Cyber Protect Cloud

24.03

Anleitung für Partner-Administratoren

REVISION: 11.04.2024

Inhaltsverzeichnis

Über dieses Dokument

Dieses Dokument richtet sich an Partner-Administratoren, die Cyber Protect Cloud einsetzen wollen, um ihren Kunden bestimmte Services anzubieten.

Dieses Dokument beschreibt, wie die in Cyber Protect Cloud verfügbaren Services mithilfe des Management-Portals eingerichtet und verwaltet werden.

Über Cyber Protect

Cyber Protect ist eine Cloud-Plattform, die es Service-Providern, Resellern und Distributoren ermöglicht, ihren Partnern und Kunden bestimmte Data Protection-Services anzubieten.

Die Services werden auf Partnerebene bereitgestellt und können dann über verschiedene Ebenen für Kundenfirmen und Endbenutzer angeboten werden.

Die Verwaltung der Services erfolgt über Webapplikationen, die **Service-Konsolen** genannt werden. Die Verwaltung von Mandanten und Benutzerkonten erfolgt über eine Webapplikation, die **Management-Portal** genannt wird.

Administratoren können mit dem Management-Portal:

- Die Nutzung der Services überwachen und auf die Service-Konsolen zugreifen
- Mandanten verwalten
- Benutzerkonten verwalten
- Services und Quotas für Mandanten konfigurieren
- Storages verwalten
- Branding verwalten
- Berichte über die Nutzung der Services generieren

Cyber Protect Services

Dieser Abschnitt beschreibt die Funktionssätze, die im März 2021 mit dem neuen Abrechnungsmodell eingeführt wurden. Weitere Informationen über die Vorteile des neuen Abrechnungsmodells finden Sie im Cyber Protect Datenblatt.

Folgende Services und Funktionssätze sind in Cyber Protect Cloud verfügbar:

- **Cyber Protect**
  - **Schutz** – umfassende Cyber Protection mit Sicherheits- und Verwaltungsfunktionen, die bereits im Basisprodukt enthalten sind, sowie optionale Disaster Recovery-, Backup- & Recovery-, Automatisierungs- und Email Security-Fähigkeiten, die auf Basis eines Pay-as-you-go-Modells (also nutzungsabhängig) verfügbar sind. Diese Funktionalität kann mit Advanced Protection-Paketen erweitert werden, für die dann zusätzliche Gebühren anfallen.
    Advanced Protection-Pakete sind Zusammenstellungen aus einzigartigen Funktionen, die für komplexere Szenarien in bestimmten Funktionsbereichen ausgelegt sind – wie etwa Advanced Backup, Advanced Security + EDR und andere. Mit diesen Advanced-Paketen kann die Funktionalität erweitert werden, die der Standard Cyber Protect Service bietet.
    Weitere Informationen über die Advanced Protection-Pakete finden Sie im Abschnitt '"Advanced Protection-Pakete" (S. 158)'.
  - **File Sync & Share** – eine Lösung zum sicheren Teilen von Unternehmensinhalten von überall, zu jeder Zeit und mit jedem Gerät.

  - **Physischer Datenversand** – eine Lösung, mit der Sie Zeit und Internetübertragungen einsparen können, indem Sie Daten mit dem Cloud-Datacenter per Festplatten-Versand austauschen.
  - **Notary** – eine Blockchain-basierte Lösung, mit der Sie die Authentizität von geteilten Inhalten sicherstellen können.
- **Cyber Infrastructure SPLA**

Im Management-Portal können Sie auswählen, welche Services und Funktionssätze für Ihre Mandanten verfügbar sein sollen. Die Konfiguration erfolgt pro Mandant, wenn Sie einen Mandanten bereitstellen oder bearbeiten, wie im Abschnitt 'Einen Mandanten erstellen' beschrieben.

Abrechnungsmodi für Cyber Protect

Ein Abrechnungsmodus ist ein Schema, um die Nutzung der Services und ihrer Funktionen zu erfassen und in Rechnung zu stellen. Der Abrechnungsmodus bestimmt, welche Abteilungen als Basis für die Preisberechnungen verwendet werden. Die Abrechnungsmodi können von den Partnern auf der Kundenebene festgelegt werden.

Die Licensing Engine übernimmt automatisch die passenden Angebotselemente, je nachdem, welche Funktionen in den Schutzplänen angefordert werden. Die Anwender können ihre jeweilige Schutzstufe und Kosten optimieren, indem sie ihre Schutzpläne anpassen.

Hinweis
Sie können nur einen Abrechnungsmodus pro Kunden-Mandanten verwenden.

Abrechnungsmodi für die Schutz-Komponente

Der Schutz hat zwei Abrechnungsmodi:

- Pro Workload
- Pro Gigabyte

Der eigentliche Funktionsumfang der beiden Abrechnungsmodi ist ansonsten identisch.

In beiden Abrechnungsmodi gehören zum Protection Service alle Standard Protection-Funktionen, die den Großteil aller Cyber Security Risiken abdecken. Die Anwender können diese daher ohne zusätzliche Kosten nutzen. Die Nutzung der enthaltenen Funktionen wird erfasst, aber nicht in Rechnung gestellt. Eine vollständige Liste der enthaltenen und abrechenbaren Angebotselemente finden Sie im Abschnitt '"Cyber Protect Services" (S. 7)'.

Auch wenn ein Advanced-Paket für einen Kunden aktiviert wurde, wird es erst in Rechnung gestellt, wenn der Kunde tatsächlich damit beginnt, die Funktionen dieses Pakets in einem Schutzplan zu nutzen. Wenn eine Advanced-Funktion in einem Schutzplan angewendet wird, weist die Licensing Engine dem geschützten Workload automatisch die erforderliche Lizenz zu.

Wenn die Advanced-Funktion nicht mehr verwendet wird, wird die Lizenz widerrufen und die Abrechnung gestoppt. Die Licensing Engine weist automatisch diejenige Lizenz zu, die der tatsächlichen Nutzung der Funktionen entspricht.

Sie können Lizenzen nur für die Cyber Protect-Standard-Service-Funktionen vergeben. Advanced-Funktionen werden auf der Basis ihrer Nutzung abgerechnet und deren Lizenzen können nicht manuell geändert werden. Diese Lizenzen werden von der Licensing Engine automatisch zugewiesen bzw. wieder freigegeben. Sie können den Lizenztyp für einen Workload manuell ändern. Er wird jedoch neu zugewiesen, wenn der Schutzplan für diesen Workload von einem Anwender geändert wird.

Hinweis
Die Abrechnung für die Advanced Protection-Funktionen beginnt nicht, wenn Sie diese aktivieren. Die tatsächliche Abrechnung beginnt erst, wenn ein Kunde damit beginnt, die Advanced-Funktionen in einem Schutzplan auch zu nutzen. Die aktivierten Funktionssätze werden erfasst und in die Nutzungsberichte aufgenommen. Sie werden aber eben erst dann in Rechnung gestellt, wenn die entsprechenden Funktionen wirklich verwendet werden.

Abrechnungsmodi für File Sync & Share

Der File Sync & Share Service hat folgende Abrechnungsmodi:

- Pro Benutzer
- Pro Gigabyte

Sie können auch die Abrechnungsregeln der File Sync & Share-Legacy-Editionen anwenden.

Hinweis
Die Abrechnung für die erweiterte File Sync & Share Funktionalität wird nicht gestartet, wenn Sie diese einfach nur aktivieren. Die Abrechnung beginnt erst, wenn ein Kunde die erweiterten Funktionen auch verwendet. Der aktivierte Advanced-Funktionssatz wird in den Nutzungsberichten zwar aufgenommen, aber erst dann in Rechnung gestellt, wenn die entsprechenden Funktionen wirklich genutzt werden.

Abrechnung für den physischen Datenversand

Die Abrechnung für den Physical Data Shipping Service erfolgt nutzungsabhängig auf Basis eines Pay-as-you-go-Modells.

Abrechnung für den Notary Service

Die Abrechnung für den Notary Service erfolgt nutzungsabhängig auf Basis eines Pay-as-you-go-Modells.

Die Abrechnungsmodi mit Legacy-Editionen verwenden

Wenn Sie noch nicht auf das aktuelle Abrechnungsmodell umgestiegen sind, verwenden Sie die Angebotselemente unter einem der Abrechnungsmodi, um die Legacy-Editionen zu ersetzen. Die Licensing Engine wird die jeweiligen Lizenzen, die dem Kunden zugewiesen werden, automatisch optimieren, damit der abzurechnende Betrag möglichst gering bleibt.

Hinweis
Sie können Editionen jedoch nicht mit Abrechnungsmodi mischen.

Von Legacy-Editionen zum aktuellen Lizenzierungsmodell wechseln

Sie können die Angebotselemente für Ihre Mandanten manuell wechseln, indem Sie deren Profil bearbeiten und Angebotselemente für diese auswählen. Weitere Informationen über den entsprechenden Prozess finden Sie im Abschnitt '"Zwischen Editionen und Abrechnungsmodi wechseln" (S. 10)'.

Wie Sie für mehrere Kunden von Editionen auf Abrechnungsmodi wechseln können, erfahren Sie im Knowledge Base-Artikel Massenumstellung von Editionen für mehrere Kunden (67942).

Zwischen Editionen und Abrechnungsmodi wechseln

Sie können im Management-Portal ein Mandanten-Konto ändern, um für bestimmte Angebotsselemente die Abrechnungsmodi ('pro Workload' zu 'pro Gigabyte' bzw. umgekehrt) umzuschalten oder um zwischen Legacy-Editionen und Abrechnungsmodi zu wechseln.

Informationen zur Massenumstellung von Mandanten finden Sie im Knowledge Base-Artikel 'Massenumstellung von Editionen für mehrere Kunden (67942)'.

Der Umstellungsprozess umfasst die nachfolgenden Schritte.

1. Die neuen Angebotselemente für einen Kunden-Mandanten bereitstellen (Angebotselemente aktivieren und Quota-Festlegung), um die passende Funktionalität des ursprünglichen Angebotselements zu ermöglichen.
2. Die Zuweisung nicht genutzter Angebotselemente aufheben und den Workloads gemäß den in den Schutzplänen verwendeten Funktionen die passenden Angebotselemente zuweisen (Nutzungsabgleich).

Die nachfolgende Tabelle veranschaulicht den Prozess in beide Richtungen.

	Umstellungsrichtung	
	Edition > Abrechnungsmodi	**Abrechnungsmodus > Abrechnungsmodus**
Angebotselemente wechseln	Angebotselemente aktivieren, um die Funktionalität zu erfüllen, die in der Quell-Editionen verfügbar war.	Ein identischer Satz von Angebotselementen wird aktiviert.

	Umstellungsrichtung	
	Edition > Abrechnungsmodi	**Abrechnungsmodus > Abrechnungsmodus**
Quota wechseln	Die Quotas werden vom Quell- zum Ziel-Angebotselement repliziert. Standard (Quelle) → Standard-Produkt (Ziel). Standard (Quelle) → Pakete (Ziel). **Hinweis** Wenn Sie von einer Editionen mit Untereditionen (beispielsweise 'Cyber Protect (pro Workload)') wechseln, werden die Quotas zusammengefasst.	Die Quotas werden vom Quell- zum Ziel-Angebotselement repliziert.
Nutzung wechseln	Die Angebotselemente werden den Workloads neu zugewiesen, entsprechend den Funktionen, die in den Schutzplänen, die diesen Workloads zugewiesen sind, angefordert werden.	

Beispiel: Von einer Cyber Protect Advanced-Edition zu einem 'pro Workload'-Abrechnungsmodus wechseln

In diesem Szenario verwendet ein Kunden-Mandant die Cyber Protect Advanced-Editionen auf acht Workstations – und die Quota ist auf zehn Workloads festgelegt. Drei der Workstations verwenden die Software-Inventarisierung und Patch-Verwaltung in ihren Schutzplänen, zwei der Workstations haben die URL-Filterung in ihren Schutzplänen aktiviert und eine der Maschinen verwendet die Funktion 'Kontinuierliche Datensicherung (CDP)'. Die nachfolgende Tabelle veranschaulicht die Umstellung von den Editionen auf die neuen Angebotselemente.

Quell-Angebotselemente – Nutzung/Quota	Ziel-Angebotselemente – Nutzung/Quota
Cyber Protect Advanced Workstation 8/10	• Workstation – 8/10 • Advanced Security + EDR - 2/10 • Advanced Backup Workstation – 1/10 • Advanced Management – 3/10

Folgende Schritte wurden während der Umstellung ausgeführt:

1. Die Angebotselemente, die die Funktionalität abdecken, die in der Quell-Edition verfügbar war, wurden automatisch aktiviert.
2. Die Quota wurde zu den neuen Angebotselementen repliziert.
3. Die Nutzung wurde auf die tatsächliche Nutzung in Schutzplänen ausgelegt: Drei Workloads verwenden Funktionen des Advanced Management-Pakets, zwei verwenden Funktionen aus dem Advanced Security + EDR-Paket und einer verwendet Funktionen des Advanced Backup-Pakets.

Beispiel: Cyber Protect-'pro Workload'-Editionen zu 'pro Workload'-Abrechnung

In diesem Beispiel hat der Kunde mehrere Editionen auf den Workloads zugewiesen. Jedem Workload kann nur eine Editionen oder ein Abrechnungsmodus zugewiesen werden.

Quell-Angebotselemente – Nutzung/Quota	Ziel-Angebotselemente – Nutzung/Quota
Cyber Protect Essentials Workstation - 6/12	• Workstation – 14/42 • Advanced Backup Workstation – 2/42 • Advanced Security + EDR - 13/42 • Advanced Management – 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standard Workstation – 1/10	

Folgende Schritte wurden während der Umstellung ausgeführt:

1. Die Angebotselemente, die die Funktionalität abdecken, die in allen Quell-Editionen verfügbar war, wurden automatisch aktiviert. Bei den Abrechnungsmodi können einem Workload je nach Bedarf mehrere Angebotselemente zugewiesen werden.
2. Die Quotas wurden zusammengefasst und repliziert.
3. Die Nutzung wurde entsprechend den Schutzplänen abgeglichen.

Den Abrechnungsmodus für einen Partner-Mandanten ändern

So können Sie den Abrechnungsmodus für einen Partner-Mandanten ändern

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den Partner-Mandanten, dessen Abrechnungsmodus Sie ändern wollen, klicken Sie anschließend zuerst auf das Drei-Punkte-Symbol und dann auf den Befehl **Konfigurieren**.
3. Wählen Sie auf der Registerkarte **Cyber Protect** den Service, für den Sie den Abrechnungsmodus ändern wollen, und klicken Sie anschließend auf **Bearbeiten**.
4. Wählen Sie den gewünschten Abrechnungsmodus und aktivieren oder deaktivieren, je nach Bedarf, die verfügbaren Angebotselemente.
5. Klicken Sie auf **Speichern**.

Den Abrechnungsmodus für einen Kunden-Mandanten ändern

Sie können die Abrechnung für einen Kunden-Mandanten ändern, indem Sie Folgendes tun:

- Den ursprünglichen Abrechnungsmodus bearbeiten, indem Sie Angebotselemente aktivieren oder deaktivieren.
- Zu einem komplett neuen Abrechnungsmodus wechseln.

Weitere Informationen über die Bearbeitung der verfügbaren Angebotselemente finden Sie im Abschnitt 'Angebotselemente aktivieren oder deaktivieren'.

So können Sie den Abrechnungsmodus für einen Kunden-Mandanten wechseln

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den Kunden-Mandanten, dessen Edition Sie ändern wollen, klicken Sie anschließend zuerst auf das Drei-Punkte-Symbol und dann auf den Befehl **Konfigurieren**.
3. Wählen Sie auf der Registerkarte **Konfigurieren** unter **Service** den neuen Abrechnungsmodus. Es erscheint ein Dialog, der Sie darüber informiert, welche Folgen der Wechsel zum neuen Abrechnungsmodus hat.
4. Geben Sie Ihren Benutzernamen ein, um Ihre Wahl zu bestätigen.

Hinweis
Die Umsetzung dieser Änderung kann bis zu 10 Minuten dauern.

Angebotselemente und Quota-Verwaltung

In diesem Abschnitt wird Folgendes beschrieben:

- Was sind Services und Angebotselemente?
- Wie werden Angebotselemente aktiviert oder deaktiviert?
- Was sind Abrechnungsmodi?
- Was sind Advanced Protection-Pakete?
- Was sind Legacy-Editionen und Untereditionen?
- Was sind weiche und harten Quotas (in Englisch auch Soft Quotas und Hard Quotas genannt)?
- Wie kann eine harte Quota überschritten werden?
- Was versteht man unter einer Backup-Quota-Transformation?
- Wie beeinflusst die Angebotselement-Verfügbarkeit die Workload-Typ-Verfügbarkeit in der Cyber Protect-Konsole?

Services und Angebotselemente

Services

Ein Cloud Service ist eine Zusammenstellung von Funktionalitäten, die von einem Partner oder in der Private Cloud eines Endkunden gehostet werden kann. In der Regel werden Services als Abonnement oder Basis eines Pay-as-you-go-Modells (also nutzungsabhängig) verkauft.

Der Cyber Protect Service integriert Cyber Security-, Data Protection- und Management-Funktionalitäten, um Endpunkte, Systeme und Daten vor Cyber Security-Bedrohungen zu schützen. Der Cyber Protect Service besteht aus mehreren Komponenten: Schutz, File Sync & Share, Notary

und physischer Datenversand (Physical Data Shipping). Einige davon können mithilfe von Advanced Protection-Paketen auf eine Advanced-Funktionalität erweitert werden. Ausführlichere Informationen zu den enthaltenen Standard- und verfügbaren Advanced-Funktionen finden Sie in Abschnitt '"Cyber Protect Services" (S. 7)'.

Angebotselemente

Ein Angebotselement ist ein Zusammenstellung von Service-Funktionen, die nach bestimmten Workloadtypen oder Funktionalitäten (z.B. Storage, Disaster Recovery-Infrastruktur und andere) gruppiert sind. Indem Sie bestimmte Angebotselemente aktivieren, bestimmen Sie, welche und wie viele Workloads geschützt werden können (durch Festlegen von Quotas) – und welche Schutzstufe für Ihre Partner, Kunden und deren Endanwender verfügbar ist (durch Aktivieren/Deaktivieren von Advanced Protection-Paketen).

Funktionalitäten, die nicht aktiviert sind, werden vor Kunden und Endanwendern verborgen – es sei denn, Sie konfigurieren ein Upselling-Szenario. Weitere Informationen über Upselling-Szenarien finden Sie im Abschnitt '"Upselling-Szenarien für Ihre Kunden konfigurieren" (S. 80)'.

Die Funktionsnutzung wird von den Services ermittelt und bei den Angebotselementen ausgewiesen. Die entsprechenden Nutzungsinformationen werden außerdem für Berichte und weitere Abrechnungen verwendet.

Abrechnungsmodi und Editionen

Bei den Legacy-Editionen können Sie ein Angebotselement pro Workload aktivieren. Bei den Abrechnungsmodi ist die Funktionalität aufgeteilt, sodass Sie mehrere Angebotselemente (Service-Funktionen und Advanced-Pakete) pro Workload aktivieren können. So können Sie den Bedürfnissen Ihrer Kunden besser gerecht werden und eine genauere Abrechnung für jeweils nur die Funktionen vornehmen, die Ihre Kunden auch tatsächlich nutzen.

Weitere Informationen zu den Abrechnungsmodi für Cyber Protect finden Sie im Abschnitt '"Abrechnungsmodi für Cyber Protect" (S. 8)'.

Sie können entweder Abrechnungsmodi oder Editionen verwenden, um zu konfigurieren, welche Services für Ihre Mandanten verfügbar sind. Sie können nur einen Abrechnungsmodus oder eine Editionen pro Kunden-Mandanten verwenden. Wenn Sie also verschiedene Abrechnungsmodi für verschiedene Service-Funktionen anwenden wollen, müssen Sie mehrere Mandanten für einen Kunden erstellen. Wenn der Kunde beispielsweise Microsoft 365-Postfächer im 'pro Gigabyte'-Abrechnungsmodus und Microsoft Teams im 'pro Workload'-Abrechnungsmodus haben will, müssen Sie zwei verschiedene Kunden-Mandanten für diesen Kunden erstellen.

Wenn Sie die Service-Nutzung in einem Angebotselement begrenzen wollen, können Sie Quotas für dieses Angebotselement definieren. Siehe Abschnitt '"Weiche und harte Quotas" (S. 16)'.

Angebotselemente aktivieren oder deaktivieren

Sie können alle für eine bestimmte Edition oder Abrechnungsmodus verfügbaren Angebotselemente aktivieren, wie im Abschnitt 'Einen Mandanten erstellen' beschrieben.

Hinweis
Wenn Sie alle Angebotselemente eines Service deaktivieren, wird nicht auch der Service automatisch deaktiviert.

Es gibt einige Beschränkungen bei der Deaktivierung von Angebotselementen, die in der nachfolgenden Tabelle aufgeführt sind.

Angebotselement	Deaktivieren	Ergebnis
Backup Storage	Kann deaktiviert werden, wenn die Nutzung gleich Null ist.	Der Cloud Storage wird innerhalb eines Kunden-Mandantens nicht mehr als Backup-Ziel verfügbar sein.
Lokales Backup	Kann deaktiviert werden, wenn die Nutzung gleich Null ist.	Der lokale Storage wird innerhalb eines Kunden-Mandantens nicht mehr als Backup-Ziel verfügbar sein.
Datenquellen (inkl. Microsoft 365 und Google Workspace)*	Kann deaktiviert werden, wenn die Nutzung gleich Null ist.	Der Schutz der deaktivierten Datenquellen (inkl. Microsoft 365 und Google Workspace) wird innerhalb eines Kunden-Mandanten folgendermaßen nicht mehr verfügbar sein:
Alle Disaster Recovery-Angebotselemente	Kann deaktiviert werden, wenn die Nutzung größer als Null ist.	Zu Details siehe den Abschnitt 'Weiche und harte Quotas'.
Alle Notary-Angebotselemente	Kann deaktiviert werden, wenn die Nutzung gleich Null ist.	Der Notary Service wird innerhalb eines Kunden-Mandantens nicht verfügbar sein.
Alle File Sync & Share-Angebotselemente	Angebotselemente können separat aktiviert oder deaktiviert werden.	Der File Sync & Share Service wird innerhalb eines Kunden-Mandantens nicht verfügbar sein.
Alle Physischer Datenversand-Angebotselemente	Kann deaktiviert werden, wenn die Nutzung gleich Null ist.	Der Service 'Physische Datenversand wird innerhalb eines Kunden-Mandantens nicht verfügbar sein.

Bei Angebotselementen, die nicht deaktiviert werden können, wenn deren Nutzung größer als Null ist, können Sie die Nutzung manuell entfernen und anschließend das entsprechende Angebotselemente deaktivieren.

* Die Angebotselemente beziehen sich auf die Workloads, die Sie in der Cyber Protect-Konsole hinzufügen können. Weitere Informationen dazu finden Sie im Abschnitt '"Workload-Abhängigkeit von Angebotselementen" (S. 26)'. Die nachfolgende Tabelle fasst zusammen, welche Workload-Typen nicht verfügbar sind, wenn ein Angebotselement, eine Kombination von Angebotselementen oder ein Advanced-Paket nicht im Management-Portal aktiviert ist.

Wenn Sie diese Angebotselemente oder Advanced-Pakete deaktivieren	Werden Sie diese Workload-Typen nicht hinzufügen können
Die folgende Kombination: • Microsoft 365-Arbeitsplätze • Microsoft 365 SharePoint online • Microsoft 365-Teams	Microsoft 365 Business
Die folgende Kombination: • Google Workspace • Google Workspace Shared Drive	Google Workspace
Die folgende Kombination: • Server • Virtuelle Maschinen	• Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory
Das folgende Angebotselement: • NAS-Gerät	Synology
Das folgende Angebotselement: • Mobilgeräte	• iOS-Geräte • Android-Geräte
Das folgende Advanced-Paket: • Advanced Backup	Oracle Database

Weiche und harte Quotas

Mit **Quotas** können Sie einschränken, ob und wie ein Mandant den Service verwenden kann. Um Quotas für einen Client festlegen zu können, müssen Sie diesen in der Registerkarte **Clients** auswählen, dann die Registerkarte des Service auswählen und anschließend auf **Bearbeiten** klicken.

Wenn eine Quota überschritten wird, wird an den Benutzer (bzw. seine E-Mail-Adresse) eine entsprechende Benachrichtigung gesendet. Wenn Sie keine Quota-Überschreitung festlegen, wird die Quota als '**weich**' angesehen. Das bedeutet, dass keine Beschränkungen für die Nutzung des Cyber Protection Service gelten.

Wenn Sie eine Quota-Überschreitung spezifizieren, wird die Quota als '**hart**' angesehen. Eine **Überschreitung** erlaubt es dem Benutzer, die Quota um den spezifizierten Wert zu überschreiten.

Wird die Überschreitung überschritten, werden Nutzungsbeschränkungen auf den Service angewendet.

Beispiel

Weiche Quota: Sie haben die Quota für Workstations auf 20 festgelegt. Wenn die Anzahl der geschützten Workstations des Kunden den Wert 20 erreicht, erhält der Kunde zwar eine E-Mail-Benachrichtigung, aber der Cyber Protection Service ist weiterhin verfügbar.

Harte Quota: Wenn Sie die Quota für Workstations auf 20 und die Überschreitung auf 5 festgelegt haben, erhält Ihr Kunde eine E-Mail-Benachrichtigung, wenn die Anzahl der geschützten Workstations 20 erreicht. Wenn die Anzahl 25 erreicht ist, wird der Cyber Protection Service für den Benutzer deaktiviert.

Wenn eine harte Quota erreicht wird, wird der Service eingeschränkt (beispielsweise kann kein weiterer Workload mehr geschützt oder weiterer Speicherplatz belegt werden). Wenn die harte Quota überschritten wird, wird an den Benutzer (bzw. seine E-Mail-Adresse) eine entsprechende Benachrichtigung gesendet.

Ebenen, auf denen Quotas definiert werden können

Die nachfolgende Tabelle führt auf, auf welchen Ebenen die Quotas festgelegt werden können.

Mandant/Benutzer	Weiche Quota (nur Quota)	Harte Quota (Quota und Überschreitung)
Partner	ja	nein
Ordner	ja	nein
Kunde	ja	ja
Abteilung	nein	nein
Benutzer	ja	ja

Die weichen Quotas können auf Partner- und Ordnerebenen festgelegt werden. Auf Abteilungsebene können keine Quotas festgelegt werden. Die harten Quotas können auf Kunden- und Benutzerebenen festgelegt werden.

Die Gesamtzahl der harten Quotas, die auf Benutzerebene festgelegt werden, darf die harte Quota des entsprechenden Kunden nicht überschreiten.

Weiche und harte Quotas einrichten

So können Sie Quotas für Ihre Kunden einrichten

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den Kunden aus, für den Sie die Quotas einrichten wollen.
3. Wählen Sie die Registerkarte **Schutz** aus und klicken Sie dann auf den Befehl **Bearbeiten**.

4. Wählen Sie die Art der Quota aus, die Sie einrichten wollen. Sie können beispielsweise **Workstations** oder **Server** wählen.
5. Klicken Sie auf der rechten Seite auf den Link **Unbegrenzt**, um das Fenster **Quota bearbeiten** zu öffnen.
   - Wenn Sie den Kunden über die Quota informieren und die Nutzungsmöglichkeit des Service für den Kunden nicht einschränken wollen, dann legen Sie den Quota-Wert im Feld **Weiche Quota** fest.
     Der Kunde wird beim Erreichen der Quota eine E-Mail-Benachrichtigung erhalten. Der Cyber Protection Service ist aber weiterhin verfügbar.
   - Wenn Sie die Nutzungsmöglichkeit des Service für den Kunden dagegen einschränken wollen, wählen Sie **Harte Quota** aus und legen Sie den Quota-Wert im Feld unter **Harte Quota** fest.
     Der Kunde wird beim Erreichen der Quota eine E-Mail-Benachrichtigung erhalten und der Cyber Protection Service wird für ihn deaktiviert.
6. Klicken Sie im Fenster **Quota bearbeiten** auf **Fertig** und anschließend auf **Speichern**.

Backup-Quotas

Sie können die Cloud Storage-Quota, die Quota für lokale Backups und die maximale Anzahl an Maschinen/Geräten/Websites spezifizieren, die ein Benutzer sichern darf. Folgende Quotas sind verfügbar.

Quotas für Geräte

- **Workstations**
- **Server**
- **Virtuelle Maschinen**
- **Mobilgeräte**
- **Webhosting-Server** (Linux-basierte physische oder virtuelle Server, die Plesk, cPanel-, DirectAdmin-, VirtualMin- oder ISPManager-Control-Panels ausführen)
- **Websites**

Ein(e) Maschine/Gerät/Website wird als 'geschützt' betrachtet, wenn auf diese(s) mindestens ein Schutzplan angewendet wurde. Ein Mobilgerät wird nach Durchführung des ersten Backups als 'geschützt' betrachtet.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Geräten erreicht ist, kann der Benutzer keinen weiteren Geräten mehr einen Schutzplan zuweisen.

Quotas für Cloud-Datenquellen

- **Microsoft 365-Arbeitsplätze**

Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen.

Die Lizenzierung der Microsoft 365-Arbeitsplätze ist abhängig vom Abrechnungsmodus, der für Cyber Protection ausgewählt wurde.

Wichtig

Der lokale Agent und der Cloud Agent verbrauchen separate Quotas. Wenn Sie dieselben Workloads mit beiden Agenten sichern, werden Ihnen zwei Gebühren berechnet. Beispiel:

- Wenn Sie die Postfächer von 120 Benutzern mit dem lokalen Agenten und die OneDrive-Dateien derselben Benutzer mit dem Cloud Agenten sichern, werden Ihnen 240 Microsoft 365-Arbeitsplätze berechnet.
- Wenn Sie die Postfächer von 120 Benutzern mit dem lokalen Agenten sichern und dieselben Postfächer zudem mit dem Cloud Agenten sichern, werden Ihnen 240 Microsoft 365-Arbeitsplätze berechnet.

Im **pro Workload**-Abrechnungsmodus wird die Quota **Microsoft 365-Arbeitsplätze** für jeden Nutzer einzeln berechnet. Ein eindeutiger Benutzer ist ein Anwender, der mindestens eine der folgenden Eigenschaften aufweist:

- Geschütztes Postfach
- Geschütztes OneDrive
- Zugriff auf mindestens eine geschützte Firmenebenen-Ressource: eine Microsoft 365 SharePoint Online-Website oder Microsoft 365 Teams.
  Wie Sie die Anzahl der Mitglieder einer Microsoft 365 SharePoint- oder Teams-Website überprüfen können, erfahren Sie in diesem Knowledge Base-Artikel.

Hinweis

Gesperrte Microsoft 365-Benutzer, die kein geschütztes persönliches Postfach oder OneDrive haben und nur auf gemeinsame Ressourcen (gemeinsame Postfächer, SharePoint-Websites und Microsoft Teams) zugreifen können, werden nicht berechnet.

Gesperrte Benutzer sind solche, die über keine gültige Anmeldung verfügen und keinen Zugriff auf die Microsoft 365-Services haben. Wie Sie alle nicht lizenzierten Benutzer in einer Microsoft 365-Organisation blockieren können, erfahren Sie unter '"Verhindern, dass sich nicht lizenzierte Microsoft 365-Benutzer anmelden können" (S. 22)'.

Die folgenden Microsoft 365-Arbeitsplätze sind nicht kostenpflichtig und erfordern keine Pro-Arbeitsplatz-Lizenz:

- Freigegebene Postfächer
- Räume und Geräte
- Externe Benutzer mit Zugriff auf gesicherte SharePoint-Websites und/oder Microsoft Teams

Weitere Informationen zu den Lizenzierungsoptionen mit dem 'pro Gigabyte'-Abrechnungsmodus finden Sie im folgenden Dokument: Cyber Protect Cloud: 'pro Gigabyte'-Abrechnungsmodus für Microsoft 365.

Weitere Informationen zu den Lizenzierungsoptionen mit dem 'pro Workload'-Abrechnungsmodus finden Sie im folgenden Dokument: Cyber Protect Cloud: Microsoft 365-Lizenzierung und Preisänderungen.

- **Microsoft 365-Teams**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota aktiviert oder deaktiviert die Möglichkeit, Microsoft 365-Teams zu schützen, und legt die maximale Anzahl von Teams fest, die geschützt werden können. Zum Schutz eines Teams ist, unabhängig von der Anzahl seiner Mitglieder oder Kanäle, nur eine Quota erforderlich. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen.
- **Microsoft 365 SharePoint Online**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota aktiviert oder deaktiviert die Möglichkeit, SharePoint Online-Websites zu schützen, und legt die maximale Anzahl von Website-Sammlungen und Gruppen-Websites fest, die geschützt werden können.

  Firmenadministratoren können die Quota im Management-Portal einsehen. Sie können außerdem die Quota und den Speicherplatz, der von den SharePoint Online-Backups belegt wird, in den Nutzungsberichten einsehen.
- **Google Workspace-Arbeitsplätze**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Der Firma kann es erlaubt werden, **Gmail**-Postfächer (inkl. Kalender und Kontakte), **Google Drive**-Dateien oder beides zu sichern. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen.
- **Google Workspace Shared Drive**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota (de)aktiviert die Möglichkeit, Google Workspace Shared Drives zu sichern. Wenn diese Quota aktiviert ist, können beliebig viele Shared Drives gesichert werden. Firmenadministratoren können zwar nicht die Quota im Management-Portal einsehen, aber den Speicherplatz in den Nutzungsberichten einsehen, der von den Shared Drive-Backups belegt wird.

  Backups von Google Workspace Shared Drives sind nur für Kunden verfügbar, die mindestens eine Quota für Google Workspace-Arbeitsplätze zusätzlich haben. Diese Quota wird nur überprüft und nicht in Anspruch genommen.

Ein Microsoft 365-Arbeitsplatz gilt als geschützt, solange mindestens ein Schutzplan auf das Postfach oder OneDrive-Laufwerk des Benutzers oder angewendet wird. Ein Google Workspace-Arbeitsplatz gilt als geschützt, solange mindestens ein Schutzplan auf das Postfach oder das Google Drive-Laufwerk des Benutzers angewendet wird.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Arbeitsplätzen erreicht ist, kann ein Firmenadministrator keinen weiteren Arbeitsplätzen mehr einen Schutzplan zuweisen.

Quotas für Storage

- **Lokales Backup**

  Die Quota '**Lokales Backup**' beschränkt die Gesamtgröße der lokalen Backups, die mithilfe der Cloud-Infrastruktur erstellt werden können. Für diese Quota kann keine Überschreitung festgelegt werden.
- **Cloud-Ressourcen**

  Die Quota **Cloud-Ressourcen** kombiniert die Quota für Backup Storage und die Quotas für Disaster Recovery. Die Backup Storage-Quota begrenzt die Gesamtgröße der Backups, die im Cloud Storage gespeichert sind. Wird die Backup Storage-Quota-Überschreitungsgrenze erreicht, werden weitere Backups fehlschlagen.

Die Quota für den Backup Storage überschreiten

Die Backup Storage-Quota kann nicht überschritten werden. Das Protection Agent-Zertifikat hat eine technische Quota, die der Backup-Quota des Mandanten + Überschreitung entspricht. Ein Backup kann nicht gestartet werden, wenn die Quota überschritten wurde. Wenn während der Backup-Erstellung zwar die Quota im Zertifikat erreicht wird, aber noch nicht die Überschreitung, dann wird das Backup noch erfolgreich abgeschlossen. Wenn während der Backup-Erstellung auch die Überschreitungsgrenze erreicht wird, wird das Backup fehlschlagen.

Beispiel:

Ein Benutzer-Mandant hat noch 1 TB an freiem Speicherplatz in seiner Quota und die für diesen Benutzer konfigurierte Überschreitung beträgt 5 TB. Der Benutzer startet ein Backup. Wenn die Größe des erstellten Backups beispielsweise 3 TB beträgt, wird das Backup erfolgreich abgeschlossen, weil der Überschreitungswert nicht erreicht wird. Wenn die Größe des erstellten Backups größer als 6 TB ist, wird das Backup fehlschlagen, weil der Überschreitungswert überschritten wurde.

Backup-Quota-Transformation

Der Erwerb einer Backup-Quota und die Zuordnung von Angebotselementen zu Ressourcentypen funktioniert grundsätzlich folgendermaßen: das System vergleich die verfügbaren Angebotselemente mit dem Ressourcentyp – und erwirbt dann die Quota für das passende Angebotselement.

Es besteht außerdem die Möglichkeit, eine andere Angebotselement-Quota zuzuordnen, auch wenn diese nicht genau zum Ressourcentyp passt. Dies wird **Backup Quota-Transformation** genannt. Wenn es kein passendes Angebotselement gibt, versucht das System, eine geeignete teurere Quota für den Ressourcentyp zu finden (automatische Backup-Quota-Transformation). Wenn eine geeignete Quota gefunden wird, können Sie in der Cyber Protect-Konsole die Service-Quota dem Ressourcentyp manuell zuordnen.

Beispiel

Sie wollen eine virtuelle Maschine (Workstation, Agenten-basiert) per Backup sichern.

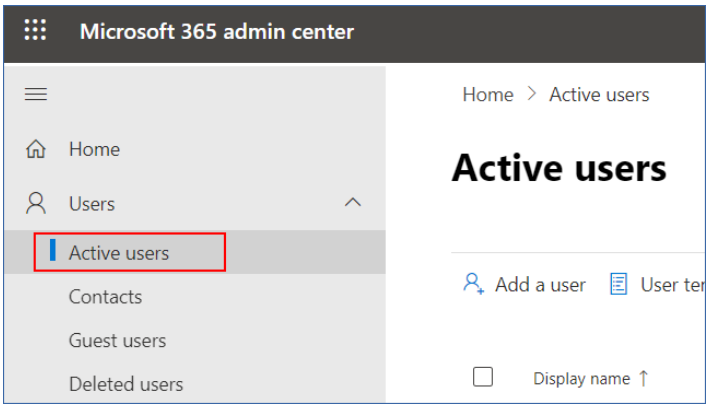
Das System wird zuerst prüfen, ob es eine zugewiesene Quota vom Typ '**Virtuelle Maschine**' gibt. Wenn diese nicht gefunden wird, versucht das System automatisch, die Quota **Workstations** zu erwerben. Wenn auch diese nicht zu finden ist, wird die andere Quota nicht mehr automatisch erworben. Wenn Sie über eine ausreichende Quota verfügen, die teurer als die Quota **Virtuelle Maschine** und auf eine virtuelle Maschine anwendbar ist, können Sie sich an der Cyber Protect-Konsole anmelden und die Quota **Server** manuell zuweisen.

Verhindern, dass sich nicht lizenzierte Microsoft 365-Benutzer anmelden können

Sie können alle nicht lizenzierten Benutzer in Ihrer Microsoft 365-Organisation daran hindern, sich anzumelden, indem Sie deren Anmeldestatus bearbeiten.

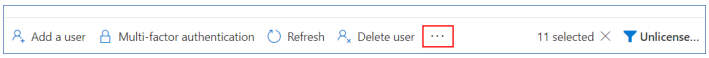
So können Sie verhindern, dass sich nicht lizenzierte Benutzer anmelden

1. Melden Sie sich im Microsoft 365 Admin Center (https://admin.microsoft.com) als globaler Administrator an.
2. Gehen Sie im Navigationsmenü zu **Benutzer** –> **Aktive Benutzer**.



3. Klicken Sie auf **Filter** und wählen Sie **Nicht lizenzierte Benutzer**.

4. vieren Sie die Kontrollkästchen neben den Benutzernamen und klicken Sie anschließend auf das Drei-Punkte-Symbol (...).



5. Wählen Sie aus dem Menü den Befehl **Anmeldestatus bearbeiten** aus.
6. Aktivieren Sie das Kontrollkästchen **Benutzer an der Anmeldung hindern** und klicken Sie anschließend auf **Speichern**.

Disaster Recovery-Quotas

Hinweis
Die Disaster Recovery-Angebotselemente sind nur mit dem Disaster Recovery-Add-on verfügbar.

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quotas für bestimmte Benutzer festlegen.

- **Disaster Recovery Storage**

  Der Disaster Recovery Storage zeigt die Backup Storage-Größe für diejenigen Server an, die per Disaster Recovery geschützt werden. Die Nutzung des Disaster Recovery Storage entspricht der Nutzung des Backup Storage derjenigen Workloads, die über Disaster Recovery-Server geschützt werden. Dieser Storage wird ab dem Zeitpunkt berechnet, an dem ein Recovery-Server erstellt wird – unabhängig davon, ob der Server gerade läuft. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server und Recovery-Server erstellt oder Laufwerke zu vorhandenen primären Servern hinzugefügt/erweitert werden. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, kann kein Failover initiiert oder ein gestoppter Server gestartet werden. Die Ausführung laufender Server wird aber fortgesetzt.
- **Berechnungspunkte**

  Diese Quota begrenzt die CPU- und RAM-Ressourcen, die die primären Server und Recovery-Server während eines Abrechnungszeitraums verbrauchen dürfen. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, werden alle primären Server und Recovery-Server heruntergefahren. Diese Server können erst wieder verwendet werden, wenn der nächste Abrechnungszeitraum beginnt. Der vorgegebene Abrechnungszeitraum ist ein voller Kalendermonat.

  Wenn die Quota deaktiviert ist, können die Server überhaupt nicht verwendet werden (unabhängig vom Abrechnungszeitraum).
- **Öffentliche IP-Adressen**

  Mit dieser Quota wird die Anzahl der öffentlichen IP-Adressen beschränkt, die primären Servern und Recovery-Servern zugewiesen werden können. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine öffentlichen IP-Adressen mehr für weitere Server aktiviert werden. Sie können einem Server die Verwendung öffentlicher IP-Adressen verbieten, wenn Sie in den Server-Einstellungen das Kontrollkästchen **Öffentliche IP-Adresse** deaktivieren. Anschließend können Sie einem anderen Server die Verwendung einer öffentlichen IP-Adresse (die normalerweise nicht dieselbe ist) erlauben.

  Wenn die Quota deaktiviert wird, hören alle Server auf, öffentliche IP-Adressen zu verwenden, und sind anschließend nicht mehr über das Internet erreichbar.
- **Cloud Server**

  Diese Quota ermöglicht es, die Gesamtzahl der primären Server und Recovery-Server zu beschränken. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt werden.

  Wenn die Quota deaktiviert wird, sind die Server zwar noch in der Cyber Protect-Konsole sichtbar, aber die einzige auf sie anwendbare Aktion ist **Löschen**.
- **Internetzugriff**

  Diese Quota (de)aktiviert den Internetzugriff für die primären Server und Recovery-Server.

  Wenn die Quota deaktiviert wird, werden die primären und Recovery-Server keine Verbindungen mit dem Internet herstellen können.

File Sync & Share-Quotas

Sie können folgende File Sync & Share-Quotas für einen Mandanten definieren:

- **Benutzer**
  Dies definiert die Grenze für die Anzahl der File Sync & Share-Benutzer.

  Hinweis
  Nur die Benutzerrollen 'Benutzer' sowie 'Benutzer + Administrator' werden auf diese Quota angerechnet.
  Die Benutzerrollen Administrator und Gast sind von dieser Quota ausgeschlossen.

- **Cloud Storage**
  Dies definiert den Grenzwert für den Cloud Storage, der dem Mandanten zugeordnet wurde.

Physischer Datenversand-Quotas

Die Quotas für den Service 'Physische Datenversand' (Physical Data Shipping) werden auf einer Pro-Laufwerk-Basis verbraucht. Sie können auf einem entsprechenden Laufwerk die anfänglichen Backups mehrerer Maschinen speichern.

Sie können folgende Physischer Datenversand-Quotas für einen Mandanten definieren:

- **In die Cloud**
  Ermöglicht es, ein anfängliches Backup per Festplattenlaufwerk an das Cloud Datacenter Ihrer Wahl zu senden. Diese Quota definiert die maximale Anzahl von Laufwerken, die zum Cloud Datacenter gesendet werden können.

Notary-Quotas

Sie können folgende Notary-Quotas für einen Mandanten definieren:

- **Notary Storage**
  Definiert den maximalen Speicherplatz im Cloud Storage für beglaubigte Dateien, signierte Dateien und Dateien, deren Beglaubigung oder Signierung gerade durchgeführt wird.
  Wenn Sie die Nutzung dieser Quota verringern wollen, können Sie bereits beglaubigte oder signierte Dateien aus dem Notary Storage löschen.
- **Beglaubigungen**
  Definiert die maximale Anzahl von Dateien, die mithilfe des Notary Service beglaubigt werden können.
  Eine Datei gilt als beglaubigt, sobald sie zum Notary Storage hochgeladen wurde und ihr Beglaubigungsstatus auf **Wird bearbeitet** geändert wurde.
  Wenn dieselbe Datei mehrfach beglaubigt wird, gilt jede Beglaubigung wie eine neue gezählt.
- **eSignaturen**
  Definiert die maximale Anzahl von digitalen eSignaturen.

Die Service-Quota von Maschinen ändern

Die Schutzstufe einer Maschine wird durch die Service-Quota definiert, die auf die Maschine angewendet wird. Service-Quotas beziehen sich auf die für den Mandanten verfügbaren

Angebotselemente, in denen die Maschine registriert ist.

Eine Service-Quota wird automatisch zugewiesen, wenn ein Schutzplan erstmalig auf eine Maschine angewendet wird.

Die am besten geeignete Quota wird in Abhängigkeit von der Art der geschützten Maschine, ihrem Betriebssystem, der erforderlichen Schutzstufe sowie der Quota-Verfügbarkeit zugewiesen. Wenn die am besten geeignete Quota nicht in Ihrem Unternehmen verfügbar ist, wird die zweitbeste Quota zugewiesen. Wenn beispielsweise die Quota **Webhosting-Server** am besten geeignet wäre, diese jedoch nicht verfügbar ist, wird die Quota **Server** zugewiesen.

Beispiele für Quota-Zuweisungen:

- Einer physischen Maschine, auf der ein Windows Server- oder ein Linux Server-Betriebssystem (wie Ubuntu Server) ausgeführt wird, wird die Quota **Server** zugewiesen.
- Einer physischen Maschine, auf der ein Windows- oder ein Linux-Desktop-Betriebssystem (wie Ubuntu Desktop) ausgeführt wird, wird die Quota **Workstation** zugewiesen.
- Einer physischen Maschine, auf der Windows 10 mit aktivierter Hyper-V-Rolle ausgeführt wird, wird die Quota **Workstation** zugewiesen.
- Einer Desktop-Maschine, die auf einer virtuellen Desktop-Infrastruktur läuft und deren Protection Agent innerhalb des Gastbetriebssystems installiert wurde (wie etwa der Agent für Windows), wird die Quota **Virtuelle Maschine** zugewiesen. Diese Art von Maschine kann auch die Quota **Workstation** verwenden, wenn die Quota **Virtuelle Maschine** nicht verfügbar ist.
- Einer Desktop-Maschine, die auf einer virtuellen Desktop-Infrastruktur läuft und deren Backup im agentenlosen Modus erstellt wird (z.B. durch den Agenten für VMware oder den Agenten für Hyper-V), wird die Quota **Virtuelle Maschine** zugewiesen.
- Einem Hyper-V- oder vSphere-Server wird die Quota **Server** zugewiesen.
- Einem Server mit cPanel oder Plesk wird die Quota **Webhosting-Server** zugewiesen. Abhängig von Art der Maschine, auf welcher der Webserver läuft, könnte er auch die Quota **Virtuelle Maschine** oder **Server** verwenden (falls die die Quota **Webhosting-Server** nicht verfügbar ist).
- Für applikationskonforme Backups ist die Quota **Server** erforderlich, auch wenn es sich bei der Maschine um eine Workstation handelt.

Sie können die ursprüngliche Zuweisung später noch manuell ändern. Wenn Sie etwa einen weitergehenden Schutzplan auf dieselbe Maschine anwenden möchten, müssen Sie möglicherweise die Service-Quota der Maschine upgraden. Wenn die von diesem Schutzplan benötigten Funktionen durch die aktuell zugewiesene Service-Quota nicht unterstützt werden, wird der Schutzplan fehlschlagen.

Sie können die Service-Quota auch noch ändern, wenn Sie eine passendere Quota erwerben, nachdem die ursprüngliche Quota zugewiesen wurde. Beispielsweise, wenn die Quota **Workstations** einer virtuellen Maschine zugewiesen wurde. Nachdem Sie ein Quota **Virtuelle Maschine** erworben haben, können Sie der Maschine dann diese Quota (statt der ursprünglichen Quota **Workstation**) manuell zuweisen.

Sie können die aktuell zugewiesene Service-Quota auch freigeben und diese Quota dann einer ganz anderen Maschine zuweisen.

Sie können die Service-Quota einer einzelnen Maschine oder für eine Gruppe von Maschinen ändern.

So können Sie die Service-Quota einer einzelnen Maschine ändern

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie die gewünschte Maschine und klicken Sie dann auf **Details**.
3. Klicken Sie im Bereich **Service-Quota** auf **Ändern**.
4. Wählen Sie im Fenster **Quota ändern** die gewünschte Service-Quota oder **Keine Quota** aus – und klicken Sie dann auf **Ändern**.

So können Sie die Service-Quota für eine Gruppe von Maschinen ändern

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wählen Sie mehr als eine Maschine aus und klicken Sie dann auf **Quota zuweisen**.
3. Wählen Sie im Fenster **Quota ändern** die gewünschte Service-Quota oder **Keine Quota** aus – und klicken Sie dann auf **Ändern**.

Workload-Abhängigkeit von Angebotselementen

Im Fensterbereich **Geräte hinzufügen** der Cyber Protect-Konsole stehen verschiedene Workload-Typen zur Verfügung, je nachdem, welche Angebotselemente aktiviert sind. In der nachfolgenden Tabelle ist aufgeführt, welche Workload-Typen bei den verschiedenen Angebotselementen verfügbar sind.

Workload-Typ (Agenten-Installer)	**Aktivierte Angebotselemente**							
	Server	**Workstations**	**Virtuelle Maschinen**	**Microsoft 365-Arbeitsplätze**	**Google Workspace-Arbeitsplätze**	**Mobilgeräte**	**Webhosting-Server**	**Websites**
Workstations – Agent für Windows		+	+					+
Workstations – Agent für macOS		+	+					+
Server – Agent für Windows	+		+				+	+

Workload-Typ (Agenten-Installer)	Aktivierte Angebotselemente							
	Server	**Workstations**	**Virtuelle Maschinen**	**Microsoft 365-Arbeitsplätze**	**Google Workspace-Arbeitsplätze**	**Mobilgeräte**	**Webhosting-Server**	**Websites**
Server – Agent für Linux	+		+				+	+
Agent für Hyper-V			+					
Agent für VMware			+					
Agent für Virtuozzo			+					
Agent für SQL	+		+					
Agent für Exchange	+		+					
Agent für Active Directory	+		+					
Microsoft 365 Business-Workloads				+				
Google Workspace-Workloads					+			
Vollständiger Installer für Windows	+	+	+				+	+
Für Mobilgeräte (iOS und Android)						+		

Das Management-Portal verwenden

Die folgenden Schritte führen Sie durch die grundlegende Nutzung des Management-Portals.

Unterstützte Webbrowser

Die Weboberfläche unterstützt folgende Webbrowser:

- Google Chrome 29 (oder höher)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

In anderen Webbrowsern (inkl. Safari-Browser, die unter anderen Betriebssystem laufen) wird möglicherweise die Benutzeroberfläche nicht korrekt angezeigt oder stehen einige Funktionen nicht zur Verfügung.

Das Administratorkonto aktivieren

Nachdem Sie die Partnerschaftsvereinbarung unterschrieben haben, erhalten Sie eine E-Mail-Nachricht mit folgenden Informationen:

- **Ihr Anmeldename.** Dies ist der Benutzername, mit dem Sie sich anmelden. Ihr Anmeldename wird auch auf der Kontoaktivierungsseite angezeigt.
- **Konto aktivieren**-Schaltfläche. Klicken Sie auf die Schaltfläche und legen Sie das Kennwort für Ihr Konto fest. Stellen Sie sicher, dass Ihr Kennwort mindestens neun Zeichen lang ist. Weitere Informationen über Kennwörter finden Sie im Abschnitt '"Anforderungen an das Kennwort" (S. 28)'.

Anforderungen an das Kennwort

Das Kennwort für ein Benutzerkonto muss mindestens 9 Zeichen lang sein. Kennwörter werden zudem auf ihre Komplexität geprüft und dabei in eine der folgenden Kategorien eingeteilt:

- Schwach
- Mittel
- Stark

Ein schwaches Kennwort kann nicht gespeichert werden, auch wenn es 9 oder mehr Zeichen enthält. Kennwörter, die den Benutzernamen, den Anmeldenamen, die Benutzer-E-Mail-Adresse oder den Namen des Mandanten, zu dem ein Benutzerkonto gehört, enthalten, gelten immer als schwach. Auch Kennwörter, die besonders gängig sind, werden als schwach eingestuft.

Wenn Sie ein Kennwort stärker machen wollen, fügen Sie ihm mehr Zeichen hinzu. Es ist nicht zwingend notwendig, unterschiedliche Zeichentypen (wie Zahlen, Groß- und Kleinbuchstaben oder Sonderzeichen) zu verwenden. Aber damit können stärkere oder kürzere Kennwörter erzeugt werden.

Auf das Management-Portal zugreifen

1. Gehen Sie zur Service-Anmeldeseite.
2. Die Adresse der Anmeldeseite war in der Aktivierungs-E-Mail-Nachricht enthalten, die Sie erhalten haben.
3. Geben Sie den Anmeldenamen ein und klicken Sie dann auf **Weiter**.
4. Geben Sie das Kennwort ein und klicken Sie dann auf **Weiter**.

   Hinweis
   Um Cyber Protect Cloud vor Brute-Force-Angriffen zu schützen, werden Sie vom Portal nach 10 erfolglosen Anmeldeversuchen ausgesperrt. Die Zeitdauer der Sperrung beträgt 5 Minuten. Die Anzahl der fehlgeschlagenen Anmeldeversuche wird nach 15 Minuten zurückgesetzt.

5. Verwenden Sie das Menü auf der rechten Seite, um im Management-Portal zu navigieren.

Das Zeitlimit für das Management-Portal beträgt 24 Stunden für aktive Sitzungen und 1 Stunde für inaktive Sitzungen.

Einige Services bieten die Möglichkeit, von der Service-Konsole zum Management-Portal zu wechseln.

Kontakte im Assistenten 'Unternehmensprofil' konfigurieren

Sie können Kontaktinformationen für Ihr Unternehmen konfigurieren. Wir werden Informationen über Updates zu neuen Funktionen und anderen wichtigen Änderungen auf der Plattform an die von Ihnen angegebenen Kontakte senden.

Wenn Sie sich erstmals am Management-Portal anmelden, wird Sie der Unternehmensprofil-Assistent durch die grundlegenden Informationen über das Unternehmen und die anzugebenden Kontakte führen.

Sie können Kontakte aus Benutzern erstellen, die bereits in der Cyber Protect-Plattform vorhanden sind, oder Kontaktinformationen von Personen hinzufügen, die keinen Zugriff auf den Service haben.

So können Sie Unternehmenskontakte mit dem Unternehmensprofil-Assistenten konfigurieren

1. Spezifizieren Sie unter **Firmeninformationen** die folgenden Angaben zu Ihrem Unternehmen:
   - **Offizieller (rechtlicher) Firmenname**
   - **Juristische Firmenadresse (Adresse des Hauptsitzes)**
     - **Land**
     - **PLZ**
2. Klicken Sie auf **Weiter**.
3. Konfigurieren Sie unter **Firmenkontakte** die entsprechenden Kontakte für folgende Zwecke:
   - **Rechnungskontakt** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
   - **Geschäftskontakt** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.
   - **Technischer Kontakt** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.

   Sie können einen Kontakt auch für mehrere Zwecke verwenden.

   Wählen Sie eine Option, um den Kontakt zu erstellen.
   - **Aus vorhandenem Benutzer erstellen**. Wählen Sie im Listenfeld einen Benutzer aus.
   - **Einen neuen Kontakt erstellen**. Geben Sie folgende Kontaktinformationen an:
     - **Vorname** – Der Vorname der Kontaktperson. Dieses Feld ist erforderlich.
     - **Nachname** – Der Nachname der Kontaktperson. Dieses Feld ist erforderlich.
     - **Geschäftliche E-Mail** – Die E-Mail-Adresse der Kontaktperson. Dieses Feld ist erforderlich.
     - **Geschäftliche Telefonnummer** – Dieses Feld ist optional.
     - **Position** – Dieses Feld ist optional.
4. Wenn Sie den Rechnungskontakt außerdem auch als geschäftlichen oder technischen Kontakt verwenden wollen, markieren Sie die entsprechenden Kennzeichnungen (Flags) im Bereich **Rechnungskontakt**:
   - **Verwenden Sie denselben Kontakt als Geschäftskontakt**
   - **Verwenden Sie denselben Kontakt als technischen Kontakt**
5. Klicken Sie auf **Fertig**.

   Als Ergebnis werden die Kontakte erstellt. Sie können die Informationen bearbeiten und weitere Kontakte im Bereich **Unternehmensverwaltung –> Unternehmensprofil** der Management-Konsole konfigurieren, wie im Abschnitt Firmenkontakte konfigurieren beschrieben.

Vom Management-Portal aus auf die Cyber Protect-Konsole zugreifen

1. Gehen Sie im Management-Portal zu **Monitoring** –> **Nutzung**.
2. Wählen Sie unter **Cyber Protect** das Element **Schutz** und klicken Sie dann auf **Service verwalten**.

   Alternativ können Sie unter **Clients** einen Kunden auswählen und dann auf **Service verwalten** klicken.

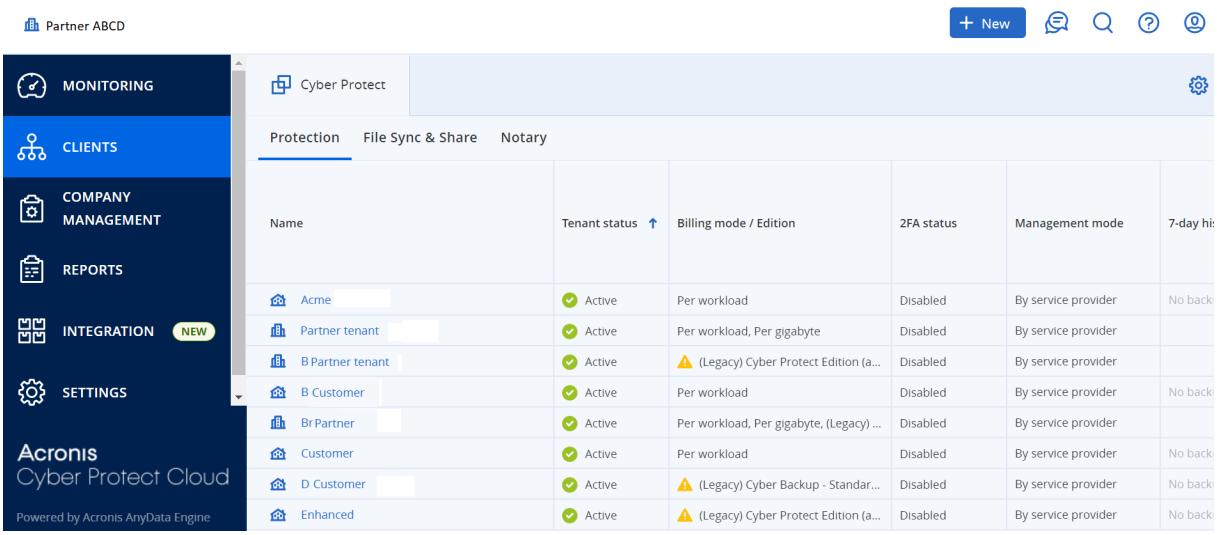
Als Ergebnis werden Sie auf die Cyber Protect-Konsole umgeleitet.

Wichtig
Wenn sich der Kunde im Verwaltungsmodus **Self-Service** befindet, können Sie keine Services für ihn verwalten. Nur die Kunden-Administratoren können den Modus des Kunden auf **Durch den Service-Provider verwaltet** ändern und dann die Services verwalten.

Im Management-Portal navigieren

Wenn Sie das Management-Portal verwenden, arbeiten Sie jederzeit innerhalb eines Mandanten. Der Name dieses Mandanten wird in der oberen linken Ecke angezeigt.

Standardmäßig ist die höchste Hierarchie-Ebene ausgewählt, die für Sie verfügbar ist. Klicken Sie auf den Namen eines Mandanten in der Liste, um durch die Hierarchie zu blättern. Wenn Sie zu einer höheren Ebene zurück wollen, klicken Sie in der linken oberen Ecke auf den entsprechenden Namen.



Alle Teile der Benutzeroberfläche betreffen und beeinflussen nur denjenigen Mandanten, in dem Sie gerade arbeiten. Beispiel:

- In der Registerkarte **Clients** werden nur solche Mandanten angezeigt, die dem Mandanten, in dem Sie gerade arbeiten, in der Hierarchie untergeordnet sind.
- In der Registerkarte **Unternehmensverwaltung** werden das Unternehmensprofil und die Benutzerkonten angezeigt, die in dem Mandanten vorhanden sind, in dem Sie gerade arbeiten.
- Mithilfe der Schaltfläche **Neu** können Sie einen Mandanten oder ein neues Benutzerkonto nur in dem Mandanten erstellen, in dem Sie gerade arbeiten. Beachten Sie, dass Ihnen in diesem Menü möglicherweise weitere Optionen angezeigt werden, je nachdem, welche Services Sie abonniert haben. Wenn Sie zum Beispiel den Advanced Automation Service aktiviert haben, können Sie auch neue Tickets und Zeiterfassungen erstellen.

Die Neuerungen im Management-Portal

Wenn neue Funktionen von Cyber Protect Cloud veröffentlicht werden, wird Ihnen bei der Anmeldung am Management-Portal ein Pop-up-Fenster mit einer kurzen Beschreibung dieser Funktionen angezeigt.

Sie können die Beschreibung der neuen Funktionen auch einsehen, indem Sie in der linken unteren Ecke des Management-Portal-Hauptfensters auf den Link **Neuerungen** klicken.

Zugriff auf die Weboberfläche beschränken

Administratoren können den Zugriff auf die Weboberfläche beschränken, indem sie eine Liste von IP-Adressen spezifizieren, über die sich die Mitglieder eines Mandanten an der Weboberfläche anmelden dürfen.

Diese Beschränkung gilt auch für Zugriffe auf das Verwaltungsportal über die API.

Hinweis
Diese Beschränkung gilt nur für die Ebene, für die sie eingerichtet wurde. Sie gilt nicht für die Mitglieder von Untermandanten.

So beschränken Sie den Zugriff auf die Weboberfläche

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, in dem Sie den Zugriff beschränken wollen.
3. Klicken Sie auf **Einstellungen** –> **Sicherheit**.
4. Aktivieren Sie den Schalter **Anmeldekontrolle**.
5. Spezifizieren Sie bei **Zulässige IP-Adressen** diejenigen IP-Adressen, die Zugriff erhalten sollen. Sie können für Ihre Eingabe jeden der folgenden Parameter verwenden, jeweils per Semikolon abgetrennt:
   - IP-Adressen, beispielsweise: 192.0.2.0
   - IP-Bereiche, beispielsweise: 192.0.2.0-192.0.2.255

- Subnetze, beispielsweise: 192.0.2.0/24

6. Klicken Sie auf **Speichern**.

Hinweis
Für Service Provider, die Cyber Infrastructure verwenden (Hybrid-Modell):

Wenn im Management-Portal der Schalter **Anmeldekontrolle** unter **Einstellungen** –> **Sicherheit** aktiviert ist, müssen Sie die externe öffentliche IP-Adresse (oder IP-Adressen) der Cyber Infrastructure-Knoten zur Liste **Zulässige IP-Adressen** hinzufügen.

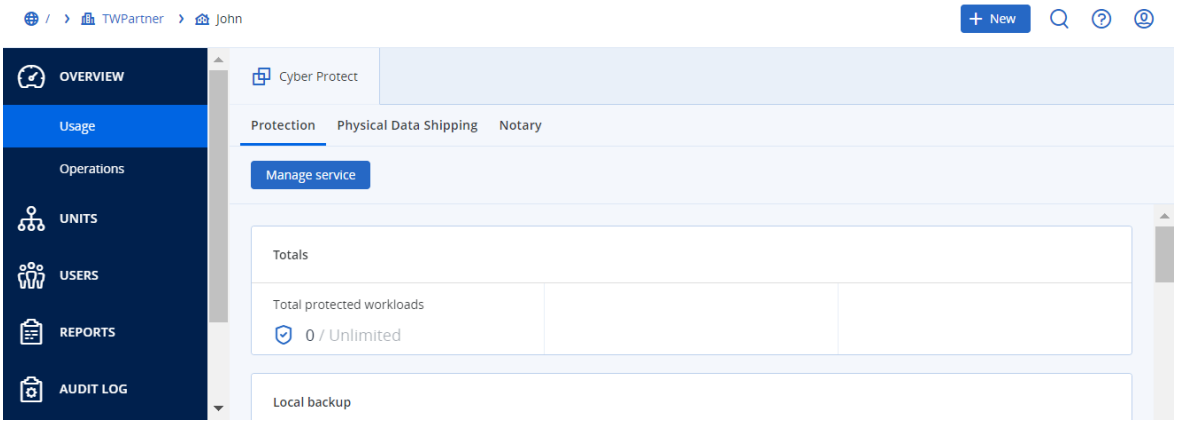
Auf die Services zugreifen

Registerkarte Überblick

Der Bereich **Überblick** –> **Nutzung** ermöglicht Ihnen eine Übersicht über die Service-Nutzung und auf die Services zuzugreifen, die für den Mandanten, in dem Sie arbeiten, verfügbar sind.

So verwalten Sie mit der Registerkarte 'Überblick' einen Service für einen Mandanten

1. Gehen Sie zu dem Mandanten, für den Sie einen Service verwalten wollen, und klicken Sie dann auf **Überblick** –> **Nutzung**.
   Beachten Sie, dass einige Services auf Ebene des übergeordneten Mandanten und des Kunden-Mandanten verwaltet werden können – während dies bei anderen Services nur auf Ebene des Kunden-Mandanten möglich ist.
2. Klicken Sie auf den Namen des Services, den Sie verwalten wollen, und anschließend auf **Service verwalten** oder **Service konfigurieren**.
   Weitere Informationen zur Nutzung der Services finden Sie in den Benutzeranleitungen, die in den Service-Konsolen verfügbar sind.

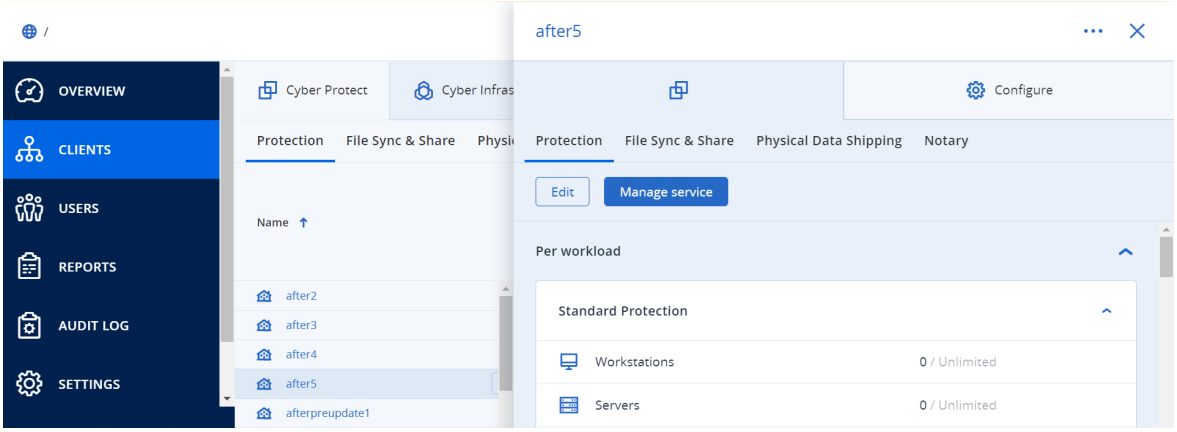


Registerkarte Clients

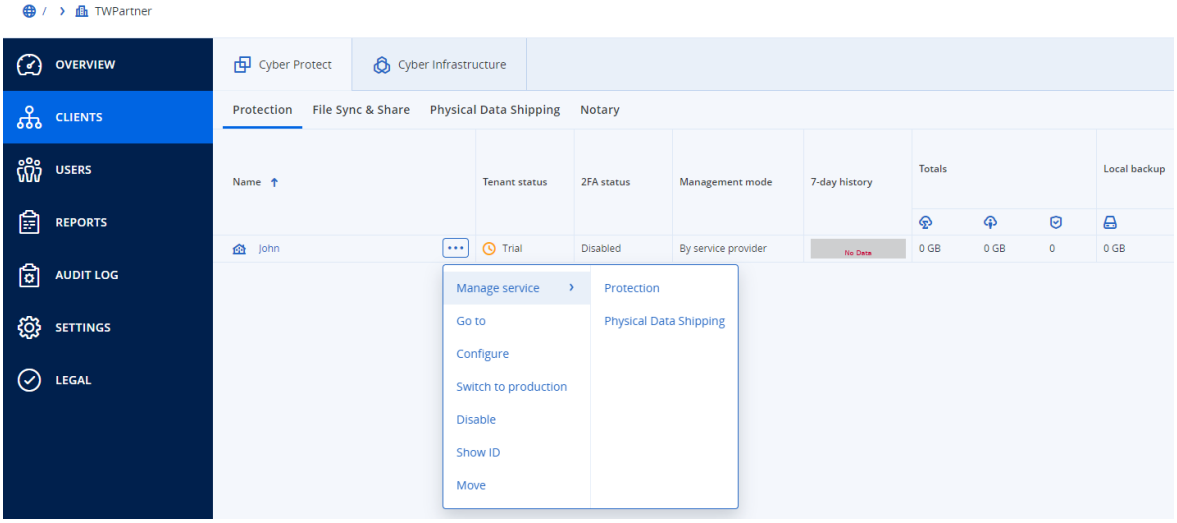
Die Registerkarte **Clients** zeigt die Untermandanten des Mandanten an, in dem Sie arbeiten, und ermöglicht Ihnen auf die Services in diesen Mandanten zuzugreifen.

So verwalten Sie mit der Registerkarte 'Clients' einen Service für einen Mandanten

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Clients**, wählen Sie den Mandanten aus, für den Sie einen Service verwalten wollen, klicken Sie auf den Namen oder das Symbol des Services, den Sie verwalten wollen, und klicken Sie anschließend auf **Service verwalten** oder **Service konfigurieren**.



   - Klicken Sie auf **Clients**, klicken Sie neben dem Namen des Mandanten, für den Sie einen Service verwalten wollen, auf das Drei-Punkte-Symbol, klicken Sie auf **Service verwalten** und wählen Sie abschließend den zu verwaltenden Service aus.



   Beachten Sie, dass einige Services auf Ebene des übergeordneten Mandanten und des Kunden-Mandanten verwaltet werden können – während dies bei anderen Services nur auf Ebene des Kunden-Mandanten möglich ist.

   Weitere Informationen zur Nutzung der Services finden Sie in den Benutzeranleitungen, die in den Service-Konsolen verfügbar sind.

7-Tage-Verlaufsleiste

In der Anzeige **Clients** zeigt die **7-Tage-Verlauf**sleiste den Status der Workload-Backups für jeden Kunden-Mandanten für die letzten sieben Tage an. Die Leiste ist in 168 farbige Linien unterteilt. Jede Linie steht für ein einstündiges Intervall und zeigt den schlechtesten Status eines Backups innerhalb des entsprechenden einstündigen Intervalls an.

Die folgende Tabelle informiert darüber, was die jeweiligen Farben dieser Linien bedeuten.

Farbe	Beschreibung
rot	mindestens eines der Backups innerhalb des einstündigen Zeitraums ist fehlgeschlagen
orange	mindestens eines der Backups innerhalb des einstündigen Zeitraums wurde mit einer Warnung (aber ohne Backup-Fehler) abgeschlossen
grün	es gab mindestens ein erfolgreiches Backup während des einstündigen Zeitraums (ohne Backup-Fehler oder Warnungen)
grau	es gab keine abgeschlossenen Backups während des einstündigen Zeitraums

In der **7-Tage-Verlauf**sleiste wird so lange 'Keine Backups' angezeigt, bis die entsprechenden Statistiken erfasst wurden.

Bei Partner-Mandanten bleibt die **7-Tage-Verlauf**sleiste leer, da hier keine aggregierten Statistiken unterstützt werden.

Benutzerkonten und Mandanten

Es gibt zwei Arten von Benutzerkonten: Administrator- und Benutzerkonten.

- **Administratoren** haben Zugriff auf das Management-Portal. Sie verfügen in allen Services über die Administratoren-Rolle.
- **Benutzer** haben keinen Zugriff auf das Management-Portal. Wie sie auf die Services zugreifen können und welche Rollen sie in den Services haben, wird von einem Administrator definiert.

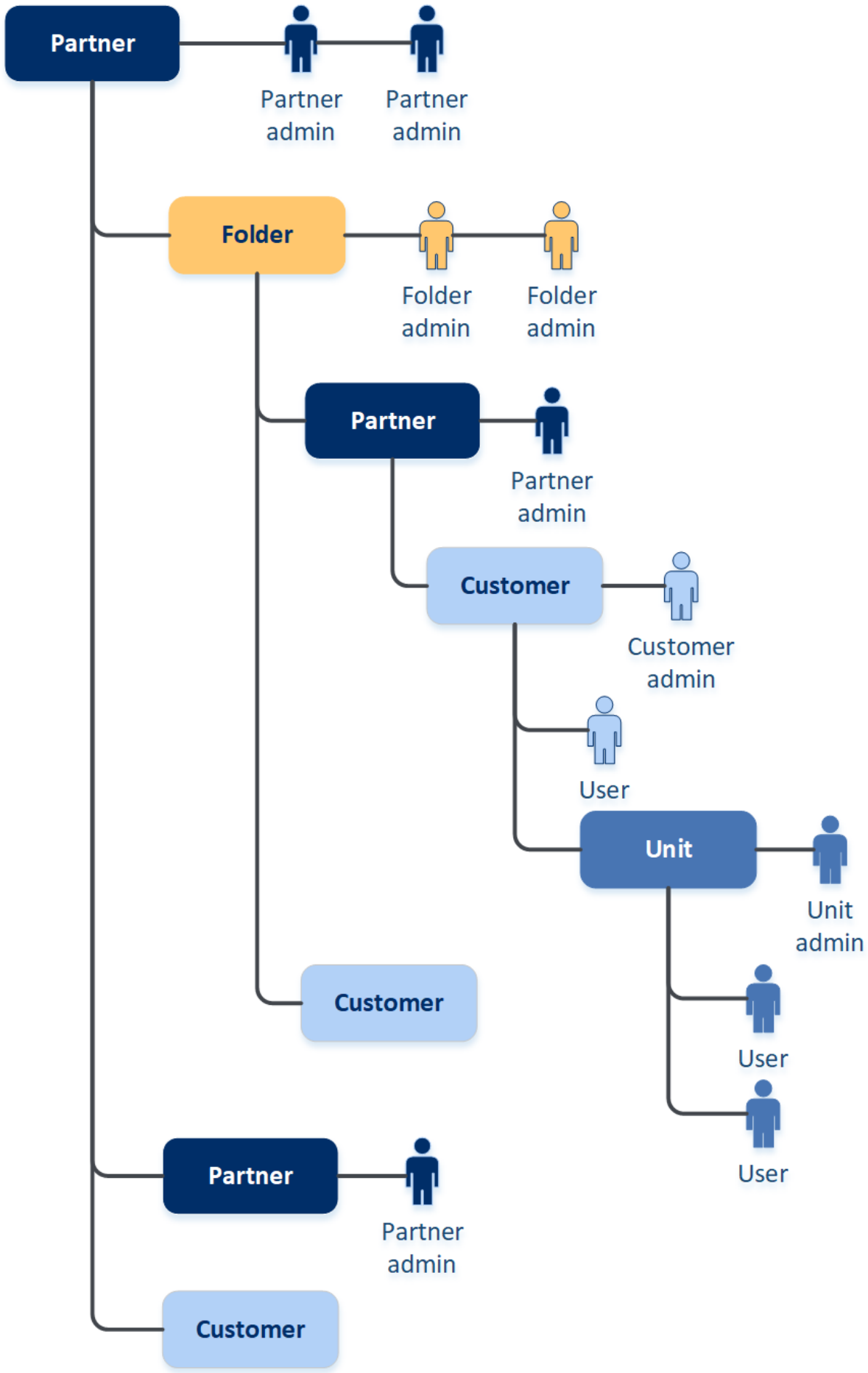
Jedes Konto gehört zu einem Mandanten. Ein Mandant ist ein Teil der Management Server-Ressourcen (wie Benutzerkonten und Untermandanten) und Service-Angebote (aktivierte Services und Angebotselemente in diesen), die für einen Partner oder Kunden bestimmt sind. Die Mandanten-Hierarchie soll die Kunde-/Dienstleister-Beziehung zwischen Service-Benutzern und Service-Anbietern widerspiegeln.

- Ein Mandant vom Typ **Partner** entspricht typischerweise einem Service-Provider, der die Services weiterverkauft/anbietet.
- Ein Mandant vom Typ **Ordner** ist ein zusätzlicher Mandant, der normalerweise von Partner-Administratoren für Gruppen-Partner und Kunden verwendet wird, um unterschiedliche Angebote und/oder ein unterschiedliches Branding zu konfigurieren.
- Der Mandant vom Typ **Kunde** entspricht typischerweise einem Unternehmen, welches diese Services verwendet.
- Der Mandant vom Typ **Abteilung** entspricht normalerweise einer bestimmten Einheit bzw. einem bestimmten Bereich innerhalb des Unternehmens.

Ein Administrator kann Mandanten, Administrator-Konten sowie Benutzerkonten innerhalb oder unterhalb seiner Ebene in der Hierarchie erstellen sowie verwalten.

Der Administrator eines übergeordneten Mandanten vom Typ **Partner** kann als untergeordneter Administrator in Mandanten vom Typ **Kunde** oder **Partner** agieren, deren Verwaltungsmodus **Durch den Service-Provider verwaltet** ist. Daher kann der Administrator auf Partnerebene beispielsweise Benutzerkonten und Services verwalten oder auf Backups und andere Ressourcen im Untermandanten zugreifen. Die Administratoren der unteren Ebene können jedoch den Zugriff von höherstufigen Administratoren auf ihre Mandanten beschränken.

Die folgende Abbildung verdeutlicht eine Beispielshierarchie mit Partner-, Ordner-, Kunden- und Abteilungs-Mandanten.


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

Die nachfolgende Tabelle fasst die Aktionen zusammen, die von Administratoren und Benutzern durchgeführt werden können.

Aktion	Benutzer	Kunden- und Abteilungsadministratoren	Partner- und Ordner-Administratoren
Mandanten erstellen	Nein	Ja	Ja
Konten erstellen	Nein	Ja	Ja
Die Software herunterladen und installieren	Ja	Ja	Nein*
Services verwalten	Ja	Ja	Ja
Berichte über die Service-Nutzung erstellen	Nein	Ja	Ja
Branding konfigurieren	Nein	Nein	Ja

Hinweis
Ein Benutzer kann aus jedem Mandantentyp erstellt werden und eine gemeinsame E-Mail-Adresse haben, solange er aus dem am meisten privilegierten zum am wenigsten privilegierten erstellt wird. Ein Beispiel: Ein Partner-Mandant kann einen Ordner-, Kunden- und Abteilungs-Mandanten erstellen, während ein Kunden-Mandant keinen Ordner-Mandanten erstellen kann.

Mandanten verwalten

Folgende Mandanten sind in Cyber Protect verfügbar:

- Ein **Partner**-Mandant wird normalerweise für jeden Partner erstellt, der die Partnerschaftsvereinbarung unterschreibt.
- Ein **Ordner**-Mandant wird normalerweise für Gruppen-Partner und Kunden erstellt, um unterschiedliche Angebote und/oder ein unterschiedliches Branding zu konfigurieren.
- Ein **Kunden**-Mandant wird normalerweise für jede(s) Organisation/Unternehmen erstellt, welche (s) sich für den Service anmeldet.
- Ein **Abteilungs**-Mandant wird innerhalb eines Kunden-Mandanten angelegt, um den Service auf eine neue Organisationseinheit zu erweitern.

Die Schritte zum Erstellen und Konfigurieren eines Mandanten hängen davon ab, welchen Mandanten Sie erstellen. Grundsätzlich besteht der Prozess aber aus folgenden Schritten:

1. Erstellen Sie den Mandanten.
2. Wählen Sie die Services für den Mandanten.
3. Konfigurieren Sie die Angebotselemente für den Mandanten.

Einen Mandanten erstellen

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, in dem Sie einen Mandanten erstellen wollen.
3. Klicken Sie in der rechten oberen Ecke auf **Neu** und dann – abhängig vom Typ des zu erstellenden Mandanten – auf eines der folgenden Elemente:
   - Ein **Partner**-Mandant wird normalerweise für jeden Partner erstellt, der die Partnerschaftsvereinbarung unterschreibt.
   - Ein **Ordner**-Mandant wird normalerweise für Gruppen-Partner und Kunden erstellt, um unterschiedliche Angebote und/oder ein unterschiedliches Branding zu konfigurieren.
   - Ein **Kunden**-Mandant wird normalerweise für jede(s) Organisation/Unternehmen erstellt, welche(s) sich für den Service anmeldet.
   - Ein **Abteilungs**-Mandant wird innerhalb eines Kunden-Mandanten angelegt, um den Service auf eine neue Organisationseinheit zu erweitern.

   Ein Mandant vom Typ **Lieferant** ist ebenfalls verfügbar, allerdings nur, wenn der Advanced Automation Service aktiviert ist. Lieferanten werden auf der Registerkarte **Lieferanten** erstellt, auf die Sie über **Verkauf und Abrechnung –> Unternehmensverwaltung** zugreifen können.

   Die verfügbaren Typen hängen vom Typ der übergeordneten Mandanten ab. Hinweis: Wenn der Advanced Automation Service aktiviert ist, können Sie im Abschnitt **Abrechnungsinformationen** auch den entsprechenden Mandantentyp auswählen (siehe Abschnitt '"Abrechnungsinformationen für einen Mandanten definieren" (S. 42)').
4. Spezifizieren Sie bei **Name** eine Bezeichnung für den neuen Mandanten.
5. [Nur beim Erstellen eines Partner-Mandanten] Geben Sie den **Offiziellen (rechtlichen) Firmennamen** (notwendig) sowie die **USt.-Identifikationsnummer/Steuernummer/Handelsregisternummer** (optional) ein.
6. [Nur bei Erstellung einer Kunden-Mandanten] Wählen Sie bei **Modus**, ob der Mandant die Services im Test- oder Produktionsmodus verwendet. Die monatlichen Service-Nutzungsberichte enthalten Nutzungsdaten für Mandanten in beiden Modi.

Wichtig

Der Testmodus bietet einen 30-tägigen Evaluierungszeitraum und ermöglicht, das Produkt vollumfänglich zu testen. Sobald ein Kunde in den Produktionsmodus umgeschaltet wird, wird dessen Service-Nutzung automatisch im nächsten Abrechnungszyklus berücksichtigt.

Sie können jederzeit in den Produktionsmodus wechseln. Beachten Sie jedoch, dass ein Wechsel vom Produktions- zurück in den Testmodus nicht möglich ist.

Wenn Sie sich entscheiden, die Testphase für einen Kunden zu beenden, müssen Sie auch den entsprechenden Kunden-Mandanten löschen. Anderenfalls wird der Kunde nach Ablauf des 30-tägigen Testzeitraums automatisch in den Produktionsmodus versetzt und dessen entsprechende Service-Nutzung im nächsten Abrechnungszyklus berücksichtigt. Weitere Informationen dazu finden Sie in diesem Knowledge Base Artikel.

7. Wählen Sie bei **Verwaltungsmodus** einen der folgenden Modi, um den Zugriff auf den Mandanten zu verwalten:
   - **Self-Service** – dieser Modus beschränkt für die Administratoren des übergeordneten Mandanten den Zugriff auf diesen Mandanten: sie können nur die Eigenschaften des Mandanten ändern, aber nicht auf dessen Elemente (z.B. Mandanten, Benutzer, Services, Backups und andere Ressourcen) zugreifen oder diese verwalten.
   - **Durch den Service-Provider verwaltet** – dieser Modus gewährt den Administratoren des übergeordneten Mandanten vollen Zugriff auf den Mandanten: Eigenschaften ändern, Mandanten, Benutzer und Services verwalten; auf Backups und andere Ressourcen zugreifen. Dieser Modus ist standardmäßig ausgewählt.

   Nur der Administrator des von Ihnen erstellten Mandanten kann den Verwaltungsmodus ändern, wenn der Modus mit **Self-Service** festgelegt ist. Hierfür kann der Administrator des erstellten Mandanten zu **Einstellungen** –> **Sicherheit** gehen und den Schalter **Support-Zugang** einstellen.

   Sie können den ausgewählten Verwaltungsmodus für Ihre Untermandanten auf der Registerkarte **Clients** überprüfen.
8. Aktivieren oder deaktivieren Sie bei **Sicherheit** die Zwei-Faktor-Authentifizierung für den Mandanten.
   Wenn diese Option aktiviert ist, müssen alle Benutzer dieses Mandanten für einen sichereren Zugriff eine Zwei-Faktor-Authentifizierung für ihre Konten einrichten. Benutzer müssen die Authentifizierungsapplikation auf ihren Zweit-Faktor-Geräten installieren und den einmalig generierten TOTP-Code zusammen mit den herkömmlichen Anmeldedaten (Benutzername, Kennwort) verwenden, um sich an der Konsole anmelden zu können. Weitere Informationen finden Sie unter 'Zwei-Faktor-Authentifizierung einrichten'. Wenn Sie den Zwei-Faktor-Authentifizierungsstatus für Ihre Kunden einsehen wollen, gehen Sie zu **Clients**.
9. [Nur wenn ein Kunden-Mandanten im Compliance-Modus erstellt wird] Aktivieren Sie bei **Sicherheit** das Kontrollkästchen **Compliance-Modus**.

   In diesem Modus sind nur verschlüsselte Backups erlaubt. Das Verschlüsselungskennwort muss auf dem geschützten Gerät festgelegt werden. Ohne dieses Kennwort wird die Erstellung von Backups fehlschlagen. Aktionen, die die Bereitstellung des Verschlüsselungskennworts für einen Cloud Service erfordern, sind nicht verfügbar. Weitere Informationen dazu finden Sie hier: "Compliance-Modus" (S. 41).

   Wichtig
   Sie können den Compliance-Modus nicht mehr deaktivieren, nachdem der Mandant erstellt wurde.

10. Konfigurieren Sie bei **Administrator erstellen** ein Administratorkonto.

    Hinweis
    Das Erstellen eines Administrators ist zwingend erforderlich für einen Kunden-Mandanten und für einen Partner-Mandanten, bei dem der **Verwaltungsmodus** auf **Self-Service** festgelegt ist.

a. Geben Sie eine E-Mail-Adresse für das Administratorkonto ein. Diese E-Mail-Adresse dient auch als Anmeldename.
b. Wenn Sie lieber einen anderen Anmeldenamen als die E-Mail-Adresse verwenden wollen, müssen Sie das Kontrollkästchen **Anderen Anmeldenamen als die E-Mail-Adresse verwenden** aktivieren und dann einen entsprechenden Anmeldenamen sowie eine E-Mail-Adresse für das Administratorkonto eingeben.
   Die übrigen Felder sind optional, ermöglichen aber weitere Kommunikationskanäle, falls wir den Administrator kontaktieren müssen.
c. Wählen Sie eine Sprache aus.
   Wenn Sie keine Sprache auswählen, wird standardmäßig Englisch verwendet.
d. Spezifizieren Sie die Firmenkontakte.
   - **Abrechnung** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
   - **Technisch** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.
   - **Geschäftlich** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.

     Sie können einem Benutzer mehr als einen Firmenkontakt zuweisen.

11. Ändern Sie bei **Sprache** die Standardsprache für die in diesem Mandanten verwendete(n) Benachrichtigungen, Berichte und Software.
12. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
    - Klicken Sie auf **Speichern und schließen**, um die Erstellung des Mandanten zu beenden. In diesem Fall werden alle Dienste für den Mandanten aktiviert. Der Abrechnungsmodus für den Schutz Service wird mit 'pro Workload' festgelegt.
    - Um Services für den Mandanten auszuwählen, klicken Sie auf **Weiter**. Siehe Abschnitt '"Die Services für einen Mandanten auswählen" (S. 44)'.

Hinweis: Wenn der Advanced Automation Service aktiviert ist, können Sie jetzt Abrechnungsinformationen für Ihren Kunden festlegen, um ihm die bereitgestellten Services und Produkte in Rechnung zu stellen.

Compliance-Modus

Der Compliance-Modus ist für Kunden mit höheren Sicherheitsanforderungen konzipiert. Dieser Modus erfordert zwingend eine Verschlüsselung aller Backups und erlaubt nur lokal festgelegte Verschlüsselungskennwörter.

Im Compliance-Modus werden alle in einem Kunden-Mandanten und seinen Abteilungen erstellten Backups automatisch mit dem AES-Algorithmus und einer Tiefe von 256 Bit verschlüsselt. Die Anwender können die Verschlüsselungskennwörter nur auf den geschützten Geräten festlegen. Sie können keine Verschlüsselungskennwörter über Schutzpläne vergeben.

Wichtig
Ein Partner-Administrator kann den Compliance-Modus nur aktivieren, wenn er einen neuen Kunden-Mandanten erstellt. Und der Modus kann nachträglich nicht mehr deaktiviert werden. Bei bereits vorhandenen Mandanten kann der Compliance-Modus nicht nachträglich aktiviert werden.

Einschränkungen

- Der Compliance-Modus ist nur mit Agenten der Version 15.0.26390 oder höher kompatibel.
- Der Compliance-Modus ist nicht für Geräte verfügbar, die unter Red Hat Enterprise Linux 4.x oder 5.x (und deren Derivaten) laufen.
- Cloud Services können nicht auf Verschlüsselungskennwörter zugreifen. Aufgrund dieser Einschränkung sind einige Funktionen für Mandanten im Compliance-Modus nicht verfügbar.

Nicht unterstützte Funktionen

Folgende Funktionen sind für Mandanten im Compliance-Modus nicht verfügbar:

- Wiederherstellungen über die Cyber Protect-Konsole
- Durchsuchen von Backups auf Dateiebene über die Cyber Protect-Konsole
- Cloud-zu-Cloud-Backup
- Website-Backup
- Applikations-Backup
- Backup für Mobilgeräte
- Antimalware-Scan von Backups
- Safe Recovery
- Automatisches Erstellen von Positivlisten für Unternehmensapplikationen
- Data Protection-Karte
- Disaster Recovery
- Berichte und Dashboards, die sich auf die nicht verfügbaren Funktionen beziehen

Abrechnungsinformationen für einen Mandanten definieren

Wenn die Advanced Automation-Funktionalität für einen Mandanten aktiviert wird, müssen Sie Abrechnungsinformationen für den Mandanten festlegen. Die Abrechnungsinformationen ermöglichen es dem Mandanten, die Services und Produkte, die er anbietet, in Rechnung zu stellen.

Hinweis
Wenn die Abrechnungsinformationen nicht in dieser Phase definiert werden, werden Sie aufgefordert, die entsprechenden Informationen einzugeben, bevor Sie bestimmte Advanced-Automation-Funktionen (etwa, wenn Sie die Zeiterfassung genehmigen oder Verträge oder Verkaufsartikel erstellen) erstmalig einsetzen. Weitere Informationen finden Sie im Abschnitt '"Onboarding von bestehenden Kunden" (S. 184)'.

So können Sie Abrechnungsinformationen definieren

1. Definieren Sie im Bereich **Abrechnungsinformationen** des Dialogs 'Mandant erstellen/bearbeiten' folgende Felder:
   - **Unternehmensname**: Der Firmenname des Mandanten.
   - **Rechtsform**: Der juristisch korrekte Unternehmensname des Mandanten.
   - **Typ**: Der Advanced Automation-Mandantentyp (über **Partner**, **Kunde**, **Interessent** auswählbar)
   - **Schuldnercode**: (Optional) Der Kundencode, der in Drittanbieter-Systemen (wie z.B. einer Buchhaltungssoftware) verwendet wird.
   - **E-Mail**: Die E-Mail-Adresse des Mandanten, die mit der E-Mail-Adresse des Administrators im Bereich **Allgemeine Informationen** vordefiniert ist.
   - **Website**: (Optional) Die Website des Mandanten.
   - **Hauptgeschäftsstelle**: (Optional) Wählen Sie das übergeordnete Unternehmen (die Muttergesellschaft) aus der Liste aus.
   - **Umsatzsteuernummer**: (Optional) Die entsprechende Umsatzsteueridentifikationsnummer.
   - **Zeiterfassungsrundung (Minuten)**: Legen Sie die Zeit (in Minuten) für Ihre Ticket-Rundungszeit fest. Wenn eine Ticket-Arbeit zur Abrechnung genehmigt wurde, werden die abrechenbaren Gesamtstunden gemäß diesem Wert aufgerundet. Wenn Sie beispielsweise den Wert für die Rundungszeit mit 15 Minuten festlegen, wird die eine Ticket-Arbeitszeit von 7 Minuten vor der Rechnungsstellung auf 15 Minuten aufgerundet. Ebenso werden 21 Minuten auf 30 Minuten, 36 Minuten auf 45 Minuten und so weiter aufgerundet. Der Standardwert beträgt **10**.
   - **Zahlungsbedingungen (Tage)**: (Optional) Legen Sie die Anzahl an Tagen fest, in denen ein Kunde seine Zahlung zu leisten hat.
   - **Lastschrift**: (Optional) Aktivieren Sie das Kontrollkästchen, wenn die Zahlung per Bankeinzug vorgenommen wird. Wenn diese Option aktiviert ist, sind in den Verträgen, Verkaufsartikeln und Rechnungen Lastschriftzahlungen möglich.

     Mit dieser Option können im Abrechnungsprozess Lastschrifteinzelposten von manuellen Zahlungseinzelposten getrennt werden. Jede dieser Einzelpostenarten wird auf zwei verschiedene Rechnungen aufgeteilt und separat verarbeitet:
     - Kunden können Rechnungen per Überweisung oder über eine der Zahlungsintegrationen (PayPal, Stripe) bezahlen.
     - Kunden können ihre Rechnungen zwecks Lastschrifteinzug an ihre Hausbank senden.

- **Zwischensummen auf der Rechnung erstellen**: (Optional) Aktivieren Sie das Kontrollkästchen bei Bedarf.
- **Die Abrechnung zu einer Rechnung konsolidieren**: (Optional) Aktivieren Sie das Kontrollkästchen bei Bedarf.
- Wählen Sie im Bereich **Verkaufssteuer** (optional) die entsprechende Verkaufssteuer (die Standardsteuer für das Unternehmen). Wenn keine Verkaufssteuer ausgewählt ist, wird der Standardsteuersatz angewendet. Sie können auch das Kontrollkästchen **Steuerbefreit** aktivieren, wenn der Mandant diese Steuer nicht entrichten muss.
- Geben Sie im Bereich **Bankkonto** (optional) die Bankkontonummer für den Mandanten ein.
- Geben Sie im Bereich **Adresse** die entsprechenden Adressfelder ein.

2. Klicken Sie auf **Weiter**, um die Services für den Mandanten zu konfigurieren. Siehe Abschnitt '"Die Services für einen Mandanten auswählen" (S. 44)'.

Die Services für einen Mandanten auswählen

Standardmäßig sind alle Services aktiviert, wenn Sie einen neuen Mandanten erstellen. Sie können festlegen, welche Services für die Benutzer innerhalb des Mandanten und seiner Untermandanten verfügbar sein sollen.

Sie können außerdem Services für mehrere bestehende Mandanten in einer Aktion auswählen und aktivieren. Weitere Informationen finden Sie im Abschnitt '"Services für mehrere bestehende Mandanten aktivieren" (S. 46)'.

Diese Prozedur ist nicht für einen Abteilungs-Mandanten anwendbar.

So können Sie die Services für einen Mandanten auswählen

1. Wählen Sie im Bereich **Services auswählen** des Dialogs 'Mandant erstellen/bearbeiten' einen Abrechnungsmodus oder eine Edition.
   - Wählen Sie den Abrechnungsmodus **Pro Workload** oder **Pro Gigabyte** – und deaktivieren Sie dann die Kontrollkästchen für diejenigen Services, die Sie für den Mandanten deaktivieren wollen.
     Die Zusammenstellung der Services ist für beide Abrechnungsmodi identisch.
     Bei der Advanced Disaster Recovery-Funktionalität: Wenn Sie einen eigenen Disaster Recovery-Speicherort unter Ihrem Konto registriert haben, können Sie den Speicherort aus dem Listenfeld auswählen.
   - Wenn Sie eine Legacy-Edition verwenden wollen, müssen Sie das Optionsfeld **Legacy-Editionen** aktivieren und eine entsprechende Edition aus dem Listenfeld auswählen.

   Deaktivierte Services werden vor den Benutzern innerhalb des Mandanten (und seiner Untermandanten) verborgen.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Speichern und schließen**, um die Erstellung des Mandanten zu beenden. In diesem Fall werden für den Mandanten alle Angebotselemente für die ausgewählten Services mit einer unbegrenzten Quota aktiviert.

- Um die Angebotselemente für den Mandanten zu konfigurieren, klicken Sie auf **Weiter**. Siehe Abschnitt '"Die Angebotselemente für einen Mandanten konfigurieren" (S. 45)'.

Die Angebotselemente für einen Mandanten konfigurieren

Wenn Sie einen neuen Mandanten erstellen, werden alle Angebotselemente für die ausgewählten Services aktiviert. Sie können festlegen, welche Angebotselemente für die Benutzer innerhalb des Mandanten und seiner Untermandanten verfügbar sein sollen – und dann Quotas für diese festlegen.

Diese Prozedur ist nicht für einen Abteilungs-Mandanten anwendbar.

So können Sie die Angebotselemente für einen Mandanten konfigurieren

1. Deaktivieren Sie im Bereich **Services konfigurieren** des Dialogs 'Mandant erstellen/bearbeiten' bei jeder Service-Registerkarte die Kontrollkästchen für diejenigen Angebotselemente, die Sie deaktivieren wollen.
   Die den deaktivierten Angebotselementen entsprechenden Funktionalitäten werden für die Benutzern innerhalb des Mandanten (und seiner Untermandanten) nicht verfügbar sein.
2. Bei einigen Services können Sie Storages auswählen, die für den neuen Mandanten verfügbar sein sollen. Storages werden nach Speicherorten gruppiert. Sie können aus der Liste von Speicherorten und Storages auswählen, die für Ihren Mandanten verfügbar sind.
   - Wenn Sie einen Partner-/Ordner-Mandanten erstellen, können Sie mehrere Speicherorte und Storages für jeden Service auswählen.
   - Wenn Sie einen Kunden-Mandanten erstellen, müssen Sie einen Speicherort auswählen und dann innerhalb dieses Speicherortes einen Storage pro Service auswählen. Die dem Kunden zugewiesenen Storages können auch zu einem späteren Zeitpunkt geändert werden, jedoch nur, wenn deren Nutzung 0 GB beträgt. Also entweder bevor der Kunde begonnen hat, den Storage zu nutzen – oder nachdem der Kunde all seine Backups aus dem Storage gelöscht hat. Die Anzeige der Informationen über die Speicherplatznutzung erfolgt nicht in Echtzeit. Die Aktualisierung dieser Informationen kann bis zu 24 Stunden dauern.

   Ausführlichere Informationen über Storages finden Sie im Abschnitt 'Speicherorte und Storage verwalten'.
3. Wenn Sie die Quota für ein Element spezifizieren wollen, müssen Sie neben dem Angebotselement auf den Link **Unbegrenzt** klicken.
   Diese Quotas sind 'weich'. Sollte einer dieser Werte überschritten werden, dann wird eine E-Mail-Benachrichtigung an die Mandanten-Administratoren und die Administratoren des übergeordneten Mandanten gesendet. Beschränkungen zur Nutzung der Services werden nicht angewendet. Für einen Partner-Mandanten wird erwartet, dass die Nutzung des Angebotselements die Quota überschreiten kann, weil beim Erstellen eines Partner-Mandanten keine Überschreitung festgelegt werden kann.
4. [Nur bei Erstellung eines Kunden-Mandanten] Spezifizieren Sie die Quota-Überschreitungen. Eine Überschreitung erlaubt es einem Kunden-Mandanten, die Quota um den spezifizierten Wert zu überschreiten. Wird die Überschreitung überschritten, werden Nutzungsbeschränkungen auf den entsprechenden Service angewendet.

5. Klicken Sie auf **Speichern und schließen**.

   Der neu erstellte Mandant wird in der Registerkarte **Clients** der Management-Konsole angezeigt.

   Wenn Sie die Mandanten-Einstellungen bearbeiten oder den Administrator ändern wollen, müssen Sie den entsprechenden Mandanten zuerst in der Registerkarte **Clients** auswählen und dann auf das Stiftsymbol in dem Bereich klicken, den Sie bearbeiten wollen.

Services für mehrere bestehende Mandanten aktivieren

Sie können Services, Editionen, Pakete und Angebotselemente für mehrere Mandanten (bis zu maximal 100 in einer Sitzung) massenweise aktivieren.

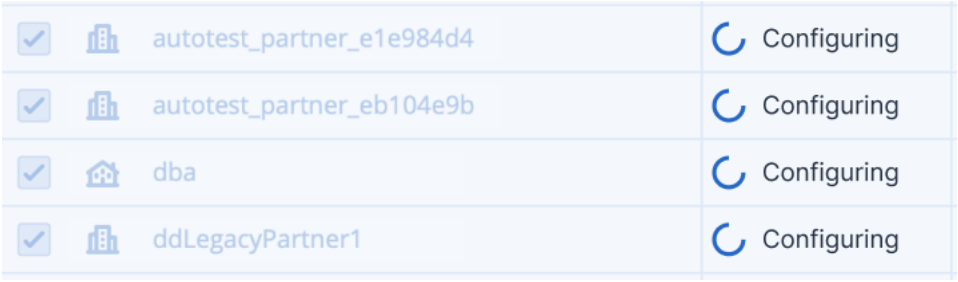
Diese Prozedur gilt für Subroot-, Partner-, Ordner- und Kunden-Mandanten. Sie können die Mandanten, egal welcher Art, gleichzeitig auswählen.

So können Sie Services für mehrere Mandanten aktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Klicken Sie in der rechten oberen Ecke auf **Services konfigurieren**.
3. Sie können jeden der Mandanten, für den Sie Services aktivieren wollen, auswählen, indem Sie das Kontrollkästchen neben dem Mandantennamen aktivieren und anschließend auf **Weiter** klicken.
4. Wählen Sie im Bereich **Services auswählen** die gewünschten Services aus, die Sie auf alle ausgewählten Mandanten anwenden wollen, und klicken Sie anschließend auf **Weiter**.

   Hinweis
   Sie können einen zuvor aktivierten Service auf dieser Anzeige nicht wieder deaktivieren. Alle Services, Editionen und Angebotselemente, die vor Beginn dieser Prozedur bereits ausgewählt waren, bleiben aktiviert.

5. Wählen Sie im Bereich **Services konfigurieren** die Service-Funktionen und Angebotselemente aus, die Sie für die ausgewählten Mandanten aktivieren wollen, und klicken Sie dann auf **Weiter**.
6. Überprüfen Sie im Bereich **Übersicht** die Änderungen, die auf die ausgewählten Mandanten angewendet werden sollen.
   Sie können auf **Alle erweitern** klicken, wenn Sie alle für die Mandanten ausgewählten Services und Angebotselemente einsehen wollen, die angewendet werden sollen. Alternativ können Sie die Anzeige für jeden Mandanten erweitern, wenn Sie die ausgewählten Services und Angebotselemente einsehen wollen, die speziell für diesen Mandanten gelten.
7. Klicken Sie auf **Änderungen anwenden**. Während die Services für einen Mandanten konfiguriert werden, wird dieser deaktiviert – und in der Spalte **Mandantenstatus** werden (wie unten dargestellt) diejenigen Services und Angebotselemente angezeigt, die gerade konfiguriert werden.



8. Wenn die Konfiguration der Services und Angebotselemente erfolgreich auf die ausgewählten Mandanten angewendet wurde, wird eine Bestätigungsmeldung angezeigt.
   Wenn die Services und Angebotselemente aus irgendeinem Grund nicht auf einen Mandanten angewendet werden konnten, wird in der Spalte **Mandantenstatus** der Wert **Nicht angewendet** angezeigt. Klicken Sie auf **Erneut versuchen**, um die Konfiguration für die ausgewählten Mandanten zu überprüfen.

Die Konfiguration eines Mandanten einsehen und aktualisieren

Nachdem ein Mandant erstellt und konfiguriert wurde, können Sie dessen konfigurierte Services und Angebote bei Bedarf einsehen und aktualisieren.

So können Sie die Konfiguration eines Mandanten einsehen und aktualisieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Klicken Sie auf das Drei-Punkte-Symbol für denjenigen Mandanten, den Sie einsehen oder aktualisieren wollen, und wählen Sie dann den Befehl **Konfigurieren**.
3. Im rechten Fensterbereich können Sie Folgendes tun:
   - Sie können die Einstellungen für die verfügbaren Services aktualisieren, indem Sie auf die Registerkarte des jeweiligen Service klicken. Klicken Sie beispielsweise auf die Registerkarte **Schutz**, um den Service zu aktualisieren und zu verwalten.
   - Wenn Sie auf die Registerkarte **Konfigurieren** klicken, können Sie die verschiedenen Bereiche der Mandanten-Konfiguration einsehen und aktualisieren:
     - **Service**: Sie können Services je nach Bedarf aktivieren oder deaktivieren.
     - **Unternehmensprofil**: Sie können bei Bedarf das Unternehmensprofil aktualisieren und Unternehmenskontakte hinzufügen oder entfernen.
     - **Allgemeine Einstellungen**: Aktualisieren Sie allgemeine Informationen über das Unternehmen (wie den Namen, das Land, die Sprache und den Status des Compliance-Modus.
     - **Abrechnungsdaten**: Nur bei aktiviertem Advanced Automation Service: Sie können hier Ihre Abrechnungs- und Adressdaten aktualisieren.
     - **Finanzen**: (Nur lesen) Nur bei aktiviertem Advanced Automation Service verfügbar: Sie können hier eine Reihe wichtiger Metriken einsehen (z.B. den aktuellen Wert von Verträgen und zu fakturierenden Verkaufsartikeln sowie die Anzahl der betreuten Endbenutzer).
     - **Tickets**: (Nur Lesen) Nur bei aktiviertem Advanced Automation Service verfügbar: Sie können hier wichtige Metriken einsehen, wie etwa offene Tickets, SLA-Verletzungen oder

nicht zugewiesene Tickets. Sie können außerdem eine Liste der aktuell offenen Tickets einsehen.

- **Service Desk**: Nur bei aktiviertem Advanced Automation Service: Sie können die Standardeinstellungen des Mandanten aktualisieren.

Hinweis
Bei Mandanten, die Lieferanten sind, werden nur die Registerkarten **Unternehmensprofil**, **Allgemeine Einstellungen** und **Abrechnungsinformationen** angezeigt.

Benachrichtigungen über Wartungsaktivitäten aktivieren

Als Partner-Benutzer können Sie Ihren Untermandanten (Partnern und Kunden) ermöglichen, Wartungsbenachrichtigungen per E-Mail direkt aus dem Cyber Protect Datacenter sowie produktinterne Wartungsbenachrichtigungen im Management-Portal zu erhalten. Dies wird Ihnen helfen, die Häufigkeit von wartungsbedingten Supportanfragen zu reduzieren.

Hinweis
Die E-Mail-Benachrichtigungen über Wartungsaktivitäten erhalten ein Branding vom jeweiligen Datacenter. Ein benutzerdefiniertes Branding für diese Benachrichtigungen wird nicht unterstützt.

So können Sie die Benachrichtigungen über Wartungsaktivitäten für untergeordnete Partner oder Kunden aktivieren

1. Melden Sie sich als Partner-Benutzer am Management-Portal an, klicken Sie dann zuerst auf **Clients** und anschließend auf den Namen eines Partner- oder Kunden-Mandanten, für den Sie die Benachrichtigungen über Wartungsaktivitäten einschalten wollen.
2. Klicken Sie auf **Konfigurieren**.
3. Suchen Sie auf der Registerkarte **Allgemeine Einstellungen** die Option **Benachrichtigungen über Wartungsaktivitäten** und aktivieren Sie diese.
   Falls Ihnen die Option **Benachrichtigungen über Wartungsaktivitäten** nicht angezeigt wird, wenden Sie sich an Ihren Service-Provider.

Hinweis
Die Benachrichtigungen über Wartungsaktivitäten werden eingeschaltet. Es werden allerdings erst dann tatsächlich Benachrichtigungen gesendet, wenn der ausgewählte Mandant diese wiederum für seine Benutzer aktiviert oder wenn er die Option an untergeordnete Partner oder Kunden weitergibt, damit diese die Benachrichtigungen für ihre jeweiligen Benutzer freischalten.

So können Sie die Benachrichtigungen über Wartungsaktivitäten für einen Benutzer aktivieren

1. Melden Sie sich am Management-Portal als Partner-Benutzer oder als Firmenadministrator an. Als Partner können Sie auf die Benutzer aller Mandanten zugreifen, die von Ihnen verwaltet werden.
2. Gehen Sie zu **Unternehmensverwaltung** –> **Benutzer** und klicken Sie dort auf den Namen eines Benutzers, für den Sie die Benachrichtigungen über Wartungsaktivitäten aktivieren wollen.

3. Klicken Sie auf der Registerkarte **Services** im Bereich **Einstellungen** auf das Stiftsymbol, um die Optionen zu bearbeiten.
4. Aktivieren Sie das Kontrollkästchen **Benachrichtigungen über Wartungsaktivitäten** und klicken Sie dann auf **Fertig**.

Der ausgewählte Benutzer wird daraufhin per E-Mail über anstehende Wartungsarbeiten im Datacenter benachrichtigt.

Selbstverwaltete Kundenprofile konfigurieren

Als Partner können Sie selbstverwaltete Kundenprofile für die von Ihnen verwalteten Mandanten konfigurieren. Mit dieser Option können Sie die Sichtbarkeit von Mandanten-Profilen und Kontaktinformationen für jeden Ihrer Kunden steuern.

So können Sie selbstverwaltete Kundenprofile konfigurieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den Kunden aus, für den Sie das selbstverwaltete Kundenprofil konfigurieren wollen.
3. Wählen Sie zuerst die Registerkarte **Konfigurieren** und anschließend die Registerkarte **Allgemeine Einstellungen**.
4. Aktivieren oder deaktivieren Sie den Schalter **Selbstverwaltetes Kundenprofil aktivieren**.

Wenn das selbstverwaltete Kundenprofil aktiviert ist, werden für diesen Kunde der Abschnitt **Unternehmensprofil** im Navigationsmenü sowie die kontaktbezogenen Felder im Assistenten zum Erstellen von Benutzern angezeigt (**Geschäftliche Telefonnummer**, **Firmenkontakt** und **Position**).

Wenn das selbstverwaltete Kundenprofil deaktiviert ist, werden der Abschnitt **Unternehmensprofil** im Navigationsmenü sowie die kontaktbezogenen Felder im Assistenten zum Erstellen von Benutzern ausgeblendet.

Firmenkontakte konfigurieren

Als Partner können Sie Kontaktinformationen für Ihr Unternehmen sowie für die von Ihnen verwalteten Mandanten konfigurieren. Wir werden Informationen über Updates zu neuen Funktionen und anderen wichtigen Änderungen auf der Plattform an die Kontakte in dieser Liste senden.

Sie können, je nach Benutzerrolle, mehrere Kontakte hinzufügen und Firmenkontakte zuweisen. Sie können Kontakte aus Benutzern erstellen, die bereits in der Cyber Protect-Plattform vorhanden sind, oder Kontaktinformationen von Personen hinzufügen, die keinen Zugriff auf den Service haben.

So können Sie die Kontakte für Ihr Unternehmen konfigurieren

1. Gehen Sie in der Management-Konsole zum Bereich **Unternehmensverwaltung** –> **Unternehmensprofil**.
2. Klicken Sie im Bereich **Kontakte** auf das **+**-Zeichen.

3. Wählen Sie eine Option, um den Kontakt zu erstellen.
   - **Aus vorhandenem Benutzer erstellen**
     - Wählen Sie im Listenfeld einen Benutzer aus.
     - Wählen Sie einen Firmenkontakt.
       - **Abrechnung** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
       - **Technisch** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.
       - **Geschäftlich** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.

       Sie können einem Benutzer mehr als einen Firmenkontakt zuweisen.

     Wenn Sie einen Kontakt, der mit einem Benutzer assoziiert ist, aus der Liste der Kontakte im Firmenprofil löschen, wird der Benutzer nicht gelöscht. Das System wird die Zuweisung aller Firmenkontakte für den Benutzer aufheben, sodass diese nicht mehr in der Spalte **Firmenkontakte** aus der Liste **Benutzer** erscheinen.

     Wenn Sie die E-Mail-Adresse des Kontakts, der mit dem Benutzer assoziiert ist, ändern wollen, wird das System die Überprüfung der neu definierten Adresse anfordern. s wird eine E-Mail an diese Adresse geschickt und der Benutzer muss dann die Änderung bestätigen.
   - **Einen neuen Kontakt erstellen**
     - Geben Sie die Kontaktinformationen an.
       - **Vorname** – Der Vorname der Kontaktperson. Dieses Feld ist erforderlich.
       - **Nachname** – Der Nachname der Kontaktperson. Dieses Feld ist erforderlich.
       - **Geschäftliche E-Mail** – Die E-Mail-Adresse der Kontaktperson. Dieses Feld ist erforderlich.
       - **Geschäftliche Telefonnummer** – Dieses Feld ist optional.
       - **Position** – Dieses Feld ist optional.
     - Wählen Sie **Firmenkontakte**.
       - **Abrechnung** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
       - **Technisch** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.
       - **Geschäftlich** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.

         Sie können einem Benutzer mehr als einen Firmenkontakt zuweisen.
4. Klicken Sie auf **Hinzufügen**.

So können Sie Kontakte für einen Mandanten konfigurieren

Hinweis
Wenn Sie die Kontaktinformationen für einen Untermandanten ändern, werden Ihre Änderungen für den Mandanten sichtbar.

1. Gehen Sie im Management-Portal zu **Clients**.
2. Klicken Sie zuerst auf den Mandanten und dann auf den Befehl **Konfigurieren**.
3. Klicken Sie im Bereich **Kontakte** auf das **+**-Zeichen.
4. Wählen Sie eine Option, um den Kontakt zu erstellen.
   - **Aus vorhandenem Benutzer erstellen**
     - Wählen Sie im Listenfeld einen Benutzer aus.
     - Wählen Sie einen Firmenkontakt.
       - **Abrechnung** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
       - **Technisch** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.
       - **Geschäftlich** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.

       Sie können einem Benutzer mehr als einen Firmenkontakt zuweisen.

     Wenn Sie einen Kontakt, der mit einem Benutzer assoziiert ist, aus der Liste der Kontakte im Firmenprofil löschen, wird der Benutzer nicht gelöscht. Das System wird die Zuweisung aller Firmenkontakte für den Benutzer aufheben, sodass diese nicht mehr in der Spalte **Firmenkontakte** aus der Liste **Benutzer** erscheinen.

     Wenn Sie die E-Mail-Adresse des Kontakts, der mit dem Benutzer assoziiert ist, ändern wollen, wird das System die Überprüfung der neu definierten Adresse anfordern. s wird eine E-Mail an diese Adresse geschickt und der Benutzer muss dann die Änderung bestätigen.
   - **Einen neuen Kontakt erstellen**
     - Geben Sie die Kontaktinformationen an.
       - **Vorname** – Der Vorname der Kontaktperson. Dieses Feld ist erforderlich.
       - **Nachname** – Der Nachname der Kontaktperson. Dieses Feld ist erforderlich.
       - **Geschäftliche E-Mail** – Die E-Mail-Adresse der Kontaktperson. Dieses Feld ist erforderlich.
       - **Geschäftliche Telefonnummer** – Dieses Feld ist optional.
       - **Position** – Dieses Feld ist optional.
     - Wählen Sie **Firmenkontakte**.
       - **Abrechnung** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
       - **Technisch** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.

- **Geschäftlich** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.

  Sie können einem Benutzer mehr als einen Firmenkontakt zuweisen.

5. Klicken Sie auf **Hinzufügen**.

Die Nutzungsdaten für einen Mandanten aktualisieren

Die Nutzungsdaten werden standardmäßig in festen Intervallen aktualisiert. Sie können die Nutzungsdaten für einen Mandanten aber auch manuell aktualisieren.

1. Gehen Sie in der Management-Konsole zu **Clients**.
2. Klicken Sie zuerst auf den Mandanten und dann in dessen Zeile auf das Drei-Punkte-Symbol.
3. Wählen Sie den Befehl **Nutzung aktualisieren**.

   Hinweis
   Das Abrufen der Daten kann bis zu 10 Minuten dauern.

4. Laden Sie die Seite neu, damit die aktualisierten Daten angezeigt werden.

Einen Mandanten deaktivieren und aktivieren

Möglicherweise müssen Sie einen Mandanten irgendwann einmal temporär deaktivieren. Beispielsweise, weil Ihr Mandant offene Zahlungsverpflichtungen zur Nutzung der Services hat.

So können Sie einen Mandaten deaktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den zu deaktivierenden Mandanten aus, klicken Sie auf das Drei-Punkte-Symbol und dann auf **Deaktivieren**.
3. Bestätigen Sie die Aktion durch Klicken auf **Deaktivieren**.

Ergebnis:

- Der Mandant und all dessen Untermandanten werden deaktiviert und deren Services gestoppt.
- Die Abrechnung mit dem Mandanten und seinen Untermandaten wird fortgesetzt, da dessen/deren Daten in Cyber Protect Cloud aufbewahrt und gespeichert werden.
- Alle API-Clients innerhalb des Mandanten und dessen Untermandanten werden deaktiviert und alle Integrationen, die diese Clients verwenden, werden nicht mehr funktionieren.

Wenn Sie einen Mandaten aktivieren wollen, müssen Sie diesen in der Client-Liste auswählen, auf das Drei-Punkte-Symbol klicken und dann auf **Aktivieren**.

Einen Mandanten zu einem anderen Mandanten verschieben

Das Management-Portal ermöglicht Ihnen, einen Mandanten von einem übergeordneten Mandanten zu einem anderen übergeordneten Mandanten zu verschieben. Dies kann nützlich sein,

wenn Sie einen Kunden von einem Partner zu einem anderen übertragen wollen. Oder wenn Sie einen Ordner-Mandanten erstellt haben, um Ihre Clients zu organisieren – und Sie einige davon zu den neu erstellten Ordner-Mandanten verschieben wollen.

Die Mandantentypen, die verschoben werden können

Mandantentyp	Kann verschoben werden	Ziel-Mandant
Partner	Ja	Partner oder Ordner
Ordner	Ja	Partner oder Ordner
Kunde	Ja	Partner oder Ordner
Abteilung	Nein	Ohne

Anforderungen und Einschränkungen

- Sie können einen Mandanten nur dann verschieben, wenn der übergeordnete Ziel-Mandant über dieselbe oder ein größere Zusammenstellung von Services und Angebotselementen verfügt, als der übergeordnete Original-Mandant.
- Wenn ein Kunden-Mandant verschoben wird, müssen alle Storages, die dem Kunden-Mandanten im übergeordneten Original-Mandanten zugewiesen waren, auch im übergeordneten Ziel-Mandanten vorhanden sein. Dies ist notwendig, weil die Service-bezogenen Daten eines Kunden nicht von einem Storage zu einem anderen verschoben werden können.
- Bei Kunden-Mandanten, die von Service-Providern verwaltet werden, kann es Pläne (z.B. Skripting-Pläne) geben, die auf Kunden-Workloads auf der Service-Provider-Ebene angewendet werden.

  Wenn Sie einen solchen Kunden-Mandanten verschieben, werden die Pläne des Service-Providers von den Kunden-Workloads entfernt. Als Folge werden auch alle Services, die mit diesen Plänen verbunden sind, für diesen Kunden nicht mehr funktionieren.
- Sie können Mandanten innerhalb der Hierarchie Ihres Partner-Kontos verschieben. Sie können außerdem einige Kunden-Mandanten zu einem Ziel-Mandanten außerhalb Ihrer Partner-Konto-Hierarchie verschieben. Wenn Sie wissen wollen, ob diese Aktion möglich ist, wenden Sie sich an Ihren Kundenbetreuer.
- Nur Administratoren (z.B. der Administrator im Management-Portal oder der Firmenadministrator) können Mandanten zu anderen übergeordneten Mandanten verschieben.

So können Sie einen Mandanten verschieben

1. Melden Sie sich am Management-Portal an.
2. Ermitteln und kopieren Sie die **Interne ID** des Zielpartners oder Ordner-Mandanten, zu dem Sie einen Mandanten verschieben wollen. Gehen Sie folgendermaßen vor:
   a. Wählen Sie in der Registerkarte **Clients** den Ziel-Mandanten, zu dem Sie einen Mandanten verschieben wollen.
   b. Klicken Sie im Fensterbereich der Mandanten-Eigenschaften auf das vertikale Drei-Punkte-Symbol und anschließend auf **ID anzeigen**.
   c. Kopieren Sie die im Feld **Interne ID** angezeigte Textzeichenfolge und klicken Sie dann auf **Abbrechen**.
3. Wählen Sie den Mandanten aus, den Sie verlagern wollen, und verschieben Sie ihn dann zum Zielpartner/-ordner. Gehen Sie folgendermaßen vor:
   a. Wählen Sie in der Registerkarte **Clients** den Mandanten, den Sie verschieben wollen.
   b. Klicken Sie im Fensterbereich der Mandaten-Eigenschaften auf das vertikale Drei-Punkte-Symbol und anschließend auf **Verschieben**.
   c. Fügen Sie die interne ID des Ziel-Mandanten über die Zwischenablage ein und klicken Sie dann auf **Verschieben**.

Die Aktion beginnt sofort und benötigt bis zu 10 Minuten.

Wenn der Mandant, den Sie verschieben, Untermandanten hat (z.B. ein Partner-Mandant oder Ordner-Mandant mit einem Kunden-Mandanten darin), wird das komplette Unterverzeichnis des Mandanten zum Ziel-Mandanten verschoben.

Einen Partner- in einen Ordner-Mandanten konvertieren (und umgekehrt)

Sie können im Management-Portal einen Partner-Mandanten in einen Ordner-Mandanten konvertieren.

Das bietet sich beispielsweise an, wenn Sie einen Partner-Mandanten zur Gruppierung verwendet haben und Sie Ihre Mandanten-Infrastruktur jetzt korrekt organisieren wollen. Und es ist nützlich, wenn Sie wollen, dass im operativen Dashboard zusammengefasste Informationen über den Mandanten aufgenommen werden.

Sie können außerdem einen Ordner-Mandanten in einen Partner-Mandanten konvertieren.

Hinweis
Die Konvertierung ist eine sichere Aktion und hat keinen Einfluss auf die Benutzer innerhalb des Mandanten oder auf irgendwelche Service-bezogene Daten.

So können Sie einen Mandanten konvertieren

1. Melden Sie sich am Management-Portal an.
2. Wählen Sie in der Registerkarte **Clients** den Mandanten, den Sie konvertieren wollen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie neben dem Mandanten-Namen auf das Drei-Punkte-Symbol.
   - Wählen Sie den Mandanten aus und klicken Sie dann in den Mandanten-Eigenschaften auf das Symbol mit den drei Punkten.
4. Klicken Sie auf **In Ordner konvertieren** oder **In Partner konvertieren**.
5. Bestätigen Sie Ihre Entscheidung.

Den Zugriff auf Ihren Mandanten einschränken

Administratoren auf der Kundenebene (und höher) können den Zugriff von höherstufigen Administratoren auf ihre Mandanten beschränken.

Wenn der Zugriff auf den Mandanten nicht eingeschränkt ist, haben die Administratoren der übergeordneten Mandanten vollen Zugriff auf Ihren Mandanten. Sie können dabei folgende Aktionen durchführen:

- Eigenschaften ändern
- Mandanten, Benutzer und Services verwalten
- Auf Backups und andere Ressourcen zugreifen

Wenn der Zugriff auf den Mandanten beschränkt ist, können die Administratoren des übergeordneten Mandanten nur noch die Mandanten-Eigenschaften ändern. Sie können weder die Konten noch Untermandanten sehen.

So verhindern Sie, dass höherstufige Administratoren auf Ihren Mandanten zugreifen können

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu **Einstellungen** –> **Sicherheit**.
3. Deaktivieren Sie den Schalter für **Support-Zugang**.

Dadurch haben die Administratoren der übergeordneten Mandants nur einen eingeschränkten Zugriff auf Ihren Mandanten. Sie können nur die Eigenschaften des Mandanten ändern, aber nicht auf dessen Elemente (z.B. Mandanten, Benutzer, Services, Backups und andere Ressourcen) zugreifen oder diese verwalten.

Einen Mandanten löschen

Möglicherweise wollen Sie einen Mandanten löschen, um die von ihm verwendeten Ressourcen freizugeben. Die Nutzungsstatistiken werden innerhalb eines Tages nach dem Löschvorgang aktualisiert. Bei größeren Mandanten kann dies länger dauern.

Bevor Sie einen Mandanten löschen können, müssen Sie diesen erst deaktivieren. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Einen Mandanten deaktivieren und aktivieren'.

Hinweis
Cyber Protect bietet zwar die Möglichkeit, Mandanten wiederherzustellen. Sie sollten dabei jedoch beachten, dass eine solche Wiederherstellung nicht für den File Sync&Share Service unterstützt wird.

So können Sie einen Mandaten löschen

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den deaktivierten Mandanten aus, den Sie löschen wollen, klicken Sie auf das Drei-Punkte-Symbol und dann auf **Löschen**.
3. Geben Sie zur Bestätigung der Aktion Ihren Anmeldenamen ein und klicken Sie dann auf **Löschen**.

Ergebnis:

- Der Mandant und seine Untermandanten werden gelöscht.
- Alle Services, die innerhalb des Mandanten und dessen Untermandanten aktiviert waren, werden gestoppt.
- Alle Benutzer in dem Mandanten und seinen Untermandanten werden gelöscht.
- Die Registrierung aller Maschinen in dem Mandanten und seinen Untermandanten wird aufgehoben.
- Alle Service-bezogenen Daten (z.B. Backups und synchronisierte Dateien) in dem Mandanten und seinen Untermandanten werden gelöscht.
- Alle API-Clients innerhalb des Mandanten und dessen Untermandanten werden gelöscht und alle Integrationen, die diese Clients verwenden, werden nicht mehr funktionieren.
- Ihnen wird der **Mandantenstatus** als **Gelöscht** angezeigt. Wenn Sie mit dem Mauszeiger über den Status **Gelöscht** fahren, wird Ihnen das Datum angezeigt, zu dem der Mandant gelöscht wurde – zusammen mit einem Hinweis, dass Sie alle relevanten Daten und Einstellungen innerhalb von 30 Tagen nach diesem Löschdatum noch wiederherstellen können.

Einen Mandanten wiederherstellen

Es kann vorkommen, dass ein Mandant versehentlich gelöscht wird. Daher bietet Cyber Protect eine Möglichkeit, Mandanten wiederherzustellen.

In folgenden Fällen kann es beispielsweise erforderlich sein, einen Mandanten wiederherzustellen:

- Der Partner hat seine Mandanten versehentlich gelöscht.
- Das Entwicklungsteam des Partners hat versehentlich einen Teil oder sogar die komplette Hierarchie der Mandanten gelöscht, als es die Integration getestet hat.

- Die Integration des Partners hat versehentlich die Bereitstellung der Applikation aufgehoben, anstatt zur neuen Edition zu wechseln, und Sie müssen nun die Daten wiederherstellen.
- Der Partner hat beim Wechseln zu einer neuen Lizenzierung versehentlich die Applikation deaktiviert – und Sie müssen nun die Daten in der deaktivierten Applikation wiederherstellen.

So können Sie einen Mandanten wiederherstellen

1. Gehen Sie im Management-Portal zu **Clients**.
2. Suchen Sie auf der **Cyber Protect**-Registerkarte denjenigen Mandanten, den Sie wiederherstellen wollen. Dessen Status wird als **Gelöscht** angezeigt.
3. Fahren Sie mit dem Mauszeiger über den Mandanten und klicken Sie dann auf das Drei-Punkte-Symbol  .
4. Klicken Sie auf **Recovery**.

   Es wird ein Bestätigungsfenster angezeigt, das darauf hinweist, dass der Mandant im gleichen Stadium wiederhergestellt wird, in dem er sich vor der Löschung befand, und dass er standardmäßig deaktiviert ist.
5. [Optional] Wenn Sie den Mandanten aktivieren müssen, schalten Sie das Kontrollkästchen **Ich will den Mandanten aktivieren** ein. Sie können den Mandanten auch zu einem späteren Zeitpunkt aktivieren.
6. Klicken Sie auf **Recovery**.

Ergebnis:

- Der Mandant und seine Untermandanten werden wiederhergestellt.
- Alle Services, die innerhalb des Mandanten und dessen Untermandanten aktiviert waren, werden neu gestartet.

  Hinweis
  Für den File Sync&Share Service wird keine Wiederherstellung unterstützt.

- Alle Benutzer in dem Mandanten und seinen Untermandanten werden wiederhergestellt.
- Alle Maschinen in dem Mandanten und seinen Untermandanten werden neu registriert.
- Alle Service-bezogenen Daten (z.B. Backups) in dem Mandanten und seinen Untermandanten werden wiederhergestellt.
- Alle API-Clients innerhalb des Mandanten und dessen Untermandanten werden wiederhergestellt und alle Integrationen, die diese Clients verwenden, werden wieder funktionieren.
- Der **Mandantenstatus** wird als **Aktiv** angezeigt, wenn Sie den Mandanten aktiviert haben – oder als **Deaktiviert**, wenn Sie den Mandanten noch nicht aktiviert haben.

Benutzer verwalten

Partner-, Kunden- und Abteilungs-Administratoren können Benutzerkonten unter den Mandanten, auf die sie Zugriff haben, konfigurieren und verwalten.

Ein Benutzerkonto erstellen

Die Erstellung zusätzlicher Konten kann in folgenden Fällen angebracht sein:

- Partner-/Ordner-Administrator-Konten – um die Service-Verwaltungsaufgaben mit anderen Personen zu teilen.
- Kunden-/Interessenten-/Abteilungs-Administrator-Konten – um die Service-Verwaltung an andere Personen zu delegieren, deren Zugriffsberechtigungen streng auf den/die entsprechende(n) Kunden/Abteilung begrenzt werden.
- Benutzerkonten innerhalb des Kunden oder eines Abteilungs-Mandanten – um es zu ermöglichen, dass Benutzer nur auf eine Teilmenge der Services zugreifen können.

Beachten Sie dabei, dass vorhandene Konten nicht zwischen Mandanten verschoben werden können. Sie müssen zuerst einen Mandanten erstellen und können diesen erst danach mit Konten „befüllen“.

So erstellen Sie ein Benutzerkonto

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, in dem Sie ein Benutzerkonto erstellen wollen. Siehe den Abschnitt '"Im Management-Portal navigieren" (S. 31)'.
3. Klicken Sie in der rechten oberen Ecke auf **Neu** –> **Benutzer**.

   Alternativ können Sie auch zu **Unternehmensverwaltung –> Benutzer** gehen und auf den Befehl **+ Neu** klicken.
4. Spezifizieren Sie die nachfolgenden Kontaktinformationen für das Konto:
   a. **E-Mail**. Diese E-Mail-Adresse dient auch als Anmeldename.
   b. Wenn Sie lieber eine andere Adresse als Anmeldenamen verwenden wollen, aktivieren Sie das Kontrollkästchen **Anderen Anmeldenamen als die E-Mail-Adresse verwenden** und geben Sie dann den **Anmeldenamen** und die **E-Mail** an.

   Wichtig
   Jedes Konto benötigt einen eindeutigen Anmeldenamen.

Wichtig
Wenn der Benutzer im File Sync & Share Service registriert ist, geben Sie bitte die E-Mail an, die für die File Sync & Share-Registrierung verwendet wurde.
Bitte beachten Sie, dass jedes Kunden-Benutzerkonto eine eindeutige E-Mail-Adresse haben muss.

c. **Vorname**

d. **Nachname**

e. [Optional] **Geschäftliche Telefonnummer**

Hinweis
Felder wie **Geschäftliche Telefonnummer**, **Position** und **Firmenkontakte** werden im Assistenten zum Erstellen von Benutzern nur angezeigt, wenn der übergeordnete Partner die Option **Selbstverwaltetes Kundenprofil aktivieren** für den Kunden-Mandanten aktiviert hat. Ansonsten werden diese Felder nicht angezeigt.

f. [Optional] **Position**

g. Ändern Sie bei **Sprache** die Standardsprache für die in diesem Konto verwendete(n) Benachrichtigungen, Berichte und Software.

5. [Optional] Spezifizieren Sie die Firmenkontakte.
   - **Abrechnung** – Die Kontaktperson, die über Updates zu wichtigen Änderungen in der Nutzungsberichterstattung auf der Plattform informiert wird.
   - **Technisch** – Die Kontaktperson, die über Updates zu wichtigen technischen Änderungen auf der Plattform informiert wird.
   - **Geschäftlich** – Die Kontaktperson, die über Updates zu wichtigen geschäftsbezogenen Änderungen auf der Plattform informiert wird.

   Sie können einem Benutzer mehr als einen Firmenkontakt zuweisen.

   Sie können die zugewiesenen Firmenkontakte für einen Benutzer in der Liste **Benutzer** (in der Spalte **Firmenkontakte**) einsehen und das entsprechende Benutzerkonto bearbeiten, wenn Sie die Firmenkontakte ändern wollen.
6. [Nicht verfügbar, wenn ein Konto in einem Partner-/Ordner-Mandanten erstellt wird] Bestimmen Sie die Services, auf die der Benutzer zugreifen kann, und die Rollen in jedem Service.

   Welche Services dabei verfügbar sind, hängt davon ab, welche Services für den Mandanten aktiviert wurden, in welchem wiederum das Benutzerkonto erstellt wird.
   - Wenn Sie das Kontrollkästchen **Firmenadministrator** auswählen, erhält der Benutzer Zugriff auf das Management-Portal – und die Administrator-Rolle in allen Services, die derzeit für den Mandanten aktiviert sind. Der Benutzer erhält die Administrator-Rolle zudem auch in allen Services, die zukünftig für den Mandanten aktiviert werden.
   - Wenn Sie das Kontrollkästchen **Abteilungsadministrator** aktivieren, erhält der Benutzer Zugriff auf das Management-Portal. Ob er die Service-Administrator-Rolle (nicht) erhält, hängt vom Service ab.

- Ansonsten erhält der Benutzer die Rollen, die Sie in den von Ihnen ausgewählten Services bestimmen.

7. Klicken Sie auf **Erstellen**.

Das neu erstellte Benutzerkonto wird in der Registerkarte **Benutzer** (unter **Unternehmensverwaltung**) angezeigt.

Wenn Sie die Benutzereinstellungen bearbeiten oder Benachrichtigungseinstellungen und Quotas (für Partner-/Ordner-Administrator nicht verfügbar) für den Benutzer spezifizieren wollen, müssen Sie den Benutzer zuerst in der Registerkarte **Benutzer** auswählen und dann auf das Stiftsymbol in dem Bereich klicken, den Sie bearbeiten wollen.

So können Sie das Kennwort eines Benutzers zurücksetzen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Wählen Sie den Benutzer aus, dessen Kennwort Sie zurücksetzen wollen, und klicken Sie dann auf das Drei-Punkte-Symbol > **Kennwort zurücksetzen**.
3. Bestätigen Sie die Aktion durch Klicken auf **Zurücksetzen**.

Der Benutzer kann nun den Zurücksetzungsprozess abschließen, indem er die Anweisungen in der ihm zugesendeten E-Mail befolgt.

Für Services, die keine Zwei-Faktor-Authentifizierung unterstützen (z.B. für die Registrierung in Cyber Infrastructure), müssen Sie möglicherweise ein Benutzerkonto zu einem *Service-Konto* konvertieren – also ein Konto, das keine Zwei-Faktor-Authentifizierung erfordert.

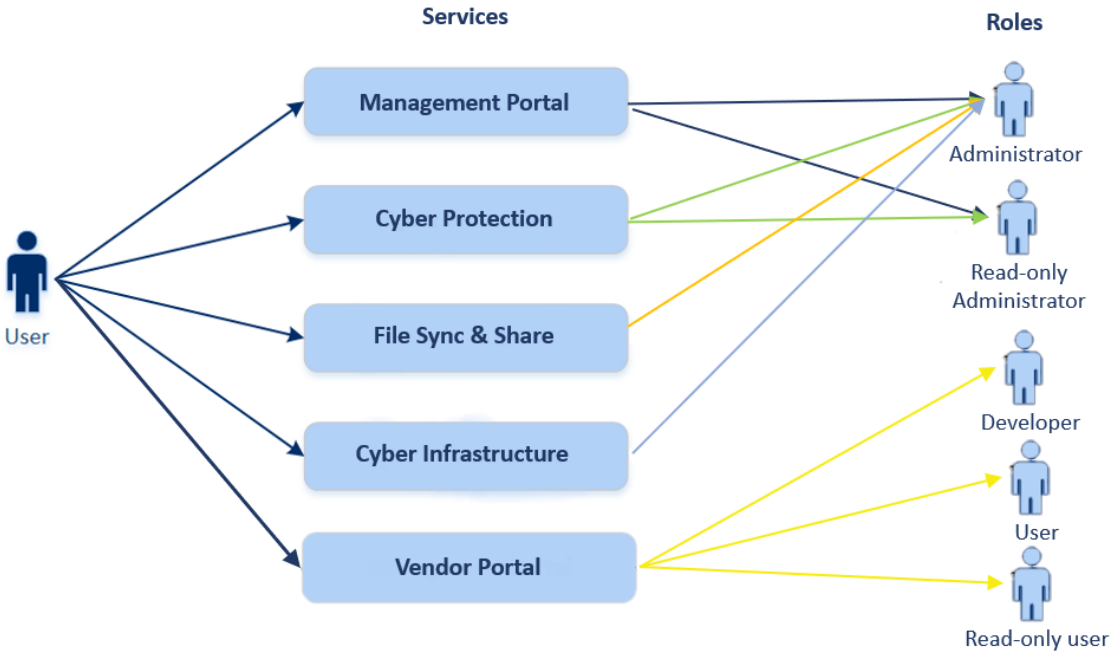
So können Sie ein Benutzerkonto in ein Service-Konto umwandeln

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Wählen Sie denjenigen Benutzer aus, dessen Konto Sie in ein Service-Konto umwandeln wollen, und klicken Sie anschließend auf das Drei-Punkte-Symbol > **Als Service-Konto kennzeichnen**.
3. Geben Sie im Bestätigungsfenster den Zwei-Faktor-Authentifizierungscode ein und bestätigen Sie Ihre Aktion.

Das Konto kann jetzt auch für Services verwendet werden, die keine Zwei-Faktor-Authentifizierung unterstützen.

Für jeden Service verfügbare Benutzerrollen

Ein Benutzer kann mehrere Rollen haben, aber nur eine Rolle je Service.



Sie können für jeden Service festlegen, welche Rolle einem Benutzer zugewiesen wird.

Service	Rolle	Beschreibung
n/a	Firmenadministrator	Diese Rolle gewährt dem Administrator vollständige Rechte für alle Services. Diese Rolle gewährt Zugriff auf die Positivliste für Unternehmensapplikationen. Wenn das Disaster Recovery-Add-on des Cyber Protection Service für die Firma aktiviert ist, gewährt die Rolle außerdem Zugriff auf die Disaster Recovery-Funktionalität.
Management-Portal	Administrator	Diese Rolle gewährt Zugriff auf das Management-Portal, wo der Administrator Benutzer innerhalb der kompletten Organisation verwalten kann.
	Nur-Lesen-Administrator Partnerebene	Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf alle Objekte im Management-Portal des Partners und auf das Management-Portal aller Kunden dieses Partners. Solche Benutzer können im Nur-Lesen-Modus auf die Daten anderer Benutzer der Organisationen zugreifen. Sie können Schutzpläne bearbeiten, aber keine Änderungen an Skripting-, Monitoring- oder Agenten-Plänen speichern.
	Nur-Lesen-Administrator Kundenebene	Diese Rolle ermöglicht einen Nur-Lesen-Zugriff auf alle Objekte im Management-Portal des gesamten Unternehmens. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen.

	Nur-Lesen-Administrator Abteilungsebene	Diese Rolle ermöglicht einen Nur-Lesen-Zugriff auf alle Objekte im Management-Portal der Firmenabteilung und deren Unterabteilungen. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen.
Vendor Portal	Entwickler	Diese Rolle gewährt volle Zugriffsrechte auf das Vendor Portal. Entwickler können CyberApps, CyberApp-Beschreibungen und CyberApp-Versionen erstellen und verwalten. Sie können auch Bereitstellungsanfragen stellen und CyberApp-Metriken überwachen.
	Benutzer	Diese Rolle ermöglicht es dem Benutzer, CyberApp-Beschreibungen zu erstellen, zu verwalten und entsprechende Genehmigungen zu beantragen.
	Schreibgeschützter Benutzer	Diese Rolle gewährt nur Lesezugriff auf das Vendor Portal.
Cyber Protection	Cyber-Administrator	Zusätzlich zu den Rechten der Administrator-Rolle ermöglicht diese Rolle, den Cyber Protection Service zu konfigurieren und zu verwalten sowie Aktionen beim Cyber Scripting zu genehmigen. Die Rolle des Cyber-Administrators ist nur für Mandanten mit aktiviertem Advanced Management-Paket verfügbar.
	Administrator	Diese Rolle ermöglicht es, die Cyber Protection-Funktionalität für Ihre Kunden zu konfigurieren und zu verwalten. Diese Rolle ist zur Konfiguration und Verwaltung der Disaster Recovery-Funktionalität sowie der Positivliste für Unternehmensapplikationen erforderlich.
	Nur-Lesen-Administrator	Die Rolle ermöglicht nur Lesezugriff auf alle Objekte im Cyber Protection Service. Solche Benutzer können auf Daten anderer Benutzer der Organisation im Nur-Lesen-Modus zugreifen. Der Nur-Lesen-Administrator kann weder die Disaster Recovery-Funktionalität noch die Positivliste für Unternehmensapplikationen konfigurieren bzw. verwalten.
	Benutzer	Diese Rolle ermöglicht die Verwendung des Protection Service, jedoch ohne administrative Berechtigungen. Es wird Zugriff auf bestimmte Funktionalitäten (wie Endpoint Detection & Response) gewährt, aber Benutzer, denen diese Rolle zugewiesen wird, können nicht auf die Daten anderer Benutzer in der Organisation zugreifen.
	Operator	Die Rolle ermöglicht den Zugriff auf Backups von Microsoft

	wiederherstellen	365- und Google Workspace- Organisationen und erlaubt deren Wiederherstellung, während der Zugriff auf sensible Inhalte eingeschränkt wird.
File Sync & Share	Administrator	Diese Rolle ermöglicht es, die File Sync & Share-Funktionalität für Ihre Benutzer zu konfigurieren und zu verwalten:
Cyber Infrastructure	Administrator	Diese Rolle ermöglicht es, die Cyber Infrastructure-Funktionalität für Ihre Kunden zu konfigurieren und zu verwalten.
Advanced Automation	Advanced Automation-Benutzern kann eine Reihe von Rollen zugewiesen werden. Weitere Informationen finden Sie im Abschnitt '"Advanced Automation-Rollen" (S. 190)'.	
Partner Portal	Partner Portal-Benutzern kann eine Reihe von Rollen zugewiesen werden. Weitere Informationen finden Sie im Abschnitt '"Partner Portal-Rollen" (S. 155)'.	

Hinweis
Das Vendor Portal ist exklusiv für Technologiepartner verfügbar, die sich ab dem 04. Oktober 2023 auf der Acronis Technology Ecosystem-Webseite registriert haben.
Wenn Sie als Anbieter eine Integration mit Acronis aufbauen wollen und Zugriff auf das Vendor Portal sowie eine dedizierte Sandbox benötigen, orientieren Sie sich bitte an den entsprechenden Anweisungen.

Nur-Lesen-Administrator-Rolle

Ein Konto mit dieser Rolle hat nur einen Lesezugriff auf die Cyber Protect-Konsole und kann Folgendes tun:

- Diagnoseinformationen sammeln (wie z.B. Systemberichte).
- Die Recovery-Punkte eines Backups anzeigen lassen, aber keine Backup-Inhalte und keine Dateien, Ordner oder E-Mails einsehen.

Ein Nur-Lesen-Administrator kann Folgendes tun:

- Irgendwelche Tasks starten oder stoppen.
  Ein Nur-Lesen-Administrator kann beispielsweise keine Wiederherstellung starten oder ein laufendes Backup stoppen.
- Auf das Dateisystem von Quell- oder Zielmaschinen zugreifen.
  Ein Nur-Lesen-Administrator kann beispielsweise keine Dateien, Ordner oder E-Mails auf einer gesicherten Maschine einsehen.
- Irgendwelche Einstellungen ändern.
  Ein Nur-Lesen-Administrator kann beispielsweise keinen Schutzplan erstellen oder dessen Einstellungen ändern.
- Irgendwelche Daten erstellen, aktualisieren oder löschen.
  Ein Nur-Lesen-Administrator kann beispielsweise keine Backups löschen.

Alle Benutzeroberflächenobjekte, auf die ein Nur-Lesen-Administrator keinen Zugriff hat, werden ausgeblendet – mit Ausnahme der Standardeinstellungen des Schutzplans. Diese Einstellungen werden zwar angezeigt, aber die Schaltfläche **Speichern** ist nicht aktiv.

Alle Änderungen, die sich auf Konten und Rollen beziehen, werden auf der Registerkarte **Aktivitäten** mit folgenden Informationen angezeigt:

- Was geändert wurde
- Wer die Änderungen durchgeführt hat
- Datum und Uhrzeit der Änderungen

Rolle 'Restore Operator'

Diese Rolle ist nur im Cyber Protection Service verfügbar und auf Microsoft 365- sowie Google Workspace-Backups beschränkt.

Ein Restore Operator kann Folgendes tun:

- Alarmmeldungen und Aktivitäten anzeigen.
- Die Liste der Backups durchsuchen und aktualisieren.
- Backups durchsuchen, ohne auf deren Inhalte zuzugreifen. Der Restore Operator kann die Namen der gesicherten Dateien sowie die Betreffs und Absender der gesicherten E-Mails sehen.
- Backups durchsuchen (Volltextsuche wird nicht unterstützt).
- Cloud-zu-Cloud-Backups an ihrem ursprünglichen Speicherort innerhalb der ursprünglichen Microsoft 365- oder Google Workspace-Organisation wiederherstellen.

Ein Restore Operator kann Folgendes nicht tun:

- Alarmmeldungen löschen.
- Microsoft 365- oder Google Workspace-Organisationen hinzufügen oder löschen.
- Backup-Speicherorte hinzufügen, löschen oder umbenennen.
- Backups löschen oder umbenennen.
- Ordner erstellen, löschen oder umbenennen, wenn ein Backup zu einem benutzerdefinierten Speicherort wiederhergestellt wird.
- Einen Backup-Plan anwenden oder ein Backup ausführen.
- Auf gesicherte Dateien oder die Inhalte von gesicherten E-Mails zugreifen.
- Gesicherte Dateien oder E-Mail-Anhänge herunterladen.
- Gesicherte Cloud-Ressourcen (wie E-Mails oder Kalenderelemente) per E-Mail versenden.
- Microsoft 365 Teams-Unterhaltungen einsehen oder wiederherstellen.
- Cloud-zu-Cloud Backups an nicht ursprünglichen Speicherorten wiederherstellen, z.B. in einem anderen Postfach, in OneDrive, Google Drive oder Microsoft 365 Team.

Benutzerrollen und Cyber-Skripting-Rechte

Die Aktionen, die mit Skripten und Skripting-Plänen verfügbar sind, hängen vom Skript-Status und Ihrer Benutzerrolle ab.

Administratoren können Objekte in ihrem eigenen Mandanten und in dessen Untermandanten verwalten. Sie können keine Objekte auf einer höheren Verwaltungsebene sehen oder auf diese zugreifen (sofern solche vorhanden sind).

Administratoren einer niedrigeren Ebene können nur lesend auf die Skripting-Pläne zugreifen, die von einem Administrator einer höheren Ebene auf ihre Workloads angewendet wurden.

Folgende Rollen gewähren Rechte, die sich auf Cyber-Skripting beziehen:

- **Firmenadministrator**
  Diese Rolle gewährt dem Administrator vollständige Rechte in allen Services. In Bezug auf Cyber-Skripting gewährt diese Rolle die gleichen Rechte wie die Rolle 'Cyber-Administrator'.
- **Cyber-Administrator**
  Diese Rolle gewährt volle Berechtigungen, einschließlich der Genehmigung von Skripten, die im Mandanten verwendet werden können – und die Fähigkeit, Skripte mit dem Status **Wird getestet** auszuführen.
- **Administrator**
  Diese Rolle gewährt Teilberechtigungen, mit der Möglichkeit, genehmigte Skripte auszuführen – sowie Skripting-Pläne zu erstellen und auszuführen, die genehmigte Skripte verwenden.
- **Nur-Lesen-Administrator**
  Diese Rolle gewährt eingeschränkte Berechtigungen, mit der Möglichkeit, Skripte und Schutzpläne einzusehen, die im Mandanten verwendet werden.
- **Benutzer**
  Diese Rolle gewährt Teilberechtigungen, mit der Möglichkeit, genehmigte Skripte auszuführen – sowie Skripting-Pläne zu erstellen und auszuführen, die genehmigte Skripte verwenden, jedoch nur auf der eigenen Maschine des Benutzers.

Die nachfolgende Tabelle fasst alle verfügbaren Aktionen zusammen, abhängig vom Skript-Status und der Benutzerrolle.

Rolle	Objekt	Skript-Status		
		Entwurf	**Wird getestet**	**Genehmigt**
Cyber-Administrator **Firmenadministrator**	Skripting-Plan	Bearbeiten (Einen Skript-Entwurf aus einem Plan entfernen) Löschen	Erstellen Bearbeiten Anwenden Aktivieren	Erstellen Bearbeiten Anwenden Aktivieren

		Widerrufen Deaktivieren Stopp	Ausführen Löschen Widerrufen Deaktivieren Stopp	Ausführen Löschen Widerrufen Deaktivieren Stopp
	Skript	Erstellen Bearbeiten Status ändern Klonen Löschen Ausführung abbrechen	Erstellen Bearbeiten Status ändern Ausführen Klonen Löschen Ausführung abbrechen	Erstellen Bearbeiten Status ändern Ausführen Klonen Löschen Ausführung abbrechen
Administrator **Benutzer** (für deren eigene Workloads)	Skripting-Plan	Anzeigen Widerrufen Deaktivieren Stopp	Anzeigen Ausführung abbrechen	Erstellen Bearbeiten Anwenden Aktivieren Ausführen Löschen Widerrufen Deaktivieren Stopp
	Skript	Erstellen Bearbeiten Klonen Löschen Ausführung abbrechen	Anzeigen Klonen Ausführung abbrechen	Ausführen Klonen Ausführung abbrechen
Nur-Lesen-Administrator	Skripting-Plan	Anzeigen	Anzeigen	Anzeigen
	Skript	Anzeigen	Anzeigen	Anzeigen

Die Benachrichtigungseinstellungen für einen Benutzer ändern

Wenn Sie die Benachrichtigungseinstellungen für einen Benutzer ändern wollen, gehen Sie zu **Unternehmensverwaltung** –> **Benutzer**. Wählen Sie den Benutzer, dessen Benachrichtigungen Sie konfigurieren wollen, und klicken Sie anschließend auf das Stiftsymbol im Bereich **Einstellungen**. Die folgenden Benachrichtigungseinstellungen sind verfügbar, wenn der Cyber Protection Service für den Mandanten aktiviert ist, in dem der Benutzer erstellt wird:

- **Benachrichtigungen über Quota-Überbenutzung** (standardmäßig aktiviert)
  Benachrichtigungen zu überschrittenen Quotas.
- **Geplante Nutzungsberichte** (standardmäßig aktiviert)
  Nutzungsberichte, die am ersten Tag eines jeden Monats gesendet werden.
- **URL-Branding-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über einen bevorstehenden Ablauf des Zertifikats, das für die benutzerdefinierte URL der Cyber Protect Cloud Services verwendet wird. Die Benachrichtigungen werden an alle Administratoren des ausgewählten Mandanten gesendet – 30 Tage, 15 Tage, 7 Tage, 3 Tage sowie 1 Tag vor Ablauf des Zertifikats.
- **Benachrichtigungen über Fehler**, **Benachrichtigungen über Warnungen** und **Benachrichtigungen über erfolgreiche Aktionen** (standardmäßig deaktiviert)
  Benachrichtigungen über die Ausführungsergebnisse von Schutzplänen und die Ergebnisse von Disaster Recovery-Aktionen für jedes Gerät.
- **Tägliche Zusammenfassung über aktive Alarmmeldungen** (standardmäßig aktiviert)
  Die tägliche Zusammenfassung wird auf der Grundlage der Liste der aktiven Alarmmeldungen erstellt, die in dem Augenblick in der Cyber Protect-Konsole vorhanden sind, wenn die Zusammenfassung generiert wird. Die Zusammenfassung wird einmal täglich zwischen 10:00 und 23:59 Uhr (UTC) generiert und gesendet. Der genaue Zeitpunkt der Berichtsgenerierung und -übermittlung hängt vom Workload im Datacenter ab. Wenn zum betreffenden Zeitpunkt keine aktiven Alarmmeldungen vorliegen, wird auch keine Zusammenfassung gesendet. Die Zusammenfassung enthält keine Informationen über frühere Alarmmeldungen, die nicht mehr aktiv sind. Wenn z.B. ein Benutzer ein fehlgeschlagenes Backup findet und die Alarmmeldungen löscht oder wenn das Backup wiederholt und dann erfolgreich abgeschlossen wird, bevor die Zusammenfassung generiert wird, dann wird die Alarmmeldung nicht mehr vorhanden sein und die Zusammenfassung wird diese nicht mehr enthalten.
- **Gerätekontrolle-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Versuche, Peripheriegeräte und Ports zu verwenden, die durch Schutzpläne mit aktiviertem Gerätekontrolle-Modul eingeschränkt werden.
- **Recovery-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Wiederherstellungsaktionen auf folgenden Ressourcen: Benutzer-E-Mail-Nachrichten und das komplette Postfach, öffentliche Ordner, OneDrive / GoogleDrive: das komplette OneDrive sowie Dateien oder Ordner, SharePoint-Dateien, Teams: Kanäle, komplette Teams, E-Mail-Nachrichten und Team-Websites.

Im Kontext dieser Benachrichtigungen werden folgende Aktionen als Wiederherstellungsaktionen betrachtet: als E-Mail senden, Herunterladen oder eine Wiederherstellung starten.

- **Data Loss Prevention-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Data Loss Prevention Alarmmeldungen, die sich auf die Aktivitäten dieses Benutzers im Netzwerk beziehen.
- **Sicherheitsvorfall-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Malware-Erkennungen bei On-Access-, On-Execution- oder On-Demand-Scans sowie über Erkennungen durch die Behavioral Engine oder die URL-Filter-Engine.
  Es stehen Ihnen zwei Optionen zur Verfügung: **Abgeschwächt** und **Nicht abgeschwächt**. Diese Optionen sind für Alarmmeldungen von Endpoint Detection & Response (EDR)-Vorfällen, EDR-Alarmmeldungen aus Bedrohungsfeeds sowie individuellen Alarmmeldungen (für Workloads, bei denen die EDR-Funktionalität nicht aktiviert ist) relevant.
  Wenn ein EDR-Alarm erstellt wird, wird eine E-Mail an den betreffenden Benutzer gesendet. Wenn sich der Bedrohungsstatus des Vorfalls ändert, wird eine neue E-Mail gesendet. Die E-Mails enthalten Aktionsschaltflächen, mit denen sich der Benutzer Details zu dem jeweiligen Vorfall anzeigen lassen kann (wenn dieser abgeschwächt wurde) oder den Vorfall untersuchen und beheben kann (wenn er nicht abgeschwächt wurde).
- **Infrastruktur-Benachrichtigungen** (standardmäßig deaktiviert)
  Benachrichtigungen über Probleme mit der Disaster Recovery-Infrastruktur: wenn die Disaster Recovery-Infrastruktur oder die VPN-Tunnel nicht verfügbar sind.

Alle Benachrichtigungen werden an die E-Mail-Adresse gesendet, die für den entsprechenden Benutzer spezifiziert wurde.

Je nach Benutzerrolle empfangene Benachrichtigungen

Die Benachrichtigungen, die Cyber Protection versendet, hängen von der Benutzerrolle ab.

Benachrichtigungstyp\Benutzerrolle	Benutzer	Kunden- und Abteilungsadministratoren	Partner- und Ordner-Administrator
Benachrichtigungen für eigene Geräte	Ja	Ja	n/a*
Benachrichtigungen für alle Geräte der Untermandanten	n/a	Ja (außer **Sicherheitsvorfall-Benachrichtigungen**)	Ja
Benachrichtigungen für Microsoft 365, Google Workspace und andere Cloud-basierte Backups	n/a	Ja	Ja

* Partner-Administratoren können keine eigenen Geräte registrieren, aber sie können ihre eigenen Kunden-Administrator-Konten erstellen und diese Konten dann verwenden, um eigene Geräte hinzuzufügen. Siehe 'Benutzerkonten und Mandanten'.

Ein Benutzerkonto deaktivieren und aktivieren

Unter bestimmten Umständen müssen Sie möglicherweise ein Benutzerkonto deaktivieren, um dessen Zugriff auf die Cloud-Plattform temporär sperren zu können.

So können Sie ein Benutzerkonto deaktivieren

1. Gehen Sie im Management-Portal zu **Benutzer**.
2. Wählen Sie das Benutzerkonto aus, welches Sie deaktivieren wollen, und klicken Sie dann auf das Drei-Punkte-Symbol > **Deaktivieren**.
3. Bestätigen Sie die Aktion durch Klicken auf **Deaktivieren**.

Als Ergebnis wird der Benutzer die Cloud-Plattform nicht mehr verwenden und keine Benachrichtungen empfangen können.

Wenn Sie ein deaktiviertes Benutzerkonto wieder aktivieren wollen, müssen Sie dieses zuerst in der Benutzerliste auswählen, dann auf das Drei-Punkte-Symbol > **Aktivieren** klicken.

Ein Benutzerkonto löschen

Möglicherweise wollen Sie ein Benutzerkonto dauerhaft löschen, um die von ihm verwendeten Ressourcen (z.B. den Speicherplatz oder die Lizenz) freizugeben. Die Nutzungsstatistiken werden innerhalb eines Tages nach dem Löschvorgang aktualisiert. Bei Konten mit vielen Daten kann es auch länger dauern.

Bevor Sie ein Benutzerkonto löschen können, müssen Sie es erst deaktivieren. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt 'Ein Benutzerkonto deaktivieren und aktivieren'.

So können Sie ein Benutzerkonto löschen

1. Gehen Sie im Management-Portal zu **Benutzer**.
2. Wählen Sie das deaktivierte Benutzerkonto aus, klicken Sie auf das Drei-Punkte-Symbol und anschließend auf **Löschen**.
3. Geben Sie zur Bestätigung der Aktion Ihren Anmeldenamen ein und klicken Sie dann auf **Löschen**.

Ergebnis:

- Alle für dieses Konto konfigurierten Benachrichtigungen werden deaktiviert.
- Alle Daten, die zu diesem Benutzerkonto gehören, werden gelöscht.
- Der Administrator wird nicht auf das Management-Portal zugreifen können.
- Alle Backups der Workloads, die mit diesem Benutzer assoziiert sind, werden gelöscht.

- Die Registrierung aller Maschinen, die mit diesem Benutzerkonto assoziiert sind, wird aufgehoben.
- Alle Schutzpläne werden von allen Workloads widerrufen, die mit diesem Benutzer assoziiert sind.
- Alle File Sync & Share-Daten, die zu diesem Benutzer gehören (z.B. Dateien und Ordner), werden gelöscht.
- Alle Notary-Daten, die zu diesem Benutzer gehören (z.B. beglaubigte Dateien, elektronisch signierte Dateien), werden gelöscht.
- Ihnen wird der **Mandantenstatus** als **Gelöscht** angezeigt. Wenn Sie mit dem Mauszeiger über den Status **Gelöscht** fahren, wird Ihnen das Datum angezeigt, zu dem der Benutzer gelöscht wurde – zusammen mit einem Hinweis, dass Sie alle relevanten Benutzerdaten und Einstellungen innerhalb von 30 Tagen nach diesem Löschdatum noch wiederherstellen können.

Ein Benutzerkonto wiederherstellen

Es kann vorkommen, dass ein Benutzerkonto versehentlich gelöscht wird. Daher bietet Cyber Protection eine Möglichkeit, Benutzerkonten wiederherzustellen.

In folgenden Fällen kann es beispielsweise erforderlich sein, ein Benutzerkonto wiederherzustellen: Der Firmenadministrator hat einen Benutzer gelöscht, der das Unternehmen verlassen hat. Sie benötigen aber noch alle Ressourcen, die unter diesem Benutzer registriert sind.

So können Sie ein Benutzerkonto wiederherstellen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie auf der Registerkarte **Benutzer** dasjenige Benutzerkonto, das Sie wiederherstellen wollen. Dessen Status wird als **Gelöscht** angezeigt.
3. Fahren Sie mit dem Mauszeiger über das Benutzerkonto und klicken Sie dann auf das Drei-Punkte-Symbol .
4. Klicken Sie auf **Recovery**.

   Es wird ein Bestätigungsfenster angezeigt, das darauf hinweist, dass das Benutzerkonto im gleichen Stadium wiederhergestellt wird, in dem es sich vor der Löschung befand, und dass es standardmäßig deaktiviert ist.
5. [Optional] Wenn Sie das Benutzerkonto aktivieren müssen, schalten Sie das Kontrollkästchen **Ich will den Benutzer aktivieren** ein. Sie können das Benutzerkonto auch zu einem späteren Zeitpunkt aktivieren.
6. Klicken Sie auf **Recovery**.

Ergebnis:

- Das Benutzerkonto wird wiederhergestellt.
- Alle Daten, die zu diesem Benutzerkonto gehören, werden wiederhergestellt.

- Alle Maschinen, die mit diesem Benutzerkonto assoziiert sind, werden neu registriert.
- Der Benutzerstatus wird als **Aktiv** angezeigt, wenn Sie das Benutzerkonto aktiviert haben – oder als **Deaktiviert**, wenn Sie das Benutzerkonto noch nicht aktiviert haben.

Die Eigentümerschaft eines Benutzerkontos übertragen

Möglicherweise müssen Sie die Eigentümerschaft eines Benutzerkontos übertragen, wenn Sie weiterhin auf die Daten eines gesperrten Benutzers zugreifen wollen.

Wichtig
Die Inhalte eines gelöschten Kontos können nicht neu zugewiesen werden.

So können Sie die Eigentümerschaft eines Benutzerkontos übertragen

1. Gehen Sie im Management-Portal zu **Benutzer**.
2. Wählen Sie das Benutzerkonto aus, dessen Eigentümerschaft Sie übertragen wollen, und klicken Sie denn im Bereich **Allgemeine Informationen** auf das Stiftsymbol.
3. Ersetzen Sie die vorliegende E-Mail-Adresse mit der E-Mail-Adresse des zukünftigen Kontobesitzers – und klicken Sie dann auf **Fertig**.
4. Bestätigen Sie die Aktion durch Klicken auf **Ja**.
5. Lassen Sie den zukünftigen Kontobesitzer seine E-Mail-Adresse verifizieren. Dazu muss er die ihm zugesendeten Anweisungen befolgen.
6. Wählen Sie das Benutzerkonto aus, dessen Eigentümerschaft Sie übertragen wollen, und klicken Sie dann auf das Drei-Punkte-Symbol > **Kennwort zurücksetzen**.
7. Bestätigen Sie die Aktion durch Klicken auf **Zurücksetzen**.
8. Lassen Sie den zukünftigen Kontobesitzer sein Kennwort zurücksetzen. Dazu muss er die Anweisungen befolgen, die ihm an seine E-Mail-Adresse zugesendet werden.

Der neue Besitzer kann jetzt auf das Konto zugreifen.

Zwei-Faktor-Authentifizierung einrichten

Die **Zwei-Faktor-Authentifizierung (2FA)** ist eine Variante der Multi-Faktor-Authentifizierung, bei der die Identität eines Benutzers anhand einer Kombination aus zwei verschiedenen Faktoren überprüft wird:

- Etwas, was der Benutzer weiß (eine PIN oder ein Kennwort)
- Etwas, was der Benutzer hat (ein Token)
- Etwas, was der Benutzer ist (Biometrik)

Die Zwei-Faktor-Authentifizierung bietet einen zusätzlichen Schutz gegen unbefugte Zugriffe auf Ihr Konto.

Die Plattform unterstützt die **TOTP (Time-based One-Time Password)**-Authentifizierung, die mit zeitlich limitierten Einmalkennwörtern arbeitet. Wenn die TOTP-Authentifizierung im System aktiviert ist, müssen Benutzer ihr herkömmlichs Kennwort sowie einen einmaligen TOTP-Code eingeben, um auf das System zugreifen zu können. Der Benutzer gibt sein Kennwort also als ersten Faktor und den TOTP-Code als zweiten Faktor ein. Der TOTP-Code wird von einer Authentifizierungsapplikation auf einem „Zweit-Faktor"-Gerät des Benutzers generiert – und zwar auf der Grundlage der aktuellen Uhrzeit und eines „Geheimnis" (auch Secret oder geheimer Schlüssel genannt, hier ein QR- oder alphanumerischen Code), welches von der Plattform bereitgestellt wird.

Und so funktioniert es

1. Sie aktivieren die Zwei-Faktor-Authentifizierung auf Ihrer Organisationsebene.
2. Die entsprechenden Anwender in Ihrem Unternehmens müssen eine Authentifizierungsapplikation auf einem ihrer Zweit-Faktor-Gerät (z.B. ein Mobiltelefon, Tablet, Laptop, Desktop-PC) installieren. Diese Applikation wird zum Generieren der einmaligen TOTP-Codes (also des Einmalkennwortes) verwendet. Diese Authentifikatoren werden empfohlen:
   - Google Authenticator
     iOS-App-Version (https://apps.apple.com/de/app/google-authenticator/id388497605)
     Android-Version
     (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     iOS-App-Version (https://apps.apple.com/de/app/microsoft-authenticator/id983156458)
     Android-Version (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Wichtig
   Die Benutzer müssen sicherstellen, dass die Uhrzeit auf dem Gerät, auf dem die Authentifizierungsapplikation installiert ist, korrekt eingestellt ist (also die aktuelle Uhrzeit widerspiegelt).
3. Die entsprechenden Benutzer Ihres Unternehmens müssen sich erneut am System anmelden.
4. Nach Eingabe ihrer Anmeldedaten (Benutzername, Kennwort) werden sie aufgefordert, eine Zwei-Faktor-Authentifizierung für ihr Benutzerkonto einzurichten.
5. Sie müssen einen angezeigten QR-Code mit ihrer Authentifizierungsapplikation scannen. Wenn es (aus welchem Grund auch immer) nicht möglich ist, den QR-Code zu scannen, kann der Benutzer alterantiv auch den 32-stelligen Code verwenden, der unter dem QR-Code angezeigt wird, und diesen dann manuell in die Authentifizierungsapplikation eingeben.

Wichtig
Es wird dringend empfohlen, diese Daten zu sichern (drucken Sie beispielsweise den QR-Code aus und notieren Sie sich das temporäre Einmalkennwort (den geheimen TOTP-Code). Verwenden Sie dabei eine Applikation, die die Sicherung von Codes per Cloud Backup unterstützt). Sie benötigen das temporäre Einmalkennwort (den TOTP-Code), um die Zwei-Faktor-Authentifizierung zurücksetzen zu können, falls das Zweit-Faktor-Gerät verloren gehen sollte.

6. Das temporäre Einmalkennwort (der TOTP-Code) wird in der Authentifizierungsapplikation generiert. Er wird alle 30 Sekunden automatisch neu generiert.
7. Der entsprechende Benutzer muss diesen einmaligen TOTP-Code dann im Fenster **Zwei-Faktor-Authentifizierung einrichten** eingeben, nachdem er zuvor sein eigenes Kennwort eingegeben hat.
8. Als Ergebnis dieser Prozedur ist dann die Zwei-Faktor-Authentifizierung für den Benutzer eingerichtet.

Wenn sich der Benutzer anschließend am System anmeldet, werden er jedes Mal aufgefordert, seine Anmeldedaten (Benutzername, Kennwort) sowie anschließend den einmaligen TOTP-Code anzugeben, der jedes Mal in der Authentifizierungsapplikation neu generiert wird. Ein Benutzer kann anschließend außerdem seinen Browser bei der Anmeldung am System als 'vertrauenswürdig' kennzeichnen. Das bewirkt, dass bei nachfolgenden Anmeldungen über diesen speziellen Browser kein einmaliger TOTP-Code mehr angefordert wird.

So können Sie die Zwei-Faktor-Authentifizierung auf einem neuen Gerät wiederherstellen

Wenn Sie Zugriff auf die zuvor eingerichtete Authentifizierungs-App für Mobilgeräte haben:

1. Installieren Sie eine Authenticator-App auf Ihrem neuen Gerät.
2. Verwenden Sie die PDF-Datei, die Sie beim Einrichten der Zwei-Faktor-Authentifizierung (2FA) auf Ihrem Gerät gesichert haben. Diese Datei enthält den 32-stelligen Code, der in der Authenticator-App eingegeben werden muss, um die Authenticator-App erneut mit Ihrem Acronis Konto verknüpfen zu können.

Wichtig
Wenn der Code korrekt ist, aber nicht funktioniert, stellen Sie sicher, dass die Uhrzeit in der Authenticator-App für Mobilgeräte synchronisiert wird.

3. Wenn Sie es beim Einrichten versäumt haben, die PDF-Datei zu sichern:

a. *Klicken Sie auf **2FA zurücksetzen** und geben Sie das Einmalkennwort ein, das in der zuvor eingerichteten Authenticator-App für Mobilgeräte angezeigt wird.*
b. Folgen Sie den Bildschirmanweisungen.

Wenn Sie keinen Zugriff auf die zuvor eingerichtete Authenticator-App für Mobilgeräte haben:

1. Nehmen Sie ein neues Mobilgerät.
2. Verwenden Sie die gespeicherte PDF-Datei, um ein neues Gerät zu verknüpfen (der Standardname der Datei ist `cyberprotect-2fa-backupcode.pdf`).
3. Stellen Sie den Zugriff auf Ihr Konto aus dem Backup wieder her. Stellen Sie sicher, dass Backups von Ihrer Mobilgeräte-App unterstützt werden.
4. Öffnen Sie die App unter dem gleichen Konto von einem anderen Mobilgerät aus, wenn dies von der App unterstützt wird.

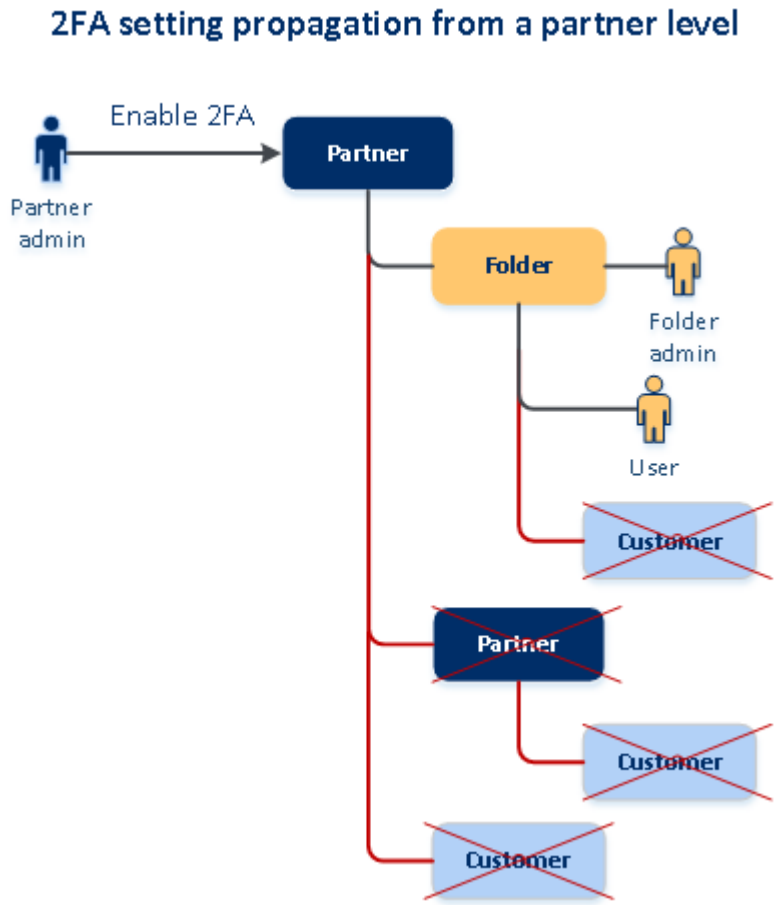
Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben

Die Zwei-Faktor-Authentifizierung wird auf der Ebene der **Organisation** (Unternehmensebene) eingerichtet. Sie können die Zwei-Faktor-Authentifizierung aktivieren oder deaktivieren:

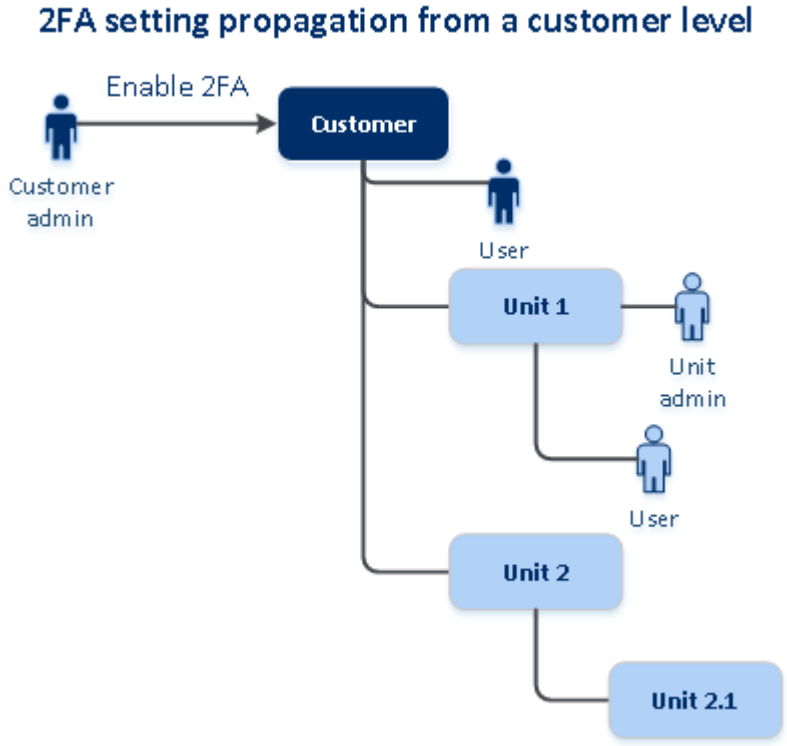
- Für Ihre eigene Organisation.
- Für Ihren Untermandanten (nur wenn die Option **Support-Zugang** in diesem Untermandanten aktiviert ist).

Die Zwei-Faktor-Authentifizierungseinstellungen werden folgendermaßen zwischen Mandantenebenen weitergegeben:

- Ordner übernehmen automatisch die Zwei-Faktor-Authentifizierungseinstellungen von ihrer Partnerorganisation. Im nachfolgenden Schema bedeuten die roten Linien, dass keine Zwei-Faktor-Authentifizierungseinstellungen weitergereicht werden können.



- Abteilungen übernehmen automatisch die Zwei-Faktor-Authentifizierungseinstellungen von ihrer Kundenorganisation.



Hinweis

1. Sie können die Zwei-Faktor-Authentifizierung für Ihre Unterorganisation nur (de)aktivieren, wenn die Option **Support-Zugang** innerhalb dieser Unterorganisation aktiviert ist.
2. Sie können die Einstellungen für die Zwei-Faktor-Authentifizierung für Benutzer der Unterorganisationen nur dann verwalten, wenn die Option **Support-Zugang** innerhalb dieser Unterorganisation aktiviert ist.
3. Es ist nicht möglich, die Zwei-Faktor-Authentifizierung auf der Ordner- oder Abteilungsebene einzurichten.
4. Sie können die Zwei-Faktor-Authentifizierungseinstellungen auch dann konfigurieren, wenn diese Einstellung für Ihre übergeordnete Organisation nicht aktiviert ist.

Die Zwei-Faktor-Authentifizierung für Ihren Mandanten einrichten

Als Administrator können Sie die Zwei-Faktor-Authentifizierung für Ihre Organisation aktivieren.

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten aktivieren

1. Gehen Sie im Management-Portal zu **Einstellungen** –> **Sicherheit**.
2. Verschieben Sie den Schalter für die **Zwei-Faktor-Authentifizierung** und klicken Sie dann auf **Aktivieren**.

Jetzt müssen alle Benutzer Organisation die Zwei-Faktor-Authentifizierung für ihre Konten einrichten. Sie werden dazu aufgefordert, wenn sie sich das nächste Mal anmelden wollen oder wenn ihre aktuelle Sitzung abläuft.

Die Fortschrittsanzeige unter dem Schalter gibt an, wie viele Benutzer eine Zwei-Faktor-Authentifizierung für ihre Konten eingerichtet haben. Wenn Sie überprüfen wollen, welche Anwender ihre Konten bereits konfiguriert haben, müssen Sie zur Registerkarte **Unternehmensverwaltung** –> **Benutzer** wechseln und die Spalte **2FA-Status** überprüfen. Der 2FA-Status von Benutzern, die noch keine Zwei-Faktor-Authentifizierung für ihre Konten konfiguriert haben, lautet **Setup erforderlich**.

Nachdem sie die Zwei-Faktor-Authentifizierung erfolgreich konfiguriert haben, müssen die Benutzer jedes Mal, wenn sie sich an der Service-Konsole anmelden, nicht nur ihren Anmeldenamen und ihr Kennwort eingeben, sondern auch einen TOTP-Code.

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten deaktivieren

1. Gehen Sie im Management-Portal zu **Einstellungen** –> **Sicherheit**.
2. Wenn Sie die Zwei-Faktor-Authentifizierung deaktivieren wollen, müssen Sie erst den Schalter ausschalten und dann auf **Deaktivieren** klicken.

3. [Wenn mindestens ein Benutzer die Zwei-Faktor-Authentifizierung innerhalb der Organisation konfiguriert hat] Geben Sie den TOTP-Code ein, der in Ihrer Authentifizierungsapplikation auf dem jeweiligen Mobilgerät generiert wurde.

Als Ergebnis wird die Zwei-Faktor-Authentifizierung für Ihre Organisation deaktiviert, alle geheimen Schlüssel werden gelöscht und alle vertrauenswürdigen Browser werden verworfen. Alle Benutzer können sich wieder nur durch Eingabe ihrer Anmeldedaten (Benutzername, Kennwort) am System anmelden. In der Registerkarte **Unternehmensverwaltung** –> **Benutzer** wird die Spalte **2FA-Status** ausgeblendet.

Die Zwei-Faktor-Authentifizierung für Benutzer verwalten

Sie können die Einstellungen für die Zwei-Faktor-Authentifizierung für all Ihre Benutzer überwachen und zudem im Management-Portal die Einstellungen in der Registerkarte **Unternehmensverwaltung** –> **Benutzer** zurücksetzen.

Monitoring

Sie können im Management-Portal, unter **Unternehmensverwaltung** –> **Benutzer**, eine Liste aller Benutzer in Ihrer Organisation einsehen. Der **2FA-Status** gibt an, ob die Zwei-Faktor-Konfiguration für einen bestimmten Benutzer eingerichtet wurde.

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer zurücksetzen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Zwei-Faktor-Authentifizierung zurücksetzen**.
4. Geben Sie den TOTP-Code ein, der in der Authentifizierungsapplikation auf Ihrem Zweit-Faktor-Gerät generiert wurde, und klicken Sie dann auf **Zurücksetzen**.

Anschließend kann der Benutzer die Zwei-Faktor-Authentifizierung wieder einrichten.

So können Sie die vertrauenswürdigen Browser eines Benutzers zurücksetzen

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Alle vertrauenswürdigen Browser zurücksetzen**.
4. Geben Sie den TOTP-Code ein, der in der Authentifizierungsapplikation auf Ihrem Zweit-Faktor-Gerät generiert wurde, und klicken Sie dann auf **Zurücksetzen**.

Der Benutzer, dessen vertrauenswürdige Browser Sie zurückgesetzt haben, muss jetzt bei seiner nächsten Anmeldung den TOTP-Code eingeben.

Die Benutzer können alle vertrauenswürdigen Browser und die Einstellungen für die Zwei-Faktor-Authentifizierung selbst zurücksetzen. Dies kann bei der Anmeldung am System erfolgen, indem Sie auf den entsprechenden Link klicken und den TOTP-Code eingeben, um die Aktion zu bestätigen.

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer deaktivieren

Wir raten davon ab, die Zwei-Faktor-Authentifizierung zu deaktivieren, weil die Mandanten damit einem erhöhten Sicherheitsrisiko ausgesetzt werden.

In Ausnahmefällen können Sie die Zwei-Faktor-Authentifizierung für einen bestimmten Benutzer deaktivieren, während Sie die Zwei-Faktor-Authentifizierung für alle anderen Benutzer des Mandanten beibehalten. Dies ist ein Workaround für solche Fälle, in denen die Zwei-Faktor-Authentifizierung in einem Mandanten aktiviert ist, bei dem eine Cloud-Integration konfiguriert ist – und diese Integration den Zugriff auf die Plattform über das Benutzerkonto (Anmelde-Kennwort) autorisiert. Um die Integration weiterhin verwenden zu können, kann der Benutzer als Übergangslösung in ein Service-Konto konvertiert werden, für das keine Zwei-Faktor-Authentifizierung erforderlich ist.

Wichtig
Es wird nicht empfohlen, reguläre Benutzer in Service-Benutzer umzuwandeln, um die Zwei-Faktor-Authentifizierung zu deaktivieren, weil dies ein Sicherheitsrisiko für den Mandanten darstellt.

Wenn Sie die Cloud-Integrationen verwenden wollen, ohne die Zwei-Faktor-Authentifizierung für die Mandanten zu deaktivieren, empfehlen wir als sichere Lösung, stattdessen API-Clients zu erstellen und Ihre Cloud-Integrationen so zu konfigurieren, dass sie mit diesen Clients funktionieren.

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Als Service-Konto kennzeichnen**. Der Benutzer erhält anschließend einen speziellen Zwei-Faktor-Authentifizierungsstatus namens **Service-Konto**.
4. [Wenn für mindestens einen Benutzer innerhalb eines Mandanten die Zwei-Faktor-Authentifizierung konfiguriert ist] Geben Sie den TOTP-Code ein, der in der Authentifizierungsapplikation auf Ihrem Zweit-Faktor-Gerät generiert wurde, um die Deaktivierung zu bestätigen.

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer aktivieren

Möglicherweise müssen Sie die Zwei-Faktor-Authentifizierung für einen bestimmten Benutzer wieder aktivieren, dessen Aktivierung Sie zuvor deaktiviert hatten.

1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.
2. Suchen Sie in der Registerkarte **Benutzer** einen Benutzer, dessen Einstellungen Sie ändern möchten – und klicken Sie anschließend auf das Drei-Punkte-Symbol.
3. Klicken Sie auf **Als Standard-Konto kennzeichnen**. Als Ergebnis dieser Prozedur muss der die Zwei-Faktor-Authentifizierung wieder einrichten oder den TOTP-Code bereitstellen, wenn er sich am System anmeldet.

Die Zwei-Faktor-Authentifizierung bei Verlust des Zweit-Faktor-Gerätes zurücksetzen

Befolgen Sie einen der nachfolgenden vorgeschlagenen Ansätze, um den Zugriff auf Ihr Konto zurückzusetzen, wenn das Zweit-Faktor-Gerät einmal verloren gehen sollte:

- Stellen Sie Ihren geheimen TOTP-Schlüssel (TOTP-„Geheimnis“ – ein QR-Code oder ein alphanumerischer Code) aus einem Backup wieder her.

  Verwenden Sie ein anderes Zweit-Faktor-Gerät und geben Sie den gespeicherte geheimen TOTP-Schlüssel in die Authentifizierungsapplikation ein, die auf diesem Alternativgerät installiert ist.
- Bitten Sie Ihren Administrator, die Zwei-Faktor-Authentifizierungseinstellungen für Sie zurückzusetzen.

Schutz vor Brute-Force-Angriffen

Bei einem Brute-Force-Angriff versucht ein Eindringling dadurch Zugang zum System zu erhalten, indem er viele Kennwörter an das System überträgt, um so das richtige Kennwort durch Ausprobieren zu erraten.

Der Brute-Force-Schutzmenachnismus der Plattform basiert auf Geräte-Cookies.

Die auf der Plattform verwendeten Einstellungen für den Brute-Force-Schutz sind vordefiniert:

Parameter	Das Kennwort eingeben	Den TOTP-Code eingeben
Versuchslimit	10	5
Versuchslimitzeitraum (das Limit wird nach dem Timeout zurückgesetzt)	15 min (900 s)	15 min (900 s)
Sperrung erfolgt bei	Versuchslimit + 1 (11. Versuch)	Versuchslimit
Sperrzeitraum	5 min (300 s)	5 min (300 s)

Wenn Sie die Zwei-Faktor-Authentifizierung aktiviert haben, wird ein Geräte-Cookie erst nach einer erfolgreichen Authentifizierung mit beiden Faktoren (Kennwort und TOTP-Code) an einen Client (Browser) ausgestellt.

Bei vertrauenswürdigen Browsern wird das Geräte-Cookie nach einer erfolgreichen Authentifizierung mit nur einem Faktor (Kennwort) ausgestellt.

Die Versuche zur Eingabe des TOTP-Codes werden pro Benutzer und nicht pro Gerät registriert. Das bedeutet, dass selbst wenn ein Benutzer versucht, den TOTP-Code mit verschiedenen Geräten einzugeben, diese (und damit er selbst) trotzdem blockiert werden.

Upselling-Szenarien für Ihre Kunden konfigurieren

Upselling ist eine Technik, um Ihre Kunden zum Kauf zusätzlicher Funktionen einzuladen.

Cyber Protection hat mehrere ältere Editionen (Legacy-Editionen), die sich in Funktionalität und Preis unterscheiden. So können Sie beispielsweise Bestandskunden, die eine Basis-Edition verwenden, eine teurere Edition mit erweiterter Funktionalität anbieten.

Sie können die Upselling-Fähigkeit für jeden Kunden aktivieren oder deaktivieren. Die Upselling-Option ist standardmäßig deaktiviert. Wenn Sie das Upselling für einen Kunden aktivieren, wird diesem eine zusätzliche Funktionalität angezeigt, die verfügbar wird, sobald der Kunde die entsprechende beworbene Edition kauft. Diese zusätzliche Funktionalität ist orange hervorgehoben und mit dem Namen oder Symbol der beworbenen Edition gekennzeichnet. Diese Upselling-Punkte werden allen Kunden angezeigt, um diese zum Kauf einer teureren Edition zu motivieren. Wenn ein Kunde auf einen solchen Upselling-Punkt klickt, wird ihm über einen angezeigten Dialog vorgeschlagen, eine teurere Edition zu kaufen, um die gewünschte Funktionalität zu aktivieren.

Das Aktionselement hängt von der Art des Kundenbenutzers ab. Der Typ des Benutzers (Käufer oder Nicht-Käufer) kann mithilfe der Plattform-API konfiguriert werden. Einzelheiten finden Sie in der API-Dokumentation. Weitere Informationen über Aktionspunkte, die Ihren Kunden gezeigt werden können, finden Sie in der nachfolgenden Tabelle:

Typ der Benutzer im Kunden-Mandanten	Aktionselement
Administrator; Käufer	Die Schaltfläche **Jetzt kaufen** wird in der Benutzeroberfläche angezeigt.*
Administrator; Nicht-Käufer	In der Benutzeroberfläche wird die Nachricht „Kontaktieren Sie Ihren Partner, um ein Upgrade der Edition durchzuführen“.
Benutzer; Käufer	In der Benutzeroberfläche wird die Nachricht „Kontaktieren Sie Ihren Partner, um ein Upgrade der Edition durchzuführen“.
Benutzer; Nicht-Käufer	In der Benutzeroberfläche wird die Nachricht „Kontaktieren Sie Ihren Partner, um ein Upgrade der Edition durchzuführen“.

* Der Link für die Schaltfläche **Jetzt kaufen**, die einen Kunden zu einer Website umleitet, um eine Advanced-Edition kaufen zu können, kann unter **Einstellungen** –> **Branding** konfiguriert werden. Im Bereich **Upselling** können Sie die Option **URL für 'Kaufen'** spezifizieren. Die Branding-Einstellungen werden auf alle direkten und indirekten untergeordneten Partner/Ordner und Kunden des Mandanten angewendet, für den das Branding konfiguriert ist.

So können Sie die Upselling-Fähigkeit für einen Kunden (de)aktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den Kunden aus, gehen Sie zum rechten Fensterbereich und klicken Sie dann auf die Registerkarte **Konfigurieren**.
3. Gehen Sie im Bereich **Upselling** folgendermaßen vor:
   - Aktivieren Sie die Option **Mehr Advanced-Editionen fördern**, um das Upselling-Szenario für Kunden einzuschalten.
   - Deaktivieren Sie die Option **Mehr Advanced-Editionen fördern**, um das Upselling-Szenario für Kunden auszuschalten.

Upselling-Punkte, die einem Kunden angezeigt werden

Schwachstellenliste

Die Schwachstellenliste kann in der Cyber Protect-Konsole unter **Software-Verwaltung** –> **Schwachstellen** gefunden werden. Wenn ein Benutzer auf das Kreuzstich-Icon klickt, wird ein Angebotsdialog geöffnet, um den Benutzer zum Kauf der teureren Edition aufzufordern.

Einen Schutzplan erstellen oder bearbeiten

Dies kann in der Cyber Protect-Konsole unter **Pläne** –> **Schutz** gefunden werden. Klicken Sie auf **Plan erstellen**. Bei den Cyber Backup-Editionen sind nur die Module **Backup** und **Schwachstellen** aktiviert. Die übrigen Module sind nur in den Cyber Protect-Editionen verfügbar. Ihr Kunde kann alle Module nach dem Kauf einer der Cyber Protect-Editionen aktivieren lassen.

Assistent für die automatische Erkennung

Dieser Assistent kann in der Cyber Protect-Konsole unter **Geräte** –> **Alle Geräte** gefunden werden. Ihr Kunde sollte den Assistenten für die automatische Erkennung starten, indem er auf **Hinzufügen** klickt, dann zum Bereich **Mehrere Geräte** geht und anschließend auf **Nur Windows** klickt. Die automatische Erkennung von Maschinen ist nur in den Advanced-Editionen verfügbar.

Aktionen in der Geräteliste

Diese Liste kann in der Cyber Protect-Konsole unter **Geräte** –> **Alle Geräte** gefunden werden. Ihr Kunde sollte die Maschine auswählen. Anschließend werden zwei zusätzliche Optionen im linken Fensterbereich angezeigt:

- **Über HTML5-Client verbinden**
- **Patchen**

Diese Optionen sind nur dann verfügbar, wenn ein Kunde eine teurere Edition als die bereits vorhandene erwirbt.

Speicherorte und Storage verwalten

Im Bereich **Einstellungen** –> **Speicherorte** werden die Cloud Storages und Disaster Recovery-Infrastrukturen angezeigt, die Sie verwenden können, um Ihren Partnern und Kunden die Services **Cyber Protection** sowie **File Sync & Share** bereitzustellen.

Storages, die für andere Services konfiguriert sind, werden in zukünftigen Produktversionen im Bereich **Speicherorte** angezeigt.

Speicherorte

Ein Speicherort ist eine Art Container, um Cloud-Storages und Disaster-Recovery-Infrastrukturen bequem gruppieren zu können. Er kann alles Ihrer Wahl darstellen, wie beispielsweise ein bestimmtes Datacenter oder einen geografischen Standort Ihrer Infrastrukturkomponenten.

Sie können beliebig viele Speicherorte erstellen und diese mit Backup Storages, Disaster Recovery-Infrastrukturen und **File Sync & Share** Storages befüllen. Ein Speicherort kann mehrere Cloud Storages enthalten, aber nur eine Disaster Recovery-Infrastruktur.

Weitere Informationen über Storages und Aktionen, die Sie mit diesen durchführen können, finden Sie im Abschnitt 'Storages verwalten'.

Speicherorte und Storages für Partner und Kunden wählen

Sie können bei der Erstellung eines Partner-/Ordner-Mandanten für jeden Service verschiedene Speicherorte und Storages auswählen, die dem neuen Mandanten dann zur Verfügung stehen.

Wenn Sie einen Kunden-Mandanten erstellen, müssen Sie einen Speicherort auswählen und dann innerhalb dieses Speicherortes einen Storage pro Service auswählen. Die dem Kunden zugewiesenen Storages können auch zu einem späteren Zeitpunkt geändert werden, jedoch nur, wenn deren Nutzung 0 GB beträgt. Also entweder bevor der Kunde begonnen hat, den Storage zu nutzen – oder nachdem der Kunde all seine Backups aus dem Storage gelöscht hat.

Informationen über die Storages, die einem Kunden-Mandanten zugewiesen wurden, werden im Fensterbereich für die Mandanten-Details angezeigt, wenn Sie einen Mandanten in der Registerkarte **Clients** auswählen. Die Anzeige der Informationen über die Speicherplatznutzung erfolgt nicht in Echtzeit. Die Aktualisierung dieser Informationen kann bis zu 24 Stunden dauern.

Informationen zur Georedundanz finden Sie im Abschnitt '"Georedundanter Storage" (S. 88)'.

Aktionen mit Speicherorten

Wenn Sie einen neuen Speicherort erstellen wollen, klicken Sie zuerst auf **Speicherort hinzufügen** und spezifizieren Sie dann einen Namen für den Speicherort.

Um einen Storage oder eine Disaster Recovery Infrastruktur an einen anderen Ort zu verschieben, wählen Sie zuerst den Storage oder die Infrastruktur aus. Klicken Sie anschließend auf das Stiftsymbol im Feld **Speicherort** und wählen Sie dann den Zielspeicherort aus.

Um einen Speicherort umzubenennen, klicken Sie zuerst neben dem Namen des Speicherortes auf das Drei-Punkte-Symbol. Klicken Sie dann auf **Umbenennen** und spezifizieren Sie abschließend einen Namen für den Speicherort.

Um einen Speicherort zu löschen, klicken Sie zuerst neben dem Namen des Speicherortes auf das Drei-Punkte-Symbol. Klicken Sie dann auf **Löschen** und bestätigen Sie abschließend Ihre Entscheidung. Nur leere Speicherorte können gelöscht werden.

Storages verwalten

Neue Storages hinzufügen

- **Cyber Protection** Service:
  - Standardmäßig werden die Backup Storages in den Datacentern verwaltet.
  - Wenn ein höherstufiger Administrator für einen Partner-Mandanten das Angebotselement **Partner-eigener Backup Storage** aktiviert, können die Partner-Administratoren unter Verwendung von Cyber Infrastructure einen Storage im Datacenter des Partners organisieren. Wenn Sie im Bereich **Speicherorte** auf den Befehl **Backup Storage hinzufügen** klicken, erhalten Sie Informationen darüber, wie Sie einen Backup Storage in Ihrem eigenen Datacenter organisieren können.
  - Wenn ein höherstufiger Administrator für einen Partner-Mandanten das Angebotselement **Partner-eigene Disaster Recovery-Infrastruktur** aktiviert, können die Partner-Administratoren eine Disaster Recovery-Infrastruktur im Datacenter des Partners organisieren. Wenn Sie weitere Informationen über das Hinzufügen einer Disaster Recovery-Infrastruktur benötigen, können Sie sich an den technischen Support wenden.

  Hinweis
  Eine Backup-Validierung ist bei Public Cloud Objekt-Storages (wie Amazon S3, Microsoft Azure, Google Cloud Storage und Wasabi), die von den Datacentern verwendet werden, nicht möglich. Eine Backup-Validierung ist bei Public Cloud Object-Storages möglich, die von Partnern verwendet werden. Es wird jedoch nicht empfohlen, diese Option zu aktivieren, weil Validierungsaktionen den ausgehenden Datenverkehr von solchen öffentlichen Objekt-Storages erhöhen und zu erheblichen Kosten führen können.

- Wenn Sie Informationen über das Hinzufügen von Storages benötigen, die von anderen Services genutzt werden, wenden Sie sich an den technischen Support.

Storages löschen

Sie können Storages löschen, die von Ihnen selbst oder einem Ihrer Untermandanten hinzugefügt wurden.

Wenn der Storage einem Kunden-Mandanten zugewiesen wurde, müssen Sie vor dem Löschen des Storages den Service deaktivieren, der den Storage für alle Kunden-Mandanten verwendet.

So können Sie einen Storage löschen

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, bei dem der Storage hinzugefügt wurde.
3. Klicken Sie auf **Einstellungen** –> **Speicherorte**.
4. Wählen Sie den Storage aus, den Sie löschen wollen.
5. Klicken Sie im Fensterbereich der Storage-Eigenschaften auf das Drei-Punkte-Symbol und anschließend auf **Storage löschen**.
6. Bestätigen Sie Ihre Entscheidung.

Unveränderlicher Storage

Über den unveränderlichen Storage können Sie während einer spezifizierten Aufbewahrungsdauer auf gelöschte Backups zugreifen. Sie können die Inhalte dieser Backups wiederherstellen, aber Sie können diese nicht ändern, verschieben oder löschen. Wenn die Aufbewahrungsdauer endet, werden die gelöschten Backups dauerhaft gelöscht.

Der unveränderliche Storage enthält folgende Backups:

- Backups, die manuell gelöscht wurden.
- Backups, die – gemäß den Einstellungen im Bereich **Aufbewahrungsdauer** in einem Schutzplan oder im Bereich **Aufbewahrungsregeln** in einem Bereinigungsplan – automatisch gelöscht wurden.

Gelöschte Backups im unveränderlichen Storage belegen weiterhin Speicherplatz und werden entsprechend abgerechnet.

Gelöschten Mandanten wird keine Speicherplatz-Belegung (auch nicht im unveränderlichen Storage) in Rechnung gestellt.

Sie können den unveränderlichen Storage sowohl auf Partner- als auch auf Kundenebene konfigurieren.

Wichtig
Diese Ebenen sind nicht voneinander abhängig. Kunden-Administratoren können den unveränderlichen Storage für ihre Mandanten aktivieren – auch wenn der unveränderliche Storage im übergeordneten Partner-Mandanten nicht aktiviert ist. Nur wenn für einen untergeordneten Mandanten keine benutzerdefinierten Einstellungen angewendet werden, wird dieser die Einstellungen des übergeordneten Mandanten übernehmen.

Zur Konfiguration der unveränderlichen Storage-Einstellungen ist eine Zwei-Faktor-Authentifizierung in dem Mandanten erforderlich, zu dem das Administratorkonto gehört.

Die Modi für den unveränderlichen Storage

Für Partner-Mandanten gibt es keine Möglichkeit, einen unveränderlichen Storage-Modus auszuwählen. Ein Administrator kann den unveränderlichen Storage deaktivieren und wieder aktivieren sowie dessen Modus und Aufbewahrungsdauer ändern.

Für Kunden-Mandanten ist der unveränderliche Storage in folgenden Modi verfügbar:

- **Governance-Modus**
  Sie können den unveränderlichen Storage erst deaktivieren und wieder aktivieren. Sie können die Aufbewahrungsdauer ändern oder auf den Compliance-Modus umschalten.
- **Compliance-Modus**

  Warnung!
  Die Auswahl des Compliance-Modus kann nicht rückgängig gemacht werden.

  Sie können den unveränderlichen Storage nicht wieder deaktivieren. Sie können weder die Aufbewahrungsdauer ändern noch zurück in den Governance-Modus wechseln.

Hinweis
Ab Version 21.12 ist für neue Partner-Mandanten der unveränderliche Storage mit einer Aufbewahrungsdauer von 14 Tagen standardmäßig aktiviert. Bei bereits vorhandenen Mandanten müssen Sie den unveränderlichen Storage erst manuell aktivieren.

Unterstützte Storages und Agenten

- Der unveränderliche Storage wird nur auf dem Cloud Storage unterstützt.
  Der unveränderliche Storage ist sowohl für von Acronis gehostete als auch für von Partnern gehostete Cloud Storages verfügbar, die Cyber Infrastructure 4.7.1 oder höher verwenden.
  Alle Storages, die mit dem Cyber Infrastructure Backup Gateway verwendet werden können, werden unterstützt. Zum Beispiel der Cyber Infrastructure Storage, Amazon S3- und EC2-Storages sowie der Microsoft Azure Storage.
  Der unveränderliche Storage erfordert, dass der TCP-Port 40440 für den Backup Gateway Service in Cyber Infrastructure geöffnet ist. Ab Version 4.7.1 wird der TCP-Port 40440 automatisch mit dem Traffic-Typ **Backup (ABGW) öffentlich** geöffnet. Weitere Informationen über die Traffic-Typen finden Sie in der Acronis Cyber Infrastructure-Dokumentation.
- Für den unveränderlichen Storage muss der Protection Agent in Version 21.12 (Build 15.0.28532) oder höher installiert sein.
- Es werden nur TIBX-Backups (Version 12) unterstützt.

Den unveränderlichen Storage aktivieren oder deaktivieren

Zur Konfiguration der unveränderlichen Storage-Einstellungen ist eine Zwei-Faktor-Authentifizierung in dem Mandanten erforderlich, zu dem das Administratorkonto gehört.

Hinweis
Wenn Sie den Zugriff auf gelöschte Backups zulassen wollen, sollte der Port 40440 für eingehende Verbindungen auf dem Backup Storage aktiviert sein.

So können Sie den unveränderlichen Storage aktivieren

Bei einem Partner-Mandanten

1. Melden Sie sich als Administrator am Management-Portal an und gehen Sie dann zu **Einstellungen** –> **Sicherheit**.
2. Aktivieren Sie den Schalter **Unveränderlicher Storage**.
3. Spezifizieren Sie eine Aufbewahrungsdauer in einem Bereich von 14 bis 3650 Tagen.
   Die standardmäßige Aufbewahrungsdauer beträgt 14 Tage. Eine längere Aufbewahrungsdauer führt zu einer erhöhten Speichernutzung.
4. Klicken Sie auf **Speichern**.

Bei einem Kunden-Mandanten

1. Melden Sie sich als Administrator am Management-Portal an und gehen Sie dann zu **Clients**.
2. Wenn Sie die Einstellungen für einen Kunden-Mandanten bearbeiten wollen, müssen Sie auf dessen Namen klicken.
3. Gehen Sie im Navigationsmenü zu **Einstellungen** –> **Sicherheit**.
4. Aktivieren Sie den Schalter **Unveränderlicher Storage**.
5. Spezifizieren Sie eine Aufbewahrungsdauer in einem Bereich von 14 bis 3650 Tagen.
   Die standardmäßige Aufbewahrungsdauer beträgt 14 Tage. Eine längere Aufbewahrungsdauer führt zu einer erhöhten Speichernutzung.
6. Wählen Sie den Modus für den unveränderlichen Storage und bestätigen Sie bei entsprechender Aufforderung Ihre Wahl.
7. Klicken Sie auf **Speichern**.

   Warnung!
   Wenn Sie den **Compliance-Modus** auswählen, so kann dies nicht rückgängig gemacht werden. Wenn Sie diesen Modus ausgewählt haben, können Sie den unveränderlichen Storage nicht mehr deaktivieren und auch nicht mehr dessen Modus oder die Aufbewahrungsdauer ändern.

8. Wenn Sie erreichen wollen, dass ein vorhandenes Archiv den unveränderlichen Storage unterstützt, müssen Sie ein neues Backup in diesem Archiv erstellen.
   Führen Sie zum Erstellen eines neuen Backups den Schutzplan entweder manuell oder über eine Planung aus.

   Warnung!
   Wenn Sie ein Backup löschen, bevor Sie bewirkt haben, dass das Archiv den unveränderlichen Storage unterstützt, wird das Backup endgültig gelöscht.

So können Sie den unveränderlichen Storage deaktivieren

Bei einem Partner-Mandanten

1. Melden Sie sich als Administrator am Management-Portal an und gehen Sie dann zu **Einstellungen** –> **Sicherheit**.
2. Deaktivieren Sie den Schalter **Unveränderlicher Storage**.

Wichtig
Diese Änderung wird an alle Untermandanten vererbt, die keine benutzerdefinierten Einstellungen für den unveränderlichen Storage verwenden.

Warnung!
Eine Deaktivierung des unveränderlichen Storage tritt nicht sofort in Kraft. Der unveränderliche Storage bleibt für eine Frist von 14 Tagen aktiv, sodass Sie entsprechend der ursprünglichen Aufbewahrungsdauer auf die entsprechenden gelöschten Backups zugreifen können. Wenn die Frist endet, werden alle Backups im unveränderlichen Storage dauerhaft gelöscht.

3. Bestätigen Sie Ihre Auswahl, indem Sie auf **Deaktivieren** klicken.

Bei einem Kunden-Mandanten

1. Melden Sie sich als Administrator am Management-Portal an und gehen Sie dann zu **Clients**.
2. Wenn Sie die Einstellungen für einen Kunden-Mandanten bearbeiten wollen, müssen Sie auf dessen Namen klicken.
3. Gehen Sie im Navigationsmenü zu **Einstellungen** –> **Sicherheit**.
4. Deaktivieren Sie den Schalter **Unveränderlicher Storage**.

Hinweis
Sie können unveränderlichen Storage nur im Governance-Modus deaktivieren.

Warnung!
Eine Deaktivierung des unveränderlichen Storage tritt nicht sofort in Kraft. Der unveränderliche Storage bleibt für eine Frist von 14 Tagen aktiv, sodass Sie entsprechend der ursprünglichen Aufbewahrungsdauer auf die entsprechenden gelöschten Backups zugreifen können. Wenn die Frist endet, werden alle Backups im unveränderlichen Storage dauerhaft gelöscht.

5. Bestätigen Sie Ihre Auswahl, indem Sie auf **Deaktivieren** klicken.

Abrechnungsbeispiel für den unveränderlichen Storage

Das nachfolgende Beispiel zeigt ein gelöschtes Backup, das für 14 Tage in den unveränderlichen Storage kommt. Dies ist die standardmäßige Aufbewahrungsdauer. Während dieses Zeitraums wird das gelöschte Backup Speicherplatz belegen. Wenn die Aufbewahrungsdauer endet, wird das gelöschte Backup dauerhaft gelöscht, woraufhin dann auch die Storage-Nutzung wieder abnimmt. Die Storage-Nutzung wird jeden Monat entsprechend abgerechnet.

Datum	Backups	Storage-Nutzung	Abrechnung
1. April	Backup A (10 GB) wird erstellt Backup B (1 GB) wird erstellt	10 GB + 1 GB = 11 GB	

Datum	Backups	Storage-Nutzung	Abrechnung
20. April	Backup B wird gelöscht und kommt in den unveränderlichen Storage (mit einer Aufbewahrungsdauer von 14 Tagen)	10 GB + 1 GB = 11 GB	
30. April			11 GB für April abgerechnet
4. Mai	Backup B wird dauerhaft gelöscht, weil die Aufbewahrungsdauer abgelaufen ist	11 GB - 1 GB = 10 GB	
31. Mai			10 GB für Mai abgerechnet

Georedundanter Storage

Der georedundante Storage gewährleistet die Dauerhaftigkeit von gespeicherten Daten, indem diese asynchron zu einem sekundären Speicherort kopiert werden, der geografisch vom primären Speicherort entfernt liegt. Dank der Georedundanz bleiben Ihre Daten auch dann verfügbar, wenn der primäre Standort nicht mehr erreichbar ist.

Den georedundanten Storage aktivieren oder deaktivieren

Voraussetzungen

- Stellen Sie sicher, dass der georedundante Storage für Ihre Cloud-Infrastruktur verfügbar ist.
- Nur Administratoren können den georedundanten Storage aktivieren oder deaktivieren. Stellen Sie sicher, dass Sie über Administratorrechte verfügen.

So können Sie den georedundanten Storage für bestehende Mandanten aktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Gehen Sie zu dem Mandanten, für den Sie die Georedundanz aktivieren wollen.

   Hinweis
   Weitere Informationen zur Aktivierung der Georedundanz für mehrere Mandanten finden Sie im Abschnitt '"Services für mehrere bestehende Mandanten aktivieren" (S. 46)'.

3. Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.
4. Aktivieren Sie bei **Cloud-Ressourcen** das Kontrollkästchen **Georedundanz** unter dem gewünschten Storage-Namen.
5. Klicken Sie auf **Speichern**.
   Georedundanz ist für den Mandanten aktiviert. Kunden-Administratoren können die Georedundanz in der Cyber Protect-Konsole deaktivieren.

So können Sie den georedundanten Storage für bestehende Mandanten deaktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Gehen Sie zu dem Mandanten, für den Sie die Georedundanz deaktivieren wollen.
3. Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.
4. Deaktivieren Sie bei **Cloud-Ressourcen** das Kontrollkästchen **Georedundanz** unter dem gewünschten Storage-Namen.
5. Klicken Sie auf **Speichern**.

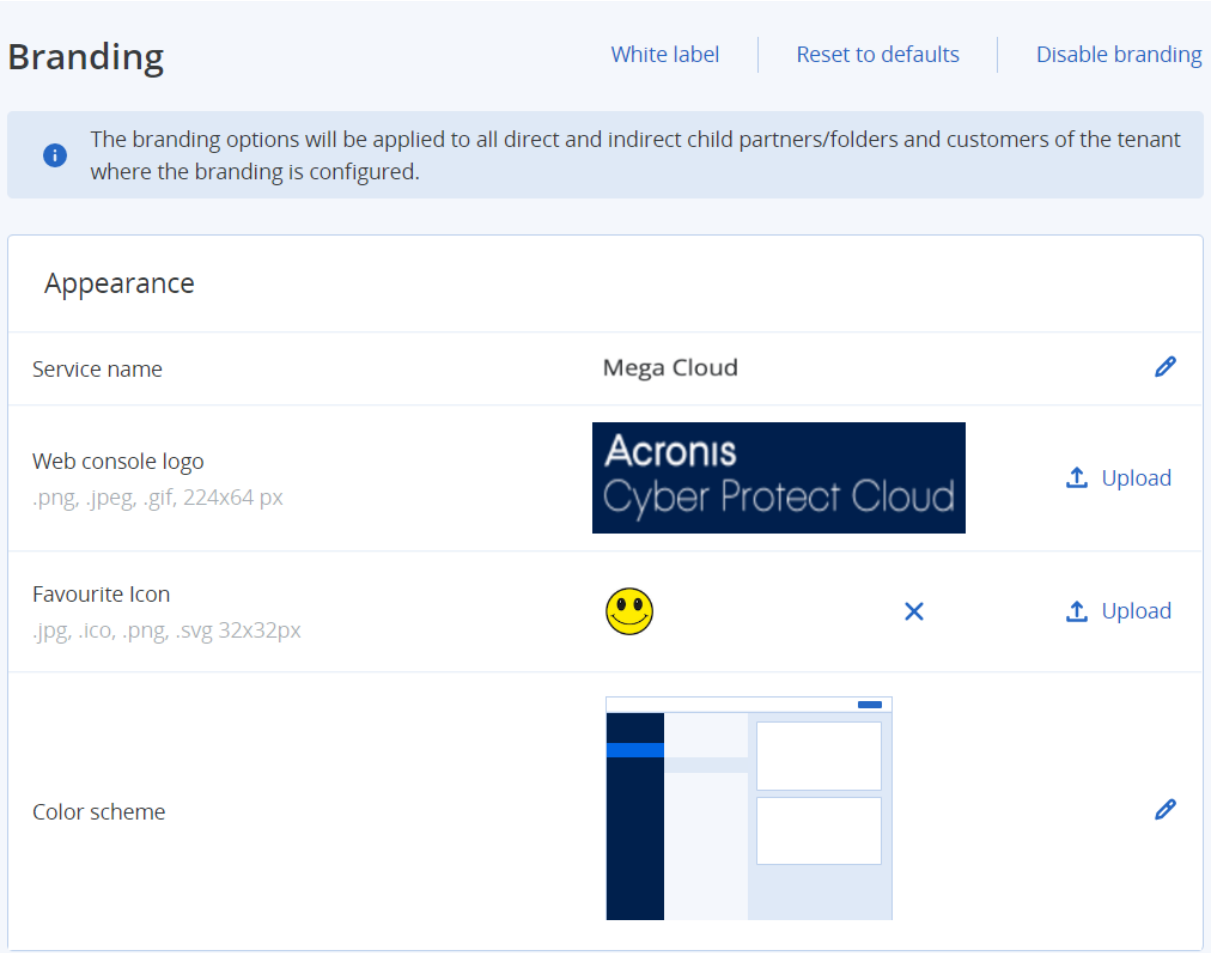
Warnung!
Die Georedundanz ist deaktiviert. Die replizierten Daten werden innerhalb eines Tages gelöscht.

Einschränkungen

- Derzeit sind sekundäre Standorte für replizierte Daten nur in den Vereinigten Staaten und Kanada verfügbar.
- Weitere Informationen zu Einschränkungen des Disaster Recovery Service bei Verwendung der Georedundanz-Funktion finden Sie in der Disaster Recovery-Dokumentation.

Branding und White-Labeling konfigurieren

Über den Bereich **Einstellungen** –> **Branding** können Partner-Administratoren die Benutzeroberfläche des Management-Portals und des **Cyber Protection** Service anpassen, um jede Assoziation mit den höherstufigen Partnern zu entfernen.



Das Branding kann auf Partner- oder Ordner-Ebene konfiguriert werden. Das Branding wird auf alle direkten und indirekten untergeordneten Partner/Ordner und Kunden des Mandanten angewendet, für den das Branding konfiguriert ist.

Andere Services bieten in ihren Service-Konsolen separate Branding-Fähigkeiten. Weitere Informationen finden Sie in den Benutzeranleitungen der entsprechenden Services.

Branding-Elemente

Aussehen

- **Service-Name**. Dieser Name wird in allen E-Mail-Nachrichten verwendet, die vom Management-Portal und den Cloud Services versendet werden (Konto-Aktivierungsnachrichten, E-Mail-Benachrichtigungen vom Service). Außerdem auf der **Willkommen**-Seite (bei der ersten Anmeldung) und als Bezeichnung für die Registerkarte des Management-Portals im Webbrowser.
- **Webkonsole-Logo**. Das Logo wird im Management-Portal und in den Services angezeigt. Klicken Sie auf **Upload**, um eine Image-Datei hochzuladen.
- **Favoriten-Icon** [Nur verfügbar, wenn eine benutzerdefinierte URL konfiguriert wurde]. Das Favicon wird in der Browser-Registerkarte neben dem Seitentitel angezeigt. Klicken Sie auf **Upload**, um eine Image-Datei hochzuladen.

- **Farbschema**. Das Farbschema definiert Farbkombinationen, die für die Elemente der Benutzeroberfläche verwendet werden können.

Hinweis
Klicken Sie auf **Schema in einer neuen Registerkarte anzeigen**, wenn Sie per Vorschau beurteilen wollen, wie die Benutzeroberfläche für Ihre Untermandanten aussehen wird. Das Branding wird erst angewendet, wenn Sie im Fensterbereich **Farbschema wählen** auf **Fertig** klicken.

Branding des Agenten und Installers

Sie können das Branding der Agent-Installationsdateien und des Tray Monitors für Windows und macOS anpassen.

Hinweis
Wenn Sie diese Funktionalität aktivieren wollen, müssen Sie die Cyber Protection Agenten auf Version 15.0.28816 (Release 22.01) oder höher aktualisieren.

- **Dateiname des Agenten-Installers**. Der Name der Installationsdatei, die auf geschützten Workloads heruntergeladen wird.
- **Logo des Agenten-Installers**. Das Logo, das während der Installation des Agenten im Setup-Assistenten angezeigt wird. Klicken Sie auf **Upload**, um eine Image-Datei hochzuladen.
- **Agenten-Name**. Das Logo, das während der Installation des Agenten im Setup-Assistenten angezeigt wird.
- **Tray Monitor-Name**. Der Name, der oben im Fenster des Tray Monitors angezeigt wird.

Dokumentation und Support

- **URL der Homepage**. Diese Seite wird geöffnet, wenn ein Benutzer im Fensterbereich **Über** auf den Firmennamen klickt.
- **URL für Support**. Diese Seite wird geöffnet, wenn ein Benutzer im Fensterbereich **Über** – oder in einer vom Management-Portal gesendeten E-Mail-Nachricht – auf den Link '**Support kontaktieren**' klickt.
- **Support-Telefon**. Diese Telefonnummer wird im Fensterbereich **Über** angezeigt.
- **URL der Knowledge Base**. Diese Seite wird geöffnet, wenn ein Benutzer in einer Fehlermeldung auf den Link '**Knowledge Base**' klickt.
- **Management-Portal-Administrator-Anleitung**. Diese Seite wird geöffnet, wenn ein Benutzer in der rechten oberen Ecke der Management-Portal-Benutzeroberfläche zuerst auf das Fragezeichensymbol und dann auf **Über** –> **Anleitung für Administratoren** klickt.
- **Management-Portal-Administrator-Hilfe**. Diese Seite wird geöffnet, wenn ein Benutzer in der rechten oberen Ecke der Management-Portal-Benutzeroberfläche zuerst auf das Fragezeichensymbol und dann auf **Hilfe** klickt.

URL für Cyber Protect Cloud Services

Sie können die Cyber Protect Cloud Services von Ihrer eigenen Domain aus verfügbar machen. Klicken Sie auf **Konfigurieren**, wenn Sie erstmalig eine benutzerdefinierte URL festlegen wollen – oder klicken Sie auf **Rekonfigurieren**, um eine bestehende URL zu ändern. Wenn Sie die vorgegebene URL (https://cloud.acronis.com) verwenden wollen, klicken Sie auf **Auf Standard zurücksetzen**. Weitere Informationen über benutzerdefinierte URLs finden Sie unter 'Eine benutzerdefinierte URL für die Weboberfläche konfigurieren'.

Einstellungen für rechtliche Dokumente:

- **URL der EULA**. Diese Seite wird geöffnet, wenn ein Benutzer im Fensterbereich **Über** auf den Link **Endbenutzer-Lizenzvereinbarung** klickt. Alternativ findet sich der Link auch auf der **Willkommen**-Anzeige (wird bei der ersten Anmeldung angezeigt) sowie auf den Zielseiten (Landing-Pages) der File Sync & Share-Upload-Anforderung.
- **URL der Plattform-Vertragsbedingungen**. Diese Seite wird geöffnet, wenn ein Partner-Administrator im Fensterbereich **Über** – oder auf der **Willkommensseite** bei der ersten Anmeldung – auf den Link **Plattform-Vertragsbedingungen** klickt.
- **URL der Datenschutzerklärung**. Diese Seite wird geöffnet, wenn ein Benutzer auf der **Willkommen**-Anzeige (wird bei der ersten Anmeldung angezeigt) auf den Link **Datenschutzerklärung** klickt. Alternativ findet sich der Link auch auf den Zielseiten (Landing Pages) der File Sync & Share-Upload-Anforderung.

Wichtig
Wenn Sie nicht wollen, dass ein Dokument auf der Willkommensseite erscheint, sollten Sie keine URL für dieses Dokument eingeben.

Hinweis
Weitere Informationen über File Sync & Share-Upload-Anforderungen finden Sie Benutzeranleitung für Cyber Files Cloud.

Upselling

- **URL für 'Kaufen'**. Diese Seite wird geöffnet, wenn ein Benutzer auf **Jetzt kaufen** klickt, um auf eine erweiterte Edition von Cyber Protection Service upzugraden. Weitere Informationen über Upselling-Szenarien finden Sie im Abschnitt 'Upselling-Szenarien für Ihre Kunden konfigurieren'.

Mobile Apps

- **App Store**. Diese Seite wird geöffnet, wenn der Benutzer im **Cyber Protection** Service auf **Hinzufügen** –> **iOS** klickt.
- **Google Play Store**. Diese Seite wird geöffnet, wenn der Benutzer im **Cyber Protection** Service auf **Hinzufügen** –> **Android** klickt.

Einstellungen für E-Mail-Server

Sie können einen benutzerdefinierten E-Mail-Server spezifizieren, der verwendet wird, um E-Mail-Benachrichtigungen vom Management-Portal und den Services zu versenden. Wenn Sie einen benutzerdefinierten E-Mail-Server spezifizieren wollen, klicken Sie auf **Anpassen** und spezifizieren Sie dann folgende Einstellungen:

- Geben Sie bei **Von** den Namen ein, der bei den E-Mail-Nachrichten im Feld **Von** angezeigt werden soll.
- Geben Sie bei **SMTP** den Namen des Postausgangsservers (SMTP) ein.
- Geben Sie bei **Port** die Port-Adresse des Postausgangsservers ein. Standardmäßig ist der Port 25 festgelegt.
- Bestimmen Sie bei **Verschlüsselung**, ob eine SSL- oder TSL-Verschlüsselung verwendet werden soll. Wählen Sie **Ohne**, um die Verschlüsselung zu deaktivieren.
- Spezifizieren Sie bei **Benutzername** und **Kennwort** die Anmeldedaten eines Kontos, welches zum Versenden der Nachrichten verwendet werden soll.

Branding konfigurieren

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, bei dem Sie das Branding konfigurieren wollen.
3. Klicken Sie auf **Einstellungen** –> **Branding**.
4. [Wenn das Branding noch nicht aktiviert wurde] Klicken Sie auf **Branding aktivieren**.
5. Konfigurieren Sie die oben beschriebenen Branding-Elemente.

Die Standardeinstellungen für das Branding wiederherstellen

Sie können alle Branding-Elemente auf ihre Standardwerte zurücksetzen.

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, bei dem Sie das Branding zurücksetzen wollen.
3. Klicken Sie auf **Einstellungen** –> **Branding**.
4. Klicken Sie im oberen rechten Fensterbereich auf **Auf Standard zurücksetzen**.

Das Branding deaktivieren

Sie können das Branding für Ihr Konto und alle Untermandanten deaktivieren.

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, bei dem Sie das Branding deaktivieren wollen.
3. Klicken Sie auf **Einstellungen** –> **Branding**.
4. Klicken Sie im oberen rechten Fensterbereich auf **Branding deaktivieren**.

White-Labeling

Sie können bestimmen, ob der Cyber Protection Agent (für Windows, macOS und Linux), der Cyber Protection Monitor (für Windows, macOS und Linux) und der Connect Client für all Ihre Partner und Kunden per Branding oder White-Labeling angepasst wird. Wenn Sie das White-Labeling aktivieren, wird der Agent, der Connect Client und der Tray Monitor ohne Markenkennzeichnung angezeigt. Diese Einstellung beeinflusst außerdem die Namen und Logos, die im Installer und Cyber Protection Monitor verwendet werden.

White-Labeling anwenden

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, bei dem Sie das White-Labeling konfigurieren wollen.
3. Klicken Sie auf **Einstellungen** –> **Branding**.
4. Klicken Sie im oberen Fenster-Bereich auf **White-Labeling**, um alle Branding-Elemente zu löschen – mit Ausnahme von **Service-Name**, **URL der EULA**, **Management-Portal-Administrator-Anleitung**, **Management-Portal-Administrator-Hilfe** und **Einstellungen für E-Mail-Server**.

Eine benutzerdefinierte URL für die Weboberfläche konfigurieren

Hinweis
Eine benutzerdefinierte URL verweist auf eine andere IP-Adresse als die Standard-URL. Beachten Sie dies, wenn Sie Firewall-Richtlinien konfigurieren.

So können Sie die Weboberflächen-URL für die Cyber Protect Cloud Services konfigurieren

1. Klicken Sie im Management-Portal auf **Einstellungen** –> **Branding**.
2. Gehen Sie folgendermaßen im Bereich **URL für Cyber Protect Cloud Services** vor:
   - Klicken Sie auf **Konfigurieren**, wenn Sie zum ersten Mal eine benutzerdefinierte URL festlegen wollen.
   - Klicken Sie auf **Rekonfigurieren**, wenn Sie eine bereits vorhandene benutzerdefinierte URL ändern wollen.
3. Bereiten Sie im Schritt **Domain-Einstellungen** Ihre Domain und den CNAME-Eintrag vor.

   Wenn Sie eine benutzerdefinierte URL verwenden wollen, müssen Sie über einen aktiven Domain-Namen und einen CNAME-Eintrag verfügen, der so konfiguriert ist, dass er auf das Datacenter verweist, wo sich Ihr Konto befindet. Die Konfiguration des CNAME-Eintrags wird von Ihrer DNS-Registrierungsstelle vorgenommen und es kann bis zu 48 Stunden dauern, bis der Eintrag sich verbreitet hat.

Wie Sie den Domain-Namen Ihres Datacenters ermitteln und die Konfiguration Ihres CNAME-Eintrags anfordern können, erfahren Sie im Artikel 'Branding der Webkonsolen-URL (58275).

4. Vergewissern Sie sich im Schritt **Überprüfen Sie Ihre URL**, dass Ihre benutzerdefinierte URL zugänglich ist und dass Ihr CNAME-Eintrag korrekt konfiguriert ist. Geben Sie dafür den Namen der Haupt-URL ein und klicken Sie auf **Überprüfen**. Wenn Sie ein SSL-Wildcard-Zertifikat (auch SSL-Platzhalter-Zertifikat genannt) verwenden, können Sie bis zu zehn alternative Domain-Namen hinzufügen. Wenn Sie ein 'Let's Encrypt'-Zertifikat verwenden, werden alternative Domain-Namen ignoriert.
5. Sie können im Schritt **SSL-Zertifikat** eine der folgenden Aktionen ausführen:
   - Erstellen Sie ein 'Let's Encrypt'-Zertifikat. KlickenSie dafür auf **Kostenloses SSL-Zertifikat mit 'Let's Encrypt'**. Diese Option verwendet 'Let's Encrypt'-Zertifikate, das von einer Drittanbieter-Entität ausgestellt wurde. Der Service-Provider übernimmt keine Haftung für Probleme, die sich aus der Verwendung dieser kostenlosen Zertifikate ergeben. Weitere Informationen zu den 'Let's Encrypt'-Bedingungen finden Sie unter https://letsencrypt.org/repository/.
   - Laden Sie Ihr Wildcard-Zertifikat (auch Platzhalter-Zertifikat genannt) hoch. Klicken Sie dafür auf **Wildcard-Zertifikat hochladen** und geben Sie dann ein Wildcard-Zertifikat und einen privaten Schlüssel an.

     Hinweis
     Es kann ein Fehler bei der Zertifikatsvalidierung mit folgender Fehlermeldung auftreten: "Das Zertifikat konnte nicht verifiziert werden: x509: Das Zertifikat wurde von einer unbekannten Zertifizierungsstelle signiert". Das bedeutet normalerweise, dass einige Zwischenzertifikate fehlen. Verwenden Sie einen Zertifikatsketten-Resolver, um die Struktur Ihres Zertifikats zu reparieren und die vollständige Zertifikatskette hochzuladen.
6. Klicken Sie auf **Übermitteln**, um die Änderungen zu übernehmen.

So können Sie die benutzerdefinierte URL auf Standard zurücksetzen

1. Klicken Sie im Management-Portal auf **Einstellungen** –> **Branding**.
2. Klicken Sie im Bereich **URL für Acronis Cyber Protect Cloud Services** auf den Befehl **Auf Standard zurücksetzen**, um die Standard-URL (https://cloud.acronis.com) zu verwenden.

Monitoring

Klicken Sie auf **Monitoring**, wenn Sie Informationen über die Service-Nutzung und durchgeführte Aktionen erhalten wollen.

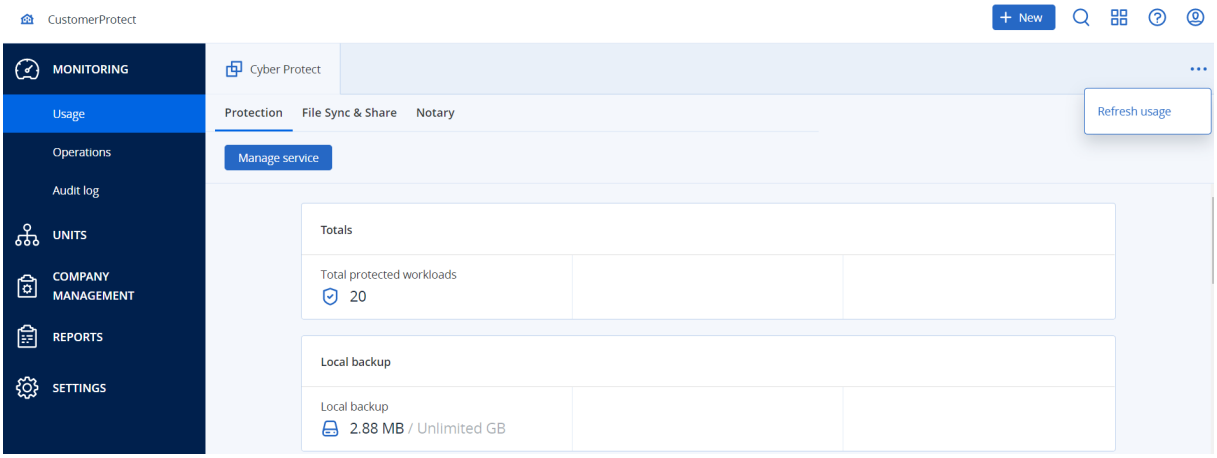
Nutzung

Die Registerkarte **Nutzung** ermöglicht Ihnen einen Überblick über die Service-Nutzung und auf die Services zuzugreifen, die für den Mandanten, in dem Sie arbeiten, verfügbar sind.

Die Nutzungsdaten umfassen sowohl Standard- als auch Advanced-Funktionen.

Wenn Sie die auf der Registerkarte angezeigten Nutzungsdaten aktualisieren wollen, klicken Sie im oberen rechten Teil des Bildschirms auf das Drei-Punkte-Symbol und wählen Sie **Nutzung aktualisieren**.

Hinweis
Das Abrufen der Daten kann bis zu 10 Minuten dauern. Laden Sie die Seite neu, damit die aktualisierten Daten angezeigt werden.



Aktionen

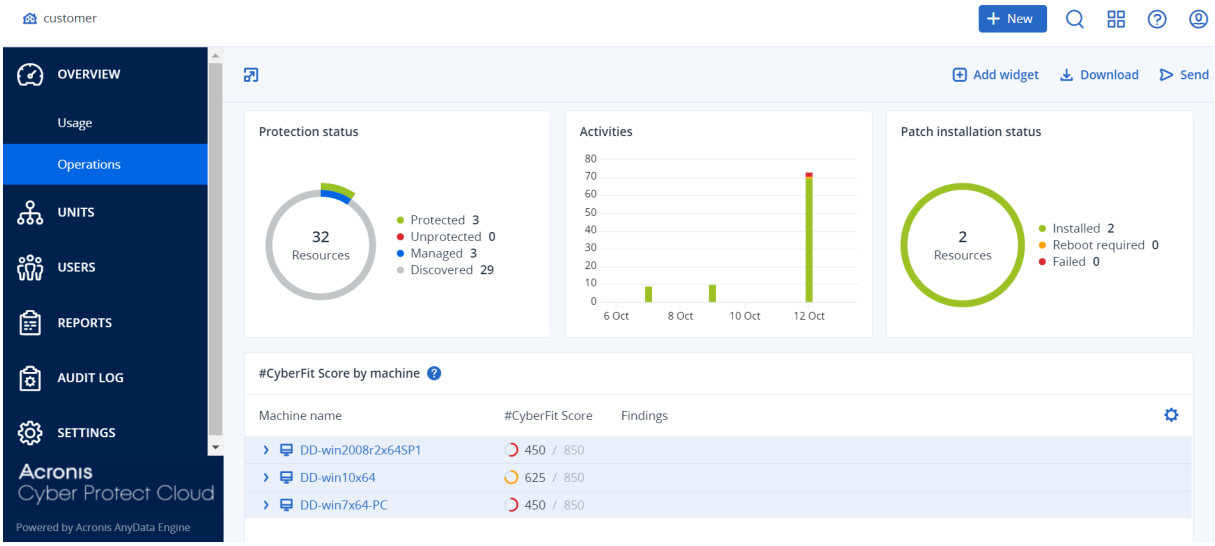
Das Dashboard **Aktionen** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Aktionen geben, die im Zusammenhang mit dem Cyber Protection Service stehen. Widgets für andere Services werden in zukünftigen Versionen verfügbar sein.

Standardmäßig werden die Daten für den Mandanten angezeigt, in dem Sie arbeiten. Sie können den angezeigten Mandanten für jedes Widget einzeln ändern, indem Sie dieses bearbeiten. Zusätzlich werden zusammengefasste Informationen über die direkt untergeordneten Kunden-Mandanten des aktuell ausgewählten Mandanten angezeigt, einschließlich solcher, die sich in Ordnern befinden. Das Dashboard zeigt *keine* Informationen über untergeordnete Partner und deren untergeordnete Mandanten an. Sie müssen zum jeweiligen Partner herunter blättern, um dessen Dashboard zu sehen. Wenn Sie jedoch einen untergeordneten Partner-Mandanten in einem Ordner-Mandanten konvertieren, werden die Informationen über die untergeordneten Kunden dieses Mandanten im Dashboard des übergeordneten Mandanten angezeigt.

Die Widgets werden alle zwei Minuten aktualisiert. Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Sie können den aktuellen Zustand des Dashboards in Form einer .pdf- und/oder .xlsx-Datei herunterladen oder als E-Mail an eine beliebige Adresse versenden (auch an externe Empfänger).

Sie können aus einer Vielzahl von Widgets wählen, die als Tabellen, Kreis- und Balkendiagramme, Listen und Treemaps (Kacheldiagramm mit Baumstruktur) angezeigt werden. Sie können mehrere Widgets desselben Typs für verschiedene Mandanten oder mit unterschiedlichen Filtern

hinzufügen.



So können Sie die Widgets auf dem Dashboard neu anordnen

Verschieben Sie die Widgets per Drag & Drop-Aktion, indem Sie zuvor auf deren Namen klicken.

So können Sie ein Widget bearbeiten

Klicken Sie neben dem Widget-Namen auf das Stiftsymbol. Mit der Funktion 'Bearbeiten' können Sie ein Widget umbenennen, den Zeitbereich ändern, Filter festlegen und den Mandanten auswählen, für den die Daten angezeigt werden.

So können Sie ein Widget hinzufügen

Klicken Sie auf **Widget hinzufügen** und gehen Sie dann nach einer der folgenden Möglichkeiten vor:

- Klicken Sie auf das hinzuzufügende Widget. Das Widget wird daraufhin mit den Standardeinstellungen hinzugefügt.
- Wenn Sie das Widgeht vor dem Hinzufügen bearbeiten wollen, dann klicken Sie nach der Auswahl des Widgets auf das Zahnradsymbol. Klicken Sie, nachdem Sie das Widget bearbeitet haben, auf **Fertig**.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

Schutzstatus

Schutzstatus

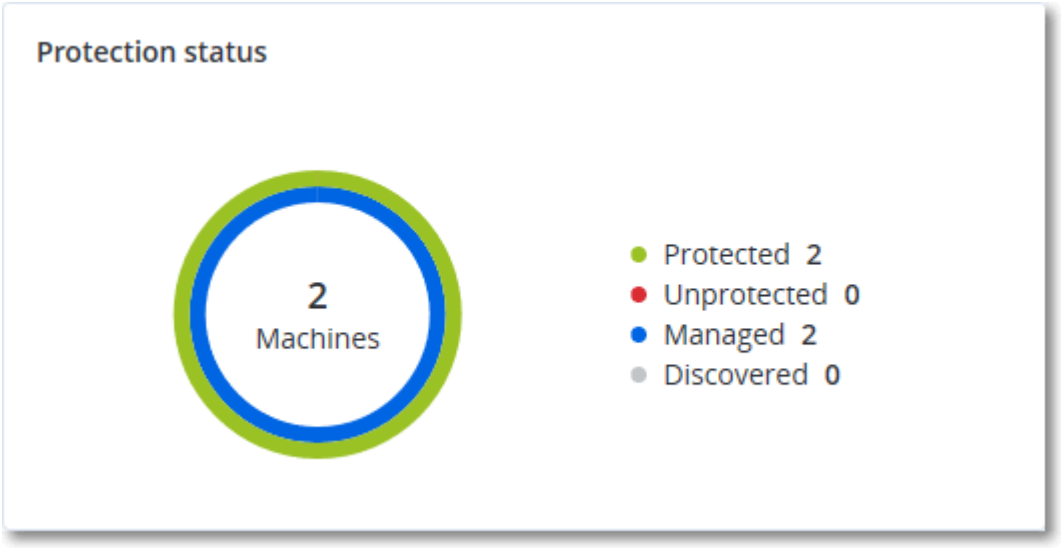
Schutzstatus

Dieses Widget zeigt den aktuellen Sicherungsstatus für alle Maschinen an.

Eine Maschine kann sich in einem der folgenden Statuszustände befinden:

- **Geschützt** – Maschinen, auf die ein Schutzplan angewendet wurde.
- **Ungeschützt** – Maschinen, auf die noch kein Schutzplan angewendet wurde. Dazu gehören sowohl erkannte als auch verwaltete Maschinen, auf die noch kein Schutzplan angewendet wurde.
- **Verwaltet** – Maschinen, auf denen ein Protection Agent installiert ist.
- **Erkannt** – Maschinen, auf denen kein Protection Agent installiert ist.

Wenn Sie auf den Maschinenstatus klicken, werden Sie zu der Liste der Maschinen mit diesem Status weitergeleitet, um weitere Details zu erhalten.



Erkannte Maschinen

Dieses Widget zeigt die Liste der erkannten Maschinen während eines spezifizierten Zeitraums an.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

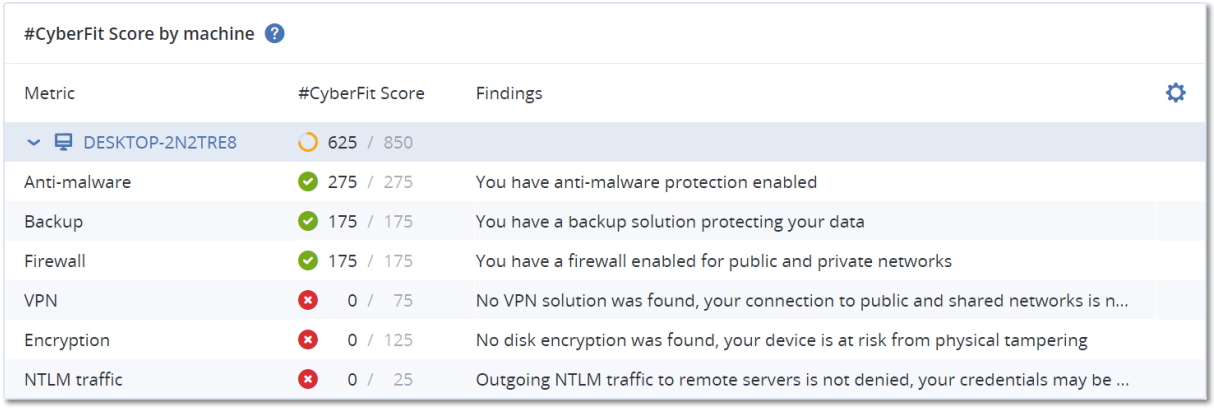
#CyberFit-Score pro Maschine

Dieses Widget zeigt für jede Maschine den #CyberFit-Gesamt-Score und die Einzel-Scores an, aus denen sich dieser Gesamtwert zusammensetzt – sowie die Ergebnisse für jede der bewerteten Metriken:

- Antimalware
- Backup
- Firewall
- VPN
- Verschlüsselung
- NTLM-Traffic

Wenn Sie den Score einer einzelnen Metrik verbessern wollen, können Sie die Empfehlungen einsehen, die in Form eines Berichts verfügbar sind.

Weitere Informationen über den #CyberFit-Score finden Sie im Abschnitt '#CyberFit-Score für Maschinen'.



Endpoint Detection & Response (EDR)-Widgets

Wichtig
Dies ist eine Early Access-Version der EDR-Dokumentation. Einige der Funktionen und Beschreibungen können daher noch unvollständig sein.

Die Endpoint Detection & Response (EDR)-Funktionalität umfasst eine Reihe von Widgets, auf die über das Dashboard **Aktionen** zugegriffen werden kann.

Folgende Widgets sind verfügbar:

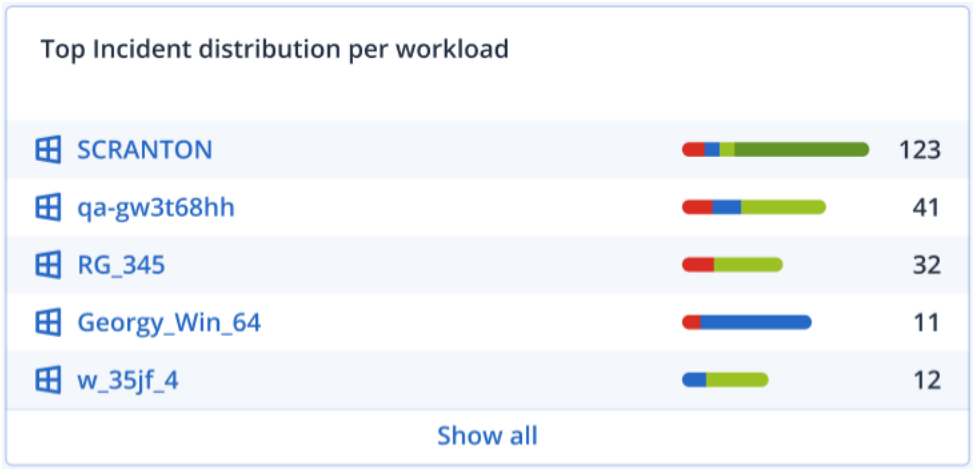
- Spitzenverteilung der Vorfälle pro Workload
- MTTR (Mittlere Problemlösungszeit) für Vorfälle

- Sicherheitsvorfall-Burndown
- Workload-Netzwerkstatus

Spitzenverteilung der Vorfälle pro Workload

Dieses Widget zeigt die fünf Workloads mit den meisten Vorfällen an (klicken Sie auf **Alle anzeigen**, um zur Vorfallsliste zu gelangen, die entsprechend den Widget-Einstellungen gefiltert wird).

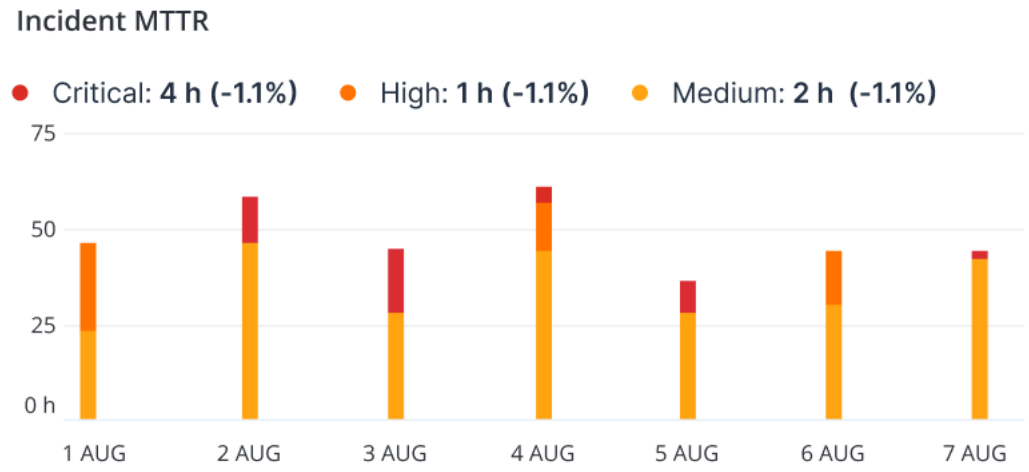
Bewegen Sie den Mauszeiger über eine Workload-Zeile, um eine Aufschlüsselung des aktuellen Untersuchungsstadiums für die Vorfälle angezeigt zu bekommen; die Untersuchungsstadien sind **Nicht gestartet**, **Wird untersucht**, **Geschlossen** und **Falsch positiv**. Klicken Sie anschließend auf einen Workload, den Sie weiter analysieren wollen, und wählen Sie den entsprechenden Kunden im angezeigten Pop-up-Fenster aus. Die Vorfallsliste wird entsprechend den Einstellungen des Widgets aktualisiert.



MTTR (Mittlere Problemlösungszeit) für Vorfälle

Dieses Widget zeigt die durchschnittliche Problemlösungszeit für Sicherheitsvorfälle an. Sie gibt an, wie schnell Vorfälle untersucht und gelöst werden.

Klicken Sie auf eine Spalte, um die Vorfälle nach ihrem Schweregrad (**Kritisch**, **Hoch** und **Mittel**) aufzuschlüsseln und zu sehen, wie lange es dauerte, die verschiedenen Schweregrade zu beheben. Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.

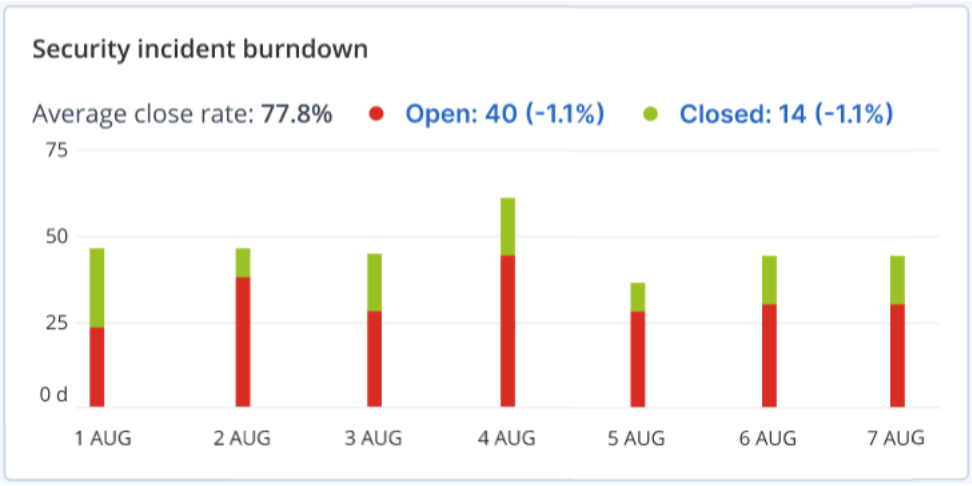


Sicherheitsvorfall-Burndown

Dieses Widget zeigt die Effizienzrate bei der Schließung von Vorfällen an; die Anzahl der offenen Vorfälle wird dabei mit der Anzahl der geschlossenen Vorfälle über einen bestimmten Zeitraum abgeglichen.

Bewegen Sie den Mauszeiger über eine Spalte, um eine Aufschlüsselung der geschlossenen und offenen Vorfälle für den jeweiligen Tag angezeigt zu bekommen. Wenn Sie auf das Element 'Öffnen' klicken, wird ein Pop-up-Fenster angezeigt, in dem Sie den entsprechenden Mandanten auswählen können. Daraufhin wird die gefilterte Vorfallsliste für den betreffenden Mandanten aufgerufen, um die derzeit offenen Vorfälle anzuzeigen (die das Stadium **Wird untersucht** oder **Nicht gestartet** haben). Wenn Sie auf das Element "Geschlossen" klicken, wird die Vorfallsliste für den betreffenden Mandanten angezeigt und so gefiltert, dass nur noch die Vorfälle angezeigt werden, die nicht mehr offen sind (die also das Stadium **Geschlossen** oder **Falsch positiv** haben).

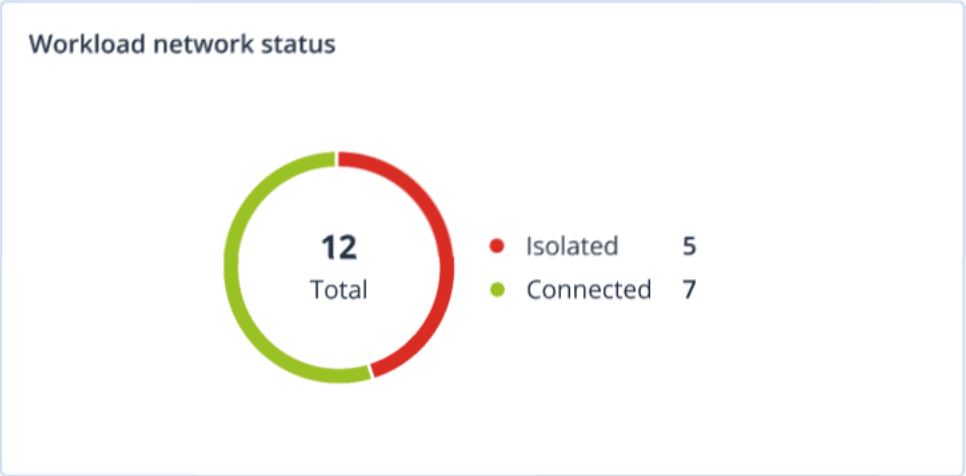
Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.



Workload-Netzwerkstatus

Dieses Widget zeigt den aktuellen Netzwerkstatus für Ihre Workloads an und informiert darüber, wie viele Workloads isoliert und wie viele verbunden sind.

Wenn Sie auf das Element 'Isoliert' klicken, wird ein Pop-up-Fenster angezeigt, in dem Sie den entsprechenden Mandanten auswählen können. Die dargestellte Workload-Ansicht wird gefiltert, sodass nur noch die isolierten Workloads angezeigt werden. Wenn Sie auf das Element 'Verbunden' klicken, wird die Liste 'Workload mit Agenten' angezeigt, die so gefiltert ist, dass die verbundenen Workloads (für den ausgewählten Mandanten) angezeigt werden.



Überwachung der Laufwerksintegrität

Die Überwachung der Laufwerksintegrität liefert Informationen über den aktuellen Laufwerksintegritätsstatus sowie eine Vorhersage über diesen. Dadurch können Sie Datenverluste vorab verhindern, die durch einen Laufwerksausfall verursacht werden könnten. Es werden sowohl Laufwerke vom Typ HDD (klassische Festplatten) als auch SSD (Flash-Speicher basierte Laufwerke) unterstützt.

Einschränkungen

- Die Vorhersage zur Laufwerksintegrität wird nur für Maschinen unterstützt, die unter Windows laufen.
- Es können nur Laufwerke von physischen Maschinen überwacht werden. Die Laufwerke von virtuellen Maschinen können nicht überwacht werden und werden daher auch nicht in den Laufwerksintegrität-Widgets angezeigt.
- RAID-Konfigurationen werden nicht unterstützt. Die Laufwerksintegrität-Widgets enthalten keine Informationen über Maschinen mit RAID-Implementierung.
- NVMe-SSDs werden nicht unterstützt.

Die Laufwerksintegrität wird durch folgende Statuszustände dargestellt:

- **OK**
  Die Laufwerksintegrität liegt zwischen 70% und 100%.

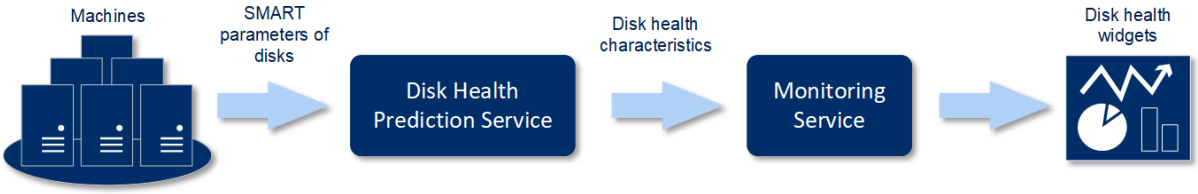
- **Warnung**
  Die Laufwerksintegrität liegt zwischen 30% und 70%.
- **Kritisch**
  Die Laufwerksintegrität liegt zwischen 0% und 30%.
- **Laufwerksdaten werden berechnet**
  Der aktuelle Laufwerksstatus und die Vorhersage werden ermittelt.

Und so funktioniert es

Der Disk Health Prediction Service verwendet ein auf künstlicher Intelligenz (KI) basierendes Vorhersagemodell.

1. Der Protection Agent sammelt die SMART-Parameter der Laufwerke und übermittelt diese Daten an den Disk Health Prediction Service:
   - SMART 5 – Reallocated Sectors Count (Anzahl neu zugewiesener Sektoren).
   - SMART 9 – Power-On Hours (Einschaltzeit).
   - SMART 187 – Reported Uncorrectable Errors (Gemeldete unkorrigierbare Fehler).
   - SMART 188 – Command Timeout (Befehls-Timeout, wegen Zeitüberschreitung abgebrochene Befehle).
   - SMART 197 – Current Pending Sector Count (Anzahl derzeit ausstehender Sektoren).
   - SMART 198 – Offline Uncorrectable Sector Count (Anzahl nicht korrigierbarer Sektoren).
   - SMART 200 – Write Error Rate (Fehlerrate beim Schreiben).
2. Der Disk Health Prediction Service verarbeitet die empfangenen SMART-Parameter, trifft Vorhersagen und stellt dann folgende Laufwerksintegritätsmerkmale bereit:
   - Aktueller Laufwerksintegritätsstatus: OK, Warnung, Kritisch.
   - Vorhersage zur Laufwerksintegrität: negativ, stabil, positiv.
   - Vorhersage-Wahrscheinlichkeit der Laufwerksintegrität in Prozent.

   Der Vorhersagezeitraum beträgt ein Monat.
3. Der Monitoring Service empfängt diese Merkmale und zeigt die entsprechenden Informationen dann in den Laufwerksintegrität-Widgets der Cyber Protect-Konsole an.



Laufwerksintegrität-Widgets

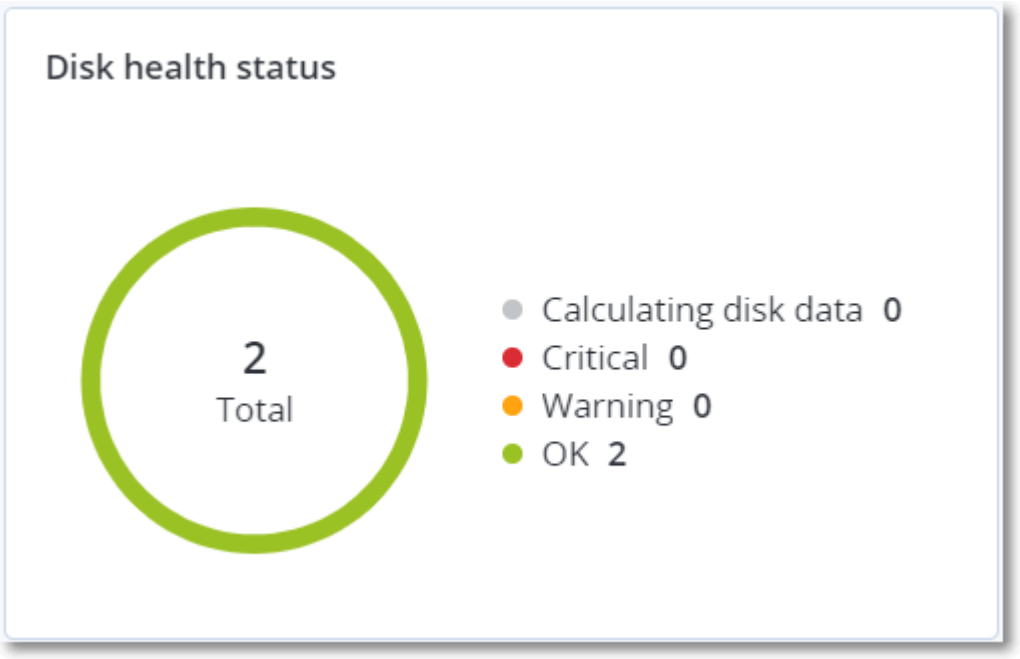
Die Ergebnisse der Laufwerksintegritätsüberwachung werden in folgenden Widgets dargestellt, die in der Cyber Protect-Konsole verfügbar sind.

- **Überblick der Laufwerksintegrität** ist ein Treemap-Widget (Kacheldiagramm mit Baumstruktur) mit zwei Detailebenen, zwischen denen umgeschaltet werden kann.
  - Maschinenebene
    Zeigt zusammengefasste Informationen über den Laufwerksintegritätsstatus für die ausgewählten Kundenmaschinen an. Es werden nur die kritischsten Laufwerkstatuszustände angezeigt. Die anderen Statuszustände werden in einem Tooltip angezeigt, wenn Sie mit dem Mauszeiger über einen bestimmten Block fahren. Die Blockgröße der Maschine hängt von der Gesamtgröße aller Laufwerke dieser Maschine ab. Die Blockfarbe der Maschine hängt vom kritischsten Laufwerksstatus ab, der gefunden wurde.

  - Laufwerksebene
    Zeigt den aktuellen Laufwerksintegritätsstatus aller Laufwerke für die ausgewählte Maschine an. Jeder Laufwerksblock zeigt eine der nachfolgenden Vorhersagen zur Laufwerksintegrität sowie die dazugehörige Wahrscheinlichkeit (in Prozent) an:
    - Wird heruntergestuft
    - Wird stabil bleiben

- Wird verbessert

- **Laufwerksintegritätsstatus** ist ein Kreisdiagramm-Widget, welches die Anzahl der Laufwerke für jeden Status anzeigt.



Alarmmeldungen zum Laufwerksintegritätsstatus

Die Laufwerksintegritätsprüfung wird alle 30 Minuten durchgeführt, während die entsprechende Alarmmeldung nur einmal täglich generiert wird. Wenn sich der Laufwerksintegritätsstatus von **Warnung** zu **Kritisch** ändert, wird immer ein Alarm generiert.

Alarmbezeichnung	Schweregrad	Laufwerksintegritätsstatus	Beschreibung
Laufwerksausfall ist möglich	Warnung	(30 – 70)	Das Laufwerk <Laufwerksname> auf dieser Maschine wird wahrscheinlich demnächst ausfallen. Sichern Sie das Laufwerk möglichst bald mit einem vollständigen Image-Backup. Bauen Sie dann ein Ersatzlaufwerk ein und stellen Sie das Image auf diesem wieder her.
Laufwerksausfall steht unmittelbar bevor	Kritisch	(0 – 30)	Das Laufwerk <Laufwerksname> auf dieser Maschine befindet sich in einem kritischen Zustand und wird höchstwahrscheinlich sehr bald ausfallen. Wir raten davon ab, jetzt noch ein Image-Backup des Laufwerks zu erstellen, da die zusätzliche Belastung zum endgültigen Laufwerksausfall führen könnte. Versuchen Sie, die wichtigsten Dateien auf dem Laufwerk umgehend zu sichern und es dann auszutauschen.

Data Protection-Karte

Die Funktion 'Data Protection-Karte' ermöglicht es Ihnen, alle für Sie wichtigen Daten zu untersuchen sowie ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller wichtigen Dateien in Form einer skalierbaren Treemap-Anzeige (Kacheldiagramm mit Baumstruktur) zu erhalten.

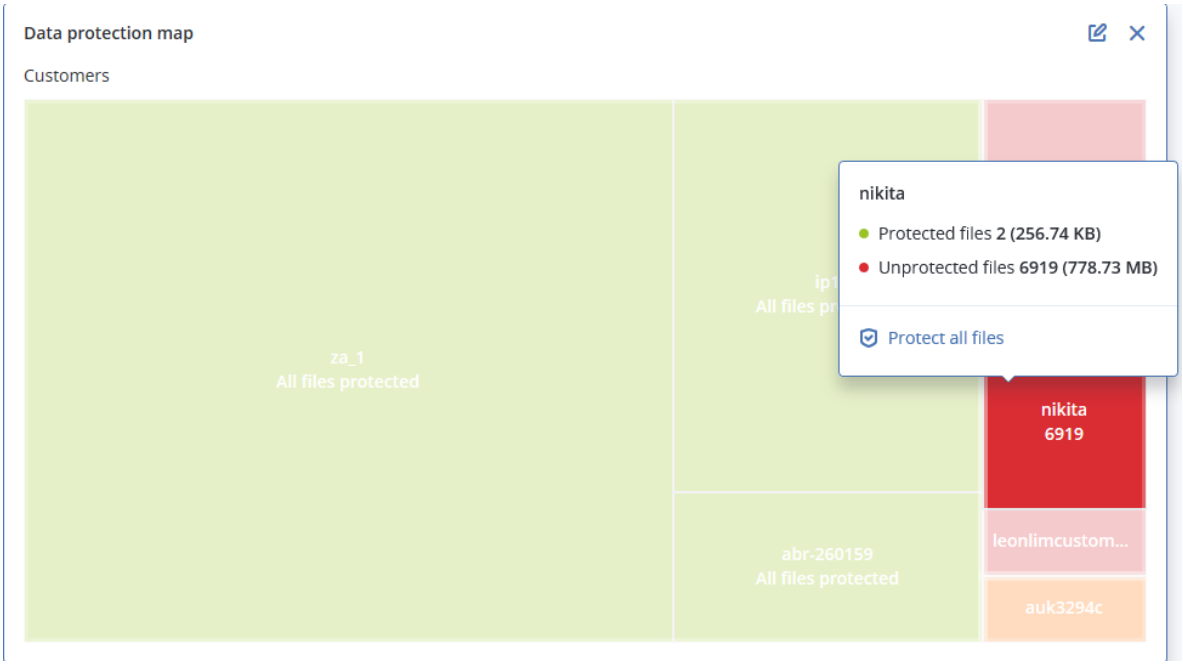
Jede Blockgröße hängt von der Gesamtzahl/Größe aller wichtigen Dateien ab, die zu einem Kunden/einer Maschine gehören.

Dateien können einen der folgenden Schutzstatus-Zustände haben:

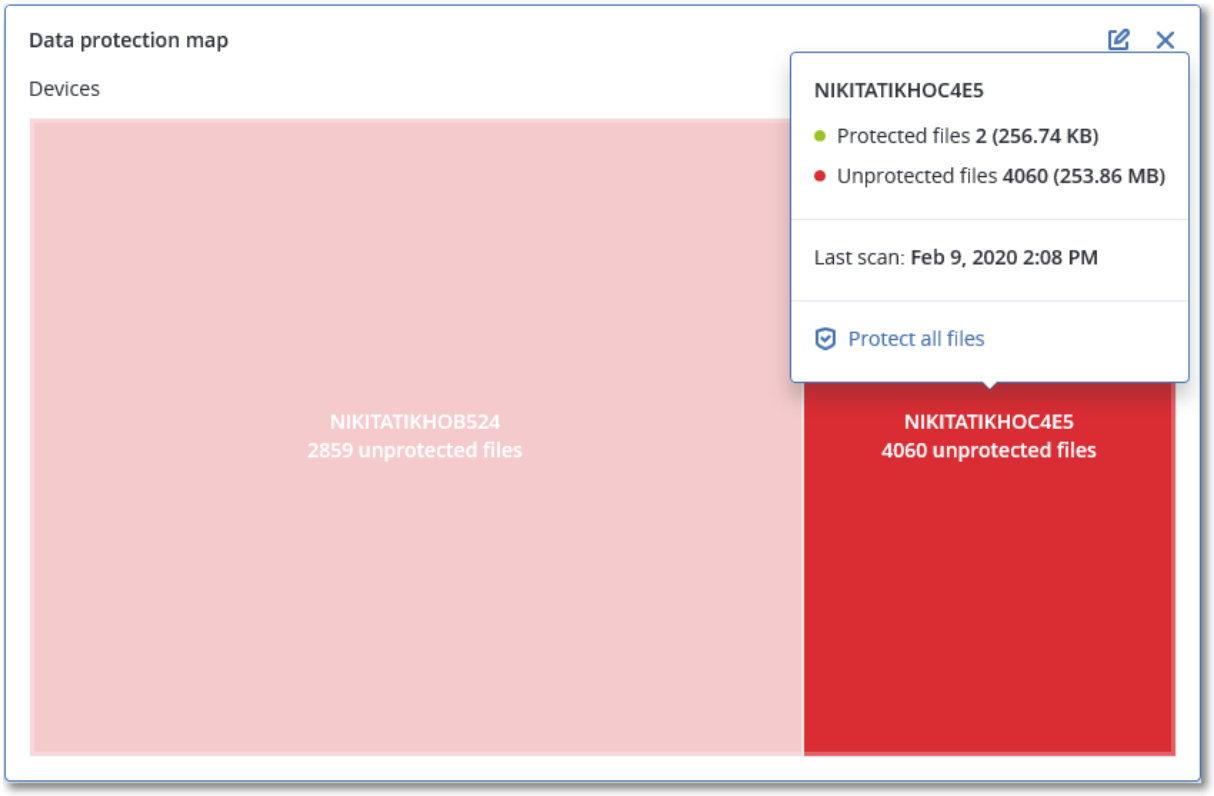
- **Kritisch** – es gibt 51-100% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für den/die ausgewählte(n) Kunden-Mandanten/Maschine/Speicherort nicht per Backup gesichert wurden.
- **Niedrig** – es gibt 21-50% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für den/die ausgewählte(n) Kunden-Mandanten/Maschine/Speicherort nicht per Backup gesichert wurden.
- **Mittel** – es gibt 1-20% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für den/die ausgewählte(n) Kunden-Mandanten/Maschine/Speicherort nicht per Backup gesichert wurden.
- **Hoch** – alle Dateien mit den von Ihnen spezifizierten Erweiterungen wurden für den/die ausgewählte(n) Kunden-Mandanten/Maschine/Speicherort per Backup gesichert.

Alle Ergebnisse der Data Protection-Untersuchtung können auf dem Dashboard im Data Protection-Karten-Widget gefunden werden – einem Treemap-Widget mit zwei umschalt- bzw. aufklappbaren Detailebenen:

- Kunden-Mandanten-Ebene – zeigt zusammengefasste Informationen über den Schutzstatus wichtiger Dateien für jeden Kunden an, den Sie ausgewählt haben.



- Maschinenebene – zeigt Informationen über den Schutzstatus wichtiger Dateien für die Maschinen des ausgewählten Kundens an.



Wenn Sie bisher noch ungesicherte Dateien schützen wollen, müssen Sie mit dem Mauszeiger über den Block fahren und dann auf den Befehl **Alle Dateien schützen** klicken. Im Dialogfenster finden Sie Informationen zur Anzahl der ungeschützten Dateien und zu deren Speicherort. Wenn Sie diese sichern wollen, klicken Sie auf **Alle Dateien schützen**.

Sie können außerdem einen ausführlichen Bericht im CSV-Format herunterladen.

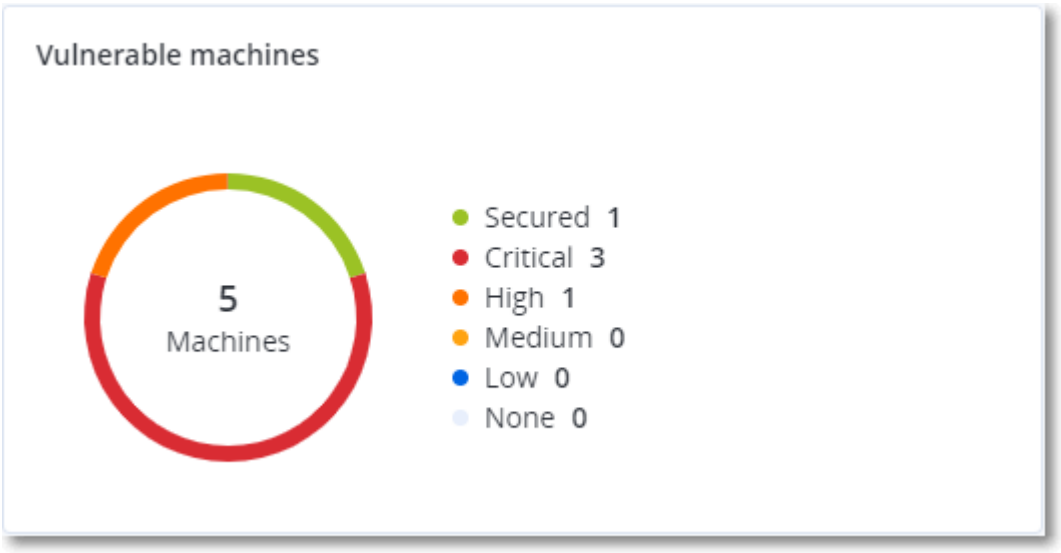
Widget für Schwachstellenbewertung

Verwundbare Maschinen

Dieses Widget zeigt die verwundbaren Maschinen nach dem Verwundbarkeitsgrad an.

Die gefundene Schwachstelle kann gemäß CVSS v3.0 (Common Vulnerability Scoring System) einen der folgenden Schweregrade haben:

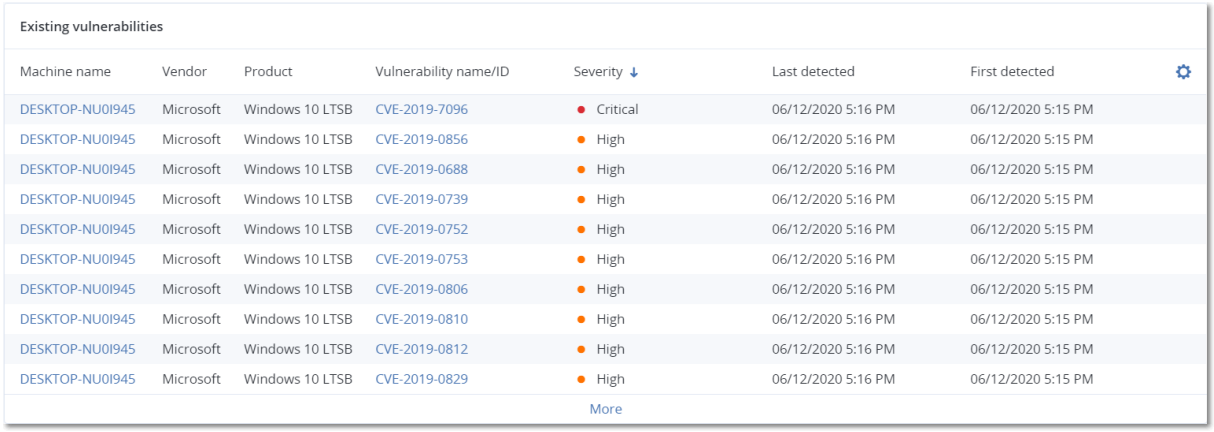
- Gesichert: es wurden keine Schwachstellen gefunden
- Kritisch: 9.0 - 10.0 CVSS
- Hoch: 7.0 - 8.9 CVSS
- Mittel: 4.0 - 6.9 CVSS
- Niedrig: 0.1 - 3.9 CVSS
- Ohne: 0.0 CVSS



Vorhandene Schwachstellen

Dieses Widget zeigt die derzeit vorhandenen Schwachstellen auf Maschinen an. Im Widget **Vorhandene Schwachstellen** gibt es zwei Spalten mit Zeitstempeln:

- **Zuerst erkannt** – Datum und Uhrzeit, als die Schwachstelle erstmals auf der Maschine erkannt wurde.
- **Zuletzt erkannt** – Datum und Uhrzeit, als die Schwachstelle das letzte Mal auf der Maschine erkannt wurde.



Widgets für Patch-Installation

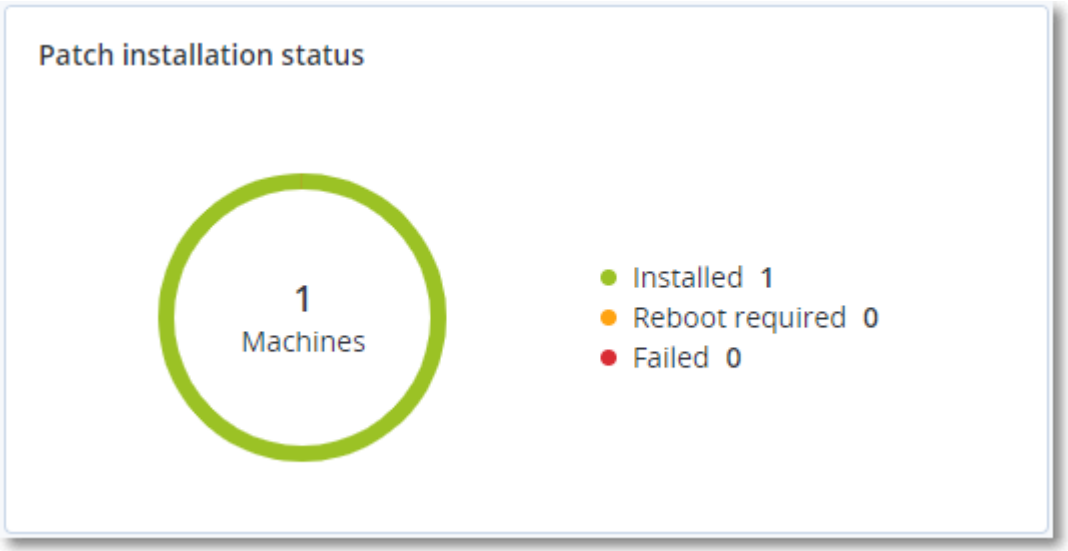
Es gibt vier Widgets im Zusammenhang mit der Patch-Verwaltungsfunktionalität.

Status der Patch-Installation

Dieses Widget zeigt die Anzahl der Maschinen gruppiert nach dem Status des Patch-Installation an.

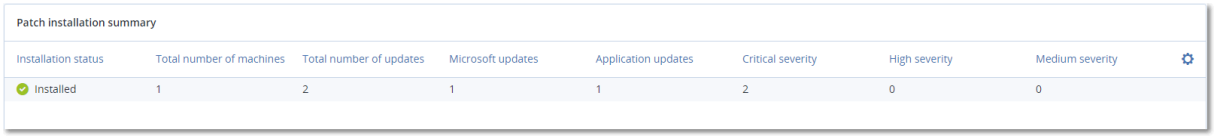
- **Installiert** – alle verfügbaren Patches sind auf einer Maschine installiert
- **Neustart erforderlich** – nach einer Patch-Installation muss eine Maschine neu gestartet werden

- **Fehlgeschlagen** – die Patch-Installation ist auf einer Maschine fehlgeschlagen



Übersicht der Patch-Installation

Dieses Widget zeigt eine Übersicht der Patches auf den Maschinen an, gruppiert nach dem Status des Patch-Installation.



Verlauf der Patch-Installation

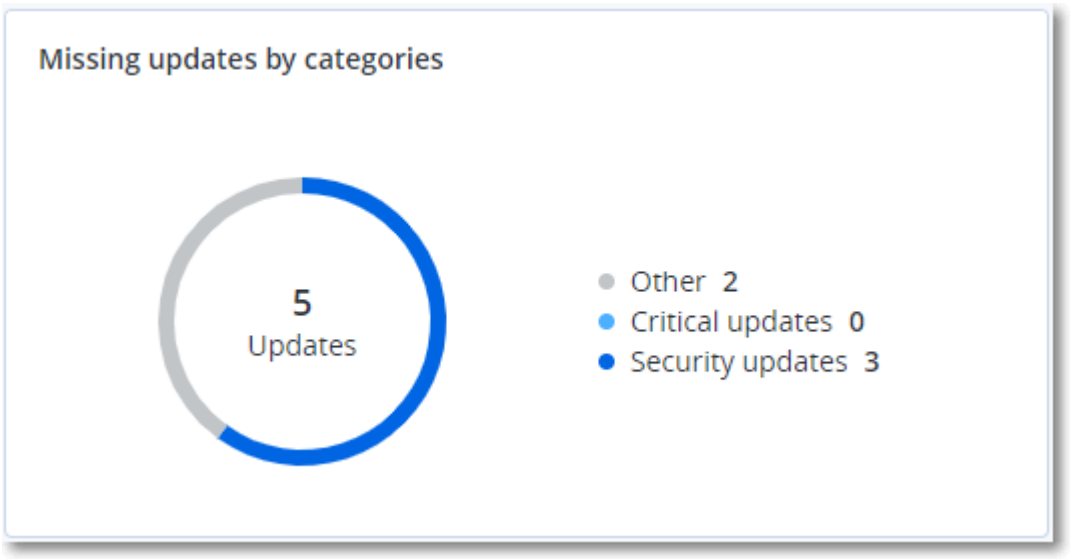
Dieses Widget zeigt ausführliche Informationen über die Patches auf den Maschinen an.

Fehlende Updates nach Kategorie

Dieses Widget zeigt die Anzahl der fehlenden Updates nach Kategorie an. Folgende Kategorien werden angezeigt:

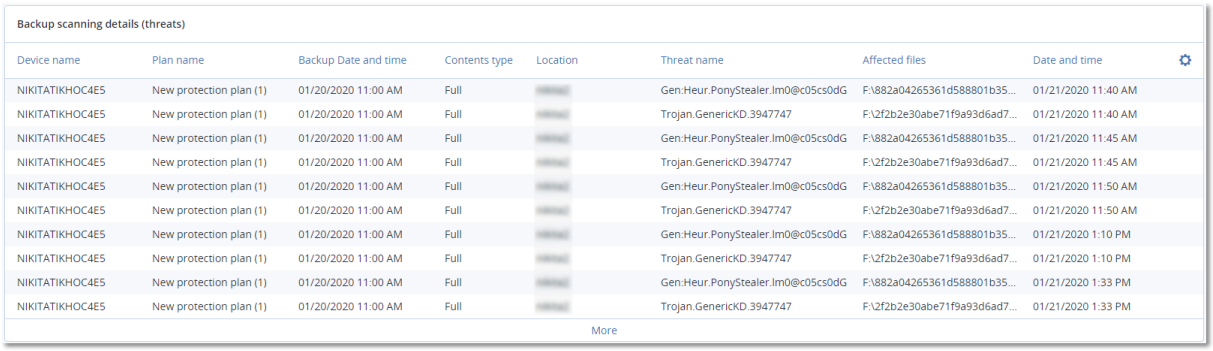
- Sicherheitsupdates
- Kritische Updates

- Anderer



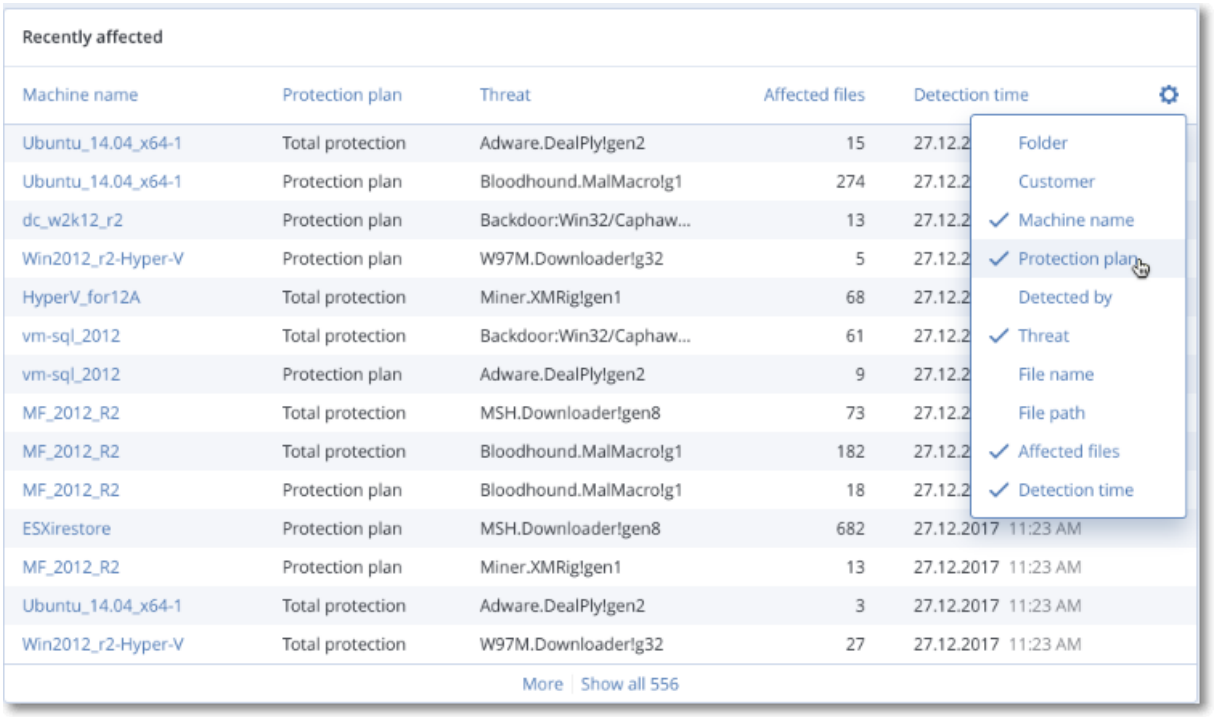
Backup-Scanning-Details

Dieses Widget zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.



Kürzlich betroffen

Dieses Widget zeigt detaillierte Informationen über Workloads an, die von Bedrohungen wie Viren, Malware und Ransomware betroffen waren. Sie können hier Informationen über die erkannten Bedrohungen, den Zeitpunkt der Erkennung sowie die Anzahl der betroffenen Dateien finden.



Daten für kürzlich betroffene Workloads herunterladen

Sie können die Daten für kürzlich betroffene Workloads herunterladen, eine CSV-Datei generieren und diese dann an die von Ihnen spezifizierten Empfänger senden.

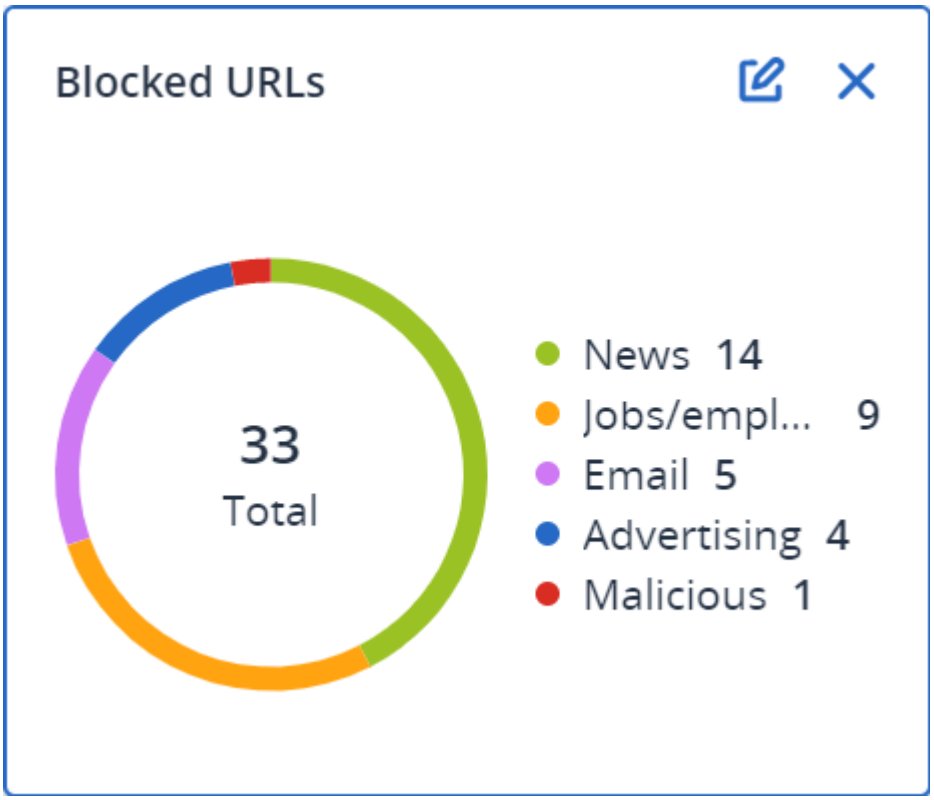
So laden Sie die Daten für kürzlich betroffene Workloads herunter

1. Klicken Sie im Widget **Kürzlich betroffen** auf den Befehl **Daten herunterladen**.
2. Geben Sie im Feld **Zeitraum** die Anzahl der Tage ein, für die Sie Daten herunterladen wollen. Die maximale Anzahl der Tage, die Sie eingeben können, beträgt 200.
3. Geben Sie im Feld **Empfänger** die E-Mail-Adressen aller Personen ein, die eine E-Mail mit einem Link zum Herunterladen der CSV-Datei erhalten sollen.
4. Klicken Sie auf **Download**.

   Das System beginnt dann damit, die CSV-Datei mit den Daten für diejenigen Workloads zu generieren, die in dem von Ihnen spezifizierten Zeitraum betroffen waren. Wenn die CSV-Datei vollständig ist, sendet das System eine E-Mail an die Empfänger. Jeder Empfänger kann dann diese CSV-Datei herunterladen.

Blockierte URLs

Das Widget zeigt die Statistiken der blockierten URLs nach Kategorie an. Weitere Informationen zum Filtern und Kategorisieren von URLs/Websites finden Sie in der Cyber Protection-Benutzeranleitung.



Widgets für Software-Inventarisierung

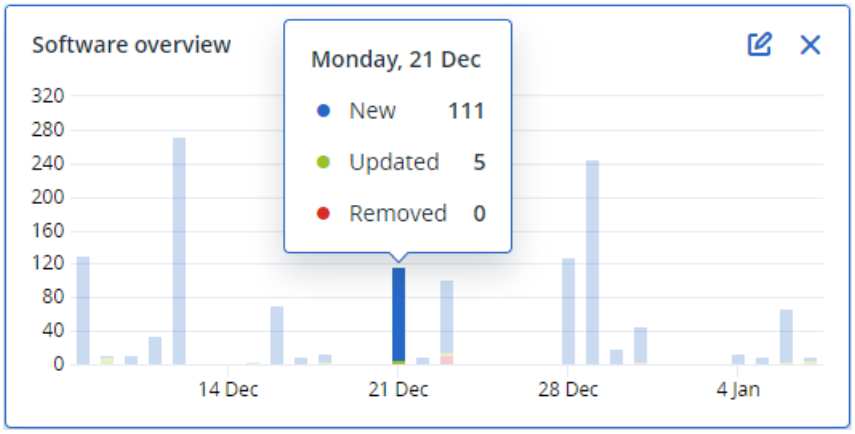
Das Tabellen-Widget **Software-Inventarisierung** zeigt ausführliche Informationen über die gesamte Software an, die auf den physischen Windows- und macOS-Geräten in den Unternehmen Ihrer Kunden installiert ist.

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+

Das Widget **Software-Überblick** X zeigt die Anzahl der neuen, aktualisierten oder gelöschten Applikationen auf Windows- und macOS-Maschinen in den Unternehmen Ihrer Kunden für einen spezifizierten Zeitraum (7 Tage, 30 Tage oder den aktuellen Monat) an.



Wenn Sie den Mauszeiger über einen bestimmten Balken im Diagramm halten, wird ein Tooltip mit folgenden Informationen angezeigt:

Neu – die Anzahl der neu installierten Applikationen.

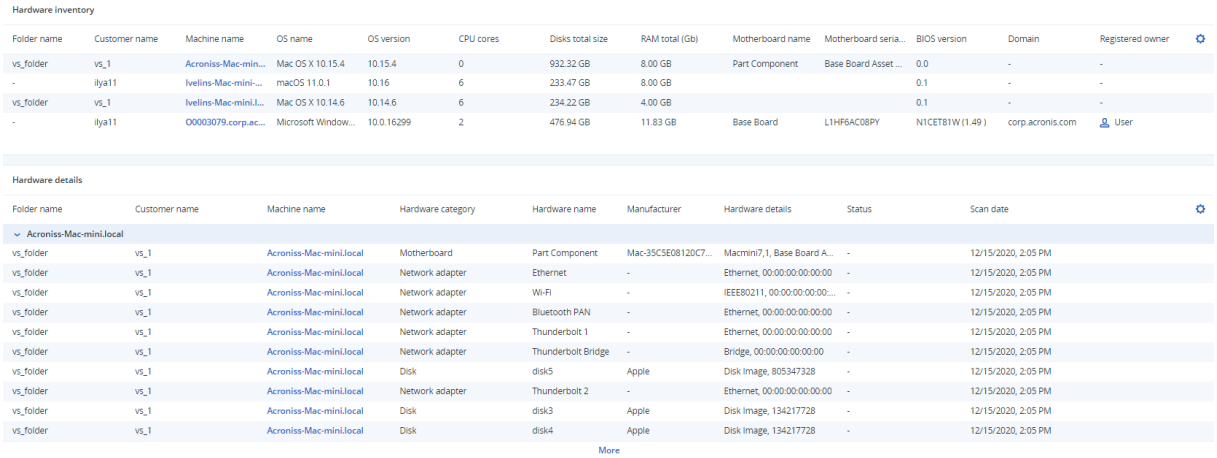
Aktualisiert – die Anzahl der aktualisierten Applikationen.

Entfernt – die Anzahl der entfernten Applikationen.

Wenn Sie auf den Balkenteil klicken, der einem bestimmten Statuszustand entspricht, wird ein Popup-Fenster geladen. Es werden alle Kunden aufgelistet, die Maschinen mit Applikationen im ausgewählten Status und zum ausgewählten Datum haben. Sie können einen Kunden aus der Liste auswählen und dann auf **Gehe zu 'Kunde'** klicken, woraufhin Sie zur Seite **Software-Verwaltung** –> **Software-Inventarisierung** in der Cyber Protect-Konsole des Kunden weitergeleitet werden. Die Informationen auf dieser Seite werden nach dem entsprechenden Datum und Status gefiltert.

Widgets für Hardware-Inventarisierung

Die Tabellen-Widgets **Hardware-Inventarisierung** und **Hardware-Details** zeigen Informationen über alle Hardware an, die von den physischen und virtuellen Windows- sowie macOS-Geräten in den Unternehmen Ihrer Kunden verwendet wird.


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

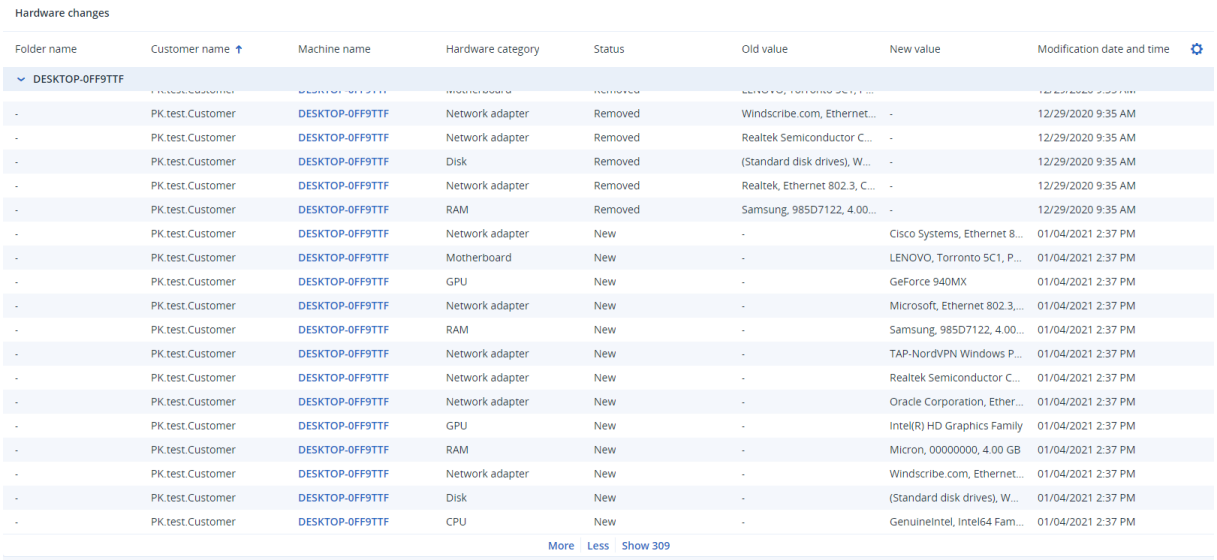
Hardware details

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

Das Tabellen-Widget **Hardware-Änderungen** zeigt Informationen über hinzugefügte, entfernte oder geänderte Hardware auf physischen und virtuellen Windows- sowie macOS-Geräten in den

Unternehmen Ihrer Kunden für einen spezifizierten Zeitraum (7 Tage, 30 Tage oder den aktuellen Monat) an.



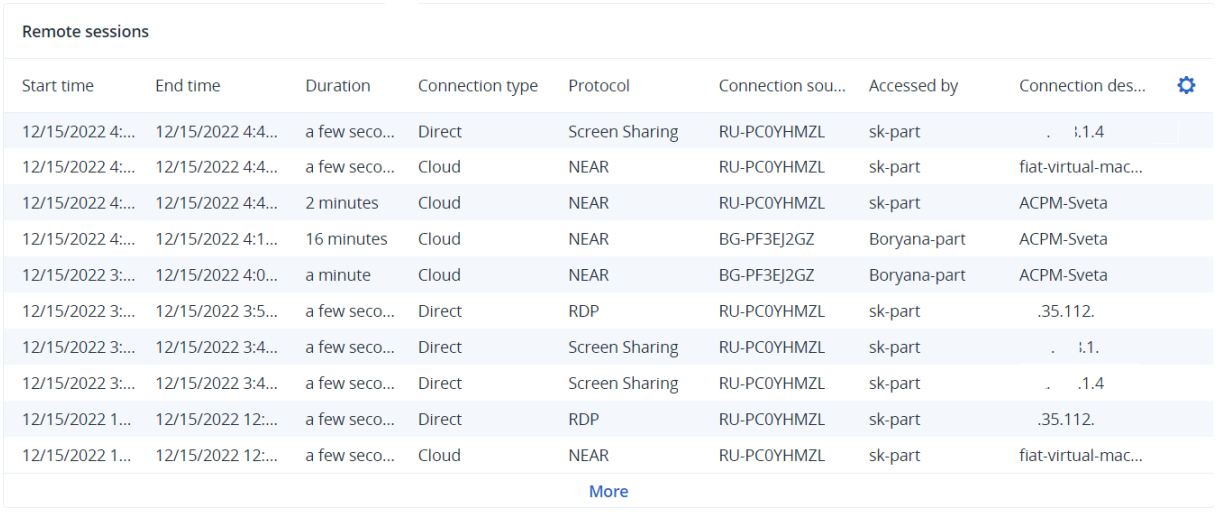
Hardware changes

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

Sitzungsverlauf

Das Widget zeigt detaillierte Informationen über die Remote-Desktop- und Dateiübertragungssitzungen an, die in den Organisation Ihrer Kunden während eines bestimmten Zeitraums durchgeführt wurden.



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

Verkauf und Abrechnung

Das Dashboard **Verkauf und Abrechnung** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Aktionen geben, die im Zusammenhang mit Advanced Automation stehen.

Standardmäßig werden die Daten für den Mandanten, in dem Sie arbeiten, sofern für diesen der Advanced Automation Service aktiviert wurde.

Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Sie können den aktuellen Zustand des Dashboards außerdem in Form einer .pdf-Datei herunterladen oder als E-Mail an eine beliebige Adresse versenden (auch an externe Empfänger).

So können Sie die Widgets auf dem Dashboard neu anordnen

Verschieben Sie das Widget per Drag & Drop, indem Sie zuvor auf dessen Namen klicken.

So können Sie ein Widget bearbeiten

Klicken Sie in der rechten oberen Ecke des Widgets auf das Stiftsymbol. Wenn Sie ein Widget bearbeiten, können Sie es auch umbenennen.

So können Sie ein Widget hinzufügen

Klicken Sie auf **Widget hinzufügen** und gehen Sie dann nach einer der folgenden Möglichkeiten vor:

- Klicken Sie auf das hinzuzufügende Widget. Das Widget wird daraufhin mit den Standardeinstellungen hinzugefügt.
- Wenn Sie das Widget vor dem Hinzufügen bearbeiten wollen, dann klicken Sie nach der Auswahl des Widgets auf den Befehl **Anpassen**. Klicken Sie, nachdem Sie das Widget bearbeitet haben, auf **Fertig**.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

Widgets 'Verkauf und Abrechnung'

In diesem Dashboard werden wichtige Metriken in Bezug auf Ihre aktuellen Verkäufe und Abrechnungen angezeigt. Wie etwa:

- **Zu fakturierende Verträge**: In diesem Bereich wird der Gesamtbetrag aller aktuellen Vertragselemente angezeigt, die noch nicht abgerechnet wurden.
- **Zu fakturierende Verkaufsartikel**: In diesem Bereich wird der Gesamtbetrag aller aktuellen Verkaufsartikel angezeigt, die noch nicht abgerechnet wurden. Sie können zur Rechnungsansicht wechseln und einen neuen Fakturierungslauf für diese Artikel starten, indem Sie auf **Fakturierungslauf starten** klicken.
- **Anzahl der betreuten Endbenutzer**: In diesem Abschnitt wird die Gesamtzahl der Benutzer und Kontakte des Endkunden angezeigt, die betreut werden (einschließlich aller aktiven und inaktiven Benutzer und Kontakte).
- **Monatlicher Service-Umsatz pro Nutzer**: In diesem Abschnitt wird der Umsatzbetrag als Verhältnis der *Zu fakturierenden Verträge* geteilt durch die *Anzahl der betreuten Endbenutzer* angezeigt. Sie können zum Kunden-Anzeige wechseln, indem Sie auf **Zu Clients gehen** klicken.
- **Net New MRR (Nettoumsatz durch Neukunden)**: In diesem Diagramm werden drei wichtige Metriken angezeigt: MRR Churn (Monatl. Umsatzeinbußen durch Kundenverlust), Expansion MRR (Neuer Umsatz mit Bestandskunden) und Net New MRR (Nettoumsatz durch Neukunden) Die drei

Metriken werden standardmäßig zusammen angezeigt, können aber durch Anklicken des jeweiligen Metrik-Namens auch einzeln dargestellt werden.

- **Umsatz aus allen Verkaufsartikeln**: In diesem Diagramm werden zwei wichtige Metriken angezeigt – Umsatz aus allen Verkaufsartikeln, die abgerechnet wurden, und Umsatz aus allen neuen Verkaufsartikeln. Die zwei Metriken werden standardmäßig zusammen angezeigt, können aber durch Anklicken des jeweiligen Metrik-Namens auch einzeln dargestellt werden.
- **Workloads**: In diesem Abschnitt wird die Anzahl der verwalteten Workloads und die Anzahl der Workloads angezeigt, die in einem Vertrag enthalten sind.

Service Desk

Das Dashboard **Service Desk** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Service Desk-Aktionen geben, die im Zusammenhang mit Advanced Automation stehen.

Standardmäßig werden die Daten für den Mandanten, in dem Sie arbeiten, sofern für diesen der Advanced Automation Service aktiviert wurde.

Die Widgets haben anklickbare Elemente, über die Sie Probleme untersuchen und beheben können. Sie können den aktuellen Zustand des Dashboards außerdem in Form einer .pdf-Datei herunterladen oder als E-Mail an eine beliebige Adresse versenden (auch an externe Empfänger).

So können Sie die Widgets auf dem Dashboard neu anordnen

Verschieben Sie das Widget per Drag & Drop, indem Sie zuvor auf dessen Namen klicken.

So können Sie ein Widget bearbeiten

Klicken Sie in der rechten oberen Ecke des Widgets auf das Stiftsymbol. Wenn Sie ein Widget bearbeiten, können Sie es auch umbenennen.

So können Sie ein Widget hinzufügen

Klicken Sie auf **Widget hinzufügen** und gehen Sie dann nach einer der folgenden Möglichkeiten vor:

- Klicken Sie auf das hinzuzufügende Widget. Das Widget wird daraufhin mit den Standardeinstellungen hinzugefügt.
- Wenn Sie das Widget vor dem Hinzufügen bearbeiten wollen, dann klicken Sie nach der Auswahl des Widgets auf den Befehl **Anpassen**. Klicken Sie, nachdem Sie das Widget bearbeitet haben, auf **Fertig**.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

Service Desk-Widgets

Im Service Desk-Dashboard werden wichtige Metriken in Bezug auf Ihre aktuellen Ticket-Aktionen angezeigt. Wie etwa:

- **Offene Tickets**: Zeigt die Gesamtzahl der aktuellen Tickets an, die nicht den Status **Geschlossen** haben.
- **SLA-Verletzungen**: Zeigt die Gesamtzahl der Tickets an, die nicht den Status **Geschlossen** haben und gegen ein SLA verstoßen. Klicken Sie auf **Alle SLA-Verletzungen anzeigen**, um die entsprechenden Tickets einzusehen.
- **Nicht zugewiesene Tickets**: Zeigt die Gesamtzahl der aktuellen Tickets an, die keinem Techniker zugewiesen wurden.
- **Heute fällige Tickets**: Zeigt die Gesamtzahl der Tickets an, die heute fällig sind. Klicken Sie auf **Zu heute fälligen Tickets gehen**, um die entsprechenden Tickets einzusehen.
- **Anstehende Besuche vor Ort**: Zeigt die Gesamtzahl der geplanten Kundenbesuche vor Ort an. Klicken Sie auf **Zu anstehende Besuche vor Ort gehen**, um die entsprechenden Tickets einzusehen.
- **Tickets**: Zeigt die Gesamtzahl der Tickets mit allen Statuszuständen an, die wiederum nach Tickets für den heutigen Tag, die aktuelle Woche und den aktuellen Monat aufgeschlüsselt sind.
- **Weiterempfehlungsrate (NPS)**: Zeigt die Weiterempfehlungsrate (NPS) für den aktuellen Monat und das aktuelle Jahr an, basierend auf den Tickets des aktuell angemeldeten Benutzers sowie auf Tickets, die Gruppen zugewiesen sind, zu denen der Benutzer ebenfalls gehört.
- **Ticket-Typen**: Zeigt ein Tortendiagramm und eine Aufschlüsselung in Prozentwerten für alle aktuell offenen Tickets pro Ticket-Typ an.
- **Ticket-Statistiken**: Zeigt die Gesamtzahl pro Woche/Monat (klicken Sie zum Wechseln der Ansicht auf **Woche** oder **Monat**) aller geschlossenen Tickets im Vergleich zu den Tickets mit SLA-Verletzungen an.
- **Auslastung**: Zeigt die durchschnittliche Auslastung der Techniker in Ihrem Unternehmen entweder für die vergangene Woche oder den vergangenen Monat an (klicken Sie zum Wechseln der Ansicht auf **Woche** oder **Monat**).

Überwachungsprotokoll

Das Überwachungsprotokoll stellt eine chronologische Aufzeichnung über folgende Ereignisse bereit:

- Aktionen, die von den Benutzern im Management-Portal durchgeführt werden
- Aktionen mit Cloud-zu-Cloud-Ressourcen, die von Benutzern in der Cyber Protect-Konsole durchgeführt werden
- Cyber Scripting-Aktionen, die von Benutzern in der Cyber Protect-Konsole durchgeführt werden
- Systemmeldungen über erreichte Quotas und deren Nutzung

Das Protokoll (Log) zeigt Ereignisse für den Mandanten (und dessen Untermandanten) an, in dem Sie sich gerade befinden. Klicken Sie auf ein Ereignis, wenn Sie mehr Informationen darüber erhalten wollen.

Überwachungsprotokolle (Audit-Logs) werden im Datacenter gespeichert, sodass deren Verfügbarkeit nicht durch Probleme auf den Endbenutzer-Maschinen beeinträchtigt werden kann.

Das Protokoll wird einmal täglich bereinigt. Die Ereignisse werden nach 180 Tagen gelöscht.

Felder im Überwachungsprotokoll

Für jedes Ereignis zeigt das Protokoll Folgendes an:

- **Ereignis**
  Eine kurze Beschreibung des Ereignisses. Beispiele: **Mandant wurde erstellt**, **Mandant wurde gelöscht**, **Benutzer wurde erstellt**, **Benutzer wurde gelöscht**, **Quota wurde erreicht**, **Backup-Inhalt wurde durchsucht**, **Skript wurde geändert**.
- **Schweregrad**
  Folgende Werte sind möglich:
  - **Fehler**
    Kennzeichnet einen Fehler.
  - **Warnung**
    Kennzeichnet eine potenziell negative Aktion. Beispiele: **Mandant wurde gelöscht**, **Benutzer wurde gelöscht**, **Quota wurde erreicht**.
  - **Hinweis**
    Kennzeichnet ein Ereignis, das möglicherweise eine Benutzerinteraktion erfordert. Beispiele: **Tenant wurde aktualisiert**, **Benutzer wurde aktualisiert**.
  - **Informationell**
    Kennzeichnet eine neutrale Information oder Aktion. Beispiele: **Mandant wurde erstellt**, **Benutzer wurde erstellt**, **Quota wurde aktualisiert**, **Skripting-Plan wurde gelöscht**.
- **Datum**
  Datum und Zeitpunkt, als das Ereignis auftrat.
- **Objektname**
  Das Objekt, mit dem die Aktion durchgeführt wurde. Beispiel: das Objekt des Ereignisses **Benutzer wurde aktualisiert** ist derjenige Benutzer, dessen Eigenschaften geändert wurden. Bei Ereignissen, die sich auf eine Quota beziehen, ist die Quota das Objekt.
- **Mandant**
  Der Name des Mandanten, zu dem das Objekt gehört.
- **Initiator**
  Der Anmeldename des Benutzers, der das Ereignis initiiert hat. Bei Systemmeldungen und Ereignissen, die von einem übergeordneten Administratoren initiiert wurden, wird **System** als Inititator angezeigt.
- **Mandant des Initiators**
  Der Name des Mandanten, zu dem der Initiator gehört. Bei Systemmeldungen und Ereignissen, die von einem übergeordneten Administrator initiiert wurden, bleibt dieses Feld leer.
- **Methode**
  Zeigt an, ob das Ereignis über das Weboberfläche oder über die API ausgelöst wurde.
- **IP**
  Die IP-Adresse der Maschine, von der aus das Ereignis ausgelöst wurde.

Filter und Suche

Sie können die Ereignisse nach Typ, Schweregrad oder Datum filtern. Sie können die Ereignisse auch nach Name, Objekt, Mandant, Initiator und Mandant des Initiators durchsuchen.

Berichte

Klicken Sie auf **Berichte**, wenn Sie Berichte über die Service-Nutzung und durchgeführte Aktionen erstellen wollen.

Nutzung

Nutzungsberichte stellen Daten über die zurückliegende Nutzung der Services zur Verfügung. Nutzungsberichte sind im CSV- und HTML-Format verfügbar.

Berichtstyp

Sie können einen der folgenden Berichtstypen wählen:

- **Aktuelle Nutzung**
  Der Bericht enthält die aktuellen Service-Nutzungsmetriken.
  Die Nutzungsmetriken werden innerhalb der Abrechnungszeiträume eines jeden der Untermandanten berechnet. Falls die im Bericht enthaltenen Mandanten unterschiedliche Abrechnungszeiträume haben, kann die Nutzung des übergeordneten Mandanten von der summierten Nutzung der untergeordneten Mandanten abweichen.
- **Aktuelle Nutzungsverteilung**
  Dieser Bericht ist nur für Partner-Mandanten verfügbar, die von einem externen Bereitstellungssystem verwaltet werden. Dieser Bericht ist nützlich, wenn die Abrechnungszeiträume für untergeordnete Mandanten nicht mit dem Abrechnungszeitraum des übergeordneten Mandanten übereinstimmen. Der Bericht enthält die Service-Nutzungsmetriken für untergeordnete Mandanten, berechnet innerhalb des aktuellen Abrechnungszeitraums des übergeordneten Mandanten. Die Nutzung des übergeordneten Mandanten entspricht garantiert der summierten Nutzung der untergeordneten Mandanten.
- **Zusammenfassung für Zeitraum**
  Der Bericht enthält die Service-Nutzungsmetriken für das Ende des spezifizierten Zeitraums und den Unterschied zwischen den Metriken zu Beginn und Ende des spezifizierten Zeitraums.
- **Täglich für einen Zeitraum**
  Der Bericht enthält die Service-Nutzungsmetriken und deren Änderungen für jeden Tag des spezifizierten Zeitraums.

Berichtsumfang

Sie können den Umfang des Berichts über die folgenden Werte bestimmen:

- **Direkte Kunden und Partner**

  Der Bericht wird nur Service-Nutzungsmetriken für die direkten Untermandanten des Mandanten enthalten, in dem Sie gerade arbeiten.
- **Alle Kunden und Partner**

  Der Bericht wird Service-Nutzungsmetriken für alle Untermandanten des Mandanten enthalten, in dem Sie gerade arbeiten.
- **Alle Kunden und Partner (einschließlich Benutzerdetails)**

  Der Bericht wird Service-Nutzungsmetriken für alle Untermandanten des Mandanten enthalten, in dem Sie gerade arbeiten, und für alle Benutzer innerhalb der Mandanten.

Metriken mit einer Nutzung von Null

Sie können die Anzahl der Zeilen im Bericht verringern, indem Sie nur Informationen über solche Metriken auflisten lassen, deren Nutzung ungleich Null ist, und zudem Informationen über Metriken ausblenden lassen, die keine Nutzung aufweisen (gleich Null ist).

Geplante Nutzungsberichte konfigurieren

Ein geplanter Bericht umfasst die Service-Nutzungsmetriken für den letzten vollen Kalendermonat. Die Berichte werden um 23:59:59 Uhr (UTC-Zeit) am ersten Tag eines Monats generiert und dann am zweiten Tag desselben Monats gesendet. Die Berichte werden an alle Administratoren Ihres Mandanten gesendet, die in den Benutzereinstellungen das Kontrollkästchen **Geplante Nutzungsberichte** aktiviert haben.

Hinweis
Die Filterung nach Datum erfolgt anhand des Zeitstempels, zu dem das Ereignis in die Cloud übermittelt wurde – und nicht anhand des Zeitpunkts, zu dem die Aktivität gestartet oder beendet wurde. Sollte also die Verbindung zum Server unterbrochen werden, kann ein täglicher Bericht Daten von mehr als einem Tag enthalten.

So (de)aktivieren Sie einen geplanten Bericht

1. Melden Sie sich am Management-Portal an.
2. Stellen Sie sicher, dass Sie in dem obersten Mandanten arbeiten, der für Sie verfügbar ist.
3. Klicken Sie auf **Berichte** –> **Nutzung**.
4. Klicken Sie auf **Geplant**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Einen monatlichen Übersichtsbericht senden**.
6. Bestimmen Sie bei **Detail-Level**, welchen Umfang der Bericht haben soll.
7. [Optional] Wählen Sie **Metriken mit einer Nutzung von Null ausblenden**, wenn Sie Metriken ausschließen wollen, bei denen es keine Nutzung gibt.

Benutzerdefinierte Nutzungsberichte konfigurieren

Dieser Berichtstyp kann bei Bedarf generiert werden, aber nicht geplant werden. Der Bericht wird an Ihre E-Mail-Adresse gesendet.

So erstellen Sie einen benutzerdefinierten Bericht

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie zu dem Mandanten, für den Sie einen Bericht erstellen wollen.
3. Klicken Sie auf **Berichte** –> **Nutzung**.
4. Wählen Sie die Registerkarte **Benutzerdefiniert**.
5. Wählen Sie – wie oben beschrieben – im Feld **Typ** den Berichtstyp aus.
6. [Nicht verfügbar für den Berichtstyp **Aktuelle Nutzung**] Wählen Sie bei **Zeitraum** den Berichtszeitraum.
   - **Aktueller Kalendermonat**
   - **Vorheriger Kalendermonat**
   - **Benutzerdefiniert**
7. [Nicht verfügbar für den Berichtstyp **Aktuelle Nutzung**] Wenn Sie einen benutzerdefinierten Berichtszeitraum spezifizieren wollen, müssen Sie die entsprechenden Start- und Endzeiten festlegen. Ansonsten können Sie diesen Schritt überspringen.
8. Bestimmen Sie bei **Detail-Level**, welchen Umfang der Bericht haben soll (wie oben beschrieben).
9. [Optional] Wählen Sie **Metriken mit einer Nutzung von Null ausblenden**, wenn Sie Metriken ausschließen wollen, bei denen es keine Nutzung gibt.
10. Um einen Bericht zu generieren, klicken Sie auf **Generieren und senden**.

Verkauf und Abrechnung

Die Komponente 'Verkauf und Abrechnung' von Advanced Automation enthält eine Reihe von Berichten, auf die über das Menü **Berichte –> Verkauf und Abrechnung** zugegriffen werden kann.

Hinweis
Verkaufs- und Abrechnungsberichte sind nur für Benutzer mit folgenden Rollen verfügbar: Administrator, Direktor, Gruppenleiter, Finanzdirektor, Personalabteilung

Jeder Verkaufs- und Abrechnungsbericht enthält Daten aus einem spezifizierten Zeitraum, der nach Bedarf geändert werden kann. Sie können jedem Bericht auch bereits vorhandene Berichte und Widgets hinzufügen, um ihn an Ihre Anforderungen anzupassen. Außerdem können Sie jeden Bericht herunterladen oder per E-Mail im XLSX- (Excel) oder PDF-Format versenden. Weitere Informationen finden Sie in den unteren Abschnitten.

Folgende Verkaufs- und Abrechnungsberichte sind verfügbar:

- Kundenumsatz
- Ausgaben
- "Prädiktive Rentabilität" (S. 126)
- Bruttogewinn pro Kunde
- Bruttogewinn Zusammenfassung

Einen Bericht hinzufügen

Sie können, ganz nach Ihren Anforderungen, jedem der Berichte einen bereits vorhandenen Bericht oder einen benutzerdefinierten Bericht hinzufügen.

1. Klicken Sie auf **Bericht hinzufügen**.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie einen vordefinierten Bericht hinzufügen wollen, müssen Sie diesen in der angezeigten Liste suchen und dann auswählen.
   - Wenn Sie einen benutzerdefinierten Bericht hinzufügen wollen, klicken Sie zuerst auf **Benutzerdefiniert**, dann auf den Berichtsnamen (die automatisch zugewiesenen Namen sehen folgendermaßen aus: **Benutzerdefiniert(1)**) und fügen Sie dann die Widgehts dem Bericht hinzu.
3. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.
4. [Optional] Bearbeiten Sie den Bericht wie nachfolgend beschrieben.

Einem Bericht ein Widget hinzufügen

Sie können, ganz nach Ihren Anforderungen, jedem der Berichte Widgets hinzufügen.

1. Klicken Sie auf **Widget hinzufügen**.
2. Suchen Sie im angezeigten Dialogfeld nach dem/den entsprechenden Widget(s) und fügen Sie dieses/diese hinzu.
3. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.
4. [Optional] Bearbeiten Sie den Bericht wie nachfolgend beschrieben.

Die Berichtseinstellungen bearbeiten

Wenn Sie einen Bericht bearbeiten wollen, müssen Sie zuerst auf dessen Namen klicken und dann auf **Einstellungen**. Durch Bearbeitung eines Berichts können Sie:

- Den Bericht umbenennen.
- Den angezeigten Mandanten für alle im Report enthaltenen Widgets ändern.
- Wenn Sie Untermandanten haben, steht Ihnen die Option **Einen Mandanten für alle Widgets festlegen** zur Verfügung. Diese Option ermöglicht Ihnen, die Daten in allen Widgets des Berichts nach dem ausgewählten Mandanten zu filtern. Wenn diese Option nicht ausgewählt ist, werden die Widgets die Daten für alle Untermandanten Ihres aktuellen Mandanten anzeigen.

- Den Zeitraum für alle im Report enthaltenen Widgets ändern.
- Eine Planung für das Versenden des Bericht im PDF- und/oder Excel-Format per E-Mail festlegen.

Einen Bericht planen

Sie können jeden Bericht planen und definieren, wer ihn in welchem Format erhalten soll.

1. Klicken Sie auf den Berichtsnamen und dann auf **Einstellungen**.
2. Aktivieren Sie den Optionsschalter **Geplant**.
3. Spezifizieren Sie die E-Mail-Adresse(n) des/der Empfänger.
4. Bestimmen Sie das Format für den Bericht: PDF, Excel oder beides
5. Bestimmen Sie die Tage und den genauen Zeitpunkt, an dem der Bericht versendet werden soll.
6. Klicken Sie in der rechten oberen Ecke auf **Speichern**.

Die Berichtsstruktur exportieren und importieren

Sie können die Berichtsstruktur (die Zusammenstellung der Widgets und die Berichtseinstellungen) als JSON-Datei exportieren oder importieren. Dies kann nützlich sein, wenn Sie die Berichtsstruktur von einem Mandanten zu einem anderen kopieren wollen.

Wenn Sie die Berichtsstruktur exportieren wollen, müssen Sie zuerst auf den Berichtsnamen klicken, dann in der rechten oberen Ecke auf das vertikale Drei-Punkte-Symbol und abschließend auf den Befehl **Exportieren**.

Wenn Sie die Berichtsstruktur importieren wollen, müssen Sie zuerst auf **Bericht hinzufügen** klicken und anschließend auf **Importieren**.

Einen Bericht herunterladen

Wenn Sie jeden Bericht herunterladen, indem Sie auf **Download** klicken und das gewünschte Format auswählen:

- **Excel und PDF**
- **Excel**
- **PDF**

Kundenumsatz

Der Kundenumsatzbericht ermöglicht es Ihnen, die wichtigsten Verkaufsmetriken für jeden Kunden nachzuverfolgen. Dazu gehören Informationen für:

- Alle Kunden, jeweils einzeln ausgewählt.
- Einen spezifizierten Zeitraum.

Wenn Sie den Kundenumsatzbericht generieren wollen, gehen Sie zu **Berichte –> Verkauf und Abrechnung** und wählen Sie dann **Kundenumsatz**. Wählen Sie dann den Kunden und den relevanten Zeitraum aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Verkauf und Abrechnung" (S. 122)'.

Der generierte Bericht enthält folgende Widgets:

- Kundenausgaben, einschließlich:
  - Gesamtbetrag wiederkehrend
  - Gesamtbetrag nicht wiederkehrend
  - Gesamtbetrag VAR
  - Gesamtbetrag
- Durchschnittlicher Stundensatz des Kunden, der den durchschnittlichen Stundensatz für Tickets für den ausgewählten Kunden in den letzten sechs Monaten anzeigt.
- Zeitaufwand des Kunden, einschließlich:
  - Zeitaufwand auf Festpreisbasis
  - Zeitaufwand für nachträgliche Berechnungsgrundlage
  - Zeitaufwand für anderes, nicht abrechenbares
- Endpunkte als Teil eines Vertrags, was die Gesamtzahl der Endpunkte angibt, die Bestandteil von Verträgen mit dem Kunden sind.
- Endpunkte insgesamt unter Verwaltung, was die Gesamtzahl der unter Verwaltung stehenden Endpunkte des Kunden angibt.
- Anzahl der betreuten Endbenutzer, was die Gesamtanzahl der Benutzer des Kunden angibt, die betreut werden.
- Zu fakturierende Verträge, was den Gesamtbetrag aller aktuellen Vertragselemente angibt.
- Monatlicher Service-Umsatz pro Nutzer, was die Gesamtsumme der abzurechnenden Verträge geteilt durch die Anzahl der betreuten Endnutzer angibt.
- Vertragselemente, was eine Auflistung der Vertragselemente einschließlich deren Wert für das gesamte Jahr anzeigt.

Ausgaben

Im Bericht 'Ausgaben' finden Sie Informationen über die Kosten der Produkte und Services, die den Kunden bereitgestellt wurden. Dazu gehören:

- Verkaufsartikel und Vertragseinzelposten innerhalb des definierten Berichtszeitraums.
- Abgerechnete oder noch nicht abgerechnete Elemente.
- Spezifische Kundeninformationen oder einen Bericht für alle Kunden.
- Spezifische Produktinformationen oder einen Bericht für alle Produkte.

Wenn Sie den Ausgabenbericht generieren wollen, gehen Sie zu **Berichte –> Verkauf und Abrechnung** und wählen Sie dann **Ausgaben**. Wählen Sie dann den Kunden, das Produkt, den

Ausgabentyp und den relevanten Zeitraum aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Verkauf und Abrechnung" (S. 122)'.

Der generierte Bericht enthält:

- Einen Abschnitt mit einer allgemeinen Zusammenfassung.
- Einen Kundenabschnitt, der eine zeilenweise Übersicht über die Produktnamen oder Services, die einem Kunden bereitgestellt wurden, enthält.

Prädiktive Rentabilität

Der prädiktive Rentabilitätsbericht gibt Aufschluss über die zukünftige Rentabilität und basiert dabei auf folgenden Informationen:

- Laufende Verträge und aktive Vertragslaufzeiten.
- Aktuelle aktive Vertragseinzelposten und die für diese Einzelposten festgelegten Zeiträume.
- Verlauf der Ticket-basierten Aktivitäten.
- Verlauf der Verkaufsartikel.
- Aktuelle Preise und Kosten für Produkte und Services.

Wenn Sie den prädiktive Rentabilitätsbericht generieren wollen, gehen Sie zu **Berichte –> Verkauf und Abrechnung** und wählen Sie dann **Prädiktive Rentabilität**. Wählen Sie dann den Kunden, das Produkt und den relevanten Zeitraum aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Verkauf und Abrechnung" (S. 122)'.

Der generierte Bericht enthält:

- Einen Abschnitt mit einer allgemeinen Zusammenfassung.
- Einen Abschnitt mit einer Zusammenfassung pro Monat, einschließlich der monatlichen und jährlichen Wachstumsraten in Prozent.
- Eine Zusammenfassung der letzten sechs Monate.
- Einen Kundenabschnitt, der eine zeilenweise Übersicht über die Produktnamen oder Services, die einem Kunden bereitgestellt wurden, enthält.

Bruttogewinn pro Kunde

Der Bericht 'Bruttogewinn pro Kunde' ermöglicht es Ihnen, die Gewinne und Kosten für bestimmte Kunden nachzuverfolgen. Das umfasst Informationen für:

- Alle Kunden, jeweils einzeln ausgewählt.
- Einen spezifizierten Zeitraum.

Wenn Sie den Bericht 'Bruttogewinn pro Kunde' generieren wollen, gehen Sie zu **Berichte –> Verkauf und Abrechnung** und wählen Sie dann **Bruttogewinn pro Kunde**. Wählen Sie dann den

Kunden und den relevanten Zeitraum aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Verkauf und Abrechnung" (S. 122)'.

Der generierte Bericht enthält:

- Einen Abschnitt mit einer Zusammenfassung.
- Eine Aufschlüsselung der einzelnen Verträge für den ausgewählten Kunden.
- Ein Überblick über die Rentabilität der Verträge, Verkaufsartikel und Arbeitskosten für den Kunden.

Bruttogewinn Zusammenfassung

Der Bericht 'Bruttogewinn Zusammenfassung' bietet Ihnen eine Gewinn- und Kostenanalyse. Das umfasst Informationen für:

- Alle Kunden, einschließlich einzeiliger Zusammenfassungen für jeden Kunden.
- Einen spezifizierten Zeitraum.
- Einen spezifizierten Aggregationszeitraum (Monat / Quartal / Jahr).

Wenn Sie den Bericht 'Bruttogewinn Zusammenfassung' generieren wollen, gehen Sie zu **Berichte –> Verkauf und Abrechnung** und wählen Sie dann **Bruttogewinn Zusammenfassung**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Verkauf und Abrechnung" (S. 122)'.

Der Bericht enthält einen Hauptabschnitt mit einer Zusammenfassung aller ausgewählten Kunden und des entsprechenden Zeitraums, wobei der Gesamtgewinn pro Kunde aus der Differenz zwischen Gewinn und Kosten berechnet wird.

Service Desk

Die Komponente 'Service Desk' von Advanced Automation enthält eine Reihe von Berichten, auf die über das Menü **Berichte –> Service Desk** zugegriffen werden kann.

Hinweis
Service Desk-Berichte sind nur für Benutzer mit folgenden Rollen verfügbar: Administrator, Direktor, Gruppenleiter, Finanzdirektor, Personalabteilung

Jeder Service Desk-Bericht enthält Daten aus einem spezifizierten Zeitraum, der nach Bedarf geändert werden kann. Sie können jedem Bericht auch bereits vorhandene Berichte und Widgets hinzufügen, um ihn an Ihre Anforderungen anzupassen. Außerdem können Sie jeden Bericht herunterladen oder per E-Mail im XLSX- (Excel) oder PDF-Format versenden. Weitere Informationen finden Sie in den unteren Abschnitten.

Folgende Service Desk-Berichte sind verfügbar:

- Dauer der abgeschlossenen Tickets
- NPS-Nachverfolgung
- Anzahl der Aktualisierungen im Ticket
- SLA-Übersicht
- Metriken zur Techniker-Performance
- Ticket-Statistiken
- Tickets mit speziellem Status

Einen Bericht hinzufügen

Sie können, ganz nach Ihren Anforderungen, jedem der Berichte einen bereits vorhandenen Bericht oder einen benutzerdefinierten Bericht hinzufügen.

1. Klicken Sie auf **Bericht hinzufügen**.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie einen vordefinierten Bericht hinzufügen wollen, müssen Sie diesen in der angezeigten Liste suchen und dann auswählen.
   - Wenn Sie einen benutzerdefinierten Bericht hinzufügen wollen, klicken Sie zuerst auf **Benutzerdefiniert**, dann auf den Berichtsnamen (die automatisch zugewiesenen Namen sehen folgendermaßen aus: **Benutzerdefiniert(1)**) und fügen Sie dann die Widgehts dem Bericht hinzu.
3. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.
4. [Optional] Bearbeiten Sie den Bericht wie nachfolgend beschrieben.
   Bei Bedarf können Sie den Bericht auch klonen oder löschen.

Einem Bericht ein Widget hinzufügen

Sie können, ganz nach Ihren Anforderungen, jedem der Berichte Widgets hinzufügen.

1. Klicken Sie auf **Widget hinzufügen**.
2. Suchen Sie im angezeigten Dialogfeld nach dem/den entsprechenden Widget(s) und fügen Sie dieses/diese hinzu.
3. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.
4. [Optional] Bearbeiten Sie den Bericht wie nachfolgend beschrieben.

So können Sie die Widgets auf dem Dashboard neu anordnen

Verschieben Sie die Widgets per Drag & Drop-Aktion, indem Sie zuvor auf deren Namen klicken.

So können Sie ein Widget bearbeiten

Klicken Sie neben dem Widget-Namen auf das Stiftsymbol. Mit der Funktion 'Bearbeiten' können Sie ein Widget umbenennen, den Zeitbereich ändern, Filter festlegen und den Mandanten auswählen, für den die Daten angezeigt werden.

So können Sie ein Widget entfernen

Klicken Sie neben dem Widget-Namen auf das X-Symbol.

Die Berichtseinstellungen bearbeiten

Wenn Sie einen Bericht bearbeiten wollen, müssen Sie zuerst auf dessen Namen klicken und dann auf **Einstellungen**. Durch Bearbeitung eines Berichts können Sie:

- Den Bericht umbenennen.
- Den angezeigten Mandanten für alle im Report enthaltenen Widgets ändern.
- Wenn Sie Untermandanten haben, steht Ihnen die Option **Einen Mandanten für alle Widgets festlegen** zur Verfügung. Diese Option ermöglicht Ihnen, die Daten in allen Widgets des Berichts nach dem ausgewählten Mandanten zu filtern. Wenn diese Option nicht ausgewählt ist, werden die Widgets die Daten für alle Untermandanten Ihres aktuellen Mandanten anzeigen.
- Den Zeitraum für alle im Report enthaltenen Widgets ändern.
- Eine Planung für das Versenden des Bericht im PDF- und/oder Excel-Format per E-Mail festlegen.

Einen Bericht planen

Sie können jeden Bericht planen und definieren, wer ihn in welchem Format erhalten soll.

1. Klicken Sie auf den Berichtsnamen und dann auf **Einstellungen**.
2. Aktivieren Sie den Optionsschalter **Geplant**.
3. Spezifizieren Sie die E-Mail-Adresse(n) des/der Empfänger.
4. Bestimmen Sie das Format für den Bericht: PDF, Excel oder beides
5. Bestimmen Sie die Tage und den genauen Zeitpunkt, an dem der Bericht versendet werden soll.
6. Klicken Sie in der rechten oberen Ecke auf **Speichern**.

Einen Bericht herunterladen

Wenn Sie jeden Bericht herunterladen, indem Sie auf **Download** klicken und das gewünschte Format auswählen:

- **Excel und PDF**
- **Excel**
- **PDF**

Dauer der abgeschlossenen Tickets

Der Bericht 'Dauer der abgeschlossenen Tickets' gibt Aufschluss darüber, wie lange die Auflösung eines Tickets gedauert hat, was sich insbesondere auf die Anzahl der Tage zwischen dem Erstellen und dem Abschluss des Tickets bezieht. Anhand dieser Informationen können Sie eventuelle Überschreitungen erkennen und diese effizienter verwalten.

Wenn Sie den Bericht 'Dauer der abgeschlossenen Tickets' generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **Dauer der abgeschlossenen Tickets**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Service Desk" (S. 127)'.

NPS-Nachverfolgung

Der Bericht NPS-Nachverfolgung (Net Promoter Score, Weiterempfehlungsrate) zeigt Ticket-Bewertungen an, die auf dem Feedback der Endbenutzer basieren. Sobald ein Ticket geschlossen wird, wird automatisch eine E-Mail an die Benutzer gesendet, damit diese die Dienstleistung bewerten können.

Mit dem Bericht können Sie eine Reihe von wichtigen Kunden-Metriken nachverfolgen, wie etwa:

- Das prozentuale Verhältnis zwischen allen Befürwortern und allen Befragten.
- Die Anzahl der befragten Befürworter (Endbenutzer) mit einer Ticket-Bewertung von 9 und 10.
- Das prozentuale Verhältnis zwischen allen Neutralen und allen Befragten.
- Die Anzahl der neutralen Befragten (Endbenutzer) mit einer Ticket-Bewertung von 7 und 8.
- Das prozentuale Verhältnis zwischen allen Kritikern und allen Befragten.
- Die Anzahl der kritischen Befragten (Endbenutzer), die ein Ticket mit einer Bewertung von 0 bis 6 versehen haben.
- Der NPS-Wert, der als durchschnittliche Bewertung für alle Befragten berechnet wird.

Wenn Sie den NPS-Nachverfolgungsbericht generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **NPS-Nachverfolgung**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Sie können zudem einen bestimmten Kunden und einen Kunden-Endbenutzer sowie einen Support-Agenten und eine Support-Gruppe auswählen, um den Bericht weiter zu verfeinern.. Weitere Informationen darüber, wie Sie den Bericht anpassen, herunterladen und per E-Mail versenden können, finden Sie im Abschnitt '"Service Desk" (S. 127)'.

Anzahl der Aktualisierungen im Ticket

Der Bericht 'Anzahl der Aktualisierungen im Ticket' gibt Aufschluss darüber, wie viele Aktualisierungen an Tickets innerhalb eines bestimmten Zeitraums vorgenommen wurden, sodass Sie Tickets ermitteln können, die Probleme verursachen und nicht schnell genug bearbeitet wurden. So können viele Aktualisierungen beispielsweise auf mangelnde Kenntnisse des Technikers hinweisen, wobei die Aktualisierungen sowohl vom Techniker als auch vom Endbenutzer erfolgt sein können, als diese versuchten, das Problem zu lösen.

Wenn Sie den Bericht 'Anzahl der Aktualisierungen im Ticket' generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **Anzahl der Aktualisierungen im Ticket**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Weitere Informationen zum Anpassen, Herunterladen und Versenden des Berichts per E-Mail finden Sie im Abschnitt '"Service Desk" (S. 127)'.

SLA-Übersicht

Der SLA-Übersichtsbericht ermöglicht es Ihnen, die wichtigsten SLA-Metriken pro Unternehmen, Gruppe und Techniker zu überprüfen.

Die folgenden drei wichtigen SLA-Metriken können in diesem Bericht nachverfolgt werden:

- SLA für erste Antwort
- Nächste Antwortzeit
- Lösungszeit

Wenn Sie den SLA-Übersichtsbericht generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **SLA-Übersicht**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Sie können zudem eine spezifische Benutzergruppe und einen Benutzer auswählen, um den Bericht genauer zu gestalten. Weitere Informationen darüber, wie Sie den Bericht anpassen, herunterladen und per E-Mail versenden können, finden Sie im Abschnitt '"Service Desk" (S. 127)'.

Metriken zur Techniker-Performance

Mit dem Bericht über die Metriken zur Techniker-Performance können Sie die wichtigsten Metriken zur Techniker-Performance nachverfolgen. Wie etwa:

- Stunden der Abdeckung – was die verfügbaren Arbeitsstunden und die tatsächlich registrierte Arbeitszeit einschließt.
- Verantwortlichkeit – wozu auch die Kosten für die Beschäftigung gehören (anhand der Anzahl der geleisteten Arbeitsstunden multipliziert mit den Kosten für diese Stunden berechnet).
- Arbeitsabdeckung für Tickets – einschließlich der Tickets, die vom ausgewählten Techniker zugewiesen und bearbeitet wurden, sowie der drei Tickets mit der höchsten Durchlaufzeit.
- Arbeitsabdeckung für Projekte – einschließlich der aktuell bearbeiteten Projekte sowie der geschlossenen Projekte, die innerhalb der budgetierten Zeit abgeschlossen bzw. nicht abgeschlossen wurden.
- Die Weiterempfehlungsrate (NPS, Net Promoter Score) für den Techniker – einschließlich der Tickets, die am besten bzw. am schlechtesten bewertet wurden.

Wenn Sie den Bericht über die Metriken zur Techniker-Performance generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **Metriken zur Techniker-Performance**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Sie können zudem einen spezifischen Benutzer auswählen, um den Bericht genauer zu gestalten. Weitere Informationen darüber, wie Sie den Bericht anpassen, herunterladen und per E-Mail versenden können, finden Sie im Abschnitt '"Service Desk" (S. 127)'.

Techniker-Kapazitätsplanung

Mit dem Bericht über die Techniker-Kapazitätsplanung können Sie die Workloads Ihrer Techniker und deren prognostizierte Kapazität für zukünftige Zeiträume nachverfolgen. Für jeden Techniker,

der in dem Bericht enthalten ist, können Sie:

- Die Gesamtzahl aller verfügbaren Arbeitsstunden (alle verfügbare Zeit abzüglich der Wochenenden sowie der genehmigten Urlaubstage, Krankheitstage und Feiertage) für den ausgewählten Zeitraum einsehen.
- Die Gesamtzahl aller geplanten Aktivitäten (Service Desk-Aktivitäten eingeschlossen) in Tagen einsehen.
- Die Gesamtzahl der arbeitsfreien Tage (einschließlich genehmigter Urlaubstage, Krankheitstage und Feiertage) für den ausgewählten Zeitraum einsehen.
- Die verfügbare Gesamtzeit für den ausgewählten Zeitraum einsehen (aus den Arbeitstagen abzüglich aller geplanten Aktivitäten berechnet).

Wenn Sie den Bericht über die Techniker-Kapazitätsplanung generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **Techniker-Kapazitätsplanung**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten und im Feld **Berichte gruppieren nach** den relevanten Gruppentyp aus. Sie können auch einen bestimmten Techniker auswählen, um den Bericht genauer zu gestalten. Weitere Informationen darüber, wie Sie den Bericht anpassen, herunterladen und per E-Mail versenden können, finden Sie im Abschnitt '"Service Desk" (S. 127)'.

Ticket-Statistiken

Der Bericht über Ticket-Statistiken zeigt ein Diagramm mit der Gesamtzahl der geschlossenen Tickets sowie der Tickets, bei denen eine SLA-Verletzung vorlag. Im Diagramm werden die Statistiken für den aktuellen Tag, für den aktuellen Monat und die Gesamtjahresstatistik angezeigt. Der Bericht ermöglicht Ihnen, schnell die Performance Ihres Teams zu beurteilen, das Verhältnis von geschlossenen Tickets zu Tickets mit SLA-Verletzungen zu ermitteln und festzustellen, ob es in den letzten Monaten Verbesserungen gegeben hat.

Wenn Sie den Bericht über Ticket-Statistiken generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **Ticket-Statistiken** . Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Sie können zudem einen spezifischen Kunden auswählen, um den Bericht genauer zu gestalten. Weitere Informationen darüber, wie Sie den Bericht anpassen, herunterladen und per E-Mail versenden können, finden Sie im Abschnitt '"Service Desk" (S. 127)'.

Tickets mit speziellem Status

Der Bericht über Tickets mit speziellem Status ermöglicht es Ihnen, Tickets zu finden, die einen bestimmten Status haben, einer bestimmten Kategorie angehören oder eine bestimmte Priorität haben.

Wenn Sie den Bericht über Tickets mit speziellem Status generieren wollen, gehen Sie zu **Berichte –> Service Desk** und wählen Sie dann **Tickets mit speziellem Status**. Wählen Sie dann im Feld **Zeitraum** die relevanten Daten aus. Sie können zudem einen Status, eine Kategorie und/oder eine Priortität auswählen, um den Bericht genauer zu gestalten. Weitere Informationen darüber, wie Sie den Bericht anpassen, herunterladen und per E-Mail versenden können, finden Sie im Abschnitt '"Service Desk" (S. 127)'.

Aktionen-Berichte

Ein Bericht über Aktionen kann einen beliebigen Satz von Dashboard-Widgets des Typs '**Aktionen**' enthalten. Standardmäßig zeigen alle Widgets die Übersichtsinformationen für denjenigen Mandanten an, in dem Sie gerade arbeiten. Sie können dies für jedes Widget einzeln ändern, indem Sie dieses bearbeiten – oder für alle Widgets, indem Sie die Berichtseinstellungen entsprechend anpassen.

Je nach Widget-Typ enthält der Bericht Daten für einen bestimmten Zeitraum oder für den Zeitpunkt des Durchsuchens oder der Berichtserstellung. Siehe Abschnitt '"Berichtsdaten je nach Widget-Typ" (S. 151)'.

Alle historischen Widgets zeigen Daten für den gleichen Zeitraum an. Sie können diesen Zeitraum in den Berichtseinstellungen ändern.

Sie können vorgegebene Berichte (Standardberichte) verwenden oder einen benutzerdefinierten Bericht erstellen.

Sie können einen Bericht herunterladen oder per E-Mail im XLSX-Format (Excel) oder PDF-Format versenden.

Die Standardberichte sind nachfolgend aufgelistet:

Berichtsname	Beschreibung
#CyberFit-Score pro Maschine	Zeigt den #CyberFit-Score, der auf der Evaluierung von Sicherheitsmetriken und Sicherheitskonfigurationen für jede Maschine basiert, und Empfehlungen für deren Verbesserungen an.
Alarmmeldungen	Zeigt Alarmmeldungen an, die während eines bestimmten Zeitraums aufgetreten sind.
Backup-Scanning-Details	Zeigt ausführliche Informationen über erkannte Bedrohungen in den Backups an.
Tägliche Aktivitäten	Zeigt Übersichtsinformationen zu Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden.
Data Protection-Karte	Zeigt ausführliche Informationen über Anzahl, Größe, Speicherort und Sicherungsstatus aller wichtigen Dateien auf den Maschinen an.
Erkannte Bedrohungen	Zeigt Details der betroffenen Maschinen anhand der Anzahl der blockierten Bedrohungen sowie der fehlerfreien und verwundbaren Maschinen an.
Erkannte Maschinen	Zeigt alle gefundene Maschinen im Organisationsnetzwerk an.
Vorhersage der Laufwerksintegrität	Zeigt den aktuellen Laufwerksstatus an sowie eine Prognose dazu, wann Ihre HDD/SSD vermutlich ausfallen wird.

Vorhandene Schwachstellen	Zeigt die existierenden Verwundbarkeiten des Betriebssystems und der Applikationen in Ihrem Unternehmen an. Der Bericht zeigt zudem Details der betroffenen Maschinen in Ihrem Netzwerk für jedes aufgelistete Produkt an.
Übersicht zur Patch-Verwaltung	Zeigt die Anzahl der fehlenden, installierten und anwendbaren Patches an. Sie können sich Detailinformationen zu den Berichten anzeigen lassen, um Informationen und Details zu den fehlenden/installierten Patches für alle Systeme zu erhalten.
Übersicht	Zeigt Übersichtsinformationen zu geschützten Geräten für einen bestimmten Zeitraum an.
Wöchentliche Aktivitäten	Zeigt Übersichtsinformationen zu Aktivitäten an, die während eines bestimmten Zeitraums durchgeführt wurden.
Software-Inventarisierung	Zeigt ausführliche Informationen über die gesamte Software an, die auf den Windows- und macOS-Geräten in den Unternehmen Ihrer Kunden installiert ist.
Hardware-Inventarisierung	Zeigt ausführliche Informationen über die gesamte Hardware an, die für die physischen und virtuellen Windows- sowie macOS-Geräte in den Unternehmen Ihrer Kunden verfügbar ist.
Remote-Sitzungen	Zeigt detaillierte Informationen über die Remote Desktop- und Dateiübertragungssitzungen an, die in den Organisationen Ihrer Kunden während eines spezifizierten Zeitraums durchgeführt wurden.
Arbeitszeittabelle	Zeigt die durchschnittliche Arbeitszeit an, die Benutzer protokolliert haben, und bietet einen schnellen Überblick darüber, wie viel Zeit für Tickets und andere Dinge (z. B. manuelle Zeiteinträge) aufgewendet wurde. Dieser Bericht ist nur verfügbar, wenn der Advanced Automation Service aktiviert ist. Weitere Informationen finden Sie im Abschnitt '"Arbeitszeittabellen" (S. 136)'.

Aktionen mit Berichten

Wenn Sie einen Bericht einsehen wollen, klicken Sie auf dessen Namen.

So können Sie einen neuen Bericht hinzufügen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Klicken Sie unter der Liste der verfügbaren Berichte auf **Bericht hinzufügen**.
3. [Um einen vordefinierten Bericht hinzuzufügen] Klicken Sie auf den Namen des vordefinierten Berichts.
4. [Um einen benutzerdefinierten Bericht hinzuzufügen] Klicken Sie auf **Benutzerdefiniert** und fügen Sie dann Widgets zum Bericht hinzu.
5. [Optional] Ordnen Sie die Widgets per Drag & Drop nach Ihren Vorstellungen neu an.

So können Sie eine Bericht bearbeiten

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, den Sie bearbeiten wollen.
   Sie können Folgendes tun:
   - Den Bericht umbenennen.
   - Den Zeitraum für alle Widgets im Report ändern.
   - Die Berichtsempfänger spezifizieren sowie den Zeitpunkt, an dem der Bericht an diese gesendet werden soll. Die verfügbaren Formate sind PDF und XLSX.

So können Sie einen Bericht löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, den Sie löschen wollen.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf den Befehl **Löschen**.
4. Bestätigen Sie Ihre Auswahl, indem Sie auf **Löschen** klicken.

So können Sie eine Bericht planen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte denjenigen Bericht aus, den Sie planen wollen, und klicken Sie anschließend auf **Einstellungen**.
3. Aktivieren Sie den Schalter **Geplant**.
   - Spezifizieren Sie die E-Mail-Adressen der Empfänger.
   - Bestimmen Sie das Format des Berichts.

     Hinweis
     Sie können bis zu 1000 Elemente in eine PDF-Datei und bis zu 10.000 Elemente in eine XLSX-Datei exportieren. Die Zeitstempel in den PDF- und XLSX-Dateien basieren auf der lokalen Zeit Ihrer Maschine.

   - Bestimmen Sie die Sprache des Berichts.
   - Konfigurieren Sie die Planung.
4. Klicken Sie auf **Speichern**.

So können Sie einen Bericht herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus und klicken Sie dann auf **Download**.
3. Bestimmen Sie das Format des Berichts.

So können Sie einen Bericht senden

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus und klicken Sie dann auf **Senden**.
3. Spezifizieren Sie die E-Mail-Adressen der Empfänger.
4. Bestimmen Sie das Format des Berichts.
5. Klicken Sie auf **Senden**.

So können Sie die Berichtsstruktur exportieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie in der Liste der Berichte den gewünschten Bericht aus.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf den Befehl **Exportieren**.

Als Ergebnis wird die Berichtsstruktur als JSON-Datei auf Ihrer Maschine gespeichert.

So können Sie die Berichtsdaten sichern

Mit dieser Option können Sie alle Daten für einen benutzerdefinierten Zeitraum (ohne Filterung) in eine CSV-Datei exportieren und diese an einen E-Mail-Empfänger senden.

Hinweis
Sie können bis zu 150.000 Elemente in eine CSV-Datei exportieren. Die Zeitstempel in der CSV-Datei verwenden die koordinierte Weltzeit (UTC).

1. Gehen Sie in der Cyber Protect-Konsole zu **Berichte**.
2. Wählen Sie aus der Liste der Berichte denjenigen Bericht aus, dessen Daten Sie sichern wollen.
3. Klicken Sie auf das Drei-Punkte-Symbol (...) und dann auf **Sicherungsdaten**.
4. Spezifizieren Sie die E-Mail-Adressen der Empfänger.
5. Spezifizieren Sie bei **Zeitraum** den benutzerdefinierten Zeitraum, für den Sie die Daten sichern wollen.

   Hinweis
   CSV-Dateien für längere Zeiträume vorzubereiten, kostet mehr Zeit.

6. Klicken Sie auf **Senden**.

Arbeitszeittabellen

Die Komponente 'Zeitmanagement' von Advanced Automation enthält einen Arbeitszeittabellen-Bericht, auf den Sie über das Menü **Berichte –> Aktionen** zugreifen können. Dieser Bericht ermöglicht Ihnen, die durchschnittliche Arbeitszeit einzusehen, die die Benutzer protokolliert haben, und bietet einen schnellen Überblick darüber, wie viel Zeit für Tickets und andere Dinge (z.B. manuelle Zeiteinträge) aufgewendet wurde.

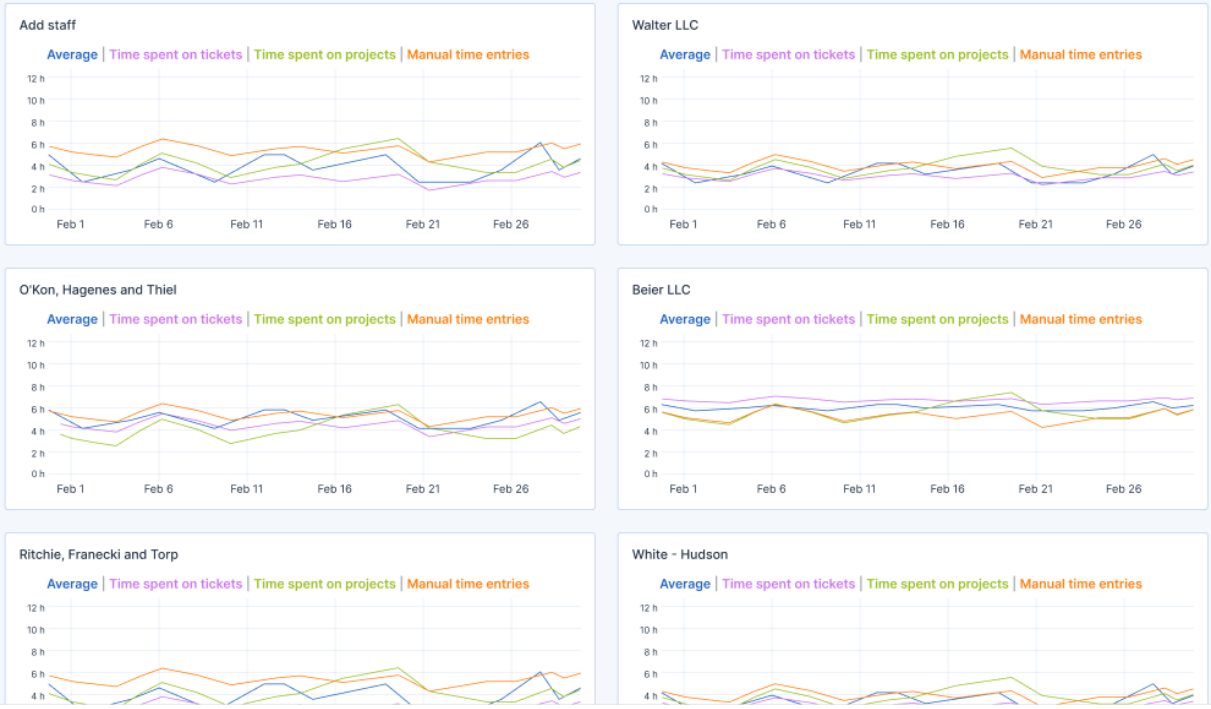
Hinweis
Der Arbeitszeittabellen-Bericht ist für Benutzer mit folgenden Rollen verfügbar: Administrator, Direktor, Gruppenleiter, Finanzdirektor, Personalabteilung

Der Arbeitszeittabellen-Bericht enthält Daten aus einem spezifizierten Zeitraum, der nach Bedarf geändert werden kann. Der Bericht besteht hauptsächlich aus zwei Widget-Typen:

- Das Widget **Alle Mitarbeiter**, welches eine Übersicht über alle aktiven Nutzer enthält.
- Individuelle Widgets für jeden Benutzer.

Jedes Widget enthält Details über die durchschnittlich protokollierte Zeit während des ausgewählten Zeitraums, die für Tickets aufgewendete Zeit, die für Projekte aufgewendete Zeit sowie die Zeit, die manuellen Zeiteinträgen zugeordnet wurde.

Sie können dem Bericht auch bereits vorhandene Berichte und Widgets hinzufügen, um ihn an Ihre Anforderungen anzupassen. Außerdem können Sie jeden Bericht herunterladen oder per E-Mail im XLSX- (Excel) oder PDF-Format versenden. Für weitere Informationen siehe die entsprechenden Abschnitte in '"Service Desk" (S. 127)'.



Kurzübersicht

Der Kurzübersichtsbericht bietet einen Überblick über den Schutzstatus der Umgebungen und geschützten Geräte Ihrer Kunden für einen spezifizierten Zeitraum.

Der Kurzübersichtsbericht enthält Bereiche mit dynamischen Widgets, die wichtige Performance-Metriken in Bezug auf die Nutzung folgender Cloud-Services durch die Kunden anzeigen: Backup,

Antimalware Protection, Schwachstellenbewertung, Patch-Verwaltung, Data Loss Prevention, Notary Service, Disaster Recovery und File Sync & Share.

Es gibt mehrere Möglichkeiten, wie Sie den Bericht anpassen können.

- Ändern oder löschen Sie Abschnitte.
- Ändern Sie die Reihenfolge von Abschnitten.
- Benennen Sie Abschnitte um.
- Verschieben Sie Widgets von einem Abschnitt zu einem anderen.
- Ändern Sie die Reihenfolge der Widgets in jedem Bereich.
- Fügen Sie Widgets hinzu oder entfernen Sie diese.
- Passen Sie die Widgets an.

Sie können die Kurzübersichtsberichte im PDF- und Excel-Format generieren und diese an die Eigentümer oder andere Projektbeteiligte der Unternehmen Ihrer Kunden senden, damit diese den technischen und geschäftlichen Wert der bereitgestellten Services leichter erkennen können.

Partner-Administratoren können den Kurzübersichtsbericht generieren und nur an Direktkunden senden. Bei komplexeren Mandanten-Hierarchien mit Subpartnern müssen die jeweiligen Subpartner den Bericht generieren.

Kurzübersicht-Widgets

Sie können Bereiche und Widgets im Kurzübersichtsbericht hinzufügen oder entfernen und dadurch bestimmen, welche Informationen im Bericht enthalten sein sollen.

Workloads-Überblick-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Workloads-Überblick**.

Widget	Beschreibung
Cloud-Workloads Schutzstatus	Dieses Widget zeigt die Anzahl der geschützten und ungeschützten Cloud-Workloads nach Typ und zum Zeitpunkt der Berichtserstellung an. Geschützte Cloud-Workloads sind Cloud-Workloads, auf die mindestens ein Backup-Plan angewendet wurde. Ungeschützte Cloud-Workloads sind Cloud-Workloads, auf die (bisher) kein Backup-Plan angewendet wurde. Folgende Cloud-Workload-Typen sind im Diagramm dargestellt (in alphabetischer Reihenfolge von A bis Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange-Postfächer • Microsoft 365-Postfächer

Widget	Beschreibung
	• Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites Für einige Workload-Typen werden folgende Workload-Gruppen verwendet: • Microsoft 365: Benutzer, Gruppen, Öffentliche Ordner, Teams und Website-Sammlungen • Google Workspace: Benutzer und Shared Drives • Hosted Exchange: Benutzer Wenn es in einer Workload-Gruppe mehr als 10.000 Workloads gibt, zeigt das Widget keine Daten für die entsprechenden Workloads an. Wenn der Kunde beispielsweise ein Microsoft 365-Konto mit 10.000 Postfächern sowie je einen OneDrive-Service für 500 Benutzer hat, so gehören diese alle zur Workload-Gruppe 'Benutzer'. Die Summe dieser Workloads beträgt 10.500, wodurch die Begrenzung von 10.000 für eine Workload-Gruppe überschritten wird. Daher wird das Widget die entsprechenden Workload-Typen ausblenden: Microsoft 365-Postfächer und Microsoft 365 OneDrive.
Cyber Protection-Übersicht	Das Widget zeigt die wichtigsten Metriken zur Cyber Protection-Performance für den spezifizierten Zeitraum an. **Gesicherte Daten** – die Gesamtgröße der Archive, die in den lokalen Storages und Cloud Storages und erstellt wurden. **Abgemilderte Bedrohungen** – die Gesamtzahl der Malware, die insgesamt auf allen Geräten blockiert wurden. **Schädliche URLs blockiert** – die Gesamtzahl der blockierten URLs auf allen Geräten. **Gepatchte Schwachstellen** – die Gesamtzahl der Schwachstellen, die durch die Installation von Software-Patches auf allen Geräten behoben wurden. **Installierte Patches** – die Gesamtzahl der Patches, die auf allen Geräten installiert wurden. **Server geschützt durch DR** – die Gesamtzahl der Server, die per Disaster Recovery geschützt werden. **File Sync & Share-Benutzer** – die Gesamtzahl der End- und Gastbenutzer, die die Cyber Files Funktionalität verwenden. **Beglaubigte Dateien** – die Gesamtzahl der beglaubigten Dateien. **Elektronisch signierte Dokumente** – die Gesamtzahl der elektronisch

Widget	Beschreibung
	signierten Dokumente. **Blockierte Peripheriegeräte** – die Gesamtzahl der Peripheriegeräte, auf die der Zugriff blockiert wird.
Workload-Netzwerkstatus	Dieses Widget informiert darüber, wie viele Workloads isoliert sind und wie viele verbunden sind (das normale Stadium des Workloads). Wählen Sie den gewünschten Kunden aus. Die dargestellte Workload-Ansicht wird gefiltert, sodass nur noch isolierte Workloads angezeigt werden. Wenn Sie auf das Element 'Verbunden' klicken, wird die Liste 'Workload mit Agenten' angezeigt, die so gefiltert ist, dass die verbundenen Workloads (für den ausgewählten Kunden) angezeigt werden.
Workloads-Schutzstatus	Das Widget zeigt die geschützten und ungeschützten Workloads nach Typ und zum Zeitpunkt der Berichtserstellung an. Geschützte Workloads sind Workloads, auf die mindestens ein Schutz- oder Backup-Plan angewendet wurde. Ungeschützte Workloads sind Workloads, auf die (bisher) kein Schutz- oder Backup-Plan angewendet wurde. Folgende Workloads werden gezählt: **Server** – physische Server und Domain-Controller-Server. **Workstations** – physische Workstations. **Virtuelle Maschinen** – sowohl agentenbasierte als auch agentenlose virtuelle Maschinen. **Webhosting-Server** – virtueller oder physischer Server, auf denen cPanel oder Plesk installiert ist. **Mobilgeräte** – physische Mobilgeräte (wie Smartphones). Ein Workload kann zu mehreren Kategorien gehören. Ein Webhosting-Server wird beispielsweise zu zwei Kategorien gezählt – **Server** und **Webhosting-Server**.

Antimalware Protection-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Threat Defense**.

Widget	Beschreibung
Antimalware-Scan von Dateien	Das Widget zeigt die Ergebnisse der On-Demand-Antimalware-Scans von den jeweiligen Geräten für den spezifizierten Datumsbereich an. **Dateien** – die Gesamtzahl der gescannten Dateien **Sauber** – die Gesamtzahl der sauberen Dateien **Erkannt, unter Quarantäne gestellt** – die Gesamtzahl der

Widget	Beschreibung
	infizierten Dateien, die unter Quarantäne gestellt wurden **Erkannt, nicht unter Quarantäne gestellt** – die Gesamtzahl der infizierten Dateien, die nicht unter Quarantäne gestellt wurden **Geräte geschützt** – die Gesamtzahl der Geräte, auf die eine Antimalware Protection-Richtlinie angewendet wurde **Gesamtzahl an registrierten Geräten** – Die Gesamtzahl der registrierten Geräte zum Zeitpunkt der Berichtserstellung
Antimalware-Scan von Backups	Das Widget zeigt die Ergebnisse der Antimalware-Scans von Backups für den spezifizierten Datumsbereich an und verwendet dabei folgende Metriken: • Gesamtzahl der gescannten Recovery-Punkte • Anzahl der sauberen Recovery-Punkte • Anzahl der sauberen Recovery-Punkte mit nicht unterstützten Partitionen • Anzahl der infizierten Recovery-Punkte. Diese Metrik beinhaltet die Anzahl der infizierten Recovery-Punkte mit nicht unterstützten Partitionen (Volumes).
Blockierte URLs	Das Widget zeigt für den spezifizierten Datumsbereich die Anzahl der blockierten URLs an, gruppiert nach Website-Kategorie. Das Widget listet die sieben Website-Kategorien mit der größten Anzahl blockierter URLs auf und fasst die übrigen Website-Kategorien unter **Andere(s)** zusammen. Weitere Informationen zu den Website-Kategorien finden Sie unter dem Thema 'URL-Filterung in Cyber Protection'.
Sicherheitsvorfall-Burndown	Dieses Widget zeigt die Effizienzrate bei der Schließung von Vorfällen für die ausgewählte Firma an; die Anzahl der offenen Vorfälle wird dabei mit der Anzahl der geschlossenen Vorfälle über einen bestimmten Zeitraum abgeglichen. Bewegen Sie den Mauszeiger über eine Spalte, um eine Aufschlüsselung der geschlossenen und offenen Vorfälle für den jeweiligen Tag angezeigt zu bekommen. Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.
MTTR (Mittlere Problemlösungszeit) für Vorfälle	Dieses Widget zeigt die durchschnittliche Problemlösungszeit für Sicherheitsvorfälle an. Sie gibt an, wie schnell Vorfälle untersucht und gelöst werden. Klicken Sie auf eine Spalte, um die Vorfälle nach ihrem Schweregrad (**Kritisch**, **Hoch** und **Mittel**) aufzuschlüsseln und zu sehen, wie lange es dauerte, die verschiedenen Schweregrade zu beheben. Der in

Widget	Beschreibung
	Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.
Bedrohungsstatus	Dieses Widget zeigt den aktuellen Bedrohungsstatus für die Workloads einer Firma an (unabhängig von der Anzahl der Workloads) und hebt dabei die aktuelle Anzahl der Vorfälle hervor, die nicht abgeschwächt wurden und die noch untersucht werden müssen. Das Widget gibt auch die Anzahl der Vorfälle an, die (manuell und/oder automatisch vom System) abgeschwächt wurden.
Erkannten Bedrohungen nach Schutztechnologie	Das Widget zeigt für den spezifizierten Datumsbereich die Anzahl der erkannten Bedrohungen an, gruppiert nach folgenden Schutztechnologien: • Antimalware-Scanning • Behavior Engine • Cryptomining Protection • Exploit-Prävention • Ransomware Active Protection • Echtzeitschutz • URL-Filterung

Backup-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Backup**.

Widget	Beschreibung
Workloads gesichert	Das Widget zeigt die Gesamtzahl der registrierten Workloads nach dem jeweiligen Backup-Status an. **Gesichert** – die Anzahl der Workloads, die während des Berichtszeitraums per Backup geschützt wurden (es muss mindestens ein erfolgreiches Backup durchgeführt worden sein). **Nicht gesichert** – die Anzahl der Workloads, die während des Berichtszeitraums nicht per Backup geschützt wurden (es wurde kein erfolgreiches Backup durchgeführt).
Laufwerksintegritätstatus nach physischen Geräten	Das Widget zeigt den aggregierten Integritätstatus von physischen Geräte an, basierend auf den Integritätstatuszuständen von deren Laufwerken. **OK** – Dieser Laufwerksintegritätsstatus bezieht sich auf bestimmte Werte [70-100]. Der Status eines Gerätes ist **OK**, wenn all seine Laufwerke den Status **OK** haben. **Warnung** – Dieser Laufwerksintegritätsstatus bezieht sich auf

Widget	Beschreibung
	bestimmte Werte [30-70]. Der Status eines Gerätes ist **Warnung**, wenn mindestens eines seiner Laufwerke den Status **Warnung** und kein Laufwerk den Status **Fehler** hat. **Fehler** – Dieser Laufwerksintegritätsstatus bezieht sich auf bestimmte Werte [0-30]. Der Status eines Gerätes ist **Fehler**, wenn mindestens eines seiner Laufwerke den Status **Fehler** hat. **Laufwerksdaten werden berechnet** – Der Status eines Gerätes ist **Laufwerksdaten werden berechnet**, wenn die Statuszustände seiner Laufwerke noch nicht berechnet wurden.
Backup Storage-Nutzung	Das Widget zeigt für den spezifizierten Zeitraum die Gesamtzahl und Gesamtgröße der Backups in der Cloud sowie im lokalen Storage an.

Widgets für Schwachstellenbewertung und Patch-Verwaltung

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Schwachstellenbewertung und Patch-Verwaltung**.

Widget	Beschreibung
Gepatchte Schwachstellen	Das Widget zeigt die Performance-Ergebnisse der Schwachstellenbewertung für den spezifizierten Datumsbereich an. **Insgesamt** – die Gesamtzahl der gepatchten Schwachstellen. **Microsoft-Software-Schwachstellen** – die Gesamtzahl der behobenen Microsoft-Schwachstellen auf allen Windows-Geräten. **Schwachstellen in Windows-Software von Drittanbietern** – die Gesamtzahl der behobenen Schwachstellen in Windows-Programmen von Drittanbietern auf allen Windows-Geräten. **Workloads gescannt** – die Gesamtzahl der Geräte, die innerhalb des spezifizierten Datumsbereichs mindestens einmal erfolgreich auf Schwachstellen gescannt wurden.
Patches installiert	Das Widget zeigt die Performance-Ergebnisse der Patch-Verwaltung für den spezifizierten Datumsbereich an. **Installiert** – die Gesamtzahl der Patches, die erfolgreich auf allen Geräten installiert wurden. **Microsoft-Software-Patches** – die Gesamtzahl der Patches für Software-Programme von Microsoft, die auf allen Windows-Geräten installiert wurden.

Widget	Beschreibung
	Patches für Windows-Software von Drittanbietern – die Gesamtzahl der Patches für Software-Programme von Drittanbietern, die auf allen Windows-Geräten installiert wurden. **Workloads gepatcht** – die Gesamtzahl der Geräte, die erfolgreich gepatcht wurden (im spezifizierten Datumsbereich wurde mindestens ein Patch erfolgreich installiert).

Disaster Recovery-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Disaster Recovery**.

Widget	Beschreibung
Disaster Recovery-Statistiken	Das Widget zeigt die wichtigsten Metriken zur Disaster Recovery-Performance für den spezifizierten Datumsbereich an. **Produktions-Failover** – die Anzahl der Produktions-Failover-Aktionen für den spezifizierten Zeitraum. **Test-Failover** – die Gesamtzahl der Test-Failover-Aktionen, die während des spezifizierten Zeitraums durchgeführt wurden. **Primäre Server** – die Gesamtzahl der primären Server zum Zeitpunkt der Berichtserstellung. **Recovery-Server** – die Gesamtzahl der Recovery-Server zum Zeitpunkt der Berichtserstellung. **Öffentliche IPs** – die Gesamtzahl der öffentlichen IP-Adresse (zum Zeitpunkt der Berichtserstellung). **Verbrauchte Berechnungspunkte insgesamt** – die Gesamtzahl der Berechnungspunkte, die während des spezifizierten Zeitraums verbraucht wurden.
Disaster Recovery-Server getestet	Das Widget zeigt Informationen über die Server an, die per Disaster Recovery geschützt werden und per Test-Failover getestet wurden. Das Widget zeigt folgende Metriken an: **Server geschützt** – die Anzahl der per Disaster Recovery geschützten Server (Server, die mindestens einen Recovery-Server haben) zum Zeitpunkt der Berichtserstellung. **Getestet** – die Anzahl der per Disaster Recovery geschützten Server, die während des festgelegten Zeitraums per Test-Failover getestet wurden (von allen per Disaster Recovery geschützten Servern). **Nicht getestet** – die Anzahl der per Disaster Recovery geschützten Server, die während des festgelegten Zeitraums nicht per Test-Failover getestet wurden

Widget	Beschreibung
	(von allen per Disaster Recovery geschützten Servern). Das Widget zeigt auch die Größe des Disaster Recovery Storage (in GB) zum Zeitpunkt der Berichtserstellung an. Dies entspricht der Summe der Backup-Größen der Cloud Server.
Server geschützt mit Disaster Recovery	Das Widget zeigt Informationen über die per Disaster Recovery geschützten Server sowie die ungeschützten Server an. Das Widget zeigt folgende Metriken an: Die Gesamtzahl der im Kunden-Mandanten registrierten Server zum Zeitpunkt der Berichtserstellung. **Geschützt** – die Anzahl der per Disaster Recovery geschützten Server (die mindestens einen Recovery-Server sowie ein Backup des kompletten Servers haben) von allen registrierten Servern und zum Zeitpunkt der Berichtserstellung. **Ungeschützt** – die Gesamtzahl der ungeschützten Server von allen registrierten Servern zum Zeitpunkt der Berichtserstellung.

Data Loss Prevention-Widget

Im nachfolgenden Abschnitt finden Sie weitere Informationen über die blockierten Peripheriegeräte im Bereich **Data Loss Prevention**.

Das Widget zeigt die Gesamtanzahl der blockierten Geräte sowie die Gesamtanzahl der blockierten Geräte an, nach Gerätetyp und für den spezifizierten Datumsbereich.

- Wechselmedien
- Verschlüsseltes Wechsellaufwerk
- Drucker
- Zwischenablage – enthält die Gerätetypen 'Zwischenablage' und 'Screenshot-Aufnahme'.
- Mobilgeräte
- Bluetooth
- Optische Laufwerke
- Diskettenlaufwerke
- USB – enthält die Gerätetypen 'USB-Port' und 'Umgeleiteter USB-Port'.
- FireWire
- Zugeordnete Laufwerke
- Umgeleitete Zwischenablage – enthält die Gerätetypen 'Umgeleitete Zwischenablage eingehend' und 'Umgeleitete Zwischenablage ausgehend'.

Das Widget zeigt die ersten sieben Gerätetypen an, die die höchste Anzahl an blockierten Geräten haben, und fasst die übrigen Gerätetypen unter dem Gerätetyp **Andere(s)** zusammen.

File Sync & Share-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **File Sync & Share**.

Widget	Beschreibung
File Sync & Share-Statistiken	Das Widget zeigt folgende Metriken an: **Verwendeter Cloud Storage insgesamt** – Die gesamte Storage-Nutzung aller Benutzer. **Endbenutzer** – die Gesamtzahl der Endbenutzer. **Durchschnittliche Storage-Nutzung pro Benutzer** – die durchschnittliche Storage-Nutzung pro Endbenutzer. **Gastbenutzer** – die Gesamtzahl der Gastbenutzer.
File Sync & Share-Storage-Nutzung durch Endbenutzer	Das Widget zeigt die Gesamtzahl der File Sync & Share-Endbenutzer an, die eine Storage-Nutzung in folgenden Bereichen haben: • 0–1 GB • 1–5 GB • 5–10 GB • 10–50 GB • 50–100 GB • 100–500 GB • 500 GB – 1 TB • Mehr als 1 TB

Notary-Widgets

In der nachfolgenden Tabelle finden Sie weitere Informationen zu den Widgets im Bereich **Notary**.

Widget	Beschreibung
Cyber Notary-Statistiken	Das Widget zeigt folgende Notary-Metriken an: **Notary Cloud Storage verwendet** – die Gesamtgröße des Storage, der für Notary Services verwendet wird. **Beglaubigte Dateien** – die Gesamtzahl der beglaubigten Dateien. **Elektronisch signierte Dokumente** – die Gesamtzahl der elektronisch signierten Dokumente und Dateien.
Beglaubigte	Zeigt die Gesamtzahl der beglaubigten Dateien für alle Endbenutzer

Widget	Beschreibung
Dateien über alle Endbenutzer hinweg	an. Die Benutzer werden nach der Anzahl der beglaubigten Dateien gruppiert, die diese haben. • Bis zu 10 Dateien • 11–100 Dateien • 101–500 Dateien • 501–1000 Dateien • Mehr als 1000 Dateien
Elektronisch signierte Dokumente über alle Endbenutzer hinweg an	Das Widget zeigt die Gesamtzahl der elektronisch signierten Dokumente und Dateien für alle Endbenutzer an. Die Benutzer werden nach der Anzahl der elektronisch signierten Dokumente und Dateien gruppiert, die diese haben. • Bis zu 10 Dateien • 11–100 Dateien • 101–500 Dateien • 501–1000 Dateien • Mehr als 1000 Dateien

Die Einstellungen des Kurzübersichtsberichts konfigurieren

Sie können die Berichtseinstellungen aktualisieren, die beim Erstellen des Kurzübersichtsberichts konfiguriert wurden.

So können Sie die Einstellungen des Kurzübersichtsberichts aktualisieren

1. Gehen Sie in der Management-Konsole zu **Berichte** –> **Kurzübersicht**.
2. Klicken Sie auf den Namen des Kurzübersichtsberichts, den Sie aktualisieren wollen.
3. Klicken Sie auf **Einstellungen**.
4. Ändern Sie die Werte der Felder nach Bedarf.
5. Klicken Sie auf **Speichern**.

Einen Kurzübersichtsbericht erstellen

Sie können einen Kurzübersichtsbericht erstellen, eine Vorschau seiner Inhalte anzeigen, die Empfänger des Berichts konfigurieren und den Zeitpunkt für den automatischen Versand planen.

So können Sie einen Kurzübersichtsbericht erstellen

1. Gehen Sie in der Management-Konsole zu **Berichte** –> **Kurzübersicht**.
2. Klicken Sie auf **Kurzübersichtsbericht erstellen**.
3. Geben Sie bei **Berichtsname** eine Bezeichnung für den Bericht ein.
4. Bestimmen Sie die Empfänger des Berichts.

- Wenn Sie den Bericht an alle Direktkunden senden wollen, wählen Sie **An alle Direktkunden senden** aus.
- Wenn Sie den Bericht an bestimmte Kunden senden wollen
  a. Deaktivieren Sie die Auswahl **An alle Direktkunden senden**.
  b. Klicken Sie auf **Kontakte wählen**.
  c. Wählen Sie die gewünschten Kunden aus. Sie können die Suchfunktion verwenden, um bestimmte Kontakte leichter zu finden.
  d. Klicken Sie auf **Auswählen**.

5. Wählen Sie den Bereich: **30 Tage** oder **Dieser Monat**
6. Bestimmen Sie das Dateiformat: **PDF**, **Excel** oder **Excel und PDF**.
7. Konfigurieren Sie die Planungseinstellungen.
   - Wenn Sie den Bericht an einem bestimmten Datum und zu einer bestimmten Uhrzeit an die Empfänger senden wollen:
     a. Aktivieren Sie die Option **Geplant**.
     b. Klicken Sie auf das Feld **Tag des Monats**, deaktivieren Sie das Feld 'Letzter Tag' und klicken Sie auf das Datum, das Sie festlegen wollen.
     c. Geben Sie im Feld **Zeit** die Stunde an, die Sie festlegen wollen.
     d. Klicken Sie auf **Anwenden**.
   - Wenn Sie den Bericht nur erstellen wollen, ohne ihn an die Empfänger zu senden, müssen Sie die Option **Geplant** deaktivieren.
8. Klicken Sie auf **Speichern**.

Den Kurzübersichtsbericht anpassen

Sie können bestimmen, welche Informationen in den Kurzübersichtsbericht aufgenommen werden sollen. Sie können Abschnitte hinzufügen oder löschen, Widgets hinzufügen oder löschen, Abschnitte umbenennen, Widgets anpassen sowie Widgets und Abschnitte per Drag & Drop verschieben, um die Reihenfolge zu ändern, in der die Informationen im Bericht erscheinen.

So können Sie einen Abschnitt hinzufügen

1. Klicken Sie auf **Element hinzufügen** –> **Abschnitt hinzufügen**.
2. Geben Sie im Fenster **Abschnitt hinzufügen** einen Namen für den Abschnitt ein oder verwenden Sie den vorgegebenen Abschnittsnamen.
3. Klicken Sie auf **Zu Bericht hinzufügen**.

So können Sie einen Abschnitt umbenennen

1. Klicken Sie in dem Abschnitt, den Sie umbenennen wollen, auf den Befehl **Bearbeiten**.
2. Geben Sie im Fenster **Abschnitt bearbeiten** den neuen Namen ein.
3. Klicken Sie auf **Speichern**.

So können Sie einen Abschnitt löschen

1. Klicken Sie in dem Abschnitt, den Sie löschen wollen, auf den Befehl **Abschnitt löschen**.
2. Klicken Sie im Bestätigungsfenster **Abschnitt löschen** auf **Löschen**.

So können Sie ein Widget mit Standardeinstellungen zu einem Abschnitt hinzufügen

1. Klicken Sie in dem Abschnitt, in dem Sie das Widget einfügen wollen, auf den Befehl **Widget hinzufügen**.
2. Klicken Sie im Fenster **Widget hinzufügen** auf dasjenige Widget, welches Sie hinzufügen wollen.

So können Sie ein benutzerdefiniertes Widget zu einem Abschnitt hinzufügen

1. Klicken Sie in dem Abschnitt, in dem Sie das Widget einfügen wollen, auf den Befehl **Widget hinzufügen**.
2. Suchen Sie im Fenster **Widget hinzufügen** das Widget, welches Sie hinzufügen wollen, und klicken Sie dann auf **Anpassen**.
3. Konfigurieren Sie die Felder nach Bedarf.
4. Klicken Sie auf **Widget hinzufügen**.

So können Sie ein Widget mit Standardeinstellungen dem Bericht hinzufügen

1. Klicken Sie auf **Element hinzufügen** –> **Widget hinzufügen**.
2. Klicken Sie im Fenster **Widget hinzufügen** auf dasjenige Widget, welches Sie hinzufügen wollen.

So können Sie ein benutzerdefiniertes Widget dem Bericht hinzufügen

1. Klicken Sie auf **Widget hinzufügen**.
2. Suchen Sie im Fenster **Widget hinzufügen** das Widget, welches Sie hinzufügen wollen, und klicken Sie dann auf **Anpassen**.
3. Konfigurieren Sie die Felder nach Bedarf.
4. Klicken Sie auf **Widget hinzufügen**.

So können Sie die Standardeinstellungen eines Widgets zurücksetzen

1. Klicken Sie in dem anzupassenden Widget auf den Befehl **Bearbeiten**.
2. Klicken Sie auf **Auf Standard zurücksetzen**.
3. Klicken Sie auf **Fertig**.

So können Sie ein Widget anpassen

1. Klicken Sie in dem anzupassenden Widget auf den Befehl **Bearbeiten**.
2. Bearbeiten Sie die Felder nach Ihrem Bedarf.
3. Klicken Sie auf **Fertig**.

Kurzübersichtsberichte senden

Sie können einen Kurzübersichtsbericht auch manuell nach Bedarf versenden. In diesem Fall wird die Einstellung **Geplant** ignoriert und der Bericht umgehend versendet. Beim Versenden des Berichts wird das System auf die Werte für Empfänger, Bereich und Dateiformat zurückgreifen, die in den entsprechenden **Einstellungen** konfiguriert wurden. Sie können diese Einstellungen vor dem Versenden des Berichts aber noch manuell ändern. Weitere Informationen finden Sie im Abschnitt '"Die Einstellungen des Kurzübersichtsberichts konfigurieren" (S. 147)'.

So können Sie einen Kurzübersichtsbericht senden

1. Gehen Sie im Management-Portal zu **Berichte** –> **Kurzübersicht**.
2. Klicken Sie auf den Namen des Kurzübersichtsberichts, den Sie versenden wollen.
3. Klicken Sie auf **Jetzt senden**.
   Das System wird den Kurzübersichtsbericht an die ausgewählten Empfänger senden.

Zeitzonen in Berichten

Die Zeitzonen, die in Berichten verwendet werden, hängen vom jeweiligen Berichtstyp ab. Die Informationen in der nachfolgenden Tabelle sollen Ihnen als Referenz dienen.

Berichtsort und -typ	Im Bericht verwendete Zeitzone
Management-Portal –> Überblick –> Aktionen (Widgets)	Die Zeit der Berichtserstellung entspricht der Zeitzone der Maschine, auf welcher der Webbrowser ausgeführt wird.
Management-Portal –> Überblick –> Aktionen (als PDF oder XSLX exportiert)	• Der Zeitstempel des exportierten Berichts entspricht der Zeitzone der Maschine, die zum Exportieren des Berichts verwendet wurde. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Berichte –> Nutzung –> Geplante Berichte	• Der Bericht wird um 23:59:59 UTC am ersten Tag des Monats erstellt. • Der Bericht wird am zweiten Tag des Monats gesendet.
Management-Portal –> Berichte –> Nutzung –> Benutzerdefinierte Berichte	Die Zeitzone und das Datum des Berichts ist UTC.
Management-Portal –> Berichte –> Aktionen	• Die Zeit der Berichtserstellung entspricht der Zeitzone der Maschine, auf welcher der Webbrowser ausgeführt wird. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.

(Widgets)	
Management-Portal –> Berichte –> Aktionen (als PDF oder XSLX exportiert)	• Der Zeitstempel des exportierten Berichts entspricht der Zeitzone der Maschine, die zum Exportieren des Berichts verwendet wurde. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Berichte –> Aktionen (geplante Übermittlung)	• Die Zeitzone und die Berichtsübermittlung ist UTC. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Benutzer –> Tägliche Zusammenfassung über aktive Alarmmeldungen	• Der Bericht wird einmal am Tag zwischen 10:00 und 23:59 UTC gesendet. Der genaue Zeitpunkt der Berichtsübermittlung hängt vom Workload im Datacenter ab. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal –> Benutzer –> Cyber Protection-Status-Benachrichtigungen	• Der Bericht wird gesendet, wenn eine Aktivität abgeschlossen wurde. **Hinweis** In Abhängigkeit vom Workload des Datacenters können einige Berichte verzögert gesendet werden. • Die Zeitzone der im Aktivität im Bericht ist UTC.

Berichtsdaten je nach Widget-Typ

Je nach dem Datenbereich, den sie anzeigen, gibt es zwei Arten von Widgets auf dem Dashboard:

- Widgets, die aktuelle Daten für den Zeitpunkt des Durchsuchens oder der Berichtserstellung anzeigen.
- Widgets, die historische Daten anzeigen.

Wenn Sie in den Berichtseinstellungen einen Datumsbereich konfigurieren, um Daten für einen bestimmten Zeitraum auszugeben, gilt der gewählte Zeitraum nur für Widgets, die historische Daten anzeigen. Für Widgets, die aktuelle Daten für den Zeitpunkt des Durchsuchens anzeigen, ist der Parameter Zeitraum nicht anwendbar.

Die nachfolgende Tabelle führt die verfügbaren Widgets und deren Datenbereiche auf.

Widget-Name	Daten, die im Widget und in Berichten angezeigt werden
#CyberFit-Score pro Maschine	Aktuell
5 neueste Alarmmeldungen	Aktuell
Details zu aktiven Alarmmeldungen	Aktuell
Aktive Alarmmeldungen – Übersicht	Aktuell

Aktivitäten	Historisch
Aktivitätsliste	Historisch
Alarmverlauf	Historisch
Antimalware-Scan von Backups	Historisch
Antimalware-Scan von Dateien	Historisch
Backup-Scanning-Details (Bedrohungen)	Historisch
Backup-Status	Historisch – in den Spalten **Ausführungen insgesamt** und **Anzahl erfolgreiche Ausführungen** Aktuell – in allen anderen Spalten
Backup Storage-Nutzung	Historisch
Blockierte Peripheriegeräte	Historisch
Blockierte URLs	Aktuell
Cloud-Applikationen	Aktuell
Cloud-Workloads Schutzstatus	Aktuell
Cyber protection	Aktuell
Cyber Protection-Übersicht	Historisch
Data Protection-Karte	Historisch
Geräte	Aktuell
Disaster Recovery-Server getestet	Historisch
Disaster Recovery-Statistiken	Historisch
Erkannte Maschinen	Aktuell
Überblick der Laufwerksintegrität	Aktuell
Laufwerksintegritätsstatus	Aktuell
Laufwerksintegritätstatus nach physischen Geräten	Aktuell
Elektronisch signierte Dokumente über alle Endbenutzer hinweg an	Aktuell
Vorhandene Schwachstellen	Historisch
File Sync & Share-Statistiken	Aktuell
File Sync & Share-Storage-Nutzung durch Endbenutzer	Aktuell

Hardware-Änderungen	Historisch
Hardware-Details	Aktuell
Hardware-Inventarisierung	Aktuell
Übersicht der historischen Alarmmeldungen	Historisch
Speicherorteübersicht	Aktuell
Fehlende Updates nach Kategorie	Aktuell
Nicht geschützt	Aktuell
Beglaubigte Dateien über alle Endbenutzer hinweg	Aktuell
Notary-Statistiken	Aktuell
Verlauf der Patch-Installation	Historisch
Status der Patch-Installation	Historisch
Übersicht der Patch-Installation	Historisch
Gepatchte Schwachstellen	Historisch
Patches installiert	Historisch
Schutzstatus	Aktuell
Kürzlich betroffen	Historisch
Remote-Sitzungen	Historisch
Sicherheitsvorfall-Burndown	Historisch
Sicherheitsvorfall-MTTR (Mittlere Problemlösungszeit)	Historisch
Server geschützt mit Disaster Recovery	Aktuell
Software-Inventarisierung	Aktuell
Software-Überblick	Historisch
Bedrohungsstatus	Aktuell
Erkannten Bedrohungen nach Schutztechnologie	Historisch
Spitzenverteilung der Vorfälle pro Workload	Aktuell
Verwundbare Maschinen	Aktuell

Workload-Netzwerkstatus	Aktuell
Workloads gesichert	Historisch
Workloads-Schutzstatus	Aktuell

Die Cyber Protect Cloud-Kosten mit dem Calculator veranschlagen

Wenn Sie eine Testversion von Cyber Protect Cloud verwenden, können Sie Ihre Kosten mit dem Calculator schätzen.

Hinweis
Der Cyber Protect Cloud Calculator ist nur für Testpartner über das Management-Portal zugänglich und nicht für deren Kunden oder Nicht-Testpartner.

So können Sie die Cyber Protect Cloud-Kosten mit dem Calculator veranschlagen

1. Klicken Sie in der linken unteren Ecke des Management-Portals auf **Monatliche Kosten berechnen**.
2. Spezifizieren Sie folgende Details für Ihre geplante Belastung:
   - Die Anzahl Ihrer Workloads nach Workload-Typ. Spezifizieren Sie beispielsweise die Anzahl der virtuellen Maschinen, Workstations, Hosting-Server, Google Workplace-Arbeitsplätze, Mobilgeräte und Microsoft 365-Arbeitsplätze.
   - Die Details Ihres Datenspeichers, wie z.B. der Standort Ihres Datacenters sowie die Speichermenge.
3. [Optional] Spezifizieren Sie die Advanced Backup-, Advanced Security- oder Advanced Management-Optionen, die Sie verwenden wollen, sowie die Anzahl der Workloads für jede von diesen.
4. Wählen Sie ein Lizenzierungsmodell: pro Workload oder pro GB.

Auf der rechten Seite werden Ihnen die geschätzten monatlichen Kosten angezeigt.

Sie können Partner werden, indem Sie auf die entsprechende Schaltfläche klicken, einen Chat mit einem Spezialisten führen oder einen Cloud Advisor anfordern, der Sie direkt kontaktiert – alles von der alculator-Seite aus.

Sie können sich auch direkt an die Vertriebsabteilung wenden, indem Sie in der linken unteren Ecke des Management-Portals auf **Vertrieb kontaktieren** klicken.

Das Partner Portal verwenden

Das Partner Portal ist für Service-Provider, Distributoren und Reseller gedacht, die am #CyberFit Partner-Program teilnehmen.

Über das Partner Portal können Sie auf Inhalte, Tools und Schulungen von zugreifen.

So können Sie das Partner Portal verwenden

1. Greifen Sie auf eine der folgenden Arten auf das Partner Portal zu:
   - Klicken Sie in der linken unteren Ecke des Management-Portals auf **Partner werden**.
   - Besuchen Sie die Partner Portal-Website.
2. Registrieren Sie Ihre Firma im Partner-Programm.
3. Sie erhalten die Zugangsdaten per E-Mail.

Partner Portal-Rollen

Das Partner Portal enthält eine Reihe von Rollen, die Sie nach Bedarf auf Ihre Benutzer anwenden können.

In der nachfolgenden Tabelle werden die verfügbaren Rollen sowie die Rechte beschrieben, die den einzelnen Rollen innerhalb des Partner Portals zugewiesen sind:

Rolle	Beschreibung
Basis	Die Standardrolle, die allen Benutzern zugewiesen wird. Diese Rolle ermöglicht den Zugriff auf wesentliche Funktionalitäten des Partner Portals (wie das Dashboard, das Partner-Programm, den Content Hub, Training und den Support).
Training	Benutzer mit dieser Rolle können auf Schulungsunterlagen zugreifen. Andere Funktionen des Partner Portals sind für diese Benutzer nicht verfügbar.
Marketing	Diese Rolle gewährt Zugriff auf Funktionalitäten des Partner-Portals, die Marketingspezialisten benötigen – wie das Dashboard, das Partner-Programm, Marketing- und Schulungsmaterialien, den Content Hub, den Support, den Datacenter-Status und die Datenbank-Verwaltung.
Verkauf	Diese Rolle gewährt Zugriff auf Funktionalitäten des Partner-Portals, die Marketingspezialisten benötigen – wie das Dashboard, das Partner-Programm, Marketing- und Schulungsmaterialien, den Content Hub, den Support, den Datacenter-Status und die Datenbank-Verwaltung.
Vertrieb und Marketing	Diese Rolle gewährt Zugriff auf Funktionalitäten des Partner-Portals, die einheitliche Vertriebs- und Marketingspezialisten benötigen – wie das Dashboard, das Partner-Programm, Vertriebs-, Marketing- und Schulungsmaterialien, den Content Hub, den Support, den Datacenter-Status und die Datenbank-Verwaltung.

Rolle	Beschreibung
Administrator	Administratoren haben Zugriff auf alle Funktionalitäten des Partner-Portals – wie das Dashboard, das Partner-Programm, Vertriebs-, Marketing- und Schulungsmaterialien, den Content Hub, den Support, den Datacenter-Status und die Datenbank-Verwaltung. Administratoren können außerdem Berechtigungen für Partner-Benutzer verwalten sowie Firmeninformationen ändern.

Das Vendor Portal verwenden

Das Vendor Portal (CyberApp Standard) ist eine Plattform, über die Software-Drittanbietern ihre Produkte und Services in Cyber Protect Cloud integrieren können.

Mit dem Vendor Portal können Sie Folgendes tun:

- Erhalten Sie Zugriff auf die Acronis Sandbox-Umgebung für Entwicklungen und Tests.
- Lassen Sie Ihre Lösungen in den Acronis Applikationskatalog aufnehmen.
- Integrieren Sie Workloads, Warnmeldungen, Widgets und Berichte in die Cyber Protect Cloud-Konsole.
- Die Sicherheit Ihrer Daten durch Maßnahmen gewährleisten, die üblichen Industriestandards entsprechen.

So können Sie das Vendor Portal verwenden

1. Registrieren Sie sich auf der Acronis Technology Ecosystem-Website.
2. Aktivieren Sie Ihr Konto.

Advanced Protection-Pakete

Die Advanced Protection-Pakete können zusätzlich zum Schutz Service aktiviert werden und sind aufpreispflichtig. Die Advanced Protection-Pakete bieten jeweils eine spezifische Funktionalität, die sich weder mit dem Standard-Funktionssatz noch mit anderen Advanced-Paketen überschneidet. Kunden können ihre Workloads mit einem, mehreren oder allen Advanced-Paketen schützen. Die Advanced Protection-Pakete sind für beide Abrechnungsmodi ('pro Gigabyte' und 'pro Workload') des Schutz Service verfügbar.

Die Advanced File Sync & Share-Funktionen können mit dem File Sync & Share Service aktiviert werden. Es ist in beiden Abrechnungsmodi verfügbar – pro Benutzer und pro Gigabyte.

Sie können folgende Advanced Protection-Pakete aktivieren:

- Advanced Backup

  Das Advanced Backup-Paket enthält eine Reihe von separaten Lizenzen und Quotas für Workstations, Server, virtuelle Maschinen, Webhosting-Server, Google Workspace-Arbeitsplätze und Microsoft 365-Arbeitsplätze.
- Advanced Management
- Advanced Security + EDR (Endpoint Detection & Response)
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share

Hinweis
Advanced-Pakete können nur verwendet werden, wenn die Standard-Funktion, die sie erweitern, aktiviert ist. Die Anwender können also keine Advanced-Funktionen verwenden, wenn die entsprechende Standard-Service-Funktion deaktiviert ist. Zum Beispiel können Anwender die Funktionen des Advanced Backup-Pakets nicht nutzen, wenn die Schutz-Funktion deaktiviert ist.

Wenn ein Advanced Protection-Paket aktiviert ist, werden dessen Funktionen im Schutzplan angezeigt und sind am Advanced-Funktionssymbol  zu erkennen. Wenn Anwender versuchen, die Funktion zu aktivieren, werden sie darauf hingewiesen, dass zusätzliche Gebühren anfallen.

Wenn ein Advanced Protection-Packet nicht aktiviert ist, aber die Upselling-Option eingeschaltet ist, werden die Advanced Protection-Funktionen im Schutzplan angezeigt, sind jedoch für die Nutzung unzugänglich. Eine Nachricht fordert die Benutzer auf, ihren Administrator zu kontaktieren, um das erforderliche erweiterte Funktionssatz zu aktivieren.

Wenn ein Advanced Protection-Paket nicht aktiviert ist und die Upselling-Option ausgeschaltet ist, wird den Kunden keine Advanced-Funktion in ihren Schutzplänen angezeigt.

In den Cyber Protect Services enthaltene Funktionen und Advanced-Pakete

Wenn Sie einen Service oder Funktionssatz in Cyber Protect aktivieren, wird eine Reihe von Funktionen aktiviert, die standardmäßig enthalten und verfügbar sind. Darüber hinaus können Sie bestimmte Advanced Protection-Pakete aktivieren.

Die nachfolgenden Abschnitte enthalten eine ausführliche Übersicht über die Cyber Protect Service-Funktionen und Advanced-Pakete. Eine vollständige Liste der Angebote finden Sie in der 'Anleitung zur Cyber Protect-Lizenzierung'.

Enthaltene Standard-Funktionen und verfügbare Advanced-Funktionen im Protection Service

Enthaltene Standard-Funktionen und verfügbare Advanced-Funktionen im Protection Service

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
Security + EDR	• #CyberFit-Score • Schwachstellenbewertung • Anti-Ransomware Protection: Active Protection • Antivirus & Antimalware Protection: Cloud-Signaturen-basierte Dateierkennung (kein Echtzeitschutz, nur planbares Scannen)* • Antivirus & Antimalware Protection: KI-basierte Analyse von Dateien vor deren Ausführung, verhaltensbasierte Cyber Engine • Microsoft Defender-Verwaltung *Um Zero-Day-Angriffe zu erkennen; Cyber Protect verwendet heuristische Scan-Regeln und Algorithmen, um nach gefährlichen Software-Befehlen zu suchen.	Das Advanced Security + EDR-Paket beinhaltet: • Verwalten Sie Vorfälle auf einer zentralen Vorfallsseite • Visualisieren Sie das Ausmaß und die Auswirkungen von Vorfällen • Empfehlungen und Behebungsmaßnahmen • Überprüfen Sie anhand von Bedrohungsfeeds, ob es öffentlich bekannte Angriffe auf Ihre Workloads gibt • Speichern Sie Sicherheitsereignisse für 180 Tage • Managed Detection & Response (MDR) • Antivirus & Antimalware Protection mit lokaler signaturbasierter Erkennung (mit Echtzeitschutz) • Exploit-Prävention • URL-Filterung • Endpunkt-Firewall-Verwaltung • Forensik-Backup, Backups nach Malware scannen, Safe Recovery-Funktionalität, Positivliste für Unternehmensapplikationen

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
		• Intelligente Schutzpläne (Integration von CPOC-Alarmmeldungen) • Zentrales Backup-Scanning nach Malware • Remote-Löschung • Microsoft Defender Antivirus • Microsoft Security Essentials Weitere Informationen zur Aktivierung von Advanced Security + EDR finden Sie unter "Advanced Security + EDR aktivieren" (S. 164).
Data Loss Prevention	• Gerätekontrolle	• Inhaltssensitiver Schutz vor dem unautorisierten Abfließen von Daten aus Workloads über Peripheriegeräte und Netzwerk-Kommunikation • Vorgefertigte automatische Erkennung von personenbezogenen Informationen (PII), geschützten Gesundheitsinformationen (PHI) und PCI DSS-Daten (Payment Card Industry Data Security Standard, Kreditkartenindustrie-Datensicherheitsstandard) sowie von Dokumenten der Kategorie 'Als vertraulich gekennzeichnet' • Automatische Erstellung von Data Loss Prevention-Richtlinien mit optionaler Unterstützung durch den Endbenutzer • Adaptive Erzwingung der Data Loss Prevention-Richtlinie mit einer automatischen, lernfähigen Richtlinien-Anpassung • Cloud-basierte zentrale Überwachungsprotokolle, Alarmmeldungen und Endbenutzer-Benachrichtigungen
Verwaltung	• Gruppenverwaltung von Workloads • Zentrale Verwaltung von Schutzplänen • Hardware-Inventarisierung • Remote-Steuerung	• Patch-Verwaltung • Laufwerksintegrität • Software-Inventarisierung • Ausfallsicheres Patching • Cyber Scripting

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
	• Remote-Aktionen • Gleichzeitige Verbindungen pro Techniker • Remote-Verbindungsprotokoll: RDP • Vier Monitore • Grenzwert-basiertes Monitoring	• Remote-Unterstützung • Dateiübertragung und -freigabe • Eine Sitzung zum Verbinden auswählen • Workloads in der Mehrfachansicht beobachten • Verbindungsmodi: Steuerung, Nur-Anzeigen und Vorhang • Verbindung über die Quick Assist-Applikation • Remote-Verbindungsprotokolle: NEAR und Apple Bildschirmfreigabe • Sitzungsaufzeichnung für NEAR-Verbindungen • Screenshot-Übertragung • Sitzungsverlaufsbericht • 24 Monitore • Grenzwert-basiertes Monitoring • Anomalie-basiertes Monitoring
E-Mail-Sicherheit	Ohne	Echtzeitschutz für Ihre Microsoft 365- und Gmail-Postfächer: • Antimalware Antispam • Scannen von URLs in E-Mails • DMARC-Analyse • Antiphishing • Impersonation Protection • Scannen von Anhängen • Content Disarm & Reconstruction (CDR) • Vertrauensgraph Siehe die Konfigurationsanleitung.
Cyber Disaster Recovery Cloud	Sie können die Disaster Recovery-Standard-Funktionen verwenden, um Disaster Recovery-Szenarien für Ihre Workloads zu testen. Beachten Sie, welche Disaster Recovery-Standardfunktionen verfügbar sind und welche Einschränkungen es gibt: • Test-Failover in einer isolierten Netzwerkumgebung. Begrenzt auf 32	Sie können das Advanced Disaster Recovery-Paket aktivieren und Ihre Workloads mit der kompletten Disaster Recovery-Funktionalität schützen. Beachten Sie, welche erweiterten Disaster Recovery-Funktionen verfügbar sind: • Produktions-Failover • Test-Failover in einer isolierten

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
	Berechnungspunkte pro Monat und bis zu 5 Test-Failover-Aktionen zur gleichen Zeit. • Recovery-Server-Konfigurationen: 1 CPU und 2 GB RAM, 1 CPU und 4 GB RAM sowie 2 CPU und 8 GB RAM. • Für Failover verfügbare Anzahl von Recovery-Punkten: nur der letzte Recovery-Punkt, der direkt nach einem Backup verfügbar ist. • Verfügbare Verbindungsmodi: Nur Cloud und Point-to-Site. • Verfügbarkeit des VPN-Gateways: Das VPN-Gateway wird temporär angehalten, wenn es 4 Stunden nach Abschluss des letzten Test-Failover inaktiv ist – und wird wieder bereitgestellt, wenn Sie einen Test-Failover starten. • Anzahl der Cloud-Netzwerke: 1. • Internetzugriff • Aktionen mit Runbooks: erstellen und bearbeiten.	Netzwerkumgebung. • Für Failover verfügbare Anzahl von Recovery-Punkten: alle Recovery-Punkte, die nach Erstellung des Recovery-Servers verfügbar sind. • Primäre Server • Konfigurationen für Recovery-Server/primäre Server: Keine Beschränkungen • Verfügbare Verbindungsmodi: Nur Cloud, Point-to-Site, Site-to-Site-OpenVPN und Multi-Site-IPsec-VPN. • Verfügbarkeit des VPN-Gateways: immer verfügbar. • Anzahl der Cloud-Netzwerke: 23. • Öffentliche IP-Adressen • Internetzugriff • Aktionen mit Runbooks: erstellen, bearbeiten und ausführen.

Pay-as-you-go- und Advanced-Funktionen im Protection Service

Pay-as-you-go- und Advanced-Funktionen im Protection Service

Funktionsgruppe	Pay-as-you-go-Funktionen	Advanced-Funktionen
Backup	• Datei-Backup • Image-Backup • Backup von Applikationen • Backup von Netzwerkfreigaben • Backups zum Cloud Storage • Backups zu einem lokalen Storage **Hinweis** Für die Cloud Storage-Nutzung fallen Gebühren an.	• One-Click Recovery • Kontinuierliche Datensicherung (CDP) • Backup support for Microsoft SQL Server clusters and Microsoft Exchange clusters – AlwaysOn-Verfügbarkeitsgruppen (AAG) und Datenbankverfügbarkeitsgruppen (DAG) • Backup-Unterstützung für MariaDB, MySQL, Oracle DB und SAP HANA • Data Protection-Karte und Compliance-Berichterstattung • Off-Host Data Processing • Backup-Häufigkeit für Microsoft 365-

Funktionsgruppe	Pay-as-you-go-Funktionen	Advanced-Funktionen
		und Google Workspace-Workloads • Remote-Aktionen mit einem Boot-Medium • Direktes Backup in den Microsoft Azure Public Cloud Storage
File Sync & Share	• Verschlüsselte dateibasierte Inhalte speichern • Dateien zwischen festgelegten Geräten synchronisieren • Dateien und Ordner mit festgelegten Personen und Systemen teilen	• Beglaubigung und E-Signaturen • Dokumentvorlagen* *Backup von synchronisierten und freigegebenen Dateien
Physischer Datenversand	Die Funktionalität 'Physischer Datenversand'	Nicht verfügbar
Notary	• Digitale Beglaubigung von Dateien (File Notarization) • Elektronisches Signieren von Dateien (File eSigning) • Dokumentvorlagen	Nicht verfügbar

Hinweis
Sie können keine Advanced Protection-Pakete aktivieren, ohne die entsprechende Standard Protection-Funktion zu aktivieren, die damit erweitert werden soll. Wenn Sie eine Funktion deaktivieren, werden auch deren Advanced-Pakete automatisch deaktiviert – und die Schutzpläne, die diese verwenden, werden automatisch widerrufen. Wenn Sie beispielsweise die Schutzfunktion deaktivieren, werden die dazugehörigen Advanced-Pakete automatisch deaktiviert und alle Pläne widerrufen, die diese verwenden.

Anwender können also keine Advanced Protection-Pakete ohne die Standard Protection verwenden, sondern müssen die integrierte Standard Protection-Funktionen zusammen mit den Advanced-Paketen für bestimmte Workloads einsetzen. In diesem Fall werden ihnen jedoch nur die Advanced-Pakete berechnet, die jeweils verwendet werden.

Weitere Informationen über Abrechnungen finden Sie im Abschnitt '"Abrechnungsmodi für Cyber Protect" (S. 8)'.

Advanced Data Loss Prevention

Das Advanced Data Loss Prevention-Modul verhindert das Durchsickern sensibler Informationen von Workstations, Servern und virtuellen Maschinen, indem es die Inhalte von Daten untersucht, die über lokale Kanäle und Netzwerkverbindungen übertragen werden, und indem es unternehmensspezifische Datenfluss-Richtlinien anwendet.

Bevor Sie das Advanced Data Loss Prevention-Modul erstmalig einsetzen, sollten Sie sich vergewissern, dass Sie die grundlegenden Konzepte und Logik der Advanced Data Loss Prevention-Verwaltung gelesen und verstanden haben, wie sie in der Grundlagen-Anleitung beschrieben sind.

Sie können zudem auch noch das Dokument zu den Technische Spezifikationen studieren.

Advanced Data Loss Prevention aktivieren

Die Advanced Data Loss Prevention-Funktionalität ist standardmäßig in der Konfiguration für neue Mandanten aktiviert. Wenn die Funktionalität während des Prozesses zum Erstellen des Mandanten deaktiviert wurde, kann sie von den Partner-Administratoren nachträglich wieder aktiviert werden.

So können Sie die Advanced Data Loss Prevention-Funktionalität aktivieren

1. Gehen Sie in der Management-Konsole von Cyber Protect Cloud zu **Clients**.
2. Wählen Sie den Mandanten aus, der bearbeitet werden soll.
3. Wählen Sie im Bereich **Services auswählen** die Option **Schutz** und wählen Sie anschließend unter dem anzuwendenden Abrechnungsmodus die Option **Advanced Data Loss Prevention**.
4. Scrollen Sie unter 'Services konfigurieren' zu **Advanced Data Loss Prevention** und konfigurieren Sie die Quotas.
   Die Quota ist standardmäßig auf unbegrenzt eingestellt.
5. Speichern Sie Ihre Einstellungen.

Advanced Security + EDR

Die Endpoint Detection & Response (EDR)-Funktionalität kann verdächtige Aktivitäten auf Workloads (einschließlich Angriffe, die unbemerkt geblieben sind) erkennen und entsprechende Vorfälle generieren. Diese Vorfälle liefern einen schrittweisen Überblick über jeden Angriff und helfen Ihnen so zu verstehen, wie es zu einem Angriff gekommen ist und wie Sie verhindern können, dass dieser erneut stattfindet. Dank der leicht verständlichen Interpretationen der einzelnen Angriffsstadien kann der Zeitaufwand für Angriffsuntersuchungen auf einige Minuten reduziert werden.

Advanced Security + EDR aktivieren

Als Partner-Administrator können Sie das Protection-Paket 'Advanced Security + EDR' aktivieren, um in den Schutzplänen der Kunden die Endpoint Detection & Response (EDR)-Funktionalität bereitzustellen.

So können Sie das Advanced Security + EDR-Paket aktivieren

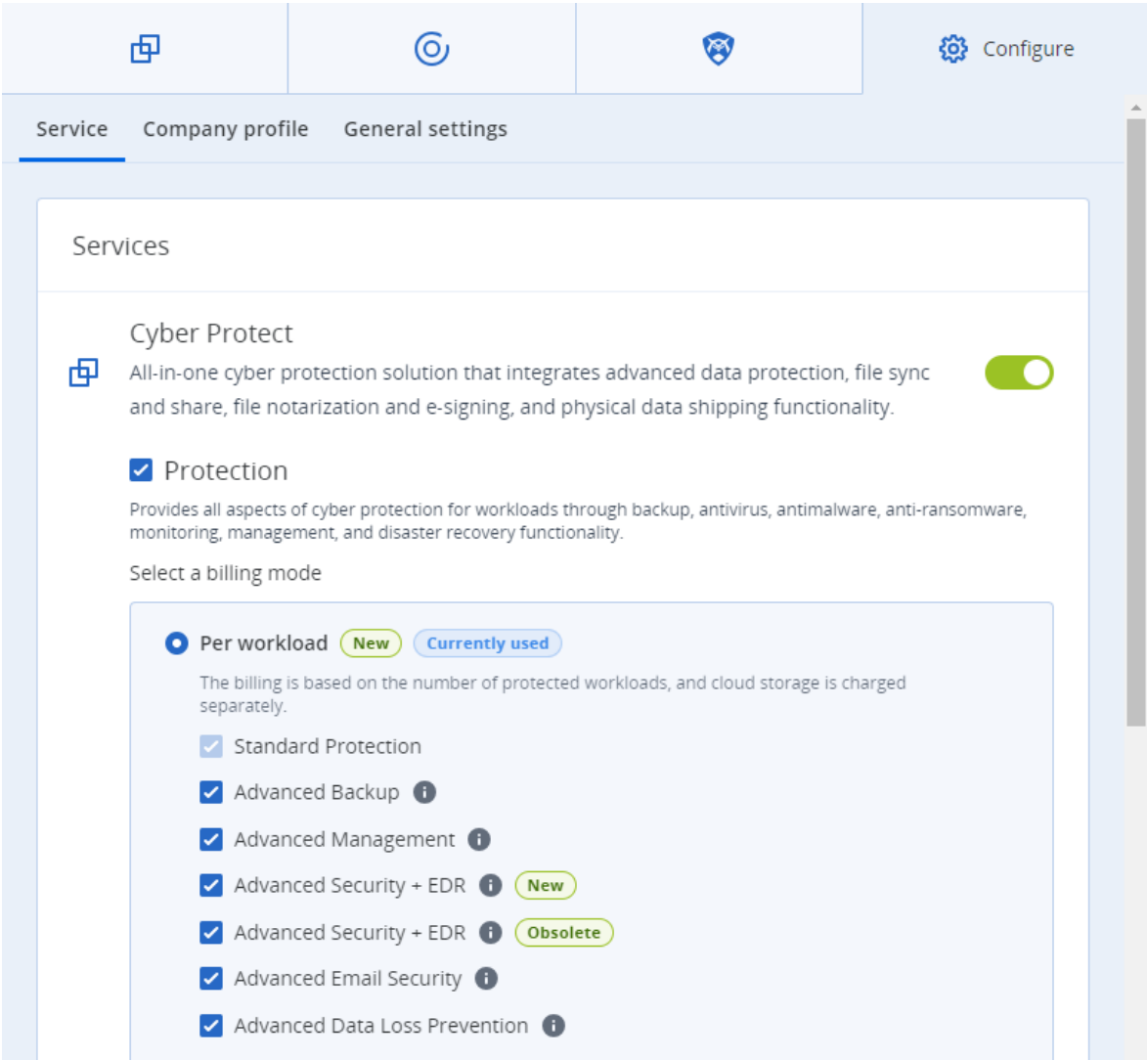
1. Melden Sie sich am Management-Portal an.

   Hinweis
   Wählen Sie bei entsprechender Aufforderung die Kunden aus, auf die Sie das Protection-Paket 'Advanced Security + EDR' anwenden wollen, und klicken Sie anschließend auf **Aktivieren**.

2. Klicken Sie im linken Navigationsbereich Sie auf **Clients**.
3. Klicken Sie unter Cyber Protect auf die Registerkarte **Schutz**.

   Die Liste der bestehenden Clients (Kunden), die den Protection Service abonniert haben, wird angezeigt.
4. Klicken Sie auf den entsprechenden Client (Kunden), dem Sie das Advanced Security + EDR-Paket hinzufügen wollen.

   Stellen Sie in der Registerkarte **Konfigurieren** im Bereich **Schutz** sicher, dass das Kontrollkästchen **Advanced Security + EDR** aktiviert ist.



Managed Detection & Response (MDR)

Die MDR-Funktionalität bietet einen 24/7-Service für MSPs, die keine In-House-Sicherheitsexpertise haben oder zusätzliche Unterstützung benötigen, um Sicherheitsvorfälle, die von der EDR-Funktionalität (Endpoint Detection & Response) erkannt werden, zu untersuchen und darauf zu reagieren.

Die MDR-Funktionalität ist im Management-Portal unter dem Advanced Security + EDR-Paket aktiviert und der MDR-Service wird von einem externen MDR-Anbieter bereitgestellt. Wenn MDR für einen bestimmten Kunden aktiviert ist, erhält der MDR-Anbieter EDR-Vorfallsdaten von Acronis für Workloads, bei denen die EDR-Funktionalität in den Schutzplänen dieses Kunden aktiviert ist. Der MDR-Anbieter wendet dann verschiedene Service-Level an, um die Vorfälle mit verfügbaren Gegenmaßnahmen (Antwortaktionen) zu bearbeiten. Weitere Informationen dazu finden Sie unter "Was ist die Managed Detection & Response (MDR)-Funktionalität?" (S. 166)

Weitere Informationen zum Arbeiten mit der EDR-Funktionalität finden Sie unter Endpoint Detection & Response (EDR).

Was ist die Managed Detection & Response (MDR)-Funktionalität?

Bei der MDR-Funktionalität handelt es sich um eine Service-Leistung, die von Drittanbietern bereitgestellt wird. Sie nutzt eine Kombination aus qualifizierten Analysten, integrierten Tools, Threat Intelligence und Technologien vom Anbieter und Acronis, um potenzielle Sicherheitsbedrohungen und Datenschutzverstöße überwachen und auf diese reagieren zu können.

Wenn die MDR-Funktionalität im Management-Portal für bestimmte Kunden aktiviert ist, leitet Acronis eine EDR-Vorfallstelemetrie an den MDR-Anbieter weiter, damit dieser Untersuchungen und Gegenmaßnahmen zu diesen Vorfällen durchführen kann. Beachten Sie, dass nur solche Vorfälle an den MDR-Anbieter weitergeleitet werden, die nicht schon automatisch durch die EDR-Funktionalität gekontert werden konnten.

Kernkomponenten der MDR-Funktionalität

Die MDR-Funktionalität besteht aus drei Hauptkomponenten:

- Monitoring
- Isolation
- Gegen- und Schadensbehebungsmaßnahmen

Monitoring

Die MDR-Anbieter überwachen die Sicherheitsalarme und Benachrichtigungen vom Endpunkt des Kunden, die von der EDR-Funktionalität erkannt wurden. Der Anbieter untersucht und priorisiert diese Alarmmeldungen und verwendet dazu Informationen über bekannte Bedrohungen, aus der eigenen Threat Intelligence und der Threat Intelligence von Drittanbietern. Der Prozess umfasst eine Vorfallsanalyse, Sicherheitsorchestrierung und die Planung von Gegenmaßnahmen. Als Ergebnis bestimmt der Anbieter, ob es sich bei den Alarmmeldungen bzw. Benachrichtigungen um einen Datenschutzverstoß oder eine Sicherheitsgefährdung handelt.

Alle Sicherheitsereignisse, die nach Ansicht des MDR-Anbieters eine potenzielle Sicherheitsbedrohung darstellen, werden zu einem kundenorientierten Sicherheitsvorfall eskaliert und in der Cyber Protect-Konsole verfügbar gemacht. Der Anbieter liefert Kontextinformationen über den Schweregrad der Bedrohung sowie die empfohlenen Schadensbehebungsmaßnahmen (einschließlich aller bereits ergriffenen Maßnahmen).

Isolation

Die Analysten des MDR-Anbieters nutzen vordefinierte Playbooks, um Gegenmaßnahmen (Antwortaktionen) zur Isolierung des Endpunkts einzuleiten. Alle diese Antwortaktionen des MDR-Anbieters werden in dem jeweiligen Sicherheitsvorfall festgehalten. Die Entscheidung, einen Endpunkt zu isolieren, wird einerseits anhand von Daten des Endpunkts und andererseits anhand von Erkenntnissen aus der allgemeinen Bedrohungsanalyse/-forschung (Threat Intelligence, Threat Research) getroffen.

Gegen- und Schadensbehebungsmaßnahmen

Die Gegen- und Schadensbehebungsmaßnahmen erfolgen in Form von definierbaren Antwortaktionen, nachdem die anfänglichen Monitoring- und Isolierungsaktivitäten abgeschlossen wurden. Wenn ein Sicherheitsvorfall entdeckt wird, leitet der MDR-Anbieter je nach Vorfall die entsprechende Maßnahmen ein. Zu diesen den Gegen- und Schadensbehebungsmaßnahmen gehören folgende Aktionen:

- Eine Anleitung, wie ein Vorfall auf der Grundlage der bereitgestellten Daten, der aktuellen Sicherheitsforschung und allgemeinen Sicherheitswarnungen abgeschwächt, gestoppt oder verhindert werden kann.
- Eine Analyse und Untersuchung der Sicherheitsereignisse, um die Ursache und das Ausmaß der jeweiligen Kompromittierung zu ermitteln.
- Die Durchführung von genehmigten Abläufen (wie in den dazugehörigen Playbooks des MDR-Anbieters definiert), um betroffene Workloads zu isolieren, gefährliche Dateien/Prozesse unter Quarantäne zu stellen oder die Bedrohung vollständig zu beseitigen.
- Dem Service Provider wird eine detailliertere Sicherheitseskalation bereitgestellt, in der der kundenseitige Sicherheitsvorfall, die entsprechende Threat Intelligence und dazugehörige Sicherheitswarnungen aufgeführt sind.
- Eine Eskalierung der Vorfälle über verschiedene Kanäle, wie etwa das Anlegen eines entsprechenden Sicherheitsvorfalls sowie das Benachrichtigen der entsprechenden Kunden per E-Mail und Telefonanruf (anhand der bereitgestellten Kontaktinformationen).
- Mit dem Kunden bis zur Beseitigung der Bedrohung in Kontakt zu bleiben und ihn über neue Erkenntnisse zeitnah zu informieren.
- Wenn die notwendigen Gegenmaßnahmen über den Umfang des vereinbarten MDR-Service hinausgehen, wird der MDR-Anbieter Empfehlungen geben, auf welche Bereiche der Kunde sich konzentrieren sollte. Dazu können auch Empfehlungen für zusätzliche Service-Angebote gehören (wie etwa Incident Response-Lösungen).

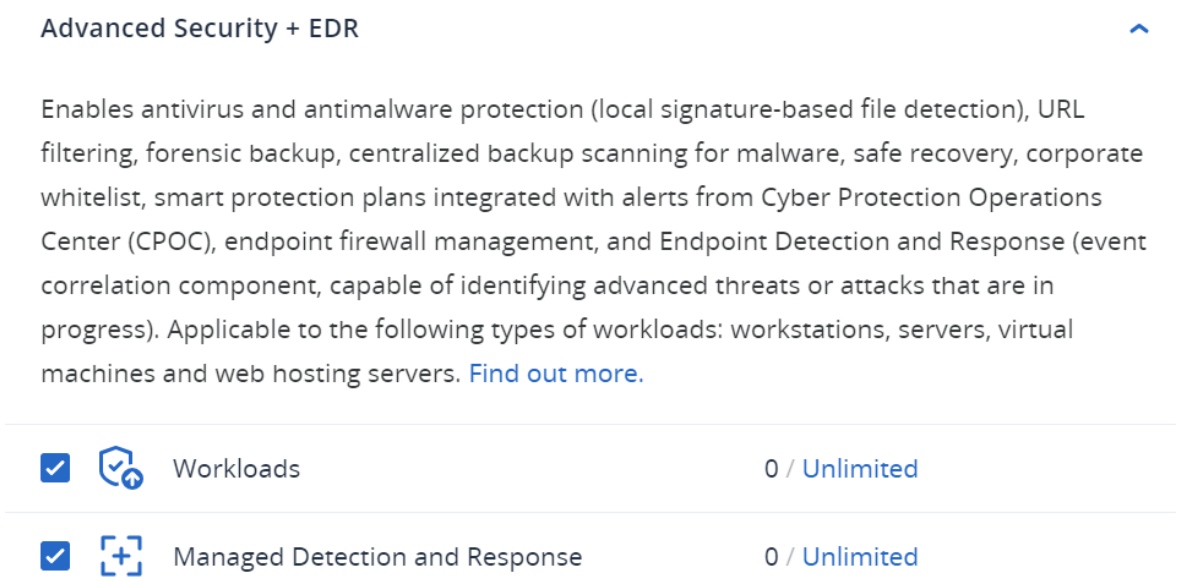
Managed Detection & Response (MDR) aktivieren

Sie können die MDR-Funktionalität für ausgewählte Kunden aktivieren, indem Sie folgende zwei Schritte ausführen:

- Schritt 1: Aktivieren Sie das MDR-Angebotselement für Kunden .
- Schritt 2: Konfigurieren Sie die Integration mit der App des MDR-Anbieters .

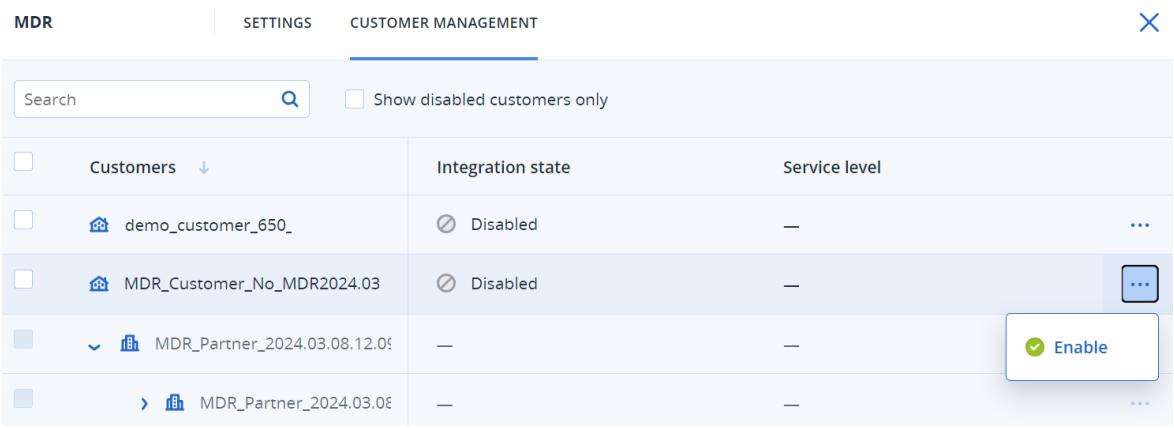
So können Sie die MDR-Funktionalität für ausgewählte Kunden aktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Klicken Sie neben dem entsprechenden Kunden auf das Drei-Punkte-Symbol (...) und wählen Sie den Befehl **Konfigurieren**.
3. Klicken Sie in der Registerkarte **Schutz** auf **Bearbeiten**.
4. Überprüfen Sie im Bereich **Advanced Security + EDR**, dass die Kontrollkästchen **Workloads** und **Managed Detection & Response** aktiviert sind. Klicken Sie anschließend auf **Speichern**, um die Änderungen zu übernehmen.



So können Sie die Integration mit der App des MDR-Anbieters konfigurieren

1. Gehen Sie im Management-Portal zu **Integrationen**.
2. Verwenden Sie die Suchleiste, um die App des MDR-Anbieters zu finden.
3. Klicken Sie in der angezeigten MDR-Katalogkarte auf **Konfigurieren**.
4. Klicken Sie in der Registerkarte **Einstellungen** auf das Stiftsymbol und geben die Kontaktdaten von mindestens einem Partnerkontakt ein. Dieser Kontakt wird vom MDR-Anbieter kontaktiert, wenn ein Sicherheitsvorfall erkannt wird. Beachten Sie, dass Sie Informationen für bis zu drei Kontakten hinzufügen können. Klicken Sie auf **Aktivieren**, wenn Sie fertig sind.
   Wenn ein Sicherheitsereignis erkannt wird, ruft der Anbieter jeden Kontakt sechsmal an, bevor er zum nächsten Kontakt wechselt. Nach einem Anruf oder falls kein Kontakt hergestellt wird, sendet der Anbieter eine E-Mail an alle Kontakte und gibt einen Überblick über die Eskalation und den Vorfall.
5. Klicken Sie in der Registerkarte **Kundenverwaltung** bei dem entsprechenden Kunden zuerst auf das Drei-Punkte-Symbol (...) in der äußersten rechten Spalte und anschließend auf **Aktivieren**.



Wenn Sie mehrere Kunden aktivieren wollen, müssen Sie das Kontrollkästchen neben den entsprechenden Kunden auswählen und dann auf der Registerkarte **Kundenverwaltung** oben links auf **Aktivieren** klicken.

6. Wählen Sie aus dem Listenfeld **Service-Level** im angezeigten Dialog die jeweilige Stufe des MDR-Services aus, die Sie auf den/die ausgewählten Kunden anwenden wollen:
   - **Standard**: Umfasst ein Rund-um-die-Uhr-Monitoring (24/7/365) der Endpunkte des Kunden, um Angriffe abzufangen, eine KI-gestützte Triage und Priorisierung von Ereignissen, die Eindämmung von Bedrohungen und die Isolierung betroffener Endpunkte sowie einen Echtzeit-Einblick über die Konsole in eine priorisierte Liste von Vorfällen.
   - **Advanced**: Zusätzlich zu den Funktionen, die in **Standard** enthalten sind, ermöglicht dieses Level auch vollständige Schadensbehebungsmaßnahmen (wie beispielsweise Rollbacks nach Angriffen, Wiederherstellungen und das Schließen von Sicherheitslücken).
7. Klicken Sie auf **Aktivieren**, um die MDR-Integration abzuschließen.

   Wenn die IP-Positivlisten-Funktion aktiviert ist (siehe "Zugriff auf die Weboberfläche beschränken" (S. 32)), werden Sie aufgefordert, die IPs des MDR-Anbieters zur Positivliste hinzuzufügen. Dies gewährleistet, dass der Anbieter die relevanten Workloads überwachen kann. Klicken Sie auf **Aktivieren**, um die Einstellungen zu bestätigen.

   MDR ist jetzt aktiviert und EDR-Sicherheitsvorfälle werden an den MDR-Anbieter weitergeleitet, um Untersuchungs- und Reaktionsaktivitäten durchzuführen. Weitere Informationen zum MDR-Service finden Sie unter "Was ist die Managed Detection & Response (MDR)-Funktionalität?" (S. 166)

Managed Detection & Response (MDR) deaktivieren

Sie können die MDR-Funktionalität auf der Angebotselementebene deaktivieren. Sie können die MDR-Funktionalität auch für einzelne Kunden in der Integrations-App des MDR-Anbieters deaktivieren.

So können Sie das MDR-Angebotselement deaktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Klicken Sie neben dem entsprechenden Kunden auf das Drei-Punkte-Symbol (...) und wählen Sie den Befehl **Konfigurieren**.

3. Klicken Sie in der Registerkarte **Schutz** auf **Bearbeiten**.
4. Überprüfen Sie im Bereich **Advanced Security + EDR**, dass die Kontrollkästchen **Workloads** und **Managed Detection & Response** nicht aktiviert sind. Klicken Sie anschließend auf **Speichern**, um Ihre Änderungen zu übernehmen.
   Alternativ können Sie den **Advanced Security + EDR** Service in der Registerkarte **Konfigurieren** deaktivieren, was automatisch auch die MDR-Funktionalität deaktiviert.

So können Sie die MDR-Funktionalität für bestimmte Kunden in der Integrations-App des MDR-Anbieters deaktivieren

1. Gehen Sie im Management-Portal zu **Integrationen**.
2. Suchen Sie nach der entsprechenden App des MDR-Anbieters.
3. Klicken Sie in der angezeigten MDR-Katalogkarte auf **Konfigurieren**.
4. Klicken Sie in der Registerkarte **Kundenverwaltung** bei dem entsprechenden Kunden zuerst auf das Drei-Punkte-Symbol (...) in der äußersten rechten Spalte und anschließend auf **Deaktivieren**.
   Wenn Sie mehrere Kunden aktivieren wollen, müssen Sie das Kontrollkästchen links neben jedem entsprechenden Kunden auswählen und dann auf der Registerkarte **Kundenverwaltung** oben links auf **Deaktivieren** klicken.

Antwortaktionen, die in der Managed Detection & Response (MDR)-Funktionalität verfügbar sind

Die MDR-Funktionalität beinhaltet eine Reihe von Antwortaktionen, die auf der Vorfallsebene angewendet werden können.

Diese Antwortaktionen werden von MDR-Sicherheitsanalysten ausgeführt, die die entsprechenden Aktionen anwenden, indem Sie auf die Cyber Protect-Konsole zugreifen oder API-Aufrufe ausführen. Diese Analysten melden sich mit der Rolle **Sicherheitsanalyst** an der Cyber Protect-Konsole an.

Alle Antwortaktionen werden in der Liste **Aktivitäten** protokolliert. Kunden können eine Liste der durchgeführten Antwortaktionen und den Status dieser Aktivitäten (Wird ausgeführt/Erfolgreich/Fehlgeschlagen) einsehen. In der Spalte **Eingeleitet durch** wird der Benutzer angezeigt, der die Aktion initiiert hat, ob es sich dabei um einen Partnerbenutzer, einen Kundenbenutzer oder den MDR-Sicherheitsanalysten handelt. Weitere Informationen dazu finden Sie unter So können Sie die Endpoint Detection & Response (EDR)-Funktionalität verwenden.

Hinweis
Die in der unteren Tabelle aufgeführten Antwortaktionen beinhalten Verweise auf die entsprechenden Abschnitte in der Endpoint Detection & Response (EDR)-Dokumentation.

Antwortaktion	Zusätzliche Informationen
Untersuchungsstadium ändern	Das Stadium kann auf einen der folgenden Werte festgelegt sein:

Antwortaktion	Zusätzliche Informationen
	• **Wird untersucht** • **Geschlossen** • **Falsch positiv** Weitere Informationen zum Ändern des Untersuchungsstadium finden Sie unter So können Sie Vorfälle in der Cyber Kill Chain untersuchen.
Netzwerk-Isolation	MDR-Sicherheitsanalysten können: • Den Workload isolieren • Die Isolierung des Workloads wieder aufheben • Das Isolationsstadium überprüfen Weitere Informationen zur Isolation von Workloads finden Sie im Abschnitt Die Netzwerk-Isolation eines Workloads verwalten.
Kommentare hinzufügen	MDR-Sicherheitsanalysten können Kommentare zu einem Vorfall hinzufügen, indem sie in der Cyber-Kill-Chain beim jeweiligen Vorfall auf den Befehl **Kommentar posten** klicken. Diese Kommentare werden in der Registerkarte **Aktivitäten** für den jeweiligen Vorfall angezeigt. Weitere Informationen dazu finden Sie unter Die Aktionen verstehen, die zur Abschwächung eines Vorfalls ergriffen wurden.
Prozess stoppen / Prozessbaum	Diese Aktion kann auf den gesamten Vorfall angewendet werden. Die Antwortaktion kann auch dann ausgelöst werden, wenn die Prozesse für den Vorfall bereits gestoppt wurden. Eine asynchrone Antwort wird gesendet, nachdem die Antwortaktion verarbeitet wurde. Die Antwort kann eine der folgenden sein: • Erfolgreich: Alle Prozesse wurden erfolgreich gestoppt. • Mit Warnung abgeschlossen: Einige Prozesse wurden erfolgreich gestoppt

Antwortaktion	Zusätzliche Informationen
	oder es gibt keine Prozesse zum Stoppen (oder die Prozesse wurden außerhalb der MDR-Funktionalität gestoppt). • Fehler: Es wurden keine Prozesse gestoppt. Weitere Informationen zum Stoppen eines Prozesses oder Prozessbaums finden Sie im Abschnitt Antwortaktionen für einen verdächtigen Prozess definieren.
Quarantäne	Diese Aktion kann auf den gesamten Vorfall angewendet werden. Die Antwortaktion kann auch dann ausgelöst werden, wenn die Dateien oder Prozesse bereits unter Quarantäne gestellt wurden. Eine asynchrone Antwort wird gesendet, nachdem die Antwortaktion verarbeitet wurde. Die Antwort kann eine der folgenden sein: • Erfolgreich: Alle Dateien und Prozesse wurden erfolgreich unter Quarantäne gestellt. • Mit Warnung abgeschlossen: Einige Dateien und Prozesse wurden erfolgreich unter Quarantäne gestellt oder es gibt keine Dateien oder Prozesse, die unter Quarantäne gestellt werden könnten (oder wurden außerhalb der MDR-Funktionalität unter Quarantäne gestellt). • Fehler: Es wurden keine Dateien oder Prozesse unter Quarantäne gestellt. Weitere Informationen darüber, wie ein Prozess unter Quarantäne gestellt werden kann, finden Sie im Abschnitt Antwortaktionen für einen verdächtigen Prozess definieren. Weitere Informationen darüber, wie Dateien unter Quarantäne gestellt werden können, finden Sie im Abschnitt Antwortaktionen für eine verdächtige Datei definieren.
Dateien löschen	Diese Aktion kann auf den gesamten Vorfall angewendet werden. Die Antwortaktion kann auch ausgelöst werden, wenn die

Antwortaktion	Zusätzliche Informationen
	Dateien bereits gelöscht wurden. Eine asynchrone Antwort wird gesendet, nachdem die Antwortaktion verarbeitet wurde. Die Antwort kann eine der folgenden sein: • Erfolgreich: Alle Dateien wurden erfolgreich gelöscht. • Mit Warnung abgeschlossen: Einige Dateien wurden erfolgreich gelöscht oder es gibt keine Dateien zum Löschen (oder sie wurden außerhalb der MDR-Funktionalität gelöscht). • Fehler: Es wurden keine Dateien gelöscht. Weitere Informationen über das Löschen von Dateien finden Sie im Abschnitt Antwortaktionen für eine verdächtige Datei definieren.
Workload neu starten	Ermöglicht es, ein Zeitintervall für den Neustart des betroffenen Workloads festzulegen oder diesen sofort neu zu starten. Weitere Informationen über das Neustarten von Workloads finden Sie im Abschnitt Einen Workload neu starten.
Eine URL, Datei oder Prozess zur Positivliste / Blockliste hinzufügen	Fügt die URLs, Dateien oder Prozesse zur Positivliste/Blockliste des Standardplans (dem Plan, der derzeit dem Workload zugewiesen ist) hinzu. Eine asynchrone Antwort wird gesendet, nachdem die Antwortaktion verarbeitet wurde. Die Antwort kann eine der folgenden sein: • Erfolgreich: Alle URLs, Dateien und Prozesse wurden erfolgreich hinzugefügt. • Mit Warnung abgeschlossen: Einige URLs, Dateien und Prozesse wurden erfolgreich hinzugefügt und einige nicht (weil diese beispielsweise bereits in der Positivliste enthalten waren). • Fehler: Die Aktion ist fehlgeschlagen.

Antwortaktion	Zusätzliche Informationen
	Weitere Informationen zum Hinzufügen von URLs, Dateien oder Prozessen zur Positivliste und Blockliste finden Sie im Abschnitt Einen Prozess, eine Datei oder ein Netzwerk zur Blockliste oder Positivliste des Schutzplans hinzufügen.

Advanced Disaster Recovery

Sie können das Advanced Disaster Recovery-Paket aktivieren und Ihre Workloads mit der kompletten Disaster Recovery-Funktionalität schützen.

Folgende erweiterte Disaster Recovery-Funktionen sind verfügbar:

- Produktions-Failover
- Test-Failover in einer isolierten Netzwerkumgebung.
- Für Failover verfügbare Anzahl von Recovery-Punkten: alle Recovery-Punkte, die nach Erstellung des Recovery-Servers verfügbar sind.
- Primäre Server
- Konfigurationen für Recovery-Server/primäre Server: Keine Beschränkungen
- Verfügbare Verbindungsmodi: Nur Cloud, Point-to-Site, Site-to-Site-OpenVPN und Multi-Site-IPsec-VPN.
- Verfügbarkeit des VPN-Gateways: immer verfügbar.
- Anzahl der Cloud-Netzwerke: 23.
- Öffentliche IP-Adressen
- Internetzugriff
- Aktionen mit Runbooks: erstellen, bearbeiten und ausführen.

Advanced Email Security

Das Advanced Email Security-Paket bietet einen Echtzeitschutz für Ihre Microsoft 365-, Google Workspace- oder Open-Xchange-Postfächer:

- Antimalware und Antispam
- Scannen von URLs in E-Mails
- DMARC-Analyse
- Antiphishing
- Impersonation Protection
- Scannen von Anhängen

- Content Disarm & Reconstruction (CDR)
- Vertrauensgraph

Sie können auch die Option Microsoft 365-Kollaborations-Apps-Arbeitsplätze aktivieren, die es ermöglicht, Microsoft 365-Cloud-Kollaborationsapplikationen vor inhaltsbasierten Sicherheitsbedrohungen zu schützen. Diese Applikationen umfassen u.a. OneDrive, SharePoint und Teams.

Die Advanced Email Security-Erweiterung kann pro Workload oder pro Gigabyte aktiviert werden und hat Auswirkungen auf Ihr Lizenzierungsmodell.

Im Datenblatt für Advanced Email Security können Sie mehr über die Advanced Email Security-Funktionalität erfahren.

Anweisungen zur Konfiguration finden Sie unter Advanced Email Security mit Perception Point.

Advanced Backup

Sie können das Advanced Backup-Paket aktivieren und dadurch Ihre Workloads mit erweiterten Backup- und Wiederherstellungsfunktionen schützen.

Es stehen folgende Funktionen zur Verfügung:

- One-Click Recovery
- Kontinuierliche Datensicherung (CDP)
- Backup support for Microsoft SQL Server clusters and Microsoft Exchange clusters – AlwaysOn-Verfügbarkeitsgruppen (AAG) und Datenbankverfügbarkeitsgruppen (DAG)
- Backup-Unterstützung für MariaDB, MySQL, Oracle DB und SAP HANA
- Data Protection-Karte und Compliance-Berichterstattung
- Off-Host Data Processing
- Backup-Häufigkeit für Microsoft 365- und Google Workspace-Workloads
- Remote-Aktionen mit einem Boot-Medium
- Direktes Backup in den Microsoft Azure Public Cloud Storage

Advanced Management

Mit der Advanced Management-Funktionalität können Sie eine schnelle, proaktive und reaktionsschnelle Verwaltungsinfrastruktur aufbauen, mit der sich die meisten Probleme vermeiden lassen.

Das Advanced-Management-Paket umfasst folgende Funktionen:

- **Software-Inventarisierung** – Lassen Sie sich eine vollständige Liste der von den Clients verwendeten Software anzeigen und sparen Sie sich Zeit und Mühe bei der Vorbereitung, Planung und Nachverfolgung von Updates.

- **Automatisierte Patch-Verwaltung** – Beheben Sie Schwachstellen, bevor diese ausgenutzt werden.
- **Ausfallsicheres Patching** – Sie können Workloads nach fehlerhaften Patches schnell und einfach wiederherstellen, indem Sie vor dem Patchen automatische System-Backups durchführen.
- **Monitoring und intelligente, auf maschinellem Lernen basierende Alarmmeldungen** – Schwächen Sie operative Risiken ab und optimieren Sie den Überwachungsaufwand mit prädiktivem Monitoring und Alarmmeldungen.
- **Direkt einsetzbares Cyber Scripting** – Automatisieren und optimieren Sie Routineaufgaben.
- **Überwachung der Laufwerksintegrität** – Verringern Sie durch Laufwerksausfälle verursachte Ausfallzeiten mithilfe einer prädiktiven Laufwerksüberwachung und dazugehörigen Alarmmeldungen.
- **Remote-Desktop- und Remote-Unterstützungsfunktionalität** – Greifen Sie auf Remote-Workloads zu, um technische Probleme schnell beheben zu können. Sparen Sie Zeit und bieten Sie einen zuverlässigen Support mit hervorragender Performance, selbst bei begrenzter Bandbreite. Die Funktion beinhaltet eine bessere Plattformabdeckung (Windows, macOS und Linux) sowie erweiterte Fähigkeiten für Sitzungsaufzeichnungen, Remote-Aktionen, Dateiübertragungen, Monitoring, Berichterstellung und die Möglichkeit zur Beobachtung von Workloads in einer Mehrfachansicht.

Advanced Automation

Der Advanced Automation Service macht es für Kunden einfach und intuitiv, die Vorteile von Business Management-Plattformen und -Programmen zu nutzen. Der Advanced Automation Service besteht aus einer Reihe von kostenpflichtigen Tools, durch die MSPs diverse alltägliche Tasks vollständig verwalten und automatisieren können – wie etwa:

- Kundenabrechnung und Rechnungsstellung.
- Kunden-Support und Service Desk-Ticketing.
- Verkauf und Projektmanagement.

Advanced Automation kann auch so eingerichtet werden, dass es gemeinsam mit anderen Cyber Protect Cloud Services genutzt werden kann, für die zusätzliche Gebühren erhoben werden. Ihr Konto wird entsprechend der Anzahl der Benutzer (oder Techniker), denen Zugriff auf den Advanced Automation Service gewährt wird, belastet.

Hinweis
Es werden mindestens drei Benutzer abgerechnet, auch wenn weniger als drei Benutzer Zugriff auf den Advanced Automation Service gewährt wird.

Was ist Advanced Automation?

Advanced Automation ist ein speziell für Managed Service Provider (MSPs) entwickeltes Business Management Tool, mit dem diese eine Vielzahl täglicher Aufgaben einfach und intuitiv verwalten und automatisieren können.

Mit Advanced Automation können Sie sicherstellen, dass Ihre Kunden den Service erhalten, den diese benötigen, während Sie gleichzeitig die volle Kontrolle über Ihre Operationen behalten. Zu den Komponenten von Advanced Automation gehören Ticketing, RMM-Integration, automatisierte Zeiterfassung sowie verbrauchsbasierte Abrechnungen. Zudem wird ein schneller und einfacher Zugriff auf die Abrechnungs- und Ticket-Daten Ihrer Kunden bereitgestellt. Sie können die spezielle Mobilgeräte-App auch für Ihre alltäglichen Service Desk-Aktionen einsetzen, wie etwa zum Monitoring und zur Bearbeitung von Tickets sowie zur Nachverfolgung und Erfassung von Arbeitszeiten. Sie können die App Acronis Advanced Automation im Apple App Store oder dem Google Play Store herunterladen.

Für jeden Benutzer, dem Zugriff auf den Service gewährt wird, wird Ihr Konto entsprechend belastet. Beachten Sie, dass Sie für mindestens drei Benutzer zahlen müssen, auch wenn weniger als drei Benutzer Zugriff auf Advanced Automation haben.

Zu den Kernfunktionen von Advanced Automation gehören:

- **Service Desk-Tickets verwalten**: Die Support-Tickets werden automatisch aus eingehenden E-Mails oder Alarmmeldungen von integrierten Drittanbieter-Plattformen konvertiert (sofern diese aktiviert sind). Weitere Informationen finden Sie im Abschnitt '"Service Desk" (S. 196)'.

- **Abrechnungen verwalten**: Die Rechnungen können automatisch generiert werden – und zwar entweder auf Basis der für den Kunden aufgewendeten Zeit oder gemäß einer Abrechnungsvereinbarung, die Sie mit dem Kunden getroffen haben. Weitere Informationen dazu finden Sie im Abschnitt '"Die Verkaufs- und Abrechnungsfunktionalität verwalten" (S. 216)'.
- **Zeiterfassungen und Aktivitäten verwalten**: Als administrativer Benutzer oder Manager können Sie Ticket-Zeiten zur Abrechnung genehmigen, freie Tage anfordern oder Urlaubstage genehmigen. Weitere Informationen finden Sie im Abschnitt '"Zeiteinträge" (S. 206)'.
- **Native Integration in Acronis Services**: Dazu gehören nutzungsbasierte Kundenabrechnungen und die Gerätekontrolle mit der Advanced Management-Funktionalität.

Advanced Automation für Kunden freischalten

Wie bereits für den Prozess zum Erstellen von Mandanten beschrieben (siehe Abschnitt '"Die Services für einen Mandanten auswählen" (S. 44)'), können Sie den Mandanten nach Bedarf bestimmte Services hinzufügen.

Der Advanced Automation Service ist für folgende Mandanten-Typen verfügbar:

- Partner
- Kunde

Hinweis
Partner können die Advanced Automation-Daten ihrer Clients (unabhängig davon, ob es sich um Subpartner oder Kunden handelt) nicht einsehen, weil es sich bei den Advanced Automation-Daten – anders als bei den Daten anderer Produkte – um private Geschäftsdaten handelt, die spezifisch für ein Subpartner- oder Kunden-Konto sind. Partner können jedoch weiterhin bestimmte Konto-Daten einsehen, wenn sie sich im Management-Portal als der entsprechende Client (Subpartner oder Kunde) anmelden.

So können Sie den Advanced Automation Service aktivieren

1. Gehen Sie im Management-Portal zu **Clients**.
2. Wählen Sie den Mandanten aus, der bearbeitet werden soll.
3. Scrollen Sie auf der Registerkarte **Konfigurieren** (unter dem Bereich **Service**) nach unten und wählen Sie **Advanced Automation**.
   Advanced Automation ist jetzt für den ausgewählten Kunden verfügbar.

Advanced Automation einrichten

In diesem Abschnitt werden die unterschiedlichen Schritte beschrieben, die Sie durchführen müssen, um Advanced Automation in Betrieb zu nehmen.

Advanced Automation aktivieren

Wenn der Advanced Automation Service für Ihr Konto freigeschaltet ist, können Sie den Service aktivieren, indem Sie zu **Einstellungen** gehen. Wenn der Advanced Automation Service nicht freigeschaltet ist, kontaktieren Sie Ihren Administrator.

So können Sie Advanced Automation aktivieren

1. Klicken Sie im Management-Portal auf **Einstellungen –> Advanced Automation**.

   Hinweis
   Nachdem Sie Advanced Automation (wie im folgenden Schritt beschrieben) aktiviert haben, ist diese Menüoption nicht mehr verfügbar.

2. Klicken Sie in der erscheinenden Anzeige auf **Advanced Automation aktivieren**.
3. Geben Sie in der Anzeige 'Advanced Automation aktivieren' auf der Registerkarte **Firmeninformationen** die entsprechenden Geschäftsdaten zu Ihrem Unternehmen an. Klicken Sie anschließend auf **Weiter**.
4. Definieren Sie auf der Registerkarte **Benutzerrollen** für jeden Benutzer die Advanced Automation-Rolle und klicken Sie anschließend auf **Weiter**. Folgende Rollen sind verfügbar:
   - Techniker
   - Personalabteilung
   - Finanzen
   - Verkauf
   - Gruppenleiter
   - Finanzdirektor
   - Direktor
   - Administrator

     Weitere Informationen zu den einzelnen Advanced Automation-Rollen und deren Berechtigungen finden Sie in Abschnitt '"Advanced Automation-Rollen" (S. 190)'.

     Hinweis
     Sie können auch neue Benutzer hinzufügen, nachdem Sie die Advanced Automation-Funktionalität aktiviert haben. Erstellen Sie zuerst das/die Benutzerkonto/-konten und wenden Sie dann die entsprechenden Services an, auf die der Benutzer Zugriff haben soll. Weitere Informationen finden Sie im Abschnitt '"Ein Benutzerkonto erstellen" (S. 58)'.

5. Überprüfen Sie auf der Registerkarte **Bestätigung** die Aktivierungsinformationen und klicken Sie anschließend auf **Aktivieren**. Der Advanced Automation Service wird konfiguriert, was ein paar Sekunden dauern kann.
6. Wählen Sie im angezeigten Onboarding-Assistenten aus den folgenden Advanced Automation-Optionen:

- **Buchhaltungsplattformen-Integration**: Klicken Sie auf **Konfigurieren**, um zur Buchhaltungsintegrationsseite weitergeleitet zu werden. Weitere Informationen finden Sie im Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)'.
- **RMM-Plattform-Integration**: Klicken Sie auf **Konfigurieren**, um zur Advanced Automation (RMM)-Integrationsseite weitergeleitet zu werden. Weitere Informationen finden Sie im Abschnitt '"Mit RMM-Plattformen integrieren" (S. 295)'.
- **Service Desk-Integration**: Klicken Sie auf **Konfigurieren**, um zum Bereich **Einstellungen –> Service Desk** weitergeleitet zu werden. Weitere Informationen finden Sie im Abschnitt '"Service Desk-Einstellungen" (S. 251)'.
- **E-Mail-Server-Konfiguration**: Klicken Sie auf **Konfigurieren**, um zur Anzeige 'E-Mail-Server konfigurieren' weitergeleitet zu werden. Weitere Informationen finden Sie im Abschnitt '"Ihre E-Mail-Einstellungen konfigurieren" (S. 192)'.

Wenn Sie die in Advanced Automation enthaltenen Funktionalitäten nicht mehr verwenden wollen, können Sie den Advanced Automation Service abbrechen. Weitere Informationen finden Sie im Abschnitt '"Den Advanced Automation Service kündigen" (S. 315)'.

Schnellstartanleitung für die Einrichtung von Advanced Automation

Diese Schnellstartanleitung beschreibt die grundlegenden Schritte, die erforderlich sind, um Advanced Automation in Betrieb zu nehmen.

Befolgen Sie die Schritte in der nachstehenden Tabelle, um sicherzustellen, dass:

- Neue und vorhandene Kunden in Advanced Automation eingerichtet sind.
- Ihre Produkte und Services eingerichtet und verfügbar sind sowie die automatische Abrechnung funktioniert.
- Ihr Service Desk eingerichtet und bereit ist, die Kunden zu unterstützen, SLAs zu überwachen sowie die für Tickets und andere Aktivitäten aufgewendete Zeit zu erfassen.
- Ihre RMM- und/oder Buchhaltungsplattform mit Advanced Automation integriert und synchronisiert ist.
- Eingehende E-Mails in Tickets konvertiert werden und die automatisierten Antworten konfiguriert sind.

Hinweis
Sie können auch die dedizierte, aber auch eingeschränktere Applikation für Mobilgeräte („Acronis Advanced Automation“, kann im Apple App Store oder Google Play Store heruntergeladen werden) verwenden, um mit Service Desk-Tickets und Zeiteinträgen zu arbeiten.

Die nachfolgende Tabelle beschreibt die allgemeinen Schritte, die erforderlich sind, um mit Advanced Automation arbeiten zu können.

Schritt	Beschreibung
SCHRITT 1: Melden	Melden Sie sich an Ihrem Konto an und greifen Sie auf das Management-Portal

Schritt	Beschreibung
Sie sich an und starten Sie den Onboarding-Assistenten von Advanced Automation	zu. Wenn Advanced Automation in Ihrem Konto verfügbar ist, werden zwei neue Menüoptionen angezeigt: **Task-Verwaltung** sowie **Verkauf und Abrechnung**. Wählen Sie eine dieser Optionen aus, um auf den Onboarding-Assistenten für Advanced Automation zuzugreifen. Klicken Sie anschließend auf **Aktivieren**, um den Service (wie in SCHRITT 2 beschrieben) zu aktivieren. Weitere Informationen finden Sie im Abschnitt '"Advanced Automation aktivieren" (S. 179)'.
SCHRITT 2: Aktivieren Sie den Advanced Automation Service	Wenn Sie den Advanced Automation Service für Ihr Konto aktivieren wollen, müssen Sie die folgenden zwei Schritte durchlaufen: a. Geben Sie auf der Registerkarte **Firmeninformationen angeben** die Geschäftsinformationen für Ihr Unternehmen (einschließlich der Bankkontodaten) an. Die Firmeninformationen werden für die Rechnungen an die Endkunden verwendet. Klicken Sie anschließend auf **Weiter**. b. Weisen Sie in Advanced Automation vorhandenen Benutzern die folgenden Rollen zu: • Techniker • Personalabteilung • Finanzen • Verkauf • Gruppenleiter • Finanzdirektor • Direktor • Administrator Beachten Sie, dass es zwei zusätzliche Rollen für die Benutzer Ihres Kunden gibt: • Kunde • Client-Manager Weitere Informationen über die Rollen in Advanced Automation finden Sie im Abschnitt '"Advanced Automation-Rollen" (S. 190)'. Bei Bedarf können Sie weitere Benutzer auch später noch hinzufügen; siehe auch den Abschnitt '"Benutzer verwalten" (S. 58)'. Danach können Sie damit beginnen, Ihre Advanced Automation-Einstellungen zu definieren (wie in den nachfolgenden Schritten beschrieben).
SCHRITT 3: Definieren Sie die Service Desk-Einstellungen	Die Service Desk-Einstellungen bestimmen wesentliche Abschnitte Ihres Ticket-Flusses im Service Desk, wozu auch die Kategorien, Standardwerte, Standardeinstellungen für Land und Sprache sowie die Service Level-Vereinbarungen (SLAs) gehören. Wenn Sie auf die Service Desk-Einstellungen zugreifen wollen, gehen Sie im Management-Portal zu **Einstellungen –> Service Desk**. Mit diesen Einstellungen können Sie:

Schritt	Beschreibung
	• Vorgefertigte Antworten konfigurieren • Prioritäten festlegen • SLAs verwalten • Kategorien und Unterkategorien definieren • Standardwerte festlegen • Die Standardeinstellungen für Land und Sprache definieren • Statuszustände aktivieren und deaktivieren • Die Standardeinstellungen für die RMM-Ticket-Integration definieren • E-Mail-Vorlagen und Benachrichtigungsvorlagen verwalten • Aktivitäten für Zeiterfassungen definieren • Integrationseinstellungen für externe Tickets definieren
SCHRITT 4: Definieren Sie die Einstellungen für Abrechnung und Angebotserstellung	Mit den Abrechnungs- und Angebotseinstellungen können Sie Ihre Rechnungen vollständig anpassen, wie etwa das Rechnungslayout, das Standard-Exportformat (falls Sie in ein anderes System importieren wollen), die Festlegung von Steuern und vieles mehr. Beachten Sie, dass Abrechnungsinformationen für Endbenutzer in den Einstellungen des jeweiligen Kunden oder beim Erstellen von Verkaufsartikeln, Verträgen und Angeboten spezifiziert werden sollten. Wenn Sie auf die Einstellungen für Abrechnung und Angebotserstellung zugreifen wollen, gehen Sie im Management-Portal zu **Einstellungen –> Abrechnung und Angebotserstellung**. Mit diesen Einstellungen können Sie: • Ihre Abrechnung definieren und anpassen • Das Erscheinungsbild Ihrer Angebote definieren und anpassen • Die zu verwendenden Steuern definieren
SCHRITT 5: Fügen Sie Ihre Kunden und Lieferanten hinzu	Im Management-Portal können Sie Ihre Kunden jederzeit nach Bedarf hinzufügen und verwalten. Beachten Sie, dass Sie in Acronis verschiedene Kontotypen für die Kunden definieren können, darunter Partner, Kunden, Interessenten und Lieferanten. Diese verschiedenen Typen werden auch als *Mandanten* bezeichnet. Weitere Informationen über die unterschiedlichen Art von Mandanten finden Sie im Abschnitt '"Benutzerkonten und Mandanten" (S. 35)'. Wenn Sie Partner, Kunden und Interessenten hinzufügen wollen, gehen Sie im Management-Portal zu **Clients**. Klicken Sie dann auf **+ Neu** und wählen Sie den gewünschten Mandantentyp aus. Wenn Sie Lieferanten hinzufügen wollen, gehen Sie zu **Verkauf und Abrechnung –> Unternehmensverwaltung** und definieren Sie die relevanten Details auf der Registerkarte **Lieferanten**. Weitere Informationen finden Sie im Abschnitt '"Mandanten verwalten" (S. 38)'.
SCHRITT 6: Definieren Sie Ihre	Sie können einen Katalog sowohl mit nicht wiederkehrenden Produkten oder Services als auch mit wiederkehrenden (verwalteten) Services erstellen, die Sie

Schritt	Beschreibung
Produkte	Ihren Kunden bereitstellen können (wie etwa Antivirus-Abonnements oder Ad-hoc-Support). Sie können bestimmte Produkte auch direkt in einem Support-Ticket zum Verkauf anbieten. Zum Beispiel, wenn ein Kunde ein Ticket anlegt, um ein Office 365-Abonnement hinzuzufügen oder zusätzlichen Arbeitsspeicher benötigt. Dadurch kann Zeit für zusätzliche administrative Prozesse eingespart werden. Wenn Sie auf die Produkte zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Produkte**. Nur Benutzer mit den Rollen Administrator, Direktor, Finanzen oder Finanzdirektor können Produkte erstellen. Diese Produkte können dann in Verträgen, Tickets, Angeboten, Verkaufsartikeln usw. verwendet werden. Weitere Informationen finden Sie im Abschnitt '"Produkte" (S. 240)'.
SCHRITT 7: Definieren Sie Verträge	Konfigurieren und definieren Sie Ihre Kundenverträge sorgfältig, um sicherzustellen, dass Advanced Automation Folgendes kann: • Bei Bedarf automatisch regelmäßige Abrechnungselemente und Vorschüsse bereitstellen und eine benutzer- oder gerätebasierte Abrechnung ermöglichen. • Eine Verbindung zwischen Konfigurationselementen, Kunden und der geltenden SLA herstellen. • Einen Service, einen Kunden und ein Konfigurationselement automatisch mit der geltenden SLA im Service Desk verknüpfen. • Neue Konfigurationselemente automatisch dem richtigen Kunden, Vertrag und der richtigen SLA zuordnen. Wenn Sie auf die Verträge zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Verträge**. Weitere Informationen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.
SCHRITT 8: Richten Sie Integrationen mit Drittanbieter-Plattformen ein	Richten Sie Ihre Integrationen mit Drittanbieter-Plattformen ein. Derzeit unterstützt Advanced Automation: • **RMM**: NinjaOne, Datto RMM, Kaseya VSA, N-able N-Central und N-able RMM • **Buchhaltung**: FreshBooks, QuickBooks, Sage, Xero und SnelStart • **VAR**: Microsoft CSP • **Zahlung**: PayPal und Stripe Wenn Sie auf Integrationen zugreifen wollen, gehen Sie im Management-Portal zu **Integrationen**. Weitere Informationen finden Sie im Abschnitt '"Den Advanced Automation Service mit Drittanbieter-Plattformen integrieren" (S. 288)'.
SCHRITT 9: Konfigurieren Sie	Dies ist der letzte Schritt bei der Einrichtung von Advanced Automation.

Schritt	Beschreibung
Ihre E-Mail-Einstellungen	Bevor Sie Ihre E-Mail-Einstellungen konfigurieren, sollten Sie sicherstellen, dass Sie vorher Ihre E-Mail antworten konfiguriert haben. Sobald Sie Ihre Einstellungen für eingehende E-Mails konfiguriert haben, wird Advanced Automation alle Nachrichten in Ihrem festgelegten Posteingang abrufen und (sofern relevant) ein Ticket für jede Nachricht erstellen. Wenn eine E-Mail verarbeitet wurde, wird diese (als zukünftige Referenz) in den Ordner 'Archiv' verschoben. Wenn es keinen Ordner 'Archiv' gibt, wird dieser für Sie erstellt. Es gibt drei E-Mail-Konfigurationen, die eingerichtet werden müssen: • **Eingehende E-Mail**: Dies wird normalerweise so konfiguriert, dass ein Help Desk- oder Support-E-Mail-Konto direkt mit dem Service Desk von Advanced Automation verbunden ist. Eingehende E-Mails werden in Tickets konvertiert und benutzerdefinierte Antworten an den Benutzer gesendet, um diesen zu informieren. • **Ausgehende E-Mail**: Der E-Mail-Server und das Konto, das zum Senden oder Beantworten von Nachrichten verwendet wird. • **Rechnungs-E-Mail**: Der E-Mail-Server und das Konto, das verwendet wird, um Rechnungen an die Kunden zu versenden. Wenn Sie auf die Einstellungen zur E-Mail-Konfiguration zugreifen wollen, gehen Sie zu **Einstellungen –> Service Desk –> Mail-Server-Konfiguration**. Weitere Informationen finden Sie im Abschnitt '"Ihre E-Mail-Einstellungen konfigurieren" (S. 192)'.

Onboarding von bestehenden Kunden

Wenn Advanced Automation für Ihr Konto aktiviert ist (siehe '"Advanced Automation aktivieren" (S. 179)'), müssen Sie Ihre bestehenden Kunden per Onboarding einbinden, um deren Service-Anforderungen abrechnen und verarbeiten zu können.

Gehen Sie folgendermaßen vor, um sicherzustellen, dass Advanced Automation für Ihre bestehenden Kunden korrekt konfiguriert haben:

- Stellen Sie Abrechnungsinformationen für bestehende Kunden bereit.
- Erstellen Sie Verträge, um bestehenden Kunden Ihre Services und Produkte in Rechnung stellen zu können.
- Stellen Sie sicher, dass Sie Service Desk-Tickets für bestehende Kunden empfangen und verarbeiten können.
- Stellen Sie sicher, dass Sie Verkaufsartikel für bestehende Kunden erstellen können.
- Stellen Sie sicher, dass Sie den Abrechnungsprozess durchführen und Rechnungen für bestehende Kunden ausstellen können.

Abrechnungsinformationen bereitstellen

Wenn Advanced Automation aktiviert ist, werden Sie aufgefordert, die Abrechnungsinformationen für Ihre bestehenden Kunden anzugeben, sobald Sie auf den Bereich **Clients** zugreifen. Die Abrechnungsinformationen stellen sicher, dass Sie Advanced Automation nutzen können, um die Service-Anforderungen für Ihre Kunden abzurechnen und zu verarbeiten.

Hinweis
Wenn für einen Kunden keine Abrechnungsinformationen angegeben werden, können Sie keine Kunden-Tickets und Zeiterfassungen genehmigen. Daher werden Sie auch aufgefordert, die Informationen für die spezifizierten Kunden einzugeben, wenn Sie diese Tickets und Anforderungen bearbeiten wollen. Auf ähnliche Weise werden Sie beim Erstellen eines Verkaufsartikels aufgefordert, die Abrechnungsinformationen für den ausgewählten Kunden zu vervollständigen, wenn diese Informationen nicht in der Advanced Automation-Funktionalität definiert wurden. Weitere Informationen finden Sie in den entsprechenden Abschnitten unten.

So können Sie Abrechnungsinformationen für bestehende Kunden hinzufügen

1. Gehen Sie im Management-Portal zu **Organisation –> Clients**.
2. Klicken Sie neben dem relevanten Kundennamen auf das Drei-Punkte-Symbol (...). Wählen Sie im angezeigten Menü **Abrechnungsinformationen hinzufügen**.
   Oder
   Klicken Sie in der angezeigten Liste auf eine Kundenzeile. Klicken Sie in der angezeigten Seitenleiste auf die Registerkarte **Konfigurieren**. Klicken Sie dann auf die Bereiche **Abrechnung** und **Adresse**, um die entsprechenden Abrechnungsinformationen hinzuzufügen.
3. Füllen Sie im angezeigten Formular die entsprechenden Felder aus. Weitere Informationen zu diesen Feldern finden Sie in Abschnitt '"Abrechnungsinformationen für einen Mandanten definieren" (S. 42)'.
4. Klicken Sie auf **Hinzufügen**, um die Festlegung der Abrechnungsinformationen abzuschließen.

   Hinweis
   Wenn Sie die Telefonnummern der Benutzer im Service Desk verwalten und darauf zugreifen wollen, klicken Sie in der gleichen Registerkarte **Konfigurieren** auf den Bereich **Allgemeine Einstellungen** und aktivieren Sie den Schalter **Selbstverwaltetes Kundenprofil aktivieren**. Wenn diese Option aktiviert ist, werden sowohl den Administratoren als auch den Benutzern die relevanten Felder zur Kontaktaufnahme angezeigt, einschließlich der Telefonnummern, des Firmenkontakts und der Stellenbezeichnung. Weitere Informationen finden Sie im Abschnitt '"Selbstverwaltete Kundenprofile konfigurieren" (S. 49)'.

Erstellen Sie Verträge, um bestehenden Kunden Services und Produkte in Rechnung stellen zu können

Verträge gewährleisten, dass Sie die Advanced Automation-Funktionalität nutzen können, um Ihren Kunden regelmäßige Rechnungen stellen zu können.

Wenn die Advanced Automation-Funktionalität aktiviert ist, werden Sie aufgefordert, Verträge für Ihre bestehenden Kunden zu erstellen, wenn Sie auf das Modul **Verkauf und Abrechnung** zugreifen. Diese Aufforderung wird nur angezeigt, wenn einem oder mehreren Kunden Services oder Produkte von Acronis zugewiesen wurden.

So können Sie Verträge für bestehende Kunden erstellen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Wenn Sie durch ein angezeigtes Banner darüber informiert werden, dass einer bestimmten Anzahl von Kunden keine Verträge zugewiesen wurden, klicken Sie auf **Erstellen**.
   Sollten Sie dieses Banner zuvor bereits geschlossen haben, klicken Sie auf den Link **Verträge für bestehende Kunden erstellen**, der sich im oberen rechten Teil der Anzeige befindet.
3. Gehen Sie im Assistenten zum Erstellen eines neuen Vertrags folgendermaßen vor:
   a. Wählen Sie den relevanten Kunden aus und klicken Sie dann auf **Weiter**.
   b. Fügen Sie die Vertragsinformationen hinzu (einschließlich der Zahlungsdetails und des Vertragszeitraums). Weitere Informationen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'. Wenn Sie fertig sind, klicken Sie auf **Weiter**.
   c. Geben Sie die Abrechnungsinformationen ein und klicken Sie dann auf **Weiter**. Beachten Sie, dass dieser Schritt nicht angezeigt wird, wenn Sie bereits Abrechnungsinformationen definiert haben (wie im Abschnitt '"Abrechnungsinformationen bereitstellen" (S. 185)' beschrieben).
   d. Fügen Sie je nach Bedarf Vertragsteile hinzu. Weitere Informationen finden Sie im Abschnitt '"Einen neuen Vertrag erstellen" (S. 226)'. Standardmässig werden der Vertragsvorlage solche Vertragsteile hinzugefügt, die auf Acronis Services basieren, die dem Kunden bereits zugewiesen wurden. Diese Vertragsteile können je nach Bedarf bearbeitet oder gelöscht werden. Achten Sie darauf, dass Sie die richtigen Preise für die Vertragsteile festlegen.
4. Klicken Sie auf **Fertig**. Der Vertrag wird auf der Registerkarte **Verträge** zur Liste der bestehenden Verträge hinzugefügt.

Stellen Sie sicher, dass Sie Service Desk-Tickets für bestehende Kunden empfangen und verarbeiten können

Wenn Advanced Automation aktiviert ist, können Sie für einen bestehenden Kunden Tickets empfangen und verarbeiten – selbst wenn für diesen Kunden keine Abrechnungsinformationen definiert wurden. Dadurch wird sichergestellt, dass Sie Tickets bei Bedarf erstellen, beantworten, auflösen und schließen können. Weitere Informationen zum Arbeiten mit den Service Desk-Funktionen finden Sie im Abschnitt '"Service Desk" (S. 196)'.

Wenn keine Abrechnungsinformationen für den betreffenden Kunden vorliegen, können Sie jedoch die von ihm gemeldete Ticketzeit nicht genehmigen. Wenn Sie versuchen, Ticket-Zeiterfassungen zu genehmigen, werden Sie aufgefordert, die für den relevanten Kunden geltenden Abrechnungsinformationen hinzuzufügen. Weitere Informationen finden Sie im Abschnitt 'Abrechnungsinformationen bereitstellen'.

Stellen Sie sicher, dass Sie Verkaufsartikel für bestehende Kunden erstellen können

Wenn Advanced Automation aktiviert ist, können Sie für einen bestehenden Kunden Verkaufsartikel erstellen – selbst wenn für diesen Kunden keine Abrechnungsinformationen definiert wurden.

Wenn Sie jedoch beim Erstellen eines Verkaufsartikels (siehe Abschnitt '"Verkaufsartikel verwalten" (S. 223)') einen Kunden ohne spezifizierte Abrechnungsinformationen auswählen, werden Sie aufgefordert, diese Abrechnungsinformationen bereitzustellen, bevor Sie mit dem Erstellen des Verkaufsartikels fortfahren können.

Wenn Sie einen bestehenden Verkaufsartikel bearbeiten, können Sie außerdem den bestehenden Kunden, der dem Verkaufsartikel zugewiesen wurde, nicht zu einem Kunden ohne spezifizierte Abrechnungsinformationen ändern. Sie werden aufgefordert, die Abrechnungsinformationen bereitzustellen, bevor Sie mit der Bearbeitung des Verkaufsartikels fortfahren können.

Stellen Sie sicher, dass Sie den Abrechnungsprozess durchführen und Rechnungen für bestehende Kunden ausstellen können

Sie werden beim ersten Fakturierungslauf aufgefordert, die Standardeinstellungen für die Rechnungsnummerierung zu überprüfen, bevor Sie die Rechnungen erstellen. Die Rechnungsnummerierung sollte mit Ihrer Buchhaltungssoftware abgestimmt sein. Dieser Schritt soll sicherstellen, dass Sie Ihre Abrechnungs- und Rechnungsinformationen korrekt festgelegt haben. Weitere Informationen finden Sie im Abschnitt '"Rechnungen" (S. 235)'.

Mit benutzerdefinierten Feldern arbeiten

Durch die Definition von benutzerdefinierten Feldern können Sie zusätzliche (optionale) Informationen für Kunden, Produkte, Verkaufsartikel, Verträge bzw. Vertragsteile sowie Tickets speichern. Benutzerdefinierte Felder werden im neuen Bereich **Zusätzliche Informationen** der jeweiligen Entität aufgeführt.

Sie können beispielsweise benutzerdefinierte Felder hinzufügen, die auf Kunden anwendbar sind. Wenn Sie einen Kunden erstellen oder bearbeiten, können Sie diese vordefinierten benutzerdefinierten Felder im Bereich **Zusätzliche Informationen** vervollständigen, die dann zu den Details des Kunden hinzugefügt werden.

In diesem Abschnitt wird beschrieben, wie Sie ein neues benutzerdefiniertes Feld hinzufügen und wie Sie ein vorhandenes benutzerdefiniertes Feld bearbeiten oder entfernen können.

Hinweis
Diese Funktion ist nur für Benutzer verfügbar, denen die Administrator-Rolle zugewiesen wurde.

Ein benutzerdefiniertes Feld erstellen

So können Sie ein benutzerdefiniertes Feld erstellen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Unternehmensverwaltung** und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Felder**.
2. Klicken Sie auf **+ Neues benutzerdefiniertes Feld**.
3. Definieren Sie Folgendes:
   - Geben Sie im Feld **Name** die Bezeichnung für das benutzerdefinierte Feld ein.
   - Wählen Sie im Feld **Typ** den gewünschten Feldtyp aus einer der folgenden Optionen:
     - Zeichenfolge
     - Ganzzahl
     - Boolesch
     - Text
     - Datum
   - Setzen Sie in der Spalte **Erforderlich** den Optionsschalter auf **Ja**, wenn Sie wollen, dass das Feld zwingend erforderlich ist.
   - Wählen Sie im Feld **Anwenden auf** die gewünschte Entität, auf die das benutzerdefinierte Feld angewendet werden soll:
     - Kunde
     - Produkt
     - Vertrag
     - Vertragsteil
     - Verkaufsartikel
     - Ticket
   - Wählen Sie in der Spalte **Status** zwischen **Aktiv** oder **Inaktiv**.
   - Geben Sie in der Spalte **Sortiernummer** einen numerischen Wert ein, der die Anzeigepräferenz für das benutzerdefinierte Feld definiert. Dies ist relevant, wenn Sie mehrere benutzerdefinierte Felder in einem angezeigten Formular haben. Je niedriger die Zahl, desto höher wird das benutzerdefinierte Feld angezeigt.
4. Klicken Sie auf **Benutzerdefiniertes Feld erstellen**, um ein neues benutzerdefiniertes Feld hinzuzufügen.

Ein benutzerdefiniertes Feld bearbeiten

In diesem Abschnitt wird beschrieben, wie Sie ein vorhandenes benutzerdefiniertes Feld bearbeiten oder entfernen können.

So können Sie ein benutzerdefiniertes Feld bearbeiten

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Unternehmensverwaltung** und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Felder**.
2. Klicken Sie auf die Zeile desjenigen benutzerdefinierten Feldes, das Sie bearbeiten wollen.
3. Führen Sie die gewünschte Bearbeitung durch. Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"Ein benutzerdefiniertes Feld erstellen" (S. 188)'.
4. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie ein benutzerdefiniertes Feld entfernen

Klicken Sie auf der Registerkarte **Benutzerdefinierte Felder** zuerst auf das Drei-Punkte-Symbol (...) in der Zeile desjenigen benutzerdefinierten Feldes, das Sie entfernen wollen, und dann auf **Entfernen**.

Das benutzerdefinierte Feld wird von der Registerkarte **Benutzerdefinierte Felder** entfernt und wird nicht mehr in der betreffenden Entität im Bereich **Zusätzliche Informationen** angezeigt.

Ihre Benutzer verwalten

Wenn Sie Advanced Automation aktiviert haben (siehe Abschnitt '"Advanced Automation aktivieren" (S. 179)'), werden Ihren vorhandenen Benutzern automatisch bestimmte Rollen zugewiesen, damit sie umgehend auf die Advanced Automation-Funktionen zugreifen können. Beachten Sie, dass den Firmenadministratoren standardmäßig die Administrator-Rolle zugewiesen wird. Allen anderen Benutzern wird die Techniker-Rolle zugewiesen, was bei Bedarf jedoch angepasst werden kann.

Sie können bei Bedarf auch Benutzer und Benutzergruppen hinzufügen. Beachten Sie, dass wenn Sie einem Benutzer eine Advanced Automation-Rolle zuweisen, dieser automatisch der vorgegebenen Benutzergruppe zugewiesen wird. Die Einstellungen für Benutzergruppen können im Einstellungsbereich aktualisiert werden (siehe Abschnitt '"Service Desk-Einstellungen" (S. 251)').

Weitere Informationen darüber, wie Sie Advanced Automation-Benutzer im Management-Portal erstellen können, finden Sie im Abschnitt '"Ein Benutzerkonto erstellen" (S. 58)'.

Benutzergruppen verwalten

Benutzern, denen die Rolle Administrator oder Direktor zugewiesen wurde, können Benutzergruppen innerhalb ihrer Organisation verwalten.

So können Sie Ihrer Organisation eine neue Benutzergruppe hinzufügen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Unternehmensverwaltung** und klicken Sie dann auf die Registerkarte **Benutzergruppen**.
   In der angezeigten Liste werden Ihre aktiven und inaktiven Gruppen angezeigt und wie viele Benutzer sich in jeder Gruppe befinden. Diese Gruppen können bearbeitet oder (de)aktiviert werden, wie unten beschrieben.
2. Klicken Sie auf **+ Neu**.

3. Geben Sie einen **Namen der Benutzergruppe** ein.
4. Wählen Sie den **Gruppenleiter** aus.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Gruppe zu aktivieren.
6. Wählen Sie die entsprechenden Benutzer aus der Liste **Benutzer** aus (im rechten Bereich). Klicken Sie dann auf den nach links zeigenden Pfeil, um die Benutzer zur Liste **Gruppenmitglieder** hinzuzufügen.
7. Klicken Sie auf **Neue Gruppe erstellen**.

So können Sie eine Benutzergruppe aktualisieren

1. Klicken Sie in der Registerkarte **Benutzergruppen** auf die Gruppe, die Sie aktualisieren wollen.
2. Klicken Sie in der rechten Seitenleiste auf das Stiftsymbol, wenn Sie die Benutzergruppe bearbeiten wollen. Neben der Möglichkeit zur Aktualisierung des Gruppennamens und Gruppenleiters können Sie außerdem die Gruppenmitglieder bearbeiten sowie die Gruppe (de)aktivieren, indem Sie das Kontrollkästchen **Aktiv** (de)aktivieren.
3. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie eine Benutzergruppe löschen

1. Klicken Sie in der Registerkarte **Benutzergruppen** auf die Gruppe, die Sie löschen wollen.
2. Klicken Sie in der rechten Seitenleiste auf das Papierkorb-Symbol.
   Die Benutzergruppe wird gelöscht.

Hinweis
Sie können eine Benutzergruppe nur dann löschen, wenn sie gerade **Inaktiv** ist und wenn alle Benutzer einer anderen Gruppe, die **Aktiv** ist, zugewiesen sind. Außerdem darf die Gruppe in keiner der Advanced Automation-Einstellungen verwendet werden, z. B. in den standardmäßigen Service Desk-Einstellungen oder den Angebotseinstellungen.

Advanced Automation-Rollen

Der Advanced Automation Service enthält eine Reihe von Rollen, die Sie nach Bedarf auf Ihre Benutzer anwenden können.

Wenn Sie den Advanced Automation Service (wie im Abschnitt '"Advanced Automation aktivieren" (S. 179)' beschrieben) aktivieren, wird allen vorhandenen Benutzern automatisch Zugriff auf die Funktionalität des Advanced Automation Service gewährt. Während des Kontoerstellungsprozesses können Sie jedem Benutzer eine entsprechende Rolle zuweisen. Beachten Sie, dass Management-Portal-Administratoren standardmäßig die Administrator-Rolle zugewiesen wird, während Nur-Lesen-Administratoren die Techniker-Rolle erhalten.

Wenn Sie die Rolle zu einem späteren Zeitpunkt aktualisieren wollen, gehen Sie zu **Unternehmensverwaltung –> Benutzer**, wählen Sie den betreffenden Benutzer aus und aktualisieren Sie auf der Registerkarte **Services** die Rolle. Sie können auf derselben Registerkarte außerdem die Advanced Automations-Funktionalität für diesen bestimmten Benutzer deaktivieren.

In der nachfolgenden Tabelle werden die verfügbaren Rollen sowie die Rechte beschrieben, die den einzelnen Rollen innerhalb des Advanced Automation Service zugewiesen sind:

Rolle	Beschreibung
Techniker	Die Standardrolle, die allen Benutzern zugewiesen wird. Beinhaltet den Zugriff auf die Module Service Desk und Projektmanagement sowie die Zeiterfassungsfunktionalität. Diese Rolle beinhaltet außerdem einen eingeschränkten Zugriff auf die Details von Kunden und deren Endbenutzern.
Personalabteilung	Beinhaltet einen eingeschränkten Zugriff auf die Module Service Desk, Projektmanagement, Berichte und Zeitmanagement.
Finanzen	Beinhaltet den Zugriff auf die Module CRM, Verkauf und Abrechnung, Service Desk, Projektmanagement sowie die Zeiterfassungsfunktionalität. Diese Rolle beinhaltet außerdem einen eingeschränkten Zugriff auf die Finanzstatistiken des Kunden, jedoch keinen Zugriff auf Unternehmensberichte.
Verkauf	Beinhaltet den Zugriff auf die Module CRM, Verkauf, Service Desk und Projektmanagement sowie die Zeiterfassungsfunktionalität. Diese Rolle beinhaltet außerdem einen eingeschränkten Zugriff auf Rechnungsdaten, jedoch keinen Zugriff auf Unternehmensberichte.
Gruppenleiter	Beinhaltet den Zugriff auf die Module CRM, Service Desk und Projektmanagement. Diese Rolle beinhaltet außerdem den vollständigen Zugriff auf die Finanzstatistiken und Unternehmensberichte des Kunden, die Zeitmanagement-Funktionalität sowie einen eingeschränkten Zugriff auf das Modul Verkauf.
Finanzdirektor	Beinhaltet den Zugriff auf die Module CRM, Verkauf und Abrechnung, Service Desk sowie Projektmanagement. Diese Rolle beinhaltet außerdem den vollständigen Zugriff auf die Finanzstatistiken und Unternehmensberichte des Kunden sowie die Zeitmanagement-Funktionalität.
Direktor	Beinhaltet den Zugriff auf alle Module, jedoch ohne die Fähigkeit, globale Firmeneinstellungen zu verwalten.
Administrator	Vollständige Zugriffsrechte sowie die Fähigkeit, die globalen Firmeneinstellungen für den Service Desk, die Abrechnung und Rechnungsstellung verwalten zu können.
*Die nachfolgenden Rollen sind für die Benutzer Ihrer Kunden verfügbar (wählen Sie den betreffenden Kunden aus und gehen Sie dann zu **Unternehmensverwaltung –> Benutzer**). Wenn Benutzer zum ersten Mal hinzugefügt werden, erhalten diese den Status 'Inaktiv' und es wird eine Einladungs-E-Mail an den Benutzer*	

Rolle	Beschreibung
gesendet. Sie können deren Zugriff auf den Advanced Automation Service jederzeit aktivieren oder deaktivieren.	
Kunde	Beinhaltet den Zugriff auf das Service Desk-Modul (beschränkt auf die Organisation eines Kunden).
Client-Manager	Beinhaltet den Zugriff auf die Module Service Desk, Rechnungen und Berichte (beschränkt auf die Organisation eines Kunden).

Ihre E-Mail-Einstellungen konfigurieren

Die Advanced Automation-Erweiterung verfügt über einen integrierten E-Mail-Parser, der eingehende E-Mails in Tickets umwandeln kann. Wenn Sie diese Funktion verwenden wollen, stellen Sie sicher, dass Sie ein dediziertes E-Mail-Konto oder ein Test-E-Mail-Konto verwenden. Beachten Sie darüber hinaus Folgendes:

- Verwenden Sie kein persönliches E-Mail-Konto mit derselben Adresse wie ein Cyber Protect Cloud-Benutzerkonto.
- Alle *ungelesenen* Nachrichten, die das System in Ihrem Posteingang findet, werden in Tickets umgewandelt.
- Benutzern, die nicht in Cyber Protect Cloud vorhanden sind, können keine Tickets zugewiesen werden, weil es für diese Benutzer dann keine Verbindung mit einer E-Mail-Adresse gibt.
- Sobald eine E-Mail-Nachricht verarbeitet wurde, wird diese von der Advanced Automation-Erweiterung in einen Archiv-Ordner verschoben (sie wird also nicht gelöscht):
  - Wenn kein Archivordner vorhanden ist, wird er erstellt.
  - Wenn Sie einen anderen E-Mail-Dienst als Microsoft 365 oder Gmail verwenden, stellen Sie sicher, dass dieser RFC 6851 unterstützt.

Um auf die Mail-Server-Einstellungen zuzugreifen, gehen Sie zu **Einstellungen –> Service Desk –> Mail-Server-Konfiguration**.

Hinweis
Die Konfiguration des Mail-Servers für ausgehende Rechnungen und eingehende Tickets ist nur verfügbar, wenn der Advanced Automation Service aktiviert ist. Auf diese Funktionalität wird auch beim ersten Onboarding mit der Advanced Automation-Erweiterung zugegriffen (wie in Abschnitt '"Advanced Automation aktivieren" (S. 179)' beschrieben).

Die Einstellungen für ausgehende E-Mails definieren

Hinweis
Kontaktieren Sie Ihren E-Mail-Administrator, um Informationen zur Einrichtung Ihres Servers zu erhalten.

1. Gehen Sie zu **Einstellungen –> Service Desk –> Mail-Server-Konfiguration**. Auf der Anzeige 'E-Mail-Server konfigurieren' wird standardmäßig die Registerkarte **Einstellungen für ausgehende E-Mails** angezeigt.
2. Klicken Sie auf den Optionsschalter **Aktiv**, um ausgehende E-Mails zu ermöglichen.
3. Wählen Sie den passenden Mail-Server-Protokolltyp aus einer der folgenden Möglichkeiten aus:
   - SMTP (Standard)
   - Exchange
   - Office365
4. Wenn Sie SSL verwenden wollen, aktivieren Sie das Kontrollkästchen **SSL aktivieren**. Mit SSL (Secure Sockets Layer) werden Ihre E-Mail-Nachrichten während der Übertragung verschlüsselt, wobei dies nur in diesen Szenarien unterstützt wird:
   - Sicher (TLS) – StartTLS – Port 587
   - Sicher (SSL) – SSL – Port 465
5. Geben Sie den Namen des Hosts und dessen Port ein.
6. Geben Sie den Benutzernamen und das Kennwort des Kontos ein.
7. Geben Sie in das Feld **Von** den Benutzernamen des Kontos ein. Wenn Sie den Protokolltyp Office365 ausgewählt haben, beachten Sie, dass dieser E-Mail-Alias-Adressen in einem einzigen Postfach unterstützt. Wenn Sie eine dieser Adressen als Absenderadresse verwenden wollen, verwenden Sie dieses Feld. Es werden nur E-Mail-Adressen verwendet, die mit dem Office365-Konto assoziiert sind. Das System täuscht keine Adressen vor.
8. Geben Sie den Wert für **Zeitlimit** in Millisekunden ein. Dieser Wert spezifiziert, wie lange das System auf eine erfolgreiche Verbindung zu Ihrem E-Mail-Server warten soll, bevor es zu einer Zeitüberschreitung kommt. Wenn Sie SMTP als Protokolltyp verwenden, aktivieren Sie das Kontrollkästchen **Erfordert Authentifizierung**.
9. Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen für ausgehende E-Mails zu überprüfen. Sobald das System alle Ihre Einstellungen überprüft hat, wird eine Bestätigungsmeldung angezeigt.
10. Klicken Sie auf **Speichern**, damit Ihre Einstellungen angewendet werden.

    Sie können auch Einstellungen für die Rechnungs-E-Mails, die Sie an Kunden senden (siehe Abschnitt '"Die E-Mail-Einstellungen für ausgehende Rechnungen definieren" (S. 193)'), sowie für eingehende E-Mails (siehe Abschnitt '"Die Einstellungen für eingehende E-Mails definieren" (S. 194)') vornehmen.

Die E-Mail-Einstellungen für ausgehende Rechnungen definieren

Hinweis
Kontaktieren Sie Ihren E-Mail-Administrator, um Informationen zur Einrichtung Ihres Mail-Servers zu erhalten.

Mit den E-Mail-Einstellungen für Rechnungen können Sie Ihren Mail-Server konfigurieren, damit dieser zum Versenden von Rechnungen an Ihre Kunden verwendet werden kann.

So können Sie Ihre E-Mail-Einstellungen für Rechnungen definieren

1. Gehen Sie zu **Einstellungen –> Service Desk –> Mail-Server-Konfiguration**.
2. Klicken Sie in der Anzeige zur Konfiguration des E-Mail-Servers auf **Rechnungs-E-Mail**.
3. Klicken Sie auf den Optionsschalter **Aktiv**, um ausgehende Rechnungs-E-Mails zu ermöglichen.
4. Wählen Sie den passenden Mail-Server-Protokolltyp aus einer der folgenden Möglichkeiten aus:
   - SMTP (Standard)
   - Exchange
   - Office365
5. Wenn Sie SSL verwenden wollen, aktivieren Sie das Kontrollkästchen **SSL aktivieren**. Mit SSL (Secure Sockets Layer) werden Ihre E-Mail-Nachrichten während der Übertragung verschlüsselt, wobei SSL nur bei diesen Szenarien unterstützt wird: Sicher (TLS) – StartTLS – Port 587Secure (SSL) – SSL – Port 465
6. Geben Sie den Namen des Hosts und dessen Port ein.
7. Geben Sie den Benutzernamen und das Kennwort des Kontos ein.
8. Geben Sie in das Feld **Von** den Benutzernamen des Kontos ein. Wenn Sie den Protokolltyp Office365 ausgewählt haben, beachten Sie, dass dieser E-Mail-Alias-Adressen in einem einzigen Postfach unterstützt. Wenn Sie eine dieser Adressen als Absenderadresse verwenden wollen, verwenden Sie dieses Feld. Es werden nur E-Mail-Adressen verwendet, die mit dem Office365-Konto assoziiert sind. Das System täuscht keine Adressen vor.
9. Geben Sie den Wert für **Zeitlimit** in Millisekunden ein. Dieser Wert spezifiziert, wie lange das System auf eine erfolgreiche Verbindung zu Ihrem E-Mail-Server warten soll, bevor es zu einer Zeitüberschreitung kommt. Wenn Sie SMTP als Protokolltyp verwenden, aktivieren Sie das Kontrollkästchen **Erfordert Authentifizierung**.
10. Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen für ausgehende E-Mails zu überprüfen. Sobald das System alle Ihre Einstellungen überprüft hat, wird eine Bestätigungsmeldung angezeigt.
11. Klicken Sie auf **Speichern**, damit Ihre Einstellungen angewendet werden.

    Sie können auch Einstellungen für ausgehende (siehe Abschnitt '"Die Einstellungen für ausgehende E-Mails definieren" (S. 192)') und eingehende E-Mails (siehe Abschnitt '"Die Einstellungen für eingehende E-Mails definieren" (S. 194)') vornehmen.

Die Einstellungen für eingehende E-Mails definieren

Hinweis
Kontaktieren Sie Ihren E-Mail-Administrator, um Informationen zur Einrichtung Ihres Mail-Servers zu erhalten.

In den Einstellungen für eingehende E-Mails können Sie Ihren Mail-Server konfigurieren, sodass Sie E-Mails von Ihren Kunden empfangen können. Advanced Automation kann diese E-Mails dann

automatisch in Tickets umwandeln und diese dem entsprechenden Benutzer oder Unternehmen zuweisen.

Wichtig
Wenn die E-Mail-Integration aktiviert ist, wird das Postfach des spezifizierten Kontos von Advanced Automation verwaltet. Alle ungelesenen Nachrichten werden automatisch verarbeitet und in den Archiv-Ordner verschoben.

So können Sie Ihre Einstellungen für eingehende E-Mails definieren

1. Gehen Sie zu **Einstellungen –> Service Desk –> Mail-Server-Konfiguration**.
2. Klicken Sie in der Anzeige zur Konfiguration des E-Mail-Servers auf **Eingehende E-Mails**.
3. Klicken Sie auf den Optionsschalter **Aktiv**, um eingehende E-Mails zu ermöglichen.
4. Wählen Sie den passenden Mail-Server-Protokolltyp aus einer der folgenden Möglichkeiten aus:
   - IMAP (Standard)
   - Exchange
   - Office365
5. Wenn Sie SSL verwenden wollen, aktivieren Sie das Kontrollkästchen **SSL aktivieren**. Mit SSL (Secure Sockets Layer) werden Ihre E-Mail-Nachrichten während der Übertragung verschlüsselt, wobei SSL nur bei diesen Szenarien unterstützt wird: Sicher (TLS) – StartTLS – Port 587Secure (SSL) – SSL – Port 465
6. Geben Sie den Namen des Hosts und dessen Port ein.
7. Geben Sie den Benutzernamen und das Kennwort des Kontos ein.
8. Geben Sie den Wert für **Zeitlimit** in Millisekunden ein. Dieser Wert spezifiziert, wie lange das System auf eine erfolgreiche Verbindung zu Ihrem E-Mail-Server warten soll, bevor es zu einer Zeitüberschreitung kommt.
9. Aktivieren Sie das Kontrollkästchen **Nachrichten von unbekannten Absendern verarbeiten**, um sicherzustellen, dass Nachrichten von unbekannten Absendern konvertiert werden, wobei die Tickets jedoch nicht automatisch einem Benutzer oder Unternehmen zugewiesen werden. Wenn diese Option nicht aktiviert ist, wird eine E-Mail, die von einer Adresse kommt, die nicht in der Kundendatenbank enthalten ist, nicht in ein Ticket umgewandelt.
10. Aktivieren Sie das Kontrollkästchen **Keine Nachricht verarbeiten, die vor dem spezifizierten Datum empfangen wurde**, um sicherzustellen, dass Tickets nur für solche E-Mails erstellt werden, die nach einem spezifizierten Datum empfangen wurden. Diese Option verhindert, dass Tickets automatisch für alle vorhandenen E-Mails erstellt werden, auch für solche, die empfangen wurden, bevor Sie Ihre Einstellungen für eingehende E-Mails definiert haben. Wenn das Kontrollkästchen aktiviert ist, werden zusätzliche Datums- und Zeitfelder angezeigt.
11. Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen für eingehende E-Mails zu überprüfen. Sobald das System alle Ihre Einstellungen überprüft hat, wird eine Bestätigungsmeldung angezeigt.
12. Klicken Sie auf **Speichern**, damit Ihre Einstellungen angewendet werden.

Sie können auch Einstellungen für die Rechnungs-E-Mails, die Sie an Kunden senden (siehe Abschnitt '"Die E-Mail-Einstellungen für ausgehende Rechnungen definieren" (S. 193)'), sowie für andere ausgehende E-Mails (siehe Abschnitt '"Die Einstellungen für ausgehende E-Mails definieren" (S. 192)') vornehmen.

Ihren Service Desk und Ihre Zeiteinträge verwalten

Über das Modul **Task-Verwaltung** von Advanced Automation können Sie Ihren Service Desk und Ihre Zeiteinträge verwalten.

- **Service Desk**: Hier können Sie Anfragen an den Kunden-Service verwalten sowie Service-Aktivitäten planen und nachverfolgen.
- **Zeiteinträge**: Hier können Sie als administrativer Benutzer oder Manager Ihre Zeiterfassungen verwalten, Ticketzeiten zur Abrechnung genehmigen, einen freien Tag anfordern und Urlaubstage genehmigen.

Hinweis
Sie können auch die dedizierte, aber auch eingeschränktere Applikation für Mobilgeräte („Acronis Advanced Automation“, kann im Apple App Store oder Google Play Store heruntergeladen werden) verwenden, um mit Service Desk-Tickets und Zeiteinträgen zu arbeiten.

Service Desk

Mit dem **Service Desk**-Modul können Sie Ihre Tickets erstellen, aktualisieren und planen.

Wenn Sie auf die Service Desk-Funktionalität zugreifen wollen, gehen Sie im Management-Portal zu **Task-Verwaltung –> Service Desk**. Auf den beiden angezeigten Registerkarten (**Tickets** und **Scheduler**) können Sie die Tickets der kompletten Organisation und deren Statuszustände (einschließlich Kundenbewertungen) einsehen. Sie können außerdem:

- Neue Tickets erstellen
- Aktuelle Tickets überprüfen und aktualisieren
- Tickets zusammenführen
- Benutzerdefinierte Ticket-Filter erstellen und ändern
- Tickets planen
- Ticket-Daten exportieren

Hinweis
Benutzer, denen die Rollen 'Client-Manager' oder 'Kunde' zugewiesen wurden, haben nur einen eingeschränkten Zugriff auf die oben genannten Service Desk-Funktionalitäten. Sie können Tickets erstellen, überprüfen und ändern (mit einigen Einschränkungen, wie in der Anleitung für Kunden-Administratoren beschrieben). Sie können außerdem bei Bedarf Ticket-Daten exportieren, jedoch keine Tickets planen oder zusammenführen.

Der Prozess der Ticket-Erstellung

Advanced Automation erstellt und aktualisiert Service Desk-Tickets, wenn er die E-Mail-Adresse in den E-Mails erkennt, die an den Advanced Automation Mail Parser weitergeleitet werden.

Beachten Sie, dass Sie bei Bedarf die Einstellungen für den eingehenden und ausgehenden E-Mail-Server konfigurieren können (siehe Abschnitt '"Ihre E-Mail-Einstellungen konfigurieren" (S. 192)').

Neue Service Desk-Tickets werden erstellt, wenn:

- Eine neue ungelesene E-Mail aus einem neuen Thread erkannt wird.
- Eine neue ungelesene E-Mail aus einem bestehenden E-Mail-Thread erkannt wird, aber ein dazugehöriges Ticket bereits geschlossen wurde.
- Ein Benutzer anhand seiner E-Mail-Adresse identifiziert wird.
- Ein Benutzer nicht anhand seiner E-Mail-Adresse identifiziert wird, aber die Einstellungen für eingehende E-Mails (siehe Abschnitt '"Die Einstellungen für eingehende E-Mails definieren" (S. 194)') es zulassen, dass Tickets von unbekannten Absendern eingereicht werden können.
- Tickets können auch manuell erstellt werden, wie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)' beschrieben.

Hinweis
Wenn ein Benutzer anhand seiner E-Mail-Adresse identifiziert wird, wird das neue Ticket auch mit der Firma des Benutzers, der Standard-SLA, der Standardpriorität, der Standardkategorie, dem Standard-Supportbenutzer und allen mit diesem Benutzer verbundenen Geräten verknüpft.

Bestehende Tickets werden aktualisiert, wenn:

- Eine ungelesene E-Mail aus einem bestehenden E-Mail-Thread identifiziert wird und das entsprechende Ticket nicht geschlossen wurde.
- Tickets können auch manuell aktualisiert werden, wie im Abschnitt '"Tickets aktualisieren" (S. 200)' beschrieben.

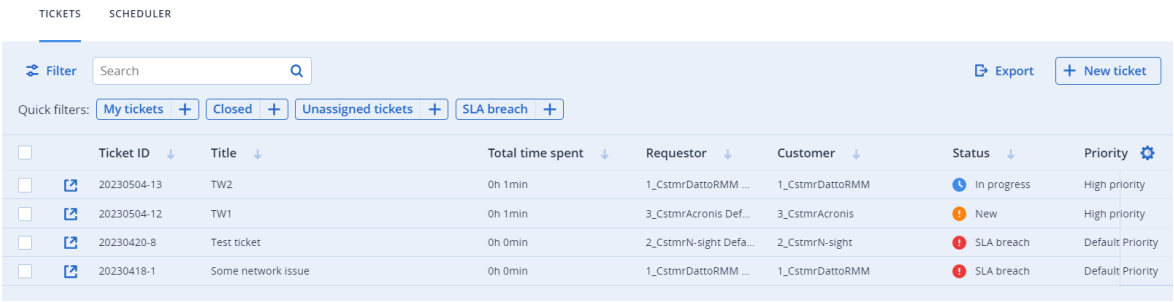
Ein neues Ticket erstellen

Neben der Möglichkeit, dass Advanced Automation Tickets automatisch erstellt (siehe Abschnitt '"Der Prozess der Ticket-Erstellung" (S. 197)'), können Sie ein Ticket, wie unten beschrieben, auch manuell erstellen.

Hinweis
Wenn Sie ein Ticket erstellen oder bearbeiten, werden viele Werte mit den standardmäßigen Service Desk-Einstellungen vorausgefüllt. Diese Einstellungen können bei Bedarf aktualisiert werden (wie im Abschnitt '"Service Desk-Einstellungen" (S. 251)' beschrieben).

So können Sie ein neues Ticket erstellen

1. Gehen Sie zu **Task-Verwaltung –> Service Desk**. Standardmäßig wird die Registerkarte **Tickets** angezeigt, auf der alle aktuellen Tickets der Organisation aufgeführt sind.

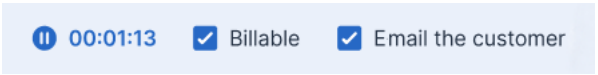


2. Klicken Sie auf **+ Neues Ticket**. Das Fenster 'Neues Ticket erstellen' wird angezeigt.

Hinweis
Wenn Advanced Automation für Ihr Konto aktiviert ist, können Sie auch in der Symbolleiste des Management-Portals am oberen Bildschirmrand auf **Neu –> Kunden-Ticket** klicken (selbst wenn Sie sich nicht im Service Desk-Modul befinden). Durch diese Option wird automatisch der Dialog 'Neues Ticket erstellen' geöffnet, über den Sie ein Ticket erstellen können (wie in den folgenden Schritten beschrieben).

---

3. In der Kopfzeile wird der Ticket-Timer angezeigt. Dieser Timer kann bei Bedarf von den Benutzern, die an dem Ticket arbeiten, pausiert und wieder gestartet werden. Beachten Sie, dass Sie den Ticket-Timer auch so einstellen können, dass er automatisch pausiert wird, wenn der Benutzer die Ticket-Anzeige verlässt (siehe Abschnitt '"Standardwerte festlegen" (S. 256)').



Zusätzlich zum Ticket-Timer können Sie bei Bedarf auch die folgenden Kontrollkästchen aktivieren:

- **Abrechenbar**: Diese Option ist standardmäßig aktiviert und legt fest, ob das Ticket fakturierbar ist. Je nach der auf das Ticket angewendeten SLA (siehe die unteren Schritte) kann das Kontrollkästchen auch aktiviert oder deaktiviert werden. Wenn die SLA beispielsweise vom Typ **Nachträgliche Berechnung** ist, wird das Kontrollkästchen aktiviert (um sicherzustellen, dass die auf dem Ticket angemeldete Arbeit abrechenbar ist). Wenn die SLA vom Typ **Festpreis** ist, ist das Kontrollkästchen deaktiviert (um sicherzustellen, dass die Arbeit am Ticket nicht abrechenbar ist).
- **E-Mail an den Kunden senden**: Diese Option ist standardmäßig aktiviert und definiert, ob Ticket-Aktualisierungen per E-Mail an den Endbenutzer gesendet werden.

4. Definieren Sie Folgendes:
   - Geben Sie im Feld **Ticket-Titel** den Titel für das Ticket ein.
   - Fügen Sie im Bereich **Kundeninformationen** die Kundendetails hinzu – wozu auch der jeweilige Endbenutzer gehört, der das Ticket angefordert hat, sowie dessen Manager. Klicken Sie auf das Feld **Endbenutzer**, um den Benutzer aus der angezeigten Liste auszuwählen. Die anderen Felder werden automatisch ausgefüllt, sofern dies erforderlich ist.

- Wählen Sie im Bereich **Konfigurationselement oder Service** entweder **Verwalteter Service** oder **IKT-Service**:
  - **Verwalteter Service**: Diese Option wird ausgewählt und mit den relevanten Details vorausgefüllt, wenn der Produkttyp 'Verwalteter Service' im Vertrag verfügbar ist. Wenn die Option ausgewählt ist, suchen Sie den Vertragsteil, dem das Gerät zugewiesen ist, und überprüfen Sie dann die SLA für diesen Vertragsteil und wenden Sie diese auf das Ticket an. Beachten Sie, dass diese Option deaktiviert ist, wenn der Vertrag keine Produkte des Typs 'Verwalteter Service' enthält.
  - **IKT-Service**: Diese Option wird ausgewählt und mit den relevanten Details vorausgefüllt, wenn der Produkttyp 'IKT-Service' (Informations- und Kommunikationstechnologie) im Vertrag verfügbar ist. Wenn die Option ausgewählt ist, wird die SLA aus dem Vertragsteil 'IKT Service' auf das Ticket angewendet. Beachten Sie, dass diese Option deaktiviert ist, wenn der Vertrag keine Produkte des Typs 'IKT-Service' enthält.
  - Das Feld **Konfigurationselement** zeigt die Geräte an, die mit dem ausgewählten 'Verwalteten Service' oder 'IKT-Service' verbunden sind (wenn es keine Integrationen gibt oder das Gerät unbekannt ist, wird **Unbekanntes KE** angezeigt). Die Auswahl eines Geräts nach der Auswahl eines Services ist optional (wenn Sie in diesem Szenario ein Gerät auswählen, wird die SLA nicht geändert, sondern bleibt die SLA, die zu dem Service gehört). Wenn das Konfigurationselement mit einem bestimmten Benutzer verknüpft wurde (siehe Abschnitt '"Konfigurationselemente einsehen" (S. 279)'), wird das entsprechende Gerät beim Erstellen des Tickets automatisch mit dem Ticket assoziiert.

    Hinweis
    Zu den verknüpften Geräten gehören auch solche mit Produkten und Services von Acronis (wie etwa Cyber Disaster Recovery Cloud oder Cyber Protection) sowie RMM-Integrationen. Wenn das Acronis Produkt oder die RMM-Integration eine Remote-Steuerungsoption für ein aufgeführtes Gerät bietet, können Sie vom Ticket aus eine Remote-Verbindung über das RDP-Protokoll oder den HTML5-Client herstellen.

  - Wählen Sie in den Feldern **Priorität** und **SLA** die entsprechende Ticket-Priorität und SLA.
- Wählen Sie im Bereich **Support-Agent** den entsprechenden Benutzer, der dem Ticket zugewiesen werden soll. Sie können auch eine **Kategorie** für das Ticket sowie eine **Support-Gruppe** auswählen (falls relevant).
- Im Bereich **Ticket-Beschreibung** können Sie:
  - Den gewünschten **Status** für das Ticket auswählen (standardmäßig wird **Neu** angezeigt).
  - Geben Sie ausführliche Textbeschreibungen und Kommentare in das angezeigte Textfeld ein (es sind auch Bilder und andere Mediendateien bis zu einer Größe von 25 MB möglich). Jedes der folgenden Datei-Formate bzw. -Typen kann hinzugefügt oder per Drag & Drop in das Textfeld gezogen werden:
    - Medien: .avi, .mp4, .mp3
    - E-Mails: .eml, .msg
    - Bilder: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg

        - Dokument- und Protokolldateien: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
        - Archive: .zip, .rar
    - Klicken Sie in das Feld **Vorgefertigte Antwort**, um eine bereits vordefinierte Antwortsvorlage auszuwählen. Beachten Sie: Wenn Sie eine vorgefertigte Antwort auswählen, wird diese die ausführliche Textbeschreibung und Kommentare ersetzen (siehe vorherigen Punkt). Weitere Informationen über das Definieren von vorgefertigten Antworten finden Sie im Abschnitt '"Eine vorgefertigte Antwort erstellen" (S. 251)'.
    - Klicken Sie in das Feld **Art der Abrechnungsaktivität**, um das relevante Produkt auszuwählen. Beachten Sie, dass nur Produkte verfügbar sind, denen das Attribut **Produkt für aktivitätsbasierte Ticket-Abrechnung** zugewiesen wurde.

  Beachten Sie, dass der Bereich **Ticket-Beschreibungen** in den Service-Desk-Einstellungen als zwingend erforderlich festgelegt werden kann (siehe Abschnitt '"Service Desk-Einstellungen" (S. 251)').
- Aktivieren Sie das Kontrollkästchen **Ticket planen**, wenn Sie das Ticket mit einer gewünschten Startzeit, einem Datum und einer Dauer planen wollen. Siehe auch Abschnitt '"Tickets planen" (S. 203)'.
- Fügen Sie im Bereich **Anhänge** alle relevanten Anhänge hinzu, indem Sie diese per Maus auswählen.
- Wählen Sie im Bereich **Abrechenbare Elemente** die gewünschten Ticket-Produkte per Maus aus, die mit dem Ticket verknüpft werden sollen.
- Fügen Sie im Bereich **Interne Notizen** bei Bedarf Notizen und Aktionen hinzu.

5. Klicken Sie auf **Erstellen**. Wenn das Ticket generiert wird, wird es der Registerkarte **Tickets** hinzugefügt.

Hinweis
Sobald Sie Tickets erstellt haben, können Sie Ihre Ticket-Daten jederzeit exportieren, indem Sie auf der Registerkarte **Tickets** auf **Exportieren** klicken. Es wird automatisch eine Excel-Datei auf Ihren Workload heruntergeladen.

Tickets aktualisieren

So können Sie ein Ticket aktualisieren

1. Gehen Sie zu **Task-Verwaltung –> Service Desk**. Als Grundeinstellung wird die Registerkarte **Tickets** angezeigt.
2. (Optional) Wenn Sie eine große Anzahl von Tickets haben, können Sie den Filter verwenden, um ein bzw. mehrere relevante Tickets zu finden.

   Klicken Sie auf **Filter** (oder **Gespeicherte Filter**, wenn Sie bereits einen Filter definiert haben) und wählen Sie die relevanten Werte in den angezeigten Feldern aus. Beachten Sie, dass Sie auf den Optionsschalter **Zu gespeicherten Filtern hinzufügen** klicken können, wenn Sie den definierten Filter zur späteren Verwendung speichern wollen. Advanced Automation verfügt

zudem über eine Reihe von vordefinierten Filtern, die je nach Bedarf ausgewählt werden können.

Alternativ können Sie auch die Leiste **Suchen** verwenden, um ein bzw. mehrere relevante Tickets zu finden.

3. Klicken Sie in der Registerkarte **Tickets** auf den Link in der Ticket-Zeile.

   Wenn Sie mehrere Tickets bearbeiten wollen, müssen Sie die relevanten Tickets auf der Registerkarte **Tickets** auswählen und dann auf **Massenbearbeitung** klicken. Die Änderungen, die Sie hier vornehmen, werden auf alle ausgewählten Tickets angewendet.

   Klicken Sie auf  , wenn Sie ein spezielles Ticket in einer neuen Browser-Registerkarte öffnen wollen.

4. Passen Sie das Ticket nach Bedarf auf einer der angezeigten Registerkarten an:

   - **Aktivitäten**: Zeigt die jüngsten Aktivitäten zu einem Ticket an – darunter den aktuellen Status und die Kommentare, die zu diesem Ticket abgegeben wurden. Sie können das Ticket auch mit anderen Tickets zusammenführen (siehe den Abschnitt '"Tickets zusammenführen" (S. 205)') und das Ticket planen (siehe den Abschnitt '"Tickets planen" (S. 203)').

     Beachten Sie, dass Sie auf dieser Registerkarte den Status des Tickets ändern können. Sie können den Status beispielsweise auf **Wird bearbeitet** ändern, wenn Sie mit dessen Bearbeitung beginnen, oder auf **Geschlossen**, wenn das Ticket abgeschlossen werden kann. Wenn der Status auf **Geschlossen** geändert wird, wird eine E-Mail mit einer Anfrage zur Ticket-Bewertung an den Kunden gesendet. Weitere Informationen finden Sie im Abschnitt '"Kunden-Feedback zu Tickets erhalten" (S. 205)'.

     Sie können auch alle früheren Aktualisierungen an dem Ticket ändern, die im unteren Bereich der Registerkarte **Aktivitäten** aufgeführt sind. Klicken Sie zuerst auf das Pfeilsymbol neben der relevanten Ticket-Aktualisierung und dann im erweiterten Bereich auf das Stiftsymbol, um die Dauer und/oder vorhandene Kommentare zu ändern.

     Hinweis
     Wenn Sie den Status eines Tickets, das durch einen Alarm in der Cyber Protect-Konsole erstellt wurde, auf **Geschlossen** ändern, wird auch der entsprechende Alarm in der Cyber Protect-Konsole geschlossen.

   - **Überblick**: Zeigt allgemeine Ticket-Einstellungen, Kundendetails und Kontakte an, die bei Bedarf geändert werden können. Weitere Informationen finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

     Sie können auch Geräte ändern, die mit einem Ticket verknüpft sind. Wenn beispielsweise ein Ticket erstellt wird, das nicht das richtige Gerät enthält, können Sie auf das Listenfeld **Konfigurationselement** klicken, um das relevante Gerät auszuwählen.

     Alternativ können Sie auch auf **Remote-Desktop öffnen** klicken, um eine Remote-Verbindung mit dem ausgewählten Gerät herzustellen. Oder wählen Sie **Zu Gerät gehen**, wenn Sie weitere Optionen sehen wollen, die für das derzeit verbundene Gerät verfügbar sind. Zu diesen Optionen gehört gegebenenfalls auch ein Zugriff auf die integrierte RMM-Plattform:

- **Ansicht 'Aktive Probleme'**: Dadurch wird eine externe Liste mit Problemen in der RMM-Plattform geöffnet.
- **Geräte-Seite – Registerkarte 'Status'**: Dadurch wird eine externe RMM-Seite mit allgemeinen Informationen über das Gerät geöffnet.
- **Geräte-Seite – Registerkarte 'Eigenschaften'**: Dadurch wird eine externe RMM-Seite mit den Eigenschaften des Gerätes geöffnet.

Hinweis
Die Option, eine Remote-Verbindung mit dem ausgewählten Gerät herzustellen, wird derzeit nur von den Integrationen für Datto RMM, N-able N-Central und N-able RMM unterstützt. Bei Geräten, die von der Acronis Plattform verwaltet werden (z.B. mithilfe eines Acronis Agenten), können Sie von einem Ticket aus direkt zu den Details des verknüpften Geräts gehen und dessen Details einsehen, eine Remote-Verbindung initiieren (falls anwendbar und für das Gerät erlaubt), das Gerät verwalten und so weiter.

- **Abrechenbare Elemente**: Zeigt alle fakturierbaren Elemente an, die auf das Ticket angewandt wurden und die bei Bedarf aktualisiert werden können. Dem Ticket können auch Produkte hinzugefügt werden. Sobald das Ticket geschlossen und dessen Zeitdaten verarbeitet werden, wird automatisch ein Verkaufsartikel für diese Produkte erstellt.
  Diese Funktionalität ermöglicht Ihnen, Ihren Kunden zusätzliche Aktivitäten und Services als Bestandteil des Tickets in Rechnung zu stellen. Beispielsweise stundenweise abrechenbare Beratungsdienste, Netzwerkkabel oder Software-Lizenzen. Verkaufsartikel können auf die übliche Weise berechnet werden.
  Beachten Sie Folgendes:
  - Es können nur solche Produkte, die als **Ticket-Produkte** (in den Einstellungen des Produkts) definiert sind, als zusätzlich abrechenbare Elemente zu den Tickets hinzugefügt werden.
  - Sie müssen das Produkt, dessen Preis und dessen Anzahl festlegen.
  - Techniker können den Standardproduktpreis nicht ändern, wenn das Kontrollkästchen **Preis durch den Techniker anpassbar** in den Produkteinstellungen nicht ausgewählt ist.
- **Interne Informationen**: Zeigt alle internen Notizen oder Aktionen an, die auf das Ticket angewendet wurden. Sie können Notizen oder Aktionen nach Bedarf hinzufügen.
- **Letzte Tickets**: (Nur Lesen) Zeigt die letzten drei Tickets von einem bestimmten Benutzer sowie die letzten drei Tickets von einem Kunden an.

Hinweis
Die Registerkarten **Abrechenbare Elemente**, **Interne Informationen** und **Letzte Tickets** werden Benutzern, denen die Rollen Client-Manager oder Client zugeordnet wurden, nicht angezeigt.

Weitere Informationen über die verschiedenen Felder, die bei der Bearbeitung eines Tickets verfügbar sind, finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

5. Klicken Sie auf **Änderungen speichern**.

Tickets planen

Auf der Registerkarte **Scheduler** werden alle Tickets angezeigt, die für Sie und, wenn Ihnen die Rolle des Gruppenleiters zugewiesen wurde, für Ihr Team geplant sind. Auf dieser Registerkarte können Sie die pro Tag zugeordneten Tickets leicht identifizieren und auf eine monatliche, wöchentliche oder tägliche Ansicht umschalten. Sie können außerdem Tickets für sich selbst oder (falls Sie ein Gruppenleiter sind) für Ihre Gruppe planen.

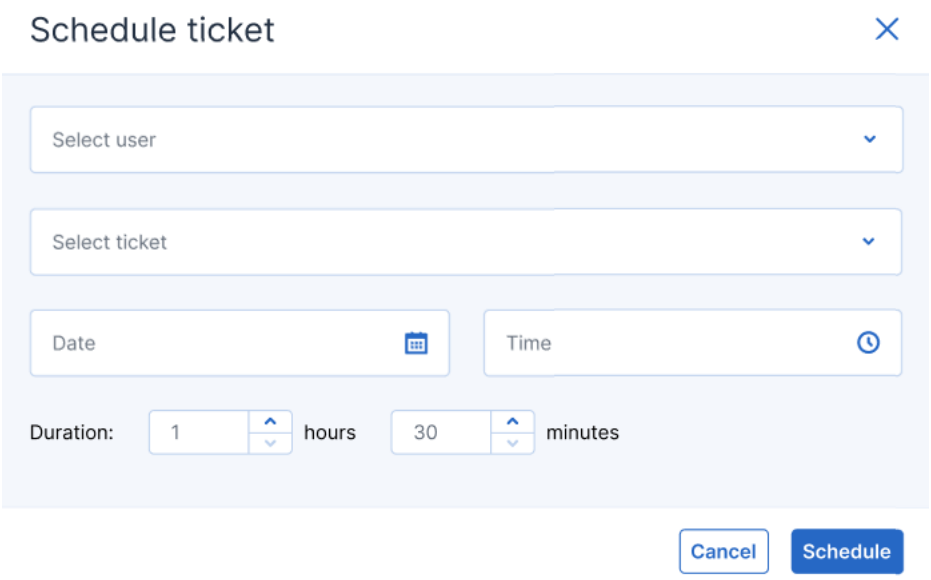
Sie können ein Ticket auch aus dem Ticket selbst heraus planen, wie unten beschrieben.

Die Registerkarte **Scheduler** ermöglicht es Ihnen auch, neue Zeiterfassungen hinzuzufügen sowie die Registerkarte **Scheduler** mit Ihrem Microsoft Outlook-Kalender zu synchronisieren. Wenn Ihr Outlook-Kalender verknüpft ist, werden Ihnen auf der Registerkarte **Scheduler** auch Outlook-Ereignisse angezeigt. Weitere Informationen dazu finden Sie in den Abschnitten '"Eine neue Zeiterfassung hinzufügen" (S. 208)' und '"Ihre Kalender mit Microsoft Outlook synchronisieren" (S. 204)'.

Hinweis
Advanced Automation verfügt über ein integriertes System zur prädiktiven Ticket-Handhabung. Es zeichnet sechs Monate lang die Zeit auf, die für die einzelnen Ticket-Kategorien aufgewendet wurde, wodurch sich eine durchschnittliche Handhabungszeit pro Ticket-Kategorie ergibt. So kann das System beispielsweise nachverfolgen, wie viel Zeit Ihre Techniker für ein Ticket mit der Kategorie *Workstation* und der Unterkategorie *Druckertreiber installieren* aufgewendet haben. Diese Informationen werden auf den aktuellen Tickets angezeigt, um die Zeit zu berechnen, die Ihr Team voraussichtlich für deren Bearbeitung benötigen wird. Dies wird auch für die einzelnen Benutzer durchgeführt, wobei die berechneten Werte ebenfalls auf der Registerkarte **Scheduler** angezeigt werden.

So können Sie ein Ticket auf der Registerkarte 'Scheduler' planen

1. Gehen Sie zu **Task-Verwaltung –> Service Desk** und klicken Sie dann auf die Registerkarte **Scheduler**.
   Auf der angezeigten Registerkarte werden verschiedene Arten von Ereignissen angezeigt:
   - Zeiterfassungen, die aus Tickets erfolgt sind
   - Zeiterfassungen, die auf dieser Registerkarte manuell definiert wurden
   - Geplante Tickets
   - Kalenderereignisse von Drittanbietern
2. Wählen Sie den gewünschten Benutzer aus den Listenfeldern **Support-Gruppe** und **Support-Agent** aus. Beachten Sie, dass diese Listen nur für Gruppenleiter verfügbar sind und die entsprechenden Benutzer mit freigegebenen Kalendern aufgelistet werden.
3. Klicken Sie zuerst auf den gewünschten Tag und dann auf **Ticket planen**. Daraufhin wird der Dialog 'Ticket planen' angezeigt.



4. Wählen Sie den gewünschten Benutzer aus (den Ticket-Besitzer).
5. Wählen das Ticket aus, das Sie planen wollen. Beachten Sie, dass Sie auch ein bereits geplantes Ticket auswählen können, um dieses neu planen zu können.
6. Legen Sie das Datum, die Uhrzeit und die voraussichtliche Dauer für das Ticket fest.
7. Klicken Sie auf **Planung**. Sie können nun das geplante Element sehen, das Sie gerade erstellt haben.

   Beachten Sie, dass Sie nur geplante Tickets und manuelle Zeiterfassungen aktualisieren können.

So können Sie ein Ticket aus dem Ticket heraus planen

1. Gehen Sie zu **Task-Verwaltung –> Service Desk** und erstellen Sie ein neues Ticket (siehe Abschnitt '"Ein neues Ticket erstellen" (S. 197)') oder suchen Sie das entsprechende Ticket auf der Registerkarte **Tickets** heraus.
2. Klicken Sie beim Erstellen eines Tickets auf den Optionsschalter **Ticket planen**, um es zu aktivieren. Legen Sie dann die Startstunde sowie die geschätzte Dauer für das Ticket fest. Klicken Sie dann, nachdem Sie die restlichen erforderlichen Felder im Dialog ausgefüllt haben, auf **Fertig**.

   Oder

   Wenn Sie ein vorhandenes Ticket planen wollen, müssen Sie auf die Registerkarte **Aktivitäten** des betreffenden Tickets klicken und dann das Kontrollkästchen **Ticket planen** aktivieren. Klicken Sie dann auf **Änderungen speichern**.

Ihre Kalender mit Microsoft Outlook synchronisieren

Sie können Tickets in der Registerkarte **Scheduler** mit Microsoft Outlook synchronisieren – und Ihren Kalender mit Kollegen per Freigabe teilen.

So können Sie Tickets mit Microsoft Outlook synchronisieren

1. Gehen Sie zu **Task-Verwaltung –> Service Desk** und klicken Sie dann auf die Registerkarte **Scheduler**.
2. Klicken Sie auf **Kalender synchronisieren**.
3. Melden Sie sich an Ihrem Outlook-Konto an und aktivieren Sie die Option, dass Ihr Kalender mit Advanced Automation synchronisiert wird.
4. Wählen Sie die Option **Inhalte der Kalendersynchronisierung mit allen teilen**, um Ihre Kalender-Inhalte für andere Advanced Automation-Benutzer freizugeben.

Tickets zusammenführen

Wenn Sie ein Ticket aktualisieren, können Sie es auch mit einem anderen bereits vorhandenen Ticket zusammenführen. Dieses kann einen beliebigen Status haben, muss aber mit demselben Kunden und Endbenutzer verknüpft sein.

So können Sie ein Ticket zusammenführen

1. Gehen Sie zu **Task-Verwaltung –> Service Desk**.
2. Wählen Sie auf der angezeigten Registerkarte **Tickets** das gewünschte Ticket aus, das Sie zusammenführen wollen.
3. Aktivieren Sie auf der Registerkarte **Aktivitäten** das Kontrollkästchen **Ticket zusammenführen**.
4. Wählen Sie zuerst das betreffende Ticket aus der Liste der verfügbaren Tickets aus und klicken Sie dann auf **Zusammenführen**.
5. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Zusammenführen**.

> **Hinweis**
> Das ursprüngliche Ticket wird dann nicht mehr verfügbar sein und wird auch nicht mehr in die Suche nach aktiven oder geschlossenen Tickets einbezogen. Jede Aktualisierung oder Zeiterfassung, die im ursprünglichen Ticket enthalten war, wird jedoch dem zusammengeführten Ticket hinzugefügt.

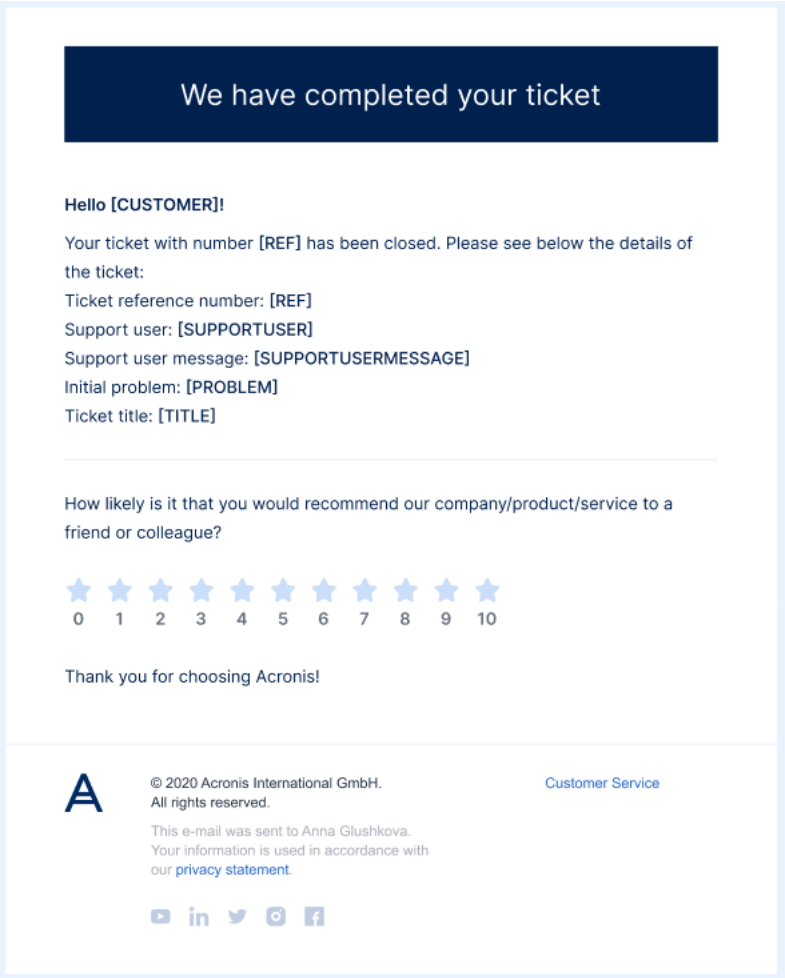
Kunden-Feedback zu Tickets erhalten

Wenn der Status eines Tickets zu **Geschlossen** aktualisiert wird, sendet Advanced Automation automatisch eine E-Mail mit einer Anfrage zur Ticket-Bewertung an den Kunden. Diese E-Mail ist standardmäßig in Advanced Automation enthalten und kann nach Bedarf angepasst werden (siehe Abschnitt '"E-Mail-Vorlagen verwalten" (S. 259)'). Die E-Mail wird nur einmal gesendet.

Wenn der Kunde die E-Mail mit der Anfrage zur Ticket-Bewertung erhält (siehe unten), kann er das Ticket wie gewünscht einstufen, indem er auf die entsprechende Sternebewertung klickt. Wenn diese angeklickt wurden, kann der Kunde auch noch Kommentare hinzufügen. Anschließend wird dem Kunden eine Bestätigungsmeldung angezeigt, in der diesem für seine Bewertung gedankt wird.

Wenn Sie das Kunden-Feedback sehen wollen, gehen Sie zu **Task-Verwaltung –> Service Desk**, suchen Sie das entsprechende Ticket und wählen Sie es aus. Klicken Sie in der angezeigten rechten Seitenleiste auf die Registerkarte **Überblick**, um sich das Feedback anzusehen.

Hinweis
Die Kunden können ihre Ticket-Bewertung unabhängig von ihrem Zugriff auf das Acronis Management-Portal oder das Cyber Protect-Portal abgeben. Sie benötigen auch keinen Zugriff auf den Advanced Automation Service oder eine spezielle Advanced Automation-Rolle.



Zeiteinträge

Das Modul **Zeiteinträge** ermöglicht es Ihnen, die Zeitaufzeichnungen der Benutzer zu verwalten und deren tägliche Aktivitäten nachzuverfolgen.

Wenn Sie auf die Zeiteinträge-Funktionalität zugreifen wollen, gehen Sie im Management-Portal zu **Task-Verwaltung –> Zeiteinträge**. In der angezeigten Registerkarte **Zeiterfassung** können Sie alle aktuellen Zeiteinträge einsehen, die in Advanced Automation registriert sind. Auf dieser Registerkarte und den zusätzlichen Zeiteinträge-Registerkarten können Sie Folgendes tun:

- Neue Zeiterfassungen hinzufügen
- Zeitfassungen einsehen und ändern
- Zeiterfassungen überprüfen und genehmigen

- Freie Tage beantragen
- Krankmeldungen hinzufügen und überprüfen
- Urlaubsanträge überprüfen und genehmigen
- Zeiterfassungsdaten exportieren

Was sind Zeiteinträge/Zeiterfassungen?

Zeit kann in Advanced Automation auf zwei Arten registriert werden:

- **Automatisch**: Automatische Zeiterfassungen werden erstellt, wenn jemand an einem Service Desk-Ticket arbeitet. Die Zeit, die an einem Ticket gearbeitet wurde, wird automatisch von einem eingebauten Ticket-Timer erfasst. Sie kann außerdem von einem Ticket-Techniker angepasst werden.
- **Manuell**: Manuelle Zeiterfassungen werden von den Technikern manuell übermittelt. Weitere Informationen finden Sie im Abschnitt '"Eine neue Zeiterfassung hinzufügen" (S. 208)'.

Durch eine korrekte und regelmäßige Zeiterfassung können Sie Ihre abrechenbare Zeit erhöhen. Sie ermöglicht außerdem in Kombination mit den integrierten Berichten von Advanced Automation einen guten Überblick über Ihre Metriken – einschließlich der für einen spezifischen Kunden aufgewendeten Zeit, der Auslastungsrate Ihrer Techniker und anderer.

Bestehende Zeiterfassungen einsehen

Gehen Sie im Management-Portal zu **Task-Verwaltung –> Zeiteinträge**, wenn Sie die vorhandenen Zeiterfassungen einsehen wollen. In der angezeigten Registerkarte **Zeiterfassung** können Sie alle aktuellen Zeiterfassungen einsehen, die in Advanced Automation registriert sind.

Es werden Informationen zu jedem Eintrag angezeigt. Wie etwa:

- Die registrierten Stunden
- Der spezifische Benutzer, der den Task durchgeführt hat
- Der Aktivitätstyp
- Der Kunde
- Ob die Zeiterfassung abrechenbar ist oder nicht
- Ein Link zum relevanten Ticket (falls vorhanden)

Die Zeiterfassungen werden nach Datum gruppiert. Außerdem wird die Gesamtstundenzahl für jeden Tag angezeigt.

Wenn Sie die Zeiterfassungsdaten exportieren wollen, müssen Sie die relevanten Zeiterfassungen auswählen und dann auf **Als XLS exportieren** klicken. Es wird eine XLS-Datei mit dem Namen **Zeiterfassungen** auf Ihren Workload heruntergeladen.

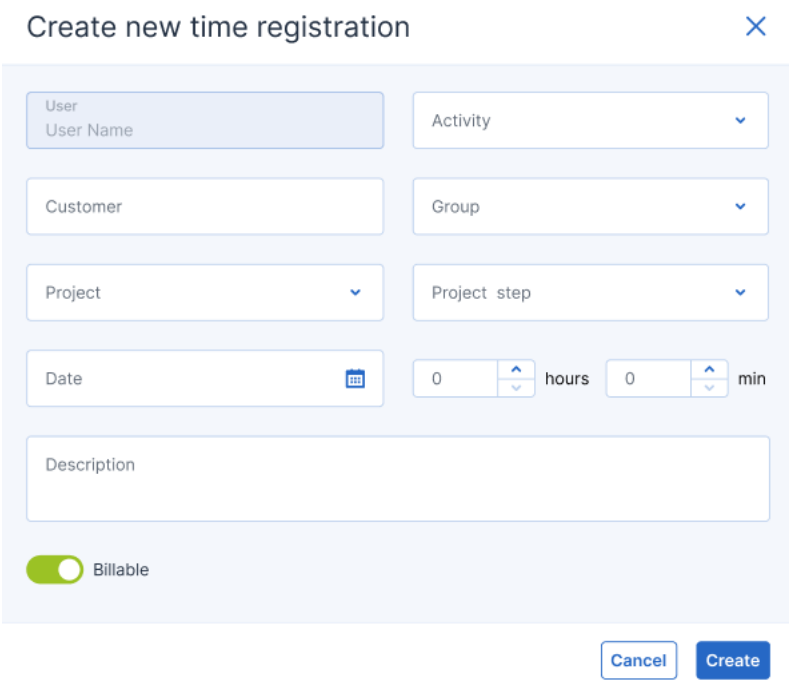
Sie können die angezeigte Liste auch filtern oder sortieren, um einen spezifischen Zeiteintrag zu finden. Wenn Sie eine erweiterte Filterung benötigen, können Sie mit dem Tool **Filter** genauer definieren, welche spezifischen Zeiteinträge angezeigt werden sollen.

Eine neue Zeiterfassung hinzufügen

Durch manuelles Hinzufügen einer neuen Zeiterfassung können Sie die Arbeitszeit protokollieren, die für die Bearbeitung von Tickets aufgewendet wurde. Dadurch können Sie sehen, womit die Techniker ihre Zeit verbringen, und (in Verbindung mit den anderen Metriken und Berichten von Advanced Automation) die entsprechenden Ressourcen ermitteln, die für bestimmte Projekte erforderlich sind.

So können Sie eine neue Zeiterfassung hinzufügen

1. Gehen Sie zu **Task-Verwaltung –> Zeiteinträge**. Als Grundeinstellung wird die Registerkarte **Zeiterfassung** angezeigt.
2. Klicken Sie auf **+ Neu**. Daraufhin wird der nachfolgende Dialog angezeigt.



Hinweis
Wenn Advanced Automation für Ihr Konto aktiviert ist, können Sie auch in der Symbolleiste des Management-Portals am oberen Bildschirmrand auf **Neu –> Zeiterfassung** klicken (selbst wenn Sie sich nicht im Modul 'Zeiteinträge' befinden). Durch diese Option wird automatisch der Dialog 'Neue Zeiterfassung erstellen' geöffnet, über den Sie eine Zeiterfassung erstellen können (wie in den folgenden Schritten beschrieben).

3. Definieren Sie Folgendes:
   - **Aktivität**: Wählen Sie die gewünschte Aktivität aus dem Listenfeld **Aktivität** aus. Weitere Informationen über Aktivitäten finden Sie im Abschnitt '"Aktivitäten für Zeiterfassungen definieren" (S. 277)'.
   - **Kunde**: Wählen Sie den gewünschten Kunden aus dem Listenfeld **Kunde** aus. Sie können Ihre eigene Organisation auswählen, wodurch dieser Eintrag nicht abrechenbar wird. Wenn Sie Arbeit für einen bestimmten Kunden registrieren wollen, geben Sie den Namen des Kunden ein.
   - **Gruppe**: Wählen Sie die gewünschte Gruppe (die Abteilung, für die Sie die Registrierung vornehmen) aus dem Listenfeld **Gruppe** aus. Es werden nur solche Gruppen angezeigt, in denen Sie vertreten sind.
   - **Projekt**: Wählen Sie das gewünschte Projekt aus dem Listenfeld **Projekt** aus. Diese Option ist nur verfügbar, wenn Sie einem Projektteam zugewiesen wurden.
   - **Projektschritt**: Wählen Sie den gewünschte Projektschritt aus dem Listenfeld **Projektschritt** aus. Diese Option ist nur verfügbar, wenn Sie einem Projektteam zugewiesen wurden und die Schritte im Projekt nicht abgeschlossen wurden.
   - **Datum**: Definieren Sie das gewünschte Datum.

- **Zeitraum**: Definieren Sie die Dauer der Zeiterfassung (in Stunden und Minuten).
- **Beschreibung**: Geben Sie eine Beschreibung für die Aktivität ein.
- **Abrechenbar**: Klicken Sie auf den Optionsschalter **Abrechenbar**, wenn diese Aktivität als abrechenbar registriert werden soll. Diese Option ist nur verfügbar, wenn Sie einen Kunden ausgewählt haben.

  Hinweis
  Wenn Sie eine neue Zeiterfassung erstellen, wird das Feld **Benutzer** automatisch mit Ihrem Namen ausgefüllt.

4. Klicken Sie auf **Erstellen**.

Eine Zeiterfassung bearbeiten

Hinweis
Sie können eine Zeiterfassung nur bearbeiten, wenn diese noch nicht verarbeitet wurde. Weitere Informationen über das Verarbeiten von Zeiterfassungen finden Sie im Abschnitt '"Zeiterfassungen zur Abrechnung genehmigen" (S. 211)'.

So können Sie eine Zeiterfassung bearbeiten

1. Gehen Sie zu **Task-Verwaltung –> Zeiteinträge**. Als Grundeinstellung wird die Registerkarte **Zeiterfassung** angezeigt.
2. Klicken Sie auf die Zeiterfassung, die Sie bearbeiten wollen.
3. Klicken Sie in der rechten Seitenleiste auf das Stiftsymbol, wenn Sie die Zeiterfassung bearbeiten wollen. Weitere Informationen über die verfügbaren Felder finden Sie im Abschnitt '"Eine neue Zeiterfassung hinzufügen" (S. 208)'.
4. Klicken Sie, wenn Sie fertig sind, auf ✓.

Abrechenbare Zeiterfassungen

Advanced Automation umfasst zwei wesentliche Szenarien zur Erfassung von abrechenbaren Zeiteinträgen:

- Die automatische Zeiterfassung, die bei der Bearbeitung von generischen Tickets und Alarm-Tickets verwendet wird.
- Manuelle Zeiteinträge.

Hinweis
Unabhängig vom Zeiterfassungsszenario entscheidet letztlich der MSP-Administrator, ob eine Zeit abgerechnet wird oder nicht. Das bedeutet, dass jede Auswahl in den unteren Abschnitten bei Bedarf abgeändert werden kann.

Weitere Informationen über das Arbeiten mit Verkaufsartikeln finden Sie im Abschnitt '"Verkaufsartikel verwalten" (S. 223)'.

Die automatische Zeiterfassung, die bei der Bearbeitung von generischen Tickets und Alarm-Tickets verwendet wird

Beachten Sie Folgendes:

- Diese Zeit kann 'nicht abrechenbar' sein, wenn in der geltenden SLA die Option **Festpreis** aktiviert ist (in einer Komplett-SLA). Diese Zeit kann abrechenbar sein, wenn in der betreffenden SLA die Option **Nachträgliche Berechnung** aktiviert ist.
- Der Abrechnungssatz kann auf verschiedenen Szenarien beruhen:
  - Standard-Abrechnungssatz für Arbeiten während der Bürozeiten.
  - Standard-Abrechnungssatz für Arbeiten außerhalb der üblichen Bürozeiten, wenn der Zeitstempel der Ticket-Aktualisierung außerhalb des SLA-Abdeckungszeitrahmens liegt.
  - Spezifischer Abrechnungssatz für den Kunden (benutzerdefinierte Preisgestaltung).
  - Spezifischer Abrechnungssatz auf Basis der Arbeitsarten im Ticket. Ein Beispiel: Update 1 im Ticket ist für 1 Stunde Standard-Support-Arbeit, während Update 2 im Ticket für 1 Stunde ist und der Aktivitätstyp 'Netzwerktechnik' im Ticket ausgewählt ist. Als Ergebnis werden dem Kunden zwei verschiedene Sätze in Rechnung gestellt. Beachten Sie jedoch, dass die Abrechnungssätze durch benutzerdefinierte Preiseinstellungen überschrieben werden können.

Manuelle Zeiteinträge

Diese Zeit kann als abrechenbare Zeit markiert werden. Für jeden manuellen Zeiterfassungs-Aktivitätstyp kann ein spezifischer Abrechnungssatz konfiguriert werden. Beachten Sie, dass dieser Satz durch benutzerdefinierte Preiseinstellungen überschrieben werden kann (für weitere Informationen siehe den Abschnitt '"Mit benutzerdefinierten Preisen arbeiten" (S. 233)').

Zeiterfassungen zur Abrechnung genehmigen

Sie können folgende Zeiterfassungen genehmigen, die in Advanced Automation erfasst und in der Registerkarte **Zeit genehmigen** aufgeführt sind:

- Noch nicht genehmigte Zeiterfassungen (das sind gemeldete Ticket-Zeiten von Tickets, die nur das Stadium **Geschlossen** haben) oder manuelle Zeiterfassungen.
- Zeiteinträge, die den Grenzwert der für ein Ticket aufgewendeten Mindestzeit erfüllen (der in den Abrechnungseinstellungen festgelegt ist, siehe Abschnitt '"Abrechnungseinstellungen" (S. 280)'). Wenn der Grenzwert beispielsweise auf **5** festgelegt ist, werden Zeiteinträge mit weniger als fünf Minuten nicht aufgeführt.

Hinweis
Zeiterfassungen können nur von Benutzern mit einer der folgenden Rollen genehmigt werden: Administrator, Direktor, Gruppenleiter, Finanzdirektor

Jede aufgeführte Zeiterfassung enthält die vollständigen Details zu jeder Aktivität und ermöglicht es Ihnen außerdem, die Daten der dazugehörigen Kunden zu verarbeiten und abzurechnen. Sie können einzelne oder mehrere Zeiterfassungen als für die Kunden abrechenbar genehmigen – oder als ausstehend oder nicht abrechenbar definieren.

Wichtig
Wenn keine Abrechnungsinformationen für den betreffenden Kunden vorliegen, können Sie die von ihm gemeldete Ticketzeit nicht genehmigen. Wenn Sie versuchen, Ticket-Zeiterfassungen zu genehmigen, werden Sie aufgefordert, Abrechnungsinformationen für die betreffenden Kunden hinzuzufügen. Weitere Informationen finden Sie unter 'Abrechnungsinformationen bereitstellen'.

So können Sie eine Zeiterfassung genehmigen

1. Gehen Sie zu **Task-Verwaltung –> Zeiteinträge**. Klicken Sie dann auf die Registerkarte **Zeit genehmigen**.
   Es wird eine Liste mit Zeiterfassungen angezeigt, die zur Genehmigung anstehen. Zu den angezeigten Informationen gehören der Kunde, das Datum und der Titel der Zeiterfassung sowie deren Dauer.

   Hinweis
   Wenn  neben der Spalte 'Dauer' angezeigt wird, bedeutet dies, dass ein Teil der registrierten Zeit außerhalb des Zeitrahmens der betreffenden SLA aufgezeichnet wurde. Wenn Sie weitere Informationen darüber erhalten wollen, welche Zeit abgerechnet wurde, befolgen Sie die nachstehenden Schritte.

2. (Optional) Wenn Sie die Details zu einer spezifischen Zeiterfassung überprüfen wollen, wählen Sie die entsprechende Zeile aus. Die Details für die ausgewählte Zeiterfassung werden in der rechten Seitenleiste angezeigt:
   - Sie können auf **Verarbeiten** klicken, um einen Verkaufsartikel für diese Zeiterfassung zu erstellen – und auf **Ticket ansehen**, um das aktuelle Ticket einzusehen. In Schritt 4 können Sie nachlesen, wie Advanced Automation die Zeiterfassung behandelt, wenn Sie auf **Verarbeiten** klicken.
   - Im Bereich **Überblick** werden Ihnen allgemeine Informationen zu der jeweiligen Zeiterfassung angezeigt. Sie können diese Informationen auch bearbeiten und den Optionsschalter **Blockstunden** aktivieren (wenn Blockstunden auf der Vertragsebene aktiviert wurden, wie etwa bei einer Vereinbarung über einen Komplett-Support mit monatlich 20 Stunden). Wenn es einen Saldo der Blockstunden gibt (wie etwa ungenutzte Support-Stunden), wird die Zeiterfassung von diesem Saldo abgezogen, ohne einen zusätzlichen Verkaufsartikel zu erstellen. Sie können diese Standardregel aber bei Bedarf auch umdefinieren und die erfasste Zeit bei Bedarf trotzdem abrechnen.
   - Im Bereich **Abrechenbare SLA-Zeit** sehen Sie den tatsächlichen aufgerundeten Zeitwert des Kunden (in Minuten), der zum Aufrunden der gesamten abrechenbaren Zeit verwendet wird. Sie können die gerundete Gesamtzeit pro Abrechnungssatz einsehen und bearbeiten. So

können Sie beispielsweise den entsprechenden Abrechnungssatz auswählen und die endgültige abrechenbare Zeit manuell anpassen.

- Im unteren Bereich der Seitenleiste können Sie bei Bedarf die Details zu den Zeiterfassungen des Tickets überprüfen. Für jede Zeiterfassung sind folgende Details verfügbar:
  - Der Benutzer, der die Zeiterfassung vorgenommen hat.
  - Der Support-Gruppen-Name des Benutzers.
  - Das Datum und die Uhrzeit der Zeiterfassung.
  - Der Stundensatz des Benutzers.
  - Eine Beschreibung der Zeiterfassung.

3. Klicken Sie, nachdem Sie die Zeiterfassung überprüft oder bearbeitet haben, in die entsprechende Zeile und wählen Sie auf der Registerkarte **Zeit genehmigen** eine der folgenden Optionen aus:
   - **Abrechenbar**: Wählen Sie diese Option, um den betreffenden Kunden zu fakturieren und eine Rechnung zu generieren.

     Hinweis
     Advanced Automation trifft automatisch eine Vorauswahl, ob ein Ticket auf Basis des SLA abgerechnet werden soll (Sie können dies aufheben, indem Sie die entsprechende Option aktivieren). Wenn ein manueller Zeiteintrag während seiner Erstellung als **Abrechenbar** markiert wird (siehe Abschnitt '"Ein neues Ticket erstellen" (S. 197)'), wird er von Advanced Automation auch auf der Registerkarte **Zeit genehmigen** als **Abrechenbar** markiert. Bei Bedarf können Sie die Abrechnungsoption auf **Ausstehend** ändern.

   - **Nicht abrechenbar**: Wählen Sie diese Option, wenn Sie die ausgewählte Zeiterfassung nicht abrechnen wollen.
   - **Ausstehend**: Wählen Sie diese Option, wenn Sie die Zeiterfassung nach dem Verarbeiten von abrechenbaren Elementen in der Liste behalten wollen.

   Sie können bei Bedarf auch mehrere Zeiterfassungen auswählen. Wenn ausgewählt, werden die entsprechenden Aktionsschaltflächen oberhalb der Liste der Zeiterfassungen aktiviert. Sie können zwischen folgenden Befehlen wählen: **Als abrechenbar markieren**, **Als nicht abrechenbar markieren**, **Als ausstehend markieren** oder **Verarbeiten** (siehe den nachfolgenden Schritt).
4. Klicken Sie auf die Aktionsschaltfläche **Verarbeiten**, um die ausgewählten Zeiterfassungen zu verarbeiten.

   Wenn eine Zeiterfassung als **Abrechenbar** festgelegt wurde, wird für den Kunden ein Verkaufsartikel mit den relevanten Firmendetails erstellt. Wenn mehrere Zeiterfassungen ausgewählt wurden, werden dem Verkaufsartikel auch mehrere Zeilen hinzugefügt. Die generierte Rechnung enthält den Ticket-Titel, die Ticket-Nummer sowie die abrechenbare Zeit auf Basis des geltenden Satzes.

   Wenn eine Zeiterfassung als **Nicht abrechenbar** festgelegt wurde, wird sie aus der Registerkarte **Zeit genehmigen** entfernt.

Wenn eine Zeiterfassung als **Ausstehend** festgelegt wurde, verbleibt Sie auf der Registerkarte **Zeit genehmigen**.

Freie Tage beantragen

Sie können Ihre Anträge auf freie Tage auf der Registerkarte **Freien Tag beantragen** einsehen und aktualisieren. Auf dieser Registerkarte werden alle Anträge auf freie Tage angezeigt, die Sie erstellt haben, sowie deren Details (wie etwa, ob sie genehmigt wurden oder nicht). Sie können bei Bedarf auch weitere freie Tage beantragen.

Hinweis
Anträge auf freie Tage können nur gestellt werden, wenn für den betreffenden Kunden im Feld **Freie Tage pro Jahr** eine gewisse Anzahl von Tagen definiert wurde. Weitere Informationen finden Sie im Abschnitt '"Standardwerte festlegen" (S. 256)'.

So können Sie freie Tage beantragen

1. Gehen Sie zu **Task-Verwaltung –> Zeiteinträge** und klicken Sie anschließend auf die Registerkarte **Freien Tag beantragen**.
2. Klicken Sie auf **+ Neu**.
3. Wählen Sie im angezeigten Dialog eine der folgenden Optionen aus:
   - **Einen freien Tag beantragen**: Bestimmen Sie den relevanten Tag und die Zeit (standardmäßig sind acht Stunden eingestellt).
   - **Mehrere freie Tage beantragen**: Bestimmen Sie das relevante Anfangs- und Enddatum.
4. Geben Sie eine Beschreibung für den Antrag ein und klicken Sie auf **Erstellen**.
   Wenn Sie mehrere freie Tage beantragt haben, wird für jeden Tag ein Antrag registriert.

   Hinweis
   Sie können auch Anträge auf freie Tage bearbeiten, die zur Genehmigung anstehen (klicken Sie dazu auf die entsprechende Zeile in der Liste der Anträge und bearbeiten Sie diese nach Bedarf). Wenn der Antrag genehmigt oder abgelehnt wurde, kann er nicht mehr bearbeitet werden.

Eine Krankmeldung erstellen

Sie können alle zu genehmigenden Krankmeldungen auf der Registerkarte **Krankmeldung** einsehen und aktualisieren. Darüber hinaus können Sie für jeden Benutzer in Ihrem Konto eine neue Krankmeldung erstellen.

Hinweis
Krankmeldungen können nur von Benutzern mit einer der folgenden Rollen erstellt werden: Administrator, Direktor, Gruppenleiter, Finanzdirektor, Personalabteilung

So können Sie eine neue Krankmeldung erstellen

1. Gehen Sie zu **Task-Verwaltung –> Zeiteinträge** und klicken Sie anschließend auf die Registerkarte **Krankmeldung**.
2. Klicken Sie auf **+ Neu**.
3. Definieren Sie in dem angezeigten Dialogfenster folgende Elemente:
   - **Benutzer**: Wählen Sie den Benutzer aus, für den Sie die Krankmeldung erstellen wollen.
   - **Einen Tag beantragen**: Bestimmen Sie den relevanten Tag und die Zeit (standardmäßig sind acht Stunden eingestellt).

     Oder

     Mehrere Tage beantragen: Bestimmen Sie das relevante Anfangs- und Enddatum.
4. Geben Sie eine Beschreibung für die Krankmeldung ein und klicken Sie auf **Erstellen**.

   Wenn Sie mehrere Krankheitstage beantragt haben, wird für jeden Tag ein Antrag registriert.

Hinweis
Sie können auch Anträge auf Krankmeldungen bearbeiten, die zur Genehmigung anstehen (klicken Sie dazu auf die entsprechende Zeile in der Liste der Krankmeldungen und bearbeiten Sie diese nach Bedarf). Wenn eine Krankmeldung genehmigt oder abgelehnt wurde, kann sie nicht mehr bearbeitet werden.

Anträge auf Urlaubs- und Krankheitstage genehmigen

Auf der Registerkarte **Anträge auf bezahlten Urlaub genehmigen** können Sie die Urlaubs- und Krankmeldungsanträge von allen Benutzern einsehen und aktualisieren. Sie können die Urlaubs- und Krankmeldungsanträge je nach Bedarf genehmigen oder ablehnen.

Hinweis
Urlaubsanträge können nur von Benutzern mit einer der folgenden Rollen genehmigt werden: Administrator, Direktor, Gruppenleiter, Finanzdirektor

So können Sie Urlaubsanträge genehmigen

1. Gehen Sie zu **Task-Verwaltung –> Zeiteinträge** und klicken Sie anschließend auf die Registerkarte **Anträge auf bezahlten Urlaub genehmigen**.
2. Wählen Sie in der Liste der angezeigten Anträge den Genehmigungsstatus – und zwar für jeden Antrag in der Spalte **Genehmigung**. Sie können eine der folgenden Optionen wählen:
   - **Genehmigen**
   - **Ablehnen**
   - **Ausstehend**

   Sie können bei Bedarf auch mehrere Anträge auswählen. Wenn ausgewählt, werden die entsprechenden Aktionsschaltflächen oberhalb der Antragsliste aktiviert. Wählen Sie eine dieser Elemente: **Als genehmigt markieren**, **Als abgelehnt markieren**, **Als ausstehend markieren** oder **Verarbeiten**.

Beachten Sie, dass in der Spalte **Verbleibende freie Tage** der verbleibende Wert in Tagen, Stunden und Minuten angezeigt wird. Dieser Wert wird als Differenz zwischen der erlaubten Anzahl von freien Tagen pro Jahr (die als Teil der Standardwerte für Ihren Service Desk festgelegt ist; siehe Abschnitt '"Standardwerte festlegen" (S. 256)') und der Gesamtzahl aller in diesem Jahr bereits genehmigten Urlaubsanträge berechnet.

Außerdem wird in der Spalte **Typ** die Antragsart angegeben, also **Bezahlter Urlaub** oder **Krankheitstage**. Wenn ein Antrag vom Typ **Bezahlter Urlaub** ist, wird in der Spalte **Verbleibende freie Tage** kein Zahlenwert angezeigt.

3. (Optional) Klicken Sie auf eine Antragszeile, um sich die Details des Antrags anzeigen zu lassen. Bei Bedarf können Sie auch einen Kommentar hinzufügen.
4. Klicken Sie auf die Aktionsschaltfläche **Verarbeiten**, um die ausgewählten Anträge zu verarbeiten.

   Wenn ein Antrag genehmigt wurde, wird er aus der angezeigten Liste auf der Registerkarte **Anträge auf bezahlten Urlaub genehmigen** entfernt – und der Wert der verbleibenden freien Tage für den Benutzer wird aktualisiert.

   Wenn ein Antrag abgelehnt wurde, wird er auch aus der Registerkarte **Anträge auf bezahlten Urlaub genehmigen** entfernt.

   Wenn ein Antrag als ausstehend markiert wurde, verbleibt er auf der Registerkarte **Anträge auf bezahlten Urlaub genehmigen**.

Die Verkaufs- und Abrechnungsfunktionalität verwalten

Im Modul 'Verkauf und Abrechnung' (im Management-Portal unter **Verkauf und Abrechnung** zu finden) können Sie folgende Funktionen verwalten:

- Angebote
- Verkaufsartikel
- Verträge
- Rechnungen
- Hauptbücher
- Produkte
- Benutzerdefinierte Preise

Hinweis
Vergewissern Sie sich, bevor Sie mit diesem Bereich fortfahren, dass Sie Ihr Konto im Bereich **Einstellungen** vollständig eingerichtet haben (einschließlich dem Erstellen von Produkten).

Verkauf

Mit dem Modul **Verkauf** können Sie folgende Funktionen verwalten:

- Angebotserstellung
- Verkaufsartikel
- Verträge
- Benutzerdefinierte Preise

Wenn Sie auf das Modul **Verkauf** zugreifen wollen, gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.

Angebote verwalten

Verwenden Sie die Angebotsfunktionalität von Advanced Automation, um Ihren Kunden Angebote für Ihre Produkte und Services bereitzustellen. Wenn ein Angebot genehmigt wird, wird es automatisch in eine Reihe von Tasks konvertiert, die Ihnen helfen sollen, den Lieferstatus für das Angebot nachzuverfolgen:

- Es wird ein allgemeines Angebotsticket für das genehmigte Angebot als Task erstellt, um dessen Fortschritt zu verfolgen, Notizen zu erstellen und den Zeitaufwand für den Task zu erfassen.
- Es wird ein Bestell-Ticket für die Angebotselemente erstellt, die gekauft werden müssen, um das Angebot zu erfüllen. Das Ticket kann auch von Ihren Teammitgliedern verwendet werden, um dessen Fortschritt zu verfolgen, wichtige Notizen (wie etwa Kaufdetails) zu speichern und die für den Task aufgewendete Zeit zu erfassen.
- Angebotselemente für Vertragsprodukte werden automatisch in neue Verträge und Vertragsteile konvertiert oder zu bestehenden Kundenverträgen hinzugefügt (abhängig von der ursprünglichen Konfiguration des Angebots für solche Angebotselemente).

Wenn Sie auf die Angebotsfunktionalität zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Angebote**. Auf der Registerkarte **Angebote** werden alle Angebote angezeigt, die Sie für Kunden erstellt haben.

Hinweis
Diese Funktion ist nur für Benutzer verfügbar, denen folgende Rollen zugewiesen wurden: Administrator, Direktor, Techniker, Gruppenleiter, Finanzdirektor, Finanzen, Verkauf

Ein Angebot erstellen

Wenn Sie ein neues Angebot erstellen, führt Sie ein Bildschirm-Assistent durch die Hauptschritte. In diesen Schritten werden Sie Folgendes tun:

- Grundlegende Angebotsinformationen hinzufügen.
- Dem Angebot Produkte und/oder Angebotsvorlagen hinzufügen.
- Das Angebot überprüfen und versenden (oder speichern, um es weiter bearbeiten und dann zu einem späteren Zeitpunkt versenden zu können).

So können Sie ein Angebot erstellen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Klicken Sie zuerst auf die Registerkarte **Angebote** und anschließend auf den Befehl **+ Neu**. Beachten Sie: Wenn Sie noch kein Angebot erstellt haben, werden Sie aufgefordert, auf **Neu erstellen** zu klicken.

   Hinweis
   Wenn Advanced Automation für Ihr Konto aktiviert ist, können Sie auch in der Symbolleiste des Management-Portals am oberen Bildschirmrand auf **Neu –> Angebot** klicken (selbst wenn Sie sich nicht im Verkaufsmodul befinden). Durch diese Option wird automatisch der Assistent 'Neues Angebot' geöffnet, mit dem Sie ein Angebot erstellen können (wie in den nachfolgenden Schritten beschrieben).

3. Definieren Sie in Schritt 1 des angezeigten Assistenten 'Neues Angebot' folgende Elemente:
   - **Beschreibung**: Geben Sie eine Beschreibung für das Angebot ein.
   - **Endbenutzer**: Wählen Sie den gewünschten Endbenutzer aus. Der ausgewählte Benutzer wird das Angebot erhalten, wenn es zur Genehmigung abgesendet wird.

     Hinweis
     Wenn für den ausgewählten Endbenutzer keine Abrechnungsinformationen definiert wurden, wird dem Abrechnungsassistenten ein zusätzlicher Schritt **Abrechnungsinformationen** hinzugefügt. Wenn Sie auf **Weiter** klicken, müssene Sie die relevanten Felder für die Abrechnungsinformationen ausfüllen (einschließlich Zahlungsbedingungen und Adresse). Diese Informationen werden dann gespeichert und verwendet, wenn der Endbenutzer in anderen Advanced Automation-Modulen ausgewählt wird. Weitere Informationen über die Felder für Abrechnungsinformationen finden Sie unter "Abrechnungsinformationen für einen Mandanten definieren" (S. 42).

   - **Firmenname**: Dieses Feld wird automatisch mit der betreffenden Firma ausgefüllt, sofern das Feld **Endbenutzer** definiert wurde.
   - (Optional) Definieren Sie im Text-Eingabefeld eine Angebotseinleitung. Dieser Text kann eine kurze Einleitung bzw. eine Beschreibung des Angebots enthalten. Beispiel: *Vielen Dank, dass Sie ein Angebot für neue Laptops angefordert haben. Wir haben eine Liste unserer neuesten Modelle beigefügt.* Sie können dem Text bei Bedarf auch formatieren und Bilder hinzufügen.
4. Klicken Sie auf **Weiter**. Der nächste Schritt des neuen Angebotsassistenten wird angezeigt.
5. Klicken Sie auf **Vorlage hinzufügen** oder **Produkt hinzufügen**, um die gewünschte Vorlage bzw. das gewünschte Produkt auszuwählen.
   - Wenn Sie auf **Vorlage hinzufügen** klicken: Werden Sie aufgefordert, eine Angebotsvorlage auszuwählen. Klicken Sie dann auf **Hinzufügen**, um dem Angebot die gewünschte Vorlage hinzuzufügen. Sie können bei Bedarf weitere Angebotsvorlagen und/oder Produkte auswählen.
   - Wenn Sie auf **Produkt hinzufügen** klicken: Wählen Sie im Feld **Produktkategorie** die gewünschte Kategorie aus. Wählen Sie dann im Feld **Produkte** ein Produkt aus der

verfügbaren Liste aus.

Wenn das von Ihnen ausgewählte Produkt kein Vertragsprodukt ist (beispielsweise ein Standard-Verkaufsartikel wie ein Hardware-Teil), definieren Sie die Felder **Bestandsartikel**, **Anzahl** und **Rabatt** (sofern zutreffend). Beachten Sie, dass die Felder **Preis**, **Lieferant** und **Beschreibung** automatisch mit den Details des ausgewählten Bestandsartikels ausgefüllt werden.

Wenn es sich bei dem von Ihnen ausgewählten Produkt um ein Vertragsprodukt handelt (wie etwa wiederholte Abrechnungen für verwaltete Services), werden folgende zusätzliche Felder angezeigt:

- **Rechnungsintervall**: Wählen Sie eine der folgenden Optionen: **Jeden Monat**, **Vierteljährlich**, **Halbjährlich** oder **Jedes Jahr**.
- **Wann die Abrechnung ansteht**: Wählen Sie entweder **Im Voraus** oder **Nachträglich**.
- **Zahlungsmethode**: Wählen Sie entweder die Option **Vorautorisierte Abbuchung** oder **Manuell bezahlen** aus. Mit der Option 'Vorautorisierte Abbuchung' können Kunden Rechnungen per Überweisung oder mithilfe einer der Zahlungsintegrationen (PayPal, Stripe) bezahlen. Die Kunden können die Rechnung auch zwecks Lastschrifteinzug an ihre Hausbank senden.
- **Vertragszeitraum (Monate)**: Wählen Sie die entsprechende Anzahl von Monaten (unabhängig davon, welche Option Sie im Feld **Rechnungsintervall** ausgewählt haben).

6. Klicken Sie auf **Hinzufügen**, um das Produkt dem Angebot hinzuzufügen.

   Wenn Sie weitere Produkte hinzufügen wollen, klicken Sie im angezeigten Fenster 'Übersicht' auf **Vorlage hinzufügen** oder **Produkt hinzufügen**.

   Hinweis
   Wenn eines der von Ihnen ausgewählten Produkte zwingend erforderliche Felder enthält, die nicht ausgefüllt wurden, werden Sie aufgefordert, diese Felder für die betreffenden Produkte auszufüllen, bevor Sie fortfahren können.

7. Klicken Sie auf **Weiter**. Der letzte Schritt des neuen Angebotsassistenten wird angezeigt.
8. Überprüfen Sie das Angebot und wählen Sie dann eine der folgenden Optionen:
   - Klicken Sie auf **Speichern**, wenn Sie das Angebot sichern wollen. Er wird nicht an die Kunden gesendet, kann aber bei Bedarf bearbeitet und zu einem späteren Zeitpunkt versendet werden.
   - Klicken Sie auf **Speichern und senden**, wenn Sie das Angebot sichern und an den ausgewählten Benutzer verschicken wollen.

Sobald der Kunde das Angebot per E-Mail oder Telefon angenommen oder abgelehnt hat, können Sie das Angebot auf der Registerkarte **Angebote** entsprechend kennzeichnen. Sollte das Angebot jedoch im Angebotsportal angenommen oder abgelehnt werden, so spiegelt sich dies automatisch auf der Registerkarte **Angebote** wider. Weitere Informationen finden Sie im Abschnitt '"Ein Angebot als angenommen oder abgelehnt markieren" (S. 221)'.

Weitere Informationen darüber, wie Advanced Automation die Ablehnung oder Annahme von Angeboten handhabt, finden Sie im Abschnitt '"Wie Advanced Automation angenommene oder abgelehnte Angebote verarbeitet" (S. 220)'.

Wie Advanced Automation angenommene oder abgelehnte Angebote verarbeitet

Wenn ein Kunde ein Angebot annimmt oder ablehnt, können Sie das entsprechende Angebot auf der Registerkarte **Angebote** suchen und es dort als angenommen oder abgelehnt markieren (weitere Informationen finden Sie im Abschnitt '"Ein Angebot als angenommen oder abgelehnt markieren" (S. 221)'). Abhängig von der gewählten Option wird dadurch dann eine Reihe von Ereignissen in Advanced Automation ausgelöst.

Wenn ein Angebot als angenommen markiert wird

Wenn Sie das Angebot als vom Kunden angenommen markieren oder der Kunde das Angebot selbst akzeptiert, finden folgende Ereignisse statt:

- Dem Kunden wird eine Dankesnachricht angezeigt.
- Der Status des Angebots auf der Registerkarte **Angebote** wird zu **Angenommen** aktualisiert. Als Folge davon kann das Angebot nicht mehr bearbeitet werden. Es kann jedoch noch kopiert werden.
- Der betreffende MSP-Benutzer (der Benutzer, der das Angebot erstellt hat) erhält eine Benachrichtigung, dass das Angebot angenommen wurde.
- Es wird ein allgemeines Angebotsticket erstellt, das alle Details zum Angebot enthält. Das Ticket wird demselben Benutzer zugewiesen, der im Angebot ausgewählt wurde, und ist über das Modul **Service Desk** zugänglich.
- Es wird ein Bestell-Ticket erstellt und dem Manager der Support-Gruppe zugewiesen, die in den Angebotseinstellungen für Bestell-Tickets festgelegt wurde. Dieses Ticket enthält nur die Details zu den Produkten, die keine Vertragsprodukte sind und die nicht auf Lager sind.
- Für Produkte, die keine Vertragsprodukte sind, werden Verkaufsartikel erstellt, die auf der Registerkarte **Verkaufsartikel** eingesehen werden können.
- Für Vertragsprodukte, die ausgewählt wurden::
  - Es wird ein neuer Vertrag für den Kunden erstellt und es werden Einzelposten für alle Vertragsprodukte in einem Angebot hinzugefügt. Beachten Sie: Wenn bei der Definition eines Angebotsprodukts kein bestimmter Vertrag ausgewählt wurde, wird ein neuer Vertrag mit diesem Vertragsteil erstellt. Wenn ein bestimmter Vertrag ausgewählt wurde, wird er um diesen Vertragsteil ergänzt.
  - Das Datum des Vertragsbeginns wird entsprechend dem Datum der Angebotsannahme festgelegt. Das Vertragsende richtet sich nach dem Datum der Angebotsannahme und der Dauer des Angebots, die im Feld **Vertragszeitraum (Monate)** des Angebots definiert ist.

Wenn ein Angebot als abgelehnt markiert wird

Wenn Sie das Angebot als vom Kunden abgelehnt markieren, finden folgende Ereignisse statt:

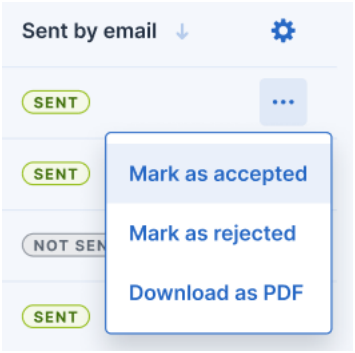
- Dem Kunden wird eine Dankesnachricht angezeigt, die ihn darüber informiert, dass das Angebot als abgelehnt gekennzeichnet wurde.
- Der Status des Angebots auf der Registerkarte **Angebote** wird zu **Abgelehnt** aktualisiert. Als Folge davon kann das Angebot nicht mehr bearbeitet werden. Es kann jedoch noch kopiert werden.
- Der betreffende MSP-Benutzer (der Benutzer, der das Angebot erstellt hat) erhält eine Benachrichtigung, dass das Angebot abgelehnt wurde.
- Bestandsartikel werden zu 'auf Lager' aktualisiert und sind für andere Angebote oder Verkaufsartikel verfügbar.

Ein Angebot als angenommen oder abgelehnt markieren

Wenn ein Kunde ein Angebot annimmt oder ablehnt, kann es auf der Registerkarte **Angebote** entsprechend gekennzeichnet werden. Dadurch werden wiederum eine Reihe von Ereignissen in Advanced Automation ausgelöst. Weitere Informationen dazu finden Sie im Abschnitt '"Wie Advanced Automation angenommene oder abgelehnte Angebote verarbeitet" (S. 220)'.

So können Sie ein Angebot als angenommen oder abgelehnt markieren

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Suchen Sie auf der Registerkarte **Angebote** das betreffende Angebot.
3. Klicken Sie in der äußeren rechten Spalte auf das Drei-Punkte-Symbol und wählen Sie eine der folgenden Optionen aus:
   - **Als 'Angenommen' markieren**
   - **Als 'Abgelehnt' markieren**

   Der Status des Angebots wird automatisch aktualisiert.

Ein Angebot aktualisieren

Sie können Angebote nach Bedarf ändern. Sie können ein Angebot jedoch nicht löschen.

Hinweis
Sie können ein Angebot nur dann ändern, wenn es den Status **Ausstehend** hat. Wenn das Angebot angenommen oder abgelehnt wurde, kann es nicht mehr aktualisiert werden (es kann jedoch kopiert werden; siehe Abschnitt '"Ein Angebot kopieren" (S. 222)').

So können Sie ein Angebot aktualisieren

1. Gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie auf die Registerkarte **Angebote**.
2. Klicken Sie auf das Angebot, das Sie aktualisieren wollen. In der rechten Seitenleiste werden die Details zum Angebot angezeigt.
3. Aktualisieren Sie die relevanten Abschnitte nach Bedarf:
   - Wählen Sie oben in der Symbolleiste in der Seitenleiste eine der folgenden Aktionen aus:
     - **Als 'Abgelehnt' markieren**: Kennzeichnet das Angebot auf der Registerkarte **Angebote** als abgelehnt. Weitere Informationen darüber, was mit einem abgelehnten Angebot geschieht, finden Sie im Abschnitt '"Wie Advanced Automation angenommene oder abgelehnte Angebote verarbeitet" (S. 220)'.
     - **PDF herunterladen**: Lädt eine Kopie des Angebots als PDF-Datei herunter.
     - **Zum Angebotsportal gehen**: Zeigt eine Online-Version des Angebots an.
     - **E-Mail erneut senden**: Sendet die E-Mail mit dem Angebot erneut an den ausgewählten Benutzer.
   - Klicken Sie im Bereich **Angebotsinformationen** auf das Stiftsymbol und aktualisieren Sie die relevanten Felder. Klicken Sie, wenn Sie fertig sind, auf ✓.
   - Klicken Sie im Bereich **Produkte** auf das Pluszeichen (+), wenn Sie ein neues Produkt hinzufügen oder ein bestehendes aktualisieren wollen, das mit dem Angebot assoziiert ist. Klicken Sie, wenn Sie fertig sind, auf ✓.
4. Schließen Sie die rechte Seitenleiste, wenn Sie die Aktualisierung des Angebots abgeschlossen haben.

Ein Angebot kopieren

Sie können ein Angebot kopieren, egal in welchem Status es sich befindet.

So können Sie ein Angebot kopieren

1. Gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie auf die Registerkarte **Angebote**.
2. Klicken Sie in der Zeile des Angebots, das Sie kopieren wollen, auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Kopieren** aus.
3. Aktualisieren Sie das Angebot nach Bedarf. Weitere Informationen finden Sie im Abschnitt '"Ein Angebot erstellen" (S. 217)'.

Angebotsvorlagen verwalten

Angebotsvorlagen ermöglichen es Ihnen, Standardangebote zu registrieren und in Angeboten für Kunden zu verwenden. Wenn Sie ein neues Angebot erstellen, müssen Sie diese also nicht mehr manuell hinzufügen und einzeln konfigurieren. Sie können beispielsweise eine Angebotsvorlage namens 'Verwaltete Services' erstellen, die eine Produktpalette mit Lösungen für Backup und Wiederherstellung, Sicherheit, verwaltete Services, Support und Monitoring enthält.

Advanced Automation ermöglicht Ihnen, Angebotsvorlagen hinzuzufügen und bei Bedarf zu ändern oder zu löschen (siehe Abschnitt '"Eine Angebotsvorlage aktualisieren oder löschen" (S. 223)').

Eine neue Angebotsvorlage hinzufügen

1. Gehen Sie zu **Verkauf und Abrechnung –> Verkauf**.
2. Klicken Sie in der erscheinenden Anzeige auf die Registerkarte **Angebotsvorlagen**.
3. Wenn es noch keine Vorlagen gibt, klicken Sie auf **Neue Vorlage hinzufügen**. Klicken Sie ansonsten auf **+ Neu**.
4. Geben Sie im Feld **Vorlagenname** die Bezeichnung für die Vorlage ein.
5. Klicken Sie in das Feld **Produkte auswählen**, um das relevante Produkt auszuwählen. Klicken Sie anschließend auf **Hinzufügen**.
6. Wenn Sie der Vorlage weitere Produkte hinzufügen wollen, müssen Sie auf **Produkt hinzufügen** klicken und dann das relevante Produkt auswählen. Wiederholen Sie dies nach Bedarf.
7. Klicken Sie auf **Fertig**. Die neue Vorlage wird auf der Registerkarte **Angebotsvorlagen** angezeigt und ist standardmäßig als **Aktiv** festgelegt.

Eine Angebotsvorlage aktualisieren oder löschen

1. Gehen Sie zu **Verkauf und Abrechnung –> Angebotsvorlagen**. Auf der angezeigten Registerkarte werden die vorhandenen Angebotsvorlagen aufgelistet.
2. Wenn Sie eine Vorlage aktualisieren wollen, klicken Sie zuerst auf die entsprechende Vorlage und dann im rechten Fensterbereich auf das Stiftsymbol. Aktualisieren Sie dann die Vorlage nach Bedarf. Klicken Sie, wenn Sie fertig sind, auf ✓.
3. Wenn Sie eine Vorlage löschen wollen, müssen Sie zuerst auf das Drei-Punkte-Symbol für die entsprechende Vorlage und dann auf den Befehl **Löschen** klicken.

Verkaufsartikel verwalten

Verkaufsartikel sind Services oder Waren, die einem Kunden zur Verfügung gestellt werden und die fakturiert werden müssen.

Hinweis
Diese Funktion ist nur für Benutzer verfügbar, denen folgende Rollen zugewiesen wurden: Administrator, Direktor, Gruppenleiter, Finanzdirektor, Finanzen, Verkauf

Verkaufsartikel werden auf der Registerkarte **Verkaufsartikel** verwaltet (gehen Sie zu **Verkauf und Abrechnung –> Verkauf**), wo Sie all Ihre aktuellen Verkaufsartikel einsehen können. Außerdem sind Informationen zu jedem Verkaufsartikel verfügbar, einschließlich zum Kunden, zum Gesamtbetrag des Verkaufsartikels (ohne Rabatte), zum Rechnungsdatum und dazu, ob der Verkaufsartikel bereits in Rechnung gestellt wurde oder nicht. Sie können die angezeigte Liste auch filtern oder sortieren, um einen einzelnen oder mehrere Verkaufsartikel zu finden. Wenn Sie eine erweiterte Filterung benötigen, können Sie mit dem Tool **Filter** genauer definieren, welche Verkaufsartikel angezeigt werden sollen.

Sie können mit dem Advanced Automation Service Verkaufsartikel verwalten, die:

- Automatisch auf Basis von Vertragsteilen registriert wurden.
- Automatisch als Ergebnis von Ticket-basierten Aktivitäten registriert wurden.
- Manuell registriert wurden.

Einen neuen Verkaufsartikel erstellen

Auf Registerkarte **Verkaufsartikel** werden alle Verkaufsartikel angezeigt, die erstellt und abgerechnet wurden. Sie können auch neue Verkaufsartikel hinzufügen.

So können Sie einen Verkaufsartikel erstellen

1. Gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie auf die Registerkarte **Verkaufsartikel**.

   Hinweis
   Wenn Advanced Automation für Ihr Konto aktiviert ist, können Sie auch in der Symbolleiste des Management-Portals am oberen Bildschirmrand auf **Neu –> Verkaufsartikel** klicken (selbst wenn Sie sich nicht im Verkaufsmodul befinden). Durch diese Option wird automatisch der Dialog 'Neuen Verkaufsartikel erstellen' geöffnet, über den Sie einen Verkaufsartikel erstellen können (wie in den folgenden Schritten beschrieben).

2. Gehen Sie im Bereich **Kundeninformationen** folgendermaßen vor:
   - Wählen Sie den gewünschten Kunden aus. Nach erfolgter Auswahl werden einige der folgenden Felder automatisch mit den entsprechenden Kundeninformationen ausgefüllt:
     - **Rechnungssteller** (wählen Sie die entsprechende Entität bzw. juristische Person manuell aus; diese wird dann auf der Rechnung aufgeführt)
     - **Zahlungsmethode** (**Vorautorisierte Abbuchung** oder **Manuell bezahlen**. Mit der Option 'Vorautorisierte Abbuchung' können Kunden Rechnungen per Überweisung oder mithilfe einer der Zahlungsintegrationen (PayPal, Stripe) bezahlen. Die Kunden können die Rechnung auch zwecks Lastschrifteinzug an ihre Hausbank senden.
     - **Rechnung versenden per** (**Rechnung per Post senden** oder **Rechnung per E-Mail senden**)
     - **E-Mail-Adresse der Kontaktperson**
   - Definieren Sie das Rechnungsdatum.
3. Im Bereich **Kundenadresse** werden die relevanten Details zum ausgewählten Kunden angezeigt. Sie können die Adresse für diesen speziellen Verkaufsartikel bei Bedarf manuell aktualisieren.
4. Klicken Sie auf **Weiter**. Auf der angezeigten Registerkarte **Produkte** können Sie dem Verkaufsartikel jetzt beliebige Produkte hinzufügen.

Hinweis
Produkte können ein Service oder Element/Artikel sein, der/das Sie an Ihre Kunden verkaufen. Zum Beispiel Antivirus-Abonnements oder Ad-hoc-Support.

5. Klicken Sie auf **Produkt hinzufügen**, um die gewünschten vordefinierten Produkte (einschließlich Acronis Produkte) in Advanced Automation auszuwählen.

Hinweis
Stellen Sie sicher, dass Sie ein oder mehrere Produkte erstellt haben, bei denen die Option **In Verträgen verwenden** deaktiviert ist. Dadurch wird gewährleistet, dass beim Erstellen eines Verkaufsartikels die relevanten Produktarten verfügbar sind. Wenn ein Produkt als **In Verträgen verwenden** festgelegt ist, kann es nur in Verträgen verwendet werden.

6. Wählen Sie im Feld **Produkt** das gewünschte Produkt aus.
7. Geben Sie in den betreffenden Feldern die **Anzahl** und den **Preis** ein.
8. (Optional) Aktivieren Sie das Kontrollkästchen **Rabatt anwenden** (wenn es aktiviert ist, können Sie einen Rabattbetrag anwenden und einen Grund für diesen angeben) und eine **Beschreibung** für das Produkt.
9. Klicken Sie auf **Hinzufügen**, um das Produkt Ihrem Verkaufsartikel hinzuzufügen. Wenn Sie weitere Produkte hinzufügen wollen, müssen Sie erneut auf **Produkt hinzufügen** klicken und die obigen Schritte wiederholen.
10. Klicken Sie auf **Weiter**. Die Registerkarte **Einzelpostennotiz** wird angezeigt.
11. Klicken Sie auf **Einzelpostennotiz hinzufügen**, geben Sie die gewünschte Beschreibung ein und klicken Sie dann auf **Hinzufügen**. Bei Bedarf können Sie den Vorgang für weitere Einzelpostennotizen wiederholen.
12. Klicken Sie auf **Fertig**. Der Verkaufsartikel wird zur Registerkarte **Verkaufsartikel** hinzugefügt.

Verkaufsartikel ändern

Sie können Verkaufsartikel nach Bedarf ändern und löschen.

Hinweis
Sie können ein Verkaufsartikel nur ändern oder löschen, wenn dieser noch nicht fakturiert wurde. Wenn ein Verkaufartikel bereits einmal abgerechnet wurde, kann er nur noch eingesehen, aber nicht mehr bearbeitet oder gelöscht werden.

So können Sie einen Verkaufsartikel ändern

1. Gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie auf die Registerkarte **Verkaufsartikel**.
2. Klicken Sie auf den Verkaufsartikel, den Sie ändern wollen. In der rechten Seitenleiste werden die Details zum Verkaufsartikel angezeigt.
3. Ändern Sie die relevanten Abschnitte nach Bedarf:

- Klicken Sie im Bereich **Kundeninformationen** auf das Stiftsymbol und bearbeiten Sie die relevanten Felder. Klicken Sie dann auf **Speichern**.
- Klicken Sie in den Bereichen **Produkte** und **Einzelpostennotizen** auf  , um neue Produkte oder Einzelpostennotizen hinzuzufügen. Alternativ können Sie auch auf die Stift- oder Papierkorbsymbole klicken, wenn Sie vorhandene Elemente bearbeiten oder löschen wollen. Klicken Sie für jedes Produkt oder jede Einzelpostennotiz, das/die Sie hinzufügen oder ändern, zum Abschluss auf **Speichern**.

Hinweis
Weitere Informationen über die bearbeitbaren Felder in einem Verkaufsartikel finden Sie im Abschnitt '"Einen neuen Verkaufsartikel erstellen" (S. 224)'.

So können Sie einen Verkaufsartikel löschen

1. Gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie auf die Registerkarte **Verkaufsartikel**.
2. Klicken Sie in der äußersten rechten Spalte des Verkaufsartikels, den Sie löschen wollen, auf das Drei-Punkte-Symbol und wählen Sie dann **Löschen**.
3. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Mit Verträgen arbeiten

Auf der Registerkarte **Verträge** werden alle Verträge angezeigt, die Sie für Kunden erstellt haben.

Jeder Vertrag definiert eine Reihe von Services, die Sie einem Kunden anbieten – einschließlich des Preises und der Vertragsbedingungen. Die Rechnungen werden dann gemäß den im Vertrag festgelegten Zahlungsbedingungen ausgestellt.

Wenn Sie einen Vertrag erstellen, befolgen Sie alle Bildschirmanweisungen des Assistenten, indem Sie die relevanten Vertragsinformationen, Abrechnungsinformationen und Vertragsteile hinzufügen.

Wenn Sie auf die Vertragsfunktionalität zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Verträge**.

Einen neuen Vertrag erstellen

Wenn Sie einen neuen Vertrag erstellen, werden Sie von einem Assistenten durch drei Hauptschritte geführt. In diesen Schritten werden Sie:

- Grundlegende Vertragsinformationen hinzufügen
- Abrechnungsinformationen hinzufügen
- Vertragsteile hinzufügen

Hinweis
Wenn Sie die Advanced Automation-Funktionalität aktiviert (siehe Abschnitt '"Advanced Automation aktivieren" (S. 179)') und einen neuen Kunden mit Abrechnungsinformationen definiert haben, werden beim Erstellen eines neuen Vertrags für diesen Kunden nur zwei Schritte im Vertragsassistenten (nämlich die grundlegenden Vertragsinformationen und die Vertragsteile) aufgeführt.

Wenn Sie den Assistenten abschließen, wird der Vertrag automatisch in die Liste der bestehenden Verträge aufgenommen (die wiederum auf der Registerkarte **Verträge** angezeigt wird). Diese können dann bei Bedarf angezeigt und aktualisiert werden (siehe Abschnitt '"Einen Vertrag ändern" (S. 231)').

So können Sie einen neuen Vertrag erstellen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Klicken Sie zuerst auf die Registerkarte **Verträge** und dann auf **+ Neuer Vertrag**.

Hinweis
Wenn Sie bestehende Kunden haben, denen keine Verträge zugewiesen wurden, werden Sie aufgefordert, für diese Kunden Verträge zu erstellen. Wenn Sie auf **Erstellen** oder **Verträge für bestehende Kunden erstellen** klicken, können Sie den entsprechenden Kunden auswählen und dann auf **Weiter** klicken. Anschließend müssen Sie, wie im nächsten Schritt beschrieben, die Vertragsinformationen festlegen.

3. Definieren Sie im angezeigten Assistenten die folgenden Vertragsinformationen:
   - **Referenznummer**: (Optional) Die Referenznummer, die häufig in Papierverträgen verwendet wird.
   - **Vertragsname**: Der Name des Vertrages.
   - **Organization**: Wählen Sie die entsprechende Organisation aus dem Listenfeld aus.
   - **Kontakt-E-Mail**: (Optional) Der E-Mail-Kontakt für diesen Vertrag.
   - **Rechnungssteller**: Wählen Sie den entsprechenden Rechnungssteller.
   - Wählen Sie im Bereich **Zahlungsdetails** einen Intervallzeitraum (**Jeden Monat**, **Vierteljährlich**, **Halbjährlich**, **Jedes Jahr**), wann die Rechnung gestellt werden soll (**Im Voraus** oder **Nachträglich**) und die Zahlungsmethode aus (**Vorautorisierte Abbuchung** oder **Manuell bezahlen**; dies ermöglicht es den Kunden, ihre Rechnungen per Überweisung oder über eine der Zahlungsintegrationen zu bezahlen. Die Kunden können außerdem die Rechnung auch zwecks Lastschrifteinzug an ihre Hausbank senden).
   - Definieren Sie im Bereich **Vertragszeitraum** den Gültigkeitszeitraum für den Vertrag (wenn der Vertrag kein festgelegtes Ende hat, aktivieren Sie das Kontrollkästchen **Unbegrenzt**) und bestimmen Sie dann, ob die Rechnung per E-Mail oder per Post zugestellt werden soll.
   - Definieren Sie im Bereich **Kundenadresse** die relevanten Adressdetails.

- Wenn Sie Blockstunden in Ihre Services einschließen wollen, aktivieren Sie den Optionsschalter **Blockstunden**. Definieren Sie dann die Anzahl der Blockstunden und den prozentualen Grenzwert für die Erneuerung. Aktivieren Sie das Kontrollkästchen **Vorschuss**, wenn es sich bei diesem Vertrag um eine Vorschussvereinbarung handelt (und die Blockstunden monatlich, viertel- oder halbjährlich abgerechnet werden). Wenn die Option aktiviert ist, können Sie:

  Verbleibende Stunden verwerfen (um die Reststunden zu verwerfen, die im Abrechnungszeitraum des Vorschusses nicht verbraucht wurden).

  Verbleibende Stunden behalten (um die Reststunden zu behalten, die während des Abrechnungszeitraums des Vorschusses nicht verbraucht wurden).

  Die für Tickets aufgewendete Zeit wird entweder separat abgerechnet, als nicht abrechenbar markiert (wenn die Arbeit Teil einer Festpreisvereinbarung ist) oder mit dem aktuellen Blockstundenguthaben verrechnet.

  Hinweis
  Mit Blockstunden können Sie einen Block von Support-Stunden für Kunden reservieren. Sie werden anhand des standardmäßigen Blockstunden-Produktsatzes abgerechnet, der in den Rechnungseinstellungen festgelegt ist. Der Grenzwert für die Erneuerung dient dazu, Sie zu benachrichtigen, wenn für den aktuellen Block nur noch eine bestimmte Anzahl von Stunden übrig ist. Die Benachrichtigung ermöglicht es Ihnen, einen Verkaufsartikel für einen neuen Block zu erstellen, indem Sie auf **Blockstunden erneuern** klicken. Sobald der neue Block abgerechnet ist, wird er in der verfügbaren Blockstundenbilanz angezeigt.

- Aktivieren Sie das Kontrollkästchen **Anteilig**, wenn Änderungen am Vertrag anteilig oder zum vollen Preis abgerechnet werden sollen.

4. Klicken Sie auf **Weiter**, um zu Schritt 2 des Vertragsassistenten (den Abrechnungsinformationen) zu gelangen. Beachten Sie: Wenn Sie für diesen Kunden bereits Abrechnungsinformationen definiert haben, dann gelangen Sie zu Schritt 3 des Vertragsassistenten (dem Hinzufügen von Vertragsteilen, siehe Schritt 7, weiter unten).
5. Definieren Sie folgende Felder:
   - **Unternehmensname**: Der vordefinierte Kundenname.
   - **Rechtsform**: Wählen Sie den zutreffenden juristischen Namen für das Unternehmen des Kunden.
   - **Schuldnercode**: (Optional) Der in Drittanbieter-Systemen verwendete Kundencode.
   - **E-Mail**: (Optional) Die vordefinierte E-Mail-Adresse des Kunden.
   - **Website**: (Optional) Die URL der Website des Kunden.
   - **Hauptgeschäftsstelle**: (Optional) Wählen Sie das übergeordnete Unternehmen (die Muttergesellschaft) aus der Liste aus.
   - **Umsatzsteuernummer**: (Optional) Die Umsatzsteueridentifikationsnummer des Kunden.
   - **Zeiterfassungsrundung (Minuten)**: Definieren Sie einen Wert, der die Standardeinstellung für die allgemeine Rundungszeit (die minimale Rundung für eine Arbeitszeiteinreichung) für

den Kunden überschreibt. Ein Beispiel: Wenn ein Techniker fünf Minuten arbeitet, kann dies automatisch auf 15 Minuten (oder auf den von Ihnen festgelegten Wert) aufgerundet werden.

- **Zahlungsbedingungen (Tage)**: (Optional) Legen Sie die Anzahl an Tagen fest, in denen ein Kunde seine Zahlung zu leisten hat.
- **Lastschrift**: (Optional) Aktivieren Sie das Kontrollkästchen, wenn die Zahlung per Bankeinzug vorgenommen wird.
- **Zwischensummen auf der Rechnung erstellen**: (Optional) Aktivieren Sie das Kontrollkästchen bei Bedarf.
- **Die Abrechnung zu einer Rechnung konsolidieren**: (Optional) Aktivieren Sie das Kontrollkästchen bei Bedarf.
- **Bankkonto**: (Optional) Geben Sie die Kontonummer des Kunden ein.

  Das Feld **Bankkonto** bezieht sich auf die Lastschrift-Funktionalität, über die Sie Anweisungen an Ihre Bank senden können, um einen bestimmten Kunden zu belasten (zusätzlich zu einer Offline-Bestätigung kann eine Rechnung an Ihre Bank übermittelt werden, um einen Kunden zu belasten; die Rechnung sollte entsprechende Angaben zum Kunden enthalten). Weitere Informationen finden Sie im Abschnitt '"Abrechnungsinformationen für einen Mandanten definieren" (S. 42)'.

6. Klicken Sie auf **Weiter**, um zu Schritt 3 des Vertragsassistenten (das Hinzufügen von Vertragsteilen) zu gelangen.
7. Klicken Sie auf **Vertragsteil hinzufügen**.

   Hinweis
   Wenn der ausgewählte Kunde bestimmte Produkte oder Services von Acronis definiert hat, werden Sie aufgefordert, diese je nach Bedarf zu bearbeiten oder zu löschen. Sie können dann (wie unten beschrieben) weitere Vertragsteile hinzufügen.

8. Definieren Sie folgende Felder:
   - **Art des Vertragsteils**: Wählen Sie die entsprechende Art des Vertragsteils aus einer der folgenden Möglichkeiten aus:
     - **Standardtyp**: Wird für allgemeine Verträge verwendet, die keine Integration verwenden.
     - **IKT-Service**: Mit diesem Typ können Sie einen IKT-Service (Informations- und Kommunikationstechnologie) (wie z.B. einen *Datei-Storage*) verkaufen. Wenn Sie diesen Service anbieten, können verschiedene IKT-Assets hinzugefügt werden – wie etwa Datacenter, Storage-Server, Netzwerk-Switches usw. Sie können diese Assets aber auch in anderen Vertragsteilen verwenden. Wenn Sie beispielsweise den IKT-Service *Datei-Storage* erstellen, können Sie ein Datacenter, einen Storage-Server und einen Switch hinzufügen. Wenn Sie einen anderen IKT-Service hinzufügen, der ebenfalls dieses Datacenter nutzt, können Sie das Datacenter immer noch in diesem anderen Vertragsteil hinzufügen. Wenn Sie ein Ticket für den Kunden erstellen, lässt Sie das System zuerst einen IKT-Service und dann das/die zugehörige(n) Asset(s) (Ressourcen) auswählen.
     - **Verwalteter Service**: Dieser Typ wird in der Regel für verwaltete Services wie *Workstation-Verwaltung* verwendet. Fügen Sie die entsprechenden Maschinen zum Vertragsteil hinzu.

Sobald dies geschehen ist, werden diese Assets aus der Liste der verfügbaren Maschinen entfernt, sodass sie mit keinem anderen Vertragsteil verbunden werden können.

- Wählen Sie im Bereich **Produkt oder Services** die entsprechenden Produkte oder Services aus, die Sie hinzufügen wollen, einschließlich der Anzahl und der Preise für das Produkt oder den Service.

  Das Feld **Tatsächliche Menge** definiert den Umfang des Service, den Sie Ihrem Kunden derzeit im Rahmen des Vertrags bieten. Dieser Wert kann folgendermaßen festgelegt sein:
  - **Manuell**: Ihrem Kunden wird pro Abrechnungszeitraum ein fester Service-Betrag in Rechnung gestellt. Beispielsweise fünf verwaltete Workstations pro Monat.
  - **Automatisch**: Ihrem Kunden wird der Service-Umfang in Rechnung gestellt, der von einer der aktivierten Integrationen gemeldet wurde. Beispielsweise kann die Acronis Cyber Cloud-Integration in einem Monat fünf Server und im folgenden Monat sechs Server melden.

  Das Feld **Mindestmenge** ermöglicht es Ihnen, eine Mindestservice-Umfang festzulegen, der dem Kunden berechnet wird. Wenn der im Feld **Tatsächliche Menge** definierte Wert höher ist als der im Feld **Mindestmenge** definierte Wert, wird die tatsächliche Menge zur Abrechnung verwendet. Wenn der im Feld **Mindestmenge** definierte Wert höher ist als der im Feld **Tatsächliche Menge** definierte Wert, wird die Mindestmenge verwendet. Diese Felder werden auch verwendet, um die Nutzungs- und Rentabilitätsangaben in Berichten zu berechnen.

  Die fakturierbare Mindestmenge verbessert die Möglichkeit, Services als Pakete zu verkaufen. Wenn Sie z.B. einen Vertrag für einen Kunden erstellen, der ein Backup von mindestens zwei Geräten und mindestens 500 GB Storage benötigt, wird die erstellte Rechnung zwei Rechnungsposten für die Geräte und für den Storage enthalten, ohne einen Verkaufsartikel für den Storage zu erstellen. Dem Kunden kann auch jede Nutzung über die im Vertrag definierte Mindestmenge hinaus in Rechnung gestellt werden (für belegten Speicherplatz über die definierten 500 GB hinaus wird ein separater Verkaufsartikel erstellt).
- Definieren Sie im Bereich **Vertragszeitraum** den relevanten Zeitraum. Wenn es kein Enddatum gibt, aktivieren Sie das Kontrollkästchen **Unbegrenzt**. Standardmäßig werden diese Daten aus den Einstellungen für die Vertragsinformationen übernommen (siehe oben). Beachten Sie, dass der Datumsbereich kürzer sein sollte als der des Hauptvertrages. Wenn Sie einen längeren Zeitraum anwenden wollen, müssen Sie zuerst den Hauptvertragszeitraum anpassen.
- Aktivieren Sie den Optionsschalter **Test**, wenn Sie wollen, dass der Vertragsteil zu einem Testzeitraum gehört. Bestimmen Sie den Testzeitraum, indem Sie die entsprechende Anzahl von Monaten auswählen. Testvertragsteile werden in Rechnungen während eines Fakturierungslaufs mit einem Preis von Null zur Information aufgenommen. Nach Ablauf des Testzeitraums wird in den generierten Rechnungen der reguläre Preis ausgewiesen.

Hinweis
Die Testoption kann pro Vertragsteil nur einmalig angewendet werden. Außerdem kann die Testoption nicht aktiviert werden, wenn für den ausgewählten Vertragsteil bereits eine Rechnung gestellt wurde.

- **Integrationen**: Wählen Sie die relevante Integration aus. Wenn eine Integration ausgewählt wird, wird ein zusätzliches Feld **Maschinen auf der Rechnung anzeigen** angezeigt. Dieses Feld definiert, ob die Rechnung Maschinendetails enthalten soll; als Voreinstellung ist **Ja** ausgewählt.

  Mithilfe von Integrationen können Sie die Anzahl eines Vertragsteils an die tatsächliche Nutzung binden, die von der ausgewählten Integration bereitgestellt wird (wie etwa die Anzahl der aktiven Workloads für einen bestimmten Kunden, die Anzahl der virtuellen Maschinen oder die Menge an Gigabytes, die ein Kunde im von gehosteten Storage verwendet).

  Zu den verfügbaren Workloads gehören auch solche mit Produkten und Services von Acronis (wie etwa Cyber Disaster Recovery Cloud oder Cyber Protection) sowie RMM-Integrationen.

  Um die relevanten integrierten Workloads zu finden, können Sie nach dem Client (d.h. nach solchen Workloads, die zu dem ausgewählten Client gehören), nach dem Workload-Typ (Workloads eines bestimmten Workload-Typs) oder nach einzelnen Workloads filtern (suchen Sie nach den relevanten Workloads und wählen Sie diese aus der Workload-Liste aus).

  In diesem Abschnitt können Sie auch eine RMM-Integration auswählen und die verschiedenen damit verbundenen Agenten verknüpfen (damit die Alarm-zu-E-Mail-RMM-Funktionalität korrekt funktioniert, müssen Sie die richtigen Maschinen zu den gültigen Verträgen hinzugefügt haben). Advanced Automation verwendet diese, um die RMM-Site oder -Gruppe mit dem richtigen Kunden zu verbinden. Mithilfe dieser Informationen kann es die SLA auf das Ticket anwenden, basierend auf dem Vertrag, mit dem die Maschine verbunden ist.

  Hinweis
  Es wird außerdem das Kontrollkästchen **Automatische Updates** angezeigt, welches die automatische Berechnung der Workload-Anzahl für Rechnungen ermöglicht. Wenn diese Option ausgewählt wird, wird das Feld **Tatsächliche Menge** im Bereich **Produkt oder Services** deaktiviert.

- **Service-Level-Vereinbarung (SLA)**: Wählen Sie die relevante SLA aus.

9. Klicken Sie auf **Hinzufügen**, um den Vertragsteil zum Vertrag hinzuzufügen.
10. (Optional) Klicken Sie auf **Vertragsteile hinzufügen**, wenn Sie weitere Vertragsteile hinzufügen wollen.
11. Klicken Sie auf **Fertig**. Der Vertrag wird auf der Registerkarte **Verträge** zur Liste der bestehenden Verträge hinzugefügt.

Einen Vertrag ändern

Sie können einen Vertrag jederzeit anpassen, wozu auch die Produkte oder Services gehören, die mit einem Vertrag verbunden sind.

Hinweis
Sie können einen Vertrag oder einen Vertragsteil nicht löschen. Stattdessen müssen Sie die Vertragslaufzeit auf 'Ende' setzen, um sie zu deaktivieren (z.B. zum Ende des aktuellen Monats). Dies sollte zuerst auf die relevanten Vertragsteile und dann erst auf den Vertrag selbst angewendet werden. Der Vertrag wird dann deaktiviert, ist aber immer noch über die Suche verfügbar.

So können Sie einen Vertrag ändern

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Klicken Sie auf der Registerkarte **Verträge** auf den Vertrag, den Sie bearbeiten wollen.
3. Ändern Sie im rechten Fensterbereich die relevanten Vertragsdetails. Klicken Sie in jedem relevanten Abschnitt auf das Stiftsymbol und anschließend auf ✓.

   Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"Einen neuen Vertrag erstellen" (S. 226)'.

   Hinweis
   Wenn Blockstunden für einen Vertrag aktiviert wurden, können Sie die Blockstunden manuell erneuern, indem Sie auf **Blockstunden erneuern** klicken. Es wird automatisch ein neuer Verkaufsartikel für Blockstunden erstellt und eine Bestätigungsmeldung angezeigt.

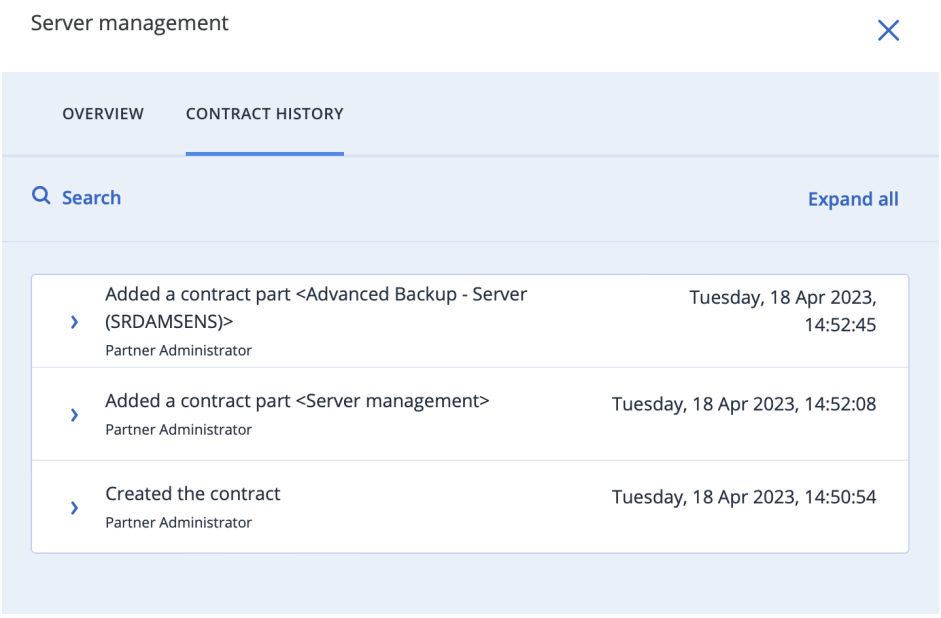
4. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

Den Änderungsverlauf eines Vertrags überprüfen

Sie können alle Änderungen überprüfen, die an einem Vertrag während seiner Laufzeit vorgenommen werden. Das Protokoll, in dem dieser Änderungsverlauf gespeichert wird, enthält die Daten zum erstmaligen Erstellen des Vertrags sowie zu allen nachfolgenden Aktualisierungen.

So können Sie Änderungsverlauf eines Vertrags überprüfen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Klicken Sie zuerst auf die Registerkarte **Verträge** und dann in der angezeigten Vertragsliste auf den gewünschten Vertrag.
3. Klicken Sie im angezeigten rechten Fensterbereich auf die Registerkarte **Vertragshistorie**.



4. [Optional] Sie können auch das **Suchen**-Werkzeug verwenden, um zu einer bestimmten Aktualisierung zu gelangen. Sie können außerdem die Optionen **Alle erweitern** / **Alle einklappen** verwenden, wenn Sie die Details zu allen Aktualisierungen anzeigen/ausblenden wollen.
5. Wenn Sie eine bestimmte Änderung am Vertrag einsehen wollen, klicken Sie auf die betreffende Zeile. Je nach der vorgenommenen Änderung werden unterschiedliche Informationen angezeigt:
   - Wann der Vertrag erstellt wurde: Es werden die meisten der beim Erstellen des Vertrags festgelegten Informationen angezeigt, einschließlich der Abrechnungsinformationen.
   - Wann der Vertrag aktualisiert wurde: Es werden nur die aktualisierten Vertragsattribute sowie deren vorherige/neue Werte angezeigt.
   - Wann ein Vertragsteil hinzugefügt wurde: Es werden die meisten der beim Hinzufügen eines Vertragsteils definierten Informationen angezeigt, einschließlich aller aktivierten Integrationen.
   - Wann ein Vertragsteil aktualisiert wurde: Es wird nur der aktualisierten Vertragsteil sowie dessen vorherigen/neuen Werte angezeigt.
   - Wann ein Vertragsteil entfernt wurde: Es wird das letzte Stadium des Vertragsteils, einschließlich aller aktivierten Integrationen, angezeigt.

Mit benutzerdefinierten Preisen arbeiten

Mit der benutzerdefinierten Preisgestaltung können Sie den Preis für ein Produkt anpassen. Dies kann Ihnen dabei helfen, die Anwendung von spezifischen Preisvereinbarungen mit Kunden zu automatisieren.

Wenn Sie z.B. normalerweise einen Stundensatz für Projektarbeit von 100 € haben, mit einem anderen Kunden jedoch einen Stundensatz von 130 € vereinbart haben, können Sie für diesen Kunden einen benutzerdefinierten Preis für den '*Stundensatz für Projektarbeit*' mit einem Preis von

130 € erstellen. Jedes Mal, wenn Sie einen Verkaufsartikel oder Tickets für diese Art von Arbeit für diesen Kunden erstellen, wird dann der benutzerdefinierte Preis angewendet.

Hinweis
Sie können einen Preis nur dann anpassen, wenn das Produkt kein Vertragsprodukt ist.

Wenn Sie auf die benutzerdefinierte Preise zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Preise**.

Einen benutzerdefinierten Preis hinzufügen

So können Sie einen benutzerdefinierten Preis hinzufügen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Preise**.
2. Klicken Sie auf **+ Neuer benutzerdefinierter Preis**.
3. Wählen Sie den Kunden aus, auf den Sie den benutzerdefinierten Preis anwenden wollen, und klicken Sie anschließend auf **Benutzerdefinierten Produktpreis hinzufügen**. Beachten Sie, dass in der Kundenliste nur Kunden angezeigt werden, für die noch keine benutzerdefinierten Preise spezifiziert wurden.
4. Wählen Sie im Feld **Produktkategorie** die relevante Kategorie aus dem Listenfeld aus.
5. Wählen Sie im Feld **Produkt** das relevante Produkt aus dem Listenfeld aus. In dieser Liste werden nur Produkte mit Standardpreisen angezeigt. Dagegen werden keine Produkte angezeigt, für die bereits ein individueller Preis definiert wurde.
6. Aktivieren Sie den Umschalter **Aktiv**, wenn Sie wollen, dass dieser benutzerdefinierte Preis verfügbar gemacht wird.
7. Geben Sie den benutzerdefinierten Produktpreis ein und klicken Sie auf **OK**.
   Für eine genauere Abrechnung können die Preise für in Verträgen, Angeboten und Verkaufsartikeln verwendete Produkte bis zu vier Stellen nach dem Dezimaltrennzeichen verwenden. Zum Beispiel: 0,0750 Euro. Diese Preise werden dann in Rechnungen, Berichten, Abrechnungspositionen in Tickets und Stundensätzen aufgerundet.
8. Wenn Sie einen weiteren benutzerdefinierten Preis hinzufügen wollen, müssen Sie auf **Benutzerdefinierten Produktpreis hinzufügen** klicken. Wenn nicht, dann klicken Sie auf **Erstellen**.

Einen benutzerdefinierten Preis bearbeiten

So können Sie einen benutzerdefinierten Preis bearbeiten

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Benutzerdefinierte Preise**.
2. Klicken Sie auf den Kunden, dessen benutzerdefinierte Preise Sie bearbeiten wollen.
3. Klicken Sie im rechten Fensterbereich auf das Stiftsymbol und nehmen Sie Ihre Änderungen vor.

Sie können beispielsweise einen neuen benutzerdefinierten Preis hinzufügen (siehe Abschnitt '"Einen benutzerdefinierten Preis hinzufügen" (S. 234)') oder die Details eines vorhandenen benutzerdefinierten Preises bearbeiten.

4. Klicken Sie, wenn Sie fertig sind, auf ✓.

Rechnungen

Mit dem Modul **Rechnungen** können Sie Rechnungen, die Sie für Ihre Kunden erstellen, verwalten und nachverfolgen. Mit diesem Modul können Sie:

- Neue Rechnungen für Kunden generieren.
- Die Zahlung einer Rechnung bestätigen.
- Eine Rechnung erneut senden.
- Den Verlauf früher ausgestellter Rechnungen nachverfolgen.
- Eine Rechnung oder einen Rechnungsstapel herunterladen und/oder exportieren.

Wenn Sie auf das Modul **Rechnungen** zugreifen wollen, gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Rechnungen**.

Hinweis
Nur Benutzer mit den Rollen Administrator, Direktor, Finanzen, Finanzdirektor oder Verkauf können Rechnungen generieren. Benutzer, denen die Rollen 'Client-Manager' oder 'Kunde' zugewiesen wurden, können nur Rechnungen anzeigen und herunterladen.

Aktuelle Rechnungen anzeigen

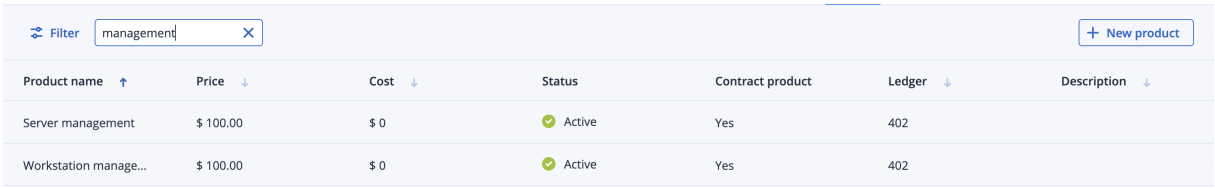
Wenn Sie Ihre aktuellen Rechnungen einsehen wollen, gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Rechnungen**. In der eingeblendeten Anzeige **Rechnungen** können Sie dann alle Rechnungen in Advanced Automation einsehen.

Es werden Informationen zu jeder Rechnung angezeigt. Wie etwa:

- Das Datum, an dem die Rechnung erstellt wurde.
- Der Zahlungsstatus (**Bestätigt** oder **Nicht bestätigt**) und, falls bezahlt, das Datum, an dem die Zahlung erfolgte.
- Falls eine E-Mail an den Kunden gesendet wurde.
- Die Höhe der Rechnung.
- Falls die Rechnung mit Ihrer Buchhaltungssoftware synchronisiert wurde (sofern aktiviert).

Klicken Sie auf eine Rechnung, wenn Sie im rechten Fensterbereich weitere Details zu dieser Rechnung einsehen wollen. Zu diesen Informationen gehören ein allgemeiner Überblick über die Rechnung sowie Details zu den einzelnen Rechnungselementen. Sie können in diesem Fensterbereich die Rechnung bei Bedarf auch herunterladen oder exportieren.

Sie können die angezeigte Liste auch filtern oder sortieren, um eine spezifische Rechnung zu finden. Wenn Sie eine erweiterte Filterung benötigen, können Sie mit dem Tool **Filter** genauer definieren, welche spezifischen Rechnungen angezeigt werden sollen.



Eine neue Rechnung generieren

Wenn Sie eine neue Rechnung oder einen neuen Rechnungsstapel generieren, erstellen Sie eigentlich die Rechnungsdaten mithilfe einer Rechnungsvorlage (wie in Abschnitt '"Abrechnungseinstellungen" (S. 280)' definiert). Diese Daten können dann über Advanced Automation als Rechnung (wenn dies so in Ihren Abrechnungs- und Vertragseinstellungen festgelegt wurde) oder auf einem anderen Weg versendet werden. So kann Ihre Buchhaltungssoftware beispielsweise so konfiguriert sein, dass sie Rechnungen per E-Mail an Ihre Kunden versendet oder die Rechnungen in Papierform verschickt werden.

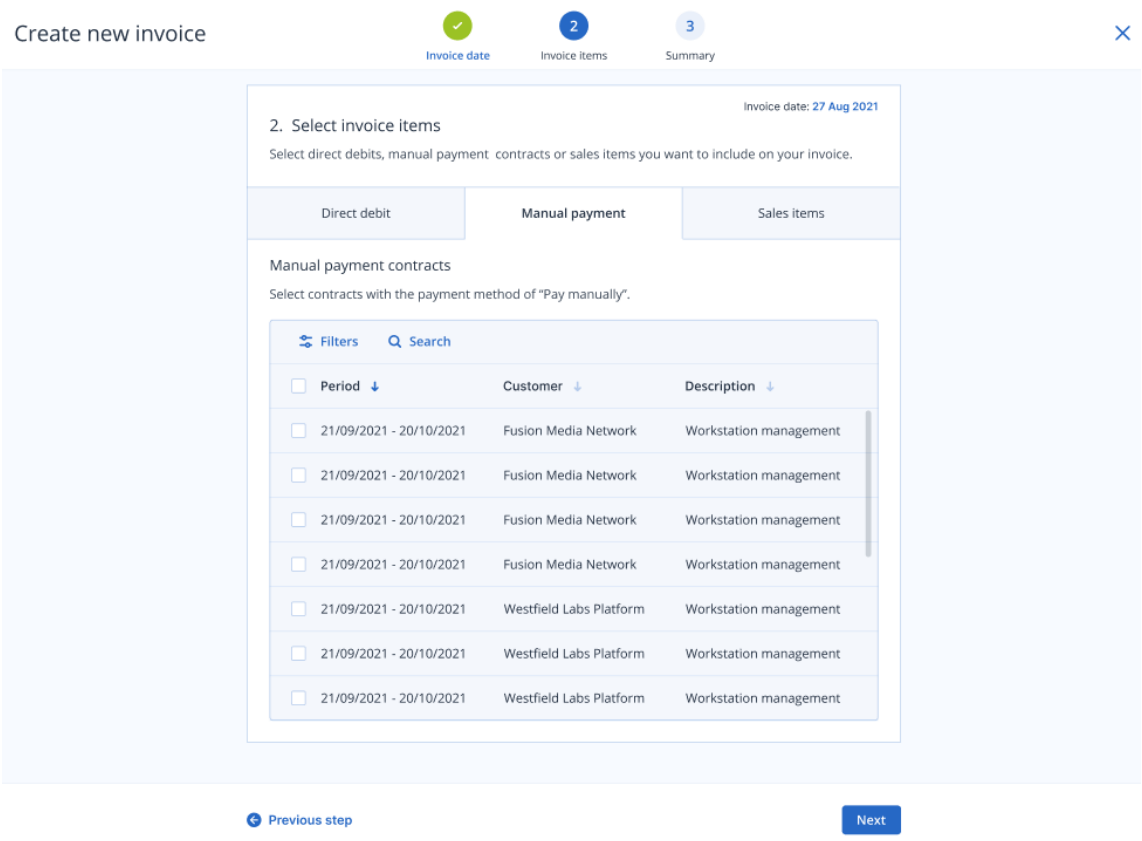
Sie können eine Rechnung bei Bedarf auch erneut senden (siehe Abschnitt '"Eine Rechnung erneut senden" (S. 238)').

So können Sie eine neue Rechnung generieren

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Rechnungen**.
2. Wenn Sie noch keine Rechnung erstellt haben, können Sie auf **Neu erstellen** klicken. Klicken Sie ansonsten auf **+ Neu**.
   Der Assistent 'Neue Rechnung erstellen' wird angezeigt.
3. Bestimmen Sie das Rechnungsdatum und den entsprechenden Rechnungssteller. Klicken Sie anschließend auf **Weiter**.
4. Wählen Sie die Lastschriften, manuellen Zahlungsverträge und Verkaufsartikel aus, die Sie in die Rechnung aufnehmen wollen:
   - Wählen Sie auf der Registerkarte **Lastschrift** die entsprechenden vorautorisierten Lastschriften aus der angezeigten Liste aus.

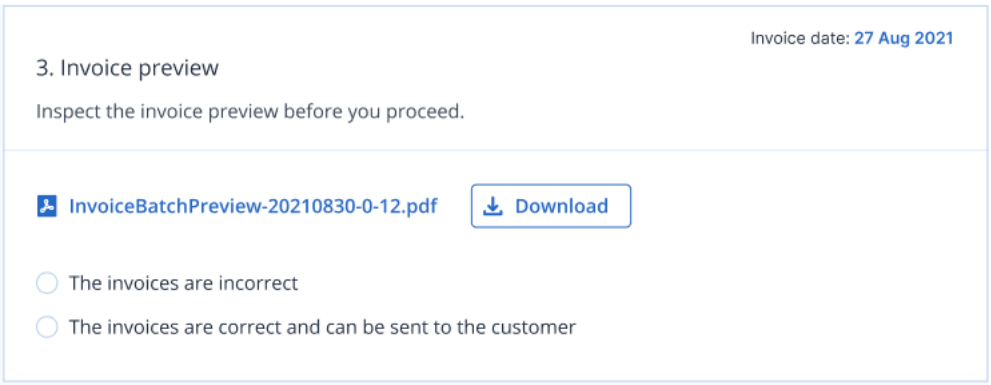
     Hinweis
     Wenn ein Vertrag mit der Zahlungsmethode **Vorautorisierte Abbuchung** definiert wurde, wird er als vorautorisierter Lastschriftvertrag kategorisiert. Dadurch können Kunden ihre Rechnungen per Überweisung oder mithilfe einer der Zahlungsintegrationen begleichen. Sie können die Rechnung auch zwecks Lastschrifteinzug an ihre Hausbank senden.

   - Wählen Sie auf der Registerkarte **Manuelle Zahlungen** diejenigen Verträge aus, die mit **Manuell bezahlen** definiert wurden.
   - Wählen Sie auf der Registerkarte **Verkaufsartikel** die entsprechenden Elemente aus.



Wenn Sie mit der Auswahl der Rechnungselemente fertig sind, können Sie auf **Weiter** klicken.

5. Klicken Sie im Übersichtsfenster auf **Download**, um sich eine Vorschau des Rechnungsstapels im PDF-Format anzusehen.



Wenn die Rechnungsvorschau korrekt ist, klicken Sie auf die Optionsschaltfläche **Die Rechnungen sind korrekt und können an den Kunden gesendet werden**.

Sollte die Rechnungsvorschau falsch sein, wählen Sie **Die Rechnungen sind nicht korrekt**. Dadurch werden Sie wieder zur Hauptansicht für die Rechnungen geleitet und der Rechnungsprozess wird gestoppt. Diese ermöglicht Ihnen außerdem, Ihre Vertrags- und Rechnungselemente neu zu bewerten. Sie können die Rechnung dann erneut erstellen lassen, sobald sie diese korrigiert haben.

6. Klicken Sie auf **Fertig**.

Sie werden zur Rechnungsliste weitergeleitet, wo Sie den soeben generierten Rechnungsstapel einsehen können. Innerhalb von diesem werden auch die einzelnen Rechnungen angezeigt. Die Rechnungen werden dann (je nach den Kundeneinstellungen) per E-Mail versendet oder nicht.

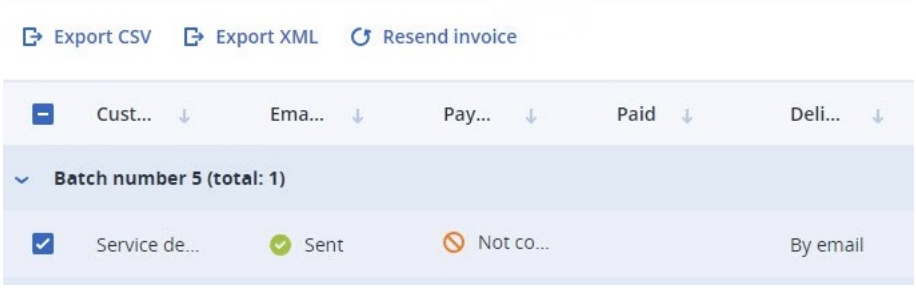
Hinweis
Sie können eine Rechnung nicht selbst aktualisieren, aber einzelne Verkaufsartikel, Zeiteinträge und Vertragsteile, die dann in eine zukünftige, korrigierte Rechnung aufgenommen werden können. Wenn Sie diese Aktualisierungen vorgenommen haben, können Sie anschließend die korrigierte Rechnung generieren.

Eine Rechnung erneut senden

Sie können jede Rechnung erneut versenden, deren Bezahlung noch nicht bestätigt wurde und für die ein Versand per E-Mail festgelegt wurde. Rechnungen, die bereits bezahlt wurden oder für die ein Versand per Post festgelegt wurde, können nicht noch einmal versendet werden.

So können Sie eine Rechnung erneut senden

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Rechnungen**.
2. Wählen Sie die Rechnung(en) aus, die Sie erneut versenden wollen. Die Schaltfläche **Rechnung erneut senden** wird angezeigt (siehe unten).



Hinweis
Wenn Sie mehrere Rechnungen auswählen, von denen jedoch eine oder mehrere als bereits bezahlt bestätigt wurden oder für die ein Versand per Post festgelegt wurde, wird die Schaltfläche **Rechnung erneut senden** zwar angezeigt, aber sie ist deaktiviert.

3. Klicken Sie auf **Rechnung erneut senden**. Die Rechnung wird erneut an den Kunden gesendet. Außerdem wird Ihnen eine Bestätigungsmeldung angezeigt.

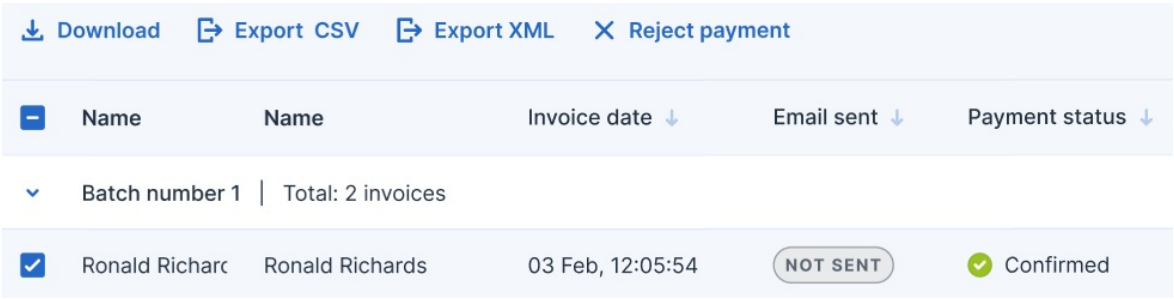
Eine Rechnungszahlung bestätigen oder ablehnen

Sie können die Zahlung für eine Rechnung je nach Bedarf manuell bestätigen oder ablehnen.

So können Sie eine Zahlung bestätigen oder ablehnen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Rechnungen**.
2. Wählen Sie die Rechnung(en) aus, die Sie bestätigen oder ablehnen wollen.

3. Wenn die Zahlung bereits bestätigt wurde, Sie diese aber aus irgendeinem Grund ablehnen müssen, klicken Sie über der Rechnungsliste in der oberen Leiste auf **Zahlung ablehnen**.



Wenn die Zahlung nicht bestätigt ist, klicken Sie auf **Zahlung bestätigen**.
Alternativ können Sie in der rechten Spalte auch auf das Drei-Punkte-Symbol (...) klicken. Klicken Sie im angezeigten Menü entweder auf **Zahlung ablehnen** oderr **Zahlung bestätigen**.
Die angezeigte Rechnungsliste wird aktualisiert.

Eine Rechnung als PDF-Datei herunterladen

Hinweis
Vergewissern Sie sich, dass Sie einen PDF-Reader auf Ihrem Gerät installiert haben, bevor Sie die nachfolgenden Schritte ausführen.

So können Sie eine Rechnung als PDF-Datei herunterladen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Rechnungen**.
2. Wählen Sie die Rechnung(en) aus, die Sie herunterladen wollen.
3. Klicken Sie in der oberen Menüleiste über der Liste der Rechnungen auf **Download**.
   Alternativ können Sie in der rechten Spalte auch auf das Drei-Punkte-Symbol (...) klicken. Klicken Sie im angezeigten Menü auf **Download**.
   Die Rechnung wird im PDF-Format auf Ihr Gerät heruntergeladen.

Eine Rechnung als CSV- oder XML-Datei exportieren

Sie können eine Rechnung als CSV- oder XML-Datei exportieren. Diese Dateien können dann in einem System eines Drittanbieters (z.B. Ihrer Buchhaltungsplattform) verwendet werden, die nicht in Advanced Automation integriert ist.

So können Sie eine Rechnung als CSV- oder XML-Datei exportieren

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Rechnungen**.
2. Wählen Sie die Rechnung(en) aus, die Sie exportieren wollen.
3. Klicken Sie in der oberen Menüleiste über der Liste der Rechnungen auf **CSV exportieren** oder **XML exportieren**.
   Alternativ können Sie in der rechten Spalte auch auf das Drei-Punkte-Symbol (...) klicken. Klicken

Sie im angezeigten Menü auf **CSV exportieren** oder **XML exportieren**.
Die Datei wird im gewählten Format auf Ihr Gerät heruntergeladen.

Produkte

Mit dem Modul **Produkte** können Sie Ihre Produkte definieren und verwalten. Bei diesen Produkten handelt es sich in der Regel um bestimmte Services oder Elemente/Verkaufsartikel, welche Sie Ihren Kunden anbieten. Zum Beispiel Antivirus-Abonnements, Ad-hoc-Support, Hardware-Lieferungen und so weiter.

Produkt können verwendet werden, wenn Sie Verträge oder Verkaufsartikel erstellen. Die Werte, die Sie für das Produktelement eingeben, werden wiederverwendet, wenn Sie einen Verkaufsartikel oder einen Vertrag erstellen. Sie können außerdem nachträglich geändert werden, um zu berücksichtigen, was mit Ihrem Kunden vereinbart wurde.

Beachten Sie, dass nur Benutzer mit den Rollen Administrator, Direktor, Finanzen oder Finanzdirektor Produkte erstellen können. Sobald die Produkte erstellt wurden, können sie von anderen Advanced Automation-Benutzern in Verträgen, Tickets, Projekten, Angeboten usw. verwendet werden.

Wenn Sie auf das Modul **Produkte** zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Produkte**.

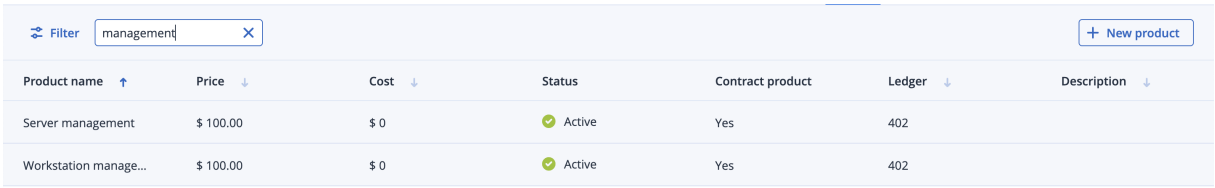
Vorhandene Produkte anzeigen

Wenn Sie die vorhandenen Produkte einsehen wollen, gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Produkte**. In der angezeigten Registerkarte **Produkte** können Sie dann alle aktuellen Produkte in Advanced Automation einsehen. Zu diesen Produkten können sowohl vorkonfigurierte Produkte und Services von Acronis als auch Ihre eigenen Produkte gehören.

Es werden Informationen zu jedem Produkt angezeigt. Wie etwa:

- Der Preis des Produkts
- Die Kosten des Produkts
- Der aktuelle Status des Produkts (**Aktiv** oder **Inaktiv**)
- Der Typ des Produkts (Vertrag, Ticket oder Projekt (in zukünftigen Versionen verfügbar))
- Das Hauptbuch, zu dem das Produkt gehört
- Eine kurze Beschreibung des Produkts

Sie können die angezeigte Liste auch filtern oder sortieren, um ein spezifisches Produkt zu finden. Wenn Sie eine erweiterte Filterung benötigen, können Sie mit dem Tool **Filter** genauer definieren, welche spezifischen Produkte angezeigt werden sollen.



Ein Produkt hinzufügen

Zusätzlich zu den Produkten und Services von Acronis, die in Advanced Automation verfügbar sind, können Sie noch eine beliebige Anzahl von eigenen Produkten und Angeboten erstellen.

So können Sie ein Produkt hinzufügen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Produkte**. Als Grundeinstellung wird die Registerkarte **Produkte** angezeigt.
2. Klicken Sie auf **+ Neues Produkt**. Das Fenster 'Neues Produkt erstellen' wird angezeigt.
3. Definieren Sie Folgendes:
   - **Name**: Geben Sie den Namen des Produkts ein.
   - **Beschreibung**: (Optional) Geben Sie eine Beschreibung für das Produkt ein.
   - **Externe ID**: (Optional) Geben Sie einen eindeutigen Bezeichner (ID) für das Produkt ein. Diese ID sollte außerhalb der aktuellen Produktreihe in Advanced Automation verwendet werden.
   - **Preis**: Geben Sie einen Preis für Ihr Produkt ein. Aktivieren Sie das Kontrollkästchen **Steuerpflichtig**, wenn das Produkt besteuert werden muss (dies hängt von Ihren nationalen Steuergesetzen ab).

     Für eine genauere Abrechnung können die Preise für in Verträgen, Angeboten und Verkaufsartikeln verwendete Produkte bis zu vier Stellen nach dem Dezimaltrennzeichen verwenden. Zum Beispiel: 0,0750 Euro. Diese Preise werden dann in Rechnungen, Berichten, Abrechnungspositionen in Tickets und Stundensätzen aufgerundet.
   - **Kosten**: Geben Sie die Kosten des Produkts oder den Preis an, den Sie an einen Anbieter oder Händler für das Produkt zahlen.

     Für eine genauere Berichtserstellung können bei den Kosten für Produkte bis zu vier Stellen nach dem Dezimaltrennzeichen (z.B. 0,0750 Euro verwendet werden).

     Hinweis
     Um mehr Informationen über die Rentabilität eines Produkts und die damit verbundenen Statistiken bereitzustellen, empfehlen wir Ihnen, dass Sie nicht nur die Preise für Produkte, sondern auch deren Kosten angeben.

   - Wählen Sie im Bereich **Produkteigenschaften** einen oder alle der folgenden Einträge:
     - **Vertragsprodukt**: Aktivieren Sie das Kontrollkästchen, wenn Sie wollen, dass das Produkt in Verträge verfügbar ist.
     - **Ticket-Produkt**: Aktivieren Sie das Kontrollkästchen, wenn Sie wollen, dass das Produkt in Tickets verfügbar ist. Wenn Sie diese Option ausgewählt haben, können Sie auch das zusätzliche Kontrollkästchen **Preis durch den Techniker anpassbar** aktivieren. Dadurch

können Techniker den Standardpreis anpassen, wenn dieses Produkt in einem Ticket verwendet wird.

- **Projekt-Produkt**: (In zukünftigen Versionen verfügbar) Aktivieren Sie das Kontrollkästchen, wenn Sie wollen, dass das Produkt in Projekten verfügbar ist. Wenn Sie diese Option ausgewählt haben, können Sie auch das zusätzliche Kontrollkästchen **Preis je nach Projekt anpassbar** aktivieren. Dadurch kann der Standardpreis angepasst werden, wenn dieses Produkt in einem bestimmten Projekt verwendet wird.
- Sie können zudem das Kontrollkästchen **Produkt für aktivitätsbasierte Ticket-Abrechnung** aktivieren, wenn Sie wollen, dass das Produkt für Techniker in Tickets aufgeführt wird. Dieses Feld ist nicht verfügbar, wenn die Option **Vertragsprodukt** ausgewählt wurde.

Hinweis
Diese Option stellt sicher, dass wenn für einen Experten zusätzliche Zeit benötigt wird (z.B. weil ein Techniker die Unterstützung eines Architekten oder Sicherheitsexperten benötigt), diese einem Ticket zugewiesen werden kann. Diese Stunden können dann mit ihrem speziellen Stundensatz statt mit dem standardmäßigen Ticket-Satz abgerechnet werden.

- **Hauptbuch**: (Optional) Wählen Sie das entsprechende Hauptbuch aus dem Listenfeld aus.
- **Aktiv**: (Optional) Aktivieren Sie das Kontrollkästchen, um das Produkt verfügbar zu machen.
- **VAR-Produkt**: (Optional) Aktivieren Sie das Kontrollkästchen, wenn Sie das Produkt weiterverkaufen, was bedeutet, dass Sie das Produkt zuerst von einem anderen Anbieter kaufen. Wenn dieses Kontrollkästchen aktiviert ist, wird der Umsatz für dieses Produkt separat als 'VAR'-Umsatz (für Value-Added Reseller) zusammengefasst.

4. Klicken Sie, nachdem Sie die Details zu Ihrem neuen Produkt überprüft haben, auf **Fertig**.

Ein Produkt bearbeiten

So können Sie ein Produkt bearbeiten

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung** –> **Produkte**. Als Grundeinstellung wird die Registerkarte **Produkte** angezeigt.
2. Klicken Sie auf ein Produkt, das Sie bearbeiten wollen.
3. Klicken Sie im rechten Fensterbereich auf das Stiftsymbol und bearbeiten Sie das Produkt. Weitere Informationen über die bearbeitbaren Felder für ein Produkt finden Sie im Abschnitt '"Ein Produkt hinzufügen" (S. 241)'.

Hinweis
Wenn ein Vertragsprodukt in einem Produkt-Bundle enthalten ist, können Sie es nicht aktualisieren. Sie werden aufgefordert, es zunächst aus dem betreffenden Produkt-Bundle zu entfernen, bevor Sie es hier aktualisieren können.

4. Klicken Sie, wenn Sie fertig sind, auf ✓.

Die Kosten und Preise von Acronis Produkten definieren

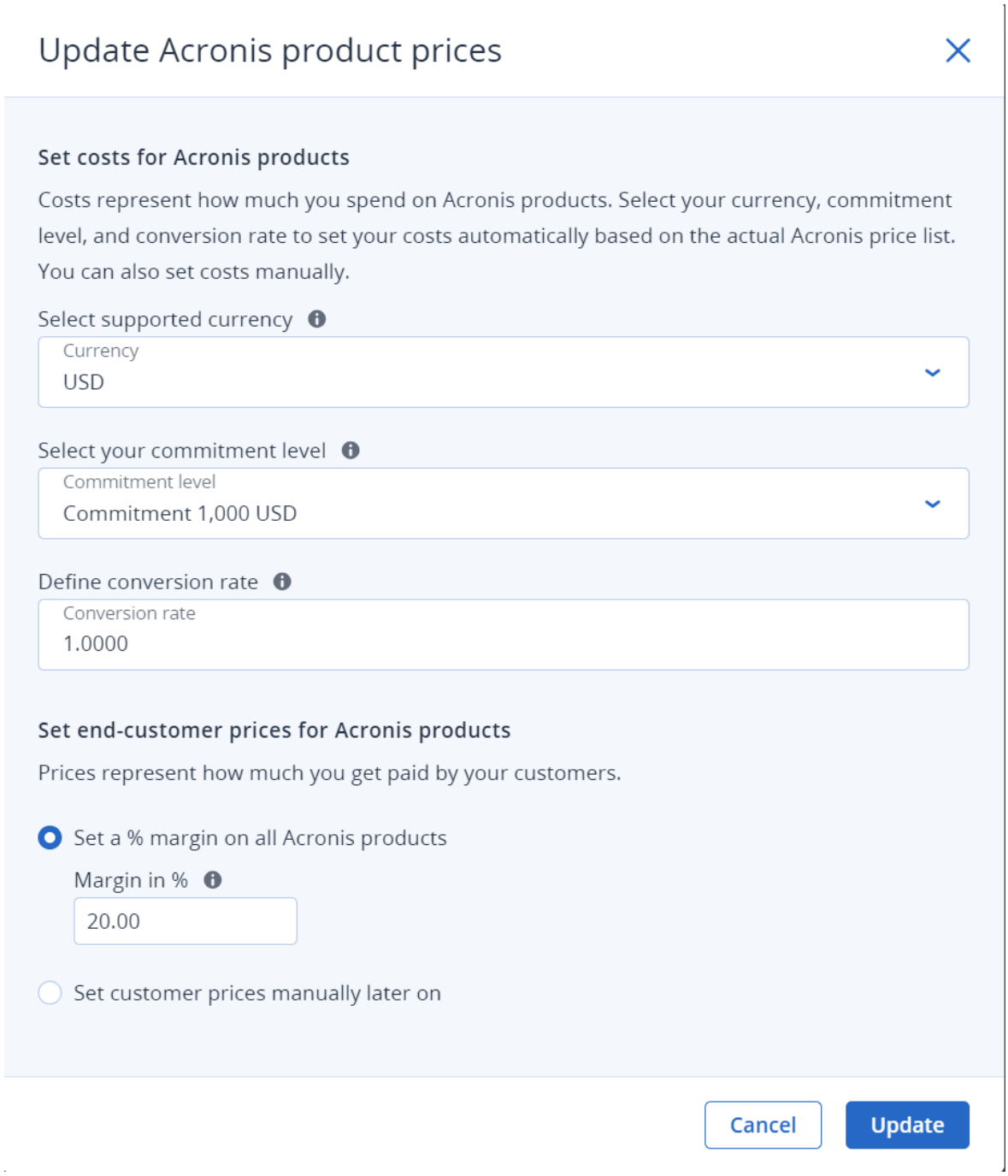
Auf der Registerkarte **Produkte** können Sie die Kosten und Preise der Acronis Produkte definieren, die in Advanced Automation verwendet werden. Die definierten *Kosten* bestimmen, wie viel Sie für Acronis Produkte ausgeben. Dagegen definieren die *Preise*, wie viel Sie von Ihren Kunden bezahlt bekommen.

Mit dieser Funktion können Sie:

- Die Kosten für Acronis Produkte auf Grundlage der aktuellen Acronis Preisliste, der Währung des jeweiligen Partners (bzw. des Wechselkurses, falls die Preisliste nicht von Acronis zur Verfügung gestellt wird) sowie dem Partner-Level (Verpflichtungsgrad) definieren.
- Die Preise von Acronis Produkten für Kunden auf der Grundlage Ihrer Kosten und eines bestimmten Margenprozentsatzes definieren.

Die Kosten und Preise von Acronis Produkten definieren

1. Gehen Sie zu **Verkauf und Abrechnung –> Produkte**.
2. Klicken Sie in der Registerkarte **Produkte** auf **Acronis Produktpreise aktualisieren**. Daraufhin wird der nachfolgende Dialog angezeigt.



3. Definieren Sie im Abschnitt **Kosten für Acronis Produkte festlegen** Folgendes:
   - Wählen Sie im Listenfeld **Unterstützte Währung auswählen** diejenige Währung aus, die für die Acronis Produkte gelten soll.

     Beachten Sie, dass Ihre in Advanced Automation festgelegte Standardwährung hier automatisch angewendet wird. Dieses Feld ist außerdem schreibgeschützt, wenn Ihre Standardwährung eine der unterstützten Währungen ist (USD, EUR, GBP, AUD, JPY, CAD, wie im obigen Beispiel gezeigt).
   - Bestimmen Sie im Listenfeld **Wählen Sie Ihren Verpflichtungsgrad** den entsprechenden Verpflichtungsgrad.

- Legen Sie im Feld **Umrechnungskurs definieren** den Umrechnungskurs für die Acronis Produkte fest. Der Standardwert ist 1,0000.

  Beachten Sie, dass dieses Feld zwingend erforderlich ist, wenn Ihre Standardwährung keiner der sechs unterstützten Währungen entspricht (siehe oben).

4. Wählen Sie im Abschnitt **Endkundenpreise für Acronis Produkte festlegen** eine der folgenden Möglichkeiten:
   - **Eine Marge in % für alle Acronis Produkte festlegen**. Wählen Sie diese Option aus, wenn Sie die entsprechende Gewinnspanne für alle Acronis Produkte festlegen wollen. Die Preise werden nach folgender Formel festgelegt:

     Preis = Kosten * 100 / (100 - Margenwert)

     Bei einer Marge von 20% auf ein Produkt von 100 € wird der Preis beispielsweise auf 125 € festgesetzt. Dabei entsprechen die 25 € einer Marge von 20% in Bezug auf die 125 €.
   - **Kundenpreise später manuell festlegen**. Wählen Sie diese Option, wenn Sie die Preise der Acronis Produkte nicht automatisch aktualisieren, sondern zu einem späteren Zeitpunkt manuell festlegen wollen.
5. Klicken Sie auf **Update**.

   Advanced Automation wendet die festgelegten Kosten und Preise automatisch auf die Acronis Produkte an, die Sie an Ihre Kunden verkaufen.

Produktkategorien

Mit dem Advanced Automation Service können Sie bei Bedarf neue Kategorien hinzufügen.

Wenn Sie Ihren Tickets Kategorien zuweisen, können Sie sich einen guten Überblick über die häufigsten Probleme verschaffen, von denen die jeweiligen Kunden betroffen sind. Wenn beispielsweise bei einem Kunden 50% der Tickets als *Workstation/Virus* kategorisiert werden, könnten Sie etwa neue Sicherheitsmaßnahmen einführen und die betreffenden Mitarbeiter besser schulen.

Durch die Kategorisierung Ihrer Produkte können Sie außerdem mehrere Produkte zu einer Gruppe zusammenfassen. Wenn Sie Hunderte von Produkten gelistet haben, können Sie diese durch das Erstellen einer Kategorie leichter finden.

Produktkategorien hinzufügen

Sie können bei Bedarf neue Produktkategorien hinzufügen.

Sobald Sie eine Kategorie erstellt haben, können Sie diese (wie unten beschrieben) aktivieren oder deaktivieren und nach Ihren Anforderungen bearbeiten (siehe '"Produktkategorien bearbeiten" (S. 247)').

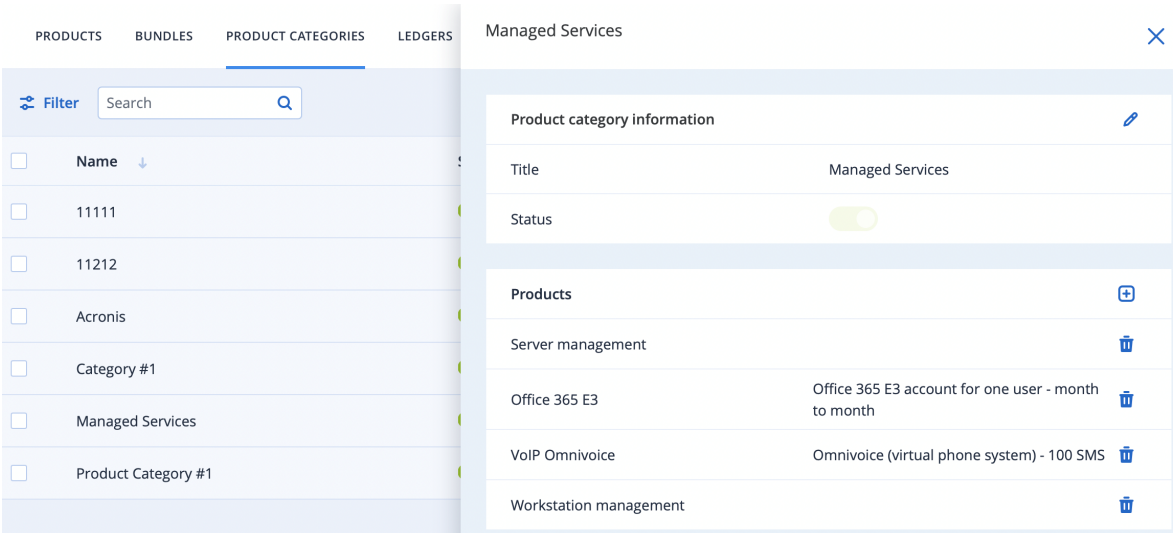
Hinweis
Diese Option ist nur für Benutzer verfügbar, denen folgende Rollen zugewiesen wurden: Administrator, Direktor, Finanzdirektor, Finanzen

Eine neue Produktkategorie hinzufügen

1. Gehen Sie zu **Verkauf und Abrechnung –> Produkte**.
2. Klicken Sie in der erscheinenden Anzeige auf die Registerkarte **Produktkategorien**.
3. Wenn es noch keine Kategorien gibt, klicken Sie auf **Neu erstellen**. Klicken Sie ansonsten auf **+ Neu**.
4. Geben Sie im Feld **Produktkategoriename** eine Bezeichnung für die Kategorie ein.
5. Klicken Sie in das Feld **Produkte auswählen**, um das relevante Produkt auszuwählen. Klicken Sie anschließend auf **Hinzufügen**.
6. Wenn Sie der Kategorie weitere Produkte hinzufügen wollen, müssen Sie auf **Produkt hinzufügen** klicken und dann das relevante Produkt auswählen. Wiederholen Sie dies nach Bedarf.
7. Klicken Sie auf **Fertig**. Die neue Kategorie wird auf der Registerkarte **Produktkategorien** angezeigt und ist standardmäßig als **Aktiv** festgelegt.

Eine Produktkategorie aktivieren oder deaktivieren

1. Gehen Sie zu **Verkauf und Abrechnung –> Produkte**. Auf der angezeigten Registerkarte **Produkte** werden die vorhandenen Kategorien aufgelistet.
2. Wenn Sie eine Kategorie aktivieren wollen, klicken Sie zuerst auf die entsprechende inaktive Kategorie und dann im rechten Fensterbereich auf das Stiftsymbol. Aktivieren Sie dann den Umschalter **Status**. Klicken Sie, wenn Sie fertig sind, auf ✓.



3. Wenn Sie eine Kategorie deaktivieren wollen, klicken Sie zuerst auf die entsprechende inaktive Kategorie und dann im rechten Fensterbereich auf das Stiftsymbol. Deaktivieren Sie dann den Umschalter **Status**. Klicken Sie, wenn Sie fertig sind, auf ✓.

Hinweis
Sie können den Kategoriestatus auch aktivieren oder deaktivieren, wenn Sie die Kategorie bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Produktkategorien bearbeiten" (S. 247)'.

Produktkategorien bearbeiten

So können Sie eine Produktkategorie bearbeiten

1. Gehen Sie zu **Verkauf und Abrechnung –> Produkte**. Auf der angezeigten Registerkarte **Produkte** werden die vorhandenen Kategorien aufgelistet.
2. Wenn Sie eine Kategorie bearbeiten wollen, klicken Sie zuerst auf die entsprechende Kategorie und dann im rechten Fensterbereich auf das Stiftsymbol.
3. Nehmen Sie die erforderlichen Änderungen vor. So können Sie beispielsweise Produkte entfernen und hinzufügen oder den Kategoriestatus auf **Aktiv**/**Inaktiv** ändern.
4. Klicken Sie, wenn Sie fertig sind, auf ✓.

Produkt-Bundles verwalten

Mit Produkt-Bundles können Sie mehrere Produkte und Services zu einem einzigen Paket zusammenfassen.

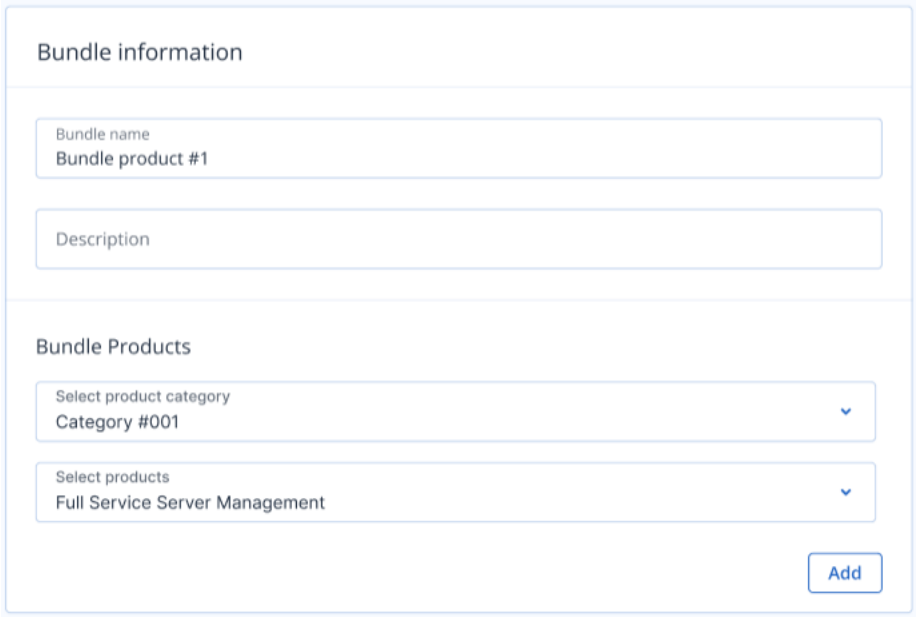
Beachten Sie, dass Produkt-Bundles derzeit nur solche Produkte unterstützen, die als Vertragsprodukte gekennzeichnet sind.

Ein Produkt-Bundle erstellen

So können Sie ein Produkt-Bundle erstellen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf** und klicken Sie dann auf die Registerkarte **Bundles**.
2. Wenn Sie Ihr erstes Bundle erstellen, klicken Sie auf **Neu erstellen**. Wenn Sie bereits Bundles haben, klicken Sie in der rechten oberen Ecke auf **Neu**.
3. Gehen Sie in dem angezeigten Dialogfeld folgendermaßen vor:
   a. Geben Sie den Namen des Bundles ein.
   b. Geben Sie eine Beschreibung für das Bundle ein.
   c. Wählen Sie eine Produktkategorie.
   d. Wählen Sie ein Produkt aus. Beachten Sie, dass nur Vertragsprodukte in Bundles ausgewählt werden können.

e. Klicken Sie auf **Hinzufügen**, um das Produkt dem Bundle hinzuzufügen.



f. Wenn Sie dem Bundle ein weiteres Produkt hinzufügen wollen, klicken Sie auf **Produkt hinzufügen**. Wählen Sie dann die gewünschte Produktkategorie und das Produkt aus – und klicken Sie anschließend auf **Hinzufügen**. Wiederholen Sie dies nach Bedarf.

4. Wenn Sie dem Bundle alle gewünschten Produkte hinzugefügt haben, klicken Sie auf **Fertig**.

   Das Bundle kann jetzt verwendet werden, wenn Sie einen Vertrag hinzufügen oder aktualisieren. Weitere Informationen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.

Produkt-Bundles bearbeiten

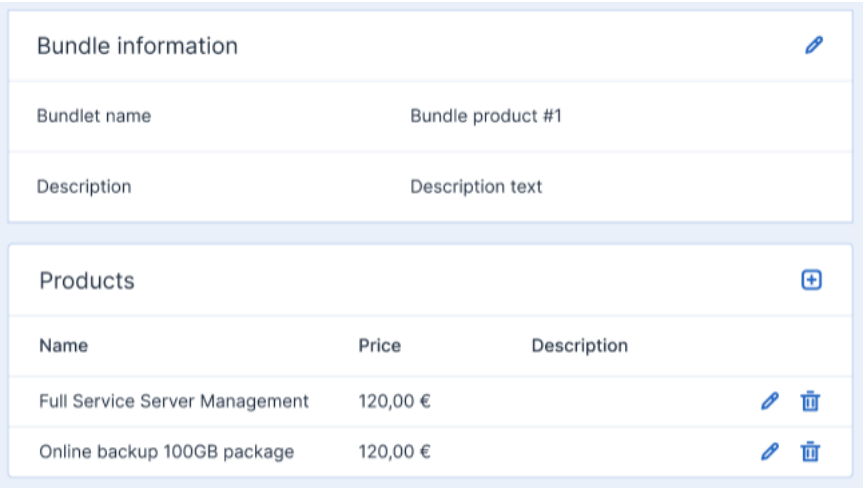
Sie können Produkt-Bundles nach Bedarf bearbeiten und löschen.

So können Sie Produkt-Bundles bearbeiten

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Verkauf**.
2. Klicken Sie auf die Registerkarte **Bundles**, um sich die vorhandenen Produkt Bundles anzeigen zu lassen.

   Wenn keine Bundles angezeigt werden, können Sie auf **Neu erstellen** klicken, um ein Bundle zu erstellen. Weitere Informationen finden Sie im Abschnitt '"Ein Produkt-Bundle erstellen" (S. 247)'.

3. Klicken Sie auf die relevante Bundle-Zeile und anschließend im rechten Fensterbereich auf das Stiftsymbol.



4. Ändern Sie im Bereich **Bundle-Informationen** den Namen und die Beschreibung des Bundles nach Ihren Vorstellungen.
5. Im Bereich **Produkte**:
   - Klicken Sie auf ⊕, um ein neues Produkt hinzuzufügen. Wählen Sie dann die gewünschte Produktkategorie und das Produkt aus – und klicken Sie anschließend auf **Hinzufügen**. Wiederholen Sie dies nach Bedarf.
   - Klicken Sie auf das Stiftsymbol, um das Produkt zu bearbeiten. So können Sie beispielsweise ein vorhandenes Produkt durch ein anderes Produkt aus derselben Kategorie ersetzen. Klicken Sie auf **Speichern**, wenn Sie fertig sind.
   - Klicken Sie auf das Papierkorb-Symbol, um ein Produkt aus dem Bundle zu löschen.
6. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie ein Produkt-Bundle löschen

1. Klicken Sie auf die relevante Bundle-Zeile und anschließend in der ganz rechts liegenden Spalte auf das Drei-Punkte-Symbol (...).
2. Wählen Sie **Löschen**. Das Bundle wird gelöscht.

> **Hinweis**
> Auch wenn ein Bundle einem laufenden Vertrag zugeordnet wurde, kann es gelöscht werden. Denn das Bundle ist im Prinzip nichts anderes als eine Zusammenfassung mehrerer Einzelprodukte zu einem Vertrag. Dem Vertrag wird dann ein Vertragsteil hinzugefügt – und zwar ein Vertragsteil für jedes Produkt. Nachdem der Vertrag erstellt wurde, kann das Bundle gelöscht werden.

Hauptbücher verwalten

Im Bereich Hauptbücher können Sie die Hauptbuch-Nummern verwalten, die Sie derzeit in Ihrem Buchhaltungssystem verwenden. Diese Hauptbücher (Englisch: Ledgers) können dann mit den Produkten verbunden werden, die Sie an Ihre Kunden verkaufen.

Wenn Sie z.B. einen CSV- oder XML-Export Ihres Fakturierungslaufs erstellen, wird der Export alle Transaktionen einschließlich der korrekten Hauptbuch-Nummer enthalten. Dies ermöglicht wiederum schnelle und einfache Importe.

Wenn Sie auf die Hauptbücher zugreifen wollen, gehen Sie zu **Verkauf und Abrechnung –> Produkte** und klicken Sie dann auf die Registerkarte **Hauptbücher**.

Ein Hauptbuch erstellen

So können Sie ein Hauptbuch erstellen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Produkte** und klicken Sie dann auf die Registerkarte **Hauptbücher**.
2. Klicken Sie auf **+ Neu**.
3. Definieren Sie in der Anzeige 'Hauptbuch-Informationen' Folgendes:
   - Definieren Sie die Hauptbuch-Nummer.
   - (Optional) Geben Sie die externe ID des Hauptbuchs ein.
   - (Optional) Geben Sie eine Beschreibung für das Hauptbuch ein.
   - Aktivieren Sie das Kontrollkästchen **Aktiv**, wenn Sie das Hauptbuch sofort verwenden wollen.
4. Klicken Sie auf **Fertig**.

Ein Hauptbuch bearbeiten

Hinweis
Hauptbücher können nach Bedarf bearbeitet, aber nicht gelöscht werden.

So können Sie Hauptbuch bearbeiten

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Produkte** und klicken Sie dann auf die Registerkarte **Hauptbücher**.
2. Klicken Sie auf die Zeile des Hauptbuchs, das Sie bearbeiten wollen.
3. Klicken Sie im angezeigten rechten Fensterbereich auf das Stiftsymbol und führen Sie die gewünschte Bearbeitung durch.
4. Wenn Sie ein aktives Hauptbuch deaktivieren wollen, müssen Sie den Umschalter **Status** deaktivieren.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

Advanced Automation-Einstellungen konfigurieren

Im Modul **Einstellungen** können Sie verschiedene Optionen für Ihr Advanced Automation-Konto konfigurieren.

Diese Einstellungen sollten vor der Arbeit mit dem Service definiert werden, da sie eine Reihe von Kerneinstellungen enthalten, die Sie für die Arbeit mit Ihrer Rechnungsstellung und Ihrem Service Desk benötigen. Dieser Bereich enthält Einstellungen für:

- Service Desk
- Abrechnung und Angebotserstellung

Service Desk-Einstellungen

Mit den Service Desk-Einstellungen können Sie alle wichtigen Bereiche Ihres Service Desks einrichten.

Es ist wichtig, dass dies korrekt durchgeführt wird, damit Ihre Tickets richtig funktionieren.

Wenn Sie auf die Service Desk-Einstellungen zugreifen wollen, gehen Sie zu **Einstellungen –> Service Desk**.

Hinweis
Sie können in den Service Desk-Einstellungen außerdem Benutzergruppen für Ihre Advanced Automation-Benutzer definieren. Dies wird in '"Benutzergruppen verwalten" (S. 189)' im Abschnitt 'Ihre Benutzer verwalten' beschrieben.

Vorgefertigte Antworten konfigurieren

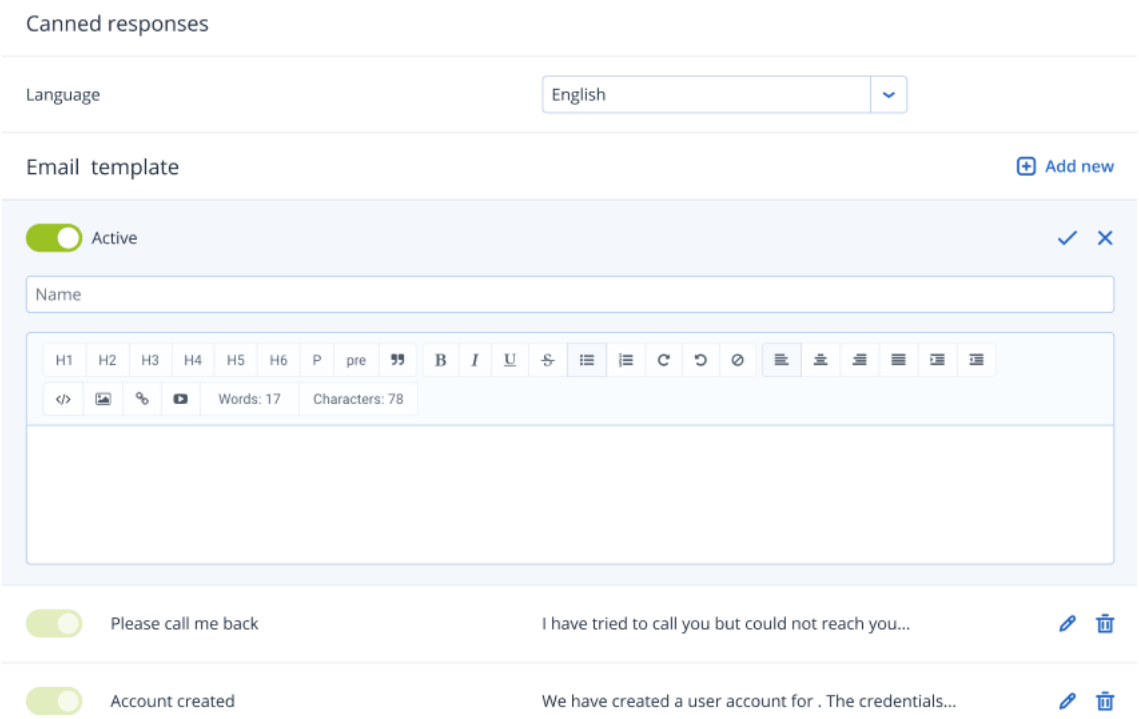
Mit vorgefertigten Antworten können Sie Kommentarvorlagen als Teil Ihrer Standardkommentare hinzufügen, wenn Sie ein neues Ticket erstellen. Diese Kommentare werden in die Beschreibung des Tickets aufgenommen.

Eine vorgefertigte Antwort erstellen

Sie können Ihrem Service Desk eine beliebige Anzahl von vorgefertigten Antworten hinzufügen.

So können Sie eine neue vorgefertigte Antwort erstellen

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Vorgefertigte Antworten**.
3. Klicken Sie auf das Symbol für **Neu hinzufügen**.
4. Definieren Sie im angezeigten Dialogfeld einen Namen für die vorgefertigte Antwort und fügen Sie den entsprechenden Inhalt hinzu.



Sie können dafür folgende Variablen verwenden:
[SUPERIOR] - Der Name des Managers des Benutzers
[ENDUSER] - Der Name des Benutzers
[SUPPORTUSER] - Der Name der Person, die das Ticket aktualisiert
[STATUS] - Der Status des Tickets
[TITLE] - Der Titel des Tickets

5. Standardmäßig ist die vorgefertigte Antwort auf **Aktiv** gesetzt. Wenn Sie die vorgefertigte Antwort deaktivieren wollen, klicken Sie auf den Optionsschalter **Aktiv**.
6. Klicken Sie auf ✓, um die vorgefertigte Antwort zu speichern. Nach dem Speichern kann die vorgefertigte Antwort als Inhalt im Feld **Kommentare**.

Eine vorgefertigte Antwort bearbeiten oder löschen

Sie können vorgefertigte Antworten nach Bedarf bearbeiten und löschen.

So können Sie eine vorgefertigte Antwort bearbeiten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Vorgefertigte Antworten**.
3. Klicken Sie auf das Stiftsymbol für die vorgefertigte Antwort, die Sie bearbeiten wollen, und führen Sie dann die gewünschten Änderungen durch. Weitere Informationen über die verfügbaren Optionen finden Sie im Abschnitt '"Eine vorgefertigte Antwort erstellen" (S. 251)'.
4. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.

So können Sie eine vorgefertigte Antwort löschen

1. Klicken Sie auf der Registerkarte **Vorgefertigte Antworten** auf das Papierkorbsymbol für die vorgefertigte Antwort, die Sie löschen wollen.
2. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Ja**.

Prioritäten einrichten

Sie können die Prioritäten für Ihre Tickets definieren. Diese Prioritäten werden bei der Verarbeitung eines Tickets verwendet. Denn diese hängt von der Priorität ab, die Sie für jedes Ticket einzeln festlegen. So wird beispielsweise ein Ticket mit der Priorität *dringend* generell vor einem Ticket mit einer normalen Priorität verarbeitet.

Eine Priorität hinzufügen

So können Sie eine neue Priorität hinzufügen

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Prioritäten**.
3. Klicken Sie auf **Neu hinzufügen**.
4. Geben Sie den Namen der Priorität ein und klicken Sie dann auf ✓. Beachten Sie, dass der Name nicht die Prioritätsstufe widerspiegelt, sondern selbstbeschreibend sein sollte.
   Die Priorität ist standardmäßig als aktiv festgelegt.
   Wenn Sie die neue Priorität erfolgreich hinzugefügt haben, kann diese im Feld **Priorität** Ihrer Tickets verwendet werden (siehe Abschnitt '"Ein neues Ticket erstellen" (S. 197)'). Bei Bedarf können Sie Standardprioritäten für Tickets und Standardprioritäten für Tickets von bestimmten Kunden festlegen.

Eine Priorität bearbeiten oder löschen

Sie können Prioritäten nach Bedarf bearbeiten und löschen.

So können Sie eine Priorität bearbeiten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Prioritäten**.
3. Klicken Sie auf das Stiftsymbol für die Priorität, die Sie bearbeiten wollen, und führen Sie dann die gewünschten Änderungen durch.
4. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.
   Beachten Sie, dass Sie eine Priorität auch deaktivieren können, indem Sie den Optionsschalter neben der entsprechenden aktiven Priorität ausschalten.

So können Sie eine Priorität löschen

1. Klicken Sie auf der Registerkarte **Prioritäten** auf das Papierkorbsymbol für die Priorität, die Sie löschen wollen.
2. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Ja**.

Hinweis
Die Priorität kann nur gelöscht werden, wenn sie derzeit deaktiviert ist und in keinem Ticket verwendet wurde.

Ihre SLA-Richtlinien verwalten

Eine SLA-Richtlinie (Service Level Agreement, Service-Qualitätsvereinbarung) ist eine offizielle Vereinbarung zwischen Ihnen und dem Kunden. Die SLA regelt, welche(n) Service(s) Sie einem Kunden anbieten und zu welcher Qualität bzw. Verfügbarkeit Sie sich dabei verpflichten.

Mit Advanced Automation können Sie SLAs verwalten, was Ihnen wiederum hilft, den Fluss der Support-Tickets zu organisieren und die Kalkulation der abrechenbaren Zeit zu automatisieren. Neben dem kundenbezogenen Aspekt können Sie damit auch sicherstellen, dass die Techniker die Tickets im Auge behalten und Tickets nicht monatelang unbearbeitet bleiben.

Sie können SLAs konfigurieren und definieren, die für Kundenverträge, Ticket-Aktivitäten und die Compliance-Nachverfolgung verwendet werden.

Eine neue SLA erstellen

So können Sie eine neue SLA erstellen

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **SLA** und dann auf **Neu hinzufügen**.
3. Geben Sie auf der erscheinenden Anzeige den Namen Ihrer neuen SLA ein.
4. Definieren Sie den geltenden Zeitraum Ihres SLA, indem Sie die erste Antwortzeit (in Stunden) und das Feedback-Intervall (in Stunden) sowie den Start- und Endzeitpunkt eingeben.
5. Aktivieren Sie das Kontrollkästchen **SLA anwenden während –> Wochenenden**, um zu aktivieren oder deaktivieren (Standardeinstellung), ob diese SLA auch an Wochenenden gelten soll.
6. Aktivieren Sie das Kontrollkästchen **SLA anwenden während –> Feiertage**, um zu aktivieren oder deaktivieren (Standardeinstellung), ob diese SLA auch an Feiertagen gelten soll.
7. Bestimmen Sie die Art der Abrechnung für Ihre SLA, indem Sie **Festpreis** oder **Nachträgliche Berechnung** auswählen.
8. Wählen Sie aus den entsprechenden Listenfeldern ein Standardprodukt für die Abrechnung und einen Abrechnungssatz für spezielle Aktivitäten aus.
   - **Standardprodukt für die Abrechnung**: Dieser optionale Parameter gibt ein abrechenbares Produkt vom Ticket-Typ für Ticket-Aktualisierungen an, die innerhalb der SLA-Stunden erfolgen. Wenn ein Techniker beispielsweise an einem Ticket arbeitet und ein SLA festgelegt wurde, wird das **Standardprodukt für die Abrechnung** als abrechenbares Produkt für die Ticket-Arbeit vorausgewählt. Das Produkt wird automatisch in den Genehmigungsprozess für die Ticket-Zeiten einbezogen, sodass einem Kunden die entsprechenden Stunden automatisch in Rechnung gestellt werden können.

- **Abrechnungssatz für spezielle Aktivitäten**: Dieser optionale Parameter entspricht dem für das **Standardprodukt für die Abrechnung**, gilt jedoch für Ticket-Aktualisierungen außerhalb der üblichen SLA-Zeiten.

9. Wenn Sie dieses SLA als Standard festlegen wollen, müssen Sie das Kontrollkästchen **Als Standard-Service-Level-Vereinbarung zuweisen** aktivieren.
10. Klicken Sie auf ✓, um die SLA zu speichern.

    Die SLA ist standardmäßig als **Aktiv** festgelegt. Wenn Sie diese deaktivieren wollen, müssen Sie auf den Optionsschalter **Aktiv** umschalten.

    Wenn Sie die neue SLA erfolgreich erstellt haben, kann diese im Feld **SLA** von IhrenTickets verwendet werden. Weitere Informationen finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

Eine SLA bearbeiten

So können Sie eine SLA bearbeiten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie zuerst auf die Registerkarte **SLA** und anschließend auf das Stiftsymbol für die relevante SLA.
3. Nehmen Sie die gewünschten Änderungen an der SLA vor. Weitere Informationen dazu finden Sie im Abschnitt '"Eine neue SLA erstellen" (S. 254)'.
4. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.

Hinweis
Wenn die SLA bereits von Kunden (in Tickets) verwendet wurde, können Sie die SLA nicht deaktivieren.

Kategorien und Unterkategorien definieren

Sie können eine beliebige Anzahl von Ticket-Kategorien definieren, die im Service Desk von Advanced Automation verwendet werden können.

Advanced Automation ist mit einer Reihe von Kategorien und Unterkategorien ausgestattet. Wenn Sie diese auf Ihre Tickets anwenden, verschaffen Ihnen die Kategorien und Unterkategorien einen guten Überblick über die Probleme, die am meisten Zeit in Anspruch nehmen, sodass Sie entsprechend reagieren können. Sie können diese Einblicke auch auf der Basis einzelner Kunden sehen.

Dies kann Ihnen wiederum helfen, Ihre Services zu verbessern. Wenn beispielsweise bei einem Kunden 50% der Tickets als *Workstation/Virus* eingestuft sind, könnten Sie sich überlegen, die Sicherheitsmaßnahmen und Mitarbeiterschulungen zu verbessern.

Eine Kategorie oder Unterkategorie erstellen

So können Sie eine neue Kategorie oder Unterkategorie definieren

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Kategorien und Unterkategorien**.
3. Klicken Sie auf **Neu hinzufügen** und geben Sie dann den Namen für die Kategorie ein. Wenn Sie die Kategorie zu einer Unterkategorie machen wollen, wählen Sie die entsprechende übergeordnete Kategorie aus. Die Kategorie oder Unterkategorie wird erstellt und kann (wie unten beschrieben) je nach Bedarf aktiviert oder deaktiviert werden.

So können Sie eine Kategorie oder Unterkategorie aktivieren/deaktivieren

Klicken Sie auf der Registerkarte **Kategorien und Unterkategorien** auf den aktiven Schalter, um die relevante Kategorie oder Unterkategorie zu aktivieren/deaktivieren.

Eine Kategorie oder Unterkategorie bearbeiten oder löschen

So können Sie eine Kategorie oder Unterkategorie bearbeiten

1. Klicken Sie auf der Registerkarte **Kategorien und Unterkategorien** auf das Stiftsymbol für die relevante Kategorie oder Unterkategorie.
2. Führen Sie die gewünschte Bearbeitung durch.

So können Sie eine Kategorie oder Unterkategorie löschen

1. Klicken Sie auf der Registerkarte **Kategorien und Unterkategorien** auf das Papierkorbsymbol für die relevante Kategorie oder Unterkategorie.
2. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Ja**.

Hinweis
Die Kategorie oder Unterkategorie kann nur gelöscht werden, wenn sie derzeit deaktiviert ist und in keinem Ticket verwendet wurde.

Standardwerte festlegen

Sie können Standardwerte für viele Advanced Automation-Funktionen definieren.

Beachten Sie, dass Sie bei jedem Kunden die allgemeinen Standardeinstellungen mit kundenspezifischen Werten überschreiben können.

So können Sie Standardwerte definieren

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Standardwerte**. Die Liste der Standardwerte wird angezeigt:
   - **Standard-SLA**: Die Standard-SLA, die auf Tickets angewendet wird. Standardmäßig ist die **Standard-SLA** ausgewählt.
   - **Kategorie**: Die Standard-Ticket-Kategorie. Standardmäßig ist **Hardware-Problem** ausgewählt.
   - **Standardpriorität**: Die Standardpriorität für Tickets. Standardmäßig ist **Normal** ausgewählt.

- **Standardgruppe**: Die Standardgruppe für Tickets. Standardmäßig ist **Support-Gruppe** ausgewählt.
- **Standard-Supportbenutzer**: Der Standard-Supportbenutzer für Tickets. Standardmäßig ist der Partner-**Admin** ausgewählt, sodass er für jeden Partner eindeutig ist.
- **Freie Tage pro Jahr**: Die standardmäßigen freien Tage pro Jahr für Benutzer. Der Standardwert ist **15**.
- **Standard-Rechnungssteller**: Der Standard-Rechnungssteller, der für Rechnungen verwendet wird. Standardmäßig ist **Standard** ausgewählt.
- **Kundendokumentation**: Ein Link zu kundenbezogener Dokumentation. Dieses Feld ist standardmäßig leer.
- **Benachrichtigungsgrenzwert für die Auslastung**: Der Benachrichtigungsgrenzwert liegt dort, wo die von Ihnen oder einer Gruppe, deren Mitglied oder Leiter Sie sind, erfasste Arbeitszeit unter den für diesen Tag festgelegten Stunden liegt. Es wird eine Erinnerung gesendet, damit die Stundenerfassung abgeschlossen wird. Standardmäßig ist **85** ausgewählt.
- **Ticket-Timer beim Verlassen des Bildschirms automatisch pausieren**: Sie können den Ticket-Timer automatisch pausieren lassen, wenn die Benutzer von ihrer aktiven Anzeige zu einer anderen wechseln. Standardmäßig ist **Nein** ausgewählt.
- **Ticket-Aktualisierung zwingend erforderlich**: Definieren Sie, ob das Feld **Ticket-Beschreibung** in den Ticket-Einstellungen zwingend erforderlich ist. Dies ermöglicht Ihnen, dass Sie Änderungen an einem Ticket während dessen Verarbeitung genauer nachverfolgen können. Standardmäßig ist **Nein** ausgewählt.
- **Link zur Ticket-Übermittlungsseite**: Die Seite, auf die nicht autorisierte Benutzer von außen zugreifen können, um ein Ticket direkt an Advanced Automation zu übermitteln. Standardmäßig ist ein vordefinierter System-Link ausgewählt.
- **Benutzerdefiniertes Feld 1** / **Benutzerdefiniertes Feld 2**: Sie können, je nach Ihren Anforderungen, bis zu zwei zusätzliche benutzerdefinierte Felder für die Ticket-Übermittlungsseite definieren. Sie können außerdem definieren, ob die Felder **Aktiv** und **Zwingend erforderlich** sein sollen.

3. Übernehmen Sie die von Ihnen gewünschten Standardwerte und klicken Sie anschließend auf **Speichern**.

Länder- und Spracheinstellungen definieren

Auf der Registerkarte **Ländereinstellungen** können Sie globale Firmeneinstellungen für die Arbeit mit Advanced Automation festlegen, wozu auch Ihr Standardland und Ihre Zeitzone gehören. Diese globalen Einstellungen wirken sich auf die Währung und das Stundenformat aus. Sie sind besonders wichtig für Stunden, die Teil einer Service Level-Vereinbarung (SLA) sind.

So können Sie die Länder- und Spracheinstellungen definieren

1. Gehen Sie zu **Einstellungen** –> **Service Desk** und klicken Sie dann auf die Registerkarte **Ländereinstellungen**.
2. Klicken Sie im Bereich **Ländereinstellungen** auf das Stiftsymbol, um eine der folgenden Einstellungen zu bearbeiten:

- **Standardland**: Wählen Sie das gewünschte Land aus. Das ausgewählte Land definiert die Standardwährung, die für alle Preise und Kosten in Advanced Automation verwendet wird.
- **Zeitzone**: Wählen Sie die gewünschte Zeitzone aus. Die Zeitzone beeinflusst die SLA-Zeiten, indem sie bestimmt, ob Tickets innerhalb oder außerhalb der SLA-Stunden empfangen werden. Sie kann sich auch auf den Preis für Ticket-basierte Arbeiten auswirken.
- **Sommerzeit**: Klicken Sie auf den Umschalter, um die Sommerzeit-Einstellung zu aktivieren.

3. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.
4. Klicken Sie im Bereich **Sprachen** auf das Stiftsymbol, um die Standard-Systemsprache festzulegen, die in Advanced Automation verwendet wird.
5. Klicken Sie auf den Umschalter, um die gewünschte Sprache zu aktivieren.
6. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.

Statuszustände aktivieren und deaktivieren

Die Registerkarte **Statuszustände** zeigt die verschiedenen Statuszustände, die für Service Desk-, Angebots- und Projekt-Tickets verfügbar sind. Sie können die Statuszustände für Tickets aktivieren oder deaktivieren.

Hinweis
Sie können einen Status weder hinzufügen oder löschen noch den Namen des Status löschen oder ändern. Bei einigen Integrationen werden Statuszustände mit Ticket-Statuszuständen verknüpft.

So können Sie Statuszustände aktivieren oder deaktivieren

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie zuerst auf die Registerkarte **Statuszustände** und anschließend auf den Befehl **Bearbeiten**.
3. Klicken Sie in der angezeigten Liste der Statuszustände auf den Ein-/Ausschalter für die relevanten Statuszustände.
   Beachten Sie: Wenn ein Status ausgegraut ist, bedeutet dies, dass der Status in Advanced Automation vordefiniert ist und nicht geändert werden kann.
4. Klicken Sie auf **Speichern**.

Die Standardeinstellungen für die RMM-Ticket-Integration definieren

Wenn Sie eine Integration mit Remote Monitoring- und Management-Systemen (RMM) einrichten, können Sie die Felder **Standard-SLA**, **Kategorie** und **Priorität** für Tickets festlegen, die von Ihrer RMM-Lösung generiert werden. Wenn ein Ticket RMM-integriert ist, werden automatisch bestimmte Standardwerte angewendet, abhängig von den Werten, die Sie in der nachfolgenden Prozedur definieren.

So können Sie die Standardeinstellungen für die RMM-Ticket-Integration definieren

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **RMM-Ticket-Integration** und dann auf **Bearbeiten**.
3. Bestimmen Sie die Werte für **Standard-SLA**, **Kategorie** und **Priorität** und klicken Sie dann auf **Speichern**.

E-Mail-Vorlagen verwalten

Auf der Registerkarte **E-Mail-Vorlagen** können Sie alle vordefinierten E-Mail-Vorlagen in Advanced Automation einsehen. Diese Vorlagen werden zur externen Kommunikation mit den Endbenutzern verwendet. Sie können die Vorlagen anpassen, indem Sie entweder den Rich-Text-Editor verwenden oder Ihren eigenen HTML-Code in den Editor einfügen.

Sie können keine der E-Mail-Vorlagen hinzufügen oder löschen.

Hinweis
Die Standard-E-Mail-Vorlagen sind darauf ausgelegt, dass sie in den meisten E-Mail-Clients auf Desktops und Mobiltelefonen korrekt angezeigt werden. Achten Sie bei Änderungen darauf, dass die korrekte Anzeige bestehen bleibt.

Eine E-Mail-Vorlage bearbeiten

So können Sie eine E-Mail-Vorlage bearbeiten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **E-Mail-Vorlagen**.
3. Klicken Sie auf das Stiftsymbol für die Vorlage, die Sie bearbeiten wollen.
4. Aktualisieren Sie die Vorlage nach Bedarf.
   Sie können für die verschiedenen Nachrichtentypen folgende Variablen verwenden:

Ticket aus E-Mail hinzufügen		**Ticket aus E-Mail aktualisieren**		**Ticket aus Applikation hinzufügen**		**Ticket aus Applikation aktualisieren**	
Betreff	**Body**	**Betreff**	**Body**	**Betreff**	**Body**	**Betreff**	**Body**
[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]
					[SUPPORTUSE		[SUPPORTUSE

					R]		R]

5. Wenn Sie die Hintergrundfarbe der E-Mail anpassen wollen, fügen Sie ein entsprechendes Style-Code-Snippet in den HTML-Code Ihrer Vorlage ein. Ansonsten wird beim Erstellen der E-Mail-Nachricht der Standardstil verwendet.

   Ein Beispiel für einen Style-Code für einen Absatz mit weißem Hintergrund:

    [INHALT IHRER E-MAIL-VORLAGE]
6. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.

Hinweis

Wenn Sie mehrere Änderungen an einer E-Mail-Vorlage vornehmen und dann die Vorlage auf ihr Standardlayout und den Standardtext zurücksetzen wollen, müssen Sie den HTML-Code für diese Vorlage erneut anwenden. Weitere Informationen finden Sie im Abschnitt '"Standardeinstellungen für E-Mail-Vorlagen" (S. 260)'

Standardeinstellungen für E-Mail-Vorlagen

Advanced Automation enthält bereits eine Reihe von anpassbaren Standard-E-Mail-Vorlagen. Wenn Sie eine Vorlage wieder auf ihre Standardeinstellungen zurücksetzen müssen, können Sie die HTML-Codes der Standardvorlagen verwenden, die unten angegeben sind.

- Geschlossenes gelöstes Ticket
- Angebot erstellt
- Neues Ticket aus E-Mail
- Ticket-Aktualisierung
- Anfrage zur Ticket-Bewertung
- Ticket-Bewertung wurde erhalten
- Angebot wurde verarbeitet
- Neues Ticket
- Neue Rechnung
- Zusammengeführtes Ticket

Geschlossenes gelöstes Ticket

Betreff: Geschlossenes gelöstes Ticket

Code:

```
<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">Solved ticket has been
closed</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;">Hallo [ENDUSER]!</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ihr Ticket mit der
Referenznummer [REF] wurde automatisch geschlossen, weil es sich seit mehr als [WAITINGDAYS]
Tagen im Status 'Gelöst' befindet.</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>
```

Angebot wurde erstellt

Betreff: Es wurde ein neues Angebot mit der Beschreibung [TITLE] für Sie erstellt

Code:

```
<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">A new quote was created
for you</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;">Hallo [CLIENT]!</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">In der Anlage finden Sie Ihr
neues Angebot mit Beschreibung [TITLE] und Nummer [number].</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Bitte verwenden Sie den
folgenden Link, um das Angebot zu überprüfen.</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">
  <a href="[QUOTE_LINK]">Neues Angebot</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>
```

Neues Ticket aus E-Mail

Betreff: Neues Ticket mit der Referenznummer: [REF]

Code:

```
<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">New ticket created from email</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;">Ein neues Ticket wurde per E-Mail mit der folgenden Referenznummer erstellt: [REF]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ticket Status: [STATUS]</td>
  </tr>
<tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ticket title: [TITLE]</td>
  </tr>
<tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Request: [UPDATE]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ein Support-Techniker wird sich so schnell wie möglich um Ihre Anfrage kümmern.</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-Aktualisierung

Betreff: Neue Aktualisierung für Ihr Ticket [TITLE] – Referenznummer – [REF]

Code:

```
<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-Update</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;"> Für Ihr Ticket mit der
Referenznummer : [REF] wurde eine neue Aktualisierung vorgenommen.</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ticket Status : [STATUS]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Nachricht des Support-
Technikers: [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>
```

Anfrage zur Ticket-Bewertung

Betreff: Anfrage zur Ticket-Bewertung

Code:

```
<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">We have closed your
ticket - Please let us know how we did</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;">Hello [CUSTOMER]!</td>
 </tr>
 <tr style="font-size: 14px;">
 <td style="font-size: 14px;vertical-align: top;">Your ticket with number [REF] has been closed. Please
find the details of the ticket here:<br>
 <br>
 </td>
 </tr>
```

```
<tr style="font-size: 14px;">
<td style="font-size: 14px;vertical-align: top;">
<div style="float: left;">Ticket reference number:</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;">Support engineer:</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;">Support engineer message:</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;">Initial problem:</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;">Ticket title:</div>
<div style="float: left;">[TITLE]<br>
<br>
</div>
</td>
</tr>
<tr style="font-size: 14px;">
<td style="font-size: 14px;vertical-align: top;">How likely is it that you would recommend our
company/product/service to a friend or colleague?</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>
```

Ticket-Bewertung wurde erhalten

Betreff: Der Kunde [Customer] hat das Ticket [REF] bewertet

Code:

```
<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">Ihr Ticket wurde
bewertet</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;">Hello [SUPPORTUSER]!</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ihr Ticket mit der Nummer
[REF] wurde bewertet:</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;"> Ticket reference number:
[REF]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;"> Note: [GRADE]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;"> Endbenutzer: [CLIENT]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;"> Kunde: [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>
```

Angebot wurde verarbeitet

Betreff: Das Angebot [DESCRIPTION] - [NUMBER] wurde [ACCEPTED]

Code:

```
<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">A quote was
processed</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;">Hallo [CLIENT]!</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Bitte beachten Sie, dass das
Angebot [DESCRIPTION] - [NUMBER] von [USER] [ACCEPTED] wurde.</td>
  </tr>
```

<tr style="font-size: 14px;">
<td class="content-block" style="font-size: 14px;vertical-align: top;">

</td>
</tr>
</tbody>
</table>
</td>
</tr>
</tbody>
</table>

</td>
<td style="font-size: 14px;vertical-align: top;"></td>
</tr>
</tbody>
</table>

Neues Ticket

Betreff: Neues Ticket wurde erstellt: [TITLE] – Referenznummer [REF] – Support-Techniker/Geschäftseinheit [SUPPORTUSER]

Code:

<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;">

<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">New ticket has been created</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;">Es wurde ein neues Ticket mit
folgender Referenznummer für Sie erstellt: [REF]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ticket-Status: [STATUS]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Ticket-Titel: [TITLE]</td>
  </tr>
<tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Anfrage: [UPDATE]</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Support-
Techniker/Geschäftseinheit: [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>
```

Neue Rechnung

Betreff: Die Rechnungsnummer [number] wurde ausgestellt

Code:

```
<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">Wir haben eine neue
Rechnung ausgestellt</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;">Hallo [CUSTOMER]!</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">In der Anlage können Sie die
Rechnung mit der Nummer [number] finden.</td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">Bitte verwenden Sie einen
dieser Links, um Ihre Zahlung abzuschließen: </td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">
  <a href="[PAYPAL_LINK]">Mit PayPal zahlen</a>
  </td>
  </tr>
  <tr style="font-size: 14px;">
  <td class="content-block" style="font-size: 14px;vertical-align: top;">
  <a href="[STRIPE_LINK]">Mit Stripe zahlen</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>
```

Zusammengeführtes Ticket

Betreff: Ihr Ticket [TITLE] – Referenznummer – [REF] wurde mit einem anderen Ticket zusammengeführt

Code:

```
<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 zusammengeführt</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;">Ihr Ticket mit der
Referenznummer [REF] </td>
</tr>
<tr style="font-size: 14px;">
<td class="content-block" style="font-size: 14px;vertical-align: top;">Wurde zur folgenden
Ticketnummer zusammengeführt:[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>
```

Vorlagen für E-Mail-Benachrichtigungen verwalten

Auf der Registerkarte **Vorlagen für E-Mail-Benachrichtigungen** können Sie den Text und das Layout von Benachrichtigungs-E-Mails verwalten, die von Advanced Automation versendet werden (beispielsweise, wenn ein Ticket aktualisiert wird). Diese Vorlagen werden zur Kommunikation mit Ihren Benutzern verwendet. Für die Kommunikation mit Endbenutzern sollten Sie die im Abschnitt '"E-Mail-Vorlagen verwalten" (S. 259)' beschriebenen E-Mail-Vorlagen verwenden.

Benutzer, die solche Nachrichten erhalten, können diese verwenden, um die Tickets zu aktualisieren, indem sie einfach auf die Nachricht antworten. Sobald das System die Antwort erhält, wird Advanced Automation das Ticket aktualisieren und den betreffenden Benutzer benachrichtigen.

So können Sie Vorlagen für E-Mail-Benachrichtigungsvorlagen für Tickets verwalten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Vorlagen für E-Mail-Benachrichtigungen**.
3. Klicken Sie auf das Stiftsymbol derjenigen Vorlage, die Sie bearbeiten wollen.
4. Führen Sie die gewünschte Bearbeitung durch.
5. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.

Aktivitäten für Zeiterfassungen definieren

Aktivitäten werden für Zeiterfassungen verwendet, die Ihnen wiederum helfen, Ihre Arbeitszeittabellen zu verstehen. Sie können zum Beispiel einsehen, wie viel Zeit bestimmte Angestellte für kundenbezogene bzw. nicht kundenbezogene Aktivitäten aufwenden. Oder wie viel Zeit sie für abrechenbare bzw. nicht abrechenbare Arbeit aufwenden.

In spezielleren Fällen können Sie für kundenbezogene abrechenbare Aktivitäten spezifische Raten anwenden, sodass diese automatisch bei einer Zeiterfassung angewendet werden. So kann beispielsweise für einen Kundenbesuch vor Ort automatisch eine spezielle, teurere Rate auf die Zeiterfassung angewendet werden.

In der Registerkarte **Aktivitäten** wird eine Liste der aktuellen Aktivitäten aufgeführt. Sie können die aufgelisteten Aktivitäten erweitern und bearbeiten sowie bei Bedarf eine Aktivität aktivieren oder deaktivieren (indem Sie auf den Umschalter **Status** klicken). Wenn Sie eine Aktivität deaktivieren, wird sie aus der Liste auf der Registerkarte **Aktivitäten** und aus der Zeiterfassung entfernt, zu der sie hinzugefügt wurde.

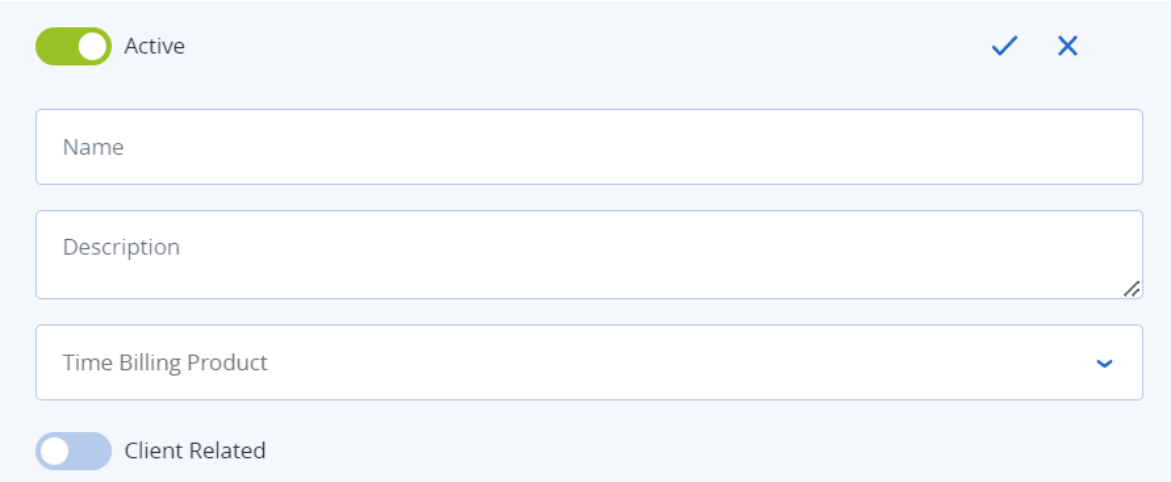
Beachten Sie, dass Advanced Automation standardmäßig mit folgenden vordefinierten Aktivitäten ausgeliefert wird:

- Buchhaltung
- Vertragsmanagement
- Mittagspause
- Projektierung
- Projektmanagement

Eine Aktivität erstellen

So können Sie eine Aktivität erstellen

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Aktivitäten** und dann auf **Neu hinzufügen**.
   Im oberen Bereich der Aktivitätenliste wird ein neuer Bereich angezeigt.



3. Gehen Sie folgendermaßen vor:
   - Klicken Sie auf den Umschalter **Aktiv**, um die Aktivität zu aktivieren (die standardmäßig vorausgewählt ist).
   - Geben Sie einen Namen für die Aktivität ein, der bis zu 50 Zeichen lang sein darf.
   - Geben Sie eine Beschreibung für die Aktivität ein. Diese wird in der Hauptliste der Aktivitäten auf der Registerkarte **Aktivitäten** angezeigt.
   - Wählen Sie das relevante Produkt aus dem Listenfeld **Zeitabrechnung-Produkt** aus. Wenn das ausgewählte Produkt in einem Vertrag oder einem Verkaufsartikel verwendet wird, wird der Fakturierungsprozess seinen Abrechnungssatz verwenden, wenn die Zeiterfassung (die die betreffende Aktivität beinhaltet) abgerechnet wird.
   - Klicken Sie auf den Umschalter **Kundenbezogen**, um ihn zu aktivieren (er ist standardmäßig deaktiviert). Wenn die Option aktiviert ist, wird die Zeit für diese Aktivität im Arbeitszeittabellen-Bericht als kundenbezogen angezeigt. Wenn die Option deaktiviert ist, wird die Zeit für diese Tätigkeit im Arbeitszeittabellen-Bericht als intern angezeigt.
4. Klicken Sie auf ✓, um die Aktivität zu speichern.

   Die Aktivität ist jetzt verfügbar, um für Aktivitäten mit aktiver Zeiterfassung verwendet zu werden. Wenn Sie beispielsweise eine neue Zeiterfassung definieren, können Sie die relevante Aktivität (wie etwa *Projektmanagement* oder *Mittagspause*), die der Zeiterfassung zugeordnet werden soll, aus dem Feld **Aktivität** auswählen.

Eine Aktivität bearbeiten

Alle Aktivitäten, einschließlich der vordefinierten Aktivitäten, die mit Advanced Automation ausgeliefert werden, sind bearbeitbar. Sie können eine Aktivität auch deaktivieren, aber nicht löschen.

So können Sie eine Aktivität bearbeiten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie zuerst auf die Registerkarte **Aktivitäten** und anschließend auf das Stiftsymbol für die relevante Aktivität.

3. Nehmen Sie die Änderungen vor, die Sie an dieser Aktivität vornehmen wollen. Weitere Informationen finden Sie im Abschnitt '"Eine Aktivität erstellen" (S. 277)'.

   Beachten Sie, dass Sie die Aktivität auch deaktivieren können, indem Sie auf den Umschalter **Aktiv** klicken. Dadurch wird sie auf der Registerkarte **Aktivitäten** aus der Liste der Aktivitäten entfernt sowie aus allen Zeiterfassungen, denen sie hinzugefügt wurde.
4. Klicken Sie auf ✓, um Ihre Änderungen zu übernehmen.

Integrationseinstellungen für externe Tickets definieren

Wenn Sie Advanced Automation so konfiguriert haben, dass dieses externe Tickets von einer RMM-Plattform (z.B. Continuum) verwalten soll, können Sie die entsprechenden Integrationseinstellungen auf der **Externe Ticket-Integration** bearbeiten.

So können Sie Ihre Integrationseinstellungen für externe Tickets bearbeiten

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Externe Ticket-Integration**.
3. Klicken Sie auf **Bearbeiten** und aktualisieren Sie die Standardeinstellungen entsprechend Ihren Anforderungen.
4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

Konfigurationselemente einsehen

Konfigurationselemente sind Assets (Kundengeräte), die von einer externen RMM-Plattform verwaltet und automatisch in Advanced Automation importiert werden. Sie können die Details zu diesen Konfigurationselementen einsehen und diese in den **Service Desk**-Einstellungen auch mit bestimmten Benutzern verknüpfen.

Hinweis
Die Synchronisierung zwischen den Kunden-Standorten und -Geräten und der RMM-Software kann bis zu 15 Minuten dauern. Ein neues Gerät, das in der RMM-Plattform eingerichtet wurde, wird also beispielsweise innerhalb von 15 Minuten in Advanced Automation sichtbar. Alle Änderungen werden in der Advanced Automation-Datenbank aktualisiert.

So können Sie Konfigurationselemente einsehen

1. Gehen Sie zu **Einstellungen –> Service Desk**.
2. Klicken Sie auf die Registerkarte **Konfigurationselemente**.
3. Klicken Sie auf die entsprechende Zeile des Konfigurationselements. Im rechten Fensterbereich werden folgende schreibgeschützte Details zu dem Konfigurationselement angezeigt:
   - Gerätename
   - RMM-Integration
   - Website-Name des Kunden

- Beschreibung
- Speicherort

4. Wenn Sie das Konfigurationselement mit einem bestimmten Benutzer verknüpfen wollen, klicken Sie in der entsprechenden Zeile auf **Mit Benutzer verknüpfen**. Wählen Sie dann den entsprechenden Benutzer aus dem Listenfeld aus und klicken Sie anschließend auf **Verknüpfung**. Das Konfigurationselement ist nun mit dem ausgewählten Benutzer verknüpft. Das bedeutet, dass alle neuen Service Desk-Tickets, die von diesem Benutzer erstellt oder ihm zugewiesen werden, automatisch mit dem Konfigurationselement verknüpft werden.

   Wenn Sie die Verknüpfung zwischen einem Konfigurationselement und einem Benutzer wieder aufheben wollen, müssen Sie in der entsprechenden Zeile auf **Mit Benutzer verknüpfen** und im rechten Fensterbereich auf **Verknüpfung aufheben** klicken.

Einstellungen für Abrechnung und Angebotserstellung

Mit Advanced Automation können Sie Ihre Abrechnungen vollständig individualisieren. Sie können das Layout, das Standard-Exportformat (falls Sie die Rechnungen in ein anderes System importieren wollen) und vieles mehr festlegen. Sie können das Erscheinungsbild anpassen, eine Adresse und Textränder festlegen sowie ein Hintergrundbild Ihrer Wahl hinzufügen.

In diesem Abschnitt können Sie auch die Steuern festlegen, die in Advanced Automation verwendet werden sollen, sowie die Integration mit Ihrer bevorzugten Buchhaltungssoftware definieren (siehe Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)').

Wenn Sie auf die Einstellungen für Abrechnung und Angebotserstellung zugreifen wollen, gehen Sie zu **Einstellungen –> Abrechnung und Angebotserstellung**.

Abrechnungseinstellungen

In diesem Abschnitt wird beschrieben, wie Sie die Standardeinstellungen für Abrechnungen und Rechnungsstellung konfigurieren können, wozu auch die Anpassung des Erscheinungsbildes für Ihre Rechnungen gehört.

Ihre Standardabrechnungseinstellungen definieren

In diesem Abschnitt wird beschrieben, wie Sie Ihre Abrechnungen einrichten und entsprechende Standardeinstellungen festlegen, einschließlich der Zeiterfassungs-Rundungszeiten und der Standardsteuer, die in den Rechnungen verwendet werden soll. Diese Einstellungen werden standardmäßig in Verkaufsartikeln, Rechnungen und Verträgen verwendet.

So können Sie Ihre Abrechnungseinstellungen konfigurieren

1. Gehen Sie im Management-Portal zu **Einstellungen –> Abrechnung und Angebotserstellung**. Als Grundeinstellung wird die Registerkarte **Abrechnungseinstellungen** angezeigt.
2. Klicken Sie auf das Stiftsymbol und ändern Sie eine beliebige der folgenden Standardeinstellungen:

- **Zeiterfassungsrundung**: Legen Sie die Zeit (in Minuten) für Ihre Ticket-Rundungszeit fest. Wenn eine Ticket-Arbeit zur Abrechnung genehmigt wurde, werden die abrechenbaren Gesamtstunden gemäß diesem Wert aufgerundet. Wenn Sie beispielsweise den Wert für die Rundungszeit mit 15 Minuten festlegen, wird die eine Ticket-Arbeitszeit von 7 Minuten vor der Rechnungsstellung auf 15 Minuten aufgerundet. Ebenso werden 21 Minuten auf 30 Minuten, 36 Minuten auf 45 Minuten und so weiter aufgerundet. Der Standardwert beträgt **10**.
- **Rundungszeit für außerhalb der Geschäftszeiten**. Legen Sie die Rundungszeit für Tickets außerhalb der üblichen Geschäftszeiten (z.B. zwischen 08:00 und 17:00 Uhr) fest. Der Standardwert beträgt **20**.
- **Verwerfen Sie Tickets zur Genehmigung mit einer Zeit, die gleich oder kürzer ist als der unten festgelegte Grenzwert**: Aktivieren Sie den Umschalter, wenn Sie Tickets verwerfen wollen, die Ihrem Mindestgrenzwert entsprechen. Definieren Sie den relevanten Grenzwert im Feld **Grenzwert, Minuten**.
- **Standard-Buchhaltungssoftware**: Wählen Sie die entsprechende Software aus der Liste der verfügbaren integrierten Buchhaltungsplattformen (siehe Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)').
- **Anzahl der zu wartenden Tage, bis das Ticket automatisch geschlossen wird**: Legen Sie fest, wie viele Tage das System warten soll, bevor es ein abgeschlossenes Ticket schließt. Der Wert ist standardmäßig mit **1** festgelegt.

  Hinweis
  Techniker können nur bei abgeschlossenen Tickets den Status auf **Abgeschlossen** setzen. Wenn die festgelegte Anzahl von Tagen verstrichen ist, werden die Tickets automatisch geschlossen. Dadurch wird sichergestellt, dass Sie, wenn Sie ein Ticket abschließen und eine E-Mail an den Kunden gesendet wird, oft ein 'Danke' als Antwort von ihm erhalten. Durch eine solche Antwort würde jedoch das Ticket erneut geöffnet, was sich auf Ihre Statistik der wiedergeöffneten Tickets auswirken würde und Sie zwingen würde, das Ticket erneut zu schließen. Mit dieser Funktionalität zum automatischen Schließen lässt sich dieses Problem lösen. Wenn Sie diese Funktionalität deaktivieren wollen, müssen Sie den Wert auf **0** setzen.

- **Standardprodukt-Hauptbuch für Rechnungsexporte**: Wählen Sie die Nummer des Standardprodukt-Hauptbuchs aus, die für Rechnungsexporte verwendet werden soll (die Standardeinstellung ist **400**). Die in der Liste angezeigten Produkt-Hauptbücher sind die aktuell verfügbaren Hauptbuch-Nummern (siehe Abschnitt '"Hauptbücher verwalten" (S. 249)').

Hinweis
Wenn Rechnungen zu Ihrer Buchhaltungssoftware exportiert werden, erfolgt dies üblicherweise in Form allgemeiner Informationen (Unternehmen, Kunde, Summen) und mit Informationen zu den einzelnen Rechnungspositionen (Produkt, Beschreibung, Hauptbuch, Menge, Preis, Summe, Steuer usw.). Dieses Feld definiert, welche Hauptbuch-Nummer standardmäßig für ein Produkt verwendet wird, wenn diesem in den Produkteinstellungen kein Hauptbuch zugewiesen wurde.

- **Standardprodukt für die Ticket-Zeitabrechnung**: Wählen Sie das Standardprodukt aus, das für die Ticket-Zeitabrechnung verwendet werden soll.
- **Standardabrechnungsprodukt für Blockstunden**: Wenn Sie Ihren Kunden Blockstunden anbieten, wählen Sie das Standardprodukt aus, das für die Blockstunden verwendet werden soll.
- **Standardumsatzsteuer**: Wählen Sie die Standardumsatzsteuer, die Sie verwenden wollen, aus der Liste der verfügbaren Steuern aus (siehe Abschnitt '"Steuer-Einstellungen" (S. 287)').
- **Standardprodukt für außerhalb der Geschäftszeiten**: Wählen Sie das Standardprodukt, das für alle Abrechnungen verwendet werden soll, deren Arbeitszeit außerhalb der üblichen Geschäftszeiten lag.

3. Klicken Sie auf ✓, um Ihre Änderungen anzuwenden.

Einen neuen Rechnungssteller hinzufügen

Mit Rechnungsstellern können Sie Rechnungen von verschiedenen juristischen Personen versenden, die zu Ihrem Unternehmen gehören. Ein Standard-Rechnungssteller wurde erstellt, als Ihr Konto erstellt wurde. Sie können außerdem die Details dieses Rechnungsstellers aktualisieren, wenn dies die einzige juristische Person ist, die Sie benötigen.

Hinweis
Nur Benutzer mit der Rolle Administrator oder Direktor können Rechnungssteller erstellen oder aktualisieren.

So können Sie einen neuen Rechnungssteller hinzufügen

1. Gehen Sie im Management-Portal zu **Verkauf und Abrechnung –> Unternehmensverwaltung**.
2. Klicken Sie auf die Registerkarte **Rechnungssteller**. Der aktuelle Rechnungssteller wird aufgelistet.
3. Klicken Sie auf **+ Neue Rechnungssteller**.
4. Definieren Sie Folgendes:
   - **Firmenname**: Geben Sie den Firmennamen ein.
   - **Bankkontonummer**: Geben Sie die entsprechende Bankkontonummer für diese juristische Person ein.

- **Rechnungsstartnummer**: Geben Sie die Startnummer der Rechnungen ein, sobald Sie anfangen, Rechnungen an Kunden zu senden.
- **Rechnungsseriennummer**: Mit dieser Option können Sie denselben Rechnungsnummernbereich beibehalten, wenn Sie in der Mitte eines Geschäftsjahres zu Advanced Automation wechseln.

5. (Optional) Aktivieren Sie den Umschalter **Rechnungsnummerierung zurücksetzen**. Dadurch werden Ihre Rechnungsnummern auf die Nummer zurückgesetzt, die Sie im Feld **Rechnungsstartnummer** festgelegt haben.
6. Aktivieren Sie den Umschalter **Aktiv**, um den neuen Rechnungssteller zu aktivieren.
7. Klicken Sie auf **Erstellen**. Der Rechnungssteller wird auf der Registerkarte **Rechnungssteller** hinzugefügt und kann ausgewählt werden, wenn Rechnungen generiert (siehe Abschnitt '"Eine neue Rechnung generieren" (S. 236)') oder Verkaufartikel (siehe Abschnitt '"Einen neuen Verkaufsartikel erstellen" (S. 224)') bzw. Verträge (siehe Abschnitt '"Einen neuen Vertrag erstellen" (S. 226)') erstellt werden.

   Bei Bedarf können Sie einen Rechnungssteller auch aktualisieren. Klicken Sie dafür auf der Registerkarte **Rechnungssteller** auf den entsprechenden Rechnungssteller und bearbeiten Sie diesen wie gewünscht. Beachten Sie, dass Sie einen Rechnungssteller nicht löschen können.

Das Erscheinungsbild der Rechnungen anpassen

Sie können das Layout Ihrer Rechnungen und Angebote, die Sie an Ihre Kunden senden, umfassend anpassen. Sie können Ihr eigenes Hintergrundbild hochladen, den Fußzeilentext Ihrer Rechnung festlegen und die Ränder für die von Advanced Automation hinzugefügten Texte einstellen.

Sie können das Hintergrundbild verwenden, um Details wie Ihr Firmenlogo, Ihre Adresse, Ihre Website oder Ihre E-Mail-Adresse in Ihre Rechnungen zu integrieren.

Hinweis
Wenn Sie mit der Anpassung Ihrer Rechnung ganz neu beginnen wollen, können Sie hier eine leere Vorlage für das Hintergrundbild herunterladen. Wenn Sie bereits ein Layout für Ihre Rechnungen im PDF-Format haben, können Sie dieses mit Online-Tools von Drittanbietern in ein hochauflösendes JPG-Bild umwandeln.

So können Sie Ihre Rechnung anpassen

1. Gehen Sie im Management-Portal zu **Einstellungen –> Abrechnung und Angebotserstellung**.
2. Klicken Sie auf die Registerkarte **Rechnungseinstellungen**.
3. Klicken Sie auf das Stiftsymbol, eine beliebige der folgenden Einstellungen zu ändern:
   - **Hintergrundbild für die Rechnung**: Ziehen Sie eine Bilddatei in das angezeigte Feld oder klicken Sie auf **Durchsuchen**, um Ihr Bild hochladen zu können. Die Bilddatei sollte ein JPEG im A4-Format mit einer maximalen Größe von 1 MB sein.
   - **Fußzeilentext der Rechnung für automatische Abbuchung**: Ändern Sie den Fußzeilentext für die automatische Abbuchung nach Bedarf. Mithilfe der in Advanced Automation verfügbaren Variablen (siehe nachfolgend) könnte Ihr Fußzeilentext für Rechnungen mit

automatischer Abbuchung beispielsweise folgendermaßen lauten:

"Automatic debit with bank account: [BANK_ACCOUNT_NUMBER], Kundenname > [CUSTOMER_NAME] und USt.-Identifikationsnummer= [VAT_NUMBER]"

Diese ermöglicht Ihren Kunden, Rechnungen per Überweisung oder über eine der Zahlungsintegrationen (PayPal, Stripe) zu bezahlen. Sie können die Rechnung auch zwecks Lastschrifteinzug an ihre Hausbank senden.

Folgende Variablen sind für die automatischen Abbuchungsinformationen auf Rechnungen verfügbar:

- [BANK_ACCOUNT_NUMBER]
- [CUSTOMER_NAME]
- [VAT_NUMBER]
- [INVOICE_NUMBER]
- [INVOICE_DUE_DAYS]

- **Fußzeilentext der Rechnung für manuelle Abbuchung**: Bearbeiten Sie den Fußzeilentext der Rechnung für Ihre manuelle Abbuchung. Der Fußzeilentext der Rechnung für eine manuelle Abbuchung kann beispielsweise folgendermaßen aussehen (unter der Annahme, dass die Fälligkeitstage für die Rechnung mit 15 festgelegt sind und die Rechnungsnummer 2022020107 lautet): "15-2022020107"
- **Fälligkeitsdaten der Rechnung**: Geben Sie eine entsprechende Anzahl von Tagen ein.
- **Präfix der Rechnungsnummer ausblenden**: Aktivieren Sie den Umschalter, wenn Sie das Präfix der Rechnungsnummer ausblenden wollen.
- **Im Voraus abrechenbarer Vertragszeitraum (Tage)**: Geben Sie eine entsprechende Anzahl von Tagen ein.
- **Position der Rechnungsadresse**: Wählen Sie **Links** oder **Rechts**.

Hinweis
Wenn Sie die Position Ihrer Rechnungsadresse ändern, sollten Sie darauf achten, dass sich diese nicht mit Ihrem Firmenlogo überschneidet.

- **Oberer Rand**: Geben Sie einen Wert für den Abstand zwischen Ihrer Firmenadresse und dem oberen Rand des Rechnungsdokuments ein.

Hinweis
Alle Angaben für die Ränder beziehen sich auf Zentimeter.

- **Oberer Rand für Seite 2 und folgende**: Geben Sie einen Wert für den Abstand zwischen Ihrer Firmenadresse und dem oberen Rand des Rechnungsdokuments ab Seite zwei ein.
- **Seitlicher Rand**: Geben Sie einen Wert für den Abstand von der linken Seite des Rechnungsdokuments ein.

- **Unterer Rand der Adresse**: Geben Sie einen Wert für den Abstand zwischen Ihrer Firmenadresse und den Datums- und Rechnungsnummernangaben auf dem Rechnungsdokument ein.
- **Unterer Seitenrand**: Geben Sie einen Wert für den Abstand zwischen der Seitenzahl und dem unteren Rand des Rechnungsdokuments ein.
- **Position der Seitenzahl**: Wählen Sie **Oben** oder **Unten**.
- **Sichtbarkeit der Seitenzahl**: Wählen Sie entweder **Auf allen Seiten anzeigen**, **Für die erste Seite ausblenden** oder **Vollständig ausblenden** als Option.

4. Klicken Sie auf **Vorschau herunterladen**, um eine Vorschau der Rechnung im PDF-Format angezeigt zu bekommen.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

   Wenn eine Rechnung generiert wird, wird die Fußzeile in Abhängigkeit von der definierten Zahlungsmethode automatisch eingefügt:
   - Wenn Lastschrift ausgewählt ist, wird die Option **Fußzeilentext der Rechnung für automatische Abbuchung** verwendet.
   - Wenn nicht Lastschrift ausgewählt ist, wird die Option **Fußzeilentext der Rechnung für manuelle Abbuchung** verwendet.

Einstellungen für die Angebotserstellung

In diesem Abschnitt wird beschrieben, wie Sie die Standardeinstellungen für die Angebotserstellung konfigurieren können, wie etwa das Erscheinungsbild der Angebots-PDF, die an die Kunden gesendet wird.

Die Standardeinstellungen für Angebote definieren

Wenn ein Angebot genehmigt wird, wird von Advanced Automation automatisch Folgendes erstellt:

- Ein Bestell-Ticket für die Artikel, die zuerst gekauft werden müssen (z.B. über einen Händler). Beachten Sie: Wenn ein Artikel bereits auf Lager ist, wird kein Bestell-Ticket erstellt.
- Ein Angebotsticket, um die Angebotselemente an den Kunden zu liefern und diesem in Rechnung zu stellen.

Die Standardeinstellungen für Angebote definieren, welchen Support-Gruppen die oben genannten Ticket-Typen automatisch zugewiesen werden sollen, wenn diese erstellt werden. Sie können auch andere Angebotseinstellungen definieren, z. B. die Standardkategorie und die Standardzahlungsmethode für Verkaufsartikel.

So können Sie die Standardeinstellungen für Angebote definieren

1. Gehen Sie im Management-Portal zu **Einstellungen –> Abrechnung und Angebotserstellung**.
2. Klicken Sie auf die Registerkarte **Angebotseinstellungen**.
3. Klicken Sie auf das Stiftsymbol und ändern Sie eine beliebige der folgenden Standardeinstellungen:

- **Gruppe für Bestell-Tickets**: Wählen Sie die gewünschte Support-Gruppe aus dem Listenfeld aus.
- **Gruppe für Angebotstickets**: Wählen Sie die gewünschte Support-Gruppe aus dem Listenfeld aus.
- **SLA für Angebotstickets**: Wählen Sie die gewünschte SLA aus dem Listenfeld aus.
- **Priorität für Angebotstickets**: Wählen Sie die gewünschte Priorität aus dem Listenfeld aus.
- **Kategorie für Angebotstickets**: Wählen Sie die gewünschte Kategorie aus dem Listenfeld aus.
- **Rechnungssteller**: Wählen Sie den gewünschten Rechnungssteller aus dem Listenfeld aus.
- **Rechung senden**: Wählen Sie entweder die Option **Post** oder **E-Mail**.
- **Zahlungsmethode für Verkaufsartikel**: Wählen Sie entweder die Option **Manuell bezahlen** oder **Vorautorisierte Abbuchung**.
- **Allgemeine Bedingungen**: Fügen Sie allen Angeboten Ihre eigenen Allgemeinen Geschäftsbedingungen hinzu. Also beispielsweise alle rechtlichen Bedingungen, die Sie aufnehmen wollen.

4. Klicken Sie auf ✓, um Ihre Änderungen anzuwenden.

Das Erscheinungsbild von Angebots-PDFs anpassen

In diesem Abschnitt wird beschrieben, wie Sie das standardmäßige Aussehen der Angebots-PDFs, die an Kunden gesendet werden, anpassen können. Sie können Ihr eigenes Hintergrundbild hochladen, den Fußzeilentext Ihres Angebots festlegen und die Ränder für die von Advanced Automation automatisch hinzugefügten Texte einstellen. Optional können Sie diese Elemente auch über ein Hintergrundbild in Ihre Angebote einbinden:

- Firmenlogo
- Adressdetails
- Bankkontonummer
- Website und E-Mail-Adresse
- USt.-Identifikationsnummer

Hinweis
Wenn Sie mit der Anpassung Ihres Angebots ganz neu beginnen wollen, können Sie hier eine leere Vorlage für das Hintergrundbild herunterladen. Wenn Sie bereits ein Layout für Ihre Angebote im PDF-Format haben, können Sie dieses mit Online-Tools von Drittanbietern in ein hochauflösendes JPG-Bild umwandeln.

So können Sie Angebots-PDFs anpassen

1. Gehen Sie im Management-Portal zu **Einstellungen –> Abrechnung und Angebotserstellung**.
2. Klicken Sie auf die Registerkarte **Einstellungen für die Angebots-PDF**.

3. Klicken Sie auf das Stiftsymbol und ändern Sie eine beliebige der folgenden Standardeinstellungen:
   - **Hintergrundbild für Angebots-PDF**: Ziehen Sie eine Bilddatei in das angezeigte Feld oder klicken Sie auf **Datei zum Hochladen hierher ziehen oder auswählen**, um Ihr Bild hochladen zu können. Die Bilddatei sollte ein JPEG im A4-Format mit einer maximalen Größe von 1 MB sein.
   - **Oberer Rand**: Geben Sie einen Wert für den Abstand zwischen Ihrer Firmenadresse und dem oberen Rand des Angebotsdokuments ein.

     Hinweis
     Alle Angaben für die Ränder beziehen sich auf Zentimeter.

   - **Oberer Rand für Seite 2 und folgende**: Geben Sie einen Wert für den Abstand zwischen Ihrer Firmenadresse und dem oberen Rand des Angebotsdokuments ab Seite zwei ein.
   - **Seitlicher Rand**: Geben Sie einen Wert für den Abstand von der linken Seite des Angebotsdokuments ein.
   - **Unterer Rand der Adresse**: Geben Sie einen Wert für den Abstand zwischen Ihrer Firmenadresse und den Datums- und Angebotsnummernangaben auf dem Angebotsdokument ein.
   - **Unterer Seitenrand**: Geben Sie einen Wert für den Abstand zwischen der Seitenzahl und dem unteren Rand des Angebotsdokuments ein.
   - **Position der Seitenzahl**: Wählen Sie **Oben** oder **Unten**.
   - **Sichtbarkeit der Seitenzahl**: Wählen Sie entweder **Auf allen Seiten anzeigen**, **Für die erste Seite ausblenden** oder **Vollständig ausblenden** als Option.
4. Klicken Sie auf **Vorschau herunterladen**, um eine Vorschau das Angebots im PDF-Format angezeigt zu bekommen.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

Steuer-Einstellungen

In diesem Abschnitt wird beschrieben, wie Sie die standardmäßigen Steuer-Einstellungen konfigurieren können, um diese in Ihren Rechnungen an Ihre Kunden zu verwenden. Die aufgeschlagenen Steuern richten sich nach Ihrem Standort und den verkauften Produkten.

Eine Steuer hinzufügen

So können Sie eine Steuer hinzufügen

1. Gehen Sie im Management-Portal zu **Einstellungen –> Abrechnung und Angebotserstellung**.
2. Klicken Sie auf die Registerkarte **Steuern**.
3. Klicken Sie auf **+ Neu hinzufügen**.

4. Geben Sie die Steuerkennziffer und den Steuernamen ein und legen Sie den entsprechenden Wert fest. Die Steuer ist standardmäßig als aktiv festgelegt.
5. Klicken Sie auf ✓, um die neue Steuer zu speichern.

   Die neue Steuer wird der Registerkarte **Steuern** hinzugefügt.

Eine Steuer bearbeiten

Sie können eine Steuer jederzeit bearbeiten und diese bei Bedarf aktivieren/deaktivieren. Sie können eine Steuer auch löschen.

So können Sie eine Steuer bearbeiten

1. Gehen Sie im Management-Konsole zu **Einstellungen –> Abrechnung und Angebotserstellung**.
2. Klicken Sie auf die Registerkarte **Steuern**.
3. Klicken Sie auf das Stiftsymbol für die Steuer, die Sie bearbeiten wollen, und führen Sie dann die gewünschten Änderungen durch.

   Sie können den Umschalter anklicken, um die Steuer zu aktivieren oder zu deaktivieren.

   Hinweis
   Wenn Sie eine Steuer löschen wollen, klicken Sie auf das Papierkorb-Symbol. Beachten Sie, dass Sie eine Steuer nicht löschen können, wenn diese bereits im System (z.B. als Umsatzsteuer) zugewiesen wurde.

4. Klicken Sie auf ✓, um Ihre Änderungen anzuwenden.

Den Advanced Automation Service mit Drittanbieter-Plattformen integrieren

Der Advanced Automation Service kann mit einigen der gängigsten Buchhaltungsplattformen, RMM-Tools, VAR- und Zahlungsplattformen integriert werden.

Folgende Integrationen werden derzeit unterstützt:

- **Buchhaltungsintegrationen**: FreshBooks, QuickBooks, Sage, Xero und SnelStart
- **RMM-Integrationen**: NinjaOne, Datto RMM, Kaseya VSA, N-able N-central und N-able RMM
- **VAR-Integrationen**: Microsoft CSP
- **Zahlungsintegrationen**: PayPal und Stripe

Wenn Sie auf Ihre Integrationen zugreifen wollen, gehen Sie im Management-Portal zum Bereich **Integrationen**.

Hinweis
Diese Funktionalität ist nur für Benutzer verfügbar, denen die Administrator-Rolle zugewiesen wurde.

Mit Buchhaltungsplattformen integrieren

Advanced Automation ermöglicht es Ihnen, sich mit einigen der beliebtesten Buchhaltungsplattformen zu integrieren. Dadurch können Sie die in Ihrer Buchhaltungsplattform gespeicherten Kunden, Produkte und Hauptbücher mit Advanced Automation synchronisieren. Außerdem können Sie damit Rechnungen, die in Advanced Automation generiert wurden, automatisch zu Ihrer Buchhaltungsplattform hochladen lassen.

Wenn Sie auf die Buchhaltungsintegrationen zugreifen wollen, gehen Sie zu **Integrationen**. Wählen Sie im links angezeigten Menü den Eintrag **Buchhaltung**.

Mit FreshBooks integrieren

In diesem Abschnitt wird beschrieben, wie Sie FreshBooks mit dem Advanced Automation Service integrieren können.

Informationen über weitere Buchhaltungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)'.

Hinweis
Wenn Sie über eine benutzerdefinierte URL für die Weboberfläche auf das Management-Portal zugreifen, sollte die Integration mit FreshBooks nur aktiviert werden, wenn Sie über die Standard-URL des Management-Portals (https://cloud.acronis.com) angemeldet sind. Weitere Informationen über das Branding und benutzerdefinierte URLs für die Weboberfläche finden Sie im Abschnitt '"Eine benutzerdefinierte URL für die Weboberfläche konfigurieren" (S. 94)'.

So können Sie FreshBooks mit dem Advanced Automation Service integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie in der FreshBooks-Kachel auf **Aktivieren**. Sie werden dann aufgefordert, den Authentifizierungsprozess zu aktivieren, woraufhin Sie zur FreshBooks-Anmeldeseite weitergeleitet werden.
3. Geben Sie die Anmeldedaten für Ihr FreshBooks-Konto ein, um die Integration zu aktivieren.
4. Wählen Sie die Daten aus, die Sie aus FreshBooks importieren wollen (wie Kunden, Hauptbücher, Produkte und Steuern), und klicken Sie dann auf **Importieren**.
   Beachten Sie, dass nach Abschluss der anfänglichen Integration jedes Mal, wenn Sie auf **Importieren** klicken, nur noch neue Kunden, Hauptbücher, Produkte und Steuern importiert werden.

5. Klicken Sie auf **Speichern**, damit Ihre Integrationseinstellungen gesichert werden. Die Integration wird jetzt auf der Registerkarte **Buchhaltung** angezeigt.

Hinweis
Wenn die Integration aktiviert ist, wird der Advanced Automation Service alle paar Minuten automatisch nach neuen Rechnungen suchen und diese mit FreshBooks synchronisieren. Sie können den Synchronisierungsstatus in der Spalte **Status der Rechnungssynchronisierung** in der Anzeige **Rechnungen** einsehen (gehen Sie zu **Verkauf und Abrechnung –> Rechnungen**).

So können Sie die FreshBooks-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der FreshBooks-Kachel auf **Konfigurieren**. Alternativ können Sie auch auf das Drei-Punkte-Symbol (...) klicken und dann den Befehl **Mehr erfahren** auswählen.
4. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre FreshBooks-Integration deaktivieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der FreshBooks-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Deaktivieren**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Mit QuickBooks integrieren

In diesem Abschnitt wird beschrieben, wie Sie QuickBooks Online mit dem Advanced Automation Service integrieren können.

Informationen über weitere Buchhaltungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)'.

Hinweis
Wenn Sie über eine benutzerdefinierte URL für die Weboberfläche auf das Management-Portal zugreifen, sollte die Integration mit QuickBooks nur aktiviert werden, wenn Sie über die Standard-URL des Management-Portals (https://cloud.acronis.com) angemeldet sind. Weitere Informationen über das Branding und benutzerdefinierte URLs für die Weboberfläche finden Sie im Abschnitt '"Eine benutzerdefinierte URL für die Weboberfläche konfigurieren" (S. 94)'.

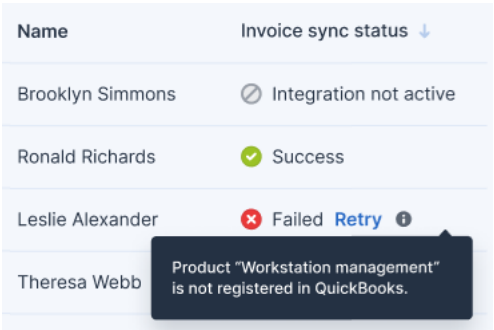
So können Sie QuickBooks mit dem Advanced Automation Service integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie in der QuickBooks-Kachel auf **Aktivieren**. Sie werden dann aufgefordert, den Authentifizierungsprozess zu aktivieren, woraufhin Sie zur QuickBooks-Anmeldeseite weitergeleitet werden.
3. Geben Sie die Anmeldedaten für Ihr QuickBooks-Konto ein, um die Integration zu aktivieren.
4. Wählen Sie die Daten aus, die Sie aus QuickBooks importieren wollen (wie Kunden, Hauptbücher, Produkte und Steuern), und klicken Sie dann auf **Importieren**.

   Beachten Sie, dass nach Abschluss der anfänglichen Integration jedes Mal, wenn Sie auf **Importieren** klicken, nur noch neue Kunden, Hauptbücher, Produkte und Steuern importiert werden.
5. Klicken Sie auf **Speichern**, damit Ihre Integrationseinstellungen gesichert werden. Die Integration wird jetzt auf der Registerkarte **Buchhaltung** angezeigt.

Hinweis

Wenn die Integration aktiv ist, wird der Advanced Automation Service alle paar Minuten automatisch nach neuen Rechnungen suchen und diese mit QuickBooks synchronisieren. Sie können den Synchronisierungsstatus in der Spalte **Status der Rechnungssynchronisierung** in der Anzeige **Rechnungen** einsehen (gehen Sie zu **Verkauf und Abrechnung –> Rechnungen**).



So können Sie die QuickBooks-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der QuickBooks-Kachel auf **Konfigurieren**. Alternativ können Sie auch auf das Drei-Punkte-Symbol (...) klicken und dann den Befehl **Mehr erfahren** auswählen.
4. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre QuickBooks-Integration deaktivieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der QuickBooks-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Deaktivieren**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Mit Sage integrieren

In diesem Abschnitt wird beschrieben, wie Sie Sage Business Cloud mit dem Advanced Automation Service integrieren können.

Informationen über weitere Buchhaltungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)'.

Hinweis
Wenn Sie über eine benutzerdefinierte URL für die Weboberfläche auf das Management-Portal zugreifen, sollte die Integration mit Sage nur aktiviert werden, wenn Sie über die Standard-URL des Management-Portals (https://cloud.acronis.com) angemeldet sind. Weitere Informationen über das Branding und benutzerdefinierte URLs für die Weboberfläche finden Sie im Abschnitt '"Eine benutzerdefinierte URL für die Weboberfläche konfigurieren" (S. 94)'.

So können Sie Sage mit dem Advanced Automation Service integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie in der Sage-Kachel auf **Aktivieren**. Sie werden dann aufgefordert, den Authentifizierungsprozess zu aktivieren, woraufhin Sie zur Sage-Anmeldeseite weitergeleitet werden.
3. Geben Sie die Anmeldedaten für Ihr Sage-Konto ein, um die Integration zu aktivieren.

   Hinweis
   Wenn die Integration aktiviert ist, überprüft Advanced Automation automatisch alle paar Minuten auf neue Rechnungen und synchronisiert diese mit Sage. Der Synchronisationsstatus kann in der Spalte **Status der Rechnungssynchronisierung** auf der Anzeige **Rechnungen** eingesehen werden (gehen Sie zu **Verkauf und Abrechnung > Rechnungen**).

   Darüber hinaus können Einheitspreise in Sage-Rechnungspositionen nur bis zu zwei Stellen nach dem Dezimaltrennzeichen haben. Andere Buchhaltungsplattformen unterstützen in der Regel vier Stellen nach dem Dezimaltrennzeichen. Preise werden in Advanced Automation automatisch auf zwei Stellen nach dem Dezimaltrennzeichen aufgerundet und dann mit Sage synchronisiert. Eine Konfiguration durch den Benutzer ist nicht erforderlich.

4. Wählen Sie die Daten aus, die Sie aus Sage importieren wollen (wie Kunden, Hauptbücher, Produkte und Steuern), und klicken Sie dann auf **Importieren**.
   Beachten Sie, dass nach Abschluss der anfänglichen Integration jedes Mal, wenn Sie auf **Importieren** klicken, nur noch neue Kunden, Hauptbücher, Produkte und Steuern importiert werden.
5. Klicken Sie auf **Speichern**, damit Ihre Integrationseinstellungen gesichert werden. Die Integration wird jetzt auf der Registerkarte **Buchhaltungsintegrationen** angezeigt.

So können Sie die Sage-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der Sage-Kachel auf **Konfigurieren**. Alternativ können Sie auch auf das Drei-Punkte-Symbol (...) klicken und dann den Befehl **Mehr erfahren** auswählen.
4. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre Sage-Integration deaktivieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der Sage-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Deaktivieren**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Mit Xero integrieren

In diesem Abschnitt wird beschrieben, wie Sie Xero mit dem Advanced Automation Service integrieren können.

Informationen über weitere Buchhaltungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)'.

Hinweis
Wenn Sie über eine benutzerdefinierte URL für die Weboberfläche auf das Management-Portal zugreifen, sollte die Integration mit Xero nur aktiviert werden, wenn Sie über die Standard-URL des Management-Portals (https://cloud.acronis.com) angemeldet sind. Weitere Informationen über das Branding und benutzerdefinierte URLs für die Weboberfläche finden Sie im Abschnitt '"Eine benutzerdefinierte URL für die Weboberfläche konfigurieren" (S. 94)'.

So können Sie Xero mit dem Advanced Automation Service integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie in der Xero-Kachel auf **Aktivieren**. Sie werden dann aufgefordert, den Authentifizierungsprozess zu aktivieren, woraufhin Sie zur Xero-Anmeldeseite weitergeleitet werden.
3. Geben Sie die Anmeldedaten für Ihr Xero-Konto ein, um die Integration zu aktivieren.
4. Wählen Sie die Daten aus, die Sie aus Xero importieren wollen (wie Kunden, Hauptbücher, Produkte und Steuern), und klicken Sie dann auf **Importieren**.
   Beachten Sie, dass nach Abschluss der anfänglichen Integration jedes Mal, wenn Sie auf **Importieren** klicken, nur noch neue Kunden, Hauptbücher, Produkte und Steuern importiert werden.
5. Klicken Sie auf **Speichern**, damit Ihre Integrationseinstellungen gesichert werden. Die Integration wird jetzt auf der Registerkarte **Buchhaltung** angezeigt.

Hinweis
Wenn die Integration aktiviert ist, wird der Advanced Automation Service alle paar Minuten automatisch nach neuen Rechnungen suchen und diese mit Xero synchronisieren. Sie können den Synchronisierungsstatus in der Spalte **Status der Rechnungssynchronisierung** in der Anzeige **Rechnungen** einsehen (gehen Sie zu **Verkauf und Abrechnung –> Rechnungen**).

So können Sie die Xero-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der Xero-Kachel auf **Konfigurieren**. Alternativ können Sie auch auf das Drei-Punkte-Symbol (...) klicken und dann den Befehl **Mehr erfahren** auswählen.
4. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre Xero-Integration deaktivieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der Xero-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Deaktivieren**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Mit SnelStart integrieren

In diesem Abschnitt wird beschrieben, wie Sie SnelStart mit Advanced Automation integrieren können.

Informationen über weitere Buchhaltungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Buchhaltungsplattformen integrieren" (S. 289)'.

Hinweis
Wenn Sie über eine benutzerdefinierte URL für die Weboberfläche auf das Management-Portal zugreifen, sollte die Integration mit SnelStart nur aktiviert werden, wenn Sie über die Standard-URL des Management-Portals (https://cloud.acronis.com) angemeldet sind. Weitere Informationen über das Branding und benutzerdefinierte URLs für die Weboberfläche finden Sie im Abschnitt '"Eine benutzerdefinierte URL für die Weboberfläche konfigurieren" (S. 94)'.

So können Sie SnelStart mit Advanced Automation integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie in der SnelStart-Kachel auf **Aktivieren**. Sie werden dann aufgefordert, den Authentifizierungsprozess zu aktivieren, woraufhin Sie zur SnelStart-Anmeldeseite weitergeleitet werden.

3. Geben Sie die Anmeldedaten für Ihr SnelStart-Konto ein, um die Integration zu aktivieren.
4. Wählen Sie die Daten aus, die Sie aus SnelStart importieren wollen (wie Kunden, Hauptbücher, Produkte und Steuern), und klicken Sie dann auf **Importieren**.

   Beachten Sie, dass nach Abschluss der anfänglichen Integration jedes Mal, wenn Sie auf **Importieren** klicken, nur noch neue Kunden, Hauptbücher, Produkte und Steuern importiert werden.
5. Klicken Sie auf **Speichern**, damit Ihre Integrationseinstellungen gesichert werden. Die Integration wird jetzt auf der Registerkarte **Verwendete Integrationen** angezeigt.

Hinweis
Wenn die Integration aktiviert ist, wird Advanced Automation alle paar Minuten automatisch nach neuen Rechnungen suchen und diese mit SnelStart synchronisieren. Sie können den Synchronisierungsstatus in der Spalte **Status der Rechnungssynchronisierung** in der Anzeige **Rechnungen** einsehen (gehen Sie zu **Verkauf und Abrechnung –> Rechnungen**).

So können Sie die SnelStart-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der SnelStart-Kachel auf **Konfigurieren**. Alternativ können Sie auch auf das Drei-Punkte-Symbol (...) klicken und dann den Befehl **Mehr erfahren** auswählen.
4. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre SnelStart-Integration deaktivieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Buchhaltung**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der SnelStart-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Deaktivieren**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Hinweis
Nach der Deaktivierung wird Advanced Automation alle Kunden, Hauptbücher, Produkte und Steuern beibehalten, sodass Sie diese weiterhin nutzen können. Neue Rechnungen in Advanced Automation werden jedoch nicht mehr mit der Buchhaltungsplattform synchronisiert.

Mit RMM-Plattformen integrieren

Advanced Automation ermöglicht es Ihnen, sich mit RMM-Plattformen (Remote Monitoring & Management) zu integrieren. Dadurch können Sie das Erstellen und Verwalten von Tickets automatisieren und die Kundenabrechnung mit den verwalteten Kundenaktiva abgleichen.

Wenn Sie auf die RMM-Integrationen zugreifen wollen, gehen Sie zu **Integrationen**. Wählen Sie im links angezeigten Menü den Eintrag **RMM/PSA**.

Wenn Sie die Integration einrichten, müssen Sie darauf achten, dass Ihre RMM-Software geöffnet bleibt, da Sie deren URL und Schlüssel benötigen, um die Integration abschließen zu können.

Mit NinjaOne integrieren

Durch die Integration von Advanced Automation mit NinjaOne können Sie:

- Kunden-Sites und Geräte automatisch aus NinjaOne importieren.
- Kunden bestimmten Sites von NinjaOne zuordnen.
- Tickets aus NinjaOne-Alarmmeldungen erstellen.
- Auf die NinjaOne-Geräteseite aus einem Ticket heraus zugreifen.
- Rechnungen für die tatsächliche Anzahl von Geräten von NinjaOne an die Kunden stellen.

NinjaOne unterstützt die OAuth 2.0-Authentifizierung, die für alle neuen Integrationen anwendbar ist. Wenn Sie eine Integration haben, die mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel eingerichtet wurde, muss diese manuell aktualisiert werden.

Hinweis
Damit NinjaOne erfolgreich mit Advanced Automation integriert werden kann, muss der Advanced Automation Service aktiviert sein. Sie müssen außerdem ein vollständig konfiguriertes NinjaOne-Konto haben.

Die NinjaOne-Integration einrichten

Es gibt zwei Hauptschritte, wenn Sie Ihre NinjaOne-Integration mit Advanced Automation einrichten. Diese werden in den nachfolgenden Prozeduren beschrieben:

1. Die Integrationseinstellungen definieren, um eine Verbindung mit der NinjaOne-Instanz herzustellen.
2. NinjaOne-Kunden zu Advanced Automation zuordnen.

So können Sie die Integrationseinstellungen definieren

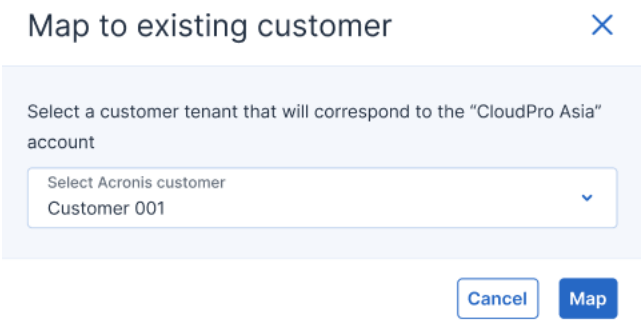
1. Gehen Sie im Management-Portal zu **Integrationen**. Wählen Sie in der angezeigten Integrationsliste den Eintrag **RMM/PSA**.
2. Klicken Sie auf der **NinjaOne**-Kachel auf **Konfigurieren**.
3. Geben Sie die relevanten NinjaOne-Anmeldedaten ein, um auf die NinjaOne-Instanz zugreifen zu können. Weitere Informationen finden Sie hier.

   Hinweis
   NinjaOne unterstützt die OAuth 2.0-Authentifizierung, die für alle neuen Integrationen anwendbar ist. Wenn Sie eine Integration haben, die mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel eingerichtet wurde, muss diese manuell aktualisiert werden.

4. Nachdem die Anmeldedaten definiert wurden, besteht der nächste Schritt bei der Einrichtung Ihrer Integration darin, die NinjaOne-Kunden bestehenden oder neuen Advanced Automation-Kunden zuzuordnen (siehe unten).

So können Sie NinjaOne-Kunden zuordnen

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf der **NinjaOne**-Kachel auf **Konfigurieren**.
3. Klicken Sie auf der Registerkarte **Kunden-Zuordnung** auf **Acronis Kunden aus NinjaOne-Sites erstellen**. Der Zuordnungsprozess wird für alle aufgeführten NinjaOne-Sites gestartet.
   Alle Kunden (Kunden-Sites) von NinjaOne werden als neue Kunden in Cyber Protect Cloud registriert, wobei alle verfügbaren Services gewährt werden.
   Sie können auch einzelne NinjaOne-Sites auswählen und diese bestehenden Cyber Protect Cloud-Kunden zuordnen. Wählen Sie dazu die entsprechende(n) Site(s) aus und klicken Sie anschließend auf **Vorhandenem Kunden-Mandanten zuordnen**. Sie werden dann aufgefordert, einen vorhandenen Kunden auszuwählen. Klicken Sie nach der Auswahl auf **Zuordnen**, um den Zuordnungsprozess abzuschließen.



4. Wenn dies abgeschlossen ist, wird in der Spalte **Zuordnung** der Status **Zugeordnet** und in der Spalte **Acronis Kunde** der entsprechende Kundenname angezeigt.

Hinweis
Wenn Sie eine Zuordnung wieder entfernen wollen, müssen Sie die betreffende Zeile mit der aktiven Zuordnung auswählen und dann auf den Befehl **Zuordnung entfernen** klicken. Klicken Sie in der angezeigten Bestätigungsfenster auf **Entfernen**.

Die NinjaOne-Integrationseinstellungen überprüfen und bearbeiten

Sie können Ihre NinjaOne-Integrationseinstellungen nach Bedarf überprüfen und bearbeiten. Sie können die NinjaOne-Integration außerdem auch löschen.

So können Sie die NinjaOne-Integrationseinstellungen überprüfen und bearbeiten

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**. Auf der Kachel **NinjaOne** können Sie den aktuellen Status der Integration einsehen.

3. Klicken Sie auf **Konfigurieren**, um die Integrationseinstellungen anzeigen und bearbeiten zu können.
   So können Sie beispielsweise die Anmeldedaten und Alarmeinstellungen auf der Registerkarte **Integrationseinstellungen** und die NinjaOne-Kunden, die der Advanced Automation zugeordnet sind, auf der Registerkarte **Kunden-Zuordnung** einsehen und bearbeiten.
4. Klicken Sie auf das Stiftsymbol, um den betreffenden Bereich zu bearbeiten. Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"Die NinjaOne-Integration einrichten" (S. 296)'.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie die NinjaOne-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dort **RMM/PSA** aus.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der rechten oberen Ecke der **NinjaOne**-Kachel auf das Drei-Punkte-Symbol (...), und wählen Sie dann den Befehl **Löschen**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Tickets aus offenen NinjaOne-Alarmmeldungen erstellen

Wenn die Integration mit NinjaOne konfiguriert ist (siehe Abschnitt '"Die NinjaOne-Integration einrichten" (S. 296)'), wird Advanced Automation automatisch neue Tickets aus offenen NinjaOne-Alarmmeldungen erstellen. Tickets bleiben mit NinjaOne synchronisiert, sodass gewährleistet ist, dass offene Alarme, die bereits mit Tickets in Advanced Automation verknüpft sind, ignoriert werden.

Beachten Sie Folgendes:

- Tickets werden nur für Kunden erstellt, die den NinjaOne-Kunden-Sites zugeordnet sind.
- Die Ticket-Parameter werden mit den Standardeinstellungen für den jeweiligen Kunden definiert (wie im Abschnitt '"Standardwerte festlegen" (S. 256)' beschrieben).
- Die Zusammenfassung und Beschreibung des Tickets wird aus der Zusammenfassung und Beschreibung des entsprechenden Alarms übernommen.
- Das Ticket enthält Links zum Cyber Protect Cloud-Kunden, zum Kundenbenutzer (über die E-Mail-Adresse des Benutzers, falls diese von NinjaOne bereitgestellt wird) und zu den mit dem Benutzer verknüpften Geräten (falls relevant; die Geräte können von den Benutzern in der Cyber Protect-Konsole eingesehen werden).
- Wenn ein Ticket mit dem Gerät eines Benutzers verknüpft ist, wird ein Link zum Bereich 'Geräteinformationen' in NinjaOne eingefügt.

Weitere Informationen über die Erstellung eines Tickets finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

Externe NinjaOne-Geräte zu Verträgen hinzufügen

Wenn die Integration mit NinjaOne konfiguriert ist (siehe Abschnitt '"Die NinjaOne-Integration einrichten" (S. 296)'), können Sie externe Geräte zu Verträgen für Kunden in Advanced Automation hinzufügen.

- Sie können einen bestimmten Vertragsteil mit der NinjaOne-Integration verknüpfen. Dies geschieht im Vertragsteilbereich eines Vertrags. Wählen Sie die relevante Integration, Gruppe/Site und den Workload-Typ aus und wählen Sie anschließend die relevanten Konfigurationselemente.
- Im Vertragsteilbereich eines Vertrages können Sie die Option **Automatisches Update** wählen, damit die Geräteanzahl für den Vertragsteil automatisch aktualisiert wird.
- Sie können auch die Option **Workloads auf der Rechnung anzeigen** wählen, damit den Kundenrechnungen auch Informationen über bestimmte Geräte hinzugefügt werden.

Weitere Informationen zum Definieren von Verträgen und Hinzufügen von Geräten zu Verträgen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.

Mit Datto RMM integrieren

Durch die Integration von Advanced Automation mit Datto RMM können Sie:

- Kunden-Sites und Geräte automatisch aus Datto RMM importieren.
- Kunden bestimmten Sites von Datto RMM zuordnen.
- Tickets aus Datto RMM-Alarmmeldungen erstellen.
- Auf die Datto RMM-Geräteseite aus einem Ticket heraus zugreifen.
- Von einem Ticket aus eine Remote-Verbindung zu einem Datto RMM-Gerät herstellen.
- Rechnungen für die tatsächliche Anzahl von Geräten, die Datto RMM nutzen, an die Kunden stellen.

Hinweis
Damit Datto RMM erfolgreich mit Advanced Automation integriert werden kann, muss der Advanced Automation Service aktiviert sein. Sie müssen außerdem ein vollständig konfiguriertes Datto RMM-Konto haben.

Die Datto RMM-Integration einrichten

Es gibt zwei Hauptschritte, wenn Sie Ihre Datto RMM-Integration mit Advanced Automation einrichten. Diese werden in den nachfolgenden Prozeduren beschrieben:

1. Die Integrationseinstellungen definieren, um eine Verbindung mit der Datto RMM-Instanz herzustellen.
2. Datto RMM-Kunden zu Advanced Automation zuordnen.

So können Sie die Integrationseinstellungen definieren

1. Gehen Sie im Management-Portal zu **Integrationen**. Wählen Sie in der angezeigten Integrationsliste den Eintrag **RMM/PSA**.
2. Klicken Sie auf der **Datto RMM**-Kachel auf **Konfigurieren**.
3. Geben Sie folgende Datto RMM-Anmeldedaten ein, um auf die Datto RMM-Instanz zugreifen zu können:
   - **Datto RMM-Server**: Geben Sie die URL des Datto RMM-Servers ein.
   - **API-Schlüssel**: Geben Sie den eindeutigen API-Schlüssel für Ihr Datto RMM-Konto ein.
   - **API-Geheimnis**: Geben Sie das eindeutige API-Geheimnis für Ihr Datto RMM-Konto ein.

     Alle oben genannten Anmeldedaten werden in Ihrem Datto RMM-Konto erstellt. Wenn Sie diese generieren wollen, müssen Sie sich zuerst an Ihrem Datto RMM-Konto anmelden. Gehen Sie zu **Setup –> Konto-Einstellungen –> Zugriffssteuerung**, und setzen Sie die Option **API-Zugriff aktivieren** auf **EIN**. Klicken Sie dann zuerst auf die Registerkarte **Benutzer** und anschließend auf den Benutzer, für den Sie den API-Zugriff aktivieren wollen. Kopieren Sie dann die angezeigte URL, den API-Schlüssel und das API-Geheimnis.
4. (Optional) Klicken Sie auf **Verbindung testen**, um die eingegebenen Anmeldedaten zu testen.
5. Klicken Sie auf **Weiter**.
6. Wenn Sie wollen, dass die Datto RMM-Alarmmeldungen automatisch mit den Tickets in Advanced Automation synchronisiert werden, müssen Sie sicherstellen, dass das Kontrollkästchen **Tickets aus Datto RMM-Alarmmeldungen erstellen** aktiviert ist (was standardmäßig der Fall ist).
7. Aktivieren Sie das Kontrollkästchen **Stummgeschaltete Alarmmeldungen ignorieren**, wenn Sie nicht wollen, dass Datto RMM-Alarme vom Typ 'stummgeschaltet' synchronisiert werden. Das Kontrollkästchen ist standardmäßig aktiviert.
8. Klicken Sie auf **Speichern**. Der nächste Schritt bei der Einrichtung Ihrer Integration besteht darin, die Datto RMM-Kunden bestehenden oder neuen Advanced Automation-Kunden zuzuordnen (siehe unten).

So können Sie Datto RMM-Kunden zuordnen

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf der **Datto RMM**-Kachel auf **Integration öffnen**.
3. Klicken Sie auf der Registerkarte **Kunden-Zuordnung** auf **Acronis Kunden aus Datto RMM-Sites erstellen**. Der Zuordnungsprozess wird für alle aufgeführten Datto RMM-Sites gestartet.

   Alle Kunden (Kunden-Sites) von Datto RMM werden als neue Kunden in Cyber Protect Cloud registriert, wobei alle verfügbaren Services gewährt werden.

   Sie können auch einzelne Datto RMM-Sites auswählen und diese bestehenden Cyber Protect Cloud-Kunden zuordnen. Wählen Sie dazu die entsprechende(n) Site(s) aus und klicken Sie anschließend auf **Vorhandenem Kunden-Mandanten zuordnen**. Sie werden dann aufgefordert, einen vorhandenen Kunden auszuwählen. Klicken Sie nach der Auswahl auf **Zuordnen**, um den Zuordnungsprozess abzuschließen.

4. Wenn dies abgeschlossen ist, wird in der Spalte **Zuordnung** der Status **Zugeordnet** und in der Spalte **Acronis Kunde** der entsprechende Kundenname angezeigt.

Hinweis
Wenn Sie eine Zuordnung wieder entfernen wollen, müssen Sie die betreffende Zeile mit der aktiven Zuordnung auswählen und dann auf den Befehl **Zuordnung entfernen** klicken. Klicken Sie in der angezeigten Bestätigungsfenster auf **Entfernen**.

Die Datto RMM-Integrationseinstellungen überprüfen und bearbeiten

Sie können Ihre Datto RMM-Integrationseinstellungen nach Bedarf überprüfen und bearbeiten. Sie können die Datto RMM-Integration außerdem auch löschen.

So können Sie die Datto RMM-Integrationseinstellungen überprüfen und bearbeiten

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**. Auf der **Datto RMM**-Kachel können Sie den aktuellen Status der Integration sowie die Anzahl der verknüpften Konten einsehen.
3. Klicken Sie auf **Integration öffnen**, um die Integrationseinstellungen anzeigen und bearbeiten zu können.
   So können Sie beispielsweise die Anmeldedaten und Alarmeinstellungen auf der Registerkarte **Integrationseinstellungen** und die Datto RMM-Kunden, die der Advanced Automation zugeordnet sind, auf der Registerkarte **Kunden-Zuordnung** einsehen und bearbeiten.
4. Klicken Sie auf das Stiftsymbol, um den betreffenden Bereich zu bearbeiten. Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"Die Datto RMM-Integration einrichten" (S. 299)'.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie die Datto RMM-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dort **RMM/PSA** aus.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der rechten oberen Ecke der **Datto RMM**-Kachel auf das Drei-Punkte-Symbol (...), und wählen Sie dann den Befehl **Löschen**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Tickets aus Datto RMM-Alarmmeldungen erstellen

Wenn die Integration mit Datto RMM konfiguriert ist (siehe Abschnitt '"Die Datto RMM-Integration einrichten" (S. 299)'), wird Advanced Automation automatisch neue Tickets aus Datto RMM-Alarmmeldungen erstellen. Tickets bleiben mit Datto RMM synchronisiert, sodass gewährleistet ist, dass offene Alarme, die bereits mit Tickets in Advanced Automation verknüpft sind, ignoriert werden.

Beachten Sie Folgendes:

- Tickets werden nur für Kunden erstellt, die den Datto RMM-Kunden-Sites zugeordnet sind.
- Die Ticket-Parameter werden mit den Standardeinstellungen für den jeweiligen Kunden definiert (wie im Abschnitt '"Standardwerte festlegen" (S. 256)' beschrieben).
- Die Zusammenfassung und Beschreibung des Tickets wird aus der Zusammenfassung und Beschreibung des entsprechenden Alarms übernommen.
- Das Ticket enthält Links zum Cyber Protect Cloud-Kunden, zum Kundenbenutzer (über die E-Mail-Adresse des Benutzers, falls diese von Datto RMM bereitgestellt wird) und zu den mit dem Benutzer verknüpften Geräten (falls relevant; die Geräte können von den Benutzern in der Cyber Protect-Konsole eingesehen werden).
- Wenn ein Ticket mit dem Gerät eines Benutzers verknüpft ist, wird ein Link zum Bereich 'Geräteinformationen' in Datto RMM eingefügt. Außerdem wird, sofern von Datto RMM angeboten, ein Link zur Initiierung einer Remote-Verbindung eingefügt.

Weitere Informationen über die Erstellung eines Tickets finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

Externe Datto RMM-Geräte zu Verträgen hinzufügen

Wenn die Integration mit Datto RMM konfiguriert ist (siehe Abschnitt '"Die Datto RMM-Integration einrichten" (S. 299)'), können Sie externe Geräte zu Verträgen für Kunden in Advanced Automation hinzufügen.

- Sie können einen bestimmten Vertragsteil mit der Datto RMM-Integration verknüpfen. Dies geschieht im Vertragsteilbereich eines Vertrags. Wählen Sie die relevante Integration, Gruppe/Site und den Workload-Typ aus und wählen Sie anschließend die relevanten Konfigurationselemente.
- Im Vertragsteilbereich eines Vertrages können Sie die Option **Automatisches Update** wählen, damit die Geräteanzahl für den Vertragsteil automatisch aktualisiert wird.
- Sie können auch die Option **Workloads auf der Rechnung anzeigen** wählen, damit den Kundenrechnungen auch Informationen über bestimmte Geräte hinzugefügt werden.

Weitere Informationen zum Definieren von Verträgen und Hinzufügen von Geräten zu Verträgen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.

Mit Kaseya VSA integrieren

Durch die Integration von Advanced Automation mit Kaseya VSA (unter Verwendung des existierenden Cyber Protect-Plug-ins) können Sie:

- Kunden-Sites und Geräte automatisch aus Kaseya VSA importieren.
- Kunden bestimmten Sites von Kaseya VSA zuordnen.
- Tickets aus Kaseya VSA-Alarmmeldungen erstellen.
- Auf die Kaseya VSA-Geräteseite aus einem Ticket heraus zugreifen.
- Von einem Ticket aus eine Remote-Verbindung zu einem Kaseya VSA-Gerät herstellen.

- Rechnungen für die tatsächliche Anzahl von Geräten, die Kaseya VSA nutzen, an die Kunden stellen.

Hinweis
Damit Kaseya VSA erfolgreich mit Advanced Automation integriert werden kann, muss der Advanced Automation Service aktiviert sein. Weitere Informationen zur Verwendung des existierenden Cyber Protect-Plug-Ins für Kaseya VSA finden Sie in dieser Anleitung.

Mit N-able N-central integrieren

Durch die Integration von Advanced Automation mit N-able N-central können Sie:

- Kunden-Sites und Geräte automatisch aus N-able N-central importieren.
- Kunden bestimmten Sites von N-able N-central zuordnen.
- Tickets aus N-able N-central-Alarmmeldungen erstellen.
- Tickets zwischen Advanced Automation und N-able N-central synchronisieren.
- Auf die N-able N-central-Geräteseite aus einem Ticket heraus zugreifen.
- Rechnungen für die tatsächliche Anzahl von Geräten von N-able N-central an die Kunden stellen.

Hinweis
Damit N-able N-central erfolgreich mit Advanced Automation integriert werden kann, muss der Advanced Automation Service aktiviert sein. Sie müssen außerdem ein vollständig konfiguriertes N-able N-central-Konto haben.

So können Sie die N-able N-central-Integration einrichten

Es gibt zwei Hauptschritte, wenn Sie Ihre N-able N-central-Integration mit Advanced Automation einrichten. Diese werden in den nachfolgenden Prozeduren beschrieben:

1. Die Integrationseinstellungen definieren, um eine Verbindung mit der N-able N-central-Instanz herzustellen.
2. N-able N-central-Kunden zu Advanced Automation zuordnen.

So können Sie die Integrationseinstellungen definieren

1. Gehen Sie im Management-Portal zu **Integrationen**. Wählen Sie in der angezeigten Integrationsliste den Eintrag **RMM/PSA**.
2. Klicken Sie auf der **N-able N-central**-Kachel auf **Konfigurieren**.
3. Geben Sie die folgenden N-able N-central-Anmeldedaten ein, um auf die N-able N-central-Instanz zugreifen zu können:
   - URL
   - Benutzername
   - Kennwort

4. (Optional) Klicken Sie auf **Verbindung testen**, um die eingegebenen Anmeldedaten zu testen.
5. Klicken Sie auf **Weiter**.
6. Wenn Sie wollen, dass die N-able N-central-Alarmmeldungen automatisch mit den Tickets in Advanced Automation synchronisiert werden, müssen Sie sicherstellen, dass das Kontrollkästchen **Ticket-Integration** aktiviert ist (was standardmäßig der Fall ist).
7. Klicken Sie auf **Speichern**. Der nächste Schritt bei der Einrichtung Ihrer Integration besteht darin, die N-able N-central-Kunden bestehenden oder neuen Advanced Automation-Kunden zuzuordnen (siehe unten).

So können Sie N-able N-central Kunden zuordnen

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf der **N-able N-central**-Kachel auf **Konfigurieren**.
3. Klicken Sie auf der Registerkarte **Kunden-Zuordnung** auf **Acronis Kunden aus N-able N-central-Sites erstellen**. Der Zuordnungsprozess wird für alle aufgeführten N-able N-central-Sites gestartet.

   Alle Kunden (Kunden-Sites) von N-able N-central werden als neue Kunden in Cyber Protect Cloud registriert, wobei alle verfügbaren Services gewährt werden.

   Sie können auch einzelne N-able N-central-Sites auswählen und diese bestehenden Cyber Protect Cloud-Kunden zuordnen. Wählen Sie dazu die entsprechende(n) Site(s) aus und klicken Sie anschließend auf **Vorhandenem Kunden-Mandanten zuordnen**. Sie werden dann aufgefordert, einen vorhandenen Kunden auszuwählen. Klicken Sie nach der Auswahl auf **Zuordnen**, um den Zuordnungsprozess abzuschließen.
4. Wenn dies abgeschlossen ist, wird in der Spalte **Zuordnung** der Status **Zugeordnet** und in der Spalte **Acronis Kunde** der entsprechende Kundenname angezeigt.

Hinweis
Wenn Sie eine Zuordnung wieder entfernen wollen, müssen Sie die betreffende Zeile mit der aktiven Zuordnung auswählen und dann auf den Befehl **Zuordnung entfernen** klicken. Klicken Sie in der angezeigten Bestätigungsfenster auf **Entfernen**.

Die N-able N-central-Integrationseinstellungen überprüfen und bearbeiten

Sie können Ihre N-able N-central-Integrationseinstellungen nach Bedarf überprüfen und bearbeiten. Sie können die N-able N-central-Integration außerdem auch löschen.

So können Sie die N-able N-central-Integrationseinstellungen überprüfen und bearbeiten

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**. Auf der **N-able N-central**-Kachel können Sie den aktuellen Status der Integration sowie die Anzahl der verknüpften Konten einsehen.
3. Klicken Sie auf **Konfigurieren**, um die Integrationseinstellungen anzeigen und bearbeiten zu können.

So können Sie beispielsweise die Anmeldedaten und Alarmeinstellungen auf der Registerkarte **Integrationseinstellungen** und die N-able N-central-Kunden, die der Advanced Automation zugeordnet sind, auf der Registerkarte **Kunden-Zuordnung** einsehen und bearbeiten.

4. Klicken Sie auf das Stiftsymbol, um den betreffenden Bereich zu bearbeiten. Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"So können Sie die N-able N-central-Integration einrichten" (S. 303)'.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie die N-able N-central-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dort **RMM/PSA** aus.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der rechten oberen Ecke der **N-able N-central**-Kachel auf das Drei-Punkte-Symbol (...), und wählen Sie dann den Befehl **Löschen**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Tickets aus N-able N-central-Alarmmeldungen erstellen

Wenn die Integration mit N-able N-central konfiguriert ist (siehe Abschnitt '"So können Sie die N-able N-central-Integration einrichten" (S. 303)'), wird Advanced Automation automatisch neue Tickets aus N-able N-central-Alarmmeldungen erstellen. Tickets bleiben mit N-able N-central synchronisiert, sodass gewährleistet ist, dass offene Alarme, die bereits mit Tickets in Advanced Automation verknüpft sind, ignoriert werden.

Beachten Sie Folgendes:

- Tickets werden nur für Kunden erstellt, die den N-able N-central-Kunden-Sites zugeordnet sind.
- Die Ticket-Parameter werden mit den Standardeinstellungen für den jeweiligen Kunden definiert (wie im Abschnitt '"Standardwerte festlegen" (S. 256)' beschrieben).
- Die Zusammenfassung und Beschreibung des Tickets wird aus der Zusammenfassung und Beschreibung des entsprechenden Alarms übernommen.
- Das Ticket enthält Links zum Cyber Protect Cloud-Kunden, zum Kundenbenutzer (über die E-Mail-Adresse des Benutzers, falls diese von N-able N-central bereitgestellt wird) und zu den mit dem Benutzer verknüpften Geräten (falls relevant; die Geräte können von den Benutzern in der Cyber Protect-Konsole eingesehen werden).
- Wenn ein Ticket mit dem Gerät eines Benutzers verknüpft ist, wird ein Link zum Bereich 'Geräteinformationen' in N-able N-central eingefügt.

Weitere Informationen über die Erstellung eines Tickets finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

Externe N-able N-central-Geräte zu Verträgen hinzufügen

Wenn die Integration mit N-able N-central konfiguriert ist (siehe Abschnitt '"So können Sie die N-able N-central-Integration einrichten" (S. 303)'), können Sie externe Geräte zu Verträgen für Kunden in Advanced Automation hinzufügen.

- Sie können einen bestimmten Vertragsteil mit der N-able N-central-Integration verknüpfen. Dies geschieht im Vertragsteilbereich eines Vertrags. Wählen Sie die relevante Integration, Gruppe/Site und den Workload-Typ aus und wählen Sie anschließend die relevanten Konfigurationselemente.
- Im Vertragsteilbereich eines Vertrages können Sie die Option **Automatisches Update** wählen, damit die Geräteanzahl für den Vertragsteil automatisch aktualisiert wird.
- Sie können auch die Option **Workloads auf der Rechnung anzeigen** wählen, damit den Kundenrechnungen auch Informationen über bestimmte Geräte hinzugefügt werden.

Weitere Informationen zum Definieren von Verträgen und Hinzufügen von Geräten zu Verträgen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.

Mit N-able RMM integrieren

Durch die Integration von Advanced Automation mit N-able RMM können Sie:

- Kunden-Sites und Geräte automatisch aus N-able RMM importieren.
- Kunden bestimmten Sites von N-able RMM zuordnen.
- Tickets aus N-able RMM-Alarmmeldungen erstellen.
- Rechnungen für die tatsächliche Anzahl von Geräten von N-able RMM an die Kunden stellen.

Hinweis
Damit N-able RMM erfolgreich mit Advanced Automation integriert werden kann, muss der Advanced Automation Service aktiviert sein. Sie müssen außerdem ein vollständig konfiguriertes N-able RMM-Konto haben.

So können Sie die N-able RMM-Integration einrichten

Es gibt zwei Hauptschritte, wenn Sie Ihre N-able RMM-Integration mit Advanced Automation einrichten. Diese werden in den nachfolgenden Prozeduren beschrieben:

1. Die Integrationseinstellungen definieren, um eine Verbindung mit der N-able RMM-Instanz herzustellen.
2. N-able RMM-Kunden zu Advanced Automation zuordnen.

So können Sie die Integrationseinstellungen definieren

1. Gehen Sie im Management-Portal zu **Integrationen**. Wählen Sie in der angezeigten Integrationsliste den Eintrag **RMM/PSA**.
2. Klicken Sie auf der **N-able RMM**-Kachel auf **Konfigurieren**.
3. Geben Sie folgende N-able RMM-Anmeldedaten ein, um auf die N-able RMM-Instanz zugreifen zu können:
   - URL
   - API-Schlüssel
4. (Optional) Klicken Sie auf **Verbindung testen**, um die eingegebenen Anmeldedaten zu testen.

5. Klicken Sie auf **Weiter**.
6. Wenn Sie wollen, dass die N-able RMM-Alarmmeldungen automatisch mit den Tickets in Advanced Automation synchronisiert werden, müssen Sie sicherstellen, dass das Kontrollkästchen **Ticket-Integration** aktiviert ist (was standardmäßig der Fall ist).
7. Klicken Sie auf **Speichern**. Der nächste Schritt bei der Einrichtung Ihrer Integration besteht darin, die N-able RMM-Kunden bestehenden oder neuen Advanced Automation-Kunden zuzuordnen (siehe unten).

So können Sie N-able RMM Kunden zuordnen

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf der **N-able RMM**-Kachel auf **Konfigurieren**.
3. Klicken Sie auf der Registerkarte **Kunden-Zuordnung** auf **Acronis Kunden aus N-able RMM-Sites erstellen**. Der Zuordnungsprozess wird für alle aufgeführten N-able RMM-Sites gestartet.
   Alle Kunden (Kunden-Sites) von N-able RMM werden als neue Kunden in Cyber Protect Cloud registriert, wobei alle verfügbaren Services gewährt werden.
   Sie können auch einzelne N-able RMM-Sites auswählen und diese bestehenden Cyber Protect Cloud-Kunden zuordnen. Wählen Sie dazu die entsprechende(n) Site(s) aus und klicken Sie anschließend auf **Vorhandenem Kunden-Mandanten zuordnen**. Sie werden dann aufgefordert, einen vorhandenen Kunden auszuwählen. Klicken Sie nach der Auswahl auf **Zuordnen**, um den Zuordnungsprozess abzuschließen.
4. Wenn dies abgeschlossen ist, wird in der Spalte **Zuordnung** der Status **Zugeordnet** und in der Spalte **Acronis Kunde** der entsprechende Kundenname angezeigt.

Hinweis
Wenn Sie eine Zuordnung wieder entfernen wollen, müssen Sie die betreffende Zeile mit der aktiven Zuordnung auswählen und dann auf den Befehl **Zuordnung entfernen** klicken. Klicken Sie in der angezeigten Bestätigungsfenster auf **Entfernen**.

Die N-able RMM-Integrationseinstellungen überprüfen und bearbeiten

Sie können Ihre N-able RMM-Integrationseinstellungen nach Bedarf überprüfen und bearbeiten. Sie können die N-able RMM-Integration außerdem auch löschen.

So können Sie die N-able RMM-Integrationseinstellungen überprüfen und bearbeiten

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **RMM/PSA**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**. Auf der **N-able RMM**-Kachel können Sie den aktuellen Status der Integration sowie die Anzahl der verknüpften Konten einsehen.
3. Klicken Sie auf **Konfigurieren**, um die Integrationseinstellungen anzeigen und bearbeiten zu können.

So können Sie beispielsweise die Anmeldedaten und Alarmeinstellungen auf der Registerkarte **Integrationseinstellungen** und die N-able RMM-Kunden, die der Advanced Automation zugeordnet sind, auf der Registerkarte **Kunden-Zuordnung** einsehen und bearbeiten.

4. Klicken Sie auf das Stiftsymbol, um den betreffenden Bereich zu bearbeiten. Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"So können Sie die N-able RMM-Integration einrichten" (S. 306)'.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie die N-able RMM-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dort **RMM/PSA** aus.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der rechten oberen Ecke der **N-able RMM**-Kachel auf das Drei-Punkte-Symbol (...), und wählen Sie dann den Befehl **Löschen**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Tickets aus N-able RMM-Alarmmeldungen erstellen

Wenn die Integration mit N-able RMM konfiguriert ist (siehe Abschnitt '"So können Sie die N-able RMM-Integration einrichten" (S. 306)'), wird Advanced Automation automatisch neue Tickets aus N-able RMM-Alarmmeldungen erstellen. Tickets bleiben mit N-able RMM synchronisiert, sodass gewährleistet ist, dass offene Alarme, die bereits mit Tickets in Advanced Automation verknüpft sind, ignoriert werden.

Beachten Sie Folgendes:

- Tickets werden nur für Kunden erstellt, die den N-able RMM-Kunden-Sites zugeordnet sind.
- Die Ticket-Parameter werden mit den Standardeinstellungen für den jeweiligen Kunden definiert (wie im Abschnitt '"Standardwerte festlegen" (S. 256)' beschrieben).
- Die Zusammenfassung und Beschreibung des Tickets wird aus der Zusammenfassung und Beschreibung des entsprechenden Alarms übernommen.
- Das Ticket enthält Links zum Cyber Protect Cloud-Kunden, zum Kundenbenutzer (über die E-Mail-Adresse des Benutzers, falls diese von N-able RMM bereitgestellt wird) und zu den mit dem Benutzer verknüpften Geräten (falls relevant; die Geräte können von den Benutzern in der Cyber Protect-Konsole eingesehen werden).
- Wenn ein Ticket mit dem Gerät eines Benutzers verknüpft ist, wird ein Link zum Bereich 'Geräteinformationen' in N-able RMM eingefügt.

Weitere Informationen über die Erstellung eines Tickets finden Sie im Abschnitt '"Ein neues Ticket erstellen" (S. 197)'.

Externe N-able RMM-Geräte zu Verträgen hinzufügen

Wenn die Integration mit N-able RMM konfiguriert ist (siehe Abschnitt '"So können Sie die N-able RMM-Integration einrichten" (S. 306)'), können Sie externe Geräte zu Verträgen für Kunden in Advanced Automation hinzufügen.

- Sie können einen bestimmten Vertragsteil mit der N-able RMM-Integration verknüpfen. Dies geschieht im Vertragsteilbereich eines Vertrags. Wählen Sie die relevante Integration, Gruppe/Site und den Workload-Typ aus und wählen Sie anschließend die relevanten Konfigurationselemente.
- Im Vertragsteilbereich eines Vertrages können Sie die Option **Automatisches Update** wählen, damit die Geräteanzahl für den Vertragsteil automatisch aktualisiert wird.
- Sie können auch die Option **Workloads auf der Rechnung anzeigen** wählen, damit den Kundenrechnungen auch Informationen über bestimmte Geräte hinzugefügt werden.

Weitere Informationen zum Definieren von Verträgen und Hinzufügen von Geräten zu Verträgen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.

Mit VAR-Plattformen integrieren

Hinweis
Diese Funktion ist nur für Benutzer verfügbar, denen die Administrator-Rolle zugewiesen wurde.

Advanced Automation ermöglicht Ihnen eine Integration mit VAR-Plattformen (Value Added Reseller), wobei zurzeit nur Microsoft CSP unterstützt wird. Dadurch können Sie auf die Abonnement-Nutzungsdaten Ihrer Kunden von Drittanbietern zugreifen und bei Bedarf wiederum Ihre Kunden in Advanced Automation nachverfolgen, fakturieren und diesen Rechnungen stellen.

Wenn Sie auf die VAR-Integrationen zugreifen wollen, gehen Sie zu **Integrationen**. Wählen Sie im links angezeigten Menü den Eintrag **Cloud-Anbieter**.

Mit Microsoft CSP integrieren

Durch die Integration von Advanced Automation mit Microsoft CSP können Sie:

- Kunden automatisch aus dem Microsoft CSP Partner Portal importieren.
- Abonnements und deren Nutzungsdaten automatisch aus dem Microsoft CSP Partner Portal importieren.
- Rechnungen für die tatsächliche Nutzung von Microsoft CSP-Abonnements an die Kunden stellen.

Damit Microsoft CSP erfolgreich mit Advanced Automation integriert werden kann, muss der Advanced Automation Service aktiviert sein. Sie müssen außerdem ein vollständig konfiguriertes Microsoft CSP-Konto haben.

Beachten Sie, dass Microsoft zwei grundlegende Partnerstufen hat, über die Service Provider die Microsoft CSP-Services und -Lizenzen an Endkunden weiterverkaufen können: Tier-1 und Tier-2.

- Tier-1 bezieht sich auf Partner, die direkt von Microsoft kaufen. So sind beispielsweise alle Distributoren, die Abonnements für das Microsoft CSP-Programm verkaufen, Tier-1-Partner.
- Tier-2 bezieht sich auf Partner, die Abonnements für das Microsoft CSP-Programm von einem Distributor (Tier-1-Partner) erwerben.

Die Partner verwalten ihre Microsoft CSP-Services und -Lizenzen in einer zentralen Konsole, dem Microsoft Partner-Portal, unabhängig davon, wo sie die Services und Lizenzen erworben haben.

Hinweis
Derzeit unterstützt Advanced Automation nur Tier-1-Partner.

So können Sie die Integrationseinstellungen definieren

1. Gehen Sie im Management-Portal zu **Integrationen**. Wählen Sie in der angezeigten Integrationsliste den Eintrag **Cloud-Anbieter**.
2. Klicken Sie in der **Microsoft CSP**-Kachel auf **Aktivieren**.
3. Geben Sie folgende Microsoft CSP-Anmeldedaten ein, um auf das Microsoft CSP-Konto zugreifen zu können:
   - **App-ID**: Geben Sie die eindeutige App-ID für Ihr Microsoft CSP-Konto ein.
   - **Geheimschlüssel**: Geben Sie dein eindeutige Geheimschlüssel für Ihr Microsoft CSP-Konto ein. Der Geheimschlüssel wird zusammen mit der App-ID generiert (siehe oben).
   - **Domain**: Geben Sie die relevante Domain ein.
4. (Optional) Klicken Sie auf **Verbindung testen**, um die eingegebenen Anmeldedaten zu testen.
5. Klicken Sie auf **Speichern**.
   Nachdem Sie die Integration definiert haben, können Sie einen Vertragsteil definieren (siehe Abschnitt '"Einen neuen Vertrag erstellen" (S. 226)') und einen Kunden aus Microsoft CSP auswählen, um die korrekten Nutzungsdaten von dem betreffenden Kunden abzurufen.

Die Microsoft CSP-Integrationseinstellungen überprüfen und bearbeiten

Sie können Ihre Microsoft CSP-Integrationseinstellungen nach Bedarf überprüfen und bearbeiten. Sie können die Microsoft CSP-Integration außerdem auch löschen.

So können Sie die Microsoft CSP-Integrationseinstellungen überprüfen und bearbeiten

1. Gehen Sie im Management-Portal zu **Integrationen** und wählen Sie dann **Cloud-Anbieter**.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**. Auf der Kachel **Microsoft CSP** können Sie den aktuellen Status der Integration einsehen.
3. Klicken Sie auf **Konfigurieren**, um die Integrationseinstellungen anzeigen und bearbeiten zu können.
4. Klicken Sie auf das Stiftsymbol, um das betreffende Feld zu bearbeiten. Weitere Informationen über die bearbeitbaren Felder finden Sie im Abschnitt '"Mit Microsoft CSP integrieren" (S. 309)'.
5. Klicken Sie, wenn Sie fertig sind, auf ✓.

So können Sie die Microsoft CSP-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dort **Cloud-Anbieter** aus.
2. Klicken Sie auf die Registerkarte **Verwendete Integrationen**.
3. Klicken Sie in der rechten oberen Ecke der **Microsoft CSP**-Kachel auf das Drei-Punkte-Symbol (...), und wählen Sie dann den Befehl **Löschen**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

Microsoft CSP-Nutzungsdaten in Verträgen verwenden

Wenn die Integration mit Microsoft CSP konfiguriert ist (siehe Abschnitt '"Mit Microsoft CSP integrieren" (S. 309)'), können Sie Microsoft CSP-Nutzungsdaten zu Verträgen für Kunden in Advanced Automation hinzufügen.

Beachten Sie Folgendes:

- Sie können einen bestimmten Vertragsteil mit der Microsoft CSP-Integration verknüpfen.
- Sie können Lizenztypen aus Microsoft CSP nach folgenden Kriterien filtern:
  - **VAR-Gruppe**: Wählen Sie den relevanten Kunden aus der Kundenliste auf dem Microsoft CSP Partner Portal aus, um die Lizenzen herauszufiltern, die sich nur auf einen bestimmten Kunden beziehen.
  - **Lizenztyp**: Wählen Sie aus den verfügbaren Lizenztypen aus dem Microsoft CSP Partner Portal aus.
- Das Kontrollkästchen **Automatisches Update** im Bereich **Vertragsteile** des Assistenten zum Erstellen eines Vertrags ist standardmäßig aktiviert und ausgeblendet: es deaktiviert automatisch das Feld **Anzahl**. Wenn diese Option konfiguriert ist, wird Advanced Automation die tatsächlichen Nutzungsdaten mit diesem Feld synchronisieren, so dass Sie die tatsächliche Lizenznutzung abrechnen können.

Weitere Informationen über das Definieren von Verträgen finden Sie im Abschnitt '"Mit Verträgen arbeiten" (S. 226)'.

Hinweis
Wenn Sie eine Rechnung für einen Kunden mit Microsoft CSP-Lizenznutzung generieren, wird diese automatisch die entsprechenden Zeilen für die verwendeten Lizenztypen mit der richtigen Anzahl und dem richtigen Preis enthalten.

Mit Zahlungsplattformen integrieren

Advanced Automation ermöglicht Ihnen eine Integration mit verschiedenen Zahlungsplattformen, wobei zurzeit nur PayPal und Stripe unterstützt werden. Dadurch können Sie Rechnungen mit Links versenden, auf die die Kunden klicken können, um über die jeweilige Plattform ihre Zahlung vorzunehmen.

Wenn Sie auf die Integration für die Zahlungsplattform zugreifen wollen, gehen Sie zu **Integrationen**. Wählen Sie im links angezeigten Menü den Eintrag **Zahlungen**.

Mit PayPal integrieren

Durch die Integration von Advanced Automation mit dem PayPal Payment Gateway können Sie die Einziehung und Nachverfolgung von Kundenzahlungen automatisieren.

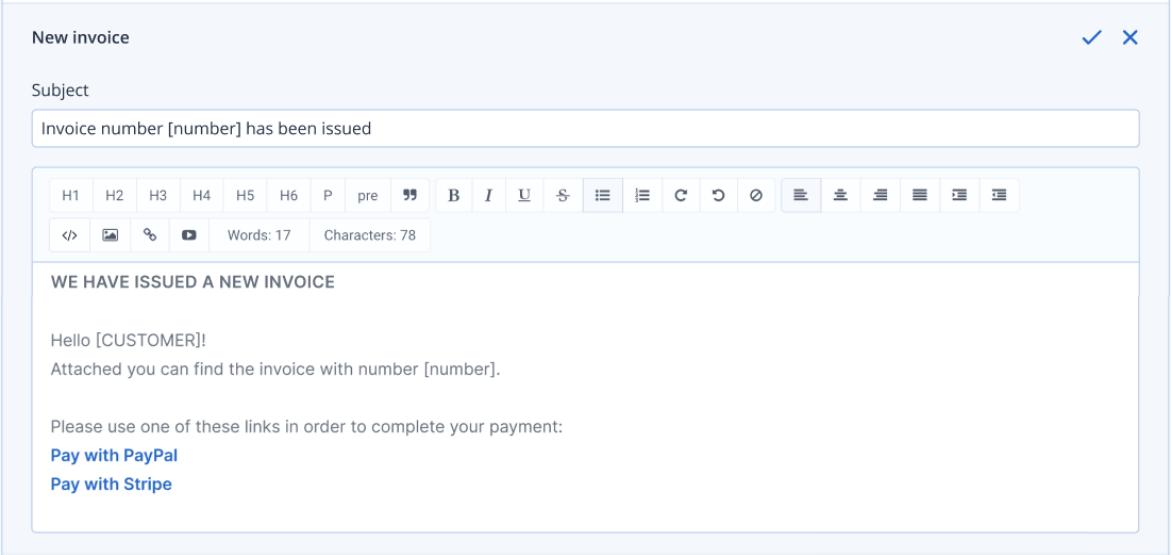
Informationen über weitere Zahlungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Zahlungsplattformen integrieren" (S. 311)'.

So können Sie PayPal integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Zahlungen**.
2. Klicken Sie in der PayPal-Kachel auf **Aktivieren**.
3. Geben Sie die folgenden PayPal-Anmeldedaten ein:
   - API-Benutzername
   - API-Kennwort
   - Signatur

   Weitere Informationen darüber, wie Sie die oben genannten Anmeldedaten von PayPal erhalten, finden Sie im Abschnitt '"So können Sie auf Ihren PayPal-API-Informationen für Benutzername, Kennwort und Signatur zugreifen" (S. 313)'.
4. Klicken Sie auf **Speichern**.

   Sie können jetzt (wie unten gezeigt) in den Rechnungen, die Sie an Ihre Kunden senden, einen Link zur Zahlung per PayPal einfügen. Weitere Informationen darüber, wie Sie diesen Link in der E-Mail-Vorlage 'Neue Rechnung' definieren können, finden Sie im Abschnitt '"E-Mail-Vorlagen verwalten" (S. 259)'.



So können Sie die PayPal-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Zahlungen**.
2. Klicken Sie in der PayPal-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann **Einstellungen**.
3. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre PayPal-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Zahlungen**.
2. Klicken Sie in der PayPal-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl

Löschen.

3. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

So können Sie auf Ihren PayPal-API-Informationen für Benutzername, Kennwort und Signatur zugreifen

Um Advanced Automation mit PayPal integrieren zu können (siehe Abschnitt '"Mit PayPal integrieren" (S. 311)'), müssen Sie den API-Benutzernamen, das API-Kennwort und die API-Signatur Ihres PayPal-Kontos in den Integrationseinstellungen festlegen. Diese Anmeldedaten finden Sie (wie unten erläutert) in den Einstellungen Ihres PayPal-Kontos.

So können Sie auf Ihren PayPal-API-Informationen für Benutzername, Kennwort und Signatur abrufen

1. Melden Sie sich an Ihrem PayPal-Konto an.
2. Gehen Sie über das Hauptmenü zu **Tools > Alle Tools**.
3. Scrollen Sie auf der Seite nach unten und klicken Sie auf **API-Anmeldedaten**.
4. Klicken Sie auf **NVP/SOAP-Integration**.

   Hinweis
   Wenn Sie zum ersten Mal die API-Anmeldedaten erstellen, wird unter der NVP/SOAP API-Integration ein Link namens **API-Berechtigung anfordern** angezeigt. Füllen Sie das Antragsformular für API-Anmeldedaten aus, aktivieren Sie das Kontrollkästchen für die Zustimmung und klicken Sie dann auf **Übermitteln**.

5. Klicken Sie bei jeder Entität auf den Link **Anzeigen** und notieren Sie sich die angezeigten Anmeldedaten. Diese können Sie dann bei der Definition Ihrer Integrationseinstellungen verwenden, wie im Abschnitt '"Mit PayPal integrieren" (S. 311)' beschrieben.

Mit Strip integrieren

Durch die Integration von Advanced Automation mit dem Stripe Payment Gateway können Sie die Einziehung und Nachverfolgung von Kundenzahlungen automatisieren.

Informationen über weitere Zahlungsplattformen, die mit dem Advanced Automation Service integriert werden können, finden Sie im Abschnitt '"Mit Zahlungsplattformen integrieren" (S. 311)'.

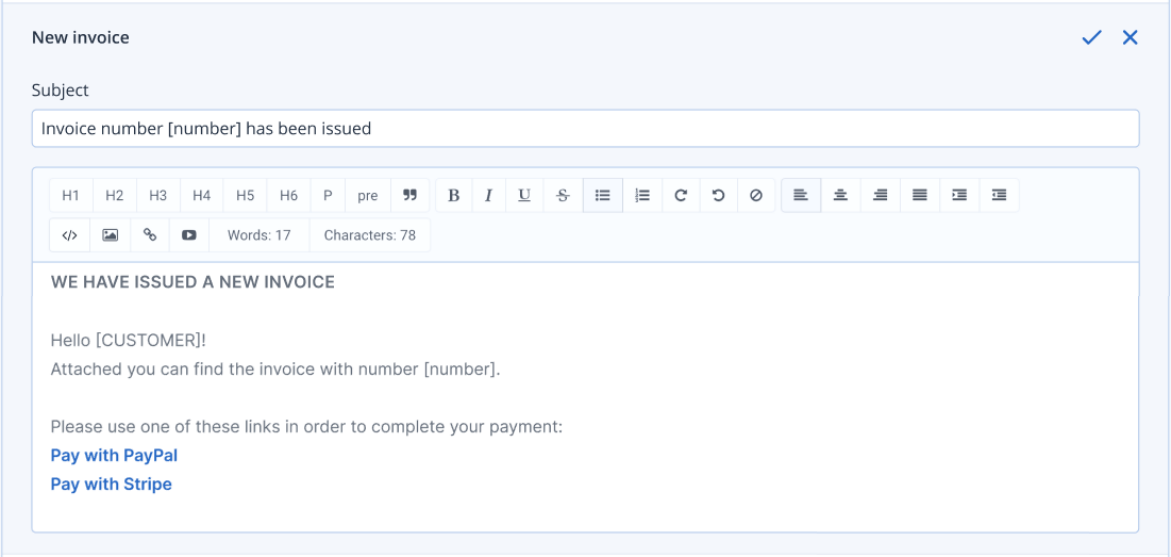
So können Sie Stripe integrieren

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Zahlungen**.
2. Klicken Sie in der Stripe-Kachel auf **Aktivieren**.
3. Geben Sie die folgenden Stripe-Anmeldedaten ein:
   - Geheimschlüssel
   - Veröffentlichbarer Schlüssel

Weitere Informationen darüber, wie Sie die oben genannten Anmeldedaten von Stripe abrufen können, finden Sie im Abschnitt '"So können Sie auf Ihre Geheim- und veröffentlichbaren Schlüssel von Stripe zugreifen" (S. 314)'.

4. Klicken Sie auf **Speichern**.

   Sie können jetzt (wie unten gezeigt) in den Rechnungen, die Sie an Ihre Kunden senden, einen Link zur Zahlung per Stripe einfügen. Weitere Informationen darüber, wie Sie diesen Link in der E-Mail-Vorlage 'Neue Rechnung' definieren können, finden Sie im Abschnitt '"E-Mail-Vorlagen verwalten" (S. 259)'.



So können Sie die Stripe-Integrationseinstellungen ändern

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Zahlungen**.
2. Klicken Sie in der Stripe-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann **Einstellungen**.
3. Ändern Sie die Einstellungen nach Bedarf (siehe oben).

So können Sie Ihre Stripe-Integration löschen

1. Gehen Sie zu **Integrationen** und wählen Sie dann die Registerkarte **Zahlungen**.
2. Klicken Sie in der Stripe-Kachel auf das Drei-Punkte-Symbol (...) und wählen Sie dann den Befehl **Löschen**.
3. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Löschen**.

So können Sie auf Ihre Geheim- und veröffentlichbaren Schlüssel von Stripe zugreifen

Um Advanced Automation mit PayPal integrieren zu können (siehe Abschnitt '"Mit Strip integrieren" (S. 313)'), müssen Sie den Geheim- und den veröffentlichbaren Schlüssel von Stripe in den Integrationseinstellungen definieren. Diese Anmeldedaten finden Sie (wie unten erläutert) in den Einstellungen Ihres Stripe-Kontos.

So können Sie Ihre Geheim- und veröffentlichbaren Schlüssel von Stripe abrufen

1. Melden Sie sich an Ihrem Stripe-Konto an.
2. Gehen Sie zu **Entwickler –> API-Schlüssel**.
3. Wenn Sie Ihren Geheimschlüssel zum ersten Mal abrufen, müssen Sie auf **Test-Schlüsseltocken einblenden** klicken, damit der Schlüssel generiert wird.
4. Notieren Sie sich die angezeigten Anmeldedaten. Diese können Sie dann bei der Definition Ihrer Integrationseinstellungen verwenden, wie im Abschnitt '"Mit Strip integrieren" (S. 313)' beschrieben.

Den Advanced Automation Service kündigen

Sie können den Advanced Automation Service kündigen, wenn Sie die in Advanced Automation enthaltenen Funktionalitäten nicht mehr verwenden wollen.

Wichtig
Wenn Sie den Advanced Automation Service kündigen, werden alle Advanced Automation-Daten entfernt und können nicht wiederhergestellt werden.

So können Sie den Advanced Automation Service kündigen

1. Klicken Sie im Management-Portal auf **Einstellungen –> Abrechnung und Angebotserstellung**.
2. Klicken Sie auf die Registerkarte **Mein Abonnement**.
   Die angezeigte Registerkarte enthält Details über die Anzahl der aktuellen Advanced Automation-Benutzer.
3. Klicken Sie auf **Advanced Automation Service kündigen**.
4. Klicken Sie in der angezeigten Bestätigungsmeldung auf **Bestätigen**.

Integrationen

Integration in Drittanbieter-Systeme

Ein Service-Provider kann Cyber Protect Cloud folgendermaßen in ein Drittherstellersystem integrieren:

- Durch Einrichten einer Plattform-Erweiterung in diesem System.

  Im Management-Portal auf der Seite **Integration** finden Sie eine Liste von Erweiterungen, die für gängige PSA- (Professional Services Automations) und RMM-Systeme (Remote Monitoring and Management) verfügbar sind.

  Das ist die empfohlene Vorgehensweise, um die Plattform zu integrieren.
- Durch Erstellen eines API-Clients für das System. Dadurch wird es dem Drittherstellersystem ermöglicht, auf die APIs (Application Programming Interfaces) der Plattform und deren Services zuzugreifen. API-Clients sind Bestandteil des OAuth 2.0-Autorisierungsframeworks der Plattform. Weitere Informationen über OAuth 2.0 finden Sie unter der Adresse https://tools.ietf.org/html/rfc6749.

  Dies ist eine Low-Level-Methode zur Integration der Plattform, für die Programmierkenntnisse erforderlich sind. Wir empfehlen diese Möglichkeit, wenn es für das System keine Plattform-Erweiterung gibt – oder wenn die Integration des Systems für Einsatzzwecke angepasst werden soll, in denen die Plattform und deren Services so verwaltet werden sollen, wie es mit der verfügbaren Erweiterung nicht möglich ist.

Eine Integration für Cyber Protect Cloud einrichten

1. Melden Sie sich am Management-Portal an.
2. Gehen Sie im Hauptnavigationsmenü zu **Integrationen**.
3. Klicken Sie auf den Namen des Drittanbieter-Systems, für welches Sie die Integration aktivieren wollen.
4. Folgen Sie den Bildschirmanweisungen.

Weitere Informationen darüber, welche Integrationen für Drittanbieter-Systeme verfügbar sind, sowie dazugehörige Schritt-für-Schritt-Anleitungen finden Sie unter https://solutions.acronis.com.

API-Clients verwalten

Sie können Drittherstellersysteme in Cyber Protect Cloud integrieren, indem Sie dessen APIs (Application Programming Interfaces, Anwendungsprogrammierschnittstellen) verwenden. Der Zugriff auf diese APIs wird über API-Clients ermöglicht, die ein integraler Bestandteil des OAuth 2.0-Autorisierungsframeworks der Plattform sind.

Was ist ein API-Client?

Ein API-Client ist ein spezielles Plattform-Konto, welches ein Drittherstellersystem repräsentieren soll, welches authentifiziert und autorisiert werden muss, um auf Daten in den APIs der Plattform und deren Services zugreifen zu können.

Der Zugriff des Clients ist auf einem Mandanten beschränkt, wo ein Administrator den Client und dessen Untermandanten erstellt.

Bei seiner Erstellung erbt der Client die Service-Rollen des Administratorkontos. Diese Rollen können später nicht mehr geändert werden. Eine Änderung der Rollen des Administratorkontos oder dessen Deaktivierung hat keine Auswirkungen auf den Client.

Die Client-Anmeldedaten bestehen aus dem eindeutigen Bezeichner (der ID) und einem geheimen Wert (auch kurz 'Geheimnis' genannt). Die Anmeldedaten verfallen nicht und können auch nicht verwendet werden, um sich am Management-Portal oder einer der Service-Konsolen anzumelden. Der geheime Wert kann zurückgesetzt werden.

Für den Client kann keine Zwei-Faktor-Authentifizierung aktiviert werden.

Eine typische Integrationsprozedur

1. Ein Administrator erstellt einen API-Client in einem Mandanten, den ein Drittherstellersystem verwalten soll.
2. Der Administrator aktiviert den OAuth 2.0-Client-Anmeldeinformationsfluss in dem Drittherstellersystem.

   Gemäß diesem Informationsfluss sollte das System, bevor es über die API auf den Mandanten und dessen Services zugreift, zunächst die Anmeldedaten des erstellten Clients mithilfe der Autorisierungs-API an die Plattform übermitteln. Die Plattform generiert ein Sicherheitstoken und sendet dieses zurück – eine eindeutige kryptische Zeichenfolge, die diesem speziellen Client zugewiesen wird. Das System muss dieses Token dann allen API-Anforderungen hinzufügen.

   Ein solches Sicherheitstoken macht es unnötig, dass die Anmeldedaten des Clients mit den API-Anforderungen übermittelt werden müssen. Zur Erhöhung der Sicherheit verfällt das entsprechende Token nach zwei Stunden. Nach diesem Zeitraum schlagen alle API-Anfragen mit dem abgelaufenen Token fehl, sodass das System ein neues Token von der Plattform anfordern muss.

Weitere Informationen zur hier verwendeten Autorisierung und den Plattform-APIs finden Sie in der Anleitung für Entwickler (Developer's Guide) unter https://developer.acronis.com/doc/account-management/v2/guide/index.

Einen API-Client erstellen

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients** –> **API-Client erstellen**.
3. Geben Sie einen Namen für den API-Client ein.

4. Klicken Sie auf **Weiter**.
   Der API-Client wird standardmäßig mit dem Status **Aktiv** erstellt.
5. Kopieren und speichern Sie die ID und den geheimen Wert (das 'Geheimnis') des Clients sowie die Datacenter-URL. Diese benötigen Sie, wenn Sie den OAuth 2.0-Client-Anmeldeinformationsfluss in dem Drittherstellersystem aktivieren wollen.

   Wichtig
   Der geheime Wert wird aus Sicherheitsgründen nur einmal anzeigt! Dieser Wert kann nicht wiederhergestellt werden, wenn Sie ihn verlieren. Sie können ihn nur zurücksetzen.

6. Klicken Sie auf **Fertig**.

Den geheimen Wert eines API-Clients zurücksetzen

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Geheimnis zurücksetzen**.
5. Klicken Sie auf **Weiter**, um Ihre Entscheidung zu bestätigen.
   Es wird ein neuer geheimer Wert generiert. Die Client-ID und Datacenter-URL werden nicht geändert.
   Alle Sicherheitstoken, die diesem Client zugewiesen wurden, verfallen sofort und alle weitere API-Anforderungen, die mit diesen Tokens erfolgen, werden fehlschlagen.
6. Kopieren und speichern Sie den neuen geheimen Wert (das 'Geheimnis') des Clients.

   Wichtig
   Der geheime Wert wird aus Sicherheitsgründen nur einmal anzeigt! Dieser Wert kann nicht wiederhergestellt werden, wenn Sie ihn verlieren. Sie können ihn nur zurücksetzen.

7. Klicken Sie auf **Fertig**.

Einen API-Client deaktivieren

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Deaktivieren**.
5. Bestätigen Sie Ihre Entscheidung.
   Der Status des Clients wird zu **Deaktiviert** geändert.

Alle API-Anforderungen mit Sicherheitstokens, die diesem Client zugewiesen wurden, werden fehlschlagen. Aber die Tokens verfallen nicht sofort. Die Deaktivierung des Clients hat keinen Einfluss auf den Ablaufzeitpunkt der Tokens.

Sie können den Client jederzeit wieder reaktivieren.

Einen deaktivierten API-Client wieder aktivieren

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Aktivieren**.

   Der Status des Clients wird zu **Aktiv** geändert.

   Alle API-Anforderungen mit Sicherheitstokens, die diesem Client zugewiesen wurden, sind erfolgreich, solange diese Tokens noch nicht abgelaufen sind.

Einen API-Client löschen

1. Melden Sie sich am Management-Portal an.
2. Klicken Sie auf **Einstellungen** –> **API-Clients**.
3. Suchen Sie in der Liste nach dem gewünschten Client.
4. Klicken Sie auf und anschließend auf **Löschen**.
5. Bestätigen Sie Ihre Entscheidung.

   Alle Sicherheitstoken, die diesem Client zugewiesen wurden, verfallen sofort und alle weitere API-Anforderungen, die mit diesen Tokens erfolgen, werden fehlschlagen.

Wichtig
Ein einmal gelöschter Client kann nicht wiederhergestellt werden!

Integrationsreferenzen

Eine Dokumentation zu jeder Integration finden Sie in unserem Integrationskatalog.

So können Sie die benötigte Dokumentation finden

1. Besuchen Sie die Seite https://solutions.acronis.com.
2. Wählen Sie die benötigte Integration aus und klicken Sie dann **Mehr erfahren**.
   Im oberen Bereich der Seite finden Sie einen Link zu entsprechenden Anleitungen oder How-to-Artikeln.

Alternativ können Sie die aktuellste Dokumentation zu den von Acronis entwickelten Integrationen unter https://www.acronis.com/de-de/support/documentation/ in den **Integrationsreferenzen** finden.

Integration in VMware Cloud Director

Ein Service Provider kann VMware Cloud Director (ehemals VMware vCloud Director) in Cyber Protect Cloud integrieren und seinen Kunden so eine direkt einsetzbare Backup-Lösung für deren virtuelle Maschinen anbieten.

Die Integration umfasst folgende Schritte:

1. Den RabbitMQ Message Broker für die VMware Cloud Director-Umgebung konfigurieren.
   RabbitMQ bietet eine SSO-Funktionalität („Single Sign-On“, Einmalanmeldung), damit Sie Ihre VMware Cloud Director-Anmeldedaten verwenden können, um sich an der Cyber Protect-Konsole anzumelden.
   Bis zur Version 23.05 von Cyber Protect Cloud (die im Mai 2023 veröffentlicht wurde) wurde RabbitMQ auch dazu verwendet, Änderungen in der VMware Cloud Director-Umgebung mit Cyber Protect Cloud zu synchronisieren.
2. Einen Management Agenten bereitstellen.
   Während der Bereitstellung des Management Agenten wird auch ein Plug-in für VMware Cloud Director installiert. Das Plug-in fügt Cyber Protection zur VMware Cloud Director-Benutzeroberfläche hinzu.
   Der Management Agent ordnet VMware Cloud Director-Organisationen bestimmten Kunden-Mandanten in Cyber Protect Cloud zu sowie Organisationsadministratoren bestimmten Kunden-Mandanten-Administratoren. Weitere Informationen zu Organisationen finden Sie in der VMware Knowledge Base im (englischsprachigen) Artikel 'Creating an Organization in VMware Cloud Director'.
   Die Kunden-Mandanten werden innerhalb des Partner-Mandanten erstellt, für den die VMware Cloud Director-Integration konfiguriert ist. Diese neuen Kunden-Mandanten befinden sich im Modus **Gesperrt** und können nicht von Partner-Administratoren in Cyber Protect Cloud verwaltet werden.

   Hinweis
   Nur Organisationsadministratoren mit eindeutigen E-Mail-Adressen in VMware Cloud Director sind Cyber Protect Cloud zugeordnet.

3. Einen oder mehrere Backup Agenten bereitstellen.
   Der Backup Agent stellt eine Backup & Recovery-Funktionalität für die virtuellen Maschinen in der VMware Cloud Director-Umgebung bereit.

Wenn Sie die Integration zwischen VMware Cloud Director und Cyber Protect Cloud deaktivieren wollen, wenden Sie sich an den technischen Support.

Einschränkungen

- Die Integration in VMware Cloud Director ist nur für Partner-Mandanten im Verwaltungsmodus **Durch den Service-Provider verwaltet** möglich, deren übergeordneter Mandant (sofern vorhanden) ebenfalls den Verwaltungsmodus **Durch den Service-Provider verwaltet** verwendet. Weitere Informationen zu den Mandanten-Typen und deren Verwaltungsmodus finden Sie in Abschnitt '"Einen Mandanten erstellen" (S. 39)'.

  Alle existierenden direkten Partner können die Integration in VMware Cloud Director konfigurieren. Partner-Administratoren können diese Option auch für Untermandanten aktivieren, indem sie beim Erstellen eines untergeordneten Partner-Mandanten das Kontrollkästchen **Partner-eigene VMware Cloud Director-Infrastruktur** aktivieren.
- Die Zwei-Faktor-Authentifizierung für den Partner-Mandanten, in dem die Integration mit VMware Cloud Director konfiguriert ist, muss deaktiviert werden.
- Ein Administrator, der in mehreren VMware Cloud Director-Organisationen die Rolle 'Organisationsadministrator' hat, kann Backups und Wiederherstellungen nur für einen Kunden-Mandanten in Cyber Protection verwalten.
- Die Cyber Protect-Konsole wird in einer neuen Registerkarte geöffnet.

Software-Anforderungen

Unterstützte VMware Cloud Director-Versionen

- VMware Cloud Director 10.4, 10.5

Unterstützte Webbrowser

- Google Chrome 29 (oder höher)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

In anderen Webbrowsern (inkl. Safari-Browser, die unter anderen Betriebssystem laufen) wird möglicherweise die Benutzeroberfläche nicht korrekt angezeigt oder stehen einige Funktionen nicht zur Verfügung.

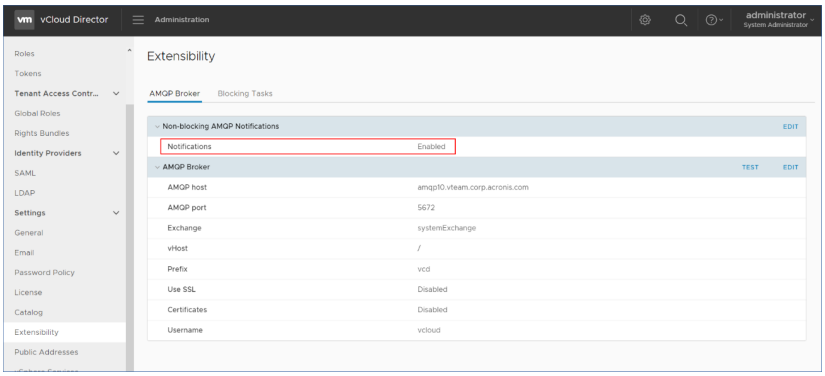
Dne RabbitMQ Message Broker konfigurieren

Diese Prozedur hängt davon ab, welche Version von Cyber Protect Cloud vorliegt. Ab der Version 23.06 (die im Juni 2023 veröffentlicht wurde) wird eine vereinfachte Prozedur verwendet.

So können Sie denRabbitMQ Message Broker konfigurieren

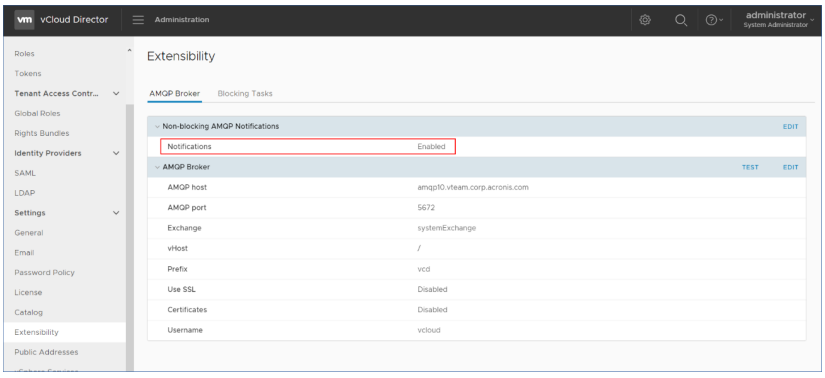
Für Version 23.06 und höher

1. Installieren Sie einen RabbitMQ AMQP Broker für Ihre VMware Cloud Director-Umgebung.
   Weitere Informationen zur Installation von RabbitMQ finden Sie in der VMware-Dokumentation: Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz.
2. Melden Sie sich am VMware Cloud Director-Provider-Portal als Systemadministrator an.
3. Gehen Sie zu **Administration** –> **Erweiterbarkeit** und stellen Sie sicher, dass unter **Nicht blockierende AMQP-Benachrichtigungen**, **Benachrichtigungen** aktiviert sind.



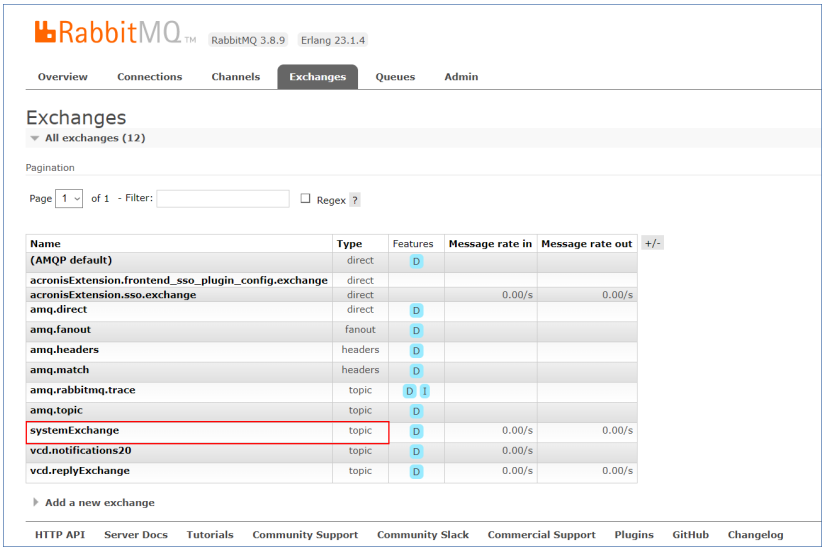
Für Version 23.05 und höher

1. Installieren Sie einen RabbitMQ AMQP Broker für Ihre VMware Cloud Director-Umgebung.
   Weitere Informationen zur Installation von RabbitMQ finden Sie in der VMware-Dokumentation: Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz.
2. Melden Sie sich am VMware Cloud Director-Provider-Portal als Systemadministrator an.
3. Gehen Sie zu **Administration** –> **Erweiterbarkeit** und stellen Sie sicher, dass unter **Nicht blockierende AMQP-Benachrichtigungen**, **Benachrichtigungen** aktiviert sind.



4. Melden Sie sich an der RabbitMQ-Management-Konsole als Administrator an.
5. Überprüfen Sie auf der Registerkarte **Exchanges** ob die Exchange (standardmäßig unter dem

Namen **SystemExchange**) erstellt wurde und diese den Typ **topic** hat.



Das Plug-in für VMware Cloud Director installieren und veröffentlichen

Das Plug-in für VMware Cloud Director wird automatisch mit installiert, wenn Sie den Management Agenten installieren.

Sie müssen das Plug-in jedoch manuell für die Mandanten veröffentlichen, die Cyber Protection verwenden.

So können Sie das Plug-in für VMware Cloud Director veröffentlichen

1. Melden Sie sich am VMware Cloud Director-Provider-Portal als Systemadministrator an.
2. Wählen Sie im Navigationsmenü **Portal anpassen**.
3. Wählen Sie in der Registerkarte **Plug-ins** das **Cyber Protection**-Plug-in aus und klicken Sie dann auf **Veröffentlichen**.
4. Konfigurieren Sie den Geltungsbereich der Veröffentlichung:
   a. Aktivieren Sie im Bereich **Geltungsbereich für** nur das Kontrollkästchen **Mandanten**.
   b. Wählen Sie im Bereich **Veröffentlichen für** die Option **Alle Mandanten**, damit das Plug-in für alle bestehenden und zukünftigen Mandanten aktiviert wird – oder wählen Sie einzelne Mandanten aus, für die Sie das Plug-in aktivieren wollen.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Vertrauen**.

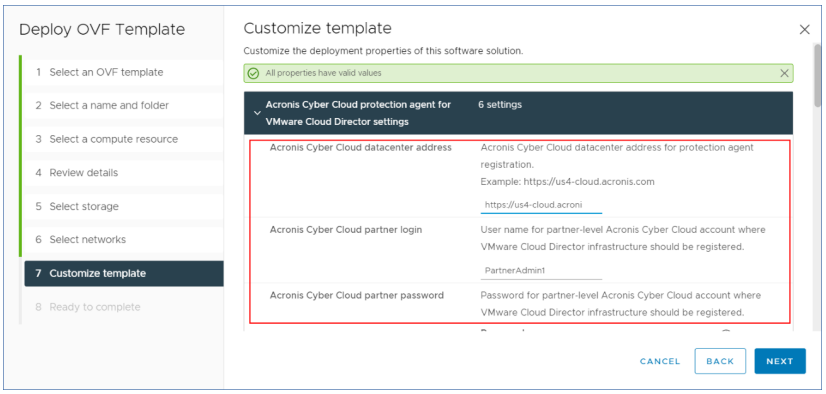
Einen Management Agenten installieren

1. Melden Sie sich am Cyber Protect Cloud-Management-Portal als Partner-Administrator an.
2. Gehen Sie zu **Einstellungen** –> **Speicherort** und klicken Sie dann auf **VMware Cloud Director hinzufügen**.

3. Wählen Sie aus dem Listenfeld **Release-Kanal** die Version des Agenten aus. Folgende Optionen sind verfügbar:
   - **Aktuell** – dies ist die neueste Version.
   - **Stabil** – es ist die Version aus der letzten Veröffentlichung.
4. Klicken Sie auf den Link **Management Agent** und laden Sie die ZIP-Datei herunter.
5. Extrahieren Sie die Management Agenten-Vorlagendatei `vCDManagementAgent.ovf` und die virtuelle Laufwerksdatei `vCDManagementAgent-disk1.vmdk`.
6. Stellen Sie im vSphere Client die OVF-Vorlage für den Management Agenten auf einem ESXi-Host unter einer vCenter-Instanz bereit, die vom VMware Cloud Director verwaltet wird.

   Wichtig
   Installieren Sie nur einen Management Agenten pro VMware Cloud Director-Umgebung.

7. Konfigurieren Sie im Assistenten **OVF-Vorlage bereitstellen** den Management Agenten, indem Sie folgende Einstellungen vornehmen:



   a. Die URL des Cyber Protect Cloud-Datacenters. Beispielsweise `https://us5-cloud.example.com`.
   b. Die Anmeldedaten des Partner-Administrators (Anmeldename und Kennwort).
   c. Die ID des Backup Storage für die virtuellen Maschinen in der VMware Cloud Director-Umgebung. Dieser Backup Storage kann nur ein Partner-eigener (vom Partner betriebener) Storage sein. Weitere Informationen über Storages finden Sie im Abschnitt '"Speicherorte und Storage verwalten" (S. 82)'.

      Wenn Sie die ID überprüfen wollen, gehen Sie zuerst im Management-Portal zu **Einstellungen** –> **Speicherorte** und wählen Sie dann den gewünschten Storage. Sie können seine ID hinter der **uuid=**-Sequenz in der URL sehen.
   d. Cyber Protect Cloud-Abrechnungsmodus: **Pro Gigabyte** oder **Pro Workload**.

      Hinweis
      Der gewählte Abrechnungsmodus gilt für alle neuen Kunden-Mandanten, die erstellt werden.

   e. VMware Cloud Director-Parameter: die Infrastrukturadresse sowie Anmeldename und Kennwort des Systemadministrators.

f. RabbitMQ-Parameter: Die Anmeldedaten des Administrators (Anmeldename und Kennwort).

g. Das Kennwort für den Benutzer `root` auf der virtuellen Maschine mit dem Agenten.

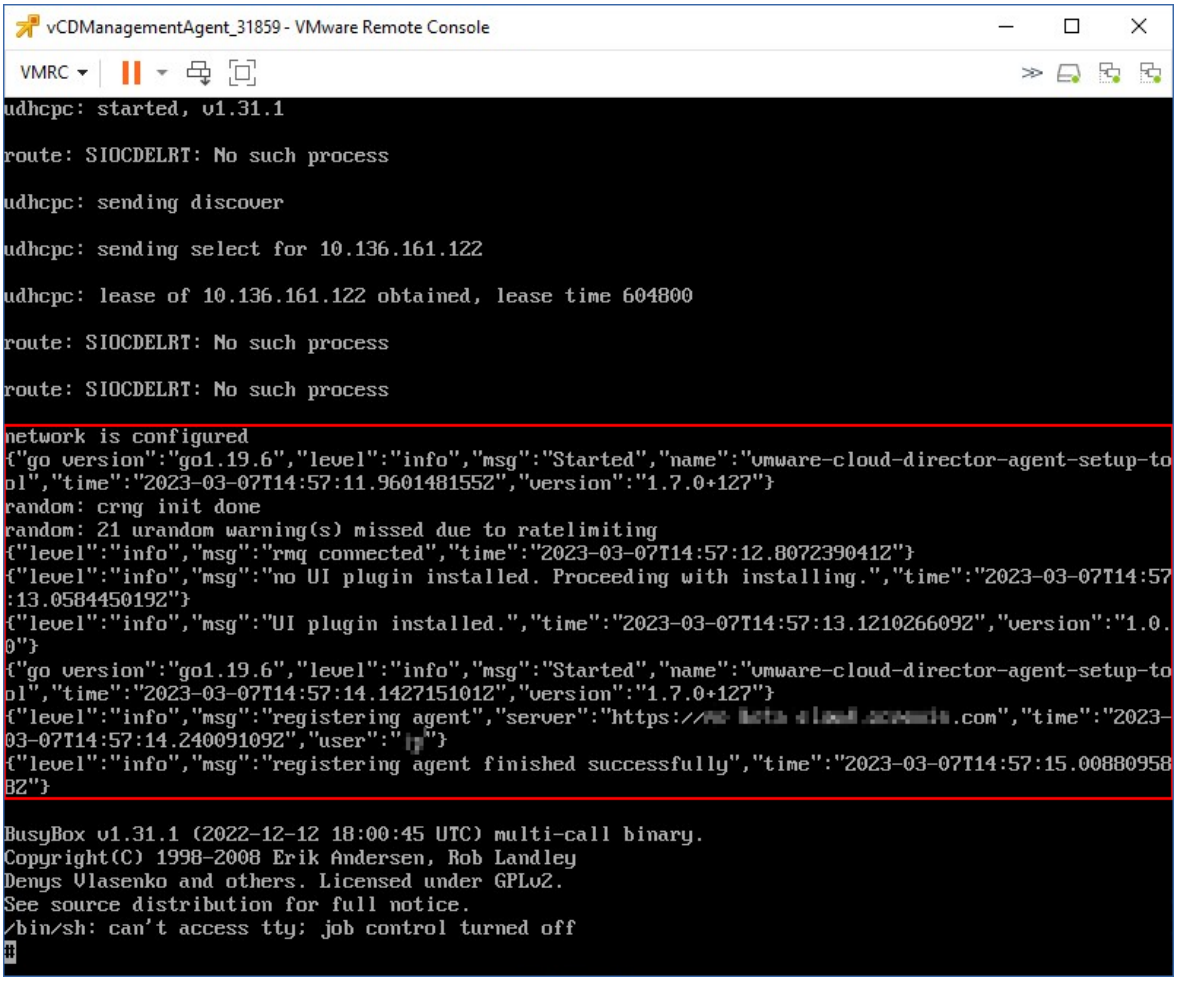
h. Netzwerkparameter: die IP-Adresse, Subnetz-Maske, Standard-Gateway, DNS, DNS-Suffix.

Standardmäßig ist nur eine Netzwerkschnittstelle aktiviert. Wenn Sie eine zweite Netzwerkschnittstelle aktivieren wollen, müssen Sie das Kontrollkästchen neben **eth1 aktivieren** aktivieren.

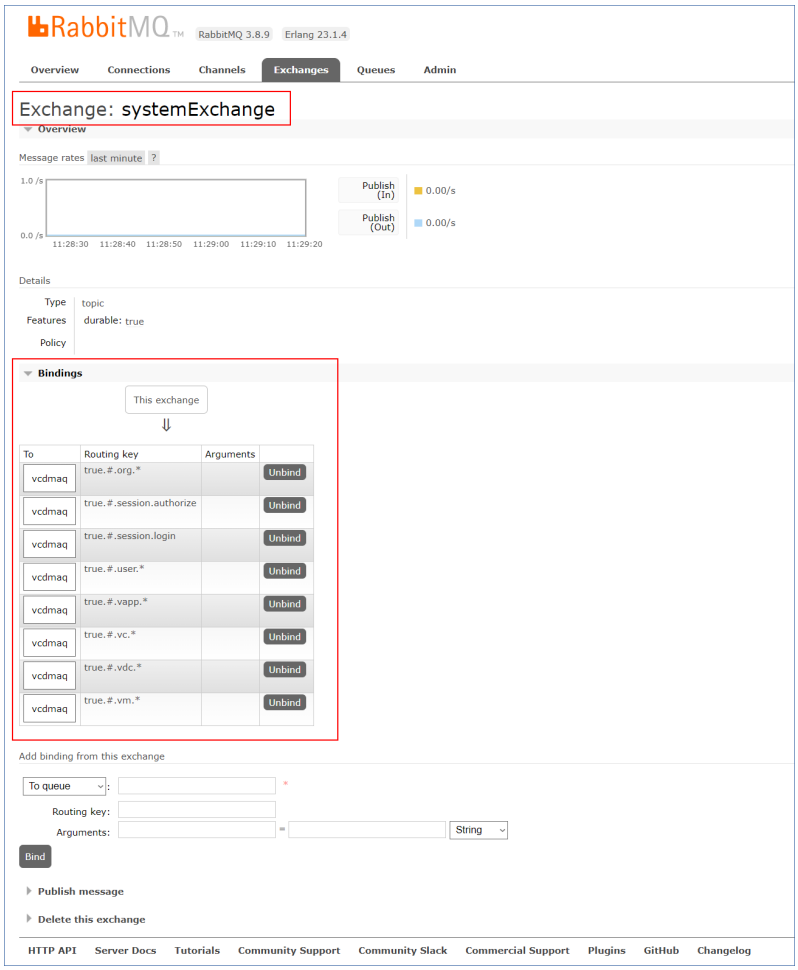
Hinweis
Stellen Sie sicher, dass Ihre Netzwerkeinstellungen dem Management Agenten sowohl den Zugriff auf die VMware Cloud Director-Umgebung als auch auf Ihr Cyber Protect Cloud-Datacenter erlauben.

Sie können die Management Agent-Einstellung auch nach dem ersten Bereitstellen konfigurieren. Fahren Sie im vSphere Client die virtuelle Maschine mit dem Management Agenten herunter und klicken Sie dann auf **Konfigurieren** –> **Einstellungen** –> **vApp-Optionen**. Nehmen Sie die gewünschten Einstellungen vor und fahren Sie dann die virtuelle Maschine mit dem Management Agenten wieder hoch.

8. [Optional] Öffnen Sie im vSphere Client die Konsole der virtuellen Maschine mit dem Management Agenten und überprüfen Sie dann Ihre Einrichtung.



9. Überprüfen Sie die RabbitMQ-Verbindung.
   a. Melden Sie sich an der RabbitMQ-Management-Konsole als Administrator an.
   b. Wählen Sie auf der Registerkarte **Exchanges** die Exchange aus, die Sie während der RabbitMQ-Installation festgelegt haben. Dereren Name lautet standardmäßig **systemExchange**.
   c. Überprüfen Sie die Bindungen an die **vcdmaq**-Warteschlange.



Backup Agenten installieren

1. Melden Sie sich am Management-Portal als Partner-Administrator an.
2. Gehen Sie zu **Einstellungen** –> **Speicherort** und klicken Sie dann auf **VMware Cloud Director hinzufügen**.
3. Wählen Sie aus dem Listenfeld **Release-Kanal** die Version des Agenten aus. Folgende Optionen sind verfügbar:
   - **Aktuell** – dies ist die neueste Version.
   - **Stabil** – es ist die Version aus der letzten Veröffentlichung.
4. Klicken Sie auf den Link **Backup Agent** und laden Sie die ZIP-Datei herunter.

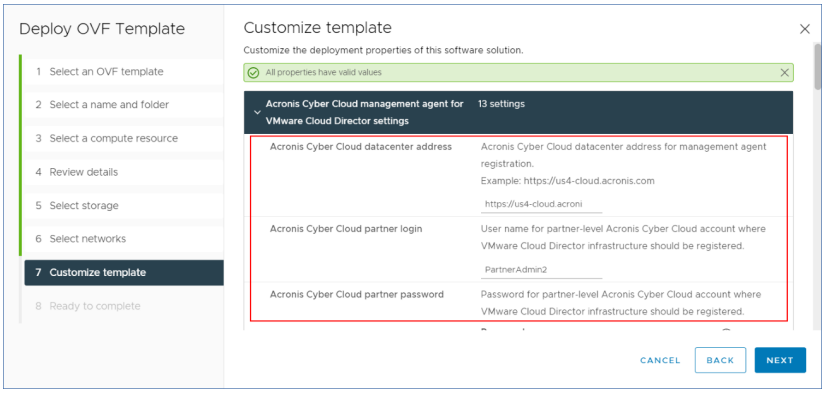
5. Extrahieren Sie die Backup Agenten-Vorlagendatei `vCDCyberProtectAgent.ovf` und die virtuelle Laufwerksdatei `vCDCyberProtectAgent-disk1.vmdk`.
6. Stellen Sie im vSphere Client die Backup Agenten-Vorlage auf dem gewünschten ESXi-Host bereit.

   Sie benötigen mindestens einen Backup Agenten pro Host. Dem Backup Agenten werden standardmäßig 8 GB RAM und 2 CPUs zugewiesen. Er kann zudem bis zu 5 Backup- oder Recovery-Tasks gleichzeitig verarbeiten.

   Wenn Sie mehr Tasks verarbeiten oder den Backup- und Recovery-Traffic verteilen wollen, müssen Sie zusätzliche Agenten auf demselben Host bereitstellen. Alternativ dazu empfehlen wir, dem vorhandenen Agenten 16 GB RAM und 4 vCPUs zuzuweisen, um Fehler durch zu wenig Arbeitsspeicher zu vermeiden.

   Hinweis
   Backups von virtuellen Maschinen auf ESXi Hosts, auf denen kein Backup Agent installiert ist, werden mit dem Fehler 'Task-Zeitlimit ist abgelaufen' fehlschlagen.

7. Konfigurieren Sie im Assistenten **OVF-Vorlage bereitstellen** den Backup Agenten, indem Sie folgende Einstellungen vornehmen:



   a. Die URL des Cyber Protect Cloud-Datacenters. Beispielsweise `https://us5-cloud.example.com`.
   b. Die Anmeldedaten des Partner-Administrators (Anmeldename und Kennwort).
   c. VMware vCenter-Parameter: Server-Adresse, Anmeldename und Kennwort.

      Der Agent wird diese Anmeldedaten verwenden, um sich mit dem vCenter Server zu verbinden. Wir empfehlen, dass Sie ein Konto verwenden, dem die Rolle **Administrator** zugewiesen ist. Alternativ können Sie auch ein Konto angeben, welches über die notwendigen Berechtigungen auf dem vCenter Server verfügt.
   d. Das Kennwort für den Benutzer `root` auf der virtuellen Maschine mit dem Agenten.
   e. Netzwerkparameter: die IP-Adresse, Subnetz-Maske, Standard-Gateway, DNS, DNS-Suffix.

      Standardmäßig ist nur eine Netzwerkschnittstelle aktiviert. Wenn Sie eine zweite Netzwerkschnittstelle aktivieren wollen, müssen Sie das Kontrollkästchen neben **eth1 aktivieren** aktivieren.

Hinweis
Stellen Sie sicher, dass Ihre Netzwerkeinstellungen dem Backup Agenten sowohl den Zugriff auf den vCenter Server als auch auf Ihr Cyber Protect Cloud-Datacenter erlauben.

f. Download-Begrenzung: die maximale Download-Geschwindigkeit (in Kbit/s), die die Lesegeschwindigkeit für das Backup-Archiv während der Wiederherstellungsaktion bestimmt. Der Standardwert ist 0 (unbegrenzt).
g. Upload-Begrenzung: die maximale Upload-Geschwindigkeit (in Kbit/s), die die Schreibgeschwindigkeit für das Backup-Archiv während der Backup-Aktion bestimmt. Der Standardwert ist 0 (unbegrenzt).

Sie können die Parameter für die Backup Agenten-Einstellung auch nach dem ersten Bereitstellen konfigurieren. Fahren Sie im vSphere Client die virtuelle Maschine mit dem Backup Agenten herunter und klicken Sie dann auf **Konfigurieren** –> **Einstellungen** –> **vApp-Optionen**. Nehmen Sie die gewünschten Einstellungen vor und fahren Sie dann die virtuelle Maschine mit dem Backup Agenten wieder hoch.

8. Stellen Sie im vSphere Client sicher, dass die Optionen **Host** und **Storage vMotion** für die virtuelle Maschine mit dem Backup Agenten deaktiviert sind.

Die Agenten aktualisieren

So können Sie einen Management Agenten aktualisieren

1. Melden Sie sich am Cyber Protect Cloud-Management-Portal als Partner-Administrator an.
2. Gehen Sie zu **Einstellungen** –> **Speicherort** und klicken Sie dann auf **VMware Cloud Director hinzufügen**.
3. Klicken Sie auf den Link **Management Agent** und laden Sie dann die ZIP-Datei mit der neuesten Agenten-Version herunter.
4. Extrahieren Sie die Management Agenten-Vorlagendatei `vCDManagementAgent.ovf` und die virtuelle Laufwerksdatei `vCDManagementAgent-disk1.vmdk`.
5. Fahren Sie im vSphere Client die virtuelle Maschine mit dem aktuellen Management Agenten herunter.
6. Stellen Sie eine virtuelle Maschine mit dem neuen Management Agenten bereit, indem Sie die neuesten `vCDManagementAgent.ovf`- und `vCDManagementAgent-disk1.vmdk`-Dateien verwenden.
7. Konfigurieren Sie den Management Agenten, indem Sie die gleichen Einstellungen wie im alten Agenten verwenden.
8. [Optional] Löschen Sie die virtuelle Maschine mit dem alten Management Agenten.

Wichtig
Sie dürfen nur einen aktiven Management Agenten pro VMware Cloud Director-Umgebung haben.

So können Sie einen Backup Agenten aktualisieren

1. Melden Sie sich am Cyber Protect Cloud-Management-Portal als Partner-Administrator an.
2. Gehen Sie zu **Einstellungen** –> **Speicherort** und klicken Sie dann auf **VMware Cloud Director hinzufügen**.
3. Klicken Sie auf den Link **Backup Agent** und laden Sie dann die ZIP-Datei mit der neuesten Agenten-Version herunter.
4. Extrahieren Sie die Management Agenten-Vorlagendatei `vCDCyberProtectAgent.ovf` und die virtuelle Laufwerksdatei `vCDCyberProtectAgent-disk1.vmdk`.
5. Fahren Sie im vSphere Client die virtuelle Maschine mit dem aktuellen Backup Agenten herunter.
   Alle Backup- und Recovery-Tasks, die möglicherweise gerade laufen, werden fehlschlagen. Wenn Sie überprüfen wollen, ob Tasks ausgeführt werden, öffnen Sie im vSphere Client die Konsole der virtuellen Maschine mit dem Backup Agenten und führen Sie dann den Befehl `ps | grep esx_worker` aus. Stellen Sie sicher, dass es keine aktiven `esx_worker`-Prozesse gibt.
6. Stellen Sie eine virtuelle Maschine mit dem neuen Backup Agenten bereit, indem Sie die neuesten `vCDCyberProtectAgent.ovf`- und `vCDCyberProtectAgent-disk1.vmdk`-Dateien verwenden.
7. Konfigurieren Sie den Backup Agenten, indem Sie die gleichen Einstellungen wie im alten Agenten verwenden.
8. [Optional] Löschen Sie die virtuelle Maschine mit dem alten Backup Agenten.

Einen Backup-Administrator erstellen

Organisationsadministratoren können die Backup-Verwaltung an spezielle Backup-Administratoren delegieren, denen diese Aufgabe extra zugewiesen wird.

So können Sie einen Backup-Administrator erstellen

1. Klicken Sie im VMware Cloud Director-Mandanten-Portal auf **Verwaltung** –> **Rollen** –> **Neu**.
2. Spezifizieren Sie im Fenster **Rolle hinzufügen** einen Namen und eine Beschreibung für die neue Rolle.
3. Scrollen Sie in der Liste der Berechtigungen nach unten und wählen Sie dann unter **Andere** die Option **Self-Service-VM-Backup-Operator** aus.

   Hinweis
   Die Berechtigung **Self-Service-VM-Backup-Operator** ist verfügbar, wenn Sie das Plug-in für VMware Cloud Director installiert haben. Weitere Informationen über die entsprechende Durchführung finden Sie im Abschnitt '"Das Plug-in für VMware Cloud Director installieren und veröffentlichen" (S. 323)'.

4. Klicken Sie im VMware Cloud Director-Mandanten-Portal auf **Benutzer**.
5. Wählen Sie einen Benutzer aus und klicken Sie dann auf **Bearbeiten**.
6. Weisen Sie diesem Benutzer die neue Rolle zu, die Sie erstellt haben.

Als Ergebnis kann der ausgewählte Benutzer die Backups für die virtuellen Maschinen in dieser Organisation verwalten.

Hinweis
Systemadministratoren der VMware Cloud Director-Umgebung können eine globale Rolle definieren, bei der die Berechtigung **Self-Service-VM-Backup-Operator** aktiviert ist, und diese Rolle dann für die Mandanten veröffentlichen. So brauchen die Organisationsadministratoren einem Benutzer einfach nur die Rolle zuweisen.

Systembericht, Protokolldateien und Konfigurationsdateien

Für Problembehebungen müssen Sie möglicherweise einen Systembericht mithilfe des Tools `sysinfo` erstellen oder die Protokoll- und Konfigurationsdateien auf einer virtuellen Maschine mit einem Agenten überprüfen.

Sie können entweder direkt auf die virtuelle Maschine zugreifen, indem Sie deren Konsole im vSphere Client öffnen, oder dies per Remote-Steuerung über einen SSH-Client tun. Um per SSH-Client auf die virtuelle Maschine zugreifen zu können, müssen Sie zuerst SSH Verbindungen zu dieser Maschine zulassen.

So können Sie SSH-Verbindungen zu einer virtuellen Maschine aktivieren

1. Öffnen Sie im vSphere Client die Konsole der virtuellen Maschine mit dem Agenten.
2. Führen Sie in der Eingabeaufforderung folgenden Befehl aus: `/bin/sshd`, um den SSH-Daemon zu starten.

Als Ergebnis können Sie eine Verbindung zu dieser virtuellen Maschine mit einem SSH-Client (wie WinSCP) herstellen.

So können Sie das Tool `sysinfo` ausführen

1. Greifen Sie auf die virtuelle Maschine mit dem Agenten zu.
   - Wenn Sie direkt auf die virtuellen Maschine zugreifen wollen, öffnen Sie im vSphere Client die Konsole der VM.
   - Wenn Sie remote auf die virtuellen Maschine zugreifen wollen, verbinden Sie sich per SSH-Client mit der VM.

     Verwenden Sie die folgenden vorgegebenen Anmeldedaten in der Kombination 'Anmeldename:Kennwort': `root`:`root`.
2. Gehen Sie zum Verzeichnis `/bin` und führen Sie dort das Tool `sysinfo` aus.

   ```
   # cd /bin/
   # ./sysinfo
   ```

   Als Ergebnis wird eine Systemberichtdatei im folgenden Standardverzeichnis gespeichert: `/var/lib/Acronis/sysinfo`.

   Sie können auch ein anderes Verzeichnis spezifizieren, wenn Sie das Tool `sysinfo` mit der Option `--target_dir` ausführen.

```
./sysinfo --target_dir path/to/report/dir
```

3. Laden Sie den generierten Systembericht mit einem SSH-Client herunter.

So können Sie auf eine Protokoll- oder Konfigurationsdatei zugreifen

1. Verbinden Sie sich per SSH-Client mit der virtuellen Maschine.
   Verwenden Sie die folgenden vorgegebenen Anmeldedaten in der Kombination 'Anmeldename:Kennwort': `root:root`.
2. Laden Sie die gewünschte Datei herunter.
   Sie können die Protokolldateien an folgenden Speicherorten finden:
   - Backup Agent: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Management Agent: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   Sie können die Konfigurationsdateien an folgenden Speicherorten finden:
   - Backup Agent: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Management Agent: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Auf die Cyber Protect-Konsole zugreifen

Folgende Administratoren können die Sicherung von virtuellen Maschinen in VMware Cloud Director-Organisationen verwalten:

- Organisationsadministratoren
- Speziell zugewiesene Backup-Administratoren
  Weitere Informationen darüber, wie man einen solchen Administrator erstellt, finden Sie im Abschnitt '"Einen Backup-Administrator erstellen" (S. 329)'.

Administratoren können auf die benutzerdefinierte Cyber Protect-Konsole zugreifen, indem sie auf das Element **Cyber Protection** im Navigationsmenü des VMware Cloud Director-Mandanten-Portals klicken.

Hinweis
Single Sign-on (Einzelanmeldung) ist nur für Organisationsadministratoren verfügbar und wird nicht für Systemadministratoren unterstützt, die das VMware Cloud Director-Mandanten-Portal verwenden.

In der Cyber Protect-Konsole können Administratoren nur auf ihre eigenen VMware Cloud Director-Organisationselemente zugreifen: virtuelle Datacenter, vApps und einzelne virtuelle Maschinen. Sie können die Backups und Wiederherstellungen der VMware Cloud Director-Organisationsressourcen verwalten.

Partner-Administratoren können auf die Cyber Protect-Konsolen ihrer Kunden-Mandanten zugreifen und in deren Auftrag Backups und Wiederherstellung verwalten.

Backups und Wiederherstellungen durchführen

Einen Schutzplan erstellen

Wenn Sie die Backup-Einstellungen konfigurieren möchten, müssen Sie einen Schutzplan erstellen.

Sie können einen Schutzplan auf mehr als eine Maschine anwenden. Außerdem können Sie mehrere Schutzpläne auf dieselbe Maschine anwenden.

Einschränkungen

- Es werden nur Backups der kompletten Maschine unterstützt. Sie können keine einzelnen Laufwerke oder Volumes sichern.
- Dateifilter (Einschlüsse/Ausschlüsse) werden nicht unterstützt.
- Als Backup-Speicherort wird nur der Cloud Storage unterstützt. Der Storage wird in den Einstellungen des Management Agenten konfiguriert und kann nicht von den Benutzern im Schutzplan geändert werden.
- Dynamische Gruppen werden nicht unterstützt.
- Folgende Backup-Schemata werden unterstützt: **Nur inkrementell (Einzeldatei)**, **Nur vollständig** und **Wöchentlich vollständig, täglich inkrementell**.
- Es werden nur Bereinigungen nach einem Backup unterstützt.

So können Sie einen Schutzplan erstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** > **VMware Cloud Director**.
2. Wählen Sie die Maschinen, die Sie schützen wollen, und klicken Sie dann auf **Schützen**.
3. [Wenn es bereits angewendete Pläne gibt] Klicken Sie auf **Plan hinzufügen**.
4. Klicken Sie auf **Plan erstellen**.
5. Konfigurieren Sie unter **Verschlüsselung** die entsprechenden Verschlüsselungseinstellungen.
6. [Optional] Um den Schutzplan umzubenennen, klicken Sie auf das Stiftsymbol und geben Sie dann den neuen Namen ein.
7. [Optional] Um das Backup-Schema oder die Planung zu ändern, klicken Sie auf **Planung** und konfigurieren Sie dann die entsprechenden Einstellungen.
8. [Optional] Um die Aufbewahrungsregeln zu ändern, klicken Sie auf **Aufzubewahrende Anzahl** und konfigurieren Sie dann die entsprechenden Einstellungen.
9. [Optional] Um die Backup-Optionen zu ändern, klicken Sie auf **Backup-Optionen** und konfigurieren Sie dann die entsprechenden Einstellungen.
10. Klicken Sie auf **Anwenden**.

Recovery einer Maschine

Sie können ein Backup zur ursprünglichen virtuellen Maschine oder zu einer neuen virtuellen Maschine wiederherstellen.

Einschränkungen

- Wiederherstellungen auf Dateiebene werden nicht unterstützt.
- Sie können Backups zu neuen virtuellen Maschinen in VMware Cloud Director 10.4 und höher wiederherstellen.

  Um ein Backup zu einer neuen virtuellen Maschine wiederherzustellen, muss das Backup von einem Agenten mit der Version 24.02 oder höher erstellt worden sein. Sie können die Agent-Version in der Datei `ProductVersion.conf` überprüfen, die sich im Verzeichnis `/etc` der virtuellen Maschine mit dem jeweiligen Agenten befindet.
- Nachdem Sie ein Backup zu einer neuen Maschine wiederhergestellt haben, erscheint die neue Maschine unter **Geräte** > **VMware Cloud Director** > Organisation > virtuelles Datacenter > **Eigenständige VMs**. Sie können keine spezifische vApp als Wiederherstellungsziel auswählen.

So können Sie eine Maschine wiederherstellen

Zur ursprünglichen Maschine

1. Wählen Sie in der Cyber Protect-Konsole Sie den Recovery-Punkt auf eine der folgenden Arten aus:
   - Gehen Sie zu **Geräte** > **VMware Cloud Director**, wählen Sie eine per Backup gesicherte Maschine aus, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt aus.
   - Gehen Sie zu **Geräte** > **VMware Cloud Director**, wählen Sie ein Backup-Archiv aus, klicken Sie auf **Backups anzeigen** und wählen Sie dann einen Recovery-Punkt aus.
2. Klicken Sie auf **Maschine wiederherstellen**.
3. Klicken Sie auf **Recovery starten**.

Zu einer neuen Maschine

1. Wählen Sie in der Cyber Protect-Konsole Sie den Recovery-Punkt auf eine der folgenden Arten aus:
   - Gehen Sie zu **Geräte** > **VMware Cloud Director**, wählen Sie eine per Backup gesicherte Maschine aus, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt aus.
   - Gehen Sie zu **Geräte** > **VMware Cloud Director**, wählen Sie ein Backup-Archiv aus, klicken Sie auf **Backups anzeigen** und wählen Sie dann einen Recovery-Punkt aus.
2. Klicken Sie auf **Maschine wiederherstellen**.
3. Klicken Sie auf **Zielmaschine** und wählen Sie dann **Neue Maschine** aus.
4. Wählen Sie das virtuelle Datacenter für die neue Maschine aus.
5. Geben Sie einen Namen für die neue Maschine an.

   Standardmäßig wird der Name der ursprünglichen Maschine vorgeschlagen.

6. Klicken Sie auf **OK**.
7. [Optional] Klicken Sie auf **VM-Einstellungen**, um eine der folgenden Einstellungen für die neue Maschine zu ändern, und klicken Sie dann auf **OK**:
   - RAM-Größe
   - Anzahl der virtuellen Prozessoren
   - Anzahl der Kerne pro Socket
   - Storage-Profil
   - Netzwerkadapter und zugewiesene Netzwerke
8. [Optional] Klicken Sie auf **Laufwerkszuordnung**, um die Laufwerkszuordnung oder das Speicherprofil für ein Laufwerk zu ändern, und klicken Sie dann auf **OK**.
9. Klicken Sie auf **Recovery starten**.

Die Integration mit VMware Cloud Director entfernen

Die Konfiguration der VMware Cloud Director-Instanz rückgängig zu machen und ihre Registrierung bei Cyber Protect Cloud aufzuheben, ist eine komplexe Prozedur. Wenden Sie sich an Ihren Support-Mitarbeiter, wenn Sie Hilfe benötigen.

Index

F

G

H

I

J

K