

Cyber Protect Cloud

23.02

Inhaltsverzeichnis

Über dieses Dokument	5
Über Cyber Protect	6
Cyber Protect Services	6
Abrechnungsmodi für Cyber Protect	7
Zwischen Editionen und Abrechnungsmodi wechseln	9
Angebotsэлеmente und Quota-Verwaltung	12
Services und Angebotsэлеmente	12
Das Management-Portal verwenden	26
Unterstützte Webbrowser	26
Das Administratorkonto aktivieren	26
Anforderungen an das Kennwort	26
Auf das Management-Portal zugreifen	27
Kontakte im Assistenten 'Unternehmensprofil' konfigurieren	27
Vom Management-Portal aus auf die Cyber Protection-Konsole zugreifen	29
Im Management-Portal navigieren	29
Den Zugriff auf die Weboberfläche einschränken	30
Auf die Services zugreifen	30
Registerkarte Überblick	30
Registerkarte Clients	31
7-Tage-Verlaufsleiste	32
Benutzerkonten und Mandanten	33
Mandanten verwalten	35
Einen Mandanten erstellen	35
Erhöhter Sicherheitsmodus	38
Die Services für einen Mandanten auswählen	39
Die Angebotsэлеmente für einen Mandanten konfigurieren	40
Services für mehrere bestehende Mandanten aktivieren	41
Benachrichtigungen über Wartungsaktivitäten aktivieren	43
Selbstverwaltete Kundenprofile konfigurieren	44
Firmenkontakte konfigurieren	44
Die Nutzungsdaten für einen Mandanten aktualisieren	47
Einen Mandanten deaktivieren und aktivieren	47
Einen Mandanten zu einem anderen Mandanten verschieben	48
Einen Partner- in einen Ordner-Mandanten konvertieren (und umgekehrt)	49
Den Zugriff auf Ihren Mandanten einschränken	50

Einen Mandanten löschen	50
Benutzer verwalten	51
Ein Benutzerkonto erstellen	51
Für jeden Service verfügbare Benutzerrollen	54
Die Benachrichtigungseinstellungen für einen Benutzer ändern	59
Ein Benutzerkonto deaktivieren und aktivieren	61
Ein Benutzerkonto löschen	62
Die Eigentümerschaft eines Benutzerkontos übertragen	62
Zwei-Faktor-Authentifizierung einrichten	63
Und so funktioniert es	63
Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben	65
Die Zwei-Faktor-Authentifizierung für Ihren Mandanten einrichten	66
Die Zwei-Faktor-Authentifizierung für Benutzer verwalten	67
Die Zwei-Faktor-Authentifizierung bei Verlust des Zweit-Faktor-Gerätes zurücksetzen	69
Schutz vor Brute-Force-Angriffen	70
Upselling-Szenarien für Ihre Kunden konfigurieren	70
Upselling-Punkte, die einem Kunden angezeigt werden	71
Speicherorte und Storage verwalten	72
Speicherorte	72
Storages verwalten	73
Unveränderlichen Storage konfigurieren	74
Branding und White-Labeling konfigurieren	77
Branding-Elemente	78
Branding konfigurieren	80
Die Standardeinstellungen für das Branding wiederherstellen	80
Das Branding deaktivieren	81
White-Labeling	81
Eine benutzerdefinierte URL für die Weboberfläche konfigurieren	81
Agenten automatisch aktualisieren	82
So können Sie Agenten automatisch aktualisieren lassen	83
So können Sie die Agenten-Updates überwachen	85
Monitoring	85
Nutzung	85
Aktionen	86
Berichte	106
Nutzung	106
Aktionen-Berichte	108

Kurzübersicht	114
Zeitzonen in Berichten	127
Berichtsdaten je nach Widget-Typ	128
Überwachungsprotokoll	131
Felder im Überwachungsprotokoll	131
Filter und Suche	132
Advanced Protection-Pakete	133
In den Cyber Protect Services enthaltene Funktionen und Advanced-Pakete	134
Enthaltene Standard-Funktionen und verfügbare Advanced-Funktionen im Protection Service	134
Pay-as-you-go- und Advanced-Funktionen im Protection Service	137
Advanced Data Loss Prevention	138
Advanced Data Loss Prevention aktivieren	139
Advanced Security + EDR	139
Advanced Security + EDR aktivieren	139
Advanced Disaster Recovery	140
Advanced Email Security	141
Integrationen	142
Integration in Drittanbieter-Systeme	142
Eine Integration für Cyber Protect Cloud einrichten	142
API-Clients verwalten	142
Integrationsreferenzen	145
Integration in VMware Cloud Director	147
Einschränkungen	148
Software-Anforderungen	148
Dne RabbitMQ Message Broker konfigurieren	149
Das Plug-in für VMware Cloud Director installieren	150
Einen Management Agenten installieren	150
Backup Agenten installieren	153
Die Agenten aktualisieren	155
Auf die Cyber Protection-Webkonsole zugreifen	156
Einen Backup-Administrator erstellen	157
Systembericht, Protokolldateien und Konfigurationsdateien	158
Die Integration mit VMware Cloud Director entfernen	159
Datenschutzeinstellungen	160
Index	161

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 einzigartiger Funktionen, die anspruchsvollere Szenarien für bestimmte Funktionsbereiche abdecken – beispielsweise Advanced Backup, Advanced Security usw. Die Advanced-Pakete erweitern die Funktionalität, die in der Standard-Version des Cyber Protect Service verfügbar ist. Weitere Informationen über die Advanced Protection-Pakete finden Sie im Abschnitt "'Advanced Protection-Pakete" (S. 133)'.
 - **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-Datcenter 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 Angebots Elemente, 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 Angebots Elemente finden Sie im Abschnitt "'Cyber Protect Services" (S. 6)'.

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 Angebotsselemente 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 Angebotsselemente für Ihre Mandanten manuell wechseln, indem Sie deren Profil bearbeiten und Angebotsselemente für diese auswählen. Weitere Informationen über den entsprechenden Prozess finden Sie im Abschnitt "Zwischen Editionen und Abrechnungsmodi wechseln" (S. 9).

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

Die nachfolgende Tabelle veranschaulicht den Prozess in beide Richtungen.

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

	Umstellungsrichtung	
	Edition > Abrechnungsmodi	Abrechnungsmodus > Abrechnungsmodus
Quota wechseln	<p>Die Quotas werden vom Quell- zum Ziel-Angebotsselement repliziert. Standard (Quelle) → Standard-Produkt (Ziel). Standard (Quelle) → Pakete (Ziel).</p> <hr/> <p>Hinweis Wenn Sie von einer Editionen mit Untereditionen (beispielsweise 'Cyber Protect (pro Workload)') wechseln, werden die Quotas zusammengefasst.</p>	Die Quotas werden vom Quell- zum Ziel-Angebotsselement repliziert.
Nutzung wechseln	Die Angebotsselemente 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 Angebotsselemente.

Quell-Angebotsselemente – Nutzung/Quota	Ziel-Angebotsselemente – Nutzung/Quota
Cyber Protect Advanced Workstation 8/10	<ul style="list-style-type: none"> • Workstation – 8/10 • Advanced Security – 2/10 • Advanced Backup Workstation – 1/10 • Advanced Management – 3/10

Folgende Schritte wurden während der Umstellung ausgeführt:

1. Die Angebotsselemente, die die Funktionalität abdecken, die in der Quell-Edition verfügbar war, wurden automatisch aktiviert.
2. Die Quota wurde zu den neuen Angebotsselementen repliziert.
3. Die Nutzung wurde entsprechend der tatsächlichen Nutzung in Schutzplänen abgeglichen: drei Workloads verwenden Funktionen des Advanced Management-Pakets, zwei verwenden Funktionen des Advanced Security-Pakets und ein Workload 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-Angebotsselemente – Nutzung/Quota	Ziel-Angebotsselemente – Nutzung/Quota
Cyber Protect Essentials Workstation - 6/12	<ul style="list-style-type: none">• Workstation – 14/42• Advanced Backup Workstation – 2/42• Advanced Security – 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 Angebotsselemente, die die Funktionalität abdecken, die in allen Quell-Editionen verfügbar war, wurden automatisch aktiviert. Bei den Abrechnungsmodi können einem Workload je nach Bedarf mehrere Angebotsselemente 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 Angebotsselemente.
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 Angebotsselemente aktivieren oder deaktivieren.
- Zu einem komplett neuen Abrechnungsmodus wechseln.

Weitere Informationen über die Bearbeitung der verfügbaren Angebots Elemente finden Sie im Abschnitt '[Angebots Elemente 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.

Angebots Elemente und Quota-Verwaltung

In diesem Abschnitt wird Folgendes beschrieben:

- Was sind Services und Angebots Elemente?
- Wie werden Angebots Elemente 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 Angebots Element-Verfügbarkeit die Installer-Verfügbarkeit in der Service-Konsole?

Services und Angebots Elemente

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. 6)'.

Angebotsselemente

Ein Angebotsselement ist eine Zusammenstellung von Service-Funktionen, die nach bestimmten Workloadtypen oder Funktionalitäten (z.B. Storage, Disaster Recovery-Infrastruktur und andere) gruppiert sind. Indem Sie bestimmte Angebotsselemente 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. 70)'.

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

Abrechnungsmodi und Editionen

Bei den Legacy-Editionen können Sie ein Angebotsselement pro Workload aktivieren. Bei den Abrechnungsmodi ist die Funktionalität aufgeteilt, sodass Sie mehrere Angebotsselemente (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. 7)'.

Sie können entweder Abrechnungsmodi oder Editionen verwenden, um zu konfigurieren, welche Services für Ihre Mandanten verfügbar sind. Sie können nur einen Abrechnungsmodus oder eine Edition 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 Angebotsselement begrenzen wollen, können Sie Quotas für dieses Angebotsselement definieren. Siehe Abschnitt "'Weiche und harte Quotas" (S. 14)'.

Angebotsselemente aktivieren oder deaktivieren

Sie können alle für eine bestimmte Edition oder Abrechnungsmodus verfügbaren Angebotsselemente 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.	Backup und Recovery von Datenquellen (inkl. Microsoft 365 und Google Workspace) wird innerhalb eines Kunden-Mandantens 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.

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 Ordnersebenen 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.

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. 20)'.

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 Angebots-elementen zu Ressourcentypen funktioniert grundsätzlich folgendermaßen: das System vergleicht die verfügbaren Angebots-elemente mit dem Ressourcentyp – und erwirbt dann die Quota für das passende Angebots-element.

Es besteht außerdem die Möglichkeit, eine andere Angebots-element-Quota zuzuordnen, auch wenn diese nicht genau zum Ressourcentyp passt. Dies wird **Backup Quota-Transformation** genannt. Wenn es kein passendes Angebots-element 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 Service-Konsole die Service-Quota dem Ressourcentyp manuell zuordnen.

Beispiel

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

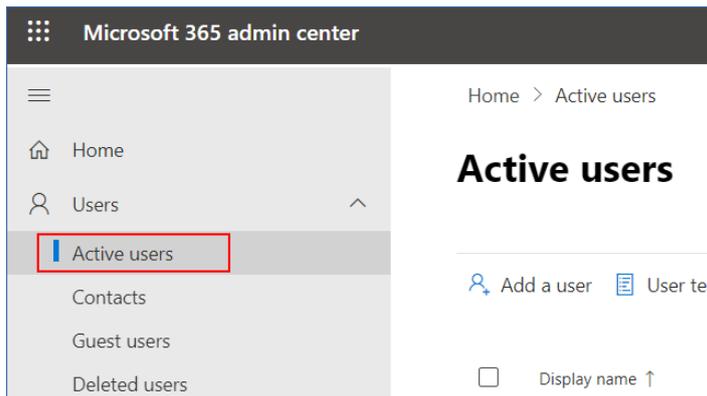
Das System wird zuerst prüfen, ob es eine zugewiesene Quota vom Typ '**Virtuelle Maschine**' gibt. Wenn diese nicht gefunden wird, versucht das System automatisch, die Quota **Workstations** zu erwerben. Wenn auch diese nicht zu finden ist, wird die andere Quota nicht mehr automatisch erworben. Wenn 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 Service-Konsole anmelden und die Quota **Server** manuell zuweisen.

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

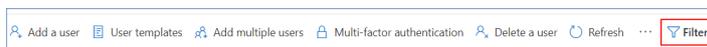
Sie können alle nicht lizenzierten Benutzer in Ihrer Microsoft 365-Organisation daran hindern, sich anzumelden, indem Sie deren Anmeldestatus bearbeiten.

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. Wählen 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-Angebots Elemente 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 Größe des „Cold Storage“ für diejenigen Server an, die per Disaster Recovery geschützt werden. Dieser Storage wird ab dem Zeitpunkt berechnet, an dem ein Recovery-Server erstellt wird (unabhängig davon, ob der Server gerade läuft oder nicht). 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-Adressen** 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 Service-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**

Diese Quota definiert eine Anzahl von Benutzern, die auf diesen Service zugreifen dürfen. Administratorkonten werden nicht als Teil dieser Quota mitgezählt.

- **Cloud Storage**

Dies ist ein Cloud Storage zum Speichern von Benutzerdateien. Die Quota definiert, wie viel Speicherplatz einem Mandanten im Cloud Storage zugewiesen ist.

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**

Der Notary Storage ist derjenige Cloud Storage, in dem die beglaubigten Dateien, signierten Dateien und die Dateien, deren Beglaubigung oder Signierung gerade durchgeführt wird, gespeichert werden. Diese Quota definiert den maximalen Speicherplatz, den diese Dateien belegen dürfen.

Wenn Sie die Quota-Nutzung verringern wollen, können Sie bereits beglaubigte oder signierte Dateien aus dem Notary Storage löschen.

- **Beglaubigungen**

Diese Quota 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 ausgeführt' geändert wurde.

Wenn dieselbe Datei mehrfach beglaubigt wird, gilt jede Beglaubigung wie eine neue gezählt.

- **eSignaturen**

Diese Quota definiert die maximale Anzahl von Dateien, die mithilfe des Notary Service signiert werden können. Eine Datei gilt als signiert, sobald diese zur Signierung versendet wurde.

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 Angebotsselemente, 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-Betriebssystem ausgeführt wird, wird die Quota **Server** zugewiesen.
- Einer physischen Maschine, auf der ein Windows-Desktop-Betriebssystem 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 Protection Service-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 **Lizenz 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 Protection Service-Konsole zu **Geräte**.
2. Wählen Sie mehr als eine Maschine aus und klicken Sie dann auf **Quota zuweisen**.
3. Wählen Sie im Fenster **Lizenz ändern** die gewünschte Service-Quota oder **Keine Quota** aus – und klicken Sie dann auf **Ändern**.

Abhängigkeit der Agenten-Installer von den Angebotselementen

Welcher Agenten-Installer in der Service-Konsole im Bereich **Geräte hinzufügen** verfügbar ist, hängt davon ab, welche Angebotselemente erlaubt sind. In der unteren Tabelle können Sie die Agenten-Installer und deren Verfügbarkeit in der Service-Konsole sehen – je in Abhängigkeit von den aktivierten Angebotselementen.

Aktiviertes Angebotselement	Server	Workstations	Virtuelle Maschinen	Microsoft 365-Arbeitsplätze	Google Workspace-Arbeitsplätze	Mobilgeräte	Webhosting-Server	Websites
Agenten-Installer								
Workstations – Agent für Windows		+	+					+
Workstations – Agent für Mac OS		+	+					+
Server – Agent für Windows	+		+				+	+
Server – Agent für Linux	+		+				+	+
Agent für Hyper-V			+					
Agent für VMware			+					

Agent für Virtuozzo			+					
Agent für SQL	+		+					
Agent für Exchange	+		+					
Agent für Active Directory	+		+					
Agent für Microsoft 365				+				
Agent für Google Workspace					+			
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 später)
- 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 Anmeldeame.** Dies ist der Benutzername, mit dem Sie sich anmelden. Ihr Anmeldeame 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. 26)'.
'

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 Anmeldeamen, 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.
Die Adresse der Anmeldeseite war in der Aktivierungs-E-Mail-Nachricht enthalten, die Sie erhalten haben.
2. Geben Sie den Anmeldenamen ein und klicken Sie dann auf **Weiter**.
3. 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.

4. 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 Protection-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 Protection-Konsole umgeleitet.

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.

Name	Tenant status	Billing mode / Edition	2FA status	Management mode	7-day hi
Acme	Active	Per workload	Disabled	By service provider	No back
Partner tenant	Active	Per workload, Per gigabyte	Disabled	By service provider	
B Partner tenant	Active	(Legacy) Cyber Protect Edition (a...	Disabled	By service provider	
B Customer	Active	Per workload	Disabled	By service provider	No back
Br Partner	Active	Per workload, Per gigabyte, (Legacy) ...	Disabled	By service provider	
Customer	Active	Per workload	Disabled	By service provider	No back
D Customer	Active	(Legacy) Cyber Backup - Standar...	Disabled	By service provider	No back
Enhanced	Active	(Legacy) Cyber Protect Edition (a...	Disabled	By service provider	No back

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.

Den Zugriff auf die Weboberfläche einschränken

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.

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

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.

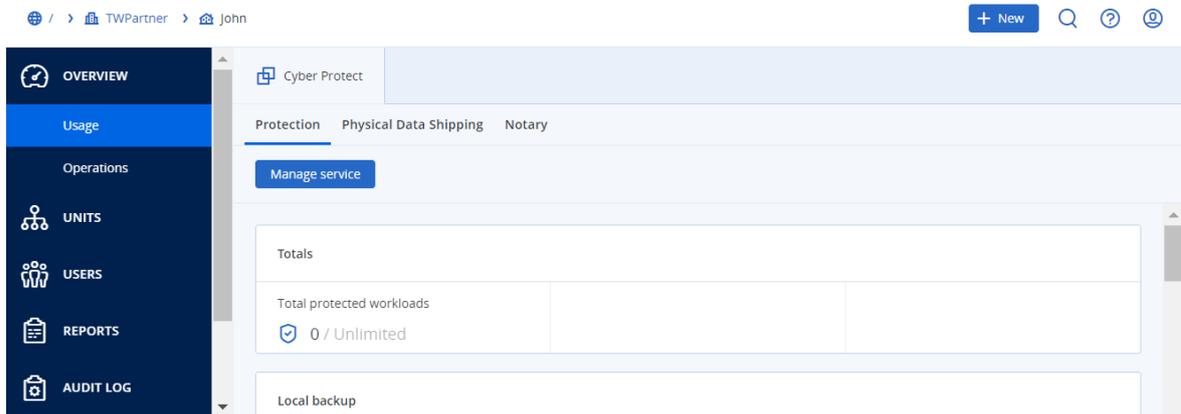
So verwalten Sie mit der Registerkarte 'Überblick' einen Service für einen Mandanten

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.

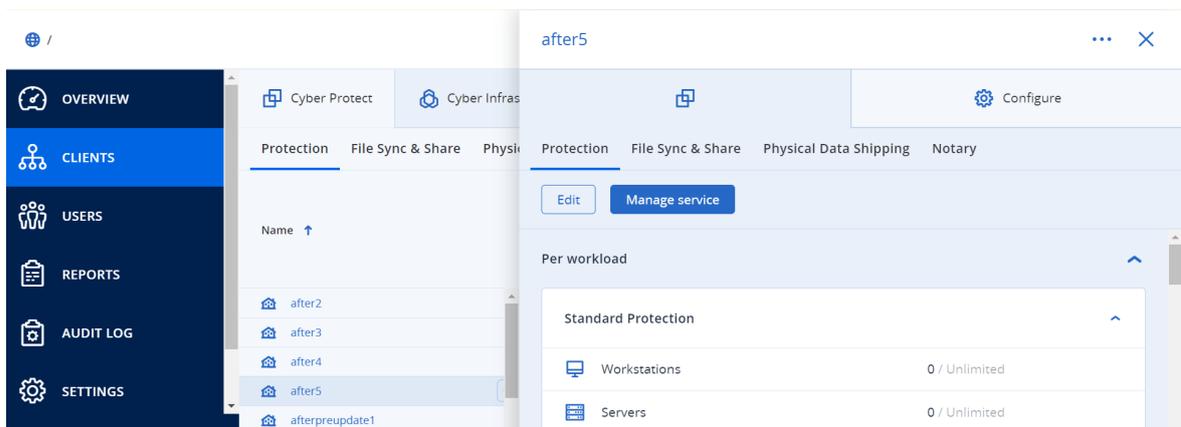


Registerkarte Clients

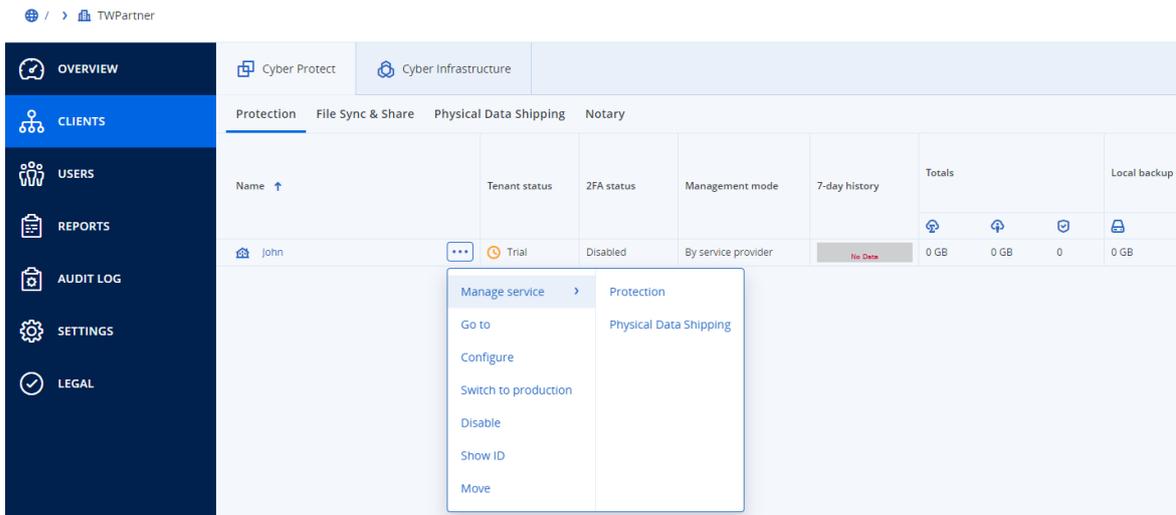
Die Registerkarte **Clients** zeigt die Untermantanten des Mandanten an, in dem Sie arbeiten, und ermöglicht Ihnen auf die Services in diesen Mandanten zuzugreifen.

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-Verlaufsleiste** 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-Verlaufsleiste** wird so lange 'Keine Backups' angezeigt, bis die entsprechenden Statistiken erfasst wurden.

Bei Partner-Mandanten bleibt die **7-Tage-Verlaufsleiste** 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.

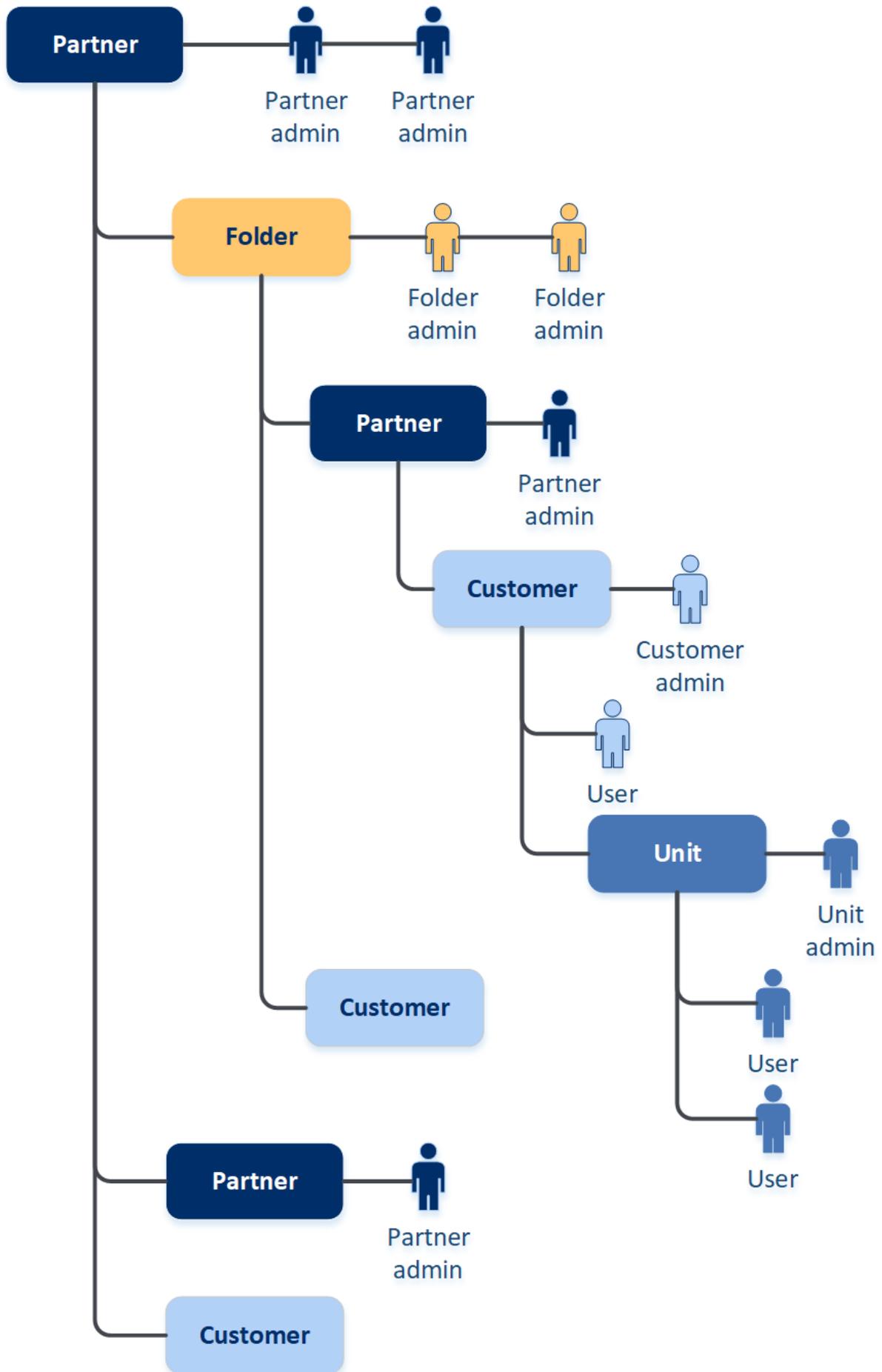
Jedes Konto gehört zu einem Mandanten. Ein Mandant ist ein Teil der Management Server-Ressourcen (wie Benutzerkonten und Untermantanten) und Service-Angebote (aktivierte Services und Angebotselemente in diesen), die für einen Partner oder Kunden bestimmt sind. Die Mandanten-Hierarchie soll die Kunde-/Dienstleister-Beziehung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



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

*Ein Partner-Administrator, der diese Aktionen durchführen muss, kann einen Kunden-Administrator oder ein Benutzerkonto für sich selbst erstellen.

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 Angebotsselemente 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.
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. Monatliche Service-Nutzungsberichte enthalten keine Nutzungsdaten von Mandanten im Testmodus.

Wichtig

Falls Sie den Modus in der Mitte eines Monats von 'Test' auf 'Produktion' umschalten, wird der gesamte Monat in den monatlichen Service-Nutzungsbericht aufgenommen. Wir empfehlen daher, dass Sie den Modus am ersten Tag eines Monats umschalten. Der Modus wird automatisch auf 'Produktion' umgestellt, wenn ein Mandant für einen kompletten Monat im Testmodus bleibt.

Es gibt zwei mögliche Szenarien, um den Testmodus der Mandanten automatisch auf den Produktionsmodus umschalten zu lassen:

- In der Mitte eines Monats. In diesem Fall wird der komplette **nächste** Monat ebenfalls in den monatlichen Service-Nutzungsbericht aufgenommen.
- [Empfohlene Option] Am ersten Tag eines Monats – dann wird nur der aktuelle Monat gezählt.

-
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.
- 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 Untermantanten 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 Zwei-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 beim Erstellen eines Kunden-Mandanten im Modus 'Erhöhte Sicherheit'] Aktivieren Sie bei **Sicherheit** das Kontrollkästchen **Erhöhter Sicherheitsmodus**.

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: "Erhöhter Sicherheitsmodus" (S. 38).

Wichtig

Sie können den erhöhten Sicherheitsmodus nicht wieder 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 einen Anmeldenamen sowie eine E-Mail-Adresse für das Administratorkonto ein. Die übrigen Felder sind optional, bieten aber weitere Kommunikationskanäle, falls wir den Administrator kontaktieren müssen.
- b. Wählen Sie eine Sprache aus. Wenn Sie keine Sprache auswählen, wird standardmäßig Englisch verwendet.
- c. 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. 39)".

Erhöhter Sicherheitsmodus

Der Modus 'Erhöhte Sicherheit' bietet spezielle Einstellungen für Clients mit erhöhten Sicherheitsanforderungen. In diesem Modus müssen alle Backups zwingend verschlüsselt werden und dürfen die Verschlüsselungskennwörter nur lokal festgelegt werden.

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

Im erhöhten Sicherheitsmodus 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 ihre Verschlüsselungskennwörter nur auf den geschützten Geräten festlegen. Es können keine Verschlüsselungskennwörter über Schutzpläne festgelegt werden.

Cloud Services können nicht auf die Verschlüsselungskennwörter zugreifen. Aufgrund dieser Einschränkung sind folgende Funktionen für Mandanten im erhöhten Sicherheitsmodus nicht verfügbar:

- Wiederherstellungen über die Service-Konsole
- Durchsuchen von Backups auf Dateiebene über die Service-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

Einschränkungen

- Der erhöhte Sicherheitsmodus ist nur mit Agenten kompatibel, deren Version 15.0.26390 oder höher ist.
- Der erhöhte Sicherheitsmodus ist nicht für Geräte verfügbar, die unter Red Hat Enterprise Linux 4.x oder 5.x (und deren Derivaten) laufen.

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 Untermantanten 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. 41)'.

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 Untermantanten) 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 Angebotsselemente für die ausgewählten Services mit einer unbegrenzten Quota aktiviert.
 - Um die Angebotsselemente für den Mandanten zu konfigurieren, klicken Sie auf **Weiter**. Siehe Abschnitt "'Die Angebotsselemente für einen Mandanten konfigurieren' (S. 40)'.

Die Angebotelemente für einen Mandanten konfigurieren

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

Diese Prozedur ist nicht für einen Abteilungs-Mandanten anwendbar.

So können Sie die Angebotelemente für einen Mandanten konfigurieren

1. Deaktivieren Sie im Bereich **Services konfigurieren** des Dialogs 'Mandant erstellen/bearbeiten' bei jeder Service-Registerkarte die Kontrollkästchen für diejenigen Angebotelemente, die Sie deaktivieren wollen.

Die den deaktivierten Angebotelementen entsprechenden Funktionalitäten werden für die Benutzern innerhalb des Mandanten (und seiner Untermantanten) nicht verfügbar sein.

Hinweis

Sie können Angebotelemente deaktivieren, die mit der Advanced Protection-Funktionalität in Verbindung stehen. Die Angebotelemente werden jedoch automatisch wieder aktiviert, wenn ein Benutzer eine Advanced-Funktion in einem Schutzplan aktiviert.

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 Angebotelement 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 Angebotelements 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 Angebotsselemente 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**.

1. Select services

Select the services and editions that you want to enable for the selected tenants.

Cyber Protect

 All-in-one cyber protection solution that integrates advanced data protection, file sync and share, file notarization and e-signing, and physical data shipping functionality. 

Protection

Provides all aspects of cyber protection for workloads through backup, antivirus, antimalware, anti-ransomware, monitoring, management, and disaster recovery functionality.

Per workload

The billing is based on the number of protected workloads, and cloud storage is charged separately.

Add advanced protection:

- Advanced Backup 
- Advanced Management 
- Advanced Security + EDR  
- Advanced Security 
- Advanced Email Security 
- Advanced Data Loss Prevention  

Hinweis

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

5. Wählen Sie im Bereich **Services konfigurieren** die Service-Funktionen und Angebotsselemente 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 Angebotsselemente einsehen wollen, die angewendet werden sollen. Alternativ können Sie die Anzeige für jeden Mandanten erweitern, wenn Sie die ausgewählten Services und Angebotsselemente 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 Angebotsselemente angezeigt, die gerade konfiguriert werden.

<input checked="" type="checkbox"/>	 autotest_partner_e1e984d4	 Configuring
<input checked="" type="checkbox"/>	 autotest_partner_eb104e9b	 Configuring
<input checked="" type="checkbox"/>	 dba	 Configuring
<input checked="" type="checkbox"/>	 ddLegacyPartner1	 Configuring

8. Wenn die Konfiguration der Services und Angebots Elemente erfolgreich auf die ausgewählten Mandanten angewendet wurde, wird eine Bestätigungsmeldung angezeigt.

Wenn die Services und Angebots Elemente 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.

Benachrichtigungen über Wartungsaktivitäten aktivieren

Als Partner-Benutzer können Sie Ihren Untermantanten (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. Es 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 Untermantanten 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. Es 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 Mandanten 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 Untermantanten werden deaktiviert und deren Services gestoppt.
- Die Abrechnung mit dem Mandanten und seinen Untermantanten wird fortgesetzt, da dessen/deren Daten in Cyber Protect Cloud aufbewahrt und gespeichert werden.
- Alle API-Clients innerhalb des Mandanten und dessen Untermantanten werden deaktiviert und alle Integrationen, die diese Clients verwenden, werden nicht mehr funktionieren.

Wenn Sie einen Mandanten 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 Angebots-elementen 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 möchten, ob diese Aktion möglich ist, wenden Sie sich an Ihren Kundenbetreuer bei .
- 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 Mandanten-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, Untermantanten 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 beschränkt ist, können die Administratoren des übergeordneten Mandanten nur noch die Mandanten-Eigenschaften ändern. Sie können weder die Konten noch Untermantanten 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 begrenzten 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.

Wenn der Schalter **Support-Zugang** aktiviert ist, erhalten die Administratoren der übergeordneten Mandanten vollständigen Zugriff auf Ihren Mandanten. Dadurch können Sie Folgendes tun: Eigenschaften ändern; Mandanten, Benutzer und Services verwalten; auf Backups und andere Ressourcen zugreifen.

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](#)'.

Wichtig

Das Löschen eines Mandanten kann nicht rückgängig gemacht werden!

So können Sie einen Mandanten 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 Untermantanten werden gelöscht.
- Alle Services, die innerhalb des Mandanten und dessen Untermantanten aktiviert waren, werden gestoppt.
- Alle Benutzer in dem Mandanten und seinen Untermantanten werden gelöscht.
- Die Registrierung aller Maschinen in dem Mandanten und seinen Untermantanten wird aufgehoben.
- Alle Service-bezogenen Daten (z.B. Backups und synchronisierte Dateien) in dem Mandanten und seinen Untermantanten werden gelöscht.
- Alle API-Clients innerhalb des Mandanten und dessen Untermantanten werden gelöscht und alle Integrationen, die diese Clients verwenden, werden nicht mehr funktionieren.

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. 29)'.
Alternativ können Sie auch zu **Unternehmensverwaltung** -> **Benutzer** gehen und auf den Befehl + **Neu** klicken.
3. Klicken Sie in der rechten oberen Ecke auf **Neu** -> **Benutzer**.
4. Spezifizieren Sie die nachfolgenden Kontaktinformationen für das Konto:

- **Anmeldename**

Wichtig

Jedes Konto benötigt einen eindeutigen Anmeldenamen.

- **E-Mail**

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.

- **Vorname**

- **Nachname**

- [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.

- [Optional] **Position**

- 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

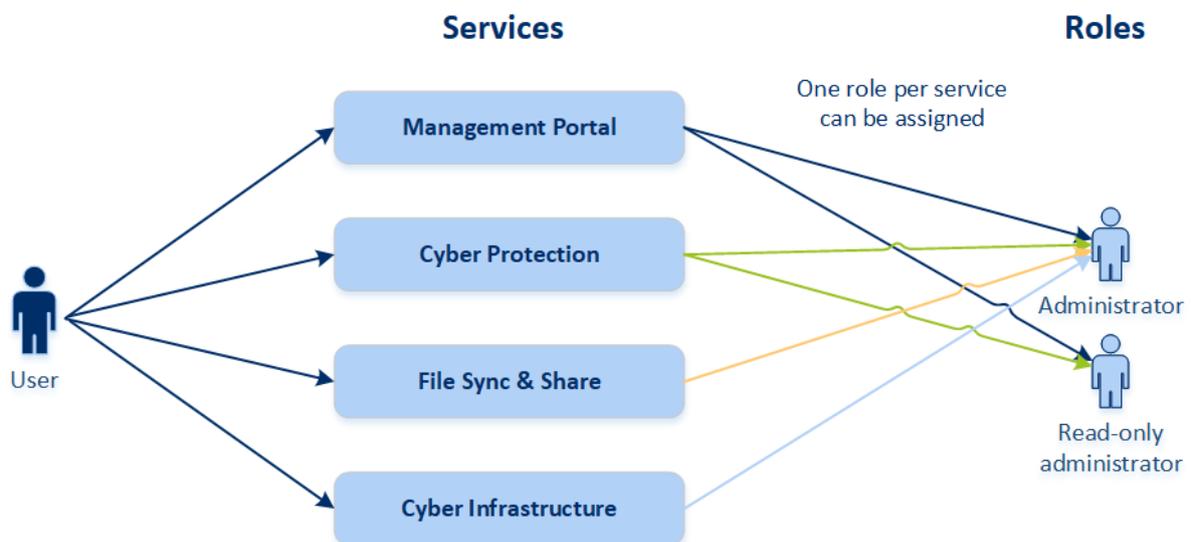
1. Gehen Sie im Management-Portal zu **Unternehmensverwaltung** –> **Benutzer**.

- 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**.
- 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	Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf alle Objekte im Management-Portal des Partners und auf das

	Partnerebene	Management-Portal aller Kunden dieses Partners. Solche Benutzer können im Nur-Lesen-Modus auf die Daten anderer Benutzer der Organisationen zugreifen.
	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.
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.
	Operator wiederherstellen	Die Rolle ermöglicht den Zugriff auf Backups von Microsoft 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.

Nur-Lesen-Administrator-Rolle

Ein Konto mit dieser Rolle hat nur einen Lesezugriff auf die Cyber Protection-Webkonsole 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 Untermantanten 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 Widerrufen Deaktivieren Stopp	Erstellen Bearbeiten Anwenden Aktivieren Ausführen Löschen Widerrufen Deaktivieren Stopp	Erstellen Bearbeiten Anwenden Aktivieren 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	Anzeigen Ausführung abbrechen	Erstellen Bearbeiten Anwenden

		Stopp		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 Service-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	Kundenadministrator
Benachrichtigungen für eigene Geräte	Ja	Ja
Benachrichtigungen für alle Geräte in der Organisation	n/a	Ja (außer Sicherheitsvorfall-Benachrichtigungen)
Benachrichtigungen für Microsoft 365, Google Workspace und andere Cloud-basierte Backups	n/a	Ja

Benachrichtigungstyp\Benutzerrolle	Benutzer	Kunden- und Abteilungsadministratoren	Partner- und Ordner-Administrator
Benachrichtigungen für eigene Geräte	Ja	Ja	n/a*
Benachrichtigungen für alle Geräte der Untermantanten	n/a	Ja	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 Benachrichtigungen 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](#)'.

Wichtig

Das Löschen eines Benutzerkontos kann nicht rückgängig gemacht werden!

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:

- Das Benutzerkonto wird gelöscht.
- Alle Daten, die zu diesem Benutzerkonto gehören, werden gelöscht.
- Die Registrierung aller Maschinen, die mit diesem Benutzerkonto assoziiert sind, wird aufgehoben.

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 herkömmliches 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 alternativ auch den geheimen TOTP-Schlüssel (das „Geheimnis“) 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 den geheimen TOTP-Schlüssel; verwenden Sie eine Applikation, die die Sicherung von Codes per Cloud Backup unterstützt). Sie benötigen den geheimen TOTP-Schlüssel, um die Zwei-Faktor-Authentifizierung zurücksetzen zu können, falls das Zwei-Faktor-Gerät verloren gehen sollte.

6. Der einmalige 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 in der Anzeige '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.

Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben

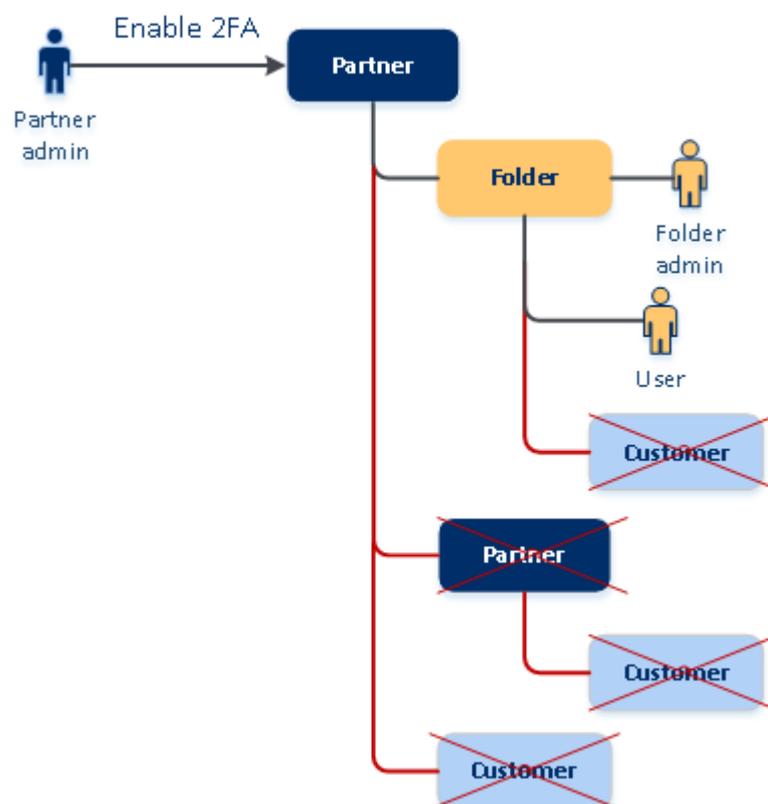
Die Zwei-Faktor-Authentifizierung wird auf der Ebene der **Organisation** (Unternehmensebene) eingerichtet. Sie können die Zwei-Faktor-Authentifizierung aktivieren oder deaktivieren:

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

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

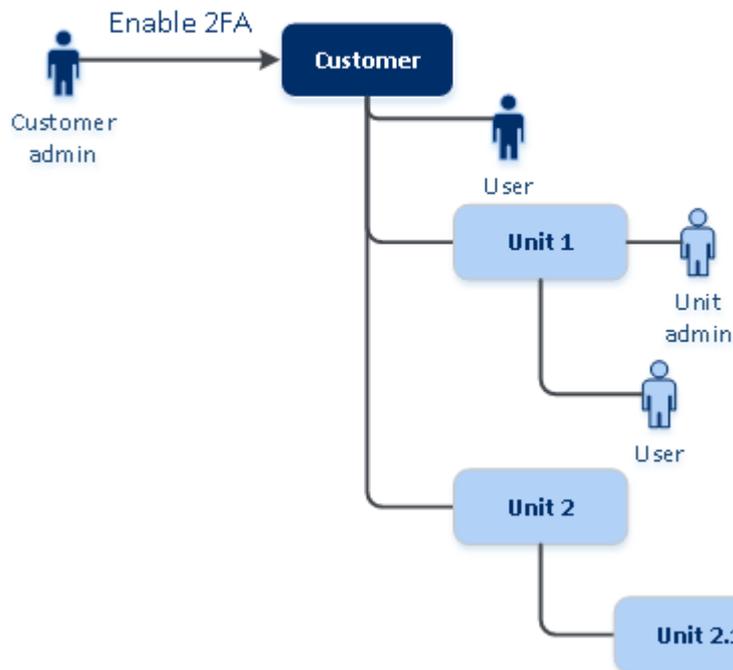
- Ordner übernehmen automatisch die Zwei-Faktor-Authentifizierungseinstellungen von ihrer Partnerorganisation. Im nachfolgenden Schema bedeuten die roten Linien, dass keine Zwei-Faktor-Authentifizierungseinstellungen weitergereicht werden können.

2FA setting propagation from a partner level



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

2FA setting propagation from a customer level



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 Zwei-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-Schutzmechanismus 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 Service-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 Service-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 Service-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

Die Liste kann in der Service-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.

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 Angebotsselement **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 Untermantanten 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.

Unveränderlichen Storage konfigurieren

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

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**

In diesem Modus kann ein Administrator den unveränderlichen Storage deaktivieren und wieder aktivieren sowie dessen Modus und Aufbewahrungsdauer ändern.

- **Compliance-Modus**

Wenn dieser Modus ausgewählt wurde, kann der unveränderliche Storage nicht mehr deaktiviert werden. Außerdem können weder dessen Modus noch die Aufbewahrungsdauer geändert werden.

Wenn für einen untergeordneten Mandanten keine benutzerdefinierten Einstellungen angewendet werden, wird dieser die Einstellungen des übergeordneten Mandanten übernehmen.

Sie können die Einstellungen für den unveränderlichen Storage nur konfigurieren, wenn für den Mandanten, zu dem das Administratorkonto gehört, die Zwei-Faktor-Authentifizierung aktiviert ist.

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

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.

So können Sie den unveränderlichen Storage für einen Partner-Mandanten aktivieren

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 999 Tagen.
Die standardmäßige Aufbewahrungsdauer beträgt 14 Tage. Eine längere Aufbewahrungsdauer kann zu einer erhöhten Speichernutzung führen.
4. Klicken Sie auf **Speichern**.

So können Sie den unveränderlichen Storage für einen Partner-Mandanten deaktivieren

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

Warnung!

Diese Änderung wird an alle Untermantanten vererbt, die keine benutzerdefinierten Einstellungen für den unveränderlichen Storage verwenden. Alle gelöschten Backups werden dauerhaft gelöscht. Auch das Löschen neuer Backups wird dann dauerhaft sein.

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

So können Sie den unveränderlichen Storage für einen Kunden-Mandanten aktivieren

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 999 Tagen.
Die standardmäßige Aufbewahrungsdauer beträgt 14 Tage. Eine längere Aufbewahrungsdauer kann zu einer erhöhten Speichernutzung führen.
6. Wählen Sie den Modus für den unveränderlichen Storage.

Warnung!

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

7. Klicken Sie auf **Speichern**.

So können Sie den unveränderlichen Storage für einen Kunden-Mandanten deaktivieren

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!

Wenn Sie den unveränderlichen Storage deaktivieren, werden alle gelöschten Backups dauerhaft entfernt. Auch das Löschen neuer Backups wird dann dauerhaft sein.

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

Einschränkungen

- Der unveränderliche Storage ist sowohl für von Acronis gehostete als auch für von Partnern gehostete Storages verfügbar, die Acronis Cyber Infrastructure Version 4.7.1 oder höher verwenden.
Für den unveränderlichen Storage muss der TCP-Port 40440 für den Backup Gateway Service in Acronis Cyber Infrastructure geöffnet sein. Ab Version 4.7.1 wird der TCP-Port 40440 automatisch mit dem Traffic-Typ **Backup (ABGW) öffentlich** geöffnet. Weitere Informationen über 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.

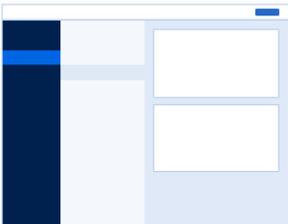
Branding und White-Labeling konfigurieren

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.

Branding

[White label](#) | [Reset to defaults](#) | [Disable branding](#)

i The branding options will be applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.

Appearance	
Service name	Mega Cloud ✎
Web console logo <small>.png, .jpeg, .gif, 224x64 px</small>	<div style="text-align: center;">  </div> 📁 Upload
Favourite Icon <small>.jpg, .ico, .png, .svg 32x32px</small>	<div style="text-align: center;">  ✕ </div> 📁 Upload
Color scheme	<div style="text-align: center;">  </div> ✎

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 Untermantanten 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 **Willkommenseite** 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 Willkommenseite 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 aufzupgraden. 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 Service auf **Hinzufügen** -> **iOS** klickt.
- **Google Play Store**. Diese Seite wird geöffnet, wenn der Benutzer im 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 TLS-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 Untermantanten 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) und der Cyber Protection Monitor (für Windows, macOS und Linux) für all Ihre Partner und Kunden per Branding oder White-Labeling angepasst wird. Wenn Sie White-Labeling aktivieren, wird der Agent und Tray Monitor ohne die Kennzeichnung auf Acronis 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. Klicken Sie 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.
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.

Agenten automatisch aktualisieren

Cyber Protect hat drei Arten von Agenten, die auf geschützten Maschinen installiert werden können: den Agenten für Windows, den Agenten für Linux und den Agenten für Mac.

Cyber Files Cloud verfügt über eine Windows- und eine macOS-Version des Desktop-Agenten für File Sync & Share. Damit können Dateien und Ordner zwischen einer Maschine und dem File Sync & Share Cloud Storage eines Benutzers synchronisiert werden, um Offline-Arbeiten und andere moderne Arbeitskonzepte – wie Homeoffice-Arbeit oder die sichere berufliche Nutzung von privaten Geräten (BYOD-Konzepte) zu unterstützen.

Wenn Sie sich die Verwaltung mehrerer Workloads erleichtern wollen, können Sie konfigurieren (oder auch komplett deaktivieren), dass alle Agenten auf sämtlichen Maschinen automatisch und unbeaufsichtigt aktualisiert werden sollen.

Wichtig

Derzeit haben nur Partner und Kunden, bei denen der Schutz aktiviert ist, Zugriff auf die Verwaltungsfunktion für Agenten-Updates.

Hinweis

Wie Sie die Agenten auf einzelnen Maschinen verwalten und die Einstellungen für die automatische Aktualisierung der Agenten anpassen können, erfahren Sie im Abschnitt Update der Agenten in der [Benutzeranleitung für Cyber Protect](#).

So können Sie Agenten automatisch aktualisieren lassen

Hinweis

Die Einstellungen für die automatische Aktualisierung des Agenten für File Sync & Share werden an die Partner und Kunden übertragen, die die Schutzfunktion nicht aktiviert haben.

So können Sie die automatische Aktualisierung der Agenten von der Einstiegsseite des Management-Portals aus festlegen

1. Wählen Sie **Einstellungen** -> **Agenten-Update**.

Update channel

Current
The most up-to-date version of agents.

Previous release
The latest version of the agents from the previous release.

Automatically update agents
Agents will be automatically updated during the specified maintenance window.

Maintenance window
New versions will be installed only in the set timeframe.

From 23:00 To 08:00

Mon Tue Wed Thu Fri Sat Sun

Save Cancel [Reset to default settings](#)

2. Wählen Sie aus, welche Version für die automatischen Updates erkannt werden soll: entweder **Aktuell** oder **Vorherige Version**.
(Die Standardeinstellung ist **Aktuell**.)
3. Schalten Sie die Option **Agenten automatisch aktualisieren** ein.
(Die Standardeinstellung ist **An**.)
4. Bestimmen Sie das Zeitfenster für den Wartungsvorgang.
(Das Standardzeitfenster liegt zwischen 23:00 und 08:00.)

Hinweis

Obwohl die Prozesse zur Aktualisierung der Agenten so konzipiert wurden, dass sie schnell und reibungslos ablaufen, empfehlen wir einen Zeitrahmen zu wählen, der die Benutzer möglichst wenig stört. Denn die Benutzer selbst können die automatischen Updates weder verhindern noch aufschieben.

5. [Optional] Wählen Sie bestimmte Tage aus, an denen die automatischen Updates stattfinden sollen.
6. Wählen Sie den Befehl **Speichern** aus.

Hinweis

Die Möglichkeit für automatische Updates ist nur für folgende Agenten verfügbar:

- Die Agenten für Cyber Protect mit der Version 15.0.26986 (veröffentlicht im Mai 2021) und höher.
- Den Desktop Agenten für File Sync & Share mit der Version 15.0.30370 oder höher.

Ältere Agenten müssen zuerst noch manuell auf die neueste Version aktualisiert werden, bevor die automatische Update-Funktion genutzt werden kann.

So können Sie die Agenten-Updates überwachen

Wichtig

Die Agenten-Updates können nur durch die Administratoren von Kunden und Partnern überwacht werden, die das Schutzmodul aktiviert haben.

Wie Sie die Aktualisierungen des Agenten überwachen können, ist in den Abschnitten für Alarmmeldungen und Aktivitäten in der [Benutzeranleitung für Cyber Protect](#) beschrieben.

Monitoring

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

Nutzung

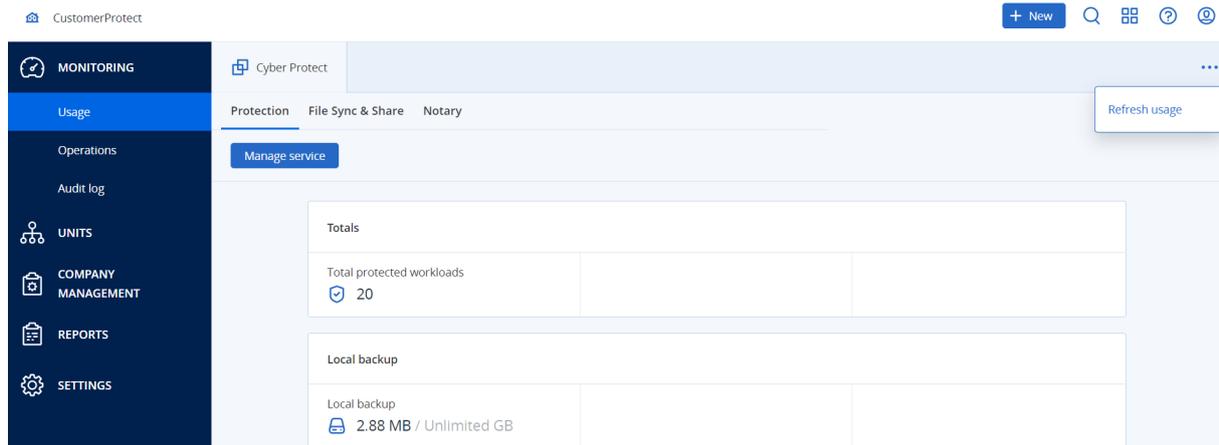
Die Registerkarte **Nutzung** ermöglicht Ihnen einen Überblick über die Service-Nutzung und auf die Services zuzugreifen, die für den Mandanten, in dem Sie arbeiten, verfügbar sind.

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

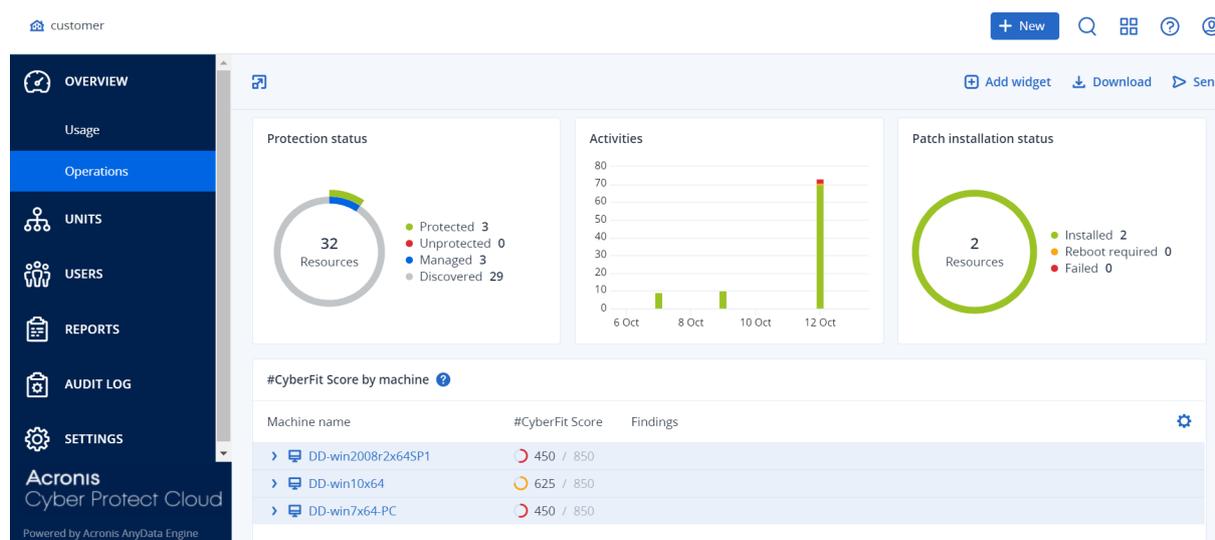
Das Dashboard **Aktionen** enthält eine Reihe benutzerdefinierbarer Widgets, die Ihnen einen Überblick über diejenigen Aktionen geben, die im Zusammenhang mit dem Cyber Protection Service stehen. Widgets für andere Services werden in zukünftigen Versionen verfügbar sein.

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 Widget 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

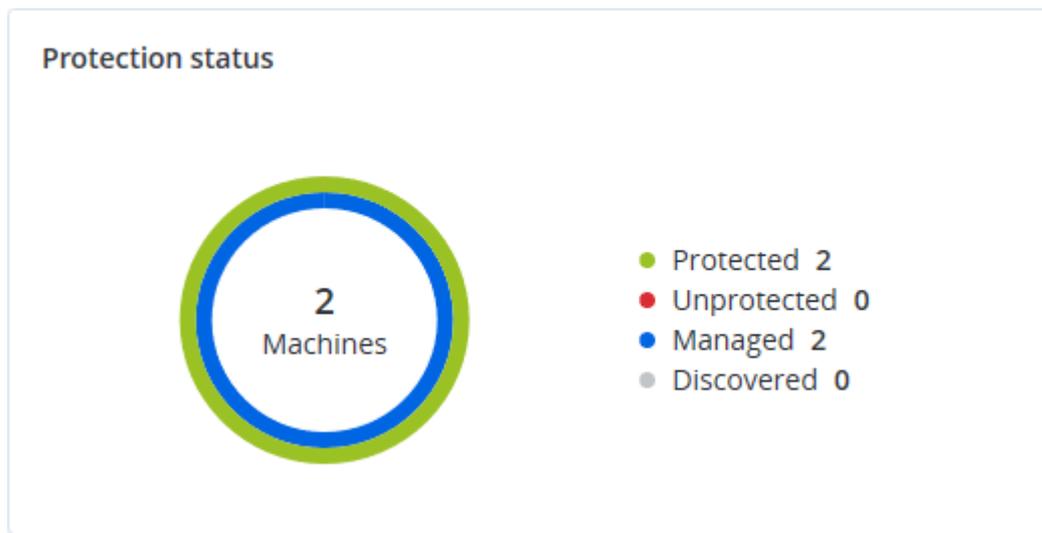
Schutzstatus

Dieses Widget zeigt den aktuellen Sicherheitsstatus 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	

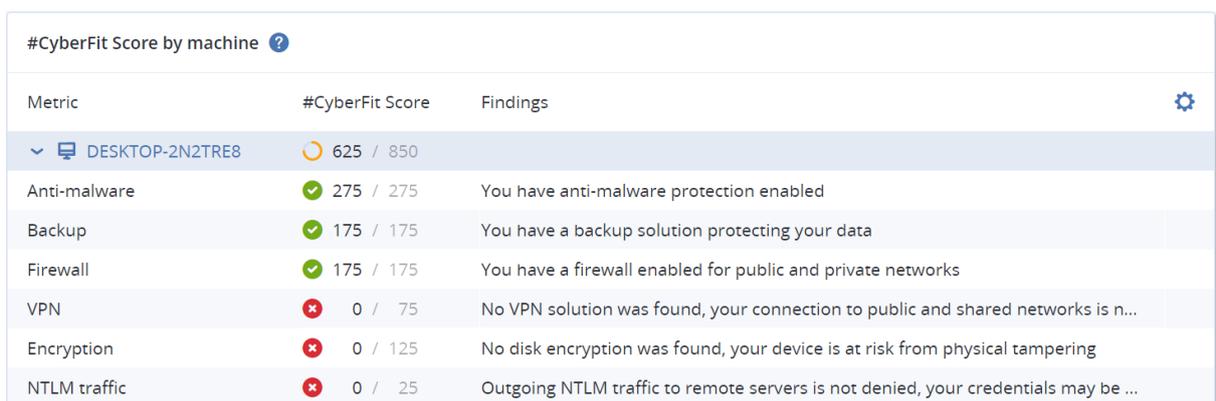
#CyberFit-Score pro Maschine

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](#)'.



Metric	#CyberFit Score	Findings	
DESKTOP-2N2TRE8	625 / 850		
Anti-malware	275 / 275	You have anti-malware protection enabled	
Backup	175 / 175	You have a backup solution protecting your data	
Firewall	175 / 175	You have a firewall enabled for public and private networks	
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...	
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering	
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...	

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.

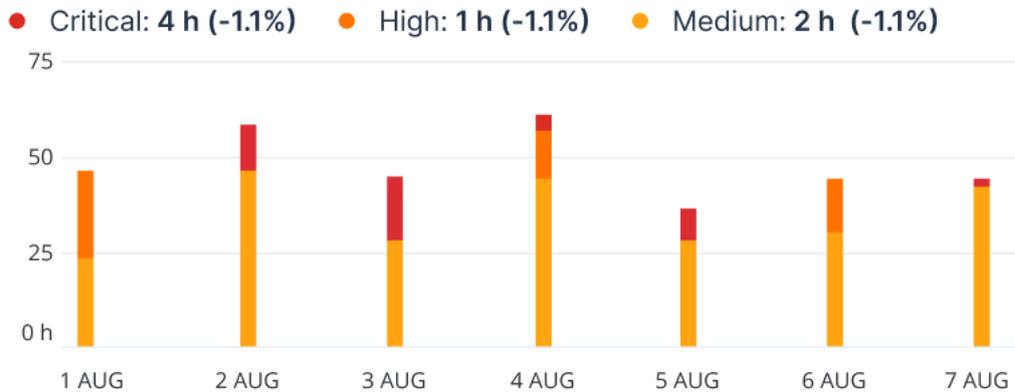


MTTR (Mittlere Problemlösungszeit) für Vorfälle

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.

Incident MTTR

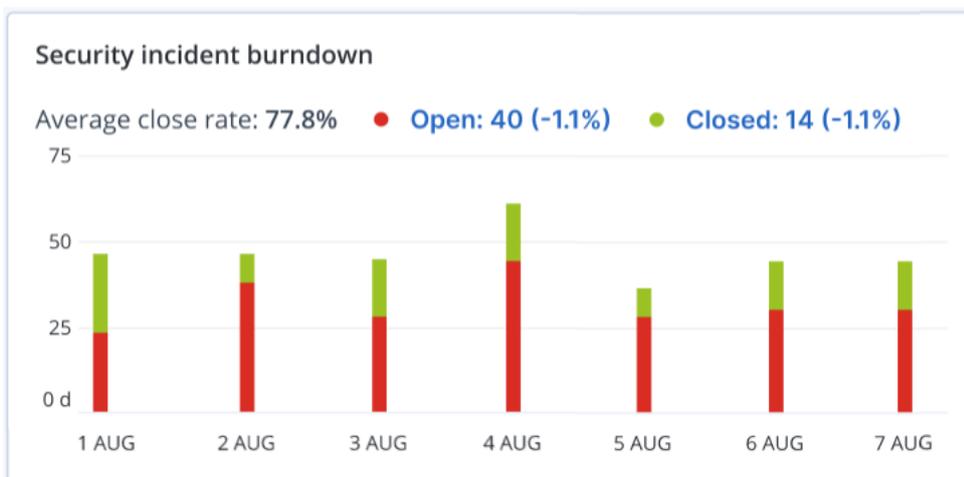


Sicherheitsvorfall-Burndown

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).

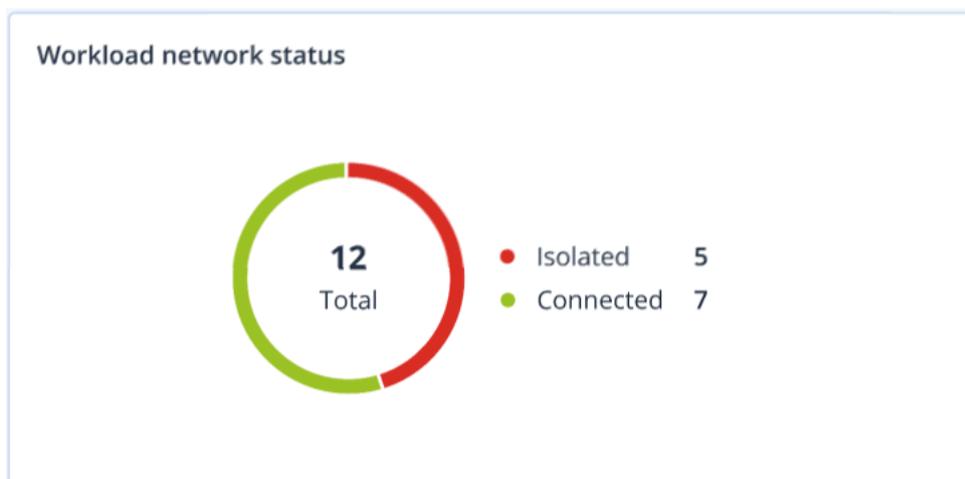
Der in Klammern angegebene Prozentwert gibt den Anstieg bzw. den Rückgang im Vergleich zum vorherigen Zeitraum an.



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.
- Bei NVMe-Laufwerken wird die Überwachung der Laufwerksintegrität nur für solche Laufwerke unterstützt, die ihre SMART-Daten über die Windows-API kommunizieren. Bei NVMe-Laufwerken, bei denen die SMART-Daten direkt aus dem Laufwerk ausgelesen werden müssen, wird die Überwachung der Laufwerksintegrität 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.

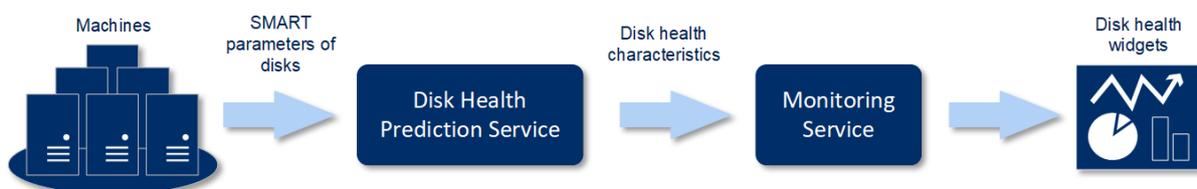
Und so funktioniert es

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.

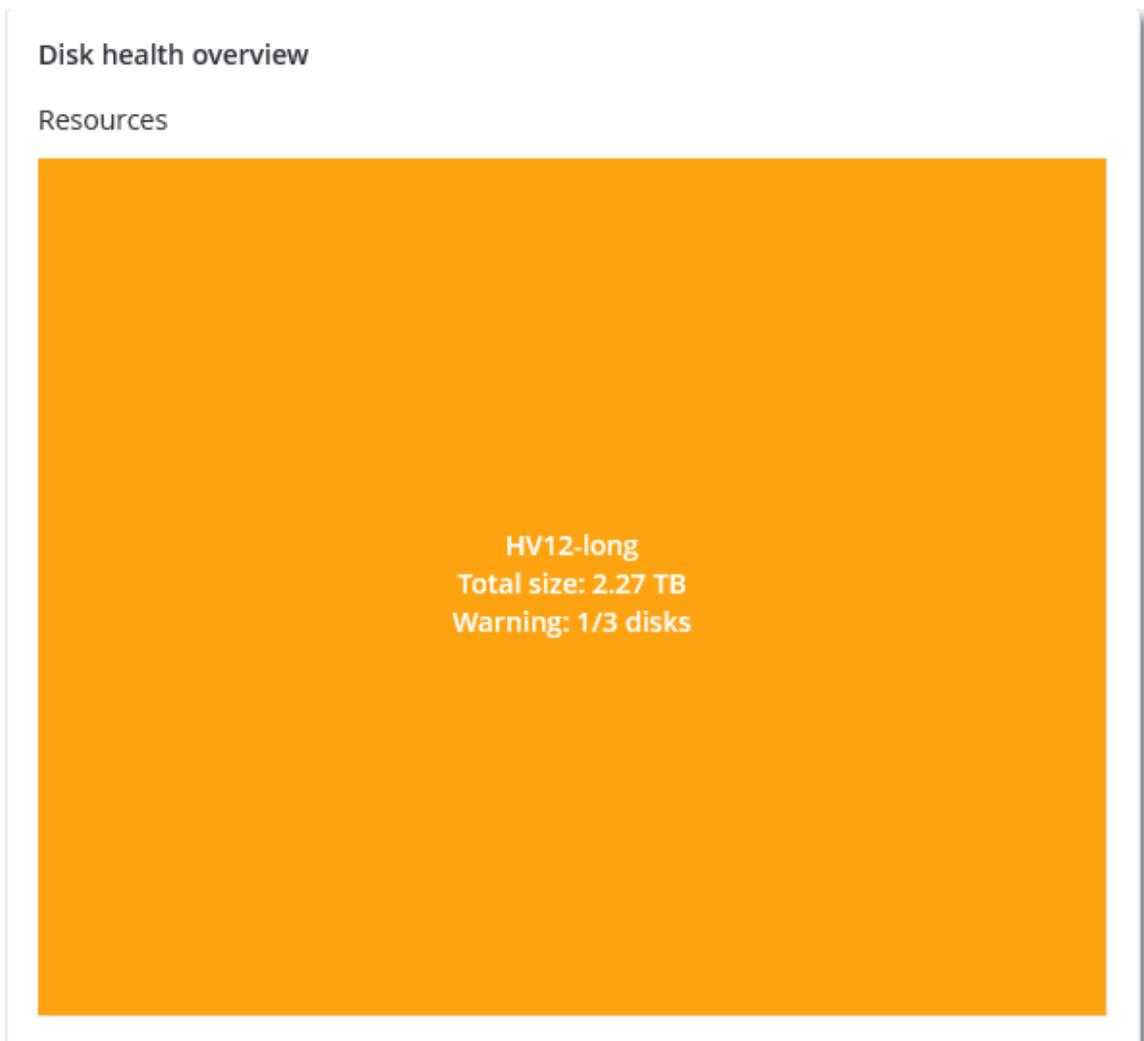
3. Der Monitoring Service empfängt diese Merkmale und zeigt die entsprechenden Informationen dann in den Laufwerksintegrität-Widgets der Service-Konsole an.



Laufwerksintegrität-Widgets

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

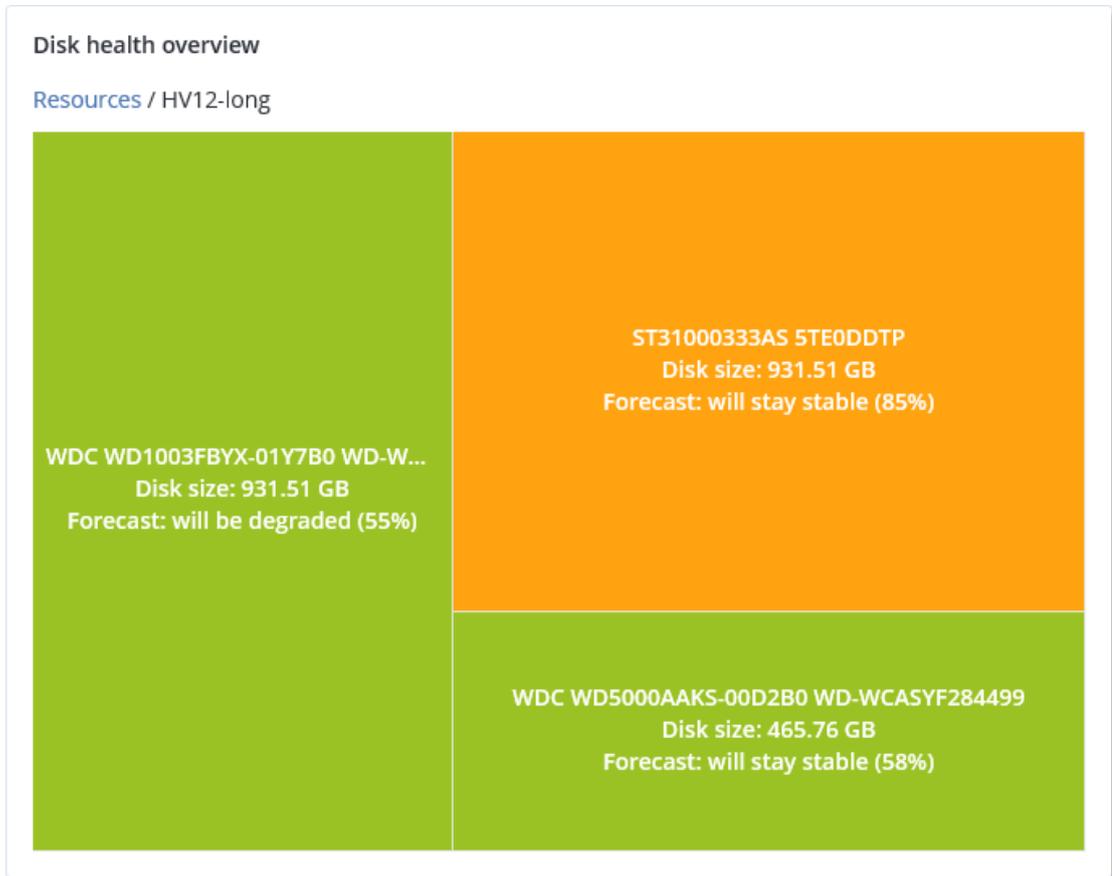
- **Überblick der Laufwerksintegrität** ist ein Treemap-Widget (Kacheldiagramm mit Baumstruktur) mit zwei Detailebenen, zwischen denen umgeschaltet werden kann.
 - **Maschinenebene**
Zeigt zusammengefasste Informationen über den Laufwerksintegritätsstatus für die ausgewählten Kundenmaschinen an. Es werden 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.



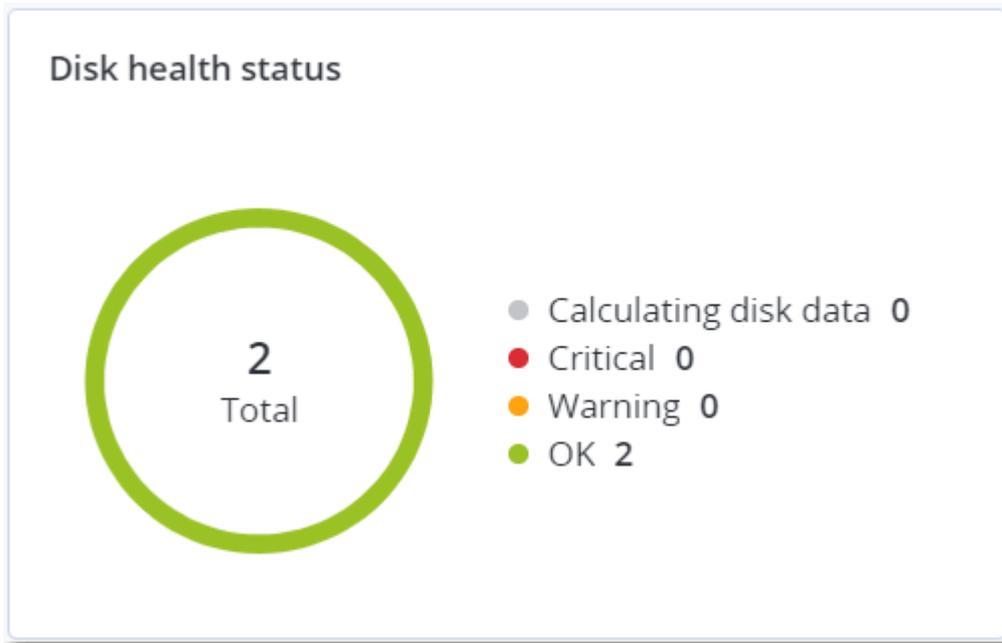
- **Laufwerksebene**
Zeigt den aktuellen Laufwerksintegritätsstatus aller Laufwerke für die ausgewählte Maschine an. Jeder Laufwerksblock zeigt eine der nachfolgenden Vorhersagen zur Laufwerksintegrität

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. Es ist nicht empfehlenswert, jetzt noch ein Image-Backup des

			<p>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.</p>
--	--	--	--

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.

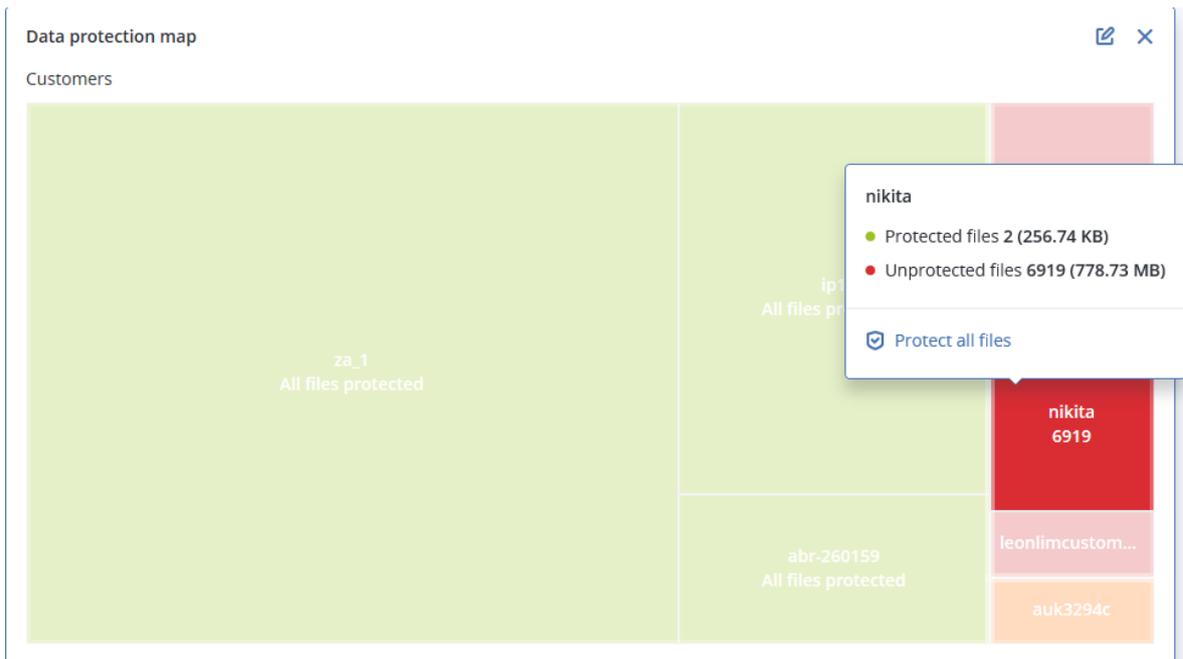
Jede Blockgröße hängt von der Gesamtzahl/Größe aller wichtigen Dateien ab, die zu einem Kunden/einer Maschine gehören.

Dateien können einen der folgenden Schutzstatus-Zustände haben:

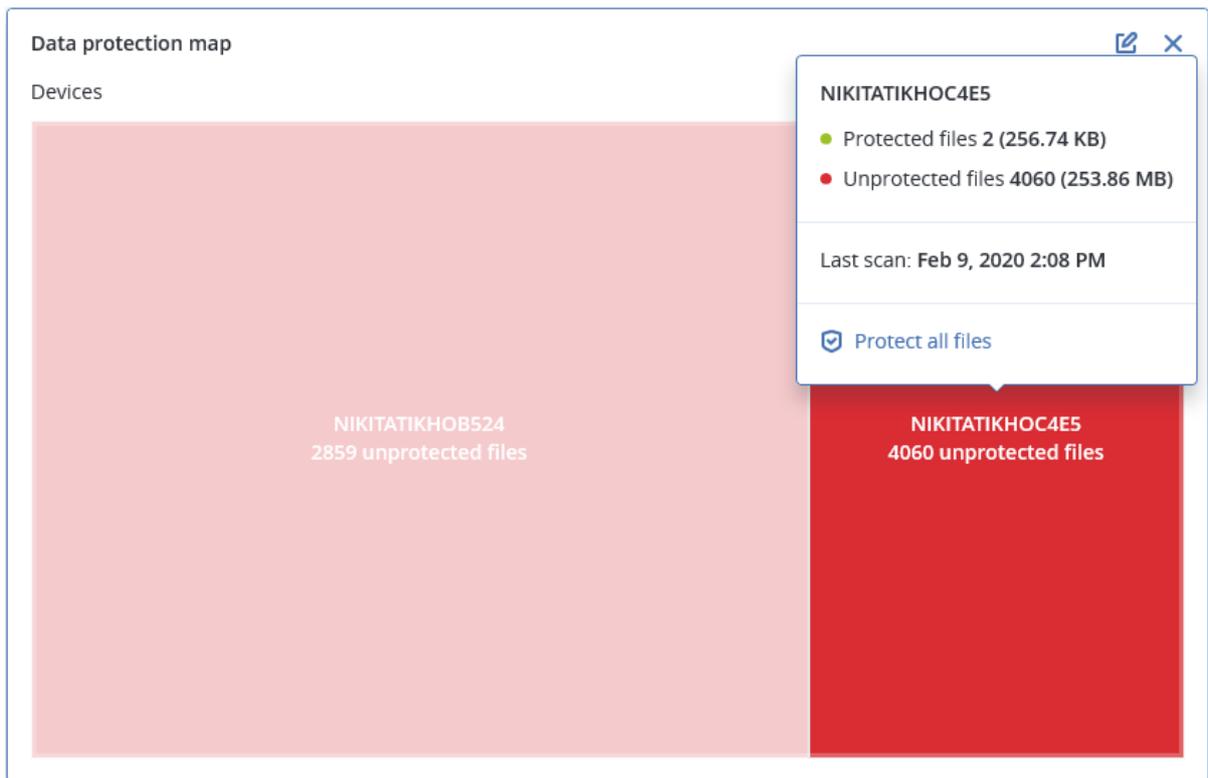
- **Kritisch** – es gibt 51-100% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen, die für den/die ausgewählte(n) Kunden-Mandanten/Maschine/Speicherort nicht per Backup gesichert wurden.
- **Niedrig** – es gibt 21-50% ungeschützte Dateien mit den von Ihnen spezifizierten Erweiterungen,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

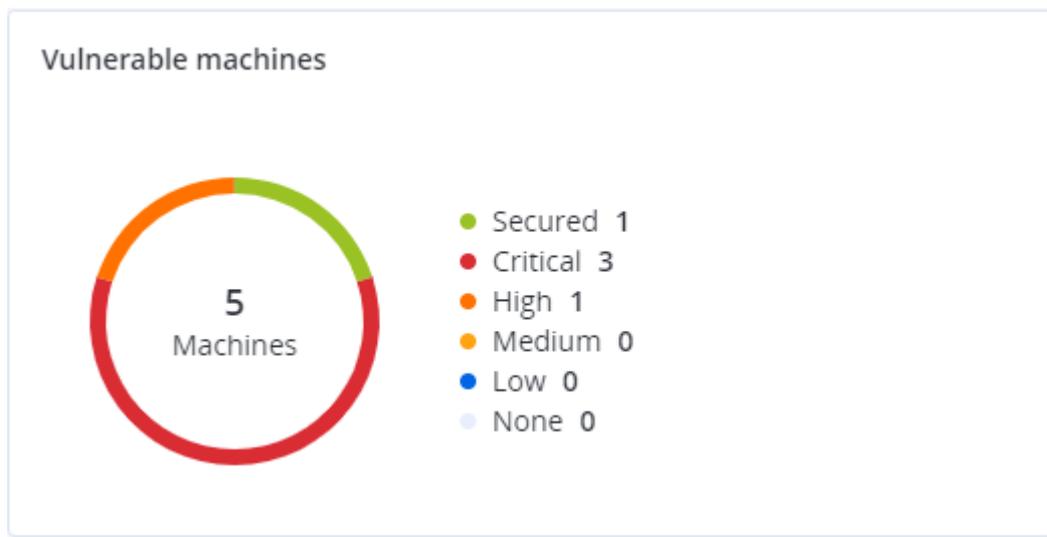
Widget für Schwachstellenbewertung

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.

Existing vulnerabilities							
Machine name	Vendor	Product	Vulnerability name/ID	Severity ↓	Last detected	First detected	⚙
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
More							

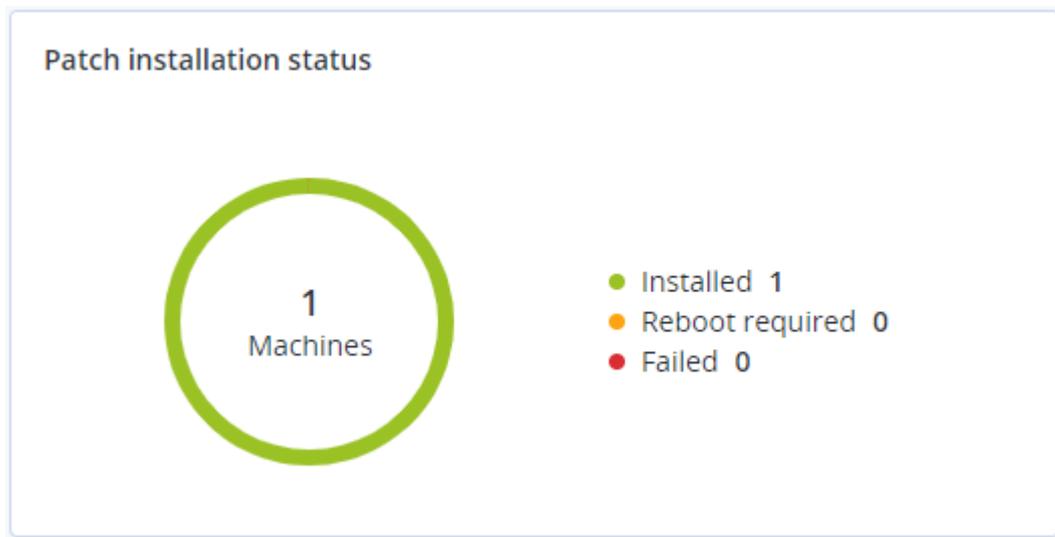
Widgets für Patch-Installation

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.

Patch installation summary								
Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity	⚙
● Installed	1	2	1	1	2	0	0	

Verlauf der Patch-Installation

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

Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date ↓
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	✓ Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	✗ Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	✓ Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	✗ Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	✓ Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	✗ Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	✓ Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	✓ Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	✗ Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	✗ Failed	02/04/2020

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.

Backup scanning details (threats)							
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full		Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

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.

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlylgen2	15	27.12.2017 11:23 AM	Folder
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacroIg1	274	27.12.2017 11:23 AM	Customer
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2017 11:23 AM	✓ Machine name
Win2012_r2-Hyper-V	Protection plan	W97M.DownloaderIg32	5	27.12.2017 11:23 AM	✓ Protection plan
HyperV_for12A	Total protection	Miner.XMRigIgen1	68	27.12.2017 11:23 AM	Detected by
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2017 11:23 AM	✓ Threat
vm-sql_2012	Protection plan	Adware.DealPlylgen2	9	27.12.2017 11:23 AM	File name
MF_2012_R2	Total protection	MSH.DownloaderIgen8	73	27.12.2017 11:23 AM	File path
MF_2012_R2	Total protection	Bloodhound.MalMacroIg1	182	27.12.2017 11:23 AM	✓ Affected files
MF_2012_R2	Protection plan	Bloodhound.MalMacroIg1	18	27.12.2017 11:23 AM	✓ Detection time
ESXirestore	Protection plan	MSH.DownloaderIgen8	682	27.12.2017 11:23 AM	
MF_2012_R2	Protection plan	Miner.XMRigIgen1	13	27.12.2017 11:23 AM	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlylgen2	3	27.12.2017 11:23 AM	
Win2012_r2-Hyper-V	Total protection	W97M.DownloaderIg32	27	27.12.2017 11:23 AM	

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

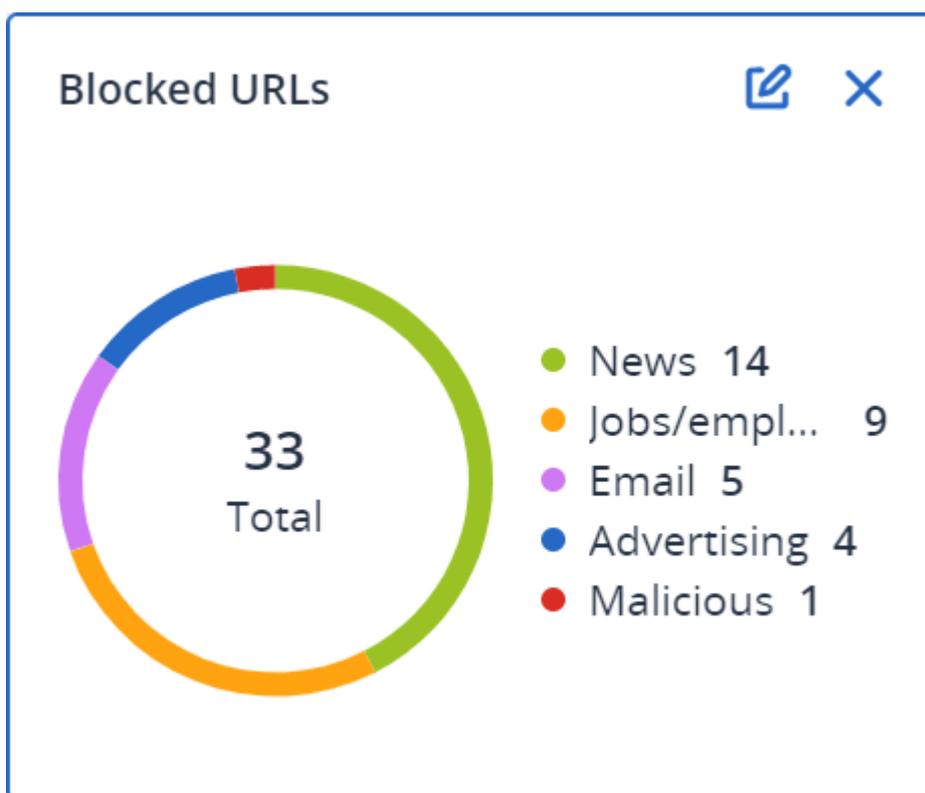
1. Klicken Sie im Widget **Kürzlich betroffen** auf den Befehl **Daten herunterladen**.
2. Geben Sie im Feld **Zeitraum** die Anzahl der Tage ein, für die Sie Daten herunterladen wollen. Die maximale Anzahl der Tage, die Sie eingeben können, beträgt 200.
3. Geben Sie im Feld **Empfänger** die E-Mail-Adressen 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](#).

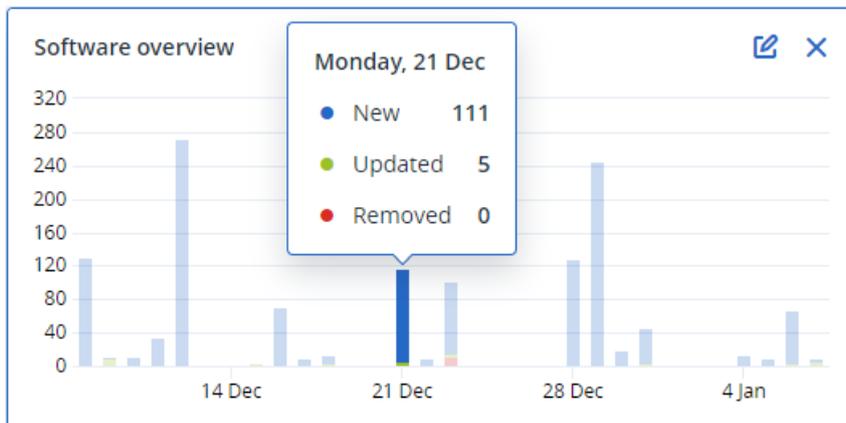


Widgets für Software-Inventarisierung

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.

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\G...	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

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.

Aktualisiert – 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 Service-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-mini...	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	00003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	NICET81W (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, 00:00:00:00:00:00	-	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

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	Motherboard	Removed	LENOVO, Toronto SC1, P...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Etherne...	-	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, Toronto SC1, 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, Etherne...	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

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	. i.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	. i.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](#)

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 Untermantanten 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 Untermantanten des Mandanten enthalten, in dem Sie gerade arbeiten.

- **Alle Kunden und Partner**

Der Bericht wird Service-Nutzungsmetriken für alle Untermantanten des Mandanten enthalten, in dem Sie gerade arbeiten.

- **Alle Kunden und Partner (einschließlich Benutzerdetails)**

Der Bericht wird Service-Nutzungsmetriken für alle Untermantanten 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.

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**.

Aktionen-Berichte

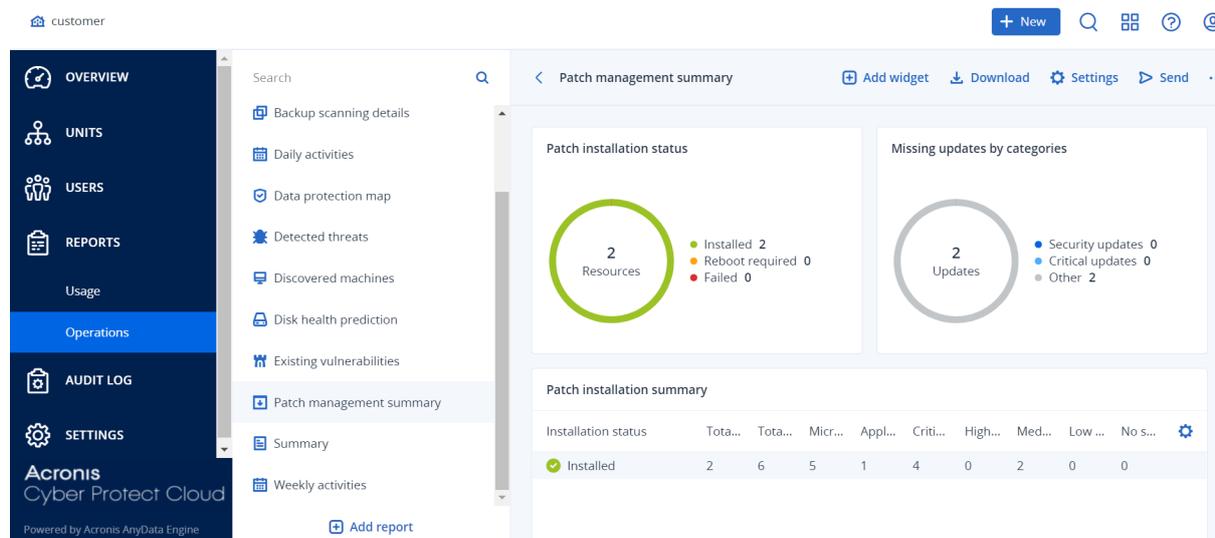
Ein Bericht über Aktionen kann einen beliebigen Satz von [Dashboard-Widgets](#) des Typs '**Aktionen**' enthalten. Standardmäßig zeigen alle Widgets die Übersichtsinformationen für denjenigen Mandanten an, in dem Sie gerade arbeiten. Sie können dies für jedes Widget einzeln ändern, indem Sie dieses bearbeiten – 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. 128)'.

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 über Aktionen herunterladen oder per E-Mail im Excel-Format (XLSX) 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.

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

Wenn Sie mit einem Bericht auf Aktionen zugreifen wollen, müssen Sie in der Berichtszeile auf das vertikale Drei-Punkte-Symbol klicken. Dieselben Aktionen sind aus dem Bericht heraus verfügbar.

Einen Bericht hinzufügen

1. Klicken Sie auf **Bericht hinzufügen**.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
 - Wenn Sie einen vordefinierten Bericht hinzufügen wollen, klicken Sie auf dessen Namen.
 - 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 Widgets 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.

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 Untermantanten haben, steht Ihnen die Option **Einen Mandanten für alle Widgets festlegen** zur Verfügung. Diese Option ermöglicht Ihnen, die Daten in allen Widgets des Reports nach dem ausgewählten Mandanten zu filtern. Wenn diese Option nicht ausgewählt ist, werden die Widgets die Daten für alle Untermantanten 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.

General

Name

Backup scanning details

Set one tenant for all widgets

Range

7 days

Scheduled

Recipients

user1@example.com; user2@example.com

File format

Excel and PDF

Language

English

Days of week

Monthly

SUN

MON

TUE

WED

THU

FRI

SAT

Send at

12:00 AM

Einen Bericht planen

1. Klicken Sie auf den Berichtsnamen und dann auf **Einstellungen**.
2. Aktivieren Sie den Schalter **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 einen Bericht herunterladen wollen, klicken Sie auf **Download** und wählen Sie das gewünschte Format aus:

- Excel oder PDF
- Excel
- PDF

Die Berichtsdaten sichern

Sie können eine Abbild (Dump) der Berichtsdaten als CSV-Datei per E-Mail versenden. Die Abbildsicherung enthält alle Berichtsdaten (ungefiltert) für einen bestimmten Zeitraum. Die Zeitstempel in CSV-Berichten verwenden das UTC-Format, während die Zeitstempel in Excel- und PDF-Berichten die aktuelle Zeitzone des Systems verwenden.

Die Software generiert die Sicherungsdaten „on the fly“. Wenn Sie einen langen Zeitraum definieren, kann die Aktion jedoch einige Zeit benötigen.

So können Sie die Berichtsdaten sichern

1. Klicken Sie auf den Berichtsnamen.
2. Klicken Sie in der rechten oberen Ecke auf das vertikale Drei-Punkte-Symbol und anschließend auf **Sicherungsdaten**.
3. Spezifizieren Sie die E-Mail-Adresse(n) des/der Empfänger.
4. Spezifizieren Sie bei **Zeitraum** den gewünschten Zeitrahmen.
5. Klicken Sie auf **Senden**.

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

Widget	Beschreibung
	<p>alphabetischer Reihenfolge von A bis Z):</p> <ul style="list-style-type: none"> • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange-Postfächer • Microsoft 365-Postfächer • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites <p>Für einige Workload-Typen werden folgende Workload-Gruppen verwendet:</p> <ul style="list-style-type: none"> • Microsoft 365: Benutzer, Gruppen, Öffentliche Ordner, Teams und Website-Sammlungen • Google Workspace: Benutzer und Shared Drives • Hosted Exchange: Benutzer <p>Wenn es in einer Workload-Gruppe mehr als 10.000 Workloads gibt, zeigt das Widget keine Daten für die entsprechenden Workloads an.</p> <p>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.</p>
<p>Cyber Protection-Übersicht</p>	<p>Das Widget zeigt die wichtigsten Metriken zur Cyber Protection-Performance für den spezifizierten Zeitraum an.</p> <p>Gesicherte Daten – die Gesamtgröße der Archive, die in den lokalen Storages und Cloud Storages und erstellt wurden.</p> <p>Abgemilderte Bedrohungen – die Gesamtzahl der Malware, die insgesamt auf allen Geräten blockiert wurden.</p> <p>Schädliche URLs blockiert – die Gesamtzahl der blockierten URLs auf allen Geräten.</p> <p>Gepatchte Schwachstellen – die Gesamtzahl der Schwachstellen, die durch die Installation von Software-Patches auf allen Geräten behoben wurden.</p> <p>Installierte Patches – die Gesamtzahl der Patches, die auf allen Geräten installiert wurden.</p>

Widget	Beschreibung
	<p>Server geschützt durch DR – die Gesamtzahl der Server, die per Disaster Recovery geschützt werden.</p> <p>File Sync & Share-Benutzer – die Gesamtzahl der End- und Gastbenutzer, die die Cyber Files Funktionalität verwenden.</p> <p>Beglaubigte Dateien – die Gesamtzahl der beglaubigten Dateien.</p> <p>Elektronisch signierte Dokumente – die Gesamtzahl der elektronisch signierten Dokumente.</p> <p>Blockierte Peripheriegeräte – die Gesamtzahl der Peripheriegeräte, auf die der Zugriff blockiert wird.</p>
<p>Workload-Netzwerkstatus</p>	<p>Dieses Widget informiert darüber, wie viele Workloads isoliert sind und wie viele verbunden sind (das normale Stadium des Workloads).</p> <p>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.</p>
<p>Workloads-Schutzstatus</p>	<p>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:</p> <p>Server – physische Server und Domain-Controller-Server.</p> <p>Workstations – physische Workstations.</p> <p>Virtuelle Maschinen – sowohl agentenbasierte als auch agentenlose virtuelle Maschinen.</p> <p>Webhosting-Server – virtueller oder physischer Server, auf denen cPanel oder Plesk installiert ist.</p> <p>Mobilgeräte – physische Mobilgeräte (wie Smartphones).</p> <p>Ein Workload kann zu mehreren Kategorien gehören. Ein Webhosting-Server wird beispielsweise zu zwei Kategorien gezählt – Server und Webhosting-Server.</p>
<p>Cloud-Workloads Schutzstatus</p>	<p>Cloud-Workloads Schutzstatus</p> <p>Das 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.</p>

Widget	Beschreibung
	<p>Folgende Cloud-Workload-Typen sind im Diagramm dargestellt (in alphabetischer Reihenfolge von A bis Z):</p> <ul style="list-style-type: none"> • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange-Postfächer • Microsoft 365-Postfächer • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites <p>Für einige Workload-Typen werden folgende Workload-Gruppen verwendet:</p> <ul style="list-style-type: none"> • Microsoft 365: Benutzer, Gruppen, Öffentliche Ordner, Teams und Website-Sammlungen • Google Workspace: Benutzer und Shared Drives • Hosted Exchange: Benutzer <p>Wenn es in einer Workload-Gruppe mehr als 10.000 Workloads gibt, zeigt das Widget keine Daten für die entsprechenden Workloads an.</p> <p>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.</p>

Antimalware Protection-Widgets

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

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

Widget	Beschreibung
	<p>infizierten Dateien, die nicht unter Quarantäne gestellt wurden</p> <p>Geräte geschützt – die Gesamtzahl der Geräte, auf die eine Antimalware Protection-Richtlinie angewendet wurde</p> <p>Gesamtzahl an registrierten Geräten – Die Gesamtzahl der registrierten Geräte zum Zeitpunkt der Berichtserstellung</p>
<p>Antimalware-Scan von Backups</p>	<p>Das Widget zeigt die Ergebnisse der Antimalware-Scans von Backups für den spezifizierten Datumsbereich an und verwendet dabei folgende Metriken:</p> <ul style="list-style-type: none"> • 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).
<p>Blockierte URLs</p>	<p>Das Widget zeigt für den spezifizierten Datumsbereich die Anzahl der blockierten URLs an, gruppiert nach Website-Kategorie.</p> <p>Das Widget listet die sieben Website-Kategorien mit der größten Anzahl blockierter URLs auf und fasst die übrigen Website-Kategorien unter Andere(s) zusammen.</p> <p>Weitere Informationen zu den Website-Kategorien finden Sie unter dem Thema 'URL-Filterung in Cyber Protection'.</p>
<p>Sicherheitsvorfall-Burndown</p>	<p>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.</p> <p>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.</p>
<p>MTTR (Mittlere Problemlösungszeit) für Vorfälle</p>	<p>Dieses Widget zeigt die durchschnittliche Problemlösungszeit für Sicherheitsvorfälle an. Sie gibt an, wie schnell Vorfälle untersucht und gelöst werden.</p> <p>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.</p>

Widget	Beschreibung
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: <ul style="list-style-type: none"> • 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. <p>Gesichert – die Anzahl der Workloads, die während des Berichtszeitraums per Backup geschützt wurden (es muss mindestens ein erfolgreiches Backup durchgeführt worden sein).</p> <p>Nicht gesichert – die Anzahl der Workloads, die während des Berichtszeitraums nicht per Backup geschützt wurden (es wurde kein erfolgreiches Backup durchgeführt).</p>
Laufwerksintegritätsstatus nach physischen Geräten	Das Widget zeigt den aggregierten Integritätsstatus von physischen Geräte an, basierend auf den Integritätsstatuszuständen von deren Laufwerken. <p>OK – Dieser Laufwerksintegritätsstatus bezieht sich auf bestimmte Werte [70-100]. Der Status eines Gerätes ist OK, wenn all seine Laufwerke den Status OK haben.</p> <p>Warnung – Dieser Laufwerksintegritätsstatus bezieht sich auf 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.</p>

Widget	Beschreibung
	<p>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.</p> <p>Laufwerksdaten werden berechnet – Der Status eines Gerätes ist Laufwerksdaten werden berechnet, wenn die Statuszustände seiner Laufwerke noch nicht berechnet wurden.</p>
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	<p>Das Widget zeigt die Performance-Ergebnisse der Schwachstellenbewertung für den spezifizierten Datumsbereich an.</p> <p>Insgesamt – die Gesamtzahl der gepatchten Schwachstellen.</p> <p>Microsoft-Software-Schwachstellen – die Gesamtzahl der behobenen Microsoft-Schwachstellen auf allen Windows-Geräten.</p> <p>Schwachstellen in Windows-Software von Drittanbietern – die Gesamtzahl der behobenen Schwachstellen in Windows-Programmen von Drittanbietern auf allen Windows-Geräten.</p> <p>Workloads gescannt – die Gesamtzahl der Geräte, die innerhalb des spezifizierten Datumsbereichs mindestens einmal erfolgreich auf Schwachstellen gescannt wurden.</p>
Patches installiert	<p>Das Widget zeigt die Performance-Ergebnisse der Patch-Verwaltung für den spezifizierten Datumsbereich an.</p> <p>Installiert – die Gesamtzahl der Patches, die erfolgreich auf allen Geräten installiert wurden.</p> <p>Microsoft-Software-Patches – die Gesamtzahl der Patches für Software-Programme von Microsoft, die auf allen Windows-Geräten installiert wurden.</p> <p>Patches für Windows-Software von Drittanbietern – die Gesamtzahl der Patches für Software-Programme von Drittanbietern, die auf allen Windows-Geräten installiert wurden.</p>

Widget	Beschreibung
	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	<p>Das Widget zeigt die wichtigsten Metriken zur Disaster Recovery-Performance für den spezifizierten Datumsbereich an.</p> <p>Produktions-Failover – die Anzahl der Produktions-Failover-Aktionen für den spezifizierten Zeitraum.</p> <p>Test-Failover – die Gesamtzahl der Test-Failover-Aktionen, die während des spezifizierten Zeitraums durchgeführt wurden.</p> <p>Primäre Server – die Gesamtzahl der primären Server zum Zeitpunkt der Berichtserstellung.</p> <p>Recovery-Server – die Gesamtzahl der Recovery-Server zum Zeitpunkt der Berichtserstellung.</p> <p>Öffentliche IPs – die Gesamtzahl der öffentlichen IP-Adresse (zum Zeitpunkt der Berichtserstellung).</p> <p>Verbrauchte Berechnungspunkte insgesamt – die Gesamtzahl der Berechnungspunkte, die während des spezifizierten Zeitraums verbraucht wurden.</p>
Disaster Recovery-Server getestet	<p>Das Widget zeigt Informationen über die Server an, die per Disaster Recovery geschützt werden und per Test-Failover getestet wurden.</p> <p>Das Widget zeigt folgende Metriken an:</p> <p>Server geschützt – die Anzahl der per Disaster Recovery geschützten Server (Server, die mindestens einen Recovery-Server haben) zum Zeitpunkt der Berichtserstellung.</p> <p>Gestestet – 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).</p> <p>Nicht getestet – die Anzahl der per Disaster Recovery geschützten Server, die während des festgelegten Zeitraums nicht per Test-Failover getestet wurden (von allen per Disaster Recovery geschützten Servern).</p> <p>Das Widget zeigt auch die Größe des Disaster Recovery Storage (in GB) zum Zeitpunkt der Berichtserstellung an. Dies entspricht der Summe der Backup-</p>

Widget	Beschreibung
	Größen der Cloud Server.
Server geschützt mit Disaster Recovery	<p>Das Widget zeigt Informationen über die per Disaster Recovery geschützten Server sowie die ungeschützten Server an.</p> <p>Das Widget zeigt folgende Metriken an:</p> <p>Die Gesamtzahl der im Kunden-Mandanten registrierten Server zum Zeitpunkt der Berichtserstellung.</p> <p>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.</p> <p>Ungeschützt – die Gesamtzahl der ungeschützten Server von allen registrierten Servern zum Zeitpunkt der Berichtserstellung.</p>

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	<p>Das Widget zeigt folgende Metriken an:</p> <p>Verwendeter Cloud Storage insgesamt – Die gesamte Storage-Nutzung aller Benutzer.</p> <p>Endbenutzer – die Gesamtzahl der Endbenutzer.</p> <p>Durchschnittliche Storage-Nutzung pro Benutzer – die durchschnittliche Storage-Nutzung pro Endbenutzer.</p> <p>Gastbenutzer – die Gesamtzahl der Gastbenutzer.</p>
File Sync & Share-Storage-Nutzung durch Endbenutzer	<p>Das Widget zeigt die Gesamtzahl der File Sync & Share-Endbenutzer an, die eine Storage-Nutzung in folgenden Bereichen haben:</p> <ul style="list-style-type: none"> • 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	<p>Das Widget zeigt folgende Notary-Metriken an:</p> <p>Notary Cloud Storage verwendet – die Gesamtgröße des Storage, der für Notary Services verwendet wird.</p> <p>Beglaubigte Dateien – die Gesamtzahl der beglaubigten Dateien.</p> <p>Elektronisch signierte Dokumente – die Gesamtzahl der elektronisch signierten Dokumente und Dateien.</p>
Beglaubigte Dateien über alle Endbenutzer hinweg	<p>Zeigt die Gesamtzahl der beglaubigten Dateien für alle Endbenutzer an. Die Benutzer werden nach der Anzahl der beglaubigten Dateien gruppiert, die diese haben.</p> <ul style="list-style-type: none"> • Bis zu 10 Dateien

Widget	Beschreibung
	<ul style="list-style-type: none"> • 11-100 Dateien • 101-500 Dateien • 501-1000 Dateien • Mehr als 1000 Dateien
Elektronisch signierte Dokumente über alle Endbenutzer hinweg an	<p>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.</p> <ul style="list-style-type: none"> • 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. 124).

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.

Zeitzone in Berichten

Die Zeitzone, 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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 (Widgets)	<ul style="list-style-type: none"> • Die Zeit der Berichtserstellung entspricht der Zeitzone der Maschine, auf welcher der Webbrowser ausgeführt wird. • Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal -> Berichte -> Aktionen	<ul style="list-style-type: none"> • Der Zeitstempel des exportierten Berichts entspricht der Zeitzone der Maschine, die zum Exportieren des Berichts verwendet wurde.

(als PDF oder XSLX exportiert)	<ul style="list-style-type: none"> Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal -> Berichte -> Aktionen (geplante Übermittlung)	<ul style="list-style-type: none"> Die Zeitzone und die Berichtsübermittlung ist UTC. Die Zeitzone der im Bericht angezeigten Aktivitäten ist UTC.
Management-Portal -> Benutzer -> Tägliche Zusammenfassung über aktive Alarmmeldungen	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Der Bericht wird gesendet, wenn eine Aktivität abgeschlossen wurde. <hr/> <p>Hinweis In Abhängigkeit vom Workload des Datacenters können einige Berichte verzögert gesendet werden.</p> <hr/> <ul style="list-style-type: none"> 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
Laufwerksintegritätsstatus 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

Überwachungsprotokoll

So können Sie das Überwachungsprotokoll (Audit-Log) einsehen wollen, klicken Sie auf **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 Protection-Service-Konsole durchgeführt werden
- Cyber-Skripting-Aktionen, die von Benutzern in der Service-Konsole von Cyber Protection durchgeführt werden
- Systemmeldungen über erreichte Quotas und deren Nutzung

Das Protokoll (Log) zeigt Ereignisse für den Mandanten (und dessen Untermantanten) 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 Initiator 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.

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
- Advanced Management
- Advanced Security
- Advanced Security + EDR
- 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-Paket nicht aktiviert ist, aber die Upselling-Option eingeschaltet ist, werden die Advanced Protection-Funktionen zwar im Schutzplan angezeigt, können aber (noch) nicht verwendet werden. Das Symbol  wird neben dem Funktionsnamen angezeigt. Eine Meldung fordert die Anwender dann auf, ihren Administrator zu kontaktieren, damit dieser den erforderlichen Advanced-Funktionssatz aktivieren kann.

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
Sicherheit	<ul style="list-style-type: none"> • #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 <p>*Um Zero-Day-Angriffe zu erkennen; Cyber Protect verwendet heuristische Scan-Regeln und Algorithmen, um nach gefährlichen Software-Befehlen zu suchen.</p>	<p>Es sind zwei Advanced Protection-Pakete verfügbar: Advanced Security und Advanced Security + EDR.</p> <p>Das Advanced Security-Paket enthält:</p> <ul style="list-style-type: none"> • 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 • Intelligente Schutzpläne (Integration von CPOC-Alarmmeldungen) • Zentrales Backup-Scanning nach Malware • Remote-Löschung <p>Das Protection-Paket 'Advanced Security + EDR' enthält alle oben genannten Funktionen sowie die folgenden Endpoint Detection & Response-Fähigkeiten, um fortschrittliche Bedrohungen oder laufende Angriffe</p>

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
		<p>erkennen zu können:</p> <ul style="list-style-type: none"> • 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 <p>Informationen zur Aktivierung von Advanced Security + EDR finden Sie im Abschnitt "'Advanced Security + EDR aktivieren" (S. 139)'.</p>
Data Loss Prevention	<ul style="list-style-type: none"> • Gerätekontrolle 	<ul style="list-style-type: none"> • 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

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
Verwaltung	<ul style="list-style-type: none"> • Gruppenverwaltung von Workloads • Zentrale Verwaltung von Schutzplänen • Hardware-Inventarisierung • Remote-Steuerung • Remote-Aktionen • Gleichzeitige Verbindungen pro Techniker • Remote-Verbindungsprotokoll: RDP 	<ul style="list-style-type: none"> • Patch-Verwaltung • Laufwerksintegrität • Software-Inventarisierung • Ausfallsicheres Patching • Cyber Scripting • Remote-Unterstützung • Dateiübertragung und -freigabe • Eine Sitzung zum Verbinden auswählen • Workloads in der Mehrfachansicht beobachten • Verbindungsmodi: Steuerung, Beobachtung und Vorhang • Verbindung über die Quick Assist-Applikation • Remote-Verbindungsprotokolle: NEAR und Bildschirmfreigabe • Sitzungsaufzeichnung für NEAR-Verbindungen • Screenshot-Übertragung • Sitzungsverlaufsbericht
E-Mail-Sicherheit	Ohne	<p>Echtzeitschutz für Ihre Microsoft 365- und Gmail-Postfächer:</p> <ul style="list-style-type: none"> • Antimalware Antispam • Scannen von URLs in E-Mails • DMARC-Analyse • Antiphishing • Impersonation Protection • Scannen von Anhängen • Content Disarm & Reconstruction (CDR) • Vertrauensgraph <p>Siehe die Konfigurationsanleitung.</p>
Cyber Disaster Recovery Cloud	<p>Sie können die Disaster Recovery-Standard-Funktionen verwenden, um Disaster Recovery-Szenarien für Ihre Workloads zu testen.</p> <p>Beachten Sie, welche Disaster Recovery-Standardfunktionen verfügbar sind und welche Einschränkungen es gibt:</p>	<p>Sie können das Advanced Disaster Recovery-Paket aktivieren und Ihre Workloads mit der kompletten Disaster Recovery-Funktionalität schützen.</p> <p>Beachten Sie, welche erweiterten Disaster Recovery-Funktionen verfügbar sind:</p>

Funktionsgruppe	Enthaltene Standard-Funktionen	Advanced-Funktionen
	<ul style="list-style-type: none"> • Test-Failover in einer isolierten Netzwerkumgebung. Begrenzt auf 32 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. 	<ul style="list-style-type: none"> • 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.

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	<ul style="list-style-type: none"> • Datei-Backup • Image-Backup • Backup von Applikationen • Backup von Netzwerkfreigaben • Backups zum Cloud Storage • Backups zu einem lokalen Storage <hr/> <p>Hinweis Für die Cloud Storage-Nutzung fallen Gebühren an.</p> <hr/>	<ul style="list-style-type: none"> • Microsoft SQL-Server und Microsoft Exchange-Cluster • Oracle Database • SAP HANA • Data Protection-Karte • Kontinuierliche Datensicherung (CDP) • Off-Host Data Processing-Pläne • Beglaubigung von Backups • Microsoft 365-Arbeitsplätze • Google Workspace-Arbeitsplätze
File Sync & Share	<ul style="list-style-type: none"> • Verschlüsselte dateibasierte Inhalte speichern 	<ul style="list-style-type: none"> • Beglaubigung und E-Signaturen • Dokumentvorlagen*

Funktionsgruppe	Pay-as-you-go-Funktionen	Advanced-Funktionen
	<ul style="list-style-type: none"> • Dateien zwischen festgelegten Geräten synchronisieren • Dateien und Ordner mit festgelegten Personen und Systemen teilen 	*Backup von synchronisierten und freigegebenen Dateien
Physischer Datenversand	Die Funktionalität 'Physischer Datenversand'	Nicht verfügbar
Notary	<ul style="list-style-type: none"> • 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. 7)'.

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.

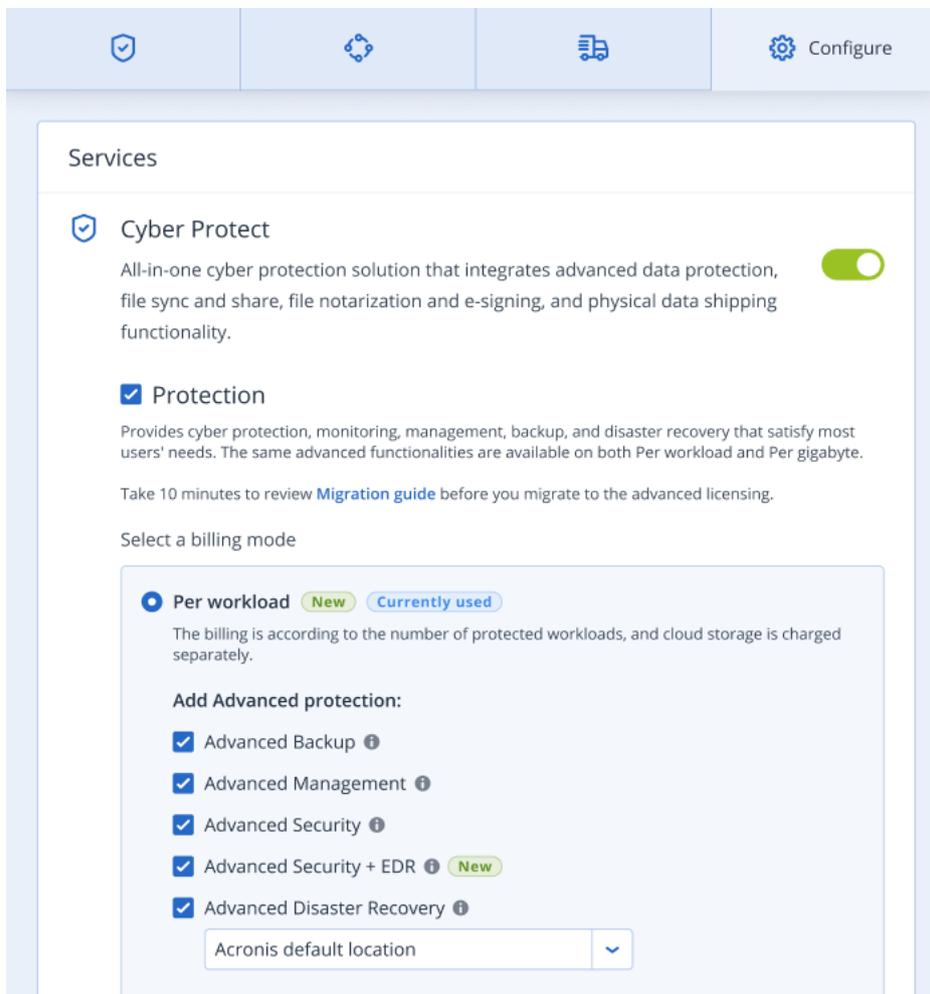
Hinweis

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 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 auf der Registerkarte **Konfigurieren** (unter dem Bereich 'Schutz') sicher, dass das Kontrollkästchen für **Advanced Security + EDR** aktiviert ist.



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

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](#).

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 Untermantanten 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 angezeigt! 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 angezeigt! 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

In der folgenden Tabelle werden die implementierten Integrationen mit Drittanbietern aufgelistet und Links zu den jeweiligen Dokumentationen angegeben.

INTEGRATION NSNAME	Online anzeigen	PDF öffnen
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue	https://www.acronis.com/support/documentation	https://dl.acronis.com/u/pdf/CloudBlueP

INTEGRATION NSNAME	Online anzeigen	PDF öffnen
PSA	tion/CloudBluePSA/	SAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
ConnectWise Control	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf
ConnectWise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPLugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableN-sightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf

INTEGRATION NSNAME	Online anzeigen	PDF öffnen
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
ServiceNow	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

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 ermöglicht es, die Änderungen in der VMware Cloud Director-Umgebung mit Cyber Protect Cloud zu synchronisieren.
2. Das Plug-in für VMware Cloud Director installieren.
Dieses Plug-in fügt Cyber Protection zur VMware Cloud Director-Benutzeroberfläche hinzu.
3. Einen Management Agenten bereitstellen.
Der Management Agent ordnet VMware Cloud Director-Organisationen automatisch 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.

4. 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. 35).

Alle existierenden direkten Partner können die Integration in VMware Cloud Director konfigurieren. Partner-Administratoren können diese Option auch für Untermantanten 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 Protection-Webkonsole wird in einer neuen Registerkarte geöffnet.

Software-Anforderungen

Unterstützte VMware Cloud Director-Versionen

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

Unterstützte Webbrowser

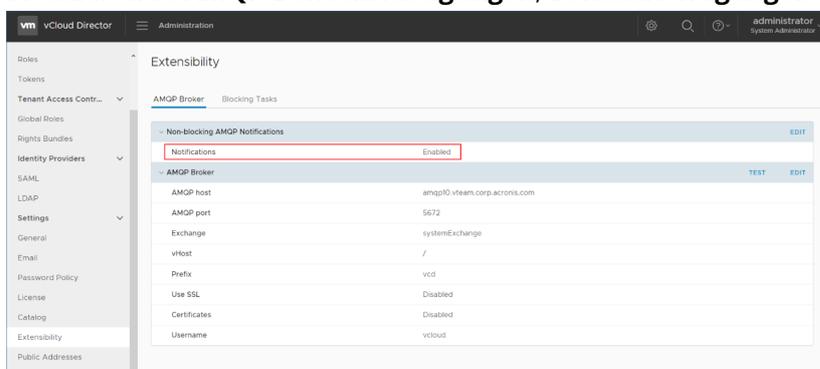
- Google Chrome 29 (oder später)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)

- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

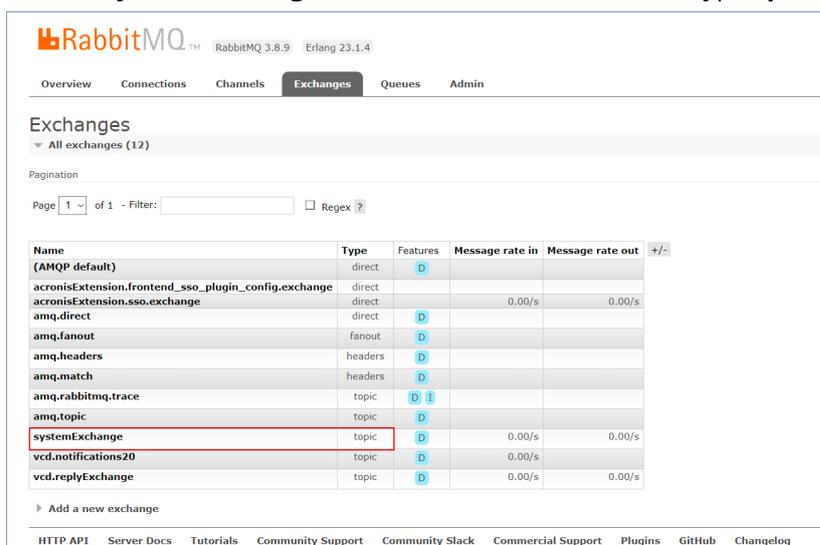
In anderen Webbrowsern (inkl. Safari-Browser, die unter anderen Betriebssystem laufen) wird möglicherweise die Benutzeroberfläche nicht korrekt angezeigt oder stehen einige Funktionen nicht zur Verfügung.

Dne RabbitMQ Message Broker konfigurieren

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

1. Klicken Sie auf folgenden Link, um die Datei **vCDPlugin.zip** herunterzuladen:
<https://dl.managed-protection.com/u/vCD/vCDPlugin.zip>.
2. Melden Sie sich am VMware Cloud Director-Provider-Portal als Systemadministrator an.
3. Wählen Sie im Navigationsmenü **Portal anpassen**.
4. Klicken Sie in der Registerkarte **Plug-Ins verwalten** und auf das Element **Upload**.
Der Assistent **Plug-In hochladen** wird geöffnet.
5. Klicken Sie auf **Plug-In-Datei auswählen** und wählen Sie dann die Datei **vCDPlugin.zip** aus.
6. Klicken Sie auf **Weiter**.
7. Den Geltungsbereich und die Veröffentlichung konfigurieren:
 - 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.
8. Klicken Sie auf **Weiter**.
9. Überprüfen Sie Ihre Einstellungen und klicken Sie dann auf **Beenden**.

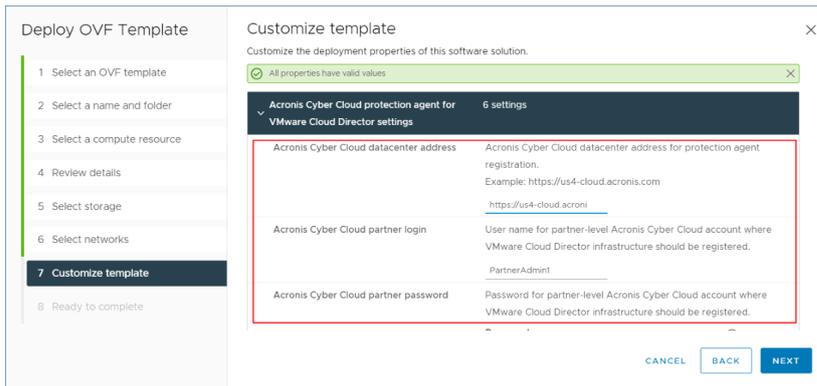
Einen Management Agenten installieren

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. Klicken Sie auf den Link **Management Agent** und laden Sie die ZIP-Datei herunter.
4. Extrahieren Sie die Management Agenten-Vorlagendatei `vCDManagementAgent.ovf` und die virtuelle Laufwerksdatei `vCDManagementAgent-disk1.vmdk`.
5. 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.

6. Konfigurieren Sie im Assistenten **OVF-Vorlage bereitstellen** den Management Agenten, indem Sie folgende Einstellungen vornehmen:



- a. Die URL des Cyber Protect Cloud-Datencenters. Beispielsweise `https://us5-cloud.beispiel.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. 72)'.

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 Server-Adresse, der Port, der Name des virtuellen Hosts, das Anmeldedaten des Administrators (Anmeldename, Kennwort).
- g. 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.

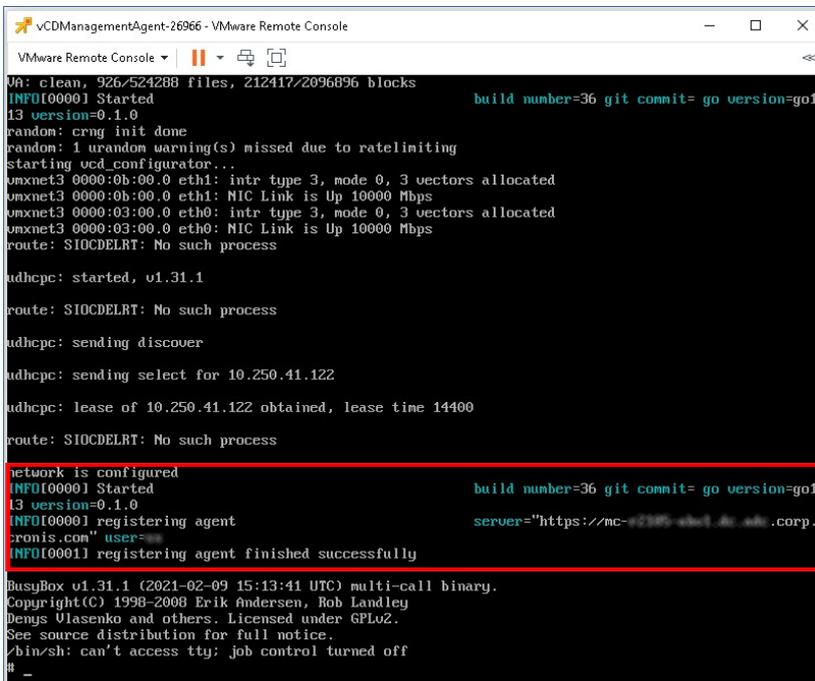
Hinweis

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-Datcenter 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.

7. [Optional] Öffnen Sie im vSphere Client die Konsole der virtuellen Maschine mit dem Management Agenten und überprüfen Sie dann Ihre Einrichtung.



```
vCDManagementAgent-26966 - VMware Remote Console
VMware Remote Console
VA: clean, 926/524288 files, 212417/2096896 blocks
INFO[0000] Started build number=36 git commit= go version=go1.
13 version=0.1.0
random: crng init done
random: 1 urandom warning(s) missed due to ratelimiting
Starting ucd_configurator...
umxnet3 0000:0b:00.0 eth1: intr type 3, mode 0, 3 vectors allocated
umxnet3 0000:0b:00.0 eth1: NIC Link is Up 10000 Mbps
umxnet3 0000:03:00.0 eth0: intr type 3, mode 0, 3 vectors allocated
umxnet3 0000:03:00.0 eth0: NIC Link is Up 10000 Mbps
route: SIOCDELRT: No such process

udhcpd: started, v1.31.1

route: SIOCDELRT: No such process

udhcpd: sending discover

udhcpd: sending select for 10.250.41.122

udhcpd: lease of 10.250.41.122 obtained, lease time 14400

route: SIOCDELRT: No such process

network is configured
INFO[0000] Started build number=36 git commit= go version=go1.
13 version=0.1.0
INFO[0000] registering agent server="https://mc-2385-eb01-4c-2a8b.corp.a
ronis.com" user=
INFO[0001] registering agent finished successfully

BusyBox v1.31.1 (2021-02-09 15:13:41 UTC) multi-call binary.
Copyright(C) 1998-2008 Erik Andersen, Rob Landley
Denys Vlasenko and others. Licensed under GPLv2.
See source distribution for full notice.
/bin/sh: can't access tty: job control turned off
#
```

8. 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. Derer Name lautet standardmäßig **systemExchange**.

- c. Überprüfen Sie die Bindungen an die **vcdmaq**-Warteschlange.

The screenshot shows the RabbitMQ management interface for the 'systemExchange'. The 'Bindings' section is highlighted with a red box. It contains a table with the following data:

To	Routing key	Arguments	Action
vcdmaq	true.#.org.*		Unbind
vcdmaq	true.#.session.authorize		Unbind
vcdmaq	true.#.session.login		Unbind
vcdmaq	true.#.user.*		Unbind
vcdmaq	true.#.vapp.*		Unbind
vcdmaq	true.#.vc.*		Unbind
vcdmaq	true.#.vdc.*		Unbind
vcdmaq	true.#.vm.*		Unbind

Below the table, there is a form to add a new binding from this exchange. The form includes fields for 'To queue', 'Routing key', and 'Arguments', along with a 'Bind' button and a 'String' dropdown menu.

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. Klicken Sie auf den Link **Backup Agent** und laden Sie die ZIP-Datei herunter.
4. Extrahieren Sie die Backup Agenten-Vorlagendatei `vCDCyberProtectAgent.ovf` und die virtuelle Laufwerksdatei `vCDCyberProtectAgent-disk1.vmdk`.
5. 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 10 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.

Hinweis

Backups von virtuellen Maschinen auf ESXi Hosts, auf denen kein Backup Agent installiert ist, werden mit dem Fehler 'Task-Zeitlimit ist abgelaufen' fehlschlagen.

6. Konfigurieren Sie im Assistenten **OVF-Vorlage bereitstellen** den Backup Agenten, indem Sie folgende Einstellungen vornehmen:

Property	Description
Acronis Cyber Cloud datacenter address	Acronis Cyber Cloud datacenter address for management agent registration. Example: https://us4-cloud.acronis.com https://us4-cloud.acronis.com
Acronis Cyber Cloud partner login	User name for partner-level Acronis Cyber Cloud account where VMware Cloud Director infrastructure should be registered. PartnerAdmin2
Acronis Cyber Cloud partner password	Password for partner-level Acronis Cyber Cloud account where VMware Cloud Director infrastructure should be registered. PartnerAdmin2

- Die URL des Cyber Protect Cloud-Datacenters. Beispielsweise `https://us5-cloud.beispiel.com`.
- Die Anmeldedaten des Partner-Administrators (Anmeldename und Kennwort).
- 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.
- 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-Datcenter erlauben.

- 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).
- 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.

7. 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.

Auf die Cyber Protection-Webkonsole 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. 157).

Administratoren können auf die benutzerdefinierte Cyber Protection-Webkonsole 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 Protection-Webkonsole 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 Protection-Webkonsolen ihrer Kunden-Mandanten zugreifen und in deren Auftrag Backups und Wiederherstellung verwalten.

Einschränkungen

Die Liste der Einschränkungen kann sich in den kommenden Versionen von Cyber Protect Cloud ändern.

Backup

- Es wird nur ein Backup der kompletten Maschine unterstützt. Dateifilter oder die Auswahl von Laufwerken bzw. Volumes sind nicht verfügbar.
- 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.

Recovery

- Es werden nur Wiederherstellungen zur ursprünglichen virtuellen Maschine unterstützt. Die ursprüngliche virtuelle Maschine muss in der VMware Cloud Director Umgebung vorhanden sein.
- Wiederherstellungen auf Dateiebene werden nicht unterstützt.

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" (S. 150)'.

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 Problembhebungen 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 Systemberichtsdatei 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

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.

Datenschutzeinstellungen

Über die Datenschutzeinstellungen können Sie angeben, ob Sie mit der Erfassung, Verwendung und Offenlegung Ihrer persönlichen Daten einverstanden sind oder nicht.

In Abhängigkeit von dem Land, in dem Sie Cyber Protect verwenden, und dem Cyber Protect Cloud Datacenter, das Ihnen bestimmte Services bereitstellt, werden Sie bei der ersten Nutzung von Cyber Protect möglicherweise aufgefordert zu bestätigen, ob Sie mit der Verwendung von Google Analytics in Cyber Protect einverstanden sind.

Mithilfe von Google Analytics können wir das Nutzerverhalten besser verstehen und die Nutzererfahrung in Cyber Protect verbessern, indem wir pseudonymisierte Daten sammeln.

Wenn Ihnen in der Benutzeroberfläche von Cyber Protect keine Einverständniserklärung und keine Menüs für Google Analytics angezeigt werden, bedeutet dies, dass Google Analytics in Ihrem Land nicht verwendet wird.

Auch wenn Sie Google Analytics beim ersten Start von Cyber Protect aktiviert oder abgelehnt haben, können Sie Ihre Entscheidung später jederzeit wieder ändern.

So können Sie Google Analytics aktivieren oder deaktivieren

1. Klicken Sie in der rechten oberen Ecke der Cyber Protect-Konsole auf das Symbol für 'Konto'.
2. Wählen Sie **Meine Datenschutzeinstellungen** aus.
3. Klicken Sie im Bereich **Google Analytics-Datenerhebung** auf eine der folgenden Schaltflächen:
 - **An** – um Google Analytics zu aktivieren
 - **Aus** – um Google Analytics zu deaktivieren

Index

#

#CyberFit-Score pro Maschine 89

7

7-Tage-Verlaufsleiste 32

A

Abhängigkeit der Agenten-Installer von den
Angebotsselementen 24

Abrechnung für den Notary Service 8

Abrechnung für den physischen
Datenversand 8

Abrechnungsmodi für Cyber Protect 7

Abrechnungsmodi für die Schutz-
Komponente 7

Abrechnungsmodi für File Sync & Share 8

Abrechnungsmodi und Editionen 13

Advanced Data Loss Prevention 138

Advanced Data Loss Prevention aktivieren 139

Advanced Disaster Recovery 140

Advanced Email Security 141

Advanced Protection-Pakete 133

Advanced Security + EDR 139

Advanced Security + EDR aktivieren 139

Agenten automatisch aktualisieren 82

Aktionen 86

Aktionen-Berichte 108

Aktionen in der Geräteliste 72

Aktionen mit Speicherorten 73

Alarmmeldungen zum
Laufwerksintegritätsstatus 96

Anforderungen an das Kennwort 26

Anforderungen und Einschränkungen 48

Angebotsselemente 13

Angebotsselemente aktivieren oder
deaktivieren 13

Angebotsselemente und Quota-Verwaltung 12

Antimalware Protection-Widgets 117

API-Clients verwalten 142

Assistent für die automatische Erkennung 72

Auf das Management-Portal zugreifen 27

Auf die Cyber Protection-Webkonsole
zugreifen 156

Auf die Services zugreifen 30

Aussehen 78

B

Backup 156

Backup-Quota-Transformation 19

Backup-Quotas 16

Backup-Scanning-Details 101

Backup-Widgets 119

Backup Agenten installieren 153

Beispiel

Cyber Protect-'pro Workload'-Editionen zu
'pro Workload'-Abrechnung 11

Von einer Cyber Protect Advanced-Edition
zu einem 'pro Workload'-
Abrechnungsmodus wechseln 10

Benachrichtigungen über Wartungsaktivitäten

aktivieren 43
Benutzer verwalten 51
Benutzerdefinierte Nutzungsberichte konfigurieren 108
Benutzerkonten und Mandanten 33
Benutzerrollen und Cyber-Skripting-Rechte 57
Berichte 106
Berichtsdaten je nach Widget-Typ 128
Berichtstyp 106
Berichtsumfang 107
Blockierte URLs 103
Branding-Elemente 78
Branding des Agenten und Installers 78
Branding konfigurieren 80
Branding und White-Labeling konfigurieren 77

C

Cyber Protect Services 6

D

Das Administratorkonto aktivieren 26
Das Branding deaktivieren 81
Das Management-Portal verwenden 26
Das Plug-in für VMware Cloud Director installieren 150
Data Loss Prevention-Widget 122
Data Protection-Karte 97
Daten für kürzlich betroffene Workloads herunterladen 102
Datenschutzeinstellungen 160
Den Abrechnungsmodus für einen Kunden-Mandanten ändern 11

Den Abrechnungsmodus für einen Partner-Mandanten ändern 11
Den geheimen Wert eines API-Clients zurücksetzen 144
Den Kurzübersichtsbericht anpassen 125
Den Zugriff auf die Weboberfläche einschränken 30
Den Zugriff auf Ihren Mandanten einschränken 50
Die Abrechnungsmodi mit Legacy-Editionen verwenden 9
Die Agenten aktualisieren 155
Die Angebots Elemente für einen Mandanten konfigurieren 40
Die Benachrichtigungseinstellungen für einen Benutzer ändern 59
Die Berichtsdaten sichern 113
Die Berichtseinstellungen bearbeiten 110
Die Berichtsstruktur exportieren und importieren 113
Die Eigentümerschaft eines Benutzerkontos übertragen 62
Die Einstellungen des Kurzübersichtsberichts konfigurieren 124
Die Integration mit VMware Cloud Director entfernen 159
Die Mandantentypen, die verschoben werden können 48
Die Nutzungsdaten für einen Mandanten aktualisieren 47
Die Quota für den Backup Storage überschreiten 19
Die Service-Quota von Maschinen ändern 22
Die Services für einen Mandanten auswählen 39

Die Standardeinstellungen für das Branding wiederherstellen 80

Die Zwei-Faktor-Authentifizierung bei Verlust des Zweit-Faktor-Gerätes zurücksetzen 69

Die Zwei-Faktor-Authentifizierung für Benutzer verwalten 67

Die Zwei-Faktor-Authentifizierung für Ihren Mandanten einrichten 66

Die Zwei-Faktoren-Einrichtung zwischen Mandantenebenen weitergeben 65

Disaster Recovery-Quotas 20

Disaster Recovery-Widgets 121

Dne RabbitMQ Message Broker konfigurieren 149

Dokumentation und Support 78

E

Ebenen, auf denen Quotas definiert werden können 15

Ein Benutzerkonto deaktivieren und aktivieren 61

Ein Benutzerkonto erstellen 51

Ein Benutzerkonto löschen 62

Eine benutzerdefinierte URL für die Weboberfläche konfigurieren 81

Eine Integration für Cyber Protect Cloud einrichten 142

Eine typische Integrationsprozedur 143

Einen API-Client deaktivieren 144

Einen API-Client erstellen 143

Einen API-Client löschen 145

Einen Backup-Administrator erstellen 157

Einen Bericht herunterladen 113

Einen Bericht hinzufügen 110

Einen Bericht planen 112

Einen deaktivierten API-Client wieder aktivieren 145

Einen Kurzübersichtsbericht erstellen 124

Einen Management Agenten installieren 150

Einen Mandanten deaktivieren und aktivieren 47

Einen Mandanten erstellen 35

Einen Mandanten löschen 50

Einen Mandanten zu einem anderen Mandanten verschieben 48

Einen Partner- in einen Ordner-Mandanten konvertieren (und umgekehrt) 49

Einen Schutzplan erstellen oder bearbeiten 72

Einschränkungen 39, 92, 148, 156

Einstellungen für E-Mail-Server 80

Einstellungen für rechtliche Dokumente 79

Endpoint Detection & Response (EDR)-Widgets 89

Enthaltene Standard-Funktionen und verfügbare Advanced-Funktionen im Protection Service 134

Erhöhter Sicherheitsmodus 38

Erkannte Maschinen 88

F

Fehlende Updates nach Kategorie 101

Felder im Überwachungsprotokoll 131

File Sync & Share-Quotas 21

File Sync & Share-Widgets 123

Filter und Suche 132

Firmenkontakte konfigurieren 44

Für jeden Service verfügbare
Benutzerrollen 54

G

Geplante Nutzungsberichte konfigurieren 107

I

Im Management-Portal navigieren 29

In den Cyber Protect Services enthaltene
Funktionen und Advanced-Pakete 134

Integration in Drittanbieter-Systeme 142

Integration in VMware Cloud Director 147

Integrationen 142

Integrationsreferenzen 145

J

Je nach Benutzerrolle empfangene
Benachrichtigungen 61

K

Kontakte im Assistenten 'Unternehmensprofil'
konfigurieren 27

Kürzlich betroffen 102

Kurzübersicht 114

Kurzübersicht-Widgets 114

Kurzübersichtsberichte senden 127

L

Laufwerksintegrität-Widgets 94

M

Mandanten verwalten 35

Metriken mit einer Nutzung von Null 107

Mobile Apps 80

Monitoring 67, 85

MTTR (Mittlere Problemlösungszeit) für
Vorfälle 90

N

Neue Storages hinzufügen 73

Notary-Quotas 22

Notary-Widgets 123

Nutzung 85, 106

P

Pay-as-you-go- und Advanced-Funktionen im
Protection Service 137

Physischer Datenversand-Quotas 22

Q

Quotas für Cloud-Datenquellen 17

Quotas für Storage 18

R

Recovery 157

Registerkarte Clients 31

Registerkarte Überblick 30

S

Schutz vor Brute-Force-Angriffen 70

Schutzstatus 87

Schwachstellenliste 71

Selbstverwaltete Kundenprofile
konfigurieren 44

Services 12

Services für mehrere bestehende Mandanten
aktivieren 41

Services und Angebots Elemente 12

Sicherheitsvorfall-Burndown 91

Sitzungsverlauf 105

So können Sie Agenten automatisch aktualisieren lassen 83

So können Sie die Agenten-Updates überwachen 85

So können Sie die vertrauenswürdigen Browser eines Benutzers zurücksetzen 68

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer aktivieren 69

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer deaktivieren 68

So können Sie die Zwei-Faktor-Authentifizierung für einen Benutzer zurücksetzen 68

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten aktivieren 66

So können Sie die Zwei-Faktor-Authentifizierung für Ihren Mandanten deaktivieren 67

So können Sie einen Mandanten verschieben 49

Software-Anforderungen 148

Speicherorte 72

Speicherorte und Storage verwalten 72

Speicherorte und Storages für Partner und Kunden wählen 73

Spitzenverteilung der Vorfälle pro Workload 90

Status der Patch-Installation 100

Storages löschen 74

Storages verwalten 73

Systembericht, Protokolldateien und

Konfigurationsdateien 158

U

Über Cyber Protect 6

Über dieses Dokument 5

Übersicht der Patch-Installation 100

Überwachung der Laufwerksintegrität 92

Überwachungsprotokoll 131

Und so funktioniert es 63, 93

Unterstützte VMware Cloud Director-Versionen 148

Unterstützte Webbrowser 26, 148

Unveränderlichen Storage konfigurieren 74

Upselling 80

Upselling-Punkte, die einem Kunden angezeigt werden 71

Upselling-Szenarien für Ihre Kunden konfigurieren 70

URL für Cyber Protect Cloud Services 79

V

Verhindern, dass sich nicht lizenzierte Microsoft 365-Benutzer anmelden können 20

Verlauf der Patch-Installation 101

Verwundbare Maschinen 99

Vom Management-Portal aus auf die Cyber Protection-Konsole zugreifen 29

Von Legacy-Editionen zum aktuellen Lizenzierungsmodell wechseln 9

Vorhandene Schwachstellen 99

W

Was ist ein API-Client? 143

Weiche und harte Quotas 14
Weiche und harte Quotas einrichten 15
White-Labeling 81
White-Labeling anwenden 81
Widget für Schwachstellenbewertung 99
Widgets für Hardware-Inventarisierung 105
Widgets für Patch-Installation 100
Widgets für Schwachstellenbewertung und
Patch-Verwaltung 120
Widgets für Software-Inventarisierung 103
Workload-Netzwerkstatus 92
Workloads-Überblick-Widgets 114

Z

Zeitzone in Berichten 127
Zwei-Faktor-Authentifizierung einrichten 63
Zwischen Editionen und Abrechnungsmodi
wechseln 9