# Cyber Protect Cloud

23.02

Podręcznik administratora partnera

WERSJA: 28.02.2023

# Spis treści

# Informacje na temat niniejszego dokumentu

Niniejszy dokument jest przeznaczony dla administratorów partnerów, którzy chcą udostępniać klientom usługi przy użyciu platformy Cyber Protect Cloud.

W tym dokumencie opisano, jak skonfigurować usługi dostępne na platformie Cyber Protect Cloud i nimi zarządzać przy użyciu portalu zarządzania.

# Cyber Protect — informacje

**Cyber Protect** to platforma chmurowa, która umożliwia usługodawcom, sprzedawcom i dystrybutorom oferowanie usług ochrony danych partnerom i klientom.

Usługi te są udostępniane zarówno na poziomie partnera, jak i na poziomie firmy klienta i wreszcie na poziomie użytkownika końcowego.

Usługami tymi można zarządzać za pośrednictwem aplikacji internetowych nazywanych **konsolami usług**. Dzierżawcami i kontami użytkowników można zarządzać za pośrednictwem aplikacji internetowej nazywanej **portalem zarządzania**.

Portal zarządzania umożliwia administratorom:

- Monitorowanie wykorzystania usług oraz uzyskiwanie dostępu do konsol usług
- Zarządzanie dzierżawcami
- Zarządzanie kontami użytkowników
- Konfigurowanie usług i limitów dla dzierżawców
- Zarządzanie magazynami
- Zarządzanie oznaczeniem marką
- Generowanie raportów dotyczących wykorzystania usługi

## Usługi Cyber Protect

W tej sekcji opisano zestawy funkcji wprowadzone w marcu 2021 r. wraz z nowym modelem rozliczeń. Dodatkowe informacje na temat zalet nowego modelu rozliczeń można znaleźć na karcie produktu Cyber Protect.

Na platformie Cyber Protect Cloud są dostępne następujące usługi i zestawy funkcji:

- **Cyber Protect**
  - **Ochrona** — pełna ochrona cybernetyczna dzięki funkcjom zabezpieczeń i zarządzania dostępnym w produkcie podstawowym oraz funkcjom odzyskiwania po awarii, tworzenia kopii zapasowych i odzyskiwania, automatyzacji oraz ochrony poczty e-mail dostępnym jako funkcje opłacane zgodnie z rzeczywistym wykorzystaniem. Funkcje te można rozszerzyć o zaawansowane pakiety ochrony, które podlegają dodatkowym opłatom.
    Pakiety ochrony zaawansowanej to zestawy unikatowych funkcji przeznaczonych do stosowania w bardziej złożonych sytuacjach w określonym obszarze funkcjonalnym, na przykład Zaawansowane kopie zapasowe, Ochrona zaawansowana i inne. Pakiety zaawansowane rozszerzają funkcje dostępne standardowo w usłudze Cyber Protect.
    Dodatkowe informacje o pakietach ochrony zaawansowanej można znaleźć w sekcji "Pakiety ochrony zaawansowanej" (s. 129).
  - **File Sync & Share** — rozwiązanie do bezpiecznego udostępniania firmowej zawartości z dowolnego miejsca, w dowolnym czasie i na dowolnym urządzeniu.

- **Fizyczne dostarczanie danych** — rozwiązanie, które oszczędza czas i zmniejsza ruch w sieci, umożliwiając wysyłanie danych do chmurowego centrum danych na dysku twardym.
- **Notary** — oparte na technologii łańcucha bloków rozwiązanie zapewniające autentyczność udostępnianej zawartości.

- **Licencja SPLA rozwiązania Cyber Infrastructure**

W portalu zarządzania można wybrać usługi i zestawy funkcji, które mają być dostępne dla dzierżawców. Konfiguracji dokonuje się w przypadku każdego dzierżawcy z osobna podczas jego inicjowania lub edycji, tak jak opisano w sekcji Tworzenie dzierżawcy.

# Tryby rozliczeń dotyczące rozwiązania Cyber Protect

Tryb rozliczeń to schemat ewidencjonowania i rozliczania związanego z korzystaniem z usług oraz ich funkcji. Tryb rozliczeń decyduje o tym, które jednostki będą podstawą do obliczania cen. Tryby rozliczeń mogą być ustawiane przez partnerów na poziomie klienta.

Mechanizm licencjonowania automatycznie uzyskuje pozycje oferty w zależności od funkcji wymaganych w planach ochrony. Użytkownicy mogą optymalizować poziom ochrony i koszty przez dostosowywanie planów ochrony do swoich potrzeb.

**Uwaga**
Można zastosować tylko jeden tryb rozliczeń na dzierżawcę-klienta.

## Tryby rozliczeń dotyczące komponentu Ochrona

Komponent Ochrona jest oferowany w dwóch trybach rozliczeń:

- Za obciążenie
- Za gigabajt

W obu trybach rozliczeń jest dostępny ten sam zestaw funkcji.

W obu trybach rozliczeń usługa Ochrona obejmuje funkcje ochrony standardowej, które sprawdzają się w przypadku większości zagrożeń związanych z bezpieczeństwem cybernetycznym. Użytkownicy mogą z nich korzystać bez dodatkowych opłat. Korzystanie ze standardowo udostępnianych funkcji może być ewidencjonowane, ale nie podlega opłatom. Pełną listę standardowo udostępnianych i podlegających rozliczeniom pozycji oferty można znaleźć w sekcji "Usługi Cyber Protect" (s. 7).

Nawet jeśli w przypadku klienta został włączony pakiet zaawansowany, rozliczanie rozpocznie się dopiero wtedy, gdy klient zacznie korzystać z funkcji tego pakietu w ramach planu ochrony. Gdy funkcja zaawansowana zostanie zastosowana w planie ochrony, mechanizm licencjonowania automatycznie przypisze wymaganą licencję do chronionego obciążenia.

Po zaprzestaniu korzystania z funkcji zaawansowanej licencja zostanie odwołana, a rozliczanie — zatrzymane. Mechanizm licencjonowania automatycznie przypisuje licencję, która odzwierciedla rzeczywiste korzystanie z funkcji.

Można przypisać tylko licencje dotyczące standardowych funkcji usługi Cyber Protect. Funkcje zaawansowane są rozliczane na podstawie wykorzystania i nie można ręcznie modyfikować ich licencji. Mechanizm licencjonowania automatycznie przypisuje licencje i cofa ich przypisanie. Typ licencji dla obciążenia można zmienić ręcznie, ale przypisanie zostanie zmienione, jeśli użytkownik zmodyfikuje plan ochrony tego obciążenia.

**Uwaga**
Rozliczanie funkcji ochrony zaawansowanej nie rozpoczyna się z chwilą ich włączenia. Rozpoczyna się dopiero wtedy, gdy klient zacznie korzystać z funkcji zaawansowanych w ramach planu ochrony. Włączone zestawy funkcji będą ewidencjonowane i uwzględniane w raportach z wykorzystania, ale nie będą uwzględniane w rozliczeniach, jeśli te funkcje nie będą używane.

## Tryby rozliczeń dotyczące usługi File Sync & Share

W przypadku usługi File Sync & Share są stosowane następujące tryby rozliczeń:

- Za użytkownika
- Za gigabajt

Można też stosować reguły rozliczeń obowiązujące w starszej wersji usługi File Sync & Share.

**Uwaga**
Rozliczanie zaawansowanej usługi File Sync & Share nie rozpoczyna się z chwilą jej włączenia. Rozpoczyna się dopiero wtedy, gdy klient zacznie korzystać z jej funkcji zaawansowanych. Włączony zestaw funkcji zaawansowanych będzie ewidencjonowany i uwzględniany w raportach o wykorzystaniu, ale nie będzie uwzględniany w rozliczeniach, jeśli te funkcje nie będą używane.

## Rozliczenia dotyczące usługi Fizyczne dostarczanie danych

Rozliczenia dotyczące usługi Fizyczne dostarczanie danych opierają się na modelu płatności zgodnie z rzeczywistym wykorzystaniem.

## Rozliczenia dotyczące usługi Notary

Rozliczenia dotyczące usługi Notary opierają się na modelu płatności zgodnie z rzeczywistym wykorzystaniem.

## Stosowanie trybów rozliczeń razem ze starszymi wersjami

Jeśli nadal nie dokonano przejścia na bieżący model rozliczeń, należy skorzystać z pozycji oferty w ramach jednego z trybów rozliczeń, aby zastąpić starsze wersje. Mechanizm licencjonowania automatycznie zoptymalizuje przypisane do klienta licencje, aby zminimalizować naliczaną kwotę.

**Uwaga**
Nie można łączyć wersji z trybami rozliczeń.

### Przechodzenie ze starszych wersji na bieżący model licencjonowania

Pozycje oferty dzierżawcy można zmienić ręcznie, edytując jego profil i wybierając dla niego pozycje oferty. Dodatkowe informacje na temat zmieniania modelu można znaleźć w sekcji "Zmienianie modelu między wersjami a trybami rozliczeń" (s. 10).

Jeśli chcesz przejść z wersji na tryby rozliczeń dla wielu klientów, zobacz artykuł Zbiorcze zmienianie wersji obejmujące wielu klientów (67942).

## Zmienianie modelu między wersjami a trybami rozliczeń

W portalu zarządzania można modyfikować konto dzierżawcy w celu zmienienia trybów rozliczeń (z Za obciążenie na Za gigabajt i na odwrót) dla pozycji oferty. Można też wprowadzać zmiany w ramach starszych wersji i trybów rozliczeń.

Informacje na temat zbiorowych zmian modelu dzierżawców można znaleźć w artykule Zbiorcze zmienianie wersji obejmujące wielu klientów (67942).

Proces zmieniania modelu obejmuje następujące kroki:

1. Przydzielenie nowych pozycji oferty dzierżawcy-klientowi (włączenie pozycji oferty i ustawienie limitów) w celu dopasowania do funkcji dostępnych w pierwotnej pozycji oferty.
2. Cofnięcie przypisania nieużywanych pozycji oferty i przypisanie pozycji oferty do obciążeń odpowiednio do funkcji używanych w planach ochrony (uzgodnienie wykorzystania).

Poniższa tabela ilustruje ten proces w obu kierunkach.

| | **Kierunek zmiany** | |
|---|---|---|
| | **Wersja > tryby rozliczeń** | **Tryb rozliczeń > tryb rozliczeń** |
| Zmiana modelu pozycji oferty | Należy włączyć pozycje oferty zapewniające wszystkie funkcje, które były dostępne w wersji źródłowej. | Zostanie włączony identyczny zestaw pozycji oferty. |
| Zmiana limitu | Limit ze źródłowej pozycji oferty zostanie zreplikowany do docelowych pozycji oferty. Źródłowy produkt standardowy → docelowy produkt standardowy. Źródłowy produkt standardowy → docelowe pakiety.<br>**Uwaga**<br>Jeśli zmieniasz model z wersji z podwersjami (na przykład „Cyber Protect (za obciążenie)”), limity zostaną zsumowane. | Limity ze źródłowej pozycji oferty zostaną zreplikowane do docelowej pozycji oferty. |
| Zmiany wykorzystania | Pozycje oferty zostaną ponownie przypisane do obciążeń zgodnie z funkcjami wymaganymi w ramach planów ochrony przypisanych do tych obciążeń. | |

## Przykład: Zmiana modelu z wersji Cyber Protect Advanced na rozliczenia Za obciążenie

W tym scenariuszu dzierżawca-klient używa wersji  Cyber Protect na 8 stacjach roboczych i ma ustawiony limit 10 obciążeń. 3 z tych stacji roboczych korzystają z inwentaryzacji oprogramowania i zarządzania poprawkami w ramach swoich planów ochrony, 2 stacje robocze mają włączone filtrowanie adresów URL w swoich planach ochrony, a 1 z komputerów korzysta z ciągłej ochrony danych. Poniższa tabela ilustruje konwersję wersji na nowe pozycje oferty.

| Źródłowe pozycje oferty — wykorzystanie/limit | Docelowe pozycje oferty — wykorzystanie/limit |
|---|---|
| Cyber Protect Advanced Workstation — 8/10 | • Stacje robocze — 8/10<br>• Ochrona zaawansowana — 2/10<br>• Zaawansowane tworzenie kopii zapasowych, stacje robocze — 1/10<br>• Zarządzanie zaawansowane — 3/10 |

Proces zmiany modelu wymagał wykonania następujących kroków:

1. Automatyczne włączenie pozycji oferty obejmujących funkcje dostępne w wersji źródłowej.
2. Zreplikowanie limitów do nowych pozycji oferty.
3. Wykorzystanie zostało uzgodnione z faktycznym wykorzystaniem w planach ochrony: trzy obciążenia korzystające z funkcji pakietu Zarządzanie zaawansowane, dwa obciążenia — z funkcji pakietu Ochrona zaawansowana, jedno obciążenie — z funkcji pakietu Zaawansowane tworzenie kopii zapasowych.

## Na przykład: wersja Cyber Protect za obciążenie na rozliczenia Za obciążenie

W tym przykładzie klient ma kilka wersji przypisanych do obciążeń. Każde obciążenie może mieć przypisaną tylko jedną wersję lub jeden tryb rozliczeń.

| Źródłowe pozycje oferty — wykorzystanie/limit | Docelowe pozycje oferty — wykorzystanie/limit |
|---|---|
| Cyber Protect Essentials — 6 stacji roboczych / 12 | • Stacje robocze — 14/42<br>• Zaawansowane tworzenie kopii zapasowych, stacje robocze — 2/42<br>• Ochrona zaawansowana — 13/42<br>• Zarządzanie zaawansowane — 5/42 |
| Cyber Protect Standard — 5 stacji roboczych / 10 | |
| Cyber Protect Advanced Workstation — 2/10 | |
| Cyber Backup Standard Workstation — 1/10 | |

Proces zmiany modelu wymagał wykonania następujących kroków:

1. Automatyczne włączenie pozycji oferty obejmujących funkcje dostępne we wszystkich wersjach źródłowych. W przypadku trybów rozliczeń do obciążeń można przypisać wiele pozycji oferty, stosownie do potrzeb.
2. Zsumowanie i zreplikowanie limitów.
3. Uzgodnienie wykorzystania z planami ochrony.

## Zmienianie trybu rozliczeń dla dzierżawcy-partnera

***Aby zmienić tryb rozliczeń dla dzierżawcy-partnera***

1. W portalu zarządzania wybierz **Klienci**.
2. Zaznacz dzierżawcę-partnera, którego tryb rozliczeń chcesz zmienić, a następnie kliknij ikonę wielokropka i **Konfiguruj**.
3. Na karcie **Cyber Protect** wybierz usługę, w której przypadku chcesz zmienić tryb rozliczeń, i kliknij **Edytuj**.
4. Wybierz tryb rozliczeń i włącz lub wyłącz dostępne pozycje oferty stosownie do potrzeb.
5. Kliknij **Zapisz**.

## Zmienianie trybu rozliczeń w przypadku dzierżawcy-klienta

W przypadku dzierżawcy-klienta rozliczenia można zmienić następująco:

- Edytować pierwotny tryb rozliczeń przez włączenie lub wyłączenie pozycji oferty.
- Przejść na zupełnie nowy tryb rozliczeń.

Dodatkowe informacje na temat edycji dostępnych pozycji oferty można znaleźć w sekcji Włączanie lub wyłączanie pozycji oferty.

***Aby zmienić tryb rozliczeń dla dzierżawcy-klienta***

1. W portalu zarządzania wybierz **Klienci**.
2. Zaznacz dzierżawcę-klienta, którego wersję chcesz zmienić, a następnie kliknij ikonę wielokropka i **Konfiguruj**.
3. Na karcie **Konfiguruj** w polu **Usługa** wybierz nowy tryb rozliczeń.

   Zostanie otwarte okno dialogowe z informacją o konsekwencjach przejścia na nowy tryb rozliczeń.
4. Wprowadź nazwę użytkownika, aby potwierdzić wybór.

**Uwaga**
Wprowadzenie tej zmiany może potrwać do 10 minut.

# Zarządzanie pozycjami oferty i limitami

W tej sekcji opisano:

- Czym są usługi i pozycje ofert?
- Jak można włączać i wyłączać pozycje ofert?
- Czym są tryby rozliczeń?
- Czym są pakiety ochrony zaawansowanej?
- Czym są starsze wersje i podwersje?
- Co to są elastyczne i sztywne limity?
- Kiedy można przekroczyć sztywny limit?
- Co to jest transformacja limitu kopii zapasowych?
- Jak dostępność pozycji oferty wpływa na dostępność instalatora w konsoli usługi?

## Usługi i pozycje oferty

### Usługi

Usługa chmurowa to zestaw funkcji, które są hostowane przez partnera albo w chmurze prywatnej klienta końcowego. Usługi są zwykle sprzedawane w ramach subskrypcji lub na zasadzie płatności zgodnie z rzeczywistym wykorzystaniem.

Usługa  Cyber Protect integruje funkcje bezpieczeństwa cybernetycznego, ochrony danych i zarządzania w celu ochrony punktów końcowych, systemów i danych przed zagrożeniami cybernetycznymi. Usługa Cyber Protect obejmuje kilka komponentów: Ochrona, File Sync & Share, Notary oraz Fizyczne dostarczanie danych. Niektóre z nich można rozszerzyć o funkcje zaawansowane za pomocą pakietów ochrony zaawansowanej. Szczegółowe informacje na temat funkcji standardowo udostępnianych i zaawansowanych można znaleźć w sekcji "Usługi Cyber Protect" (s. 7).

### Pozycje oferty

Pozycja oferty to zestaw funkcji usługi zgrupowanych według określonego typu obciążenia lub funkcjonalności, takiego jak pamięć masowa, infrastruktura odzyskiwania po awarii itd. Włączając pozycję oferty, określasz, które obciążenia mogą być chronione, ile obciążeń może być chronionych (przez ustawienie limitów) oraz jaki poziom ochrony będzie dostępny dla Twoich partnerów, klientów i ich użytkowników (przez włączenie lub wyłączenie pakietów ochrony zaawansowanej).

Funkcje, które nie zostaną włączone, będą ukryte przed klientami i użytkownikami, chyba że zostanie skonfigurowany scenariusz sprzedaży dodatkowej. Więcej informacji o scenariuszach sprzedaży dodatkowej można znaleźć w sekcji "Konfigurowanie scenariuszy sprzedaży dodatkowej dla klientów" (s. 69).

Dane o korzystaniu z funkcji są zbierane z usług i odzwierciedlane w pozycjach oferty, co jest wykorzystywane w raportach i późniejszych rozliczeniach.

## Tryby rozliczeń i wersje

W przypadku korzystania ze starszych wersji można włączyć tylko jedną pozycję oferty na obciążenie. W przypadku korzystania z trybów rozliczeń funkcje są podzielone, dzięki czemu można włączyć wiele pozycji oferty (funkcje usług i pakiety zaawansowane) na obciążenie, aby zapewnić lepsze dostosowanie do potrzeb klientów i precyzyjniejsze rozliczenia — tylko za funkcje, których klienci faktycznie używają.

Dodatkowe informacje na temat trybów rozliczeń za usługę Cyber Protect można znaleźć w sekcji "Tryby rozliczeń dotyczące rozwiązania Cyber Protect" (s. 8).

W celu konfigurowania usług dostępnych dla dzierżawców można stosować tryby rozliczeń lub wersje. Można wybrać tylko jeden tryb rozliczeń lub jedną wersję na dzierżawcę-klienta. W związku z tym w celu zastosowania różnych trybów rozliczeń w przypadku różnych funkcji usługi należy utworzyć dla klienta wielu dzierżawców. Jeśli więc na przykład klient chce mieć skrzynki pocztowe Microsoft 365 w trybie rozliczeń Za gigabajt, a program Teams w trybie rozliczeń Za obciążenie, należy utworzyć dla niego dwóch dzierżawców.

Aby ograniczyć korzystanie z usług w ramach pozycji oferty, można dla niej zdefiniować limity. Zobacz "Elastyczne i sztywne limity" (s. 15).

## Włączanie lub wyłączanie pozycji oferty

Można włączyć wszystkie pozycje oferty dostępne w ramach danej wersji lub trybu rozliczeń — zgodnie z opisem podanym w sekcji Tworzenie dzierżawcy.

**Uwaga**
Wyłączenie wszystkich pozycji oferty usługi nie powoduje automatycznego wyłączenia usługi.

Występują pewne ograniczenia w zakresie wyłączania pozycji oferty. Wymieniono je w poniższej tabeli.

| Pozycja oferty | Wyłączanie | Wynik |
|---|---|---|
| Magazyn kopii zapasowych | Można wyłączyć, gdy poziom wykorzystania jest równy zeru. | Chmura przestanie być dostępna jako miejsce docelowe kopii zapasowych w obszarze dzierżawcy klienta. |
| Lokalne kopie zapasowe | Można wyłączyć, gdy poziom wykorzystania jest równy zeru. | Magazyn lokalny przestanie być dostępny jako miejsce docelowe kopii zapasowych u dzierżawcy klienta. |
| Źródła danych (w tym Microsoft 365 i Google Workspace) | Można wyłączyć, gdy poziom wykorzystania jest równy zeru. | Tworzenie kopii zapasowych i odzyskiwanie źródeł danych (w tym Microsoft 365 i Google Workspace) przestanie być dostępne w obszarze dzierżawcy-klienta. |

| | | |
|---|---|---|
| Wszystkie pozycje oferty usługi Odzyskiwanie po awarii | Można wyłączyć, gdy poziom wykorzystania jest większy niż zero. | Szczegółowe informacje można znaleźć w sekcji „Elastyczne i sztywne limity”. |
| Wszystkie pozycje oferty usługi Notary | Można wyłączyć, gdy poziom wykorzystania jest równy zeru. | Usługa Notary będzie niedostępna w obszarze dzierżawcy klienta. |
| Wszystkie pozycje oferty usługi File Sync & Share | Pozycji ofert nie można włączać i wyłączać osobno. | Usługa File Sync & Share będzie niedostępna w obszarze dzierżawcy klienta. |
| Wszystkie pozycje oferty usługi Fizyczne dostarczanie danych | Można wyłączyć, gdy poziom wykorzystania jest równy zeru. | Usługa Fizyczne dostarczanie danych będzie niedostępna w obszarze dzierżawcy klienta. |

W przypadku pozycji oferty, której nie można wyłączyć, gdy poziom wykorzystania jest większy niż zero, można ręcznie usunąć dane o wykorzystaniu, a następnie wyłączyć daną pozycję oferty.

## Elastyczne i sztywne limity

**Limity** pozwalają ograniczać możliwości korzystania z usługi przez danego dzierżawcę. Aby ustawić te limity, wybierz klienta na karcie **Klienci**, wybierz kartę usługi, a następnie kliknij **Edytuj**.

W przypadku przekroczenia limitu na adres e-mail użytkownika jest wysyłane stosowne powiadomienie. Jeśli nie zostanie ustawiona nadwyżka limitu, limit jest uznawany za „**elastyczny**”. Oznacza to, że ograniczenia dotyczące korzystania z usługi Cyber Protection nie są stosowane.

Jeśli zostanie ustawiona nadwyżka limitu, limit jest uznawany za „**sztywny**”. **Nadwyżka** umożliwia użytkownikowi przekroczenie limitu o określoną wartość. W przypadku przekroczenia nadwyżki zostaną zastosowane ograniczenia dotyczące korzystania z usługi.

**Przykład**

**Elastyczny limit**: Został ustawiony limit 20 stacji roboczych. Gdy liczba chronionych stacji roboczych klienta sięgnie 20, klient otrzyma stosowne powiadomienie pocztą e-mail, ale usługa Cyber Protection nadal będzie dostępna.

**Sztywny limit**: Jeśli ustawiono limit 20 stacji roboczych, a nadwyżka wynosi 5, to gdy liczba chronionych stacji roboczych sięgnie 20, klient otrzyma stosowne powiadomienie pocztą e-mail, ale gdy liczba ta wyniesie 25, usługa Cyber Protection zostanie wyłączona.

Po osiągnięciu sztywnego limitu usługa zostaje ograniczona (nie można objąć ochroną kolejnego obciążenia ani korzystać z dodatkowego miejsca w pamięci masowej). W przypadku przekroczenia sztywnego limitu na adres e-mail użytkownika jest wysyłane stosowne powiadomienie.

### Poziomy, na których można określać limity

Limity można ustawiać na poziomach wymienionych w poniższej tabeli.

| Dzierżawca/użytkownik | Elastyczny limit (tylko limit) | Sztywny limit (limit i nadwyżka) |
|---|---|---|
| Partner | tak | nie |
| Folder | tak | nie |
| Klient | tak | tak |
| Jednostka | nie | nie |
| Użytkownik | tak | tak |

Elastyczne limity można ustawiać na poziomach partnerów i folderów. Na poziomie jednostki nie można ustawić żadnego limitu. Sztywne limity można ustawiać na poziomach klientów i użytkowników.

Suma sztywnych limitów ustawionych na poziomie użytkowników nie może przekroczyć odpowiadającego mu sztywnego limitu klienta.

## Konfigurowanie elastycznych i sztywnych limitów

***Aby skonfigurować limity dla klientów***

1. W portalu zarządzania wybierz **Klienci**.
2. Wybierz klienta, dla którego chcesz skonfigurować limity.
3. Wybierz kartę **Ochrona**, a następnie kliknij **Edytuj**.
4. Wybierz typ ustawianego limitu. Na przykład wybierz **Stacje robocze** lub **Serwery**.
5. Kliknij widoczne po prawej stronie łącze **Bez ograniczeń**, aby otworzyć okno **Edycja limitu**.
   - Jeśli chcesz poinformować klienta o limicie, a nie chcesz mu ograniczać możliwości korzystania z usługi, ustaw wartość limitu w polu **Elastyczny limit**.
     Po osiągnięciu limitu klient otrzyma powiadomienie e-mail, ale usługa Cyber Protection nadal będzie dla niego dostępna.
   - Jeśli chcesz ograniczyć możliwość korzystania z usługi przez klienta, wybierz **Sztywny limit** i ustaw wartość limitu w polu widocznym pod opcją **Sztywny limit**.
     Po osiągnięciu limitu klient otrzyma powiadomienie e-mail i usługa Cyber Protection zostanie dla niego wyłączona.
6. W oknie **Edycja limitu** kliknij **Gotowe**, a następnie kliknij **Zapisz**.

## Limity dotyczące usługi Kopia zapasowa

Możesz określić limit miejsca w chmurze, limit lokalnych kopii zapasowych oraz maksymalną liczbę komputerów / urządzeń / witryn internetowych, które może chronić użytkownik. Dostępne są niżej wymienione limity.

## Limity urządzeń

- **Stacje robocze**
- **Serwery**
- **Maszyny wirtualne**
- **Urządzenia mobilne**
- **Serwery hostingu witryn internetowych** (serwery fizyczne i wirtualne z systemem Linux oraz uruchomionym panelem sterowania Plesk, cPanel, DirectAdmin, VirtualMin lub ISPManager)
- **Witryny internetowe**

Komputer, urządzenie lub witryna internetowe są uznawane za chronione, gdy jest do nich stosowany co najmniej jeden plan ochrony. Urządzenie mobilne staje się chronione po utworzeniu pierwszej kopii zapasowej.

W przypadku przekroczenia nadwyżki liczby urządzeń użytkownik nie może zastosować planu ochrony do kolejnych urządzeń.

## Limity chmurowych źródeł danych

- **Stanowiska Microsoft 365**

  Dostawca usługi stosuje ten limit dla całej firmy. Administratorzy firmy mogą wyświetlać ten limit oraz monitorować poziom jego wykorzystania w portalu zarządzania.

  Licencjonowanie stanowisk Microsoft 365 zależy od wybranego trybu rozliczeniowego za rozwiązanie Cyber Protection.

  W trybie rozliczeń **Za obciążenie** limit **Stanowiska Microsoft 365** jest liczony według liczby unikatowych użytkowników. Unikatowy użytkownik to użytkownik, który ma co najmniej jeden z następujących elementów:

  - Chroniona skrzynka pocztowa
  - Chronione dane OneDrive
  - Uzyskaj dostęp do co najmniej jednego chronionego zasobu na poziomie firmy: Witryna Microsoft 365 SharePoint Online lub Microsoft 365 Teams.
    Aby się dowiedzieć, jak sprawdzić liczbę członków witryny Microsoft 365 SharePoint lub Teams, zapoznaj się z tym artykułem bazy wiedzy Knowledge Base.

  **Uwaga**

  Blokowani użytkownicy usług Microsoft 365, którzy nie mają chronionej osobistej skrzynki pocztowej ani konta OneDrive i mają dostęp tylko do udostępnionych zasobów (udostępnione skrzynki pocztowe, witryny SharePoint i Microsoft Teams), nie są uwzględniani w opłatach.

  Blokowani użytkownicy to ci, którzy nie mają ważnej nazwy logowania i nie mogą uzyskać dostępu do usług Microsoft 365. Informacje o tym, jak zablokować wszystkich użytkowników nielicencjonowanych z organizacji Microsoft 365, można znaleźć w sekcji "Blokowanie logowania się nielicencjonowanych użytkowników usługi Microsoft 365" (s. 20).

Następujące stanowiska Microsoft 365 nie są objęte opłatą i nie wymagają licencji na stanowisko:

- Udostępnione skrzynki pocztowe
- Pomieszczenia i wyposażenie
- Użytkownicy zewnętrzni mający dostęp do witryn SharePoint i/lub Microsoft Teams uwzględnionych w kopii zapasowej

Więcej informacji na temat opcji licencjonowania w trybie rozliczeniowym za gigabajt można znaleźć w artykule Cyber Protect Cloud: licencjonowanie usługi Microsoft 365 za GB.

Więcej informacji na temat opcji licencjonowania w trybie rozliczeniowym za obciążenie można znaleźć w artykule Cyber Protect Cloud: zmiany w licencjonowaniu i cenach usługi Microsoft 365.

- **Microsoft 365 Teams**

  Dostawca usługi stosuje ten limit dla całej firmy. Ten limit powoduje włączenie lub wyłączenie funkcji ochrony instancji Microsoft 365 Teams oraz ustawienie maksymalnej liczby chronionych zespołów. Do ochrony jednego zespołu, niezależnie od liczby jego członków lub kanałów, wymagany jest jeden limit. Administratorzy firmy mogą wyświetlać ten limit oraz monitorować poziom jego wykorzystania w portalu zarządzania.

- **Microsoft 365 SharePoint Online**

  Dostawca usługi stosuje ten limit dla całej firmy. Ten limit powoduje włączenie lub wyłączenie możliwości ochrony witryn programu SharePoint Online oraz ustawienie maksymalnej liczby chronionych zbiorów witryn i witryn grup.

  Administratorzy firmy mogą wyświetlać ten limit w portalu zarządzania. Mogą też wyświetlać ten limit oraz ilość miejsca w pamięci masowej zajmowanego przez kopie zapasowe SharePoint Online w raportach dotyczących wykorzystania.

- **Stanowiska Google Workspace**

  Dostawca usługi stosuje ten limit dla całej firmy. Firma może chronić skrzynki pocztowe **Gmail** (w tym kalendarz i kontakty), pliki z **Dysku Google** lub oba te rodzaje elementów. Administratorzy firmy mogą wyświetlać ten limit oraz monitorować poziom jego wykorzystania w portalu zarządzania.

- **Dysk współdzielony Google Workspace**

  Dostawca usługi stosuje ten limit dla całej firmy. Ten limit powoduje włączenie lub wyłączenie funkcji ochrony Dysków współdzielonych Google Workspace. W przypadku jego włączenia można chronić dowolną liczbę Dysków współdzielonych. Administratorzy firmy nie mogą przeglądać limitu w portalu zarządzania, ale mogą przeglądać ilość miejsca w pamięci masowej zajmowanego przez kopie zapasowe Dysków współdzielonych w raportach dotyczących wykorzystania.

  Tworzenie kopii zapasowych Dysków współdzielonych Google Workspace jest dostępne tylko dla klientów, którzy dodatkowo mają co najmniej jeden limit stanowisk Google Workspace. Limit ten jest tylko sprawdzany — nie jest wykorzystywany.

Stanowisko Microsoft 365 jest uznawane za chronione, gdy do skrzynki pocztowej lub danych OneDrive użytkownika jest stosowany co najmniej jeden plan ochrony. Stanowisko Google Workspace jest uznawane za chronione, gdy do skrzynki pocztowej lub danych Dysku Google użytkownika jest stosowany co najmniej jeden plan ochrony.

W przypadku przekroczenia nadwyżki stanowisk administrator firmy nie może zastosować planu ochrony do kolejnych stanowisk.

## Limity miejsca w pamięci masowej

- **Lokalne kopie zapasowe**

  Limit **Lokalnych kopii zapasowych** ogranicza łączny rozmiar lokalnych kopii zapasowych tworzonych za pomocą infrastruktury chmury. Dla tego limitu nie można ustawić nadwyżki.
- **Zasoby chmury**

  Limit **Zasoby chmury** łączy w sobie limit miejsca w pamięci masowej na kopie zapasowe oraz limity odzyskiwania po awarii. Limit miejsca w pamięci masowej na kopie zapasowe wyznacza łączny rozmiar kopii zapasowych znajdujących się w danej chmurze. W przypadku przekroczenia nadwyżki limitu miejsca w pamięci masowej na kopie zapasowe tworzenie kopii zapasowej zakończy się niepowodzeniem.

## Przekroczenie limitu magazynu kopii zapasowych

Limitu magazynu kopii zapasowych nie można przekroczyć. Certyfikat agenta ochrony ma limit techniczny równy sumie limitu kopii zapasowych i nadwyżki dzierżawcy. W przypadku przekroczenia tego limitu nie można rozpocząć operacji tworzenia kopii zapasowej. W przypadku wyczerpania limitu określonego w certyfikacie podczas tworzenia kopii zapasowej operacja ta zostanie pomyślnie ukończona. W przypadku wykorzystania nadwyżki podczas tworzenia kopii zapasowej operacja ta zakończy się niepowodzeniem.

**Przykład**:

Dzierżawca-użytkownik ma 1 TB wolnego miejsca w ramach limitu, a skonfigurowana dla niego nadwyżka wynosi 5 TB. Użytkownik uruchamia operację tworzenia kopii zapasowej. Jeśli rozmiar tworzonej kopii zapasowej wynosi na przykład 3 TB, tworzenie kopii zapasowej zostanie pomyślnie ukończona, ponieważ nie zostanie przekroczona nadwyżka. Jeśli rozmiar tworzonej kopii zapasowej przekracza 6 TB, w chwili przekroczenia nadwyżki operacja tworzenia kopii zapasowej zakończy się niepowodzeniem.

## Transformacja limitu kopii zapasowych

Ogólnie rzecz biorąc, uzyskiwanie limitu kopii zapasowych i mapowanie pozycji oferty na typy zasobów działa następująco: system porównuje dostępne pozycje oferty z typem zasobów, a następnie uzyskuje limit dotyczący dopasowanej pozycji oferty.

Możliwe jest również przypisanie innego limitu pozycji oferty, nawet jeśli nie odpowiada ona dokładnie typowi zasobów. Funkcja ta jest nazywana **transformacją limitu kopii zapasowych**. Jeśli nie ma pasującej pozycji oferty, system próbuje znaleźć droższy odpowiedni limit dla danego typu zasobów (automatyczna transformacja limitu kopii zapasowych). Jeśli nie znajdzie się nic odpowiedniego, można ręcznie przypisać limit usługi do typu zasobów w konsoli usługi.

**Przykład**

Chcesz utworzyć kopię zapasową maszyny wirtualnej (stacji roboczej, opartej na agencie).

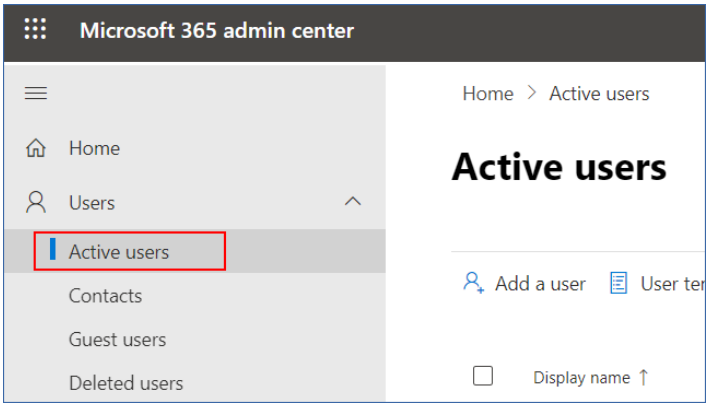
Najpierw system sprawdzi, czy został przypisany limit **Maszyny wirtualne**. Jeśli nie zostanie on znaleziony, system automatycznie spróbuje uzyskać limit **Stacje robocze**. Jeśli i on nie zostanie znaleziony, inny limit nie zostanie automatycznie uzyskany. Jeśli masz wystarczająco duży limit, który jest droższy od limitu **Maszyny wirtualne** i może zostać zastosowany do maszyny wirtualnej, możesz się zalogować do konsoli usługi i ręcznie przypisać limit **Serwery**.

## Blokowanie logowania się nielicencjonowanych użytkowników usługi Microsoft 365

Aby uniemożliwić logowanie się wszystkim użytkownikom nielicencjonowanym z organizacji Microsoft 365, należy edytować ich status logowania.

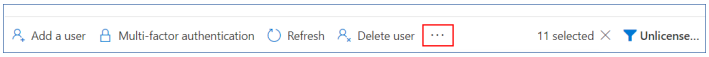
***Aby zablokować logowanie się użytkowników nielicencjonowanych***

1. Zaloguj się do centrum administracyjnego usługi Microsoft 365 (https://admin.microsoft.com) jako administrator globalny.
2. W menu nawigacyjnym wybierz **Użytkownicy** > **Aktywni użytkownicy**.




3. Kliknij **Filtruj**, a następnie wybierz **Użytkownicy nielicencjonowani**.


4. Zaznacz pola wyboru obok nazw użytkowników, a następnie kliknij ikonę wielokropka (...).




5. W menu wybierz **Edytuj status logowania**.
6. Zaznacz pole wyboru **Blokuj logowanie się użytkowników** i kliknij **Zapisz**.

## Limity dotyczące usługi Odzyskiwanie po awarii

**Uwaga**
Pozycje ofert usługi odzyskiwania po awarii są dostępne tylko wraz z dodatkiem Disaster Recovery.

Dostawca usługi stosuje te limity dla całej firmy. Administratorzy firmy mogą przeglądać limity oraz monitorować wykorzystanie w portalu zarządzania, ale nie mogą ustawiać limitów użytkowników.

- **Magazyn odzyskiwania po awarii**
  W magazynie odzyskiwania po awarii wyświetlany jest rozmiar pamięci „cold storage" serwerów chronionych za pomocą usługi Odzyskiwanie po awarii. Rozmiar ten jest obliczane od chwili

utworzenia serwera odzyskiwania, niezależnie od tego, czy ten serwer jest aktualnie uruchomiony. W przypadku osiągnięcia nadwyżki tego limitu nie będzie można tworzyć serwerów podstawowych bądź serwerów odzyskiwania ani dodawać/rozszerzać dysków już istniejących serwerów podstawowych. W przypadku przekroczenia nadwyżki tego limitu nie będzie można inicjować przełączania awaryjnego ani uruchamiać zatrzymanego serwera. Działające serwery kontynuują pracę.

- **Punkty obliczeniowe**

  Limit ogranicza zasoby procesora i pamięci RAM wykorzystywane przez serwery podstawowe oraz serwery odzyskiwania podczas okresu rozliczeniowego. W przypadku osiągnięcia nadwyżki tego limitu wszystkie serwery podstawowe i serwery odzyskiwania są wyłączane. Nie można użyć tych serwerów aż do rozpoczęcia następnego okresu rozliczeniowego. Domyślny okres rozliczeniowy to pełny miesiąc kalendarzowy.

  W przypadku wyłączenia tego limitu nie można korzystać z serwerów — niezależnie od okresu rozliczeniowego.
- **Publiczne adresy IP**

  Ten limit ogranicza liczbę publicznych adresów IP, które można przypisać serwerom podstawowym i serwerom odzyskiwania. W przypadku osiągnięcia nadwyżki tego limitu nie można włączać publicznych adresów IP dla kolejnych serwerów. Możesz zablokować możliwość używania publicznego adresu IP na danym serwerze, odznaczając pole wyboru **Publiczny adres IP** w ustawieniach serwera. Następnie możesz pozwolić innemu serwerowi używać publicznego adresu IP, który najczęściej będzie inny.

  W przypadku wyłączenia tego limitu wszystkie serwery przestają używać publicznych adresów IP, przez co stają się niedostępne z Internetu.
- **Serwery chmurowe**

  Ten limit ogranicza łączną liczbę serwerów podstawowych i serwerów odzyskiwania. W przypadku wyczerpania nadwyżki tego limitu nie można tworzyć serwerów podstawowych ani serwerów odzyskiwania.

  W przypadku wyłączenia tego limitu serwery są widoczne w konsoli usługi, ale dostępna jest jedynie operacja **Usuń**.
- **Dostęp do Internetu**

  Ten limit umożliwia włączanie lub wyłączanie dostępu do Internetu z serwerów podstawowych i serwerów odzyskiwania.

  W przypadku wyłączenia tego limitu serwery podstawowe i serwery odzyskiwania nie będą mogły nawiązać połączenia z Internetem.

## Limity dotyczące usługi File Sync & Share

Dla dzierżawcy można określić następujące limity dotyczące usługi File Sync & Share:

- **Użytkownicy**

  Ten limit określa liczbę użytkowników mających dostęp do usługi.

  Konta administratorów nie są wliczane do tego limitu.
- **Chmura**

To ustawienie dotyczy pamięci w chmurze przeznaczonej na pliki użytkowników. Limit określa ilość miejsca w chmurze przydzielonego dzierżawcy.

## Limity dotyczące usługi Fizyczne dostarczanie danych

Wykorzystanie limitów dotyczących usługi Fizyczne dostarczanie danych jest szacowane na podstawie liczby dysków. Na jednym dysku można zapisać początkowe kopie zapasowe wielu komputerów.

Dla dzierżawcy można określić następujące limity dotyczące usługi Fizyczne dostarczanie danych:

- **W chmurze**
  Umożliwia wysłanie początkowej kopii zapasowej do chmurowego centrum danych na dysku twardym. Ten limit określa maksymalną liczbę dysków, które można przesłać do chmurowego centrum danych.

## Limity dotyczące usługi Notary

Dla dzierżawcy można określić następujące limity dotyczące usługi Notary:

- **Magazyn Notary**
  Magazyn Notary to chmura, w której są przechowywane notaryzowane pliki, podpisane pliki praz pliki w trakcie notaryzacji lub podpisywania. Ten limit oznacza maksymalną ilość miejsca, które mogą zajmować te pliki.
  Aby zmniejszyć poziom wykorzystania tego limitu, można usunąć z magazynu Notary pliki już notaryzowane lub podpisane.
- **Notaryzacje**
  Ten limit oznacza maksymalną liczbę plików, które można notaryzować przy użyciu usługi Notary. Plik jest uznawany za notaryzowany, gdy tylko zostanie przesłany do magazynu Notary, a jego status notaryzacji zostanie zmieniony na W toku.
  W przypadku kilkukrotnej notaryzacji tego samego pliku każda notaryzacja jest liczona osobno.
- **E-podpisy**
  Ten limit oznacza maksymalną liczbę plików, które można podpisać przy użyciu usługi Notary. Plik jest uznawany za podpisany, gdy tylko zostanie wysłany do podpisu.

## Zmienianie limitów usług komputerów

Poziom ochrony komputera jest wyznaczany przez zastosowany do niego limit usług. Limity usług odnoszą się do pozycji ofert dostępnych dla dzierżawcy, w ramach którego jest zarejestrowany dany komputer.

Limit usług jest przypisywany automatycznie w chwili pierwszego zastosowania planu ochrony do komputera.

Przypisywany jest najbardziej odpowiedni limit — z uwzględnieniem typu chronionego komputera, jego systemu operacyjnego, wymaganego poziomu ochrony i dostępności limitu. Jeśli najbardziej odpowiedni limit nie jest dostępny w danej organizacji, przypisywany jest drugi w kolejności spośród

najbardziej odpowiednich. Jeśli na przykład najbardziej odpowiednim limitem jest **Serwer hostingu witryn internetowych**, ale nie jest on dostępny, zostanie przypisany limit **Serwer**.

Przykłady przypisania limitów:

- Komputerowi fizycznemu z systemem operacyjnym Windows Server lub Linux zostanie przypisany limit **Serwer**.
- Komputerowi fizycznemu z systemem operacyjnym Windows dla komputerów osobistych zostanie przypisany limit **Stacja robocza**.
- Komputerowi fizycznemu z systemem operacyjnym Windows 10 z włączoną rolą Hyper-V zostanie przypisany limit **Stacja robocza**.
- Komputerowi działającemu w ramach infrastruktury VDI, której agent ochrony jest zainstalowany w systemie operacyjnym gościa (np. agent dla systemu Windows), zostanie przypisany limit **Maszyna wirtualna**. Może też zostać zastosowany limit **Stacja robocza**, jeśli limit **Maszyna wirtualna** jest niedostępny.
- Komputerowi działającemu w ramach infrastruktury VDI i uwzględnianemu w kopii zapasowej w trybie bezagentowym (np. za pomocą agenta dla VMware lub agenta dla Hyper-V), zostanie przypisany limit **Maszyna wirtualna**.
- Serwerowi Hyper-V lub vSphere zostanie przypisany limit **Serwer**.
- Serwerowi z panelem sterowania cPanel lub Plesk zostanie przypisany limit **Serwer hostingu witryn internetowych**. W tym przypadku może też zostać zastosowany limit **Maszyna wirtualna** lub **Serwer** — w zależności od typu maszyny, na której działa serwer witryn internetowych — jeśli limit **Serwer hostingu witryn internetowych** jest niedostępny.
- Kopia zapasowa uwzględniająca aplikacje wymaga limitu **Serwer**, nawet w przypadku stacji roboczej.

Później można ręcznie zmienić pierwotne przypisanie. Aby na przykład zastosować bardziej zaawansowany plan ochrony do tego samego komputera, może być konieczne podwyższenie limitu usług komputera. Jeśli funkcje wymagane przez ten plan ochrony nie są obsługiwane przez aktualnie przypisany limit usług, wykonanie planu ochrony się nie powiedzie.

Jeśli po przypisaniu pierwotnego limitu zostanie wykupiony bardziej odpowiedni limity usług, można go zmienić. Załóżmy, że do maszyny wirtualnej został przypisany limit **Stacja robocza**. Po wykupieniu limitu **Maszyny wirtualne** można go ręcznie przypisać do tej maszyny, zastępując pierwotny limit **Stacja robocza**.

Można też zwolnić aktualnie przypisany limit usług i przypisać go do innego komputera lub maszyny wirtualnej.

Istnieje możliwość zmiany limitu usług dla jednego komputera lub maszyny wirtualnej bądź grupy komputerów lub maszyn.

***Aby zmienić limit usług dla wybranego komputera***

1. W konsoli usługi Cyber Protection przejdź do sekcji **Urządzenia**.
2. Wybierz właściwy komputer i kliknij **Szczegóły**.

3. W sekcji **Limit usług** kliknij **Zmień**.
4. W oknie **Zmień licencję** wybierz odpowiedni limit usług lub opcję **Brak limitu** i kliknij **Zmień**.

***Aby zmienić limit usług dla grupy komputerów***

1. W konsoli usługi Cyber Protection przejdź do sekcji **Urządzenia**.
2. Wybierz więcej niż jeden komputer i kliknij **Przypisz limit**.
3. W oknie **Zmień licencję** wybierz odpowiedni limit usług lub opcję **Brak limitu** i kliknij **Zmień**.

## Zależność instalatorów agentów od pozycji oferty

W zależności od dozwolonych pozycji oferty, w sekcji **Dodaj urządzenia** konsoli usługi będzie dostępny odpowiedni instalator agenta. W poniższej tabeli przedstawiono instalatory agentów i ich dostępność w konsoli usługi w zależności od włączonych pozycji oferty.

| **Włączona pozycja oferty** / **Instalator agenta** | **Serwery** | **Stacje robocze** | **Maszyny wirtualne** | **Stanowiska Microsoft 365** | **Stanowiska Google Workspace** | **Urządzenia mobilne** | **Serwery hostingu witryn internetowych** | **Witryny internetowe** |
|---|---|---|---|---|---|---|---|---|
| Stacje robocze — agent dla systemu Windows | | + | + | | | | | + |
| Stacje robocze — agent dla systemu Mac OS | | + | + | | | | | + |
| Serwery — agent dla systemu Windows | + | | + | | | | + | + |
| Serwery — agent dla systemu | + | | + | | | | + | + |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Linux | | | | | | | | |
| Agent dla Hyper-V | | | + | | | | | |
| Agent dla VMware | | | + | | | | | |
| Agent dla Virtuozzo | | | + | | | | | |
| Agent dla SQL | + | | + | | | | | |
| Agent dla programu Exchange | + | | + | | | | | |
| Agent dla usługi Active Directory | + | | + | | | | | |
| Agent dla usługi Microsoft 365 | | | | + | | | | |
| Agent dla Google Workspace | | | | | + | | | |
| Pełny instalator dla systemu Windows | + | + | + | | | | + | + |
| Wersja | | | | | | + | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| mobilna (iOS i Android) | | | | | | | | |

# Korzystanie z portalu zarządzania

Opisane poniżej czynności stanowią wskazówki dotyczące użytkowania portalu zarządzania w podstawowym zakresie.

## Obsługiwane przeglądarki internetowe

Interfejs internetowy obsługuje następujące przeglądarki internetowe:

- Google Chrome 29 lub nowsza
- Mozilla Firefox 23 lub nowsza
- Opera 16 lub nowsza
- Microsoft Edge 25 lub nowsza
- Safari 8 lub nowsza w systemach operacyjnych macOS oraz iOS

W innych przeglądarkach internetowych (oraz w programie Safari działającym w innych systemach operacyjnych) interfejs użytkownika może być wyświetlany niepoprawnie lub niektóre funkcje mogą być niedostępne.

## Aktywacja konta administratora

Po podpisaniu umowy partnerskiej otrzymasz wiadomość e-mail zawierającą następujące informacje:

- **Nazwa logowania.** Nazwa użytkownika, której używasz do logowania się. Nazwa logowania jest też widoczna na stronie aktywacji konta.
- Przycisk **Aktywuj konto**. Kliknij ten przycisk i ustaw hasło do konta. Hasło musi się składać z co najmniej dziewięciu znaków. Dodatkowe informacje na temat hasła można znaleźć w sekcji "Wymagania dotyczące hasła" (s. 27).

### Wymagania dotyczące hasła

Hasło do konta użytkownika musi się składać z co najmniej 9 znaków. Hasła są też sprawdzane pod kątem złożoności i oceniane przy użyciu jednej z następujących kategorii:

- Słabe
- Średni
- Silne

Nie można zapisać słabego hasła, nawet jeśli składa się ono z 9 lub większej liczby znaków. Hasła, w których jest powtarzana nazwa użytkownika, nazwa logowania, adres e-mail użytkownika lub nazwa dzierżawcy, do którego przynależy konto użytkownika, są zawsze uważane za słabe. Za słabe też uznaje się najpopularniejsze hasła.

Aby zwiększyć siłę hasła, należy dodać do niego kolejne znaki. Stosowanie różnych rodzajów znaków, na przykład cyfr, małych i wielkich liter oraz znaków specjalnych, nie jest konieczne, ale pozwala uzyskać większą siłę hasła przy mniejszej liczbie znaków.

# Dostęp do portalu zarządzania

1. Przejdź do strony logowania do usługi.
   Adres strony logowania znajduje się w otrzymanej przez Ciebie aktywacyjnej wiadomości e-mail.
2. Wpisz nazwę logowania i kliknij **Dalej**.
3. Wpisz hasło i kliknij **Dalej**.

   **Uwaga**
   Aby chronić platformę Cyber Protect Cloud przed atakami brute force, portal blokuje dostęp po 10 nieudanych próbach zalogowania się. Blokada pozostanie aktywna przez 5 minut. Liczba nieudanych prób logowania zostanie zresetowana po 15 minutach.

4. Do poruszania się po portalu zarządzania służy menu dostępne po prawej stronie.

Limit czasu w portalu zarządzania wynosi 24 godziny w przypadku sesji aktywnych i 1 godzinę w przypadku sesji nieaktywnych.

Niektóre usługi oferują możliwość przechodzenia z konsoli usługi do portalu zarządzania.

# Konfigurowanie kontaktów w Kreatorze profilu firmy

Możesz skonfigurować informacje o osobach do spraw kontaktów z firmą. Do wskazanych osób będziemy wysyłać aktualne informacje o nowych funkcjach i innych ważnych zmianach na platformie.

Kiedy po raz pierwszy zalogujesz się do portalu zarządzania, Kreator profilu firmy przeprowadzi Cię przez procedurę podania podstawowych informacji o firmie oraz kontaktach.

Można utworzyć kontakty na podstawie użytkowników już istniejących na platformie Cyber Protect lub dodać informacje kontaktowe osób, które nie mają dostępu do tej usługi.

***Aby skonfigurować kontakty w firmie w Kreatorze profilu firmy***

1. W sekcji **Informacje o firmie** podaj następujące dane swojej firmy:
   - **Oficjalna (prawna) nazwa firmy**
   - **Adres prawny firmy (adres centrali)**
     - **Kraj**
     - **Kod pocztowy**
2. Kliknij **Dalej**.
3. W sekcji **Osoby kontaktowe w firmie** skonfiguruj kontakty do następujących celów:

- **Kontakt w sprawie rozliczeń** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
- **Kontakt biznesowy** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.
- **Kontakt w sprawach technicznych** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.

Dany kontakt może być przeznaczony do więcej niż jednego celu.

Wybierz opcję, aby utworzyć kontakt.

- **Utwórz na podstawie już istniejącego użytkownika**. Wybierz użytkownika z listy rozwijanej.
- **Utwórz nowy kontakt**. Podaj następujące informacje kontaktowe:
  - **Imię** — imię osoby do kontaktów. To pole jest wymagane.
  - **Nazwisko** — nazwisko osoby do kontaktów. To pole jest wymagane.
  - **Służbowy adres e-mail** — adres e-mail osoby do kontaktów. To pole jest wymagane.
  - **Telefon służbowy** — to pole jest opcjonalne.
  - **Stanowisko** — to pole jest opcjonalne.

4. Jeśli kontakt w sprawie rozliczeń ma też służyć jako kontakt biznesowy lub kontakt w sprawach technicznych, zaznacz odpowiednie flagi w sekcji **Kontakt w sprawie rozliczeń**:
   - **Używaj tego samego kontaktu w sprawach biznesowych**
   - **Używaj tego samego kontaktu w sprawach technicznych**
5. Kliknij **Gotowe**.

   W wyniku tych działań zostaną utworzone kontakty. Można edytować podane informacje i skonfigurować inne kontakty w sekcji **Zarządzanie firmą > Profil firmy** konsoli zarządzania zgodnie z opisem podanym w sekcji Konfigurowanie kontaktów w firmie.

# Uzyskiwanie dostępu do konsoli Cyber Protection z portalu zarządzania

1. W portalu zarządzania wybierz **Monitorowanie** > **Wykorzystanie**.
2. W obszarze **Cyber Protect** wybierz **Ochrona**, a następnie kliknij **Zarządzaj usługą**.

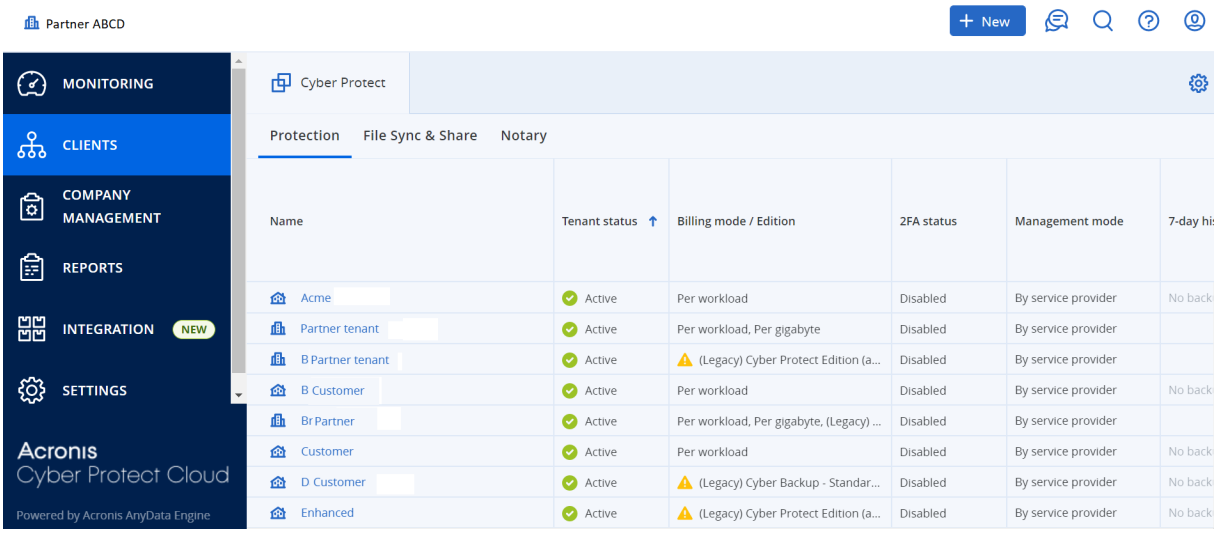
   Możesz też wybrać klienta w obszarze **Klienci**, a następnie kliknąć **Zarządzaj usługą**.

W wyniku tego nastąpi przekierowanie do konsoli Cyber Protection.

# Nawigacja po portalu zarządzania

Korzystając z portalu zarządzania, cały czas działasz w ramach jakiegoś dzierżawcy. Nazwa dzierżawcy jest widoczna w lewym górnym rogu ekranu.

Domyślnie jest wybrany najwyższy dostępny dla Ciebie poziom w hierarchii. Aby przejść na niższy poziom hierarchii, kliknij nazwę dzierżawcy na liście. Aby wrócić na najwyższy poziom, kliknij jego nazwę w lewym górnym rogu.




Wszystkie elementy interfejsu użytkownika wyświetlają tylko dane dotyczące dzierżawcy, w ramach którego aktualnie działasz, i tylko na niego mają wpływ. Na przykład:

- Na karcie **Klienci** są wyświetlani tylko ci dzierżawcy będącymi bezpośrednimi elementami podrzędnymi dzierżawcy, w ramach którego aktualnie działasz.
- Na karcie **Zarządzanie firmą** wyświetlane są tylko te profile firm i konta użytkowników, które znajdują się w obszarze dzierżawcy, w ramach którego aktualnie podejmujesz działania.
- Za pomocą przycisku **Nowe** możesz utworzyć dzierżawcę lub nowe konto użytkownika tylko w obszarze dzierżawcy, w ramach którego aktualnie działasz.

# Ograniczanie dostępu do interfejsu internetowego

Administratorzy mogą ograniczyć dostęp do interfejsu internetowego, określając listę adresów IP, z których mogą się logować członkowie dzierżawcy.

To ograniczenie dotyczy również dostępu do portalu zarządzania za pośrednictwem interfejsu API.

Ograniczenie to dotyczy tylko poziomu, na którym zostało ustawione. *Nie* jest ono stosowane w przypadku członków dzierżawców podrzędnych.

***Aby ograniczyć dostęp do interfejsu internetowego***

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz ograniczyć dostęp.
3. Kliknij **Ustawienia** > **Zabezpieczenia**.
4. Włącz przełącznik **Kontrola logowania**.
5. W polu **Dozwolone adresy IP** określ dozwolone adresy IP.

Możesz wprowadzić dowolne z poniższych parametrów, oddzielając je średnikiem:

- Adresy IP, na przykład: 192.0.2.0
- Zakresy adresów IP, na przykład: 192.0.2.0–192.0.2.255
- Podsieci, na przykład: 192.0.2.0/24

6. Kliknij **Zapisz**.

---

**Uwaga**
Dotyczy usługodawców, którzy korzystają z rozwiązania Cyber Infrastructure (modelu hybrydowego):

Jeśli zostanie włączony przełącznik **Kontrola logowania** w obszarze **Ustawienia** > **Zabezpieczenia** portalu zarządzania, dodaj zewnętrzne publiczne adresy IP węzłów Cyber Infrastructure do listy **Dozwolone adresy IP**.

---

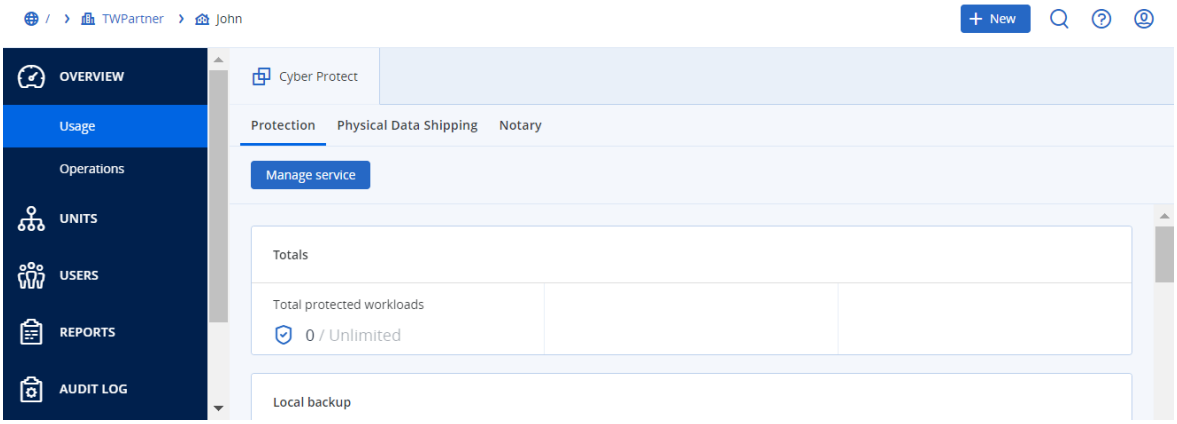
# Dostęp do usług

## Karta Omówienie

Sekcja **Przegląd** > **Wykorzystanie** udostępnia zestawienie informacji o wykorzystaniu usług oraz umożliwia uzyskanie dostępu do usług w obszarze dzierżawcy, w ramach którego działasz.

***Aby zarządzać usługą dla dzierżawcy za pomocą karty Omówienie***

1. Przejdź do dzierżawcy, w którego przypadku chcesz zarządzać usługą, i kliknij **Przegląd** > **Wykorzystanie**.
   Warto zauważyć, że niektórymi usługami można zarządzać na poziomie dzierżawcy-partnera i dzierżawcy-klienta, a innymi — tylko na poziomie dzierżawcy-klienta.
2. Kliknij nazwę usługi, którą chcesz zarządzać, a następnie kliknij **Zarządzaj usługą** lub **Konfiguruj usługę**.
   Więcej informacji na temat korzystania z usług można znaleźć w podręcznikach użytkownika dostępnych w konsolach usług.

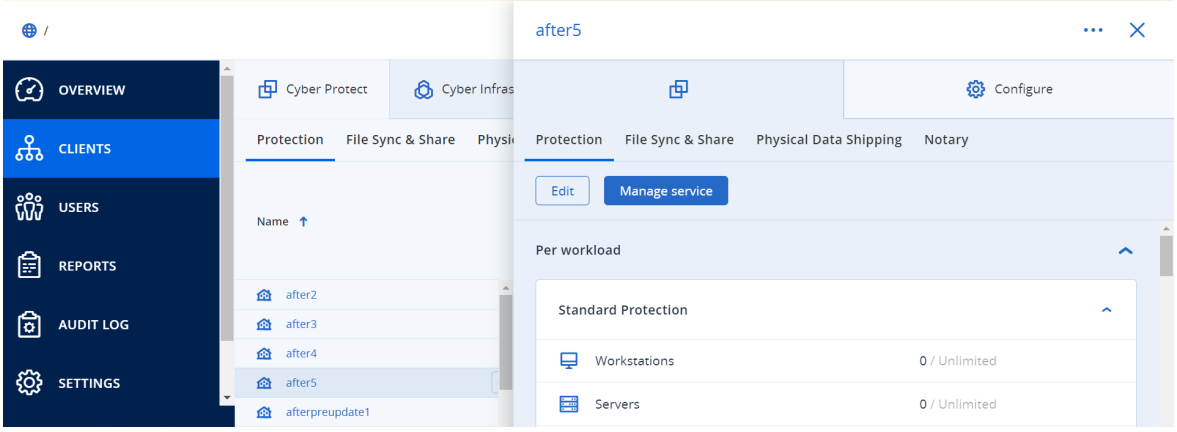


# Karta Klienci

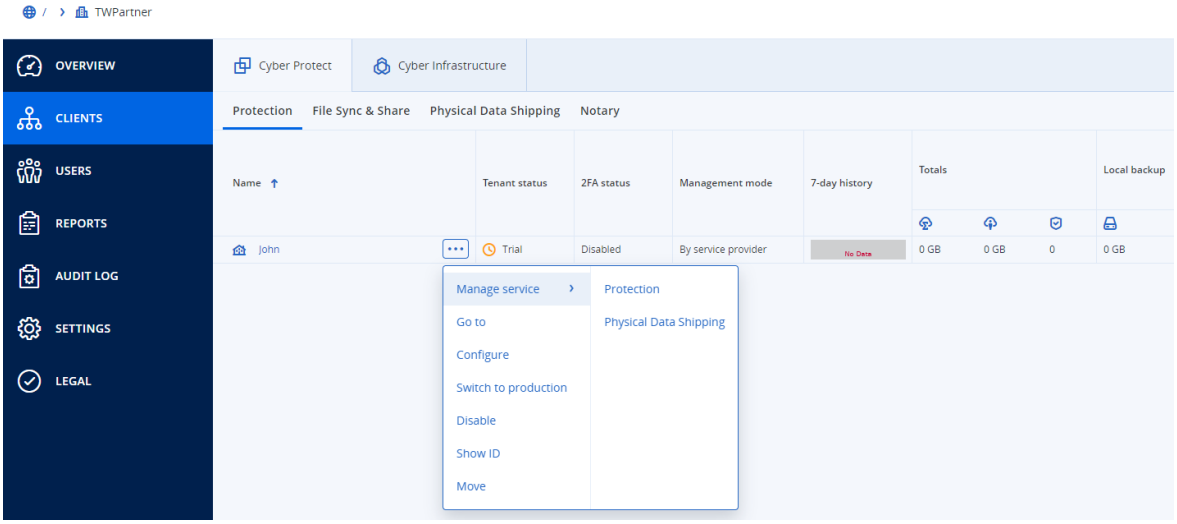
Karta **Klienci** udostępnia listę dzierżawców podrzędnych dzierżawcy, w ramach którego działasz, oraz umożliwia dostęp do usług w obszarach tych dzierżawców.

***Aby zarządzać usługą dla dzierżawcy za pomocą karty Klienci***

1. Wykonaj jedną z następujących czynności:
   - Kliknij **Klienci**, wybierz dzierżawcę, którego usługą chcesz zarządzać, kliknij nazwę lub ikonę usługi, którą chcesz zarządzać, a następnie kliknij **Zarządzaj usługą** lub **Konfiguruj usługę**.




   - Kliknij **Klienci**, następnie kliknij ikonę wielokropka obok nazwy dzierżawcy, którego usługą chcesz zarządzać, kliknij **Zarządzaj usługą**, a następnie wybierz usługę, którą chcesz zarządzać.




Warto zauważyć, że niektórymi usługami można zarządzać na poziomie dzierżawcy-partnera i dzierżawcy-klienta, a innymi — tylko na poziomie dzierżawcy-klienta.

Więcej informacji na temat korzystania z usług można znaleźć w podręcznikach użytkownika dostępnych w konsolach usług.

# Pasek Historia 7-dniowa

Dostępny na ekranie **Klienci** pasek **Historia 7-dniowa** odzwierciedla status kopii zapasowych obciążeń każdego dzierżawcy-klienta z ostatnich 7 dni. Pasek jest podzielony na 168 kolorowych linii. Każda linia reprezentuje przedział jednogodzinny i najgorszy stan kopii zapasowej w danym jednogodzinnym zakresie czasu.

Poniższa tabela zawiera informacje na temat znaczeń poszczególnych kolorów linii.

| Kolor | Opis |
|---|---|
| czerwony | co najmniej jedna operacja tworzenia kopii zapasowej w ciągu danej godziny zakończyła się niepowodzeniem |
| pomarańczowy | co najmniej jedna operacja tworzenia kopii zapasowej w ciągu danej godziny została ukończona z ostrzeżeniem, ale bez błędów |
| zielony | co najmniej jedna operacja tworzenia kopii zapasowej w ciągu danej godziny została ukończona pomyślnie — bez błędów i ostrzeżeń |
| szary | w ciągu danej godziny nie ukończono żadnej operacji tworzenia kopii zapasowej |

Dopóki nie zostaną zebrane odpowiednie dane statystyczne, na pasku **Historia 7-dniowa** jest wyświetlany komunikat „Brak kopii zapasowych”.

W przypadku dzierżawców-partnerów pasek **Historia 7-dniowa** jest pusty, ponieważ statystyki zagregowane nie są obsługiwane.

# Konta użytkowników oraz dzierżawcy

Dostępne są dwa rodzaje kont użytkowników: konta administratorów oraz konta użytkowników.

- **Administratorzy** mają dostęp do portalu zarządzania. Mają rolę administratora we wszystkich usługach.
- **Użytkownicy** nie mają dostępu do portalu zarządzania. Ich dostęp do usług oraz role są określane przez administratora.

Każde konto należy do jakiegoś dzierżawcy. Dzierżawca jest częścią zasobów portalu zarządzania (takich jak konta użytkowników i dzierżawcy podrzędni) oraz ofert usług (włączone usługi i pozycje ofert w ich obszarach) przeznaczonych dla partnera lub klienta. Hierarchia dzierżawców powinna odzwierciedlać relacje klient/dostawca między użytkownikami a dostawcami usługi.

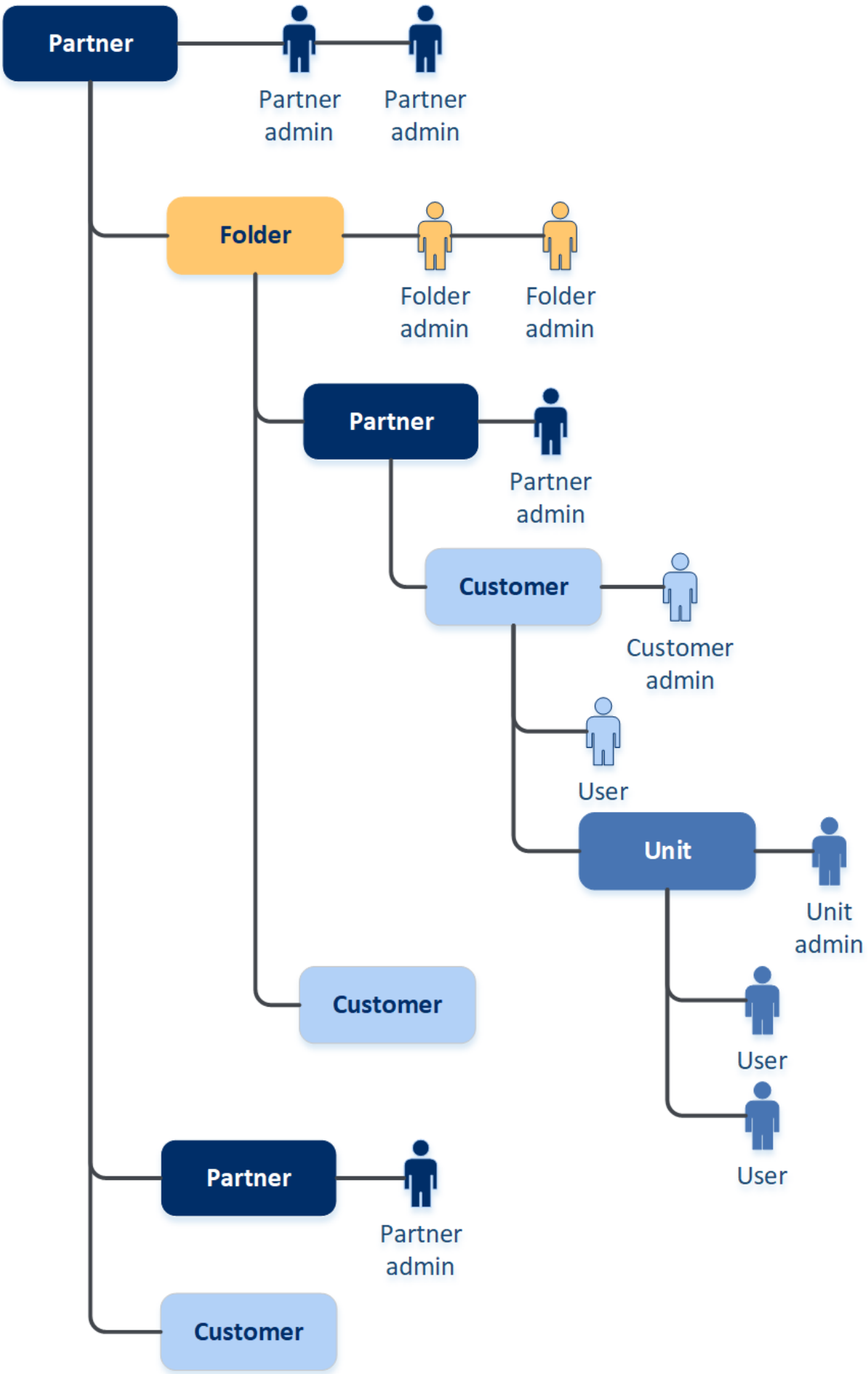
- Dzierżawca typu **Partner** zwykle odpowiada usługodawcy odsprzedającemu usługi.
- Dzierżawca typu **Folder** jest dzierżawcą pomocniczym, używanym zwykle przez administratorów partnerów do pogrupowania partnerów i klientów w celu skonfigurowania osobnych pozycji ofert i/lub innego oznaczenia marką.
- Dzierżawca typu **Klient** zwykle odpowiada organizacjom korzystającym z usług.

- Dzierżawca typu **Jednostka** zwykle odpowiada jednostkom organizacyjnym lub działom organizacji.

Administrator może tworzyć dzierżawców, konta administratorów i konta użytkowników oraz zarządzać nimi na własnym lub niższym poziomie hierarchii.

Administrator dzierżawcy nadrzędnego typu **Partner** może pełnić rolę administratora niższego poziomu w odniesieniu do dzierżawców typu **Klient** lub **Partner**, którzy korzystają z trybu zarządzania **Zarządzane przez dostawcę usługi**. W ten sposób administrator na poziomie partnera może na przykład zarządzać kontami i usługami użytkowników lub uzyskiwać dostęp do kopii zapasowych i innych zasobów w obszarze dzierżawcy podrzędnego. Administratorzy niższego poziomu mogą jednak ograniczać dostęp administratorów wyższego poziomu do swojego dzierżawcy.

Poniższy diagram przedstawia przykładową hierarchię dzierżawców typu partner, folder, klient oraz jednostka.


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

Poniższa tabela zawiera zestawienie operacji, które mogą wykonywać administratorzy oraz użytkownicy.

| Operacja | Użytkownicy | Administratorzy klientów i jednostek | Administratorzy partnerów i folderów |
|---|---|---|---|
| Tworzenie dzierżawców | Nie | Tak | Tak |
| Tworzenie kont | Nie | Tak | Tak |
| Pobieranie i instalacja oprogramowania | Tak | Tak | Nie* |
| Zarządzaj usługami | Tak | Tak | Tak |
| Tworzenie raportów dotyczących użytkowania usługi | Nie | Tak | Tak |
| Konfiguracja oznaczenia marką | Nie | Nie | Tak |

* Administrator partnera, który musi wykonać te operacje, może sobie utworzyć konto administratora klienta lub użytkownika.

# Zarządzanie dzierżawcami

W ramach oprogramowania Cyber Protect są dostępni następujący dzierżawcy:

- Dzierżawcę typu **Partner** zwykle tworzy się w przypadku każdego partnera, który podpisał umowę partnerską.
- Dzierżawcę typu **Folder** zwykle tworzy się w celu pogrupowania partnerów i klientów w celu skonfigurowania osobnych pozycji ofert i/lub innego oznaczenia marką.
- Dzierżawcę typu **Klient** zwykle tworzy się w przypadku każdej organizacji zarejestrowanej w celu uzyskania dostępu do usługi.
- W ramach dzierżawcy-klienta zostanie utworzony dzierżawca typu **Jednostka** w celu rozszerzenia usługi na nową jednostkę organizacyjną.

Kroki wykonywane w celu utworzenia i skonfigurowania dzierżawcy różnią się w zależności od tworzonego dzierżawcy, ale ogólna instrukcja wygląda następująca:

1. Utwórz dzierżawcę.
2. Wybierz usługi dla dzierżawcy.
3. Skonfiguruj pozycje oferty dla dzierżawcy.

## Tworzenie dzierżawcy

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w ramach którego chcesz utworzyć dzierżawcę.

3. W prawym górnym rogu kliknij **Nowe**, a następnie kliknij jedną z następujących opcji, w zależności od tego, jakiego typu dzierżawcę chcesz utworzyć:
   - Dzierżawcę typu **Partner** zwykle tworzy się w przypadku każdego partnera, który podpisał umowę partnerską.
   - Dzierżawcę typu **Folder** zwykle tworzy się w celu pogrupowania partnerów i klientów w celu skonfigurowania osobnych pozycji ofert i/lub innego oznaczenia marką.
   - Dzierżawcę typu **Klient** zwykle tworzy się w przypadku każdej organizacji zarejestrowanej w celu uzyskania dostępu do usługi.
   - W ramach dzierżawcy-klienta zostanie utworzony dzierżawca typu **Jednostka** w celu rozszerzenia usługi na nową jednostkę organizacyjną.
4. W polu **Nazwa** określ nazwę nowego dzierżawcy.
5. [Tylko w przypadku tworzenia dzierżawcy-partnera] Wprowadź wartość w polach **Oficjalna (prawna) nazwa firmy** (wartość wymagana) i **Numer VAT / numer identyfikacji podatkowej / numer rejestracyjny firmy** (wartość opcjonalna).
6. [Tylko w przypadku tworzenia dzierżawcy-klienta] W polu **Tryb** wskaż, czy dzierżawca korzysta z usług w trybie próbnym, czy w trybie produkcyjnym. Miesięczne raporty dotyczące wykorzystania usług nie obejmują danych wykorzystania dotyczących dzierżawców pracujących w trybie próbnym.

   **Ważne**
   W przypadku przejścia z trybu próbnego na tryb produkcyjny w trakcie miesiąca w miesięcznym raporcie znajdą się dane dotyczące użytkowania usługi z całego miesiąca. Dlatego tryb najlepiej jest zmieniać w pierwszym dniu miesiąca. Jeśli dzierżawca pozostanie w trybie próbnym przez cały miesiąc, tryb zostanie automatycznie zmieniony na produkcyjny.

   Możliwe są dwa scenariusze automatycznego zmieniania trybu próbnego dzierżawcy na tryb produkcyjny:
   - W trakcie miesiąca, w którym to przypadku w miesięcznym raporcie dotyczących wykorzystania usługi zostanie uwzględniony również cały ***następny*** miesiąc.
   - [Opcja zalecana] Pierwszego dnia miesiąca — wówczas pod uwagę zostanie wzięty tylko bieżący miesiąc.

7. W sekcji **Tryb zarządzania** wybierz jeden z poniższych trybów zarządzania dostępem do dzierżawcy:
   - **Samoobsługa** — ten tryb ogranicza dostęp administratorów dzierżawcy nadrzędnego do tego dzierżawcy tak, że mogą oni jedynie modyfikować właściwości dzierżawcy, ale nie mają dostępu do żadnych zasobów w jego obszarze (np. dzierżawców, użytkowników, usług, kopii zapasowych i innych) i nie mogą nimi zarządzać.
   - **Zarządzane przez dostawcę usługi** — w tym trybie administratorzy dzierżawcy nadrzędnego mają pełny dostęp do dzierżawcy i mogą modyfikować właściwości, zarządzać dzierżawcami, użytkownikami i usługami oraz uzyskiwać dostęp do kopii zapasowych i innych zasobów.

   W przypadku ustawienia trybu **Samoobsługa** tryb zarządzania będzie mógł zmienić tylko administrator utworzonego przez Ciebie dzierżawcy. W tym celu administrator tworzonego

dzierżawcy może przejść do sekcji **Ustawienia** > **Zabezpieczenia** i skonfigurować przełącznik **Dostęp do pomocy technicznej**.

Tryb zarządzania wybrany dla dzierżawców podrzędnych można sprawdzić na karcie **Klienci**.

8. W sekcji **Bezpieczeństwo** włącz lub wyłącz uwierzytelnianie dwuskładnikowe dla dzierżawcy. W przypadku włączenia tej funkcji każdy użytkownik w ramach tego dzierżawcy będzie musiał skonfigurować uwierzytelnianie dwuskładnikowe na swoim koncie, aby wzmocnić zabezpieczenia dostępu. Użytkownicy muszą zainstalować aplikację uwierzytelniającą na swoich urządzeniach używanych do obsługi drugiego składnika uwierzytelniania i w celu zalogowania się do konsoli podać — oprócz tradycyjnej nazwy logowania i hasła — wygenerowany jednorazowy kod TOTP. Więcej informacji można znaleźć w sekcji „Konfigurowanie uwierzytelniania dwuskładnikowego". Aby wyświetlić statusy uwierzytelniania dwuskładnikowego swoich klientów, przejdź do sekcji **Klienci**.
9. [Tylko w przypadku tworzenia dzierżawcy-klienta w trybie Rozszerzone zabezpieczenia] W polu **Zabezpieczenia** zaznacz pole wyboru **Tryb Rozszerzone zabezpieczenia**.

   W tym trybie dozwolone są tylko szyfrowane kopie zapasowe. Na chronionym urządzeniu musi być ustawione hasło szyfrowania — bez tego operacja tworzenia kopii zapasowej się nie powiedzie. Wszystkie operacje wymagające podania hasła szyfrowania do usługi chmurowej są w tym trybie niedostępne. Więcej informacji można znaleźć w sekcji "Tryb Rozszerzone zabezpieczenia" (s. 39).

   **Ważne**
   Po utworzeniu dzierżawcy nie można wyłączyć trybu Rozszerzone zabezpieczenia.

10. W sekcji **Utwórz administratora** skonfiguruj konto administratora.

    **Uwaga**
    W przypadku dzierżawcy-klienta oraz dzierżawcy-partnera, który ma ustawiony **Tryb zarządzania** jako **Samoobsługa**, utworzenie administratora jest wymagane.

    a. Wprowadź nazwę logowania i adres e-mail konta administratora. Pozostałe pola są opcjonalne, ale zapewniają więcej kanałów komunikacji na wypadek, gdybyśmy musieli skontaktować się z administratorem.
    b. Wybierz język.
       Jeśli nie wybierzesz języka, domyślnie będzie używany język angielski.
    c. Określ kontakty w firmie.
       - **Rozliczenia** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
       - **Techniczne** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.
       - **Biznesowe** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.

         Użytkownikowi można przypisać więcej niż jeden typ kontaktu w firmie.

11. W polu **Język** zmień domyślny język powiadomień, raportów i oprogramowania, który będzie używany w przypadku danego dzierżawcy.
12. Wykonaj jedną z następujących czynności:
    - Aby ukończyć tworzenie dzierżawcy, kliknij **Zapisz i zamknij**. W takim przypadku wszystkie usługi zostaną włączone dla dzierżawcy. Zostanie ustawiony tryb rozliczeń usługi Ochrona „Za obciążenie”.
    - Kliknij **Dalej**, aby wybrać usługi dla dzierżawcy. Zobacz "Wybieranie usług dla dzierżawcy" (s. 40).

## Tryb Rozszerzone zabezpieczenia

Tryb Rozszerzone zabezpieczenia udostępnia specjalne ustawienia dla klientów, którzy mają większe wymagania w zakresie bezpieczeństwa. Ten tryb wymaga szyfrowania wszystkich kopii zapasowych i zezwala tylko na lokalnie ustawione hasła szyfrowania.

Administrator partnera może włączyć tryb Rozszerzone zabezpieczenia tylko podczas tworzenia nowego klienta i nie może go później wyłączyć. W przypadku już istniejących dzierżawców nie można włączyć trybu Rozszerzone zabezpieczenia.

W trybie Rozszerzone zabezpieczenia wszystkie kopie zapasowe utworzone w ramach dzierżawcy-klienta i jego jednostek są automatycznie szyfrowane algorytmem AES z kluczem 256-bitowym. Użytkownicy mogą ustawiać hasła szyfrowania tylko na chronionych urządzeniach — nie mogą ich ustawiać w planach ochrony.

Usługi chmurowe nie mają dostępu do haseł szyfrowania. Ze względu na te ograniczenia dzierżawcy w trybie Rozszerzone zabezpieczenia nie mają dostępu do następujących funkcji:

- Odzyskiwanie przy użyciu konsoli usługi
- Przeglądanie kopii zapasowych na poziomie plików przy użyciu konsoli usługi
- Kopia zapasowa z chmury do chmury
- Kopia zapasowa witryny internetowej
- Kopia zapasowa aplikacji
- Kopia zapasowa urządzeń mobilnych
- Skanowanie antywirusowe kopii zapasowych
- Bezpieczne odzyskiwanie
- Automatyczne tworzenie firmowych białych list
- Mapa ochrony danych
- Odzyskiwanie po awarii
- Raporty i pulpity nawigacyjne związane z niedostępnymi funkcjami

## Ograniczenia

- Tryb Rozszerzone zabezpieczenia jest kompatybilny tylko z agentami w wersji 15.0.26390 lub nowszej.
- Tryb Rozszerzone zabezpieczenia nie jest dostępny w przypadku urządzeń z systemami Red Hat Enterprise Linux 4.x i 5.x oraz ich pochodnymi.

# Wybieranie usług dla dzierżawcy

Po utworzeniu nowego dzierżawcy domyślnie są włączone wszystkie usługi. Możesz wybrać usługi, które mają być dostępne dla użytkowników w ramach dzierżawcy i jego dzierżawców podrzędnych.

Możesz też wybrać i włączyć usługi dla wielu dzierżawców naraz. Aby uzyskać więcej informacji, zobacz "Włączanie usług dla wielu dzierżawców" (s. 41).

Procedura ta nie dotyczy dzierżawcy-jednostki.

***Aby wybrać usługi dla dzierżawcy***

1. W sekcji **Wybierz usługi** okna dialogowego tworzenia/edycji dzierżawcy wybierz tryb rozliczeń lub wersję.
   - Wybierz tryb rozliczeń **Za obciążenie** lub **Za gigabajt** i wyczyść pola wyboru odpowiadające usługom, które chcesz wyłączyć dla dzierżawcy.
     W obu trybach rozliczeń jest dostępny ten sam zestaw usług.

     Jeśli korzystasz z pakietu Zaawansowane odzyskiwanie po awarii i masz zarejestrowaną własną lokalizację odzyskiwania po awarii w ramach swojego konta, możesz wybrać tę lokalizację na potrzeby odzyskiwania po awarii z listy rozwijanej.
   - Aby skorzystać ze starszej wersji, zaznacz przycisk radiowy **Starsze wersje** i wybierz wersję z listy rozwijanej.

   Wyłączone usługi zostaną ukryte przed użytkownikami w obszarach tego dzierżawcy i jego dzierżawców podrzędnych.
2. Wykonaj jedną z następujących czynności:
   - Aby ukończyć tworzenie dzierżawcy, kliknij **Zapisz i zamknij**. W takim przypadku wszystkie pozycje oferty wybranych usług zostaną włączone dla dzierżawcy z nieograniczonym limitem.
   - Kliknij **Dalej**, aby skonfigurować pozycje oferty dla dzierżawcy. Zobacz "Konfigurowanie pozycji oferty dla dzierżawcy" (s. 40).

# Konfigurowanie pozycji oferty dla dzierżawcy

Gdy utworzysz nowego dzierżawcę, zostaną włączone wszystkie pozycje oferty dla wybranych usług. Możesz wybrać pozycje oferty, które mają być dostępne dla użytkowników w ramach dzierżawcy i jego dzierżawców podrzędnych, a także ustawić ich limity.

Procedura ta nie dotyczy dzierżawcy-jednostki.

***Aby skonfigurować pozycje oferty dla dzierżawcy***

1. W sekcji **Konfiguruj usługi** okna dialogowego tworzenia/edytowania dzierżawcy wyczyść pola wyboru pozycji oferty, które chcesz wyłączyć.
   Funkcje odpowiadające wyłączonym pozycjom oferty będą niedostępne dla użytkowników w obszarach tego dzierżawcy i jego dzierżawców podrzędnych.

   **Uwaga**
   Możesz wyłączyć pozycje oferty związane z funkcjami ochrony zaawansowanej, ale zostaną one automatycznie ponownie włączone, jeśli użytkownik włączy funkcję zaawansowaną w planie ochrony.

2. W przypadku niektórych usług można wybrać magazyny, które będą dostępne dla nowego dzierżawcy. Magazyny są pogrupowane według lokalizacji. Możesz wybrać z listy lokalizacji i magazynów dostępnych dla dzierżawcy.
   - W przypadku tworzenia dzierżawcy-partnera/folderu można wybrać wiele lokalizacji i magazynów dla każdej usługi.
   - W przypadku tworzenia dzierżawcy-klienta trzeba wybrać jedną lokalizację, a następnie jeden magazyn na usługę w obrębie tej lokalizacji. Przypisane klientowi magazyny można później zmienić, ale tylko pod warunkiem, że poziom ich wykorzystania wynosi 0 GB — czyli albo zanim klient zacznie z nich korzystać z magazynu, albo po usunięciu z nich wszystkich kopii zapasowych. Informacje na temat wykorzystania miejsca w magazynie nie są aktualizowane w czasie rzeczywistym. Ich aktualizacja może potrwać do 24 godzin.

   Szczegółowe informacje na temat magazynów można znaleźć w sekcji „Zarządzanie lokalizacjami i magazynami”.
3. Aby określić limit pozycji oferty, kliknij widoczny obok niej link **Bez ograniczeń**.
   Limity są elastyczne. Jeśli którakolwiek z tych wartości zostanie przekroczona, do administratorów dzierżawcy i administratorów dzierżawcy nadrzędnego zostanie wysłane stosowne powiadomienie e-mail. Ograniczenia dotyczące korzystania z usług nie są stosowane. W przypadku dzierżawcy-partnera zakłada się, że poziom wykorzystania pozycji oferty może przekroczyć limit, ponieważ podczas tworzenia dzierżawcy-partnera nie można ustawić nadwyżki.
4. [Tylko w przypadku tworzenia dzierżawcy-klienta] Określ nadwyżki limitów.
   Nadwyżka umożliwia dzierżawcy-klientowi przekroczenie limitu o określoną wartość. W przypadku przekroczenia nadwyżki zostaną zastosowane ograniczenia dotyczące korzystania z danej usługi.
5. Kliknij **Zapisz i zamknij**.

Nowo utworzony dzierżawca pojawi się na karcie **Klienci** w konsoli zarządzania.

Jeśli zechcesz edytować ustawienia dzierżawcy lub zmienić administratora, zaznacz tego dzierżawcę na karcie **Klienci**, a następnie kliknij ikonę ołówka w sekcji, którą chcesz edytować.

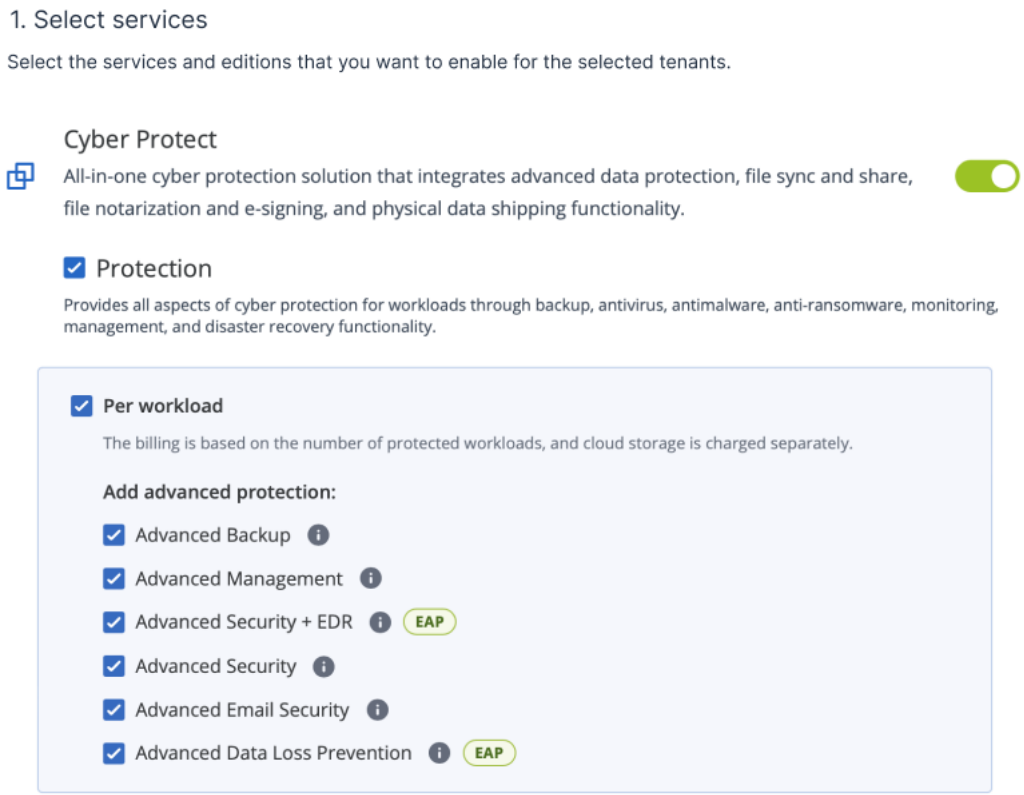
## Włączanie usług dla wielu dzierżawców

Usługi, wersje, pakiety i pozycje oferty można włączać zbiorczo dla wielu dzierżawców (maksymalnie 100 w jednej sesji).

Procedura ta dotyczy grup podrzędnych w grupie głównej, partnerów, folderów i dzierżawców-klientów. Można wybrać jednocześnie dzierżawców dowolnego z tych różnych typów.

***Aby włączyć usługi dla wielu dzierżawców***

1. W portalu zarządzania wybierz **Klienci**.
2. Kliknij **Konfiguruj usługi** w prawym górnym rogu.
3. Zaznacz pola wyboru obok nazw dzierżawców, dla których chcesz włączyć usługi, a następnie kliknij **Dalej**.
4. W sekcji **Wybierz usługi** wybierz odpowiednie usługi, które chcesz zastosować do wszystkich wybranych dzierżawców, a następnie kliknij **Dalej**.

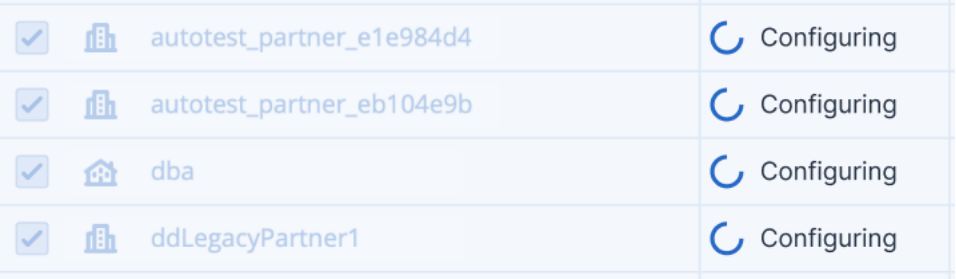



**Uwaga**
Na tym ekranie nie można wyłączyć wcześniej włączonej usługi. Wszystkie usługi, wersje i pozycje oferty wybrane przed rozpoczęciem tej procedury pozostaną włączone.

5. W sekcji **Konfiguruj usługi** wybierz funkcje i pozycje oferty usługi, które chcesz włączyć dla wybranych dzierżawców, a następnie kliknij **Dalej**.
6. W sekcji **Podsumowanie** przejrzyj zmiany, które zostaną zastosowane do wybranych dzierżawców.

   Możesz kliknąć **Rozwiń wszystko**, aby zobaczyć wszystkie wybrane usługi i pozycje oferty dzierżawców, które zostaną zastosowane. Możesz też rozwinąć obszar każdego dzierżawcy, aby zobaczyć wybrane usługi i pozycje oferty dotyczące tego dzierżawcy.

7. Kliknij **Zastosuj zmiany**. W czasie konfigurowania usług dla poszczególnych dzierżawców dany dzierżawca jest wyłączony, a wartość w kolumnie **Status dzierżawcy** wskazuje, że usługi i pozycje oferty są właśnie konfigurowane, jak pokazano na poniższej ilustracji.




8. Po pomyślnym zastosowaniu konfiguracji usług i pozycji oferty do wybranych dzierżawców zostanie wyświetlony komunikat z potwierdzeniem.

   Jeśli z jakiegoś powodu nie uda się zastosować usług i pozycji oferty do dzierżawcy, w kolumnie **Status dzierżawcy** będzie wyświetlana wartość **Niezastosowane**. Kliknij **Spróbuj ponownie**, aby przejrzeć konfigurację w przypadku wybranych dzierżawców.

## Włączanie powiadomień o konserwacji

Jako użytkownik partnera możesz zezwolić dzierżawcom podrzędnym (partnerom i klientom) na odbieranie wiadomości e-mail z powiadomieniami o konserwacji bezpośrednio z centrum danych usługi Cyber Protect i odbierać w portalu zarządzania powiadomienia o konserwacji dostępne wewnątrz produktu. Pomoże to zmniejszyć liczbę przypadków kontaktowania się z pomocą techniczną w związku z konserwacją.

**Uwaga**
Wiadomości e-mail z powiadomieniami o konserwacji są oznaczone marką centrum danych. W przypadku tych powiadomień nie jest obsługiwane niestandardowe oznaczenie marką.

***Aby włączyć powiadomienia o konserwacji dla partnerów podrzędnych lub klientów***

1. Zaloguj się w portalu zarządzania jako użytkownik partnera, kliknij **Klienci**, a następnie kliknij nazwę dzierżawcy będącego partnerem lub klientem, dla którego chcesz włączyć powiadomienia o konserwacji.
2. Kliknij **Konfiguruj**.
3. Na karcie **Ustawienia ogólne** znajdź opcję **Powiadomienia o konserwacji** i ją włącz.
   Jeśli nie widzisz opcji **Powiadomienia o konserwacji**, skontaktuj się z usługodawcą.

**Uwaga**
Powiadomienia o konserwacji są włączone, ale nie będą wysyłane, dopóki wybrany dzierżawca nie włączy powiadomień dla swoich użytkowników lub nie włączy tej opcji dalej dla swoich partnerów podrzędnych lub klientów, aby udostępnić powiadomienia ich użytkownikom.

***Aby włączyć powiadomienia o konserwacji dla użytkownika***

1. Zaloguj się w portalu zarządzania jako użytkownik partnera lub administrator firmy.
   Jako partner masz dostęp do użytkowników wszystkich zarządzanych przez Ciebie dzierżawców.
2. Przejdź do obszaru **Zarządzanie firmą** > **Użytkownicy**, a następnie kliknij nazwę użytkownika, dla którego chcesz włączyć powiadomienia o konserwacji.
3. Na karcie **Usługi** w sekcji **Ustawienia** kliknij ołówek, aby edytować opcje.
4. Zaznacz pole wyboru **Powiadomienia o konserwacji** i kliknij **Gotowe**.

Wybrany użytkownik będzie otrzymywać powiadomienia e-mail o nadchodzących działaniach związanych z konserwacją w centrum danych.

## Konfigurowanie samodzielnie zarządzanego profilu klienta

Jako partner możesz skonfigurować samodzielnie zarządzane profile klientów dla zarządzanych przez Ciebie dzierżawców. Ta opcja pozwala sterować widocznością profilu dzierżawcy i informacji kontaktowych dla poszczególnych klientów.

***Aby skonfigurować samodzielnie zarządzany profil klienta***

1. W portalu zarządzania wybierz **Klienci**.
2. Wybierz klienta, dla którego chcesz skonfigurować samodzielnie zarządzany profil klienta.
3. Wybierz kartę **Konfiguruj**, a następnie kartę **Ustawienia ogólne**.
4. Włącz lub wyłącz przełącznik **Włącz samodzielnie zarządzany profil klienta**.

W przypadku włączenia samodzielnie zarządzanego profilu klienta klient będzie widział sekcję **Profil firmy** w menu nawigacyjnym oraz pola związane z osobami kontaktowymi w kreatorze tworzenia użytkowników (**telefon służbowy**, **osoba kontaktowa w firmie** i **stanowisko**).

W przypadku wyłączenia samodzielnie zarządzanego profilu klienta sekcja **Profil firmy** w menu nawigacyjnym oraz pola związane z osobami kontaktowymi w kreatorze tworzenia użytkowników będą ukryte.

## Konfigurowanie kontaktów w firmie

Jako partner możesz skonfigurować informacje kontaktowe dotyczące Twojej firmy oraz zarządzanych przez Ciebie dzierżawców. Do kontaktów z tej listy będziemy wysyłać aktualne informacje o nowych funkcjach i innych ważnych zmianach na platformie.

Można dodać wiele kontaktów i przypisać im typy kontaktów w firmie w zależności od roli użytkownika. Można utworzyć kontakty na podstawie użytkowników już istniejących na platformie Cyber Protect lub dodać informacje kontaktowe osób, które nie mają dostępu do tej usługi.

***Aby skonfigurować kontakty w przypadku firmy***

1. W konsoli zarządzania przejdź do sekcji **Zarządzanie firmą** > **Profil firmy**.
2. W sekcji **Kontakty** kliknij **+**.
3. Wybierz opcję, aby utworzyć kontakt.

- **Utwórz na podstawie już istniejącego użytkownika**
  - Wybierz użytkownika z listy rozwijanej.
  - Wybierz typ kontaktu w firmie.
    - **Rozliczenia** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
    - **Techniczne** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.
    - **Biznesowe** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.

      Użytkownikowi można przypisać więcej niż jeden typ kontaktu w firmie.

    W przypadku usunięcia kontaktu skojarzonego z użytkownikiem z listy kontaktów w profilu firmy użytkownik ten nie zostanie usunięty. System cofnie przypisanie do danego użytkownika wszystkich typów kontaktów w firmie, więc nie będą one już widoczne w kolumnie **Osoby kontaktowe w firmie** na liście **Użytkownicy**.

    Jeśli zechcesz zmienić adres e-mail kontaktu skojarzonego z użytkownikiem, system poprosi o weryfikację nowo zdefiniowanego adresu. Zostanie wysłana na ten adres wiadomość e-mail i użytkownik będzie musiał potwierdzić zmianę.
- **Utwórz nowy kontakt**
  - Podaj dane kontaktowe.
    - **Imię** — imię osoby do kontaktów. To pole jest wymagane.
    - **Nazwisko** — nazwisko osoby do kontaktów. To pole jest wymagane.
    - **Służbowy adres e-mail** — adres e-mail osoby do kontaktów. To pole jest wymagane.
    - **Telefon służbowy** — to pole jest opcjonalne.
    - **Stanowisko** — to pole jest opcjonalne.
  - Wybierz **Osoby kontaktowe w firmie**.
    - **Rozliczenia** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
    - **Techniczne** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.
    - **Biznesowe** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.

      Użytkownikowi można przypisać więcej niż jeden typ kontaktu w firmie.

4. Kliknij **Dodaj**.

***Aby skonfigurować kontakty w przypadku dzierżawcy***

**Uwaga**

Jeśli zmodyfikujesz informacje kontaktowe w przypadku dzierżawcy podrzędnego, zmiany te będą widoczne w ramach dzierżawcy.

1. W portalu zarządzania wybierz **Klienci**.
2. Kliknij dzierżawcę i kliknij **Konfiguruj**.
3. W sekcji **Kontakty** kliknij **+**.
4. Wybierz opcję, aby utworzyć kontakt.
   - **Utwórz na podstawie już istniejącego użytkownika**
     - Wybierz użytkownika z listy rozwijanej.
     - Wybierz typ kontaktu w firmie.
       - **Rozliczenia** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
       - **Techniczne** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.
       - **Biznesowe** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.

         Użytkownikowi można przypisać więcej niż jeden typ kontaktu w firmie.

     W przypadku usunięcia kontaktu skojarzonego z użytkownikiem z listy kontaktów w profilu firmy użytkownik ten nie zostanie usunięty. System cofnie przypisanie do danego użytkownika wszystkich typów kontaktów w firmie, więc nie będą one już widoczne w kolumnie **Osoby kontaktowe w firmie** na liście **Użytkownicy**.

     Jeśli zechcesz zmienić adres e-mail kontaktu skojarzonego z użytkownikiem, system poprosi o weryfikację nowo zdefiniowanego adresu. Zostanie wysłana na ten adres wiadomość e-mail i użytkownik będzie musiał potwierdzić zmianę.
   - **Utwórz nowy kontakt**
     - Podaj dane kontaktowe.
       - **Imię** — imię osoby do kontaktów. To pole jest wymagane.
       - **Nazwisko** — nazwisko osoby do kontaktów. To pole jest wymagane.
       - **Służbowy adres e-mail** — adres e-mail osoby do kontaktów. To pole jest wymagane.
       - **Telefon służbowy** — to pole jest opcjonalne.
       - **Stanowisko** — to pole jest opcjonalne.
     - Wybierz **Osoby kontaktowe w firmie**.
       - **Rozliczenia** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
       - **Techniczne** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.
       - **Biznesowe** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.

         Użytkownikowi można przypisać więcej niż jeden typ kontaktu w firmie.
5. Kliknij **Dodaj**.

## Odświeżanie danych o wykorzystaniu dotyczących dzierżawcy

Domyślnie dane o wykorzystaniu są odświeżane w stałych odstępach. Dane o wykorzystaniu dotyczące dzierżawcy można odświeżać ręcznie.

1. W konsoli zarządzania przejdź do sekcji **Klienci**.
2. Kliknij dzierżawcę, a następnie ikonę wielokropka w tym samym wierszu.
3. Wybierz **Odśwież dane o wykorzystaniu**.

   **Uwaga**
   Pobieranie danych może potrwać do 10 minut.

4. Odśwież stronę, aby wyświetlić zaktualizowane dane.

## Wyłączanie i włączanie dzierżawcy

Czasem może być konieczne tymczasowe wyłączenie dzierżawcy. Na przykład w sytuacji, gdy dzierżawca ma długi za korzystanie z usług.

***Aby wyłączyć dzierżawcę***

1. W portalu zarządzania wybierz **Klienci**.
2. Wybierz dzierżawcę, którego chcesz wyłączyć, a następnie kliknij ikonę wielokropka > **Wyłącz**.
3. Potwierdź czynność, klikając **Wyłącz**.

Wskutek tego:

- Dzierżawca oraz wszyscy jego poddzierżawcy zostaną wyłączeni, a ich usługi zostaną zatrzymane.
- Dzierżawca i jego poddzierżawcy nadal będą rozliczani, ponieważ ich dane zostaną zachowane na platformie Cyber Protect Cloud.
- Wszystkie klienty API w ramach dzierżawcy i jego poddzierżawców zostaną wyłączeni, a wszystkie integracje utworzone przy użyciu tych klientów przestaną działać.

Aby włączyć dzierżawcę, zaznacz go na liście klientów, a następnie kliknij ikonę wielokropka > **Włącz**.

## Przenoszenie dzierżawcy do innego dzierżawcy

Portal zarządzania umożliwia przeniesienie dzierżawcy od jednego dzierżawcy nadrzędnego do drugiego. Funkcja ta może się przydać na przykład wtedy, gdy zechcesz przenieść klienta od jednego partnera do drugiego lub gdy utworzysz dzierżawcę-folder w celu zorganizowania klientów i zechcesz przenieść część z nich do nowo utworzonego dzierżawcy-folderu.

## Typ dzierżawców, których można przenosić

| Typ dzierżawcy | Można przenieść | Dzierżawca docelowy |
|---|---|---|
| Partner | Tak | Partner lub Folder |
| Folder | Tak | Partner lub Folder |
| Klient | Tak | Partner lub Folder |
| Jednostka | Nie | Brak |

## Wymagania i ograniczenia

- Dzierżawcę można przenieść tylko wtedy, gdy docelowy dzierżawca nadrzędny ma co najmniej taki sam zestaw usług i pozycji ofert jak pierwotny dzierżawca nadrzędny.
- W przypadku przenoszenia dzierżawcy-klienta wszystkie magazyny przypisane do tego dzierżawcy-klienta w ramach pierwotnego dzierżawcy nadrzędnego muszą być dostępne również u docelowego dzierżawcy nadrzędnego. Jest to konieczne, ponieważ danych związanych z obsługą klienta nie można przenieść do innego magazynu.
- W przypadku dzierżawców-klientów, którymi zarządzają dostawcy usług, mogą istnieć plany stosowane do obciążeń klientów z poziomu dostawcy usług (na przykład plany skryptów).

  Podczas przenoszenia takiego dzierżawcy-klienta plany dostawcy usług zostaną odwołane z obciążeń klienta i wszystkie usługi związane z tymi planami przestaną działać w przypadku tego klienta.
- Dzierżawców można przenosić w ramach hierarchii konta partnera. Niektórych dzierżawców-klientów można też przenieść do dzierżawcy docelowego spoza hierarchii konta partnera. Aby sprawdzić, czy taka operacja jest możliwa, skontaktuj się z opiekunem klienta w firmie .
- Tylko administratorzy (na przykład administrator w Portalu zarządzania lub administrator firmy) mogą przenosić dzierżawców do innych dzierżawców nadrzędnych.

## Jak przenieść dzierżawcę

1. Zaloguj się do portalu zarządzania.
2. Znajdź i skopiuj **Identyfikator wewnętrzny** dzierżawcy-partnera lub dzierżawcy-folderu, do którego chcesz przenieść dzierżawcę. Wykonaj następujące czynności:
   a. Na karcie **Klienci** wybierz dzierżawcę docelowego, do którego chcesz przenieść danego dzierżawcę.
   b. W panelu właściwości dzierżawcy kliknij ikonę pionowego wielokropka, a następnie kliknij **Pokaż identyfikator**.
   c. Skopiuj ciąg znaków widoczny w polu **Identyfikator wewnętrzny**, a następnie kliknij **Anuluj**.
3. Wybierz dzierżawcę, którego chcesz przenieść, a następnie przenieś go do docelowego partnera/folderu. Wykonaj następujące czynności:

a. Na karcie **Klienci** wybierz dzierżawcę, którego chcesz przenieść.
b. W panelu właściwości dzierżawcy kliknij ikonę pionowego wielokropka, a następnie kliknij **Przenieś**.
c. Wklej identyfikator wewnętrzny dzierżawcy docelowego i kliknij **Przenieś**.

Operacja rozpocznie się niezwłocznie i potrwa do 10 minut.

Jeśli przenoszony dzierżawca ma dzierżawców podrzędnych (na przykład jest dzierżawcą-partnerem lub dzierżawcą-folderem obejmującym dzierżawcę-klienta), to całe jego poddrzewo zostanie przeniesione do dzierżawcy docelowego.

## Konwersja dzierżawcy-partnera do dzierżawcy-folderu i na odwrót

Portal zarządzania pozwala na konwersję dzierżawcy-partnera do dzierżawcy-folderu.

Funkcja ta może się przydać na przykład wtedy, gdy użyłeś dzierżawcy-partnera w celu grupowania, a teraz chcesz prawidłowo zorganizować infrastrukturę swoich dzierżawców. Jest również przydatna wtedy, gdy chcesz, aby pulpit operacyjny zawierał informacje zbiorcze o dzierżawcy.

Możesz również przekonwertować dzierżawcę-folder na dzierżawcę-partnera.

**Uwaga**
Konwersja jest bezpieczna i nie ma wpływu na użytkowników w ramach dzierżawcy ani żadne dane dotyczące usługi.

***Aby przekonwertować dzierżawcę***

1. Zaloguj się do portalu zarządzania.
2. Na karcie **Klienci** wybierz dzierżawcę, którego chcesz przekonwertować.
3. Wykonaj jedną z następujących czynności:
   - Kliknij ikonę wielokropka obok nazwy dzierżawcy.
   - Wybierz dzierżawcę, a następnie kliknij ikonę wielokropka w panelu właściwości dzierżawcy.
4. Kliknij **Konwertuj na partnera** lub **Konwertuj na folder**.
5. Potwierdź decyzję.

## Ograniczanie dostępu do dzierżawcy

Administratorzy na poziomie klienta lub wyższym mogą ograniczać administratorom wyższych poziomów dostęp do swoich dzierżawców.

Jeśli dostęp do dzierżawcy jest ograniczony, administratorzy dzierżawcy nadrzędnego mogą tylko modyfikować właściwości dzierżawcy. Konta ani dzierżawcy podrzędni nie są dla nich widoczni.

***Aby zablokować administratorom wyższych poziomów dostęp do dzierżawcy***

1. Zaloguj się do portalu zarządzania.
2. Przejdź do sekcji **Ustawienia** > **Bezpieczeństwo**.
3. Wyłącz przełącznik **Dostęp do pomocy technicznej**.

W wyniku tego administratorzy dzierżawców nadrzędnych będą mieć ograniczony dostęp do Twojego dzierżawcy. Będą mogli jedynie modyfikować właściwości dzierżawcy, ale nie będą mieć dostępu do żadnych zasobów w jego obszarze (np. dzierżawców, użytkowników, usług, kopii zapasowych i innych) i nie będą mogli nimi zarządzać.

W przypadku włączenia przełącznika **Dostęp do pomocy technicznej** administratorzy dzierżawców nadrzędnych będą mieć pełny dostęp do Twojego dzierżawcy. Będą mogli modyfikować właściwości, zarządzać dzierżawcami, użytkownikami i usługami oraz uzyskiwać dostęp do kopii zapasowych i innych zasobów.

## Usuwanie dzierżawcy

Czasem warto usunąć dzierżawcę w celu zwolnienia wykorzystywanych przez niego zasobów. Statystyki wykorzystania zostaną zaktualizowane w ciągu jednego dnia od usunięcia. W przypadku dużych dzierżawców może to potrwać dłużej.

Przed usunięciem konta dzierżawcy trzeba je wyłączyć. Więcej informacji o tym, jak to zrobić, można znaleźć w sekcji „Wyłączanie i włączanie dzierżawcy”.

**Ważne**
Usunięcie dzierżawcy jest nieodwracalne!

***Aby usunąć dzierżawcę***

1. W portalu zarządzania wybierz **Klienci**.
2. Zaznacz wyłączonego dzierżawcę, które chcesz usunąć, a następnie kliknij ikonę wielokropka  > **Usuń**.
3. Aby potwierdzić operację, wprowadź swoją nazwę logowania i kliknij **Dalej**.

Wskutek tego:

- Dzierżawca i jego poddzierżawcy zostaną usunięci.
- Wszystkie usługi, które były włączone w ramach dzierżawcy i jego poddzierżawców, zostaną zatrzymane.
- Wszyscy użytkownicy w ramach dzierżawcy i jego poddzierżawców zostaną usunięci.
- Wszystkie komputery w ramach dzierżawcy i jego poddzierżawców zostaną wyrejestrowane.
- Wszystkie dane związane z usługami, np. kopie zapasowe i synchronizowane pliki, w ramach dzierżawcy i jego poddzierżawców zostaną usunięte.
- Wszystkie klienty API w ramach dzierżawcy i jego poddzierżawców zostaną usunięte, a wszystkie integracje utworzone przy użyciu tych klientów przestaną działać.

# Zarządzanie użytkownikami

Administratorzy partnerów, administratorzy klientów i administratorzy jednostek mogą konfigurować konta użytkowników w ramach dostępnych dla nich dzierżawców i nimi zarządzać.

## Tworzenie konta użytkownika

Być może zechcesz utworzyć dodatkowe konta w następujących sytuacjach:

- Konta administratorów partnerów/folderów — w celu podzielenia się obowiązkiem zarządzania usługami z innymi osobami.
- Konta administratorów klientów / potencjalnych klientów / jednostek — w celu przekazania zarządzania usługami innym osobom, których uprawnienia dostępu będą ściśle ograniczone do odpowiednich klientów / potencjalnych klientów / jednostek.
- Konta użytkowników w ramach klienta lub dzierżawcy-jednostki — w celu umożliwienia użytkownikom dostępu tylko do określonej części usług.

Uwaga: utworzonych kont nie można przenosić między dzierżawcami. Najpierw należy utworzyć dzierżawcę, a potem dodać do niego konta.

***Aby utworzyć konto użytkownika***

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz utworzyć konto użytkownika. Zobacz "Nawigacja po portalu zarządzania" (s. 29).
3. W prawym górnym rogu kliknij **Nowe** > **Użytkownik**.
   Możesz też przejść do sekcji **Zarządzanie firmą > Użytkownicy** i kliknąć **+ Nowe**.
4. Określ następujące informacje kontaktowe na potrzeby konta:
   - **Nazwa logowania**

     **Ważne**
     Każde konto musi mieć unikatową nazwę logowania.

   - **E-mail**

     **Ważne**
     Jeśli użytkownik jest zarejestrowany w usłudze File Sync & Share, podaj adres e-mail użyty do rejestracji w usłudze File Sync & Share.
     Należy pamiętać, że każde konto użytkownika klienta musi mieć unikatowy adres e-mail.

   - **Imię**
   - **Nazwisko**
   - [Opcjonalnie] **Telefon służbowy**

**Uwaga**
Takie pola jak **Telefon służbowy**, **Stanowisko** czy **Osoba kontaktowa w firmie** będą wyświetlane w kreatorze użytkownika tylko wtedy, gdy partner nadrzędny włączy dla dzierżawcy-klienta opcję **Włącz samodzielnie zarządzany profil klienta**. Jeśli tego nie zrobi, pola te nie będą wyświetlane.

- [Opcjonalnie] **Stanowisko**
- W polu **Język** zmień domyślny język powiadomień, raportów i oprogramowania, który będzie używany na danym koncie.

5. [Opcjonalnie] Określ osoby kontaktowe w firmie.
   - **Rozliczenia** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach w raportach o wykorzystaniu na platformie.
   - **Techniczne** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów technicznych.
   - **Biznesowe** — kontakt, który będzie otrzymywać aktualne informacje o ważnych zmianach na platformie dotyczących aspektów biznesowych.

     Użytkownikowi można przypisać więcej niż jeden typ kontaktu w firmie.

   Typy kontaktów w firmie przypisane do danego użytkownika można sprawdzić na liście **Użytkownicy** w kolumnie **Osoby kontaktowe w firmie** i w razie potrzeby zmienić, edytując konto użytkownika.
6. [Opcja niedostępna w przypadku tworzenia konta w ramach dzierżawcy-partnera/folderu] Wybierz usługi, do których użytkownik będzie mieć dostęp, oraz role w każdej z usług.

   Dostępność usług zależy od usług włączonych dla dzierżawcy, w ramach którego jest tworzone konto użytkownika.
   - Jeśli zaznaczysz pole wyboru **Administrator firmy**, użytkownik będzie mieć dostęp do portalu zarządzania i rolę administratora we wszystkich usługach aktualnie włączonych dla danego dzierżawcy. Użytkownik będzie też mieć rolę administratora we wszystkich usługach, które zostaną włączone dla danego dzierżawcy w przyszłości.
   - Jeśli zaznaczysz pole wyboru **Administrator jednostki**, użytkownik będzie mieć dostęp do portalu zarządzania, ale może nie mieć roli administratora usługi — w zależności od usługi.
   - Jeśli go nie zaznaczysz, użytkownik będzie mieć wybrane przez Ciebie role w wybranych usługach.
7. Kliknij **Utwórz**.

Nowo utworzone konto użytkownika pojawi się na karcie **Użytkownicy** w sekcji **Zarządzanie firmą**.

Jeśli zechcesz edytować ustawienia użytkownika lub określić dla niego ustawienia powiadomień i limity (niedostępne dla administratorów partnerów i folderów), zaznacz tego użytkownika na karcie **Użytkownicy**, a następnie kliknij ikonę ołówka w sekcji, którą chcesz edytować.

***Aby zresetować hasło użytkownika***

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Zaznacz użytkownika, którego hasło chcesz zresetować, a następnie kliknij ikonę wielokropka ••• > **Resetuj hasło**.
3. Potwierdź czynność, klikając **Resetuj**.

Teraz użytkownik może zresetować hasło, postępując zgodnie z instrukcjami zawartymi w otrzymanej wiadomości e-mail.

W przypadku usług, które nie obsługują uwierzytelniania dwuskładnikowego (na przykład rejestracji w rozwiązaniu  Cyber Infrastructure), może być konieczne przekonwertowanie konta użytkownika na *konto usługi* — takie konto nie wymaga uwierzytelniania dwuskładnikowego.

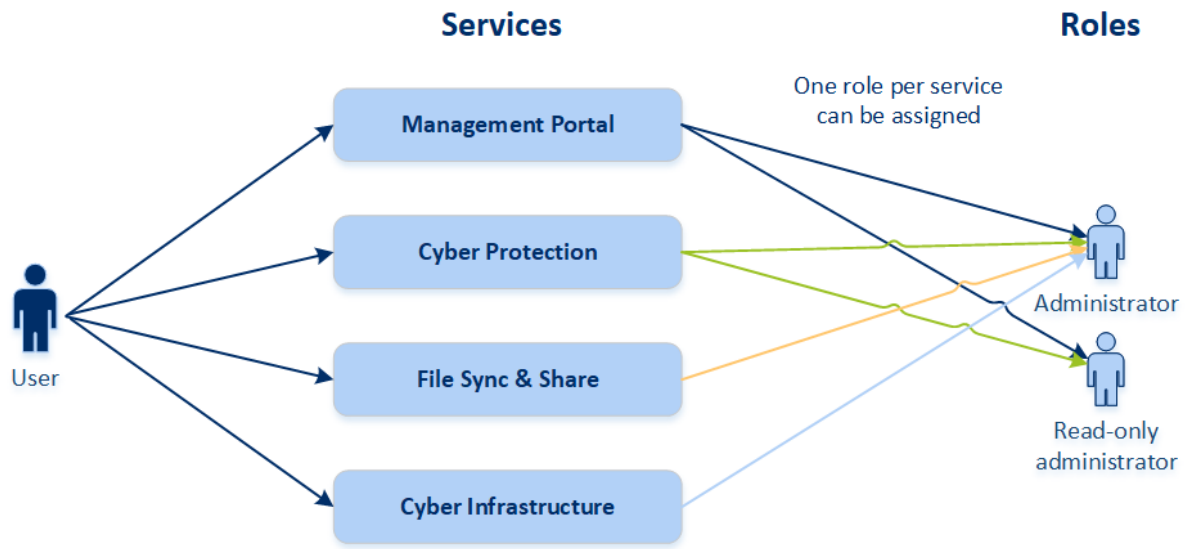
***Aby przekonwertować konto użytkownika na konto usługi***

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Wybierz użytkownika, którego konto chcesz przekonwertować na konto usługi, a następnie kliknij ikonę wielokropka ••• > **Oznacz jako konto usługi**.
3. W oknie z monitem o potwierdzenie wprowadź kod uwierzytelniania dwuskładnikowego i potwierdź czynność.

Tego konta można teraz używać na potrzeby usług, które nie obsługują uwierzytelniania dwuskładnikowego.

## Role użytkowników dostępne w przypadku poszczególnych usług

Jeden użytkownik może mieć kilka ról, ale tylko jedną rolę w ramach danej usługi.




Rolę użytkownika można definiować dla każdej usługi z osobna.

| Usługa | Rola | Opis |
|---|---|---|

| | | |
|---|---|---|
| n/d | Administrator firmy | Ta rola oznacza przyznanie pełnych praw administratora w przypadku wszystkich usług.<br><br>Ta rola zapewnia dostęp do firmowej listy dozwolonych. Jeśli dla firmy włączono dodatek Disaster Recovery usługi Cyber Protection, rola ta zapewnia również dostęp do funkcji odzyskiwania po awarii. |
| Portal zarządzania | Administrator | Ta rola zapewnia dostęp do portalu zarządzania, gdzie administrator może zarządzać użytkownikami w całej organizacji. |
| | Administrator w trybie tylko do odczytu<br><br>Poziom partnera | Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów w portalu zarządzania partnera oraz portalu zarządzania wszystkich klientów tego partnera. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu. |
| | Administrator w trybie tylko do odczytu<br><br>Poziom klienta | Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów w portalu zarządzania całej firmy. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu. |
| | Administrator w trybie tylko do odczytu<br><br>Poziom jednostki | Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów w portalu zarządzania jednostki i podjednostek firmy. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu. |
| Cyber Protection | Administrator środowiska cybernetycznego | Oprócz praw roli Administrator rola ta daje możliwość konfigurowania usługi Cyber Protection i zarządzania nią oraz zatwierdzania czynności w ramach funkcji Skrypty cybernetyczne.<br><br>Rola Administrator środowiska cybernetycznego jest dostępna tylko w przypadku dzierżawców, którzy mają włączony pakiet Advanced Management. |
| | Administrator | Ta rola umożliwia konfigurowanie usługi Cyber Protection dla klientów i zarządzanie nią.<br><br>Ta rola jest wymagana do konfigurowania funkcji Odzyskiwanie po awarii i firmowej listy dozwolonych, a także zarządzania nimi. |
| | Administrator w trybie tylko do odczytu | Ta rola zapewnia dostęp tylko do odczytu do wszystkich obiektów usługi Cyber Protection. Użytkownicy z tą rolą mają dostęp do danych innych użytkowników z organizacji w trybie tylko do odczytu.<br><br>Administrator w trybie tylko do odczytu nie może konfigurować funkcji Odzyskiwanie po awarii i firmowej listy dozwolonych ani nimi zarządzać. |
| | Operator | Ta rola umożliwia uzyskiwanie dostępu do kopii zapasowych |

| | | |
|---|---|---|
| | przywracania | organizacji Microsoft 365 i Google Workspace oraz ich odzyskiwanie przy jednoczesnym ograniczeniu dostępu do wrażliwej zawartości. |
| File Sync & Share | Administrator | Ta rola umożliwia konfigurowanie usługi File Sync & Share dla użytkowników i zarządzanie nią. |
| Cyber Infrastructure | Administrator | Ta rola umożliwia konfigurowanie usługi Cyber Infrastructure dla użytkowników i zarządzanie nią. |

## Rola Administrator w trybie tylko do odczytu

Konto z tą rolą ma dostęp tylko do odczytu do konsoli internetowej Cyber Protection i umożliwia wykonywanie następujących operacji:

- Zbieranie danych diagnostycznych, na przykład raportów systemowych.
- Przeglądanie punktów odzyskiwania kopii zapasowej, ale bez możliwości przejścia do zawartości kopii zapasowej i przeglądania plików, folderów oraz wiadomości e-mail.

Administrator w trybie tylko do odczytu nie może:

- Uruchamiać ani zatrzymywać żadnych zadań.

  Na przykład administrator w trybie tylko do odczytu nie może rozpocząć odzyskiwania ani zatrzymać rozpoczętej operacji tworzenia kopii zapasowej.
- Uzyskiwać dostępu do systemu plików na komputerze źródłowym lub docelowym.

  Na przykład administrator w trybie tylko do odczytu nie może przeglądać plików, folderów ani wiadomości e-mail na komputerze uwzględnionym w kopii zapasowej.
- Zmieniać jakichkolwiek ustawień.

  Na przykład administrator w trybie tylko do odczytu nie może utworzyć planu ochrony ani zmienić jego ustawień.
- Tworzyć, aktualizować ani usuwać jakichkolwiek danych.

  Na przykład administrator w trybie tylko do odczytu nie może usunąć kopii zapasowych.

Wszelkie obiekty interfejsy użytkownika niedostępne dla administratora w trybie tylko do odczytu są ukryte, z wyjątkiem domyślnych ustawień planu ochrony. Te ustawienia są widoczne, ale przycisk **Zapisz** jest nieaktywny.

Wszelkie zmiany dotyczące kont i ról są wyświetlane na karcie **Działania** wraz z następującymi informacjami:

- Co zostało zmienione
- Autorzy zmian
- Daty i godziny zmian

## Rola Operator przywracania

Ta rola jest dostępna tylko w usłudze Cyber Protection i jest ograniczona do kopii zapasowych danych Microsoft 365 i Google Workspace.

Operator przywracania może wykonywać następujące czynności:

- Wyświetlanie alertów i działań.
- Przeglądanie i odświeżanie listy kopii zapasowych.
- Przeglądanie kopii zapasowych bez uzyskiwania dostępu do ich zawartości. Operator przywracania może zobaczyć nazwy plików oraz tematy i nadawców wiadomości e-mail uwzględnionych w kopii zapasowej.
- Przeszukiwanie kopii zapasowych (wyszukiwanie pełnotekstowe nie jest obsługiwane).
- Odzyskiwanie kopii zapasowych utworzonych z chmury do chmury do ich pierwotnej lokalizacji w ramach pierwotnej organizacji Microsoft 365 lub Google Workspace.

Operator przywracania nie może wykonywać następujących czynności:

- Usuwanie alertów.
- Dodawanie lub usuwanie organizacji Microsoft 365 lub Google Workspace.
- Dodawanie, usuwanie lub zmienianie nazw lokalizacji kopii zapasowych.
- Usuwanie lub zmienianie nazw kopii zapasowych.
- Tworzenie, usuwanie lub zmienianie nazw folderów podczas odzyskiwania kopii zapasowej do niestandardowej lokalizacji.
- Stosowanie planu tworzenia kopii zapasowych lub uruchamianie operacji tworzenia kopii zapasowej.
- Uzyskiwanie dostępu do plików lub zawartości wiadomości e-mail uwzględnionych w kopii zapasowej.
- Pobieranie plików lub załączników wiadomości e-mail z kopii zapasowej.
- Wysyłanie uwzględnionych w kopii zapasowej zasobów chmury, takich jak wiadomości e-mail lub elementy kalendarza, jako wiadomości e-mail.
- Wyświetlanie lub odzyskiwanie konwersacji z usługi Microsoft 365 Teams.
- Odzyskiwanie kopii zapasowych utworzonych z chmury do chmury do innych lokalizacji niż pierwotne, na przykład do innej skrzynki pocztowej, usługi OneDrive, Dysku Google lub usługi Microsoft 365 Teams.

## Role użytkowników a prawa do funkcji Skrypty cybernetyczne

Czynności dostępne w przypadku skryptów i planów skryptów zależą od statusu skryptu i roli użytkownika.

Administratorzy mogą zarządzać obiektami w ramach własnego dzierżawcy oraz jego dzierżawców podrzędnych. Nie widzą obiektów na wyższym poziomie administracji, jeśli taki poziom istnieje, ani nie mogą uzyskiwać do nich dostępu.

Administratorzy niższych poziomów mają dostęp tylko do odczytu do planów skryptów stosowanych do ich obciążeń roboczych przez administratora wyższego poziomu.

Poniższe role zapewniają prawa związane z funkcją Skrypty cybernetyczne:

- Administrator firmy

  Ta rola oznacza przyznanie pełnych praw administratora w przypadku wszystkich usług. Jeśli chodzi o funkcję Skrypty cybernetyczne, zapewnia ona takie same prawa jak rola Administrator środowiska cybernetycznego.

- Administrator środowiska cybernetycznego

  Ta rola oznacza przyznanie pełnych uprawnień, w tym do zatwierdzania skryptów, które mogą być używane w ramach dzierżawcy, oraz do uruchamiania skryptów ze statusem **Testowanie**.
- Administrator

  Ta rola oznacza przyznanie częściowych uprawnień, w tym możliwość uruchamiania zatwierdzonych skryptów, a także tworzenia i uruchamiania planów skryptów korzystających z zatwierdzonych skryptów.
- Administrator w trybie tylko do odczytu

  Ta rola oznacza przyznanie ograniczonych uprawnień, w tym możliwości wyświetlania skryptów i planów ochrony używanych w ramach dzierżawcy.
- Użytkownik

  Ta rola oznacza przyznanie częściowych uprawnień, w tym możliwość uruchamiania zatwierdzonych skryptów, a także tworzenia i uruchamiania planów skryptów korzystających z zatwierdzonych skryptów, ale tylko na komputerze użytkownika.

W poniższej tabeli zestawiono wszystkie dostępne czynności z uwzględnieniem statusu skryptu i roli użytkownika.

| **Rola** | **Obiekt** | **Status skryptu** | | |
|---|---|---|---|---|
| | | **Wersja robocza** | **Testowanie** | **Zatwierdzono** |
| Administrator środowiska cybernetycznego<br>Administrator firmy | Plan skryptów | Edytuj (usuń z planu roboczą wersję skryptu)<br>Usuń<br>Odwołaj<br>Wyłącz<br>Zatrzymaj | Utwórz<br>Edytuj<br>Zastosuj<br>Włącz<br>Uruchom<br>Usuń<br>Odwołaj | Utwórz<br>Edytuj<br>Zastosuj<br>Włącz<br>Uruchom<br>Usuń<br>Odwołaj |

| | | | | |
|---|---|---|---|---|
| | | | Wyłącz<br>Zatrzymaj | Wyłącz<br>Zatrzymaj |
| | Script | Utwórz<br>Edytuj<br>Zmień status<br>Klonuj<br>Usuń<br>Anuluj uruchomienie | Utwórz<br>Edytuj<br>Zmień status<br>Uruchom<br>Klonuj<br>Usuń<br>Anuluj uruchomienie | Utwórz<br>Edytuj<br>Zmień status<br>Uruchom<br>Klonuj<br>Usuń<br>Anuluj uruchomienie |
| Administrator<br>Użytkownik (w przypadku własnych obciążeń) | Plan skryptów | Widok<br>Odwołaj<br>Wyłącz<br>Zatrzymaj | Widok<br>Anuluj przebieg | Utwórz<br>Edytuj<br>Zastosuj<br>Włącz<br>Uruchom<br>Usuń<br>Odwołaj<br>Wyłącz<br>Zatrzymaj |
| | Script | Utwórz<br>Edytuj<br>Klonuj<br>Usuń<br>Anuluj uruchomienie | Widok<br>Klonuj<br>Anuluj uruchomienie | Uruchom<br>Klonuj<br>Anuluj uruchomienie |
| Administrator w trybie tylko do odczytu | Plan skryptów | Widok | Widok | Widok |
| | Script | Widok | Widok | Widok |

## Zmienianie ustawień powiadomień dla użytkownika

Aby zmienić ustawienia powiadomień dla użytkownika, przejdź do karty **Zarządzanie firmą** > **Użytkownicy**. Wybierz użytkownika, dla którego chcesz skonfigurować powiadomienia, a następnie

kliknij ikonę ołówka w sekcji **Ustawienia**. Jeśli usługa Cyber Protection jest włączona dla dzierżawcy, w ramach którego jest tworzony użytkownik, dostępne są następujące ustawienia powiadomień:

- **Powiadomienia o nadużyciu limitów** (domyślnie włączone)
  Powiadomienia o przekroczeniu limitów.
- **Zaplanowane raporty z wykorzystania** (domyślnie włączone)
  Raporty z wykorzystania, które są wysyłane pierwszego dnia każdego miesiąca.
- **Powiadomienia o oznaczeniu marką adresu URL** (domyślnie wyłączone)
  Powiadomienia o zbliżającym się wygaśnięciu certyfikatu używanego na potrzeby niestandardowego adresu URL dla usług Cyber Protect Cloud. Powiadomienia są wysyłane do wszystkich administratorów wybranego dzierżawcy — na 30 dni, 15 dni, 7 dni, 3 dni i 1 dzień przed wygaśnięciem certyfikatu.
- **Powiadomienia o błędach**, **Powiadomienia o ostrzeżeniach** oraz **Powiadomienia o udanych operacjach** (domyślnie wyłączone)
  Powiadomienia o wynikach wykonywania planów ochrony oraz operacji odzyskiwania po awarii w przypadku każdego urządzenia.
- **Codziennie zestawienie aktywnych alertów** (domyślnie włączone)
  Codzienne zestawienie jest generowane na podstawie listy alertów aktywnych w konsoli usługi w chwili generowania zestawienia. Takie zestawienie jest generowane i wysyłane raz dziennie między 10:00 a 23:59 czasu UTC. Godzina wygenerowania i wysłania raportu zależy od obciążenia centrum danych. Jeśli w danym czasie nie ma żadnych aktywnych alertów, zestawienie nie jest wysyłane. Zestawienie nie zawiera informacji dotyczących wcześniejszych alertów, które nie są już aktywne. Na przykład w sytuacji, gdy użytkownik wykryje nieudaną operację tworzenia kopii zapasowej i wyczyści alert lub taka operacja zostanie ponowiona i zakończy się pomyślnie, zanim zostanie wygenerowane zestawienie, dotyczący jej alert nie będzie już aktywny i nie zostanie uwzględniony w zestawieniu.
- **Powiadomienia funkcji Kontrola urządzeń** (domyślnie wyłączone)
  Powiadomienia o próbach użycia urządzeń peryferyjnych i portów, do których dostęp jest ograniczony przez plany ochrony z włączonym modułem kontroli urządzeń.
- **Powiadomienia dotyczące odzyskiwania** (domyślnie wyłączone)
  Powiadomienia o czynnościach związanych z odzyskiwaniem w odniesieniu do następujących zasobów: wiadomości e-mail i cała skrzynka pocztowa użytkownika, foldery publiczne, OneDrive / Dysk Google: cały OneDrive oraz pliki lub foldery, pliki programu SharePoint, Teams: kanały, cały zespół, wiadomości e-mail i witryna zespołu.
  W kontekście tych powiadomień następujące czynności są uznawane za związane z odzyskiwaniem: wysłanie jako wiadomość e-mail, pobranie lub rozpoczęcie operacji odzyskiwania.
- **Powiadomienia funkcji Zapobieganie utracie danych** (domyślnie wyłączone)
  Powiadomienia o alertach dotyczących zapobiegania utracie danych związanych z działaniami danego użytkownika w sieci.
- **Powiadomienia dotyczące incydentów bezpieczeństwa** (domyślnie wyłączone)

Powiadomienia o złośliwym oprogramowaniu wykrytym w ramach skanowania podczas uzyskiwania dostępu, podczas wykonywania i na żądanie, a także o zdarzeniach wykrytych przez mechanizm zachowań i mechanizm filtrowania adresów URL.

Dostępne są dwie opcje: **Zniwelowano** i **Nie zniwelowano**. Opcje te dotyczą alertów o incydentach zgłaszanych przez pakiet Endpoint Detection and Response (EDR), alertów EDR z kanałów dotyczących zagrożeń oraz alertów indywidualnych (w przypadku obciążeń, na których nie włączono EDR).

Po utworzeniu alertu EDR wysyłana jest wiadomość e-mail do odpowiedniego użytkownika. Jeśli status zagrożenia w ramach incydentu ulegnie zmianie, zostanie wysłana nowa wiadomość e-mail. Takie wiadomości zawierają przyciski czynności, które umożliwiają użytkownikowi zapoznanie się ze szczegółami incydentu (jeśli został on zniwelowany) lub poddanie incydentu dochodzeniu i naprawienie jego skutków (jeśli nie został on zniwelowany).

- **Powiadomienia dotyczące infrastruktury** (domyślnie wyłączone)
  Powiadomienia o problemach z infrastrukturą odzyskiwania po awarii: gdy infrastruktura odzyskiwania po awarii jest niedostępna lub tunele VPN są niedostępne.

Wszystkie powiadomienia są wysyłane na adres e-mail użytkownika.

## Powiadomienia odbierane przez użytkownika z daną rolą

Powiadomienia wysyłane przez usługę Cyber Protection zależą od roli użytkownika.

| Typ powiadomienia \ Rola użytkownika | Użytkownik | Administrator klienta |
|---|---|---|
| Powiadomienia dotyczące własnych urządzeń | Tak | Tak |
| Powiadomienia dotyczące wszystkich urządzeń w organizacji | n/d | Tak (z wyjątkiem kategorii **Powiadomienia dotyczące incydentów bezpieczeństwa**) |
| Powiadomienia dotyczące usług Microsoft 365, Google Workspace i innych operacji tworzenia kopii zapasowych w chmurze | n/d | Tak |

| Typ powiadomienia \ Rola użytkownika | Użytkownik | Administratorzy klientów i jednostek | Administrator partnerów i folderów |
|---|---|---|---|
| Powiadomienia dotyczące własnych urządzeń | Tak | Tak | n/d* |
| Powiadomienia dotyczące wszystkich urządzeń dzierżawców podrzędnych | n/d | Tak | Tak |
| Powiadomienia dotyczące usług Microsoft 365, Google Workspace i innych operacji tworzenia kopii zapasowych w chmurze | n/d | Tak | Tak |

* Administratorzy partnerów nie mogą rejestrować własnych urządzeń, ale mogą tworzyć konta administratorów klientów i dodawać własne urządzenia za ich pomocą. Zobacz Konta użytkowników oraz dzierżawcy.

## Wyłączanie i włączanie konta użytkownika

Czasem może być konieczne wyłączenie konta użytkownika w celu tymczasowego ograniczenia jego dostępu do chmury.

***Aby wyłączyć konto użytkownika***

1. W portalu zarządzania przejdź do sekcji **Użytkownicy**.
2. Zaznacz konto użytkownika, które chcesz wyłączyć, a następnie kliknij ikonę wielokropka > **Wyłącz**.
3. Potwierdź operację, klikając **Wyłącz**.

Od tej pory ten użytkownik nie będzie mógł korzystać z chmury ani otrzymywać żadnych powiadomień.

Aby włączyć wyłączone konto użytkownika, zaznacz je na liście użytkowników, a następnie kliknij ikonę wielokropka > **Włącz**.

## Usuwanie konta użytkownika

Czasem może być konieczne nieodwracalne usunięcie konta użytkownika w celu zwolnienia wykorzystywanych przez nie zasobów, na przykład miejsca na dysku lub licencji. Statystyki wykorzystania zostaną zaktualizowane w ciągu jednego dnia od usunięcia. W przypadku kont z dużą ilością danych może to potrwać dłużej.

Przed usunięciem konta użytkownika trzeba je wyłączyć. Więcej informacji o tym, jak to zrobić, można znaleźć w sekcji „Wyłączanie i włączanie konta użytkownika”.

**Ważne**
Usunięcie konta użytkownika jest nieodwracalne!

***Aby usunąć konto użytkownika***

1. W portalu zarządzania przejdź do sekcji **Użytkownicy**.
2. Zaznacz wyłączone konto użytkownika, a następnie kliknij ikonę wielokropka > **Usuń**.
3. Aby potwierdzić operację, wprowadź swoją nazwę logowania i kliknij **Dalej**.

Wskutek tego:

- Konto użytkownika zostanie usunięte.
- Wszystkie dane z tego konta użytkownika zostaną usunięte.

- Wszystkie komputery powiązane z tym kontem użytkownika zostaną wyrejestrowane.

## Przenoszenie własności konta użytkownika

Czasem może być konieczne przeniesienie własności konta użytkownika, aby zachować dostęp do zastrzeżonych danych użytkownika.

**Ważne**
Zawartości usuniętego konta nie można ponownie przypisać.

***Aby przenieść własność konta użytkownika***

1. W portalu zarządzania przejdź do sekcji **Użytkownicy**.
2. Zaznacz konto użytkownika, którego własność chcesz przenieść, a następnie kliknij ikonę ołówka w sekcji **Informacje ogólne**.
3. Zastąp dotychczasowy adres e-mail adresem e-mail przyszłego właściciela konta, a następnie kliknij **Gotowe**.
4. Potwierdź operację, klikając **Tak**.
5. Poczekaj, aż przyszły właściciel konta zweryfikuje adres e-mail, postępując zgodnie z wysłanymi na ten adres instrukcjami.
6. Zaznacz konto użytkownika, którego własność przenosisz, a następnie kliknij ikonę wielokropka ••• > **Resetuj hasło**.
7. Potwierdź czynność, klikając **Resetuj**.
8. Poczekaj, aż przyszły właściciel konta zresetuje hasło, postępując zgodnie z instrukcjami wysłanymi na jego adres e-mail.

Od tej pory nowy właściciel będzie mieć dostęp do konta.

# Konfigurowanie uwierzytelniania dwuskładnikowego

**Uwierzytelnianie dwuskładnikowe (2FA)** jest typem uwierzytelniania wieloskładnikowego, w którego ramach tożsamość użytkownika jest sprawdzana na podstawie dwóch elementów:

- Czegoś, co użytkownik zna (numer PIN lub hasło)
- Czegoś, co użytkownik ma (token)
- Czegoś, co jest nieodłączną cechą użytkownika (dane biometryczne)

Uwierzytelnianie dwuskładnikowe zapewnia dodatkową ochronę przed nieuprawnionym dostępem do konta.

Ta platforma obsługuje uwierzytelnianie przy użyciu **czasowych haseł jednorazowych (Time-based One-Time Password, TOTP)**. Jeśli w systemie jest włączone uwierzytelnianie TOTP, w celu uzyskania dostępu do systemu użytkownicy muszą podać swoje tradycyjne hasło oraz jednorazowy kod TOTP. Innymi słowy, użytkownik podaje hasło (pierwszy składnik) i kod TOTP (drugi składnik).

Kod TOTP jest generowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania na podstawie bieżącego czasu i klucza tajnego (kodu QR lub alfanumerycznego) udostępnianego przez platformę.

## Sposób działania

1. Uwierzytelnianie dwuskładnikowe włącza się na poziomie organizacji.
2. W takiej sytuacji każdy użytkownik z organizacji musi zainstalować aplikację uwierzytelniającą na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania (telefonie komórkowym, laptopie, komputerze stacjonarnym lub tablecie). Aplikacja ta będzie służyć do generowania jednorazowych kodów TOTP. Zalecane aplikacje uwierzytelniające:
   - Google Authenticator

     Aplikacja w wersji dla systemu iOS (https://apps.apple.com/app/google-authenticator/id388497605)

     Aplikacja w wersji dla systemu Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator

     Aplikacja w wersji dla systemu iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)

     Aplikacja w wersji dla systemu Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   **Ważne**
   Użytkownik musi zadbać, aby czas na urządzeniu z zainstalowaną aplikacją uwierzytelniającą był prawidłowo ustawiony i odzwierciedlał czas bieżący.

3. Użytkownik z organizacji musi ponownie się zalogować do systemu.
4. Po wprowadzeniu nazwy logowania i hasła zostanie poproszony o skonfigurowanie uwierzytelniania dwuskładnikowego na swoim koncie.
5. Musi zeskanować kod QR przy użyciu aplikacji uwierzytelniającej. Jeśli nie można zeskanować kodu QR, można użyć klucza tajnego TOTP widocznego pod kodem QR i podać go ręcznie w aplikacji uwierzytelniającej.

   **Ważne**
   Zdecydowanie warto go zachować (wydrukować kod QR, zanotować klucz tajny TOTP, skorzystać z aplikacji do tworzenia kopii zapasowych kodów w chmurze). Klucz tajny TOTP będzie potrzebny do zresetowania uwierzytelniania dwuskładnikowego w razie utraty urządzenia używanego do obsługi drugiego składnika uwierzytelniania.

6. W aplikacji uwierzytelniającej zostanie wygenerowany jednorazowy kod TOTP. Jest on automatycznie generowany ponownie co 30 sekund.
7. Po wprowadzeniu hasła użytkownik musi wprowadzić kod TOTP na ekranie „Skonfiguruj uwierzytelnianie dwuskładnikowe”.

8. W ten sposób zostanie skonfigurowane uwierzytelnianie dwuskładnikowe na koncie użytkownika.

Teraz podczas logowania się do systemu użytkownik będzie monitowany o podanie nazwy logowania i hasła oraz jednorazowego kodu TOTP wygenerowanego w aplikacji uwierzytelniającej. Logując się do systemu, użytkownik może oznaczyć przeglądarkę jako zaufaną, dzięki czemu przy kolejnych operacjach logowania się przy użyciu tej przeglądarki kod TOTP nie będzie wymagany.

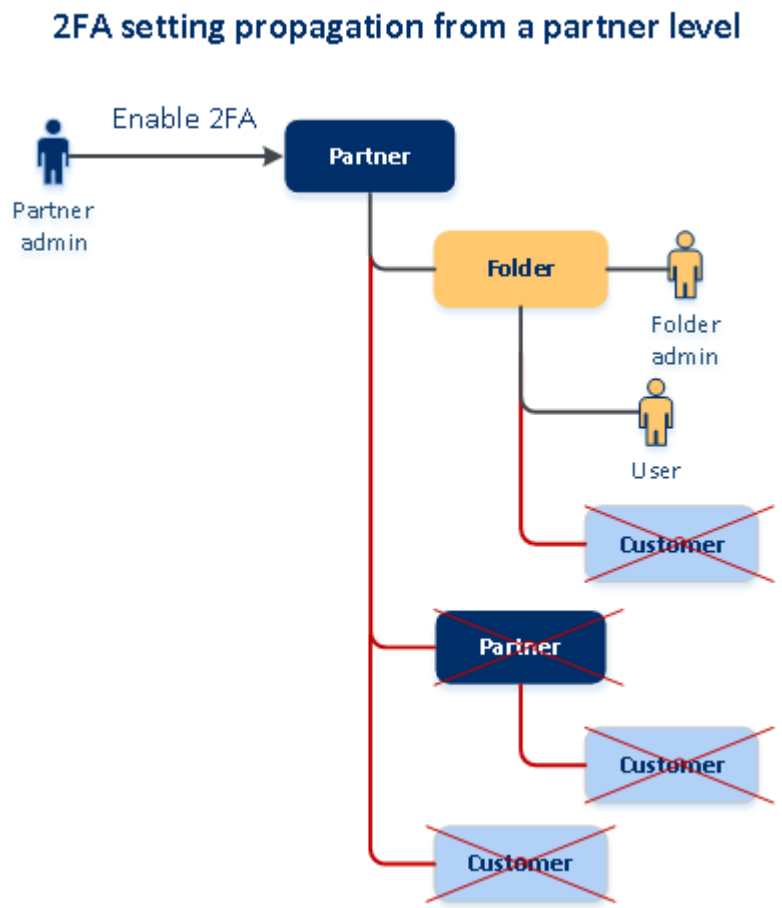
## Propagacja konfiguracji uwierzytelniania dwuskładnikowego na wszystkich poziomach dzierżawców

Uwierzytelnianie dwuskładnikowe konfiguruje się na poziomie **organizacji**. Uwierzytelnianie dwuskładnikowe można włączyć lub wyłączyć:

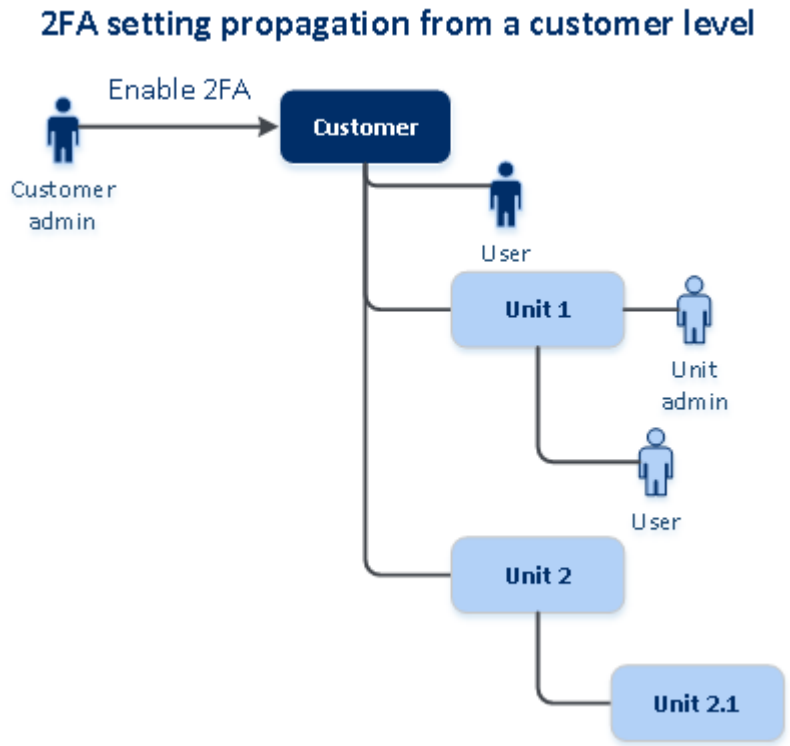
- Dla własnej organizacji.
- Dla swojego dzierżawcy podrzędnego (tylko w przypadku włączonej opcji **Dostęp do pomocy technicznej** w ramach dzierżawcy podrzędnego).

Ustawienia uwierzytelniania dwuskładnikowego są propagowane na wszystkich poziomach dzierżawców w następujący sposób:

- Foldery automatycznie dziedziczą ustawienia uwierzytelniania dwuskładnikowego z organizacji partnera. Czerwone linie na poniższym schemacie oznaczają brak możliwości propagacji ustawień uwierzytelniania dwuskładnikowego.




- Jednostki automatycznie dziedziczą ustawienia uwierzytelniania dwuskładnikowego z organizacji klienta.



**Uwaga**

1. Uwierzytelnianie dwuskładnikowe można włączyć lub wyłączyć dla organizacji podrzędnych tylko w przypadku włączonej opcji **Dostęp do pomocy technicznej** w ramach danej organizacji podrzędnej.
2. Ustawieniami uwierzytelniania dwuskładnikowego można zarządzać w przypadku użytkowników z organizacji podrzędnych tylko w przypadku włączonej opcji **Dostęp do pomocy technicznej** w ramach tej organizacji podrzędnej.
3. Nie można skonfigurować uwierzytelniania dwuskładnikowego na poziomie folderu lub jednostki.
4. Uwierzytelnianie dwuskładnikowe można skonfigurować nawet wtedy, gdy organizacja nadrzędna nie ma go włączonego.

# Konfigurowanie uwierzytelniania dwuskładnikowego dla dzierżawcy

Jako administrator możesz włączyć uwierzytelnianie dwuskładnikowe dla organizacji.

## Aby skonfigurować uwierzytelnianie dwuskładnikowe dla dzierżawcy

1. W portalu zarządzania wybierz **Ustawienia** > **Zabezpieczenia**.
2. Przesuń przełącznik **Uwierzytelnianie dwuskładnikowe** i kliknij **Włącz**.

Teraz każdy użytkownik z organizacji musi skonfigurować uwierzytelnianie dwuskładnikowe na swoim koncie. Zostanie o to poproszony przy następnej próbie zalogowania się lub po wygaśnięciu jego bieżącej sesji.

Pasek postępu wskazuje, ilu użytkowników skonfigurowało uwierzytelnianie dwuskładnikowe na swoich kontach. Aby sprawdzić, którzy użytkownicy skonfigurowali swoje konta, przejdź do karty **Zarządzanie firmą** > **Użytkownicy** i przyjrzyj się kolumnie **Status 2FA**. W przypadku użytkowników, którzy jeszcze nie skonfigurowali uwierzytelniania dwuskładnikowego na swoich kontach, w kolumnie Status 2FA jest wyświetlana wartość **Wymagana konfiguracja**.

Po pomyślnym skonfigurowaniu uwierzytelniania dwuskładnikowego użytkownicy będą musieli podawać nazwę logowania, hasło oraz kod TOTP przy każdym logowaniu się do konsoli usługi.

## Aby wyłączyć uwierzytelnianie dwuskładnikowe dla dzierżawcy

1. W portalu zarządzania wybierz **Ustawienia** > **Zabezpieczenia**.
2. Aby wyłączyć uwierzytelnianie dwuskładnikowe, wyłącz przełącznik i kliknij **Wyłącz**.
3. [Jeśli co najmniej jeden użytkownik skonfigurował uwierzytelnianie dwuskładnikowe w ramach organizacji] Wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu mobilnym.

W wyniku tych działań zostanie wyłączone uwierzytelnianie dwuskładnikowe dla organizacji, zostaną usunięte wszystkie klucze tajne i zostaną zapomniane wszystkie zaufane przeglądarki. Każdy

użytkownik będzie mógł się zalogować do systemu przy użyciu tylko nazwy logowania i hasła. Kolumna Status 2FA na karcie **Zarządzanie firmą** > **Użytkownicy** zostanie ukryta.

# Zarządzanie uwierzytelnianiem dwuskładnikowym dla użytkowników

Na karcie **Zarządzanie firmą** > **Użytkownicy** w portalu zarządzania można monitorować i resetować ustawienia uwierzytelniania dwuskładnikowego wszystkich swoich użytkowników.

## Monitorowanie

Na karcie **Zarządzanie firmą** > **Użytkownicy** w portalu zarządzania jest wyświetlana lista wszystkich użytkowników z danej organizacji. Wartość **Status 2FA** wskazuje, czy dany użytkownik ma skonfigurowane uwierzytelnianie dwuskładnikowe.

## Aby zresetować uwierzytelnianie dwuskładnikowe dla użytkownika

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Resetuj uwierzytelnianie dwuskładnikowe**.
4. Wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania i kliknij **Resetuj**.

W rezultacie użytkownik znów będzie mógł skonfigurować uwierzytelnianie dwuskładnikowe.

## Aby zresetować zaufane przeglądarki użytkownika

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Resetuj wszystkie zaufane przeglądarki**.
4. Wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania i kliknij **Resetuj**.

Użytkownik, którego wszystkie zaufane przeglądarki zostały zresetowane, przy następnym logowaniu się będzie musiał podać kod TOTP.

Użytkownicy mogą sami resetować wszystkie zaufane przeglądarki i ustawienia uwierzytelniania dwuskładnikowego. Jest to możliwe po zalogowaniu się do systemu: należy kliknąć odpowiednie łącze i wpisać kod TOTP w celu potwierdzenia operacji.

## Aby wyłączyć uwierzytelnianie dwuskładnikowe na koncie użytkownika

Lepiej nie wyłączać uwierzytelniania dwuskładnikowego, ponieważ może to ułatwiać naruszenie zabezpieczeń dzierżawcy.

W drodze wyjątku można wyłączyć uwierzytelnianie dwuskładnikowe w przypadku jakiegoś użytkownika, a zachować je w kontekście pozostałych użytkowników w ramach dzierżawcy. Jest to obejście przydatne w sytuacjach, gdy uwierzytelnianie dwuskładnikowe jest włączone w ramach dzierżawcy, dla którego skonfigurowano integrację z chmurą, przy czym integracja ta autoryzuje swój dostęp do platformy przy użyciu danego konta użytkownika (hasła logowania). Aby dalej korzystać z integracji, można tymczasowo przekształcić konto użytkownika w konto usługi, w którego przypadku nie jest stosowane uwierzytelnianie dwuskładnikowe.

**Ważne**

Zmiana zwykłych użytkowników w użytkowników usługi w celu wyłączenia uwierzytelniania dwuskładnikowego nie jest zalecana, ponieważ zwiększa zagrożenie dla bezpieczeństwa dzierżawcy.

Zalecanym bezpiecznym rozwiązaniem umożliwiającym korzystanie z integracji z chmurą bez wyłączania uwierzytelniania dwuskładnikowego dla dzierżawców jest utworzenie klientów API i skonfigurowanie integracji z chmurą tak, aby z nimi współpracowały.

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Oznacz jako konto usługi**. W wyniku tego użytkownik otrzyma specjalny status uwierzytelniania dwuskładnikowego o nazwie **Konto usługi**.
4. [Jeśli co najmniej jeden użytkownik w obszarze dzierżawcy skonfigurował uwierzytelnianie dwuskładnikowe] Aby potwierdzić wyłączenie, wprowadź kod TOTP wygenerowany w aplikacji uwierzytelniającej na urządzeniu używanym do obsługi drugiego składnika uwierzytelniania.

### Aby włączyć uwierzytelnianie dwuskładnikowe na koncie użytkownika

Czasem może wystąpić potrzeba włączenia uwierzytelniania dwuskładnikowego na koncie użytkownika, na którym zostało ono wcześniej wyłączone.

1. W portalu zarządzania przejdź do karty **Zarządzanie firmą** > **Użytkownicy**.
2. Na karcie **Użytkownicy** znajdź użytkownika, którego ustawienia chcesz zmienić, a następnie kliknij ikonę wielokropka.
3. Kliknij **Oznacz jako zwykłe konto**. W rezultacie użytkownik będzie musiał skonfigurować uwierzytelnianie dwuskładnikowe lub podać kod TOTP podczas logowania się do systemu.

## Resetowanie uwierzytelniania dwuskładnikowego w razie utraty urządzenia używanego do obsługi drugiego składnika

Aby zresetować dostęp do konta w przypadku utraty urządzenia używanego do obsługi drugiego składnika uwierzytelniania, skorzystaj z jednej z sugerowanych metod:

- Przywróć klucz tajny TOTP (kod QR lub alfanumeryczny) z kopii zapasowej.

  Skorzystaj z innego urządzenia do obsługi drugiego składnika uwierzytelniania i wprowadź zachowany klucz tajny TOTP w aplikacji uwierzytelniającej zainstalowanej na tym urządzeniu.

- Poproś administratora o zresetowanie ustawień uwierzytelniania dwuskładnikowego na Twoim koncie.

## Ochrona przed atakami brute force

Brute force to atak, podczas którego haker próbuje uzyskać dostęp do systemu, przesyłając wiele haseł z nadzieją, że jedno z nich okaże się poprawne.

Mechanizm ochrony przed atakami brute force dostępny na tej platformie jest oparty na plikach cookie urządzenia.

Stosowane są predefiniowane ustawienia ochrony przed atakami brute force:

| Parametr | Wprowadzenie hasła | Wprowadzenie kodu TOTP |
|---|---|---|
| Limit prób | 10 | 5 |
| Odstęp między limitami prób (limit jest resetowany po upływie określonego czasu) | 15 min (900 s) | 15 min (900 s) |
| Aktywacja blokady | Limit prób + 1 (11. próba) | Limit prób |
| Okres blokady | 5 min (300 s) | 5 min (300 s) |

W przypadku włączonego uwierzytelniania dwuskładnikowego plik cookie jest wysyłany do klienta (przeglądarki) wyłącznie po pomyślnym uwierzytelnieniu przy użyciu obu składników (hasła i kodu TOTP).

W przypadku zaufanych przeglądarek plik cookie urządzenia jest wysyłany po pomyślnym uwierzytelnieniu przy użyciu tylko jednego składnika (hasła).

Próby wprowadzenia kodu TOTP są rejestrowane w kontekście użytkownika, a nie urządzenia. Oznacza to, że blokada zostanie aktywowana nawet wtedy, gdy użytkownik będzie próbował wprowadzić kod TOTP z różnych urządzeń.

# Konfigurowanie scenariuszy sprzedaży dodatkowej dla klientów

Techniki sprzedaży dodatkowej polegają na zachęcaniu klientów do wykupienia kolejnych funkcji.

Usługa Cyber Protection jest dostępna w kilku starszych wersjach, które różnią się pod względem funkcji i cen. Czasem warto promować droższe wersje z bardziej zaawansowanymi funkcjami wśród obecnych klientów, którzy już korzystają z podstawowych wersji.

Funkcje sprzedaży dodatkowej można włączać lub wyłączać w przypadku poszczególnych klientów. Domyślnie opcja sprzedaży dodatkowej jest wyłączona. Jeśli włączysz u klienta opcję sprzedaży dodatkowej, będzie on widzieć dodatkowe funkcje, które jednak nie będą dla niego dostępne,

dopóki nie kupi promowanej wersji. Te dodatkowe funkcje są oznaczone etykietami z nazwą lub ikoną promowanej wersji w kolorze pomarańczowym. Takie pozycje do sprzedaży dodatkowej będą pokazywane klientowi, aby go zachęcić do zakupu droższej wersji. Po kliknięciu takiej pozycji do sprzedaży dodatkowej klient zobaczy okno dialogowe z propozycją zakupu droższej wersji, która zapewni mu dostęp do pożądanych funkcji.

Dostępne czynności zależą od typu użytkownika-klienta. Typy użytkowników (nabywca lub nienabywca) można skonfigurować za pomocą interfejsu API platformy — szczegółowe informacje zawiera dokumentacja interfejsów API. Więcej informacji na temat dostępnych pozycjo czynności widocznych dla klientów zawiera poniższa tabela:

| Typ użytkowników u dzierżawcy-klienta | Czynność |
|---|---|
| Administrator, nabywca | W interfejsie użytkownika jest wyświetlany przycisk **Kup teraz***. |
| Administrator; nienabywca | W interfejsie użytkownika jest wyświetlany komunikat „Aby uaktualnić wersję, skontaktuj się z partnerem”. |
| Użytkownik; nabywca | W interfejsie użytkownika jest wyświetlany komunikat „Aby uaktualnić wersję, skontaktuj się z partnerem”. |
| Użytkownik; nienabywca | W interfejsie użytkownika jest wyświetlany komunikat „Aby uaktualnić wersję, skontaktuj się z partnerem”. |

* Łącze przycisku **Kup teraz**, które przekieruje klienta do witryny internetowej umożliwiającej wykupienie bardziej zaawansowanej wersji, można skonfigurować w sekcji **Ustawienia**> **Oznaczenie marką**. W sekcji **Sprzedaż dodatkowa** można zdefiniować opcję **Adres URL przycisków Kup**. Ustawienia oznaczenia marką zostaną zastosowane do wszystkich bezpośrednich oraz pośrednich partnerów/folderów i klientów podrzędnych dzierżawcy, u którego jest konfigurowane oznaczenie marką.

***Aby włączyć lub wyłączyć funkcję sprzedaży dodatkowej w przypadku klienta***

1. W portalu zarządzania wybierz **Klienci**.
2. Wybierz klienta, przejdź do okienka po prawej stronie, a następnie kliknij kartę **Konfiguruj**.
3. W sekcji **Sprzedaż dodatkowa** zrób tak:
   - Włącz opcję **Promuj bardziej zaawansowane wersje**, aby włączyć scenariusz sprzedaży dodatkowej dla klientów.
   - Wyłącz opcję **Promuj bardziej zaawansowane wersje**, aby wyłączyć scenariusz sprzedaży dodatkowej dla klientów.

## Pozycje sprzedaży dodatkowej widoczne dla klienta

### Lista luk w zabezpieczeniach

W konsoli usługi listę luk w zabezpieczeniach można znaleźć w sekcji **Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**. Gdy użytkownik kliknie ikonę ściegu krzyżykowego, zostanie otwarte okno dialogowe promocji z zachętą do zakupu droższej wersji.

### Tworzenie lub edytowanie planu ochrony

W konsoli usługi te ustawienia można znaleźć w sekcji **Plany** > **Ochrona**. Kliknij **Utwórz plan**. W wersjach Cyber Backup są włączone tylko moduły **Kopia zapasowa** i **Luka w zabezpieczeniach** — pozostałe moduły są dostępne tylko w wersjach Cyber Protect. Klient będzie mieć dostęp do wszystkich modułów po zakupie jednej z wersji Cyber Protect.

### Kreator wykrywania automatycznego

W konsoli usługi ten kreator można znaleźć w sekcji **Urządzenia** > **Wszystkie urządzenia**. Klient powinien uruchomić Kreator automatycznego wykrywania. W tym celu należy kliknąć **Dodaj**, a następnie przejść do sekcji **Wiele urządzeń** i kliknąć **Tylko Windows**. Metody automatycznego wykrywania komputerów będą dostępne tylko w wersjach Advanced.

### Czynności na liście urządzeń

W konsoli usługi tę listę można znaleźć w sekcji **Urządzenia** > **Wszystkie urządzenia**. Klient powinien zaznaczyć komputer, a wówczas w lewym okienku pojawią się dwie dodatkowe opcje:

- **Połącz przez klienta HTML5**
- **Zastosuj poprawkę**

Opcje te będą dostępne tylko wtedy, gdy klient kupi wersję droższą od obecnie używanej.

# Zarządzanie lokalizacjami i magazynami

W sekcji **Ustawienia** > **Lokalizacje** są wyświetlane chmury oraz infrastruktury odzyskiwania po awarii, których można użyć w celu udostępnienia partnerom i klientom usług **Cyber Protection** oraz **File Sync & Share**.

Magazyny skonfigurowane na potrzeby innych usług będą pokazywane w sekcji **Lokalizacje** w przyszłych wersjach.

## Lokalizacje

Lokalizacja to kontener, który pozwala na wygodne grupowanie magazynów w chmurze i infrastruktur odzyskiwania po awarii. Może przedstawiać dowolną rzecz, na przykład konkretne centrum danych lub lokalizację geograficzną komponentów Twojej infrastruktury.

Możesz utworzyć tyle lokalizacji, ile chcesz, i wypełnić je magazynami kopii zapasowych, infrastrukturami odzyskiwania po awarii oraz magazynami usługi **File Sync & Share**. W jednej lokalizacji może mieścić się wiele magazynów w chmurze, ale dozwolona jest tylko jedna infrastruktura odzyskiwania po awarii.

Informacje o operacjach na magazynach można znaleźć w sekcji „Zarządzanie magazynami".

## Wybór lokalizacji i magazynów dla partnerów i klientów

W przypadku tworzenia dzierżawcy-partnera / folderu można wybrać wiele lokalizacji i magazynów do każdej usługi, które będą dostępne w ramach nowego dzierżawcy.

W przypadku tworzenia dzierżawcy-klienta trzeba wybrać jedną lokalizację, a następnie jeden magazyn na usługę w obrębie tej lokalizacji. Przypisane klientowi magazyny można później zmienić, ale tylko pod warunkiem, że poziom ich wykorzystania wynosi 0 GB — czyli albo zanim klient zacznie z nich korzystać z magazynu, albo po usunięciu z nich wszystkich kopii zapasowych.

Informacje na temat magazynów przypisanych do dzierżawcy-klienta są pokazywane w panelu szczegółów dzierżawcy po wybraniu dzierżawcy na karcie **Klienci**. Informacje na temat wykorzystania miejsca w magazynie nie są aktualizowane w czasie rzeczywistym. Ich aktualizacja może potrwać do 24 godzin.

## Operacje na lokalizacjach

Aby utworzyć nową lokalizację, kliknij **Dodaj lokalizację**, a następnie określ nazwę lokalizacji.

Aby przenieść magazyn lub infrastrukturę odzyskiwania po awarii do innej lokalizacji, wybierz magazyn lub infrastrukturę, kliknij ikonę ołówka w obszarze **lokalizacja**, a następnie wybierz docelową lokalizację.

Aby zmienić nazwę lokalizacji, kliknij ikonę wielokropka obok nazwy lokalizacji, kliknij **Zmień nazwę**, a następnie wpisz nową nazwę.

Aby usunąć lokalizację, kliknij ikonę wielokropka obok nazwy lokalizacji, kliknij **Usuń**, a następnie potwierdź decyzję. Tylko puste lokalizacje mogą zostać usunięte.

# Zarządzanie magazynami

## Dodawanie nowych magazynów

- Usługa **Cyber Protection** :
  - Domyślnie magazyny kopii zapasowych znajdują się w centrach danych .
  - Jeśli pozycja oferty **Magazyn kopii zapasowych partnera** została włączona dla dzierżawcy-partnera przez administratora wyższego poziomu, administratorzy partnerów mogą zorganizować magazyn w centrum danych partnera, korzystając z oprogramowania Cyber Infrastructure. Aby znaleźć informacje na temat organizowania magazynu kopii zapasowych we własnym centrum danych, w sekcji **Lokalizacje** kliknij **Dodaj magazyn kopii zapasowych**.

- Jeśli pozycja oferty z **infrastruktury odzyskiwania po awarii partnera** została włączona dla dzierżawcy-partnera przez administratora wyższego poziomu, administratorzy partnerów mogą zorganizować infrastrukturę odzyskiwania po awarii w centrum danych partnera. Aby uzyskać informacje na temat dodawania infrastruktury odzyskiwania po awarii, skontaktuj się z zespołem pomocy technicznej.

**Uwaga**
Sprawdzanie poprawności kopii zapasowych nie jest możliwe w przypadku publicznych magazynów obiektów w chmurze, takich jak Amazon S3, Microsoft Azure, Google Cloud Storage i Wasabi, które są używane w centrach danych firmy .
Sprawdzanie poprawności kopii zapasowych jest możliwe w przypadku publicznych magazynów obiektów w chmurze partnerów firmy . Włączenie tej opcji nie jest jednak zalecane, ponieważ operacje sprawdzania poprawności zwiększają ruch wychodzący z tych publicznych magazynów obiektów i mogą powodować znaczne koszty.

- Aby uzyskać informacje na temat dodawania magazynów, z których będą korzystać inne usługi, skontaktuj się z zespołem pomocy technicznej.

## Usuwanie magazynów

Możesz usuwać magazyny dodane przez Ciebie lub Twoich dzierżawców podrzędnych.

Jeśli magazyn jest przypisany do dzierżawców-klientów, musisz wyłączyć u wszystkich właściwych dzierżawców-klientów usługę korzystającą z tego magazynu, zanim go usuniesz.

***Aby usunąć magazyn***

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, do którego dodany został magazyn.
3. Kliknij **Ustawienia** > **Lokalizacje**.
4. Wybierz magazyn, które chcesz usunąć.
5. W panelu właściwości magazynu kliknij ikonę wielokropka, a następnie kliknij **Usuń magazyn**.
6. Potwierdź decyzję.

# Konfigurowanie niezmiennego magazynu

Niezmienny magazyn można skonfigurować na poziomie partnera i na poziomie klienta.

W przypadku dzierżawców-partnerów nie ma wyboru trybów niezmiennego magazynu. Administrator może wyłączyć i ponownie włączyć niezmienny magazyn, a także zmienić jego tryb i okres przechowywania.

W przypadku dzierżawców-klientów niezmienny magazyn jest dostępny w następujących trybach:

- **Tryb nadzoru**
  W tym trybie administrator może wyłączyć i ponownie włączyć niezmienny magazyn, a także zmienić jego tryb i okres przechowywania.
- **Tryb zgodności**
  Po wybraniu tego trybu nie można już wyłączyć niezmiennego magazynu i nie można zmienić jego trybu ani okresu przechowywania.

Jeśli w przypadku dzierżawcy podrzędnego nie zostaną zastosowane żadne ustawienia niestandardowe, to odziedziczy on ustawienia skonfigurowane dla dzierżawcy nadrzędnego.

Ustawienia niezmiennego magazynu można skonfigurować tylko wtedy, gdy w przypadku dzierżawcy, do którego należy konto administratora, jest włączone uwierzytelnianie dwuskładnikowe.

Usunięte kopie zapasowe przechowywane w niezmiennym magazynie wciąż zajmują miejsce w pamięci masowej i są za nie naliczane odpowiednie opłaty.

**Uwaga**
Od wersji 21.12 w przypadku nowych dzierżawców domyślnie jest włączany niezmienny magazyn z okresem przechowywania wynoszącym 14 dni. W przypadku już istniejących dzierżawców należy ręcznie włączyć niezmienny magazyn.

***Aby włączyć niezmienny magazyn dla dzierżawcy-partnera***

1. Zaloguj się do portalu zarządzania jako administrator, a następnie wybierz **Ustawienia** > **Bezpieczeństwo**.
2. Włącz przełącznik **Niezmienny magazyn**.
3. Ustaw okres przechowywania wynoszący od 14 do 999 dni.
   Domyślny okres przechowywania to 14 dni. Dłuższy okres przechowywania danych może skutkować zajęciem większej ilości miejsca w magazynie.
4. Kliknij **Zapisz**.

***Aby wyłączyć niezmienny magazyn dla dzierżawcy-partnera***

1. Zaloguj się do portalu zarządzania jako administrator, a następnie wybierz **Ustawienia** > **Bezpieczeństwo**.
2. Wyłącz przełącznik **Niezmienny magazyn**.

   **Ostrzeżenie!**
   Ta zmiana zostanie odziedziczona przez wszystkich dzierżawców podrzędnych, którzy nie stosują niestandardowych ustawień niezmiennego magazynu. Wszystkie usunięte kopie zapasowe zostaną trwale skasowane. Trwałe też będzie usunięcie nowych kopii zapasowych.

3. Potwierdź wybór, klikając **Wyłącz**.

***Aby włączyć niezmienny magazyn dla dzierżawcy-klienta***

1. Zaloguj się do portalu zarządzania jako administrator, a następnie wybierz **Klienci**.
2. Aby edytować ustawienia dla dzierżawcy-klienta, kliknij jego nazwę.
3. W menu nawigacyjnym wybierz **Ustawienia** > **Bezpieczeństwo**.
4. Włącz przełącznik **Niezmienny magazyn**.
5. Ustaw okres przechowywania wynoszący od 14 do 999 dni.

   Domyślny okres przechowywania to 14 dni. Dłuższy okres przechowywania danych może skutkować zajęciem większej ilości miejsca w magazynie.
6. Wybierz tryb niezmiennego magazynu.

   **Ostrzeżenie!**
   Wyboru opcji **Tryb zgodności** nie można cofnąć. Nie można już wyłączyć niezmiennego magazynu i nie można zmienić jego trybu ani okresu przechowywania.

7. Kliknij **Zapisz**.

***Aby wyłączyć niezmienny magazyn dla dzierżawcy-klienta***

1. Zaloguj się do portalu zarządzania jako administrator, a następnie wybierz **Klienci**.
2. Aby edytować ustawienia dla dzierżawcy-klienta, kliknij jego nazwę.
3. W menu nawigacyjnym wybierz **Ustawienia** > **Bezpieczeństwo**.
4. Wyłącz przełącznik **Niezmienny magazyn**.

   **Uwaga**
   Niezmienny magazyn można wyłączyć tylko w trybie nadzoru.

   **Ostrzeżenie!**
   Jeśli wyłączysz niezmienny magazyn, wszystkie wykryte kopie zapasowe zostaną trwale skasowane. Trwałe też będzie usunięcie nowych kopii zapasowych.

5. Potwierdź wybór, klikając **Wyłącz**.

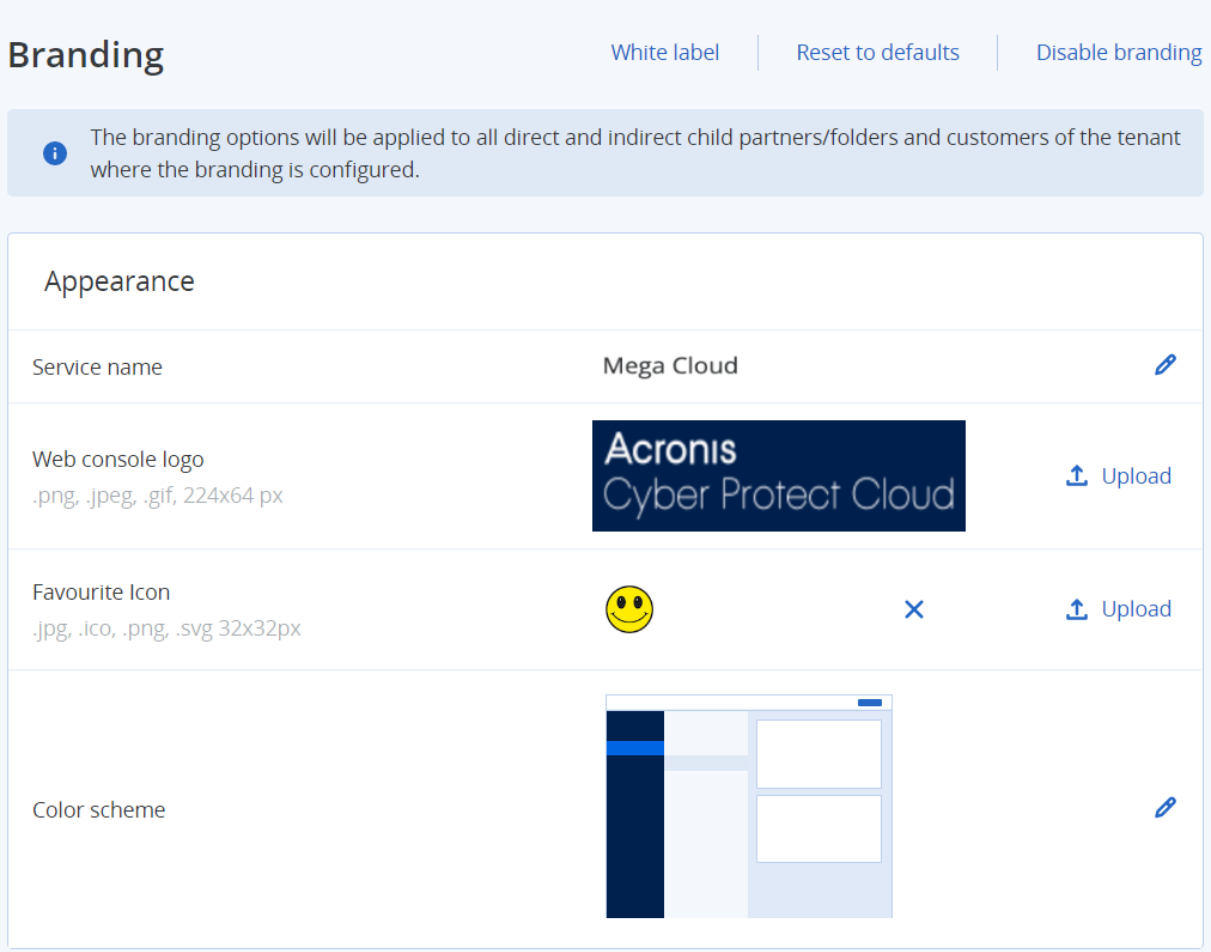
## Ograniczenia

- Niezmienny magazyn jest dostępny w przypadku magazynów hostowanych przez firmę Acronis oraz partnerów, które korzystają z rozwiązania Acronis Cyber Infrastructure w wersji 4.7.1 lub nowszej.

  Niezmienny magazyn wymaga otwarcia portu TCP 40440 na potrzeby usługi Backup Gateway dostępnej w oprogramowaniu Acronis Cyber Infrastructure. W wersji 4.7.1 lub nowszej port TCP 40440 jest automatycznie otwarty dla ruchu publicznego typu **Backup (ABGW)**. Więcej informacji o typach ruchu można znaleźć w dokumentacji rozwiązania Acronis Cyber Infrastructure.
- Niezmienny magazyn wymaga agenta ochrony w wersji 21.12 (kompilacja 15.0.28532) lub nowszej.
- Obsługiwane są tylko kopie zapasowe w formacie TIBX (Wersja 12).

# Konfigurowanie oznaczenia marką i modelu White label

Sekcja **Ustawienia** > **Oznaczenie marką** umożliwia administratorom partnerów dostosowanie interfejsu użytkownika portalu zarządzania i usługi **Cyber Protection** w celu usunięcia wszelkich powiązań z partnerami wyższych poziomów.




Oznaczenie marką można konfigurować na poziomie partnera lub folderu. Opcje oznaczenia marką są stosowane do wszystkich bezpośrednich i pośrednich partnerów/folderów i klientów podrzędnych dzierżawcy, w ramach którego oznaczenie marką jest konfigurowane.

Inne usługi udostępniają osobne opcje oznaczenia marką w swoich konsolach. Więcej informacji można znaleźć w podręcznikach użytkownika odpowiednich usług.

## Elementy oznaczenia marką

### Wygląd

- **Nazwa usługi**. Ta nazwa jest używana we wszystkich wiadomościach e-mail wysyłanych przez portal zarządzania i usługi chmurowe (dotyczących aktywacji konta, zawierających powiadomienia dotyczące usług itp.), na **ekranie powitalnym** wyświetlanym po pierwszym zalogowaniu się

użytkownika oraz jako nazwa karty portalu zarządzania w przeglądarce.

- **Logo konsoli internetowej**. Logo jest wyświetlane w portalu zarządzania i usługach. Kliknij **Prześlij**, aby przesłać plik obrazu.
- **Ikona Ulubione** [Dostępna tylko wtedy, gdy skonfigurowano niestandardowy adres URL]. Favicon ten jest wyświetlany obok tytułu strony na karcie przeglądarki. Kliknij **Prześlij**, aby przesłać plik obrazu.
- **Schemat kolorów**. Schemat kolorów określa kombinację kolorów stosowanych do wszystkich elementów interfejsu użytkownika.

**Uwaga**
Kliknij **Wyświetl podgląd schematu w nowej karcie**, aby sprawdzić, jak będzie wyglądać interfejs z perspektywy dzierżawców podrzędnych. Oznaczenie marką nie zostanie zastosowane, dopóki nie klikniesz **Gotowe** na panelu **Wybierz schemat kolorów**.

## Oznaczenie agenta i instalatora marką

Można dostosować oznaczenie marką plików instalacyjnych agenta oraz monitora na pasku zadań w przypadku systemów Windows i macOS.

**Uwaga**
Aby włączyć funkcję oznaczenia marką, trzeba zaktualizować agenty usługi Cyber Protection do wersji 15.0.28816 (wydanie 22.01) lub nowszej.

- **Nazwa pliku instalatora agenta**. Nazwa pliku instalacyjnego pobieranego na chronione obciążenia.
- **Logo instalatora agenta**. Logo wyświetlane w kreatorze instalacji podczas instalowania agenta. Kliknij **Prześlij**, aby przesłać plik obrazu.
- **Nazwa agenta**. Nazwa wyświetlana w kreatorze instalacji podczas instalowania agenta.
- **Nazwa monitora paska zadań**. Nazwa wyświetlana u góry okna monitora dostępnego na pasku zadań.

## Dokumentacja i pomoc techniczna

- **Adres URL strony głównej**. Ta strona jest otwierana, gdy użytkownik kliknie nazwę firmy w panelu **Informacje**.
- **Adres URL pomocy technicznej**. Ta strona jest otwierana, gdy użytkownik kliknie łącze **Kontakt z pomocą techniczną** w panelu **Informacje** lub w wiadomości e-mail wysłanej przez portal zarządzania.
- **Telefon do pomocy technicznej**. Ten numer telefonu jest pokazywany w panelu **Informacje**.
- **Adres URL bazy wiedzy**. Ta strona jest otwierana, gdy użytkownik kliknie łącze **Baza wiedzy** w komunikacie o błędzie.

- **Podręcznik administratora portalu zarządzania**. Ta strona jest otwierana, gdy użytkownik kliknie ikonę znaku zapytania widoczną w prawym górnym rogu interfejsu użytkownika portalu zarządzania, a następnie kliknie **Informacje** > **Podręcznik administratora**.
- **Pomoc dla administratora portalu zarządzania**. Ta strona jest otwierana, gdy użytkownik kliknie ikonę znaku zapytania widoczną w prawym górnym rogu interfejsu użytkownika portalu zarządzania, a następnie kliknie **Pomoc**.

## Adres URL usług Cyber Protect Cloud

Można skonfigurować usługi Cyber Protect Cloud tak, aby były dostępne z niestandardowej domeny. Kliknij **Konfiguruj**, aby ustawić niestandardowy adres URL po raz pierwszy, lub kliknij **Zmień konfigurację**, aby zmienić dotychczasowy adres. Aby użyć domyślnego adresu URL (https://cloud.acronis.com), kliknij **Przywróć domyślne**. Dodatkowe informacje na temat niestandardowych adresów URL można znaleźć w sekcji „Konfigurowanie niestandardowych adresów URL interfejsu internetowego".

## Ustawienia dokumentów prawnych

- **Adres URL Umowy licencyjnej użytkownika oprogramowania**. Ta strona jest otwierana, gdy użytkownik kliknie łącze **Umowa licencyjna użytkownika oprogramowania** w panelu **Informacje** lub na **ekranie powitalnym** po pierwszym zalogowaniu się i na stronach docelowych żądań przesłania w ramach usługi File Sync & Share.
- **Adres URL warunków platformy**. Ta strona jest otwierana, gdy administrator partnera kliknie łącze **Adres URL warunków platformy** w panelu **Informacje** lub na **ekranie powitalnym** po pierwszym zalogowaniu się.
- **Adres URL Zasad zachowania prywatności**. Ta strona jest otwierana, gdy użytkownik kliknie łącze **Zasady zachowania prywatności** na **ekranie powitalnym** po pierwszym zalogowaniu się i na stronach docelowych żądań przesłania w ramach usługi File Sync & Share.

**Ważne**
Jeśli nie chcesz, aby dokument był wyświetlany na ekranie powitalnym, nie wprowadzaj adresu URL tego dokumentu.

**Uwaga**
Więcej informacji na temat żądań przesłania w ramach usługi File Sync & Share można znaleźć w Podręczniku użytkownika programu Cyber Files Cloud.

## Sprzedaż dodatkowa

- **Adres URL przycisków Kup**. Ta strona jest otwierana, gdy użytkownik kliknie **Kup teraz** w celu przejścia na bardziej zaawansowaną wersję usługi Cyber Protection. Więcej informacji na temat scenariuszy sprzedaży dodatkowej można znaleźć w sekcji „Konfigurowanie scenariuszy sprzedaży dodatkowej dla klientów".

## Aplikacje mobilne

- **App Store**. Ta strona jest otwierana, gdy użytkownik kliknie **Dodaj** > **iOS** w usłudze **Cyber Protection**.
- **Google Play**. Ta strona jest otwierana, gdy użytkownik kliknie **Dodaj** > **Android** w usłudze **Cyber Protection**.

## Ustawienia serwera e-mail

Można określić niestandardowy serwer e-mail, który będzie używany do wysyłania powiadomień e-mail z portalu zarządzania oraz usług. Aby określić niestandardowy serwer e-mail, kliknij **Dostosuj**, a następnie określ następujące ustawienia:

- W polu **Od** wprowadź imię i nazwisko bądź nazwę, które będą widoczne w polu **Od** w powiadomieniach e-mail.
- W polu **SMTP** wprowadź nazwę serwera poczty wychodzącej (SMTP).
- W polu **Port** wprowadź port serwera poczty wychodzącej. Domyślnie jest to port 25.
- W polu **Szyfrowanie** wybierz, czy chcesz stosować szyfrowanie SSL, czy TLS. Wybierz **Brak**, aby wyłączyć szyfrowanie.
- W polach **Nazwa użytkownika** i **Hasło** określ poświadczenia konta, które będzie używane do wysyłania wiadomości.

# Konfiguracja oznaczenia marką

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz skonfigurować oznaczenie marką.
3. Kliknij **Ustawienia** > **Oznaczenie marką**.
4. [Jeśli oznaczenie marką nie zostało jeszcze włączone] Kliknij **Włącz oznaczenie marką**.
5. Skonfiguruj opisane wcześniej elementy oznaczenia marką.

# Przywracanie domyślnych ustawień oznaczenia marką

Istnieje możliwość zresetowania wszystkich elementów oznaczenia marką do wartości domyślnych.

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz zresetować oznaczenie marką.
3. Kliknij **Ustawienia** > **Oznaczenie marką**.
4. W prawym górnym rogu kliknij **Przywróć ustawienia domyślne**.

# Wyłączanie oznaczenia marką

Można wyłączyć oznaczenie marką dla konta i wszystkich dzierżawców podrzędnych.

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz wyłączyć oznaczenie marką.
3. Kliknij **Ustawienia** > **Oznaczenie marką**.
4. W prawym górnym rogu kliknij **Wyłącz oznaczenie marką**.

## Model White label

Można określić, czy agent usługi Cyber Protection (dla systemu Windows, macOS i Linux) oraz narzędzie Cyber Protection Monitor (dla systemu Windows, macOS i Linux) będą miały oznaczenie marką, czy będą udostępniane w modelu White label dla wszystkich partnerów podrzędnych i klientów. W przypadku włączenia modelu White label agent i monitor na pasku zadań będą udostępniane bez oznaczenia marką dostawcy. Ustawienie to wpłynie również na nazwy i logo pokazywane w instalatorze oraz narzędziu Cyber Protection Monitor.

### Stosowanie modelu White label

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz zastosować model White label.
3. Kliknij **Ustawienia** > **Oznaczenie marką**.
4. W prawym górnym rogu kliknij **White label**, aby wyczyścić wszystkie elementy oznaczenia marką, z wyjątkiem następujących: **Nazwa usługi**, **Adres URL Umowy licencyjnej użytkownika oprogramowania**, **Podręcznik administratora portalu zarządzania**, **Pomoc dla administratora portalu zarządzania** oraz **Ustawienia serwera e-mail**.

# Konfigurowanie niestandardowych adresów URL interfejsu internetowego

**Uwaga**
Niestandardowy adres URL będzie wskazywał na inny adres IP niż domyślny adres URL. Należy o tym pamiętać podczas konfigurowania zasad zapory.

***Aby skonfigurować adres URL interfejsu internetowego usług Cyber Protect Cloud***

1. W portalu zarządzania kliknij **Ustawienia** > **Oznaczenie marką**.
2. W sekcji **Adres URL usług Cyber Protect Cloud**:
   - Kliknij **Konfiguruj**, aby ustawić niestandardowy adres URL po raz pierwszy.
   - Kliknij **Zmień konfigurację**, aby zmienić dotychczasowy niestandardowy adres.
3. W ramach kroku **Ustawienia domeny** przygotuj domenę i rekord CNAME.
   Aby użyć niestandardowego adresu URL, trzeba mieć aktywną nazwę domeny i rekord CNAME skonfigurowany tak, aby wskazywał na centrum danych, w którym znajduje się konto.

Konfiguracja rekordu CNAME jest wykonywana przez rejestrator DNS, a jej propagacja może potrwać do 48 godzin.

Aby odszukać nazwę domeny centrum danych i poprosić o konfigurację rekordu CNAME, zapoznaj się z artykułem Oznaczenie marką w adresie URL konsoli internetowej (58275).

4. W ramach kroku **Sprawdź swój adres URL** sprawdź, czy Twój niestandardowy adres URL jest dostępny i czy rekord CNAME jest poprawnie skonfigurowany. W tym celu wprowadź nazwę głównego adresu URL i kliknij **Sprawdź**. Jeśli korzystasz z wieloznacznego certyfikatu SSL, możesz dodać do dziesięciu alternatywnych nazw domen. Jeśli korzystasz z certyfikatu „Let's Encrypt", alternatywne nazwy domen będą ignorowane.
5. W ramach kroku **Certyfikat SSL** możesz wykonać jedną z następujących czynności:
   - Utwórz certyfikat „Let's Encrypt". W tym celu kliknij **Bezpłatny certyfikat SSL dzięki „Let's Encrypt"**. W tym przypadku są używane certyfikaty „Let's Encrypt" wydane przez podmiot zewnętrzny. Dostawca usługi nie odpowiada za żadne problemy wynikające z używania tych bezpłatnych certyfikatów. Dodatkowe informacje na temat regulaminu użytkowania certyfikatów „Let's Encrypt" można znaleźć na stronie https://letsencrypt.org/repository/.
   - Prześlij certyfikat wieloznaczny. W tym celu kliknij **Prześlij certyfikat wieloznaczny**, a następnie udostępnij certyfikat wieloznaczny i klucz prywatny.
6. Kliknij **Prześlij**, aby zastosować zmiany.

***Aby zresetować niestandardowy URL do wartości domyślnej***

1. W portalu zarządzania kliknij **Ustawienia** > **Oznaczenie marką**.
2. W sekcji **Adres URL usług Acronis Cyber Protect Cloud** kliknij **Przywróć domyślne**, aby użyć domyślnego adresu URL (https://cloud.acronis.com).

# Automatyczne aktualizowanie agentów

Usługa Cyber Protect udostępnia trzy typy agentów do instalowania na chronionych komputerach: agent dla systemu Windows, agent dla systemu Linux i agent dla system Mac.

Program Cyber Files Cloud udostępnia agenta komputerowego dla File Sync & Share w wersji dla systemu Windows i w wersji dla systemu MacOS. Umożliwia on synchronizację plików i folderów między komputerem a magazynem w chmurze File Sync & Share użytkownika na potrzeby promowania pracy offline, a także pracy z domu i używania do pracy własnych urządzeń (BYOD, Bring Your Own Device).

Aby ułatwić zarządzanie wieloma obciążeniami, można skonfigurować (i wyłączyć) automatyczne, nienadzorowane aktualizacje dla wszystkich agentów na wszystkich komputerach.

**Ważne**
Obecnie tylko partnerzy i klienci z włączonym składnikiem Ochrona mają dostęp do funkcji zarządzania aktualizacjami agentów.

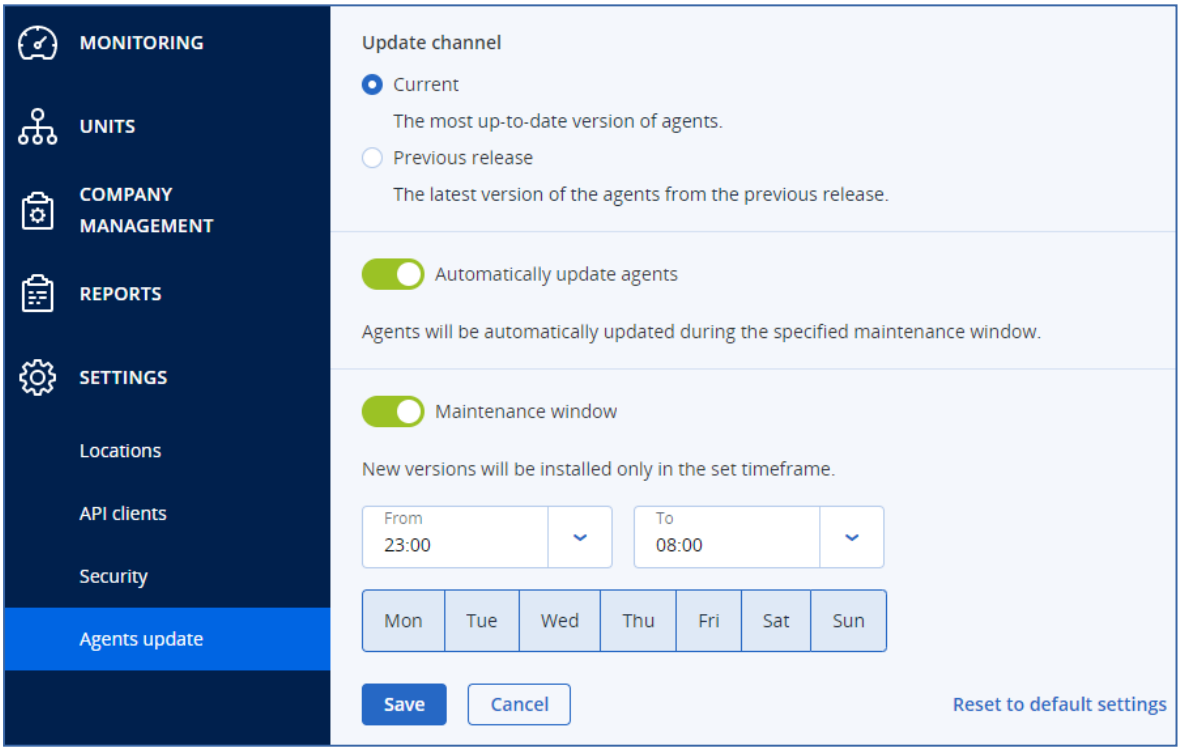
**Uwaga**
Aby zarządzać agentami na poszczególnych komputerach i dostosować ustawienia automatycznego aktualizowania, zapoznaj się z sekcją Podręcznika użytkownika usługi Cyber Protect dotyczącą aktualizacji agentów.

## Aby automatycznie aktualizować agentów

**Uwaga**
Ustawienia automatycznego aktualizowania agenta dla File Sync & Share są dziedziczone przez partnerów i klientów, którzy nie mają włączonej ochrony.

***Aby skonfigurować automatyczne aktualizowanie agentów na stronie początkowej portalu zarządzania***

1. Wybierz **Ustawienia > Aktualizacja agentów**.




2. Wybierz wersję do wykrywania pod kątem aktualizacji automatycznych: **Bieżąca** lub **Poprzednia wersja**.
   (Ustawienie domyślne to **Bieżąca**).
3. Włącz opcję **Automatycznie aktualizuj agenty**.
   (Domyślnie jest ona **włączona**).
4. Ustaw ramy czasowe konserwacji.
   (Ustawienie domyślne to: od 23:00 do 08:00).

**Uwaga**
Mimo że procesy aktualizacji agentów zaprojektowano tak, aby były one szybkie i bezproblemowe, zalecamy wybranie takiego przedziału czasowego, w którym zakłócenia dla użytkowników będą minimalne, ponieważ użytkownicy nie mogą zapobiegać stosowaniu aktualizacji automatycznych ani ich odkładać.

5. [Opcjonalnie] Wybierz określone dni, w których mają być stosowane aktualizacje automatyczne.
6. Wybierz **Zapisz.**

**Uwaga**
Aktualizacje automatyczne są dostępne tylko dla:

- Agentów usługi Cyber Protect w wersji 15.0.26986 (wydanej w maju 2021 r.) lub nowszej.
- Agenta komputerowego dla File Sync & Share w wersji 15.0.30370 lub nowszej.

Aby aktualizacje automatyczne zaczęły działać, starsze agenty trzeba najpierw ręcznie zaktualizować do najnowszej wersji.

## Aby monitorować aktualizacje agentów

**Ważne**
Aktualizacje agentów mogą monitorować tylko administratorzy partnerów i klientów, którzy mają włączony moduł Ochrona.

Aby monitorować aktualizacje agentów, zapoznaj się z sekcjami dotyczącymi alertów i działań w Podręczniku użytkownika usługi Cyber Protect.

# Monitorowanie

Aby uzyskać dostęp do informacji o wykorzystaniu usług i operacjach, kliknij **Monitorowanie**.

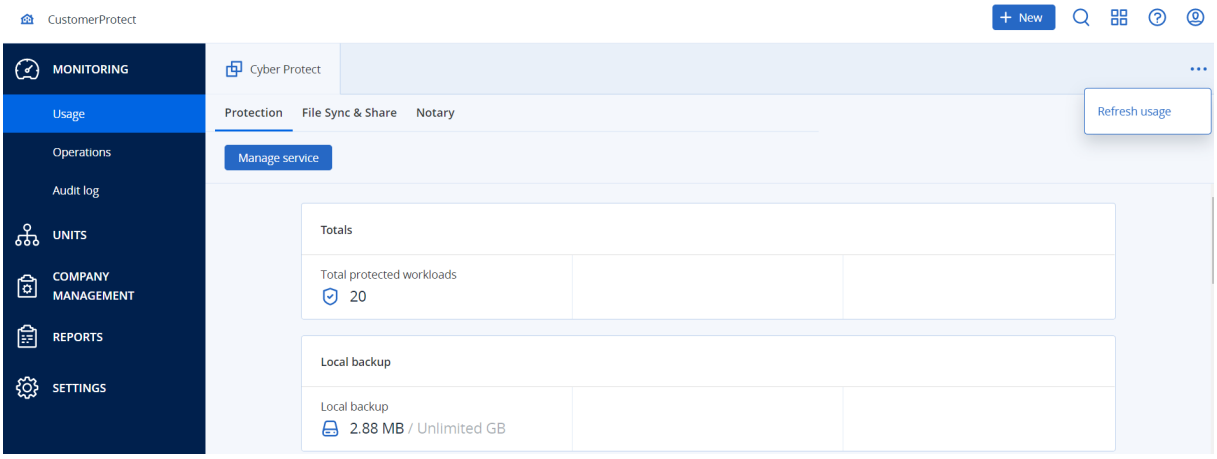
## dysku

Karta **Wykorzystanie** udostępnia zestawienie informacji o wykorzystaniu usług oraz umożliwia uzyskanie dostępu do usług w obszarze dzierżawcy, w ramach którego działasz.

Dane o wykorzystaniu obejmują zarówno standardowo udostępniane funkcje, jak i funkcje zaawansowane.

Aby odświeżyć dane o wykorzystaniu wyświetlane na karcie, kliknij ikonę wielokropka w prawym górnym rogu ekranu i wybierz **Odśwież dane o wykorzystaniu**.

**Uwaga**
Pobieranie danych może potrwać do 10 minut. Odśwież stronę, aby wyświetlić zaktualizowane dane.




# Operacje

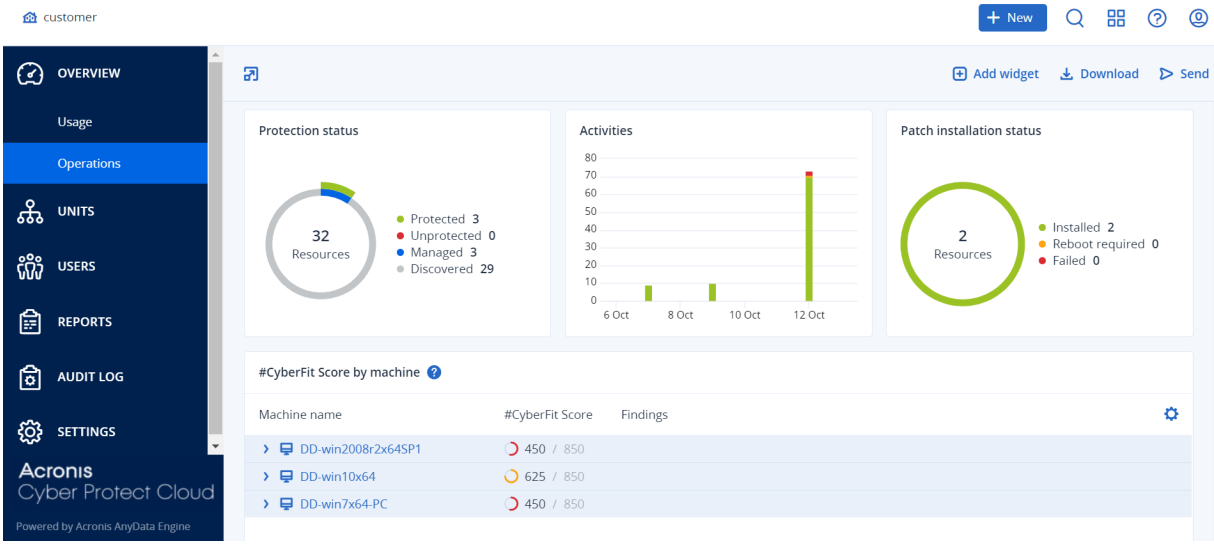
Pulpit nawigacyjny **Operacje** udostępnia szereg dostosowywalnych widżetów zapewniających ogólny obraz operacji związanych z usługą Cyber Protection. Widżety dla pozostałych usług będą dostępne w przyszłych wersjach.

Domyślnie wyświetlane są dane dzierżawcy, w ramach którego działasz. Możesz zmienić dzierżawcę wyświetlanego w danym widżecie, edytując ten widżet. Wyświetlane są również informacje zbiorcze o dzierżawcach-klientach będących bezpośrednimi elementami podrzędnymi wybranego dzierżawcy, w tym o dzierżawcach-klientach znajdujących się w folderach. Na pulpicie nawigacyjnym *nie są* wyświetlane informacje o partnerach podrzędnych oraz ich dzierżawcach podrzędnych. Aby zobaczyć pulpit danego partnera, konieczne jest przejście na jego poziom. Jednak jeśli przekonwertujesz dzierżawcę podrzędnego na dzierżawcę-folder, informacje o klientach podrzędnych tego dzierżawcy pojawią się na pulpicie nawigacyjnym dzierżawcy podrzędnego.

Widżety są aktualizowane co 2 minuty. Widżety mają klikalne elementy, które pozwalają badać i rozwiązywać problemy. Możesz pobrać bieżący stan pulpitu nawigacyjnego lub przesłać go za pomocą poczty e-mail na dowolny adres (w tym do odbiorców zewnętrznych)w formacie .pdf oraz/lub .xlsx.

Możesz wybierać spośród różnorodnych widżetów przedstawianych w formie tabel, wykresów kołowych, wykresów słupkowych, list i map drzew. Możesz dodać wiele widżetów tego samego typu

dla różnych dzierżawców lub z różnymi filtrami.




***Aby zmienić ustawienie widżetów na pulpicie nawigacyjnym***

Klikaj nazwy widżetów i zmieniaj ich ustawienie metodą „przeciągnij i upuść”.

***Aby edytować widżet***

Kliknij ikonę ołówka obok nazwy widżetu. Edycja widżetu pozwala zmienić jego nazwę, zmodyfikować zakres czasu, wybrać dzierżawcę, którego dane mają być wyświetlane, i ustawić filtry.

***Aby dodać widżet***

Kliknij **Dodaj widżet** i wykonaj jedną z następujących czynności:

- Kliknij widżet, który chcesz dodać. Widżet zostanie dodany z domyślnymi ustawieniami.
- Aby edytować widżet przed dodaniem, wybierz widżet i kliknij ikonę koła zębatego. Po skończonej edycji widżetu kliknij **Gotowe**.

***Aby usunąć widżet***

Kliknij symbol X obok nazwy widżetu.

# Status ochrony

## Status ochrony

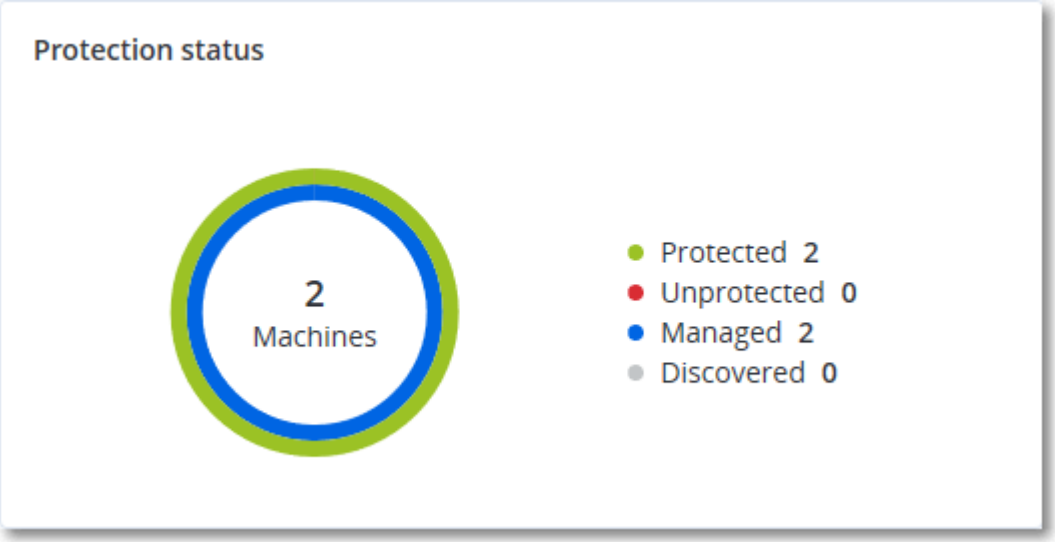
Ten widżet umożliwia wyświetlenie aktualnego statusu ochrony wszystkich komputerów.

Komputer może mieć jeden z następujących statusów:

- **Chronione** — komputery z zastosowanym planem ochrony.
- **Niechronione** — komputery bez zastosowanego planu ochrony. Są to zarówno wykryte, jak i zarządzane komputery, do których nie zastosowano planu ochrony.

- **Zarządzane** — komputery z zainstalowanym agentem ochrony.
- **Wykryto** — komputery bez zainstalowanego agenta ochrony.

Kliknięcie statusu komputera spowoduje przejście do listy komputerów o danym statusie, gdzie można znaleźć dodatkowe informacje.




## Wykryte komputery

Ten widżet przedstawia listę komputerów wykrytych we wskazanym okresie.

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 |

## Wynik #CyberFit według komputerów

W przypadku tego widżetu jest pokazywany łączny wynik #CyberFit, jego wyniki składowe oraz diagnozy z badań poszczególnych wskaźników:

- Ochrona antywirusowa
- Kopia zapasowa
- Zapora
- VPN
- Szyfrowanie
- Ruch NTLM

Aby poprawić wartości poszczególnych wskaźników, zapoznaj się z zaleceniami przedstawionymi w raporcie.

Więcej informacji na temat wyniku #CyberFit można znaleźć w sekcji „Wyniki #CyberFit komputerów".

#CyberFit Score by machine

| 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 ... |

## Widżety pakietu Endpoint Detection and Response (EDR)

**Ważne**
Niniejsza wersja dokumentacji pakietu EDR jest udostępniana w ramach Programu wczesnego dostępu. Niektóre zestawienia funkcji i opisy mogą być niekompletne.

Endpoint Detection and Response (EDR) obejmuje szereg widżetów dostępnych z pulpitu nawigacyjnego **Operacje**.

Dostępne są następujące widżety:

- Podział najliczniejszych incydentów według obciążeń
- Średni czas rozwiązywania problemu incydentu
- Wykres spalania dotyczący incydentów bezpieczeństwa
- Status sieciowy obciążeń

### Podział najliczniejszych incydentów według obciążeń

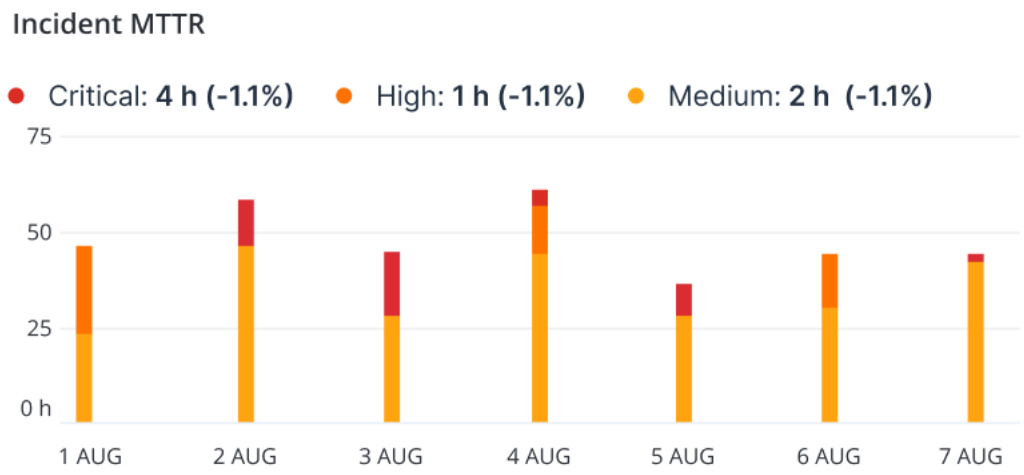
Ten widżet przedstawia pięć obciążeń z największą liczbą incydentów (kliknij **Pokaż wszystko**, aby przejść do listy incydentów przefiltrowanej zgodnie z ustawieniami widżetu).

Zatrzymaj wskaźnik myszy na wierszu z obciążeniem, aby wyświetlić podział bieżącego stanu dochodzenia poszczególnych incydentów. Stany dochodzenia to **Nie uruchomiono**, **Trwa dochodzenie**, **Zamknięto** i **Fałszywe zgłoszenie**. Następnie kliknij obciążenie, które chcesz poddać dalszym analizom, i w wyświetlonym wyskakującym okienku wybierz odpowiedniego klienta. Lista incydentów jest odświeżana zgodnie z ustawieniami widżetu.


## Średni czas rozwiązywania problemu incydentu

Na tym widżecie jest przedstawiany średni czas rozwiązywania problemu związanego z incydentem bezpieczeństwa. Wskazuje on, jak szybko problemy incydentów są badane w ramach dochodzenia i rozwiązywane.

Kliknij kolumnę, aby wyświetlić podział incydentów według ich ważności (**Krytyczny**, **Wysoki** i **Średni**) oraz wskazanie, ile czasu zajęło rozwiązanie problemu o różnym poziomie ważności. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.

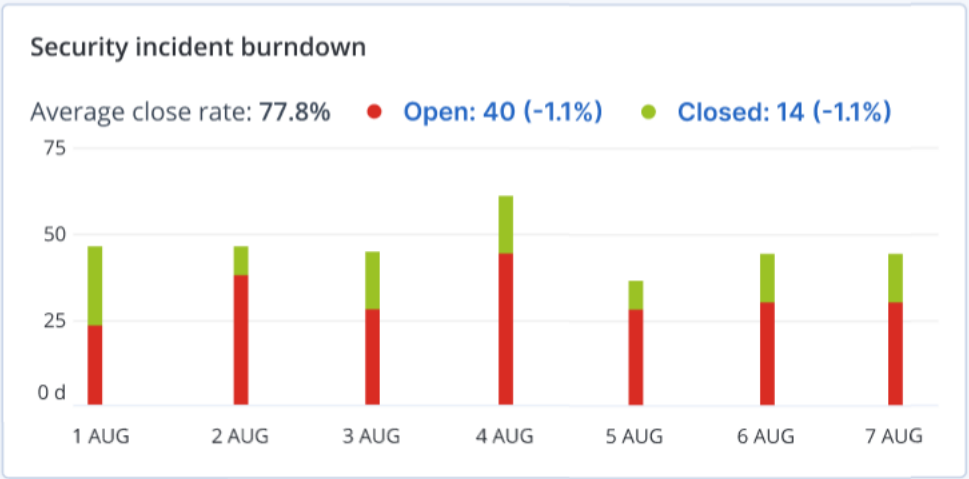



## Wykres spalania dotyczący incydentów bezpieczeństwa

Ten widżet przedstawia wskaźnik efektywności zamykania incydentów. Liczba otwartych incydentów jest ujmowana w stosunku do liczby zamkniętych incydentów w danym okresie.

Zatrzymaj wskaźnik myszy na dowolnej kolumnie, aby wyświetlić podział zamkniętych i otwartych incydentów z wybranego dnia. Kliknięcie wartości Otwarte powoduje wyświetlenie wyskakującego okienka, w którym należy wybrać odpowiedniego dzierżawcę. W celu wyświetlenia aktualnie otwartych incydentów (mających stan **Trwa dochodzenie** lub **Nie uruchomiono**) zostanie wyświetlona przefiltrowana lista incydentów dotyczących wybranego dzierżawcy. Jeśli klikniesz wartość Zamknięto, zostanie wyświetlona lista incydentów dotyczących wybranego dzierżawcy i przefiltrowana w celu wyświetlenia incydentów, które nie są już otwarte (mających stan **Zamknięto** lub **Fałszywe zgłoszenie**).

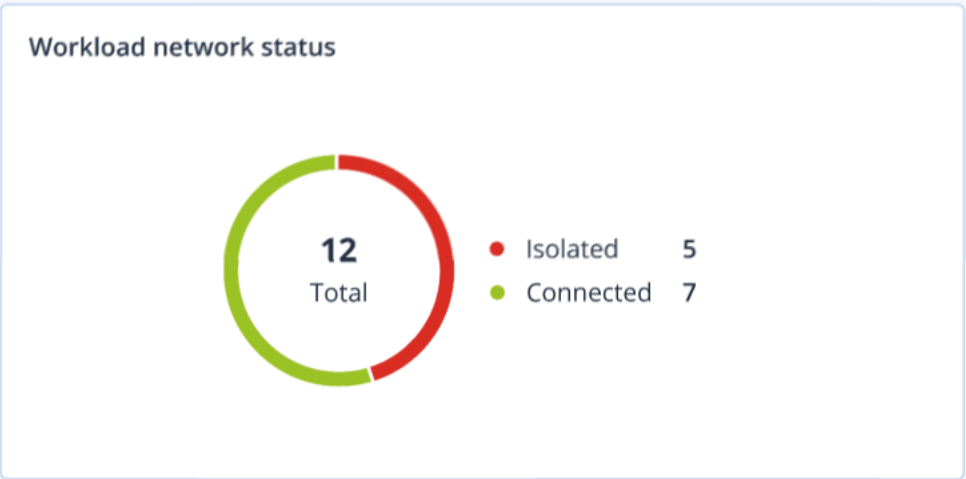
Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.




## Status sieciowy obciążeń

Ten widżet przedstawia bieżący status sieciowy obciążeń oraz wskazuje, ile obciążeń jest odizolowanych i ile połączonych.

Kliknięcie wartości Izolowano powoduje wyświetlenie wyskakującego okienka, w którym należy wybrać odpowiedniego dzierżawcę. Wyświetlony widok obciążeń zostanie przefiltrowany w celu wyświetlenia odizolowanych obciążeń. Kliknij wartość Podłączono, aby wyświetlić listę obciążeń z agentami przefiltrowaną w celu wyświetlenia połączonych obciążeń (w kontekście wybranego dzierżawcy).



## Monitorowanie kondycji dysków

Monitorowanie kondycji dysków dostarcza informacji o bieżącej kondycji dysku i prognozach na jej temat, dzięki czemu można zapobiec utracie danych, do której mogłoby dojść wskutek awarii dysku. Obsługiwane są zarówno dyski HDD, jak i dyski SSD.

### Ograniczenia

- Prognoza kondycji dysków jest obsługiwana tylko w przypadku komputerów z systemem Windows.
- Monitorowane są tylko dyski komputerów fizycznych. Dyski maszyn wirtualnych nie mogą być monitorowane ani pokazywane na widżetach kondycji dysków.
- Konfiguracje macierzy RAID nie są obsługiwane.
- W przypadku dysków NVMe monitorowanie kondycji dysków jest obsługiwane tylko w przypadku dysków, które przekazują dane SMART za pośrednictwem interfejsu API systemu Windows. Monitorowanie kondycji dysków nie jest obsługiwane w przypadku dysków NVMe, które wymagają odczytu danych SMART bezpośrednio z dysku.

Kondycja dysku może być odzwierciedlana przez jeden z następujących statusów:

- **OK**
  Kondycja dysku w zakresie 70–100%.
- **Ostrzeżenie**
  Kondycja dysku w zakresie 30–70%.
- **Krytyczne**
  Kondycja dysku w zakresie 0–30%.
- **Obliczanie danych dysku**
  Trwa obliczanie aktualnego statusu dysku i generowanie prognozy.

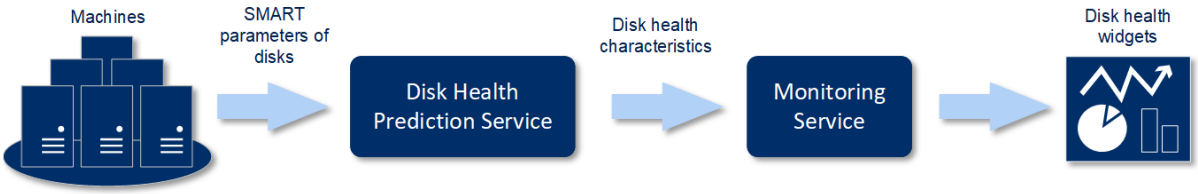
### Sposób działania

Usługa Prognoza kondycji dysków korzysta z modelu predykcyjnego opartego na sztucznej inteligencji.

1. Agent ochrony zbiera parametry SMART dysków i przekazuje te dane do usługi Prognoza kondycji dysków:
   - SMART 5 — liczba ponownie alokowanych sektorów.
   - SMART 9 — liczba godzin w stanie zasilania.
   - SMART 187 — zgłoszone nienaprawialne błędy.
   - SMART 188 — przekroczony limit czasu wykonywania polecenia.
   - SMART 197 — liczba oczekujących sektorów.
   - SMART 198 — liczba nienaprawialnych sektorów w trybie offline.
   - SMART 200 — wskaźnik błędów zapisu.

2. Usługa Prognoza kondycji dysków przetwarza uzyskane parametry SMART, sporządza prognozy i udostępnia następujące charakterystyki kondycji dysków:
   - Bieżący stan dysku: OK, Ostrzeżenie, Krytyczne.
   - Prognoza kondycji dysków: negatywna, stabilna, pozytywna.
   - Prawdopodobieństwo prognozy kondycji dysku w procentach.

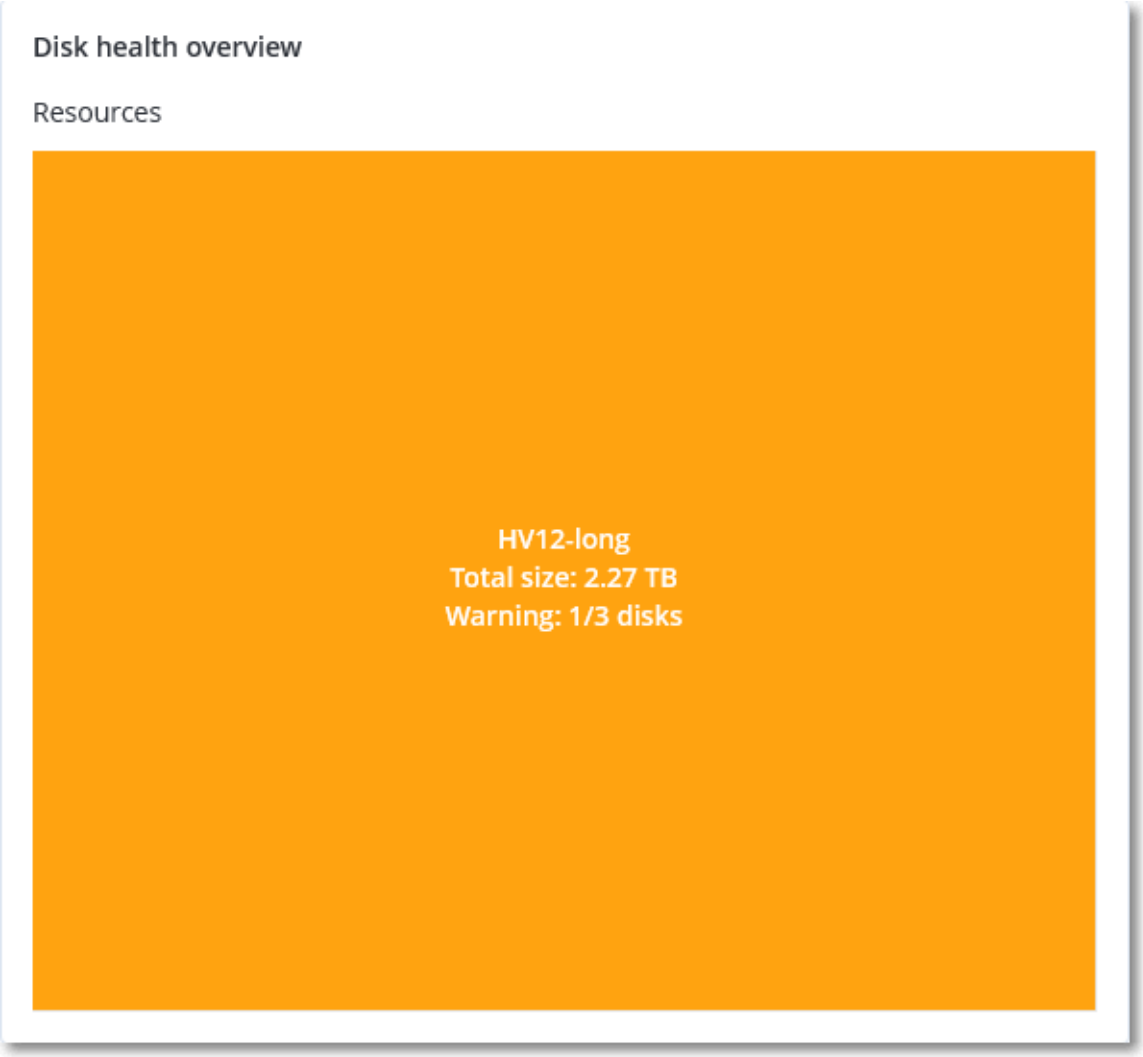
   Prognoza obejmuje okres najbliższego miesiąca.
3. Usługa monitorowania odbiera te właściwości, a następnie wyświetla odpowiednie informacje na widżetach kondycji dysków w konsoli usługi.




## Widżety kondycji dysków

Wyniki monitorowania kondycji dysków są prezentowane na następujących widżetach dostępnych w konsoli usługi.

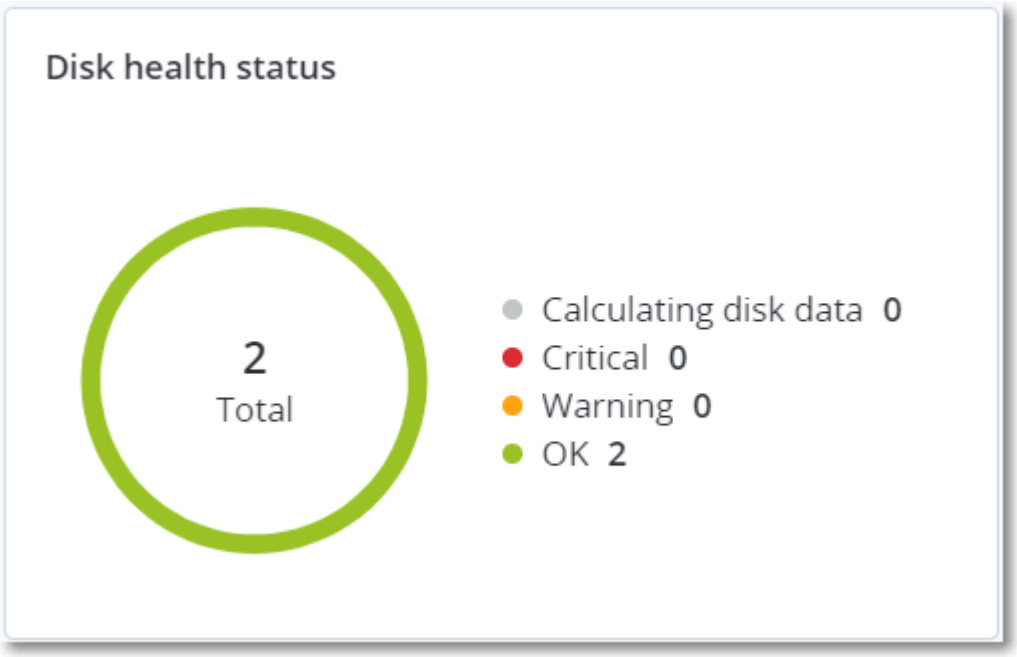
- **Przegląd kondycji dysków** — widżet w formie mapy drzewa obejmującej dwa poziomy szczegółów, które można zmieniać przez pogłębianie analizy.
  - Poziom komputera
    Zawiera podsumowanie statusów kondycji dysków wybranych komputerów klientów. Widoczny jest tylko najbardziej krytyczny status dysku. Pozostałe statusy są pokazywane na etykietce wyświetlanej po wskazaniu danego bloku myszą. Rozmiar bloku komputera zależy od łącznego rozmiaru dysków tego komputera. Kolor bloku komputera zależy od najbardziej krytycznego wykrytego statusu dysku.




- Poziom dysku
  Zawiera aktualne statusy kondycji wszystkich dysków wybranego komputera. Każdy blok dysków zawiera jedną z następujących prognoz kondycji dysków wraz z jej prawdopodobieństwem wyrażonym w procentach:
  - Ulegnie pogorszeniu
  - Pozostanie stabilne

- Ulegnie poprawie


- **Status kondycji dysków** — widżet w postaci wykresu kołowego przedstawiający liczby dysków według poszczególnych statusów.



### Alerty dotyczące statusów kondycji dysków

Kondycja dysku jest sprawdzana co 30 minut, a raz dziennie jest generowany odpowiedni alert. Gdy kondycja dysku zmieni się z **Ostrzeżenie** na **Krytyczne**, zawsze zostanie wygenerowany alert.

| Nazwa alertu | Ważność | Status kondycji dysków | Opis |
|---|---|---|---|
| Możliwość awarii dysku | Ostrzeżenie | (30 – 70) | Dysk <nazwa dysku> komputera prawdopodobnie ulegnie awarii. Jak najszybciej utwórz pełną kopię zapasową obrazu dysku, wymień go, a następnie odzyskaj obraz na nowy dysk. |
| Bliska awaria dysku | Krytyczny | (0 – 30) | Dysk <nazwa dysku> komputera jest w stanie krytycznym i najprawdopodobniej bardzo szybko ulegnie awarii. Nie zaleca się utworzenia kopii zapasowej obrazu tego dysku, ponieważ dodatkowe obciążenie może spowodować jego awarię. Niezwłocznie utwórz kopię zapasową wszystkich najważniejszych plików z tego dysku i go wymień. |

## Mapa ochrony danych

Funkcja mapy ochrony danych pozwala na sprawdzenie wszystkich ważnych danych i uzyskanie szczegółowych informacji o liczbie, rozmiarze, lokalizacji oraz statusach ochrony wszystkich ważnych plików w skalowalnym widoku mapy drzewa.

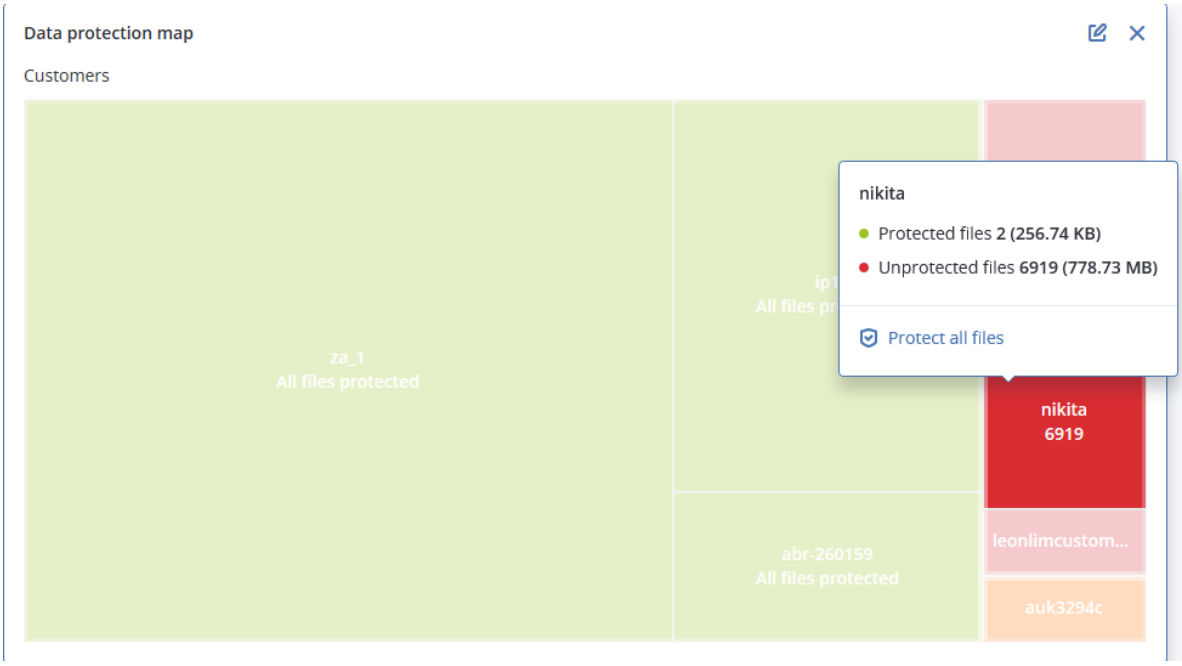
Każdy rozmiar bloku zależy od łącznej liczby lub łącznego rozmiaru wszystkich ważnych plików klienta bądź komputera.

Pliki mogą mieć jeden z następujących statusów ochrony:

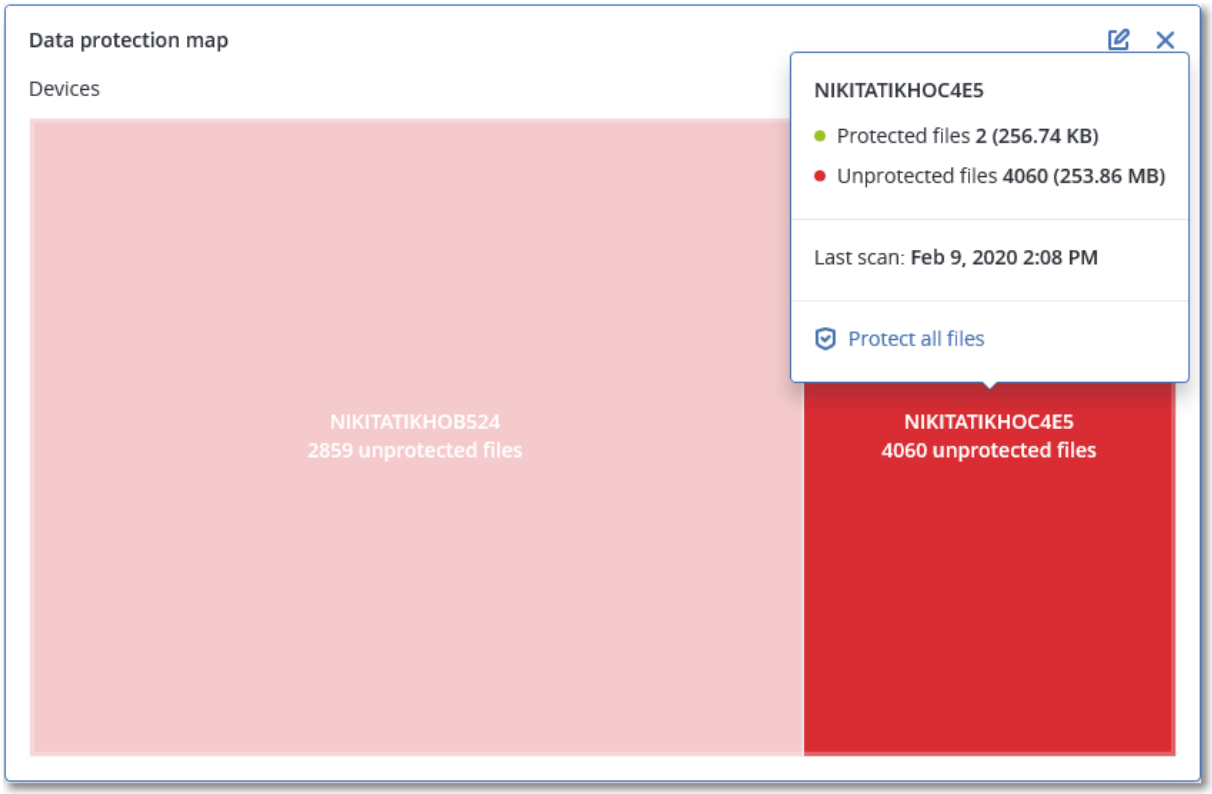
- **Krytyczny** — 51–100% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych wybranego dzierżawcy-klienta, wybranego komputera lub wybranej lokalizacji.
- **Niski** — 21–50% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych wybranego dzierżawcy-klienta, wybranego komputera lub wybranej lokalizacji.
- **Średni** — istnieje 1–20% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych wybranego dzierżawcy-klienta, wybranego komputera lub wybranej lokalizacji.
- **Wysoki** — wszystkie pliki z podanymi rozszerzeniami są chronione (uwzględniane w kopiach zapasowych) w przypadku wybranego dzierżawcy-klienta, wybranego komputera lub wybranej lokalizacji.

Wyniki kontroli ochrony danych można znaleźć na pulpicie nawigacyjnym w widżecie Mapa ochrony danych — jest to mapa drzewa obejmująca dwa poziomy szczegółów, które można zmieniać przez kliknięcie poziomu hierarchii:

- Poziom dzierżawcy-klienta — zawiera podsumowanie statusów ochrony ważnych plików wybranych klientów.




- Poziom komputera — zawiera informacje o statusach ochrony ważnych plików na poszczególnych komputerach wybranego klienta.



Aby zacząć chronić niechronione pliki, zatrzymaj wskaźnik myszy na bloku i kliknij **Chroń wszystkie pliki**. W tym oknie dialogowym znajdziesz informacje o liczbie niechronionych plików i ich lokalizacjach. Aby objąć te pliki ochroną, kliknij **Chroń wszystkie pliki**.

Możesz też pobrać szczegółowy raport w formacie CSV.

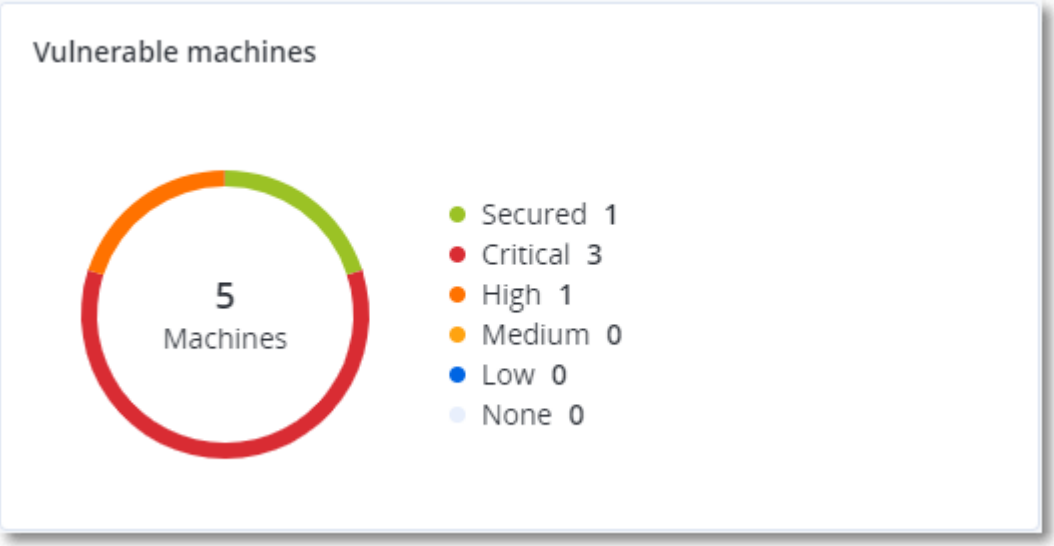
## Widżety dotyczące oceny luk w zabezpieczeniach

### Komputery z lukami w zabezpieczeniach

Ten widżet przedstawia komputery z lukami w zabezpieczeniach uporządkowane według ważności luk.

Znaleziona luka może mieć jeden z następujących poziomów ważności określony zgodnie z systemem Common Vulnerability Scoring System (CVSS) w wersji 3.0:

- Bezpieczny: nie znaleziono luk w zabezpieczeniach
- Krytyczny: 9,0–10,0 w skali CVSS
- Wysoki: 7,0–8,9 w skali CVSS
- Średni: 4,0–6,9 w skali CVSS
- Niski: 0,1–3,9 w skali CVSS
- Brak: 0,0 w skali CVSS




### Występujące luki w zabezpieczeniach

Ten widżet przedstawia obecnie występujące luki w zabezpieczeniach na komputerach. W widżecie **Istniejące luki w zabezpieczeniach** są dostępne dwie kolumny z sygnaturami czasowymi:

- **Pierwsze wykrycie** — data i godzina pierwszego wykrycia luki na komputerze.
- **Ostatnie wykrycie** — data i godzina ostatniego wykrycia luki na komputerze.

Existing vulnerabilities

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

More

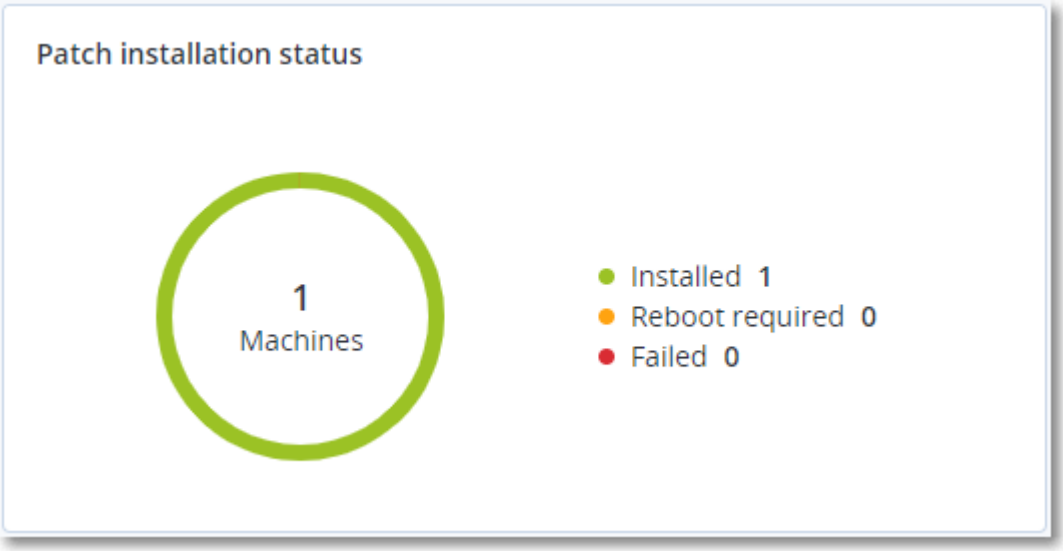
## Widżety dotyczące instalacji poprawek

Występują cztery widżety związane z funkcjami zarządzania poprawkami.

### Status instalacji poprawek

Ten widżet przedstawia liczbę komputerów pogrupowanych według statusów instalacji poprawek.

- **Zainstalowane** — na komputerze zainstalowano wszystkie dostępne poprawki
- **Wymagane ponowne uruchomienie** — po zainstalowaniu poprawki wymagane jest ponowne uruchomienie komputera
- **Niepowodzenie** — instalacja poprawki zakończyła się niepowodzeniem




### Podsumowanie instalacji poprawek

Ten widżet przedstawia podsumowanie poprawek na komputerach według statusów ich instalacji.

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 |

## Historia instalacji poprawek

Ten widżet przedstawia szczegółowe informacje o poprawkach na komputerach.

Patch installation history

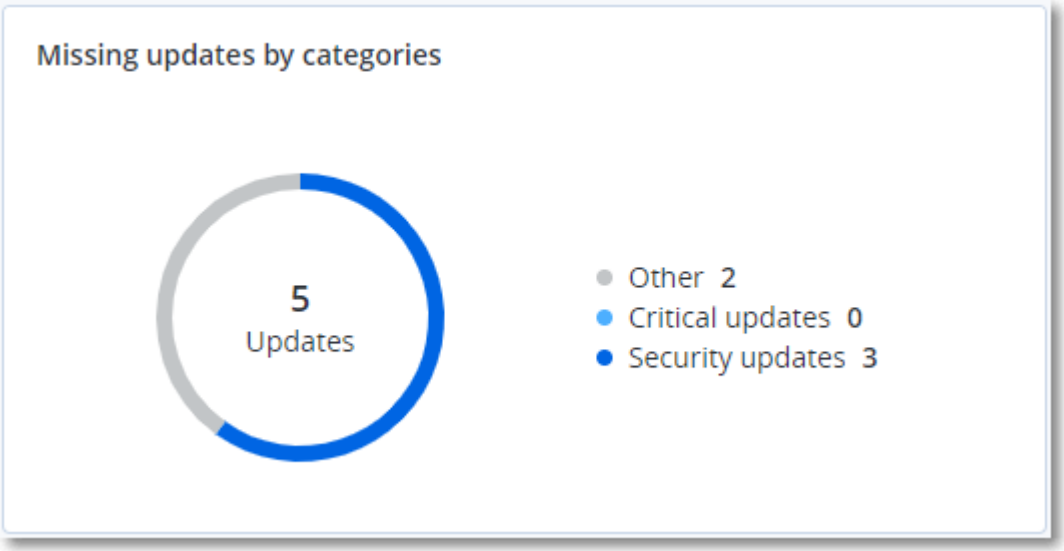
| Machine name | Update name | Version | Severity | Approval status | Installation status | Installation date |
|---|---|---|---|---|---|---|
| NIKITATIKHOC4E5 | FastStone Soft FastStone I... | 5.9 | Medium | New | Installed | 02/05/2020 |
| NIKITATIKHOB524 | Mozilla Firefox | 72.0.1 | Critical | Approved | 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 |

More

## Brakujące aktualizacje według kategorii

Ten widżet przedstawia liczbę brakujących aktualizacji według kategorii. Pokazywane są następujące kategorie:

- Aktualizacje zabezpieczeń
- Aktualizacje krytyczne
- Inne




## Szczegóły skanowania kopii zapasowej

Ten widżet przedstawia szczegółowe informacje o wykrytych zagrożeniach w kopiach zapasowych.

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 | [illegible] | Gen:Heur.PonyStealer.lm0@c05cs0dG | F:\882a04265361d588801b35... | 01/21/2020 11:40 AM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Trojan.GenericKD.3947747 | F:\2f2b2e30abe71f9a93d6ad7... | 01/21/2020 11:40 AM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Gen:Heur.PonyStealer.lm0@c05cs0dG | F:\882a04265361d588801b35... | 01/21/2020 11:45 AM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Trojan.GenericKD.3947747 | F:\2f2b2e30abe71f9a93d6ad7... | 01/21/2020 11:45 AM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Gen:Heur.PonyStealer.lm0@c05cs0dG | F:\882a04265361d588801b35... | 01/21/2020 11:50 AM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Trojan.GenericKD.3947747 | F:\2f2b2e30abe71f9a93d6ad7... | 01/21/2020 11:50 AM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Gen:Heur.PonyStealer.lm0@c05cs0dG | F:\882a04265361d588801b35... | 01/21/2020 1:10 PM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Trojan.GenericKD.3947747 | F:\2f2b2e30abe71f9a93d6ad7... | 01/21/2020 1:10 PM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Gen:Heur.PonyStealer.lm0@c05cs0dG | F:\882a04265361d588801b35... | 01/21/2020 1:33 PM |
| NIKITATIKHOC4E5 | New protection plan (1) | 01/20/2020 11:00 AM | Full | [illegible] | Trojan.GenericKD.3947747 | F:\2f2b2e30abe71f9a93d6ad7... | 01/21/2020 1:33 PM |

More

## Ostatnio dotknięte problemem

Ten widżet przedstawia szczegółowe informacje o obciążeniach, które ucierpiały wskutek zagrożeń, takich jak wirusy, złośliwe oprogramowanie czy ramsomware. Dostępne są informacje o wykrytych zagrożeniach, czasie ich wykrycia oraz liczbie plików, na które miały one wpływ.

Recently affected

| Machine name | Protection plan | Threat | Affected files | Detection time |
|---|---|---|---|---|
| Ubuntu_14.04_x64-1 | Total protection | Adware.DealPly!gen2 | 15 | 27.12.2 |
| Ubuntu_14.04_x64-1 | Protection plan | Bloodhound.MalMacro!g1 | 274 | 27.12.2 |
| dc_w2k12_r2 | Protection plan | Backdoor:Win32/Caphaw... | 13 | 27.12.2 |
| Win2012_r2-Hyper-V | Protection plan | W97M.Downloader!g32 | 5 | 27.12.2 |
| HyperV_for12A | Total protection | Miner.XMRig!gen1 | 68 | 27.12.2 |
| vm-sql_2012 | Total protection | Backdoor:Win32/Caphaw... | 61 | 27.12.2 |
| vm-sql_2012 | Protection plan | Adware.DealPly!gen2 | 9 | 27.12.2 |
| MF_2012_R2 | Total protection | MSH.Downloader!gen8 | 73 | 27.12.2 |
| MF_2012_R2 | Total protection | Bloodhound.MalMacro!g1 | 182 | 27.12.2 |
| MF_2012_R2 | Protection plan | Bloodhound.MalMacro!g1 | 18 | 27.12.2 |
| ESXirestore | Protection plan | MSH.Downloader!gen8 | 682 | 27.12.2017 11:23 AM |
| MF_2012_R2 | Protection plan | Miner.XMRig!gen1 | 13 | 27.12.2017 11:23 AM |
| Ubuntu_14.04_x64-1 | Total protection | Adware.DealPly!gen2 | 3 | 27.12.2017 11:23 AM |
| Win2012_r2-Hyper-V | Total protection | W97M.Downloader!g32 | 27 | 27.12.2017 11:23 AM |

Folder
Customer
✓ Machine name
✓ Protection plan
Detected by
✓ Threat
File name
File path
✓ Affected files
✓ Detection time

More | Show all 556

## Pobieranie danych dotyczących ostatnio dotkniętych problemem obciążeń

Można pobrać dane dotyczące ostatnio dotkniętych problemem obciążeń, wygenerować plik CSV i wysłać go do wskazanych odbiorców.

***Aby pobrać dane dotyczące ostatnio dotkniętych problemem obciążeń***

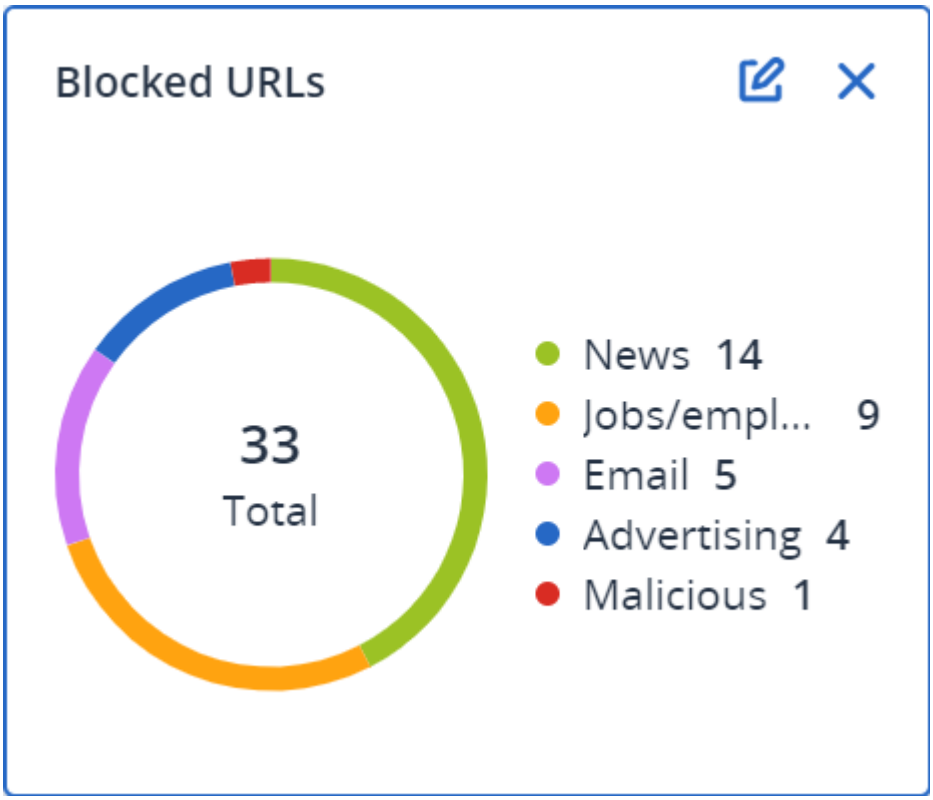
1. W widżecie **Ostatnio dotknięte problemem** kliknij **Pobierz dane**.
2. W polu **Okres** wprowadź liczbę dni, których mają dotyczyć pobierane dane. Można wprowadzić maksymalnie 200 dni.
3. W polu **Odbiorcy** wprowadź adresy e-mail wszystkich osób, które otrzymają wiadomość e-mail z łączem umożliwiającym pobranie pliku CSV.

4. Kliknij **Pobierz**.

   System zacznie generować plik CSV z danymi dotyczącymi obciążeń, które zostały dotknięte problemem we wskazanym okresie. Gdy plik CSV będzie gotowy, system wyśle wiadomość e-mail do odbiorców. Każdy odbiorca będzie mógł pobrać ten plik CSV.

## Zablokowane adresy URL

Ten widżet przedstawia dane statystyczne dotyczące zablokowanych adresów URL według kategorii. Więcej informacji na temat filtrowania i określania kategorii adresów URL można znaleźć w podręczniku użytkownika rozwiązania Cyber Protection.




## Widżet inwentaryzacji oprogramowania

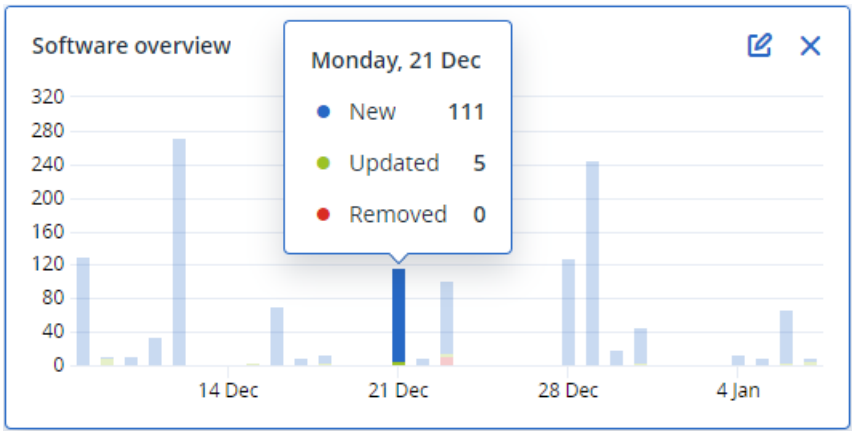
W widżecie tabeli **Inwentaryzacja oprogramowania** są wyświetlane szczegółowe informacje na temat wszystkich programów zainstalowanych na urządzeniach organizacji klienta z systemem Windows lub macOS.

Software inventory

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

More | Less | Show 1000+

W widżecie tabeli **Przegląd oprogramowania** są wyświetlane liczby nowych, zaktualizowanych i usuniętych we wskazanym okresie (7 dni, 30 dni lub bieżący miesiąc) aplikacji na urządzeniach organizacji klienta z systemem Windows lub macOS.




Po wskazaniu myszą określonego słupka wykresu pojawia się etykieta z następującymi informacjami:

**Nowe** — liczba nowo zainstalowanych aplikacji.

**Zaktualizowano** — liczba zaktualizowanych aplikacji.

**Usunięto** — liczba usuniętych aplikacji.

Po kliknięciu części słupka odpowiadającej danemu statusowi zostanie załadowane wyskakujące okienko. Zawiera ono listę wszystkich klientów, którzy mają urządzenia z aplikacjami o wybranym statusie w wybranym dniu. Można wybrać klienta z listy: kliknij **Przejdź do klienta**, a wówczas nastąpi przekierowanie do strony **Zarządzanie oprogramowaniem** -> **Inwentaryzacja oprogramowania** w konsoli usługi klienta. Informacje dostępne na tej stronie są filtrowane według odpowiedniej daty i statusu.

## Widżety inwentaryzacji sprzętu

W widżetach tabeli **Inwentaryzacja sprzętu** i **Szczegóły sprzętu** są pokazywane informacje na temat wszystkich elementów sprzętowych zainstalowanych w fizycznych i wirtualnych urządzeniach z systemem Windows lub macOS należących do organizacji klientów.

Hardware inventory

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

Hardware details

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

More

W widżecie tabeli **Zmiany sprzętowe** są wyświetlane informacje na temat sprzętu w należących do organizacji klientów fizycznych i wirtualnych urządzeniach z systemem Windows lub macOS, który dodano, usunięto i zmieniono we wskazanym okresie (7 dni, 30 dni lub bieżący miesiąc).

Hardware changes

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

More | Less | Show 309

## Historia sesji

Ten widżet umożliwia wyświetlenie szczegółowych informacji o sesjach pulpitu zdalnego i przesyłania plików zrealizowanych w ramach organizacji klientów we wskazanym okresie.

Remote sessions

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

More

# Raportowanie

Aby tworzyć raporty z wykorzystania usług i operacji, kliknij **Raporty**.

## dysku

Raporty dotyczące wykorzystania zawierają dane historyczne o korzystaniu z usług. Raporty dotyczące wykorzystania są dostępne zarówno w formacie CSV, jak i HTML.

### Typ raportu

Możesz wybrać jeden z następujących typów raportów:

- **Obecne wykorzystanie**

  Raport zawiera aktualne wskaźniki wykorzystania usługi.

  Wskaźniki wykorzystania są obliczane w ramach okresów rozliczeniowych dla każdego z dzierżawców podrzędnych. Jeśli dzierżawcy uwzględniani w raporcie mają różne okresy rozliczeniowe, wykorzystanie usługi w przypadku dzierżawcy nadrzędnego może się różnić od łącznego wykorzystania przez dzierżawców podrzędnych.
- **Rozkład obecnego wykorzystania**

  Ten raport jest dostępny tylko w przypadku dzierżawców-partnerów, którzy są zarządzani przez zewnętrzny system alokowania. Ten raport jest przydatny w sytuacji, gdy okresy rozliczeniowe dzierżawców podrzędnych są inne niż okres rozliczeniowy dzierżawcy nadrzędnego. Raport zawiera wskaźniki wykorzystania usługi przez dzierżawców podrzędnych obliczone w bieżącym okresie rozliczeniowym dzierżawcy nadrzędnego. Wykorzystanie usługi w przypadku dzierżawcy nadrzędnego będzie równe sumie wykorzystania w przypadku dzierżawców podrzędnych.
- **Podsumowanie okresu**

  Raport zawiera wskaźniki wykorzystania usługi z końca wskazanego okresu oraz różnice między wskaźnikami z początku i końca tego okresu.
- **Dzień po dniu w podanym okresie**

Raport zawiera wskaźniki wykorzystania usługi i ich zmiany w poszczególnych dniach wskazanego okresu.

## Zakres raportu

W razie potrzeby można wskazać zakres raportu, wybierając jedną z poniższych wartości:

- **Bezpośredni klienci i partnerzy**
  Raport będzie zawierać wskaźniki wykorzystania usług dotyczące tylko bezpośrednich dzierżawców podrzędnych dzierżawcy, w ramach którego działasz.
- **Wszyscy klienci i partnerzy**
  Raport będzie zawierać wskaźniki wykorzystania usług dotyczące wszystkich bezpośrednich dzierżawców podrzędnych dzierżawcy, w ramach którego działasz.
- **Wszyscy klienci i partnerzy (w tym szczegółowe dane użytkownika)**
  Raport będzie zawierać wskaźniki wykorzystania usług dotyczące wszystkich bezpośrednich dzierżawców podrzędnych dzierżawcy, w ramach którego działasz, a także wszystkich użytkowników w obszarach tych dzierżawców.

## Wskaźniki wskazujące zerowy stan wykorzystania

Można zmniejszyć liczbę wierszy w raporcie, ograniczając wyświetlanie informacji wyłącznie do wskaźników wskazujących niezerowy poziom wykorzystania przez ukrycie informacji o wskaźnikach wskazujących poziom zerowy.

## Konfigurowanie zaplanowanych raportów z wykorzystania

Zaplanowany raport obejmuje wskaźniki wykorzystania usług z ostatniego pełnego miesiąca kalendarzowego. Raporty są generowane pierwszego dnia miesiąca o godzinie 23:59:59 czasu UTC i wysyłane drugiego dnia tego samego miesiąca. Raporty są wysyłane do wszystkich administratorów dzierżawcy, którzy zaznaczyli pole wyboru **Zaplanowane raporty z użytkowania** w swoich ustawieniach użytkownika.

***Aby włączyć lub wyłączyć zaplanowany raport***

1. Zaloguj się do portalu zarządzania.
2. Upewnij się, że działasz na poziomie dzierżawcy znajdującego się najwyżej w hierarchii spośród wszystkich, którzy są dla Ciebie dostępni.
3. Kliknij **Raporty** > **Wykorzystanie**.
4. Kliknij **Zaplanowane**.
5. Zaznacz lub wyczyść pole wyboru **Wysyłaj miesięczny raport podsumowujący**.
6. W polu **Poziom szczegółów** wybierz zakres raportu.
7. [Opcjonalnie] Wybierz **Ukryj wskaźniki wskazujące zerowy stan wykorzystania**, jeśli chcesz wykluczyć z raportu wskaźniki wskazujące zerowy poziom wykorzystania.

## Konfigurowanie niestandardowych raportów z wykorzystania

Tego typu raport można wygenerować na żądanie — nie można go zaplanować. Raport zostanie wysłany na Twój adres e-mail.

***Aby wygenerować raport niestandardowy***

1. Zaloguj się do portalu zarządzania.
2. Przejdź do dzierżawcy, w którego przypadku chcesz utworzyć raport.
3. Kliknij **Raporty** > **Wykorzystanie**.
4. Wybierz kartę **Niestandardowe**.
5. W polu **Typ** wybierz typ raportu zgodnie z wcześniejszym opisem.
6. [Opcja niedostępna w przypadku typu raportu **Obecne wykorzystanie**] W polu **Okres** wybierz okres raportowania:
   - **Obecny miesiąc kalendarzowy**
   - **Poprzedni miesiąc kalendarzowy**
   - **Niestandardowe**
7. [Opcja niedostępna w przypadku typu raportu **Obecne wykorzystanie**] Jeśli chcesz wskazać niestandardowy okres raportowania, wybierz datę początkową i końcową. W przeciwnym razie pomiń ten krok.
8. W polu **Poziom szczegółów** wybierz zakres raportu zgodnie z wcześniejszym opisem.
9. [Opcjonalnie] Wybierz **Ukryj wskaźniki wskazujące zerowy stan wykorzystania**, jeśli chcesz wykluczyć z raportu wskaźniki wskazujące zerowy poziom wykorzystania.
10. Aby wygenerować raport, kliknij **Wygeneruj i wyślij**.

## Raporty z operacji

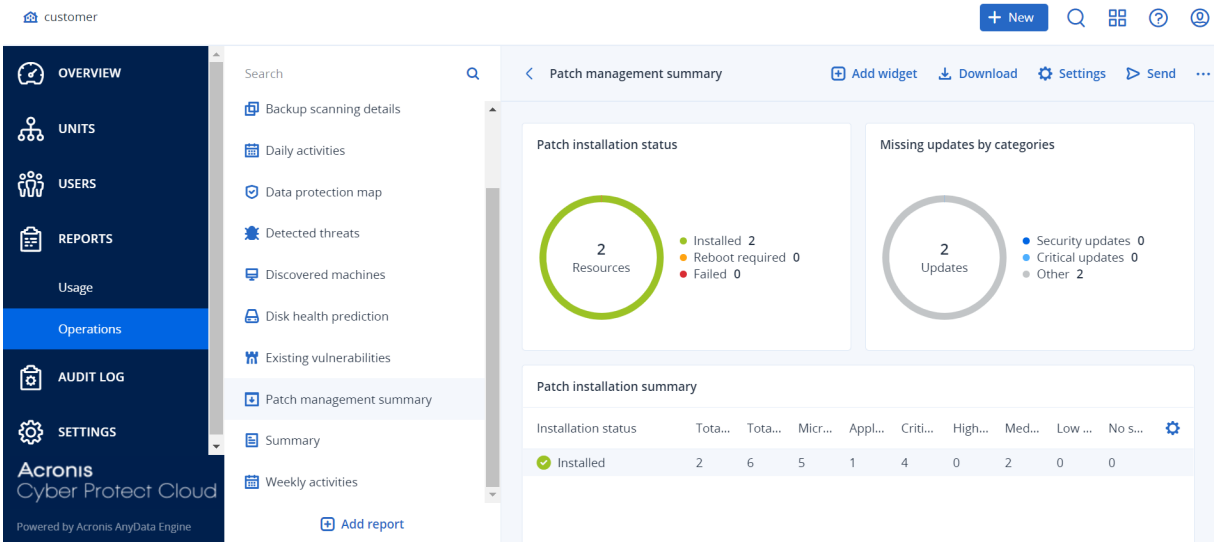
Raport z operacji może zawierać dowolny zestaw widżetów pulpitu nawigacyjnego dla **operacji**. Domyślnie wszystkie widżety przedstawiają skrócone informacje dotyczące dzierżawcy, w ramach którego działasz. Możesz to ustawienie dla danego widżetu, edytując ten widżet, lub dla wszystkich widżetów, zmieniając ustawienia raportu.

W zależności od typu widżetu raport zawiera dane ze wskazanego zakresu czasu lub z chwili przeglądania bądź generowania raportu. Zobacz "Raportowane dane zależnie od typu widżetu" (s. 124).

Wszystkie widżety historyczne przedstawiają dane z tego samego zakresu czasu. Zakres ten można zmienić w ustawieniach raportów.

Można korzystać z raportów domyślnych lub utworzyć raport niestandardowy.

Możesz pobrać raport o operacjach lub wysłać go pocztą e-mail w formacie Excel (XLSX) lub PDF.




Raporty domyślne wymieniono poniżej:

| Nazwa raportu | Opis |
|---|---|
| Wynik #CyberFit według komputerów | Pokazuje wynik #CyberFit oszacowany na podstawie oceny wskaźników zabezpieczeń i konfiguracji poszczególnych komputerów oraz zalecenia dotyczące możliwych udoskonaleń. |
| Alerty | Zawiera alerty zgłoszone w podanym okresie. |
| Szczegóły skanowania kopii zapasowej | Zawiera szczegółowe informacje o wykrytych zagrożeniach w kopiach zapasowych. |
| Codzienne działania | Zawiera zestawienie informacji o działaniach wykonanych w podanym okresie. |
| Mapa ochrony danych | Zawiera szczegółowe informacje o liczbie, rozmiarze, lokalizacji i statusach ochrony wszystkich ważnych plików na komputerach. |
| Wykryte zagrożenia | Zawiera szczegółowe informacje o zagrożonych komputerach według liczby zablokowanych zagrożeń oraz o komputerach będących w dobrej kondycji i mających luki w zabezpieczeniach. |
| Wykryte komputery | Zawiera listę wszystkich komputerów znalezionych w sieci organizacji. |
| Prognoza kondycji dysków | Zawiera prognozowane terminy awarii dysków HDD/SSD oraz aktualne statusy dysków. |
| Występujące luki w zabezpieczeniach | Zawiera listę istniejących luk w zabezpieczeniach systemów operacyjnych i aplikacji organizacji. Raport obejmuje również szczegółowe informacje dotyczące zagrożonych komputerów w sieci w przypadku każdego produktu z listy. |

| | |
|---|---|
| Podsumowanie zarządzania poprawkami | Zawiera liczbę brakujących, zainstalowanych i możliwych poprawek. W ramach raportów można wyświetlać bardziej szczegółowe informacje, aby sprawdzać brakujące bądź zainstalowane poprawki oraz informacje na temat wszystkich systemów. |
| Podsumowanie | Zawiera podsumowanie informacji o chronionych urządzeniach w podanym okresie. |
| Działania w tygodniu | Zawiera zestawienie informacji o działaniach wykonanych w podanym okresie. |
| Inwentaryzacja oprogramowania | Zawiera szczegółowe informacje na temat wszystkich programów zainstalowanych na komputerach organizacji klientów z systemem Windows lub macOS. |
| Inwentaryzacja sprzętu | Zawiera szczegółowe informacje na temat wszystkich elementów sprzętowych dostępnych w komputerach fizycznych i maszynach wirtualnych z systemem Windows lub macOS należących do organizacji klientów. |
| Sesje zdalne | Umożliwia wyświetlenie szczegółowych informacji o sesjach pulpitu zdalnego i przesyłania plików zrealizowanych w ramach organizacji klientów we wskazanym okresie. |

Aby zobaczyć raport, kliknij jego nazwę.

Aby uzyskać dostęp do operacji na raporcie, kliknij ikonę pionowego wielokropka na linii raportu. Te same operacje są dostępne po otworzeniu raportu.

## Dodawanie raportu

1. Kliknij **Dodaj raport**.
2. Wykonaj jedną z następujących czynności:
   - Aby zobaczyć wstępnie zdefiniowany raport, kliknij jego nazwę.
   - Aby dodać raport niestandardowy, kliknij **Niestandardowe**, kliknij nazwę raportu (domyślnie nadawane nazwy wyglądają tak: **Niestandardowe(1)**), a następnie dodaj widżety do raportu.
3. [Opcjonalnie] Zmień ustawienie widżetów metodą „przeciągnij i upuść".
4. [Opcjonalnie] Edytuj raport zgodnie z poniższymi instrukcjami.

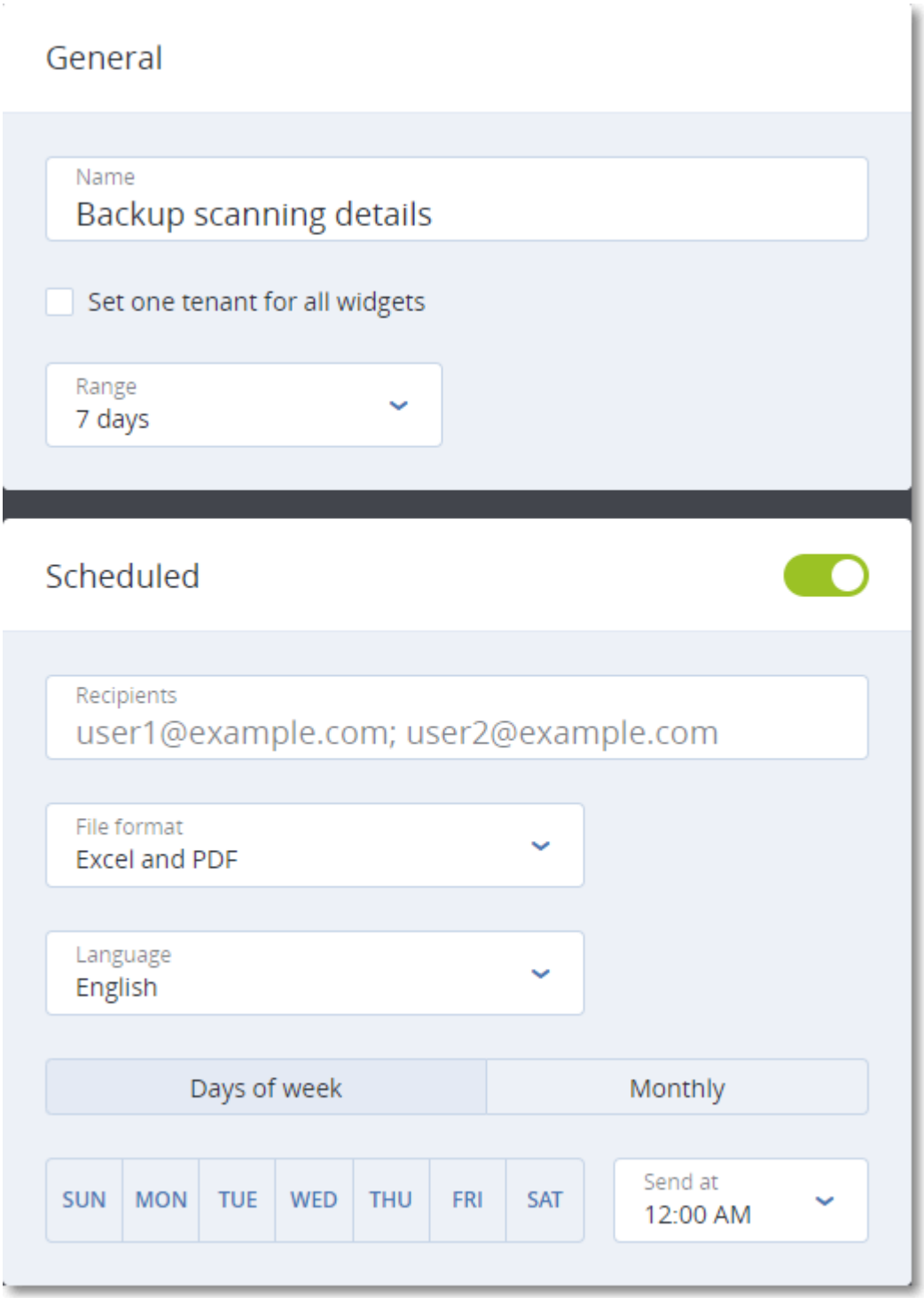
## Edytowanie ustawień raportu

Aby edytować raport, kliknij jego nazwę, a następnie kliknij **Ustawienia**. Edycja raportu pozwala na:

- zmianę nazwy raportu,
- zmianę dzierżawców pokazywanych we wszystkich widżetach w raporcie oraz
  Jeśli masz dzierżawców podrzędnych, masz dostępną opcję **Ustaw jednego dzierżawcę w przypadku wszystkich widżetów**. Umożliwia ona filtrowanie danych we wszystkich widżetach

raportu według wybranego dzierżawcy. Jeśli ta opcja nie zostanie wybrana, w widżetach będą widoczne dane dotyczące wszystkich dzierżawców podrzędnych bieżącego dzierżawcy.

- zmianę zakresów czasu wszystkich widżetów w raporcie oraz
- zaplanowanie wysyłania raportu za pomocą poczty e-mail w formacie PDF i/lub Excel



## Planowanie raportu

1. Kliknij nazwę raportu, a następnie kliknij **Ustawienia**.
2. Włącz przełącznik **Zaplanowane**.
3. Podaj adresy e-mail odbiorców.
4. Wybierz format raportu: PDF, Excel lub oba.
5. Wybierz dni oraz godzinę wysłania raportu.
6. Kliknij **Zapisz** w prawym górnym rogu.

## Eksportowanie i importowanie struktury raportu

Możesz wyeksportować oraz zaimportować strukturę raportu (zestaw widżetów i ustawienia raportu) do pliku JSON. Może być to przydatne w razie kopiowania struktury raportu jednego dzierżawcy do innego dzierżawcy.

Aby wyeksportować strukturę raportu, kliknij jego nazwę, kliknij pionową ikonę wielokropka w prawym górnym rogu, a następnie kliknij **Eksportuj**.

Aby zaimportować strukturę raportu, kliknij **Dodaj raport**, a następnie kliknij **Importuj**.

## Pobieranie raportu

Istnieje możliwość pobrania raportu. W tym celu kliknij **Pobierz** i wybierz potrzebne formaty:

- Excel i PDF
- Excel
- PDF

## Składowanie danych raportu

Możesz wysłać pocztą e-mail zrzut danych raportu w pliku CSV. Zrzut zawiera wszystkie dane raportu (bez filtrowania) dla niestandardowego okresu. Sygnatury czasowe w raportach CSV są dodawane według czasu UTC, a w raportach Excel i PDF — według bieżącej strefy czasowej.

Oprogramowanie generuje zrzut danych na bieżąco. Jeśli określisz długi okres, ta akcja może długo potrwać.

***Aby składować dane raportu***

1. Kliknij nazwę raportu.
2. Kliknij pionową ikonę wielokropka w prawym górnym rogu, a następnie kliknij **Dane zrzutu**.
3. Podaj adresy e-mail odbiorców.
4. W polu **Zakres czasu** określ przedział czasu.
5. Kliknij **Wyślij**.

# Podsumowanie

Raport podsumowujący stanowi ogólny przegląd statusu ochrony środowisk klientów i chronionych urządzeń we wskazanym okresie.

Raport podsumowujący zawiera sekcje z widżetami dynamicznymi, na których są wyświetlane kluczowe wskaźniki wydajności związane z korzystaniem przez klienta z następujących usług chmurowych: Kopia zapasowa, Ochrona przed złośliwym oprogramowaniem, Ocena luk w zabezpieczeniach, Zarządzanie poprawkami, Zapobieganie utracie danych, Notary, Odzyskiwanie po awarii oraz File Sync & Share.

Raport można dostosować na kilka sposobów, takich jak:

- Dodanie lub usunięcie sekcji.
- Zmiana kolejności sekcji.
- Zmiana nazwy sekcji.
- Przeniesienie widżetów do innej sekcji.
- Zmiana kolejności widżetów w poszczególnych sekcjach.
- Dodanie lub usunięcie widżetów.
- Dostosowanie widżetów.

Raporty podsumowujące można generować w formacie PDF i Excel, a następnie przesyłać odpowiednim zainteresowanym lub właścicielom organizacji klientów, aby mogli w przystępnej formie zobaczyć techniczną i biznesową wartość świadczonych usług.

Administratorzy partnerów mogą generować raporty podsumowujące i wysyłać je tylko do bezpośrednich klientów. W przypadku bardziej złożonej hierarchii dzierżawców, która obejmuje partnerów podrzędnych, partnerzy podrzędni muszą sami generować raport.

## Widżety usługi Podsumowanie

Możesz dodawać lub usuwać sekcje oraz widżety w ramach raportu podsumowującego i w ten sposób określać, jakie informacje mają być w nim zawarte.

### Widżety usługi Przegląd obciążeń

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Przegląd obciążeń**.

| Widżet | Opis |
|---|---|
| **Status ochrony obciążeń w chmurze** | Ten widżet przedstawia liczbę chronionych i niechronionych obciążeń w chmurze według typów w chwili wygenerowania raportu. Chronione obciążenia w chmurze to obciążenia, do których zastosowano co najmniej jeden plan tworzenia kopii zapasowych. Niechronione obciążenia w |

| Widżet | Opis |
| --- | --- |
| | chmurze to obciążenia, do których nie zastosowano żadnego planu tworzenia kopii zapasowych. Na wykresie przedstawiono następujące typy obciążeń w chmurze (w kolejności alfabetycznej od A do Z):<br>• Dysk Google Workspace<br>• Gmail Google Workspace<br>• Dysk współdzielony Google Workspace<br>• Skrzynki pocztowe usługi Hosted Exchange<br>• Skrzynki pocztowe Microsoft 365<br>• Microsoft 365 OneDrive<br>• Microsoft 365 SharePoint Online<br>• Microsoft Teams<br>• Witryny internetowe<br>W przypadku niektórych typów obciążeń są stosowane następujące grupy obciążeń:<br>• Microsoft 365: Użytkownicy, Grupy, Foldery publiczne, Zespoły i Kolekcje witryn<br>• Google Workspace: Użytkownicy i Dyski współdzielone<br>• Hosted Exchange: Użytkownicy<br>Jeśli w jednej grupie obciążeń znajduje się więcej niż 10 000 obciążeń, widżet nie wyświetla żadnych danych na temat poszczególnych obciążeń.<br>Jeśli więc na przykład klient ma konto Microsoft 365 z 10 000 skrzynek pocztowych oraz usługę OneDrive dla 500 użytkowników, to wszystkie one należą do grupy obciążeń Użytkownicy. Łącznie jest to 10 500 obciążeń, co oznacza przekroczenie limitu 10 000 obciążeń w grupie. W związku z tym widżet będzie ukrywać odpowiadające im typy obciążeń: Skrzynki pocztowe Microsoft 365 i Microsoft 365 OneDrive. |
| **Podsumowanie ochrony cybernetycznej** | Ten widżet przedstawia kluczowe wskaźniki wydajności ochrony cybernetycznej we wskazanym okresie.<br>**Dane uwzględnione w kopii zapasowej** — łączny rozmiar archiwów utworzonych w chmurze i magazynach lokalnych.<br>**Ograniczone zagrożenia** — całkowita liczba złośliwych programów zablokowanych na wszystkich urządzeniach.<br>**Zablokowane złośliwe adresy URL** — łączna liczba adresów URL zablokowanych na wszystkich urządzeniach.<br>**Luki w zabezpieczeniach, do których zastosowano poprawki** — łączna liczba luk w zabezpieczeniach wyeliminowanych przez zainstalowanie poprawek oprogramowania na wszystkich urządzeniach.<br>**Zainstalowane poprawki** — łączna liczba zainstalowanych poprawek na wszystkich urządzeniach. |

| Widżet | Opis |
| --- | --- |
| | **Serwery chronione przez usługę Odzyskiwanie po awarii** — łączna liczba serwerów chronionych przy użyciu usługi Odzyskiwanie po awarii.<br><br>**Użytkownicy usługi File Sync & Share** — łączna liczba użytkowników i gości korzystających z rozwiązania Cyber Files.<br><br>**Notaryzowane pliki** — łączna liczba notaryzowanych plików.<br><br>**Dokumenty podpisane elektronicznie** — łączna liczba dokumentów podpisanych elektronicznie.<br><br>**Zablokowane urządzenia peryferyjne** — łączna liczba zablokowanych urządzeń peryferyjnych. |
| **Status sieciowy obciążeń** | Ten widżet wskazuje, ile obciążeń jest odizolowanych i ile połączonych (jest to normalny stan obciążenia).<br><br>Wybierz odpowiedniego klienta. Wyświetlony widok obciążeń zostanie przefiltrowany w celu wyświetlenia odizolowanych obciążeń. Kliknij wartość Podłączono, aby wyświetlić listę obciążeń z agentami przefiltrowaną w celu wyświetlenia połączonych obciążeń (w kontekście wybranego klienta). |
| **Status ochrony obciążeń** | Ten widżet przedstawia chronione i niechronione obciążenia według typów w chwili wygenerowania raportu. Obciążenia chronione to obciążenia, do których zastosowano co najmniej jeden plan ochrony lub plan tworzenia kopii zapasowych. Obciążenia niechronione to obciążenia, do których nie zastosowano żadnego planu ochrony ani planu tworzenia kopii zapasowych. Wliczane są następujące obciążenia:<br>**Serwery** — serwery fizyczne i serwery będące kontrolerami domen.<br><br>**Stacje robocze** — fizyczne stacje robocze.<br><br>**Maszyny wirtualne** — maszyny wirtualne z agentami i bez agentów.<br><br>**Serwery hostingu witryn internetowych** — serwery wirtualne lub fizyczne z zainstalowanymi panelami sterowania cPanel lub Plesk.<br><br>**Urządzenia mobilne** — fizyczne urządzenia mobilne.<br><br>Jedno obciążenie może należeć do więcej niż jednej kategorii. Na przykład serwer hostingu witryn internetowych jest wliczany do dwóch kategorii: **Serwery** i **Serwery hostingu witryn internetowych**. |
| **Status ochrony obciążeń w chmurze** | **Status ochrony obciążeń w chmurze**<br>Ten widżet przedstawia liczbę chronionych i niechronionych obciążeń w chmurze według typów w chwili wygenerowania raportu. Chronione obciążenia w chmurze to obciążenia, do których zastosowano co najmniej jeden plan tworzenia kopii zapasowych. Niechronione obciążenia w chmurze to obciążenia, do których nie zastosowano żadnego planu tworzenia kopii zapasowych. Na wykresie przedstawiono następujące typy obciążeń w chmurze (w kolejności alfabetycznej od A do Z): |

| Widżet | Opis |
|---|---|
| | • Google Workspace Drive<br>• Google Workspace Gmail<br>• Dysk współdzielony Google Workspace<br>• Skrzynki pocztowe usługi Hosted Exchange<br>• Skrzynki pocztowe Microsoft 365<br>• Microsoft 365 OneDrive<br>• Microsoft 365 SharePoint Online<br>• Microsoft Teams<br>• Witryny internetowe<br><br>W przypadku niektórych typów obciążeń są stosowane następujące grupy obciążeń:<br><br>• Microsoft 365: Użytkownicy, Grupy, Foldery publiczne, Zespoły i Kolekcje witryn<br>• Google Workspace: Użytkownicy i Dyski współdzielone<br>• Hosted Exchange: Użytkownicy<br><br>Jeśli w jednej grupie obciążeń znajduje się więcej niż 10 000 obciążeń, widżet nie wyświetla żadnych danych na temat poszczególnych obciążeń.<br><br>Jeśli więc na przykład klient ma konto Microsoft 365 z 10 000 skrzynek pocztowych oraz usługę OneDrive dla 500 użytkowników, to wszystkie one należą do grupy obciążeń Użytkownicy. Łącznie jest to 10 500 obciążeń, co oznacza przekroczenie limitu 10 000 obciążeń w grupie. W związku z tym widżet będzie ukrywać odpowiadające im typy obciążeń: Skrzynki pocztowe Microsoft 365 i Microsoft 365 OneDrive. |

## Widżety usługi Ochrona przed złośliwym oprogramowaniem

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Obrona przed zagrożeniami**.

| Widżet | Opis |
|---|---|
| **Skanowanie antywirusowe plików** | Ten widżet przedstawia wyniki wykonywanego na żądanie skanowania antywirusowego urządzeń we wskazanym okresie.<br>**Pliki** — łączna liczba przeskanowanych plików.<br><br>**Czyste** — łączna liczba czystych plików.<br><br>**Wykryto, zastosowano kwarantannę** — łączna liczba zainfekowanych plików poddanych kwarantannie.<br><br>**Wykryto, nie zastosowano kwarantanny** — łączna liczba zainfekowanych plików, których nie poddano kwarantannie.<br><br>**Chronione urządzenia** — łączna liczba urządzeń z zastosowanymi zasadami ochrony przed złośliwym oprogramowaniem. |

| Widżet | Opis |
| --- | --- |
| | **Łączna liczba zarejestrowanych urządzeń** — łączna liczba zarejestrowanych urządzeń w czasie generowania raportu. |
| **Skanowanie antywirusowe kopii zapasowych** | Ten widżet przedstawia wyniki skanowania antywirusowego kopii zapasowych we wskazanym okresie według następujących wskaźników:<br>• Łączna liczba przeskanowanych punktów odzyskiwania<br>• Liczba czystych punktów odzyskiwania<br>• Liczba czystych punktów odzyskiwania z nieobsługiwanymi partycjami<br>• Liczba zainfekowanych punktów odzyskiwania — ten wskaźnik obejmuje liczbę zainfekowanych punktów odzyskiwania z nieobsługiwanymi partycjami. |
| **Zablokowane adresy URL** | Ten widżet przedstawia liczbę zablokowanych adresów URL we wskazanym okresie pogrupowanych według kategorii witryn.<br>W widżecie jest wymienionych siedem kategorii witryn internetowych, w których przypadku odnotowano największą liczbę zablokowanych adresów URL. Pozostałe kategorie witryn są wyświetlane łącznie i oznaczone jako **Inne**.<br>Więcej informacji na temat kategorii witryn można znaleźć w temacie Filtrowanie adresów URL w sekcji Cyber Protection. |
| **Wykres spalania dotyczący incydentów bezpieczeństwa** | Ten widżet przedstawia wskaźnik efektywności zamykania incydentów w ramach wybranej firmy. Liczba otwartych incydentów jest ujmowana w stosunku do liczby zamkniętych incydentów w danym okresie.<br>Zatrzymaj wskaźnik myszy na dowolnej kolumnie, aby wyświetlić podział zamkniętych i otwartych incydentów z wybranego dnia. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem. |
| **Średni czas rozwiązywania problemu incydentu** | Na tym widżecie jest przedstawiany średni czas rozwiązywania problemu związanego z incydentem bezpieczeństwa. Wskazuje on, jak szybko problemy incydentów są badane w ramach dochodzenia i rozwiązywane.<br>Kliknij kolumnę, aby wyświetlić podział incydentów według ich ważności (**Krytyczny**, **Wysoki** i **Średni**) oraz wskazanie, ile czasu zajęło rozwiązanie problemu o różnym poziomie ważności. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem. |
| **Status zagrożeń** | Ten widżet przedstawia aktualny status zagrożeń w przypadku obciążeń w firmie (niezależnie od liczby obciążeń) z wyraźnym zaznaczeniem bieżącej liczby incydentów, których skutki nie zostały zniwelowane i które wymagają dochodzeń. Widżet wskazuje również liczbę incydentów, których skutki zostały zniwelowane (ręcznie i/lub automatycznie przez system). |
| **Wykryte** | Ten widżet przedstawia liczbę wykrytych zagrożeń we wskazanym okresie |

| Widżet | Opis |
| --- | --- |
| **zagrożenia według technologii ochrony** | pogrupowanych według następujących technologii ochrony:<br>• Skanowanie antywirusowe<br>• Mechanizm zachowań<br>• Ochrona przed cryptominingiem<br>• Ochrona przed exploitami<br>• Aktywna ochrona przed ransomware<br>• Ochrona w czasie rzeczywistym<br>• Filtrowanie adresów URL |

## Widżety usługi Kopia zapasowa

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Kopia zapasowa**.

| Widżet | Opis |
| --- | --- |
| **Obciążenia uwzględnione w kopii zapasowej** | Ten widżet przedstawia łączną liczbę zarejestrowanych obciążeń według statusów kopii zapasowych.<br><br>**Utworzono kopię zapasową** — liczba obciążeń uwzględnionych w kopii zapasowej (wykonano co najmniej jedną udaną kopię zapasową) w okresie ujętym w raporcie.<br><br>**Nie utworzono kopii zapasowej** — liczba obciążeń, które nieuwzględnionych w kopii zapasowej (nie wykonano żadnej udanej kopii zapasowej) w okresie ujętym w raporcie. |
| **Status kondycji dysków według urządzeń fizycznych** | Ten widżet przedstawia zagregowany status kondycji urządzeń fizycznych oceniony na podstawie statusów kondycji ich dysków.<br><br>**OK** — ten status kondycji dysków dotyczy wartości [70–100]. Urządzenie ma status **OK**, gdy wszystkie jego dyski mają status **OK**.<br><br>**Ostrzeżenie** — ten status kondycji dysków dotyczy wartości [30–70]. Urządzenie ma status **Ostrzeżenie**, gdy status choćby jednego z jego dysków ma status **Ostrzeżenie** i żaden z pozostałych dysków nie ma statusu **Błąd**.<br><br>**Błąd** — ten status kondycji dysków dotyczy wartości [0–30]. Urządzenie ma status **Błąd**, gdy status choćby jednego z jego dysków ma status **Błąd**.<br><br>**Obliczanie danych dysku** — urządzenie ma status **Obliczanie danych dysku**, gdy jeszcze nie obliczono statusów jego dysków. |
| **Wykorzystanie magazynu kopii zapasowych** | Ten widżet przedstawia łączną liczbę i łączny rozmiar kopii zapasowych w chmurze oraz magazynie lokalnym we wskazanym okresie. |

## Widżety usługi Ocena luk w zabezpieczeniach i zarządzanie poprawkami

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Ocena luk w zabezpieczeniach i zarządzanie poprawkami**.

| Widżet | Opis |
|---|---|
| **Luki w zabezpieczeniach, do których zastosowano poprawki** | Ten widżet przedstawia wyniki wykonania oceny luk w zabezpieczeniach we wskazanym okresie.<br><br>**Łącznie** — łączna liczba luk w zabezpieczeniach, do których zastosowano poprawki.<br><br>**Luki w zabezpieczeniach oprogramowania firmy Microsoft** — łączna liczba usuniętych luk w zabezpieczeniach oprogramowania Microsoft na wszystkich urządzeniach z systemem Windows.<br><br>**Luki w zabezpieczeniach oprogramowania innych firm przeznaczonego do systemu Windows** — łączna liczba usuniętych luk w zabezpieczeniach oprogramowania innych firm przeznaczonego do systemu Windows na wszystkich urządzeniach z systemem Windows.<br><br>**Przeskanowane obciążenia** — łączna liczba urządzeń, które zostały pomyślnie przeskanowane pod kątem luk w zabezpieczeniach co najmniej raz we wskazanym okresie. |
| **Zainstalowane poprawki** | Ten widżet przedstawia wyniki zarządzania poprawkami we wskazanym okresie.<br><br>**Zainstalowane** — łączna liczba poprawek pomyślnie zainstalowanych na wszystkich urządzeniach.<br><br>**Poprawki do oprogramowania firmy Microsoft** — łączna liczba poprawek do oprogramowania firmy Microsoft pomyślnie zainstalowanych na wszystkich urządzeniach z systemem Windows.<br><br>**Poprawki do oprogramowania innych firm przeznaczonego do systemu Windows** — łączna liczba poprawek do oprogramowania innych firm przeznaczonego do systemu Windows pomyślnie zainstalowanych na wszystkich urządzeniach z systemem Windows.<br><br>**Obciążenia z zastosowanymi poprawkami** — łączna liczba urządzeń, do których pomyślnie zastosowano poprawki (co najmniej jedna poprawka pomyślnie zainstalowana we wskazanym okresie). |

## Widżety usługi Odzyskiwanie po awarii

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Odzyskiwanie po awarii**.

| Widżet | Opis |
| --- | --- |
| **Statystyki usługi Odzyskiwanie po awarii** | Ten widżet przedstawia kluczowe wskaźniki wydajności odzyskiwania po awarii we wskazanym okresie.<br><br>**Produkcyjne przełączenia awaryjne** — liczba operacji produkcyjnego przełączania awaryjnego we wskazanym okresie.<br><br>**Testowe przełączenia awaryjne** — liczba operacji testowego przełączania awaryjnego wykonanych we wskazanym okresie.<br><br>**Serwery podstawowe** — łączna liczba serwerów podstawowych w chwili wygenerowania raportu.<br><br>**Serwery odzyskiwania** — łączna liczba serwerów odzyskiwania w chwili wygenerowania raportu.<br><br>**Publiczne adresy IP** — łączna liczba publicznych adresów IP w chwili wygenerowania raportu.<br><br>**Wykorzystane punkty obliczeniowe łącznie** — łączna liczba punktów obliczeniowych wykorzystanych we wskazanym okresie. |
| **Przetestowane serwery odzyskiwania po awarii** | Ten widżet przedstawia informacje o serwerach chronionych przez usługę Odzyskiwanie po awarii i przetestowanych przez wykonanie testowego przełączenia awaryjnego.<br><br>Ten widżet przedstawia następujące wskaźniki:<br><br>**Chronione serwery** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii (serwerów mających co najmniej jeden serwer odzyskiwania) w chwili wygenerowania raportu.<br><br>**Przetestowane** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii przetestowanych przy użyciu testowego przełączania awaryjnego we wskazanym okresie spośród wszystkich serwerów chronionych przez usługę Odzyskiwanie po awarii.<br><br>**Nieprzetestowane** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii nieprzetestowanych przy użyciu testowego przełączania awaryjnego we wskazanym okresie spośród wszystkich serwerów chronionych przez usługę Odzyskiwanie po awarii.<br><br>Ten widżet przedstawia również rozmiar magazynu odzyskiwania po awarii (w GB) w chwili wygenerowania raportu. Jest to suma rozmiarów kopii zapasowych serwerów chmurowych. |
| **Serwery chronione przy użyciu usługi Odzyskiwanie po awarii** | Ten widżet przedstawia informacje o serwerach chronionych przez usługę Odzyskiwanie po awarii i serwerach niechronionych.<br><br>Ten widżet przedstawia następujące wskaźniki:<br><br>Łączna liczba serwerów zarejestrowanych w ramach dzierżawcy-klienta w chwili wygenerowania raportu. |

| Widżet | Opis |
| --- | --- |
| | **Chronione** — liczba serwerów chronionych przez usługę Odzyskiwanie po awarii (mających co najmniej jeden serwer odzyskiwania i kopię zapasową całego serwera) spośród wszystkich zarejestrowanych serwerów w chwili wygenerowania raportu.<br><br>**Niechronione** — łączna liczba niechronionych serwerów spośród wszystkich zarejestrowanych serwerów w chwili wygenerowania raportu. |

## Widżet usługi Zapobieganie utracie danych

Poniższy temat zawiera dodatkowe informacje na temat zablokowanych urządzeń peryferyjnych w sekcji **Zapobieganie utracie danych**.

Ten widżet przedstawia łączną liczbę zablokowanych urządzeń we wskazanym okresie i łączną liczbę zablokowanych urządzeń według ich typów.

- Magazyn wymienny
- Zaszyfrowane urządzenie wymienne
- Drukarki
- Schowek — obejmuje typy urządzeń powiązane ze schowkiem i do rejestrowania zrzutów ekranu.
- Urządzenia mobilne
- Bluetooth
- Dyski optyczne
- Dyskietki
- USB — obejmuje typy urządzeń do portów USB i przekierowywanych portów USB.
- FireWire
- Zamapowane dyski
- Przekierowane dane schowka — obejmuje typy urządzeń powiązane z przychodzącymi i wychodzącymi przekierowanymi danymi schowka.

Ten widżet przedstawia pierwsze siedem typów urządzeń, w których przypadku odnotowano najwyższą liczbę zablokowanych urządzeń, a pozostałe typy urządzeń są wyświetlane łącznie i oznaczone jako **Inne**.

## Widżety usługi File Sync & Share

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **File Sync & Share**.

| Widżet | Opis |
| --- | --- |
| **Statystyki usługi File Sync & Share** | Ten widżet przedstawia następujące wskaźniki: |

| Widżet | Opis |
| --- | --- |
| | **Łączne wykorzystanie pamięci w chmurze** — łączne wykorzystanie magazynu przez wszystkich użytkowników.<br>**Użytkownicy** — łączna liczba użytkowników.<br>**Średnie wykorzystanie magazynu na użytkownika** — średnie wykorzystanie magazynu na użytkownika.<br>**Użytkownicy-goście** — łączna liczba użytkowników-gości. |
| **Wykorzystanie magazynu usługi File Sync & Share przez użytkowników** | Ten widżet przedstawia łączne liczby użytkowników usługi File Sync & Share korzystających z magazynu w następujących zakresach:<br>• 0–1 GB<br>• 1–5 GB<br>• 5–10 GB<br>• 10–50 GB<br>• 50–100 GB<br>• 100–500 GB<br>• 500 GB–1 TB<br>• 1+ TB |

## Widżety usługi Notary

Poniższa tabela zawiera dodatkowe informacje na temat widżetów dostępnych w sekcji **Notary**.

| Widżet | Opis |
| --- | --- |
| **Statystyki usługi Cyber Notary** | Ten widżet przedstawia następujące wskaźniki dotyczące usługi Notary:<br>**Wykorzystanie pamięci w chmurze usługi Notary** — łączny rozmiar magazynu wykorzystywany na potrzeby usługi Notary.<br>**Notaryzowane pliki** — łączna liczba notaryzowanych plików.<br>**Dokumenty podpisane elektronicznie** — łączna liczba dokumentów i plików podpisanych elektronicznie. |
| **Notaryzowane pliki użytkowników** | Przedstawia łączną liczbę notaryzowanych plików wszystkich użytkowników. Użytkownicy są pogrupowani według liczb swoich notaryzowanych plików.<br>• Do 10 plików<br>• 11–100 plików<br>• 101–500 plików<br>• 501–1000 plików<br>• 1000+ plików |
| **Podpisane** | Ten widżet przedstawia łączną liczbę podpisanych elektronicznie |

| Widżet | Opis |
| --- | --- |
| **elektronicznie dokumenty użytkowników** | dokumentów i plików wszystkich użytkowników. Użytkownicy są pogrupowani według liczb swoich dokumentów i plików podpisanych elektronicznie.<br>• Do 10 plików<br>• 11–100 plików<br>• 101–500 plików<br>• 501–1000 plików<br>• 1000+ plików |

## Konfigurowanie ustawień raportu podsumowującego

Ustawienia raportu skonfigurowane podczas tworzenia raportu podsumowującego można zaktualizować.

***Aby zaktualizować ustawienia raportu podsumowującego***

1. W konsoli zarządzania przejdź do sekcji **Raporty** > **Podsumowanie**.
2. Kliknij nazwę raportu podsumowującego, który chcesz zaktualizować.
3. Kliknij **Ustawienia**.
4. Zmień wartości pól stosownie do potrzeb.
5. Kliknij **Zapisz**.

## Tworzenie raportu podsumowującego

Można utworzyć raport podsumowujący, wyświetlić podgląd jego zawartości, skonfigurować odbiorców raportu i zaplanować jego automatyczne wysłanie.

***Aby utworzyć raport podsumowujący***

1. W konsoli zarządzania przejdź do sekcji **Raporty** > **Podsumowanie**.
2. Kliknij **Utwórz raport podsumowujący**.
3. W polu **Nazwa raportu** wpisz nazwę raportu.
4. Wybierz odbiorców raportu.
   - Jeśli chcesz wysłać raport do wszystkich bezpośrednich klientów, wybierz **Wyślij do wszystkich bezpośrednich klientów**.
   - Jeśli chcesz wysłać raport do wybranych klientów
     a. Wyczyść pole wyboru **Wyślij do wszystkich bezpośrednich klientów**.
     b. Kliknij **Wybierz kontakty**.
     c. Wybierz określonych klientów. Aby łatwo znaleźć określony kontakt, możesz skorzystać z

pola Szukaj.

d. Kliknij **Wybierz**.

5. Wybierz zakres: **30 dni** lub **Ten miesiąc**
6. Wybierz format pliku: **PDF**, **Excel** lub **Excel i PDF**.
7. Skonfiguruj ustawienia harmonogramu.
   - Jeśli chcesz wysłać raport do wybranych odbiorców w określonym dniu o określonej godzinie:
     a. Włącz opcję **Zaplanowane**.
     b. Kliknij **Dzień miesiąca**, wyczyść pole Ostatni dzień i kliknij odpowiednią datę.
     c. W polu **Godzina** wprowadź odpowiednią godzinę.
     d. Kliknij **Zastosuj**.
   - Jeśli chcesz utworzyć raport bez wysyłania go do odbiorców, wyłącz opcję **Zaplanowane**.
8. Kliknij **Zapisz**.

## Dostosowywanie raportu podsumowującego

Można określać, jakie informacje mają być zawarte w raporcie podsumowującym. Można dodawać lub usuwać sekcje, dodawać lub usuwać widżety, zmieniać nazwy sekcji, dostosowywać widżety oraz przeciągać widżety i sekcje, aby zmienić kolejność wyświetlania informacji w raporcie.

***Aby dodać sekcję***

1. Kliknij **Dodaj element** > **Dodaj sekcję**.
2. W oknie **Dodaj sekcję** wpisz nazwę sekcji lub użyj nazwy domyślnej.
3. Kliknij **Dodaj do raportu**.

***Aby zmienić nazwę sekcji***

1. W sekcji, której nazwę chcesz zmienić, kliknij **Edytuj**.
2. W oknie **Edytuj sekcję** wpisz nową nazwę.
3. Kliknij **Zapisz**.

***Aby usunąć sekcję***

1. W sekcji, którą chcesz usunąć, kliknij **Usuń sekcję**.
2. W oknie potwierdzenia operacji **Usuń sekcję** kliknij **Usuń**.

***Aby dodać do sekcji widżet z ustawieniami domyślnymi***

1. W sekcji, do której chcesz dodać widżet, kliknij **Dodaj widżet**.
2. W oknie **Dodaj widżet** kliknij widżet, który chcesz dodać.

***Aby dodać do sekcji dostosowany widżet***

1. W sekcji, do której chcesz dodać widżet, kliknij **Dodaj widżet**.
2. W oknie **Dodaj widżet** znajdź widżet, który chcesz dodać, i kliknij **Dostosuj**.
3. Skonfiguruj pola stosownie do potrzeb.
4. Kliknij **Dodaj widżet**.

***Aby dodać do raportu widżet z ustawieniami domyślnymi***

1. Kliknij **Dodaj element** > **Dodaj widżet**.
2. W oknie **Dodaj widżet** kliknij widżet, który chcesz dodać.

***Aby dodać do raportu dostosowany widżet***

1. Kliknij **Dodaj widżet**.
2. W oknie **Dodaj widżet** znajdź widżet, który chcesz dodać, i kliknij **Dostosuj**.
3. Skonfiguruj pola stosownie do potrzeb.
4. Kliknij **Dodaj widżet**.

***Aby zresetować ustawienia domyślne widżetu***

1. W widżecie, który chcesz dostosować, kliknij **Edytuj**.
2. Kliknij **Przywróć domyślne**.
3. Kliknij **Gotowe**.

***Aby dostosować widżet***

1. W widżecie, który chcesz dostosować, kliknij **Edytuj**.
2. Edytuj pola stosownie do potrzeb.
3. Kliknij **Gotowe**.

## Wysyłanie raportów podsumowujących

Raport podsumowujący można wysłać na żądanie. W takim przypadku ustawienie **Zaplanowane** jest ignorowane i raport zostaje niezwłocznie wysłany. W przypadku wysyłania raportu system korzysta z ustawień Odbiorcy, Zakres i Format pliku skonfigurowanych w sekcji **Ustawienia**. Ustawienia te można ręcznie zmienić przed wysłaniem raportu. Aby uzyskać więcej informacji, zobacz "Konfigurowanie ustawień raportu podsumowującego" (s. 120).

***Aby wysłać raport podsumowujący***

1. W portalu zarządzania przejdź do sekcji **Raporty** > **Podsumowanie**.
2. Kliknij nazwę raportu podsumowującego, który chcesz wysłać.
3. Kliknij **Wyślij teraz**.
   System wyśle raport podsumowujący do wybranych odbiorców.

## Strefy czasowe w raportach

Strefy czasowe stosowane w raportach różnią się w zależności od typu raportu. Poniższa tabela zawiera odpowiednie informacje referencyjne.

| Lokalizacja i typ raportu | Strefa czasowa w raporcie |
|---|---|
| Portal zarządzenia > Przegląd > Operacje<br>(widżety) | Czas wygenerowania raportu jest zgodny ze strefą czasową komputera, na którym działa przeglądarka. |
| Portal zarządzenia > Przegląd > Operacje<br>(eksportowany jako PDF lub xslx) | • Sygnatura czasowa wyeksportowanego raportu jest zgodna ze strefą czasową komputera użytego do wyeksportowania raportu.<br>• Strefą czasową działań widocznych w raporcie jest UTC. |
| Portal zarządzania > Raporty > Użytkowanie > Zaplanowane raporty | • Raport jest generowany pierwszego dnia miesiąca o godzinie 23:59:59 czasu UTC.<br>• Jest wysyłany drugiego dnia miesiąca. |
| Portal zarządzania > Raporty > Użytkowanie > Raporty niestandardowe | Strefą czasową i datą raportu jest UTC. |
| Portal zarządzenia > Raporty > Operacje<br>(widżety) | • Czas wygenerowania raportu jest zgodny ze strefą czasową komputera, na którym działa przeglądarka.<br>• Strefą czasową działań widocznych w raporcie jest UTC. |
| Portal zarządzenia > Raporty > Operacje<br>(eksportowany jako PDF lub xslx) | • Sygnatura czasowa wyeksportowanego raportu jest zgodna ze strefą czasową komputera użytego do wyeksportowania raportu.<br>• Strefą czasową działań widocznych w raporcie jest UTC. |
| Portal zarządzenia > Raporty > Operacje<br>(zaplanowane dostarczenie) | • Strefą czasową dostarczenia raportu jest UTC.<br>• Strefą czasową działań widocznych w raporcie jest UTC. |
| Portal zarządzania > Użytkownicy > Codzienne zestawienie aktywnych alertów | • Ten raport jest wysyłany raz dziennie między 10:00 a 23:59 czasu UTC. Godzina wysłania raportu zależy od obciążenia centrum danych.<br>• Strefą czasową działań widocznych w raporcie jest UTC. |
| Portal zarządzania > Użytkownicy > Powiadomienia o statusie cyberochrony | • Ten raport jest wysyłany po zakończeniu działania.<br>**Uwaga**<br>Niektóre raporty mogą być wysyłane z opóźnieniem — w zależności od obciążenia centrum danych.<br>• Strefą czasową działania w raporcie jest UTC. |

## Raportowane dane zależnie od typu widżetu

Ze względu na wyświetlany zakres danych można wyróżnić dwa rodzaje widżetów na pulpicie nawigacyjnym:

- Widżety wyświetlające dane aktualne w chwili przeglądania lub generowania raportu.
- Widżety wyświetlające dane historyczne.

W przypadku skonfigurowania zakresu dat w ustawieniach raportu w celu utworzenia zrzutu danych z pewnego okresu, wybrany zakres czasu będzie miał zastosowanie tylko do widżetów wyświetlających dane historyczne. W przypadku widżetów wyświetlających dane aktualne w chwili przeglądania lub generowania raportu parametr zakresu czasu nie ma zastosowania.

W poniższej tabeli zamieszczono listę dostępnych widżetów i ich zakresów dat.

| Nazwa widżetu | Dane wyświetlane w widżetach i raportach |
|---|---|
| Wynik #CyberFit według komputerów | Aktualne |
| 5 ostatnich alertów | Aktualne |
| Szczegóły aktywnych alertów | Aktualne |
| Podsumowanie aktywnych alertów | Aktualne |
| Działania | Historyczne |
| Lista działań | Historyczne |
| Historia alertów | Historyczne |
| Skanowanie antywirusowe kopii zapasowych | Historyczne |
| Skanowanie antywirusowe plików | Historyczne |
| Szczegóły skanowania kopii zapasowej (zagrożenia) | Historyczne |
| Status kopii zapasowej | Historyczne — w kolumnach **Operacje łącznie** i **Liczba pomyślnych operacji**<br>Aktualne — w pozostałych kolumnach |
| Wykorzystanie magazynu kopii zapasowych | Historyczne |
| Zablokowane urządzenia peryferyjne | Historyczne |
| Zablokowane adresy URL | Aktualne |
| Aplikacje w chmurze | Aktualne |
| Status ochrony obciążeń w chmurze | Aktualne |

| | |
|---|---|
| Cyber protection | Aktualne |
| Podsumowanie ochrony cybernetycznej | Historyczne |
| Mapa ochrony danych | Historyczne |
| Urządzenia | Aktualne |
| Przetestowane serwery odzyskiwania po awarii | Historyczne |
| Statystyki odzyskiwania po awarii | Historyczne |
| Wykryte komputery | Aktualne |
| Przegląd kondycji dysków | Aktualne |
| Status kondycji dysków | Aktualne |
| Status kondycji dysków według urządzeń fizycznych | Aktualne |
| Podpisane elektronicznie dokumenty użytkowników | Aktualne |
| Występujące luki w zabezpieczeniach | Historyczne |
| Statystyki usługi File Sync & Share | Aktualne |
| Wykorzystanie magazynu usługi File Sync & Share przez użytkowników | Aktualne |
| Zmiany sprzętowe | Historyczne |
| Szczegóły sprzętu | Aktualne |
| Inwentaryzacja sprzętu | Aktualne |
| Historyczne zestawienie alertów | Historyczne |
| Podsumowanie lokalizacji | Aktualne |
| Brakujące aktualizacje według kategorii | Aktualne |
| Niechroniony | Aktualne |
| Notaryzowane pliki użytkowników | Aktualne |
| Statystyki usługi Notary | Aktualne |
| Historia instalacji poprawek | Historyczne |
| Status instalacji poprawek | Historyczne |
| Podsumowanie instalacji poprawek | Historyczne |
| Luki w zabezpieczeniach, do których | Historyczne |

| | |
|---|---|
| zastosowano poprawki | |
| Zainstalowane poprawki | Historyczne |
| Status ochrony | Aktualne |
| Ostatnie objęte wpływem | Historyczne |
| Sesje zdalne | Historyczne |
| Wykres spalania dotyczący incydentów bezpieczeństwa | Historyczne |
| Średni czas rozwiązywania problemu incydentu bezpieczeństwa | Historyczne |
| Serwery chronione przez usługę Odzyskiwanie po awarii | Aktualne |
| Inwentaryzacja oprogramowania | Aktualne |
| Przegląd oprogramowania | Historyczne |
| Status zagrożeń | Aktualne |
| Wykryte zagrożenia według technologii ochrony | Historyczne |
| Podział najliczniejszych incydentów według obciążeń | Aktualne |
| Komputery z lukami w zabezpieczeniach | Aktualne |
| Status sieciowy obciążeń | Aktualne |
| Obciążenia uwzględnione w kopii zapasowej | Historyczne |
| Status ochrony obciążeń | Aktualne |

# Dziennik inspekcji

Aby przejrzeć dziennik inspekcji, kliknij **Dziennik inspekcji**.

Dziennik inspekcji udostępnia chronologiczny zapis następujących zdarzeń:

- Operacje wykonywane przez użytkowników w portalu zarządzania
- Operacje dotyczące zasobów obsługiwanych między chmurami wykonywane przez użytkowników w konsoli usługi Cyber Protection
- Operacje skryptów cybernetycznych wykonywane przez użytkowników w konsoli usługi Cyber Protection
- Komunikaty systemowe o osiągnięciu i stopniu wykorzystania limitów

W dzienniku widoczne są zdarzenia dotyczące dzierżawcy, w ramach którego aktualnie pracujesz, oraz jego dzierżawców podrzędnych. Kliknięcie zdarzenia umożliwia wyświetlenie dodatkowych informacji na jego temat.

Dzienniki inspekcji są przechowywane w centrum danych i problemy na komputerach użytkowników nie ograniczają ich dostępności.

Dziennik jest codziennie oczyszczany. Zdarzenia są usuwane po 180 dniach.

## Pola dziennika inspekcji

W przypadku każdego zdarzenia w dzienniku są dostępne następujące informacje:

- **Zdarzenie**
  Krótki opis zdarzenia. Na przykład **Dzierżawca został utworzony**, **Dzierżawca został usunięty**, **Użytkownik został utworzony**, **Użytkownik został usunięty**, **Limit został osiągnięty**, **Przeglądano zawartość kopii zapasowej**, **Skrypt został zmieniony**.
- **Ważność**
  Może być jedna z następujących:
  - **Błąd**
    Oznacza błąd.
  - **Ostrzeżenie**
    Oznacza potencjalnie negatywną czynność. Na przykład **Dzierżawca został usunięty**, **Użytkownik został usunięty**, **Limit został osiągnięty**.
  - **Powiadomienie**
    Oznacza, że zdarzenie może wymagać uwagi. Na przykład **Dzierżawca został zaktualizowany**, **Użytkownik został zaktualizowany**.
  - **Informacja**
    Oznacza informację o neutralnej w skutkach zmianie lub czynności. Na przykład **Dzierżawca został utworzony**, **Użytkownik został utworzony**, **Limit został zaktualizowany**, **Plan skryptów został usunięty**.
- **Data**
  Data i godzina wystąpienia zdarzenia.
- **Nazwa obiektu**
  Obiekt, na którym została wykonana operacja. Na przykład obiektem zdarzenia **Użytkownik został zaktualizowany** jest użytkownik, którego właściwości zostały zmienione. W przypadku zdarzeń dotyczących limitu obiektem jest limit.
- **Dzierżawca**
  Nazwa dzierżawcy, do którego należy obiekt.
- **Inicjator**
  Nazwa logowania użytkownika inicjującego zdarzenie. W przypadku komunikatów systemowych i zdarzeń inicjowanych przez administratorów wyższego poziomu inicjator jest pokazywany jako **System**.

- **Dzierżawca inicjatora**

  Nazwa dzierżawcy, do którego należy inicjator. W przypadku komunikatów systemowych i zdarzeń inicjowanych przez administratorów wyższego poziomu to pole pozostaje puste.
- **Metoda**

  Pokazuje, czy zdarzenie zostało zainicjowane za pomocą interfejsu internetowego czy za pośrednictwem interfejsu API.
- **Adres IP**

  Adres IP urządzenia, z którego zainicjowano zdarzenie.

## Filtrowanie i wyszukiwanie

Zdarzenia można filtrować według typu, ważności lub daty. Można też je przeszukiwać według nazwy, obiektu, dzierżawcy, inicjatora i dzierżawcy inicjatora.

# Pakiety ochrony zaawansowanej

Pakiety ochrony zaawansowanej można włączyć jako uzupełnienie usługi Ochrona i korzystanie z nich podlega dodatkowym opłatom. Pakiety ochrony zaawansowanej udostępniają unikatowe funkcje, które nie pokrywają się z zestawem funkcji standardowych ani z innymi pakietami zaawansowanymi. Klienci mogą chronić obciążenia za pomocą jednego, kilku lub wszystkich pakietów zaawansowanych. Pakiety ochrony zaawansowanej są dostępne w obu trybach rozliczeń usługi Ochrona — Za obciążenie i Za gigabajt.

Funkcje Advanced File Sync & Share można włączyć w ramach usługi File Sync & Share. Są one dostępne w obu trybach rozliczeń: Za użytkownika i Za gigabajt.

Można włączyć następujące pakiety ochrony zaawansowanej:

- Zaawansowane tworzenie kopii zapasowych
- Zarządzanie zaawansowane
- Zabezpieczenia zaawansowane
- Zabezpieczenia zaawansowane + EDR
- Zaawansowane zapobieganie utracie danych
- Zaawansowane odzyskiwanie po awarii
- Zaawansowana ochrona poczty e-mail
- Advanced File Sync & Share

**Uwaga**
Pakietów zaawansowanych można używać tylko pod warunkiem, że jest włączona funkcja, którą rozszerzają. Użytkownicy nie mogą korzystać z funkcji zaawansowanej, jeśli standardowa funkcja usługi jest wyłączona. Na przykład nie mogą korzystać z funkcji pakietu Zaawansowane kopie zapasowe, jeśli jest wyłączona funkcja Ochrona.

Jeśli jest włączony pakiet ochrony zaawansowanej, jego funkcje będą widoczne w planie ochrony i oznaczone ikoną funkcji zaawansowanej . Próba włączenia tej funkcji spowoduje wyświetlenie komunikatu o związanych z nią rozliczeniach.

Jeśli pakiet ochrony zaawansowanej nie jest włączony, ale jest włączona sprzedaż dodatkowa, to funkcje ochrony zaawansowanej są widoczne w planie ochrony, ale nie są dostępne i nie można z nich korzystać. Obok nazwy funkcji jest wyświetlana następująca ikona . Użytkownicy zobaczą komunikat z monitem o skontaktowanie się z administratorem w celu włączenia wymaganego zestawu funkcji zaawansowanych.

Jeśli pakiet ochrony zaawansowanej nie jest włączony i jest wyłączona sprzedaż dodatkowa, klienci nie będą widzieć funkcji zaawansowanych w swoich planach ochrony.

# Standardowo udostępniane funkcje i pakiety zaawansowane usługi Cyber Protect

Włączając usługę lub zestaw funkcji w usłudzeCyber Protect, włączasz pewne funkcje, które są standardowo zawarte w usłudze i domyślnie dostępne. Możesz też włączyć pakiety ochrony zaawansowanej.

Poniższe sekcje zawierają ogólne informacje o funkcjach i pakietach zaawansowanych usługi Cyber Protect. Pełną listę ofert można znaleźć w Podręczniku licencjonowania rozwiązania Cyber Protect.

## Standardowo udostępniane i zaawansowane funkcje usługi Ochrona

Standardowo udostępniane i zaawansowane funkcje usługi Ochrona

| Grupa funkcji | Funkcje standardowo udostępniane | Funkcje zaawansowane |
|---|---|---|
| Zabezpieczenia | • Wynik #CyberFit<br>• Ocena luk w zabezpieczeniach<br>• Ochrona przed atakami ransomware: Active Protection<br>• Ochrona przed wirusami i złośliwym oprogramowaniem: Wykrywanie plików w chmurze na podstawie sygnatur (brak ochrony w czasie rzeczywistym, tylko skanowanie zaplanowane)*<br>• Ochrona przed wirusami i złośliwym oprogramowaniem: Moduł analizy plików przed wykonaniem oparty na sztucznej inteligencji, mechanizm cybernetyczny oparty na zachowaniach<br>• Zarządzanie programem Windows Defender<br><br>* Do wykrywania ataków zero day usługa Cyber Protect wykorzystuje heurystyczne reguły i algorytmy skanowania w poszukiwaniu złośliwych poleceń. | Dostępne są dwa pakiety ochrony zaawansowanej: **Zabezpieczenia zaawansowane** i **Zabezpieczenia zaawansowane + EDR**.<br><br>Pakiet Advanced Security obejmuje następujące elementy:<br><br>• Ochrona przed wirusami i złośliwym oprogramowaniem z lokalnym wykrywaniem plików opartym na sygnaturach (z ochroną w czasie rzeczywistym)<br>• Ochrona przed exploitami<br>• Filtrowanie adresów URL<br>• Zarządzanie zaporą w punktach końcowych<br>• Kopie zapasowe na potrzeby analizy śledczej, skanowanie kopii zapasowych pod kątem złośliwego oprogramowania, bezpieczne odzyskiwanie, firmowa lista dozwolonych<br>• Inteligentne plany ochrony (integracja z alertami CPOC)<br>• Scentralizowane skanowanie kopii zapasowych pod kątem złośliwego oprogramowania<br>• Wymazywanie zdalne<br><br>Pakiet ochrony Zabezpieczenia |

| Grupa funkcji | Funkcje standardowo udostępniane | Funkcje zaawansowane |
|---|---|---|
| | | zaawansowane + EDR obejmuje wszystkie powyższe funkcje oraz następujące funkcje modułu Endpoint Detection and Response (EDR) umożliwiające identyfikowanie zaawansowanych zagrożeń lub już prowadzonych ataków:<br>• Zarządzanie incydentami na scentralizowanej stronie incydentów<br>• Wizualizowanie zakresu i wpływu incydentów<br>• Zalecenia i kroki naprawcze<br>• Sprawdzanie pod kątem ujawnionych publicznie ataków na używane obciążenia za pomocą kanałów dotyczących zagrożeń<br>• Przechowywanie zdarzeń zabezpieczeń przez 180 dni<br>Informacje na temat włączania pakietu Zabezpieczenia zaawansowane + EDR można znaleźć w sekcji "Włączanie pakietu Zabezpieczenia zaawansowane + EDR" (s. 136). |
| Ochrona przed utratą danych | • Kontrola urządzeń | • Zapobieganie utracie danych z obciążeń uwzględniające zawartość obsługiwane za pośrednictwem urządzeń peryferyjnych i komunikacji sieciowej<br>• Wbudowane automatyczne wykrywanie danych osobowych (personally identifiable information, PII), chronionych informacji dotyczących zdrowia (protected health information, PHI) oraz danych zgodnych z normą bezpieczeństwa danych w branży kart płatniczych (Payment Card Industry Data Security Standard, PCI DSS), a także dokumentów z kategorii „Oznaczono jako poufne”<br>• Automatyczne tworzenie zasad zapobiegania utracie danych z opcjonalną pomocą dla użytkownika |

| Grupa funkcji | Funkcje standardowo udostępniane | Funkcje zaawansowane |
|---|---|---|
| | | • Adaptacyjne wdrażanie zapobiegania utracie danych z automatycznym korygowaniem zasad dzięki uczeniu się<br>• Centralne, oparte na chmurze tworzenie dzienników inspekcji, generowanie alertów i powiadamianie użytkowników |
| Zarządzanie | • Grupowe zarządzanie obciążeniami<br>• Scentralizowane zarządzanie planami ochrony<br>• Inwentaryzacja sprzętu<br>• Zdalne sterowanie<br>• Zdalnie wykonywane czynności<br>• Jednoczesne połączenia na technika<br>• Protokół połączenia zdalnego: RDP | • Zarządzanie poprawkami<br>• Kondycje dysków<br>• Inwentaryzacja oprogramowania<br>• Bezpieczne dla plików instalowanie poprawek<br>• Skrypty cybernetyczne<br>• Pomoc zdalna<br>• Przesyłanie i udostępnianie plików<br>• Wybieranie sesji do połączenia<br>• Obserwowanie obciążeń w multiwidoku<br>• Tryby połączeń: sterowanie, obserwowanie i zasłona<br>• Połączenie przez aplikację Quick Assist<br>• Protokoły połączeń zdalnych: NEAR i Udostępnianie ekranu<br>• Nagrywanie sesji w przypadku połączeń NEAR<br>• Przesyłanie zrzutu ekranu<br>• Raport z historii sesji |
| Ochrona poczty e-mail | Brak | Ochrona w czasie rzeczywistym dla skrzynek pocztowych Microsoft 365 i Gmail:<br>• Ochrona przed złośliwym oprogramowaniem Ochrona przed spamem<br>• Skanowanie adresów URL w wiadomościach e-mail<br>• Analiza DMARC<br>• Ochrona przed phishingiem<br>• Ochrona przed podszywaniem się<br>• Skanowanie załączników |

| Grupa funkcji | Funkcje standardowo udostępniane | Funkcje zaawansowane |
|---|---|---|
| | | • Rozbrajanie i rekonstrukcja zawartości<br>• Schemat relacji zaufania<br><br>Zobacz podręcznik konfiguracji. |
| Cyber Disaster Recovery Cloud | Standardowe funkcje odzyskiwania po awarii można wykorzystać do testowania różnych scenariuszy odzyskiwania obciążeń po wystąpieniu awarii.<br><br>Należy zwrócić uwagę na dostępność funkcji odzyskiwania po awarii i ich ograniczenia:<br><br>• Testowe przełączanie awaryjne w odizolowanym środowisku sieciowym. Ograniczenie do 32 punktów obliczeniowych miesięcznie i 5 jednoczesnych testowych operacji przełączania awaryjnego.<br>• Konfiguracje serwerów odzyskiwania: 1 procesor i 2 GB pamięci RAM, 1 procesor i 4 GB pamięci RAM oraz 2 procesory i 8 GB pamięci RAM.<br>• Liczba punktów odzyskiwania dostępnych w przypadku przełączania awaryjnego: tylko ostatni punkt odzyskiwania, który jest dostępny zaraz po utworzeniu kopii zapasowej.<br>• Dostępne tryby łączności: Tylko chmura i Point-to-site.<br>• Dostępność bramy VPN: Brama VPN zostanie tymczasowo zawieszona, jeśli będzie nieaktywna przez 4 godziny po zakończeniu ostatniego testowego przełączania awaryjnego, i zostanie ponownie wdrożona po rozpoczęciu testowego przełączania awaryjnego.<br>• Liczba sieci w chmurze: 1.<br>• Dostęp do Internetu<br>• Operacje przy użyciu runbooków: tworzenie i edycja. | Można włączyć pakiet Zaawansowane odzyskiwanie po awarii i chronić obciążenia przy użyciu pełnej gamy funkcji odzyskiwania po awarii.<br><br>Należy zwrócić uwagę na dostępne zaawansowane funkcje odzyskiwania:<br><br>• Produkcyjne przełączanie awaryjne<br>• Testowe przełączanie awaryjne w odizolowanym środowisku sieciowym.<br>• Liczba punktów odzyskiwania dostępnych na potrzeby przełączania awaryjnego: wszystkie punkty odzyskiwania dostępne po utworzeniu serwera odzyskiwania.<br>• Serwery podstawowe<br>• Konfiguracje serwera odzyskiwania/podstawowego: Brak ograniczeń<br>• Dostępne tryby łączności: Tylko chmura, Point-to-site, Open VPN site-to-site i IPsec VPN multi-site.<br>• Dostępność bramy VPN: stała.<br>• Liczba sieci w chmurze: 23.<br>• Publiczne adresy IP<br>• Dostęp do Internetu<br>• Operacje przy użyciu runbooków: tworzenie, edycja i wykonywanie. |

## Dostępne w modelu płatności zgodnie z rzeczywistym wykorzystaniem i zaawansowane funkcje usługi Ochrona

Dostępne w modelu płatności zgodnie z rzeczywistym wykorzystaniem i zaawansowane funkcje usługi Ochrona

| Grupa funkcji | Funkcje dostępne w modelu płatności zgodnie z rzeczywistym wykorzystaniem | Funkcje zaawansowane |
|---|---|---|
| Kopia zapasowa | • Kopia zapasowa plików<br>• Kopie zapasowe obrazów<br>• Kopie zapasowe aplikacji<br>• Tworzenie kopii zapasowych udziałów sieciowych<br>• Tworzenie kopii zapasowych w magazynie w środowisku chmurowym<br>• Tworzenie kopii zapasowych w magazynie lokalnym<br><br>**Uwaga**<br>Naliczane są opłaty za wykorzystanie pamięci w chmurze. | • Microsoft SQL Server i klastry programu Microsoft Exchange<br>• Baza danych Oracle<br>• SAP HANA<br>• Mapa ochrony danych<br>• Ciągła ochrona danych<br>• Plany przetwarzania danych poza hostem<br>• Notaryzowanie kopii zapasowych<br>• Stanowiska Microsoft 365<br>• Stanowiska Google Workspace |
| File Sync & Share | • Przechowywanie zaszyfrowanej zawartości w formie plików<br>• Synchronizowanie plików na wskazanych urządzeniach<br>• Udostępnianie folderów i plików wyznaczonym osobom i systemom | • Notaryzacja i e-podpis<br>• Szablony dokumentów*<br><br>* Kopie zapasowe plików przeznaczonych do synchronizacji i udostępniania |
| Fizyczne dostarczanie danych | Funkcja Fizyczne dostarczanie danych | N.d. |
| Notary | • Notaryzowanie plików<br>• Elektroniczne podpisywanie plików<br>• Szablony dokumentów | N.d. |

**Uwaga**
Nie można włączyć pakietów ochrony zaawansowanej bez włączenia funkcji ochrony standardowej, którą one rozszerzają. Jeśli wyłączysz daną funkcję, jej pakiety zaawansowane zostaną automatycznie wyłączone, a korzystające z nich plany ochrony zostaną automatycznie odwołane. Jeśli na przykład wyłączysz funkcję Ochrona, jej pakiety zaawansowane zostaną automatycznie wyłączone, a wszystkie korzystające z nich plany zostaną automatycznie odwołane.

Użytkownicy nie mogą korzystać z pakietów ochrony zaawansowanej, jeśli nie mają włączonej ochrony standardowej — mogą korzystać tylko z zawartych w usłudze funkcji ochrony standardowej oraz pakietów zaawansowanych zastosowanych do określonych obciążeń. W takiej sytuacji opłaty będą naliczane jedynie za używane przez nich pakiety zaawansowane.

Informacje na temat rozliczeń można znaleźć w sekcji "Tryby rozliczeń dotyczące rozwiązania Cyber Protect" (s. 8).

# Zaawansowane zapobieganie utracie danych

Moduł Zaawansowane zapobieganie utracie danych zapobiega wyciekowi informacji wrażliwych ze stacji roboczych, serwerów i maszyn wirtualnych dzięki sprawdzaniu zawartości danych przesyłanych przez kanały lokalne i sieciowe i stosowanie opracowanych specjalnie dla danej organizacji reguł przepływów danych.

Zanim zaczniesz korzystać z modułu Zaawansowane zapobieganie utracie danych, koniecznie zapoznaj się z podstawowymi pojęciami oraz logiką zarządzania tym modułem, które opisano w podręczniku Podstawowe informacje.

Warto też zapoznać się z dokumentem Dane techniczne.

## Włączanie usługi Zaawansowane zapobieganie utracie danych

Usługa Zaawansowane zapobieganie utracie danych jest domyślnie włączona w konfiguracji dla nowych dzierżawców. Jeśli ta funkcja zostanie wyłączona podczas tworzenia dzierżawcy, administratorzy partnera mogą ją później włączyć.

***Aby włączyć usługę Zaawansowane zapobieganie utracie danych***

1. W konsoli zarządzania Cyber Protect Cloud przejdź do sekcji **Klienci**.
2. Wybierz dzierżawcę do edycji.
3. W sekcji **Wybierz usługi** przewiń do pozycji **Ochrona** i w obszarze trybu rozliczeń, który chcesz zastosować, zaznacz **Zaawansowane zapobieganie utracie danych**.
4. W obszarze Konfiguruj usługi przewiń do sekcji **Zaawansowane zapobieganie utracie danych** i skonfiguruj limity.
   Domyślnie jest wybrana opcja Bez ograniczeń.
5. Zapisz ustawienia.

# Zabezpieczenia zaawansowane + Zaawansowana ochrona EDR

Moduł Endpoint Detection and Response (EDR) wykrywa podejrzane działania na obciążeniach, w tym dotąd niezauważone ataki, i generuje incydenty. Incydenty te udostępniają szczegółowy przegląd każdego ataku, co ułatwia ustalenie, jak doszło do ataku i jak można zapobiec jego ponownemu wystąpieniu. Dzięki przystępnym interpretacjom każdego etapu ataku dochodzenie w jego sprawie zajmuje znacznie mniej czasu — staje się kwestią minut.

## Włączanie pakietu Zabezpieczenia zaawansowane + EDR

Jako administrator partnera możesz włączyć pakiet ochrony Zabezpieczenia zaawansowane + EDR, aby udostępnić funkcje wykrywania i reagowania w punktach końcowych (Endpoint detection and response, EDR) w planach ochrony klienta.

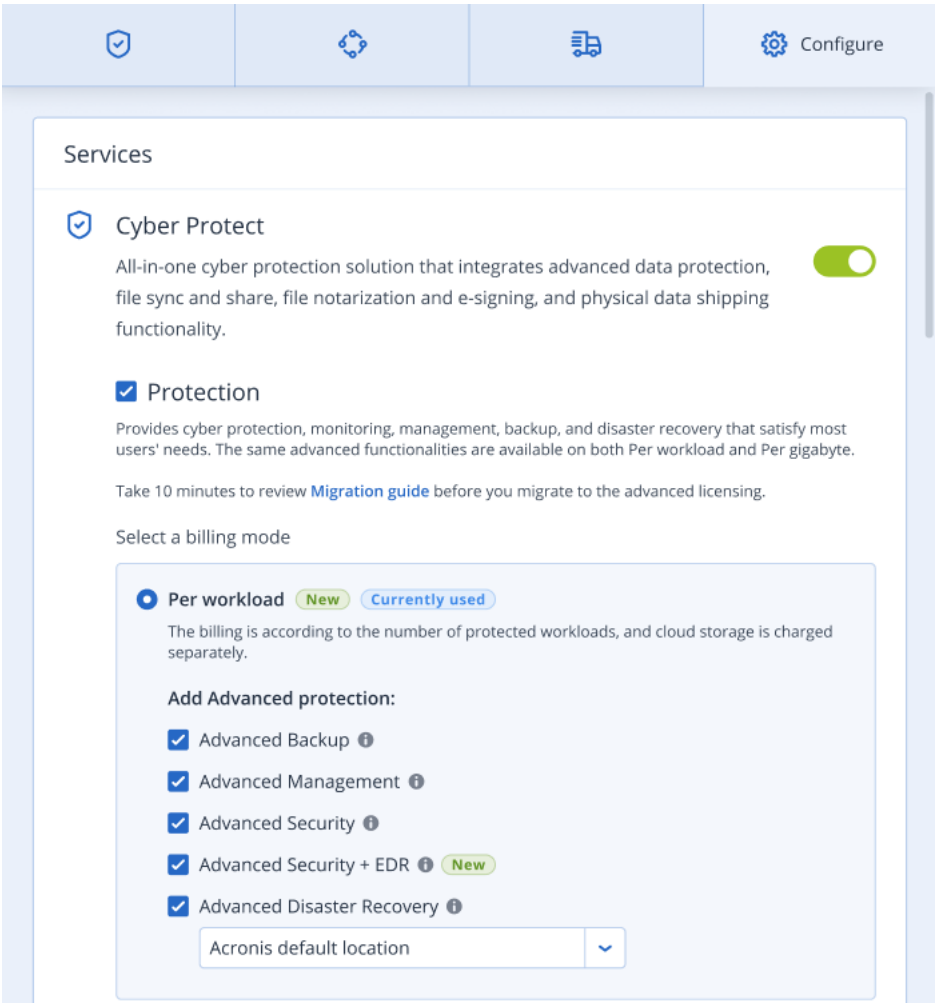
***Aby włączyć pakiet Zabezpieczenia zaawansowane + EDR***

1. Zaloguj się do portalu zarządzania.

   **Uwaga**
   Jeśli zostanie wyświetlony monit, wybierz klienty, do których chcesz zastosować pakiet ochrony Zabezpieczenia zaawansowane + EDR, a następnie kliknij **Włącz**.

2. W lewym panelu nawigacyjnym kliknij **KLIENCI**.
3. W obszarze Cyber Protect kliknij kartę **Ochrona**.
   Zostanie wyświetlona lista już istniejących klientów subskrybujących usługę Ochrona.
4. Kliknij klienta, do którego chcesz dodać pakiet Zabezpieczenia zaawansowane + EDR.
   Na karcie **Konfiguruj** w sekcji Ochrona koniecznie zaznacz pole wyboru **Zabezpieczenia**

**zaawansowane + EDR**.




# Zaawansowane odzyskiwanie po awarii

Można włączyć pakiet Zaawansowane odzyskiwanie po awarii i chronić obciążenia przy użyciu pełnej gamy funkcji odzyskiwania po awarii.

Dostępne są następujące zaawansowane funkcje modułu Odzyskiwanie po awarii:

- Produkcyjne przełączanie awaryjne
- Testowe przełączanie awaryjne w odizolowanym środowisku sieciowym.
- Liczba punktów odzyskiwania dostępnych na potrzeby przełączania awaryjnego: wszystkie punkty odzyskiwania dostępne po utworzeniu serwera odzyskiwania.
- Serwery podstawowe
- Konfiguracje serwera odzyskiwania/podstawowego: Brak ograniczeń
- Dostępne tryby łączności: Tylko chmura, Point-to-site, Open VPN site-to-site i IPsec VPN multi-site.
- Dostępność bramy VPN: stała.
- Liczba sieci w chmurze: 23.

- Publiczne adresy IP
- Dostęp do Internetu
- Operacje przy użyciu runbooków: tworzenie, edycja i wykonywanie.

## Zaawansowana ochrona poczty e-mail

Zaawansowana ochrona poczty e-mail umożliwia chronienie skrzynek pocztowych Microsoft 365, Google Workspace lub Open-Xchange w czasie rzeczywistym:

- Ochrona przed złośliwym oprogramowaniem i Ochrona przed spamem
- Skanowanie adresów URL w wiadomościach e-mail
- Analiza DMARC
- Ochrona przed phishingiem
- Ochrona przed podszywaniem się
- Skanowanie załączników
- Rozbrajanie i rekonstrukcja zawartości
- Schemat relacji zaufania

Dodatkowe informacje na temat funkcji Zaawansowana ochrona poczty e-mail można znaleźć na karcie produktu Zaawansowana ochrona poczty e-mail.

Instrukcje konfiguracji można znaleźć w sekcji Zaawansowana ochrona poczty e-mail z rozwiązaniem Perception Point.

# Integracje

## Integracja z systemami innych firm

Dostawca usług może zintegrować platformę Cyber Protect Cloud z systemem innej firmy:

- Przez skonfigurowanie rozszerzenia platformy w tym systemie.

  Na stronie **Integracja** portalu zarządzania znajdują się rozszerzenia dostępne w przypadku najpopularniejszych systemów do automatyzacji usług profesjonalnych (Professional Services Automations, PSA) i systemów zdalnego monitorowania i zarządzania (Remote Monitoring and Management, RMM).

  To jest zalecana metoda integracji platformy.
- Przez utworzenie klienta API dla systemu, a tym samym umożliwienie systemowi dostępu do interfejsów programowania aplikacji (API) platformy i jej usług. Klienty API stanowiących część środowiska autoryzacji OAuth 2.0 platformy. Więcej informacji na temat OAuth 2.0 można znaleźć na stronie https://tools.ietf.org/html/rfc6749 .

  Jest to niskopoziomowa metoda integracji platformy, która wymaga umiejętności programistycznych. Zalecamy jej wybranie w przypadku braku rozszerzenia platformy dla danego systemu lub w sytuacji, gdy system musi zostać dostosowany do takich metod zarządzania platformą i jej usługami, które nie są uwzględnione w dostępnym rozszerzeniu.

### Konfigurowanie integracji dla platformy Cyber Protect Cloud

1. Zaloguj się do portalu zarządzania.
2. Przejdź do pozycji **Integracje** w głównym menu nawigacyjnym.
3. Kliknij nazwę systemu innej firmy, którego dotyczy aktywowana integracja.
4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Więcej informacji na temat dostępnych integracji z systemami innych firm, w tym szczegółową dokumentację, można znaleźć pod adresem https://solutions.acronis.com.

### Zarządzanie klientami API

Istnieje możliwość zintegrowania systemów innych firm z platformą Cyber Protect Cloud za pomocą jej interfejsów programowania aplikacji (application programming interface, API). Dostęp do interfejsów API można uzyskać za pośrednictwem klientów API, które stanowią integralną część środowiska autoryzacji OAuth 2.0 tej platformy.

#### Co to jest klient API?

Klient API to specjalne konto na platformie przeznaczone do reprezentowania systemu zewnętrznego, który musi się uwierzytelnić oraz uzyskać prawa dostępu do danych w interfejsach API platformy i jej usług.

Dostęp klienta jest ograniczony do dzierżawcy, w którego ramach administrator tworzy klienta, a także jego poddzierżawców.

Tworzony klient dziedziczy role usług konta administratora i ról tych nie można później zmienić. Zmiana lub wyłączenie ról konta administratora nie wpływa na klienta.

Poświadczenia klienta obejmują unikatowy identyfikator (ID) oraz wartość tajną. Te poświadczenia nie wygasają i nie można ich używać do logowania się do portalu zarządzania czy którejkolwiek konsoli usługi. Wartość tajną można zresetować.

Dla klienta nie można włączyć uwierzytelniania dwuskładnikowego.

## Standardowa procedura integracji

1. Administrator tworzy klienta API w ramach dzierżawcy, którym będzie zarządzać system zewnętrzny.
2. Administrator włącza przepływ poświadczeń klienta OAuth 2.0 w systemie zewnętrznym.

   Zgodnie z tym przepływem przed uzyskaniem dostępu do dzierżawcy i jego usług za pośrednictwem interfejsu API system powinien najpierw wysłać do platformy poświadczenia utworzonego klienta za pośrednictwem autoryzacyjnego interfejsu API. Platforma generuje i wysyła systemowi token zabezpieczeń, czyli unikatowy ciąg kryptograficzny przypisany do tego konkretnego klienta. Potem system musi dodawać ten token do wszystkich żądań API.

   Token zabezpieczeń eliminuje konieczność przekazywania poświadczeń klienta razem z żądaniami API. Dla dodatkowego bezpieczeństwa token wygasa po dwóch godzinach. Gdy się to stanie, wszystkie żądania API z wygasłym tokenem zakończą się niepowodzeniem i system będzie zażądać od platformy nowego tokenu.

Więcej informacji na temat korzystania z autoryzacyjnego interfejsu API i interfejsów API platformy można znaleźć w podręczniku dewelopera pod adresem https://developer.acronis.com/doc/account-management/v2/guide/index.

## Tworzenie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API** > **Utwórz klienta API**.
3. Wprowadź nazwę klienta API.
4. Kliknij **Dalej**.

   Klient API jest domyślnie tworzony ze statusem **Aktywny**.
5. Skopiuj i zapisz identyfikator oraz wartość tajną klienta, a także adres URL centrum danych. Dane te będą potrzebne do włączenia przepływu poświadczeń klienta OAuth 2.0 w systemie zewnętrznym.

   **Ważne**

   Ze względów bezpieczeństwa wartość tajna jest wyświetlana tylko raz. W razie utraty tej wartości

nie da się jej odzyskać — można ją tylko zresetować.

6. Kliknij **Gotowe**.

## Resetowanie wartości tajnej klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij ••• , a następnie **Resetuj klucz tajny**.
5. Potwierdź decyzję, klikając **Dalej**.

   Zostanie wygenerowana nowa wartość tajna. Identyfikator klienta i adres URL centrum danych się nie zmienią.

   Wszystkie tokeny zabezpieczeń przypisane do tego klienta natychmiast wygasną, a żądania API z tymi tokenami zakończą się niepowodzeniem.
6. Skopiuj i zapisz nową wartość tajną klienta.

   **Ważne**
   Ze względów bezpieczeństwa wartość tajna jest wyświetlana tylko raz. W razie utraty tej wartości nie da się jej odzyskać — można ją tylko zresetować.

7. Kliknij **Gotowe**.

## Wyłączanie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij ••• , a następnie kliknij **Wyłącz**.
5. Potwierdź decyzję.

   Status klienta zostanie zmieniony na **Wyłączono**.

   Żądania API z tokenami zabezpieczeń przypisanymi do tego klienta zakończą się niepowodzeniem, ale tokeny nie wygasną od razu. Wyłączenie klienta nie ma wpływu na czas ważności tokenów.

   W każdej chwili będzie można ponownie włączyć tego klienta.

## Włączanie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.

3. Znajdź pożądanego klienta na liście.
4. Kliknij ••• , a następnie kliknij **Włącz**.

   Status klienta zostanie zmieniony na **Włączono**.

   Jeśli tokeny jeszcze nie wygasły, żądania API z tokenami zabezpieczeń przypisanymi do tego klienta zakończą się powodzeniem.

## Usuwanie klienta API

1. Zaloguj się do portalu zarządzania.
2. Kliknij **Ustawienia** > **Klienty API**.
3. Znajdź pożądanego klienta na liście.
4. Kliknij ••• , a następnie kliknij **Usuń**.
5. Potwierdź decyzję.

   Wszystkie tokeny zabezpieczeń przypisane do tego klienta natychmiast wygasną, a żądania API z tymi tokenami zakończą się niepowodzeniem.

   **Ważne**
   Usuniętego klienta nie da się odzyskać.

# Informacje na temat integracji

W poniższej tabeli zestawiono zaimplementowane integracje z rozwiązaniami innych firm oraz łącza do odpowiedniej dokumentacji.

| NAZWA INTEGRACJI | Wyświetl online | Otwórz plik PDF |
|---|---|---|
| **Autotask PSA** | https://www.acronis.com/support/documentation/AutotaskPSA/ | https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf |
| **CloudBlue Commerce** | https://www.acronis.com/support/documentation/CloudBlueCommerce/ | https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf |
| **CloudBlue PSA** | https://www.acronis.com/support/documentation/CloudBluePSA/ | https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf |
| **ConnectWise Automate** | https://www.acronis.com/support/documentation/ConnectWiseAutomate/ | https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf |

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

| NAZWA INTEGRACJI | Wyświetl online | Otwórz plik PDF |
|---|---|---|
| **PRTG** | https://www.acronis.com/support/documentation/PRTG/ | https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf |
| **Service Now** | 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 |

# Integracja ze środowiskiem VMware Cloud Director

Dostawca usług może zintegrować środowisko VMware Cloud Director (wcześniej: VMware vCloud Director) z platformą Cyber Protect Cloud i udostępniać klientom gotowe rozwiązanie do tworzenia kopii zapasowych maszyn wirtualnych.

Integracja obejmuje następujące kroki:

1. Skonfigurowanie brokera wiadomości RabbitMQ dla środowiska VMware Cloud Director.

   Oprogramowanie RabbitMQ umożliwia synchronizowanie zmian wprowadzonych w środowisku VMware Cloud Director z platformą Cyber Protect Cloud.
2. Instalowanie wtyczki dla środowiska VMware Cloud Director.

   Wtyczka ta powoduje dodanie usługi Cyber Protection do interfejsu użytkownika środowiska VMware Cloud Director.
3. Wdrożenie agenta zarządzania.

   Agent zarządzania automatycznie mapuje organizacje VMware Cloud Director na dzierżawców-klientów na platformie Cyber Protect Cloud oraz administratorów organizacji na administratorów dzierżawców-klientów. Więcej informacji o organizacjach można znaleźć w artykule Creating an Organization in VMware Cloud Director (Tworzenie organizacji w środowisku ) w bazie wiedzy VMware Knowledge Base.

   Dzierżawcy-klienci są tworzeni w ramach dzierżawcy-partnera, dla którego jest konfigurowana integracja ze środowiskiem VMware Cloud Director. Nowi dzierżawcy-klienci znajdują się w trybie **Zablokowano** i administratorzy partnerów nie mogą nimi zarządzać na platformie Cyber Protect Cloud.

**Uwaga**
Na platformę Cyber Protect Cloud są mapowani tylko administratorzy organizacji z unikatowymi adresami e-mail w środowisku VMware Cloud Director.

4. Wdrożenie co najmniej jednego agenta kopii zapasowych.
   Agent kopii zapasowych udostępnia funkcje tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych w środowisku VMware Cloud Director.

Aby wyłączyć integrację między środowiskiem VMware Cloud Director a platformą Cyber Protect Cloud, skontaktuj się z zespołem pomocy technicznej.

# Ograniczenia

- Integracja ze środowiskiem VMware Cloud Director jest możliwa tylko w przypadku dzierżawców-partnerów w trybie zarządzania **Zarządzane przez dostawcę usługi**, których dzierżawca nadrzędny (jeśli istnieje) również używa trybu **Zarządzane przez dostawcę usługi**. Więcej informacji na temat typów dzierżawców i ich trybu zarządzania można znaleźć w sekcji "Tworzenie dzierżawcy" (s. 36).
  Każdy obecny bezpośredni partner może skonfigurować integrację ze środowiskiem VMware Cloud Director. Administratorzy partnerów mogą włączyć tę opcję również dla poddzierżawców, zaznaczając pole wyboru **Infrastruktura VMware Cloud Director należąca do partnera** podczas tworzenia podrzędnego dzierżawcy-partnera.
- W przypadku dzierżawcy-partnera, w ramach którego jest konfigurowana integracja ze środowiskiem VMware Cloud Director, musi być wyłączone uwierzytelnianie dwuskładnikowe.
- Administrator z rolą administratora organizacji w wielu organizacjach VMware Cloud Director może zarządzać tworzeniem kopii zapasowych i odzyskiwaniem tylko w przypadku jednego dzierżawcy-klienta w usłudze Cyber Protection.
- Konsola internetowa Cyber Protection zostanie otwarta w nowej karcie.

## Wymagania dotyczące oprogramowania

### Obsługiwane wersje środowiska VMware Cloud Director

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

### Obsługiwane przeglądarki internetowe

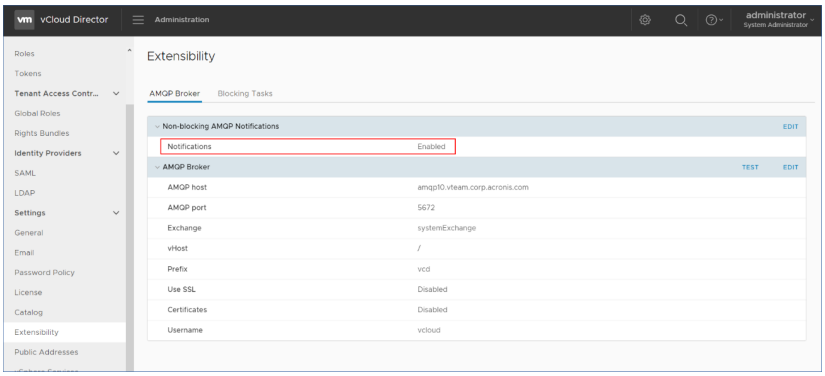
- Google Chrome 29 lub nowsza
- Mozilla Firefox 23 lub nowsza
- Opera 16 lub nowsza
- Microsoft Edge 25 lub nowsza
- Safari 8 lub nowsza w systemach operacyjnych macOS oraz iOS

W innych przeglądarkach internetowych (oraz w programie Safari działającym w innych systemach operacyjnych) interfejs użytkownika może być wyświetlany niepoprawnie lub niektóre funkcje mogą być niedostępne.

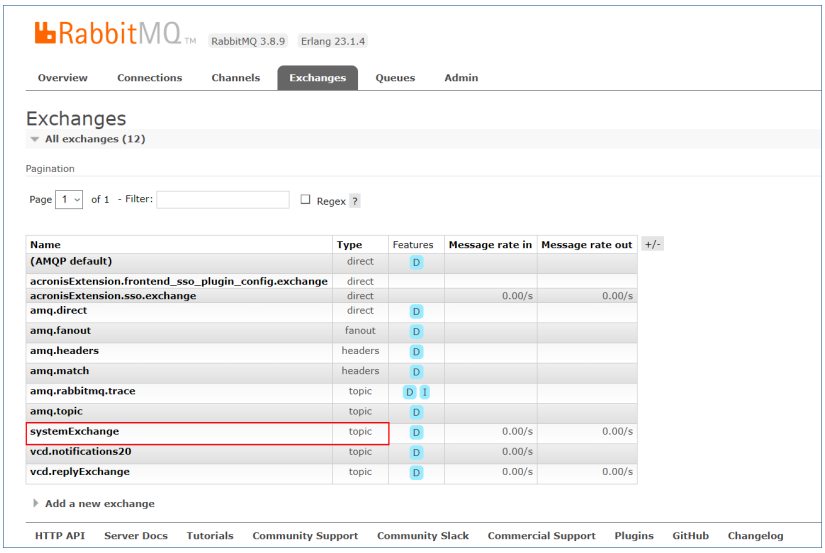
## Konfigurowanie brokera wiadomości RabbitMQ

1. Zainstaluj brokera AMQP RabbitMQ dla swojego środowiska VMware Cloud Director.

   Więcej informacji na temat instalacji oprogramowania RabbitMQ można znaleźć w dokumentacji środowiska VMware: Install and Configure a RabbitMQ AMQP Broker (Instalowanie i konfigurowanie brokera AMQP RabbitMQ).
2. Zaloguj się do portalu dostawców środowiska VMware Cloud Director jako administrator systemu.
3. Przejdź do sekcji **Administration** (Administracja) > **Extensibility** (Możliwości rozszerzeń) i sprawdź, czy w obszarze **Non-blocking AMQP Notifications** (Nieblokujące powiadomienia AMQP) jest włączona opcja **Notifications** (Powiadomienia).




4. Zaloguj się do konsoli zarządzania oprogramowania RabbitMQ jako administrator.
5. Na karcie **Exchanges** (Wymiany) sprawdź, czy została utworzona wymiana (domyślnie nosząca nazwę **SystemExchange**) i ma typ **topic** (temat).



## Instalowanie wtyczki dla środowiska VMware Cloud Director

1. Kliknij poniższe łącze, aby pobrać plik **vCDPlugin.zip**: https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Zaloguj się do portalu dostawców środowiska VMware Cloud Director jako administrator systemu.
3. W menu nawigacyjnym wybierz **Customize Portal** (Dostosuj portal).
4. Na karcie **Manage Plugins** (Zarządzaj wtyczkami) kliknij **Upload** (Prześlij).

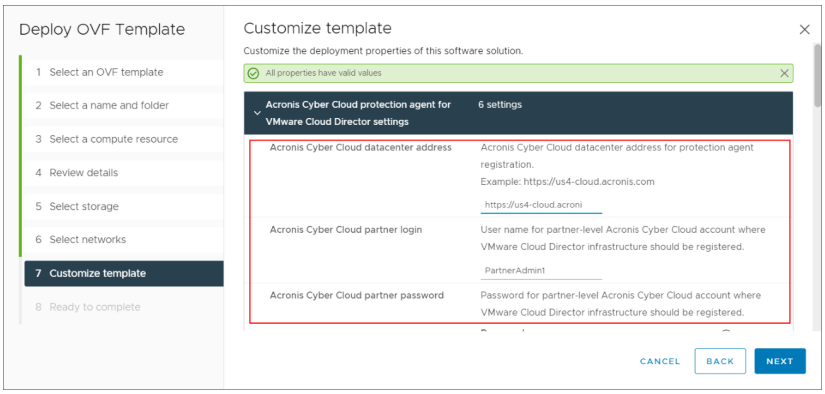
   Zostanie otwarty kreator **Upload Plugin** (Prześlij wtyczkę).
5. Kliknij **Select Plugin File** (Wybierz plik wtyczki), a następnie wybierz plik **vCDPlugin.zip**.
6. Kliknij **Dalej**.
7. Skonfiguruj zakres i ustawienia publikacji:
   a. W sekcji **Scope to** (Zakres dla) zaznacz tylko pole wyboru **Tenants** (Dzierżawcy).
   b. W sekcji **Publish to** (Opublikuj dla) wybierz **All tenants** (Wszyscy dzierżawcy), aby włączyć wtyczkę dla wszystkich obecnych i przyszłych dzierżawców, lub wybierz dzierżawców, dla których chcesz włączyć wtyczkę.
8. Kliknij **Dalej**.
9. Przejrzyj ustawienia i kliknij **Finish** (Zakończ).

## Instalowanie agenta zarządzania

1. Zaloguj się do portalu zarządzania  Cyber Protect Cloud jako administrator partnera.
2. Przejdź do sekcji **Ustawienia** > **Lokalizacja** i kliknij **Dodaj środowisko VMware Cloud Director**.
3. Kliknij łącze **Agent zarządzania** i pobierz plik ZIP.
4. Wyodrębnij plik szablonu agenta zarządzania `vCDManagementAgent.ovf` i plik wirtualnego dysku twardego `vCDManagementAgent-disk1.vmdk`.
5. W kliencie vSphere wdróż szablon OVF agenta zarządzania na hoście ESXi w ramach instancji środowiska vCenter zarządzanej przez środowisko VMware Cloud Director.

   **Ważne**
   Zainstaluj tylko jednego agenta zarządzania na środowisko VMware Cloud Director.

6. W kreatorze **Wdróż szablon OVF** skonfiguruj agenta zarządzania przy użyciu następujących ustawień:




a. Adres URL centrum danych  Cyber Protect Cloud. Na przykład `https://us5-cloud.example.com`.

b. Nazwa logowania i hasło administratora partnera.

c. Identyfikator magazynu kopii zapasowych dla maszyn wirtualnych w środowisku VMware Cloud Director. Magazyn ten może tylko należeć do partnera. Aby uzyskać więcej informacji na temat magazynów, zobacz "Zarządzanie lokalizacjami i magazynami" (s. 71).

   Aby sprawdzić identyfikator, w portalu zarządzania wybierz **Ustawienia** > **Lokalizacje**, a następnie zaznacz odpowiedni magazyn. Jego identyfikator będzie widoczny po cząstce **uuid=** adresu URL.

d. Tryb rozliczeń za platformę  Cyber Protect Cloud: **Za gigabajt** lub **Za obciążenie**.

   **Uwaga**
   Wybrany tryb rozliczeń dotyczy wszystkich nowo utworzonych dzierżawców-klientów.

e. Parametry środowiska VMware Cloud Director: adres infrastruktury, nazwa logowania i hasło administratora systemu.

f. Parametry oprogramowania RabbitMQ: adres serwera, port, nazwa hosta wirtualnego, nazwa logowania i hasło administratora.

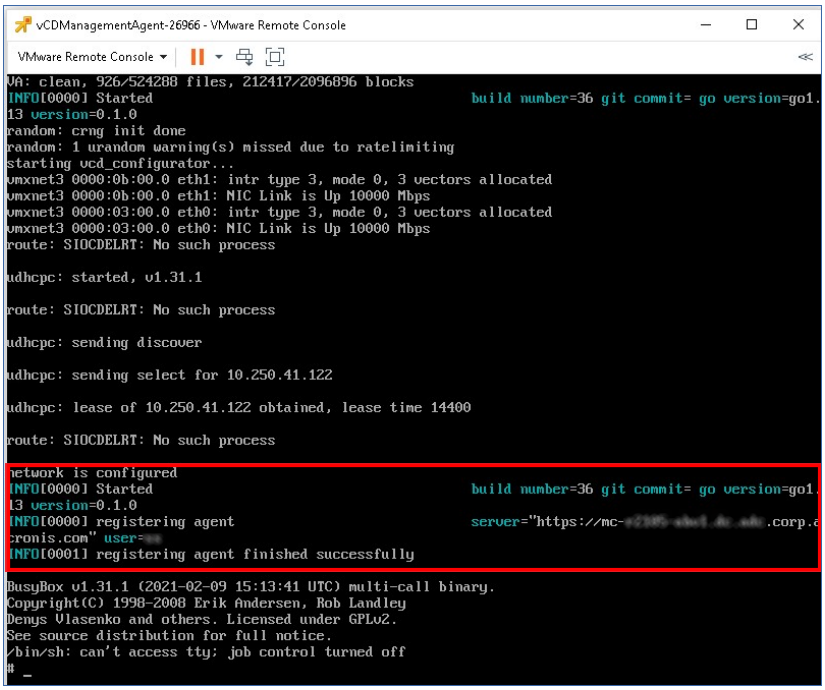
g. Parametry sieci: adres IP, maska podsieci, brama domyślna, DNS, sufiks DNS.

   Domyślnie jest włączony tylko jeden interfejs sieciowy. Aby włączyć drugi interfejs sieciowy, zaznacz pole wyboru obok pozycji **Włącz eth1**.

   **Uwaga**
   Upewnij się, że ustawienia sieciowe umożliwiają agentowi zarządzania dostęp do zarówno środowiska VMware Cloud Director, jak i centrum danych  Cyber Protect Cloud.

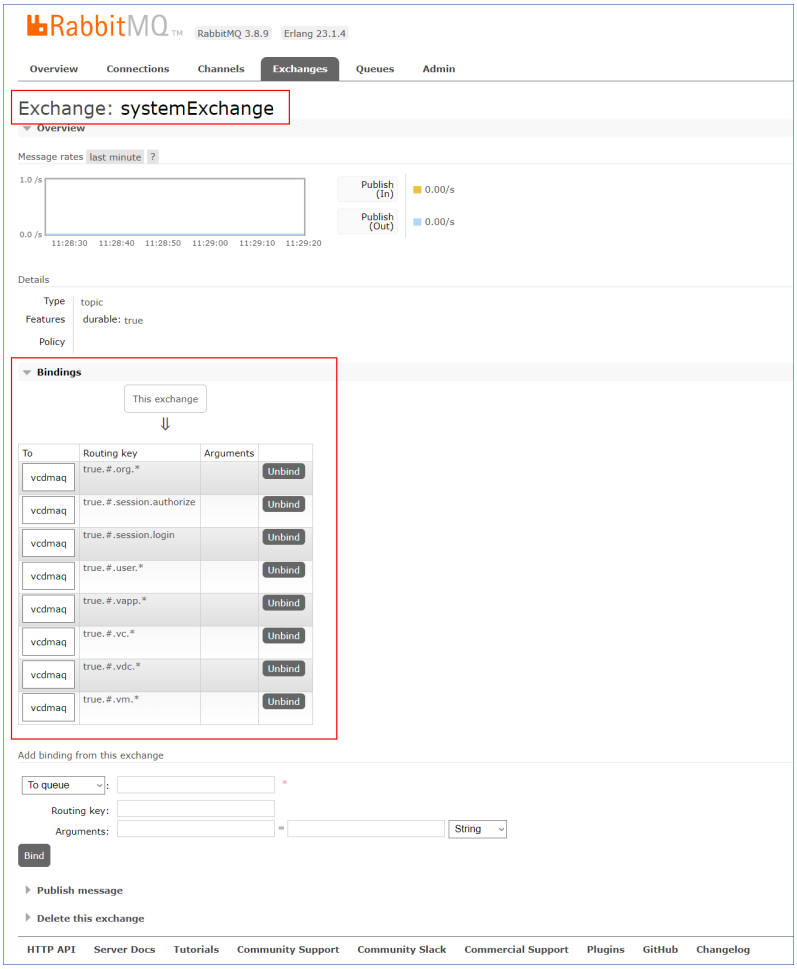
Parametry ustawień agenta zarządzania można też skonfigurować po początkowym wdrożeniu. W kliencie vSphere wyłącz maszynę wirtualną z agentem zarządzania, a następnie kliknij **Configure** (Konfiguruj) > **Settings** (Ustawienia) > **vApp Options** (Opcje obiektów vApp). Zastosuj odpowiednie ustawienia, a następnie włącz maszynę wirtualną z agentem zarządzania.

7. [Opcjonalnie] W kliencie vSphere otwórz konsolę maszyny wirtualnej z agentem zarządzania i sprawdź swoją konfigurację.




8. Sprawdź połączenie z oprogramowaniem RabbitMQ.
   a. Zaloguj się do konsoli zarządzania oprogramowania RabbitMQ jako administrator.
   b. Na karcie **Exchanges** (Wymiany) wybierz wymianę ustawioną podczas instalacji oprogramowania RabbitMQ. Domyślnie ma ona nazwę **systemExchange**.

c. Zweryfikuj powiązania z kolejką **vcdmaq**.




## Instalowanie agentów kopii zapasowych

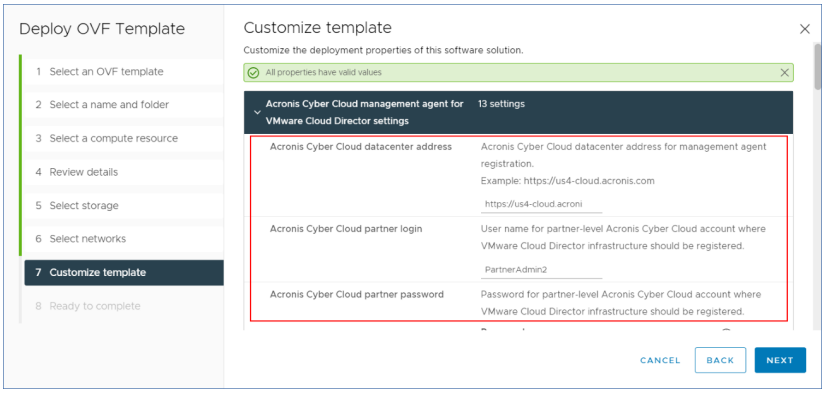
1. Zaloguj się do portalu zarządzania jako administrator partnera.
2. Przejdź do sekcji **Ustawienia** > **Lokalizacja** i kliknij **Dodaj środowisko VMware Cloud Director**.
3. Kliknij łącze **Agent kopii zapasowych** i pobierz plik ZIP.
4. Wyodrębnij plik szablonu agenta kopii zapasowych `vCDCyberProtectAgent.ovf` i plik wirtualnego dysku twardego `vCDCyberProtectAgent-disk1.vmdk`.
5. W kliencie vSphere wdróż szablon agenta kopii zapasowych na pożądanym hoście ESXi.

   Potrzebny jest co najmniej jeden agent kopii zapasowych na host. Domyślnie agentowi kopii zapasowych zostaje przypisane 8 GB pamięci RAM oraz 2 procesory i może on przetwarzać równolegle maksymalnie 10 zadań tworzenia kopii zapasowych lub odzyskiwania. Aby było możliwe przetwarzanie większej liczby zadań lub dystrybucja ruchu związanego z tworzeniem kopii zapasowych i odzyskiwaniem, należy wdrożyć na tym samym hoście dodatkowe agenty.

**Uwaga**

Operacje tworzenia kopii zapasowych maszyn wirtualnych na hostach ESXi, na których nie ma zainstalowanego agenta kopii zapasowych, zakończą niepowodzeniem z komunikatem o błędzie: „Upłynął limit czasu zadania”.

6. W kreatorze **Wdróż szablon OVF** skonfiguruj agenta kopii zapasowych przy użyciu następujących ustawień:




   a. Adres URL centrum danych  Cyber Protect Cloud. Na przykład `https://us5-cloud.example.com`.
   b. Nazwa logowania i hasło administratora partnera.
   c. Parametry środowiska VMware vCenter: adres serwera, nazwa logowania i hasło.

      Agent użyje tych poświadczeń, aby nawiązać połączenie z serwerem vCenter. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. Jeśli to niemożliwe, należy zadbać o dostęp do konta mającego niezbędne uprawnienia na serwerze vCenter.
   d. Parametry sieci: adres IP, maska podsieci, brama domyślna, DNS, sufiks DNS.

      Domyślnie jest włączony tylko jeden interfejs sieciowy. Aby włączyć drugi interfejs sieciowy, zaznacz pole wyboru obok pozycji **Włącz eth1**.

      **Uwaga**

      Upewnij się, że ustawienia sieciowe umożliwiają agentowi kopii zapasowych dostęp do zarówno serwera vCenter, jak i centrum danych  Cyber Protect Cloud.

   e. Limit pobierania: maksymalna szybkość pobierania (w Kb/s), która określa szybkość odczytu archiwum kopii zapasowej podczas operacji odzyskiwania. Wartość domyślna to „0” — bez ograniczeń.
   f. Limit przesyłania: maksymalna szybkość przesyłania (w Kb/s), która określa szybkość zapisu w archiwum kopii zapasowej podczas operacji tworzenia kopii zapasowej. Wartość domyślna to „0” — bez ograniczeń.

Parametry ustawień agenta kopii zapasowych można też skonfigurować po początkowym wdrożeniu. W kliencie vSphere wyłącz maszynę wirtualną z agentem kopii zapasowych, a następnie kliknij **Configure** (Konfiguruj) > **Settings** (Ustawienia) > **vApp Options** (Opcje

obiektów vApp). Zastosuj odpowiednie ustawienia, a następnie włącz maszynę wirtualną z agentem kopii zapasowych.

7. W kliencie vSphere upewnij się, że opcje **Host** i **Storage vMotion** są wyłączone w przypadku tej maszyny wirtualnej z agentem kopii zapasowych.

## Aktualizowanie agentów

***Aby zaktualizować agenta zarządzania***

1. Zaloguj się do portalu zarządzania Cyber Protect Cloud jako administrator partnera.
2. Przejdź do sekcji **Ustawienia** > **Lokalizacja** i kliknij **Dodaj środowisko VMware Cloud Director**.
3. Kliknij łącze **Agent zarządzania** i pobierz plik ZIP z najnowszym agentem.
4. Wyodrębnij plik szablonu agenta zarządzania `vCDManagementAgent.ovf` i plik wirtualnego dysku twardego `vCDManagementAgent-disk1.vmdk`.
5. W kliencie vSphere wyłącz maszynę wirtualną z obecnym agentem zarządzania.
6. Wdróż maszynę wirtualną z nowym agentem zarządzania przy użyciu najnowszych plików `vCDManagementAgent.ovf` i `vCDManagementAgent-disk1.vmdk`.
7. Skonfiguruj agenta zarządzania przy użyciu tych samych ustawień co w starym agencie.
8. [Opcjonalnie] Usuń maszynę wirtualną ze starym agentem zarządzania.

**Ważne**
Może być aktywny tylko jeden agent zarządzania na środowisko VMware Cloud Director.

***Aby zaktualizować agenta kopii zapasowych***

1. Zaloguj się do portalu zarządzania Cyber Protect Cloud jako administrator partnera.
2. Przejdź do sekcji **Ustawienia** > **Lokalizacja** i kliknij **Dodaj środowisko VMware Cloud Director**.
3. Kliknij łącze **Agent kopii zapasowych** i pobierz plik ZIP z najnowszym agentem.
4. Wyodrębnij plik szablonu agenta kopii zapasowych `vCDCyberProtectAgent.ovf` i plik wirtualnego dysku twardego `vCDCyberProtectAgent-disk1.vmdk`.
5. W kliencie vSphere wyłącz maszynę wirtualną z obecnym agentem kopii zapasowych.
   Wszystkie ewentualnie uruchomione zadania tworzenia kopii zapasowych i odzyskiwania zakończą się niepowodzeniem. Aby sprawdzić, czy są uruchomione jakieś zadania, w kliencie vSphere otwórz konsolę maszyny wirtualnej z agentem kopii zapasowych, a następnie wykonaj polecenie `ps | grep esx_worker`. Upewnij się, że nie ma żadnego aktywnego procesu `esx_worker`.
6. Wdróż maszynę wirtualną z nowym agentem kopii zapasowych przy użyciu najnowszych plików `vCDCyberProtectAgent.ovf` i `vCDCyberProtectAgent-disk1.vmdk`.
7. Skonfiguruj agenta kopii zapasowych przy użyciu tych samych ustawień co w starym agencie.
8. [Opcjonalnie] Usuń maszynę wirtualną ze starym agentem kopii zapasowych.

## Dostęp do konsoli internetowej Cyber Protection

Następujący administratorzy mogą zarządzać kopiami zapasowymi maszyn wirtualnych w ramach organizacji VMware Cloud Director:

- Administratorzy organizacji
- Specjalnie przypisani administratorzy kopii zapasowych
  Dodatkowe informacje na temat tworzenia takich administratorów można znaleźć w sekcji "Tworzenie administratora kopii zapasowych" (s. 154).

Administratorzy mogą uzyskiwać dostęp do swoich niestandardowych konsol internetowych Cyber Protection, klikając pozycję **Ochrona cybernetyczna** w menu nawigacyjnym portalu dzierżawców środowiska VMware Cloud Director.

**Uwaga**
Pojedyncze logowanie jest dostępne tylko dla administratorów organizacji i nie jest obsługiwane w przypadku administratorów systemu korzystających z portalu dzierżawców środowiska VMware Cloud Director.

W konsoli internetowej Cyber Protection administratorzy mogą uzyskiwać dostęp do elementów własnej organizacji VMware Cloud Director: wirtualnych centrów danych, obiektów vApp oraz poszczególnych maszyn wirtualnych. Mogą zarządzać tworzeniem kopii zapasowych i odzyskiwaniem zasobów organizacji VMware Cloud Director.

Administratorzy partnerów mogą uzyskiwać dostęp do konsol internetowych Cyber Protection swoich dzierżawców-klientów i zarządzać tworzeniem kopii zapasowych oraz odzyskiwaniem w ich imieniu.

## Ograniczenia

Lista ograniczeń może ulec zmianie w następnych wersjach platformy Cyber Protect Cloud.

### Kopia zapasowa

- Obsługiwane są tylko kopie zapasowe całego komputera. Nie ma możliwości stosowania filtrów plików ani wybierania dysków lub woluminów.
- Jako lokalizacja kopii zapasowych jest obsługiwana tylko chmura. Magazyn ten jest konfigurowany w ustawieniach agenta zarządzania i użytkownicy nie mogą go zmieniać w planie ochrony.
- Grupy dynamiczne nie są obsługiwane.
- Obsługiwane są następujące schematy tworzenia kopii zapasowych: **Zawsze przyrostowe (jeden plik)**, **Zawsze pełne** i **Tygodniowe pełne, dzienne przyrostowe**.
- Czyszczenie jest obsługiwane dopiero po utworzeniu kopii zapasowej.

### Odzyskiwanie

- Obsługiwane jest odzyskiwanie tylko na oryginalną maszynę wirtualną. Oryginalna maszyna wirtualna musi istnieć w środowisku VMware Cloud Director.
- Odzyskiwanie na poziomie plików nie jest obsługiwane.

## Tworzenie administratora kopii zapasowych

Administratorzy organizacji mogą delegować zarządzanie kopiami zapasowymi do specjalnie przypisanych administratorów kopii zapasowych.

***Aby utworzyć administratora kopii zapasowych***

1. W portalu dzierżawców VMware Cloud Director kliknij **Administracja** > **Role** > **Nowe**.
2. W oknie **Dodaj rolę** określ nazwę i opis nowej roli.
3. Przewiń w dół listę uprawnień i w sekcji **Inne** wybierz **Samoobsługujący się operator kopii zapasowych maszyn wirtualnych**.

   **Uwaga**
   Uprawnienie **Samoobsługujący się operator kopii zapasowych maszyn wirtualnych** staje się dostępne po zainstalowaniu wtyczki do portalu VMware Cloud Director. Dodatkowe informacje o tym, jak to zrobić, można znaleźć w sekcji "Instalowanie wtyczki dla środowiska VMware Cloud Director" (s. 147).

4. W portalu dzierżawców VMware Cloud Director kliknij **Użytkownicy**.
5. Wybierz użytkownika, a następnie kliknij **Edytuj**.
6. Przypisz temu użytkownikowi nowo utworzoną rolę.

W wyniku tego wybrany użytkownik będzie mógł zarządzać kopiami zapasowymi maszyn wirtualnych w ramach danej organizacji.

**Uwaga**
Administratorzy systemu środowiska VMware Cloud Director mogą zdefiniować globalną rolę z włączonym uprawnieniem **Samoobsługujący się operator kopii zapasowych maszyn wirtualnych**, a następnie ją opublikować dla dzierżawców. Dzięki temu administratorzy organizacji będą musieli jedynie przypisać tę rolę do użytkownika.

## Raport systemowy, pliki dzienników i pliki konfiguracyjne

Rozwiązanie napotkanego problemu może wymagać utworzenia raportu systemowego przy użyciu narzędzia `sysinfo` lub sprawdzenia plików dziennika i plików konfiguracyjnych na maszynie wirtualnej z agentem.

Dostęp do maszyny wirtualnej można uzyskać zarówno bezpośrednio, otwierając jej konsolę w kliencie vSphere, jak i zdalnie — za pośrednictwem klienta SSH. Aby uzyskać dostęp do maszyny wirtualnej za pośrednictwem klienta SSH, trzeba najpierw włączyć połączenie SSH z tą maszyną.

***Aby włączyć połączenie SSH z maszyną wirtualną***

1. W kliencie vSphere otwórz konsolę maszyny wirtualnej z agentem.
2. W wierszu polecenia uruchom polecenie `/bin/sshd`, aby uruchomić demona SSH.

W wyniku tego można nawiązać połączenie z tą maszyną wirtualną za pomocą klienta SSH, na przykład klienta WinSCP.

***Aby uruchomić narzędzie `sysinfo`***

1. Uzyskaj dostęp do maszyny wirtualnej z agentem.
   - Aby uzyskać do niej dostęp bezpośrednio, otwórz jej konsolę w kliencie vSphere.
   - Aby uzyskać do niej dostęp zdalnie, nawiąż połączenie z maszyną wirtualną za pośrednictwem klienta SSH.

     Użyj następującej domyślnej kombinacji „nazwa logowania:hasło”: `root`:`root`.
2. Przejdź do katalogu `/bin` i uruchom narzędzie `sysinfo`.

   ```
   # cd /bin/
   # ./sysinfo
   ```

   W wyniku tego plik raportu systemowego zostanie zapisany w katalogu domyślnym: `/var/lib/Acronis/sysinfo`.

   Możesz też określić inny katalog, uruchamiając narzędzie `sysinfo` z opcją `--target_dir`.

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```

3. Pobierz wygenerowany raport systemowy za pomocą klienta SSH.

***Aby uzyskać dostęp do pliku konfiguracyjnego***

1. Nawiąż połączenie z maszyną wirtualną za pośrednictwem klienta SSH.

   Użyj następującej domyślnej kombinacji „nazwa logowania:hasło”: `root`:`root`.
2. Pobierz odpowiedni plik.

   Pliki dzienników można znaleźć w następujących lokalizacjach:
   - Agent kopii zapasowych: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Agent zarządzania: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   Pliki konfiguracyjne można znaleźć w następujących lokalizacjach:
   - Agent kopii zapasowych: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Agent zarządzania: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

## Usuwanie integracji ze środowiskiem VMware Cloud Director

Procedura przywracania konfiguracji i wyrejestrowywanie instancji środowiska VMware Cloud Director z platformy Cyber Protect Cloud jest złożona. Aby uzyskać pomoc, skontaktuj się z przedstawicielem zespołu pomocy technicznej.

# Ustawienia ochrony prywatności

Ustawienia prywatności pomagają określić, czy wyrażasz zgodę na zbieranie, wykorzystywanie i ujawnianie Twoich danych osobowych.

W zależności od kraju, w którym korzystasz z usługi Cyber Protect, i centrum danych  Cyber Protect Cloud, które świadczy usługi, przy pierwszym uruchomieniu usługi Cyber Protect może pojawić się prośba o potwierdzenie, że zgadzasz się na korzystanie z usługi Google Analytics w usłudze Cyber Protect.

Usługa Google Analytics pomaga nam lepiej zrozumieć zachowanie użytkowników i poprawić środowisko użytkownika usługi Cyber Protect dzięki zbieraniu pseudonimizowanych danych.

Jeśli w interfejsie usługi Cyber Protect nie pojawiają się menu i informacje o zgodzie dotyczące usługi Google Analytics, oznacza to, że usługa Google Analytics nie jest używana w Twoim kraju.

W przypadku włączenia lub odmowy włączenia usługi Google Analytics przy pierwszym uruchomieniu usługi Cyber Protect, możesz później zmienić tę decyzję w dowolnym momencie.

***Aby włączyć lub wyłączyć usługę Google Analytics***

1. W konsoli Cyber Protect kliknij ikonę konta widoczną w prawym górnym rogu.
2. Wybierz **Moje ustawienia ochrony prywatności**.
3. W sekcji **Zbieranie danych przez narzędzie Google Analytics** kliknij jeden z następujących przycisków:
   - **Włącz**, aby włączyć usługę Google Analytics
   - **Wyłącz**, aby wyłączyć usługę Google Analytics

# Indeks

## W



## Z