti correnti lavorati e i progetti chiusi completati/non completati entro il tempo preventivato.
- Punteggio Net Promoter Score del tecnico, inclusi i ticket con la migliore/peggiore valutazione.

Per generare il report Metriche di prestazione dei tecnici, passare a **Report > Service Desk**, quindi selezionare **Metriche di prestazione dei tecnici**. Selezionare le date pertinenti nel campo **Periodo**; è inoltre possibile selezionare un utente specifico per ottimizzare ulteriormente il report.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Pianificazione delle capacità dei tecnici

Il report Pianificazione delle capacità dei tecnici permette di tenere traccia dei workload dei tecnici e delle capacità previste per i periodi futuri. Per ogni tecnico incluso nel report, è possibile:

- Visualizzare il numero totale di tutte le ore lavorative disponibili (tutto il tempo disponibile meno i fine settimana, le ferie retribuite approvate, i periodi di malattia e le festività nazionali) per il periodo selezionato.
- Visualizzare il numero totale di tutte le attività pianificate (incluse quelle del Service Desk e dei progetti) in giorni.
- Visualizzare il numero totale delle giornate non lavorative (inclusi ferie retribuite approvate, periodi di malattia e festività nazionali) per il periodo selezionato.
- Visualizzare il tempo totale disponibile per il periodo selezionato (tutti i giorni di lavoro meno tutte le attività pianificate).

Per generare il report Pianificazione delle capacità dei tecnici, passare a **Report** > **Service Desk**, quindi selezionare **Pianificazione delle capacità dei tecnici**. Selezionare le date pertinenti nel campo **Periodo** e il tipo di gruppo desiderato nel campo **Report di gruppo per**; è inoltre possibile selezionare un tecnico specifico per ottimizzare ulteriormente il report.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Statistiche ticket

Il report Statistiche ticket visualizza un grafico relativo al numero totale di ticket chiusi e di ticket che presentano una violazione dello SLA. Il report visualizza le statistiche relative alla giornata corrente, al mese corrente e le statistiche annuali complessive. Il report consente di visualizzare rapidamente le prestazioni del team e di identificare i ticket chiusi a fronte dei ticket con violazioni; mostra inoltre gli eventuali miglioramenti registrati negli ultimi mesi.

Per generare il report Statistiche ticket, passare a **Report > Service Desk**, quindi selezionare **Statistiche ticket**. Selezionare le date pertinenti nel campo **Periodo**; è inoltre possibile selezionare un cliente specifico per ottimizzare ulteriormente il report.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Ticket con stato specifico

Il report Ticket con stato specifico consente di individuare i ticket con uno stato specifico, che appartengono a una categoria specifica o che hanno una determinata priorità.

Per generare il report Ticket con stato specifico, passare a **Report > Service Desk**, quindi selezionare **Ticket con stato specifico**. Selezionare le date rilevanti nel campo **Periodo**; è inoltre

possibile selezionare uno stato, una categoria e/o una priorità per ottimizzare ulteriormente il report.

Per ulteriori informazioni su come personalizzare, scaricare e inviare il report tramite e-mail, consultare "Service Desk" (pag. 142).

Schede attività

Il componente Monitoraggio orario di Advanced Automation (PSA) include un report Schede attività al quale è possibile accedere dal menu **Report** > **Service desk**. Tale report consente di visualizzare la media delle ore di lavoro registrate dagli utenti e fornisce una rapida panoramica del tempo dedicato ai ticket e ad altre attività, ad esempio le voci orario manuali.

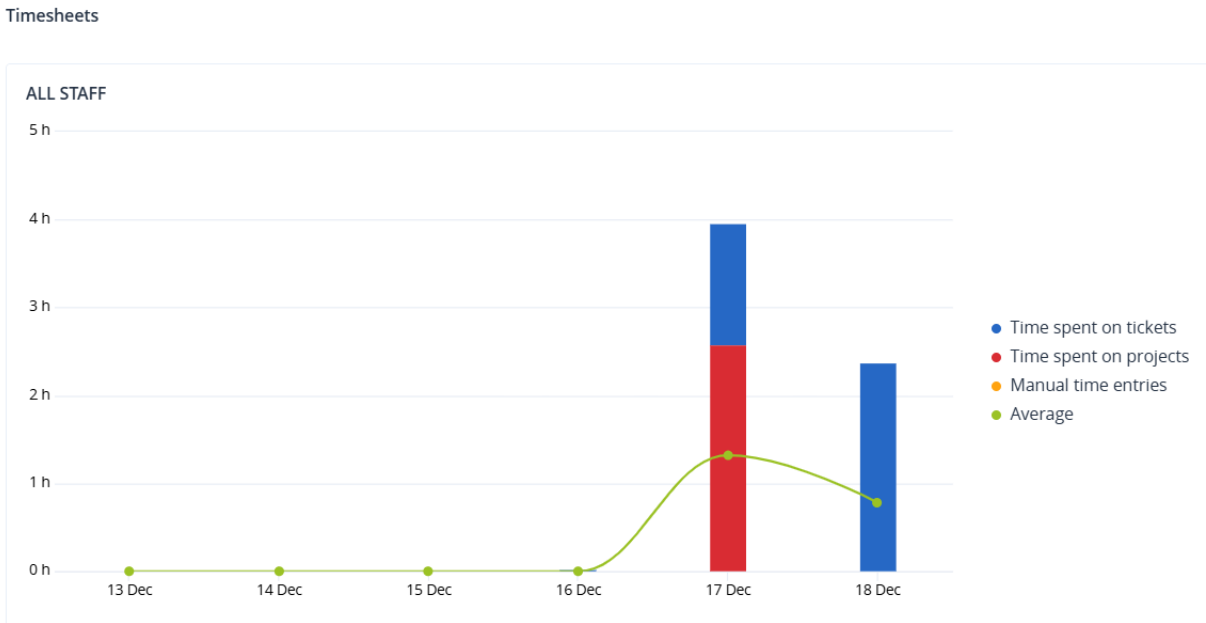
Nota
Il report Schede attività è disponibile agli utenti che dispongono dei ruoli seguenti: Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità, Risorse umane

Il report Schede attività include informazioni relative a un intervallo di tempo specificato, che può essere modificato come necessario. Il report include due tipi di widget:

- Il widget **Tutto il personale**, che include un riepilogo di tutti gli utenti attivi.
- Singoli widget per ogni utente.

Ogni widget include informazioni sul tempo medio di connessione durante il periodo selezionato, il tempo dedicato ai ticket, il tempo dedicato ai progetti e il tempo allocato per l'inserimento manuale delle voci orario.

È inoltre possibile aggiungere al report altri report e widget esistenti per personalizzarlo in base alle esigenze, oltre a scaricare ogni report o inviarlo tramite e-mail in formato Excel (XLSX) o PDF. Vedere le sezioni pertinenti in "Service Desk" (pag. 142) per ulteriori informazioni.



Report Operazioni

Un report relativo alle operazioni può includere qualsiasi insieme di widget della dashboard **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. 165).

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 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.
Dispositivi individuati	Mostra tutti i dispositivi individuati nelle reti dei clienti.
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.

Azioni con i report

Aggiungi

Per aggiungere un nuovo report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report disponibili, fare clic su **Aggiungi report**.
3. [Per aggiungere un report predefinito] Fare clic sul nome del report predefinito.
4. [Per aggiungere un report personalizzato] Fare clic su **Personalizzato** e quindi aggiungere i widget al report.
5. [Facoltativo] Trascinare e rilasciare i widget per riorganizzarli.

Visualizzazione

Per visualizzare un report

- Per visualizzare un report, fare clic sul relativo nome.

Modifica

Per modificare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da modificare.
3. Nell'angolo in alto a destra dello schermo, fare clic su **Impostazioni**.
4. Apportare le modifiche necessarie al report e fare clic su **Salva**.

Elimina

Per eliminare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da eliminare.
3. Nell'angolo in alto a destra dello schermo, fare clic sull'icona dei puntini di sospensione, quindi su **Elimina report**.
4. Nella finestra di conferma, fare clic su **Elimina**.

Pianificazione

Per programmare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report da pianificare.
3. Nell'angolo in alto a destra dello schermo, fare clic su **Impostazioni**.
4. Abilitare l'opzione accanto a **Pianificato**.
   - Specificare gli indirizzi e-mail dei destinatari.
   - Selezionare il formato del report.

     Nota
     È possibile esportare fino a 1.000 voci in un file PDF e fino a 10.000 voci in un file XLSX. I timestamp nei file PDF e XLSX utilizzano l'ora locale del sistema.

   - Selezionare la lingua del report.
   - Configurare la pianificazione.
5. Fare clic su **Salva**.

Download

Per scaricare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report.
3. Nell'angolo in alto a destra dello schermo, fare clic su **Download**.
4. Selezionare il formato del report.

Nel computer viene scaricato un file nel formato selezionato.

Selezionando **Excel e PDF**, nel sistema viene scaricato un file ZIP.

Invia

Per inviare un report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report.

3. Nell'angolo in alto a destra dello schermo, fare clic su **Invia**.
4. Specificare gli indirizzi e-mail dei destinatari.
5. Selezionare il formato del report.
6. Fare clic su **Invia**.

Esporta struttura

Per esportare la struttura del report

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report.
3. Nell'angolo in alto a destra dello schermo, fare clic sull'icona dei puntini di sospensione, quindi su **Esporta**.

La struttura del report viene salvata nel sistema come file JSON.

Esegui il dump dei dati

Per effettuare il dumping dei dati del report

È possibile esportare tutti i dati relativi a un periodo personalizzato, senza filtrarli, in un file CSV e poi inviarlo a un destinatario di posta elettronica. Il file CSV contiene solo i dati relativi ai widget inclusi nel report.

Nota
È possibile esportare fino a 150.000 voci in un file CSV. I timestamp nel file CSV utilizzano l'orario UTC (Coordinated Universal Time).

1. Nella console di Cyber Protect, passare a **Report**.
2. Nell'elenco dei report, selezionare il report con i dati di cui eseguire il dump.
3. Nell'angolo in alto a destra dello schermo, fare clic sull'icona dei puntini di sospensione, quindi su **Esegui il dump dei dati**.
4. Specificare gli indirizzi e-mail dei destinatari.
5. In **Intervallo di tempo**, specificare l'intervallo temporale del cliente per il quale eseguire il dump dei dati.

   Nota
   La preparazione dei file CSV relativi a periodi più lunghi richiede più tempo.

6. 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, Gestione patch, 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): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Caselle di posta di Exchange ospitato

Widget	Descrizione
	• 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. **Data esecuzione 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. **Dispositivi periferici bloccati** - Il numero totale di dispositivi periferici bloccati.
Stato della rete del	Questo widget mostra il numero di workload isolati e di quelli connessi (questo è lo stato normale dei workload).

Widget	Descrizione
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**.
Dispositivi individuati	Il widget mostra le informazioni seguenti sui dispositivi individuati nelle reti del dei clienti in un periodo specificato: **Nome cliente** **Nome cartella** **Nome periferica** **Tipo di dispositivo** **Sistema operativo** **Produttore** **Modello** **Indirizzo IP** È possibile modificare il widget e filtrare le informazioni visualizzate per tenant, unità organizzativa, tipo di dispositivo, tipo di individuazione, data della prima individuazione, data dell'ultima individuazione, indirizzo IP, indirizzo MAC e tipo di individuazione.

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 anti-malware 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 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 filtro 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 (**Critico**, **Alto** e **Medio**) e un'indicazione del tempo impiegato

Widget	Descrizione
	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**.

Widget	Descrizione
	Calcolo dei dati del disco in corso - Lo stato del dispositivo corrisponde a **Calcolo dei dati del disco** quando gli stati dei relativi dischi non sono ancora stati calcolati.
Utilizzo dello storage 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 Vulnerability assessment e gestione patch

La tabella seguente fornisce più informazioni sui widget presenti nella sezione **Vulnerability assessment e gestione patch**.

Widget	Descrizione
Vulnerabilità con patch applicate	Il widget mostra i risultati delle prestazioni di Vulnerability assessment 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 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 Software

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

Widget	Descrizione
Stato installazione	Questo widget visualizza il numero totale di attività di installazione sui dispositivi gestiti dei clienti, raggruppate per stato. Facendo clic su un segmento del grafico a ciambella, il sistema reindirizza alla pagina **Attività**, in cui vengono visualizzate solo le attività con lo stato corrispondente, in ordine cronologico.
Stato della disinstallazione	Questo widget visualizza il numero totale di attività di disinstallazione sui dispositivi gestiti dei clienti, raggruppate per stato. Facendo clic su un segmento del grafico a ciambella, il sistema reindirizza alla pagina **Attività**, in cui vengono visualizzate solo le attività con lo stato corrispondente, in ordine cronologico.
Cronologia delle installazioni di software	Questo widget fornisce informazioni dettagliate sulle installazioni software remote sui dispositivi gestiti dei clienti. Facendo clic su uno stato nella colonna **Stato installazione**, il sistema reindirizza alla pagina **Attività**, in cui vengono visualizzate le attività con lo stato corrispondente, in ordine cronologico.
Cronologia delle disinstallazioni di software	Questo widget fornisce informazioni dettagliate sullo stato delle disinstallazioni software remote dai dispositivi gestiti dei clienti. Facendo clic su uno stato nella colonna **Stato della disinstallazione**, il sistema reindirizza alla pagina **Attività**, in cui vengono visualizzate le attività con lo stato corrispondente, in ordine cronologico.

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.

Widget	Descrizione
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. **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: **Cloud storage totale utilizzato** - 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: **Cloud storage 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 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 allo stato predefinito**.
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. 161).

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 > Monitoraggio > 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 > Monitoraggio > 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 >	• L'indicatore data e ora del report esportato è indicato nel fuso

Operazioni (esportato in PDF o xslx)	orario del sistema utilizzato per esportare il report. • Il fuso orario delle attività visualizzate nel report è il fuso UTC.
Portale di gestione > Report > Operazioni (distribuzione pianificata)	• Il fuso orario della distribuzione del report è il fuso UTC. • 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 anti-malware dei file	Cronologici
Informazioni sulla scansione del backup (minacce)	Cronologici
Stato backup	Cronologici - nelle colonne **Totale esecuzioni** e **Numero di esecuzioni riuscite** Correnti - in tutte le altre colonne
Utilizzo dello storage 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 testate	Cronologici
Statistiche di Disaster Recovery	Cronologici
Dispositivi individuati	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 del workload	Correnti
Workload con backup eseguito	Cronologici
Stato di protezione dei workload	Correnti

Stima dei costi di Cyber Protect Cloud con il calcolatore

Se si sta utilizzando una versione di prova di Cyber Protect Cloud, è possibile stimare i costi previsti avvalendosi del calcolatore.

Nota
Ubicato nel portale di gestione, il calcolatore Cyber Protect Cloud è accessibile solo ai Partner in prova e non ai loro clienti o a Partner non in prova.

Per stimare i costi di Cyber Protect Cloud con il calcolatore

1. Nell'angolo in basso a sinistra del portale di gestione, fare clic su **Calcola costi mensili**.
2. Specificare i dettagli seguenti relativi al carico pianificato:
   - Numero di workload per tipo di workload. Indicare, ad esempio, il numero di virtual machine, workstation, server di hosting, utenze di Google Workplace, dispositivi mobili e utenze di Microsoft 365.
   - Dettagli sullo storage dei dati, ad esempio la posizione del data center e il volume dello storage.
3. [Facoltativo] Specificare le opzioni di backup avanzato, sicurezza o gestione che si prevede di utilizzare, e il numero di workload per ogni opzione.
4. Selezionare un modello di licensing: per workload o per gigabyte.

A destra viene visualizzato il costo mensile stimato.

La pagina del calcolatore offre anche diversi modi per diventare Partner: facendo clic sul pulsante corrispondente, avviando una chat con uno dei nostri esperti o chiedendo di essere direttamente contattati da un Consulente cloud.

Nell'angolo in basso a sinistra del portale di gestione è possibile comunicare con il reparto vendite facendo clic su **Contatta il reparto vendite**.

Copilot

Copilot è l'assistente di chat AI del prodotto. Copilot utilizza la documentazione ufficiale di Cyber Protect Cloud e la guida di licensing come origine e genera risposte che assistono e guidano l'utente nelle seguenti attività:

- Comprendere il funzionamento del prodotto.
- Comprendere gli argomenti di licensing.
- Comprendere come configurare i tenant.
- Comprendere come configurare i servizi.
- Iniziare a utilizzare il prodotto senza difficoltà.
- Ottenere risposte tempestive alle domande sull'utilizzo delle funzionalità.

Se Copilot non può rispondere alle domande poste, può trasferire la chat a uno specialista reale o inviare un ticket, se lo specialista non è attualmente disponibile.

È possibile avviare una chat con specialisti reali non solo in inglese, ma anche nella propria lingua madre. Copilot traduce automaticamente tutti i messaggi in lingue diverse dall'inglese, facilitando la comunicazione con specialisti in qualunque lingua.

È possibile rimuovere la finestra della chat e spostarla in qualsiasi altra posizione all'interno della finestra dell'applicazione, posizionando la chat nel punto più comodo per l'utente.

Lavorare con Copilot

Copilot può fornire informazioni sul prodotto e sui modelli di licensing e fornire assistenza nelle più comuni attività di configurazione. Se occorre assistenza più specializzata, Copilot può connettere l'utente a uno specialista reale. Se non sono disponibili specialisti, Copilot consente di creare un ticket tramite il quale lo specialista contatterà al più presto l'utente.

È possibile valutare la chat con Copilot e lasciare un feedback.

Avvia chat

Per avviare una chat con Copilot

1. Fare clic su **Copilot**.
2. Nella finestra della chat visualizzata, procedere come segue:
   - Per ottenere informazioni su uno degli argomenti o delle domande comuni predefiniti, fare clic sull'argomento o sulla domanda.
   - Per ottenere informazioni su un altro argomento o una risposta a un'altra domanda, digitare il testo nel campo del messaggio e premere Invio o fare clic sull'icona a freccia.
3. Ripetere il passaggio 2 fino a quando non si ottengono le informazioni richieste.
4. [Facoltativo] Per copiare la risposta di Copilot, fare clic sull'icona di copia sotto la risposta.
   Il testo viene copiato negli appunti del sistema.

Avviare una chat con uno specialista reale

Per avviare una chat con uno specialista reale

1. Fare clic su **Copilot**.
2. Aprire una chat nuova o esistente.
3. Chiedere a Copilot di avviare un collegamento con un specialista reale.
4. Chattare con uno specialista.

> **Nota**
> Se lo specialista chiude la chat, verrà visualizzato un modulo di feedback nella finestra della chat.

Valutare la risposta

È possibile valutare le risposte di Copilot nella chat.

Per valutare una risposta

1. Fare clic su **Copilot**.
2. Nella finestra della chat visualizzata, procedere come segue:
   - Per ottenere informazioni su uno degli argomenti o delle domande comuni predefiniti, fare clic sull'argomento o sulla domanda.
   - Per ottenere informazioni su un altro argomento o una risposta a un'altra domanda, digitare il testo nel campo del messaggio e premere Invio o fare clic sull'icona a freccia.
3. Per valutare la risposta di Copilot, eseguire una delle seguenti azioni:
   - Se la risposta è stata utile, fai clic sull'icona "Mi piace" sotto di essa.
   - Se la risposta non è stata utile, fare clic sull'icona "Non mi piace" sotto di essa.

Valutare la chat

È possibile valutare una chat contenente risposte di Copilot quando la si abbandona.

Per valutare la chat

1. Nella finestra di una chat attiva, fare clic sull'icona **X**.
   Viene visualizzato il modulo di feedback.
2. Valutare la propria esperienza con la chat da 1 (scarsa) a 5 (ottima).
3. Nella casella di testo, inserire il proprio feedback.

   Nota
   Questo passaggio è obbligatorio per i punteggi da 1 a 4, ma può essere saltato per il punteggio 5.

4. Fare clic su **Invia feedback**.
   La finestra della chat si chiude.

Uscire dalla chat

Quando si esce da una chat con Copilot, la cronologia della chat non viene eliminata. Verrà chiesto di valutare l'esperienza.

Per uscire da una chat

1. Nella finestra di una chat attiva, fare clic sull'icona **X**.
   Si apre la finestra di feedback. È possibile inviare un feedback o saltare questo passaggio.
2. [Facoltativo] Se si desidera inviare un feedback, fare clic su **Ignora**.
   La finestra della chat si chiude. Fino a quando la chat non sarà eliminata, sarà possibile accedervi dall'elenco delle chat. Se non è stato inviato un feedback, il modulo verrà visualizzato ogni volta che la chat viene chiusa.

Gestire le chat

È possibile visualizzare l'elenco delle sessioni di chat avute con Copilot ed eliminare quelle che non servono più.

Per visualizzare l'elenco delle chat e eliminarne una

1. Fare clic su **Copilot**.
2. Fare clic sull'icona a tre linee per visualizzare l'elenco delle chat.
3. Passare il mouse sul riquadro della chat da eliminare e fare clic sull'icona del cestino.

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
  Il pacchetto Advanced Backup include un numero di licenze e quote distinte per workstation, server, virtual machine, server di web hosting, utenze di Google Workspace e di Microsoft 365.
- Advanced Management (RMM)
- Advanced Security + XDR (Extended Detection and Response)
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share
- Formazione avanzata di sensibilizzazione alla sicurezza
  Offre formazione agli utenti sui rischi e sulle minacce associati alla sicurezza delle informazioni, addestrandoli con e-mail di phishing simulate e fornendo le conoscenze e le competenze necessarie per proteggere sé stessi e la propria organizzazione dagli attacchi informatici.

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 di protezione Advanced ma l'upselling è attivato, le funzionalità di protezione avanzate verranno visualizzate nel piano di protezione, ma non saranno

accessibili all'utente. Verrà 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, consulta la Guida al licencing 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
Security + XDR	• #CyberFit Score • Vulnerability assessment • 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.	Il pacchetto Advanced Security + XDR include Extended Detection and Response (XDR), Endpoint Detection and Response (EDR) e Managed Detection and Response (MDR): • Integrazione con soluzioni di terze parti, tra cui Advanced Email Security, applicazioni di collaborazione Microsoft 365 e Microsoft Entra ID • 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 sulle minacce • Archiviare gli eventi di sicurezza per 180 giorni • Managed Detection and Response (MDR)

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
		• Protezione anti-ransomware: Active Protection • Protezione antivirus e anti-malware 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, elenco degli elementi consentiti aziendale • Piani di protezione smart (integrazione con gli avvisi dei CPOC) • Scansione centralizzata del backup alla ricerca del malware • Cancellazione remota • Microsoft Defender Antivirus • Microsoft Security Essentials • Scansione del backup alla ricerca di malware delle caselle di posta Microsoft 365 Per informazioni su come abilitare Advanced Security + XDR, consultare "Abilitazione di Advanced Security + XDR" (pag. 179).
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

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
		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	Per gli endpoint: • Gestione gruppi • Gestione centralizzata dei piani di protezione • Inventario hardware • Controllo da remoto • Azioni remote • Connessioni simultanee per tecnico • Protocollo di connessione remota: RDP • Quattro monitor • Monitoraggio basato su soglia • Mostra l'ultimo utente connesso • Vulnerability assessment per sistemi Windows e macOS Per le utenze Microsoft 365: • Verifica del livello di sicurezza di Microsoft 365 con baseline basate su best practice, gestione e onboarding degli utenti	Il pacchetto Advanced Management (RMM) include le funzionalità seguenti: Per gli endpoint: • Gestione patch • Integrità del disco • Inventario software • Vulnerability assessment dei prodotti di terze parti per sistemi operativi Windows • Patch a prova di errore • 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, solo visualizzazione e tenda • Connessione tramite applicazione Quick Assist • Protocolli di connessione remota: NEAR e Condivisione schermo di Apple • Sessione di registrazione per connessioni NEAR • Trasmissione screenshot • Report della cronologia della sessione • 24 monitor • Monitoraggio basato su soglia • Monitoraggio basato sulle anomalie • Deployment software da remoto con

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
		DeployPilot • Vulnerability assessment per applicazioni Windows di terzi • Tracciamento della geolocalizzazione • Chat dell'helpdesk Per le utenze Microsoft 365: • Correzione automatica e manuale delle deviazioni dalla baseline e offboarding dell'utente
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.
Formazione di sensibilizzazione alla sicurezza		• Formazione di sensibilizzazione alla sicurezza • Formazione sulla conformità • Simulazione di phishing • Gestione dell'accettazione delle policy
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 calcolo al mese, e a un massimo di 5 failover di prova contemporanei.	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. • Numero di punti di ripristino disponibili per il failover: tutti i punti

Gruppo di funzionalità	Funzionalità Standard incluse	Caratteristiche avanzate
	• 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.	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 cloud storage • Backup su archivio locale **Nota** Si applicano tariffe per l'utilizzo del cloud storage.	• One-click Recovery • Protezione continua dei dati • Supporto per il backup di cluster Microsoft SQL Server e cluster di Microsoft Exchange - Gruppo di disponibilità Always On (AAG) e Gruppo di Disponibilità Database (DAG) • Supporto per il backup di database MariaDB, MySQL, Oracle DB e SAP HANA • Mappa della protezione dati e report di conformità • Elaborazione dei dati al di fuori dell'host • Frequenza di backup per workload

Gruppo di funzionalità	Funzionalità a consumo	Caratteristiche avanzate
		Microsoft 365 e Google Workspace • Operazioni remoto con un supporto di avvio • Backup diretto su Microsoft Azure, Amazon S3 e cloud storage pubblico Wasabi
File Sync & Share	• Archiviazione di contenuto crittografato basato su file • Sincronizzazione di file tra dispositivi designati • Condivisione di file e cartelle con persone e sistemi designati	• Autenticazione e firma elettronica • Modelli di documento* *Backup di file con sincronizzazione e condivisione
Consegna fisica dei dati	Funzionalità del servizio Consegna fisica dei dati	N/D
Notary	• 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. 9).

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 + XDR

Il pacchetto Advanced Security + XDR (Extended Detection and Response) fornisce una soluzione completa, nativamente integrata e altamente efficiente, progettata appositamente per gli MSP.

Con Advanced Security + XDR è possibile:

- Estendere la sicurezza degli ambienti dei clienti a tutte le superfici di attacco vulnerabili, con una visibilità estesa che copre endpoint, e-mail, Microsoft Entra ID e le applicazioni Microsoft 365 (SharePoint, OneDrive, Teams), garantendo protezione contro le minacce più recenti e complesse.
- Integrazione nativa tra Cyber Security, protezione dati e gestione degli endpoint. XDR è progettato per proteggere le superfici di attacco vulnerabili garantendo una continuità operativa senza confronti.
- Efficienza migliorata delle capacità di avvio, gestione, scalabilità ed erogazione di servizi di sicurezza. XDR, inoltre, include l'analisi degli incidenti basata su AI e una funzione di risposta con un solo clic per semplificare le indagini, un unico agente e un'unica console per tutti i servizi e una piattaforma personalizzabile per integrare strumenti aggiuntivi nello stack tecnologico.

Il pacchetto Advanced Security + XDR è composto da Extended Detection and Response (XDR), Endpoint Detection and Response (EDR) e "Managed Detection and Response (MDR)" (pag. 188), e protegge in modo continuativo i workload da tutte le minacce malware.

Abilitazione di Advanced Security + XDR

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

Nota
È inoltre necessario abilitare Endpoint Detection and Response (EDR) nel piano di protezione per tutti i workload da proteggere. Per ulteriori informazioni, consultare Abilitazione di EDR.

Per abilitare il pacchetto Advanced Security + XDR

1. Accedere al portale di gestione.

   Nota
   Se richiesto, selezionare i clienti ai quali applicare il pacchetto di protezione Advanced Security + XDR, 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 + XDR.
   Nella sezione **Protezione** della scheda **Configura**, verificare che la casella di controllo **Advanced Security + XDR** sia selezionata.

Integrazione di Advanced Security + XDR con piattaforme di terze parti

Advanced Security + XDR supporta le integrazioni seguenti:

- Perception Point
- Microsoft Entra ID
- Servizi Microsoft 365

Per accedere alle integrazioni dell'utente, nel portale di gestione passare a **Integrazioni**.

Nota
Questa funzionalità è disponibile solo agli utenti ai quali è assegnato il ruolo di Amministratore.

Integrazione con Perception Point

In questo argomento viene illustrato come integrare Perception Point con Advanced Security + XDR.

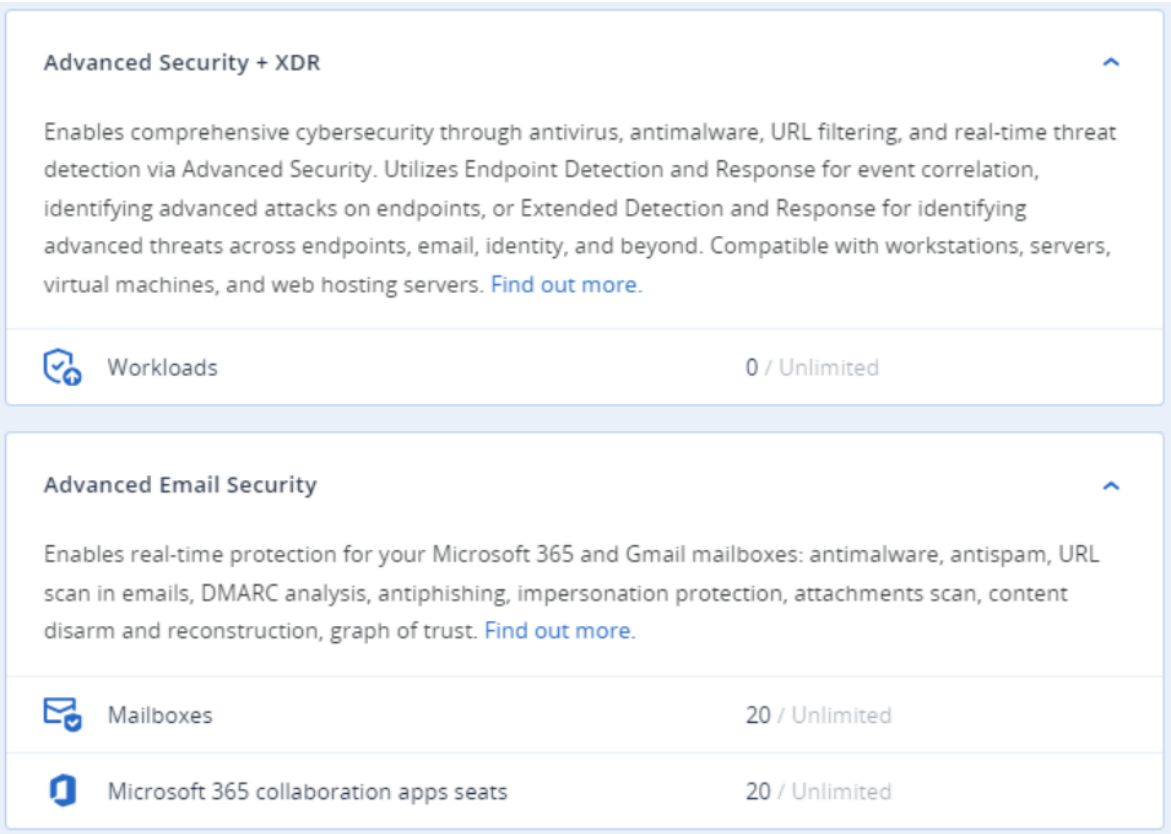
Questa integrazione consente di offrire una soluzione XDR (Extended Detection and Response) ai clienti che utilizzano Microsoft 365 per la sicurezza delle e-mail e le app di collaborazione. L'integrazione XDR arricchisce le funzionalità della soluzione EDR (Endpoint Detection and Response) esistente con Perception Point.

Per integrare Perception Point con Advanced Security + XDR, è necessario seguire tre passaggi:

1. Abilitare i pacchetti di protezione avanzata richiesti.
2. In Perception Point, configurare i canali di sicurezza delle e-mail e/o delle app di collaborazione ed estrarre una chiave API.
3. Abilitare l'integrazione Perception Point XDR per i clienti.

Per abilitare i pacchetti di protezione avanzata richiesti

1. Nel portale di gestione, accedere al cliente per il quale attivare l'integrazione.
2. Abilitare il pacchetto Advanced Security + XDR e il pacchetto Advanced Email Security. Per ulteriori informazioni, consultare "Pacchetti Advanced Protection" (pag. 172).

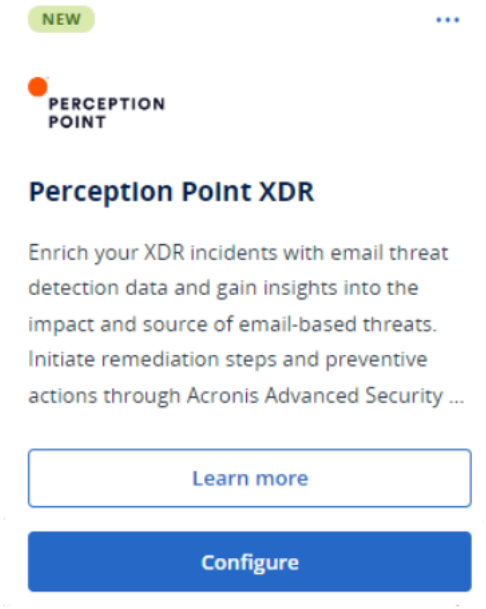


Per configurare i canali di sicurezza delle e-mail e/o delle app di collaborazione ed estrarre una chiave API in Perception Point

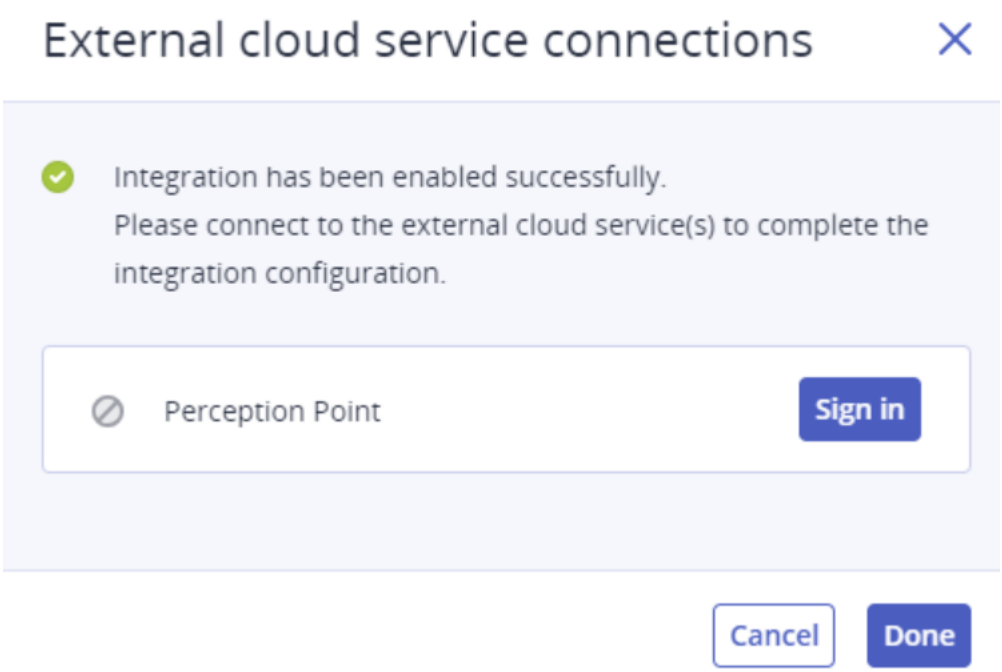
1. Nel portale di gestione, accedere al cliente per il quale attivare l'integrazione, quindi fare clic su **Gestisci servizio** per aprire la console di Cyber Protect.
2. Passare a **Sicurezza e-mail**, quindi fare clic su **Passare alla console della sicurezza e-mail** per aprire Perception Point.
3. Creare i canali di sicurezza delle e-mail e/o delle app di collaborazione pertinenti in Perception Point. Per ulteriori informazioni, consultare la documentazione di Perception Point.
4. Nel menu di navigazione a sinistra, fare clic su **Profilo**.
5. Nella sezione **Sicurezza**, fare clic sull'icona per la copia accanto alla chiave API. Questa chiave viene utilizzata per abilitare l'integrazione XDR, come descritto nella procedura seguente.

Per abilitare l'integrazione di Perception Point XDR per i clienti

1. Nel portale di gestione, passare a **Integrazioni**.
2. Individuare l'integrazione di **Perception Point XDR** e, nella scheda visualizzata, fare clic su **Configura**.



3. Fare clic sulla scheda **Gestione clienti**, selezionare il cliente per il quale abilitare l'integrazione XDR e fare clic su **Abilita**.
4. Nella finestra di dialogo visualizzata, fare clic su **Accedi**.



5. Immettere la chiave API di Perception Point copiata nella procedura precedente e fare clic su **Fine**.

6. Per verificare che l'integrazione sia attiva e funzionante, controllare che nella colonna **Stato di abilitazione** sia visualizzato **Abilitato** e che nella colonna **Connessioni del servizio** sia visualizzato **1 di 1** (una connessione è in esecuzione).

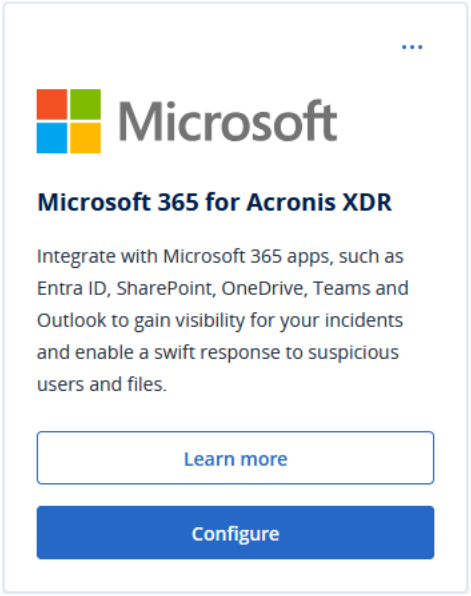
Integrazione con i servizi Microsoft 365

Questo argomento illustra come integrare i servizi di Microsoft 365 con Advanced Security + XDR.

Questa integrazione fornisce metadati arricchiti per gli incidenti di Endpoint Detection and Response (EDR) e di Extended Detection and Response (XDR) ai clienti finali che utilizzano Microsoft 365 per le applicazioni di collaborazione. L'integrazione fornisce anche dettagli sull'utente autenticato interessato dal problema. È anche possibile eseguire azioni di risposta, come bloccare o limitare l'accesso per l'account utente.

Per eseguire l'integrazione con i servizi Microsoft 365

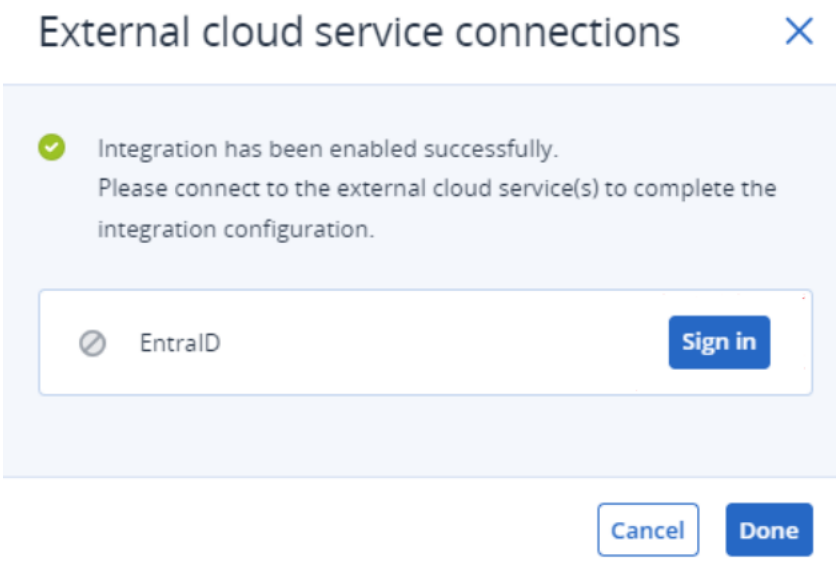
1. Aprire il portale Microsoft Azure e accedere come tenant cliente.
2. Seguire le istruzioni visualizzate per creare una nuova applicazione e assegnare a questa i ruoli necessari. Per ulteriori informazioni sulla configurazione dell'accesso API a Microsoft 365, consultare questo articolo della Knowledge Base.
3. Nel portale di gestione, verificare che per il tenant del cliente pertinente sia abilitata l'opzione **Workpack** nel pacchetto Advanced Security + XDR.
4. Passare a **Integrazioni** e individuare l'integrazione **Microsoft 365 XDR**.
5. Nella scheda del catalogo **Microsoft 365 per XDR**, fare clic su **Configura**, quindi su **Abilita**.



6. Fare clic sulla scheda **Gestione clienti**, selezionare i tenant del cliente per i quali abilitare l'integrazione e fare clic su **Abilita**.
7. Definire quanto segue:
   - **Dominio personalizzato**: se il cliente utilizza un dominio personalizzato in Microsoft 365, immetterlo qui. Se non è in uso alcun dominio personalizzato, lasciare vuoto il campo.

- **Regione**: selezionare la regione pertinente per i tenant di Microsoft 365 dall'elenco a discesa.

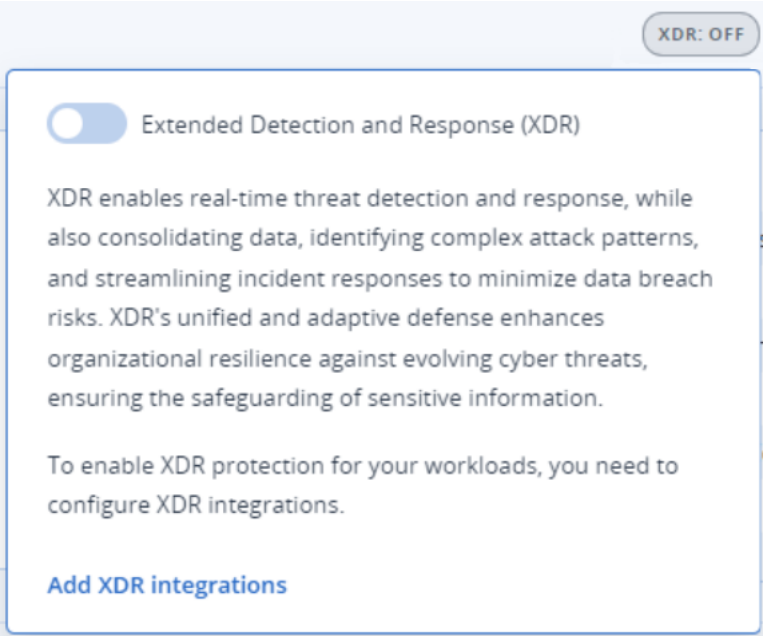
8. Fare clic su **Abilita**. Nella finestra di dialogo visualizzata, fare clic su **Accedi**.



9. Immettere i dati seguenti:
   - **ID**: l'ID oggetto dell'applicazione creata nel passaggio 2.

     Nota
     In Microsoft 365, assicurarsi di copiare l'ID oggetto dalla pagina **Registrazioni dell'app** > **Panoramica** facendo clic sul collegamento al nome dell'app nel campo **Applicazione gestita nella directory locale** e selezionando l'ID oggetto nella pagina visualizzata. Non copiare l'ID oggetto visualizzato nella pagina principale **Registrazioni dell'app** > **Panoramica**.

   - **Segreto**: il segreto del client API creato per l'applicazione.
   - **ID tenant**: il tenant Microsoft 365.
10. Fare clic su **Accedi**, quindi su **Fine**.
    Per verificare il funzionamento della connessione, controllare che nella colonna **Connessioni del servizio** sia visualizzato **1 di 1** (una connessione è in esecuzione).
11. Passare a **Clienti**, selezionare il cliente per cui abilitare XDR e fare clic su **Gestisci servizio**.
    Viene visualizzata la console di Cyber Protect.
12. Passare a **Protezione**, quindi fare clic su **XDR: Disattivato**.
13. Nella finestra popup visualizzata, fare clic sull'interruttore per abilitare XDR.



I problemi che interessano un workload registrato in Microsoft 365 includono ora informazioni XDR e azioni di risposta dettagliate per questo utente.

Integrazione con Fortinet

In questo argomento viene illustrato come integrare Fortinet con Advanced Security + XDR.

Questa integrazione fornisce metadati arricchiti per gli incidenti rilevati da Endpoint Detection and Response (EDR) e da Extended Detection and Response (XDR), mediante l'inserimento e la correlazione di eventi dai software e dalle appliance di sicurezza Fortinet.

Importante
Per consentire il corretto funzionamento dell'integrazione, i clienti devono disporre di una licenza FortiGate Cloud Service per la rete di riferimento.

Per integrare Fortinet con Advanced Security + XDR, è necessario completare tre passaggi:

- Abilitare il pacchetto Advanced Security + XDR.
- Configurare Fortinet affinché funzioni con Acronis.
- Abilitare l'integrazione nel portale di gestione.

Per abilitare il pacchetto Advanced Security + XDR

1. Nel portale di gestione, accedere al cliente per il quale attivare l'integrazione.
2. Assicurarsi che il pacchetto Advanced Security + XDR sia abilitato. Per ulteriori informazioni, consultare "Pacchetti Advanced Protection" (pag. 172).

Per configurare Fortinet affinché funzioni con Acronis

1. Accedere al proprio account FortiGate o FortiGate Cloud Service.
2. Per azioni di risposta per bloccare un URL o un indirizzo IP:
   - Passare a **Security Profiles** > **Web Filter** e definire un filtro con il nome **Acronis Web Filter**. Nella sezione **Static URL Filter**, fare clic sull'opzione **URL Filter** per abilitarla.
   - Passare a **Policy & Objects** > **Firewall Policy** e verificare che **Acronis Web Filter** sia aggiunto alla policy pertinente (nella sezione **Security Profiles**).

   Quando l'azione di risposta viene avviata, la reputazione viene ricevuta da Fortinet, anche se non sono stati definiti né il filtro web né la policy del firewall. L'aggiunta del filtro web consente di bloccare l'URL o l'indirizzo IP.

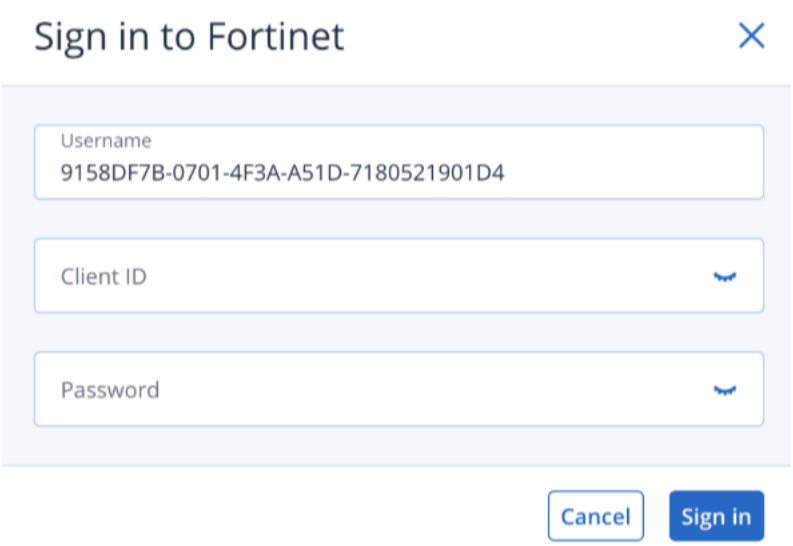
   Nota
   Se l'opzione **Acronis Web Filter** non viene definita o individuata, l'azione di risposta di blocco non viene visualizzata nel grafico XDR.

3. Per isolare un endpoint:
   - Passare a **Policy & Objects** > **Firewall Policy** e definire due policy per bloccare e accettare le connessioni in entrata (per i domini Acronis e gli indirizzi IP).
   - Passare a **Policy & Objects** > **Addresses** e, nella scheda **Address Groups**, definire quanto segue:
     - Il gruppo **Acronis Isolated Group**, in cui vengono archiviati automaticamente gli indirizzi bloccati. **Acronis Isolated Group** è un tipo di **Group** e deve essere collegato alla policy di blocco.
     - Il gruppo **Acronis Allowed Hosts**, in cui vengono archiviati gli indirizzi e i domini consentiti. **Acronis Allowed Hosts** è un tipo di **Group** e deve essere collegato alla policy che accetta le connessioni in uscita. Ad esempio **Acronis Isolated Group** deve essere aggiunto al campo **Source** nella policy, e il gruppo **Acronis Allowed Hosts** deve essere aggiunto al campo **Destination**.

       Nota
       Gli indirizzi e le porte del data center Acronis necessari per il funzionamento dell'agente Acronis sono elencati qui.

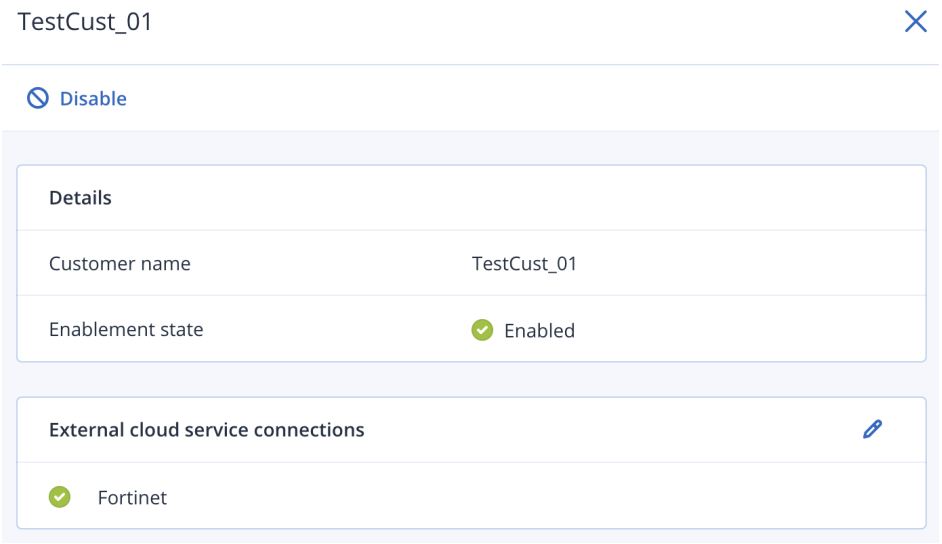
Per abilitare l'integrazione di Fortinet XDR per i clienti

1. Nel portale di gestione, passare a **Integrazioni**.
2. Individuare l'integrazione **Fortinet XDR** e, nella scheda visualizzata, fare clic su **Configura**.
3. Fare clic sulla scheda **Gestione cliente**, selezionare il cliente per il quale abilitare l'integrazione XDR e fare clic su **Abilita**.
4. Nella finestra di dialogo, immettere il nome utente, l'ID cliente e la password Fortinet corrispondenti.



Nota
Le credenziali Fortinet vengono generate quando si crea l'utente API IAM e si impostano le autorizzazioni di amministratore per FortiGate Cloud. Per ulteriori informazioni, consultare la documentazione di FortiGate Cloud. In alternativa, se si è clienti Fortinet e si ha accesso alle pagine della rete degli sviluppatori, consultare questa documentazione.

5. Fare clic su **Accedi**.
6. Per garantire che l'integrazione funzioni correttamente, fare clic sulla riga del cliente corrispondente e verificare che nel campo **Stato abilitazione** sia visualizzato **Abilitato**.



7. [Facoltativo] Per aggiornare il nome utente, l'ID cliente e la password di Fortinet, fare clic sull'icona a matita nella sezione **Connessioni a servizi cloud esterni**.

Per disabilitare l'integrazione Fortinet XDR

1. Nel portale di gestione, passare a **Integrazioni**.
2. Individuare l'integrazione **Fortinet XDR** e, nella scheda visualizzata, fare clic su **Configura**.
3. Fare clic sulla scheda **Gestione cliente**, selezionare il cliente per il quale abilitare l'integrazione XDR e fare clic su **Disabilita**.

Managed Detection and Response (MDR)

MDR offre un servizio 24 ore su 24, 7 giorni su 7, agli MSP che non hanno risorse interne esperte in sicurezza, o che necessitano di assistenza aggiuntiva per indagare e rispondere ai problemi di sicurezza rilevati da Endpoint Detection and Response (EDR) e da Extended Detection and Response (XDR).

La funzionalità MDR viene abilitata nel portale di gestione con il pacchetto Advanced Security + XDR; il servizio MDR è fornito da un fornitore esterno di servizi MDR. Se la funzionalità MDR viene abilitata per un cliente specifico, il fornitore di servizi MDR riceve da Acronis i dati relativi ai problemi per i workload sui quali EDR o XDR è abilitato nei piani di protezione appartenenti allo specifico cliente. Il fornitore MDR applica quindi diversi livelli di servizio per gestire i problemi utilizzando le azioni di risposta disponibili. Per ulteriori informazioni, consultare "Cos'è Managed Detection and Response (MDR)" (pag. 188).

Per ulteriori informazioni sul funzionamento di XDR, consultare Extended Detection and Response (XDR).

Per ulteriori informazioni sul funzionamento di EDR, consultare Endpoint Detection and Response (EDR).

Cos'è Managed Detection and Response (MDR)

MDR è un servizio fornito da fornitori terzi che utilizza una combinazione di analisti esperti, strumenti integrati, intelligence sulle minacce e tecnologie sia del fornitore che di Acronis per monitorare e rispondere alle potenziali minacce e violazioni della sicurezza.

Quando MDR è abilitato per i clienti nel portale di gestione, Acronis inoltra la telemetria dei problemi rilevati al fornitore MDR, che conduce indagini e avvia le azioni di risposta appropriate ai problemi. Solo i problemi non mitigati automaticamente vengono inoltrati al fornitore MDR.

Componenti chiave di MDR

MDR è composto da tre componenti principali:

- Monitoraggio
- Isolamento
- Risposta e correzione

Monitoraggio

I fornitori di servizi MDR monitorano gli avvisi e le notifiche di sicurezza rilevati sugli endpoint del cliente. Il fornitore associa gli avvisi e assegna le priorità in base alle minacce comuni, all'intelligence sulle minacce e all'intelligence sulle minacce di terze parti, avvalendosi di funzionalità di analisi, orchestrazione della sicurezza e azioni di risposta. Il fornitore determina quindi se gli avvisi o le notifiche rappresentano una violazione o una compromissione.

Qualsiasi evento di sicurezza ritenuto dal fornitore MDR una potenziale minaccia alla sicurezza viene elevato a problema di sicurezza sul lato cliente, e reso disponibile nella console di Cyber Protect. Il fornitore offre più contesto relativamente alla gravità della minaccia e alla soluzione di correzione raccomandata, inclusa qualsiasi azione già intrapresa.

Isolamento

Gli analisti dei fornitori MDR utilizzano playbook predefiniti per avviare le azioni di risposta per l'isolamento degli endpoint. Qualsiasi azione di risposta da parte del fornitore MDR si riflette nel problema di sicurezza pertinente. La decisione di isolare un endpoint viene raggiunta attingendo ai dati dall'endpoint, con ulteriori input dall'intelligence sulle minacce e dalla ricerca sulle minacce.

Risposta e correzione

Le attività di risposta e correzione vengono eseguite dopo il completamento delle attività iniziali di monitoraggio e isolamento. Al rilevamento di un problema di sicurezza, il fornitore di MDR avvia le azioni di risposta in base al problema di sicurezza. Le attività di risposta e correzione includono:

- Istruzioni su come mitigare, arrestare o prevenire un problema di sicurezza in base ai dati, alle informazioni e agli avvisi forniti.
- Analisi e indagini sugli eventi di sicurezza, finalizzate a determinare la causa principale e l'entità della compromissione.
- Esecuzione di flussi di lavoro approvati (come definito nei playbook di risposta del fornitore MDR) per isolare i workload, mettere in quarantena le minacce o risolvere completamente la minaccia.
- Invio al fornitore del servizio dell'escalation di sicurezza dettagliata, citando il problema di sicurezza sul lato cliente, l'intelligence sulle minacce e gli avvisi pertinenti.
- Escalation dei problemi attraverso vari canali, tra cui la creazione di un problema di sicurezza, l'invio di notifiche via e-mail e telefono, il tutto tramite i dettagli di contatto forniti dal cliente.
- Gestione delle comunicazioni con il cliente fino alla risoluzione della minaccia, offrendo aggiornamenti tempestivi non appena emergono nuove informazioni.
- Se le azioni di risposta non rientrano nell'ambito del servizio MDR, il fornitore MDR fornisce raccomandazioni sulle aree su cui concentrarsi, ad esempio consigliando servizi aggiuntivi, come l'incident response.

Abilitazione di Managed Detection and Response (MDR)

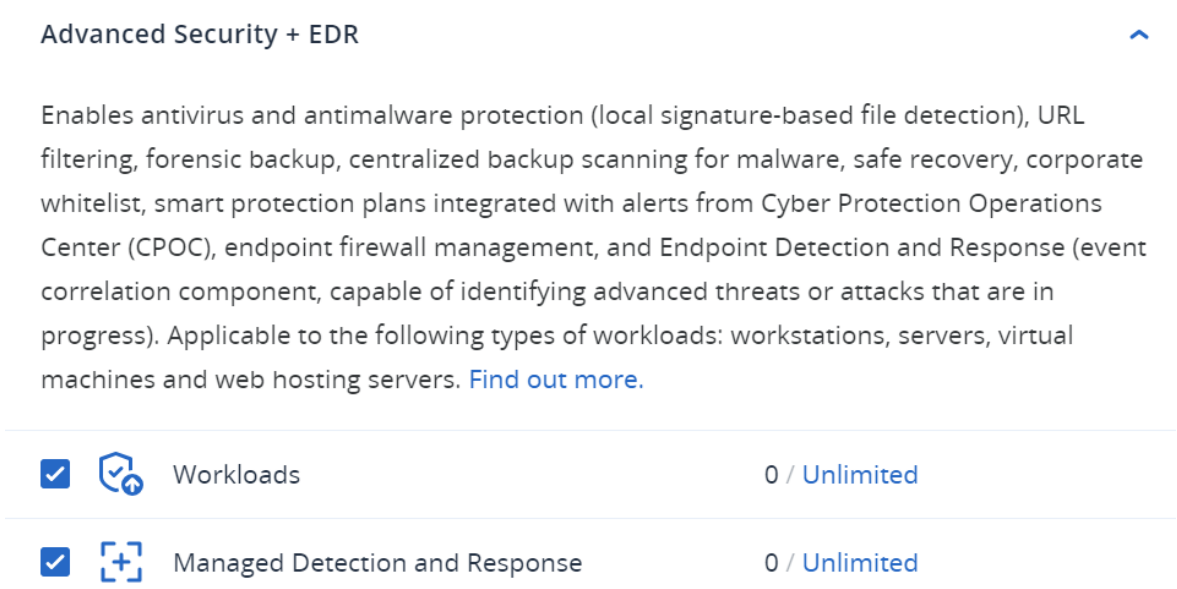
Per abilitare MDR per i clienti desiderati procedere con i due passaggi seguenti:

- Passaggio 1: abilitare l'elemento in offerta MDR per i clienti.
- Passaggio 2: configurare l'integrazione con l'app del fornitore MDR.

Nota
I clienti autogestiti non possono abilitare MDR. Per ulteriori informazioni sulla configurazione dei clienti autogestiti, consultare "Configurazione del profilo cliente autogestito" (pag. 53).

Per abilitare MDR per clienti selezionati

1. Nel portale di gestione, passare a **Clienti**.
2. Fare clic sull'icona dei puntini di sospensione accanto al cliente pertinente, quindi selezionare **Configura**.
3. Nella scheda **Protezione**, fare clic su **Modifica**.
4. Nella sezione **Advanced Security + EDR**, verificare che le caselle di controllo **Workload** e **Managed Detection and Response** siano selezionate. Quindi fare clic su **Salva** per applicare le eventuali modifiche.

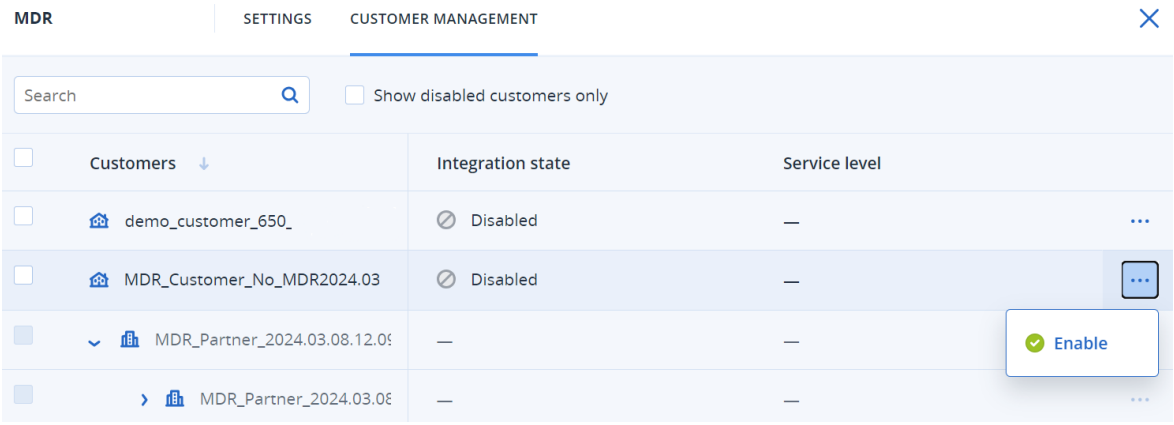


Per configurare l'integrazione con l'app del fornitore MDR

1. Nel portale di gestione, passare a **Integrazioni**.
2. Utilizzare la barra di ricerca per individuare l'app del fornitore MDR.
3. Nella scheda del catalogo MDR visualizzata, fare clic su **Configura**.
4. Nella scheda **Impostazioni**, fare clic sull'icona a matita e inserire i dettagli di contatto di almeno un contatto del Partner. È il contatto utilizzato dal fornitore MDR quando viene rilevato un evento di sicurezza. È possibile aggiungere i dettagli di un massimo di tre contatti. Al termine, fare clic su **Abilita**.
   Quando viene rilevato un evento inerente la sicurezza, il fornitore chiama ciascun contatto sei volte prima di passare al contatto successivo. Dopo una chiamata, o nel caso in cui non si riesca

a stabilire un contatto, il fornitore invia un'email a tutti i contatti, fornendo una panoramica dell'escalation e del problema.

5. Nella scheda **Gestione clienti**, fare clic sull'icona dei puntini di sospensione, nella colonna più a destra del cliente pertinente, quindi selezionare **Abilita**.



Per abilitare più clienti, selezionare la casella di controllo accanto ai clienti interessati, quindi fare clic su **Abilita** nella scheda **Gestione clienti**, in alto a sinistra.

6. Nell'elenco a discesa **Livello di servizio** nella finestra di dialogo visualizzata, selezionare il livello di servizio MDR da applicare ai clienti selezionati.
   - **Standard**: questo livello include il monitoraggio 24 ore su 24, 7 giorni su 7, degli endpoint del cliente per intercettare gli attacchi; il triage degli eventi e la prioritizzazione potenziati da intelligenza artificiale; il contenimento delle minacce e l'isolamento degli endpoint interessati; la visibilità in tempo reale nella console su un elenco di problemi con priorità.
   - **Advanced**: oltre alle funzionalità incluse nel livello **Standard**, questo livello abilita la correzione completa dell'incidente, inclusi il rollback dell'attacco, il ripristino e la riparazione delle falle di sicurezza.
7. Fare clic su **Abilita** per completare l'integrazione MDR.

   Se è stata abilitata la funzionalità Indirizzi IP consentiti (consultare "Limitazione dell'accesso all'interfaccia Web" (pag. 36)), il sistema chiede di aggiungere gli IP del fornitore MDR all'elenco di IP consentiti. In questo modo, il fornitore può monitorare i workload pertinenti. Fare clic su **Abilita** per confermare.

   Il modulo MDR è ora abilitato; i problemi di sicurezza vengono inoltrati al fornitore MDR, che eseguirà le attività di risposta e indagine. Per ulteriori informazioni sul servizio MDR, consultare "Cos'è Managed Detection and Response (MDR)" (pag. 188).

Disabilitazione di Managed Detection and Response (MDR)

È possibile disabilitare MDR a livello dell'elemento in offerta. È inoltre possibile disabilitare MDR per i singoli clienti nell'app di integrazione del fornitore MDR.

Per disabilitare l'elemento in offerta MDR

1. Nel portale di gestione, passare a **Clienti**.
2. Fare clic sull'icona dei puntini di sospensione accanto al cliente pertinente, quindi selezionare **Configura**.
3. Nella scheda **Protezione**, fare clic su **Modifica**.
4. Nella sezione **Advanced Security + EDR**, verificare che le caselle di controllo **Workload** e **Managed Detection and Response** non siano selezionate. Quindi fare clic su **Salva** per applicare le modifiche.
   In alternativa, è possibile disabilitare il servizio **Advanced Security + EDR** nella scheda **Configura**. Questa azione disabilita automaticamente MDR.

Per disabilitare MDR per i singoli clienti nell'app di integrazione del fornitore di MDR

1. Nel portale di gestione, passare a **Integrazioni**.
2. Individuare l'app del fornitore MDR pertinente.
3. Nella scheda del catalogo MDR visualizzata, fare clic su **Configura**.
4. Nella scheda **Gestione clienti**, fare clic sull'icona dei puntini di sospensione, nella colonna più a destra del cliente pertinente e selezionare **Disabilita**.
   Per disabilitare più clienti, selezionare la casella di controllo a sinistra di ogni cliente, quindi fare clic su **Disabilita** nella scheda **Gestione clienti**, in alto a sinistra.

Azioni di risposta disponibili in Managed Detection and Response (MDR)

MDR prevede una serie di azioni di risposta applicabili a livello di problema.

Le azioni di risposta vengono eseguite dagli analisti della sicurezza MDR, che applicano le azioni pertinenti accedendo alla console di Cyber Protect o eseguendo chiamate API. Questi analisti accedono alla console di Cyber Protect con il ruolo **Analista della sicurezza**.

Tutte le azioni di risposta vengono registrate nell'elenco **Attività**. I clienti possono visualizzare nell'elenco le attività eseguite come azioni di risposta e il relativo stato (In corso/Non riuscito/Riuscito). La colonna **Avviato da** visualizza l'utente che ha avviato l'azione, che sia un utente Partner, un utente Cliente o l'analista della sicurezza MDR.

Nota
Le azioni di risposta elencate nella tabella seguente includono anche il riferimento alle relative sezioni nella documentazione di Endpoint Detection and Response (EDR).

Azione di risposta	Informazioni aggiuntive
Modifica stato indagine	Lo stato può essere impostato su uno dei seguenti: • **Indagine in corso** • **Chiuso** • **Falso positivo**

Azione di risposta	Informazioni aggiuntive
	Per ulteriori informazioni su come modificare lo stato dell'indagine, consultare Come indagare sui problemi rilevati nella sequenza di attacco.
Isolamento della rete	Gli analisti della sicurezza MDR possono: • Isolare il workload • Annullare l'isolamento del workload • Controllare lo stato di isolamento Per ulteriori informazioni sull'isolamento del workload, consultare Gestire l'isolamento della rete di un workload.
Aggiunta di commenti	Gli analisti della sicurezza MDR possono aggiungere commenti al problema facendo clic su **Pubblica commento** nella sequenza della catena di attacco del problema. I commenti inseriti vengono visualizzati nella scheda **Attività** dell'incidente specifico. Per ulteriori informazioni, consultare Comprendere le azioni intraprese per mitigare un problema.
Arresta processo/struttura processo	Questa azione può essere applicata all'intero problema. L'azione di risposta può essere attivata anche se i processi del problema sono già stati arrestati. Dopo che l'azione di risposta è stata elaborata, viene inviata una risposta asincrona. Tale risposta può essere una delle seguenti: • Esito positivo: tutti i processi sono stati arrestati correttamente. • Esito positivo con avvisi: alcuni processi sono stati arrestati correttamente o non ci sono processi da arrestare (o sono stati arrestati al di fuori di MDR). • Errore: nessun processo è stato arrestato. Per ulteriori informazioni su come arrestare un processo o una struttura del processo, consultare Definire le azioni di risposta per un processo sospetto.
Quarantena	Questa azione può essere applicata all'intero

Azione di risposta	Informazioni aggiuntive
	incidente. L'azione di risposta può essere attivata anche se i file o i processi sono già stati messi in quarantena. Dopo che l'azione di risposta è stata elaborata, viene inviata una risposta asincrona. Tale risposta può essere una delle seguenti: • Esito positivo: tutti i file e i processi sono stati messi in quarantena correttamente. • Esito positivo con avvisi: alcuni file e processi sono stati mesi in quarantena correttamente o non ci sono file o processi da mettere in quarantena (o sono stati messi in quarantena al di fuori di MDR). • Errore: nessun file o processo è stato messo in quarantena. Per ulteriori informazioni su come mettere in quarantena un processo, consultare Definire le azioni di risposta per un processo sospetto. Per ulteriori informazioni sulla messa in quarantena dei file, consultare Definire le azioni di risposta per un file sospetto.
Elimina file	Questa azione può essere applicata all'intero problema. L'azione di risposta può essere attivata anche se i file sono già stati eliminati. Dopo che l'azione di risposta è stata elaborata, viene inviata una risposta asincrona. Tale risposta può essere una delle seguenti: • Esito positivo: tutti i file sono stati eliminati correttamente. • Esito positivo con avvisi: alcuni file sono stati eliminati correttamente o non ci sono file da eliminare (o sono stati eliminati al di fuori di MDR). • Errore: nessun file è stato eliminato. Per ulteriori informazioni sull'eliminazione dei file, consultare Definire le azioni di

Azione di risposta	Informazioni aggiuntive
	risposta per un file sospetto.
Riavvia workload	Consente di impostare l'intervallo di tempo che deve trascorre prima del riavvio del workload o di riavviarlo immediatamente. Per ulteriori informazioni sul riavvio dei workload, consultare Riavviare un workload.
Aggiunta di URL, file o processo all'elenco degli elementi consentiti/bloccati	Aggiunge gli URL, i file o i processi all'elenco degli elementi consentiti/bloccati nel piano predefinito (il piano attualmente assegnato al workload). Dopo che l'azione di risposta è stata elaborata, viene inviata una risposta asincrona. Tale risposta può essere una delle seguenti: • Esito positivo: tutti gli URL, i file e i processi sono stati aggiunti correttamente. • Esito positivo con avvisi: alcuni URL, file e processi sono stati aggiunti correttamente e altri no (ad esempio, erano già inclusi nell'elenco degli elementi consentiti). • Errore: l'azione non è riuscita. Per ulteriori informazioni sull'aggiunta di URL, file o processi all'elenco degli elementi consentiti e bloccati, consultare Aggiungere un processo, file o rete all'elenco degli elementi consentiti o bloccati del piano di protezione.

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
- Rimozione self-service dello spam in quarantena da parte del proprietario della casella di posta

È inoltre possibile abilitare le utenze per le app di collaborazione di Microsoft 365, per proteggere le applicazioni di collaborazione nel cloud di Microsoft 365 dalle minacce alla sicurezza perpetrate tramite contenuti. Queste applicazioni includono, tra le altre, OneDrive, SharePoint e Teams.

È possibile abilitare Advanced Email Security per workload o per gigabyte; la scelta incide sul modello di licensing.

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

Per le istruzioni sulla configurazione, consultare la documentazione di Advanced Email Security.

Advanced Backup

È possibile abilitare il pacchetto Advanced Backup e proteggere i workload utilizzando le funzionalità di backup avanzato e disaster recovery.

Sono disponibili le seguenti funzionalità:

- One-click Recovery
- Protezione continua dei dati
- Supporto per il backup di cluster Microsoft SQL Server e cluster di Microsoft Exchange - Gruppo di disponibilità Always On (AAG) e Gruppo di Disponibilità Database (DAG)
- Supporto per il backup di database MariaDB, MySQL, Oracle DB e SAP HANA
- Mappa della protezione dati e report di conformità
- Elaborazione dei dati al di fuori dell'host
- Frequenza di backup per workload Microsoft 365 e Google Workspace
- Operazioni remoto con un supporto di avvio
- Backup diretto su Microsoft Azure, Amazon S3 e cloud storage pubblico Wasabi

Formazione avanzata di sensibilizzazione alla sicurezza

I Partner possono abilitare il servizio Formazione avanzata di sensibilizzazione alla sicurezza per i tenant dei clienti in modo che gli utenti dell'organizzazione possano accedere ai materiali di formazione di sensibilizzazione alla sicurezza dalla console di Protezione.

L'accesso diretto alla formazione di sensibilizzazione alla sicurezza dalla console cloud di Cyber Protection promuove la diffusione e l'adozione presso un maggior numero di utenti, aiutando i clienti a soddisfare i requisiti relativi a conformità (PCI, HIPPA, FedRamd, Soc 2), gestione del rischio dei fornitori, assicurazione informatica e altro. Inoltre, la formazione aiuta i clienti a migliorare la propria sicurezza informatica riducendo il rischio di errori umani.

Il servizio è fornito da un sistema di gestione degli apprendimenti indipendente, Wizer, che supporta le seguenti funzionalità:

- Multitenancy: nel pannello di amministrazione Wizer, un amministratore del Partner può visualizzare tutti i clienti e gli utenti diretti che si sono registrati per la Formazione di sensibilizzazione alla sicurezza. La piattaforma non supporta la visualizzazione a più livelli, ovvero i Partner non possono visualizzare i Partner figlio e i tenant figlio. Gli amministratori del cliente possono visualizzare solo gli utenti della propria organizzazione.
- Provisioning automatico di tenant e utenti amministratore: quando il servizio viene abilitato per la prima volta nella console di Cyber Protect Cloud, l'integrazione crea automaticamente un nuovo tenant in Wizer per l'amministratore che ha abilitato l'integrazione. L'amministratore accede quindi al Pannello di amministrazione di Wizer per aggiungere gli utenti manualmente o configurare l'accesso SSO. Consultare Come aggiungere utenti.
- Contenuti coinvolgenti che rendono la formazione divertente
- Facilità d'uso
- Abbonamento mensile

Per ulteriori informazioni su Wizer, visitare il sito https://www.wizer-training.com/.

Abilitazione del servizio Formazione avanzata di sensibilizzazione alla sicurezza

La Formazione di sensibilizzazione alla sicurezza è erogata da un fornitore di terze parti, Wizer, come integrazione nella console Cyber Protect Cloud. I Partner devono abilitare l'integrazione per il proprio tenant prima di poter abilitare il servizio per i propri clienti.

L'abilitazione del servizio consiste nei seguenti passaggi.

1. Nella console di gestione Cloud, un amministratore del Partner abilita il servizio Formazione di sensibilizzazione alla sicurezza per un cliente (una volta per ciascun cliente).
2. Nella console di Cyber Protect Cloud, un amministratore abilita l'integrazione con Wizer nella propria organizzazione (una volta per organizzazione).
3. L'utente amministratore accede alla console di amministrazione di Wizer per aggiungere utenti alla piattaforma di formazione.

Nota
Il servizio non è accessibile agli amministratori di unità e di cartelle.

Per abilitare il servizio Formazione avanzata di sensibilizzazione alla sicurezza per un tenant cliente

Ruolo richiesto: amministratore del Partner

1. Nella console di gestione Cloud, fare clic su **Clienti** e individuare il cliente per cui abilitare il servizio.
2. Nel menu contestuale, fare clic su **Configura**.
3. Nell'elenco dei servizi, in **Per workload**, selezionare la casella di controllo **Formazione avanzata di sensibilizzazione alla sicurezza**.

Per abilitare l'integrazione con Wizer per un'organizzazione

Ruolo richiesto: Amministratore del Partner, Amministratore del cliente, Amministratore della protezione o Amministratore Cyber.

Nota
Questa configurazione iniziale viene eseguita una sola volta.

1. Accedere alla console di Cyber Protect Cloud.
2. Nel menu di navigazione, fare clic su **Formazione di sensibilizzazione alla sicurezza** > **Dashboard Sensibilizzazione**.
3. Fare clic su **Abilita integrazione**.
4. Fare clic su **Abilita** per confermare.

Una volta abilitata l'integrazione, nella piattaforma Wizer viene eseguito il provisioning di un nuovo tenant per l'organizzazione. Se si dispone già di un account in Wizer e si desidera utilizzare tale account invece di un nuovo tenant, contattare il service provider di riferimento.

È possibile accedere al Pannello di amministrazione di Wizer e aggiungere gli utenti manualmente, importando un file CSV o configurando l'accesso SSO con Active Directory, Octa, Google o un altro fornitore di identità. Consultare Come aggiungere utenti.

Advanced Management (RMM)

Advanced Management (RMM) offre un livello avanzato di monitoraggio e gestione degli endpoint e delle utenze Microsoft 365. Per ulteriori informazioni o richiedere una demo cliccare qui.

- Per gli endpoint, RMM fornisce quanto segue:
  - **Inventario software**: consente di visualizzare l'elenco completo dei software utilizzati dai clienti e permette di risparmiare tempo e lavoro durante le fasi di preparazione, pianificazione o tracciabilità degli aggiornamenti.
  - **Deployment software con DeployPilot**: consente di distribuire software in modo remoto sui workload gestiti. Utilizzare i piani di deployment software per automatizzare il processo di distribuzione del software e garantire che il deployment del software sui workload sia uniforme.
  - **Patch management automatizzato**: per correggere le vulnerabilità prima che possano essere sfruttate.
  - **Applicazione sicura delle patch**: ripristino rapido e semplice dei workload in presenza di patch difettose grazie all'esecuzione di backup automatici del sistema prima che le patch vengano applicate.
  - **Monitoraggio e avvisi intelligenti basati su machine learning**: riduzione dei rischi operativi e ottimizzazione delle attività di monitoraggio con monitoraggio e avvisi predittivi.
  - **Cyber Scripting pronto all'uso**: automazione e ottimizzazione delle attività più ripetitive.
  - **Monitoraggio dell'integrità delle unità**: grazie al monitoraggio e agli avvisi predittivi è possibile ridurre in modo proattivo le interruzioni operative causate da guasti del disco.
  - **Desktop remoto e assistenza remota**: accesso ai workload remoti per risolvere rapidamente i problemi tecnici. Risparmio di tempo ed erogazione servizi di supporto affidabili con prestazioni eccellenti, anche in presenza di larghezza di banda limitata. La funzionalità prevede una migliore copertura delle piattaforme (Windows, macOS e Linux) e capacità migliorate per la registrazione delle sessioni, le azioni da remoto, i trasferimenti di file, il monitoraggio, la creazione di report e l'osservazione dei workload su più viste.
  - **Vulnerability assessment per le applicazioni Windows di terze parti**: migliora il livello della postura di sicurezza delle applicazioni Windows di terze parti, rilevando e gestendo le vulnerabilità in 314 applicazioni critiche, con il supporto di un database gestito internamente. La funzionalità di Vulnerability assessment per le applicazioni Windows di terze parti è ora parte del pacchetto Advanced Management (RMM) e potrebbe comportare costi aggiuntivi. Per interrompere la protezione di queste applicazioni e disabilitare la funzionalità o abilitarla in più piani esistenti, consultare "Attivazione e disattivazione in blocco del Vulnerability assessment per le applicazioni Windows di terze parti" (pag. 201).
  - **Tracciamento della geolocalizzazione** - Visualizza la posizione fisica in tempo reale dei workload gestiti.
  - **Chat dell'helpdesk** - Utilizza lo strumento di comunicazione in tempo reale tra tecnici e utenti remoti di workload gestiti Windows e macOS per fornire una risoluzione dei problemi più rapida e un servizio clienti migliore.

- Alle utenze Microsoft 365, RMM fornisce una valutazione continua del livello di sicurezza di Microsoft 365, con baseline basate su best practice e correzione delle deviazioni dalle baseline. Se si abilita il servizio di gestione Microsoft 365, sono disponibili due modalità di prodotto:
  - **Gratuita**: abilita la verifica del livello di sicurezza di Microsoft 365 con baseline basate su best practice e onboarding degli utenti. La modalità Gratuita è disponibile nel set di funzionalità di protezione standard.
  - **Avanzata**: include tutte le funzionalità della modalità Gratuita e consente anche la correzione automatica delle deviazioni dalla baseline del livello di sicurezza e l'offboarding dell'utente.

Attivazione e disattivazione in blocco del Vulnerability assessment per le applicazioni Windows di terze parti

Disattivare e attivare la funzionalità di Vulnerability assessment per le applicazioni Windows di terze parti su più tenant cliente con più workload gestiti, spesso risultano attività dispendiose in termini di tempo. Per questo motivo abbiamo creato strumenti per la disattivazione e l'attivazione in blocco di tale funzionalità. Per ulteriori dettagli, consultare questi articoli della Knowledge Base:

- Se la funzionalità di Vulnerability assessment per le applicazioni Windows di terze parti è stata configurata nei piani di protezione, ma il cliente non ha abilitato il pacchetto Advanced Management (RMM) nel proprio tenant, utilizzare questo strumento per disabilitare il Vulnerability assessment per le applicazioni Windows di terze parti in tutti i piani interessati, senza apportare modifiche a tutti gli altri componenti della funzionalità: https://care.acronis.com/s/article/Acronis-Cyber-Protect-Disabling-Vulnerability-Assessment-of-Third-Party-Windows-Applications-when-Advanced-Management-pack-is-not-enabled-for-the-tenant.
- Se è necessario abilitare la funzionalità di Vulnerability assessment per le applicazioni Windows di terze parti per garantirne la protezione in tutti i piani di protezione in cui la policy di Vulnerability assessment generale è già attiva e il pacchetto Advanced Management (RMM) è abilitato per i tenant corrispondenti, utilizzare questo strumento per abilitare in blocco la policy secondaria:https://care.acronis.com/s/article/Acronis-Cyber-Protect-Enabling-Vulnerability-Assessment-for-Windows-Third-Party-Applications-when-Vulnerability-Assessment-module-is-enabled-in-Protection-plans.

Advanced Automation (PSA)

Il servizio Advanced Automation (PSA) contribuisce a rendere facile e intuitivo sfruttare le piattaforme e i software di gestione aziendale. Costituito da numerosi di strumenti di pagamento, Advanced Automation (PSA) consente agli MSP di gestire e automatizzare completamente varie attività quotidiane, tra cui:

- Creazione ed emissione delle fatture ai clienti.
- Supporto ai clienti e creazione dei ticket del service desk.
- Gestione delle vendite e dei progetti.

È possibile abilitare Advanced Automation (PSA) affinché operi in tandem con altri servizi Portale di gestione, con un addebito aggiuntivo. Il costo addebitato all'account è basato sul numero di utenti (o di tecnici) ai quali è concesso l'accesso al servizio Advanced Automation (PSA).

Cos'è il modulo Advanced Automation (PSA)?

Advanced Automation (PSA) è uno strumento di gestione aziendale progettato per i managed service provider (MSP), volto a semplificare e a rendere intuitive agli MSP la gestione e l'automazione di numerose attività quotidiane.

Advanced Automation (PSA) garantisce ai clienti di ricevere il servizio che richiedono e all'MSP di mantenere il controllo delle operazioni. In Advanced Automation (PSA) convergono diversi componenti, tra cui la creazione dei ticket, l'integrazione con le soluzioni RMM, la gestione dei progetti, la registrazione automatica degli orari e la fatturazione basata sui consumi; il modulo fornisce anche l'accesso facile e veloce ai dati relativi alla fatturazione e ai ticket dei clienti. È inoltre possibile utilizzare l'applicazione mobile dedicata per le attività di Service Desk quotidiane, tra cui il monitoraggio e l'elaborazione dei ticket, la traccia e la registrazione degli orari di lavoro. L'applicazione Acronis Advanced Automation (PSA) è scaricabile da App Store e da Google Play Store.

Dopo l'attivazione del servizio Advanced Automation (PSA), all'account viene addebitato ogni utente a cui è concesso l'accesso al servizio.

Le funzionalità chiave di Advanced Automation (PSA) includono:

- **Gestione dei ticket del Service Desk**: se le funzionalità richieste sono abilitate, le e-mail in arrivo e gli avvisi provenienti da piattaforme integrate di terze parti vengono automaticamente convertiti in ticket di supporto. Per ulteriori informazioni, consultare "Service Desk" (pag. 221).
- **Gestione della fatturazione**: in base al tempo dedicato al cliente o agli accordi di fatturazione sottoscritti con il cliente stesso, le fatture vengono generate automaticamente. Per ulteriori informazioni, consultare "Gestione della funzionalità Vendite e fatturazione" (pag. 271).
- **Gestione progetti**: creare piani di progetto orientati al cliente con scadenze e budget definiti e assegnare passaggi del progetto da completare ai membri del team. Monitorare e tenere traccia

del progresso dei progetti e fatturare ai clienti le attività di lavoro sul progetto. Per ulteriori informazioni, consultare "Progetti" (pag. 238).

- **Gestione delle registrazioni orario e delle attività**: approvazione degli orari dei ticket per la fatturazione, richieste di permessi e approvazione delle ferie come utente amministratore o responsabile. Per ulteriori informazioni, consultare "Voci orario" (pag. 262).
- **Integrazione nativa con i servizi Acronis**: include la fatturazione ai clienti basata sul consumo e il controllo dei dispositivi con Advanced Management.

Abilitazione di Advanced Automation (PSA) per i clienti

Come descritto durante il processo di creazione del tenant (consultare "Selezione dei servizi per un tenant" (pag. 48)), è possibile aggiungere ai tenant i servizi richiesti.

Il servizio Advanced Automation (PSA) è disponibile per i tipi di tenant indicati di seguito.

- Partner
- Cliente

Nota
I Partner non possono visualizzare i dati di Advanced Automation (PSA) dei loro clienti (siano essi sub-Partner o clienti), perché, a differenza di altri prodotti , i dati di Advanced Automation (PSA) sono dati aziendali privati specifici per un account di sub-Partner (o cliente). Tuttavia, i Partner possono comunque visualizzare i dati specifici dell'account accedendo al portale di gestione come cliente pertinente (sub-Partner o cliente).

Per abilitare Advanced Automation (PSA)

1. Nel portale di gestione, passare a **Clienti**.
2. Selezionare il tenant da modificare.
3. Nella scheda **Configura**, nella sezione **Servizio**, scorrere verso il basso e selezionare **Advanced Automation (PSA)**.
   Ora il servizio Advanced Automation (PSA) è disponibile per il cliente selezionato.

Impostazione di Advanced Automation (PSA)

Questa sezione descrive tutti i passaggi da completare per iniziare a usare Advanced Automation (PSA).

Attivazione di Advanced Automation (PSA)

Se il servizio Advanced Automation (PSA) è stato attivato per l'account, è possibile attivarlo passando a **Impostazioni**. Se il servizio Advanced Automation (PSA) non è abilitato, contattare l'amministratore.

Per attivare Advanced Automation (PSA)

1. Nel portale di gestione, fare clic su **Impostazioni > Advanced Automation (PSA)**.

   Nota
   Dopo aver attivato Advanced Automation (PSA), come descritto nei passaggi seguenti, questa opzione di menu non sarà più disponibile.

2. Nella schermata visualizzata, fare clic su **Attivare Advanced Automation (PSA)**.
3. Nella schermata Attivare Advanced Automation (PSA), nella scheda **Informazioni sull'azienda** inserire i dati richiesti, quindi fare clic su **Avanti**.
4. Nella scheda **Ruoli utente**, indicare il ruolo Advanced Automation (PSA) per ogni utente, quindi fare clic su **Avanti**. Sono disponibili i ruoli seguenti:
   - Tecnico
   - Risorse umane
   - Contabilità
   - Vendite
   - Responsabile gruppo
   - Responsabile contabilità
   - Direttore
   - Amministratore

   Per comprendere meglio ognuno dei ruoli di Advanced Automation (PSA) e i rispettivi privilegi di accesso, vedere "Ruoli di Advanced Automation (PSA)" (pag. 216).

   Nota
   Dopo aver attivato Advanced Automation (PSA), è anche possibile aggiungere nuovi utenti. Creare innanzitutto gli account utente e quindi applicare i servizi a cui l'utente potrà accedere. Per ulteriori informazioni, consultare "Creazione di un account utente" (pag. 61).

5. Nella scheda **Conferma**, controllare le informazioni di attivazione e fare clic su **Attiva**. La configurazione del servizio Advanced Automation (PSA) potrebbe richiedere alcuni secondi.
6. Nella schermata della procedura guidata di onboarding, selezionare una tra le seguenti opzioni di Advanced Automation (PSA):
   - **Integrazione di piattaforme di contabilità**: Fare clic su **Configura** per essere reindirizzati alla pagina delle integrazioni dei sistemi di contabilità. Per ulteriori informazioni, consultare "Integrazione con piattaforme di contabilità" (pag. 345).
   - **Integrazione con piattaforme RMM**: Fare clic su **Configura** per essere reindirizzati alla pagina delle integrazioni di Advanced Automation (PSA) RMM. Per ulteriori informazioni, consultare "Integrazione con piattaforme RMM" (pag. 351).
   - **Configurazione del Service Desk**: fare clic su **Configura** per il reindirizzamento verso **Impostazioni > Service Desk**. Per ulteriori informazioni, consultare "Impostazioni di Service Desk" (pag. 314).

- **Configurazione del server di posta**: Fare clic su **Configura** per essere reindirizzati alla schermata Configura server e-mail. Per ulteriori informazioni, consultare "Configurazione delle impostazioni e-mail" (pag. 217).

Se non si ha intenzione di utilizzare le funzionalità incluse in Advanced Automation (PSA), è possibile disattivare il servizio Advanced Automation (PSA). Per ulteriori informazioni, consultare "Disattivazione del servizio Advanced Automation (PSA)" (pag. 370).

Guida rapida alla configurazione di Advanced Automation (PSA)

Questa guida rapida descrive tutti i passaggi da completare per iniziare a usare Advanced Automation (PSA).

Seguire i passaggi indicati nella tabella seguente per garantire che:

- I clienti nuovi ed esistenti siano configurati in Advanced Automation (PSA).
- I prodotti e i servizi offerti dall'MSP siano configurati e disponibili, e che anche la fatturazione automatica sia pronta per essere utilizzata.
- Il Service Desk sia configurato e pronto per supportare i clienti, monitorare gli SLA e tenere traccia del tempo dedicato ai ticket e ad altre attività.
- La piattaforma RMM e/o di contabilità in uso sia integrata e sincronizzata con Advanced Automation (PSA).
- Le e-mail in arrivo siano convertite in ticket e le risposte automatizzate configurate.

Nota
È inoltre possibile utilizzare l'applicazione mobile dedicata, benché più limitata ("Acronis Advanced Automation (PSA)", reperibile su App Store e Google Play Store), per operare con i ticket del Service Desk e le voci orario.

La tabella seguente descrive i passaggi generali necessari per iniziare a lavorare con Advanced Automation (PSA).

Passaggio	Descrizione
PASSAGGIO 1: Accedere e avviare la procedura guidata di onboarding di Advanced Automation (PSA)	Accedere al proprio account e al portale di gestione. Se Advanced Automation (PSA) è disponibile per l'account, vengono visualizzate due nuove opzioni di menu: **Gestione attività** e **Vendite e fatturazione**. Selezionarne una per accedere alla procedura guidata di onboarding di Advanced Automation (PSA); fare clic su **Attiva** per attivare il servizio, come descritto nel Passaggio 2. Per ulteriori informazioni, consultare "Attivazione di Advanced Automation (PSA)" (pag. 203).
PASSAGGIO 2: Attivare il servizio	Per attivare il servizio Advanced Automation (PSA) per l'account, è necessario completare i due passaggi indicati di seguito:

Passaggio	Descrizione
Advanced Automation (PSA)	a. Fornire le informazioni richieste, inclusi i dettagli del conto bancario, nella scheda **Informazioni sull'azienda**. Le informazioni inserite vengono utilizzate anche per creare le fatture destinate ai clienti finali. Quindi, fare clic su **Avanti**. b. Assegnare gli utenti esistenti ai ruoli di Advanced Automation (PSA) indicati di seguito: • Tecnico • Risorse umane • Contabilità • Vendite • Responsabile gruppo • Responsabile contabilità • Direttore • Amministratore Tenere presenti che esistono due ruoli aggiuntivi per gli utenti dei clienti: • Cliente • Gestore cliente Per ulteriori informazioni sui ruoli in Advanced Automation (PSA), consultare "Ruoli di Advanced Automation (PSA)" (pag. 216). Se necessario, è possibile aggiungere altri utenti in un secondo momento; consultare anche "Gestione degli utenti" (pag. 61). Al termine, è possibile iniziare a definire le impostazioni di Advanced Automation (PSA), come descritto nei passaggi seguenti.
PASSAGGIO 3: Definire le impostazioni di Service Desk	Le impostazioni di Service Desk determinano le sezioni principali del flusso di ticket del Service Desk, tra cui categorie, valori predefiniti, impostazioni predefinite relative a Paese e lingua, e contratto sui livelli di servizio (SLA). Per accedere alle impostazioni di Service Desk, nel portale di gestione passare a **Impostazioni > Service Desk**. Queste impostazioni consentono di effettuare le operazioni indicate di seguito. • Configurare le risposte definite • Impostare le priorità • Gestire gli SLA • Definire categorie e sottocategorie • Impostare valori predefiniti • Definire le impostazioni relative al Paese e alla lingua • Attivare e disattivare gli stati • Definire le impostazioni per l'integrazione dei ticket RMM predefiniti • Gestione dei modelli e-mail • Definire le attività con monitoraggio degli orari • Impostare l'entità di fatturazione dei progetti predefinita
PASSAGGIO 4:	Le impostazioni della sezione Fatturazione e offerte consentono di personalizzare le modalità di fatturazione, ad esempio il layout delle fatture, il formato di esportazione

Passaggio	Descrizione
Definizione delle impostazioni della sezione Fatturazione e offerte	predefinito (se è necessario importare la fattura in un altro sistema), le imposte e molto altro ancora. Tenere presente che le informazioni di fatturazione per gli utenti finali devono essere specificate in ogni impostazione del cliente o durante la creazione di articoli di vendita, contratti e preventivi. Per accedere alle impostazioni per la fatturazione e le offerte, nel portale di gestione passare a **Impostazioni > Fatturazione e offerte**. Queste impostazioni consentono di effettuare le operazioni indicate di seguito. • Definire e personalizzare le modalità di fatturazione • Definire e personalizzare l'aspetto dei preventivi • Definire le imposte da utilizzare
PASSAGGIO 5: Aggiungere clienti	Il portale di gestione consente di aggiungere e gestire i clienti, come e quando necessario. Acronis permette di definire diversi tipi di account per i clienti, inclusi Partner, clienti e potenziali clienti. Queste diverse tipologie di account vengono indicate con il termine *tenant*. Per ulteriori informazioni sui diversi tipi di tenant, consultare "Account utente e tenant" (pag. 39). Per aggiungere Partner, clienti e potenziali clienti nel portale di gestione, passare a **Clienti**, quindi fare clic su **+ Nuovo** e selezionare il tipo di tenant pertinente. Per ulteriori informazioni, consultare "Gestione dei tenant" (pag. 42).
PASSAGGIO 6: Definire i prodotti	È possibile creare un catalogo che contiene sia i prodotti o i servizi non ricorrenti sia i servizi (gestiti) ricorrenti che vengono erogati ai clienti, come gli abbonamenti antivirus o il supporto ad-hoc. È inoltre possibile rendere determinati prodotti disponibili alla vendita direttamente in un ticket di supporto quando, ad esempio, un cliente registra un ticket per aggiungere un abbonamento a Office 365 o richiedere memoria aggiuntiva. Ciò consente di risparmiare il tempo altrimenti dedicato a ulteriori procedure amministrative. Per accedere ai prodotti, passare a **Vendite e fatturazione > Vendite**, e fare clic sulla scheda **Prodotti**. Gli utenti con i ruoli Amministratore, Direttore, Contabilità o Responsabile contabilità possono creare prodotti. Una volta creati, i prodotti possono essere utilizzati nei contratti, nei ticket, nei preventivi e negli articoli di vendita. Per ulteriori informazioni, consultare "Prodotti" (pag. 295).
PASSAGGIO 7: Definire i contratti	Configurare e definire i contratti per i clienti con attenzione, per garantire che Advanced Automation (PSA) sia in grado di: • Fornire automaticamente gli articoli e gli acconti per la fatturazione periodica e abilitare la fatturazione per gli utenti o i dispositivi quando necessario. • Associare elementi della configurazione, clienti e SLA applicabili. • Collegare automaticamente un servizio, un cliente e l'elemento della configurazione allo SLA applicabile nel Service Desk.

Passaggio	Descrizione
	• Allocare automaticamente i nuovi elementi della configurazione al cliente, al contratto e allo SLA corretti. Per accedere ai contratti, passare a **Vendite e fatturazione > Vendite**, e fare clic sulla scheda **Contratti**. Per ulteriori informazioni, consultare "Lavorare con i contratti" (pag. 282).
PASSAGGIO 8: Configurare le integrazioni con le piattaforme di terze parti	Configurare le integrazioni con le piattaforme di terze parti. Al momento, Advanced Automation (PSA) supporta: • **RMM**: NinjaOne, Datto RMM, Kaseya VSA, N-able N-Central e N-able RMM • **Contabilità**: FreshBooks, QuickBooks, Sage, Xero e SnelStart • **VAR**: Microsoft CSP • **Pagamento**: PayPal e Stripe Per accedere alle integrazioni, nel portale di gestione passare a **Integrazioni**. Per ulteriori informazioni, consultare "Integrazione di Advanced Automation (PSA) con piattaforme di terze parti" (pag. 344).
PASSAGGIO 9: Configurare le impostazioni e-mail	Questo è l'ultimo passaggio per la configurazione di Advanced Automation (PSA). Prima di configurare le impostazioni e-mail, verificare di aver già configurato le risposte e-mail. Dopo aver configurato le impostazioni delle e-mail in arrivo, Advanced Automation (PSA) intercetta tutti i messaggi nella casella di arrivo specificata e crea un ticket per ogni messaggio, se necessario. Una volta elaborata, l'e-mail viene spostata nella cartella di archivio per eventuali riferimenti futuri. Il sistema crea la cartella di archivio se questa non è presente. È necessario definire tre impostazioni e-mail: • **E-mail in arrivo**: questa configurazione permette di disporre di un account e-mail per l'help desk o il supporto direttamente collegato al Service Desk di Advanced Automation (PSA). Le e-mail in arrivo vengono convertite in ticket e le risposte personalizzabili inviate agli utenti finali per tenerli al corrente. • **E-mail in uscita**: il server e l'account di posta utilizzati per inviare o rispondere ai messaggi. • **E-mail fattura**: il server e l'account di posta utilizzati per inviare le fatture ai clienti. Per accedere alle impostazioni di configurazione e-mail, passare a **Impostazioni > Service Desk > Configurazione del server di posta**. Per ulteriori informazioni, consultare "Configurazione delle impostazioni e-mail" (pag. 217).

Onboarding di clienti esistenti

Una volta attivato il servizio Advanced Automation (PSA) per l'account (consultare "Attivazione di Advanced Automation (PSA)" (pag. 203)), è necessario eseguire l'onboarding dei clienti esistenti per fatturare ed elaborare le loro richieste di servizi.

Importante
Advanced Automation (PSA) attualmente supporta i tenant di Partner e Clienti diretti e i tenant di Partner e Clienti situati sotto i tenant di Cartella. I tenant di Cartella vengono gestiti allo stesso modo dei tenant di Partner e Cliente diretti, e tutti sono disponibili per la selezione di tutte le funzionalità di Advanced Automation (PSA). Per ulteriori informazioni, vedere "Gestione dei tenant" (pag. 42).

Per verificare che Advanced Automation (PSA) sia configurato correttamente per i clienti esistenti, procedere come segue:

- Fornire le informazioni di fatturazione per i clienti esistenti.
- Creare i contratti per iniziare a fatturare i servizi e i prodotti ai clienti esistenti.
- Verificare che sia possibile ricevere ed elaborare i ticket del Service Desk per i clienti esistenti.
- Verificare di poter creare articoli di vendita per i clienti esistenti.
- Verificare di poter eseguire il processo di fatturazione e l'emissione delle fatture per i clienti esistenti.

Nota
Se i clienti sono tenant Partner, non è possibile visualizzare i clienti o i dati di fatturazione dei clienti gestiti come account tenant Partner. Tuttavia, è possibile convertire i tenant Partner in tenant di Cartella per attivare Advanced Automation (PSA) con la trasparenza necessaria per fatturare i tenant di un Partner. Per ulteriori informazioni, consultare "Conversione di un tenant partner in un tenant cartella e viceversa" (pag. 58).

Allo stesso modo, per qualsiasi tenant di Cartella definito, è possibile visualizzare i dati di fatturazione per ciascun tenant Cliente o Partner sotto un tenant di Cartella. Tuttavia, nei report Advanced Automation (PSA), non sarà possibile visualizzare i dati di fatturazione aggregati o i dati del report del Service Desk se si seleziona un tenant di Cartella, poiché tali tenant non vengono visualizzati nell'elenco clienti di Advanced Automation (PSA) (ad esempio, quando si seleziona un cliente per un'anteprima del report).

Fornire le informazioni di fatturazione

Se Advanced Automation (PSA) è attivato, quando si accede alla sezione **Clienti** verrà richiesto di inviare le informazioni di fatturazione relative ai clienti esistenti. Questi dati garantiscono di poter utilizzare Advanced Automation (PSA) per fatturare ed elaborare le richieste di servizio per i clienti.

Nota
Se per un cliente non sono state fornite le informazioni di fatturazione, non sarà possibile approvare i ticket e le registrazioni orario del cliente; quando si elaborano tali ticket, verrà visualizzato un messaggio che chiede di inserire le informazioni mancanti per i clienti specificati. Allo stesso modo, quando si crea un articolo di vendita, verrà visualizzato un messaggio che chiede di inserire le informazioni di fatturazione complete per il cliente selezionato, se tali informazioni non sono già state definite in Advanced Automation (PSA). Vedere le sezioni pertinenti più sotto per ulteriori informazioni.

Per aggiungere informazioni di fatturazione per i clienti esistenti

1. Nel portale di gestione, passare a **Organizzazione > Clienti**.
2. Fare clic sull'icona dei puntini di sospensione accanto al nome del cliente. Nel menu visualizzato, selezionare **Aggiungi informazioni di fatturazione**.

   Oppure

   Fare clic su una colonna Cliente nell'elenco visualizzato. Nella barra laterale visualizzata, fare clic sulla scheda **Configura**. Quindi, fare clic sulle sezioni **Fatturazione** e **Indirizzo** per aggiungere le informazioni di fatturazione pertinenti.
3. Completare i campi inclusi nel modulo visualizzato. Per ulteriori informazioni su questi campi, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47).
4. Fare clic su **Aggiungi** per completare l'impostazione delle informazioni di fatturazione.

   Nota
   Per gestire e poter accedere ai numeri di telefono degli utenti nel Service Desk, nella stessa scheda **Configura** fare clic su nella sezione **Impostazioni generali** e abilitare l'interruttore **Abilita profilo cliente autogestito**. Se abilitata, questa opzione permette agli amministratori e agli utenti del cliente di visualizzare i campi relativi ai contatti pertinenti, inclusi i numeri di telefono (oltre al contatto aziendale e alla posizione professionale). Per ulteriori informazioni, consultare "Configurazione del profilo cliente autogestito" (pag. 53).

Creare i contratti per iniziare a fatturare i servizi e i prodotti ai clienti esistenti

I contratti garantiscono di poter utilizzare Advanced Automation (PSA) per emettere con regolarità le fatture ai clienti.

Se Advanced Automation (PSA) è attivato, quando si accede al modulo **Vendite e fatturazione** verrà richiesto di creare i contratti per i clienti esistenti. La richiesta ha luogo solo se a uno o più clienti sono assegnati prodotti o servizi Acronis.

Per creare contratti per clienti esistenti

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Se il banner visualizzato segnala che un numero specifico di clienti non ha contratti assegnati, fare clic su **Crea**.

In alternativa, se in precedenza il banner è stato chiuso, fare clic sul link **Crea contratti per clienti esistenti** che si trova nella parte superiore destra dello schermo.

3. Nella procedura guidata Crea nuovo contratto, procedere come segue.
   a. Selezionare il cliente pertinente e fare clic su **Avanti**.
   b. Aggiungere le informazioni sul contratto, inclusi i dettagli del pagamento e il periodo di durata del contratto. Per ulteriori informazioni, consultare "Lavorare con i contratti" (pag. 282). Al termine, fare clic su **Avanti**.
   c. Aggiungere le informazioni di fatturazione, quindi fare clic su **Avanti**. Questo passaggio non viene visualizzato se le informazioni di fatturazione sono già state definite, come descritto in "Fornire le informazioni di fatturazione" (pag. 209).
   d. Aggiungere le parti del contratto come necessario. Per ulteriori informazioni, consultare "Creazione di un nuovo contratto" (pag. 282). Per impostazione predefinita, le parti del contratto basate su servizi Acronis già assegnate al cliente vengono aggiunte al modello di contratto. Queste parti del contratto possono essere modificate o eliminate. Verificare di aver impostato i prezzi corretti per le parti del contratto.
4. Fare clic su **Fine**. Il contratto viene aggiunto all'elenco dei contratti esistenti visualizzato nella scheda **Contratti**.

Verificare che sia possibile ricevere ed elaborare i ticket del Service Desk per i clienti esistenti

Se Advanced Automation (PSA) è attivato, è possibile ricevere ed elaborare i ticket per un cliente esistente anche se per tale cliente non sono state definite informazioni di fatturazione. Ciò garantisce la possibilità di creare, rispondere, risolvere e chiudere i ticket quando e come necessario. Per ulteriori informazioni su come lavorare con le funzionalità del Service Desk, consultare "Service Desk" (pag. 221).

Non è possibile approvare un orario ticket riferito da un cliente se per tale cliente non sono state fornite le informazioni di fatturazione. Quando si tenta di approvare le registrazioni orario riferite a un ticket, verrà richiesto di aggiungere le informazioni di fatturazione del cliente in questione; per altre informazioni consultare Fornire le informazioni di fatturazione.

Verificare di poter creare articoli di vendita per i clienti esistenti

Quando Advanced Automation (PSA) è attivo, è possibile creare articoli di vendita per un cliente esistente anche se le informazioni di fatturazione non sono definite per quel cliente. Quando non vengono fornite informazioni di fatturazione, gli articoli di vendita in stato **Bozza** vengono generati automaticamente per i clienti (vedere "Come funziona l'automazione della fatturazione in Advanced Automation (PSA)" (pag. 212)).

Tuttavia, durante la creazione di un articolo di vendita (consultare "Gestione degli articoli di vendita" (pag. 278)), se si seleziona un cliente per il quale non sono state specificate informazioni di fatturazione, viene richiesto di fornirle prima di poter procedere alla creazione dell'articolo.

Inoltre, quando si modifica un articolo di vendita esistente, non è possibile sostituire il cliente esistente assegnato all'articolo con un cliente senza informazioni di fatturazione specificate. Viene richiesto di fornire tali informazioni prima di poter procedere con la modifica dell'articolo.

Verificare di poter eseguire il processo di fatturazione e l'emissione delle fatture per i clienti esistenti

Durante il primo ciclo di fatturazione, viene richiesto di verificare le impostazioni di numerazione delle fatture prima di generare le fatture; i numeri delle fatture create devono essere allineati a quelli del software di contabilità in uso. Questo passaggio garantisce che le informazioni di fatturazione e di emissione delle fatture siano state configurate correttamente. Per ulteriori informazioni, consultare "Fatture" (pag. 289).

Come funziona l'automazione della fatturazione in Advanced Automation (PSA)

Advanced Automation (PSA) offre una fatturazione mensile completamente automatizzata per i servizi per impostazione predefinita.

Per impostazione predefinita, il primo giorno di ogni mese, il sistema genera automaticamente articoli di vendita per tutti i clienti con prodotti in uso nel mese appena concluso. Questo processo di fatturazione mensile si basa sulla creazione di report sull'utilizzo della piattaforma Cyber Protect Cloud e copre completamente il modello di fatturazione PAYG (a consumo) per i provider. Inoltre, i contratti possono essere configurati per i clienti, per consentire ai provider di configurare regole e termini di fatturazione specifici.

Quando Advanced Automation (PSA) è attivo, il sistema procede automaticamente alla fatturazione mensile per l'ultimo mese trascorso, consentendo ai provider di testare immediatamente la funzionalità di fatturazione. Questa fatturazione iniziale viene visualizzata sotto forma di articoli di vendita entro 15-20 minuti (a seconda della base clienti) dall'attivazione di Advanced Automation (PSA). Gli articoli di vendita si basano sull'utilizzo del mese precedente.

Il primo giorno di un nuovo mese, il sistema procede automaticamente alla fatturazione del contratto, ciò include la preparazione dei dati di fatturazione per i clienti e gli articoli di vendita per quegli articoli che superano l'impegno minimo definito nel contratto. La fatturazione include anche gli articoli di vendita definiti per l'utilizzo al di fuori dei contratti.

Limitazioni

- Per i clienti senza informazioni di fatturazione, gli articoli di vendita vengono generati con stato **Bozza**. Questi articoli non possono essere fatturati fino a quando non vengono fornite le informazioni di fatturazione del cliente.
- Non vengono generati articoli di vendita per i clienti in prova, indipendentemente dal fatto che si stia eseguendo la fatturazione iniziale o dei mesi successivi.

Lavorare con i campi personalizzati

La definizione di campi personalizzati permette di archiviare informazioni aggiuntive (facoltative) relative a clienti, prodotti, articoli di vendita, contratti, parti del contratto e ticket. I campi personalizzati sono elencati nella nuova sezione **Informazioni aggiuntive** nell'entità pertinente.

Ad esempio, è possibile aggiungere campi personalizzati applicabili ai clienti. Durante la creazione o la modifica di un cliente, è possibile completare i campi personalizzati predefiniti nella sezione **Informazioni aggiuntive**; questi dati vengono aggiunti alle informazioni relative al cliente.

Questa sezione descrive come aggiungere un nuovo campo personalizzato e come modificare o rimuovere un campo personalizzato esistente.

Nota
Questa funzionalità è disponibile solo agli utenti ai quali è assegnato il ruolo di Amministratore.

Creazione di un campo personalizzato

Per creare un campo personalizzato

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Campi personalizzati**.
2. Fare clic su **+ Nuovo campo personalizzato**.
3. Definire quanto segue:
   - Nel campo **Nome**, inserire il nome del campo personalizzato.
   - Nel campo **Tipo**, selezionare il tipo di campo pertinente tra una delle seguenti opzioni:
     - Stringa
     - Numero intero
     - Booleano
     - Testo
     - Data
   - Nella colonna **Obbligatorio**, far scorrere l'interruttore su **Sì** per rendere il campo obbligatorio.
   - Nel campo **Applica a**, selezionare l'entità alla quale applicare il campo personalizzato:
     - Cliente
     - Prodotto
     - Progetto
     - Fase progetto
     - Contratto
     - Parte del contratto
     - Articolo di vendita

- Ticket

  Nota
  Il campo personalizzato applicato ai ticket interessa tutti i tipi di ticket (inclusi i ticket del service desk, i preventivi e altri).

- Articolo di inventario

- Nella colonna **Stato**, selezionare una delle due opzioni **Attivo** o **Inattivo**.
- Nella colonna **Numero ordine**, inserire un valore numerico che definisce la preferenza di visualizzazione per il campo personalizzato. Questa opzione è importante quando si dispone di una serie di campi personalizzati all'interno di un modulo visualizzato; più basso è il numero, più in alto verrà visualizzato il campo personalizzato.

4. Fare clic su **Crea campo personalizzato** per aggiungere il nuovo campo personalizzato.

Modifica di un campo personalizzato

Questa sezione descrive come modificare o rimuovere un campo personalizzato esistente.

Per modificare un campo personalizzato

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Campi personalizzati**.
2. Fare clic sulla riga del campo personalizzato da modificare.
3. Modificare come necessario. Per ulteriori informazioni sui campi modificabili, consultare "Creazione di un campo personalizzato" (pag. 213).
4. Al termine, fare clic su ✓.

Per rimuovere un campo personalizzato

Nella schermata **Campi personalizzati**, fare clic sull'icona dei puntini di sospensione nella riga del campo personalizzato da rimuovere, quindi fare clic su **Rimuovi**.

Il campo personalizzato viene rimosso dalla schermata **Campi personalizzati** e non sarà più visibile nella sezione **Informazioni aggiuntive** dell'entità pertinente.

Gestione degli utenti

Dopo aver attivato Advanced Automation (PSA) (consultare "Attivazione di Advanced Automation (PSA)" (pag. 203)), agli utenti esistenti vengono automaticamente assegnati i ruoli necessari per l'accesso immediato alle funzionalità di Advanced Automation (PSA). Per impostazione predefinita, agli amministratori dell'azienda è concesso il ruolo Amministratore; a tutti gli altri utenti viene assegnato il ruolo Tecnico, che può tuttavia essere modificato secondo le esigenze.

È inoltre possibile aggiungere utenti e gruppi di utenti, come necessario. Quando si assegna un utente con un ruolo di Advanced Automation (PSA), l'utente viene automaticamente assegnato al

gruppo di utenti predefinito. Le impostazioni dei gruppi utente possono essere aggiornate nella sezione Impostazioni (consultare "Impostazioni di Service Desk" (pag. 314)).

Per ulteriori informazioni sulla creazione degli utenti di Advanced Automation (PSA) nel portale di gestione, consultare "Creazione di un account utente" (pag. 61).

Gestione dei gruppi di utenti

Gli utenti a cui è assegnato il ruolo di Amministratore o di Direttore possono gestire i gruppi di utenti all'interno dell'organizzazione.

Per aggiungere un nuovo gruppo di utenti all'organizzazione

1. Nel portale di gestione, passare a **Impostazioni** > **Service Desk**, quindi selezionare **Gruppi utenti**.
   L'elenco visualizzato mostra i gruppi attivi e inattivi e il numero di utenti contenuti in ciascun gruppo. Questi gruppi possono essere modificati o attivati e disattivati, come descritto di seguito.
2. Fare clic su **+ Nuovo**.
3. Inserire un **Nome per il gruppo di utenti**.
4. Selezionare il **Responsabile gruppo**.
5. Selezionare la casella di controllo **Attivo** per attivare il gruppo.
6. Selezionare gli utenti da inserire nel gruppo dall'elenco **Utenti** a destra. Fare quindi clic sull'icona della freccia a sinistra per aggiungere gli utenti all'elenco **Membri del gruppo**.
7. Fare clic su **Crea nuovo gruppo**.

Per aggiornare un gruppo di utenti

1. Nella schermata **Gruppi utenti**, fare clic sul gruppo da aggiornare.
2. Nella barra laterale destra, fare clic sull'icona a forma di matita per modificare il gruppo di utenti. Oltre ad aggiornare il nome e il responsabile del gruppo, è anche possibile modificare i membri del gruppo e attivare o disattivare il gruppo selezionando o deselezionando la casella di controllo **Attivo**.
3. Al termine, fare clic su ✓.

Per eliminare un gruppo di utenti

1. Nella schermata **Gruppi utenti**, fare clic sul gruppo da eliminare.
2. Nella barra laterale destra, fare clic sull'icona a forma di cestino.
   Il gruppo di utenti viene eliminato.

> **Nota**
> È possibile eliminare un gruppo di utenti solo se al momento è **Inattivo** e tutti gli utenti sono stati assegnati a un altro gruppo **Attivo**. Inoltre, il gruppo non deve essere utilizzato in nessuna altra impostazione di Advanced Automation (PSA), come ad esempio le impostazioni predefinite del Service Desk o delle quote.

Ruoli di Advanced Automation (PSA)

Advanced Automation (PSA) include una serie di ruoli che possono essere assegnati agli utenti come necessario.

Dopo aver attivato Advanced Automation (PSA) (come descritto in "Attivazione di Advanced Automation (PSA)" (pag. 203)), a tutti gli utenti esistenti è automaticamente concesso l'accesso alla funzionalità di Advanced Automation (PSA). Durante il processo di creazione dell'account, è possibile assegnare il ruolo pertinente a ciascun utente. Tenere presente che, per impostazione predefinita, agli amministratori del portale di gestione è concesso il ruolo Amministratore e che agli amministratori di sola lettura è concesso il ruolo Tecnico.

Per aggiornare il ruolo in un secondo momento, passare a **La mia azienda** > **Utenti**, selezionare l'utente pertinente e nella scheda **Servizi** aggiornare il ruolo. Nella stessa scheda è possibile disabilitare la funzionalità di Advanced Automation (PSA) per quello specifico utente.

La tabella seguente descrive ogni ruolo disponibile e i diritti assegnati a ciascun ruolo in Advanced Automation (PSA):

Ruolo	Descrizione
Tecnico	Il ruolo predefinito applicato a tutti gli utenti. Questo ruolo consente all'utente di accedere ai moduli Service Desk, Gestione progetti e alla funzionalità di monitoraggio orario. Il ruolo prevede anche l'accesso limitato alle informazioni del cliente e ai suoi utenti finali.
Risorse umane	Questo ruolo consente all'utente accesso limitato ai moduli Service Desk, Gestione progetti, Report e Voci orario.
Contabilità	Questo ruolo consente di accedere ai moduli CRM, Vendite e fatturazione, Service Desk, Gestione progetti e alla funzionalità di monitoraggio orario. Il ruolo prevede anche l'accesso limitato alle statistiche finanziarie del cliente, ma non consente l'accesso ai report aziendali.
Vendite	Questo ruolo consente all'utente di accedere ai moduli CRM, Vendite, Service Desk, Gestione progetti e alla funzionalità di monitoraggio orario. Il ruolo prevede anche l'accesso limitato ai dati delle fatture, ma non consente l'accesso ai report aziendali.
Responsabile gruppo	Questo ruolo consente all'utente di accedere ai moduli CRM, Service Desk, Gestione progetti. Il ruolo prevede anche l'accesso completo alle statistiche finanziarie del cliente, ai report aziendali e alla funzionalità di monitoraggio orario, oltre all'accesso limitato al modulo Vendite.
Responsabile contabilità	Questo ruolo consente all'utente di accedere ai moduli CRM,

Ruolo	Descrizione
	Vendite e fatturazione, Service Desk, Gestione progetti. Il ruolo prevede anche l'accesso completo alle statistiche finanziarie del cliente, ai report aziendali e alla funzionalità di monitoraggio orario.
Direttore	Questo ruolo consente all'utente di accedere a tutti i moduli, ma non consente di gestire le impostazioni globali dell'azienda.
Amministratore	Questo ruolo concede all'utente diritti di accesso completo e la capacità di gestire le impostazioni globali dell'azienda relativamente ai moduli Service Desk, Vendite e fatturazione.
*I ruoli seguenti sono disponibili agli utenti dei clienti. Selezionare il cliente di interesse e quindi passare a **Gestione azienda > Utenti**. Quando si aggiungono gli utenti per la prima volta, il loro stato è su Inattivo e viene loro inviata un'e-mail di invito. È possibile attivare o disattivare il loro accesso ad Advanced Automation (PSA) in qualsiasi momento.*	
Cliente	Questo ruolo consente all'utente di accedere al modulo Service Desk (limitandosi all'organizzazione del cliente).
Gestore cliente	Questo ruolo consente all'utente di accedere ai moduli Service Desk, Fatture e Report (limitandosi all'organizzazione del cliente).

Configurazione delle impostazioni e-mail

Advanced Automation (PSA) include un parser e-mail integrato che converte le e-mail in arrivo in ticket. Per utilizzare la funzionalità, accertarsi di utilizzare un account e-mail dedicato o un account e-mail di prova. Tenere inoltre presente quanto segue:

- Non utilizzare un account e-mail personale con lo stesso indirizzo di un account utente Portale di gestione.
- Tutti i messaggi *non letti* che il sistema trova nella casella della posta in arrivo vengono convertiti in ticket.
- I ticket non possono essere assegnati a utenti non presenti in Portale di gestione, perché non sarà disponibile alcuna associazione con un indirizzo e-mail.
- Una volta elaborato un messaggio e-mail, Advanced Automation (PSA) lo sposta in una cartella di archivio (il messaggio non viene eliminato).
  - Se non è presente alcuna cartella di archivio, verrà creata al momento.
  - Se si utilizza un server di posta diverso da Office 365 o Gmail, verificare che supporti RFC 6851.

Per accedere alle impostazioni del server di posta, passare a **Impostazioni > Service Desk > Configurazione del server di posta**.

Nota
La configurazione del server di posta per le fatture in uscita e i ticket in entrata è disponibile solo quando il servizio Advanced Automation (PSA) è attivato. Questa funzionalità è accessibile anche al primo onboarding in Advanced Automation (PSA), come descritto in "Attivazione di Advanced Automation (PSA)" (pag. 203).

Definizione delle impostazioni e-mail in uscita

Nota
Contattare l'amministratore del servizio e-mail per i dettagli di configurazione del server di posta.

1. Passare a **Impostazioni** > **Service Desk** > **Configurazione del server di posta**.
2. Nella riga **Impostazioni e-mail in uscita**, fare clic sull'icona della matita.
3. Per abilitare le e-mail in uscita, attivare l'interruttore **Attiva**.
4. Selezionare il tipo di protocollo del server di posta pertinente tra una delle seguenti opzioni:
   - SMTP (predefinito)
   - Exchange
   - Office 365
5. Per abilitare il protocollo SSL, selezionare la casella di controllo **Abilita SSL**. Il protocollo SSL (Secure Sockets Layer) crittografa i messaggi e-mail durante il trasporto ed è supportato solo negli scenari seguenti:
   - Secure (TLS) - StartTLS - Porta 587
   - Secure (SSL) - SSL - Porta 465
6. Inserire il nome dell'host e la relativa porta.
7. Inserire il nome utente e la password dell'account.
8. Nel campo **Da**, immettere il nome utente dell'account. Nella selezione, tenere presente che il protocollo Office 365 supporta gli indirizzi e-mail alias in una singola casella di posta. Se si desidera utilizzare uno di questi indirizzi come indirizzo del mittente, utilizzare questo campo. Vengono utilizzati solo gli indirizzi e-mail associati all'account Office 365. Il sistema non effettua lo spoofing degli indirizzi.
9. Inserire il valore del **Timeout** espresso in millisecondi. Questo valore specifica per quanto tempo il sistema attende la riuscita della connessione al server di posta prima del timeout. Se si utilizza un tipo di protocollo SMTP, selezionare la casella di controllo **Richiede autenticazione**.
10. Fare clic su **Prova connessione** per verificare le impostazioni e-mail in uscita. Il sistema convalida tutte le impostazioni e quindi visualizza un messaggio di conferma.
11. Fare clic su ✓ per applicare le impostazioni.

    È inoltre possibile definire le impostazioni per le e-mail delle fatture da inviare ai clienti (consultare "Definizione delle impostazioni e-mail per le fatture in uscita" (pag. 219)) e le

impostazioni per le e-mail in arrivo (consultare "Definizione delle impostazioni per le e-mail in arrivo" (pag. 220)).

Definizione delle impostazioni e-mail per le fatture in uscita

Nota
Contattare l'amministratore del servizio e-mail per i dettagli di configurazione del server di posta.

Le impostazioni per l'e-mail della fattura consentono di configurare il server di posta con cui inviare le fatture ai clienti.

Per definire le impostazioni e-mail per la fattura

1. Passare a **Impostazioni > Service Desk > Configurazione del server di posta**.
2. Nella riga **Impostazioni e-mail fattura**, fare clic sull'icona della matita.
3. Per abilitare le e-mail per le fatture in uscita, attivare l'interruttore **Attiva**.
4. Selezionare il tipo di protocollo del server di posta pertinente tra una delle seguenti opzioni:
   - SMTP (predefinito)
   - Exchange
   - Office 365
5. Per abilitare il protocollo SSL, selezionare la casella di controllo **Abilita SSL**. Il protocollo SSL (Secure Sockets Layer) crittografa i messaggi e-mail durante il trasporto ed è supportato solo negli scenari seguenti:
   - Secure (TLS) - StartTLS - Porta 587
   - Secure (SSL) - SSL - Porta 465
6. Inserire il nome dell'host e la relativa porta.
7. Inserire il nome utente e la password dell'account.
8. Nel campo **Da**, immettere il nome utente dell'account. Nella selezione, tenere presente che il protocollo Office 365 supporta gli indirizzi e-mail alias in una singola casella di posta. Se si desidera utilizzare uno di questi indirizzi come indirizzo del mittente, utilizzare questo campo. Vengono utilizzati solo gli indirizzi e-mail associati all'account Office 365. Il sistema non effettua lo spoofing degli indirizzi.
9. Inserire il valore del **Timeout** espresso in millisecondi. Questo valore specifica per quanto tempo il sistema attende la riuscita della connessione al server di posta prima del timeout. Se si utilizza un tipo di protocollo SMTP, selezionare la casella di controllo **Richiede autenticazione**.
10. Fare clic su **Prova connessione** per verificare le impostazioni e-mail in uscita. Il sistema convalida tutte le impostazioni e quindi visualizza un messaggio di conferma.
11. Fare clic su ✓ per applicare le impostazioni.

    È inoltre possibile definire le impostazioni per le e-mail in uscita (consultare "Definizione delle impostazioni e-mail in uscita" (pag. 218)) e le e-mail in arrivo (consultare "Definizione delle impostazioni per le e-mail in arrivo" (pag. 220)).

Definizione delle impostazioni per le e-mail in arrivo

Nota
Contattare l'amministratore del servizio e-mail per i dettagli di configurazione del server di posta.

Le impostazioni per l'e-mail in arrivo consentono di configurare il server di posta per ricevere le e-mail dai clienti. Advanced Automation (PSA) converte automaticamente queste e-mail in ticket e li assegna all'utente o all'azienda pertinenti.

Importante
Se l'integrazione e-mail è attivata, Advanced Automation (PSA) gestisce la casella di posta in arrivo dell'account specificato. Qualsiasi messaggio non letto viene automaticamente elaborato e spostato nella cartella Archivio.

Per definire le impostazioni delle e-mail in arrivo

1. Passare a **Impostazioni > Service Desk > Configurazione del server di posta**.
2. Nella riga **Impostazioni e-mail in arrivo**, fare clic sull'icona della matita.
3. Per abilitare le e-mail in arrivo, attivare l'interruttore **Attiva**.
4. Selezionare il tipo di protocollo del server di posta pertinente tra una delle seguenti opzioni:
   - IMAP (predefinito)
   - Exchange
   - Office 365
5. Per abilitare il protocollo SSL, selezionare la casella di controllo **Abilita SSL**. Il protocollo SSL (Secure Sockets Layer) crittografa i messaggi e-mail durante il trasporto ed è supportato solo negli scenari seguenti:
   - Secure (TLS) - StartTLS - Porta 587
   - Secure (SSL) - SSL - Porta 465
6. Inserire il nome dell'host e la relativa porta.
7. Inserire il nome utente e la password dell'account.
8. Inserire il valore del **Timeout** espresso in millisecondi. Questo valore specifica per quanto tempo il sistema attende la riuscita della connessione al server di posta prima del timeout.
9. Selezionare la casella di controllo **Elabora i messaggi da utenti sconosciuti** per garantire la conversione dei messaggi provenienti da utenti sconosciuti; questi ticket, tuttavia, non verranno assegnati automaticamente a un utente o a un'azienda. Se l'opzione non viene selezionata, le e-mail provenienti da un indirizzo non presente nel database dei clienti non vengono convertite in ticket.
10. Selezionare la casella di controllo **Non elaborare i messaggi ricevuti prima della data specificata** per garantire che vengano creati i ticket solo per le e-mail ricevute dopo una data specificata. Questa opzione impedisce la creazione automatica dei ticket per tutte le e-mail

esistenti, incluse quelle ricevute prima di aver definito le impostazioni delle e-mail in arrivo. Dopo aver selezionato la casella di controllo vengono visualizzati i campi relativi alla data e all'ora.

11. Fare clic su **Prova connessione** per verificare le impostazioni delle e-mail in arrivo. Il sistema convalida tutte le impostazioni e quindi visualizza un messaggio di conferma.
12. Fare clic su ✓ per applicare le impostazioni.

    È inoltre possibile definire le impostazioni per le e-mail delle fatture inviate ai clienti (consultare "Definizione delle impostazioni e-mail per le fatture in uscita" (pag. 219)) e le impostazioni per le e-mail in uscita (consultare "Definizione delle impostazioni e-mail in uscita" (pag. 218)).

Gestione del Service Desk, dei progetti e delle voci orario

Nel modulo **Gestione attività** di Advanced Automation (PSA) è possibile gestire il Service Desk, i progetti e le voci orario.

- **Service Desk**: per gestire le richieste del servizio clienti, pianificare e tenere traccia delle attività di assistenza.
- **Progetti**: gestire i progetti, le fasi e i passaggi che compongono un progetto e fatturare ai clienti le attività del progetto.
- **Voci orario**: per gestire le registrazioni orario, approvare i ticket orario da fatturare, richiedere giorni liberi e approvare le richieste di ferie come utente amministratore o responsabile.

Nota
È inoltre possibile utilizzare l'applicazione mobile dedicata, benché più limitata ("Acronis Advanced Automation (PSA)", reperibile su App Store e Google Play Store), per operare con i ticket del Service Desk e le voci orario. Nell'applicazione mobile non sono disponibili i progetti.

Service Desk

Il modulo **Service Desk** consente di creare, aggiornare e pianificare i ticket.

Per accedere alle funzionalità di Service Desk, nel portale di gestione passare a **Gestione attività > Service Desk**. Dalle due schede (**Ticket** e **Strumento di pianificazione**), è possibile visualizzare i ticket dell'intera organizzazione e i relativi stati, oltre alle valutazioni dei clienti. È anche possibile:

- Creare nuovi ticket
- Rivedere e aggiornare i ticket correnti
- Unire ticket
- Creare e modificare filtri per ticket personalizzati
- Pianificare i ticket
- Esportare i dati dei ticket

Nota
Gli utenti a cui sono stati assegnati i ruoli Cliente o Responsabile clienti potranno accedere in modo limitato alla funzionalità Service Desk illustrata in precedenza. Potranno rivedere, creare e modificare i ticket (con alcune limitazioni come descritto nella Guida dell'amministratore del cliente). Potranno inoltre esportare i dati dei ticket come richiesto, ma non pianificare o unire i ticket.

Creazione e aggiornamento dei ticket

Advanced Automation (PSA) crea e aggiorna i ticket del Service Desk da più fonti. Oltre a creare e aggiornare i ticket manualmente nel portale di gestione, gli utenti (o richiedenti), possono creare ticket tramite il portale pubblico dei ticket e tramite avvisi RMM integrati.

Creazione dei ticket

Per la creazione dei ticket in Advanced Automation (PSA) sono disponibili quattro opzioni:

- I ticket vengono creati manualmente dai clienti o dagli MSP utilizzando il portale di gestione. Per ulteriori informazioni, consultare "Creazione di un nuovo ticket" (pag. 223).
- I ticket vengono creati a partire da un messaggio e-mail in entrata:
  - Viene identificato un nuovo messaggio e-mail non letto di un nuovo thread.
  - Viene identificato un nuovo messaggio non letto di un thread e-mail esistente, ma un ticket associato risulta già chiuso.
  - Un richiedente viene identificato tramite l'indirizzo e-mail.
  - Un richiedente non viene identificato tramite l'indirizzo e-mail, ma le impostazioni delle e-mail in arrivo (consultare "Definizione delle impostazioni per le e-mail in arrivo" (pag. 220)) consentono l'invio di ticket da parte di utenti sconosciuti.
- I ticket vengono creati tramite il portale pubblico dei ticket, quando configurato a tal fine (consultare "Impostazione dei valori predefiniti" (pag. 319)). Al portale dei ticket gli utenti possono accedere senza registrarsi né accedere al sistema (consultare Invio di ticket del Service Desk tramite il portale dei ticket).
  - Se l'indirizzo e-mail è riconosciuto dal sistema o il provider ha selezionato di non limitare le richieste da utenti non registrati, il ticket viene creato.
  - Se l'indirizzo e-mail non viene riconosciuto e il provider ha selezionato di non elaborare le richieste degli utenti non registrati, il ticket non viene creato.
- I ticket vengono creati a partire da avvisi RMM integrati:
  - I ticket vengono creati automaticamente se per l'integrazione RMM è abilitata la sincronizzazione bidirezionale tra avvisi e ticket.
  - I ticket vengono creati manualmente da avvisi Cyber Protect Cloud tramite la console di Cyber Protect.

  Quando i ticket vengono creati da avvisi RMM, e-mail in arrivo o tramite il portale pubblico dei ticket, vengono applicati i seguenti valori predefiniti:

- Se il richiedente non è identificato, vengono utilizzati i valori predefiniti del Service Desk (vedere "Impostazione dei valori predefiniti" (pag. 319)).
- Se un ticket viene creato da un avviso RMM, tre valori predefiniti (**SLA predefinito**, **Categoria** e **Priorità**) vengono presi dalle impostazioni RMM predefinite (vedere "Definizione delle impostazioni per l'integrazione dei ticket RMM predefiniti" (pag. 324)).
- Se il richiedente è identificato, il nuovo ticket viene associato alle impostazioni del Service Desk dell'azienda, SLA predefinito, priorità predefinita, categoria predefinita, utente di supporto predefinito e ogni dispositivo collegato a questo specifico utente.

Aggiornamento dei ticket

Per l'aggiornamento dei ticket in Advanced Automation (PSA) sono disponibili tre opzioni:

- È possibile aggiornare manualmente i ticket (consultare "Aggiornamento dei ticket" (pag. 226)).
- Tramite un messaggio e-mail in entrata, viene identificato un nuovo messaggio non letto di un thread e-mail esistente e il ticket corrispondente non è chiuso.
- I ticket possono essere aggiornati automaticamente da avvisi collegati da RMM integrato o da avvisi Cyber Protect Cloud.

Creazione di un nuovo ticket

In Advanced Automation (PSA) i ticket vengono creati automaticamente (consultare "Creazione e aggiornamento dei ticket" (pag. 222)), ma è anche possibile creare un ticket manualmente attenendosi alla procedura descritta di seguito.

Nota
Quando si crea un ticket, molti valori vengono pre-compilati utilizzando le impostazioni predefinite del Service Desk. È possibile aggiornare queste informazioni all'occorrenza e come descritto in "Impostazioni di Service Desk" (pag. 314).

Per creare un nuovo ticket

1. Passare a **Gestione attività > Service Desk**. La scheda **Ticket**, che elenca tutti i ticket correnti dell'organizzazione, è visualizzata per impostazione predefinita.

2. Fare clic su **+ Nuovo ticket**. Viene visualizzata la schermata Crea nuovo ticket.

Nota
Se il modulo Advanced Automation (PSA) è attivato per l'account, è anche possibile fare clic su **Nuovo > Ticket cliente** nella barra degli strumenti del portale di gestione posizionata nella parte superiore dello schermo, anche se l'utente non si trova nel modulo Service Desk. Questa opzione apre automaticamente la finestra di dialogo Crea nuovo ticket, tramite la quale è possibile creare un ticket come descritto nei passaggi seguenti.

3. Nella riga di intestazione, è visualizzato il timer del ticket. Questo timer può essere messo in pausa e avviato a seconda delle esigenze dagli addetti che lavorano sul ticket. È anche possibile impostare il timer del ticket affinché venga messo in pausa in automatico se l'utente abbandona temporaneamente la schermata del ticket (consultare "Impostazione dei valori predefiniti" (pag. 319)).

Oltre al timer del ticket, è possibile selezionare le seguenti caselle di controllo, a seconda delle esigenze.

- **Fatturabile**: selezionata per impostazione predefinita, questa opzione indica se il ticket è fatturabile. In base allo SLA applicato al ticket (vedere i passaggi seguenti), la casella di controllo può essere selezionata o deselezionata; in uno SLA di tipo **Calcolo successivo**, ad esempio, la casella di controllo è selezionata, per garantire che il lavoro indicato nel ticket sia fatturabile. In uno SLA di tipo **Prezzo fisso**, la casella di controllo è deselezionata, per garantire che qualsiasi lavoro effettuato sul ticket non sia fatturabile.
- **Invia al cliente via e-mail**: selezionata per impostazione predefinita, questa opzione indica se gli aggiornamenti del ticket vengono inviati all'utente finale tramite e-mail.

4. Definire quanto segue:
   - Nel campo **Titolo del ticket**, aggiungere il titolo del ticket.
   - Nella sezione **Informazioni cliente**, aggiungere i dettagli, incluso l'utente finale che ha richiesto il ticket e il rispettivo responsabile. Fare clic sul campo **Utente finale** per selezionare l'utente dall'elenco visualizzato; gli altri campi vengono compilati automaticamente dove necessario.
   - Nella sezione **Elemento o servizio della configurazione**, selezionare una tra le opzioni **Servizio gestito** o **Servizio ICT**.
     - **Servizio gestito**: questa opzione viene selezionata e precompilata con i dettagli corrispondenti se nel contratto è disponibile il tipo di prodotto Servizio gestito. Quando l'opzione è selezionata, individuare la parte del contratto alla quale è assegnato il dispositivo, quindi verificare lo SLA su tale parte del contratto e applicarla al ticket. L'opzione è disabilitata se nel contratto non è presente il tipo di prodotto Servizio gestito.
     - **Servizio ICT**: Questa opzione viene selezionata e precompilata con i dettagli corrispondenti se nel contratto è disponibile il tipo di prodotto Servizio ICT (Information and Communication Technology). Quando l'opzione è selezionata, lo SLA presente nella parte

del contratto del servizio ICT viene applicato al ticket. L'opzione è disabilitata se nel contratto non sono presenti tipi di prodotto Servizio ICT.

- Il campo **Articolo di configurazione** mostra i dispositivi collegati al servizio ICT o al servizio gestito selezionato (viene visualizzata la voce **Elemento della configurazione sconosciuto** se non sono presenti integrazioni o se il dispositivo è sconosciuto); è facoltativo selezionare un dispositivo dopo aver selezionato un servizio (quando si seleziona un dispositivo in questo scenario, lo SLA non cambia e resta quello appartenente al servizio).

  Se l'elemento della configurazione è stato collegato a uno specifico utente (consultare "Visualizzazione di elementi di configurazione" (pag. 335)), il dispositivo corrispondente viene automaticamente associato al ticket quando questo viene creato.

  Nota
  I dispositivi elencati includono quelli con i prodotti e i servizi Acronis (ad esempio Cyber Disaster Recovery Cloud e Cyber Protection) e le integrazioni RMM. Se il prodotto Acronis o l'integrazione RMM fornisce un'opzione di controllo remoto per un dispositivo in elenco, è possibile connettersi da remoto direttamente dal ticket utilizzando il protocollo RDP o il client HTML5.

- Nei campi **Priorità** e **SLA**, selezionare la priorità del ticket e lo SLA pertinenti.

- Nella sezione **Agente di supporto**, selezionare l'utente specifico da assegnare al ticket (è impostato di default l'utente o il tecnico attuale). Se necessario, è inoltre possibile selezionare una **Categoria** e un **Gruppo di supporto** per il ticket.

  Puoi impostare il ticket come "non assegnato" selezionando **Gruppo di supporto** > **Pool di ticket**. Ciò significa che fino a quando il ticket non viene assegnato a qualcuno, viene considerato non assegnato e visualizzato come tale nella scheda **Ticket**, nei dashboard e nei report.
- Nella sezione **Descrizione ticket**, è possibile:
  - Selezionare lo **Stato** del ticket (per impostazione predefinita è visualizzato lo stato **Nuovo**).
  - Aggiungere i destinatari pertinenti nei campi **A**, **Cc** e **Ccn**. È possibile aggiungere un massimo di 20 destinatari in ciascun campo.

    Se il campo **Utente finale** è stato definito (vedere sopra), il destinatario selezionato non può essere rimosso dal campo **A**.

    Nota
    L'applicazione mobile Acronis Advanced Automation (PSA) non mostra i campi **A**, **Cc** e **Ccn**. Tuttavia, sono supportate le notifiche ai destinatari in **A**, **Cc** e **Ccn** quando il ticket viene aggiornato. Queste notifiche vengono inviate se la casella di controllo **Invia al cliente via e-mail** è selezionata.

  - Aggiungere descrizioni e commenti formattati alla casella di testo visualizzata, incluse immagini e altri file multimediali per un massimo di 25 MB. Nella casella di testo è possibile aggiungere oppure trascinare e rilasciare tutti i formati e i tipi di file seguenti:

- File multimediali: .avi, .mp4, .mp3
- E-mail: .eml, .msg
- Immagini: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
- Documenti e file di registro: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
- Archivi: .zip, .rar

◦ Nel campo **Risposta definita**, fare clic per selezionare una delle risposte predefinite. Tenere presente che se si seleziona una risposta predefinita, questa sostituirà la descrizione e i commenti formattati (vedere il punto precedente). Per ulteriori informazioni sulla definizione delle risposte definite, consultare "Creazione di una risposta definita" (pag. 314).

◦ Nel campo **Tipo di attività di fatturazione**, selezionare il nome del prodotto pertinente. Sono disponibili soltanto i prodotti ai quali è assegnato l'attributo **Prodotto per fatturazione di ticket basata su attività**.

La sezione **Descrizione ticket** può essere impostata su obbligatoria nelle impostazioni del Service Desk (consultare "Impostazioni di Service Desk" (pag. 314)).

- Nella sezione **Pianificazione**, selezionare l'opzione **Pianifica ticket** per pianificare il ticket con l'orario e la data di inizio, e la durata. Vedere anche "Pianificazione dei ticket" (pag. 228).

  Quando l'opzione **Pianifica ticket** è abilitata, è possibile abilitare anche l'opzione **Ticket ricorrenti** per definire una pianificazione ricorrente per questo ticket. Per ulteriori informazioni, consultare "Definizione di ticket ricorrenti" (pag. 230).
- Nella sezione **Allegati**, fare clic per aggiungere qualsiasi allegato desiderato.
- Nella sezione **Elementi fatturabili**, fare clic per aggiungere i prodotti ticket pertinenti da collegare al ticket.
- Nella sezione **Note interne**, fare clic per aggiungere note e azioni.

5. Fare clic su **Crea**. Una volta generato il ticket, questo viene aggiunto alla scheda **Ticket**.

Nota
Dopo aver creato i ticket, è possibile esportare i dati dei ticket in qualsiasi momento facendo clic su **Esporta** nella scheda **Ticket**. Un file di Excel viene automaticamente scaricato nel workload.

Aggiornamento dei ticket

Per aggiornare un ticket

1. Passare a **Gestione attività > Service Desk**. La scheda **Ticket** è visualizzata per impostazione predefinita.
2. (Facoltativo) In presenza di un numero elevato di ticket, utilizzare il filtro per individuare i ticket a cui si è interessati.

   Fare clic su **Filtra** (o su **Filtri salvati** se è stato precedentemente definito un filtro) e selezionare i valori pertinenti dai campi visualizzati. È possibile fare clic sull'opzione **Aggiungi a filtri salvati**

per salvare il filtro definito e utilizzarlo successivamente. Advanced Automation (PSA) viene distribuito con una serie di filtri predefiniti, che possono essere selezionati come necessario.

In alternativa, utilizzare la barra **Cerca** per individuare i ticket pertinenti.

3. Fare clic sul collegamento alla riga Ticket nella scheda **Ticket**.

   Per modificare in blocco una serie di ticket, selezionare i ticket nella scheda **Ticket** e quindi fare clic su **Modifica in blocco**. Le modifiche apportate vengono applicate a tutti i ticket selezionati.

   Per aprire un ticket specifico in una nuova scheda del browser, fare clic su  .

4. Modificare il ticket come necessario in una qualsiasi delle schede visualizzate:

   - **Attività**: Visualizza le attività recenti effettuate sul ticket, incluso lo stato corrente e i commenti aggiunti al ticket. In questa scheda è anche possibile unire i ticket (consultare "Unione di più ticket" (pag. 235)) e pianificarli (consultare "Pianificazione dei ticket" (pag. 228)).

     Nella scheda è possibile modificare lo stato del ticket. Ad esempio, impostare lo stato del ticket su **In corso** quando si inizia a lavorare sul ticket o modificarlo in **Chiuso** quando è possibile chiuderlo. Quando lo stato viene impostato su **Chiuso**, al cliente viene inviata un'e-mail con la richiesta di valutare il ticket. Per ulteriori informazioni, consultare "Ricezione dei feedback relativi ai ticket dai clienti" (pag. 236).

     È inoltre possibile modificare qualsiasi aggiornamento precedente effettuato sul ticket; tutti gli aggiornamenti sono elencati nella parte inferiore della scheda **Attività**. Fare clic sull'icona a freccia accanto all'aggiornamento del ticket pertinente, e, nella sezione visualizzata, fare clic sull'icona a matita per modificare la durata e/o i commenti esistenti.

     Nota
     Se lo stato di un ticket generato da un avviso nella console di Cyber Protect viene impostato su **Chiuso**, viene chiuso anche l'avviso nella console di Cyber Protect.

   - **Panoramica**: visualizza le impostazioni generali del ticket nonché dettagli e informazioni di contatto del cliente, che possono essere modificate come necessario. Per ulteriori informazioni, consultare "Creazione di un nuovo ticket" (pag. 223).

     Nella sezione **Agente di supporto**, è possibile impostare un ticket su "non assegnato" selezionando **Gruppo di supporto** > **Pool di ticket**. Tuttavia, se si aggiorna un ticket assegnato al **Pool di ticket** ma non si riassegna il ticket a un altro utente, il ticket viene automaticamente assegnato all'utente.

     È possibile modificare i dispositivi collegati a un ticket; ad esempio, se è stato creato un ticket che non include il dispositivo corretto, è possibile fare clic sull'elenco a discesa **Articolo di configurazione** per selezionare il dispositivo pertinente.

     In alternativa, fare clic su **Apri desktop remoto** per avviare la connessione remota al dispositivo selezionato, oppure su **Passa al dispositivo** per visualizzare le ulteriori opzioni disponibili per il dispositivo attualmente connesso. Queste opzioni prevedono l'accesso alla piattaforma RMM integrata, dove applicabile:

     - **Visualizzazione problemi attivi**: apre un elenco esterno dei problemi riscontrati nella piattaforma RMM.

- **Pagina Dispositivo - Scheda Stato**: apre una pagina RMM esterna contenente le informazioni generiche sul dispositivo.
- **Pagina Dispositivo - Scheda Proprietà**: apre una pagina RMM esterna contenente le proprietà del dispositivo.

Nota
Al momento, solo le integrazioni Datto RMM, N-able N-Central e N-able RMM supportano l'opzione per la connessione remota al dispositivo selezionato. Per i dispositivi gestiti tramite la piattaforma Acronis (ad esempio con un agente Acronis), è possibile navigare direttamente ai dettagli del dispositivo collegato a partire da un ticket e rivederne le informazioni, avviare una connessione remota (se applicabile e se è consentito dal dispositivo), gestire il dispositivo e così via.

- **Elementi fatturabili**: visualizza tutti gli elementi fatturabili applicati al ticket, che possono essere aggiornati come necessario. Al ticket è possibile aggiungere dei prodotti. Una volta chiuso il ticket ed elaborato l'orario di lavorazione, verrà automaticamente creato un articolo di vendita per il prodotto.
  Questa funzionalità consente di fatturare ai clienti le attività e i servizi extra come parte del ticket stesso. Ad esempio, i servizi di consulenza con tariffa oraria, i cavi di rete o le licenze software. Gli articoli di vendita potranno quindi essere fatturati secondo le modalità standard.
  Tenere presente quanto segue:
  - Solo i prodotti definiti come **Prodotti ticket** nelle impostazioni del prodotto potranno essere aggiunti ai ticket come articoli fatturabili aggiuntivi.
  - È necessario selezionare il prodotto, il prezzo e la quantità.
  - I tecnici non possono modificare il prezzo del prodotto standard se la casella di controllo **Prezzo regolabile dal tecnico** non è selezionata nelle impostazioni del prodotto.
- **Informazioni interne**: visualizza qualsiasi nota o azione interna che è stata applicata al ticket. È possibile aggiungere note o azioni, a seconda della necessità.
- **Ultimi ticket**: (sola lettura) visualizza gli ultimi tre ticket dell'utente specifico, e gli ultimi tre ticket del cliente.

Nota
Le schede **Elementi fatturabili**, **Informazioni interne** e **Ultimi ticket** non sono visualizzabili dagli utenti ai quali sono assegnati i ruoli di Responsabile cliente o Cliente.

Per ulteriori informazioni sui vari campi disponibili quando si modifica un ticket, consultare "Creazione di un nuovo ticket" (pag. 223).

5. Fare clic su **Salva modifiche**.

Pianificazione dei ticket

La scheda **Strumento di pianificazione** visualizza tutti i ticket pianificati per l'utente e, se questo è assegnato al ruolo Responsabile gruppo, per il team. La scheda è ideata per identificare con facilità i

ticket allocati ogni giorno; è possibile modificare la visualizzazione a un formato mensile, settimanale o quotidiano. È anche possibile pianificare i ticket per sé stessi, o, se si è il responsabile di un gruppo, pianificare i ticket per il gruppo.

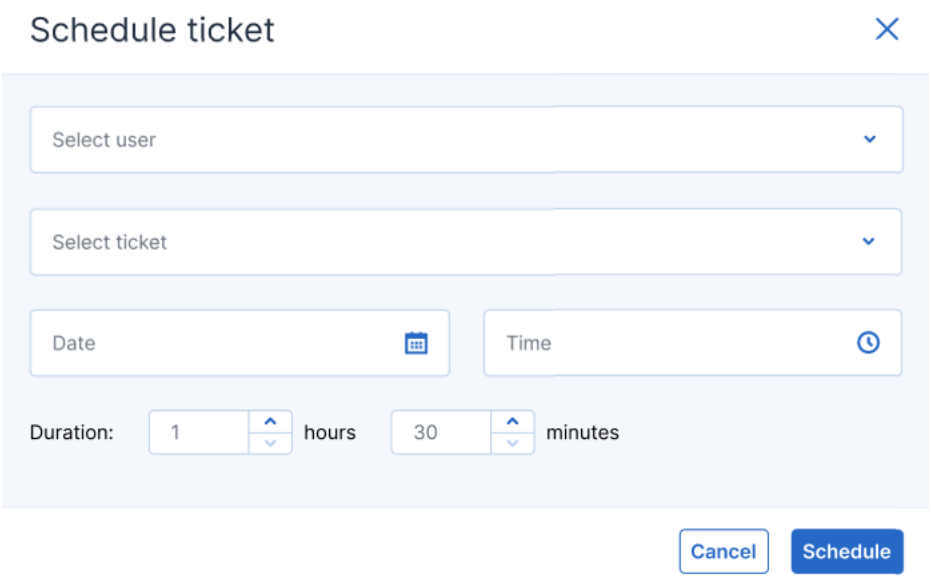
È inoltre possibile pianificare un ticket dal ticket stesso, come descritto di seguito.

Anche la scheda **Strumento di pianificazione** permette di aggiungere nuove registrazioni orario, di approvare o rifiutare le richieste di permesso e di sincronizzare la scheda **Strumento di pianificazione** con il calendario Microsoft Outlook. Se il calendario di Outlook è associato, nella scheda **Strumento di pianificazione** è anche possibile visualizzare gli eventi di Outlook. Per ulteriori dettagli, consultare "Aggiunta di una nuova registrazione orario" (pag. 264) e "Sincronizzazione del calendario con Microsoft Outlook" (pag. 234).

Nota
In Advanced Automation (PSA) è integrato un sistema di gestione dei ticket predittivo. Gestisce i record acquisiti durante un semestre e relativi al tempo dedicato a ogni categoria di ticket, che aggrega per ottenere il tempo di gestione medio per ogni categoria di ticket. Ad esempio, il sistema è in grado di tracciare il tempo dedicato da un tecnico a un ticket con categoria *Workstation* e sottocategoria *Installazione di driver di stampa*. Questa informazione viene mostrata sui ticket attuali per calcolare il tempo necessario al team per elaborarli. La stessa operazione può essere svolta per i singoli utenti, e i valori calcolati sono mostrati anche nella scheda **Strumento di pianificazione**.

Per pianificare un ticket nella scheda Strumento di pianificazione

1. Passare a **Gestione attività > Service Desk**, quindi fare clic sulla scheda **Strumento di pianificazione**.
   La scheda visualizzata mostra diversi tipi di eventi:
   - Registrazioni orario eseguite dai ticket
   - Registrazioni orario definite manualmente in questa scheda
   - Ticket pianificati
   - Notifiche di ferie e permessi per malattia
   - Eventi di calendari di terze parti
2. Selezionare l'utente pertinente dagli elenchi a discesa **Gruppo di supporto** e **Agente di supporto**. Questi elenchi sono disponibili solo ai Responsabili gruppo, ed elencano gli utenti pertinenti con calendari condivisi.
3. Fare clic sul giorno desiderato e quindi su **Pianifica ticket**. Viene visualizzata la schermata Pianifica ticket.



4. Selezionare l'utente pertinente (il proprietario del ticket).
5. Selezionare il ticket da pianificare. È inoltre possibile selezionare un ticket già pianificato per ripianificarlo.
6. Impostare la data, l'ora e la durata prevista del ticket.
7. Fare clic su **Pianificazione**. L'elemento pianificato appena creato è ora visualizzato.
   È possibile aggiornare solo i ticket pianificati e le registrazioni orario manuali.

Per pianificare un ticket dal ticket stesso

1. Passare a **Gestione attività > Service Desk** e creare un nuovo ticket (consultare "Creazione di un nuovo ticket" (pag. 223)) o individuare il ticket pertinente nella scheda **Ticket**.
2. Durante la creazione di un ticket, fare selezionare la casella di controllo **Pianifica ticket** per abilitarlo. Definire quindi l'orario di inizio e la durata stimata del ticket, e, dopo aver completato i campi obbligatori rimanenti nella finestra di dialogo, fare clic su **Fine**.
   Oppure
   Durante la pianificazione di un ticket esistente, fare clic sulla scheda **Attività** del ticket pertinente, quindi selezionare la casella di controllo **Pianifica ticket**. Quindi fare clic su **Salva modifiche**.
   Quando l'opzione **Pianifica ticket** è abilitata, è possibile definire anche una pianificazione ricorrente per il ticket selezionato. Per ulteriori informazioni, consultare "Definizione di ticket ricorrenti" (pag. 230).

Definizione di ticket ricorrenti

Definendo un ticket ricorrente, è possibile automatizzare la creazione di ticket del Service Desk per attività ripetitive.

Ad esempio, è possibile:

- Pianificare un'attività settimanale per esaminare i report sui problemi e fornire aggiornamenti sullo stato.
- Pianificare un'attività mensile per installare gli aggiornamenti del server e inviare un report.
- Pianificare attività annuali per il rinnovo di un dominio e di un certificato SSL.
- Pianificare sessioni di formazione IT annuali per i clienti.

Nota
I ticket ricorrenti sono disponibili solo per i ticket del Service Desk. Non è possibile impostare una pianificazione ricorrente per i ticket di progetto e di preventivo.

Inoltre, i ticket ricorrenti - sia il ticket originale che le sue istanze ricorrenti - sono inclusi nelle dashboard e nei report come parte dei ticket del Service Desk.

Per definire un ticket ricorrente

1. Crea o aggiorna un ticket del Service Desk.
2. [Quando si crea un ticket] Fare clic sulla sezione **Pianificazione** per espanderla, quindi fare clic sull'interruttore dell'opzione **Pianifica ticket** per abilitarla.
   [Quando si aggiorna un ticket] Nella scheda **Attività** del ticket, selezionare la casella di controllo **Pianifica ticket** per espandere la sezione di pianificazione.

   Nota
   Se l'opzione **Pianifica ticket** viene disabilitata nel ticket originale, anche le impostazioni del ticket ricorrente vengono disabilitate.

   Se l'opzione **Ticket ricorrente** viene disabilitata, i ticket precedentemente pianificati per la creazione non verranno creati. Le istanze di ticket ricorrenti non modificate vengono eliminate e rimosse dal sistema. Le istanze di ticket modificati (ad esempio, il ticket è stato riassegnato a un altro utente) vengono salvate come non pianificate. Questi ticket salvati possono essere aggiornati o chiusi solo manualmente.
3. Definire la pianificazione per il ticket. Per ulteriori informazioni, consultare "Pianificazione dei ticket" (pag. 228).
4. Fare clic sull'interruttore dell'opzione **Ticket ricorrente** per abilitarlo.
5. Definisci le impostazioni ricorrenti:
   - Selezionare una data di inizio.

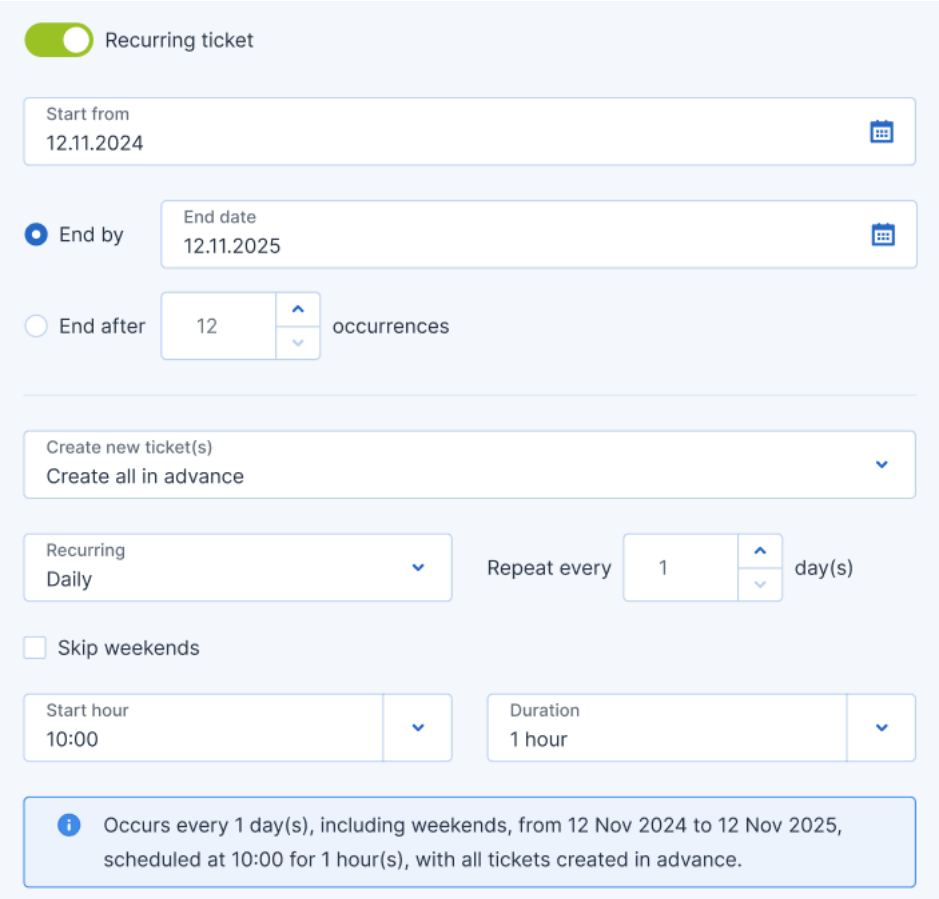
     Nota
     È possibile selezionare una data di inizio nel passato. Tuttavia, le istanze di ticket ricorrenti vengono pianificate solo per il futuro. Di conseguenza, non verranno create le istanze ricorrenti pianificate nel passato (tra la data di inizio e oggi).

- Selezionare l'opzione **Termina entro il** per selezionare una data di fine, oppure selezionare l'opzione **Termina dopo** per terminare la pianificazione ricorrente dopo un determinato numero di occorrenze.
- Selezionare come vengono creati i nuovi ticket ricorrenti da una delle seguenti opzioni:
  - Selezionare **Quando il precedente ticket pianificato viene chiuso** per garantire che il ticket pianificato successivo venga creato solo quando il ticket precedente è chiuso. Il primo ticket viene creato quando si fa clic su **Crea** (il ticket originale non è il primo ticket).
  - Selezionare **Un determinato numero di giorni prima della data pianificata** per garantire che il ticket venga creato un determinato numero di giorni prima della data pianificata. Selezionare il numero di giorni pertinenti a seconda delle necessità.
  - Seleziona **Crea tutti in anticipo** per creare tutti i ticket in anticipo (fino a un massimo di 100). Tutti i ticket saranno disponibili nel tuo calendario facendo clic su **Crea**.
- Dal menu a discesa **Ricorrente**, selezionare **Ogni giorno**, **Ogni settimana**, **Ogni mese** o **Ogni anno**. Quindi definire la frequenza nel campo **Ripeti ogni**. Ad esempio, se si desidera creare un ticket ogni due settimane, selezionare **Ogni settimana**, quindi **2** nel campo **Ripeti ogni**.

  Quando si seleziona **Ogni giorno**, selezionare la casella di controllo **Ignora i fine settimana** per garantire che non venga creato un ticket ricorrente nel fine settimana (sabato e domenica).

  Quando si seleziona **Ogni settimana**, selezionare il/i giorno/i della settimana in cui si desidera venga creato il ticket. Ad esempio, se si desidera che venga creato un ticket tre volte a settimana, selezionare i giorni pertinenti.

  Quando si seleziona **Ogni mese**, selezionare una delle seguenti opzioni:
  - Un giorno specifico del mese. Ad esempio, il 21 di ogni mese. Se un ticket è pianificato per il 31, il ticket viene creato nell'ultimo giorno del mese per i mesi con meno di 31 giorni.
  - Il [primo/secondo/terzo/quarto] [giorno della settimana] del mese. Ad esempio, il secondo mercoledì del mese.
  - L'ultimo [giorno della settimana] del mese. Ad esempio, l'ultimo mercoledì del mese.
  - Il primo giorno del mese.
  - L'ultimo giorno del mese.
- Nei campi **Ora di avvio** e **Durata**, definire l'ora e la durata in cui la pianificazione ricorrente del ticket deve essere eseguita.



6. [Quando si crea un ticket] Fare clic su **Crea**.
   [Quando si aggiorna un ticket] Fare clic su **Salva modifiche**.
   Il ticket iniziale ricorrente è pianificato e può essere visualizzato nella scheda **Strumento di pianificazione**. Anche le istanze ricorrenti del ticket create vengono visualizzate nella scheda **Strumento di pianificazione**.
   Le istanze ricorrenti del ticket sono impostate con lo stato di **Attività pianificate** e includono i dettagli sulla data del prossimo contatto (data dell'istanza del ticket), la data, l'ora e la durata dell'istanza del ticket pianificata, oltre ad altri dettagli impostati nel ticket iniziale.
   Per informazioni sull'aggiornamento di una pianificazione di ticket ricorrenti e delle relative istanze di ticket, consultare "Aggiornamento dei ticket ricorrenti" (pag. 233).

Nota
Le istanze di ticket ricorrenti sono pianificate per una data futura. Non vengono create istanze di ticket pianificate nel passato (prima della data attuale/oggi).

Aggiornamento dei ticket ricorrenti

La pianificazione ricorrente può essere aggiornata o disabilitata solo dal ticket iniziale in cui è stata definita. Le istanze di ticket ricorrenti non possono essere pianificate o rimosse, ma è possibile aggiornare la loro data, ora di inizio e durata.

Tenere inoltre presente quanto segue:

- Quando si aggiorna la pianificazione ricorrente e si devono aggiungere o rimuovere i ticket:
  - Le nuove istanze di ticket vengono create in base alla nuova pianificazione.
  - Le istanze di ticket create che sono state aggiornate (ad esempio, con il tempo registrato, gli utenti riassegnati o lo stato aggiornato) vengono mantenute così come sono. Le nuove istanze di ticket verranno create se non ci sono ticket pianificati nelle date pertinenti nella pianificazione aggiornata.
  - Le istanze di ticket create non ancora aggiornate vengono rimosse dal sistema.
- Se vengono modificati solo i campi **Ora di avvio** e **Durata**:
  - Tutte le istanze di ticket create che non sono state ancora aggiornate verranno aggiornate automaticamente.
  - Le istanze di ticket create che sono state aggiornate vengono mantenute così come sono.
- Qualsiasi altro aggiornamento apportato al ticket originale viene applicato a tutte le nuove istanze di ticket create.

Sincronizzazione del calendario con Microsoft Outlook

È possibile sincronizzare con Microsoft Outlook i ticket nella scheda **Strumento di pianificazione** e condividere il calendario con i colleghi.

Per sincronizzare i ticket con Microsoft Outlook

1. Passare a **Gestione attività > Service Desk**, quindi fare clic sulla scheda **Strumento di pianificazione**.
2. Fare clic su **Sincronizzazione calendario**.
3. Accedere all'account Outlook e abilitare il calendario alla sincronizzazione con Advanced Automation (PSA).
4. Selezionare l'opzione **Condividi il contenuto sincronizzato del calendario con tutti** per condividere il contenuto del calendario con altri utenti di Advanced Automation (PSA).

Approvazione e rifiuto delle richieste di permesso

È possibile approvare o rifiutare le richieste di ferie retribuite o permessi per malattia in sospeso nella scheda **Strumento di pianificazione**.

I giorni di ferie retribuite o i permessi di malattia approvati e in attesa vengono visualizzati nella scheda **Strumento di pianificazione** in tutte le modalità di visualizzazione (**Giorno**, **Settimana** o **Mese**). I giorni approvati e in attesa non vengono sincronizzati con il calendario dell'utente, se l'integrazione del calendario è abilitata.

Nota
Le richieste di permesso vengono visualizzate in base al ruolo di Advanced Automation (PSA). Ad esempio, gli amministratori e i responsabili possono visualizzare le richieste dei propri dipendenti, mentre i dipendenti possono visualizzare solo la propria pianificazione.

Per approvare o rifiutare le richieste di permesso

1. Passare a **Gestione attività > Service Desk**, quindi fare clic sulla scheda **Strumento di pianificazione**.
2. Selezionare l'utente pertinente dagli elenchi a discesa **Gruppo di supporto** e **Agente di supporto**. Questi elenchi sono disponibili solo ai Responsabili gruppo, ed elencano gli utenti pertinenti con calendari condivisi.
3. Nel calendario visualizzato, fare clic sulla richiesta di permesso o permesso di malattia in sospeso e quindi su **Visualizza**.
4. [Facoltativo] Nel pannello di destra, aggiungere una risposta nel campo **Commento** e fare clic su **Salva**.

   Nella sezione **Informazioni sul saldo tempo**, è possibile visualizzare anche il saldo rimanente dell'utente per confermare che siano disponibili i giorni richiesti. È possibile visualizzare anche le richieste di permesso approvate, respinte o non esaminate.
5. Fare clic su **Approva** o **Rifiuta**.

   Il calendario viene aggiornato immediatamente.

   Se una richiesta è stata approvata, il saldo dei giorni liberi rimanenti dell'utente viene aggiornato.

Unione di più ticket

Durante l'aggiornamento di un ticket è possibile scegliere di unirlo a un ticket esistente (che può essere impostato su qualsiasi stato, ma deve essere associato allo stesso cliente e utente finale).

Nota
I ticket impostati con una pianificazione ricorrente non possono essere uniti se sono il ticket originale in cui è definita la pianificazione. Tuttavia, le istanze ricorrenti impostate da questo ticket originale possono essere unite ad altri ticket del Service Desk, come descritto di seguito.

Per unire più ticket

1. Passare a **Gestione attività > Service Desk**.
2. Nella scheda **Ticket** visualizzata, selezionare il ticket da unire.
3. Nella scheda **Attività**, selezionare la casella di controllo **Unisci ticket**.
4. Selezionare il ticket desiderato dall'elenco dei ticket disponibili e fare clic su **Unisci**.
5. Nel messaggio di conferma visualizzato, fare clic su **Unisci**.

Nota
Il ticket originale non è più disponibile e non verrà incluso in alcuna ricerca di ticket attivi o chiusi. Tuttavia, eventuali aggiornamenti o registrazioni di tempo inclusi nel ticket originale vengono aggiunti al ticket unito.

Inoltre, i destinatari selezionati nei campi **A**, **Cc** e **Ccn** del ticket originale vengono aggiunti al ticket unito.

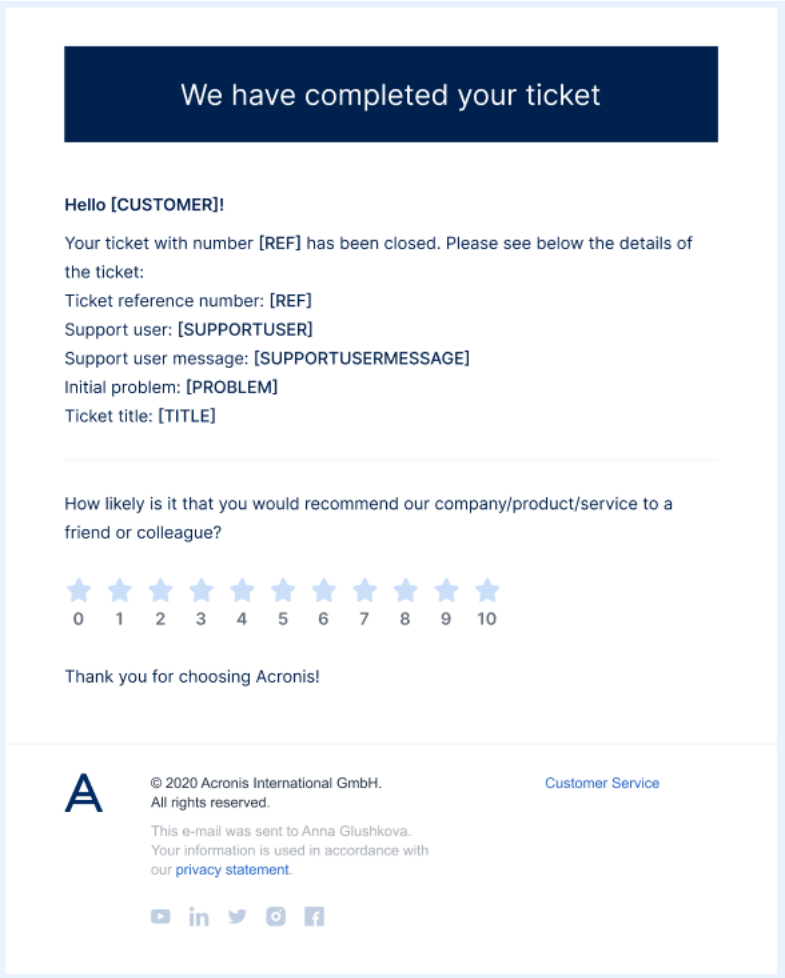
Ricezione dei feedback relativi ai ticket dai clienti

Quando lo stato di un ticket è aggiornato su **Chiuso**, Advanced Automation (PSA) invia automaticamente al cliente un'e-mail con una richiesta di valutazione del ticket. L'e-mail è inclusa per impostazione predefinita in Advanced Automation (PSA) e può essere personalizzata come necessario (consultare "Gestione dei modelli di e-mail" (pag. 324)). L'e-mail viene inviata una sola volta.

Quando il cliente riceve l'e-mail con la richiesta di valutazione del ticket, come mostrato di seguito, può dare la propria valutazione del ticket facendo clic sul voto corrispondente, espresso in stelle. Dopo aver fatto clic sulla classificazione può anche aggiungere un commento. Al termine, il cliente visualizza un messaggio di conferma che lo ringrazia per il feedback e la valutazione.

Per visualizzare il feedback del cliente, passare a **Gestione attività > Service Desk** e individuare il ticket corrispondente. Nella barra laterale destra, fare clic sulla scheda **Panoramica** per visualizzare il feedback.

Nota
I clienti possono inviare le proprie valutazioni del ticket anche senza accedere ai portali di gestione o di Cyber Protect. Inoltre, non devono necessariamente accedere al servizio Advanced Automation (PSA) né disporre di uno specifico ruolo di Advanced Automation (PSA).



Incorporare il modulo di invio ticket nel proprio sito web

È possibile aggiungere un modulo di invio ticket pubblico per i propri clienti finali incorporando il codice iframe incluso nella seguente procedura nel proprio sito web.

Per incorporare il modulo del ticket in un sito web del cliente

1. Nel Portale di Gestione passare a **Impostazioni** > **Service Desk**, quindi fare clic sulla scheda **Valori predefiniti**.
2. Abilitare l'impostazione **Portale dei ticket pubblico**, quindi fare clic su **Salva**.
3. Copiare l'URL del portale.
4. Modificare il proprio sito web con il seguente codice.

> **Nota**
> Sostituire l'URL `src` con l'URL del portale copiato nel passaggio 2.

```
<html>
<body>
<h1>MSP ticket portal</h1>
<iframe title="MSP ticket portal" width="800" height="1000" src="https://portal-url">
</iframe>
```

```
</body>
</html>
```

5. Per verificare che il modulo funzioni, inviare un ticket tramite il modulo.

Progetti

Nel modulo Progetti è possibile creare, pianificare e gestire i progetti.

Utilizzare gli accurati strumenti di pianificazione e monitoraggio del budget del modulo per migliorare la redditività di ogni progetto. Questi strumenti consentono di monitorare con precisione le spese del progetto e lo stato del progetto e di individuare rapidamente ritardi e problemi di budget, potenziali o esistenti. È inoltre possibile emettere le fatture ai clienti interessati utilizzando opzioni di fatturazione flessibili e diversi modelli di fatturazione.

Una volta definiti i dettagli del progetto (consultare "Creazione di un progetto" (pag. 240)), è necessario pianificare fasi e passaggi, ovvero i due elementi principali di ogni progetto:

- **Fasi**: le fasi consistono in tutti i passaggi necessari per completare la fase del progetto. Sono esempi di fasi la pianificazione, la progettazione, l'avvio del progetto e i test finali.
- **Passaggi**: all'interno di una fase è possibile creare più passaggi. Per ogni passaggio viene creato un ticket che viene assegnato al membro del team selezionato.

Per accedere al modulo Progetti, nel portale di gestione passare a **Gestione attività** > **Progetti**.

Nota
I ticket di progetto sono inclusi nella scheda **Service Desk** con i ticket del service desk e dei preventivi, ma differiscono da questi tipi di ticket in quanto vengono creati automaticamente quando si crea un passaggio di progetto. Per ulteriori informazioni, consultare "Lavorare con i ticket del progetto" (pag. 252).

Visualizzazione di progetti

Per visualizzare tutti i progetti, nel portale di gestione, passare a **Gestione attività** > **Progetti**. Nella schermata **Progetti** è possibile visualizzare tutti i progetti del tenant presenti in Advanced Automation (PSA).

Vengono visualizzate le informazioni relative a ogni progetto, incluso:

- Il nome del progetto
- Lo stato corrente del progetto (**Nuovo**, **Avvio in sospeso**, **In corso**, **Ritardato**, **In attesa** o **Completato**)

Nota
Lo stato del progetto viene calcolato in base allo stato dei passaggi e delle fasi del progetto. A ogni stato del passaggio e della fase viene assegnato un valore e lo stato complessivo del progetto viene calcolato in base all'ordine seguente: **In attesa** > **Ritardato** > **In corso** > **Avvio in sospeso** > **Nuovo** > **Completato**.

Ad esempio, se un progetto ha tre fasi negli stati **Avvio in sospeso**, **Ritardato** e **In attesa**, lo stato del progetto viene visualizzato come **In attesa**.

Per impostazione predefinita, non vengono visualizzati i progetti con lo stato **Completato**.

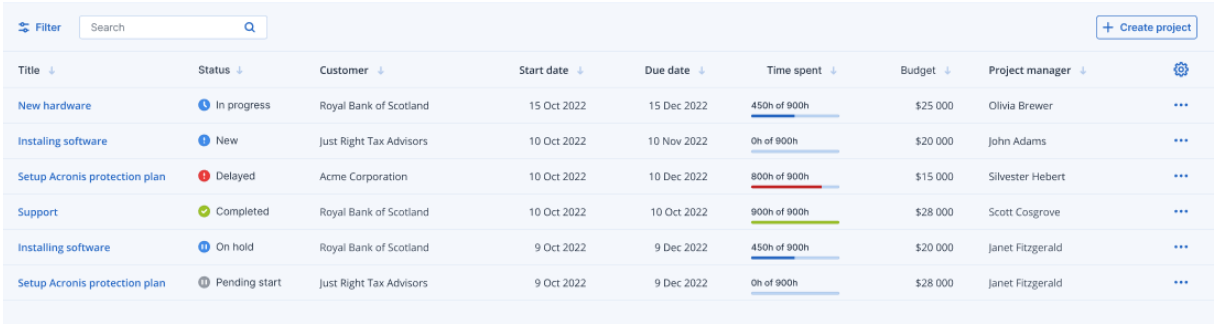
- Il cliente per il quale viene creato il progetto
- Le date di inizio e di scadenza del progetto
- Il tempo impiegato sul progetto da tutti i membri del team del progetto
- Il budget complessivo del progetto

Nota
Si tratta del ricavo previsto per il progetto, calcolato in base alle ore pianificate moltiplicate per il prezzo del prodotto.

- Il responsabile del progetto assegnato

Nella colonna più a destra di ogni riga del progetto, fare clic sull'icona dei puntini di sospensione per aprire, copiare (consultare "Copia di un progetto" (pag. 241)), o eliminare (consultare "Aggiornamento di un progetto" (pag. 243)) il progetto.

È inoltre possibile filtrare e ordinare l'elenco visualizzato per individuare uno specifico progetto; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali progetti devono essere visualizzati.



Per visualizzare il riepilogo di un progetto specifico, fare clic sulla riga del progetto. Nel riquadro di destra è possibile visualizzare un riepilogo degli aspetti finanziari e dello stato di avanzamento correnti del progetto. È inoltre possibile visualizzare se il progetto è a rischio (a causa di un problema di budget o di pianificazione, come indicato dal campo **Integrità del progetto**). Per accedere e modificare il progetto, fare clic sul collegamento **Apri progetto**.

Creazione di un progetto

Una procedura suddivisa in tre fasi principali guida l'utente durante la creazione di un nuovo progetto. Le tre fasi prevedono:

- L'inserimento delle informazioni di base sul progetto
- La definizione del budget del progetto
- La definizione del team del progetto

Al completamento della procedura guidata, il progetto viene automaticamente aggiunto all'elenco dei progetti esistenti visualizzato nella schermata Progetti. I progetti possono essere visualizzati, copiati e aggiornati secondo necessità; come necessario.

Per creare un progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella schermata Progetti, fare clic su **+ Progetto**.
   Se non ci sono progetti esistenti, fare clic su **Crea progetto**.
   Viene visualizzata la procedura guidata **Crea nuovo progetto**.
3. Nella scheda **Informazioni sul progetto**, definire quanto segue:
   - **Titolo del progetto**: il nome del progetto.
   - **Nome cliente**: selezionare il cliente pertinente dall'elenco a discesa.

     Nota
     Se per il cliente selezionato non sono state definite le informazioni di fatturazione, alla procedura guidata per la creazione del progetto viene aggiunto l'ulteriore passaggio **Dati di fatturazione**. Facendo clic su **Avanti**, è possibile completare i campi relativi alle informazioni di fatturazione, inclusi i termini di pagamento e l'indirizzo. Queste informazioni vengono quindi salvate e utilizzate quando si seleziona il cliente in altri moduli di Advanced Automation (PSA). Per ulteriori informazioni sui campi delle informazioni di fatturazione, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47).

   - **Data di inizio**: la data di inizio del progetto.
   - **Data di scadenza**: la data in cui è prevista la fine del progetto.
   - **Responsabile del progetto**: selezionare l'utente pertinente dall'elenco a discesa.
   - **Sponsor del progetto**: selezionare il contatto o l'utente del cliente rilevante dall'elenco a discesa.
   - **Modello di fatturazione**: selezionare uno dei seguenti modelli: **Fattura per passaggio completato**, **Fattura per anticipo sul totale** o **Fattura per obiettivi**. Per ulteriori informazioni, consultare "Fatturazione dei progetti" (pag. 261).
   - [Facoltativo] **Note del progetto**: aggiungere brevi riepiloghi di informazioni importanti del progetto nell'editor di testo.

4. Fare clic su **Avanti**.
5. Nella scheda **Budget del progetto**, selezionare i prodotti rilevanti dall'elenco visualizzato. Questi prodotti possono essere selezionati durante la creazione del progetto o in un momento successivo, quando il progetto è già in corso.

   È possibile modificare il prezzo di un prodotto solo se il campo **Prezzo regolabile per progetto** nelle proprietà del prodotto è impostato su **Sì**. Per ulteriori informazioni sulla configurazione delle proprietà del prodotto, consultare "Aggiunta di un prodotto" (pag. 295).

   Nota
   Per includere un prodotto in un progetto, deve essere definito come prodotto progetto. Per ulteriori informazioni sull'aggiunta di prodotti, consultare "Aggiunta di un prodotto" (pag. 295).
6. Fare clic su **Avanti**.
7. Nella scheda **Team del progetto**, selezionare i membri del team del progetto pertinenti. I membri del team possono essere selezionati ora o in un secondo momento, ma devono essere aggiunti al progetto prima di definirne i passaggi.
8. Se sono stati definiti campi personalizzati da applicare ai progetti, viene visualizzata la scheda **Informazioni aggiuntive**. In questa scheda, definire i campi personalizzati come necessario. Per ulteriori informazioni, consultare "Lavorare con i campi personalizzati" (pag. 213).

   Nota
   Se sono stati definiti campi personalizzati da applicare ai passaggi del progetto, questi vengono visualizzati durante la creazione di un passaggio del progetto. Per ulteriori informazioni, consultare "Aggiunta di fasi al progetto" (pag. 247).
9. Fare clic su **Crea**.

   Il progetto viene aggiunto alla schermata Progetti, dove è possibile definire ulteriori dettagli, ad esempio aggiungere le fasi e i passaggi del progetto. Per ulteriori informazioni, consultare "Gestione dei progetti" (pag. 244).

Copia di un progetto

È possibile copiare un progetto per crearne uno nuovo simile a uno esistente, senza dover creare manualmente tutte le fasi, i passaggi, i membri del team e il budget.

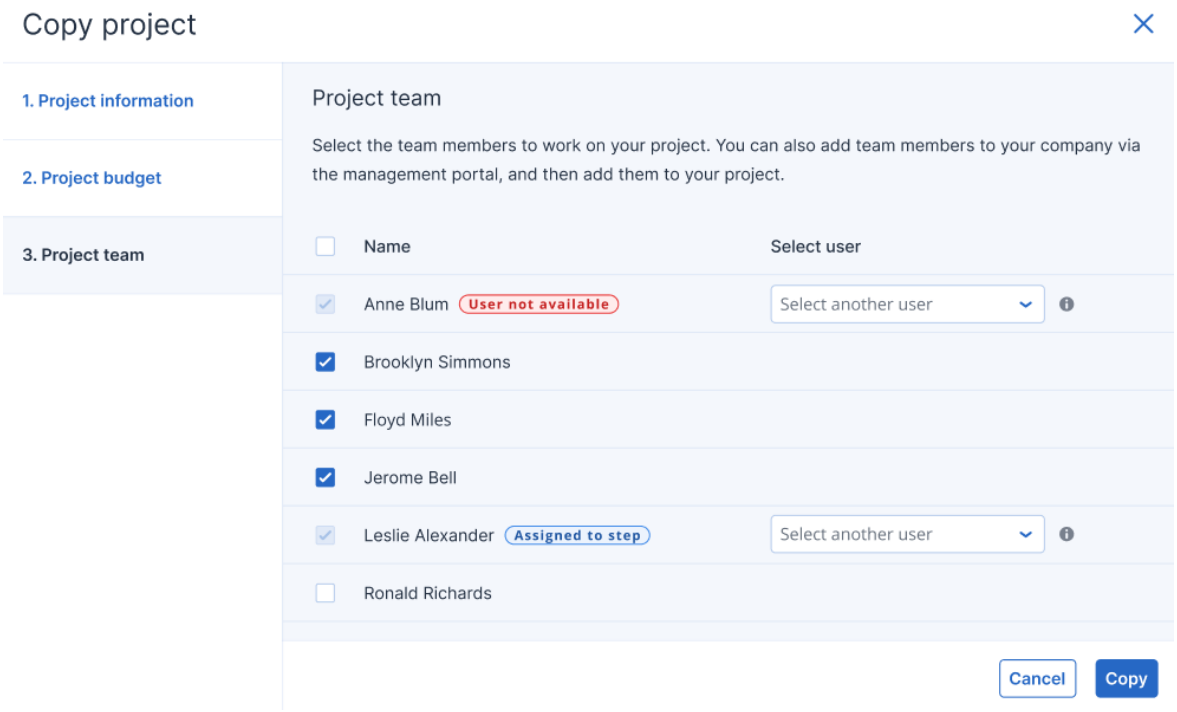
Nota
Quando si copia un progetto, tutti i passaggi del progetto vengono impostati con lo stato **Nuovo**. Inoltre, se il nome del progetto non viene aggiornato, nella schermata Progetti viene visualizzato un nuovo progetto con lo stesso nome. È preferibile modificare il nome del nuovo progetto per evitare confusione.

Per copiare un progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto da copiare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Copia**.
3. Nella scheda **Informazioni sul progetto**, definire la data rilevante nel campo **Data di inizio**.
   Quando viene impostata la data di inizio, il campo **Data di scadenza** viene automaticamente impostato in base alle impostazioni del progetto originale.
   Tutti gli altri campi vengono popolati in base al progetto che si sta copiando.

   Nota
   Se il responsabile del progetto originale non è più disponibile a causa della nuova data di inizio, il sistema chiede di selezionare un nuovo responsabile dal menu a discesa **Responsabile del progetto**.

4. Fare clic su **Avanti**.
5. Nella scheda **Budget del progetto**, definire i prodotti per il progetto.
   Tenere presente quanto segue:
   - I prezzi vengono impostati in base al prezzo del prodotto corrente o al prezzo del prodotto personalizzato per il cliente.
   - Non è possibile rimuovere un prodotto assegnato a uno o più passaggi del progetto.
   - È possibile modificare un prodotto in elenco solo se il campo **Prezzo regolabile per progetto** nelle proprietà del prodotto è impostato su **Sì**. Per ulteriori informazioni sulla configurazione delle proprietà del prodotto, consultare "Aggiunta di un prodotto" (pag. 295).
   - Non è possibile impostare il budget su un valore inferiore al tempo necessario per completare i passaggi del progetto.
   - È possibile aggiungere prodotti aggiuntivi dopo aver copiato il progetto. Per ulteriori informazioni, consultare "Gestione dei progetti" (pag. 244).
6. Fare clic su **Avanti**.
7. Nella scheda **Team del progetto**, selezionare i membri del team del progetto.
   Tenere presente quanto segue:
   - Se uno dei membri del team originale non è disponibile, il sistema chiede di selezionare un altro utente per sostituirlo.
   - È possibile sostituire un membro del team a cui sono state assegnate attività nel progetto copiato. Queste attività verranno assegnate all'utente che sostituisce il membro del team copiato.
   - È possibile aggiungere o rimuovere membri del team dopo aver copiato un progetto. Per ulteriori informazioni, consultare "Gestione dei progetti" (pag. 244).



8. Se sono stati definiti campi personalizzati da applicare ai progetti, fare clic su **Avanti** per visualizzare la scheda **Informazioni aggiuntive**. In questa schermata definire i campi personalizzati come necessario. Per ulteriori informazioni, consultare "Lavorare con i campi personalizzati" (pag. 213).
9. Al termine, fare clic su **Copia**.

   Il progetto copiato viene aggiunto alla schermata Progetti, dalla quale è possibile aprirlo e aggiungere o aggiornare le fasi, i passaggi, il budget e i membri del team. Per ulteriori informazioni, consultare "Gestione dei progetti" (pag. 244).

Aggiornamento di un progetto

È possibile aggiornare ed eliminare i progetti come necessario.

È possibile aggiornare un progetto anche se è impostato come **Completato**. È possibile aggiungere nuovi passaggi al progetto e aggiungere o modificare le ore registrate in un passaggio anche dopo che è stato impostato come **Completato**. Per ulteriori aggiornamenti, ad esempio l'aggiunta o l'aggiornamento di prodotti e l'aggiornamento della pianificazione, è necessario creare un nuovo passaggio. Per ulteriori informazioni, consultare "Aggiunta di passaggi del progetto" (pag. 248).

Importante
Quando si elimina un progetto, vengono eliminati anche tutti gli elementi associati al progetto, ad esempio ticket, articoli di vendita ed elementi pianificati. Solo gli articoli di vendita che sono stati fatturati non vengono eliminati.

Per aggiornare un progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto da aggiornare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. Nella scheda **Dettagli del progetto**, aggiornare il progetto come necessario. Per ulteriori informazioni sui campi e le impostazioni disponibili, consultare "Creazione di un progetto" (pag. 240).

   Quando si aggiorna un progetto alcuni campi non possono essere modificati, ad esempio i campi **Nome cliente**, **Data di inizio** e **Modello di fatturazione**. Il campo **Data di scadenza** non può essere impostato su una data antecedente a uno qualsiasi dei passaggi esistenti.

   Non è inoltre possibile modificare qualsiasi prodotti nel budget assegnato a un passaggio. Se l'impostazione **Prezzo regolabile per progetto** del prodotto è impostata su **No**, il prezzo è disabilitato.

Per eliminare un progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto da eliminare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Elimina**.
3. Nella finestra di dialogo di conferma, fare clic su **Elimina**.

   Il progetto e tutti gli elementi associati al progetto, ad esempio i ticket, gli articoli di vendita e gli elementi pianificati, vengono eliminati.

Nota
Gli articoli di vendita per i quali è stata fattura non vengono eliminati.

Gestione dei progetti

Dopo aver definito i dettagli principali del progetto (consultare "Creazione di un progetto" (pag. 240)), è possibile definire e gestire ulteriori elementi del progetto, tra cui:

- Fasi e passaggi del progetto
- Membri del team del progetto e rispettiva capacità disponibile
- Ticket del progetto

Lavorare con i piani del progetto

Nel piano del progetto vengono definite le fasi e i passaggi del progetto.

Dopo aver creato le fasi e i passaggi del progetto, il piano del progetto fornisce una panoramica dello stato corrente del progetto, incluso l'avanzamento. È inoltre possibile personalizzare la visualizzazione utilizzando una visualizzazione in tabella (predefinita) o a nel formato diagramma di Gantt.

Visualizzazione e comprensione di un piano di progetto

È possibile gestire un progetto in un piano di progetto, che permette di definire e monitorare le fasi e i passaggi del progetto.

Per accedere alla piano del progetto, passare alla scheda **Pianificazione del progetto**. In questa scheda è possibile:

- Visualizzare il piano del progetto in due visualizzazioni diverse: la visualizzazione in tabella o la visualizzazione in diagramma di Gantt. Per ulteriori informazioni, consultare Visualizzazioni dei piani del progetto.
- Aggiungere fasi e passaggi del progetto. Per ulteriori informazioni, consultare "Aggiunta di fasi al progetto" (pag. 247) e "Aggiunta di passaggi del progetto" (pag. 248).
- Aggiornare ed eliminare fasi e passaggi del progetto. Per ulteriori informazioni, consultare "Aggiornamento ed eliminazione delle fasi del progetto" (pag. 249) e "Aggiornamento ed eliminazione di passaggi del progetto" (pag. 251).
- Visualizza lo stato corrente di una fase o di un passaggio (**Completato**, **Nuovo**, **Avvio in sospeso**, **In corso**, **Ritardato** o **In attesa**).
- Visualizzare il membro del team assegnato a un passaggio e qualsiasi relativo problema di capacità che potrebbe mettere a rischio il progetto.
- Visualizzare le date di inizio e di fine di una fase o di un passaggio.
- Visualizzare le ore pianificate per una fase o un passaggio e le ore rimanenti per completare la fase o il passaggio.
- Monitorare l'avanzamento attuale in percentuale di una fase o di un passaggio.

Nota
Il progresso si basa sulla percentuale di lavoro completato, non sul tempo impiegato per il progetto.

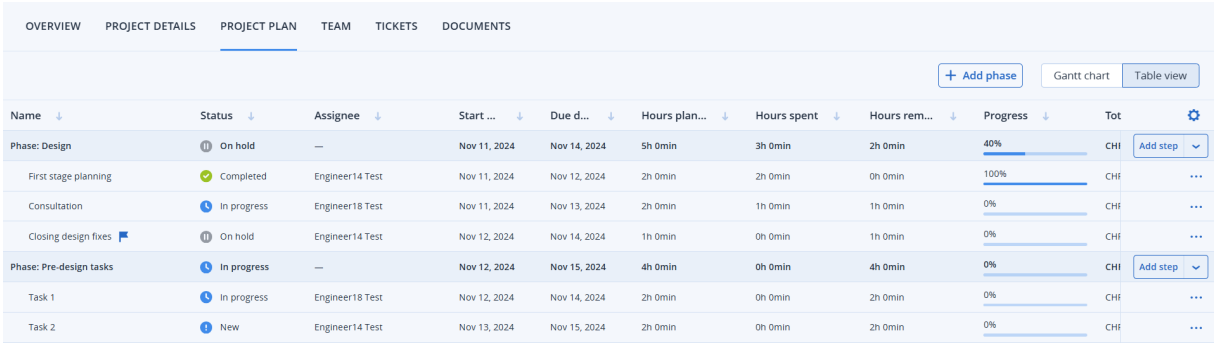
- Visualizzare il valore monetario corrente totale di una fase o di un passaggio, in base ai prodotti del progetto selezionati e alle ore pianificate.
- Fare clic su un collegamento per visualizzare il ticket del passaggio del progetto.

Visualizzazioni del piano del progetto

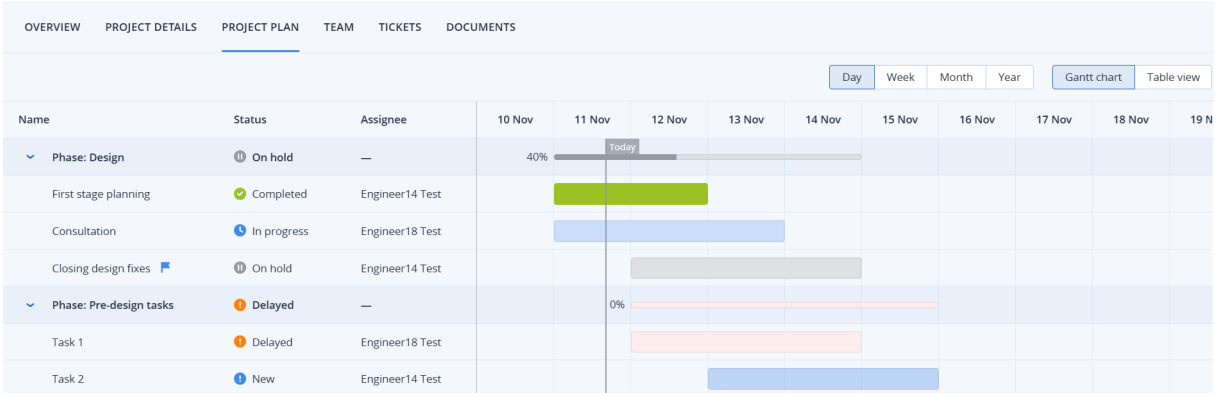
Il piano del progetto può essere visualizzato in due modi diversi, la visualizzazione in tabella (predefinita) o la visualizzazione in diagramma di Gantt. Nella scheda **Pianificazione del progetto**, fare clic su **Visualizzazione tabella** o **Diagramma di Gantt** per visualizzare la versione corrispondente.

Nota
È possibile visualizzare e modificare le fasi e i passaggi in entrambe le visualizzazioni. È possibile aggiungere nuove fasi e nuovi passaggi solo nella visualizzazione in tabella.

La visualizzazione in tabella mostra tutte le colonne disponibili, nonché i pulsanti per aggiungere, visualizzare ed eliminare le fasi e i passaggi del progetto.



La visualizzazione in diagramma di Gantt, come mostrato di seguito, fornisce una visualizzazione grafica del progresso del progetto, consentendo di tenere traccia dello stato delle fasi e dei passaggi e di identificare rapidamente ritardi potenziali o effettivi. È possibile visualizzare il diagramma in quattro periodi diversi: **Giorno**, **Settimana**, **Mese** o **Anno**.



Nota

Nel diagramma di Gantt vengono visualizzate solo le fasi che includono passaggi.

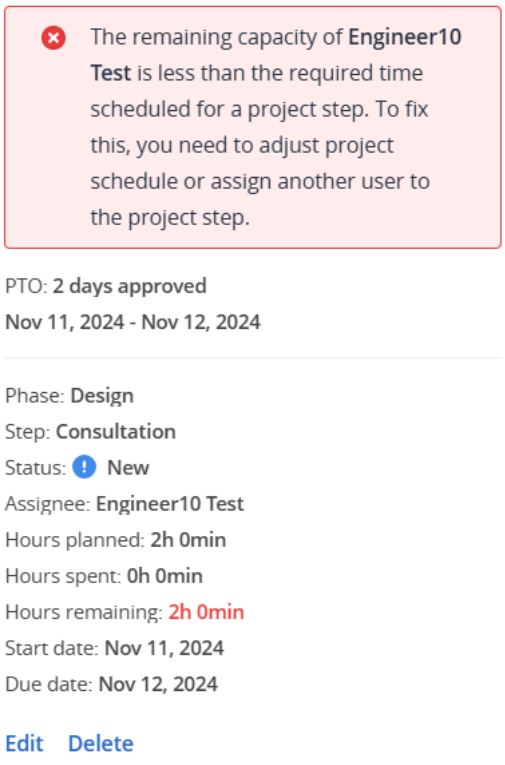
Inoltre, solo le fasi mostrano un'indicazione del progresso della fase (in %). Il progresso dei singoli passaggi non viene mostrato in questa visualizzazione.

Il diagramma di Gantt fornisce una comprensione più grafica di eventuali problemi o ritardi. Nell'esempio precedente viene mostrato un passaggio **Ritardato** (Passaggio 1) e l'impatto che ha sul progetto. Anche la fase è impostata su **Ritardato** e sia la fase che il passaggio sono in evidenza nel diagramma di Gantt.

I passaggi del progetto possono anche essere impostati su **Scaduto** se la data di scadenza del passaggio è trascorsa o se la data in cui il passaggio è stato completato è successiva alla data di scadenza. Inoltre, se uno qualsiasi dei membri del team assegnato ai passaggi del progetto riscontra problemi di capacità, viene evidenziato nel grafico come **Problema relativo alla capacità utente**.

Nota
L'evidenziazione visiva di un problema di un passaggio nel diagramma di Gantt, ad esempio **Scaduto** o **Problema relativo alla capacità utente**, fornisce solo un'indicazione della presenza del problema, ma non implica l'aggiornamento automatico dello stato della fase. Lo stato della fase viene calcolato automaticamente in funzione dello stato dei passaggi, che può essere aggiornato solo manualmente.

Fare clic sul passaggio per visualizzare ulteriori dettagli e regolare i dettagli del passaggio come necessario. Ad esempio, il membro del team assegnato al passaggio potrebbe non avere abbastanza ore disponibili per lavorare al passaggio. Il sistema chiede di regolare la pianificazione del progetto o di assegnare un altro utente al passaggio. Per ulteriori informazioni, consultare "Riassegnazione dei membri del team ai passaggi del progetto" (pag. 257).



Aggiunta di fasi al progetto

È possibile aggiungere fasi a qualsiasi progetto, indipendentemente dallo stato in cui si trova.

Per aggiungere una fase del progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto a cui aggiungere le fasi, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. Fare clic sulla scheda **Piano del progetto**.
4. Se si sta aggiungendo la prima fase al progetto, fare clic su **Crea fase**.

Se si stanno aggiungendo fasi aggiuntive al progetto, fare clic su **Aggiungi fase**.

5. Inserire una descrizione per la fase, quindi fare clic su **Crea**.
   La fase viene aggiunta al progetto corrispondente ed è possibile aggiungere passaggi alla fase. Per ulteriori informazioni, consultare "Aggiunta di passaggi del progetto" (pag. 248).

Nota
Lo stato della fase viene calcolato in base allo stato dei passaggi del progetto. A ogni stato del passaggio viene assegnato un valore e lo stato della fase viene calcolato in base all'ordine seguente: **In attesa** > **Ritardato** > **In corso** > **Avvio in sospeso** > **Nuovo** > **Completato**.

Ad esempio, se una fase ha tre passaggi negli stati **Avvio in sospeso**, **Ritardato** e **In attesa**, lo stato della fase viene visualizzato come **In attesa**.

Aggiunta di passaggi del progetto

È possibile aggiungere passaggi a qualsiasi progetto, indipendentemente dallo stato del progetto.

Per aggiungere un passaggio al progetto

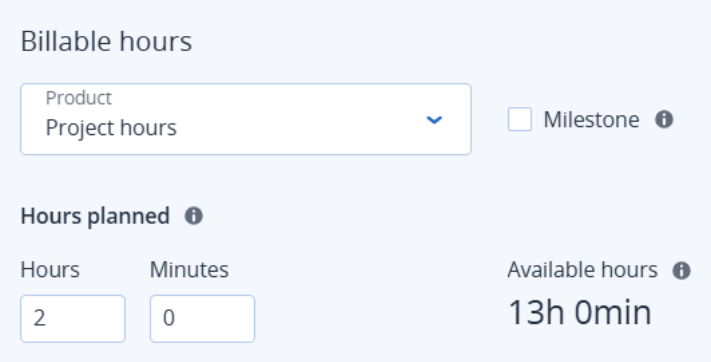
1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto a cui aggiungere i passaggi, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. Nella scheda **Pianificazione del progetto**, fare clic su **Aggiungi passaggio** nella riga del passaggio pertinente.
4. Nella scheda **Informazioni sul passaggio**, definire quanto segue:
   - **Titolo**: il nome del passaggio.
   - **Note**: una descrizione opzionale del passaggio.
   - **Assegnatario**: selezionare il membro del team rilevante dal menu a discesa.
   - **Stato**: selezionare una tra le opzioni **Nuovo** (impostazione predefinita), **In corso**, **Ritardato**, **Avvio in sospeso** o **In attesa** dall'elenco a discesa.
   - **Data di inizio**: definire una data di inizio per il passaggio. La data selezionata inizia alle 00:00:00.

     Nota
     Quando si crea il primo passaggio in un progetto, la data di inizio del progetto viene impostata automaticamente come data di inizio predefinita per il passaggio.

   - **Data di scadenza**: definire una data di scadenza per il passaggio. La data selezionata termina alle 23:59:59.

     Nota
     La data di scadenza del passaggio deve essere compresa tra la data di inizio e la data di scadenza del progetto.

5. Nella sezione **Ore fatturabili**, eseguire le seguenti operazioni:
   - Selezionare il prodotto pertinente da assegnare al passaggio. È possibile selezionare solo i prodotti disponibili nel budget del progetto.
   - Nella sottosezione **Ore pianificate**, definire il numero di ore e minuti necessari per il passaggio. Il numero di ore non deve superare le **Ore disponibili** visualizzate.
   - Se il passaggio deve essere un obiettivo, selezionare la casella di controllo **Obiettivo**. Ciò garantisce che il passaggio venga fatturato automaticamente quando il modello di fatturazione scelto richiede il pagamento di ogni obiettivo completato. Per ulteriori informazioni, consultare "Fatturazione dei progetti" (pag. 261).



6. Se sono stati definiti campi personalizzati da applicare ai passaggi del progetto, viene visualizzata la scheda **Informazioni aggiuntive**. In questa sezione, definire i campi personalizzati come necessario. Per ulteriori informazioni, consultare "Lavorare con i campi personalizzati" (pag. 213).
7. Fare clic su **Salva**.

   In alternativa, fare clic su **Salva questo passaggio e aggiungi un nuovo passaggio** per salvare il passaggio e aggiungerne un altro. Ripetere la procedura sopra descritta, come richiesto.

   Il passaggio salvato viene aggiunto alla fase del progetto corrispondente.

   Viene inoltre creato un ticket del progetto, in cui deve essere registrato il tempo impiegato per il passaggio. Il ticket può essere visualizzato nella scheda **Ticket**. Per ulteriori informazioni, consultare "Lavorare con i ticket del progetto" (pag. 252).

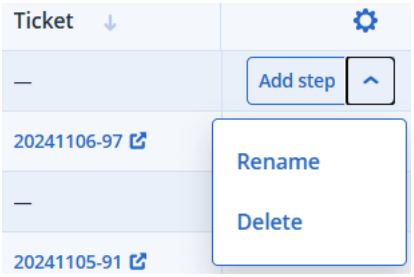
Aggiornamento ed eliminazione delle fasi del progetto

È possibile aggiornare una fase del progetto rinominandola, indipendentemente dallo stato della fase. È possibile rinominare ed eliminare la fase sia nella visualizzazione tabella che nel diagramma di Gantt.

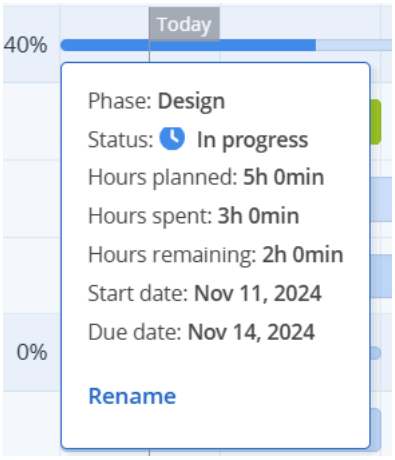
Nota
È possibile eliminare una fase solo se lo stato è impostato su **Nuova**. L'operazione elimina anche tutti i ticket e i tempi registrati del passaggio del progetto.

Per rinominare una fase

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto da eliminare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. [Nella visualizzazione Tabella] Nella scheda **Pianificazione del progetto**, fare clic sull'icona a freccia accanto al menu **Aggiungi passaggio** nella riga della fase del progetto pertinente, quindi selezionare **Rinomina**.



[Nella visualizzazione Diagramma di Gantt] Nella scheda **Pianificazione del progetto**, fare clic su **Diagramma di Gantt**. Fare clic sul nodo della fase pertinente e, nella finestra a comparsa visualizzata, fare clic su **Rinomina**.



4. Nella finestra di dialogo **Rinomina fase**, immettere un nuovo nome per la fase e fare clic su **Rinomina**.

Per eliminare una fase

1. [Nella visualizzazione Tabella] Nella scheda **Pianificazione del progetto**, fare clic sull'icona a freccia accanto al menu **Aggiungi passaggio** nella riga della fase del progetto pertinente, quindi selezionare **Elimina**.

   [Nella visualizzazione Diagramma di Gantt] Nella scheda **Pianificazione del progetto**, fare clic su **Diagramma di Gantt**. Fare clic sul nodo della fase pertinente e, nella finestra a comparsa visualizzata, fare clic su **Elimina**.

   Nota
   Se lo stato della fase del progetto è impostato su qualsiasi valore diverso da **Nuova**, non è possibile eliminarla.

2. Nella finestra di dialogo di conferma, fare clic su **Elimina**.

Vengono eliminati tutti i passaggi (compresi i relativi ticket e il tempo registrato) della fase. Inoltre, lo stato del progetto e le metriche relative al progresso vengono ricalcolate per tenere conto della fase e dei passaggi eliminati.

Aggiornamento ed eliminazione di passaggi del progetto

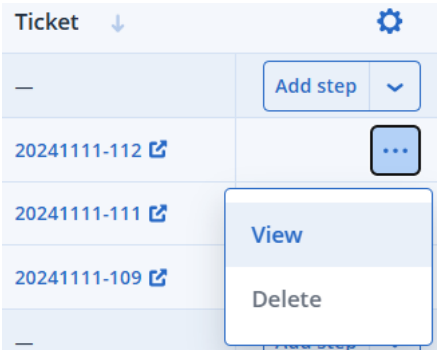
È possibile aggiornare i dettagli di un passaggio del progetto (incluso lo stato, il membro del team assegnato e le date di inizio e di scadenza) e le ore fatturabili per qualsiasi passaggio non impostato come **Completato**. È inoltre possibile eliminare qualsiasi passaggio impostato come **Nuovo**.

È possibile aggiornare ed eliminare i passaggi del progetto sia nella visualizzazione in tabella che nel diagramma di Gantt.

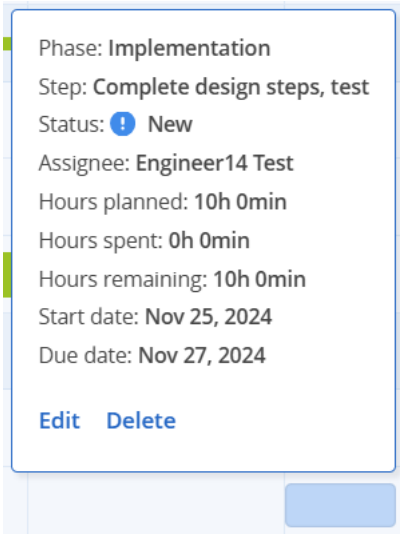
Nota
Se il passaggio del progetto è già in corso o è impostato su uno stato diverso da **Nuovo**, non è possibile eliminarlo.

Per aggiornare un passaggio del progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto da eliminare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. [Nella visualizzazione Tabella] Nella scheda **Pianificazione del progetto**, fare clic sull'icona dei puntini di sospensione nella riga del passaggio del progetto interessato, quindi selezionare **Visualizza**.



[Nella visualizzazione Diagramma di Gantt] Nella scheda **Pianificazione del progetto**, fare clic su **Diagramma di Gantt**. Fare clic sul passaggio della fase pertinente e, nella finestra a comparsa visualizzata, fare clic su **Modifica**.



4. Nel pannello di destra, fare clic sull'icona a matita per aggiornare i campi pertinenti nelle sezioni **Informazioni sul passaggio** e **Ore fatturabili**.

   Per ulteriori informazioni sui campi e le informazioni disponibili, consultare "Aggiunta di passaggi del progetto" (pag. 248).
5. Fare clic su ✓ per confermare le modifiche.

   Le modifiche vengono applicate al ticket esistente del passaggio. Inoltre, le metriche relative allo stato e al progresso del progetto vengono ricalcolate per tenere conto del passaggio aggiornato.

Per eliminare un passaggio del progetto

1. [Nella visualizzazione Tabella] Nella scheda **Pianificazione del progetto**, fare clic sull'icona dei puntini di sospensione nella riga del passaggio del progetto interessato, quindi selezionare **Elimina**.

   [Nella visualizzazione Diagramma di Gantt] Nella scheda **Pianificazione del progetto**, fare clic su **Diagramma di Gantt**. Fare clic sul passaggio pertinente e, nella finestra a comparsa visualizzata, fare clic su **Elimina**.

   Nota
   Un passaggio del progetto può essere eliminato solo se lo stato è impostato su **Nuovo**.

2. Nella finestra di dialogo di conferma, fare clic su **Elimina**.

   Le metriche relative allo stato e al progresso del progetto vengono ricalcolate per tenere conto del passaggio eliminato. Ad esempio, le ore pianificate per il passaggio diventano nuovamente disponibili e possono essere utilizzate in altri passaggi del progetto. Viene inoltre eliminato il ticket relativo al passaggio eliminato.

Lavorare con i ticket del progetto

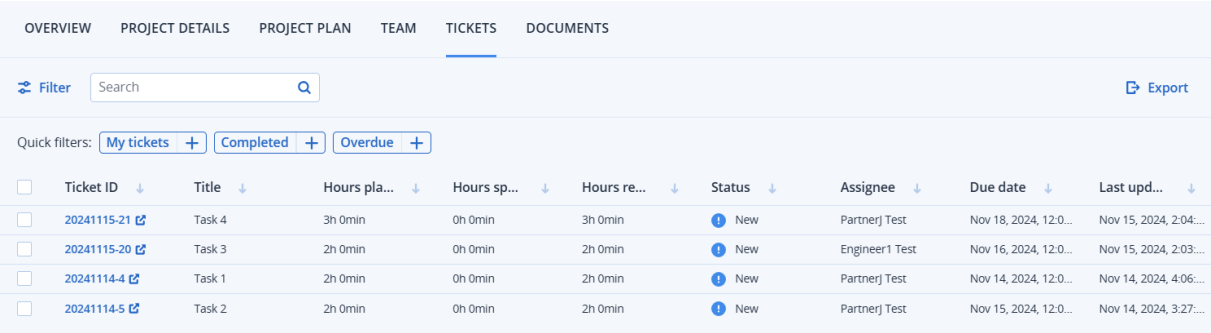
I ticket del progetto consentono di tenere traccia del tempo impiegato per i passaggi del progetto. Qualsiasi tempo impiegato su un passaggio del progetto deve essere registrato nel ticket di progetto corrispondente.

Advanced Automation (PSA) crea automaticamente i ticket del progetto durante la creazione di un passaggio del progetto. Se viene apportata una modifica al passaggio del progetto, le informazioni pertinenti vengono aggiornate nel ticket del progetto. Se lo stato di un ticket del progetto viene aggiornato, viene aggiornato anche lo stato del passaggio del progetto.

Nota
I passaggi del progetto possono essere completati solo impostando lo stato del ticket del progetto su **Completato**.

Tutti i ticket del progetto vengono visualizzati nella scheda **Ticket** del progetto corrispondente. In questa scheda è possibile visualizzare lo stato di ogni ticket (è anche lo stato del passaggio del progetto), le ore già impiegate sul ticket, il membro del team assegnato al ticket e l'ultima data di aggiornamento del ticket. Per ulteriori informazioni su come monitorare i tempi e la lavorazione del ticket, consultare "Visualizzazione e modifica di un ticket del progetto" (pag. 253).

È inoltre possibile esportare il contenuto della scheda **Ticket** facendo clic su **Esporta**. Viene creato e scaricato automaticamente un file in formato XLS.



Nota
I ticket del progetto possono essere visualizzati anche nel modulo **Service Desk**, benché non siano visualizzati per impostazione predefinita. Passare a **Gestione attività** > **Service Desk** e utilizzare lo strumento **Filtro** per selezionare e visualizzare i tipi di ticket **Progetto**.

Visualizzazione e modifica di un ticket del progetto

È possibile visualizzare, modificare e tenere traccia del tempo e del progresso di qualsiasi ticket del progetto.

Importante
Il tempo impiegato per un passaggio del progetto deve essere registrato esclusivamente nel ticket del progetto e non può essere registrato in nessun altro punto di Advanced Automation (PSA).

In ogni ticket è possibile:

- Registrare il tempo impiegato per il passaggio del progetto.
- Completare il passaggio del progetto (i passaggi del progetto possono essere completati solo impostando lo stato del ticket del progetto su **Completato**).

- Aggiungi un commento o una risposta definita.
- Aggiornamenti via email al cliente (che è definito come sponsor del progetto al momento della creazione del progetto).
- Cambia lo stato del passaggio del progetto (solo se il ticket non è stato impostato come **Completato**).
- Allegare i file.
- Pianificare il ticket (la data di inizio o di scadenza del passaggio non viene modificata). Questo consente di regolare la pianificazione del ticket in modo più preciso se, ad esempio, si imposta l'ora pianificata su un tempo inferiore a quello dell'intervallo di tempo del passaggio.

Per aggiornare un ticket del progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto per cui aggiornare un ticket, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. Fare clic sulla scheda **Ticket**.
4. Nell'elenco dei ticket del passaggio del progetto, fare clic sul ticket da aggiornare.

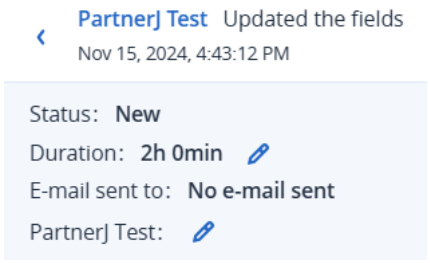
   Nota
   È inoltre possibile accedere al ticket del passaggio del progetto dalla sezione **Ticket del progetto** nel passaggio del progetto corrispondente, nel piano del progetto.

5. Utilizzando il timer nella parte superiore del pannello del passaggio del progetto, definire il tempo impiegato nel passaggio.

6. Selezionare la casella di controllo **Invia al cliente via e-mail** per inviare al cliente gli aggiornamenti dei ticket.
7. Nella scheda **Attività** del ticket:
   - Fare clic sul menu a discesa **Stato** per aggiornare lo stato del ticket su **Completato**, **Nuovo**, **Avvio in sospeso**, **In corso**, **Ritardato** o **In attesa**.
     Quando un ticket viene impostato su **Completato**, il passaggio del progetto associato viene automaticamente impostato su **Completato**. Il ticket non può essere riaperto e il suo stato non può essere aggiornato. Tuttavia, è possibile registrare un tempo aggiuntivo per il ticket, se necessario.
   - È possibile aggiungere alla casella di testo descrizioni e commenti formattati, incluse immagini e altri file multimediali per un massimo di 25 MB; i tipi e i formati supportati sono elencati sotto al collegamento **Allega file**.
   - Fare clic su **Allega file** per caricare i file. È possibile allegare uno qualsiasi dei seguenti formati e tipi di file, per un massimo di 25 MB.
     - File multimediali: .avi, .mp4, .mp3
     - E-mail: .eml, .msg

  - Immagini: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
  - Documenti e file di registro: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
  - Archivi: .zip, .rar
- Nell'elenco a discesa **Risposta definita** selezionare la risposta definita corrispondente. La risposta viene aggiunta alla casella di testo.
- Selezionare la casella di controllo **Pianifica ticket** per pianificare il ticket a un'ora e una data specifiche. L'intervallo di tempo impostato per la pianificazione non influisce sulle ore pianificate per il passaggio e viene utilizzato per bloccare alcune ore nel calendario. È possibile visualizzare i ticket pianificati nella scheda **Strumento di pianificazione**, a cui si accede dal modulo **Service Desk**.
- Nella sezione inferiore della scheda è possibile visualizzare le azioni recenti eseguite sul ticket. Fare clic sull'icona a freccia accanto a ogni azione per modificare alcuni campi, ad esempio il tempo impiegato per il ticket, o aggiungere ulteriori commenti.



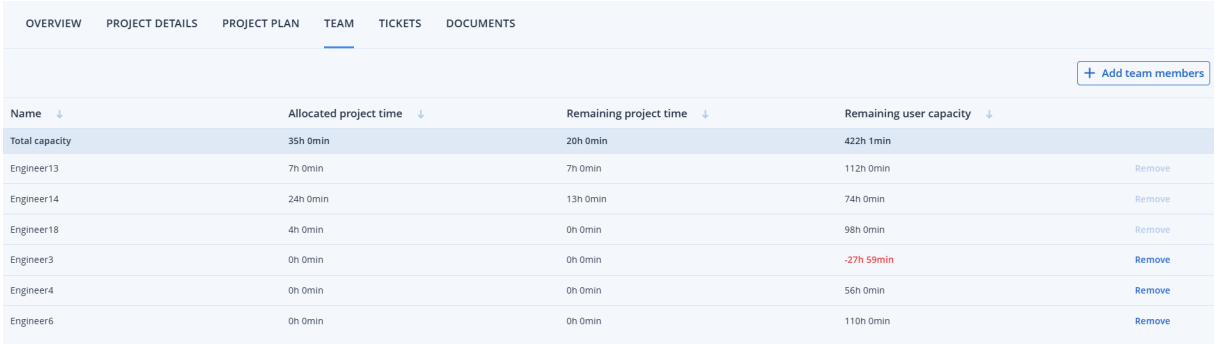
Nota
Se viene aggiornato il campo **Durata**, anche il campo **Ore trascorse** viene ricalcolato.

8. Nella scheda **Panoramica** del ticket:
   - Per aggiornare i dettagli del ticket, fare clic su **Modifica passaggio del progetto**. È inoltre possibile accedere ai collegamenti al progetto e al passaggio del progetto nella sezione **Informazioni sul progetto**.
   - Nella sezione **Allegati**, caricare i file da aggiungere al ticket.
9. Fare clic su **Salva modifiche**.
   Qualunque aggiornamento del ticket, ad esempio il tempo di registrazione aggiuntivo, viene aggiunto al progetto. Le metriche relative al progresso vengono ricalcolate per tenere conto del ticket aggiornato.
   Il tempo registrato nel ticket viene visualizzato anche nella scheda **Registrazione orario**, a cui si accede dal modulo **Service Desk**. Per ulteriori informazioni, consultare "Voci orario" (pag. 262).

Gestione del team del progetto

Nella scheda **Team** del progetto selezionato è possibile aggiungere ulteriori membri del team al progetto (consultare "Aggiunta di membri del team a un progetto" (pag. 256)), controllare il lavoro pianificato e rimanente ed esaminare la capacità utente per ciascun membro del team (consultare "Analisi della capacità dei membri del team" (pag. 259)).

Il team iniziale del progetto viene definito durante la creazione del progetto (consultare "Creazione di un progetto" (pag. 240)). Con il progredire del progetto, può essere necessario riassegnare i passaggi ad altri membri del team, a causa di problemi di capacità. Questa operazione viene eseguita nel piano del progetto, in cui si gestiscono le fasi e i passaggi del progetto, o nella scheda **Team**. Per ulteriori informazioni, consultare "Riassegnazione dei membri del team ai passaggi del progetto" (pag. 257).



Aggiunta di membri del team a un progetto

È possibile aggiungere e rimuovere membri del team a e da un progetto, come necessario.

Nota
Non è possibile rimuovere un membro del team da un progetto fino a quando è assegnato a un passaggio del progetto stesso.

Per aggiungere membri del team

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto a cui aggiungere i membri del team, fare clic sull'icona dei puntini di sospensione e selezionare **Apri**.
3. Fare clic sulla scheda **Team**, quindi su **Aggiungi membri del team**.
4. Nella finestra di dialogo Aggiungi membri del team, selezionare i membri del team da aggiungere nell'elenco visualizzato.

   Nota
   È possibile assegnare i membri del team tra gli utenti assegnati a un ruolo di Advanced Automation (PSA). Per aggiungere ulteriori utenti da selezionare, passare a **Gestione azienda > Utenti** e definire gli utenti corrispondenti.

5. Fare clic su **Aggiungi**.
   I membri del team selezionati vengono aggiunti al progetto e possono essere assegnati ai passaggi del progetto pertinenti.

Per rimuovere i membri del team

1. Nella scheda **Team** del progetto selezionato, fare clic su **Rimuovi** nella riga del membro del team da rimuovere.

   Nota
   L'opzione **Rimuovi** è disabilitata se un membro del team è assegnato a un passaggio del progetto. Per rimuovere il membro del team dal progetto, è necessario prima rimuoverlo dai passaggi del progetto pertinenti e riassegnare i passaggi a un altro membro del team. Per ulteriori informazioni, consultare "Riassegnazione dei membri del team ai passaggi del progetto" (pag. 257).

2. Nella finestra di conferma, fare clic su **Rimuovi**.

Riassegnazione dei membri del team ai passaggi del progetto

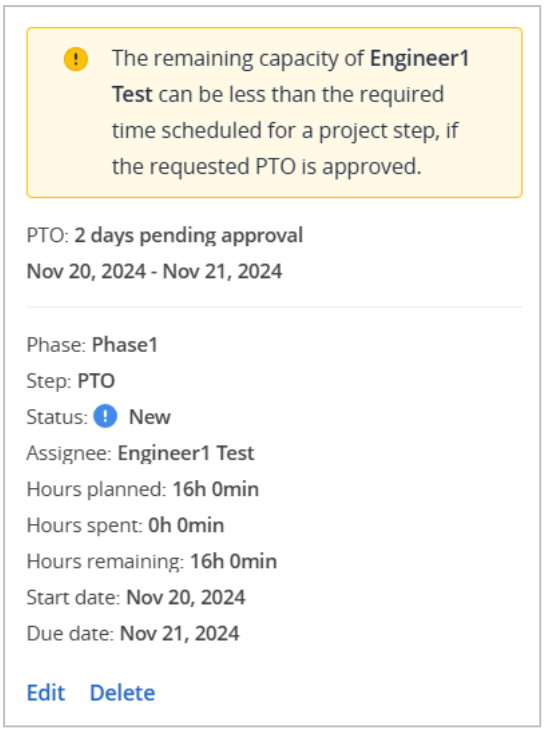
È possibile riassegnare i membri del team ai passaggi del progetto quando:

- È necessario riassegnare i membri del team se, ad esempio, un altro membro del team è più adatto al passaggio.
- C'è un problema di capacità del team. Ad esempio, i giorni di ferie retribuite o di malattia in sospeso di un membro del team esistente possono far sì che il progetto subisca ritardi. Per ulteriori informazioni su come analizzare la comprensione della capacità del team, consultare "Analisi della capacità dei membri del team" (pag. 259).

I membri del team devono essere riassegnati tramite il piano del progetto, come descritto di seguito. Per ulteriori informazioni su come lavorare con il piano del progetto, consultare "Visualizzazioni del piano del progetto" (pag. 245).

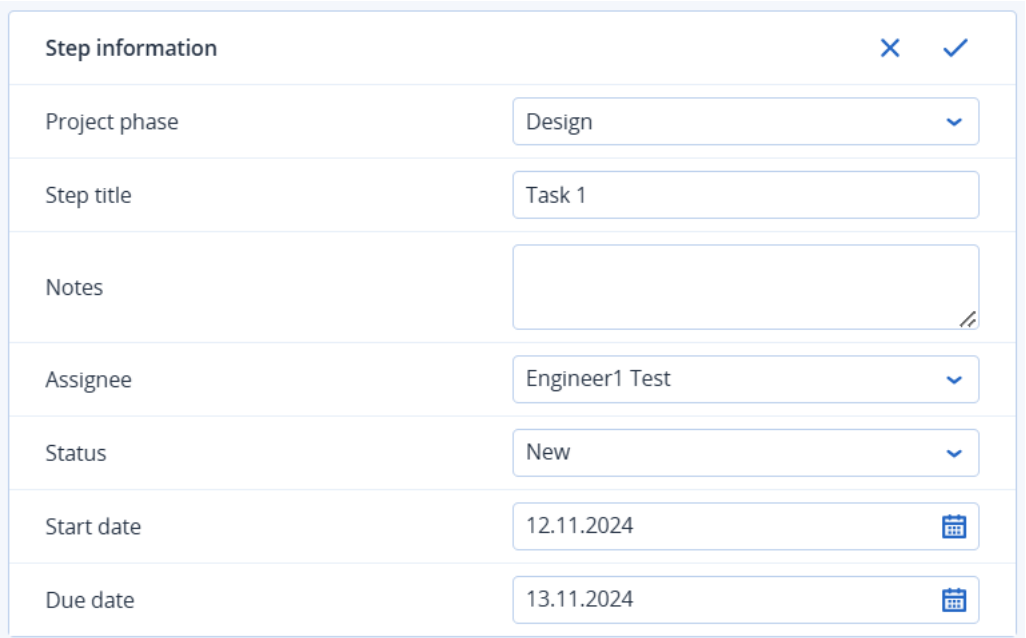
Per riassegnare i membri del team ai passaggi del progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto nel quale riassegnare i membri del team, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. Fare clic sulla scheda **Piano del progetto**.
4. Fare clic sul passaggio evidenziato con un problema di capacità utente (evidenziato in rosso) o un avviso (evidenziato in giallo).
   L'esempio seguente mostra che l'approvazione delle ferie retribuite in sospeso può incidere sulla capacità del membro del team.



5. Fare clic su **Modifica**.

   Il pannello di destra mostra le informazioni sul passaggio, incluse le informazioni sul membro del team attualmente assegnato.
6. Nella sezione **Informazioni sul passaggio**, fare clic sull'icona a matita.
7. Nel menu a discesa **Assegnatario**, selezionare il membro del team con cui sostituire il membro del team attualmente assegnato al passaggio.



8. Fare clic su ✓.

   Le metriche relative allo stato e all'avanzamento del progetto vengono ricalcolate in modo da valutare il membro del team riassegnato.

Analisi della capacità dei membri del team

Con Capacità del membro del team si intende il tempo di lavoro a disposizione di un membro del team per un progetto (in ore e minuti).

La capacità del membro del team viene calcolata in base a tutte le ore lavorative disponibili per il membro nel periodo del progetto (dal giorno corrente in poi), sottraendo qualsiasi giorno di ferie retribuite o permesso per malattia approvato, qualsiasi periodo di tempo assegnato ad altri ticket di Advanced Automation (PSA) (diversi dai ticket del progetto) e qualsiasi periodo di tempo rimanente in altri passaggi del progetto di altri progetti. I problemi di capacità si verificano quando le ore lavorative disponibili del membro del team sono inferiori alle ore richieste per completare un passaggio del progetto.

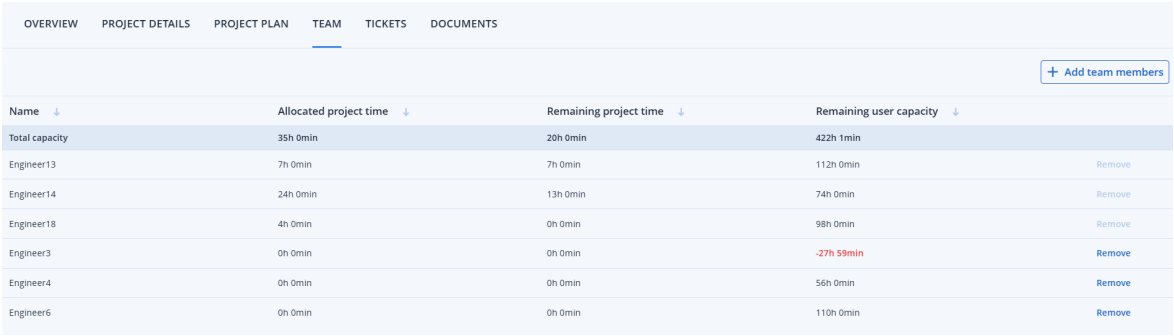
Gli eventuali problemi che si verificano con la capacità dei membri del team vengono visualizzati:

- A livello di passaggio del progetto, nel widget **Pianificazione del progetto** della scheda **Panoramica**, come descritto di seguito.
- Nei singoli passaggi del progetto nella scheda **Pianificazione del progetto**. Per ulteriori informazioni, consultare "Visualizzazioni del piano del progetto" (pag. 245).

È inoltre possibile visualizzare la disponibilità o la capacità corrente dei membri del team del progetto nella scheda **Team** del progetto selezionato, come descritto di seguito.

Per analizzare la capacità dei membri del team nella scheda Team

1. Aprire il progetto pertinente e fare clic sulla scheda **Team**.
   Viene visualizzato l'elenco corrente dei membri del team del progetto. La colonna **Capacità utente rimanente** mostra la capacità corrente di ciascun membro del team.



2. Fare clic sulla riga di un membro del team per visualizzare i dettagli seguenti:
   - **Tempo di progetto allocato**: mostra le ore totali pianificate per i passaggi assegnati al membro del team.
   - **Tempo di progetto rimanente** : mostra il tempo di progetto rimanente del membro del team (in ore e minuti) nei passaggi assegnati.

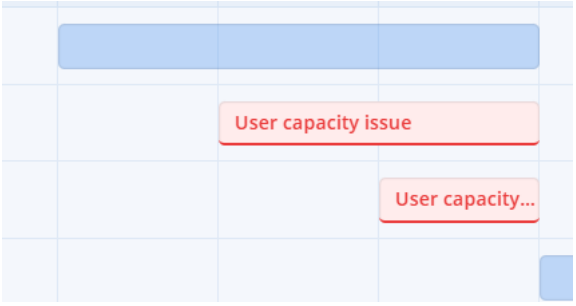
Nota
Il valore **Tempo di progetto rimanente** è uguale alle ore pianificate meno le ore segnalate come lavorate. Il valore visualizzato include il tempo registrato dagli altri membri del team che hanno lavorato al passaggio.

Ad esempio, a un passaggio del progetto assegnato al membro del team A sono state allocate dieci ore. Il membro del team A non ha ancora registrato alcun tempo lavorato sul passaggio, ma il membro del team B ha registrato tre ore lavorate. In questo scenario, il tempo di progetto rimanente per il passaggio assegnato al membro del team A è di sette ore.

- **Capacità utente rimanente**: mostra il tempo di lavoro del membro del team ancora disponibile per un progetto (in ore e minuti).
  Se si verifica un problema con la capacità del membro del team, il campo **Capacità utente rimanente** viene evidenziato in rosso e un messaggio di avviso viene visualizzato nella parte superiore del riquadro. I problemi di capacità si verificano quando il valore **Capacità utente rimanente** è inferiore al valore **Tempo di progetto rimanente**.
- **Giorni liberi**: mostra i dettagli dei giorni di ferie e di malattia approvati (e in attesa di approvazione) durante il periodo del progetto.

Per risolvere i problemi di capacità, è necessario regolare la pianificazione del progetto o assegnare un altro utente i passaggi del progetto rilevanti. Per ulteriori informazioni, consultare "Riassegnazione dei membri del team ai passaggi del progetto" (pag. 257).

Per esaminare la capacità dei membri del team a livello di passaggio del progetto

1. Nel portale di gestione, passare a **Gestione attività** > **Progetti**.
2. Nella colonna più a destra del progetto di riferimento, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Apri**.
3. Nella scheda **Panoramica**, scorrere verso il basso fino al widget **Pianificazione del progetto**.
   Gli eventuali problemi di capacità dei membri del team vengono visualizzati nel widget, come mostrato di seguito.
   

4. Fare clic sul problema per visualizzare ulteriori dettagli e modificare i dettagli del passaggio come necessario. Ad esempio, il membro del team assegnato al passaggio potrebbe non avere abbastanza ore disponibili per lavorare sul passaggio. Il sistema chiede di adeguare la pianificazione del progetto o di assegnare un altro utente all'attività. Per ulteriori informazioni, consultare "Riassegnazione dei membri del team ai passaggi del progetto" (pag. 257).

La capacità del membro del team viene ricalcolata quando un membro del team viene aggiunto al progetto o rimosso dal progetto, o quando il progetto viene aggiornato e l'aggiornamento incide sul tempo di progetto allocato, il tempo di progetto rimanente o la capacità rimanente.

Fatturazione dei progetti

Le attività dei progetti vengono fatturate come articoli di vendita creati automaticamente in base al modello di fatturazione del progetto, che viene definito al momento della creazione del progetto.

Gli articoli di vendita creati possono essere aggiornati, eliminati (se non sono ancora stati fatturati) e fatturati tramite i regolari cicli di fatturazione in Advanced Automation (PSA). Per ulteriori informazioni su come operare con gli articoli di vendita, consultare "Gestione degli articoli di vendita" (pag. 278).

Nel modulo **Progetti** sono disponibili tre modelli di fatturazione:

- **Fattura per passaggio completato**: un nuovo articolo di vendita viene creato automaticamente quando un ticket associato a un passaggio del progetto viene completato. Per ulteriori informazioni, consultare Fatturazione per passaggio completato.
- **Fattura per anticipo sul totale**: un nuovo articolo di vendita viene creato automaticamente quando viene creato un progetto con almeno un prodotto del progetto selezionato. Per ulteriori informazioni, consultare Fatturazione per anticipo sul totale.
- **Fattura per obiettivo**: un nuovo articolo di vendita viene creato automaticamente quando viene completato un passaggio contrassegnato come passaggio **Obiettivo**. Per ulteriori informazioni, consultare Fatturazione per obiettivi.

Fatturazione per passaggio completato

Se è abilitato il modello **Fattura per passaggio completato**, il sistema genera un articolo di vendita quando un membro del team completa un passaggio del progetto.

Quando il ticket di progetto associato è impostato su **Completato**, è ancora possibile accedere o modificare l'orario e aggiungere commenti e allegati, ma non è possibile modificare le date, gli orari pianificati o lo stato. Viene generato un articolo di vendita in base alle ore pianificate per il passaggio del progetto e l'addebito al cliente viene effettuato in base al flusso di fatturazione esistente in Advanced Automation (PSA).

Fatturazione per anticipo sul totale

Se è abilitato il modello di fatturazione **Fattura per anticipo sul totale**, esistono tre modalità per creare un articolo di vendita:

- **Quando viene creato un progetto con un budget**: se viene creato un progetto (da zero o copiando un progetto esistente) con un budget (cioè selezionando almeno un prodotto del progetto), viene generato automaticamente un articolo di vendita. A questo punto, è possibile fatturare al cliente in base al flusso di fatturazione esistente.
- **Quando viene creato un progetto senza un budget**: se viene creato un progetto (da zero o copiando un progetto esistente) senza un budget (ovvero non vengono selezionati prodotti del

progetto), il sistema non genera alcun articolo di vendita. Prima di creare l'articolo di vendita, è necessario impostare il budget del progetto aggiungendo i prodotti del progetto e allocando le ore corrispondenti. È quindi necessario creare manualmente un articolo di vendita che corrisponda al budget del progetto. A questo punto, è possibile fatturare al cliente in base al flusso di fatturazione esistente.

- **Quando si aggiorna un progetto**: se si sta lavorando a un progetto ed è necessario aumentarne il budget, ma al cliente sono già state fatturate le ore previste dal budget, è necessario creare manualmente un articolo di vendita. L'articolo di vendita deve corrispondere all'incremento del budget del progetto. A questo punto, è possibile fatturare al cliente in base al flusso di fatturazione esistente. Se la fattura al cliente non è ancora stata emessa, è possibile aggiornare il budget del progetto e l'articolo di vendita esistente.

Fatturazione per obiettivi

Se è abilitato il modello **Fattura per obiettivi**, viene generato un articolo di vendita quando un membro del team completa un passaggio definito come **Obiettivo**.

L'articolo di vendita include le voci di ogni passaggio completato (incluso l'ultimo passaggio obiettivo) dal completamento dell'ultimo passaggio obiettivo o dall'avvio del progetto:

- Al completamento del primo obiettivo, viene emessa una fattura relativa a tutti i passaggi completati dall'avvio del progetto.
- Al completamento dell'obiettivo successivo, viene emessa una fattura relativa a tutti i passaggi completati dopo l'ultimo obiettivo completato. Da quel punto in poi, se vengono lavorati e impostati come **Completati** altri passaggi del progetto, questi vengono inclusi nella fattura al completamento del successivo obiettivo.

Impostazione dell'entità di fatturazione dei progetti predefinita

Advanced Automation (PSA) consente di creare più entità di fatturazione. Ciò significa che è possibile fatturare da più attività e che ogni entità di fatturazione potrà emettere fatture con impostazioni, sfondo e altre caratteristiche personalizzate. Nella schermata **Gestione progetto** delle impostazioni del Service Desk è possibile impostare l'entità di fatturazione predefinita per gli articoli di vendita creati per la fatturazione del progetto.

Per impostare l'entità di fatturazione dei progetti predefinita

1. Passare a **Impostazioni > Service Desk**, quindi selezionare **Gestione progetto**.
2. Fare clic su **Modifica**, quindi selezionare l'entità di fatturazione pertinente.
3. Fare clic su **Salva**.

Voci orario

Il modulo **Voci orario** consente di gestire le registrazioni orarie degli utenti e tenere traccia delle rispettive attività quotidiane.

Per accedere alla funzionalità Voci orario, nel portale di gestione passare a **Gestione attività** > **Voci orario**. Nella scheda **Registrazione orario** visualizzata, è possibile vedere tutte le voci orario correnti registrate in Advanced Automation (PSA). In questa scheda e nelle schede Voci orario aggiuntive, è possibile:

- Aggiungere nuove registrazioni orario
- Visualizzare e modificare le registrazioni orario esistenti
- Rivedere e approvare le registrazioni orario
- Richiedere giorni liberi
- Aggiungere e rivedere gli avvisi di malattia
- Rivedere e approvare le registrazioni OTP
- Esportare i dati delle registrazioni orario

Cosa sono le voci orario/registrazioni orario?

In Advanced Automation (PSA) sono disponibili due opzioni per la registrazione degli orari di lavoro:

- **Automaticamente**: il sistema crea automaticamente le registrazioni orario quando individua un operatore che lavora su un ticket del Service Desk. Il tempo dedicato al ticket viene acquisito automaticamente grazie a un timer integrato; può anche essere modificato da un tecnico dei ticket.
- **Manualmente**: le registrazioni orario manuali vengono inviate manualmente dai tecnici. Per ulteriori informazioni, consultare "Aggiunta di una nuova registrazione orario" (pag. 264).

Una registrazione degli orari regolare e accurata consente di aumentare gli orari fatturabili. Inoltre, grazie ai report integrati in Advanced Automation (PSA), fornisce una valida panoramica delle metriche aziendali, tra cui il tempo dedicato a uno specifico cliente, le percentuali di occupazione dei tecnici e altro ancora.

Visualizzazione delle registrazioni orario esistenti

Per visualizzare le registrazioni orario esistenti, nel portale di gestione passare a **Gestione attività** > **Voci orario**. Nella scheda **Registrazione orario** visualizzata, è possibile vedere tutte le registrazioni orario correnti registrate in Advanced Automation (PSA).

Vengono visualizzate informazioni su ogni voce, incluso:

- Le ore registrate
- L'utente specifico che ha eseguito l'attività
- Il tipo di attività
- Il cliente
- Se la registrazione orario è fatturabile o meno
- Un collegamento al ticket pertinente (se necessario)

Le registrazioni orario sono raggruppate per data, e viene visualizzato il totale delle ore di ogni giornata.

Per esportare i dati delle registrazioni orario, selezionare le registrazioni pertinenti e quindi fare clic su **Esporta in formato XLS**. Un file con estensione XLS e denominato **Registrazioni orario** verrà scaricato nel workload.

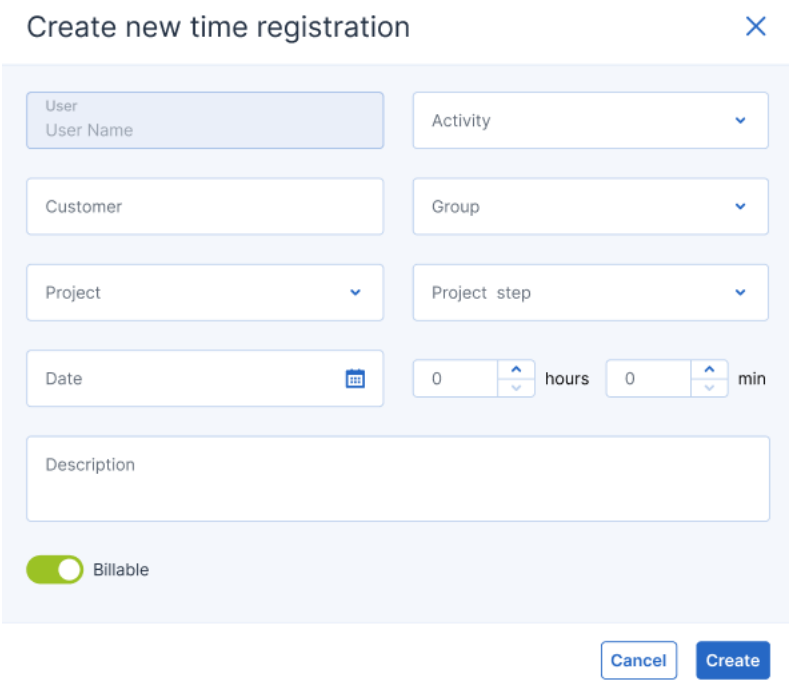
È inoltre possibile filtrare e ordinare l'elenco visualizzato per individuare una specifica voce orario; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali voci orario dovranno essere visualizzate.

Aggiunta di una nuova registrazione orario

Aggiungendo manualmente una nuova registrazione orario, è possibile registrare il tempo trascorso lavorando sui ticket. Ciò consente di visualizzare le attività di cui si occupano i tecnici e, in combinazione con gli altri parametri e report di Advanced Automation (PSA), determinare le risorse più adatte ai progetti specifici.

Per aggiungere una nuova registrazione orario

1. Passare a **Gestione attività > Voci orario**. La scheda **Registrazione orario** è visualizzata per impostazione predefinita.
2. Fare clic su **+ Nuovo**. Viene visualizzata la finestra di dialogo seguente.



Nota
Se il modulo Advanced Automation (PSA) è attivato per l'account, è anche possibile fare clic su **Nuova > Registrazione orario** nella barra degli strumenti del portale di gestione posizionata nella parte superiore dello schermo, anche se l'utente non si trova nel modulo Voci orario. Questa opzione apre automaticamente la finestra di dialogo Crea nuova registrazione orario, tramite la quale è possibile creare una registrazione orario come descritto nei passaggi seguenti.

3. Definire quanto segue:
   - **Attività**: selezionare l'attività pertinente dall'elenco a discesa **Attività**. Per ulteriori informazioni sulle attività, consultare "Definizione delle attività con monitoraggio degli orari" (pag. 333).
   - **Cliente**: selezionare il cliente pertinente dall'elenco a discesa **Cliente**. È inoltre possibile selezionare la propria organizzazione, ma in questo caso la voce inserita non sarà fatturabile. Per registrare il lavoro eseguito per uno specifico cliente, inserire il nome del cliente.
   - **Gruppo**: selezionare il gruppo pertinente (il reparto per il quale si sta eseguendo la registrazione) dall'elenco a discesa **Gruppo**. Vengono visualizzati solo i gruppi dei quali si è membri.
   - **Progetto**: selezionare il progetto pertinente dall'elenco a discesa **Progetto**. Questa opzione è disponibile solo se si è stati assegnati a un team di progetto.
   - **Fase progetto**: selezionare la fase di progetto pertinente dall'elenco a discesa **Fase progetto**. Questa opzione è disponibile solo se si è stati assegnati a un team di progetto e se le fasi del progetto non sono chiuse.
   - **Data**: definire la data pertinente.
   - **Periodo di tempo**: definire la durata della registrazione orario, in ore e minuti.

- **Descrizione**: inserire una descrizione per l'attività.
- **Fatturabile**: fare clic sull'interruttore **Fatturabile** per registrare l'attività come tale. Questa opzione è disponibile solo se è stato selezionato un cliente.

Nota
Quando si crea una nuova registrazione orario, il campo **Utente** viene compilato automaticamente con il nome dell'utente.

4. Fare clic su **Crea**.

Modifica di una registrazione orario

Nota
È possibile modificare una registrazione orario solo se non è stata elaborata. Per ulteriori informazioni sull'elaborazione delle registrazioni orario, consultare "Approvazione delle registrazioni orario per la fatturazione" (pag. 267).

Per modificare una registrazione orario

1. Passare a **Gestione attività > Voci orario**. La scheda **Registrazione orario** è visualizzata per impostazione predefinita.
2. Fare clic sulla registrazione orario da modificare.
3. Nella barra laterale destra, fare clic sull'icona a matita per modificare la registrazione orario. Per ulteriori informazioni sui campi disponibili, consultare "Aggiunta di una nuova registrazione orario" (pag. 264).
4. Al termine, fare clic su ✓.

Registrazioni orario fatturabili

Advanced Automation (PSA) prevede due scenari principali di fatturazione per le voci orario:

- Registrazioni orario automatiche quando si lavora su ticket generici e ticket di avviso.
- Voci orario manuali.

Nota
Indipendentemente dallo scenario della voce orario, è l'amministratore dell'MSP che determina se il tempo dedicato deve essere fatturato o meno. Ciò significa che tutte le selezioni effettuate nelle sezioni seguenti possono essere annullate se necessario.

Per ulteriori informazioni su come lavorare con gli articoli di vendita, consultare "Gestione degli articoli di vendita" (pag. 278).

Registrazioni orario automatiche quando si lavora su ticket generici e ticket di avviso

Tenere presente quanto segue:

- Questo orario può essere non fatturabile se per lo SLA applicabile è abilitata l'opzione **Prezzo fisso** (in uno SLA "tutto compreso"); questo orario può essere fatturabile se per lo SLA applicabile è impostata l'opzione **Calcolo successivo**.
- La tariffa di fatturazione può essere basata su diversi scenari:
  - Tariffa di fatturazione predefinita per lavoro durante le ore di ufficio.
  - Tariffa di fatturazione predefinita per lavoro esterno durante le ore di ufficio se il timestamp dell'aggiornamento del ticket non rientra nell'intervallo di copertura dello SLA.
  - Tariffa di fatturazione specifica per il cliente (prezzo personalizzato).
  - Tariffa di fatturazione specifica basata sulle tipologie di lavoro nel ticket. Ad esempio, l'Aggiornamento 1 nel ticket è per un'ora di attività di supporto standard; l'Aggiornamento 2 nel ticket è per un'ora e il tipo di attività 'Progettazione rete' è selezionata nel ticket. Il risultato finale è che al cliente vengono fatturate due diverse tariffe; tuttavia, tali tariffe di fatturazione possono essere sovrascritte dalle impostazioni di prezzo personalizzate.

Voci orario manuali

È possibile contrassegnare questo orario come fatturabile. Per ogni tipo di attività di registrazione orario manuale è possibile configurare una specifica tariffa di fatturazione. Tenere presente che questa tariffa può essere sovrascritta dalle impostazioni di prezzo personalizzate (per ulteriori informazioni, consultare "Lavorare con i prezzi personalizzati" (pag. 288)).

Approvazione delle registrazioni orario per la fatturazione

È possibile approvare le seguenti registrazioni orario incluse in Advanced Automation (PSA) ed elencate nella scheda **Approva orario**.

- Registrazioni orario non ancora approvate, ovvero orari dei ticket segnalati provenienti solo dai ticket che si trovano nello stato **Chiuso**, o per le registrazioni orario manuali.
- Registrazioni orario che soddisfano la soglia del tempo minimo dedicato a un ticket (valore definito nelle impostazioni di fatturazione, consultare "Impostazioni di fatturazione" (pag. 336)). Ad esempio, se la soglia è impostata su **5**, le voci orario di durata inferiore ai 5 minuti non sono visualizzate nell'elenco.

Nota
Le registrazioni orario possono essere approvate solo da utenti con i ruoli seguenti: Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità

Ogni registrazione orario elencata include tutte le informazioni su ciascuna attività e consente inoltre di elaborare ed emettere la fattura ai clienti associati. È possibile approvare registrazioni orario singole o multiple da fatturare ai clienti; in alternativa è anche possibile impostare le registrazioni orario come in sospeso o non fatturabili.

Importante
Non è possibile approvare un orario ticket riferito da un cliente se per tale cliente non sono state fornite le informazioni di fatturazione. Quando si tenta di approvare le registrazioni orario riferite a un ticket, verrà richiesto di aggiungere le informazioni di fatturazione del cliente in questione. Per ulteriori informazioni, consultare Fornire le informazioni di fatturazione.

Per approvare una registrazione orario

1. Passare a **Gestione attività > Voci orario**. Fare quindi clic sulla scheda **Approva orario**.
   Viene visualizzato l'elenco delle registrazioni orario in attesa di approvazione. Le informazioni visualizzate includono il cliente, la data, la descrizione della registrazione orario e la relativa durata.

   Nota
   La visualizzazione del simbolo  accanto alla colonna Durata indica che alcuni degli orari registrati non rientrano nell'intervallo di tempo del contratto SLA pertinente. Per ottenere più informazioni su quale orario è stato fatturato, attenersi alla procedura seguente.

2. (Facoltativo) Per verificare i dettagli di una specifica registrazione orario, selezionare la riga corrispondente. I dettagli della registrazione orario selezionata vengono visualizzati nella barra laterale destra.
   - È possibile fare clic su **Elabora** per creare un articolo di vendita per questa registrazione orario e su **Visualizza ticket** per visualizzare il ticket corrispondente. Visualizzare il Passaggio 4 per ulteriori informazioni su come Advanced Automation (PSA) gestisce la registrazione orario quando si fa clic su **Elabora**.
   - Nella sezione **Panoramica**, vengono visualizzate informazioni generiche sulla registrazione orario. È anche possibile modificare le informazioni e abilitare l'interruttore **Blocco ore** (se i blocchi ore sono abilitati nel contratto in questione, come nel caso di un accordo che prevede 20 ore di assistenza tutto incluso al mese). Se è presente un saldo disponibile di blocchi ore (ad esempio, ore di assistenza non utilizzate), la registrazione orario viene dedotta da questo saldo, senza necessità di creare un articolo di vendita in più. È possibile ridefinire questa regola predefinita in base alle necessità, e continuare a fatturare il tempo già registrato.
   - Nella sezione **Orario fatturabile SLA** è visualizzato il valore orario arrotondato riferito al cliente (in minuti) che verrà utilizzato per arrotondare il tempo fatturabile totale. È possibile visualizzare e modificare il tempo arrotondato totale relativo alla tariffa di fatturazione. Ad esempio, è possibile selezionare la tariffa di fatturazione da considerare e adeguare manualmente il tempo di fatturazione finale.
   - Nella sezione inferiore della barra laterale, è possibile rivedere i dettagli delle registrazioni orario relative al ticket. Per ogni registrazione orario sono disponibili le informazioni seguenti:
     - L'utente che ha inserito la registrazione orario.
     - Il nome del gruppo di supporto dell'utente.
     - La data e l'ora della registrazione orario.

- La tariffa oraria dell'utente.
- Una descrizione della registrazione orario.

3. Dopo aver verificato o modificato la registrazione orario, fare clic sulla riga pertinente e selezionare una delle opzioni seguenti nella scheda **Approva orario**.
   - **Fatturabile**: selezionare questa opzione per fatturare al cliente corrispondente ed emettere la fattura.

     Nota
     Advanced Automation (PSA) preseleziona in modo automatico l'opzione di fatturazione del ticket in base allo SLA (è possibile ignorare questa opzione selezionando quella pertinente). Quando una voce orario manuale viene contrassegnata come **Fatturabile** durante la creazione (consultare "Creazione di un nuovo ticket" (pag. 223)), Advanced Automation (PSA) la contrassegna come **Fatturabile** nella scheda **Approva orario**. Se necessario, è possibile modificare l'opzione di fatturazione in **In sospeso**.

   - **Non fatturabile**: selezionare questa opzione se non si desidera fatturare la registrazione orario selezionata.
   - **In sospeso**: selezionare questa opzione per lasciare la registrazione orario nell'elenco dopo aver elaborato ogni articolo fatturabile.

   Se necessario, è inoltre possibile selezionare più registrazioni orario. Una volta effettuata la selezione, i pulsanti corrispondenti all'azione scelta vengono abilitati nell'area superiore all'elenco delle registrazioni orario. È possibile selezionare le opzioni **Contrassegna come fatturabile**, **Contrassegna come non fatturabile**, **Contrassegna come in sospeso** o **Elabora** (consultare il passaggio successivo).
4. Fare clic sul pulsante di azione **Elabora** per elaborare le registrazioni orario selezionate.
   Se una registrazione orario è stata impostata come **Fatturabile**, viene creato un articolo di vendita con i dettagli dell'azienda corrispondente al cliente. Inoltre, se sono state selezionate più registrazioni orario, all'articolo di vendita vengono aggiunte più righe. La fattura generata include il titolo e il numero del ticket e l'orario fatturabile in base alla tariffa applicabile.
   Se una registrazione orario è stata impostata come **Non fatturabile**, viene rimossa dalla scheda **Approva orario**.
   Se una registrazione orario è stata impostata come **In sospeso**, non viene eliminata dalla scheda **Approva orario**.

Richiesta di giorni liberi

È possibile visualizzare e aggiornare le richieste di giorni liberi nella scheda **Richiedi giorno libero**. Questa scheda visualizza tutte le richieste di giorni liberi create e i rispettivi dettagli, incluso se hanno ricevuto o meno l'approvazione. Se necessario, è anche possibile richiedere ulteriori giorni liberi.

Nota
Le richieste di giorni liberi si basano sui campi **Giorni liberi per anno** e **Policy per i giorni di ferie rimanenti** nelle impostazioni predefinite del Service Desk. Per ulteriori informazioni, consultare "Impostazione dei valori predefiniti" (pag. 319).

Per richiedere giorni liberi

1. Passare a **Gestione attività > Voci orario**, quindi fare clic sulla scheda **Richiedi giorno libero**.
2. Fare clic su **+ Nuovo**.
3. Nella finestra di dialogo visualizzata, selezionare una delle seguenti opzioni:
   - **Richiedi un giorno**: selezionare il giorno e le ore richieste (per impostazione predefinita sono selezionate otto ore).
   - **Richiedi più giorni**: selezionare le date di inizio e fine richieste.
4. Inserire una descrizione per la richiesta, quindi fare clic su **Crea**.
   Se vengono richiesti più giorni liberi, viene registrata una richiesta per ogni giorno.

   Nota
   È inoltre possibile modificare le richieste di giorni liberi in attesa di approvazione facendo clic sulla riga corrispondente nell'elenco delle richieste e quindi apportando le modifiche necessarie. Se la richiesta viene approvata o rifiutata, non può essere modificata.

Creazione di un avviso di malattia

È possibile visualizzare e aggiornare tutti gli avvisi di malattia in attesa di approvazione nella scheda **Avviso di malattia**. È inoltre possibile creare un nuovo avviso di malattia per qualsiasi utente dell'account.

Nota
Gli avvisi di malattia possono essere creati solo da utenti con i ruoli seguenti: Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità, Risorse umane

Per creare un nuovo avviso di malattia

1. Passare a **Gestione attività > Voci orario**, quindi fare clic sulla scheda **Avviso di malattia**.
2. Fare clic su **+ Nuovo**.
3. Nella finestra di dialogo visualizzata, procedere come segue.
   - **Utente**: selezionare l'utente per il quale si desidera creare l'avviso di malattia.
   - **Richiedi un giorno**: selezionare il giorno e le ore richieste (per impostazione predefinita sono selezionate otto ore).

     Oppure

     Richiedi più giorni: selezionare le date di inizio e fine richieste.
4. Inserire la descrizione dell'avviso di malattia e fare clic su **Crea**.

Se vengono richiesti più giorni di malattia, viene registrata una richiesta per ogni giorno.

Nota
È inoltre possibile modificare le richieste di malattia in attesa di approvazione facendo clic sulla riga corrispondente nell'elenco degli avvisi di malattia e quindi apportando le modifiche necessarie. Se l'avviso di malattia è stato approvato o rifiutato, non può essere modificato.

Approvazione di richieste di ferie retribuite e permessi per malattia

È possibile visualizzare e aggiornare le richieste di ferie retribuite e di permessi per malattia di tutti gli utenti nella scheda **Approva richiesta ferie retribuite**. È possibile approvare o rifiutare una richiesta di ferie retribuite o di permessi per malattia.

Nota
Le richieste di ferie retribuite possono essere approvate solo da utenti con i ruoli seguenti: Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità

Per approvare le richieste di ferie retribuite

1. Passare a **Gestione attività > Voci orario**, quindi fare clic sulla scheda **Approva richiesta ferie retribuite**.
2. Nell'elenco delle richieste, selezionare la richiesta rilevante e fare clic su **Approva** o **Rifiuta**.
   È inoltre possibile selezionare più richieste.
   Se una richiesta è stata approvata, viene rimossa dall'elenco visualizzato nella scheda **Approva richiesta ferie retribuite**; il valore dei giorni di ferie residue dell'utente viene aggiornato. Se una richiesta è stata rifiutata, viene rimossa anche dalla scheda **Approva richiesta ferie retribuite**.
   La colonna **Tipo** indica il tipo di richiesta, ovvero **Ferie retribuite** o **Giorni di malattia**.
3. (Facoltativo) Fare clic sulla riga di una richiesta per visualizzare i dettagli della richiesta. Se necessario, è anche possibile aggiungere un commento.
   Tenere presente che la colonna **Giorni liberi rimanenti** nella sezione **Informazioni sul saldo tempo** mostra il valore in giorni, ore e minuti rimanenti. Questo valore viene calcolato come la differenza tra il numero di giorni liberi consentito durante l'anno (valore impostato tra quelli predefiniti del Service Desk; consultare "Impostazione dei valori predefiniti" (pag. 319)) e la quantità totale di tutte le richieste di ferie retribuite già approvate durante l'anno in corso.

Gestione della funzionalità Vendite e fatturazione

Dal modulo Vendite e fatturazione (nel portale di gestione, passare a **Vendite e fatturazione**) è possibile gestire le funzionalità indicate di seguito.

- Preventivi
- Articoli di vendita
- Contratti

- Fatture
- Registri contabili
- Prodotti
- Prezzi personalizzati

Nota
Prima di continuare con questa sezione, verificare di aver configurato completamente l'account nella sezione **Impostazioni**, inclusa la creazione di prodotti.

Vendite

Il modulo **Vendite** consente di gestire quanto indicato di seguito.

- Offerte
- Articoli di vendita
- Contratti
- Prezzi personalizzati

Per accedere al modulo **Vendite**, nel portale di gestione passare a **Vendite e fatturazione > Vendite**.

Gestione dei preventivi

Utilizzare la funzionalità per le offerte di Advanced Automation (PSA) per fornire ai clienti i preventivi relativi ai prodotti e ai servizi offerti. Successivamente all'approvazione, un preventivo viene automaticamente convertito in una serie di attività che aiutano a tenerne traccia e a segnalarne lo stato di lavorazione.

- Per il preventivo approvato, viene creato un ticket preventivo generico, che permette di tenere traccia dell'avanzamento, di aggiungere note e di registrare il tempo dedicato all'attività.
- Per gli articoli del preventivo che devono essere acquistati per poter evadere l'ordine viene creato un ticket ordine di acquisto. Tale ticket può essere utilizzato dai membri del team per tenere traccia dell'avanzamento, conservare note importanti come i dettagli di acquisto e registrare il tempo dedicato all'attività.
- Gli articoli dei preventivi per i prodotti dei contratti vengono automaticamente convertiti in nuovi contratti e parti del contratto oppure aggiunti ai contratti dei clienti esistenti, in base alla configurazione originale del preventivo relativa a tali articoli.

Per accedere alle funzionalità per i preventivi, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Preventivi**. La scheda **Preventivi** mostra tutti i preventivi creati per i clienti.

Nota
Questa funzionalità è disponibile solo agli utenti ai quali sono stati assegnati i ruoli seguenti. Amministratore, Direttore, Tecnico, Responsabile gruppo, Responsabile contabilità, Contabilità, Vendite

Creazione di un preventivo

Una procedura suddivisa in fasi principali guida l'utente durante la creazione di un nuovo report. Le fasi prevedono:

- L'inserimento delle informazioni di base sul preventivo.
- L'aggiunta di prodotti e/o di modelli di preventivo all'offerta.
- La revisione e l'invio del preventivo (o il suo salvataggio per essere modificato e inviato in un secondo momento).

Per creare un preventivo

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Fare clic sulla scheda **Preventivi**, quindi scegliere **+ Nuovo**. Se non è ancora stato creato un preventivo, viene richiesto di fare clic su **Crea nuovo**.

   Nota
   Se per l'account è attivato il modulo Advanced Automation (PSA), è anche possibile fare clic su **Nuovo** > **Preventivo** nella barra degli strumenti del portale di gestione posizionata nella parte superiore dello schermo, anche se l'utente non si trova nel modulo Vendite. Questa opzione apre automaticamente la procedura per la creazione guidata di nuovi preventivi, tramite la quale è possibile creare i preventivi come descritto nei passaggi seguenti.

3. Nel Passaggio 1 della procedura guidata per la creazione del nuovo preventivo, definire quanto segue.
   - **Descrizione**: inserire una descrizione per il preventivo.
   - **Utente finale**: selezionare l'utente finale pertinente. L'utente selezionato riceverà il preventivo non appena viene inviato all'approvazione.

     Nota
     Se per l'utente finale selezionato non sono state definite le informazioni di fatturazione, alla procedura guidata per la creazione del preventivo viene aggiunto l'ulteriore passaggio **Dati di fatturazione**. Facendo clic su **Avanti**, è possibile completare i campi relativi alle informazioni di fatturazione, inclusi i termini di pagamento e l'indirizzo. Queste informazioni vengono quindi salvate e utilizzate quando si seleziona l'utente finale in altri moduli di Advanced Automation (PSA). Per ulteriori informazioni sui campi delle informazioni di fatturazione, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47).

- **Nome società**: questo campo viene compilato automaticamente con l'azienda corrispondente quando viene definito il campo **Utente finale**.
- (Facoltativo) Nella casella dell'editor, definire un'introduzione per il preventivo. Questo testo può includere una breve presentazione con descrizione del preventivo. Per esempio: *Grazie per aver richiesto un preventivo per l'acquisto di nuovi laptop. Abbiamo incluso un elenco dei nostri modelli più recenti.* Se necessario, è possibile aggiungere al testo formattazione e immagini.

4. Fare clic su **Avanti**. Viene visualizzato il passaggio successivo della procedura guidata per la creazione del nuovo preventivo.
5. Fare clic su **Aggiungi modello** o su **Aggiungi prodotto** per selezionare il prodotto o il modello pertinente.
   - Se si fa clic su **Aggiungi modello**, viene richiesto di selezionare un modello di preventivo; fare clic su **Aggiungi** per aggiungere il modello corrispondente al preventivo. È possibile selezionare modelli di preventivo e/o prodotti aggiuntivi come necessario.
   - Se si fa clic su **Aggiungi prodotto**, selezionare la categoria pertinente nel campo **Categoria prodotto**. Quindi selezionare un prodotto dall'elenco disponibile nel campo **Prodotti**.

     Se il prodotto selezionato è un prodotto non di contratto (cioè un articolo di vendita standard, come un componente hardware), definire i campi **Articolo di inventario**, **Quantità** e **Sconto**, come necessario. I campi **Prezzo** e **Descrizione** vengono compilati automaticamente con i dettagli dell'articolo di inventario selezionato.

     Se il prodotto selezionato è un prodotto contratto (ad esempio una fatturazione ripetuta per i servizi gestiti) vengono visualizzati i seguenti campi aggiuntivi:
     - **Intervallo di fatturazione**: selezionare una tra le opzioni **Ogni mese**, **Trimestrale**, **Semestrale** o **Ogni anno**.
     - **Quando emettere fattura**: selezionare una tra le opzioni **Anticipatamente** o **Successivamente**.
     - **Metodo di pagamento**: scegliere tra **Pagamento manuale** o **Addebito diretto**. L'opzione **Addebito diretto** consente ai clienti di saldare le fatture tramite bonifico bancario o tramite una delle integrazioni con i sistemi di pagamento disponibili (PayPal, Stripe) o di inviare la fattura ai propri istituti bancari per l'elaborazione dell'addebito diretto.
     - **Periodo di contratto (mesi)**: selezionare il numero di mesi desiderato (indipendentemente dall'opzione selezionata nel campo **Intervallo di fatturazione**).
6. Fare clic su **Aggiungi** per aggiungere il prodotto al preventivo.

   Se si desidera aggiungere altri prodotti, nella schermata di riepilogo visualizzata fare clic su **Aggiungi modello** o **Aggiungi prodotto**.

   Nota
   Se uno qualsiasi dei prodotti selezionati include campi obbligatori che non sono stati completati, prima di procedere verrà richiesto di completare questi campi per i prodotti pertinenti.

7. Fare clic su **Avanti**. Viene visualizzato l'ultimo passaggio della procedura guidata per la creazione del nuovo preventivo.
8. Rivedere il preventivo, quindi selezionare:

- **Salva** per salvare il preventivo. Il preventivo non viene inviato ai clienti, ma potrà essere modificato come necessario e inviato in un secondo momento.
- Fare clic su **Salva e invia** per salvare e inviare il preventivo all'utente selezionato.

Se il preventivo viene accettato o rifiutato dal cliente tramite e-mail o telefono, contrassegnare il preventivo nella scheda **Preventivi** come necessario. Se invece il preventivo viene accettato o rifiutato dal cliente nel portale dei preventivi, la scelta effettuata viene automaticamente riportata nella scheda **Preventivi**. Per ulteriori informazioni, consultare "Contrassegnare un preventivo come accettato o rifiutato" (pag. 276).

Per ulteriori informazioni su come Advanced Automation (PSA) gestisce l'accettazione o il rifiuto dei preventivi, consultare "In che modo Advanced Automation (PSA) elabora i preventivi accettati o rifiutati" (pag. 275).

In che modo Advanced Automation (PSA) elabora i preventivi accettati o rifiutati

Quando un cliente accetta o rifiuta un preventivo, è possibile individuare il preventivo pertinente nella scheda **Preventivi** e contrassegnarlo come accettato o rifiutato (per ulteriori informazioni, consultare "Contrassegnare un preventivo come accettato o rifiutato" (pag. 276)). A seconda dell'opzione selezionata, Advanced Automation (PSA) avvia diversi eventi.

Quando un preventivo viene contrassegnato come accettato

Quando si contrassegna un preventivo come accettato dal cliente, o il cliente accetta il preventivo, vengono avviati i seguenti eventi:

- Il cliente visualizza un messaggio di ringraziamento.
- Lo stato del preventivo nella scheda **Preventivi** viene aggiornato a **Accettato**. A questo punto non è più possibile modificare il preventivo, che potrà soltanto essere copiato.
- All'utente MSP pertinente (l'utente che ha creato il preventivo) viene inviata una notifica che informa che il preventivo è stato accettato.
- Il sistema crea un ticket generico inerente al preventivo, che contiene tutti i dettagli dell'offerta. Il ticket viene assegnato allo stesso utente selezionato nel preventivo, al quale è possibile accedere tramite il modulo **Service Desk**.
- Viene creato un ticket di tipo ordine di acquisto, che è quindi assegnato al responsabile del gruppo di supporto impostato per questo tipo di ticket nelle impostazioni del preventivo. Questo ticket include solo i dettagli dei prodotti non di contratto e che non sono in magazzino.
- Per i prodotti non di contratto, vengono creati gli articoli di vendita, che possono essere visualizzati nella scheda **Articoli di vendita**.
- Per i prodotti di contratto selezionati:
  - Viene creato un nuovo contratto per il cliente e aggiunte le voci relative a tutti i prodotti di contratto inclusi nel preventivo. Se durante la definizione di un prodotto del preventivo non è stato selezionato uno specifico contratto, viene creato un nuovo contratto con questa parte del contratto. Se è stato selezionato un contratto specifico, la parte del contratto pertinente viene aggiunta al contratto specificato.

- La data di inizio del contratto è impostata in base alla data di accettazione del preventivo. La data di fine del contratto è impostata in base alla data di accettazione del preventivo a cui si somma la durata del contratto definita nel campo **Periodo di contratto (mesi)** del preventivo.

Quando un preventivo viene contrassegnato come rifiutato

Quando si contrassegna un preventivo come rifiutato dal cliente, vengono avviati i seguenti eventi:

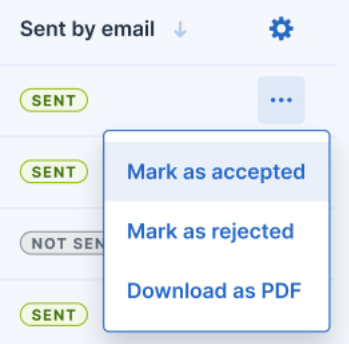
- Il cliente visualizza un messaggio di ringraziamento, che lo informa che il preventivo è stato contrassegnato come rifiutato.
- Lo stato del preventivo nella scheda **Preventivi** viene aggiornato a **Rifiutato**. A questo punto non è più possibile modificare il preventivo, che potrà soltanto essere copiato.
- All'utente MSP pertinente (l'utente che ha creato il preventivo) viene inviata una notifica per informare che il preventivo è stato rifiutato.
- Gli articoli di inventario vengono aggiornati come 'in magazzino', e resi disponibili per altri preventivi o articoli di vendita.

Contrassegnare un preventivo come accettato o rifiutato

Quando un cliente accetta o rifiuta un preventivo, questo può essere contrassegnato come necessario nella scheda **Preventivi**. L'operazione attiva una serie di eventi in Advanced Automation (PSA). Per ulteriori informazioni, consultare "In che modo Advanced Automation (PSA) elabora i preventivi accettati o rifiutati" (pag. 275).

Per contrassegnare un preventivo come accettato o rifiutato

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Nella scheda **Preventivi**, individuare il preventivo pertinente.
3. Nella colonna più a destra, fare clic sull'icona dei puntini di sospensione e selezionare una delle opzioni seguenti:
   - **Contrassegna come accettato**
   - **Contrassegna come rifiutato**



   Lo stato del preventivo viene automaticamente aggiornato.

Aggiornamento di un preventivo

È possibile modificare i preventivi come necessario. Non è possibile eliminare un preventivo.

Nota
È possibile modificare un preventivo solo se il relativo stato è impostato su **In sospeso**. Non è possibile aggiornare un preventivo se è stato accettato o rifiutato (può tuttavia essere copiato; consultare "Copia di un preventivo" (pag. 277)).

Per aggiornare un preventivo

1. Passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Preventivi**.
2. Fare clic sul preventivo da aggiornare. I dettagli del preventivo sono visualizzati nella barra laterale destra.
3. Aggiornare le sezioni pertinenti come necessario.
   - Nella barra degli strumenti nella parte alta della barra laterale selezionare una tra le seguenti opzioni:
     - **Contrassegna come rifiutato**: contrassegna il preventivo come rifiutato nella scheda **Preventivi**. Per ulteriori informazioni su ciò che accade quando il preventivo viene rifiutato, consultare "In che modo Advanced Automation (PSA) elabora i preventivi accettati o rifiutati" (pag. 275).
     - **Scarica PDF**: scarica una copia del preventivo in formato PDF.
     - **Vai al portale dei preventivi**: visualizza la versione online del preventivo.
     - **Invia nuovamente e-mail**: invia nuovamente l'e-mail con il preventivo all'utente selezionato.
   - Nella sezione **Informazioni sul preventivo**, fare clic sull'icona a matita e aggiornare i campi pertinenti. Al termine, fare clic su ✓.
   - Nella sezione **Prodotti**, fare clic sul + per aggiungere un nuovo prodotto o aggiornare un prodotto esistente associato al preventivo. Al termine, fare clic su ✓.
4. Dopo aver completato l'aggiornamento del preventivo, chiudere la barra laterale.

Copia di un preventivo

È possibile copiare un preventivo in qualsiasi stato esso sia.

Per copiare un preventivo

1. Passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Preventivi**.
2. Nella riga del preventivo da copiare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Copia**.
3. Aggiornare il preventivo come necessario. Per ulteriori informazioni, consultare "Creazione di un preventivo" (pag. 273).

Gestione dei modelli di preventivo

I modelli di preventivo consentono di registrare le offerte standard e di utilizzarle nei preventivi per i clienti, così da evitare di aggiungerle e configurarle singolarmente e manualmente quando si crea un nuovo preventivo. Ad esempio, è possibile creare un modello di preventivo chiamato "Servizi

gestiti" che include una gamma di prodotti tra cui soluzioni di backup, sicurezza, ripristino, servizi gestiti, supporto e monitoraggio.

Advanced Automation (PSA) consente di aggiungere, modificare o eliminare i modelli di preventivo come necessario (consultare "Modifica o eliminazione di un modello di preventivo" (pag. 278)).

Nota
Al momento, i modelli di preventivo non supportano gli articoli di inventario.

Aggiunta di un nuovo modello di preventivo

1. Passare a **Vendite e fatturazione > Vendite**.
2. Nello schermo visualizzato, fare clic sulla scheda **Modelli di preventivo**.
3. Se non sono presenti modelli di preventivo, fare clic su **Aggiungi nuovo modello**. Altrimenti, fare clic su **+ Nuovo**.
4. Nel campo **Nome modello**, inserire un nome per il modello.
5. Nel campo **Seleziona prodotti**, selezionare il prodotto pertinente. Fare quindi clic su **Aggiungi**.
6. Per aggiungere ulteriori prodotti al modello, fare clic su **Aggiungi prodotto** e selezionare il prodotto pertinente. Ripetere questi passaggi secondo necessità.
7. Fare clic su **Fine**. Il nuovo modello è mostrato nella scheda **Modelli di preventivo**, ed è impostato su **Attivo** per impostazione predefinita.

Modifica o eliminazione di un modello di preventivo

1. Passare a **Vendite e fatturazione > Vendite > Modelli di preventivo**. La scheda visualizzata elenca i modelli di preventivo esistenti.
2. Per aggiornare un preventivo, fare clic sul modello pertinente e quindi sull'icona a matita nel pannello a destra. Aggiornare il modello come necessario. Al termine, fare clic su ✓.
3. Per eliminare un modello, fare clic sull'icona dei puntini di sospensione del modello pertinente, quindi fare clic su **Elimina**.

Gestione degli articoli di vendita

Gli articoli di vendita sono servizi o merci forniti a un cliente che dovranno essere contabilizzati e fatturati.

Nota
Questa funzionalità è disponibile solo agli utenti ai quali sono stati assegnati i ruoli seguenti. Amministratore, Direttore, Responsabile gruppo, Responsabile contabilità, Contabilità, Vendite

Gli articoli di vendita sono gestiti nella scheda **Articoli di vendita** nel menu **Vendite e fatturazione > Vendite**), da cui è possibile visualizzare tutti gli articoli di vendita in uso. Sono inoltre disponibili informazioni su ciascun articolo, incluso il cliente, il volume totale delle vendite per l'articolo (sconti esclusi), la data di fatturazione e se l'articolo di vendita è stato fatturato o meno. È inoltre possibile filtrare e ordinare gli articoli visualizzati per individuare più facilmente un articolo o un set di articoli

specifici; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali articoli di vendita dovranno essere visualizzati.

Nota
Per i clienti che utilizzano i servizi e i prodotti Acronis, il sistema crea automaticamente gli articoli di vendita come parte della fatturazione mensile e a partire dalla prima attivazione di Advanced Automation (PSA) per ciascun partner.

Gli articoli di vendita in **Bozza** vengono creati per aiutare ad automatizzare la fatturazione dei clienti, tuttavia non si può fatturare un cliente fino a quando non vengono inviati i dati di fatturazione. È possibile fornire i dati di fatturazione dell cliente in diversi modi, anche durante la creazione di un contratto o facendo clic sull'articolo di vendita pertinente nella scheda **Articoli di vendita** e quindi facendo clic su **Aggiungi informazioni di fatturazione** nel messaggio del banner. Per ulteriori informazioni, vedere "Onboarding di clienti esistenti" (pag. 209).

Dopo aver fornito i dati di fatturazione per il cliente, gli articoli di vendita in **Bozza** vengono automaticamente modificati in **In attesa** e saranno disponibili per la fatturazione.

Advanced Automation (PSA) consente di gestire gli articoli di vendita che sono:

- Registrati automaticamente in base alle parti del contratto.
- Registrati automaticamente come risultato di attività basate su ticket.
- Registrazione automatica dei clienti che utilizzano i servizi e i prodotti Acronis, ma senza parti del contratto.
- Registrati manualmente.

Creazione di un nuovo articolo di vendita

La scheda **Articoli di vendita** visualizza tutti gli articoli di vendita che sono stati creati e fatturati. È inoltre possibile aggiungere nuovi articoli di vendita.

Per creare un articolo di vendita

1. Passare a **Vendite e fatturazione** > **Vendite** e fare clic sulla scheda **Articoli di vendita**.

   Nota
   Se il modulo Advanced Automation (PSA) è attivato per l'account, è anche possibile fare clic su **Nuovo** > **Articolo di vendita** nella barra degli strumenti del portale di gestione posizionata nella parte superiore dello schermo, anche se l'utente non si trova nel modulo Vendite. Questa opzione apre automaticamente la procedura per la creazione guidata di nuovi articoli di vendita, tramite la quale è possibile creare gli articoli come descritto nei passaggi seguenti.

2. Nella sezione **Informazioni cliente**, procedere come segue.
   - Selezionare il cliente pertinente. Una volta selezionato il cliente, alcuni dei campi seguenti verranno compilati automaticamente con le informazioni pertinenti sul cliente:

  - **Entità di fatturazione** (Selezionare manualmente l'entità da inserire; tale entità verrà inclusa nella fattura).
  - **Metodo di pagamento** (**Pagamento manuale** o **Addebito diretto**. L'opzione **Addebito diretto** consente ai clienti di saldare le fatture tramite bonifico bancario o tramite una delle integrazioni con i sistemi di pagamento disponibili (PayPal, Stripe) o di inviare la fattura ai propri istituti bancari per l'elaborazione dell'addebito diretto).
  - **Invia fattura tramite** (**Posta** o **E-mail**).
  - **Indirizzo di posta elettronica del contatto**.
- Indicazione della data della fattura.

3. Nella sezione **Indirizzo cliente** vengono visualizzati i dettagli relativi al cliente selezionato. Se necessario, è possibile aggiornare manualmente l'indirizzo per questo specifico articolo di vendita.

   Nota
   Se per il cliente selezionato non sono state definite le informazioni di fatturazione, viene aggiunto l'ulteriore passaggio **Dati di fatturazione**. Facendo clic su **Avanti**, è possibile completare i campi relativi alle informazioni di fatturazione, inclusi i termini di pagamento e l'indirizzo. Queste informazioni vengono quindi salvate e utilizzate quando si seleziona il cliente in altri moduli di Advanced Automation (PSA). Per ulteriori informazioni sui campi delle informazioni di fatturazione, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47).

4. Fare clic su **Avanti**. Viene visualizzata la scheda **Prodotti**, nella quale è possibile aggiungere qualsiasi prodotto all'articolo di vendita.

   Nota
   Un prodotto è un servizio o un articolo che viene venduto ai clienti. Ad esempio, abbonamenti per antivirus o supporto ad-hoc.

5. Fare clic su **Aggiungi prodotto** per selezionare i prodotti predefiniti pertinenti in Advanced Automation (PSA) (inclusi i prodotti Acronis).

   Nota
   Verificare di aver creato uno o più prodotti con l'opzione **Utilizza nei contratti** disabilitata. Ciò garantisce che i tipi di prodotto pertinenti siano disponibili quando si crea un articolo di vendita (se un prodotto ha l'impostazione **Utilizza nei contratti**, può essere utilizzato solo nei contratti).

6. Nel campo **Prodotto**, selezionare il prodotto pertinente.
7. Specificare **Quantità** e **Prezzo** nei rispettivi campi.
8. (Facoltativo) Selezionare la casella di controllo **Applica sconto** (se selezionata, è possibile inserire il valore dello sconto e il motivo per cui viene effettuato) e una **Descrizione** del prodotto.

9. Fare clic su **Aggiungi** per aggiungere il prodotto all'articolo di vendita. Per aggiungere ulteriori prodotti, fare clic su **Aggiungi prodotto** e ripetere i passaggi precedenti.
10. Fare clic su **Avanti**. Viene visualizzata la scheda **Nota per voce**.
11. Fare clic su **Aggiungi nota per voce**, inserire la descrizione richiesta, quindi fare clic su **Aggiungi**. Ripetere la procedura per aggiungere note per voci aggiuntive.
12. Fare clic su **Fine**. L'articolo di vendita viene aggiunto alla scheda **Articoli di vendita**.

Modifica di articoli di vendita

È possibile modificare ed eliminare qualsiasi articolo di vendita, come necessario.

Nota
La modifica o l'eliminazione di un articolo di vendita è possibile solo se l'articolo non è ancora stato fatturato. Dopo essere stato incluso in una fattura, l'articolo di vendita può solo essere visualizzato e non può essere modificato né eliminato.

Per modificare un articolo di vendita

1. Passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Articoli di vendita**.
2. Fare clic sull'articolo di vendita da modificare. I dettagli dell'articolo di vendita sono visualizzati nella barra laterale destra.
3. Modificare le rispettive sezioni come necessario.
   - Nella sezione **Informazioni cliente**, fare clic sull'icona a matita e modificare i campi pertinenti. Quindi fare clic su **Salva**.
   - Nelle sezioni **Prodotti** e **Note per voce**, fare clic su  per aggiungere nuovi prodotti o note per voci. In alternativa, fare clic sull'icona a matita o a cestino per modificare o eliminare le voci esistenti. Per ogni prodotto o nota per voce aggiunti o modificati, al termine fare clic su **Salva**.

     Nota
     Se un articolo di vendita è in stato **Bozza**, è possibile modificare le parti del prodotto e le righe dell'articolo, ma non la sezione **Informazioni cliente**. È possibile anche inviare le informazioni di fatturazione al cliente facendo clic su **Aggiungi informazioni di fatturazione** nel messaggio del banner visualizzato. Così facendo, lo stato dell'articolo di vendita cambia a sua volta in **In sospeso**, il che significa che ora potrà essere fatturato.

     Per ulteriori informazioni sui campi modificabili in un articolo di vendita, vedere "Creazione di un nuovo articolo di vendita" (pag. 279).

Per eliminare un articolo di vendita

1. Passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Articoli di vendita**.
2. Nella colonna a destra dell'articolo di vendita da eliminare, fare clic sull'icona dei puntini di sospensione, quindi selezionare **Elimina**.

   [Facoltativo] Per selezionare più articoli di vendita da eliminare, selezionare innanzitutto le caselle di controllo nella colonna di sinistra delle righe degli articoli di vendita pertinenti. Fare clic su **Elimina** (sopra all'elenco degli articoli di vendita). L'opzione di eliminazione in blocco non è abilitata se si selezionano sia articoli di vendita fatturati sia non fatturati.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Lavorare con i contratti

La scheda **Contratti** mostra tutti i contratti creati per i clienti.

Ogni contratto definisce l'insieme di servizi che vengono forniti a un cliente, incluso prezzo, termini e condizioni. Le fatture vengono emesse in base ai termini di pagamento definiti nel contratto.

Durante la creazione di un contratto, completare la procedura guidata visualizzata a schermo aggiungendo le informazioni pertinenti sul contratto, i dati di fatturazione e le parti del contratto.

Per accedere alle funzionalità per i contratti, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Contratti**.

Creazione di un nuovo contratto

Una procedura suddivisa in tre fasi principali guida l'utente durante la creazione di un nuovo contratto. Le tre fasi prevedono:

- L'inserimento delle informazioni di base sul contratto
- L'aggiunta dei dati di fatturazione
- L'aggiunta di parti del contratto

> **Nota**
> Se è stata attivata la funzionalità Advanced Automation (PSA) (consultare "Attivazione di Advanced Automation (PSA)" (pag. 203)) ed è stato definito un nuovo cliente con le relative informazioni di fatturazione, al momento della creazione di un nuovo contratto per tale cliente la procedura guidata prevede solo due fasi: l'inserimento delle informazioni di base sul contratto e l'aggiunta delle parti del contratto.

Al completamento della procedura guidata, il contratto viene automaticamente aggiunto all'elenco dei contratti esistenti visualizzato nella scheda **Contratti**. I contratti possono essere visualizzati e aggiornati secondo necessità; fare riferimento a "Modifica di un contratto" (pag. 286).

Per creare un nuovo contratto

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Fare clic sulla scheda **Contratti**, quindi scegliere **+ Nuovo contratto**.

Nota
Se sono presenti clienti esistenti ai quali non è assegnato alcun contratto, verrà richiesto di creare contratti per questi clienti. Fare clic su **Crea** o **Crea contratti per clienti esistenti** per selezionare il cliente di interesse, quindi fare clic su **Avanti**. È necessario definire le informazioni del contratto, come descritto nella prossima fase.

3. Nella procedura guidata visualizzata, definire le seguenti informazioni sul contratto:
   - **Numero di riferimento**: (Facoltativo) Il numero di riferimento che è spesso utilizzato nei contratti cartacei.
   - **Nome del contratto**: Il nome del contratto.
   - **Organizzazione**: Selezionare l'organizzazione pertinente dall'elenco a discesa.
   - **E-mail di contatto**: (Facoltativo) E-mail di contatto per questo contratto.
   - **Entità di fatturazione**: Selezionare l'entità di fatturazione pertinente.
   - Nella sezione **Dettagli di pagamento**, scegliere il periodo di fatturazione (**Ogni mese**, **Trimestrale**, **Semestrale**, **Ogni anno**), quando fatturare (**Anticipatamente** o **Successivamente**) e selezionare il metodo di pagamento (**Pagamento manuale** o **Addebito diretto**. L'opzione **Addebito diretto** consente ai clienti di saldare le fatture tramite bonifico bancario o tramite una delle integrazioni con i sistemi di pagamento disponibili (PayPal, Stripe) o di inviare la fattura ai propri istituti bancari per l'elaborazione dell'addebito diretto).
   - Nella sezione **Periodo di contratto**, definire la durata del contratto (se il contratto non ha un termine definito, selezionare la casella di controllo **Per sempre**); scegliere se inviare la fattura per posta ordinaria o per e-mail.
   - Nella sezione **Indirizzo cliente**, inserire i dettagli dell'indirizzo pertinente.
   - Se si desidera includere un blocco ore per i servizi offerti, abilitare l'opzione **Blocco ore**. Definire quindi il numero di blocchi ore e la percentuale relativa alla soglia di rinnovo. Selezionare la casella di controllo **Acconto** se il contratto prevede un accordo con acconto (e se i blocchi ore vengono fatturati ogni mese, ogni trimestre o ogni semestre). Una volta effettuata la selezione, sono disponibili due opzioni:

     Scarta ore rimanenti (per scartare le ore rimanenti non consumate durate il periodo di fatturazione in acconto).

     Mantieni ore rimanenti (per conservare le ore rimanenti non consumate durate il periodo di fatturazione in acconto).

     Il tempo dedicato ai ticket viene fatturato separatamente oppure contrassegnato come non fatturabile se il lavoro fa parte di un accordo a prezzo fisso, o prenotato a fronte del credito di blocchi ore corrente.

Nota
Le ore di blocco consentono di riservare un blocco di ore di supporto per i clienti; vengono fatturate in base alla tariffa prodotto del blocco ore predefinita, come specificato nelle impostazioni della fattura. La soglia di rinnovo viene utilizzata per inviare una notifica quando nel blocco corrente resta un numero specificato di ore. La notifica consente di creare un articolo di vendita per un nuovo blocco facendo clic su **Rinnova blocchi ore**. Una volta fatturato il nuovo blocco, viene visualizzato nel saldo blocco ore disponibile.

- Selezionare la casella di controllo **Rateizzato** se le modifiche apportate al contratto verranno fatturate in rate o al prezzo pieno.

4. Fare clic su **Avanti** per passare alla Fase 2 della procedura guidata del contratto, l'inserimento delle informazioni di fatturazione. Per ulteriori informazioni sui campi di fatturazione disponibili, consultare "Definizione delle informazioni di fatturazione per un tenant" (pag. 47). Se per questo cliente sono già state inserite le informazioni di fatturazione, passare alla Fase 3 della procedura guidata, che prevede l'aggiunta delle parti del contratto (vedere di seguito).
5. Fare clic su **Avanti** per passare alla Fase 3 della procedura guidata del contratto, l'aggiunta delle parti del contratto.
6. Fare clic su **Aggiungi parte del contratto**.

Nota
Se il cliente selezionato ha definito prodotti o servizi Acronis, verrà richiesto di modificarli o eliminarli, secondo necessità. È quindi possibile aggiungere ulteriori parti del contratto, come descritto di seguito.

7. Definire i campi seguenti:
   - **Tipo di parte del contratto**: Selezionare il tipo di parte pertinente del contratto tra una delle seguenti opzioni:
     - **Tipo predefinito**: Utilizzato per contratti generici che non si avvalgono di integrazioni.
     - **Servizio ICT**: questo tipo di servizio permette di vendere un servizio ICT (Information and Communication Technology), ad esempio lo *storage di file*. Quando si offre questo tipo di servizio, è possibile aggiungere più risorse ICT, tra cui data center, server di storage, switch di rete, ecc. Queste risorse possono anche essere utilizzate in altre parti del contratto. Quando, ad esempio, si crea il servizio ICT *Storage di file*, è possibile aggiungere il data center, il server di storage e lo switch; quando si aggiunge un altro servizio ICT che utilizza il data center, è possibile aggiungere il data center anche in questa altra parte del contratto. Quando si crea un ticket per il cliente, il sistema permette di selezionare un servizio ICT e quindi le risorse a questo associate.
     - **Servizio gestito**: Questo tipo di contratto viene utilizzato in genere per i servizi gestiti, ad esempio la *Gestione di workstation*. Aggiungere i sistemi pertinenti alla parte del contratto. Al termine, le risorse vengono rimosse dall'elenco dei sistemi disponibili che così non potranno essere collegati ad altre parti del contratto.

- Nella sezione **Prodotto o servizi**, selezionare i prodotti o i servizi pertinenti che si desidera aggiungere, inclusa la quantità e il prezzo del prodotto o del servizio.

  Nel campo **Quantità effettiva** viene definita la quantità di servizio attualmente fornita al cliente nell'ambito del contratto. Questo valore può essere impostato:
  - **Manualmente**: al cliente viene fatturato un importo fisso del servizio per ogni periodo di fatturazione. Ad esempio, cinque workstation gestite ogni mese.
  - **Automaticamente**: al cliente viene fatturato l'importo del servizio segnalato da una delle integrazioni abilitate. Ad esempio, cinque server vengono segnalati dall'integrazione di Acronis Cyber Cloud in un mese, e sei server vengono segnalati il mese successivo.

  Il campo **Quantità minima** permette di impostare una quantità minima di servizio da fatturare ai clienti. Se il valore definito nel campo **Quantità effettiva** è superiore al valore definito nel campo **Quantità minima**, per la fatturazione viene utilizzata la quantità effettiva. Se il valore definito nel campo **Quantità minima** è superiore al valore definito nel campo **Quantità effettiva**, viene utilizzata la quantità minima. Questi campi vengono utilizzati anche per calcolare l'utilizzo e la redditività nei report.

  La quantità minima fatturabile migliora l'opportunità di vendere servizi come pacchetti. Ad esempio, se si crea un contratto con un cliente per il backup di almeno due dispositivi e l'utilizzo di almeno 500 GB di storage, la fattura creata include due voci per i dispositivi e per lo storage, senza creare un articolo di vendita per lo storage. Al cliente può essere fatturato anche qualsiasi utilizzo superiore alla quantità minima specificata nel contratto; in questo caso viene creato un articolo di vendita separato per lo storage utilizzato oltre ai 500 GB definiti.
- Nella sezione **Periodo di contratto**, definire il periodo pertinente. Se il contratto non ha data di fine, selezionare la casella di controllo **Per sempre**. Per impostazione predefinita, queste date vengono copiate dalle impostazioni delle informazioni del contratto (vedere sopra). Tenere presente che l'intervallo delle date non può essere inferiore all'intervallo delle date del contratto principale. Per applicare un periodo più lungo, sarà necessario adeguare il contratto principale.
- Fare clic sull'opzione **Prova** se si desidera che il contratto faccia parte di un periodo di prova. Per definire il periodo di prova, selezionare il numero di mesi desiderati. Le parti del contratto di prova vengono incluse durante un ciclo di fatturazione con prezzi pari a zero, a solo scopo informativo. Al termine del periodo di prova, la parte del contratto mostrerà il prezzo standard nelle fatture generate.

  Nota
  L'opzione di prova può essere applicata solo una volta per ogni parte del contratto. Inoltre, se la parte del contratto selezionata è già stata fatturata in precedenza, non è possibile abilitare l'opzione di prova.

- **Integrazioni**: Selezionare l'integrazione pertinente. Quando un'integrazione è selezionata, viene visualizzato il campo **Mostra sistemi in fattura**. Questo campo determina se i dettagli del sistema sono inclusi nella fattura; per impostazione predefinita è selezionata l'opzione **Sì**.

Le integrazioni consentono di collegare la quantità di una parte di contratto all'utilizzo effettivo fornito dall'integrazione selezionata (ad esempio il numero di workload attivi per un cliente specifico oppure il numero di virtual machine o la quantità di gigabyte utilizzati da un cliente nello storage in hosting).

I workload disponibili includono quelli con i prodotti e servizi Acronis (ad esempio Cyber Disaster Recovery Cloud e Cyber Protection) e le integrazioni RMM.

Per trovare i workload integrati pertinenti, applicare un filtro per cliente (ovvero filtrare i workload correlati al cliente selezionato), per tipo di workload (i workload di un tipo specifico) e per singoli workload (eseguire una ricerca e selezionare i workload pertinenti dall'elenco dei workload).

In questa sezione è anche possibile selezionare un'integrazione RMM e collegare i diversi agenti associati a tale integrazione (affinché la funzionalità di avviso tramite e-mail di RMM funzioni correttamente, è necessario che i sistemi corretti siano stati aggiunti a contratti validi). Advanced Automation (PSA) utilizza questi agenti per connettere il gruppo o il sito RMM al cliente corretto. Avvalendosi di queste informazioni, può applicare lo SLA al ticket, in base al contratto al quale è collegato il sistema.

Nota
Viene inoltre visualizzata un'ulteriore casella di controllo **Aggiornamenti automatici** e abilitato il calcolo automatico del numero di workload per le fatture. Quando selezionata, disabilita il campo **Quantità effettiva** nella sezione **Prodotto o servizi**.

- **Contratto sui livelli di servizio (SLA)**: Selezionare lo SLA pertinente.

8. Fare clic su **Aggiungi** per aggiungere la parte del contratto al contratto.
9. (Facoltativo) Fare clic su **Aggiungi parte del contratto** per aggiungere ulteriori parti del contratto.
10. Fare clic su **Fine**. Il contratto viene aggiunto all'elenco dei contratti esistenti visualizzato nella scheda **Contratti**.

Modifica di un contratto

In qualsiasi momento è possibile modificare un contratto, inclusi i prodotti o i servizi collegati a un contratto.

Nota
Non è possibile eliminare un contratto o una parte di contratto. Per bloccare un contratto, è necessario impostare il periodo di contratto su "fine" (ad esempio, alla fine del mese corrente). Questa impostazione dovrebbe essere applicata prima alle parti del contratto pertinente, e quindi al contratto stesso. Il contratto risulterà quindi inattivo, ma ancora disponibile se si esegue una ricerca.

Per modificare un contratto

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Nella scheda **Contratti**, fare clic sul contratto da modificare.
3. Nel pannello a destra, modificare le informazioni del contratto pertinente. Fare clic sull'icona a matita in ogni sezione come necessario; al termine fare clic su ✓.

   Per ulteriori informazioni sui campi modificabili, consultare "Creazione di un nuovo contratto" (pag. 282).

   Nota
   Se per un contratto sono stati abilitati i blocchi ore, è possibile rinnovarli manualmente facendo clic su **Rinnova blocchi ore**. Viene creato automaticamente un nuovo articolo di vendita e viene visualizzato un messaggio di conferma.

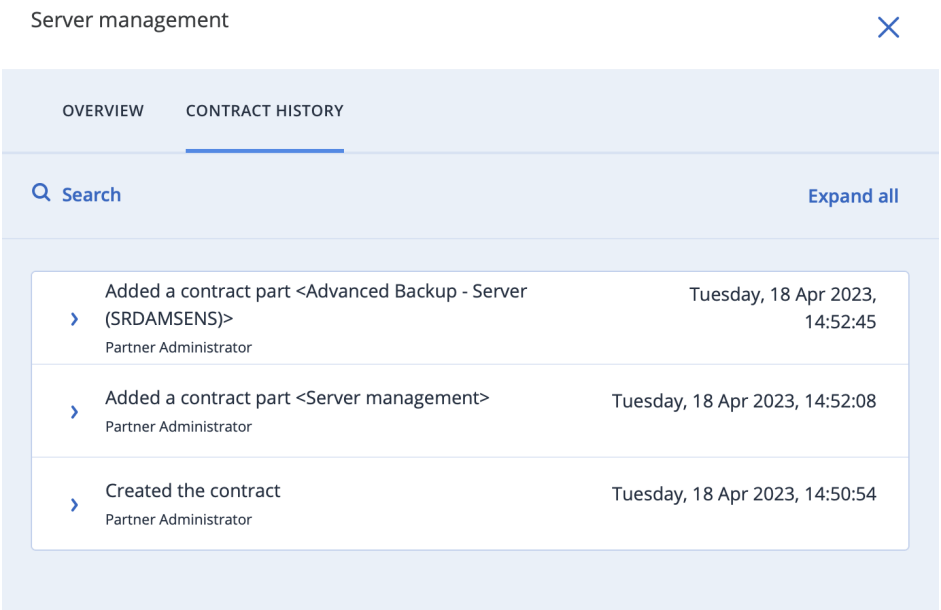
4. Al termine, fare clic su **Salva**.

Rivedere la cronologia delle modifiche apportate a un contratto

È possibile rivedere le modifiche apportate a un contratto durante tutto il ciclo di vita del contratto. Il registro che archivia la cronologia delle modifiche parte dalla creazione iniziale del contratto e prosegue con tutti gli aggiornamenti successivi.

Per rivedere la cronologia delle modifiche apportate a un contratto

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Fare clic sulla scheda **Contratti** e nell'elenco dei contratti visualizzato fare clic sul contratto pertinente.
3. Nel pannello visualizzato a destra, fare clic sulla scheda **Cronologia contratto**.



4. [Facoltativo] Utilizzare gli strumenti **Cerca** per navigare nell'aggiornamento pertinente. È anche possibile utilizzare le opzioni **Espandi tutto**/**Comprimi tutto** per visualizzare/nascondere i dettagli di tutti gli aggiornamenti.
5. Per rivedere una specifica modifica apportata a un contratto, fare clic sulla riga corrispondente. In base alla modifica apportata, vengono mostrate diverse informazioni.
   - Quando il contratto viene creato: vengono visualizzate la maggior parte delle informazioni definite al momento della creazione del contratto, incluse le informazioni per la fatturazione.
   - Quando il contratto viene aggiornato: vengono visualizzati solo gli attributi del contratto aggiornati e i rispettivi valori precedenti/nuovi.
   - Quando viene aggiunta una parte del contratto: vengono visualizzate la maggior parte delle informazioni definite al momento dell'aggiunta della parte del contratto, incluse le integrazioni abilitate.
   - Quando viene aggiornata una parte del contratto: viene visualizzata solo la parte del contratto aggiornata e i rispettivi valori precedenti/nuovi.
   - Quando viene rimossa una parte del contratto: viene visualizzato lo stato più recente della parte del contratto, incluse le integrazioni abilitate.

Lavorare con i prezzi personalizzati

Definendo prezzi personalizzati è possibile definire il prezzo di un prodotto per un cliente specifico. La funzionalità permette di automatizzare l'applicazione dei prezzi concordati con i clienti.

Se, ad esempio, la tariffa standard per un lavoro di progetto è $100 l'ora, ma con uno specifico cliente è stata concordata una tariffa di $130 l'ora, è possibile creare un prezzo personalizzato per la '*tariffa oraria lavoro di progetto*' per tale cliente, che sarà pari a $130. Ogni volta che si crea un articolo di vendita o un ticket per questo tipo di lavoro per questo specifico cliente, viene applicato il prezzo personalizzato.

Nota
È possibile personalizzare un prezzo solo se il prodotto non è un prodotto contratto.

Per accedere ai prezzi personalizzati, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Prezzi personalizzati**.

Aggiunta di un prezzo personalizzato

Per aggiungere un prezzo personalizzato

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Prezzi personalizzati**.
2. Fare clic su **+ Nuovo prezzo personalizzato**.
3. Selezionare il cliente al quale applicare il prezzo personalizzato, quindi fare clic su **Aggiungi prezzo personalizzato prodotto**. Tenere presente che l'elenco dei clienti mostra solo i clienti per i quali non sono stati ancora specificati prezzi personalizzati.
4. Nel campo **Categoria prodotto**, selezionare la categoria pertinente dall'elenco a discesa.

5. Nel campo **Prodotto**, selezionare il prodotto pertinente dall'elenco a discesa. Questo elenco mostra soltanto i prodotti con prezzi standard; i prodotti per i quali è già stato definito un prezzo personalizzato non vengono visualizzati.
6. Se si desidera rendere disponibile questo prezzo personalizzato, abilitare l'interruttore **Attivo**.
7. Inserire il prezzo personalizzato del prodotto e fare clic su **OK**.

   Per una fatturazione più precisa, nei prezzi dei prodotti utilizzati nei contratti, nei preventivi e negli articoli di vendita è possibile utilizzare fino a quattro cifre dopo il separatore decimale, come ad esempio: $0,0750. Tali prezzi vengono arrotondati nelle fatture, nei report, nelle voci fatturabili nei ticket e nelle tariffe orarie.
8. Per aggiungere un altro prezzo personalizzato, fare clic su **Aggiungi prezzo personalizzato prodotto**, oppure fare clic su **Crea**.

Modifica di un prezzo personalizzato

Per modificare un prezzo personalizzato

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Prezzi personalizzati**.
2. Fare clic sul cliente di cui modificare il prezzo personalizzato.
3. Nel pannello destra, fare clic sull'icona a matita e apportare le modifiche.

   Ad esempio, è possibile aggiungere un nuovo prezzo personalizzato (consultare "Aggiunta di un prezzo personalizzato" (pag. 288)) o modificare i dettagli di un prezzo personalizzato esistente.
4. Al termine, fare clic su ✓.

Fatture

Il modulo **Fatture** consente di gestire e tenere traccia delle fatture create per i clienti. Utilizzando questo metodo, è possibile:

- Generare nuove fatture per i clienti.
- Confermare il pagamento di una fattura.
- Inviare nuovamente una fattura.
- Tenere traccia delle fatture emesse.
- Scaricare e/o esportare una fattura o un gruppo di fatture.

Per accedere al modulo **Fatture**, nel portale di gestione passare a **Vendite e fatturazione > Fatture**.

Nota
Solo gli utenti con i ruoli Amministratore, Direttore, Contabilità, Responsabile contabilità o Vendite possono generare le fatture. Gli utenti a cui sono assegnati i ruoli di Responsabile cliente o Cliente possono solo visualizzare e scaricare le fatture.

Visualizzazione delle fatture correnti

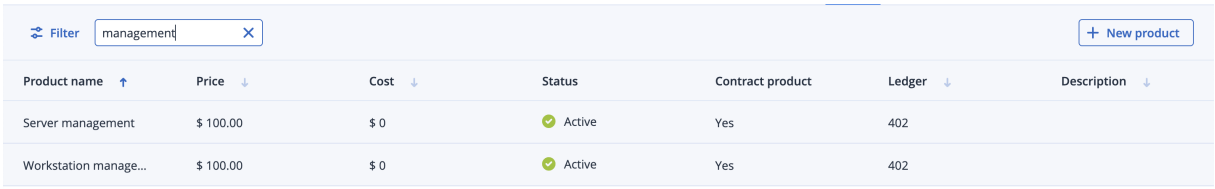
Per visualizzare le fatture correnti, nel portale di gestione passare a **Vendite e fatturazione** > **Fatture**. Nella scheda **Fatture** visualizzata, è possibile vedere tutte le fatture generate in Advanced Automation (PSA).

Vengono visualizzate informazioni su ogni fattura, incluso:

- La data in cui la fattura è stata creata.
- Lo stato del pagamento (**Confermato** o **Non confermato**), e, se il pagamento è stato saldato, la data in cui è stato eseguito.
- Se al cliente è stata inviata un'e-mail.
- L'importo della fattura.
- Se la fattura è stata sincronizzata con il software di contabilità (se attivato).

Fare clic su una fattura per visualizzare ulteriori informazioni sulla fattura stessa nel pannello a destra. Queste informazioni includono una panoramica generale della fattura, e dettagli su ogni elemento incluso nel documento. Dal pannello è anche possibile scaricare ed esportare la fattura, come necessario.

È inoltre possibile filtrare e ordinare l'elenco visualizzato per individuare una fattura specifica; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali fatture dovranno essere visualizzate.



Generazione di una nuova fattura

Quando si genera una nuova fattura o un lotto di fatture, i dati relativi alle fatture vengono inseriti utilizzando un modello di fattura (come descritto in "Impostazioni di fatturazione" (pag. 336)). Questi dati possono quindi essere inviati in forma di fattura tramite Advanced Automation (PSA) (se questo processo è stato definito nelle impostazioni di fatturazione e del contratto), oppure inviato in modo alternativo. Ad esempio, il software di contabilità in uso potrebbe essere configurato per inviare le fatture ai clienti, oppure per inviare le fatture in copia cartacea.

Se necessario, è anche possibile inviare nuovamente una fattura; consultare "Inviare nuovamente una fattura" (pag. 293).

Per generare una nuova fattura

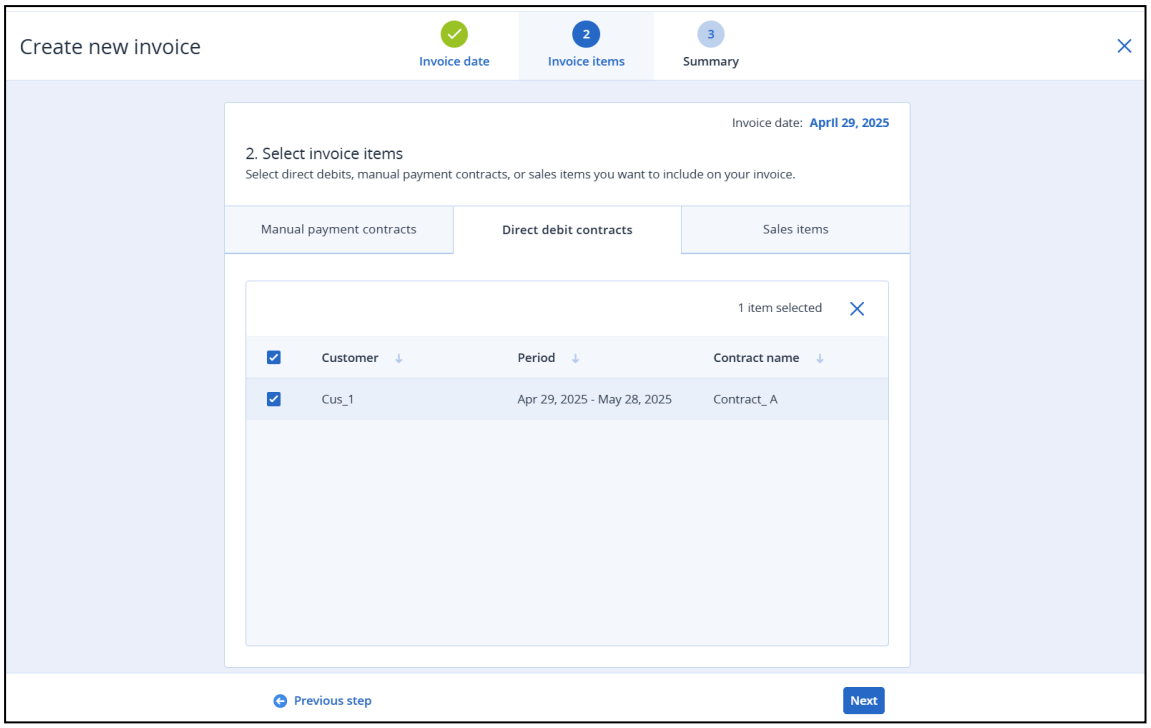
1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Fatture**.
2. Se non è ancora stata creata nessuna fattura, fare clic su **Crea nuovo**. Altrimenti, fare clic su **+ Nuovo**.

   Viene visualizzata la procedura guidata Crea nuova fattura.
3. Selezionare la data della fattura e l'entità di fatturazione pertinente. Quindi, fare clic su **Avanti**.
4. Selezionare gli addebiti diretti, i contratti con pagamento manuale e gli articoli di vendita da includere nella fattura.
   - Nella scheda **Contratti con pagamento manuale**, selezionare i contratti definiti con **Pagamento manuale**.
   - Nella scheda **Contratti con addebito diretto**, selezionare gli addebiti diretti pertinenti dall'elenco mostrato.

     Nota
     Se per un contratto è stato definito il metodo di pagamento **Addebito diretto**, viene categorizzato come contratto con addebito diretto. In questo modo i clienti possono saldare le fatture tramite bonifico bancario o tramite una delle integrazioni con i sistemi di pagamento disponibili. Possono inoltre inviare le fatture ai rispettivi istituti bancari per l'elaborazione dell'addebito diretto.

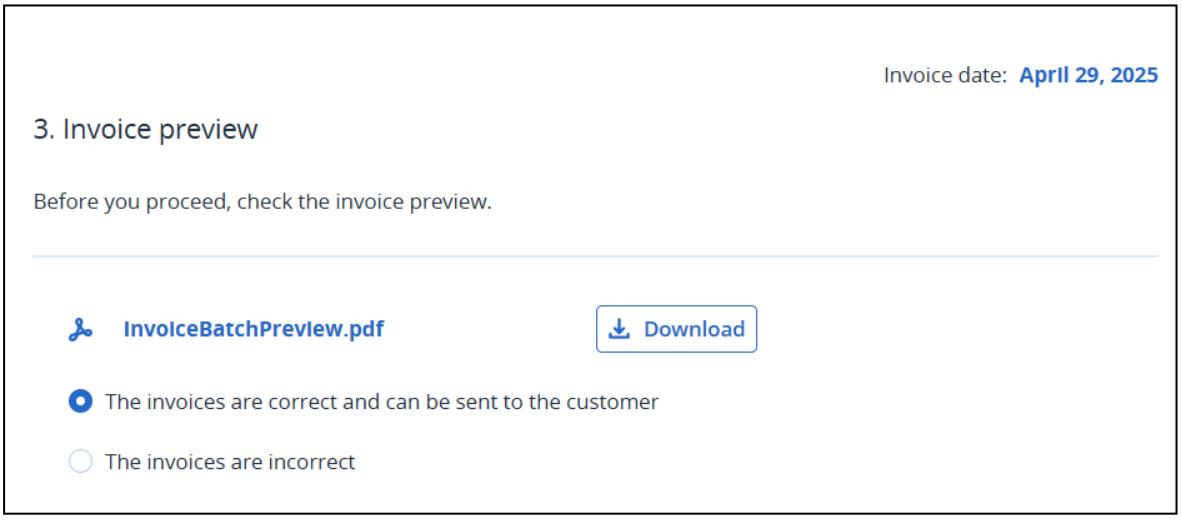
   - Nella scheda **Articoli di vendita**, selezionare gli articoli di vendita pertinenti.

     Nota
     Non è possibile selezionare gli articoli di vendita in stato **Bozza**. Tuttavia, è possibile passare il mouse sopra l'articolo e quindi fare clic su **Aggiungi informazioni di fatturazione**. Definite le informazioni di fatturazione per il cliente, l'articolo di vendita sarà disponibile per la fatturazione.



Dopo aver completato la selezione degli articoli della fattura, fare clic su **Avanti**.

5. Nella schermata Riepilogo, fare clic su **Scarica** per visualizzare un'anteprima del lotto di fatture in formato PDF.



Se l'anteprima della fattura è corretta, selezionare l'opzione **Le fatture sono corrette e possono essere inviate al cliente**.

Se l'anteprima della fattura non è corretta, selezionare l'opzione **Le fatture non sono corrette**. L'utente viene reindirizzato nella scherma Fatture e il sistema arresta il processo di fatturazione. L'utente può così ricontrollare il contratto e le voci della fattura. È possibile rielaborare la fattura fino a quando non sarà corretta.

6. Fare clic su **Fine**.

L'utente viene reindirizzato all'elenco delle fatture, dove è possibile visualizzare il lotto di fatture appena generato; vengono anche mostrate le singole fatture incluse nel lotto. A seconda delle impostazioni del cliente, le fatture vengono inviate per e-mail oppure con altri metodi.

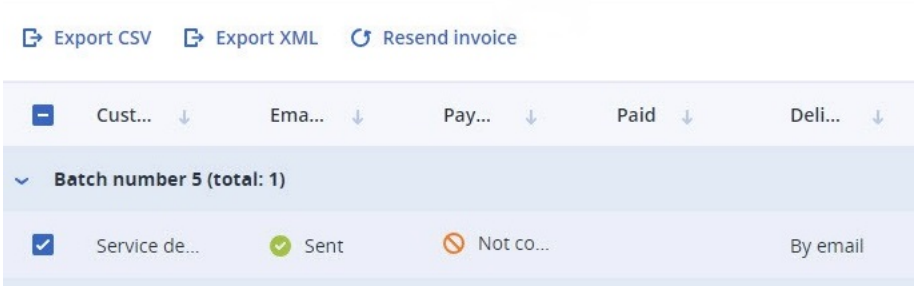
Nota
Non è possibile aggiornare una fattura, ma è possibile aggiornare singoli articoli di vendita, voci orario e parti del contratto che verranno inclusi in una fattura futura corretta. Dopo aver apportato questi aggiornamenti, è possibile generare la fattura corretta.

Inviare nuovamente una fattura

È possibile inviare nuovamente qualsiasi fattura che non sia stata ancora confermata come pagata, e che sia stata impostata per l'invio tramite e-mail. Non è possibile inviare nuovamente le fatture già pagate o impostate per l'invio tramite posta ordinaria.

Per inviare nuovamente una fattura

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Fatture**.
2. Selezionare le fatture da inviare nuovamente. Viene visualizzato il pulsante **Reinvia fattura**, come mostrato di seguito.



Nota
Se sono state selezionate più fatture ma una o più tra queste è già stata confermata come pagata o è stata impostata per l'invio tramite posta ordinaria, il pulsante **Reinvia fattura** è visualizzato, ma disabilitato.

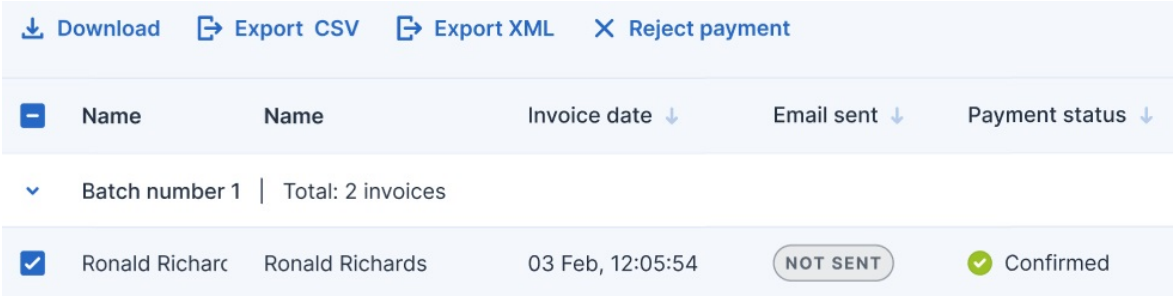
3. Fare clic su **Reinvia fattura**. La fattura viene inviata nuovamente al cliente, e viene visualizzato un messaggio di conferma.

Conferma o rifiuto del pagamento di una fattura

È possibile confermare o rifiutare manualmente il pagamento di una fattura, come necessario.

Per confermare o rifiutare un pagamento

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Fatture**.
2. Selezionare le fatture da confermare o rifiutare.
3. Se il pagamento è già stato confermato, ed è necessario rifiutarlo per qualche ragione, fare clic su **Rifiuta pagamento** nella barra superiore posizionata sopra all'elenco delle fatture.



Se il pagamento non è confermato, fare clic su **Conferma pagamento**.

In alternativa, fare clic sull'icona dei puntini di sospensione nella colonna più a destra. Nel menu visualizzato, fare clic su **Rifiuta pagamento** o su **Conferma pagamento**.

L'elenco delle fatture visualizzato viene aggiornato.

Scaricare una fattura come file PDF

Nota
Prima di procedere con i passaggi seguenti, verificare che nel dispositivo sia installato un lettore di file PDF.

Per scaricare una fattura come file PDF

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Fatture**.
2. Selezionare le fatture da scaricare.
3. Nella barra dei menu posizionata sopra all'elenco delle fatture, fare clic su **Scarica**.
   In alternativa, fare clic sull'icona dei puntini di sospensione nella colonna più a destra. Nel menu visualizzato, fare clic su **Scarica**.
   La fattura viene scaricata nel dispositivo in formato PDF.

Esportazione di una fattura come file CSV o XML

È possibile esportare una fattura come file CSV o XML. Questi file possono essere utilizzati nei sistemi di terze parti, ad esempio la piattaforma di contabilità in uso, che non è integrata in Advanced Automation (PSA).

Per esportare una fattura come file CSV o XML

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Fatture**.
2. Selezionare le fatture da esportare.
3. Nella barra dei menu posizionata sopra all'elenco delle fatture, fare clic su **Esporta CSV** o su **Esporta XML**.
   In alternativa, fare clic sull'icona dei puntini di sospensione nella colonna più a destra. Nel menu visualizzato, fare clic su **Esporta CSV** o su **Esporta XML**.
   Il file viene scaricato nel dispositivo nel formato scelto.

Prodotti

Il modulo **Prodotti** consente di definire e gestire i prodotti, ovvero i servizi o gli articoli che vengono venduti ai clienti. Ad esempio, abbonamenti per antivirus, supporto ad-hoc, forniture di hardware e così via.

I prodotti possono essere utilizzati durante la creazione di contratti o di articoli di vendita. I valori indicati nell'articolo di prodotto vengono riutilizzati al momento della creazione di un articolo di vendita o di un contratto; possono essere modificati per riflettere quanto concordato con il cliente.

Tenere presente che solo gli utenti con i ruoli Amministratore, Direttore, Contabilità o Responsabile contabilità possono creare prodotti. Una volta creati, i prodotti possono essere utilizzati nei contratti, nei progetti, nelle offerte e da altri utenti di Advanced Automation (PSA).

Per accedere al modulo **Prodotti**, passare a **Vendite e fatturazione > Prodotti**.

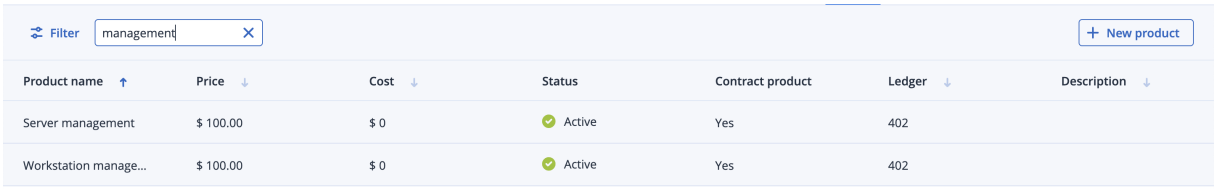
Visualizzazione di prodotti esistenti

Per visualizzare i prodotti esistenti, nel portale di gestione passare a **Vendite e fatturazione** > **Prodotti**. Nella scheda **Prodotti** visualizzata, è possibile vedere tutti i prodotti correnti in Advanced Automation (PSA). Sono inclusi i prodotti e i servizi Acronis preconfigurati nonché i prodotti di proprietà dell'utente.

Vengono visualizzate informazioni su ogni prodotto, incluso:

- Il prezzo del prodotto
- Il costo del prodotto
- Lo stato corrente del prodotto (**Attivo** o **Inattivo**)
- Il tipo di prodotto (contratto, ticket o progetto (disponibile nelle versioni future))
- Il registro contabile a cui appartiene il prodotto
- Una breve descrizione del prodotto

È inoltre possibile filtrare e ordinare l'elenco visualizzato per individuare uno specifico prodotto; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali prodotti dovranno essere visualizzati.



Aggiunta di un prodotto

Oltre ai prodotti e ai servizi Acronis disponibili in Advanced Automation (PSA), è anche possibile creare un numero illimitato di nuovi prodotti e offerte.

Per aggiungere un prodotto

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Prodotti**. La scheda **Prodotti** è visualizzata per impostazione predefinita.
2. Fare clic su **+ Nuovo prodotto**. Viene visualizzata la schermata Crea nuovo prodotto.
3. Definire quanto segue:
   - **Nome**: inserire il nome del prodotto.
   - **Descrizione**: (facoltativo) inserire una descrizione del prodotto.
   - **ID esterno**: (facoltativo) inserire l'identificatore unico del prodotto; in Advanced Automation (PSA), questo ID deve essere utilizzato al di fuori della gamma di prodotti corrente.
   - **Prezzo**: inserire un prezzo per il prodotto. Selezionare la casella di controllo **Tassabile** se il prodotto è un articolo tassabile (quest'opzione dipende dalla legislazione fiscale locale).

     Per una fatturazione più precisa, nei prezzi dei prodotti utilizzati nei contratti, nei preventivi e negli articoli di vendita è possibile utilizzare fino a quattro cifre dopo il separatore decimale, come ad esempio: $0,0750. Tali prezzi vengono arrotondati nelle fatture, nei report, nelle voci fatturabili nei ticket e nelle tariffe orarie.
   - **Costo**: inserire il costo del prodotto o il prezzo pagato a un fornitore o a un distributore per il prodotto.

     Per una creazione di report più precisa, nel costo dei prodotti è possibile utilizzare fino a quattro cifre dopo il separatore decimale, come ad esempio: $0,0750.

     Nota
     Al fine di fornire più informazioni sulla redditività di un prodotto e sulle relative statistiche, è consigliabile configurare non soltanto i prezzi dei prodotti, ma anche i loro costi.

   - Nella sezione **Proprietà del prodotto**, selezionare una o tutte le opzioni seguenti.
     - **Prodotto contratto**: selezionare la casella di controllo per rendere disponibile il prodotto nei contratti.
     - **Prodotto ticket**: selezionare la casella di controllo per rendere disponibile il prodotto nei ticket. È anche possibile selezionare la casella di controllo aggiuntiva **Prezzo regolabile dal tecnico**; in questo modo il tecnico potrà regolare il prezzo predefinito quando questo prodotto viene utilizzato in un ticket.
     - **Prodotto progetto**: selezionare la casella di controllo per rendere disponibile il prodotto nei progetti. Dopo averla selezionata, selezionare la casella di controllo aggiuntiva **Prezzo regolabile per progetto**; in questo modo il prezzo predefinito potrà essere regolato quando questo prodotto viene utilizzato in un progetto specifico. Per ulteriori informazioni, consultare "Progetti" (pag. 238).
     - Selezionare la casella di controllo **Prodotto per fatturazione basata su attività** per far sì che i tecnici visualizzino il prodotto nei ticket. Questo campo non è disponibile se è stata selezionata l'opzione **Prodotto contratto**.

Nota
L'opzione garantisce la possibilità di assegnare a un ticket l'ulteriore tempo di lavoro richiesto agli esperti, ad esempio quando un tecnico richiede assistenza a un architetto o a un esperto della sicurezza. Queste ore possono essere fatturate in base alla rispettiva tariffa speciale invece che alla tariffa predefinita del ticket.

- **Registro contabile**: (facoltativo) selezionare il registro contabile pertinente dall'elenco a discesa.
- **Attivo**: (facoltativo) selezionare la casella di controllo per rendere disponibile il prodotto.
  Tenere presente che la casella di controllo **Attivo** è disabilitata quando il prodotto è:
  - Impostato come prodotto predefinito nelle impostazioni di fatturazione (consultare "Definizione delle impostazioni di fatturazione predefinite" (pag. 336)).
  - Parte di un pacchetto.
  - Aggiunto a un contratto.
- **Prodotto VAR**: (facoltativo) selezionare la casella di controllo se si rivende il prodotto, ovvero se il prodotto è stato precedentemente acquistato da una terza parte. Quando questa casella di controllo è selezionata, l'utile di questo prodotto viene considerato separatamente come utile 'VAR'.

4. Dopo aver esaminato i dettagli del nuovo prodotto, fare clic su **Fine**.

Modifica di un prodotto

Per modificare un prodotto

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Prodotti**. La scheda **Prodotti** è visualizzata per impostazione predefinita.
2. Fare clic sul prodotto da modificare.
3. Nel pannello destra, fare clic sull'icona a matita e modificare il prodotto. Per ulteriori informazioni sui campi modificabili di un prodotto, consultare "Aggiunta di un prodotto" (pag. 295).

   Nota
   Se un prodotto contratto è incluso in un pacchetto di prodotti, non è possibile aggiornarlo. Prima di aggiornarlo, sarà necessario rimuoverlo dal pacchetto di prodotti corrispondente.

4. Al termine, fare clic su ✓.

Definizione dei costi e dei prezzi dei prodotti Acronis

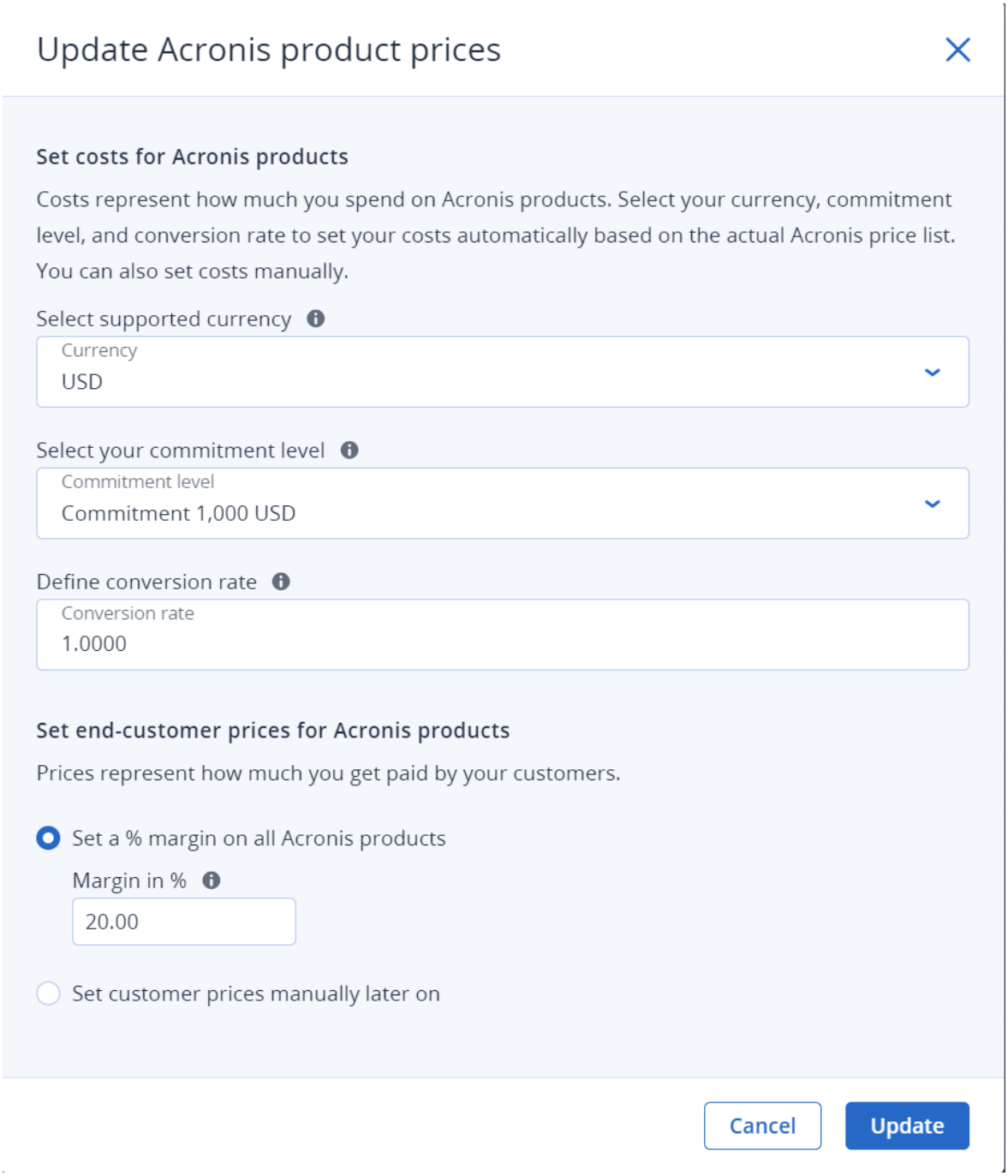
Nella scheda **Prodotti** è possibile definire il costo e i prezzi dei prodotti Acronis utilizzati in Advanced Automation (PSA). Il *costo* definito determina il volume di spesa per i prodotti Acronis, mentre i *prezzi* definiscono l'ammontare dei pagamenti da parte dei clienti.

Questa funzionalità consente di:

- Definire i costi dei prodotti Acronis in base al listino prezzi attuale di Acronis, la valuta del Partner interessato (e l'eventuale tasso di cambio, se il listino prezzi non è fornito da Acronis), il livello di partnership, ovvero il livello di impegno del Partner.
- Definire i prezzi dei prodotti Acronis per i clienti in base ai costi e a una percentuale di margine specificata.

Per definire i costi e i prezzi dei prodotti Acronis

1. Passare a **Vendite e fatturazione** > **Prodotti**.
2. Nella scheda **Prodotti**, fare clic su **Aggiornare i prezzi del prodotto Acronis**.
   Viene visualizzata la finestra di dialogo seguente.



3. Nella sezione **Impostare i costi dei prodotti Acronis**, definire quanto segue:
   - Nell'elenco a discesa **Selezionare la valuta supportata**, selezionare la valuta da applicare ai prodotti Acronis.

     Nota
     La valuta predefinita impostata in Advanced Automation (PSA) viene applicata automaticamente. Inoltre, questo campo è di sola lettura se la valuta predefinita è una delle valute supportate (USD, EUR, GBP, AUD, JPY, CAD, BRL, INR), come mostrato nell'esempio sopra.

   - Nell'elenco a discesa **Selezionare il livello di impegno**, selezionare il livello di impegno pertinente.
   - Nel campo **Definire il tasso di conversione**, impostare il tasso di conversione per i prodotti Acronis. Il valore predefinito è 1.0000.

     Nota
     Questo campo è obbligatorio se la valuta predefinita non è una delle valute supportate (vedere sopra).

4. Nella sezione **Impostare i prezzi per il cliente finale per i prodotti Acronis**, selezionare una delle seguenti opzioni:
   - **Impostare un margine % su tutti i prodotti Acronis**. Selezionare questa opzione per impostare il margine di profitto pertinente su tutti i prodotti Acronis. I prezzi sono stabiliti con la formula seguente:

     Prezzo = Costo * 100 / (100 - Valore del margine)

     Ad esempio, se viene definito un margine del 20% su un prodotto da 100$, il prezzo verrà impostato a 125$ ovvero 25$ di margine a rappresentare il 20% di 125$.
   - **Impostare in seguito i prezzi per i clienti manualmente**. Selezionare questa opzione se non si vuole aggiornare automaticamente i prezzi dei prodotti Acronis ma si preferisce impostarli manualmente in un secondo momento.
5. Fare clic su **Aggiorna**.

   Advanced Automation (PSA) applica automaticamente i costi e i prezzi definiti ai prodotti Acronis venduti ai clienti.

Gestione dell'inventario

Il modulo Inventario consente di aggiungere record all'inventario e di gestire, vendere e analizzare l'inventario delle scorte (articoli come server, computer, apparecchiature di rete e periferiche che devono essere disponibili per le vendite occasionali ai clienti). Gli articoli dell'inventario possono essere offerti nei preventivi o venduti come articoli di vendita selezionando un prodotto non di contratto, ad esempio 'Vendita hardware'.

A differenza dei prodotti basati su abbonamento, gli articoli di inventario hanno limiti di quantità e non sono ricorrenti. Ad esempio, quando si aggiunge un articolo ai preventivi o ad articoli di vendita,

la quantità viene 'consumata', il che significa che non può essere aggiunta ad altri preventivi o articoli di vendita. Se il preventivo viene rifiutato o se la quantità o l'articolo vengono rimossi dal preventivo o dall'articolo di vendita, l'articolo torna disponibile nel modulo Inventario. Potrà quindi essere aggiunto ad altri articoli di vendita o preventivi. Per ulteriori informazioni su come lavorare in modo efficiente con l'inventario, consultare "Creazione di un articolo di inventario con un numero di serie" (pag. 304).

Per accedere e gestire l'inventario, passare a **Vendite e fatturazione > Prodotti**, quindi fare clic sulla scheda **Inventario**. Da questa scheda, è possibile tenere traccia e gestire gli articolo di inventario su più posizioni, identificare gli articoli da rifornire e monitorare l'utilizzo dell'inventario. È possibile gestire quantità, prezzi, numeri di serie, dettagli della garanzia e dati del fornitore e dell'acquisto, oltre a definire e utilizzare campi personalizzati come necessario.

Con il modulo Inventario è possibile ottimizzare la gestione dell'inventario e dei processi di vendita, migliorare i servizi offerti ai clienti e ottenere informazioni finanziarie e sull'inventario fruibili.

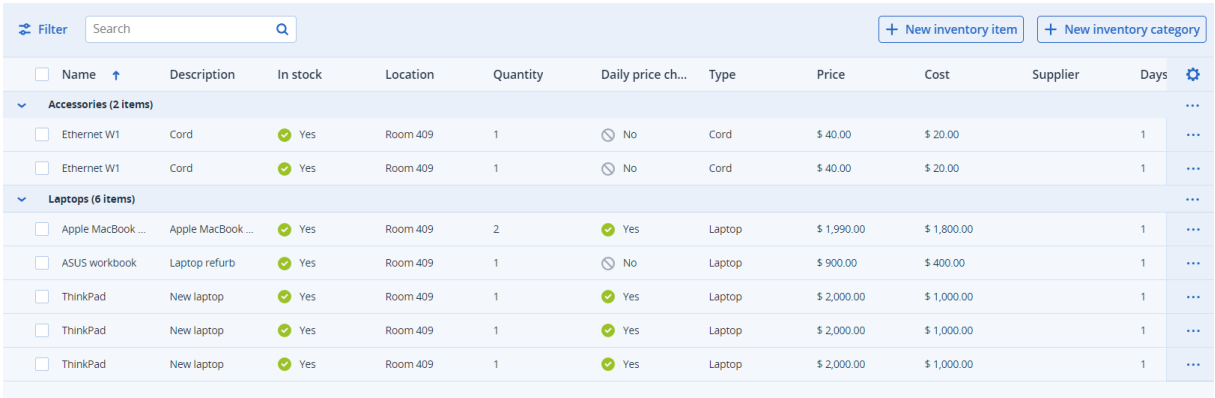
Visualizzazione di inventari esistenti

Per visualizzare gli inventari esistenti, nel portale di gestione passare a **Vendite e fatturazione > Prodotti**.

Fare clic sulla scheda **Inventario** per visualizzare tutti gli articoli di inventario (inclusi gli articoli venduti) in Advanced Automation (PSA). È possibile visualizzare le informazioni su ciascun articolo di inventario, incluso:

- Il nome dell'articolo.
- Una breve descrizione dell'articolo.
- Un'indicazione del fatto che l'articolo è attualmente in magazzino (**Sì** o **No**) e da quanto tempo è in magazzino.
- La posizione dell'articolo.
- La quantità attuale di articolo disponibile per la vendita.
- Il costo (prezzo di acquisto) e il prezzo (prezzo di vendita) dell'articolo.
- Il tipo di articolo e la categoria.
- Il numero di serie dell'articolo.

Gli articoli di inventario sono raggruppati per categoria. È possibile filtrare e ordinare l'elenco visualizzato per individuare uno specifico articolo; per applicare filtri più avanzati, utilizzare lo strumento **Filtra** per definire quali articoli dovranno essere visualizzati.



Aggiunta di un articolo di inventario

Quando si aggiunge un articolo di inventario con una quantità maggiore di 0, l'articolo può quindi essere offerto come parte di un preventivo o venduto tramite un articolo di vendita.

Per aggiungere un articolo di inventario

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Prodotti** e fare clic sulla scheda **Inventario**.
2. Se si sta aggiungendo il primo articolo di inventario, fare clic su **Crea nuovo**. Se sono già presenti articoli di inventario, fare clic su **+ Nuovo articolo di inventario**.

   Viene visualizzata la procedura guidata **Crea nuovo articolo di inventario**.
3. Nella schermata **Informazioni generali**, definire quanto segue:
   - **Nome**: inserire il nome dell'articolo di inventario.
   - **Descrizione**: inserire una descrizione dell'articolo.
   - **Categoria**: selezionare una categoria dall'elenco delle categorie attive corrente. È possibile aggiungere una nuova categoria facendo clic su **+ Nuova categoria di inventario** nell'elenco a discesa.
   - **Posizione**: (facoltativo) selezionare una posizione dall'elenco delle posizioni corrente. È possibile aggiungere una nuova posizione facendo clic su **+ Nuova posizione** nell'elenco a discesa.

     Nota
     Se è stata definita una posizione di inventario predefinita, nell'elenco viene mostrata la posizione predefinita, che potrà poi essere modificata. Per ulteriori informazioni, consultare "Aggiunta di una posizione di inventario" (pag. 307).

   - **Tipo**: (facoltativo) selezionare un tipo dall'elenco dei tipi corrente. È possibile aggiungere un nuovo tipo facendo clic su **+ Nuovo tipo** nell'elenco a discesa.
4. Fare clic su **Avanti**.
5. Nella scheda **Dettagli dell'elemento** definire quanto segue:
   - **Costo**: per impostazione predefinita, il costo è impostato su 0.
   - **Prezzo**: per impostazione predefinita, il prezzo è impostato su 0.

- **Quantità**: per impostazione predefinita, la quantità è impostata su 0. Se, tuttavia, vengono immessi dei numeri di serie (vedere di seguito), questo campo visualizza automaticamente il numero di numeri di serie aggiunti. Quando viene aggiunta a un articolo di vendita o a un preventivo, la quantità disponibile viene "prenotata"; non è quindi possibile aggiungere la stessa quantità due volte.
- Nella casella di testo **Numeri di serie** immettere un numero di serie univoco per ogni articolo di inventario, con un massimo di 60 caratteri. È possibile aggiungere fino a 1000 numeri di serie, delimitati da una nuova riga o da uno spazio.

6. Fare clic su **Avanti**.
7. Nella scheda **Dettagli acquisto** definire quanto segue:
   - **Fornitore**: (facoltativo) selezionare un fornitore dall'elenco dei fornitori corrente.
   - **Ordine d'acquisto del fornitore**: (facoltativo) immettere il numero dell'ordine di acquisto del fornitore.
   - **Ordine d'acquisto interno**: (facoltativo) immettere il numero dell'ordine d'acquisto interno.
   - **Numero fattura fornitore**: (facoltativo) immettere il numero della fattura fornitore.
   - Selezionare la casella di controllo **Controllo prezzi giornaliero** per indicare se il prezzo dell'articolo di inventario deve essere verificato manualmente dai dipendenti prima dell'acquisto da un fornitore o di una vendita ai clienti. Se è selezionata, la colonna **Controllo prezzi giornaliero** nella schermata principale dell'inventario mostra **Sì** nella riga dell'articolo di inventario pertinente.
8. Nella scheda **Informazioni aggiuntive** è possibile visualizzare tutti i campi personalizzati relativi all'articolo di inventario. La scheda viene visualizzata solo quando i campi personalizzati sono configurati ed è presente almeno un campo personalizzato attivo per l'inventario.
   Ad esempio, se il campo personalizzato **Garanzia valida fino a** è stato definito e applicato agli articoli di inventario, il campo viene visualizzato per tutti gli articoli di inventario durante la creazione o l'aggiornamento dell'articolo. Tutti gli articoli di inventario avranno valori diversi applicabili a questo campo, o potranno anche essere lasciati vuoti. Per ulteriori informazioni sulla definizione dei campi personalizzati, consultare "Lavorare con i campi personalizzati" (pag. 213).
9. Fare clic su **Crea**.

Per ulteriori informazioni su come lavorare in modo efficiente con l'inventario, consultare "Creazione di un articolo di inventario con un numero di serie" (pag. 304).

Modifica di un articolo di inventario

È possibile modificare o rimuovere un articolo di inventario come necessario.

Per modificare un articolo di inventario

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Prodotti** e fare clic sulla scheda **Inventario**.
2. Fare clic sull'articolo di inventario da modificare.

3. Nel pannello a destra, fare clic sull'icona della matita nelle sezioni pertinenti (**Informazioni generali**, **Dettagli articolo** e **Dettagli acquisto**) e modificare come necessario. Per ulteriori informazioni sui campi modificabili per un articolo di inventario, consultare "Aggiunta di un articolo di inventario" (pag. 301).

   Tenere presente quanto segue:

   - Non è possibile modificare il campo **Quantità** se all'articolo di inventario sono stati aggiunti numeri di serie. Il valore di sola lettura mostrato è **1** (se il prodotto non è incluso come parte di un articolo di vendita o di un preventivo) o **0** (se il prodotto è stato aggiunto a un articolo di vendita o a un preventivo). È possibile modificare i numeri di serie solo se l'articolo di inventario non è stato aggiunto a un preventivo in sospeso (il preventivo non è stato accettato o rifiutato) o a un articolo di vendita (che è stato fatturato o non fatturato). Per modificare il numero di serie, è necessario rimuovere l'articolo di inventario, cambiare il numero di serie e quindi aggiungere di nuovo l'articolo.
   - È possibile aggiornare le posizioni di un numero di articoli in blocco selezionando gli articoli di interesse e facendo clic su **Aggiorna posizione dell'oggetto**. Nella finestra di dialogo visualizzata, selezionare la nuova posizione e fare clic su **Aggiorna**. La nuova posizione verrà applicata a tutti gli articoli selezionati.
   - Se si aggiorna il prezzo, il nome o la descrizione dell'articolo di inventario, è necessario aggiornare manualmente questi campi per tutti gli articoli di vendita e i preventivi associati.
   - Se si imposta un articolo **Inattivo** su **Attivo**, anche la posizione dell'inventario viene impostata su **Attiva**.
4. Al termine, fare clic su **Salva**.

Per rimuovere un articolo di inventario

1. Nella riga relativa all'articolo di inventario, fare clic sull'icona dei puntini di sospensione (...), quindi selezionare **Rimuovi**.
2. Nella finestra di conferma visualizzata, fare clic su **Rimuovi**.

   L'articolo di inventario viene impostato su **Inattivo**. Le operazioni di vendita, fatturazione e acquisto esistenti in cui è utilizzato l'articolo non sono interessate dalla modifica.

   È comunque possibile visualizzare gli articoli di inventario **Inattivi** nella schermata principale dell'inventario utilizzando l'opzione **Filtro** e selezionando **Stato** > **Inattivo**.

Come lavorare con l'inventario

Dopo aver aggiunto l'inventario (consultare "Aggiunta di un articolo di inventario" (pag. 301)), Advanced Automation (PSA) consente di operare con l'inventario con attività di aggiornamento, registrazione e vendita degli articoli di inventario tramite i preventivi e gli articoli di vendita pertinenti.

Le seguenti sezioni offrono alcuni suggerimenti che aiutano a gestire l'inventario, tra cui:

- Lavorare con l'inventario con i numeri di serie
- Vendita di articoli di inventario tramite articoli di vendita e preventivi

- Aggiornamento di preventivi, articoli di vendita e inventario

Lavorare con l'inventario con i numeri di serie

Creazione di un articolo di inventario con un numero di serie

È possibile creare un articolo di inventario con un numero di serie (consultare "Aggiunta di un articolo di inventario" (pag. 301)). Se un numero di serie viene applicato durante la creazione di un articolo di inventario, la quantità dell'articolo viene impostata automaticamente su 1 e non può essere modificata manualmente.

È inoltre possibile creare articoli di inventario in blocco (fino a 1000 voci) con numeri di serie. Questa operazione viene eseguita nella stessa finestra di dialogo utilizzata per creare un singolo articolo di inventario aggiungendo più numeri di serie. La quantità dell'articolo nella procedura guidata di creazione si basa automaticamente sul numero di numeri di serie forniti e non può essere modificata manualmente. Al termine della procedura guidata di creazione, viene aggiunto un singolo articolo di inventario (con una quantità pari a 1) per ogni numero di serie.

Nota
Applicando un numero di serie a un articolo di inventario, è possibile tenere facilmente traccia dei dettagli della garanzia, dei numeri di serie e di qualsiasi altra informazione aggiunta tramite l'uso dei campi personalizzati. Ciò consente di gestire l'inventario in modo più efficiente.

È anche possibile riutilizzare un articolo di inventario senza un numero di serie se non è necessario tenere traccia di questi dettagli. In questo modo, è possibile aumentare la quantità dell'articolo dell'inventario e vendere quanto richiesto.

Aggiornamento di un articolo di inventario con un numero di serie

La quantità di un articolo di inventario con un numero di serie non può essere aggiornata: la quantità è 1 (se non ancora venduta o offerta in un preventivo) o 0 (se offerta in un preventivo in sospeso o in un articolo di vendita in sospeso, o se venduta). Tenere presente che la quantità dell'articolo diminuisce automaticamente a 0 se offerta in un preventivo o venduta come articolo di vendita.

È possibile impostare un numero di serie su un articolo di inventario esistente al quale non è stato assegnato alcun numero di serie. Se, tuttavia, un numero di serie viene applicato a un articolo di inventario, la quantità dell'articolo viene reimpostata su 1, il che può causare una discrepanza tra il numero reale di articoli e gli articoli catalogati in Advanced Automation (PSA). Pertanto, è consigliabile:

- Creare un nuovo articolo di inventario con il numero di serie corrispondente.
- Ridurre manualmente la quantità dell'articolo di inventario.

Dopo la vendita

Quando viene venduto, l'articolo di inventario viene archiviato solo per scopi contabili, il che consente anche di tracciare il numero di serie e la garanzia dell'articolo e qualsiasi altra informazione che potrebbe essere aggiunta tramite l'uso di campi personalizzati.

È possibile anche tenere traccia dell'inventario nei report Vendite e fatturazione. Per ulteriori informazioni, consultare "Vendite e fatturazione" (pag. 138).

Vendita di articoli di inventario tramite articoli di vendita e preventivi

Gli articoli di inventario possono essere venduti con due modalità: con vendita diretta degli articoli di vendita e con l'offerta di articoli di inventario in un preventivo. Tenere presente che gli articoli di inventario vengono aggiunti agli articoli di vendita e ai preventivi specificando un prodotto non di contratto (con l'opzione **Utilizza nei contratti** disabilitata) e quindi selezionando gli articoli di inventario disponibili in magazzino.

- Per vendere articoli di inventario tramite articoli di vendita:
  a. Creare gli articoli di vendita pertinenti per i clienti e aggiungere gli articoli di inventario. Per ulteriori informazioni, consultare "Creazione di un nuovo articolo di vendita" (pag. 279).
  b. Creare una fattura per il cliente utilizzando gli articoli di vendita pertinenti. Per ulteriori informazioni, consultare "Generazione di una nuova fattura" (pag. 290).

  Nota
  Il registro contabile incluso nella riga di fattura è il registro contabile configurato per il prodotto (i registri contabili sono definiti a livello di prodotto, non a livello di inventario). Per ulteriori informazioni, consultare "Gestione dei registri contabili" (pag. 312).

  Allo stesso modo, l'imposta applicata nella fattura è l'imposta definita per il prodotto (quando importata tramite l'integrazione di un sistema di contabilità) o l'imposta di sistema predefinita. Per ulteriori informazioni, consultare "Configurazione delle imposte" (pag. 343).

- Per offrire articoli di inventario in un preventivo:
  a. Creare un preventivo con gli articoli di inventario pertinenti. Per ulteriori informazioni, consultare "Creazione di un preventivo" (pag. 273).

  Quando il cliente accetta il preventivo, viene creato un articolo di vendita e un ticket del preventivo. È possibile tracciare il processo di vendita e registrarne i tempi tramite il ticket del preventivo. Per ulteriori informazioni, consultare "In che modo Advanced Automation (PSA) elabora i preventivi accettati o rifiutati" (pag. 275).
  b. Emettere la fattura per il cliente, creandola dall'articolo di vendita. Per ulteriori informazioni, consultare "Generazione di una nuova fattura" (pag. 290).

Importante
Solo gli articoli di inventario disponibili in magazzino in quantità maggiore di 0 possono essere venduti come articoli di vendita o nei preventivi. È possibile vendere solo la quantità disponibile.

La quantità di ciascun articolo di inventario viene aggiornata automaticamente quando:

- L'articolo viene aggiunto a un preventivo o a un articolo di vendita. L'articolo di inventario viene automaticamente prenotato dal magazzino e non può essere offerto in un altro preventivo o in un altro articolo di vendita.
- Gli articoli di vendita vengono eliminati o i preventivi vengono rifiutati. La quantità prenotata degli articoli di inventario viene restituita al magazzino e torna quindi disponibile; potrà essere utilizzata in altri preventivi e in altri articoli di vendita.

Aggiornamento di preventivi, articoli di vendita e inventario

Quando si aggiornano preventivi, articoli di vendita e articoli di inventario, tenere presente quanto segue:

- Quando si aggiornano il nome e la descrizione dell'articolo di inventario, non viene aggiornata automaticamente la descrizione degli stessi articoli inclusi nei preventivi o negli articoli di vendita. Tali descrizioni devono essere aggiornate manualmente.
- La rettifica del prezzo dell'articolo di inventario comporta la rettifica automatica del prezzo impostato nel preventivo o nell'articolo di vendita. Al contrario, se si rettifica il prezzo dell'articolo di inventario nel preventivo o nell'articolo di vendita, è necessario aggiornare manualmente il prezzo dell'articolo di inventario.
- Se è necessario aggiornare il numero di serie assegnato a un articolo di inventario incluso in un preventivo o in un articolo di vendita, procedere come segue:
  a. Rimuovere l'articolo di inventario dal preventivo o dall'articolo di vendita.
  b. Aggiornare il numero di serie dell'articolo di inventario.
  c. Aggiungere l'articolo di inventario aggiornato al preventivo o all'articolo di vendita.
- Al momento, i modelli di preventivo non supportano gli articoli di inventario.

Gestione delle categorie di inventario

Le categorie di inventario consentono di individuare e monitorare rapidamente lo stato di specifici articoli di inventario.

È possibile aggiungere categorie di inventario come necessario. È anche possibile modificare e rimuovere le categorie di inventario.

Per aggiungere una categoria di inventario

1. Nel portale di gestione, passare a **Vendite e fatturazione** > **Prodotti** e fare clic sulla scheda **Inventario**.
2. Fare clic su **+ Aggiungi categoria di inventario**.

3. Immettere il nome della categoria di inventario e fare clic su **Aggiungi**.
   La categoria di inventario è ora disponibile per essere selezionata durante la creazione o la modifica di un articolo di inventario.

Per modificare una categoria di inventario

1. Nella scheda **Inventario**, fare clic sull'icona dei puntini di sospensione (...) nella riga della categoria di inventario pertinente, quindi selezionare **Modifica**.
2. Apportare le modifiche richieste. È possibile:
   - Rinominare la categoria di inventario.
   - Modificare lo stato della categoria di inventario in **Attiva** o **Inattiva**.

   Nota
   Non è possibile impostare una categoria di inventario **Attiva** su **Inattiva** se a questa sono assegnati articoli di inventario **Attivi**. È necessario spostare gli articoli di inventario in un'altra categoria o impostarli come **Inattivi**, quindi riprovare.

3. Fare clic su **Salva**.

Per rimuovere una categoria di inventario

1. Nella scheda **Inventario**, fare clic sull'icona dei puntini di sospensione (...) nella riga della categoria di inventario pertinente e quindi selezionare **Rimuovi**.
2. Se la categoria di inventario è vuota o non contiene articoli di inventario **Attivi**, viene rimossa.

Nota
Non è possibile rimuovere una categoria di inventario se a questa sono assegnati articoli di inventario **Attivi**. È necessario spostare gli articoli di inventario in un'altra categoria o impostarli come **Inattivi**, quindi riprovare.

Gestione delle posizioni di inventario

Advanced Automation (PSA) consente di definire e gestire le posizioni di inventario delle scorte, aiutando i dipendenti a trovare facilmente la posizione degli articoli di inventario esistenti da inviare ai clienti e la posizione di consegna delle scorte acquistate.

Per visualizzare e gestire le posizioni di inventario, passare a **Vendite e fatturazione > Prodotti**, quindi fare clic sulla scheda **Posizioni di inventario**.

Nota
Per ulteriori informazioni su come visualizzare, creare e modificare articoli di inventario, consultare "Gestione dell'inventario" (pag. 299).

Aggiunta di una posizione di inventario

Per aggiungere una posizione di inventario

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Posizioni di inventario**.
2. Se si sta aggiungendo la prima posizione, fare clic su **Crea nuova**. Se sono già presenti posizioni esistenti, fare clic su **Aggiungi posizione** nell'angolo in alto a destra.
3. Nella finestra di dialogo visualizzata:
   a. Inserire il nome della posizione.
   b. Inserire una descrizione della posizione.
   c. (Facoltativo) Selezionare la casella di controllo **Posizione predefinita**. Questa opzione garantisce che questa posizione sia selezionata per impostazione predefinita quando si aggiunge un nuovo articolo di inventario. Per ulteriori informazioni, consultare "Aggiunta di un articolo di inventario" (pag. 301).
   d. Fare clic su **Aggiungi** per aggiungere la posizione.

   La posizione viene aggiunta all'elenco delle posizioni esistenti e, per impostazione predefinita, viene impostata su **Attiva**.

   Per ulteriori informazioni sull'aggiornamento della posizione e del relativo stato, consultare "Modifica di una posizione di inventario" (pag. 308).

Modifica di una posizione di inventario

È possibile modificare ed eliminare le posizioni di inventario come necessario.

Per modificare una posizione di inventario

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Fare clic sulla scheda **Posizione inventario** per visualizzare le posizioni esistenti.

   Se non è visualizzata alcuna posizione, fare clic su **Crea nuova** per aggiungere una posizione. Per ulteriori informazioni, consultare "Aggiunta di una posizione di inventario" (pag. 307).
3. Nella riga relativa alla posizione di inventario, fare clic sull'icona dei puntini di sospensione (...), quindi su **Modifica**.
4. Modificare i campi visualizzati come necessario. Ad esempio, se si desidera che la posizione sia inattiva, deselezionare la casella di controllo **Stato attivo**.
5. Al termine, fare clic su **Salva**.

Per eliminare una posizione di inventario

1. Nella riga relativa alla posizione di inventario, fare clic sull'icona dei puntini di sospensione (...), quindi su **Elimina**.
2. Nella finestra di dialogo di conferma visualizzata, fare clic su **Elimina**. La posizione viene eliminata.

Nota
Se la posizione di inventario è attualmente in uso, viene richiesto di assegnare prima l'inventario associato a un'altra posizione di inventario. In alternativa, è possibile deselezionare la casella di controllo **Stato attivo** per rendere la posizione inattiva e quindi riprovare.

Categorie prodotto

Se necessario, Advanced Automation (PSA) consente di aggiungere nuove categorie.

Applicando le categorie ai ticket si ottiene una valida panoramica dei problemi più comuni a cui deve far fronte ciascun cliente. Ad esempio, se un cliente presenta il 50% dei ticket categorizzato come *Workstation/virus*, potrebbe essere necessario sostituire alcune misure di sicurezza e offrire una formazione aggiornata al personale interessato.

La categorizzazione dei prodotti consente inoltre di organizzare più prodotti in un singolo gruppo. Se sono presenti elenchi con centinaia di prodotti, la creazione di categorie ne semplifica l'individuazione.

Aggiunta di categorie prodotto

È possibile aggiungere nuove categorie prodotto come necessario.

Una volta creata la categoria, questa potrà essere abilitata o disabilitata come descritto di seguito, e modificata come necessario (consultare "Modifica di categorie prodotto" (pag. 310)).

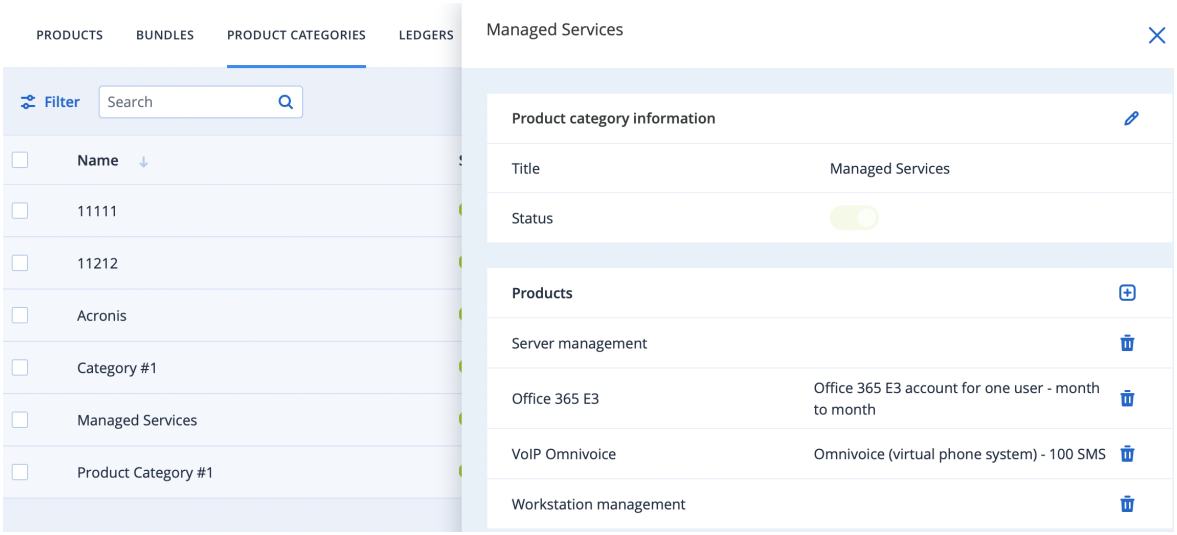
Nota
Questa opzione è disponibile solo agli utenti ai quali sono stati assegnati i ruoli seguenti: Amministratore, Direttore, Responsabile contabilità, Contabilità

Aggiunta di una nuova categoria prodotto

1. Passare a **Vendite e fatturazione > Prodotti**.
2. Nella schermata visualizzata, fare clic sulla scheda **Categorie prodotto**.
3. Se non sono presenti categorie, fare clic su **Crea nuovo**. Altrimenti, fare clic su **+ Nuovo**.
4. Nel campo **Nome categoria prodotto**, inserire un nome per la categoria.
5. Nel campo **Seleziona prodotti**, selezionare il prodotto pertinente. Fare quindi clic su **Aggiungi**.
6. Per aggiungere ulteriori prodotti alla categoria, fare clic su **Aggiungi prodotto** e selezionare il prodotto pertinente. Ripetere questi passaggi secondo necessità.
7. Fare clic su **Fine**. La nuova categoria è visualizzata nella scheda **Categorie prodotto**, ed è impostata su **Attiva** per impostazione predefinita.

Abilitazione o disabilitazione di una categoria prodotto

1. Passare a **Vendite e fatturazione > Prodotti**. La scheda **Prodotti** visualizzata elenca le categorie esistenti.
2. Per attivare una categoria, fare clic sulla categoria inattiva corrispondente e poi sull'icona a matita nel pannello a destra. Quindi abilitare l'interruttore **Stato**. Al termine, fare clic su ✓.



3. Per disabilitare una categoria, fare clic sulla categoria inattiva corrispondente e poi sull'icona a matita nel pannello a destra. Quindi disabilitare l'interruttore **Stato**. Al termine, fare clic su ✓.

Nota
È inoltre possibile abilitare o disabilitare lo stato della categoria quando si modifica la categoria. Consultare "Modifica di categorie prodotto" (pag. 310) per ulteriori informazioni.

Modifica di categorie prodotto

Per modificare una categoria prodotto

1. Passare a **Vendite e fatturazione > Prodotti**. La scheda **Prodotti** visualizzata elenca le categorie esistenti.
2. Per modificare una categoria, fare clic sulla categoria pertinente e quindi sull'icona a matita nel pannello a destra.
3. Apportare le modifiche necessarie. È possibile, ad esempio, rimuovere e aggiungere un prodotto, oppure modificare lo stato della categoria su **Attiva**/**Inattiva**.
4. Al termine, fare clic su ✓.

Gestione dei pacchetti prodotto

I pacchetti prodotto consentono di raggruppare più prodotti e servizi in un unico pacchetto.

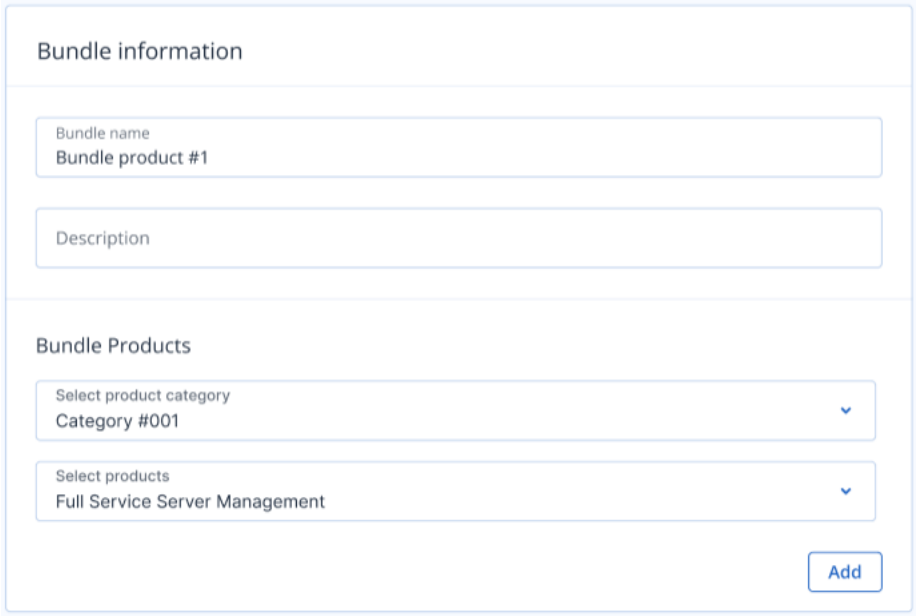
Tenere presente che al momento i pacchetti prodotto possono includere soltanto prodotti contrassegnati come prodotti contratto.

Creazione di un pacchetto di prodotti

Per creare un pacchetto di prodotti

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite** e fare clic sulla scheda **Pacchetti**.

2. Se si desidera creare il primo pacchetto di prodotti, fare clic su **Crea nuovo**. Se sono presenti pacchetti esistenti, fare clic su **Nuovo** nell'angolo in alto a destra.
3. Nella finestra di dialogo visualizzata, procedere come segue:
   a. Inserire il nome del pacchetto.
   b. Inserire una descrizione del pacchetto.
   c. Selezionare una categoria di prodotto.
   d. Selezionare un prodotto. Solo i prodotti dei contratti sono disponibili per essere selezionati nei pacchetti.
   e. Fare clic su **Aggiungi** per aggiungere il prodotto al pacchetto.



   f. Fare clic su **Aggiungi prodotto** per aggiungere un ulteriore prodotto al pacchetto. Quindi selezionare la categoria di prodotto e il prodotto corrispondenti e fare clic su **Aggiungi**. Ripetere questi passaggi secondo necessità.
4. Dopo aver aggiunto tutti i prodotti necessari al pacchetto, fare clic su **Fine**.
   Il pacchetto è ora disponibile e può essere utilizzato per essere aggiunto a un contratto o per aggiornare un contratto. Per ulteriori informazioni, consultare "Lavorare con i contratti" (pag. 282).

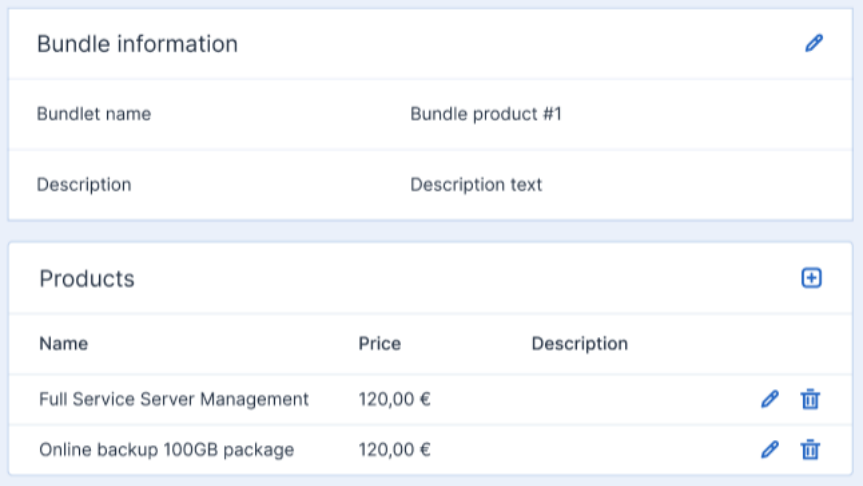
Modifica di pacchetti prodotto

È possibile modificare ed eliminare i pacchetti prodotto come necessario.

Per modificare i pacchetti prodotto

1. Nel portale di gestione, passare a **Vendite e fatturazione > Vendite**.
2. Fare clic sulla scheda **Pacchetti** per visualizzare tutti i pacchetti prodotto esistenti.
   Se non è visualizzato alcun pacchetto, fare clic su **Crea nuovo** per creare un pacchetto. Consultare "Creazione di un pacchetto di prodotti" (pag. 310) per ulteriori informazioni.

3. Fare clic sulla riga del pacchetto corrispondente e, nel pannello a destra, sull'icona a matita.



4. Nella sezione **Informazioni sul pacchetto**, modificare il nome e la descrizione del pacchetto come necessario.
5. Nella sezione **Prodotti**:
   - Fare clic su per aggiungere un nuovo prodotto. Quindi selezionare la categoria di prodotto e il prodotto corrispondenti e fare clic su **Aggiungi**. Ripetere questi passaggi secondo necessità.
   - Fare clic sull'icona a matita per modificare il prodotto. Ad esempio, può essere necessario sostituire un prodotto esistente con un prodotto diverso della stessa categoria. Al termine, fare clic su **Salva**.
   - Fare clic sull'icona a cestino per eliminare un prodotto dal pacchetto.
6. Al termine, fare clic su .

Per eliminare un pacchetto prodotto

1. Fare clic sulla riga del pacchetto corrispondente e, nella colonna a destra, fare clic sull'icona dei puntini di sospensione.
2. Fare clic su **Elimina**. Il pacchetto viene eliminato.

Nota
Un pacchetto prodotto può essere eliminato anche se è stato assegnato a un contratto corrente e in vigore. Di fatto un pacchetto è sostanzialmente un insieme di singoli prodotti inseriti in un contratto; al contratto viene aggiunta una parte di contratto per ogni prodotto. Dopo aver creato il contratto, è possibile eliminare il pacchetto.

Gestione dei registri contabili

La sezione Registri contabili consente di gestire i numeri dei registri presenti nel sistema di contabilità attualmente in uso. I registri possono così essere connessi ai prodotti venduti ai clienti.

Quando, ad esempio, si crea un file in formato CSV o XML per esportare un ciclo di fatturazione, il file conterrà tutte le transazioni, incluso il numero di registro corretto. Ciò rende semplice e rapida l'importazione.

Per accedere ai registri, passare a **Vendite e fatturazione > Prodotti** e fare clic sulla scheda **Registri contabili**.

Creazione di un registro contabile

Per creare un registro contabile

1. Nel portale di gestione, passare a **Vendite e fatturazione > Prodotti** e fare clic sulla scheda **Registri contabili**.
2. Fare clic su **+ Nuovo**.
3. Nella schermata delle informazioni sul registro contabile, definire quanto segue.
   - Definire il nome del registro contabile.
   - (Facoltativo) Inserire l'ID esterno del registro contabile.
   - (Facoltativo) Inserire una descrizione per il registro contabile.
   - Per utilizzare immediatamente il registro contabile, selezionare la casella di controllo **Attivo**.
4. Fare clic su **Fine**.

Modifica di un registro contabile

Nota
È possibile modificare i registri contabili come necessario, ma non è possibile eliminarli.

Per modificare un registro contabile

1. Nel portale di gestione, passare a **Vendite e fatturazione > Prodotti** e fare clic sulla scheda **Registri contabili**.
2. Fare clic sulla riga del registro contabile da modificare.
3. Nel pannello destra, fare clic sull'icona a matita e modificare il registro contabile come necessario.
4. Per disattivare un registro contabile attivo, disabilitare l'interruttore **Stato**.
5. Al termine, fare clic su ✓.

Configurazione delle impostazioni di Advanced Automation (PSA)

Nel modulo **Impostazioni** è possibile configurare diverse impostazioni relative all'account di Advanced Automation (PSA).

È necessario definire tali impostazioni prima di operare con il servizio, poiché queste includono numerose impostazioni chiave necessarie per avviare le attività di fatturazione e di Service Desk. Questa sezione include le impostazioni relative a:

- Service Desk
- Fatturazione e offerte

Impostazioni di Service Desk

Le impostazioni di Service Desk consentono di configurare tutte le sezioni essenziali del Service Desk.

Affinché i ticket funzionino correttamente, è importante che queste impostazioni siano configurate correttamente.

Per accedere alle impostazioni di Service Desk, passare a **Impostazioni > Service Desk**.

Nota
Nelle impostazioni di Service Desk è possibile anche definire i gruppi di utenti per i propri utenti di Advanced Automation (PSA). Questa impostazione è descritta in "Gestione dei gruppi di utenti" (pag. 215), nella sezione Gestione degli utenti.

Configurazione delle risposte definite

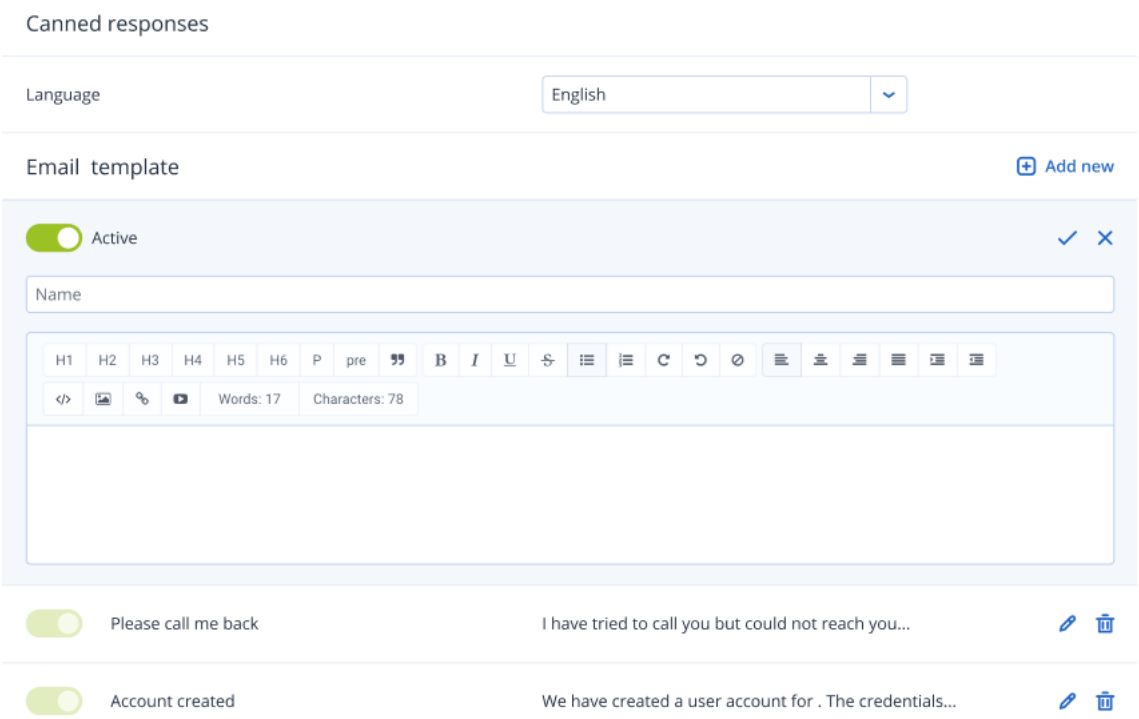
Le risposte definite consentono di aggiungere modelli di commento ai commenti standard durante la creazione di un nuovo ticket. Questi commenti vengono inclusi nella descrizione del ticket.

Creazione di una risposta definita

È possibile aggiungere qualsiasi numero di risposte definite al Service Desk.

Per creare una nuova risposta definita

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Risposte definite**.
2. Fare clic su **Aggiungi nuova**.
3. Definire un nome per la risposta definita e quindi aggiungere il contenuto pertinente.



È possibile utilizzare le seguenti variabili:
[SUPERIOR] - Il nome del responsabile dell'utente
[ENDUSER] - Il nome dell'utente
[SUPPORTUSER] - Il nome della persona che aggiorna il ticket
[STATUS] - Lo stato del ticket
[TITLE] - La descrizione del ticket

4. Per impostazione predefinita, la risposta definita è **Attiva**. Per disattivare la risposta definita, disattivare l'interruttore **Attiva**.
5. Fare clic su ✓ per salvare la risposta definita. Una volta salvata, la risposta definita può essere utilizzata come contenuto del campo **Commenti**.

Modifica o eliminazione di una risposta definita

È possibile modificare ed eliminare le risposte definite come necessario.

Per modificare una risposta definita

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Risposte definite**.
2. Fare clic sull'icona a matita accanto alla risposta definita da modificare e apportare le modifiche necessarie. Per ulteriori informazioni sulle opzioni disponibili, consultare "Creazione di una risposta definita" (pag. 314).
3. Fare clic su ✓ per salvare le modifiche.

Per eliminare una risposta definita

1. Nella schermata **Risposte definite**, fare clic sull'icona a cestino accanto alla risposta definita da eliminare.

2. Nel messaggio di conferma visualizzato, fare clic su **Sì**.

Configurazione delle priorità

È possibile definire le priorità dei ticket. Le priorità vengono utilizzate durante l'elaborazione di un ticket; tale processo dipende dalla priorità impostata per ogni singolo ticket. Ad esempio, un ticket con priorità *urgente* viene in genere elaborato prima di un ticket con priorità normale.

Aggiunta di una priorità

Per aggiungere una nuova priorità

1. Passare a **Impostazioni** > **Service Desk**, quindi fare clic su **Priorità**.
2. Fare clic su **Aggiungi nuova**.
3. Inserire il nome della priorità e fare clic su ✓. Tenere presente che il nome non riflette il livello di priorità, ma dovrebbe essere descrittivo.
   Per impostazione predefinita, la priorità è impostata come attiva.
   Dopo aver aggiunto correttamente la nuova priorità, questa potrà essere usata nel campo **Priorità** dei ticket (consultare "Creazione di un nuovo ticket" (pag. 223)). Se necessario, è possibile impostare priorità predefinite per i ticket standard e per i ticket provenienti da clienti specifici.

Modifica o eliminazione di una priorità

È possibile modificare ed eliminare le priorità come necessario.

Per modificare una priorità

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Priorità**.
2. Fare clic sull'icona a matita accanto alla priorità da modificare e apportare le modifiche necessarie.
3. Fare clic su ✓ per salvare le modifiche.
   È inoltre possibile disattivare una priorità disabilitando l'interruttore accanto alla priorità attiva corrispondente.

Per eliminare una priorità

1. Nella schermata **Priorità**, fare clic sul cestino accanto alla priorità da eliminare.
2. Nel messaggio di conferma visualizzato, fare clic su **Sì**.

Nota
La priorità può essere eliminata solo se è disattivata e se non è stata utilizzata in nessun ticket.

Gestione delle policy degli SLA

Una policy di un contratto sui livelli di servizio (SLA) è un impegno ufficiale sottoscritto tra l'utente e il cliente. Lo SLA descrive la qualità e la disponibilità del servizio che viene offerto al cliente e

l'impegno al rispetto di quanto sancito.

Semplificando la gestione degli SLA, Advanced Automation (PSA) aiuta a organizzare il flusso dei ticket di supporto e l'automazione dei conteggi relativi agli orari di lavoro fatturabili. Oltre a migliorare l'interazione con i clienti, permette di assicurare che i tecnici possano seguire le richieste di assistenza, evitando che i ticket restino per mesi senza risposta.

È possibile configurare e definire gli SLA da utilizzare per i contratti dei clienti, le attività relative ai ticket e per tenere traccia della conformità.

Creazione di un nuovo SLA

Per creare un nuovo SLA

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **SLA**.
2. Fare clic su **Aggiungi nuova**.
3. Nella schermata visualizzata, inserire il nome del nuovo SLA.
4. Definire l'intervallo di tempo applicabile dello SLA inserendo il tempo per la risposta iniziale (in ore) e l'intervallo di feedback (in ore), quindi inserire il tempo di inizio e di fine.
5. Selezionare la casella di controllo **Applica SLA durante** > **Fine settimana** per attivare o disattivare questo SLA durante i fine settimana.
6. Selezionare la casella di controllo **Applica SLA durante** > **Vacanze** per attivare o disattivare questo SLA durante i periodi di vacanza.
7. Configurare la tipologia di prezzo dello SLA in questione, selezionando tra **Prezzo fisso** o **Calcolo successivo**.
8. Selezionare un prodotto predefinito per la fatturazione e un'attività a tariffa speciale di fatturazione nei relativi elenchi a discesa.
   - **Prodotto predefinito per fatturazione**: questo parametro opzionale indica un prodotto di tipologia ticket fatturabile per gli aggiornamenti dei ticket effettuati nell'ambito delle ore lavorative previste dallo SLA. Ad esempio, quando un tecnico dei ticket lavora su un ticket ed è stato configurato uno SLA, il parametro **Prodotto predefinito per fatturazione** è preselezionato come prodotto fatturabile per il lavoro eseguito sul ticket. Il prodotto viene incluso automaticamente nel processo di approvazione degli orari relativi al ticket, in modo che al cliente possano essere automaticamente fatturare le ore pertinenti.
   - **Attività a tariffa speciale di fatturazione**: questo parametro opzionale equivale al parametro **Prodotto predefinito per fatturazione**, ma è utilizzato per gli aggiornamenti ai ticket eseguiti fuori dall'ambito delle ore lavorative previste dallo SLA.
9. Per impostare questo SLA come predefinito, selezionare la casella di controllo **Assegna un contratto di servizio predefinito**.
10. Fare clic su ✓ per salvare lo SLA.

    Per impostazione predefinita, lo SLA è **Attivo**; per disattivarlo, disabilitare l'opzione **Attivo**.

    Dopo aver creato il nuovo SLA, questo potrà essere utilizzando nel campo **SLA** dei ticket. Per ulteriori dettagli, consultare "Creazione di un nuovo ticket" (pag. 223).

Modifica di uno SLA

Per modificare uno SLA

1. Passare a **Impostazioni > Service Desk**, quindi selezionare **SLA**.
2. Fare clic sull'icona della matita per lo SLA pertinente.
3. Apportare le modifiche desiderate allo SLA. Per ulteriori dettagli, consultare "Creazione di un nuovo SLA" (pag. 317).
4. Fare clic su ✓ per salvare le modifiche.

Nota
Se lo SLA è stato precedentemente utilizzato dai clienti (nei ticket), non sarà possibile disattivarlo.

Definizione di categorie e sottocategorie

È possibile definire un numero illimitato di categorie di ticket da utilizzare nel Service Desk di Advanced Automation (PSA).

Advanced Automation (PSA) è disponibile con una gamma precompilata di categorie e sottocategorie; se applicate ai ticket, le categorie e le sottocategorie forniscono una valida panoramica delle problematiche che richiedono i tempi di risposta più lunghi e consentono di intraprendere le azioni adeguate. Queste informazioni possono essere visualizzate anche per ogni singolo cliente.

La panoramica permette di migliorare l'erogazione dei servizi. Ad esempio, se un cliente presenta il 50% dei ticket categorizzato come *Workstation/virus*, potrebbe essere necessario aggiornare alcune misure di sicurezza e offrire formazione al personale interessato.

Creazione di una categoria o sottocategoria

Per definire una nuova categoria o sottocategoria

1. Passare a **Impostazioni > Service Desk**, quindi fare clic su **Categorie e sottocategorie**.
2. Fare clic su **Aggiungi nuova**, quindi inserire il nome della categoria. Per convertire una categoria in sottocategoria, selezionare la categoria padre pertinente. Una volta creata la categoria o sottocategoria, questa potrà essere attivata o disattivata come necessario, come descritto di seguito.

Per attivare/disattivare una categoria o sottocategoria

Nella schermata **Categorie e sottocategorie**, fare clic sull'interruttore attivo per attivare o disattivare la specifica categoria o sottocategoria.

Modifica o eliminazione di una categoria o sottocategoria

Per modificare una categoria o sottocategoria

1. Nella schermata **Categorie e sottocategorie**, fare clic sull'icona della matita della categoria o sottocategoria pertinente.
2. Modificare come necessario.

Per eliminare una categoria o sottocategoria

1. Nella schermata **Categorie e sottocategorie**, fare clic sul cestino relativo alla categoria o sottocategoria pertinente.
2. Nel messaggio di conferma visualizzato, fare clic su **Sì**.

Nota
La categoria o sottocategoria può essere eliminata solo se è disattivata e se non è stata utilizzata in nessun ticket.

Impostazione dei valori predefiniti

È possibile definire i valori predefiniti per molte funzionalità di Advanced Automation (PSA).

Importante
Le impostazioni predefinite iniziali del sistema vengono applicate all'attivazione di tutti i clienti esistenti. Quando vengono creati nuovi clienti, le impostazioni predefinite correnti (elencate di seguito) vengono applicate alle impostazioni del servizio clienti. In seguito però, se vengono aggiornate le impostazioni predefinite, i valori del servizio clienti non vengono aggiornati automaticamente, e quindi dovranno essere aggiornati manualmente.

Nota
È possibile sovrascrivere le impostazioni predefinite generali con valori specifici per il cliente nelle impostazioni di ciascun cliente. Per accedere a queste impostazioni specifiche per il cliente, passare a **Clienti**, fare clic sull'icona dei puntini di sospensione per il tenant pertinente e quindi selezionare **Configura**. Poi fare clic sulla scheda **Configura** e, nella sezione **Service Desk**, fare clic sull'icona della matita per aggiornare le impostazioni predefinite pertinenti per il cliente selezionato.

I valori che possono essere aggiornati includono: **SLA predefinito**, **Categoria predefinita**, **Priorità predefinita**, **Gruppo predefinito**, **Supporto utente predefinito**, **Contatto principale predefinito** e **Documentazione cliente**.

L'impostazione **Giorni liberi per anno** può essere aggiornata nella sezione **Impostazioni utente**. Per accedere a queste impostazioni, passare a **La mia azienda** > **Utenti**, selezionare l'utente pertinente e quindi fare clic su **Impostazioni utente**.

Per definire i valori predefiniti

1. Passare a **Impostazioni > Service Desk**.
2. Selezionare **Valori predefiniti**.
   Viene visualizzato l'elenco dei valori predefiniti:

- **SLA predefinito**: lo SLA predefinito applicato ai ticket. Per impostazione predefinita, è selezionata l'opzione **SLA predefinito**.
- **Categoria**: la categoria predefinita del ticket. Per impostazione predefinita, è selezionata l'opzione **Problema hardware**.
- **Priorità predefinita**: la priorità predefinita per i ticket. Per impostazione predefinita, è selezionata l'opzione **Normale**.
- **Gruppo predefinito**: il gruppo predefinito per i ticket. Per impostazione predefinita, è selezionata l'opzione **Gruppo di supporto**.
- **Utente del supporto predefinito**: l'utente del supporto predefinito per i ticket. Per impostazione predefinita, viene selezionato l'utente che ha attivato il servizio Advanced Automation (PSA). In alternativa, è possibile selezionare **Pool di ticket**, per garantire che i nuovi ticket vengano assegnati automaticamente al pool di ticket, piuttosto che a un utente specifico.
- **Giorni liberi per anno**: i giorni liberi per anno predefiniti per gli utenti. Per impostazione predefinita, il valore è **15**.
- **Policy per i giorni di ferie rimanenti**: la regola organizzativa per i giorni di ferie residui per gli utenti. Quando inizia un nuovo anno (1 gennaio, 00:00), Advanced Automation (PSA) ricalcola automaticamente i saldi dei giorni di ferie retribuite per tutti gli utenti con un ruolo Advanced Automation (PSA) in base alla policy specificata. Selezionare una delle seguenti opzioni:
  - **Elimina giorni di ferie rimanenti** (impostazione predefinita)
  - **Sposta tutti i giorni di ferie rimanenti all'anno successivo**
  - **Sposta alcuni giorni di ferie all'anno successivo**

    Quando è selezionata l'opzione **Sposta alcuni giorni di ferie all'anno successivo**, viene visualizzato il campo aggiuntivo **Numero massimo di giorni di ferie da spostare**, in cui è possibile definire il numero richiesto.
- **Documenti del cliente**: un collegamento alla documentazione relativa al cliente. Per impostazione predefinita, questo campo è vuoto.

  Quando viene definito un collegamento, viene visualizzato un collegamento alla **Documentazione per i clienti** nella schermata **Crea nuovo ticket** quando si crea un nuovo ticket (vedere "Creazione di un nuovo ticket" (pag. 223)) e nella scheda **Panoramica** quando si modifica un ticket (vedere "Aggiornamento dei ticket" (pag. 226)).
- **Soglia di notifica della percentuale di presenza**: si raggiunge la soglia di notifica quando il tempo di lavoro registrato dall'utente o dal gruppo del quale l'utente è membro o responsabile è inferiore alle ore stabilite per quel giorno; viene inviato un promemoria che ricorda di completare la registrazione orario. Per impostazione predefinita, è selezionato il valore **85**.
- **Sospendi automaticamente il timer del ticket alla schermata di uscita**: è possibile mettere automaticamente in pausa il timer del ticket ogni volta che gli utenti passano dalla schermata attiva a un'altra schermata. Per impostazione predefinita, è selezionata l'opzione **No**.

- **Aggiornamento ticket obbligatorio**: indica se il campo **Descrizione ticket** nelle impostazioni del ticket è obbligatorio. Questa impostazione consente di tracciare le modifiche apportate a un ticket con maggiore precisione durante l'elaborazione del ticket stesso. Per impostazione predefinita, è selezionata l'opzione **No**.
- **Portale dei ticket pubblico**: la pagina a cui gli utenti possono accedere per inviare i ticket direttamente, senza registrarsi o accedere al sistema. Quando è abilitata, viene visualizzato l'**URL del portale dei ticket** (un collegamento generato dal sistema).
  Per ulteriori informazioni su come inviare un ticket, consultare Invio di ticket del Service Desk tramite il portale dei ticket.

  Nota
  Il portale pubblico dei ticket ha lo stesso branding definito per il proprio tenant, come descritto in "Configurazione del branding e del marchio personalizzabile" (pag. 97).

  È possibile anche incorporare il modulo dei ticket nei siti web di terze parti. Per ulteriori informazioni, consultare "Incorporare il modulo di invio ticket nel proprio sito web" (pag. 237).

  - **Elaborazione delle richieste provenienti da utenti sconosciuti**: stabilisce se il portale pubblico dei ticket elabora le richieste provenienti da utenti non registrati nel sistema. Questa opzione è visualizzata solo se l'opzione **Portale dei ticket pubblico** è abilitata. Per impostazione predefinita, è selezionata l'opzione **Disattivato**.

3. Applicare i valori predefiniti desiderati e fare clic su **Salva**.

Definizione delle impostazioni relative al Paese e alla lingua

La schermata **Impostazioni Paese** permette di definire le impostazioni globali dell'azienda che vengono utilizzate quando si lavora con Advanced Automation (PSA), incluso il Paese e il fuso orario predefiniti. Queste impostazioni globali incidono sulla valuta e sull'orario visualizzati, e sono molto importanti per definire gli orari che rientrano in un contratto sui livelli di servizio (SLA).

Per definire le impostazioni relative al Paese e alla lingua

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Impostazioni Paese**.
2. Nella sezione **Impostazioni Paese**, fare clic sull'icona a matita per modificare le impostazioni seguenti.
   - **Paese predefinito**: selezionare il Paese pertinente. Il Paese selezionato definisce la valuta predefinita utilizzata in Advanced Automation (PSA) per tutti i prezzi e i costi.
   - **Fuso orario**: selezionare il fuso orario pertinente. Il fuso orario incide sulle ore dello SLA perché determina se i ticket ricevuti rientrano negli orari previsti dallo SLA oppure no. Può anche incidere sul prezzo delle attività eseguite sui ticket.
   - **Ora legale**: fare clic sull'interruttore per abilitare l'ora legale.
3. Fare clic su ✓ per salvare le modifiche.

4. Nella sezione **Lingue**, fare clic sull'icona a matita per definire la lingua di sistema predefinita utilizzata in Advanced Automation (PSA).
5. Fare clic sull'interruttore per abilitare la lingua pertinente.
6. Fare clic su ✓ per salvare le modifiche.

Attivazione e disattivazione degli stati

La schermata **Stati** mostra i vari stati disponibili per il Service Desk, i preventivi e i ticket di progetto. È possibile attivare o disattivare gli stati dei ticket.

Nota
Non è possibile aggiungere o eliminare uno stato o modificarne il nome. In alcune integrazioni, gli stati sono collegati agli stati dei ticket.

Per attivare o disattivare gli stati

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Stati**.
2. Fare clic su **Modifica**.
3. Nell'elenco degli stati visualizzato, selezionare l'opzione di attivazione/disattivazione degli stati pertinenti.
   Se uno stato non è modificabile, significa che è predefinito in Advanced Automation (PSA) e non può essere modificato. Inoltre, se uno stato è attualmente in uso, non può essere disattivato.

   Nota
   I seguenti stati non possono essere disattivati perché sono utilizzati nel flusso predefinito dei ticket e nelle integrazioni:

   - Nuovo
   - In corso
   - Violazione dello SLA
   - In attesa di risposta
   - Completato
   - Riaperto
   - Risolto
   - Chiuso

   Per ulteriori informazioni sui tipi di stato del ticket disponibili per il Service Desk, i preventivi e i progetti, consultare "Tipi di stato del ticket" (pag. 323).
4. Fare clic su **Salva**.

Tipi di stato del ticket

L'elenco completo dei tipi di stato dei ticket obbligatori e facoltativi è mostrato nella schermata **Stati**.

Gli stati del ticket obbligatori sono predefiniti dal sistema e non possono essere disattivati. Gli stati del ticket facoltativi possono essere attivati e disattivati, come necessario. Per ulteriori informazioni, consultare "Attivazione e disattivazione degli stati" (pag. 322).

Stati del ticket obbligatori

Stato	Incluso in Service Desk (ticket del Service Desk e del preventivo)	Incluso nei progetti (ticket dei passaggi del progetto)
Nuovo	Sì	Sì
In corso	Sì	Sì
Completato	No	Sì
Chiuso	Sì	No
Risolto	Sì	No
In attesa di risposta	Sì	No
Violazione dello SLA	Sì	No
Riaperto	Sì	No

Stati del ticket facoltativi

Stato	Incluso in Service Desk (ticket del Service Desk e del preventivo)	Incluso nei progetti (ticket dei passaggi del progetto)
Lavoro in sede pianificato	Sì	No
Problema	Sì	No
Preventivo in sospeso	Sì	No
Attività pianificate	Sì	No
In attesa di approvazione	Sì	No
Modifica	Sì	No
Aggiornamento da dipendente	Sì	No
Aggiornamento cliente ricevuto	Sì	No

Stato	Incluso in Service Desk (ticket del Service Desk e del preventivo)	Incluso nei progetti (ticket dei passaggi del progetto)
Attività pianificate	Sì	No
Pianifica attività in sede	Sì	No
Aggiornamento aggiunto da fornitore	Sì	No
Fornitore in sospeso	Sì	No
In attesa	Sì	Sì
Avvio in sospeso	No	Sì
Ritardato	No	Sì

Definizione delle impostazioni per l'integrazione dei ticket RMM predefiniti

Quando si procede all'integrazione con i sistemi Remote Monitoring and Management (RMM), è possibile impostare i campi **SLA predefinito**, **Categoria** e **Priorità** per i ticket generati dal sistema RMM. Se un ticket è integrato in RMM, vengono applicati automaticamente i valori predefiniti, che corrisponderanno a quelli impostati con la procedura indicata di seguito.

Per definire le impostazioni per l'integrazione dei ticket RMM predefiniti

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Integrazione ticket RMM**.
2. Fare clic su **Modifica**.
3. Impostare i valori relativi a **SLA predefinito**, **Categoria** e **Priorità** e fare clic su **Salva**.

Gestione dei modelli di e-mail

Nella schermata **Modelli e-mail** è possibile visualizzare tutti i modelli di e-mail predefiniti inclusi in Advanced Automation (PSA). Questi modelli sono utilizzati per le comunicazioni esterne con gli utenti finali. È possibile personalizzare i modelli utilizzando l'editor per testi formattati o incollando nell'editor il codice HTML personalizzato.

Non è possibile aggiungere o eliminare i modelli e-mail.

Nota
I modelli e-mail predefiniti sono progettati per essere visualizzati correttamente con la maggior parte dei client di posta su desktop e dispositivi mobili. Quando si apportano le modifiche, verificare che venga mantenuta la visualizzazione corretta.

Modifica di un modello e-mail

Per modificare un modello e-mail

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Modelli e-mail**.
2. Fare clic sull'icona a matita relativa al modello da modificare.
3. Aggiornare il modello come necessario.
   È possibile utilizzare le seguenti variabili per i diversi tipi di messaggio:

Aggiungi ticket da e-mail		**Aggiorna ticket da e-mail**		**Aggiungi ticket da applicazione**		**Aggiorna ticket da applicazione**	
Oggetto	**Testo del messaggio**	**Oggetto**	**Testo del messaggio**	**Oggetto**	**Testo del messaggio**	**Oggetto**	**Testo del messaggio**
[REF]	[REF]	[REF]	[REF]	[REF]	[REF]	[REF]	[REF]
[TITLE]	[STATUS]	[TITLE]	[STATUS]	[TITLE]	[STATUS]	[TITLE]	[STATUS]
	[TITLE]		[TITLE]	[SUPPORTUSER]	[TITLE]		[TITLE]
	[UPDATE]		[UPDATE]		[UPDATE]		[UPDATE]
	[ENDUSER]		[ENDUSER]		[ENDUSER]		[ENDUSER]
					[SUPPORTUSER]		[SUPPORTUSER]

4. Per personalizzare il colore dello sfondo dell'e-mail, aggiungere uno snippet di codice di stile al codice HTML del modello. Altrimenti, al momento della creazione del messaggio e-mail viene aggiunto lo stile predefinito.
   Esempio di codice di stile per un paragrafo con sfondo bianco:
    [CONTENUTO DEL MODELLO E-MAIL]
5. Fare clic su ✓ per salvare le modifiche.

Nota
Se si apporta una serie di modifiche a un modello e-mail e poi si decide di ripristinare il modello al layout e al testo predefinito è necessario riapplicare il codice HTML del modello. Per ulteriori informazioni, consultare "Modelli di e-mail predefiniti" (pag. 325)

Modelli di e-mail predefiniti

Advanced Automation (PSA) include una serie di modelli di e-mail predefiniti personalizzabili. Se è necessario ripristinare un modello alla versione predefinita, è possibile utilizzare i codici HTML dei modelli predefiniti forniti di seguito.

- Ticket risolto chiuso
- Preventivo creato
- Nuovo ticket da e-mail

- Aggiornamento ticket
- Richiesta di valutazione ticket
- Valutazione ticket ricevuta
- Preventivo elaborato
- Nuovo ticket
- Nuova fattura
- Ticket unificato

Ticket risolto chiuso

Oggetto: Ticket risolto chiuso

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6">  <tbody> <tr style="font-size: 14px;">  <td
style="font-size: 14px;vertical-align: top;"> </td>    <td class="container"
width="600" style="font-size: 14px;vertical-align: top;">  <div class="content"
style="font-size: 14px;">  <table class="main" width="100%" cellpadding="0"
cellspacing="0" style="font-size: 14px;background-color: #fff;"
bgcolor="#fff">        <tbody>  <tr style="font-size: 14px;">    <td class="alert
alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align:
center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3"> Il ticket
risolto è stato chiuso</td>  </tr>    <tr style="font-size: 14px;">    <td
class="content-wrap" style="font-size: 14px;vertical-align: top;">    <table
width="100%" cellpadding="0" cellspacing="0" style="font-size:
14px;">        <tbody> <tr style="font-size: 14px;">  <td class="content-block"
style="font-size: 14px;vertical-align: top;"> </td>            </tr>  <tr
style="font-size: 14px;">  <td class="content-block" style="font-size:
14px;vertical-align: top;">Gentile [ENDUSER],</td> </tr>  <tr style="font-size:
14px;">    <td class="content-block" style="font-size: 14px;vertical-align: top;">il
ticket con numero di riferimento [REF] è stato chiuso automaticamente perché è
rimasto nello stato 'Risolto' per più di [WAITINGDAYS] giorni.</td>      </tr>  <tr
style="font-size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-
align: top;">          <br>
</td>    </tr>  </tbody>        </table>        </td>  </tr>    </tbody>  </table>
<div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
</div>  </td>    <td style="font-size: 14px;vertical-align:
top;"></td>  </tr>    </tbody>  </table>
```

Preventivo creato

Oggetto: È stato creato un nuovo preventivo con descrizione: [TITLE]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> </tr> <tr> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Abbiamo creato il tuo nuovo
preventivo</td> </tr> <tr style="font-size: 14px;"> <td class="content-wrap"
style="font-size: 14px;vertical-align: top;"> <table width="100%" cellpadding="0"
cellspacing="0" style="font-size: 14px;"> <tbody> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;"></td> </tr> <tr
style="font-size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-
align: top;">Gentile [CLIENT],</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;">puoi trovare in
allegato il nuovo preventivo con descrizione [TITLE] e numero [number].</td> </tr>
<tr style="font-size: 14px;"> <td class="content-block" style="font-size:
14px;vertical-align: top;">Puoi utilizzare il seguente link per esaminare il
preventivo.</td> </tr> <tr style="font-size: 14px;"> <td class="content-block"
style="font-size: 14px;vertical-align: top;"> <a href="[QUOTE_LINK]">Nuovo
preventivo</a> </td> </tr> <tr style="font-size: 14px;"> <td class="content-block"
style="font-size: 14px;vertical-align: top;"> <br> </td> </tr> </tbody> </table>
</td> </tr> </tbody> </table> <div class="footer" style="font-size: 14px;width:
100%;color: #999;"></div> </div> </td> <td style="font-size: 14px;vertical-align:
top;"></td> </tr> </tbody> </table>
```

Nuovo ticket da e-mail

Oggetto: Nuovo ticket con numero di riferimento: [REF]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Nuovo ticket creato da e-mail</td>
</tr> <tr style="font-size: 14px;"> <td class="content-wrap" style="font-size:
14px;vertical-align: top;"> <table width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;"></td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
top;">Un nuovo ticket è stato creato dall'e-mail che riporta il seguente numero di
riferimento: [REF]</td> </tr> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;">Stato del ticket: [STATUS]</td>
```

```
</tr> <tr style="font-size: 14px;"> <td class="content-block" style="font-size:
14px;vertical-align: top;">Titolo del ticket: [TITLE]</td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
top;">Richiesta: [UPDATE]</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;">Un tecnico del
supporto gestirà la tua richiesta nel più breve tempo possibile.</td> </tr> <tr
style="font-size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-
align: top;"> <br> </td> </tr> </tbody> </table> </td> </tr> </tbody> </table> <div
class="footer" style="font-size: 14px;width: 100%;color: #999;"></div> </div> </td>
<td style="font-size: 14px;vertical-align: top;"></td> </tr> </tbody> </table>
```

Aggiornamento ticket

Oggetto: Nuovo aggiornamento per il ticket [TITLE] con numero di riferimento [REF]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Aggiornamento ticket</td> </tr> <tr
style="font-size: 14px;"> <td class="content-wrap" style="font-size: 14px;vertical-
align: top;"> <table width="100%" cellpadding="0" cellspacing="0" style="font-size:
14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-block" style="font-
size: 14px;vertical-align: top;"></td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;"> È stato
effettuato un nuovo aggiornamento per il ticket con numero di riferimento:
[REF]</td> </tr> <tr style="font-size: 14px;"> <td class="content-block"
style="font-size: 14px;vertical-align: top;">Stato del ticket: [STATUS]</td> </tr>
<tr style="font-size: 14px;"> <td class="content-block" style="font-size:
14px;vertical-align: top;">Messaggio del tecnico di supporto: [UPDATE]</td> </tr>
<tr style="font-size: 14px;"> <td class="content-block" style="font-size:
14px;vertical-align: top;"> <br> </td> </tr> </tbody> </table> </td> </tr> </tbody>
</table> <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
</div> </td> <td style="font-size: 14px;vertical-align: top;"></td> </tr> </tbody>
</table>
```

Richiesta di valutazione ticket

Oggetto: Richiesta di valutazione ticket

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> </tr> <tr> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Abbiamo chiuso il tuo ticket.
Segnalaci le tue impressioni sul nostro lavoro</td> </tr> <tr style="font-size:
14px;"> <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
<table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">
<tbody> <tr style="font-size: 14px;"> <td style="font-size: 14px;vertical-align:
top;"></td> </tr> <tr style="font-size: 14px;"> <td style="font-size: 14px;vertical-
align: top;">Gentile [CUSTOMER],</td> </tr> <tr style="font-size: 14px;"> <td
style="font-size: 14px;vertical-align: top;"> il tuo ticket con numero [REF] è stato
chiuso. Di seguito le informazioni sul ticket:<br> <br> </td> </tr> <tr style="font-
size: 14px;"> <td style="font-size: 14px;vertical-align: top;"> <div style="float:
left;">Numero di riferimento del ticket:</div> <div style="float: left;">[REF]</div>
</td> </tr> <tr style="font-size: 14px;"> <td style="font-size: 14px;vertical-align:
top;"> <div style="float: left;">Tecnico del supporto:</div> <div style="float:
left;">[SUPPORTUSER]</div> </td> </tr> <tr style="font-size: 14px;"> <td
style="font-size: 14px;vertical-align: top;"> <div style="float: left;">Messaggio
del tecnico del supporto:</div> <div style="float: left;">[SUPPORTUSERMESSAGE]</div>
</td> </tr> <tr style="font-size: 14px;"> <td style="font-size: 14px;vertical-align:
top;"> <div style="float: left;">Problema iniziale:</div> <div style="float: left;">
[PROBLEM]</div> </td> </tr> <tr style="font-size: 14px;"> <td style="font-size:
14px;vertical-align: top;"> <div style="float: left;">Titolo del ticket:</div> <div
style="float: left;"> [TITLE]<br> <br> </div> </td> </tr> <tr style="font-size:
14px;"> <td style="font-size: 14px;vertical-align: top;">Con quale probabilità
consiglieresti la nostra azienda/prodotto/servizio a un conoscente o a un
collega?</td> </tr> <tr style="font-size: 14px;"> <td style="font-size:
14px;vertical-align: top;"> <table cellspacing="0"> <tbody> <tr> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=0" class="fa fa-star" id="rating0"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">0</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=1" class="fa fa-star" id="rating1"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">1</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=2" class="fa fa-star" id="rating2"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">2</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=3" class="fa fa-star" id="rating3"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">3</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=4" class="fa fa-star" id="rating4"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">4</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=5" class="fa fa-star" id="rating5"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">5</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=6" class="fa fa-star" id="rating6"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">6</div> </a> </td> <td style="width:
```

```
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=7" class="fa fa-star" id="rating7"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">7</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=8" class="fa fa-star" id="rating8"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">8</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=9" class="fa fa-star" id="rating9"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">9</div> </a> </td> <td style="width:
50px;height: 50px;text-align: center;vertical-align: middle;"> <a href="[URL]/?key=
[KEY]&amp;rateValue=10" class="fa fa-star" id="rating10"> <div style="font-size:
14px;vertical-align: bottom;color:#666f7b">10</div> </a> </td> </tr> </tbody>
</table> </td> </tr> <tr style="font-size: 14px;"> <td style="font-size:
14px;vertical-align: top;"> <br> </td> </tr> </tbody> </table> </td> </tr> </tbody>
</table> <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
</div> </td> <td style="font-size: 14px;vertical-align: top;"></td> </tr> </tbody>
</table>
```

Valutazione ticket ricevuta

Oggetto: Il cliente [Customer] ha valutato il ticket [REF]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Il tuo ticket è stato valutato</td>
</tr> <tr style="font-size: 14px;"> <td class="content-wrap" style="font-size:
14px;vertical-align: top;"> <table width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;"></td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
top;">Gentile [SUPPORTUSER],</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;">il tuo ticket con
numero di riferimento [REF] è stato valutato: </td> </tr> <tr style="font-size:
14px;"> <td class="content-block" style="font-size: 14px;vertical-align: top;">
Numero di riferimento del ticket: [REF]</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;"> Livello:
[GRADE]</td> </tr> <tr style="font-size: 14px;"> <td class="content-block"
style="font-size: 14px;vertical-align: top;"> Utente finale: [CLIENT]</td> </tr> <tr
style="font-size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-
align: top;"> Cliente: [CUSTOMER]</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;"> <br> </td> </tr>
</tbody> </table> </td> </tr> </tbody> </table> <div class="footer" style="font-
size: 14px;width: 100%;color: #999;"></div> </div> </td> <td style="font-size:
14px;vertical-align: top;"></td> </tr> </tbody> </table>
```

Preventivo elaborato

Oggetto: Il preventivo [DESCRIPTION] - [NUMBER] è stato [ACCEPTED]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> </tr> <tr> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Il preventivo è stato elaborato</td>
</tr> <tr style="font-size: 14px;"> <td class="content-wrap" style="font-size:
14px;vertical-align: top;"> <table width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;"></td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
top;">Gentile [CLIENT],</td> </tr> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;">ti scriviamo per informarti che
il preventivo [DESCRIPTION] - [NUMBER] è stato [ACCEPTED] da [USER].</td> </tr> <tr
style="font-size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-
align: top;"> <br> </td> </tr> </tbody> </table> </td> </tr> </tbody> </table> <div
class="footer" style="font-size: 14px;width: 100%;color: #999;"></div> </div> </td>
<td style="font-size: 14px;vertical-align: top;"></td> </tr> </tbody> </table>
```

Nuovo ticket

Oggetto: Nuovo ticket creato: [TITLE] - numero di riferimento [REF] - Tecnico del supporto/Unità aziendale [SUPPORTUSER]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">È stato creato un nuovo ticket</td>
</tr> <tr style="font-size: 14px;"> <td class="content-wrap" style="font-size:
14px;vertical-align: top;"> <table width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;"></td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
```

```
top;">Abbiamo creato per te un nuovo ticket con il seguente numero di riferimento:
[REF]</td> </tr> <tr style="font-size: 14px;"> <td class="content-block"
style="font-size: 14px;vertical-align: top;">Stato del ticket: [STATUS]</td> </tr>
<tr style="font-size: 14px;"> <td class="content-block" style="font-size:
14px;vertical-align: top;">Titolo del ticket: [TITLE]</td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
top;">Richiesta: [UPDATE]</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;">Tecnico del
supporto/Unità aziendale: [SUPPORTUSER]</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;"> <br> </td> </tr>
</tbody> </table> </td> </tr> </tbody> </table> <div class="footer" style="font-
size: 14px;width: 100%;color: #999;"></div> </div> </td> <td style="font-size:
14px;vertical-align: top;"></td> </tr> </tbody> </table>
```

Nuova fattura

Oggetto: È stata emessa la fattura numero [number]

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> </tr> <tr> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Abbiamo emesso una nuova fattura</td>
</tr> <tr style="font-size: 14px;"> <td class="content-wrap" style="font-size:
14px;vertical-align: top;"> <table width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-
block" style="font-size: 14px;vertical-align: top;"></td> </tr> <tr style="font-
size: 14px;"> <td class="content-block" style="font-size: 14px;vertical-align:
top;">Gentile [CUSTOMER],</td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;">puoi trovare in
allegato la fattura con numero [number].</td> </tr> <tr style="font-size: 14px;">
<td class="content-block" style="font-size: 14px;vertical-align: top;">Utilizza uno
dei seguenti link per completare il pagamento: </td> </tr> <tr style="font-size:
14px;"> <td class="content-block" style="font-size: 14px;vertical-align: top;"> <a
href="[PAYPAL_LINK]">Paga con PayPal</a> </td> </tr> <tr style="font-size: 14px;">
<td class="content-block" style="font-size: 14px;vertical-align: top;"> <a href="
[STRIPE_LINK]">Paga con Stripe</a> </td> </tr> <tr style="font-size: 14px;"> <td
class="content-block" style="font-size: 14px;vertical-align: top;"> <br> </td> </tr>
</tbody> </table> </td> </tr> </tbody> </table> <div class="footer" style="font-
size: 14px;width: 100%;color: #999;"></div> </div> </td> <td style="font-size:
14px;vertical-align: top;"></td> </tr> </tbody> </table>
```

Ticket unificato

Oggetto: Il ticket [TITLE] - numero di riferimento - [REF] è stato unito a un altro ticket

Codice:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6"> <tbody> <tr style="font-size: 14px;"> <td style="font-
size: 14px;vertical-align: top;"></td> <td class="container" width="600"
style="font-size: 14px;vertical-align: top;"> <div class="content" style="font-size:
14px;"> <table class="main" width="100%" cellpadding="0" cellspacing="0"
style="font-size: 14px;background-color: #fff;" bgcolor="#fff"> <tbody> <tr
style="font-size: 14px;"> <td class="alert alert-warning" style="font-size:
16px;vertical-align: top;color: #fff;text-align: center;background-color:
#0065E3;text-align: center;" bgcolor="#0065E3">Ticket unificato</td> </tr> <tr
style="font-size: 14px;"> <td class="content-wrap" style="font-size: 14px;vertical-
align: top;"> <table width="100%" cellpadding="0" cellspacing="0" style="font-size:
14px;"> <tbody> <tr style="font-size: 14px;"> <td class="content-block" style="font-
size: 14px;vertical-align: top;">Il ticket con numero di riferimento: [REF]</td>
</tr> <tr style="font-size: 14px;"> <td class="content-block" style="font-size:
14px;vertical-align: top;">è stato unito al ticket con numero di riferimento:
[MERGETARGETTICKETNUMBER]</td> </tr> </tbody> </table> </td> </tr> </tbody> </table>
<div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div> </div>
</td> <td style="font-size: 14px;vertical-align: top;"></td> </tr> </tbody> </table>
```

Definizione delle attività con monitoraggio degli orari

Le attività vengono utilizzate per le registrazioni orario, che a loro volta aiutano a comprendere le schede delle attività. Ad esempio, è possibile monitorare il tempo dedicato dai dipendenti alle attività relative o non relative ai clienti, oppure il tempo trascorso in attività fatturabili o non fatturabili.

In alcuni casi più specifici, alle attività fatturabili dei clienti è possibile applicare tariffe specifiche, in modo che queste vengano applicate automaticamente durante una registrazione orario. Ad esempio, è possibile applicare automaticamente una tariffa più alta a una registrazione orario relativa a un intervento nella sede di un cliente.

La schermata **Attività** mostra un elenco delle attività correnti. Puoi aggiungerne e modificare le attività elencate, e attivare o disattivare un'attività (facendo clic sull'interruttore **Stato**), come necessario. Disattivata un'attività, questa viene rimossa dall'elenco della schermata **Attività** e da qualsiasi registrazione alla quale è stata aggiunta nel tempo.

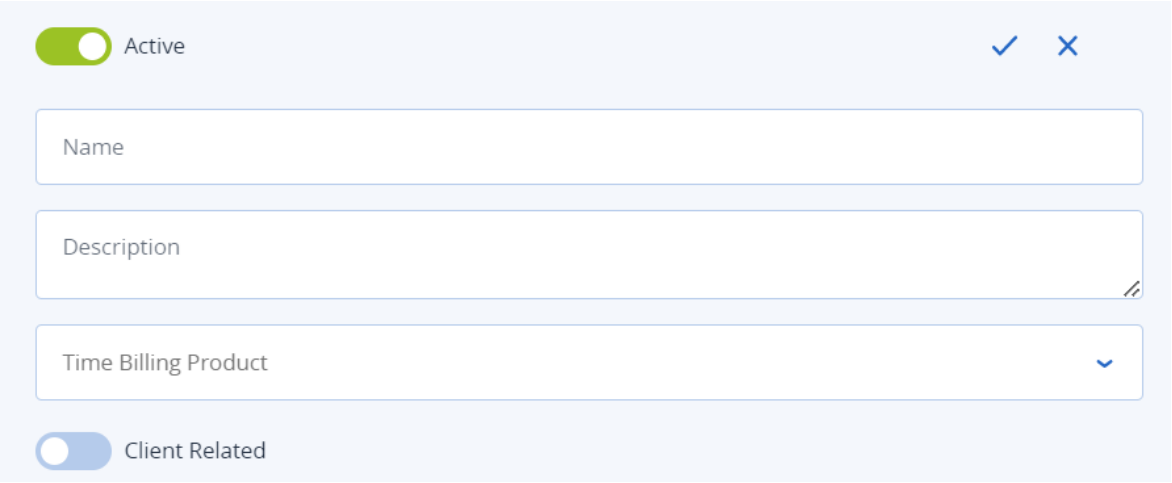
In Advanced Automation (PSA) sono incluse le seguenti attività predefinite.

- Gestione registri contabili
- Gestione contratti
- Pausa pranzo
- Progettazione
- Gestione progetto

Creazione di un'attività

Per creare un'attività

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Attività**.
2. Fare clic su **Aggiungi nuova**.
   Nella parte superiore dell'elenco Attività viene visualizzata una nuova sezione.



3. Eseguire le seguenti operazioni:
   - Fare clic sull'interruttore **Attiva** per abilitare l'attività (è abilitata per impostazione predefinita).
   - Inserire un nome per l'attività, con una lunghezza massima di 50 caratteri.
   - Inserire una descrizione per l'attività. Sarà visibile nell'elenco principale delle attività mostrato nella schermata **Attività**.
   - Selezionare il prodotto pertinente dall'elenco a discesa **Prodotto per fatturazione oraria**. Quando il prodotto selezionato viene utilizzato in un contratto o in un articolo di vendita, il processo di fatturazione utilizza la relativa tariffa di fatturazione al momento della fatturazione della registrazione orario (che include l'attività pertinente).
   - Fare clic sull'interruttore **Relativo al cliente** per attivarla. Quando attiva, l'orario dell'attività viene mostrato come relativo al cliente nel report Schede attività. Quando non è attiva invece, l'orario di tale attività viene mostrato come orario interno nel report Schede attività.
4. Fare clic su ✓ per salvare l'attività.

   Ora l'attività è disponibile e può essere utilizzata nelle attività con monitoraggio degli orari. Quando si definisce una nuova registrazione orario, è possibile selezionare l'attività da assegnare alla registrazione orario dal campo **Attività**, ad esempio *Gestione progetto* oppure *Pausa pranzo*.

Modifica di un'attività

Tutte le attività sono modificabili, incluse quelle predefinite incluse in Advanced Automation (PSA). È possibile disattivare un'attività, ma non eliminarla.

Per modificare un'attività

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Attività**.
2. Fare clic sull'icona della matita per l'attività pertinente.

3. Apportare le modifiche desiderate all'attività. Per ulteriori dettagli, consultare "Creazione di un'attività" (pag. 333).
   È possibile disattivare l'attività facendo clic sull'interruttore **Attiva**. L'attività viene così rimossa dall'elenco delle attività della schermata **Attività**, e da qualsiasi registrazione oraria alla quale è stata aggiunta.
4. Fare clic su ✓ per salvare le modifiche.

Visualizzazione di elementi di configurazione

Gli elementi di configurazione rappresentano le risorse (dispositivi del cliente) gestite tramite una piattaforma RMM esterna che vengono importate automaticamente in Advanced Automation (PSA). Nelle impostazioni relative a **Service Desk** è possibile visualizzare i dettagli degli elementi di configurazione e anche associarli a utenti specifici.

Nota
La sincronizzazione tra siti e dispositivi dei clienti e software RMM può richiedere fino a 15 minuti. Ciò significa che la configurazione di un nuovo dispositivo nella piattaforma RMM diventa visibile in Advanced Automation (PSA) entro 15 minuti. Tutte le modifiche vengono aggiornate nel database di Advanced Automation (PSA).

Per visualizzare gli elementi di configurazione

1. Passare a **Impostazioni** > **Service Desk**, quindi selezionare **Elementi della configurazione**.
2. Fare clic sulla riga dell'articolo di configurazione pertinente. Nel pannello di destra vengono visualizzati i seguenti dettagli di sola lettura sull'articolo di configurazione:
   - Nome periferica
   - Integrazione RMM
   - Nome sito cliente
   - Descrizione
   - Posizione
3. Per collegare l'articolo di configurazione a un utente specifico, fare clic su **Collega a utente** nella riga corrispondente. Quindi selezionare l'utente desiderato dall'elenco a discesa e fare clic su **Collega**. Ora l'articolo della configurazione è collegato all'utente selezionato; ciò significa che ogni nuovo ticket del Service Desk creato o assegnato all'utente viene automaticamente collegato all'articolo di configurazione.
   Per scollegare un utente da un articolo della configurazione, fare clic su **Collega a utente** nella riga corrispondente, e, nel pannello visualizzato a destra, fare clic su **Annulla collegamento**.

Impostazione dell'entità di fatturazione dei progetti predefinita

Advanced Automation (PSA) consente di creare più entità di fatturazione. Ciò significa che è possibile fatturare da più attività e che ogni entità di fatturazione potrà emettere fatture con impostazioni, sfondo e altre caratteristiche personalizzate. Nella schermata **Gestione progetto**

delle impostazioni del Service Desk è possibile impostare l'entità di fatturazione predefinita per gli articoli di vendita creati per la fatturazione del progetto.

Per impostare l'entità di fatturazione dei progetti predefinita

1. Passare a **Impostazioni > Service Desk**, quindi selezionare **Gestione progetto**.
2. Fare clic su **Modifica**, quindi selezionare l'entità di fatturazione pertinente.
3. Fare clic su **Salva**.

Impostazioni della sezione Fatturazione e offerte

Advanced Automation (PSA) consente la completa personalizzazione delle attività di fatturazione. È possibile, ad esempio, impostare il layout, il formato di esportazione predefinito (se è necessario importare la fattura in un altro sistema) e molto altro ancora. È possibile impostare l'aspetto della fattura, configurare un indirizzo, i margini di testo e aggiungere un'immagine di sfondo.

In questa sezione è inoltre possibile configurare le imposte da utilizzare in Advanced Automation (PSA) e definire l'integrazione con il software di contabilità preferito (consultare "Integrazione con piattaforme di contabilità" (pag. 345)).

Per accedere alle impostazioni della sezione Fatturazione e offerte, aprire il portale di gestione e passare a **Impostazioni > Fatturazione e offerte**.

Impostazioni di fatturazione

In questa sezione viene descritto come configurare le impostazioni predefinite di fatturazione ed emissione delle fatture, inclusa la personalizzazione dell'aspetto delle fatture.

Definizione delle impostazioni di fatturazione predefinite

Questa sezione descrive come configurare le impostazioni di fatturazione e come definire quelle predefinite, inclusi gli arrotondamenti delle registrazioni orario e le imposte predefinite da utilizzare nelle fatture. Queste impostazioni vengono utilizzate in modalità predefinita negli articoli di vendita, nelle fatture e nei contratti.

Non è possibile disattivare un prodotto che impostato come prodotto predefinito nelle impostazioni di fatturazione. Se è impostato come prodotto predefinito, nelle impostazioni del prodotto la casella di controllo **Attivo** è disabilitata. Per ulteriori informazioni, consultare "Aggiunta di un prodotto" (pag. 295).

Per configurare le impostazioni di fatturazione

1. Nel portale di gestione, passare a **Impostazioni > Fatturazione e offerte**. Per impostazione predefinita viene visualizzata la schermata **Impostazioni di fatturazione**.
2. Fare clic sull'icona a matita per modificare le impostazioni predefinite seguenti.
   - **Arrotondamento registrazione orario**: impostare l'orario (in minuti) dell'arrotondamento della registrazione orario. Quando il lavoro sul ticket viene approvato per la fatturazione, le

ore totali fatturabili verranno arrotondate in base a questo valore. Ad esempio, se si imposta il valore dell'arrotondamento su 15 minuti, se vengono svolti 7 minuti di lavoro sul ticket, questi verranno arrotondati a 15 minuti prima della fatturazione. Allo stesso modo, 21 minuti vengono arrotondati a 30, 36 minuti a 45 e così via. Il valore predefinito è **10**.

- **Arrotondamento per ore al di fuori dell'orario lavorativo**. Impostare l'arrotondamento orario dei ticket lavorati al di fuori, ad esempio dell'orario d'ufficio tipico, ad esempio dalle 08:00 alle 17:00. Il valore predefinito è **20**.
- **Scarta ticket per approvazione con un orario uguale o inferiore alla soglia impostata sotto**: abilitare l'interruttore per scartare i ticket che soddisfano la soglia minima specificata. Il valore della soglia corrispondente viene definito nel campo **Valore soglia (in minuti)**.
- **Numero di giorni prima della chiusura automatica del ticket**: imposta il numero di giorni di attesa prima che il sistema chiuda un ticket completato. Per impostazione predefinita, è impostato su **1**.

Nota
I tecnici possono impostare lo stato di un ticket completato solo su **Completato**. Una volta trascorso il numero di giorni stabilito, i ticket si chiudono automaticamente. Ciò garantisce che quando si completa un ticket e un'e-mail viene inviata al cliente, venga ricevuta una risposta di ringraziamento. Tale risposta, tuttavia, riapre il ticket e incide sulle statistiche relative ai ticket riaperti, obbligando a chiudere di nuovo il ticket. La funzionalità di chiusura automatica aiuta a risolvere questa problematica. Per disabilitare la funzionalità, impostare il valore su **0**.

- **Software di gestione dei registri contabili predefinito**: selezionare il software desiderato dall'elenco delle piattaforme di contabilità integrate disponibili (consultare "Integrazione con piattaforme di contabilità" (pag. 345)).
- **Registro contabile prodotti predefinito per esportazioni fatture**: selezionare il registro contabile prodotti predefinito da utilizzare per esportare le fatture (il valore predefinito è **400**). I registri contabili prodotti visualizzati nell'elenco sono quelli attualmente disponibili (consultare "Gestione dei registri contabili" (pag. 312)).

Nota
Quando vengono esportate nel software di contabilità, le fatture vengono in genere esportate come informazioni generiche (azienda, clienti, totali) con dati relative alle righe della fattura (prodotto, descrizione, registro contabile, quantità, prezzo, totale, imposta e così via). Questo campo definisce il numero del registro contabile che viene utilizzato come predefinito per un prodotto se nelle impostazioni del prodotto in questione non è stato assegnato un registro specifico.

- **Prodotto predefinito per fatturazione orario ticket**: selezionare il prodotto predefinito da utilizzare per la fatturazione degli orari dei ticket. Per impostazione predefinita, questa opzione è impostata su **Supporto per ora**.

- **Prodotto predefinito per ore al di fuori dell'orario lavorativo**: selezionare il prodotto predefinito da utilizzare per tutte le fatturazioni impostate per l'assistenza al di fuori dell'orario di lavoro. Per impostazione predefinita, questa opzione è impostata su **Oltre l'orario lavorativo**.
- **Prodotto di fatturazione predefinito per blocco ore**: se ai clienti vengono offerti dei blocchi ore, selezionare il prodotto predefinito da utilizzare per i blocchi ore. L'impostazione predefinita è **Blocco ore**.
- **Imposta vendite predefinita**: selezionare l'imposta vendite predefinita da utilizzare dall'elenco delle imposte disponibili (consultare "Configurazione delle imposte" (pag. 343)). L'impostazione predefinita è **Imposta predefinita**.
- **Invia fatture tramite**: selezionare il metodo predefinito per l'invio delle fatture. Per impostazione predefinita, questa opzione è impostata su **Posta**. Questo campo viene applicato automaticamente:
  - Quando si crea un cliente.
  - Nella scheda **Dati di fatturazione**, quando si definiscono le informazioni di fatturazione per i clienti per i quali non sono state definite (ad esempio, se il cliente esisteva già prima dell'attivazione di Advanced Automation (PSA)).
  - Nella scheda **Dati di fatturazione**, durante la creazione di un preventivo, di un contratto, di un articolo di vendita o di un progetto per i clienti per i quali non sono state definite informazioni di fatturazione (ad esempio, se il cliente esisteva già prima dell'attivazione di Advanced Automation (PSA)).
  - Quando si crea manualmente un nuovo contratto o un articolo di vendita (il valore selezionato del campo **Invia fatture tramite** deriva dalle informazioni di fatturazione definite per il cliente; se queste informazioni non sono state definite, viene applicato il valore predefinito **Posta**).

  Anche il campo **Invia fatture tramite** è impostato nelle impostazioni predefinite del preventivo e viene applicato quando si crea un contratto o un articolo di vendita accettando un preventivo. Questo è l'unico caso in cui il campo **Invia fatture tramite** viene applicato diversamente dalle impostazioni predefinite di fatturazione o dalle impostazioni di fatturazione del cliente. Per ulteriori informazioni, consultare "Definizione delle impostazioni predefinite del preventivo" (pag. 341).
- **Entità di fatturazione predefinita**: l'entità di fatturazione predefinita utilizzata per le fatture. Per impostazione predefinita, è selezionata l'opzione **Entità di fatturazione predefinita**.

3. Fare clic su ✓ per applicare le modifiche.

Aggiunta di una nuova entità di fatturazione

Le entità di fatturazione consentono di inviare fatture dalle varie entità legali che fanno parte dell'azienda. Al momento della creazione dell'account viene creata un'entità di fatturazione predefinita. Se questa è la sola entità di fatturazione necessaria, è possibile aggiornarne le informazioni.

Nota
Solo gli utenti con i ruoli Amministratore o Direttore possono creare e aggiornare le entità di fatturazione.

Per aggiungere una nuova entità di fatturazione

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Entità di fatturazione**.
   Viene visualizzata l'entità di fatturazione corrente.
2. Fare clic su **+ Nuove entità di fatturazione**.
3. Definire quanto segue:
   - **Nome società**: inserire il nome dell'azienda.
   - **Numero conto bancario**: inserire il numero di conto bancario corrispondente all'entità.
   - **Numero iniziale fatture**: inserire il numero iniziale delle fatture da applicare quando si inizia a inviare le fatture al cliente.
   - **Numero sequenziale fatture**: questa opzione consente di mantenere lo stesso intervallo di numerazione delle fatture nel caso in cui si passi ad Advanced Automation (PSA) nel corso dell'anno fiscale.
4. (Facoltativo) Abilitare l'interruttore **Ripristina numerazione fatture**. In questo modo la numerazione delle fatture viene ripristinata al numero impostato nel campo **Numero iniziale fatture**.
5. Abilitare l'interruttore **Attiva** per abilitare la nuova entità di fatturazione.
6. Fare clic su **Crea**. L'entità di fatturazione viene aggiunta alla schermata **Entità di fatturazione** e può essere selezionata quando si generano le fatture (vedere "Generazione di una nuova fattura" (pag. 290)), gli articoli di vendita (vedere "Creazione di un nuovo articolo di vendita" (pag. 279)) e i contratti (vedere "Creazione di un nuovo contratto" (pag. 282)).
   È possibile aggiornare un'entità di fatturazione come necessario. Fare clic sull'entità da modificare nella schermata **Entità di fatturazione** e apportare le modifiche necessarie. Tenere presente che non è possibile eliminare un'entità di fatturazione.

Personalizzazione dell'aspetto delle fatture

Il layout delle fatture e dei preventivi che vengono inviati ai clienti può essere completamente personalizzato. È possibile scaricare l'immagine di sfondo, impostare il testo del piè di pagina della fattura e impostare i margini per i testi aggiunti da Advanced Automation (PSA).

L'immagine di sfondo scelta dall'utente può includere informazioni quali il logo, l'indirizzo, il sito web e l'indirizzo e-mail dell'azienda, che verranno quindi visualizzati nelle fatture.

Nota
Per avviare la personalizzazione della fattura da zero, è possibile scaricare un'immagine di modello vuota da qui. Se è già disponibile un layout della fattura in PDF, è possibile convertirlo in JPG in alta risoluzione utilizzando strumenti online di terzi.

Per personalizzare la fattura

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Impostazioni fattura**.
2. Fare clic sull'icona a matita per modificare le impostazioni seguenti.
   - **Immagine di sfondo fattura**: trascinare un file di immagine nella casella visualizzata oppure fare clic su **Sfoglia** per caricare l'immagine desiderata. Il file di immagine deve essere un formato A4 JPEG con una dimensione massima di 1 MB.
   - **Testo piè di pagina fattura per addebito diretto**: modificare il testo del piè di pagina per l'addebito diretto come necessario. Ad esempio, utilizzando le variabili disponibili in Advanced Automation (PSA) (vedere più sotto), il testo del piè di pagina per le fatture impostate con un addebito diretto potrebbe essere simile al seguente:

     "Addebito diretto su conto corrente bancario: [BANK_ACCOUNT_NUMBER], nome cliente > [CUSTOMER_NAME] e Partita IVA = [VAT_NUMBER]"

     In questo modo, i clienti potranno saldare le fatture tramite bonifico o utilizzando una delle integrazioni con i sistemi di pagamento disponibili (PayPal, Stripe). Potranno inoltre inviare le fatture ai rispettivi istituti bancari per l'elaborazione dell'addebito diretto.

     Le variabili disponibili per le fatture con addebito diretto sono:
     - [BANK_ACCOUNT_NUMBER]
     - [CUSTOMER_NAME]
     - [VAT_NUMBER]
     - [INVOICE_NUMBER]
     - [INVOICE_DUE_DAYS]
   - **Testo piè di pagina fattura per pagamento manuale**: modificare il testo del piè di pagina della fattura per il pagamento manuale. Ad esempio, il testo del piè di pagina di una fattura per il pagamento manuale potrebbe essere simile al seguente: (presupponendo che la scadenza della fattura sia a 15 giorni e che il numero di fattura sia 2022020107): "15-2022020107"
   - **Data scadenza fattura**: inserire il numero di giorni pertinente.
   - **Nascondi prefisso numero fattura**: abilitare l'interruttore se si desidera nascondere il prefisso del numero della fattura.
   - **Periodo di contratto fatturabile in anticipo (giorni)**: inserire il numero di giorni pertinente.
   - **Posizione indirizzo fattura**: selezionare una delle opzioni **Sinistra** o **Destra**.

> **Nota**
> Prima di modificare la posizione dell'indirizzo sulla fattura, verificare che non si sovrapponga al logo dell'azienda.

- **Margine superiore**: inserire il valore dello spazio tra l'indirizzo dell'azienda e la parte superiore del documento della fattura.

> **Nota**
> Tutti i valori dei margini sono espressi in centimetri.

- **Margine superiore a partire da pagina 2**: inserire il valore dello spazio tra l'indirizzo dell'azienda e la parte superiore del documento della fattura, da pagina 2 in avanti.
- **Lato margine**: inserire il valore dello spazio dalla sinistra del documento della fattura.
- **Margine inferiore indirizzo**: inserire il valore dello spazio tra l'indirizzo dell'azienda e i dettagli su data e numero di fattura del documento della fattura.
- **Margine inferiore pagina**: inserire il valore dello spazio tra il numero di pagina e la parte inferiore del documento della fattura.
- **Posizione numero pagina**: selezionare una delle opzioni **In alto** o **In basso**.
- **Visibilità numero pagina**: selezionare una delle opzioni **Visualizza su tutte le pagine**, **Nascondi sulla prima pagina** o **Nascondi completamente**.

3. Fare clic su **Scarica anteprima** per visualizzare un'anteprima della fattura in formato PDF.
4. Al termine, fare clic su ✓.

   Quando viene generata una fattura, il piè di pagina viene applicato automaticamente, a seconda dell'opzione del metodo di pagamento specificata.
   - Se è selezionato l'addebito diretto, viene utilizzata l'opzione **Testo piè di pagina fattura per addebito diretto**.
   - Se non è selezionato l'addebito diretto, viene utilizzata l'opzione **Testo piè di pagina fattura per pagamento manuale**.

Impostazioni delle offerte

Questa sezione descrive come configurare le impostazioni predefinite per le offerte, inclusa la personalizzazione dell'aspetto del preventivo in formato PDF inviato ai clienti.

Definizione delle impostazioni predefinite del preventivo

Quando un preventivo viene approvato, Advanced Automation (PSA) crea automaticamente gli elementi indicati di seguito:

- Un ticket di ordine di acquisto per gli articoli che devono prima essere acquistati, ad esempio tramite un distributore. Tenere presente che se un articolo è già in magazzino, non verrà creato alcun ticket ordine di acquisto.
- Un ticket preventivo per inviare e fatturare gli articoli di preventivo al cliente.

Le impostazioni predefinite del preventivo definiscono a quale gruppo di supporto viene automaticamente assegnato ognuno dei tipi di ticket indicati sopra al momento della loro creazione. È inoltre possibile definire altre impostazioni per il preventivo, come la categoria predefinita e il metodo di pagamento predefinito per gli articoli di vendita.

Per definire le impostazioni predefinite del preventivo

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Impostazioni preventivo**.
2. Fare clic sull'icona a matita per modificare le impostazioni predefinite seguenti.
   - **Gruppo per ticket ordine di acquisto**: selezionare il gruppo di supporto pertinente dall'elenco a discesa.
   - **Gruppo per ticket preventivo**: selezionare il gruppo di supporto pertinente dall'elenco a discesa.
   - **SLA per ticket preventivo**: selezionare lo SLA pertinente dall'elenco a discesa.
   - **Priorità per ticket preventivo**: selezionare la priorità pertinente dall'elenco a discesa.
   - **Categoria per ticket preventivo**: selezionare la categoria pertinente dall'elenco a discesa.
   - **Entità di fatturazione**: selezionare l'entità di fatturazione pertinente dall'elenco a discesa.
   - **Invia fatture tramite**: selezionare **Posta** o **E-mail** . Per impostazione predefinita, questa opzione è impostata su **Posta** .

     Il campo **Invia fatture tramite** viene applicato quando si crea un contratto o un articolo di vendita accettando un preventivo. Questo è l'unico caso in cui il campo **Invia fatture tramite** viene applicato diversamente dalle impostazioni di fatturazione predefinite o dalle impostazioni di fatturazione del cliente.
   - **Metodo di pagamento articoli di vendita**: selezionare **Pagamento manuale** o **Addebito diretto**.
   - **Condizioni generali**: aggiungere le condizioni generali desiderate a tutti i preventivi. Qui è possibile aggiungere, ad esempio, qualsiasi termine o condizione legale da includere.
3. Fare clic su ✓ per applicare le modifiche.

Personalizzazione dell'aspetto dei PDF dei preventivi

Questa sezione descrive come personalizzare l'aspetto dei preventivi in formato PDF che vengono inviati ai clienti. È possibile scaricare l'immagine di sfondo, impostare il testo del piè di pagina del preventivo e impostare i margini per i testi aggiunti automaticamente da Advanced Automation (PSA). Facoltativamente, l'immagine di sfondo scelta può includere gli elementi indicati di seguito.

- Logo aziendale
- Dettagli dell'indirizzo
- Numero conto bancario
- Sito web e indirizzo e-mail
- Partita IVA

Nota
Per avviare la personalizzazione del preventivo da zero, è possibile scaricare un'immagine di modello vuota da qui. Se è già disponibile un layout del preventivo in PDF, è possibile convertirlo in JPG in alta risoluzione utilizzando strumenti online di terzi.

Per personalizzare i PDF dei preventivi

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Impostazioni PDF preventivo**.
2. Fare clic sull'icona a matita per modificare le impostazioni predefinite seguenti.
   - **Immagine di sfondo PDF preventivo**: trascinare un file di immagine nella casella visualizzata oppure fare clic su **Trascina o seleziona file da caricare** per caricare l'immagine desiderata. Il file di immagine deve essere un formato A4 JPEG con una dimensione massima di 1 MB.
   - **Margine superiore**: inserire il valore dello spazio tra l'indirizzo dell'azienda e la parte superiore del documento del preventivo.

     Nota
     Tutti i valori dei margini sono espressi in centimetri.

   - **Margine superiore a partire da pagina 2**: inserire il valore dello spazio tra l'indirizzo dell'azienda e la parte superiore del documento del preventivo, da pagina 2 in avanti.
   - **Lato margine**: inserire il valore dello spazio dalla sinistra del documento del preventivo.
   - **Margine inferiore indirizzo**: inserire il valore dello spazio tra l'indirizzo dell'azienda e i dettagli su data e numero di preventivo del documento del preventivo.
   - **Margine inferiore pagina**: inserire il valore dello spazio tra il numero di pagina e la parte inferiore del documento del preventivo.
   - **Posizione numero pagina**: selezionare una delle opzioni **In alto** o **In basso**.
   - **Visibilità numero pagina**: selezionare una delle opzioni **Visualizza su tutte le pagine**, **Nascondi sulla prima pagina** o **Nascondi completamente**.
3. Fare clic su **Scarica anteprima** per visualizzare un'anteprima del preventivo in formato PDF.
4. Al termine, fare clic su ✓.

Configurazione delle imposte

Questa sezione descrive come configurare le impostazioni relative alle imposte predefinite da utilizzare nelle fatture da inviare ai clienti. In una fattura, le imposte vengono applicate in base al Paese di appartenenza e ai prodotti venduti.

Aggiunta di un'imposta

Per aggiungere un'imposta

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Imposte**.
2. Fare clic su **+ Aggiungi nuova**.
3. Inserire nei rispettivi campi il codice, il nome e il valore dell'imposta. Per impostazione predefinita, l'imposta è impostata come attiva.
4. Fare clic su ✓ per salvare la nuova imposta.

   La nuova tassa verrà aggiunta alla schermata **Imposte**.

Modifica di un'imposta

È possibile modificare un'imposta in qualsiasi momento, e attivarla/disattivarla a seconda delle esigenze. È anche possibile eliminare un'imposta.

Per modificare un'imposta

1. Nel portale di gestione, passare a **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Imposte**.
2. Fare clic sull'icona a matita accanto all'imposta da modificare e apportare le modifiche necessarie.

   Fare clic sull'interruttore per attivare o disattivare l'imposta.

   Nota
   Per eliminare un'imposta, fare clic sull'icona a cestino. Non è possibile eliminare un'imposta se è già stata assegnata nel sistema, ad esempio come imposta di vendita.
3. Fare clic su ✓ per applicare le modifiche.

Integrazione di Advanced Automation (PSA) con piattaforme di terze parti

È possibile integrare Advanced Automation (PSA) con le principali piattaforme di contabilità, strumenti RMM, VAR e piattaforme di pagamento.

Attualmente sono supportate le seguenti integrazioni:

- **Integrazioni di sistemi contabili**: FreshBooks, QuickBooks, Sage, Xero e SnelStart
- **Integrazioni RMM**: NinjaOne, Datto RMM, Kaseya VSA, N-able N-central e N-able RMM
- **Integrazioni VAR**: Microsoft CSP
- **Integrazioni con sistemi di pagamento**: PayPal e Stripe

Per accedere alle integrazioni dell'utente, nel portale di gestione passare a **Integrazioni**.

Nota
Questa funzionalità è disponibile solo agli utenti ai quali è assegnato il ruolo di Amministratore.

Integrazione con piattaforme di contabilità

È possibile integrare Advanced Automation (PSA) con le piattaforme di contabilità più diffuse. Le integrazioni automatizzano le funzionalità seguenti:

- Importazione dati iniziale

  Questa funzionalità consente di evitare i trasferimenti iniziali di dati di routine dalla piattaforma di contabilità alla piattaforma Acronis Cyber Protect Cloud e di importare i principali dati aziendali per la fatturazione dei clienti con Advanced Automation (PSA). I dati principali includono clienti, prodotti, imposte e registri.

- Esportazione dei dati di fatturazione

  Ogni nuova fattura generata in Advanced Automation (PSA) viene automaticamente esportata nella piattaforma di contabilità senza richiedere alcuna azione manuale.

Se le integrazioni attualmente supportate non sono compatibili con la piattaforma in uso, Advanced Automation (PSA) consente di inviare le fatture al software di contabilità tramite file CSV o XML.

Per accedere alle integrazioni delle piattaforme di contabilità, passare a **Integrazioni**. Nel menu visualizzato a sinistra, selezionare **Automazione** > **Contabilità e finanza**.

Integrazione con FreshBooks

Questo paragrafo descrive come eseguire l'integrazione di FreshBooks in Advanced Automation (PSA).

Per altre informazioni sulle ulteriori piattaforme di contabilità integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di contabilità" (pag. 345).

Nota
Quando si accede al portale di gestione utilizzando un URL dell'interfaccia web personalizzato, l'integrazione con FreshBooks deve essere abilitata solo quando si effettua l'accesso tramite l'URL predefinito del portale di gestione(https://cloud.acronis.com). Per ulteriori informazioni sul branding e sugli URL di interfaccia web personalizzati, consultare "Configurazione degli URL delle interfacce web personalizzate" (pag. 102).

Per integrare FreshBooks in Advanced Automation (PSA)

1. Passare a **Integrazioni** e selezionare **Automazione** > **Contabilità e finanza**.
2. Nel riquadro relativo a FreshBooks, fare clic su **Configura**, quindi su **Attiva**. Verrà visualizzato un messaggio che richiede di attivare il processo di autenticazione, che reindirizza alla pagina di login di FreshBooks.
3. Inserire le credenziali dell'account di FreshBooks per abilitare l'integrazione.
4. Selezionare i dati da importare da FreshBooks (Clienti, Registri contabili, Prodotti e Imposte) e fare clic su **Importa**.

Una volta completata l'integrazione iniziale, quando si utilizza di nuovo il pulsante **Importa** verranno importati solo i clienti, i registri contabili, i prodotti e le imposte inseriti di recente.

5. Fare clic su **Salva** per salvare le impostazioni di integrazione.

Nota
Una volta abilitata l'integrazione, Advanced Automation (PSA) controlla automaticamente la presenza di nuove fatture a intervalli di pochi minuti, e le sincronizza con FreshBooks. È possibile visualizzare lo stato della sincronizzazione nella colonna **Stato sincronizzazione fattura** nella schermata **Fatture** (passare a **Vendite e fatturazione > Fatture**).

Per modificare le impostazioni di integrazione di FreshBooks

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a FreshBooks, fare clic su **Gestisci**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con FreshBooks

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a FreshBooks, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Integrazione con QuickBooks

Questo paragrafo descrive come eseguire l'integrazione di QuickBooks Online in Advanced Automation (PSA).

Per altre informazioni sulle ulteriori piattaforme di contabilità integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di contabilità" (pag. 345).

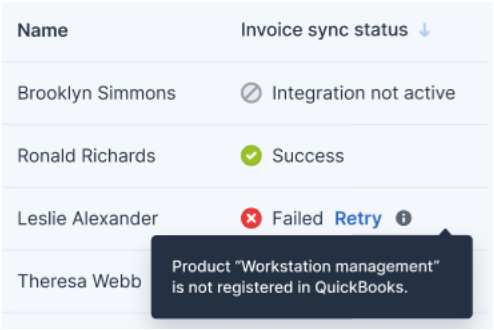
Nota
Quando si accede al portale di gestione utilizzando un URL dell'interfaccia web personalizzato, l'integrazione con QuickBooks deve essere abilitata solo quando si effettua l'accesso tramite l'URL predefinito del portale di gestione(https://cloud.acronis.com). Per ulteriori informazioni sul branding e sugli URL di interfaccia web personalizzati, consultare "Configurazione degli URL delle interfacce web personalizzate" (pag. 102).

Per integrare QuickBooks in Advanced Automation (PSA)

1. Passare a **Integrazioni** e selezionare **Automazione** > **Contabilità e finanza**.
2. Nel riquadro relativo a QuickBooks, fare clic su **Configura**, quindi su **Attiva**. Verrà visualizzato un messaggio che richiede di attivare il processo di autenticazione, che reindirizza alla pagina di login di QuickBooks.
3. Inserire le credenziali dell'account di QuickBooks per abilitare l'integrazione.

4. Selezionare i dati da importare da QuickBooks (Clienti, Registri contabili, Prodotti e Imposte) e fare clic su **Importa**.
   Una volta completata l'integrazione iniziale, quando si utilizza di nuovo il pulsante **Importa** verranno importati solo i clienti, i registri contabili, i prodotti e le imposte inseriti di recente.
5. Fare clic su **Salva** per salvare le impostazioni di integrazione.

Nota
Una volta attivata l'integrazione, Advanced Automation (PSA) controlla automaticamente la presenza di nuove fatture a intervalli di pochi minuti, e le sincronizza con QuickBooks. È possibile visualizzare lo stato della sincronizzazione nella colonna **Stato sincronizzazione fattura** nella schermata **Fatture** (passare a **Vendite e fatturazione > Fatture**).



Per modificare le impostazioni di integrazione di QuickBooks

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a QuickBooks, fare clic su **Gestisci**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con QuickBooks

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a QuickBooks, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Integrazione con Sage Business Cloud

Questo paragrafo descrive come eseguire l'integrazione di Sage Business Cloud in Advanced Automation (PSA).

Al momento, Advanced Automation (PSA) supporta solo Sage Accounting.

Per altre informazioni sulle ulteriori piattaforme di contabilità integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di contabilità" (pag. 345).

Nota
Quando si accede al portale di gestione utilizzando un URL dell'interfaccia web personalizzato, l'integrazione con Sage Business Cloud deve essere abilitata solo quando si effettua l'accesso tramite l'URL predefinito del portale di gestione (https://cloud.acronis.com). Per ulteriori informazioni sul branding e sugli URL di interfaccia web personalizzati, consultare "Configurazione degli URL delle interfacce web personalizzate" (pag. 102).

Per integrare Sage Business Cloud in Advanced Automation (PSA)

1. Passare a **Integrazioni**, poi fare clic su **Automazione** > **Contabilità e finanza**.
2. Nel riquadro relativo a Sage Business Cloud, fare clic su **Configura**, quindi su **Attiva**.
   Verrà visualizzato un messaggio che richiede di attivare il processo di autenticazione, che reindirizza alla pagina di login di Sage Business Cloud.
3. Inserire le credenziali dell'account di Sage Business Cloud per abilitare l'integrazione.

   Nota
   Una volta abilitata l'integrazione, Advanced Automation (PSA) controlla automaticamente la presenza di nuove fatture a intervalli di pochi minuti, e le sincronizza con Sage Business Cloud. È possibile visualizzare lo stato della sincronizzazione nella colonna **Stato sincronizzazione fattura** nella schermata **Fatture** (passare a **Vendite e fatturazione > Fatture**).

   Inoltre, in Sage Business Cloud sono consentite solo due cifre dopo il separatore decimale per i prezzi unitari nelle voci delle righe della fattura. In altre piattaforme di contabilità sono in genere supportate fino a quattro cifre dopo il separatore decimale. In Advanced Automation (PSA), i prezzi vengono automaticamente arrotondati alle due cifre dopo il separatore decimale e quindi sincronizzati con Sage Business Cloud. Non è richiesta alcuna configurazione da parte dell'utente.
4. Selezionare i dati da importare da Sage Business Cloud (Clienti, Registri contabili, Prodotti e Imposte) e fare clic su **Importa**.
   Una volta completata l'integrazione iniziale, quando si utilizza di nuovo il pulsante **Importa** verranno importati solo i clienti, i registri contabili, i prodotti e le imposte inseriti di recente.
5. Fare clic su **Salva** per salvare le impostazioni di integrazione.

Per modificare le impostazioni di integrazione di Sage Business Cloud

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a Sage Business Cloud, fare clic su **Gestisci**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con Sage Business Cloud

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a Sage Business Cloud, fare clic su **Disattiva**.

3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Integrazione con Xero

Questo paragrafo descrive come eseguire l'integrazione di Xero in Advanced Automation (PSA).

Per altre informazioni sulle ulteriori piattaforme di contabilità integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di contabilità" (pag. 345).

Nota
Quando si accede al portale di gestione utilizzando un URL dell'interfaccia web personalizzato, l'integrazione con Xero deve essere abilitata solo quando si effettua l'accesso tramite l'URL predefinito del portale di gestione(https://cloud.acronis.com). Per ulteriori informazioni sul branding e sugli URL di interfaccia web personalizzati, consultare "Configurazione degli URL delle interfacce web personalizzate" (pag. 102).

Per eseguire l'integrazione di Xero in Advanced Automation (PSA)

1. Passare a **Integrazioni** e selezionare **Automazione** > **Contabilità e finanza**.
2. Nel riquadro relativo a Xero, fare clic su **Configura**, quindi su **Attiva**. Verrà visualizzato un messaggio che richiede di attivare il processo di autenticazione, che reindirizza alla pagina di login di Xero.
3. Inserire le credenziali dell'account di Xero per abilitare l'integrazione.
4. Selezionare i dati da importare da Xero (Clienti, Registri contabili, Prodotti e Imposte) e fare clic su **Importa**.
   Una volta completata l'integrazione iniziale, quando si utilizza di nuovo il pulsante **Importa** verranno importati solo i clienti, i registri contabili, i prodotti e le imposte inseriti di recente.
5. Fare clic su **Salva** per salvare le impostazioni di integrazione.

   Nota
   Una volta abilitata l'integrazione, Advanced Automation (PSA) controlla automaticamente la presenza di nuove fatture a intervalli di pochi minuti, e le sincronizza con Xero. È possibile visualizzare lo stato della sincronizzazione nella colonna **Stato sincronizzazione fattura** nella schermata **Fatture** (passare a **Vendite e fatturazione > Fatture**).

Per modificare le impostazioni di integrazione di Xero

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a Xero, fare clic su **Gestisci**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con Xero

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a Xero, fare clic su **Disattiva**.

3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Integrazione con SnelStart

Questo paragrafo descrive come eseguire l'integrazione di SnelStart in Advanced Automation (PSA).

Per altre informazioni sulle ulteriori piattaforme di contabilità integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di contabilità" (pag. 345).

Nota
Quando si accede al portale di gestione utilizzando un URL dell'interfaccia web personalizzato, l'integrazione con SnelStart deve essere abilitata solo quando si effettua l'accesso tramite l'URL predefinito del portale di gestione(https://cloud.acronis.com). Per ulteriori informazioni sul branding e sugli URL di interfaccia web personalizzati, consultare "Configurazione degli URL delle interfacce web personalizzate" (pag. 102).

Per integrare SnelStart in Advanced Automation (PSA)

1. Passare a **Integrazioni** e selezionare **Automazione** > **Contabilità e finanza**.
2. Nel riquadro relativo a SnelStart, fare clic su **Configura**, quindi su **Attiva**.
   Verrà visualizzato un messaggio che richiede di attivare il processo di autenticazione, che reindirizza alla pagina di login di SnelStart.
3. Inserire le credenziali dell'account di SnelStart per abilitare l'integrazione.
4. Selezionare i dati da importare da SnelStart (Clienti, Registri contabili, Prodotti e Imposte) e fare clic su **Importa**.
   Una volta completata l'integrazione iniziale, quando si utilizza di nuovo il pulsante **Importa** verranno importati solo i clienti, i registri contabili, i prodotti e le imposte inseriti di recente.
5. Fare clic su **Salva** per salvare le impostazioni di integrazione.

   Nota
   Una volta abilitata l'integrazione, Advanced Automation (PSA) controlla automaticamente la presenza di nuove fatture a intervalli di pochi minuti, e le sincronizza con SnelStart. È possibile visualizzare lo stato della sincronizzazione nella colonna **Stato sincronizzazione fattura** nella schermata **Fatture** (passare a **Vendite e fatturazione > Fatture**).

Per modificare le impostazioni di integrazione di SnelStart

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a SnelStart, fare clic su **Gestisci**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con SnelStart

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a SnelStart, fare clic su **Disattiva**.

3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Nota
Anche dopo aver disattivato l'integrazione, Advanced Automation (PSA) conserva tutti i clienti, i registri contabili, i prodotti e le imposte, che potranno continuare a essere utilizzati. Le nuove fatture create in Advanced Automation (PSA) non verranno più sincronizzate con la piattaforma di contabilità.

Risoluzione dei problemi relativi all'integrazione della piattaforma di contabilità

Quando Advanced Automation (PSA) invia una fattura a una piattaforma di contabilità, questa in genere prevede di ricevere i seguenti codici di mapping obbligatori, per garantire la corrispondenza dei dati tra i due sistemi (Cyber Protect Cloud e la piattaforma di contabilità):

- L'"ID esterno" di un cliente, che deve corrispondere a un tenant cliente e conferma il collegamento tra una nuova fattura e il cliente corretto.
- L'"ID esterno" di un prodotto, che deve corrispondere a un prodotto in una riga della fattura e confermare il collegamento tra la riga della fattura e il prodotto corretto.

Quando si importano clienti e prodotti dalle piattaforme di contabilità, questi codici di mapping vengono impostati automaticamente in Cyber Protect Cloud. Possono essere visualizzati nel portale di gestione e aggiornati manualmente, se necessario.

Le mancate corrispondenze tra i codici di mapping dei due sistemi sono generalmente il risultato di modifiche manuali e possono comportare il mancato recapito di una fattura alla piattaforma di contabilità.

Risoluzione dei problemi relativi alle fatture

Lo stato di un'esportazione di fatture non riuscita può essere visualizzato passando a **Vendite e fatturazione > Fatture**, quindi visualizzando il valore **Stato sincronizzazione fattura** nella riga della fattura pertinente. La piattaforma di contabilità visualizza un messaggio che indica il motivo esatto della mancata esportazione.

Se il messaggio di errore indica un errore nel riconoscimento di un cliente o di un prodotto, il problema è in genere dovuto a codici di mapping vuoti o non corretti relativi a un cliente o un prodotto in Cyber Protect Cloud.

Per ulteriori informazioni su Advanced Automation (PSA) e sulla sincronizzazione con piattaforme di contabilità di terze parti, consultare questo articolo della Knowledge Base.

Integrazione con piattaforme RMM

È possibile integrare Advanced Automation (PSA) con le piattaforme RMM (Remote Monitoring and Management) più diffuse. L'integrazione con queste piattaforme consente di automatizzare la

creazione e la gestione dei ticket e di allineare la fatturazione ai clienti con le risorse gestite del cliente.

Per accedere alle integrazioni delle piattaforme RMM, passare a **Integrazioni**. Nel menu visualizzato a sinistra, selezionare **Gestione** > **Monitoraggio e gestione remota**.

Durante la configurazione dell'integrazione, accertarsi che il software RMM resti aperto, perché per completare l'attività sono necessari gli URL e le chiavi della soluzione.

Integrazione con NinjaOne

L'integrazione di Advanced Automation (PSA) con NinjaOne consente di:

- Importare automaticamente siti di clienti e dispositivi da NinjaOne.
- Abbinare i clienti ai siti da NinjaOne.
- Creare ticket dagli avvisi di NinjaOne.
- Accedere alla pagina dei dispositivi NinjaOne da un ticket.
- Fatturare ai clienti il numero di dispositivi effettivo utilizzando NinjaOne.

NinjaOne supporta l'autenticazione OAuth 2.0, applicabile a tutte le nuove integrazioni. Se l'integrazione è stata configurata con un ID della chiave di accesso e una chiave di accesso privata, dovrà essere aggiornata manualmente.

Nota
Per integrare in modo corretto NinjaOne con Advanced Automation (PSA), è necessario abilitare il servizio Advanced Automation (PSA). Inoltre, deve essere disponibile un account NinjaOne configurato in tutte le sue parti.

Configurazione dell'integrazione NinjaOne

Due passaggi principali consentono di configurare l'integrazione di NinjaOne con Advanced Automation (PSA), come descritto nelle procedure seguenti.

1. Definizione delle impostazioni di integrazione per la connessione con l'istanza di NinjaOne.
2. Mapping dei clienti di NinjaOne ad Advanced Automation (PSA).

Per definire le impostazioni di integrazione

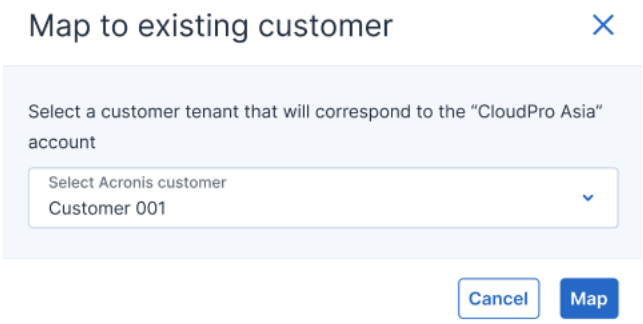
1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **NinjaOne**, fare clic su **Configura**.
3. Inserire le credenziali NinjaOne necessarie per accedere all'istanza della soluzione. Per ulteriori informazioni, vedere qui.

Nota
NinjaOne supporta l'autenticazione OAuth 2.0, applicabile a tutte le nuove integrazioni. Se l'integrazione è stata configurata con un ID della chiave di accesso e una chiave di accesso privata, dovrà essere aggiornata manualmente.

4. Il passaggio successivo per configurare l'integrazione è il mapping dei clienti di NinjaOne ai clienti esistenti o nuovi di Advanced Automation (PSA). Attenersi alla procedura seguente.

Per il mapping dei clienti NinjaOne

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **NinjaOne**, fare clic su **Configura**.
3. Nella scheda **Mapping del cliente**, fare clic su **Creazione di clienti Acronis dai siti di NinjaOne**. Il processo di mapping viene avviato per tutti i siti di NinjaOne in elenco.
   Tutti i clienti (siti dei clienti) derivanti da NinjaOne vengono registrati come nuovi clienti in Portale di gestione, insieme a tutti i servizi disponibili garantiti.
   È inoltre possibile scegliere singoli siti di NinjaOne e abbinarli a clienti di Portale di gestione esistenti; selezionare i siti pertinenti e quindi fare clic su **Mapping a tenant di cliente esistente**. Il sistema chiede di selezionare un cliente esistente. Una volta effettuata la selezione, fare clic su **Mapping** per completare il processo.



4. Al termine del processo, nella colonna **Mapping** viene visualizzato lo stato **Mappato**, e la colonna **Cliente Acronis** visualizza il nome del cliente corrispondente.

Nota
Per rimuovere un mapping, selezionare la riga attualmente mappata e fare clic su **Rimuovi mapping**. Nella finestra popup di conferma visualizzata, fare clic su **Rimuovi**.

Revisione e modifica delle impostazioni dell'integrazione NinjaOne

È possibile rivedere e modificare le impostazioni dell'integrazione NinjaOne come necessario. È anche possibile disattivare l'integrazione NinjaOne.

Per rivedere e modificare le impostazioni dell'integrazione NinjaOne

1. Nel portale di gestione, passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
   Nel riquadro relativo a **NinjaOne** è possibile visualizzare lo stato corrente dell'integrazione.
2. Fare clic su **Gestisci** per visualizzare e modificare le impostazioni dell'integrazione.
   Ad esempio, è possibile visualizzare e modificare le credenziali e le impostazioni degli avvisi nella scheda **Impostazioni di integrazione**, e i clienti NinjaOne con mapping ad Advanced Automation (PSA) nella scheda **Mapping del cliente**.
3. Fare clic sull'icona a matita per modificare la sezione pertinente. Per ulteriori informazioni sui campi modificabili, consultare "Configurazione dell'integrazione NinjaOne" (pag. 352).
4. Al termine, fare clic su ✓.

Per disattivare l'integrazione NinjaOne

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a **NinjaOne**, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Creazione di ticket da avvisi aperti di NinjaOne

Quando è configurata l'integrazione con NinjaOne (consultare "Configurazione dell'integrazione NinjaOne" (pag. 352)), Advanced Automation (PSA) crea automaticamente nuovi ticket a partire dagli avvisi aperti di NinjaOne. I ticket sono costantemente sincronizzati con NinjaOne, garantendo che gli avvisi aperti già collegati ai ticket in Advanced Automation (PSA) vengano ignorati.

Tenere presente quanto segue:

- I ticket sono creati solo per i clienti associati ai siti dei clienti di NinjaOne.
- I parametri dei ticket sono definiti in base alle impostazioni predefinite per il cliente corrispondente, come descritto in "Impostazione dei valori predefiniti" (pag. 319).
- Il riepilogo e la descrizione del ticket derivano dal riepilogo e dalla descrizione dell'avviso.
- Il ticket include i collegamenti al cliente di Portale di gestione, all'utente del cliente (tramite il rispettivo indirizzo e-mail, se fornito da NinjaOne) e ai dispositivi collegati all'utente (se pertinente; gli utenti possono visualizzare i dispositivi nella console di Cyber Protect).
- Se un ticket è collegato al dispositivo di un utente, nella sezione Informazioni dispositivo di NinjaOne è presente il relativo link.

Per ulteriori informazioni sulla creazione dei ticket, consultare "Creazione di un nuovo ticket" (pag. 223).

Aggiunta di dispositivi NinjaOne esterni ai contratti

Se è stata configurata l'integrazione con NinjaOne (consultare "Configurazione dell'integrazione NinjaOne" (pag. 352)), è possibile aggiungere dispositivi esterni ai contratti per i clienti in Advanced Automation (PSA).

- È possibile collegare una parte del contratto specifica all'integrazione NinjaOne. Questa azione viene eseguita nella sezione delle parti del contratto di un contratto; selezionare l'integrazione

pertinente, il sito o gruppo e il tipo di workload, quindi selezionare gli articoli della configurazione corrispondenti.

- Nella sezione delle parti del contratto di un contratto è possibile selezionare **Aggiornamento automatico** per aggiornare la quantità di dispositivi relativa alla parte in questione.
- È inoltre possibile selezionare **Mostra workload in fattura** per aggiungere informazioni su dispositivi specifici alle fatture del cliente.

Per ulteriori informazioni sulla definizione dei contratti e sull'aggiunta dei dispositivi ai contratti, consultare "Lavorare con i contratti" (pag. 282).

Integrazione con Datto RMM

L'integrazione di Advanced Automation (PSA) con Datto RMM consente di:

- Importare automaticamente siti di clienti e dispositivi da Datto RMM.
- Abbinare i clienti ai siti da Datto RMM.
- Creare ticket dagli avvisi di Datto RMM.
- Accedere alla pagina dei dispositivi Datto RMM da un ticket.
- Connettersi da remoto a un dispositivo Datto RMM da un ticket.
- Fatturare ai clienti il numero di dispositivi effettivo utilizzando Datto RMM.

Nota
Per integrare in modo corretto Datto RMM con Advanced Automation (PSA), è necessario abilitare il servizio Advanced Automation (PSA). Inoltre, deve essere disponibile un account Datto RMM configurato in tutte le sue parti.

Configurazione dell'integrazione Datto RMM

Due passaggi principali consentono di configurare l'integrazione di Datto RMM con Advanced Automation (PSA), come descritto nelle procedure seguenti.

1. Definizione delle impostazioni di integrazione per la connessione con l'istanza di Datto RMM.
2. Mapping dei clienti di Datto RMM ad Advanced Automation (PSA).

Per definire le impostazioni di integrazione

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **Datto RMM**, fare clic su **Configura**.
3. Inserire le credenziali Datto RMM seguenti per accedere all'istanza Datto RMM:
   - **Server Datto RMM**: inserire l'URL del server Datto RMM.
   - **Chiave API**: inserire la chiave API univoca per l'account Datto RMM.
   - **Segreto API**: inserire il segreto API univoco per l'account Datto RMM.

Tutte le credenziali sopra indicate vengono create nell'account Datto RMM. Per generarle, è necessario innanzitutto accedere all'account Datto RMM. Passare a **Configurazione > Impostazioni account > Controllo accesso**, e impostare **Abilita accesso API** su **ON**. Quindi fare clic sulla scheda **Utenti** e poi sull'utente per il quale abilitare l'accesso API. Copiare l'URL, la chiave API e il segreto API visualizzati.

4. (Facoltativo) Fare clic su **Prova connessione** per verificare la credenziali inserite.
5. Fare clic su **Avanti**.
6. Per fare in modo che gli avvisi di Datto RMM siano automaticamente sincronizzati con i ticket in Advanced Automation (PSA), verificare che la casella di controllo **Creare ticket dagli avvisi di Datto RMM** sia selezionata (è selezionata per impostazione predefinita).
7. Selezionare la casella di controllo **Ignora avvisi silenziati** se non si desidera sincronizzare gli avvisi di Datto RMM che sono stati silenziati. La casella di controllo è selezionata per impostazione predefinita.
8. Fare clic su **Salva**. Il passaggio successivo per configurare l'integrazione è il mapping dei clienti di Datto RMM ai clienti esistenti o nuovi di Advanced Automation (PSA). Attenersi alla procedura seguente.

Per il mapping dei clienti di Datto RMM

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **Datto RMM**, fare clic su **Gestisci**.
3. Nella scheda **Mapping del cliente**, fare clic su **Creazione di clienti Acronis dai siti di Datto RMM**. Il processo di mapping viene avviato per tutti i siti di Datto RMM in elenco.
   Tutti i clienti (siti dei clienti) derivanti da Datto RMM vengono registrati come nuovi clienti in Portale di gestione, insieme a tutti i servizi disponibili garantiti.
   È inoltre possibile scegliere singoli siti di Datto RMM e abbinarli a clienti di Portale di gestione esistenti; selezionare i siti pertinenti e quindi fare clic su **Mapping a tenant di cliente esistente**. Il sistema chiede di selezionare un cliente esistente. Una volta effettuata la selezione, fare clic su **Mapping** per completare il processo.
4. Al termine del processo, nella colonna **Mapping** viene visualizzato lo stato **Mappato**, e la colonna **Cliente Acronis** visualizza il nome del cliente corrispondente.

Nota
Per rimuovere un mapping, selezionare la riga attualmente mappata e fare clic su **Rimuovi mapping**. Nella finestra popup di conferma visualizzata, fare clic su **Rimuovi**.

Revisione e modifica delle impostazioni dell'integrazione Datto RMM

È possibile rivedere e modificare le impostazioni dell'integrazione Datto RMM come necessario. È anche possibile disattivare l'integrazione Datto RMM.

Per rivedere e modificare le impostazioni dell'integrazione Datto RMM

1. Nel portale di gestione, passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
   Nel riquadro relativo a **Datto RMM** è possibile visualizzare lo stato corrente dell'integrazione e il numero di account collegati.
2. Fare clic su **Apri integrazione** per visualizzare e modificare le impostazioni dell'integrazione.
   Ad esempio, è possibile visualizzare e modificare le credenziali e le impostazioni degli avvisi nella scheda **Impostazioni di integrazione**, e i clienti Datto RMM con mapping ad Advanced Automation (PSA) nella scheda **Mapping del cliente**.
3. Fare clic sull'icona a matita per modificare la sezione pertinente. Per ulteriori informazioni sui campi modificabili, consultare "Configurazione dell'integrazione Datto RMM" (pag. 355).
4. Al termine, fare clic su ✓.

Per disattivare l'integrazione Datto RMM

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a **Datto RMM**, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Creazione di ticket dagli avvisi di Datto RMM

Quando è configurata l'integrazione con Datto RMM (consultare "Configurazione dell'integrazione Datto RMM" (pag. 355)), Advanced Automation (PSA) crea automaticamente nuovi ticket a partire dagli avvisi di Datto RMM. I ticket sono costantemente sincronizzati con Datto RMM, garantendo che gli avvisi aperti già collegati ai ticket in Advanced Automation (PSA) vengano ignorati.

Tenere presente quanto segue:

- I tickets sono creati solo per i clienti associati ai siti dei clienti di Datto RMM.
- I parametri dei ticket sono definiti in base alle impostazioni predefinite per il cliente corrispondente, come descritto in "Impostazione dei valori predefiniti" (pag. 319).
- Il riepilogo e la descrizione del ticket derivano dal riepilogo e dalla descrizione dell'avviso.
- Il ticket include i collegamenti al cliente di Portale di gestione, all'utente del cliente (tramite il rispettivo indirizzo e-mail, se fornito da Datto RMM) e ai dispositivi collegati all'utente (se pertinente; gli utenti possono visualizzare i dispositivi nella console di Cyber Protect).
- Se un ticket è collegato al dispositivo di un utente, nella sezione Informazioni dispositivo di Datto RMM è presente il relativo link. Inoltre, viene incluso il link per avviare una connessione remota, se fornito da Datto RMM.

Per ulteriori informazioni sulla creazione dei ticket, consultare "Creazione di un nuovo ticket" (pag. 223).

Aggiunta di dispositivi Datto RMM esterni ai contratti

Se è stata configurata l'integrazione con Datto RMM (consultare "Configurazione dell'integrazione Datto RMM" (pag. 355)), è possibile aggiungere dispositivi esterni ai contratti per i clienti in Advanced Automation (PSA).

- È possibile collegare una parte del contratto specifica all'integrazione Datto RMM. Questa azione viene eseguita nella sezione delle parti del contratto di un contratto; selezionare l'integrazione pertinente, il sito o gruppo e il tipo di workload, quindi selezionare gli elementi di configurazione corrispondenti.
- Nella sezione delle parti del contratto di un contratto è possibile selezionare **Aggiornamento automatico** per aggiornare la quantità di dispositivi relativa alla parte in questione.
- È inoltre possibile selezionare **Mostra workload in fattura** per aggiungere informazioni su dispositivi specifici alle fatture del cliente.

Per ulteriori informazioni sulla definizione dei contratti e sull'aggiunta dei dispositivi ai contratti, consultare "Lavorare con i contratti" (pag. 282).

Integrazione con Kaseya VSA

Integrando Advanced Automation (PSA) con Kaseya VSA tramite il plug-in esistente Cyber Protect, è possibile:

- Importare automaticamente siti di clienti e dispositivi da Kaseya VSA.
- Abbinare i clienti ai siti da Kaseya VSA.
- Creare ticket dagli avvisi di Kaseya VSA.
- Accedere alla pagina dei dispositivi Kaseya VSA da un ticket.
- Connettersi da remoto a un dispositivo Kaseya VSA da un ticket.
- Fatturare ai clienti il numero di dispositivi effettivo utilizzando Kaseya VSA.

Nota
Per integrare in modo corretto Kaseya VSA con Advanced Automation (PSA), è necessario abilitare il servizio Advanced Automation (PSA). Per ulteriori informazioni sull'utilizzo del plug-in esistente Cyber Protect per Kaseya VSA, consultare questa guida.

Integrazione con N-able N-central

L'integrazione di Advanced Automation (PSA) con N-able N-central consente di:

- Importare automaticamente siti di clienti e dispositivi da N-able N-central.
- Abbinare i clienti ai siti da N-able N-central.
- Creare ticket dagli avvisi di N-able N-central.
- Sincronizzare ticket tra Advanced Automation (PSA) e N-able N-central.
- Accedere alla pagina dei dispositivi N-able N-central da un ticket.
- Fatturare ai clienti il numero di dispositivi effettivo utilizzando N-able N-central.

Nota
Per integrare in modo corretto N-able N-central con Advanced Automation (PSA), è necessario abilitare il servizio Advanced Automation (PSA). Inoltre, deve essere disponibile un account N-able N-central configurato in tutte le sue parti.

Configurazione dell'integrazione N-able N-central

Due passaggi principali consentono di configurare l'integrazione di N-able N-central con Advanced Automation (PSA), come descritto nelle procedure seguenti.

1. Definizione delle impostazioni di integrazione per la connessione con l'istanza di N-able N-central.
2. Mapping dei clienti di N-able N-central ad Advanced Automation (PSA).

Per definire le impostazioni di integrazione

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **N-able N-central**, fare clic su **Configura**.
3. Inserire le credenziali N-able N-central seguenti per accedere all'istanza N-able N-central:
   - URL
   - Nome utente
   - Password
4. (Facoltativo) Fare clic su **Prova connessione** per verificare la credenziali inserite.
5. Fare clic su **Avanti**.
6. Per fare in modo che gli avvisi di N-able N-central siano automaticamente sincronizzati con i ticket in Advanced Automation (PSA), verificare che la casella di controllo **Integrazione ticket** sia selezionata (è selezionata per impostazione predefinita).
7. Fare clic su **Salva**. Il passaggio successivo per configurare l'integrazione è il mapping dei clienti di N-able N-central ai clienti esistenti o nuovi di Advanced Automation (PSA). Attenersi alla procedura seguente.

Per il mapping dei clienti di N-able N-central

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **N-able N-central**, fare clic su **Gestisci**.
3. Nella scheda **Mapping del cliente**, fare clic su **Creazione di clienti Acronis dai siti di N-able N-central**. Il processo di mapping viene avviato per tutti i siti di N-able N-central in elenco.
   Tutti i clienti (siti dei clienti) derivanti da N-able N-central vengono registrati come nuovi clienti in Portale di gestione, insieme a tutti i servizi disponibili garantiti.
   È inoltre possibile scegliere singoli siti di N-able N-central e abbinarli a clienti di Portale di gestione esistenti; selezionare i siti pertinenti e quindi fare clic su **Mapping a tenant di cliente**

esistente. Il sistema chiede di selezionare un cliente esistente. Una volta effettuata la selezione, fare clic su **Mapping** per completare il processo.

4. Al termine del processo, nella colonna **Mapping** viene visualizzato lo stato **Mappato**, e la colonna **Cliente Acronis** visualizza il nome del cliente corrispondente.

Nota
Per rimuovere un mapping, selezionare la riga attualmente mappata e fare clic su **Rimuovi mapping**. Nella finestra popup di conferma visualizzata, fare clic su **Rimuovi**.

Revisione e modifica delle impostazioni dell'integrazione N-able N-central

È possibile rivedere e modificare le impostazioni dell'integrazione N-able N-central come necessario. È anche possibile disattivare l'integrazione N-able N-central.

Per rivedere e modificare le impostazioni dell'integrazione N-able N-central

1. Nel portale di gestione, passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**. Nel riquadro relativo a **N-able N-central** è possibile visualizzare lo stato corrente dell'integrazione e il numero di account collegati.
2. Fare clic su **Gestisci** per visualizzare e modificare le impostazioni dell'integrazione.
   Ad esempio, è possibile visualizzare e modificare le credenziali e le impostazioni degli avvisi nella scheda **Impostazioni di integrazione**, e i clienti N-able N-central con mapping ad Advanced Automation (PSA) nella scheda **Mapping del cliente**.
3. Fare clic sull'icona a matita per modificare la sezione pertinente. Per ulteriori informazioni sui campi modificabili, consultare "Configurazione dell'integrazione N-able N-central" (pag. 359).
4. Al termine, fare clic su ✓.

Per disattivare l'integrazione N-able N-central

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a **N-able N-central**, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Creazione di ticket dagli avvisi di N-able N-central

Quando è configurata l'integrazione con N-able N-central (consultare "Configurazione dell'integrazione N-able N-central" (pag. 359)), Advanced Automation (PSA) crea automaticamente nuovi ticket a partire dagli avvisi di N-able N-central. I ticket sono costantemente sincronizzati con N-able N-central, garantendo che gli avvisi aperti già collegati ai ticket in Advanced Automation (PSA) vengano ignorati.

Tenere presente quanto segue:

- I tickets sono creati solo per i clienti associati ai siti dei clienti di N-able N-central.
- I parametri dei ticket sono definiti in base alle impostazioni predefinite per il cliente corrispondente, come descritto in "Impostazione dei valori predefiniti" (pag. 319).

- Il riepilogo e la descrizione del ticket derivano dal riepilogo e dalla descrizione dell'avviso.
- Il ticket include i collegamenti al cliente di Portale di gestione, all'utente del cliente (tramite il rispettivo indirizzo e-mail, se fornito da N-able N-central) e ai dispositivi collegati all'utente (se pertinente; gli utenti possono visualizzare i dispositivi nella console di Cyber Protect).
- Se un ticket è collegato al dispositivo di un utente, nella sezione Informazioni dispositivo di N-able N-central è presente il relativo link.

Per ulteriori informazioni sulla creazione dei ticket, consultare "Creazione di un nuovo ticket" (pag. 223).

Aggiunta di dispositivi N-able N-central esterni ai contratti

Se è stata configurata l'integrazione con N-able N-central (consultare "Configurazione dell'integrazione N-able N-central" (pag. 359)), è possibile aggiungere dispositivi esterni ai contratti per i clienti in Advanced Automation (PSA).

- È possibile collegare una parte del contratto specifica all'integrazione N-able N-central. Questa azione viene eseguita nella sezione delle parti del contratto di un contratto; selezionare l'integrazione pertinente, il sito o gruppo e il tipo di workload, quindi selezionare gli articoli della configurazione corrispondenti.
- Nella sezione delle parti del contratto di un contratto è possibile selezionare **Aggiornamento automatico** per aggiornare la quantità di dispositivi relativa alla parte in questione.
- È inoltre possibile selezionare **Mostra workload in fattura** per aggiungere informazioni su dispositivi specifici alle fatture del cliente.

Per ulteriori informazioni sulla definizione dei contratti e sull'aggiunta dei dispositivi ai contratti, consultare "Lavorare con i contratti" (pag. 282).

Integrazione con N-able RMM

L'integrazione di Advanced Automation (PSA) con N-able RMM consente di:

- Importare automaticamente siti di clienti e dispositivi da N-able RMM.
- Abbinare i clienti ai siti da N-able RMM.
- Creare ticket dagli avvisi di N-able RMM.
- Fatturare ai clienti il numero di dispositivi effettivo utilizzando N-able RMM.

Nota
Per integrare in modo corretto N-able RMM con Advanced Automation (PSA), è necessario abilitare il servizio Advanced Automation (PSA). Inoltre, deve essere disponibile un account N-able RMM configurato in tutte le sue parti.

Configurazione dell'integrazione N-able RMM

Due passaggi principali consentono di configurare l'integrazione di N-able RMM con Advanced Automation (PSA), come descritto nelle procedure seguenti.

1. Definizione delle impostazioni di integrazione per la connessione con l'istanza di N-able RMM.
2. Mapping dei clienti di N-able RMM ad Advanced Automation (PSA).

Per definire le impostazioni di integrazione

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **N-able RMM**, fare clic su **Configura**.
3. Inserire le credenziali N-able RMM seguenti per accedere all'istanza N-able RMM:
   - URL
   - Chiave API
4. (Facoltativo) Fare clic su **Prova connessione** per verificare la credenziali inserite.
5. Fare clic su **Avanti**.
6. Per fare in modo che gli avvisi di N-able RMM siano automaticamente sincronizzati con i ticket in Advanced Automation (PSA), verificare che la casella di controllo **Integrazione ticket** sia selezionata (è selezionata per impostazione predefinita).
7. Fare clic su **Salva**. Il passaggio successivo per configurare l'integrazione è il mapping dei clienti di N-able RMM ai clienti esistenti o nuovi di Advanced Automation (PSA). Attenersi alla procedura seguente.

Per il mapping dei clienti di N-able RMM

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Gestione** > **Monitoraggio e gestione remota**.
2. Nel riquadro relativo a **N-able RMM**, fare clic su **Gestisci**.
3. Nella scheda **Mapping del cliente**, fare clic su **Creazione di clienti Acronis dai siti di N-able RMM**. Il processo di mapping viene avviato per tutti i siti di N-able RMM in elenco.
   Tutti i clienti (siti dei clienti) derivanti da N-able RMM vengono registrati come nuovi clienti in Portale di gestione, insieme a tutti i servizi disponibili garantiti.
   È inoltre possibile scegliere singoli siti di N-able RMM e abbinarli a clienti di Portale di gestione esistenti; selezionare i siti pertinenti e quindi fare clic su **Mapping a tenant di cliente esistente**. Il sistema chiede di selezionare un cliente esistente. Una volta effettuata la selezione, fare clic su **Mapping** per completare il processo.
4. Al termine del processo, nella colonna **Mapping** viene visualizzato lo stato **Mappato**, e la colonna **Cliente Acronis** visualizza il nome del cliente corrispondente.

Nota
Per rimuovere un mapping, selezionare la riga attualmente mappata e fare clic su **Rimuovi mapping**. Nella finestra popup di conferma visualizzata, fare clic su **Rimuovi**.

Revisione e modifica delle impostazioni dell'integrazione N-able RMM

È possibile rivedere e modificare le impostazioni dell'integrazione N-able RMM come necessario. È anche possibile disattivare l'integrazione N-able RMM.

Per rivedere e modificare le impostazioni dell'integrazione N-able RMM

1. Nel portale di gestione, passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
   Nel riquadro relativo a **N-able RMM** è possibile visualizzare lo stato corrente dell'integrazione e il numero di account collegati.
2. Fare clic su **Gestisci** per visualizzare e modificare le impostazioni dell'integrazione.
   Ad esempio, è possibile visualizzare e modificare le credenziali e le impostazioni degli avvisi nella scheda **Impostazioni di integrazione**, e i clienti N-able RMM con mapping ad Advanced Automation (PSA) nella scheda **Mapping del cliente**.
3. Fare clic sull'icona a matita per modificare la sezione pertinente. Per ulteriori informazioni sui campi modificabili, consultare "Configurazione dell'integrazione N-able RMM" (pag. 361).
4. Al termine, fare clic su ✓.

Per disattivare l'integrazione N-able RMM

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a **N-able RMM**, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Creazione di ticket dagli avvisi di N-able RMM

Quando è configurata l'integrazione con N-able RMM (consultare "Configurazione dell'integrazione N-able RMM" (pag. 361)), Advanced Automation (PSA) crea automaticamente nuovi ticket a partire dagli avvisi di N-able RMM. I ticket sono costantemente sincronizzati con N-able RMM, garantendo che gli avvisi aperti già collegati ai ticket in Advanced Automation (PSA) vengano ignorati.

Tenere presente quanto segue:

- I ticket sono creati solo per i clienti associati ai siti dei clienti di N-able RMM.
- I parametri dei ticket sono definiti in base alle impostazioni predefinite per il cliente corrispondente, come descritto in "Impostazione dei valori predefiniti" (pag. 319).
- Il riepilogo e la descrizione del ticket derivano dal riepilogo e dalla descrizione dell'avviso.
- Il ticket include i collegamenti al cliente di Portale di gestione, all'utente del cliente (tramite il rispettivo indirizzo e-mail, se fornito da N-able RMM) e ai dispositivi collegati all'utente (se pertinente; gli utenti possono visualizzare i dispositivi nella console di Cyber Protect).
- Se un ticket è collegato al dispositivo di un utente, nella sezione Informazioni dispositivo di N-able RMM è presente il relativo link.

Per ulteriori informazioni sulla creazione dei ticket, consultare "Creazione di un nuovo ticket" (pag. 223).

Aggiunta di dispositivi N-able RMM esterni ai contratti

Se è stata configurata l'integrazione con N-able RMM (consultare "Configurazione dell'integrazione N-able RMM" (pag. 361)), è possibile aggiungere dispositivi esterni ai contratti per i clienti in Advanced Automation (PSA).

- È possibile collegare una parte del contratto specifica all'integrazione N-able RMM. Questa azione viene eseguita nella sezione delle parti del contratto di un contratto; selezionare l'integrazione pertinente, il sito o gruppo e il tipo di workload, quindi selezionare gli articoli della configurazione corrispondenti.
- Nella sezione delle parti del contratto di un contratto è possibile selezionare **Aggiornamento automatico** per aggiornare la quantità di dispositivi relativa alla parte in questione.
- È inoltre possibile selezionare **Mostra workload in fattura** per aggiungere informazioni su dispositivi specifici alle fatture del cliente.

Per ulteriori informazioni sulla definizione dei contratti e sull'aggiunta dei dispositivi ai contratti, consultare "Lavorare con i contratti" (pag. 282).

Integrazione con piattaforme VAR

Nota
Questa funzionalità è disponibile solo agli utenti ai quali è assegnato il ruolo di Amministratore.

Advanced Automation (PSA) consente l'integrazione con le piattaforme di rivenditori a valore aggiunto (VAR). Al momento è supportato solo Microsoft CSP. L'integrazione permette di accedere ai dati di utilizzo degli abbonamenti dei clienti dai fornitori terzi, e quindi tenere traccia, contabilizzare ed emettere le fatture dei clienti in Advanced Automation (PSA), come necessario.

Per accedere alle integrazioni delle piattaforme VAR, passare a **Integrazioni**. Nel menu visualizzato a sinistra, selezionare **Automazione** > **Commercio cloud e marketplace**.

Integrazione con Microsoft CSP

L'integrazione di Advanced Automation (PSA) con Microsoft CSP consente di:

- Importare automaticamente i clienti dal portale dei partner Microsoft CSP.
- Importare automaticamente gli abbonamenti e i relativi dati di utilizzo dal portale dei partner Microsoft CSP.
- Fatturare ai clienti l'utilizzo effettivo degli abbonamenti a Microsoft CSP.

Per integrare in modo corretto Microsoft CSP con Advanced Automation (PSA), è necessario abilitare il servizio Advanced Automation (PSA). Inoltre, deve essere disponibile un account Microsoft CSP configurato in tutte le sue parti.

Microsoft ha due livelli di partnership di base che permettono ai service provider di rivendere servizi e licenze Microsoft CSP ai clienti finali: Livello 1 e Livello 2.

- Il Livello 1 fa riferimento ai partner che acquistano direttamente da Microsoft. Ad esempio, tutti i distributori che vendono abbonamenti al programma Microsoft CSP sono partner di Livello 1.
- Il Livello 2 fa riferimento ai partner che acquistano gli abbonamenti al programma Microsoft CSP da un distributore (Partner di Livello 1).

I partner gestiscono i propri servizi e licenze Microsoft CSP da una console centralizzata, il portale dei partner Microsoft, indipendentemente da dove hanno acquistato tali servizi e licenze.

Nota
Al momento, Advanced Automation (PSA) supporta solo i partner di Livello 1.

Per definire le impostazioni di integrazione

1. Nel portale di gestione, passare a **Integrazioni**, quindi selezionare **Automazione** > **Commercio cloud e marketplace**.
2. Nel riquadro relativo a **Microsoft CSP**, fare clic su **Configura**, quindi su **Attiva**.
3. Inserire le credenziali Microsoft CSP seguenti per accedere all'account Microsoft CSP:
   - **ID app**: inserire l'ID app univoco per l'account Microsoft CSP.
   - **Chiave privata**: inserire la chiave privata univoca per l'account Microsoft CSP. La chiave privata viene generata insieme all'ID app (vedere sopra).
   - **Dominio**: inserire il dominio pertinente.
4. (Facoltativo) Fare clic su **Prova connessione** per verificare la credenziali inserite.
5. Fare clic su **Salva**.
   Una volta definita l'integrazione, è possibile definire una parte del contratto (consultare "Creazione di un nuovo contratto" (pag. 282)) e selezionare un cliente da Microsoft CSP per ottenerne i dati di utilizzo corretti.

Revisione e modifica delle impostazioni dell'integrazione Microsoft CSP

È possibile rivedere e modificare le impostazioni dell'integrazione Microsoft CSP come necessario. È anche possibile disattivare l'integrazione Microsoft CSP.

Per rivedere e modificare le impostazioni dell'integrazione Microsoft CSP

1. Nel portale di gestione, passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**. Nel riquadro relativo a **Microsoft CSP**, è possibile visualizzare lo stato corrente dell'integrazione.
2. Fare clic su **Gestisci** per visualizzare e modificare le impostazioni dell'integrazione.
3. Fare clic sull'icona a matita per modificare i campi pertinenti. Per ulteriori informazioni sui campi modificabili, consultare "Integrazione con Microsoft CSP" (pag. 364).
4. Al termine, fare clic su ✓.

Per disattivare l'integrazione Microsoft CSP

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a **Microsoft CSP**, fare clic su **Disattiva**.

3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Uso dei dati di utilizzo di Microsoft CSP nei contratti

Se è stata configurata l'integrazione con Microsoft CSP (consultare "Integrazione con Microsoft CSP" (pag. 364)), è possibile aggiungere i dati di utilizzo di Microsoft CSP ai contratti per i clienti in Advanced Automation (PSA).

Tenere presente quanto segue:

- È possibile collegare una specifica parte del contratto all'integrazione Microsoft CSP.
- È possibile filtrare i tipi di licenza da Microsoft CSP per:
  - **Gruppo VAR**: selezionare il cliente pertinente dall'elenco dei clienti nel portale dei partner Microsoft CSP per poter applicare un filtro alle licenze collegate a un unico cliente specifico.
  - **Tipo di licenza**: selezionare i tipi di licenza disponibili dal portale dei partner Microsoft CSP.
- La casella di controllo **Aggiornamento automatico** nella sezione **Parti del contratto** della procedura guidata di creazione del contratto è abilitata per impostazione predefinita e nascosta: essa disabilita automaticamente il campo **Quantità**. Se configurato a tal fine, Advanced Automation (PSA) sincronizza i dati relativi all'utilizzo effettivo con questo campo, così da consentire la fatturazione dell'utilizzo effettivo della licenza.

Per ulteriori informazioni sulla definizione dei contratti, consultare "Lavorare con i contratti" (pag. 282).

Nota
Quando si genera una fattura per un cliente con utilizzo della licenza Microsoft CSP, la fattura include automaticamente le righe pertinenti per i tipi di licenza utilizzati, con la quantità e il prezzo corretti.

Integrazione con piattaforme di pagamento

Advanced Automation (PSA) consente l'integrazione con diverse piattaforme di pagamento (al momento sono supportate solo PayPal e Stripe). Queste integrazioni consentono di inviare fatture che contengono link sui quali i clienti possono agire per effettuare il pagamento tramite la piattaforma corrispondente.

Per accedere alle integrazioni della piattaforme dei pagamenti, passare a **Integrazioni**. Nel menu visualizzato a sinistra, selezionare **Automazione** > **Elaborazione pagamento**.

Integrazione con PayPal

L'integrazione di Advanced Automation (PSA) con il gateway dei pagamenti PayPal consente di automatizzare la raccolta e la registrazione dei pagamenti effettuati dai clienti.

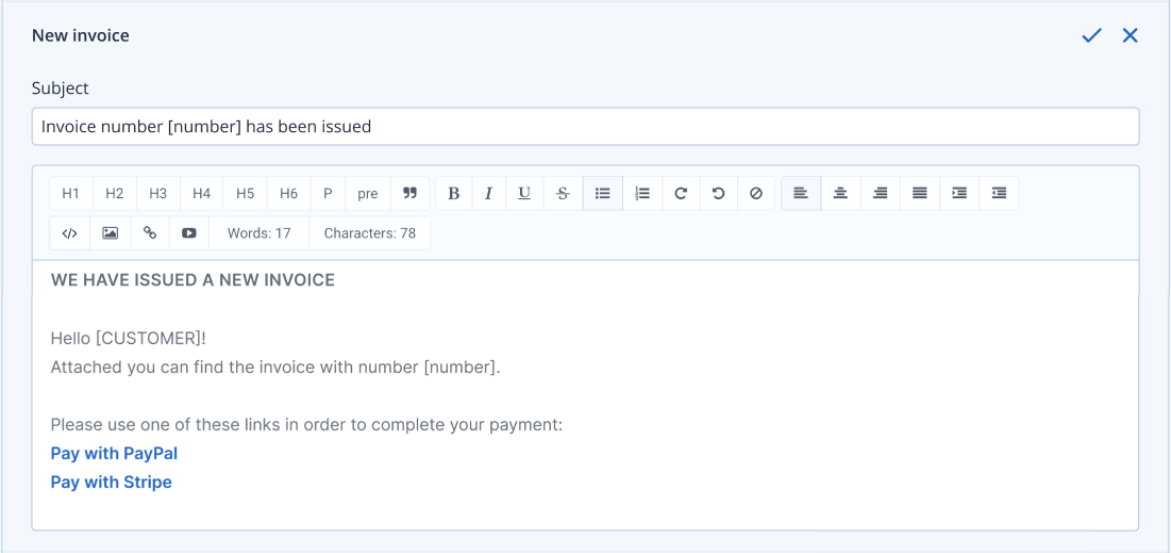
Per altre informazioni sulle ulteriori piattaforme di pagamento integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di pagamento" (pag. 366).

Per attivare l'integrazione con PayPal

1. Passare a **Integrazioni** e selezionare **Automazione** > **Elaborazione pagamento**.
2. Nel riquadro relativo a PayPal, fare clic su **Configura**, quindi su **Attiva**.
3. Inserire le credenziali di PayPal richieste:
   - Nome utente API
   - Password API
   - Firma

   Per ulteriori informazioni su come ottenere le credenziali indicate da PayPal, consultare "Modalità di accesso alle informazioni su nome utente, password e firma dell'API PayPal" (pag. 368).
4. Fare clic su **Salva**.

   Nelle fatture inviate è ora possibile includere un link che consente ai clienti di effettuare il pagamento tramite PayPal, come mostrato di seguito. Per ulteriori informazioni su come definire questo link nel modello e-mail "Nuova fattura", consultare "Gestione dei modelli di e-mail" (pag. 324).



Per modificare le impostazioni di integrazione di PayPal

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a PayPal, fare clic su **Gestisci**, quindi selezionare **Impostazioni**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con PayPal

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a PayPal, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Modalità di accesso alle informazioni su nome utente, password e firma dell'API PayPal

Per integrare Advanced Automation (PSA) e PayPal (consultare "Integrazione con PayPal" (pag. 366)), è necessario definire il nome utente, la password e la firma per l'API PayPal nelle impostazioni dell'integrazione. Queste credenziali sono reperibili nelle impostazioni dell'account PayPal, come descritto di seguito.

Per ottenere le informazioni su nome utente, password e firma dell'API PayPal

1. Accedere all'account PayPal.
2. Dal menu principale, passare a **Strumenti > Tutti gli strumenti**.
3. Scorrere la pagina verso il basso e fare clic su **Credenziali API**.
4. Fare clic su **Integrazione NVP/SOAP**.

   Nota
   Se è la prima volta che si creano le credenziali, al di sotto dell'integrazione API NVP/SOAP viene visualizzato il link **Richiedi credenziali API**. Completare il modulo di richiesta delle credenziali API, selezionare la casella di controllo del contratto e fare clic su **Invia**.

5. Fare clic sul collegamento **Mostra** accanto a ogni entità corrispondente e prendere nota delle credenziali visualizzate. Tali credenziali dovranno essere utilizzate per definire le impostazioni dell'integrazione, come descritto in "Integrazione con PayPal" (pag. 366).

Integrazione con Stripe

L'integrazione di Advanced Automation (PSA) con il gateway dei pagamenti Stripe consente di automatizzare la raccolta e la registrazione dei pagamenti effettuati dai clienti.

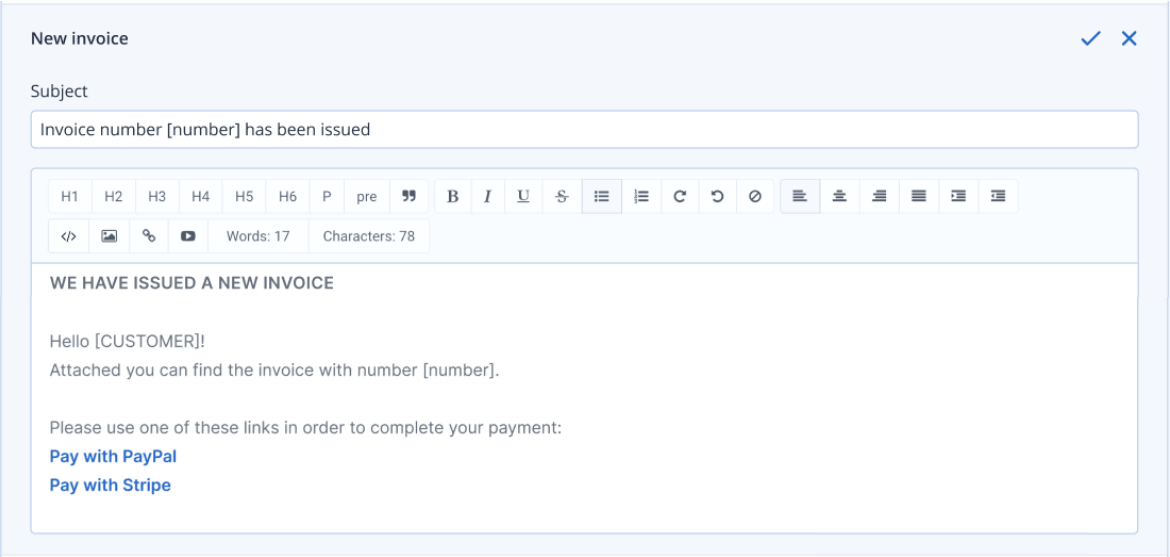
Per altre informazioni sulle ulteriori piattaforme di pagamento integrabili in Advanced Automation (PSA), consultare "Integrazione con piattaforme di pagamento" (pag. 366).

Per attivare l'integrazione con Stripe

1. Passare a **Integrazioni** e selezionare **Automazione** > **Elaborazione pagamento**.
2. Nel riquadro relativo a Stripe, fare clic su **Configura**, quindi su **Attiva**.
3. Inserire le credenziali Stripe indicate di seguito:
   - Chiave privata
   - Chiave pubblicabile

   Per ulteriori informazioni su come ottenere le credenziali indicate da Stripe, consultare "Come accedere alle chiavi private e pubblicabili di Stripe" (pag. 369).
4. Fare clic su **Salva**.
   Nelle fatture inviate è ora possibile includere un link che consente ai clienti di effettuare il pagamento tramite Stripe, come mostrato di seguito. Per ulteriori informazioni su come definire

questo link nel modello e-mail "Nuova fattura", consultare "Gestione dei modelli di e-mail" (pag. 324).



Per modificare le impostazioni di integrazione di Stripe

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a Stripe, fare clic su **Gestisci**, quindi selezionare **Impostazioni**.
3. Modificare le impostazioni come necessario (vedi sopra).

Per disattivare l'integrazione con Stripe

1. Passare a **Integrazioni**, quindi fare clic sulla scheda **Integrazioni in uso**.
2. Nel riquadro relativo a Stripe, fare clic su **Disattiva**.
3. Nel messaggio di conferma visualizzato, fare clic su **Elimina**.

Come accedere alle chiavi private e pubblicabili di Stripe

Per integrare Advanced Automation (PSA) e Stripe (consultare "Integrazione con Stripe" (pag. 368)), è necessario definire le chiavi private e pubblicabili di Stripe nelle impostazioni dell'integrazione. Queste credenziali sono reperibili nelle impostazioni dell'account Stripe, come descritto di seguito.

Per ottenere le chiavi private e pubblicabili di Stripe

1. Accedere all'account Stripe.
2. Passare a **Sviluppatori > Chiavi API**.
3. Se è la prima volta che si richiede la chiave privata, fare clic su **Rivela token chiave di test** per generare la chiave.
4. Prendere nota delle credenziali visualizzate. Tali credenziali dovranno essere utilizzate per definire le impostazioni dell'integrazione, come descritto in "Integrazione con Stripe" (pag. 368).

Disattivazione del servizio Advanced Automation (PSA)

È possibile disattivare il servizio Advanced Automation (PSA) se non si ha intenzione di utilizzarne le funzionalità incluse.

La disattivazione è immediata. Tuttavia, è possibile selezionare l'eliminazione immediata delle impostazioni e dei dati archiviati in Advanced Automation (PSA) o pianificarne l'eliminazione entro 30 giorni.

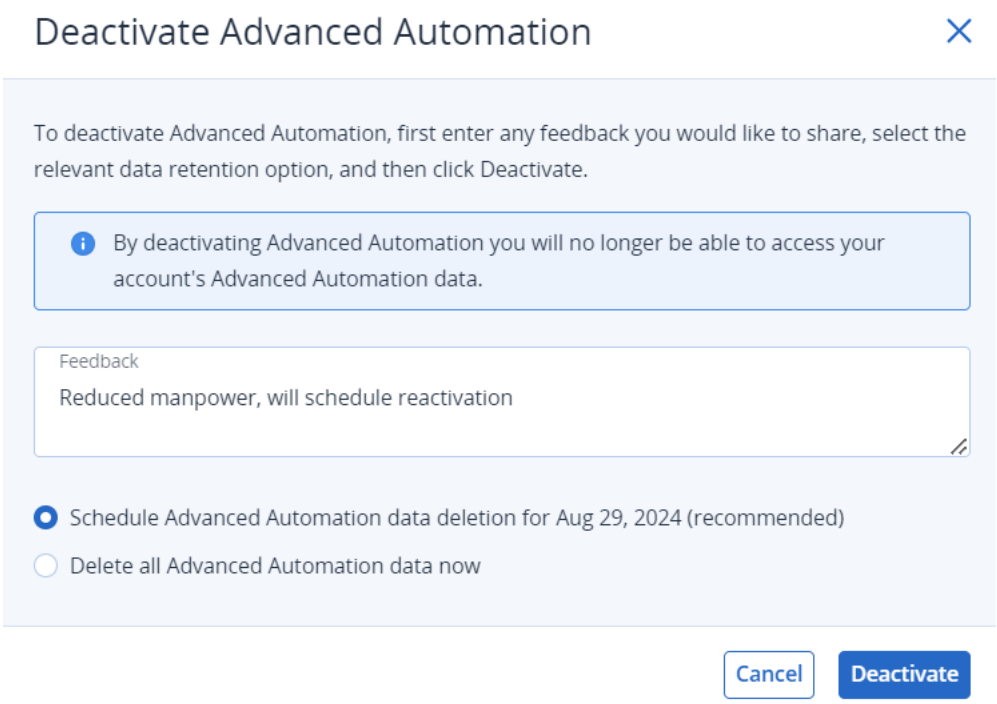
Importante
Se si sceglie di eliminare immediatamente tutti i dati di Advanced Automation (PSA), tutti i dati e le impostazioni di Advanced Automation (PSA) vengono rimossi dal sistema. Se in seguito si decide di utilizzare nuovamente Advanced Automation (PSA), sarà necessario attivare il servizio Advanced Automation (PSA) e ripetere l'onboarding. Per ulteriori informazioni, consultare "Impostazione di Advanced Automation (PSA)" (pag. 203).

Se si sceglie di pianificare l'eliminazione dei dati di Advanced Automation (PSA) entro 30 giorni, le impostazioni e i dati vengono conservati e Advanced Automation (PSA) potrà essere riattivato in qualsiasi momento nei 30 giorni successivi. Nessun costo viene addebitato per l'utilizzo di Advanced Automation (PSA) durante il periodo di conservazione di 30 giorni. Per ulteriori informazioni sulla riattivazione, vedere la procedura riportata di seguito.

Per disattivare il servizio Advanced Automation (PSA)

1. Nel portale di gestione, fare clic su **Impostazioni** > **Fatturazione e offerte**, quindi selezionare **Advanced Automation (PSA)**.
   La schermata visualizzata include informazioni sul numero di utenti corrente di Advanced Automation (PSA).
2. Fare clic su **Disattiva Advanced Automation (PSA)**.
3. Nella finestra di dialogo visualizzata, inserire eventuali feedback da condividere.
4. Selezionare una delle seguenti opzioni:
   - Pianificare l'eliminazione dei dati di Advanced Automation (PSA) entro 30 giorni da oggi (viene visualizzata la data effettiva di eliminazione). Questa opzione consente di riattivare Advanced Automation (PSA) in qualsiasi momento entro i prossimi 30 giorni, come descritto nella procedura seguente.
   - Eliminare subito tutti i dati di Advanced Automation (PSA). Questa opzione elimina immediatamente tutti i dati e le impostazioni di Advanced Automation (PSA), l'azione non è

reversibile.



5. Fare clic su **Disattiva**.
   Se si sceglie di pianificare l'eliminazione dei dati di Advanced Automation (PSA) entro 30 giorni, viene visualizzata la pagina di destinazione principale di Advanced Automation (PSA). Per riattivare il servizio, è possibile fare clic su **Riattiva** in qualsiasi momento entro i prossimi 30 giorni. Per ulteriori informazioni sulla riattivazione, vedere la procedura riportata di seguito.
   Se si sceglie di eliminare tutti i dati di Advanced Automation (PSA) ora, viene visualizzata la pagina di destinazione principale di Advanced Automation (PSA), ma solo con l'opzione **Attiva** per il servizio Advanced Automation (PSA). Per attivare nuovamente Advanced Automation (PSA) è necessario completare di nuovo il processo di onboarding.

Per riattivare il servizio Advanced Automation (PSA)

1. Nel portale di gestione, fare clic su **Impostazioni > Advanced Automation (PSA)**.
2. Fare clic su **Riattiva**.

   Nota
   L'opzione **Riattiva** è disponibile solo se è stata selezionata l'opzione per la pianificazione dell'eliminazione dei dati di Advanced Automation (PSA) entro 30 giorni, come descritto nella procedura precedente.

3. Nella finestra di conferma visualizzata, fare clic su **Riattiva**.

Nota
Se non è stato completato in precedenza il processo di onboarding, viene visualizzata la schermata della procedura guidata di onboarding. Configurare le opzioni di Advanced Automation (PSA) pertinenti (consultare "Attivazione di Advanced Automation (PSA)" (pag. 203)).

Anche se il servizio Advanced Automation (PSA) è stato riattivato e la maggior parte delle impostazioni è stata ripristinata, è necessario eseguire manualmente le seguenti operazioni:

- Rivedere e aggiornare i ruoli Advanced Automation (PSA) per gli utenti del tenant.
- Rivedere e attivare le integrazioni della piattaforma di contabilità e di pagamento, se precedentemente in uso.
- Esaminare e configurare le integrazioni RMM, se precedentemente in uso. È necessario aggiornare tutte le integrazioni RMM attive per abilitare gli avvisi di terze parti per la sincronizzazione dei ticket.
- Rivedere e configurare i server di posta in arrivo e in uscita.
- Controllare le date di scadenza nei contratti e aggiornarle se necessario.
- Gli utenti del tenant potrebbero dover abilitare manualmente Outlook per i calendari.

Integrazioni

Questo capitolo fornisce le informazioni necessarie per individuare e attivare le integrazioni.

Le integrazioni offrono Cyber Protection di terze parti, gestione degli endpoint, gestione dei clienti, monitoraggio, analisi, ecc., insieme ai prodotti standard della console di Cyber Protect e, allo stesso tempo, offrono le nostre soluzioni tramite piattaforme software di terze parti. Attualmente oltre 200 integrazioni permettono di automatizzare le attività di routine, aumentando l'efficienza dei nostri partner e dei loro clienti.

Le integrazioni sono elencate nei cataloghi delle integrazioni.

Nota
Alcune integrazioni richiedono un client API per accedere alle interfacce di programmazione delle applicazioni (API).

Cataloghi delle integrazioni

Negli elenchi dei cataloghi delle integrazioni sono elencate le integrazioni disponibili:

- Il Catalogo delle applicazioni.
  Questo catalogo è disponibile al pubblico, tuttavia non è possibile attivare le integrazioni da questo catalogo.
  Se uno dei clienti del Partner identifica un'integrazione che intende utilizzare, dovrà contattare il Partner per attivarla.
- Cataloghi del data center.
  Questi cataloghi sono specifici del data center e da essi è possibile attivare direttamente le integrazioni.
  Gli amministratori del portale di gestione a livello Partner possono:
  - Visualizzare tutte le integrazioni distribuite nel data center.
  - Attivare tutte le integrazioni distribuite nel data center, sia per sé stessi che per i propri clienti.

  Gli amministratori del portale di gestione a livello cliente possono:
  - Vedere solo le integrazioni che lo sviluppatore dell'integrazione imposta esplicitamente come visibili per i clienti.
  - Attivare solo le integrazioni che lo sviluppatore dell'integrazione imposta esplicitamente come attivabili dai clienti.

    Nota
    L'amministratore del portale di gestione a livello Partner deve attivare l'integrazione a tale livello prima che possa essere attivata da un amministratore del portale di gestione a livello cliente.

Voci del catalogo

Le voci del catalogo sono costituite da due parti:

- La scheda del catalogo offre una panoramica dell'integrazione.
- La pagina dei dettagli del catalogo fornisce altre informazioni, come una descrizione completa delle funzionalità, schermate, video, un elenco delle funzionalità, i dettagli di contatto, i collegamenti alle risorse dell'integrazione, ecc.

Apertura del catalogo delle integrazioni del data center

Nei cataloghi delle integrazioni del data center (DC), passare il mouse sopra una scheda del catalogo per accedere a una breve descrizione del prodotto, il pulsante **Configura** e un collegamento **Per saperne di più**:

- Il collegamento **Per saperne di più**

  Ogni voce del catalogo delle integrazioni dispone di una pagina con i dettagli dell'integrazione, ad esempio una descrizione completa delle funzionalità, schermate, video, un elenco delle funzionalità, i dettagli di contatto, i collegamenti alle risorse dell'integrazione, ecc.

  Fare clic su questo collegamento per aprire la pagina dei dettagli dell'integrazione.
- Il pulsante **Configura**

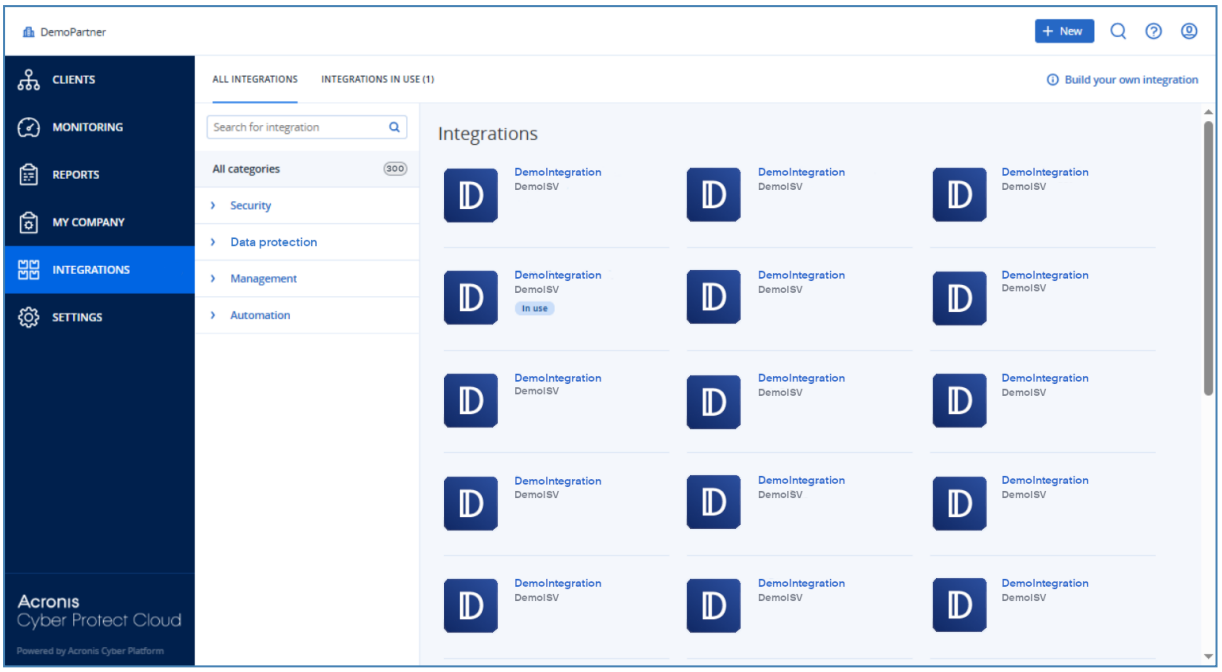
  Fare clic su questo pulsante per attivare l'integrazione.

Nota
Le schede del catalogo che rappresentano integrazioni inattive sono visualizzate in grigio e disabilitate.

Per aprire il catalogo delle integrazioni del data center

1. Aprire il portale di gestione.
2. Selezionare **Integrazioni** nel menu principale.

   Per impostazione predefinita, il sistema apre la scheda **Tutte le integrazioni**. Vengono visualizzate le schede del catalogo delle integrazioni attualmente disponibili nel data center.
3. [Facoltativo] Scegliere una categoria e inserire del testo nel campo di ricerca per filtrare le schede del catalogo.

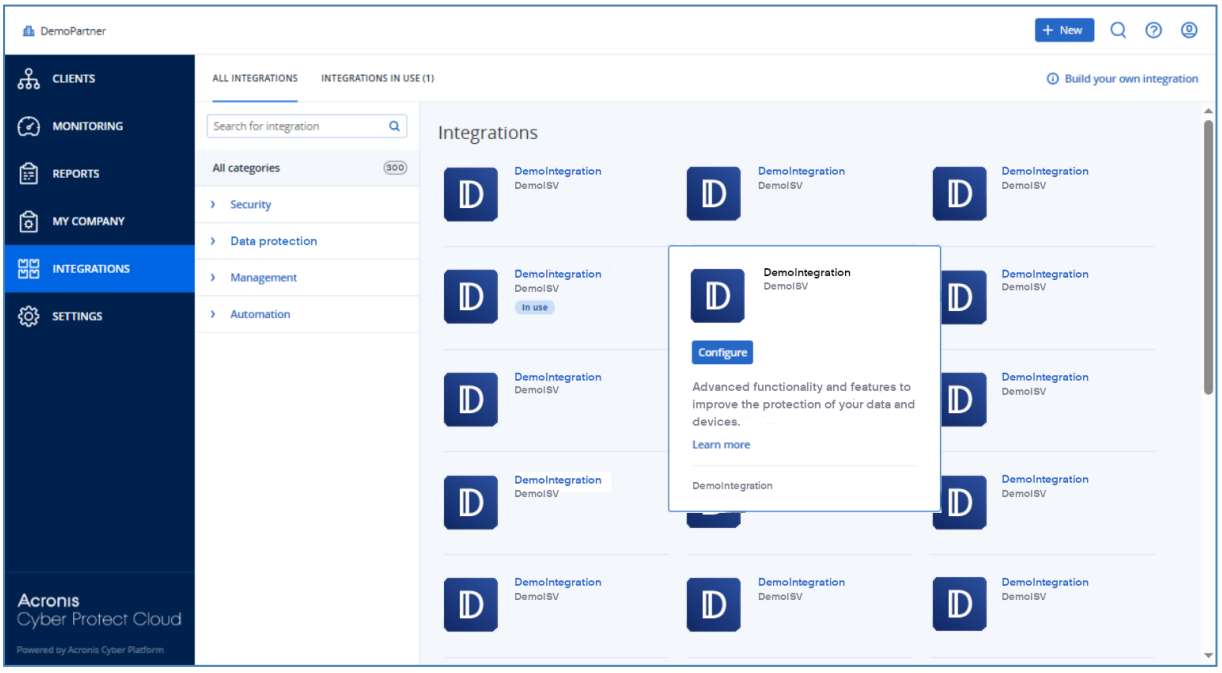


Apertura di una pagina dei dettagli dell'integrazione

Per aprire una pagina dei dettagli dell'integrazione

1. Aprire il catalogo delle integrazioni nel data center.
2. Individua la scheda del catalogo per l'integrazione.
3. Passare il mouse sulla scheda del catalogo.
4. Clicca su **Per saperne di più**.

Si apre la pagina dei dettagli dell'integrazione.

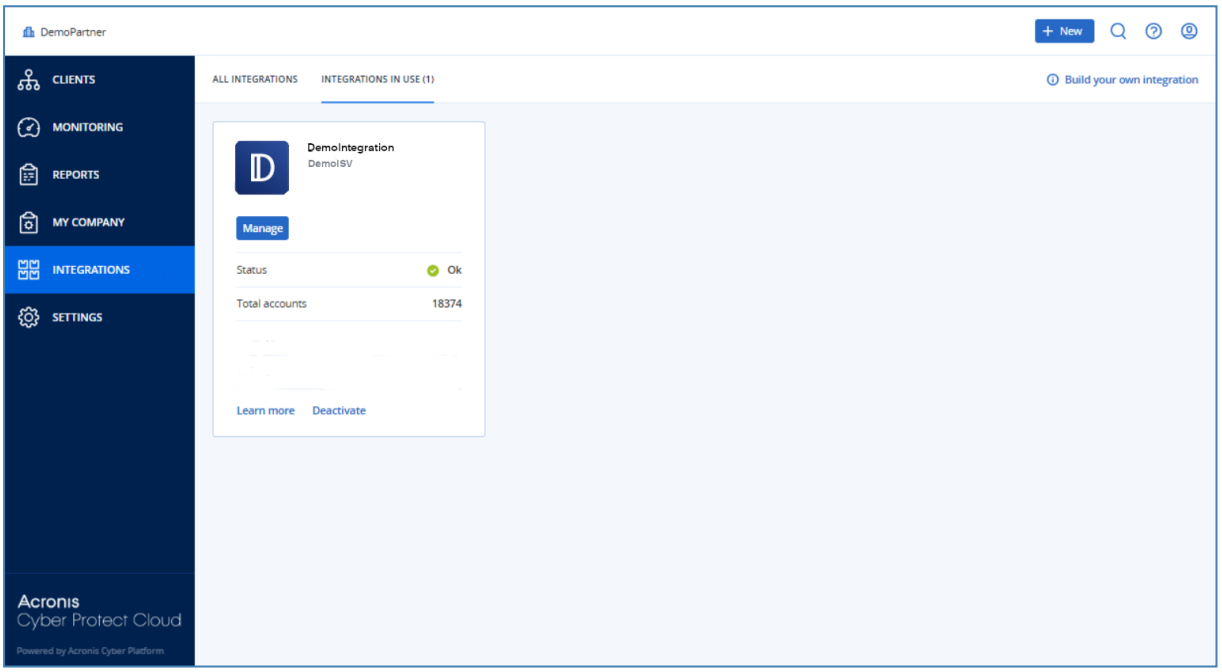


Visualizzazione delle integrazioni attivate

La scheda **Integrazioni in uso** del catalogo delle integrazioni visualizza una scheda per ogni integrazione attivata.

Per visualizzare le integrazioni attivate

1. Aprire il catalogo delle integrazioni nel data center.
2. Selezionare la scheda **Integrazioni in uso**.



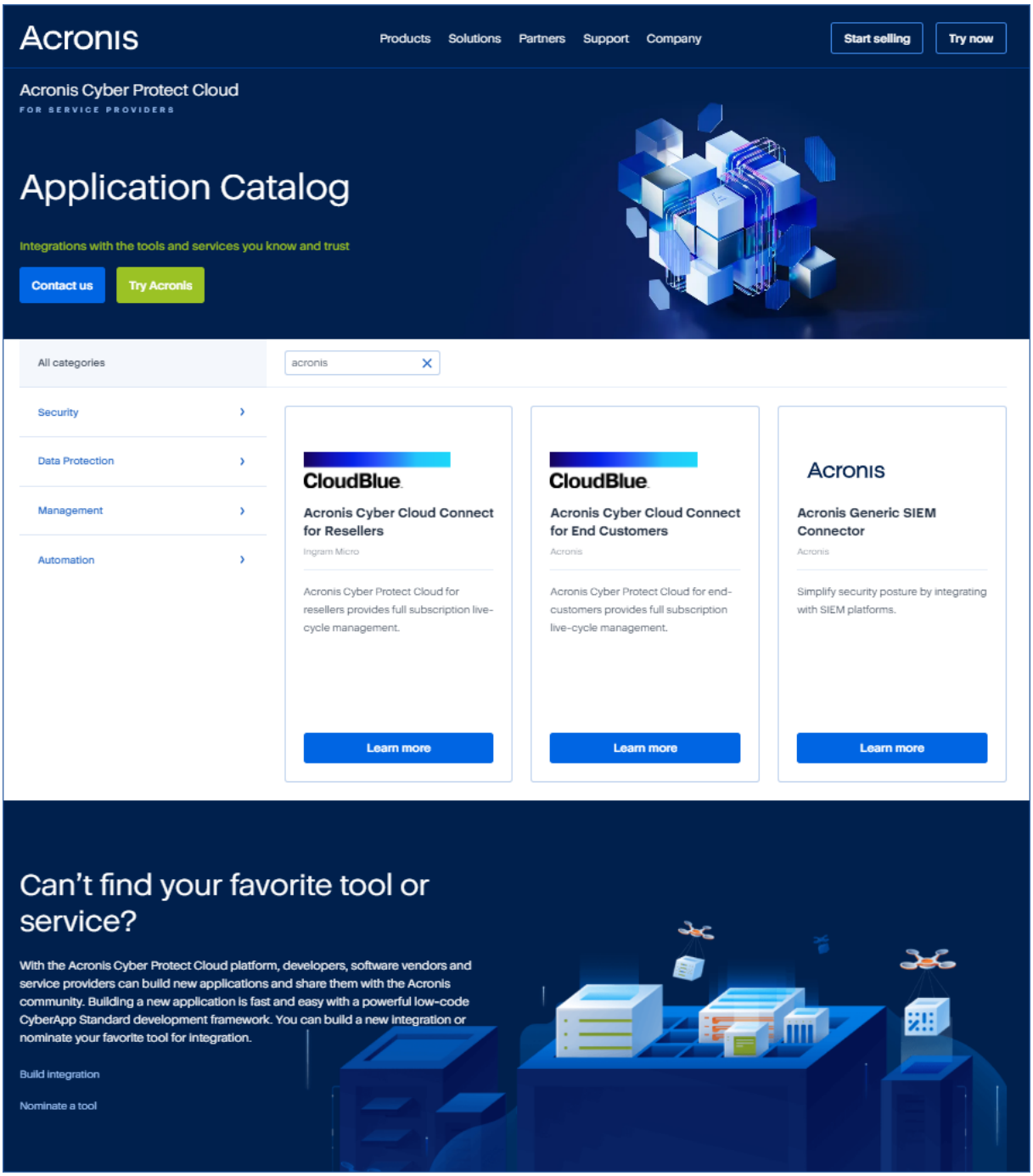
Apertura del catalogo delle applicazioni

Nel Catalogo delle applicazioni sono elencate tutte le integrazioni di Cyber Protect Cloud.

Nota
Il catalogo delle applicazioni è uno strumento di riferimento è non è possibile utilizzarlo per abilitare un'integrazione.
È invece possibile attivare un'integrazione dal catalogo delle integrazioni del data center nel portale di gestione.

Per aprire il Catalogo delle applicazioni

1. Visitare solutions.acronis.com.
   La vista iniziale è una griglia di tutte le schede del catalogo.
2. [Facoltativo] Scegliere una categoria e inserire del testo nel campo di ricerca per filtrare le schede del catalogo.



Apertura di una pagina dei dettagli dell'integrazione

Ogni voce del catalogo dispone anche di una pagina con i dettagli dell'integrazione, ad esempio una descrizione completa delle funzionalità, schermate, video, un elenco delle funzionalità, i dettagli di contatto, i collegamenti alle risorse dell'integrazione, ecc.

Per aprire una pagina dei dettagli dell'integrazione

1. Visitare solutions.acronis.com.
2. Individuare la scheda del catalogo dell'integrazione a cui si è interessati.

3. Fare clic su **Per saperne di più** nella scheda del catalogo.

Some features might not be available in your data center yet.

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud

FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

← Back to integrations

Have a question or need help?

Acronis

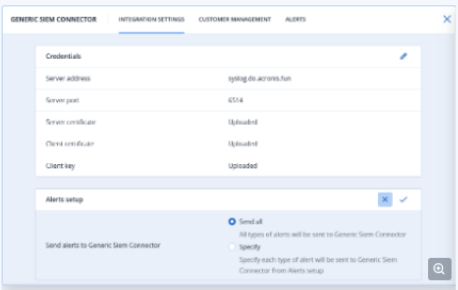
Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Website

Acronis Generic SIEM Connector

SIEM (Security Information and Event Management) platforms are used by many MSPs for security incident investigation and remediation, threat hunting, and compliance. Acronis Generic SIEM Connector allows MSPs to forward Acronis Cyber Protect Cloud alerts to any SIEM system that supports the CEF event format over SYSLOG for further correlation and analysis to reveal patterns of activity that may indicate an attempt of intrusion.

Integration Overview



Simplify security posture by integrating with SIEM platforms.

SIEMs empower MSPs security specialists to identify attack rout across the network and get visibility into compromised files. Now with Acronis Generic SIEM connector, MSPs will gain extra visibility into customers networks, will be able to search for threats across all managed workloads, and correlate events from both security and data protection applications, and run response actions.

Features

Support of core event format
Acronis supports core event format - CEF (Common Event Format), enabling MSPs to work with any SIEM that supports CEF format out of the box. Alerts are transferred to SIEM via syslog server.

Threat hunting across all managed companies
Integration allows MSPs to select which customer tenants in Acronis should send alerts to SIEM. Since alerts are sent to the same SIEM instance, it's possible to run correlation, threat hunting and perform investigation for all customers in the same console. It also empowers MSPs to search for threats, that were discovered on one workload in one customer tenant, in other customers environments.

Simple integration enablement
It's very easy to enable the integration by obtaining server and client certificates, establishing connection to the server and specifying the server port.

Select data you want to see
It is possible to select which alerts should be sent to SIEM. With this functionality, MSPs benefit from reducing the amount of sent to SIEM data and, therefore, lower SIEM invoice. MSPs can select and work only with the data that is necessary.

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build integration

Nominate a tool

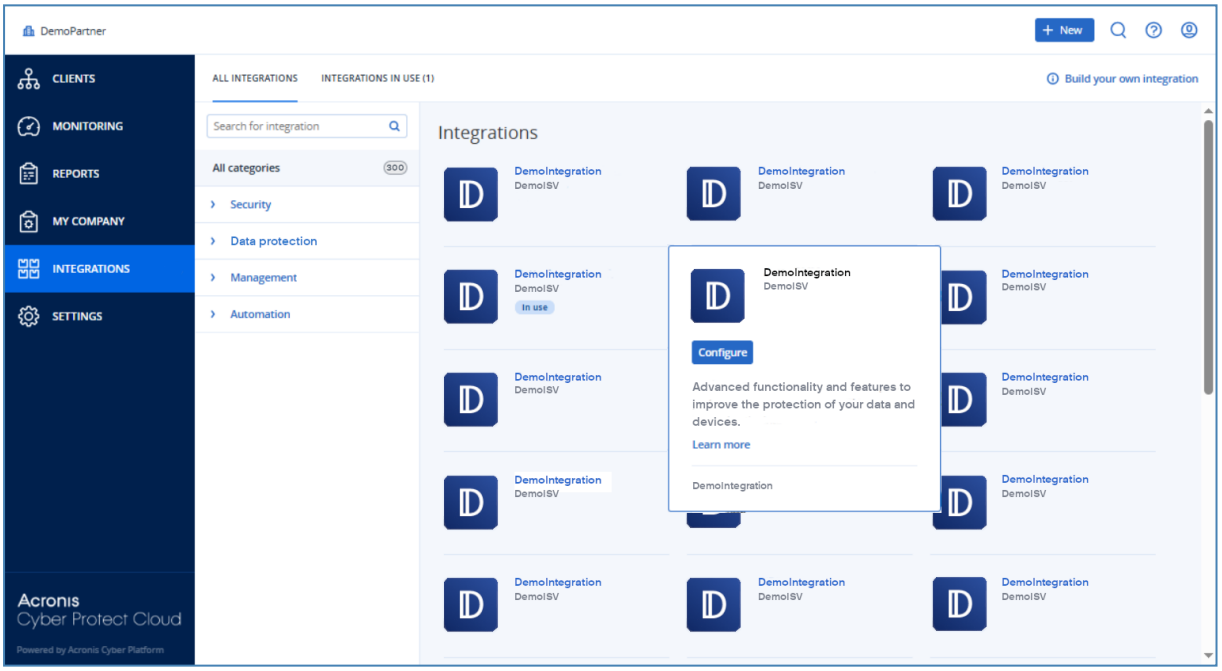
Engage with Acronis

Acronis © 2003–2024 Acronis International GmbH. Legal information | Privacy policy

Attivazione di un'integrazione

Per attivare un'integrazione

1. Aprire il catalogo delle integrazioni nel data center.
2. Individuare la scheda del catalogo relativa all'integrazione da attivare.
   Per filtrare le integrazioni:
   - [Facoltativo] Selezionare una categoria.
   - [Facoltativo] Immettere una stringa nel campo di ricerca.
3. Passare il mouse sulla scheda del catalogo.
4. Fare clic su **Configura**.
5. Seguire le istruzioni a video.

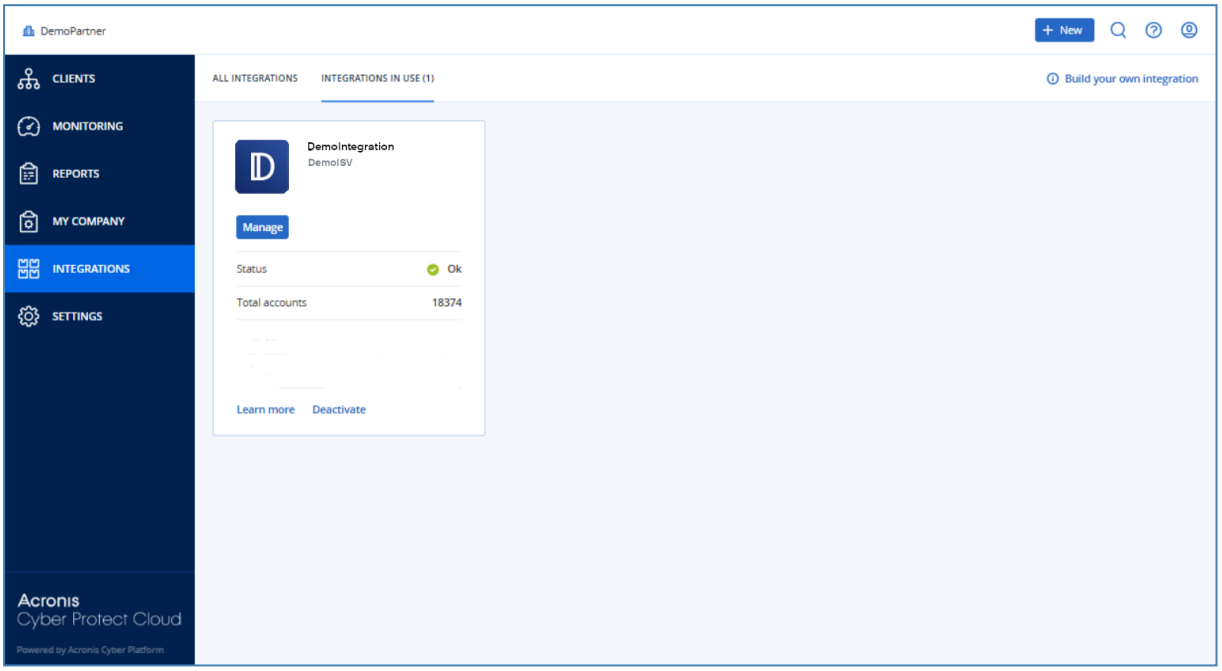


Configurazione di un'integrazione attiva

Per configurare un'integrazione attiva

1. Aprire il catalogo delle integrazioni nel data center.
2. Selezionare la scheda **Integrazioni in uso**.
3. Individuare la scheda del catalogo relativa all'integrazione da configurare.
4. Fare clic su **Gestisci**.
   Viene visualizzata la schermata di configurazione dell'integrazione.
5. Seguire le istruzioni visualizzate o consultare la documentazione di integrazione.

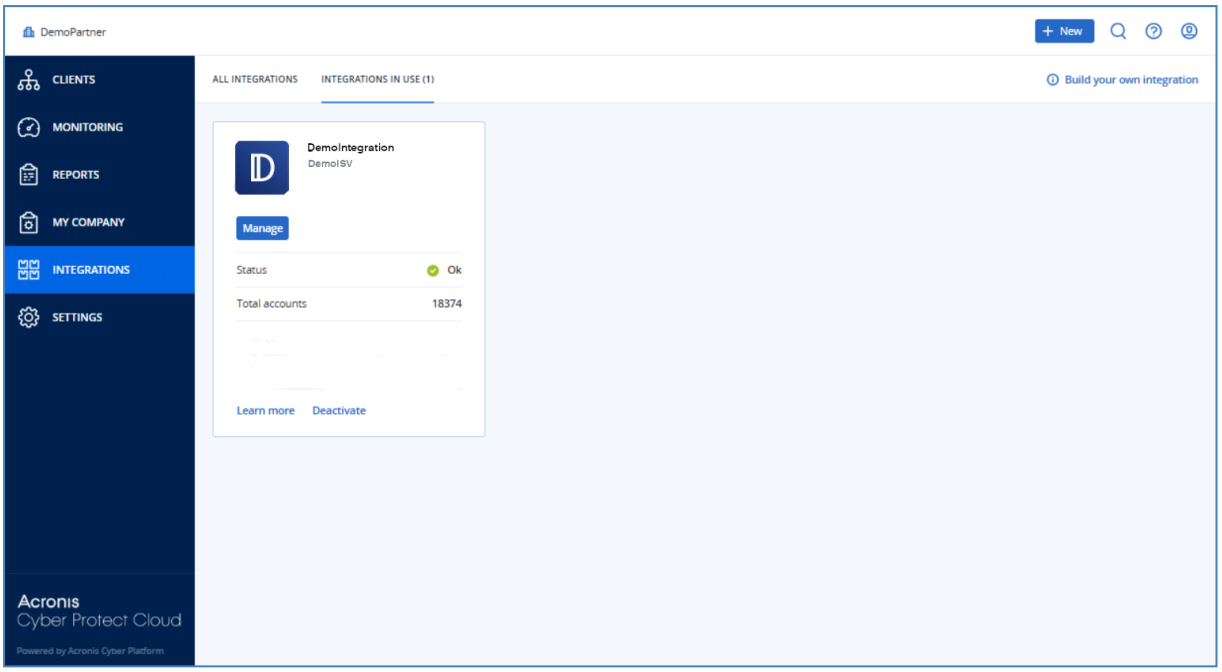
Nota
La documentazione è solitamente disponibile nella pagina dei dettagli del catalogo. Per ulteriori informazioni, vedere Apertura di una pagina dei dettagli dell'integrazione.



Disattivazione di un'integrazione attiva

Per disattivare un'integrazione

1. Aprire il catalogo delle integrazioni nel data center.
2. Selezionare la scheda **Integrazioni in uso**.
3. Individuare la scheda del catalogo dell'integrazione da disabilitare.
4. Fare clic su **Disattiva**.
5. Fare clic su **Elimina**.



Client API

Le integrazioni di sistema di terze parti possono utilizzare le interfacce di programmazione delle applicazioni (API). L'accesso alle API viene abilitato tramite i client API, parte integrante della struttura di autorizzazione OAuth 2.0 della piattaforma.

Un client API è uno speciale account della piattaforma che rappresenta il sistema della terza parte che deve effettuare l'autenticazione ed essere autorizzato per accedere ai dati della piattaforma e ai dati dei servizi. L'accesso del client API è limitato al tenant per il quale l'amministratore del portale di gestione ha creato il client e a eventuali tenant figlio.

Nota
Il client API eredita i ruoli di servizio dell'account dell'amministratore, che non possono essere modificati in un secondo momento. La modifica dei ruoli dell'account dell'amministratore o la sua disabilitazione non incide sul client.

Credenziali del client API

Le credenziali del client API sono composte dall'identificatore (ID) univoco e da un valore segreto. Tali credenziali non scadono e non possono essere utilizzate per accedere al portale di gestione o a qualsiasi altra console di servizio.

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

Flusso del client API

1. Un amministratore del portale di gestione crea un client API.
2. Un amministratore abilita il flusso di credenziali del client OAuth 2.0 nel sistema della terza parte.
3. 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 API alla piattaforma, utilizzando l'autorizzazione API.
4. La piattaforma genera e restituisce un token di sicurezza, una stringa crittografata univoca assegnata a questo client specifico.
5. Il sistema della terza parte deve aggiungere questo token a tutte le richieste API.

Nota
Il token di sicurezza evita di dover passare le credenziali del client con le richieste API.
Per ulteriore sicurezza, il token scade dopo due ore.
Al termine di questo periodo, tutte le richieste API effettuate con il token scaduto non avranno esito positivo e il sistema dovrà ottenere un nuovo token dalla piattaforma.

Creazione di un client API

Per creare 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, il client API è impostato sullo stato predefinito **Attivo**.
5. Copiare e salvare l'ID e il valore del segreto del client API e l'URL del data center. Saranno necessari durante l'abilitazione del flusso di credenziali del client OAuth 2.0 nel sistema di terzi.

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

6. Fare clic su **Fine**.

Reimpostazione del valore segreto di un client API

In caso di perdita del valore segreto del client API, è possibile generarne uno nuovo. L'ID del client e l'URL del data center non cambiano.

Importante
Se si reimposta il valore segreto, tutti i token di sicurezza assegnati al client scadranno immediatamente e le richieste API effettuate con questi token non avranno esito positivo.

Per reimpostare il 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. Fare clic su **Avanti** per confermare la decisione.
6. Copiare e salvare il nuovo valore segreto del client API.

   Nota
   Per ragioni di sicurezza, il valore segreto viene visualizzato solo una volta. In caso di perdita, non è possibile recuperare questo valore, che può tuttavia essere ripristinato ripetendo i passaggi indicati.

7. Fare clic su **Fine**.

Disabilitazione di un client API

È possibile disabilitare i client API. Se disabilitati, le richieste API che utilizzano i token di sicurezza assegnati al client non avranno esito positivo, ma i token non scadranno immediatamente.

Nota
La disabilitazione del client non ha effetto sulla scadenza dei token.

È possibile riabilitare il client API in qualsiasi momento.

Per disabilitare 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.

Abilitazione di un client API disabilitato

Se si abilita un client API precedentemente disabilitato, le richieste API che utilizzano i token di sicurezza assegnati al client avranno esito positivo **se tali token non sono ancora scaduti**.

Per abilitare 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 API cambia in **Attivo**.

Eliminazione di un client API

Se si elimina un client API, tutti i token di sicurezza assegnati a tale client scadranno immediatamente. Le richieste API che utilizzano tali token non avranno esito positivo.

Importante
Non è possibile recuperare un client eliminato.

Per eliminare 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.

Creazione di un'integrazione

Se si dispone di dati o servizi da integrare con Cyber Protect Cloud, è possibile creare una CyberApp nativa utilizzando il Vendor Portal o le chiamate API .

CyberApp

Vendor Portal è una piattaforma online che consente ai fornitori di software di terze parti di integrare in modo nativo prodotti e servizi in Cyber Protect Cloud, in conformità alle best practice di CyberApp Standard. Le integrazioni del Vendor Portal sono denominate CyberApp.

Nota
Per ulteriori informazioni sulle CyberApp e sul Vendor Portal, consultare la Guida all'integrazione.

Integrazioni API

È disponibile un set completo di API per le integrazioni.

Nota

Per ulteriori informazioni sulle API, consultare il capitolo sulle API della piattaforma della Guida all'integrazione.

Integrazione di Cyber Protect Cloud 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.
   Poiché RabbitMQ include funzionalità Single Sign-On (SSO), è possibile utilizzare le credenziali personali di VMware Cloud Director per accedere alla console di Cyber Protect.
   In Cyber Protect Cloud versione 23.05 (rilasciata a maggio 2023) e nelle precedenti, RabbitMQ viene utilizzato anche per sincronizzare le modifiche all'ambiente VMware Cloud Director in Cyber Protect Cloud.
2. Distribuzione di un agente di gestione.
   Durante il deployment dell'agente di gestione, viene installato anche un plug-in per VMware Cloud Director. Questo plug-in aggiunge Cyber Protection all'interfaccia utente di VMware Cloud Director.
   L'agente di gestione associa 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.

3. 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 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. 43).

  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.
- Se per il tenant è abilitata l'autenticazione a due fattori, è necessario utilizzare un account di amministratore Partner contrassegnato come account di servizio. In caso contrario, l'agente non sarà in grado di autenticarsi su Cyber Protect Cloud.

  Si consiglia di utilizzare un account dedicato per l'agente. Per ulteriori informazioni su come creare un account di servizio, consultare "Per convertire un account utente in un account di servizio" (pag. 63).
- 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 di Cyber Protect viene visualizzata in una nuova scheda.

Requisiti software

Versioni di VMware Cloud Director supportate

VMware Cloud Director 10.4 e 10.5 richiedono il broker dei messaggi RabbitMQ. Per ulteriori informazioni, vedere "Configurazione del broker dei messaggi di RabbitMQ" (pag. 389). Dopo l'aggiornamento a VMware Cloud Director 10.6, è necessario aggiornare gli agenti di gestione e backup alle versioni più recenti. Per ulteriori informazioni, vedere "Aggiornamento degli agenti" (pag. 397).

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.

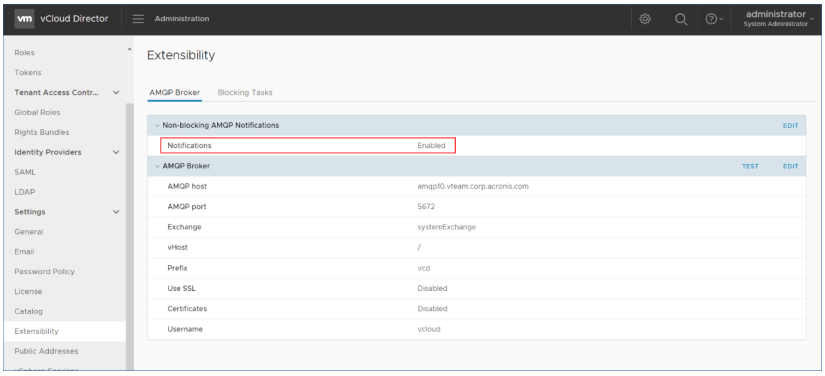
Configurazione del broker dei messaggi di RabbitMQ

Questa procedura dipende dalla versione di Cyber Protect Cloud. Per la versione 23.06 (rilasciata a giugno 2023) e per quelle successive, viene utilizzata una procedura semplificata.

Per configurare RabbitMQ

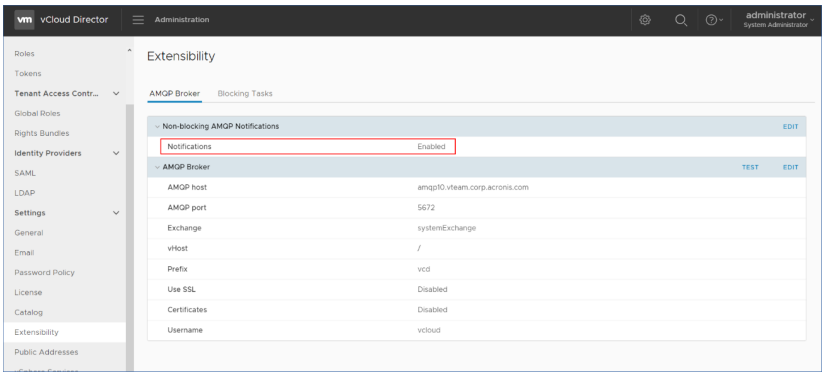
Per la versione 23.06 e successive

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**.

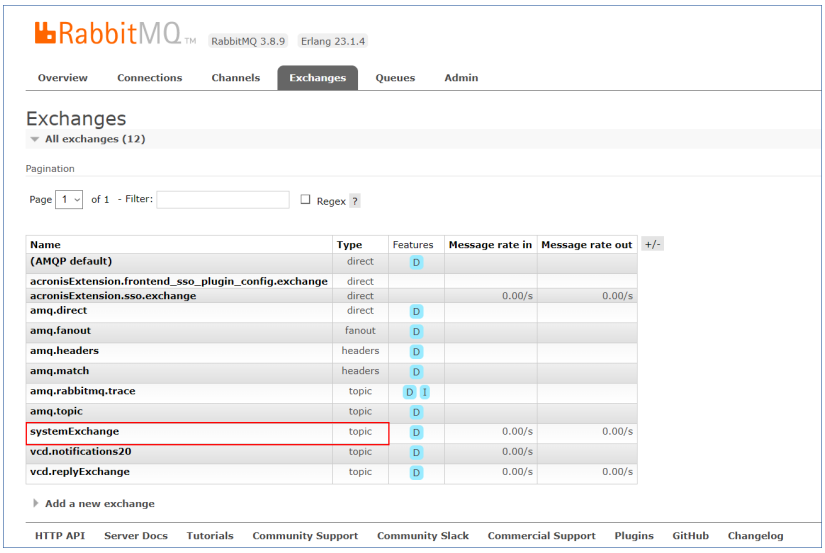


Per la versione 23.05 e precedenti

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 e pubblicazione del plug-in per VMware Cloud Director

Il plug-in per VMware Cloud Director viene installato automaticamente quando si installa l'agente di gestione.

È tuttavia necessario pubblicare manualmente il plug-in nei tenant che utilizzeranno Cyber Protection.

Per pubblicare il plug-in per VMware Cloud Director

1. Accedere al portale del provider VMware Cloud Director come amministratore di sistema.
2. Nel menu di navigazione, selezionare **Customize Portal**.
3. Nella scheda **Plugins**, in **Cyber Protection** selezionare il plug-in e quindi fare clic su **Publish**.

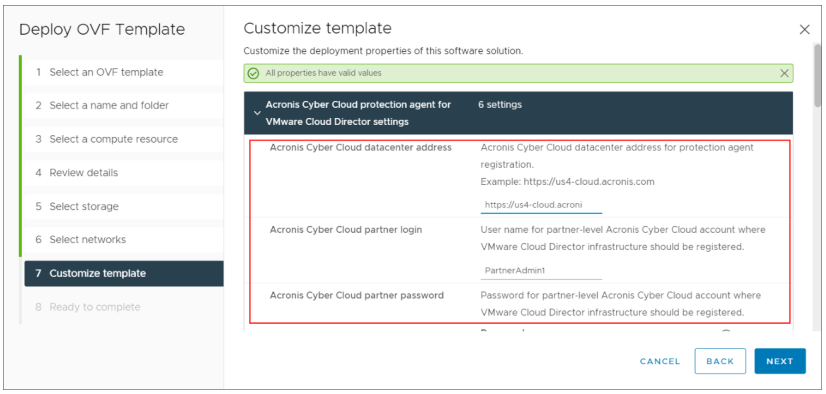
4. Configurare l'ambito della pubblicazione:
   a. Nella sezione **Scope to**, selezionare solo la casella di controllo **Tenant**.
   b. Nella sezione **Publish to**, selezionare **All tenants** per abilitare il plug-in per tutti i tenant esistenti e futuri, o selezionare i singoli tenant per i quali abilitare il plug-in.
5. Fare clic su **Salva**.
6. Fare clic su **Trust**.

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. Nell'elenco a discesa **Canale di release** selezionare la versione dell'agente. Sono disponibili le seguenti opzioni:
   - **Più recente**: la versione più recente disponibile.
   - **Versione stabile precedente**: la versione più recente e stabile dell'agente di protezione dalle versioni precedenti.
4. Fare clic sul link **Agente di gestione** e scaricare il file ZIP.
5. Estrarre il file del modello dell'agente di gestione `vCDManagementAgent.ovf` e il file del disco rigido virtuale `vCDManagementAgent-disk1.vmdk`.
6. 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.

7. Nella procedura guidata **Distribuisci modello OVF**, configurare l'agente di gestione impostando quanto segue:



   a. URL del data center Cyber Protect Cloud. Ad esempio, `https://us5-cloud.example.com`.
   b. Login e password dell'amministratore del partner.

Nota
Se per il tenant è abilitata l'autenticazione a due fattori, è necessario utilizzare un account di amministratore Partner contrassegnato come account di servizio. In caso contrario, l'agente non sarà in grado di autenticarsi su Cyber Protect Cloud.
Si consiglia di utilizzare un account dedicato per l'agente. Per ulteriori informazioni su come creare un account di servizio, consultare "Per convertire un account utente in un account di servizio" (pag. 63).

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. 87).
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**.

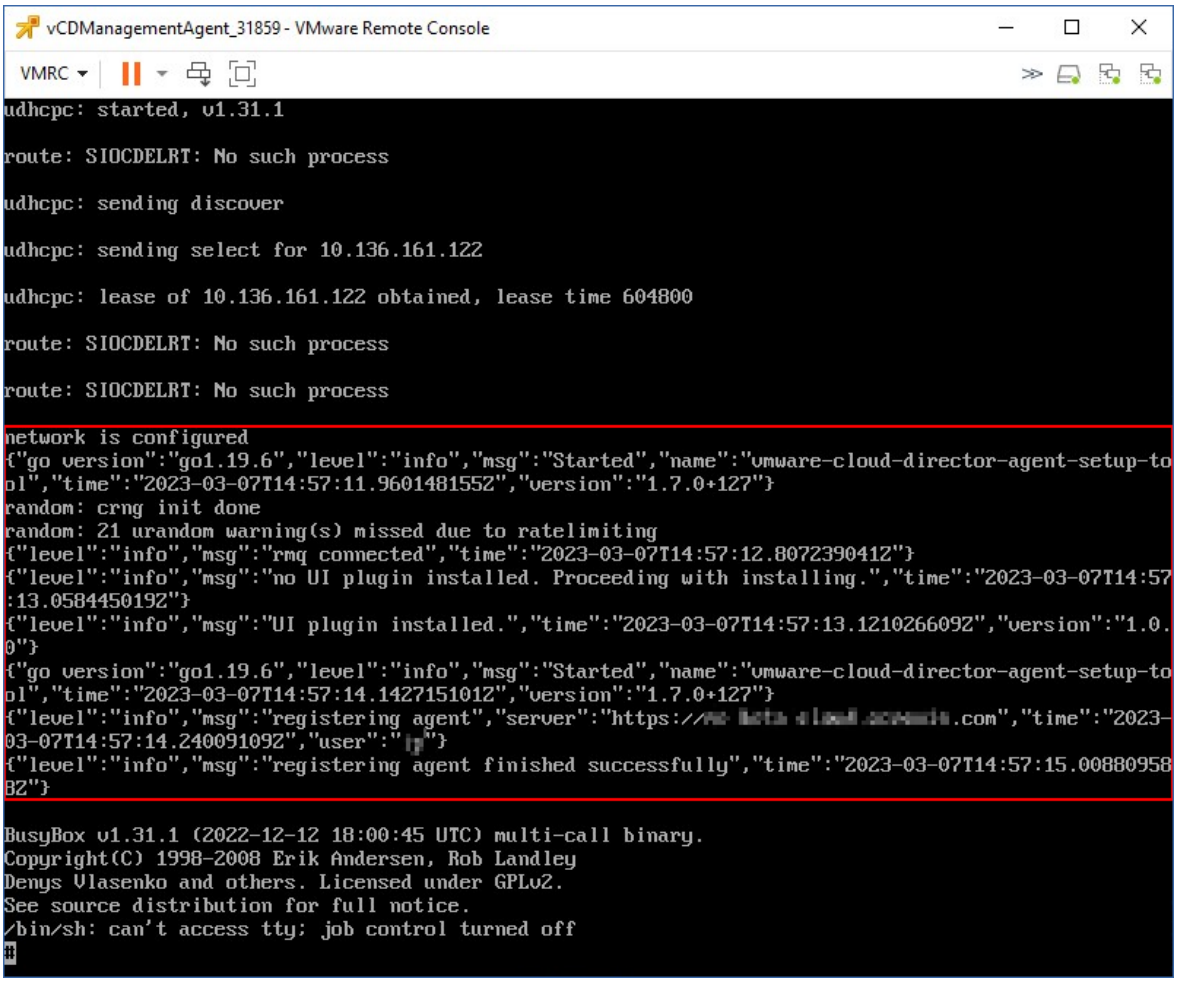
Nota
La modalità di fatturazione selezionata verrà applicata a tutti i nuovi tenant cliente che verranno creati.

e. Parametri di VMware Cloud Director: indirizzo dell'infrastruttura, login dell'amministratore di sistema e password.
f. [Se utilizzi VMware Cloud Director 10.5 o versioni precedenti] Parametri di RabbitMQ: accesso e password dell'amministratore.
g. La password per l'utente `root` sulla virtual machine con l'agente.
h. 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**.

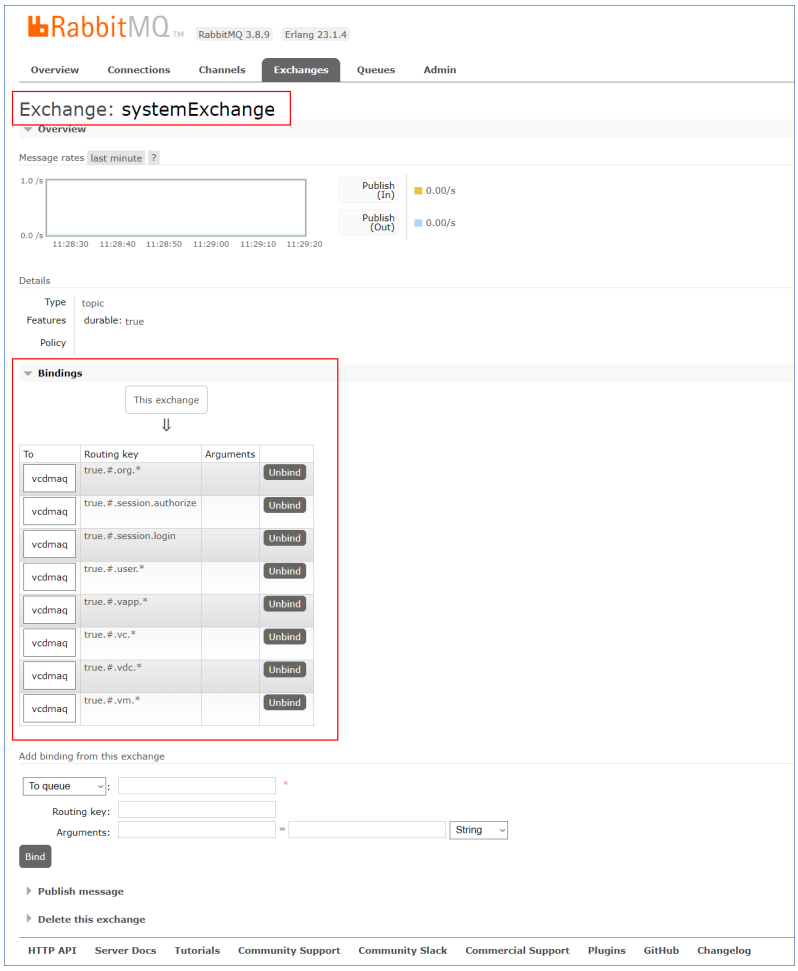
Nota
Verificare che le impostazioni di rete consentano all'agente di gestione di accedere sia all'ambiente VMware Cloud Director sia al data center Cyber Protect Cloud.

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.

8. [Facoltativo] Nel client vSphere, aprire la console della virtual machine con l'agente di gestione e verificare la configurazione.



9. 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**.



Passaggi successivi

Se la build dell'agente è 24.12.39185 o versione successiva e l'ambiente è VMware vSphere 8.x o versione successiva, è possibile abilitare la modalità conforme a FIPS. Consultare "Abilitazione della modalità conforme a FIPS per VMware Cloud Director" (pag. 396).

Installazione degli agenti di backup

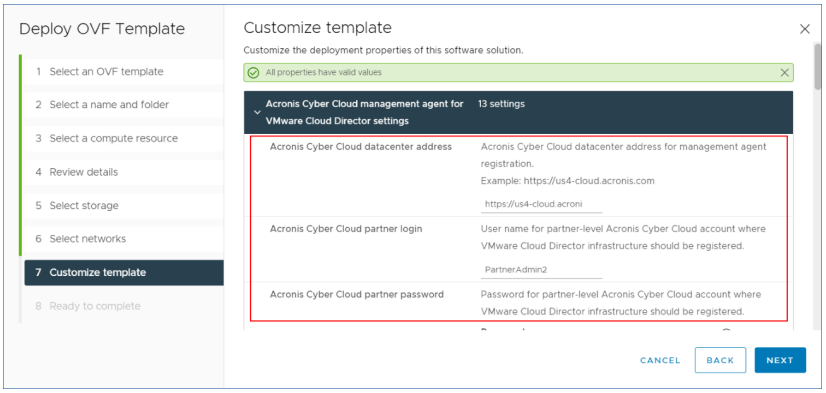
1. Accedere al portale di gestione come amministratore del partner.
2. Passare a **Impostazioni** > **Posizione**, quindi fare clic su **Aggiungi VMware Cloud Director**.
3. Nell'elenco a discesa **Canale di release** selezionare la versione dell'agente. Sono disponibili le seguenti opzioni:
   - **Più recente**: la versione più recente disponibile.
   - **Versione stabile precedente**: la versione più recente e stabile dell'agente di protezione dalle versioni precedenti.
4. Fare clic sul link **Agente di backup** e scaricare il file ZIP.
5. Estrarre il file del modello dell'agente di backup `vCDCyberProtectAgent.ovf` e il file del disco rigido virtuale `vCDCyberProtectAgent-disk1.vmdk`.
6. 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 CPU; è in grado di eseguire fino a 5 backup o operazioni di ripristino contemporaneamente.

Per elaborare più attività o distribuire il traffico di backup e ripristino, è necessario distribuire agenti aggiuntivi nello stesso host. In alternativa, per evitare problemi causati dalla memoria insufficiente, è consigliabile assegnare 16 GB di RAM e 4 vCPU all'agente esistente.

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".

7. Nella procedura guidata **Distribuisci modello OVF**, configurare l'agente di backup impostando quanto segue:



a. URL del data center Cyber Protect Cloud. Ad esempio, `https://us5-cloud.example.com`.

b. Login e password dell'amministratore del partner.

   Se per il tenant è abilitata l'autenticazione a due fattori, è necessario utilizzare un account di amministratore Partner contrassegnato come account di servizio. In caso contrario, l'agente non sarà in grado di autenticarsi su Cyber Protect Cloud.

   Si consiglia di utilizzare un account dedicato per l'agente. Per ulteriori informazioni su come creare un account di servizio, consultare "Per convertire un account utente in un account di servizio" (pag. 63).

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. La password per l'utente `root` sulla virtual machine con l'agente.

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

   Per impostazione predefinita, è abilitata 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.

f. Limite di download: la velocità massima di download (in Kbps), che definisce la velocità di lettura del cloud storage durante un'operazione di ripristino. Il valore predefinito è 0 - Senza limiti.
g. Limite di upload: la velocità massima di upload (in Kbps), che definisce la velocità di scrittura del cloud storage 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.

8. Nel client vSphere, verificare che le opzioni **Host** e **Storage vMotion** siano disabitate per la virtual machine con l'agente di backup.

Passaggi successivi

Se la build dell'agente è 24.12.39185 o versione successiva e l'ambiente è VMware vSphere 8.x o versione successiva, è possibile abilitare la modalità conforme a FIPS. Consultare "Abilitazione della modalità conforme a FIPS per VMware Cloud Director" (pag. 396).

Abilitazione della modalità conforme a FIPS per VMware Cloud Director

La modalità conforme a FIPS può essere abilitata per le build dell'agente 24.12.39185 e successive, in VMware vSphere 8.x e successive. In questa modalità, l'agente di backup utilizza una libreria crittografica conforme a FIPS 140-2 per tutte le operazioni di crittografia. Per ulteriori informazioni, consultare Modalità conforme a FIPS.

Importante
Per funzionare come previsto, la modalità FIPS deve essere abilitata sia sull'agente di gestione che sugli agenti di backup.

Per abilitare la modalità conforme a FIPS per gli agenti Cyber Protect in un'istanza di Cloud Director

1. Nel client vSphere, individuare la virtual machine dell'agente di gestione vCD, aprire la console remota e quindi eseguire il comando seguente:

```
fips-mode-setup --enable
```

2. Tornare al client vSphere, individuare la virtual machine vCD dell'agente Cyber Protect su cui abilitare la modalità conforme a FIPS, aprire la console remota e quindi eseguire il comando seguente:

```
fips-mode-setup --enable
```

3. Eseguire il comando su tutte le altre virtual machine vCD dell'agente Cyber Protect Agent in cui abilitare la modalità conforme a FIPS.

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.
6. 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.

7. Distribuire una virtual machine con il nuovo agente di backup utilizzando i file `vCDCyberProtectAgent.ovf` e `vCDCyberProtectAgent-disk1.vmdk` più recenti.
8. Configurare l'agente di backup utilizzando le stesse impostazioni dell'agente precedente.
9. Eliminare la virtual machine con l'agente di backup obsoleto.

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 e pubblicazione del plug-in per VMware Cloud Director" (pag. 390).

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`

Accesso alla console di Cyber Protect

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. 398).

Gli amministratori possono accedere alla console personalizzata di Cyber Protect 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 di Cyber Protect , 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 di Cyber Protect dei tenant dei propri clienti e gestire le attività di backup e ripristino per loro conto.

Esecuzione del backup e del ripristino

Creazione di un piano di protezione

Per configurare le impostazioni di backup, è necessario creare un piano di protezione.

È possibile applicare un piano di protezione a più sistemi e più piani di protezione allo stesso sistema.

Limitazioni

- Sono supportati solo i backup dell'intero sistema. Non è possibile eseguire il backup di singoli dischi o volumi.
- I filtri file (inclusioni/esclusioni) non sono supportati.
- Il cloud storage è l'unica posizione di backup disponibile. Lo storage viene configurato nelle impostazioni dell'agente di gestione e non è modificabile dagli utenti nel piano di protezione.
- Sono supportati i seguenti schemi di backup: **Sempre incrementale (a file singolo)**, **Sempre completo** e **Settimanale completo, Giornaliero incrementale**.
- È supportata la pulizia solo dopo il backup.

Per creare un piano di protezione

1. Nella console di Cyber Protect, passare a **Dispositivi** > **VMware Cloud Director**.
2. Selezionare i sistemi da proteggere, quindi fare clic su **Proteggi**.
3. [Se sono già presenti piani applicati] Fare clic su **Aggiungi piano**.

4. Fare clic su **Crea piano**.
5. In **Crittografia**, configurare le impostazioni di crittografia.
6. [Facoltativo] Per rinominare il piano di protezione, fare clic sull'icona a matita, quindi inserire il nuovo nome.
7. [Facoltativo] Per modificare lo schema o la programmazione del backup, fare clic su **Pianificazione**, quindi configurare le impostazioni.
8. [Facoltativo] Per modificare le regole di conservazione, fare clic su **Numero da conservare**, quindi configurare le impostazioni.
9. [Facoltativo] Per modificare le opzioni di backup, fare clic su **Opzioni di backup**, quindi configurare le impostazioni.
10. Fare clic su **Applica**.

Ripristino di una macchina

È possibile ripristinare un backup sulla virtual machine originale o su una nuova virtual machine.

Limitazioni

- Non è supportato il ripristino a livello di file.
- È possibile ripristinare i backup su nuove virtual machine con VMware Cloud Director 10.4 e versioni successive.

  Per ripristinare un backup su una nuova virtual machine, il backup deve essere creato con la versione dell'agente 24.02 o successiva. È possibile controllare la versione dell'agente nel file `ProductVersion.conf`, che si trova nella directory `/etc` della virtual machine con l'agente.
- Dopo aver ripristinato un backup su un nuovo sistema, quest'ultimo viene visualizzato in **Dispositivi** > **VMware Cloud Director** > Organizzazione > Datacenter virtuale > **VM autonome**. Non è possibile selezionare una vApp specifica come destinazione di ripristino.

Per ripristinare un sistema

Nel sistema di origine

1. Nella console di Cyber Protect, selezionare il punto di ripristino in uno dei modi seguenti:
   - Passare a **Dispositivi** > **VMware Cloud Director**, selezionare un sistema con backup, fare clic su **Ripristino**, quindi selezionare un punto di ripristino.
   - Passare a **Dispositivi** > **VMware Cloud Director**, selezionare un archivio di backup, fare clic su **Mostra backup**, quindi selezionare un punto di ripristino.
2. Fare clic su **Ripristina sistema**.
3. Fare clic su **Avvia ripristino**.

In un nuovo sistema

1. Nella console di Cyber Protect, selezionare il punto di ripristino in uno dei modi seguenti:
   - Passare a **Dispositivi** > **VMware Cloud Director**, selezionare un sistema con backup, fare clic su **Ripristino**, quindi selezionare un punto di ripristino.
   - Passare a **Dispositivi** > **VMware Cloud Director**, selezionare un archivio di backup, fare clic su **Mostra backup**, quindi selezionare un punto di ripristino.
2. Fare clic su **Ripristina sistema**.
3. Fare clic su **Macchina di destinazione**, e quindi selezionare **Nuova macchina**.
4. Selezionare il datacenter virtuale per il nuovo sistema.
5. Specificare il nome del nuovo sistema.
   Per impostazione predefinita, viene suggerito il nome del sistema originale.
6. Fare clic su **OK**.
7. [Facoltativo] Fare clic su **Impostazioni MV** per modificare una delle seguenti impostazioni per il nuovo sistema, quindi fare clic su **OK**:
   - Dimensione RAM
   - Numero di processori virtuali
   - Numero di core per socket
   - Profilo di storage
   - Adattatori di rete e reti assegnate
8. [Facoltativo] Fare clic su **Mappatura disco** per modificare la mappatura del disco o il profilo di storage di un disco, quindi fare clic su **OK**.
9. Fare clic su **Avvia ripristino**.

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.

Utilizzo del Partner Portal

Il Partner Portal è progettato per i service provider, i distributori e i rivenditori che hanno aderito al #CyberFit Partner Program.

Dal portale è possibile accedere ai contenuti, agli strumenti e alla formazione che mette a disposizione.

Per iniziare a utilizzare il Partner Portal

1. Accedere al Partner Portal con uno dei seguenti metodi:
   - Nell'angolo in basso a sinistra del portale di gestione, fare clic su **Diventa un partner**.
   - Visitare il sito web del Partner Portal.
2. Registrare l'azienda al programma per i Partner.
3. I dettagli per l'accesso vengono inviati via e-mail.

Ruoli del Partner Portal

Il Partner Portal include una serie di ruoli che possono essere assegnati agli utenti come necessario.

La tabella seguente descrive ogni ruolo disponibile e i diritti assegnati a ciascun ruolo nel Partner Portal:

Ruolo	Descrizione
Di base	Il ruolo predefinito applicato a tutti gli utenti. Questo ruolo concede l'accesso alle funzionalità essenziali del Partner Portal, inclusi Dashboard, Partner Program, Hub contenuti e Formazione.
Formazione	Gli utenti con questo ruolo possono accedere ai materiali di formazione. Altre funzionalità del Partner Portal non saranno disponibili per questi utenti.
Marketing	Questo ruolo concede l'accesso alle funzionalità del Partner Portal necessarie per un addetto al marketing, inclusi Dashboard, Partner Program, Marketing, Hub contenuti, Formazione, Stato del datacenter e Gestione del database.
Vendite	Gli utenti con questo ruolo possono accedere alle funzionalità del Partner Portal necessarie per un addetto alle vendite, come Dashboard, Partner Program, Vendite, Hub contenuti, Formazione, Stato del datacenter e Gestione del database.
Vendite e marketing	Questo ruolo concede l'accesso alle funzionalità necessarie del Partner Portal per uno specialista delle vendite e del marketing, come Dashboard, Partner Program, Vendite, Marketing, Hub contenuti, Formazione, Stato del datacenter e Gestione del database.
Amministratore	Gli amministratori possono accedere a tutte le funzionalità del Partner Portal, inclusi Dashboard, Partner Program, Vendite, Marketing, Hub contenuti, Formazione, Stato del datacenter e Gestione del database. Inoltre, possono gestire le autorizzazioni per gli utenti Partner e modificare le informazioni sull'azienda.

Indice

S

W