Cyber Cloud

21.10

Gids voor partnerbeheerders

REVISIE: 1-11-2021

Inhoudsopgave

1 Over dit document

Dit document is bedoeld voor partnerbeheerders die Cyber Cloud willen gebruiken om hun klanten services te bieden.

Dit document beschrijft hoe u de services die beschikbaar zijn in Cyber Cloud, kunt instellen en beheren via de beheerportal.

2 Over Cyber Cloud

Cyber Cloud is een cloudplatform waarmee serviceproviders, resellers en distributeurs services voor gegevensbescherming kunnen leveren aan hun partners en klanten.

De services worden geleverd op diverse niveaus: vanaf partnerniveau tot op het niveau van klantbedrijven en eindgebruikers.

Het beheer van de services is beschikbaar via webapplicaties, de zogenaamde **serviceconsoles**. Het beheer van tenants en gebruikersaccounts is beschikbaar via een webapplicatie, de zogenaamde **beheerportal**.

Met de beheerportal kunnen beheerders:

- Het gebruik van services en toegang tot de serviceconsoles bewaken
- Tenants beheren
- Gebruikersaccounts beheren
- Services en quota's voor tenants configureren
- Opslag beheren
- Branding beheren
- Rapporten genereren over het servicegebruik

2.1 Opties en quotabeheer

In dit gedeelte wordt het volgende beschreven:

- Wat zijn services en opties?
- Hoe worden opties ingeschakeld of uitgeschakeld?
- Wat zijn factureringsmodi?
- Wat zijn geavanceerde beschermingspakketten?
- Wat zijn verouderde edities en subedities?
- Wat zijn softe en harde quota's?
- Wanneer kan de harde quota worden overschreden?
- Wat is back-upquotatransformatie?
- In hoeverre is de beschikbaarheid van installatieprogramma's in de serviceconsole afhankelijk van de beschikbare opties?

2.1.1 Services en opties

Services

Een cloudservice is een set functies die wordt gehost door een partner of in de privécloud van een eindklant. Gewoonlijk worden services verkocht als abonnement of met betalen naar gebruik.

De Cyber Protect-service integreert cyberbeveiliging, gegevensbescherming en beheer om uw eindpunten, systemen en gegevens te beschermen tegen cyberbeveiligingsbedreigingen. De Cyber Protect-service bestaat uit verschillende onderdelen: Bescherming, File Sync & Share, Notary en Physical Data Shipping. Sommige kunnen worden uitgebreid met geavanceerde functionaliteit door gebruik te maken van geavanceerde beschermingspakketten. Zie "De Cyber Protect-service en pakketten voor geavanceerde bescherming" (p. 8) voor gedetailleerde informatie over inbegrepen en geavanceerde functies.

Opties

Een optie is een set servicefuncties die zijn gegroepeerd per specifiek type workload of functionaliteit, bijvoorbeeld opslag, infrastructuur voor noodherstel, enzovoort. Door specifieke opties in te schakelen bepaalt u welke workloads kunnen worden beschermd, hoeveel workloads kunnen worden beschermd (door quota's in te stellen) en welk beschermingsniveau beschikbaar is voor uw partners, klanten en hun eindgebruikers (door geavanceerde beschermingspakketten in of uit te schakelen).

De functionaliteit die niet is ingeschakeld, wordt verborgen voor klanten en gebruikers, tenzij u een upsell-scenario configureert. Zie "Upsell-scenario's voor uw klanten configureren" (p. 61) voor meer informatie over upsell-scenario's.

Het functiegebruik wordt verzameld bij de services en weergegeven bij de opties en wordt gebruikt voor de rapporten en verdere facturering.

Factureringsmodi en edities

Met verouderde edities kunt u één optie per workload inschakelen. Met factureringsmodi wordt de functionaliteit opgesplitst, zodat u meerdere opties (servicefuncties en geavanceerde pakketten) per workload kunt inschakelen om beter aan de behoeften van uw klanten te voldoen en een nauwkeurigere facturering toe te passen, namelijk alleen voor de functies die uw klanten daadwerkelijk gebruiken.

Voor meer informatie over de factureringsmodi voor Cyber Protect raadpleegt u "Overschakelen van verouderde edities naar het nieuwe factureringsmodel" (p. 14).

U kunt factureringsmodi of edities gebruiken om de services te configureren die beschikbaar zijn voor uw tenants. U kunt één factureringsmodus of één editie selecteren per klanttenant. Dus als u verschillende factureringsmodi wilt toepassen voor verschillende servicefuncties, moet u meerdere tenants voor een klant maken. Als de klant bijvoorbeeld Microsoft 365-postvakken wil hebben in de

factureringsmodus Per gigabyte en Teams in de factureringsmodus Per workload, moet u twee verschillende klanttenants voor deze klant maken.

Als u het gebruik van services in een optie wilt beperken, kunt u quota's definiëren voor die optie. Zie "Softe en harde quota's" (p. 26).

De Cyber Protect-service en pakketten voor geavanceerde bescherming

In dit gedeelte worden de functiesets beschreven die in maart 2021 zijn ingevoerd samen met het nieuwe factureringsmodel. Lees meer over de voordelen van het nieuwe factureringsmodel in de datasheet Cyber Protect.

Verouderde edities zijn nog steeds beschikbaar, maar worden niet aanbevolen omdat ze minder flexibiliteit bieden bij de facturering. Zie "Cyber Protect-editie" (p. 18) voor informatie over verouderde edities en subedities.

De volgende services en functiesets zijn beschikbaar in Cyber Cloud:

- **Cyber Protect**
  - **Bescherming**: volledige cyberbescherming zonder extra kosten met back-ups en herstel, noodherstel, automatisering, beheer, beveiliging en e-mailbeveiliging. Deze functionaliteit kan worden uitgebreid met geavanceerde beschermingspakketten, waarvoor extra kosten in rekening worden gebracht.
  - **File Sync & Share**: een oplossing voor het veilig delen van bedrijfsinformatie vanaf elke locatie, op elk moment en op elk apparaat.
  - **Physical Data Shipping**: een oplossing waarmee u tijd bespaart en het netwerkverkeer vermindert doordat de gegevens naar het clouddatacentrum worden verzonden op een harde schijf.
  - **Notary**: een op blockchain gebaseerde oplossing die de authenticiteit van gedeelde inhoud waarborgt.
- **Cyber Infrastructure SPLA**

In de beheerportal kunt u selecteren welke services en functiesets beschikbaar zijn voor uw tenants. De configuratie gebeurt per tenant op het moment dat u een tenant inricht of bewerkt, zoals beschreven in Een tenant maken.

Advanced-pakketten

Geavanceerde beschermingspakketten zijn pakketten met unieke functies voor meer geavanceerde scenario's op een specifiek functioneel gebied, bijvoorbeeld Advanced Backup, Advanced Security, enzovoort. Advanced-pakketten bieden een uitbreiding van de functionaliteit die beschikbaar is in de standaard Cyber Protect-service.

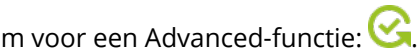
Geavanceerde beschermingspakketten kunnen worden ingeschakeld in combinatie met de functie van de Bescherming-service en hiervoor worden extra kosten in rekening gebracht. Geavanceerde beschermingspakketten bieden unieke functionaliteit die niet is inbegrepen in de standaardfunctieset en andere geavanceerde pakketten. Klanten kunnen hun workloads

beschermen met één, meerdere of alle geavanceerde pakketten. De geavanceerde beschermingspakketten zijn beschikbaar voor beide factureringsmodi van de Bescherming-service: per workload en per gigabyte.

U kunt de volgende geavanceerde beschermingspakketten inschakelen:

- Advanced Backup
- Advanced Management
- Advanced Security
- Advanced Disaster Recovery
- Advanced Email Security

Opmerking
Geavanceerde pakketten kunnen alleen worden gebruikt als de functie die ze uitbreiden, is ingeschakeld. Gebruikers kunnen geen geavanceerde functies gebruiken wanneer de functie voor standaardservice is uitgeschakeld. Gebruikers kunnen bijvoorbeeld de functies van het Advanced Backup-pakket niet gebruiken als de functie Bescherming is uitgeschakeld.

Als een pakket voor geavanceerde bescherming is ingeschakeld, worden de betreffende functies in het beschermingsschema weergegeven met het pictogram voor een Advanced-functie:  . Wanneer gebruikers de functie proberen in te schakelen, zien ze een bericht dat hiervoor extra kosten in rekening worden gebracht.

Als een pakket voor geavanceerde bescherming niet is ingeschakeld, maar upsell wel is ingeschakeld, worden de geavanceerde beschermingsfuncties weergegeven in het beschermingsschema, maar zijn ze niet toegankelijk voor gebruik. Het volgende pictogram wordt weergegeven naast de naam van de functie  . Gebruikers zien een bericht dat ze contact moeten opnemen met hun beheerder om de vereiste geavanceerde functieset in te schakelen.

Wanneer een pakket voor geavanceerde bescherming niet is ingeschakeld en upsell is uitgeschakeld, kunnen klanten de geavanceerde functies niet zien in hun beschermingsschema's.

Inbegrepen functies en geavanceerde pakketten in Cyber Protect-services

Wanneer u een service of functieset inschakelt in Cyber Protect, schakelt u daarmee een aantal functies in die standaard zijn inbegrepen en beschikbaar zijn. Daarnaast kunt u geavanceerde beschermingspakketten inschakelen.

De volgende gedeelten bevatten een algemeen overzicht van de functies en geavanceerde pakketten van de Cyber Protect-service. Zie de Cyber Protect-licentiegids voor een volledige lijst met aanbiedingen.

Inbegrepen en geavanceerde functies in de Protection-service

Inbegrepen en geavanceerde functies in de Protection-service

Functiegroep	Inbegrepen standaardlicenties	Geavanceerde functies
Beveiliging	• #CyberFit-score • Evaluatie van beveiligingsproblemen • Antiransomwarebescherming: Active Protection • Antivirus- en antimalwarebeveiliging: Bestandsdetectie in de cloud op basis van handtekeningen (geen realtime bescherming, alleen geplande scans)* • Antivirus- en antimalwarebeveiliging: Op AI gebaseerde bestandsanalyse voorafgaand aan de uitvoering, op gedrag gebaseerde Cyber Engine • Microsoft Defender-beheer *Cyber Protect detecteert zero-day-aanvallen met behulp van heuristische scanregels en algoritmen om te zoeken naar schadelijke opdrachten.	• Antivirus- en antimalwarebeveiliging met lokale detectie op basis van handtekeningen (met realtime bescherming) • Preventie tegen aanvallen • URL-filtering • Forensische back-up, scannen van back-ups op malware, veilig herstel, acceptatielijst van bedrijf • Schema's voor slimme bescherming
Preventie van gegevensverlies	• Apparaatbesturing	N.v.t.
Management	• Groepsbeheer van workloads • Gecentraliseerd beheer van beschermingsschema's • Extern bureaublad • Hulp op afstand • Hardware-inventaris	• Patchbeheer • HDD-integriteit • Software-inventaris • Veilige bestandspatches • Cyberscripts • Toolbox voor MSP • Op AI gebaseerde controle • Software-implementatie
E-mailbeveiliging	• Antispambescherming • URL-filtering	Realtime bescherming voor uw Microsoft 365- en Gmail-postvakken: • Antimalware Antispam • URL-scan in e-mails • DMARC-analyse • Antiphishing • Bescherming tegen imitatie • Scan van bijlagen • Content Disarm and Reconstruction • Vertrouwensgrafiek

Functiegroep	Inbegrepen standaardlicenties	Geavanceerde functies
		Zie de configuratiegids.
Disaster Recovery Cloud	Met de standaardfuncties van Disaster Recovery kunt u scenario's voor noodherstel testen voor uw workloads. Noteer de standaardfuncties van Disaster Recovery die beschikbaar zijn, en de beperkingen ervan: • Testfailover in een geïsoleerde netwerkomgeving. Beperkt tot 32-computepunten per maand, en tot 5 gelijktijdige testfailoverbewerkingen. • Herstelserverconfiguraties: 1 CPU en 2 GB RAM, 1 CPU en 4 GB RAM, en 2 CPU en 8 GB RAM. • Aantal herstelpunten beschikbaar voor failover: alleen het laatste herstelpunt dat direct beschikbaar is na een back-up. • Beschikbare connectiviteitsmodi: Alleen cloud en point-to-site. • Beschikbaarheid van de VPN-gateway: De VPN-gateway wordt tijdelijk opgeschort als deze gedurende 4 uur inactief is nadat de laatste testfailover is voltooid, en wordt opnieuw geïmplementeerd wanneer u een testfailover start. • Aantal cloudnetwerken: 1. • Internettoegang • Bewerkingen met runbooks: maken en bewerken.	U kunt het Advanced Disaster Recovery-pakket inschakelen en uw workloads beschermen met de volledige Disaster Recovery-functionaliteit. Noteer de geavanceerde functies van Disaster Recovery die beschikbaar zijn: • Productiefailover • Testfailover in een geïsoleerde netwerkomgeving. • Aantal herstelpunten beschikbaar voor failover: alle herstelpunten die beschikbaar zijn na het maken van de herstelserver. • Primaire servers • Configuraties van herstel-/primaire server: Geen beperkingen • Beschikbare connectiviteitsmodi: Alleen cloud, point-to-site, site-to-site OpenVPN, en multi-site IPsec VPN. • Beschikbaarheid van de VPN-gateway: altijd beschikbaar. • Aantal cloudnetwerken: 5. • Openbare IP-adressen • Internettoegang • Bewerkingen met runbooks: maken, bewerken en uitvoeren.

Functies met betalen naar gebruik en geavanceerde functies in de Protection-service

Functies met betalen naar gebruik en geavanceerde functies in de Protection-service

Functiegroep	Functies met betalen naar gebruik	Geavanceerde functies
Back-up	• Bestandsback-up	• Microsoft SQL Server en

Functiegroep	Functies met betalen naar gebruik	Geavanceerde functies
	• Systeemkopieback-up • Back-up van toepassingen • Back-up naar netwerkshares • Back-up naar cloudopslag • Back-up naar lokale opslag **Opmerking** Er worden kosten voor gebruik van cloudopslag in rekening gebracht.	• Microsoft Exchange-clusters • Oracle DB • SAP HANA • Overzicht van gegevensbescherming • Continue gegevensbescherming
File Sync & Share	• Versleutelde op bestanden gebaseerde inhoud opslaan • Bestanden synchroniseren op aangewezen apparaten • Mappen en bestanden delen met aangewezen personen en systemen	N.v.t.
Physical Data Shipping	Functies van Physical Data Shipping	N.v.t.
Notarisatie	• Bestandsnotarisatie • Elektronisch ondertekenen van bestanden • Documentsjablonen	N.v.t.

Opmerking
U kunt geavanceerde beschermingspakketten alleen inschakelen als de standaardbeschermingsfunctie die ze uitbreiden, is ingeschakeld. Als u een functie uitschakelt, worden de betreffende geavanceerde pakketten automatisch uitgeschakeld en worden de beschermingsschema's die er gebruik van maken, automatisch ingetrokken. Als u bijvoorbeeld de Protection-functie uitschakelt, worden de geavanceerde pakketten automatisch uitgeschakeld en worden alle schema's die er gebruik van maken, ingetrokken.

Gebruikers kunnen geen geavanceerde beschermingspakketten gebruiken zonder standaardbescherming, maar kunnen wel de inbegrepen functies van standaardbescherming samen met geavanceerde pakketten gebruiken voor specifieke workloads. In dit geval worden alleen de gebruikte geavanceerde pakketten in rekening gebracht.

Zie "Overschakelen van verouderde edities naar het nieuwe factureringsmodel" (p. 14) voor informatie over facturering.

Factureringsmodi voor Cyber Protect

Een factureringsmodus is een schema voor het verrekenen en factureren van het gebruik van services en de bijbehorende functies. De factureringsmodus bepaalt welke eenheden worden gebruikt als basis voor de prijsberekeningen.

Met verouderde edities kunt u één editie per workload toewijzen. Het resultaat is dat uw klanten betalen voor alle functies die in een editie zijn inbegrepen, zelfs als ze sommige functies niet gebruiken. Met factureringsmodi en geavanceerde pakketten wordt de functionaliteit opgesplitst in meerdere opties en zijn meerdere opties per workload mogelijk. De opties worden automatisch opgehaald door de licentie-engine, afhankelijk van de functies die worden gevraagd in de beschermingsschema's. Gebruikers kunnen het beschermingsniveau en de kosten optimaliseren door hun beschermingsschema's aan te passen.

Opmerking
U kunt slechts één factureringsmodus of één verouderde editie gebruiken per tenant.

Factureringsmodi voor het onderdeel Bescherming

De Bescherming heeft twee factureringsmodi:

- Per workload
- Per gigabyte

De functiesets van beide factureringsmodi zijn identiek.

De Protection-service biedt functies voor standaardbescherming tegen de meeste cyberbeveiligingsrisico's, ongeacht welk van beide factureringsmodi wordt gebruikt. Gebruikers kunnen deze zonder extra kosten gebruiken. Het gebruik van de inbegrepen functies wordt geteld, maar niet gefactureerd. Zie "De Cyber Protect-service en pakketten voor geavanceerde bescherming" (p. 8) voor een volledige lijst met inbegrepen en factureerbare opties.

Wanneer een geavanceerd pakket is ingeschakeld voor een klant, begint de facturering pas nadat de klant de functies van dat pakket in een beschermingsschema gaat gebruiken. Wanneer een klant sommige geavanceerde functies in een beschermingsschema wil gebruiken, wordt de vereiste licentie automatisch aan de gebruiker toegewezen door de licentie-engine.

Wanneer een gebruiker stopt met het gebruik van een geavanceerde functie, wordt de licentie ingetrokken en stopt de facturering. De licentie-engine wijst automatisch de licentie toe die overeenkomt met het werkelijke gebruik van de functies.

U kunt alleen licenties toewijzen voor de standaardfuncties van de Cyber Protect-service. Geavanceerde functies worden gefactureerd op basis van het gebruik en de licenties daarvoor kunnen niet handmatig worden gewijzigd. Het toewijzen of het ongedaan maken van toewijzingen wordt automatisch uitgevoerd door de licentie-engine. U kunt het licentietype voor een workload handmatig wijzigen, maar het type wordt opnieuw toegewezen wanneer het beschermingsschema voor die workload wordt gewijzigd door een gebruiker.

Opmerking
De facturering voor de geavanceerde beschermingsfuncties begint niet meteen wanneer u deze inschakelt. De facturering begint pas wanneer een klant de geavanceerde functies in een beschermingsschema gaat gebruiken. Ingeschakelde functiesets worden meegeteld en opgenomen in gebruiksrapporten, maar worden pas gefactureerd als de betreffende functies worden gebruikt.

Factureringsmodi voor File Sync & Share

File Sync & Share heeft de volgende factureringsmodi:

- Per gebruiker
- Per gigabyte

U kunt ook de factureringsregels van de verouderde File Sync & Share-editie toepassen.

Opmerking
De facturering voor Advanced File Sync & Share begint niet meteen wanneer u deze functies inschakelt. Facturering begint pas nadat een klant de geavanceerde functies begint te gebruiken. De ingeschakelde set geavanceerde functies wordt meegeteld en opgenomen in gebruiksrapporten, maar wordt niet gefactureerd, tenzij de functies worden gebruikt.

Facturering voor Physical Data Shipping

Het model voor betalen naar gebruik wordt toegepast op de facturering voor Physical Data Shipping.

Facturering voor Notary

Het model voor betalen naar gebruik wordt toegepast op de facturering voor Notary.

De factureringsmodi gebruiken met verouderde edities

Voor tenants van bestaande klanten kunt u de verouderde opties blijven gebruiken of u kunt de opties voor een van de factureringsmodi gebruiken om de verouderde edities te vervangen. De licentie-engine zal automatisch de aan de klant toegewezen licenties optimaliseren om het factureerbare bedrag zo laag mogelijk te houden.

Opmerking
U kunt edities niet combineren met factureringsmodi.

2.1.2 Overschakelen van verouderde edities naar het nieuwe factureringsmodel

U kunt de opties voor uw tenants handmatig overschakelen door het profiel van de tenants te bewerken en nieuwe opties te selecteren. Zie "Schakelen tussen edities en factureringsmodi" (p. 15) voor meer informatie over het overschakelen.

Als u wilt overschakelen van edities naar factureringsmodi voor meerdere klanten, raadpleegt u Edities groepsgewijs overschakelen voor meerdere klanten (67942).

Schakelen tussen edities en factureringsmodi

In de beheerportal kunt u een tenantaccount wijzigen om opties over te schakelen naar een andere factureringsmodus (per workload naar per gigabyte en vice versa), of tussen edities en factureringsmodi en vice versa.

Zie Edities groepsgewijs overschakelen voor meerdere klanten (67942) voor informatie over het groepsgewijs overschakelen van tenants.

Het overschakelingsproces omvat de volgende stappen.

1. Richt de nieuwe opties in voor een klanttenant (waardoor opties en quota's kunnen worden ingesteld), zodat ze overeenkomen met de functionaliteit die beschikbaar was in de oorspronkelijke optie.
2. Maak de toewijzing van ongebruikte opties ongedaan en wijs de opties toe aan workloads, in overeenstemming met de functies die worden gebruikt in de beschermingsschema's (gebruiksreconciliatie).

De volgende tabel geeft het proces in beide richtingen weer.

	Richting wijzigen		
	Editie > Factureringsmodi	**Factureringsmodi > editie (niet aanbevolen)**	**Factureringsmodus > Factureringsmodus**
Opties overschakelen	Schakel opties in om de functionaliteit te verkrijgen die beschikbaar was in de editie van de bron.	Schakel opties in om de functionaliteit te verkrijgen die beschikbaar was in de factureringsmodus van de bron. **Opmerking** De opties van de Advanced-pakketten van de bron kunnen niet worden overgeschakeld omdat de edities geen pakketten bevatten. Als gevolg daarvan worden die opties uitgeschakeld tijdens de overschakeling.	De identieke set opties wordt ingeschakeld.
Quota's overschakelen	De quota wordt gerepliceerd van de bronoptie naar de doeloptie. Bron: Standard → doel: Standard-product. Bron: Standard → doel: pakketten.	De quota van de Standard-productoptie wordt standaard gebruikt als quota voor de doeloptie. **Opmerking** Quota's van de bronpakketten worden opnieuw ingesteld tijdens de overschakeling.	De quota's worden gerepliceerd van de bronoptie naar de doeloptie.

	Richting wijzigen		
	Editie > Factureringsmodi	**Factureringsmodi > editie (niet aanbevolen)**	**Factureringsmodus > Factureringsmodus**
	Opmerking Als u overschakelt van een editie met subedities (bijvoorbeeld 'Cyber Protect (per workload)'), worden de quota's samengevat.		
Gebruik overschakelen	Opties worden opnieuw toegewezen aan de workloads, in overeenstemming met de gevraagde functies in de beschermingsschema's die zijn toegewezen aan deze workloads.		

Voorbeeld: Overschakelen van Cyber Protect Advanced-editie naar Facturering per workload

In dit scenario heeft een klanttenant Cyber Protect Advanced-editie gebruikt op 8 werkstations, en de quota is ingesteld op 10 workloads. 3 van de werkstations maken gebruik van software-inventaris en patchbeheer in de beschermingsschema's, voor 2 van de werkstations is URL-filtering ingeschakeld in de beschermingsschema's, en een van de machines maakt gebruik van continue gegevensbescherming. De volgende tabel geeft de overschakeling van de editie naar nieuwe opties weer.

Bronopties - gebruik/quota	Doelopties - gebruik/quota
Cyber Protect Advanced workstation 8/10	• Werkstation - 8/10 • Advanced Security - 2/10 • Advanced Backup-werkstation - 1/10 • Advanced Management - 3/10

De volgende stappen zijn uitgevoerd tijdens de overschakeling:

1. De opties voor de functionaliteit die beschikbaar was in de broneditie, zijn automatisch ingeschakeld.
2. De quota is gerepliceerd naar de nieuwe opties.
3. Het gebruik is in overeenstemming gebracht met het werkelijke gebruik in beschermingsschema's: drie workloads gebruiken functies van het Advanced Management-pakket, twee workloads gebruiken functies van het Advanced Security-pakket, en één workload gebruikt functies van het Advanced Backup-pakket.

Voorbeeld: Cyber Protect-editie per workload naar Facturering per workload

In dit voorbeeld heeft de klant meerdere edities toegewezen aan workloads. Aan elke workload kan slechts één editie of één factureringsmodus worden toegewezen.

Bronopties - gebruik/quota	Doelopties - gebruik/quota
Cyber Protect Essentials Workstation - 6/12	• Werkstation - 14/42 • Advanced Backup-werkstation - 2/42 • Advanced Security - 13/42 • Advanced Management - 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standard-werkstation - 1/10	

De volgende stappen zijn uitgevoerd tijdens de overschakeling:

1. De opties voor de functionaliteit die beschikbaar was in alle bronedities, zijn automatisch ingeschakeld. Met factureringsmodi kunnen naar behoefte meerdere opties worden toegewezen aan een workload.

2. De quota's zijn samengevat en gerepliceerd.

2. Het gebruik is in overeenstemming gebracht met de beschermingsschema's.

Edities en subedities van de Cyber Protection-service

Dit gedeelte bevat informatie over het werken met services, edities en opties die beschikbaar waren als onderdeel van het licentiemodel in Cyber Cloud 21.02 en eerder. Deze opties en edities worden nog steeds ondersteund en kunnen naar behoefte worden geconfigureerd voor tenants, maar worden niet aanbevolen. Ze worden nu beschouwd als verouderd.

Opmerking
De services, edities en opties die voor u beschikbaar zijn, worden overgenomen van de opties die beschikbaar zijn voor uw bovenliggende tenant. Als een optie niet beschikbaar is voor de partner die uw account heeft gemaakt, zal die optie niet beschikbaar zijn voor u, en kunt u deze niet inschakelen voor uw partners of klanten.

Zie "De Cyber Protect-service en pakketten voor geavanceerde bescherming" (p. 8) voor informatie over de nieuwe opties.

De volgende edities zijn beschikbaar:

- Cyber Protect
- Cyber Backup

2.1.3 Cyber Protect-editie

Deze editie is gelicentieerd per workload, dat wil zeggen afhankelijk van het aantal beschermde machines, ongeacht de grootte van de gegevens waarvan een back-up is gemaakt.

Binnen de Cyber Protect-editie zijn de volgende subedities beschikbaar:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard

De Cyber Protect-editie is flexibel en stelt partnerbeheerders in staat om functies van verschillende subedities te combineren in één klanttenant. Zie Opties van verschillende subedities combineren voor meer informatie over hoe u een aanbod op maat kunt maken.

2.1.4 Cyber Backup Edition

Deze editie is gelicentieerd per GB, dat wil zeggen afhankelijk van de grootte van de gegevens waarvan een back-up is gemaakt, ongeacht het aantal beschermde machines.

De Cyber Backup-editie bevat geen subedities, alleen Cyber Backup Standard-opties zijn beschikbaar.

2.1.5 Edities vergelijken

Het aantal en de omvang van de beschikbare functies zijn afhankelijk van de editie van de Cyber Protection-service. Zie Cyber Protection-edities vergelijken voor een gedetailleerde vergelijking tussen de functies in elke editie en subeditie.

2.1.6 Disaster Recovery-add-on

De Disaster Recovery-add-on biedt herstelfunctionaliteit ontworpen voor bedrijven die hoge eisen stellen aan de RPO (Recovery Time Objective). Deze add-on is alleen beschikbaar met de Cyber Protect-editie.

Opmerking
De Disaster Recovery-add-on kan niet worden gebruikt met de Cyber Protect Essentials-editie.

Opties uit verschillende subedities combineren

Voor een partnertenant kan meer dan één editie beschikbaar zijn.

Voor een klanttenant kan slechts één editie worden geselecteerd: Cyber Protect of Cyber Backup.

Met de Cyber Protect-editie kunnen opties uit verschillende subedities worden gecombineerd. Opties van Cyber Backup Standard kunnen ook worden toegevoegd aan de combinatie, maar deze

worden gefactureerd per workload, net als alle andere opties in de Cyber Protect-editie, inclusief de **Lokale opslag**.

Zo kunnen in een klanttenant met de Cyber Protect-editie verschillende workloads worden beschermd door functies uit verschillende subedities. Zo kunnen sommige machines in deze tenant worden beschermd met de optie **Werkstations** van de Cyber Protect Essentials-subeditie, en andere met de optie **Servers** van de Cyber Protect Advanced-subeditie.

U kunt ook parallelle opties uit verschillende subedities combineren, bijvoorbeeld **Werkstations** van de Cyber Protect Essentials-subeditie en **Werkstations** van de Cyber Protect Standard-subeditie.

Het respectieve beschermingsniveau wordt automatisch toegewezen aan een machine op basis van het type, de instellingen van het eerste beschermingsschema en deze volgorde van prioriteiten:

1. Cyber Protect Essentials
2. Cyber Backup Standard
3. Cyber Protect Standard
4. Cyber Protect Advanced

Een beheerder met toegang tot de Cyber Protection-serviceconsole kan het beschermingsniveau van een specifieke machine handmatig wijzigen door een geschikte servicequota te selecteren. Zie De servicequota van machines wijzigen voor meer informatie over hoe u dit kunt doen.

3 De servicequota van machines wijzigen

Het beschermingsniveau van een machine wordt bepaald door de toegepaste servicequota. Servicequota's hebben betrekking op de opties voor de tenant waarin de machine is geregistreerd.

De servicequota wordt automatisch toegewezen wanneer een beschermingsschema voor het eerst wordt toegepast op een machine.

U kunt de oorspronkelijke toewijzing later handmatig wijzigen. Als u bijvoorbeeld een geavanceerder beschermingsschema wilt toepassen op dezelfde machine, moet u de servicequota van de machine mogelijk upgraden. Als de door dit beschermingsschema vereiste functies niet worden ondersteund door de momenteel toegewezen servicequota, mislukt het beschermingsschema. U kunt de servicequota ook wijzigen als u na de oorspronkelijke toewijzing quota's aanschaft die meer geschikt zijn. Er wordt bijvoorbeeld een quota voor **werkstations** toegewezen aan een virtuele machine. Na aankoop van een quota voor **Virtuele machines** kunt u deze handmatig toewijzen aan deze machine. U kunt ook de momenteel toegewezen servicequota vrijgeven en vervolgens toewijzen aan een andere machine.

U kunt de servicequota van een afzonderlijke machine of voor een groep machines wijzigen.

De servicequota van een afzonderlijke machine wijzigen

1. Ga in de Cyber Protection-serviceconsole naar **Apparaten**.
2. Selecteer de gewenste machine en klik op **Details**.
3. Klik in het gedeelte **Servicequota** op **Wijzigen**.
4. Open het venster **Licentie wijzigen**, selecteer de gewenste servicequota of **Geen quota** en klik vervolgens op **Wijzigen**.

De servicequota voor een groep machines wijzigen

1. Ga in de Cyber Protection-serviceconsole naar **Apparaten**.
2. Selecteer meer dan één machine en klik vervolgens op **Quota toewijzen**.
3. Open het venster **Licentie wijzigen**, selecteer de gewenste servicequota of **Geen quota** en klik vervolgens op **Wijzigen**.

Verouderde edities

Cyber Protect en Cyber Backup-edities zijn beschikbaar voor alle partners.

De volgende oudere edities zijn mogelijk ook beschikbaar voor sommige partners:

- (Verouderd) Cyber Backup – Standard
- (Verouderd) Cyber Backup – Advanced
- (Verouderd) Cyber Backup - Disaster Recovery Edition
- (Verouderd) Cyber Protect – Standard

- (Verouderd) Cyber Protect – Advanced
- (Verouderd) Cyber Protect – Disaster Recovery

Editie	Beschrijving
(Verouderd) Cyber Backup – Standard	Biedt het volgende: • Back-up- en herstelfunctionaliteit die voorziet in de behoeften van kleine en middelgrote omgevingen • Evaluatie van beveiligingsproblemen en basisfunctionaliteit voor bescherming tegen ransomware en cryptomining • Standaardfunctionaliteit voor externe installatie van agenten
(Verouderd) Cyber Backup – Advanced	Biedt het volgende: • Back-up- en herstelfunctionaliteit speciaal voor de bescherming van geavanceerde workloads, zoals Microsoft Exchange- en Microsoft SQL-clusters in grote omgevingen • Groepsbeheer en schemabeheer • Evaluatie van beveiligingsproblemen en basisfunctionaliteit voor bescherming tegen ransomware en cryptomining • Geavanceerde functionaliteit voor externe installatie van agenten
(Verouderd) Cyber Backup - Disaster Recovery Edition	Biedt het volgende: • Back-up- en herstelfunctionaliteit speciaal voor de bescherming van geavanceerde workloads, zoals Microsoft Exchange- en Microsoft SQL-clusters in grote omgevingen • Groepsbeheer en schemabeheer • Evaluatie van beveiligingsproblemen en basisfunctionaliteit voor bescherming tegen ransomware en cryptomining • Geavanceerde functionaliteit voor externe installatie van agenten • Noodherstelfunctie ontworpen voor bedrijven die hoge eisen stellen aan de RPO (Recovery Time Objective)
(Verouderd) Cyber Protect – Standard	Biedt het volgende: • Back-up- en herstelfunctionaliteit die voorziet in de behoeften van kleine en middelgrote omgevingen • Standaardfunctionaliteit voor externe installatie van agenten • Functionaliteit voor de evaluatie van beveiligingsproblemen en patchbeheer • Geavanceerde functionaliteit voor antimalwarebeveiliging en webbeveiliging • Functionaliteit voor extern bureaublad • Functionaliteit voor beveiligingsbeheer zoals Windows Defender-beheer • Bedreigingsfeed: Waarschuwingen op basis van gegevens van Cyber Protection Operations Center • Overzicht van gegevensbescherming

(Verouderd) Cyber Protect – Advanced	Biedt het volgende: • Back-up- en herstelfunctionaliteit speciaal voor de bescherming van geavanceerde workloads, zoals Microsoft Exchange- en Microsoft SQL-clusters in grote omgevingen • Groepsbeheer en schemabeheer • Geavanceerde functionaliteit voor externe installatie van agenten • Functionaliteit voor de evaluatie van beveiligingsproblemen en patchbeheer • Geavanceerde functionaliteit voor antimalwarebeveiliging en webbeveiliging • Functionaliteit voor extern bureaublad • Functionaliteit voor beveiligingsbeheer zoals Windows Defender-beheer • Bedreigingsfeed: Waarschuwingen op basis van gegevens van Cyber Protection Operations Center • Overzicht van gegevensbescherming
(Verouderd) Cyber Protect – Disaster Recovery	Biedt het volgende: • Back-up- en herstelfunctionaliteit speciaal voor de bescherming van geavanceerde workloads, zoals Microsoft Exchange- en Microsoft SQL-clusters in grote omgevingen • Groepsbeheer en schemabeheer • Geavanceerde functionaliteit voor externe installatie van agenten • Functionaliteit voor de evaluatie van beveiligingsproblemen en patchbeheer • Geavanceerde functionaliteit voor antimalwarebeveiliging en webbeveiliging • Functionaliteit voor extern bureaublad • Functionaliteit voor beveiligingsbeheer zoals Windows Defender-beheer • Bedreigingsfeed: Waarschuwingen op basis van gegevens van Cyber Protection Operations Center • Overzicht van gegevensbescherming • Noodherstelfunctie ontworpen voor bedrijven die hoge eisen stellen aan de RPO (Recovery Time Objective)

4 Upgraden van een oude editie

Alle oudere edities kunnen worden gefactureerd per workload of per GB, maar de Cyber Protect-editie wordt alleen gefactureerd per workload en de Cyber Backup-editie alleen per GB. Bij het overschakelen tussen oudere en nieuwe edities kan er een volledige of gedeeltelijke overeenkomst zijn wat betreft de beschikbare functies of het factureringsmodel.

Hier zijn de aanbevolen patronen voor het overschakelen van oudere edities naar Cyber Protect of de Cyber Backup-editie.

Bron		**Doel**				
Editie	**Facturering**	**Editie**	**Subeditie**	**Functiecombinatie**	**Facturering**	**Factureringscombinatie**
Cyber Backup – Standard	Per workload	Cyber Protect	Cyber Backup Standard	Voltooid	Per workload	Ja
Cyber Backup – Advanced			Cyber Protect Advanced	Gedeeltelijk		
Cyber Backup – Disaster Recovery			Cyber Protect Advanced + Disaster Recovery-add-on	Gedeeltelijk		
Cyber Protect – Standard			Cyber Protect Standard	Voltooid		
Cyber Protect – Advanced			Cyber Protect Advanced	Voltooid		
Cyber Protect –			Cyber Protect Advanced	Voltooid		

Bron		Doel				
Editie	**Facturering**	**Editie**	**Subeditie**	**Functiecombinatie**	**Facturering**	**Factureringscombinatie**
Disaster Recovery			+ Disaster Recovery-add-on			
Cyber Backup – Standard	Per GB	Cyber Backup	Cyber Backup Standard	Voltooid	Per GB	
Cyber Backup – Advanced		Cyber Protect	Cyber Protect Advanced	Gedeeltelijk	Per workload	Nee
Cyber Backup – Disaster Recovery			Cyber Protect Advanced + Disaster Recovery-add-on	Gedeeltelijk		
Cyber Protect – Standard			Cyber Protect Standard	Voltooid		
Cyber Protect – Advanced			Cyber Protect Advanced	Voltooid		
Cyber Protect – Disaster Recovery			Cyber Protect Advanced + Disaster Recovery-add-on	Voltooid		

Edities voor een partnertenant wijzigen

De beschikbare edities voor een partnertenant wijzigen

1. Ga in de beheerportal naar **Klanten**.
2. Selecteer de partnertenant waarvoor u de edities wilt wijzigen, klik op het ellipspictogram en klik vervolgens op **Configureren**.
3. Open het tabblad **Configureren** en selecteer de gewenste edities.
4. Voer uw gebruikersnaam in om uw keuze te bevestigen.

De editie voor een klanttenant wijzigen ...

U kunt de editie voor een klanttenant als volgt wijzigen:

- De oorspronkelijke editie bewerken door opties in- of uit te schakelen.
- Overschakelen naar een volledig nieuwe editie.

Zie Opties inschakelen of uitschakelen voor meer informatie over het bewerken van de oorspronkelijke editie.

De editie voor een klanttenant wijzigen

1. Ga in de beheerportal naar **Klanten**.
2. Selecteer de klanttenant waarvoor u de edities wilt wijzigen, klik op het ellipspictogram en klik vervolgens op **Configureren**.
3. Open het tabblad **Configureren** en selecteer de nieuwe editie.
4. Voer uw gebruikersnaam in om uw keuze te bevestigen.

Deze wijziging kan tot 10 minuten duren.

Opmerking
U kunt overschakelen van de Cyber Protect-editie met meerdere parallelle opties (bijvoorbeeld **Werkstations** van verschillende subedities) naar een editie met slechts één vergelijkbare optie, bijvoorbeeld Cyber Backup. Als u dit wilt doen, moet u eerst al het gebruik in de broneditie verplaatsen naar een van de parallelle opties.

4.0.1 Opties in- of uitschakelen

U kunt alle beschikbare opties voor een bepaalde editie of factureringsmodus inschakelen, zoals beschreven in Een tenant maken.

Opmerking
Door alle opties van een service uit te schakelen wordt de service zelf niet automatisch uitgeschakeld.

Er zijn enkele beperkingen voor het uitschakelen van opties. Zie onderstaande tabel.

Optie	Uitschakelen ...	Resultaat
Back-upopslag	Kan worden uitgeschakeld wanneer het gebruik gelijk is aan nul.	De cloudopslag is dan niet meer beschikbaar als bestemming voor back-ups binnen een klanttenant.
Lokale back-up	Kan worden uitgeschakeld wanneer het gebruik gelijk is aan nul.	De lokale opslag is dan niet meer beschikbaar als bestemming voor back-ups binnen een klanttenant.
Gegevensbronnen (waaronder Microsoft 365 en Google Workspace)	Kan worden uitgeschakeld wanneer het gebruik gelijk is aan nul.	Back-ups en herstel van gegevensbronnen (waaronder Microsoft 365 en Google Workspace) zijn dan niet meer beschikbaar binnen een klanttenant.
Alle opties voor noodherstel	Kan worden uitgeschakeld wanneer het gebruik meer is dan nul.	Ga naar 'Softe en harde quota's' voor de details.
Alle opties voor notarisatie	Kan worden uitgeschakeld wanneer het gebruik gelijk is aan nul.	De service voor notarisatie is dan niet meer beschikbaar binnen een klanttenant.
Alle opties voor File Sync & Share	Het is niet mogelijk om afzonderlijke opties in- of uit te schakelen.	De service voor File Sync & Share wordt dan uitgeschakeld.
Alle opties voor Physical Data Shipping	Kan worden uitgeschakeld wanneer het gebruik gelijk is aan nul.	De service voor Physical Data Shipping is dan niet meer beschikbaar binnen een klanttenant.

Als u een optie wilt uitschakelen waarvan het gebruik meer dan nul is, kunt u het gebruik handmatig verwijderen en vervolgens de bijbehorende optie uitschakelen.

4.0.2 Softe en harde quota's

Met **quota's** kunt u beperkingen instellen voor het gebruik van de service door tenants. Als u de quota's wilt instellen, selecteert u de klant op het tabblad **Klanten**, selecteert u het tabblad Service en klikt u op **Bewerken**.

Wanneer de quota wordt overschreden, wordt een melding verzonden naar het e-mailadres van de gebruiker. Als u geen quota-uitbreiding instelt, wordt de quota beschouwd als '**soft**'. Dit betekent dat beperkingen voor het gebruik van de Cyber Protection-service niet worden toegepast.

Wanneer u de quota-uitbreiding opgeeft, wordt de quota beschouwd als '**hard**'. Met een **uitbreiding** kan de gebruiker de quota overschrijden met de opgegeven waarde. Wanneer de uitbreiding wordt overschreden, worden er beperkingen toegepast voor het gebruik van de service.

Voorbeeld

Softe quota: U hebt de quota voor werkstations ingesteld op 20. Zodra het aantal beschermde werkstations van de klant 20 is, krijgt de klant een melding per e-mail. De Cyber Protection-service blijft beschikbaar.

Harde quota: Als u de quota voor werkstations hebt ingesteld op 20 en de uitbreiding 5 is, dan krijgt uw klant een melding per e-mail zodra het aantal beschermde werkstations 20 is. De Cyber Protection-service wordt uitgeschakeld wanneer het aantal van 25 wordt bereikt.

Niveaus waarop quota's kunnen worden ingesteld

De quota's kunnen worden ingesteld op de niveaus zoals weergegeven in onderstaande tabel.

Tenant/Gebruiker	Softe quota (alleen quota)	Harde quota (quota en uitbreiding)
Partner	ja	nee
Map	ja	nee
Klant	ja	ja
Eenheid	nee	nee
Gebruiker	ja	ja

De softe quota's kunnen worden ingesteld op het niveau van de partner en de map. Op het niveau van de eenheid kunnen geen quota's worden ingesteld. De harde quota's kunnen worden ingesteld op het niveau van de klant en de gebruiker.

De totale hoeveelheid harde quota's die op gebruikersniveau zijn ingesteld, kan niet groter zijn dan de harde quota van de betreffende klant.

Quota's voor back-ups

U kunt waarden opgeven voor de cloudopslagquota, de quota voor lokale back-up en het maximale aantal machines/apparaten/websites dat de gebruiker mag beveiligen. De volgende quota's zijn beschikbaar.

Quota's voor apparaten

- **Werkstations**
- **Servers**
- **Virtuele machines**
- **Mobiele apparaten**

- **Webhostingservers** (op Linux gebaseerde fysieke of virtuele servers waarop een Plesk-, cPanel-, DirectAdmin-, VirtualMin- of ISPManager-besturingspaneel wordt uitgevoerd)
- **Websites**

Een machine/apparaat/website wordt beschouwd als beschermd zolang hierop ten minste één beschermingsschema wordt toegepast. Een mobiel apparaat is beveiligd na de eerste backup.

Wanneer de uitbreiding voor een aantal apparaten wordt overschreden, kan de gebruiker geen beschermingsschema toepassen voor meer apparaten.

Quota's voor cloudgegevensbronnen

- **Microsoft 365-seats**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota en het gebruik bekijken in de beheerportal.

  Licenties voor de Microsoft 365-seats zijn afhankelijk van de geselecteerde factureringsmodus voor Cyber Protection.

  Meer informatie over de beschikbare licentieopties voor de factureringsmodus per gigabyte vindt u in Cyber Protect Cloud: Licenties voor Microsoft 365 per GB.

  Meer informatie over de beschikbare licentieopties voor de factureringsmodus per workload vindt u in Cyber Protect Cloud: Wijzigingen van de licenties en prijzen voor Microsoft 365.
- **Microsoft 365 Teams**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Met deze quota wordt de mogelijkheid om Microsoft 365 Teams te beschermen in- of uitgeschakeld. Daarnaast wordt ook ingesteld wat het maximale aantal teams is dat kan worden beschermd. Voor de bescherming van één team, ongeacht het aantal leden of kanalen, is één quota vereist. Bedrijfbeheerders kunnen de quota en het gebruik bekijken in de beheerportal.
- **Microsoft 365 SharePoint Online**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Met deze quota wordt de mogelijkheid om SharePoint Online-sites te beschermen in- of uitgeschakeld. Daarnaast wordt ook ingesteld wat het maximale aantal siteverzamelingen en groepssites is dat kan worden beschermd.

  Bedrijfbeheerders kunnen de quota bekijken in de beheerportal. Ze kunnen ook de quota, samen met de hoeveelheid opslagruimte voor de back-ups van SharePoint Online, bekijken in de gebruiksrapporten.
- **Google Workspace-seats**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Het bedrijf kan toestemming hebben om **Gmail**-postvakken (met inbegrip van agenda en contacten), **Google Drive**-bestanden of beide te beveiligen. Bedrijfbeheerders kunnen de quota en het gebruik bekijken in de beheerportal.
- **Gedeelde Drive in Google Workspace**

  Deze quota wordt door de serviceprovider toegepast op het hele bedrijf. Met deze quota wordt de mogelijkheid om gedeelde Drives in Google Workspace te beschermen in- of uitgeschakeld.

Als de quota is ingeschakeld, kan een willekeurig aantal gedeelde Drives worden beveiligd. Bedrijfbeheerders kunnen de quota in de beheerportal niet bekijken, maar kunnen in de gebruiksrapporten wel zien hoeveel opslagruimte in beslag wordt genomen door de back-ups van de gedeelde Drives.

Een back-up van gedeelde Drives in Google Workspace is alleen beschikbaar voor klanten die daarnaast ten minste één quota voor Google Workspace-seats hebben. Deze quota wordt alleen geverifieerd en wordt niet opgenomen.

Een Microsoft 365-seat wordt beschouwd als beschermd zolang er ten minste één beschermingsschema wordt toegepast op het postvak of OneDrive van de gebruiker. Een Google Workspace-seat wordt beschouwd als beschermd zolang er ten minste één beschermingsschema wordt toegepast op het postvak of Google Drive van de gebruiker.

Wanneer de uitbreiding voor een aantal seats wordt overschreden, kan een bedrijfbeheerder geen beschermingsschema toepassen voor meer seats.

Quota's voor opslag

- **Lokale back-up**

  De quota voor **Lokale back-up** beperkt de totale grootte van lokale back-ups die worden gemaakt met behulp van de cloudinfrastructuur. U kunt geen uitbreiding instellen voor deze quota.
- **Cloudresources**

  De quota voor **cloudresources** combineert de quota voor back-upopslag en de quota's voor noodherstel. De quota voor back-upopslag beperkt de totale omvang van de back-ups in de cloudopslag. Wanneer de uitbreiding van de back-upopslagquota wordt overschreden, mislukken de back-ups.

Overschrijding van de quota voor back-upopslag

De quota voor back-upopslag kan niet worden overschreden. Het certificaat van de beveiligingsagent heeft een technische quota die gelijk is aan de back-upquota van de tenant + uitbreiding. Een back-up kan niet worden gestart als de quota is overschreden. Als de quota in het certificaat, maar niet de uitbreiding wordt bereikt tijdens het maken van de back-up, zal de back-up worden voltooid. Als de quota van de uitbreiding wordt bereikt tijdens het maken van de back-up, mislukt de back-up.

Bijvoorbeeld:

Een gebruikerstenant heeft 1 TB vrije ruimte van de quota, en de geconfigureerde uitbreiding voor deze gebruiker is 5 TB. De gebruiker start een back-up. Als de grootte van de gemaakte back-up bijvoorbeeld 3 TB is, zal de back-up worden voltooid omdat de uitbreiding niet wordt overschreden. Als de grootte van de gemaakte back-up groter is dan 6 TB, mislukt de back-up wanneer de uitbreiding wordt overschreden.

Back-upquotatransformatie

De gebruikelijke procedure voor het ophalen van een back-upquota en het toewijzen van een optie aan een resourcetype is als volgt: de beschikbare opties worden automatisch vergeleken met het resourcetype en vervolgens wordt de quota voor de overeenkomstige optie opgehaald.

Er is ook een mogelijkheid om een andere optiequota toe te wijzen, zelfs als deze niet precies overeenkomt met het resourcetype. Dit wordt **back-upquotatransformatie** genoemd. Als er geen overeenkomstige optie is, wordt automatisch geprobeerd een duurdere geschikte quota te vinden voor het resourcetype (automatische back-upquotatransformatie). Als er niets wordt gevonden dat geschikt is, dan kunt u de servicequota handmatig toewijzen aan het resourcetype in de serviceconsole.

Voorbeeld

U wilt een back-up maken van een virtuele machine (werkstation, met agent).

Eerst wordt gecontroleerd of er een toegewezen quota is voor **Virtuele machines** . Als deze niet wordt gevonden, dan wordt automatisch geprobeerd de quota voor **werkstations** op te halen. Als deze ook niet wordt gevonden, wordt er geen andere quota automatisch opgehaald. Als u voldoende quota hebt die duurder is dan de quota voor de **virtuele machines** en deze van toepassing is op een virtuele machine, dan kunt u zich aanmelden bij de serviceconsole en de quota voor **servers** handmatig toewijzen.

Quota's voor noodherstel

Opmerking
De opties voor noodherstel zijn alleen beschikbaar in de Disaster Recovery-add-on.

Deze quota's worden door de serviceprovider toegepast op het hele bedrijf. Bedrijfbeheerders kunnen de quota's en het gebruik in de beheerportal bekijken, maar kunnen geen quota's voor een gebruiker instellen.

- **Noodherstelopslag**
  Deze opslag wordt gebruikt door primaire en herstelservers. Als de maximale uitbreiding voor deze quota wordt bereikt, kunt u geen primaire en herstelservers maken, en geen schijven van de bestaande primaire servers toevoegen/uitbreiden. Als de maximale uitbreiding voor deze quota's wordt overschreden, kunt u geen failover starten en ook geen gestopte server starten. Actieve servers blijven actief.
- **Compute-punten**
  Deze quota beperkt de CPU- en RAM-resources die worden verbruikt door primaire servers en herstelservers gedurende een factureringsperiode. Als de maximale uitbreiding voor deze quota wordt bereikt, worden alle primaire en herstelservers afgesloten. U kunt deze servers pas weer gebruiken bij het begin van de volgende factureringsperiode. De standaardfactureringsperiode is een volledige kalendermaand.

Wanneer de quota wordt uitgeschakeld, kunnen de servers niet worden gebruikt, ongeacht de factureringsperiode.

- **Openbare IP-adressen**

  Deze quota beperkt het aantal openbare IP-adressen dat kan worden toegewezen aan de primaire en herstelservers. Als de maximale uitbreiding voor deze quota wordt bereikt, kunt u geen openbare IP-adressen inschakelen voor meer servers. U kunt verhinderen dat een server een openbaar IP-adres gebruikt door het selectievakje **Openbaar IP-adres** uit te schakelen in de serverinstellingen. Vervolgens kunt u toestaan dat een andere server een openbaar IP-adres gebruikt. Dit is doorgans niet hetzelfde adres.

  Wanneer de quota wordt uitgeschakeld, maken alle servers geen gebruik meer van openbare IP-adressen, zodat ze niet meer bereikbaar zijn vanaf internet.
- **Cloudservers**

  Deze quota beperkt het totale aantal primaire en herstelservers. Als de maximale uitbreiding voor deze quota is bereikt, kunt u geen primaire of herstelservers maken.

  Wanneer de quota wordt uitgeschakeld, worden de servers weergegeven in de serviceconsole, maar de enige beschikbare bewerking is **Verwijderen**.
- **Internettoegang**

  Met deze quota wordt de internettoegang vanaf primaire en herstelservers in- of uitgeschakeld.

  Wanneer de quota wordt uitgeschakeld, kunnen de primaire en herstelservers geen verbinding maken met internet.

Quota's voor File Sync & Share

U kunt de volgende quota's voor File Sync & Share instellen voor een tenant:

- **Gebruikers**

  Met deze quota definieert u het aantal gebruikers dat toegang krijgt tot deze service.
- **Cloudopslag**

  Dit is cloudopslag voor het opslaan van gebruikersbestanden. De quota bepaalt de toegewezen ruimte voor een tenant in de cloudopslag.

Quota's voor Physical Data Shipping

De quota's voor de Physical Data Shipping-service worden per station verbruikt. U kunt de initiële back-ups van meerdere machines op één harde schijf opslaan.

U kunt de volgende quota's voor Physical Data Shipping instellen voor een tenant:

- **Naar de cloud**

  Hiermee kunt u een initiële back-up naar het clouddatacentrum verzenden via een hardeschijfstation. Met deze quota definieert u het maximale aantal stations dat wordt overgezet naar het clouddatacentrum.

Quota's voor notarisatie

U kunt de volgende notarisatiequota's instellen voor een tenant:

- **Notarisatieopslag**

  De notarisatieopslag is de cloudopslag waar de genotariseerde bestanden, ondertekende bestanden en bestanden die nog worden genotariseerd of ondertekend, worden opgeslagen. Deze quota definieert de maximale ruimte die door deze bestanden kan worden ingenomen.

  Als u dit quotagebruik wilt verminderen, kunt u de reeds genotariseerde of ondertekende bestanden verwijderen uit de notarisatieopslag.
- **Notarisaties**

  Deze quota definieert het maximale aantal bestanden dat kan worden genotariseerd met Notary-service. Een bestand wordt beschouwd als genotariseerd zodra het naar de notarisatieopslag wordt geüpload en de notarisatiestatus wordt gewijzigd in Wordt uitgevoerd.

  Als hetzelfde bestand meerdere keren wordt genotariseerd, telt elke keer als een nieuwe notarisatie.
- **eSignatures**

  Deze quota definieert het maximale aantal bestanden dat kan worden ondertekend met Notary-service. Een bestand wordt beschouwd als ondertekend zodra het wordt verzonden voor ondertekening.

4.0.3 Opties en installatieprogramma's van agenten

Of het installatieprogramma van de agent beschikbaar is in het gedeelte **Apparaten toevoegen** in de serviceconsole, hangt af van de toegestane opties. In de volgende tabel ziet u welke installatieprogramma's van de agent beschikbaar zijn in de serviceconsole al naargelang de ingeschakelde opties.

Ingeschakelde optie **Installatieprogramma van agent**	**Servers**	**Werkstations**	**Virtuele machines**	**Microsoft 365-seats**	**Google Workspace-seats**	**Mobiele apparaten**	**Webhostingservers**	**Websites**
Werkstations – Agent voor Windows		+	+					+
Werkstations – Agent voor Mac OS		+	+					+
Servers – Agent voor Windows	+		+				+	+
Servers – Agent voor Linux	+		+				+	+
Agent voor Hyper-V			+					

Agent voor VMware			+					
Agent voor Virtuozzo			+					
Agent voor SQL	+		+					
Agent voor Exchange	+		+					
Agent voor Active Directory	+		+					
Agent voor Microsoft 365				+				
Agent voor Google Workspace					+			
Volledig installatieprogramma voor Windows	+	+	+				+	+
Mobiel (iOS en Android)						+		

4.1 Gebruikersaccounts en tenants

Er zijn twee typen gebruikersaccounts: beheerdersaccounts en gebruikersaccounts.

- **Beheerders** hebben toegang tot de beheerportal. Ze hebben de beheerdersrol in alle services.
- **Gebruikers** hebben geen toegang tot de beheerportal. Hun toegang tot de services een hun rollen in de services worden gedefinieerd door een beheerder.

Elk account behoort tot een tenant. Een tenant is een deel van de resources (zoals gebruikersaccounts en onderliggende tenants) en serviceopties (ingeschakelde services en opties binnen de resources) van de beheerportal, die specifiek zijn bedoeld voor een bepaalde partner of klant. De tenanthiërarchie moet in principe overeenkomen met de klant/leverancierrelaties tussen de servicegebruikers en de leveranciers.

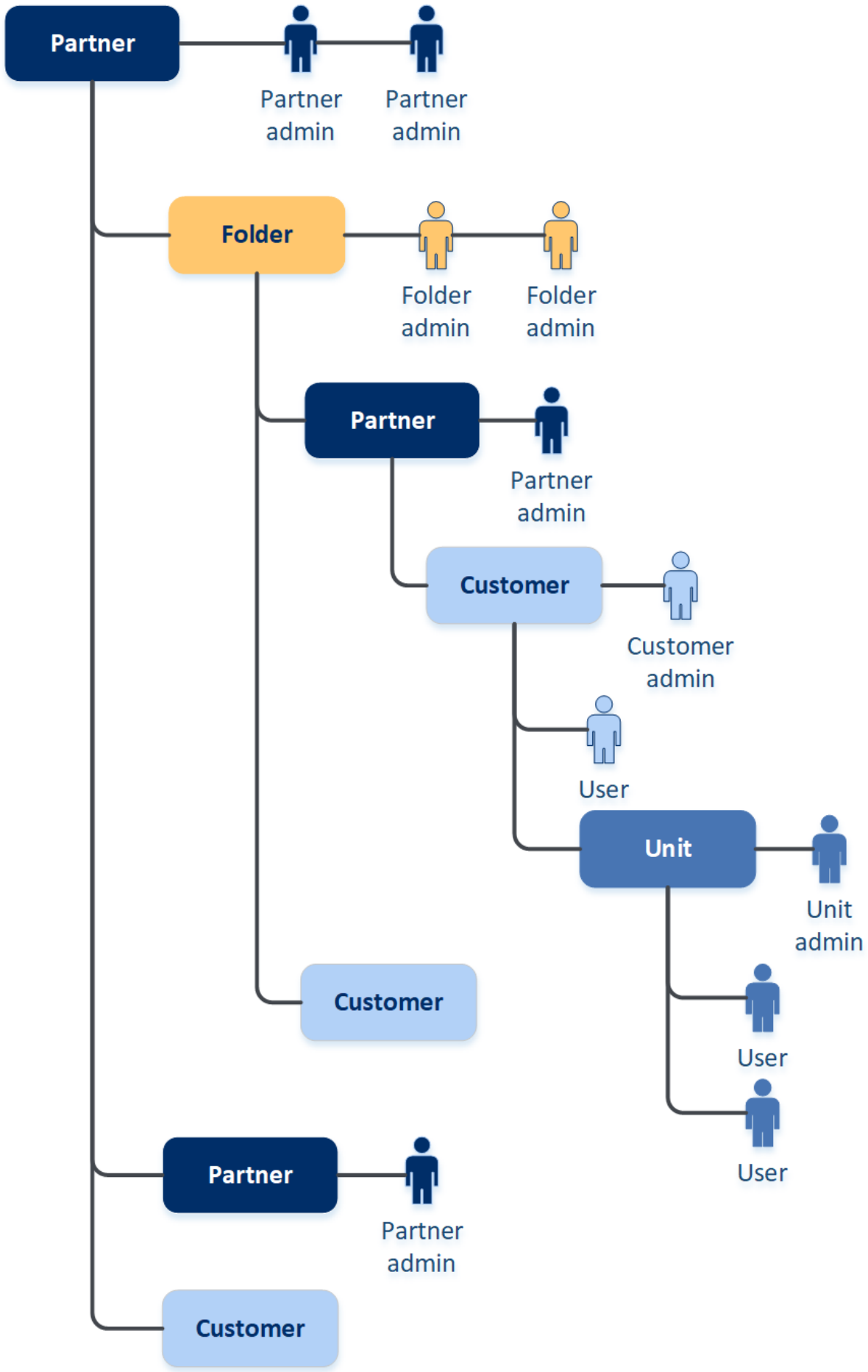
- Een tenant van het type **Partner** komt doorgaans overeen met de serviceproviders die de services doorverkopen.
- Een tenant van het type **Map** is een aanvullende tenant die doorgaans wordt gebruikt door partnerbeheerders om partners en klanten te groeperen en hiervoor afzonderlijke opties en/of verschillende branding te configureren.
- Een tenant van het type **Klant** komt meestal overeen met organisaties die de services gebruiken.

- Een tenant van het type **Eenheid** komt doorgaans overeen met eenheden of afdelingen binnen de organisatie.

Een beheerder kan tenants, beheerdersaccounts en gebruikersaccounts maken en beheren op het eigen niveau in de hiërarchie of op een lager niveau.

Een beheerder van een bovenliggende tenant van het type **Partner** kan optreden als beheerder van een lager niveau voor tenants van het type **Klant** of **Partner** met beheermodus **Beheerd door serviceprovider**. Zo kan de beheerder op partnerniveau bijvoorbeeld gebruikersaccounts en services beheren, of toegang krijgen tot back-ups en andere resources in de onderliggende tenant. Beheerders op het lagere niveau kunnen echter de toegang tot hun tenant beperken voor beheerders op hoger niveau.

Het volgende diagram bevat een voorbeeldhiërarchie van de tenants: partner, map, klant en eenheid.


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

De volgende tabel bevat een overzicht van de bewerkingen die door beheerders en gebruikers kunnen worden uitgevoerd.

Bewerking	Gebruikers	Klant- en eenheidbeheerders	Partner- en mapbeheerders
Tenants maken	Nee	Ja	Ja
Accounts maken	Nee	Ja	Ja
De software downloaden en installeren	Ja	Ja	Nee*
Services beheren	Ja	Ja	Ja
Rapporten maken over het servicegebruik	Nee	Ja	Ja
Branding configureren	Nee	Nee	Ja

*Een partnerbeheerder die deze bewerkingen moet uitvoeren, kan een account als klantbeheerder of als gebruiker maken voor zichzelf.

4.2 Modus Verbeterde beveiliging

De modus Verbeterde beveiliging biedt speciale instellingen voor klanten met verhoogde beveiligingseisen. In deze modus is versleuteling van alle back-ups vereist en zijn alleen lokaal ingestelde versleutelingswachtwoorden toegestaan.

Een partnerbeheerder kan de modus Verbeterde beveiliging alleen inschakelen wanneer een nieuwe klanttenant wordt gemaakt en deze modus kan later niet worden uitgeschakeld. De modus Verbeterde beveiliging kan niet worden ingeschakeld voor reeds bestaande tenants.

Met de modus Verbeterde beveiliging worden alle back-ups die in een klanttenant en de eenheden daarvan zijn gemaakt, automatisch versleuteld met het AES-algoritme en een 256-bits sleutel. Gebruikers kunnen hun versleutelingswachtwoorden alleen instellen op de beschermde apparaten en kunnen de versleutelingswachtwoorden niet instellen in de beschermingsschema's.

Cloudservices hebben geen toegang tot de versleutelingswachtwoorden. Als gevolg van deze beperking zijn de volgende functies niet beschikbaar voor tenants in de modus Verbeterde beveiliging:

- Herstel via de serviceconsole
- Bladeren door back-ups op bestandsniveau via de serviceconsole
- Cloud-to-cloud back-up
- Back-ups van websites
- Back-up van applicatie
- Back-up van mobiele apparaten

- Antimalwarescan van back-ups
- Veilig herstel
- Automatische aanmaak van witte lijsten voor bedrijven
- Overzicht van gegevensbescherming
- Noodherstel
- Rapporten en dashboards over niet-beschikbare functies

4.2.1 Beperkingen

- De modus Verbeterde beveiliging is alleen compatibel met agenten met versie 15.0.26390 of hoger.
- De modus Verbeterde beveiliging is niet beschikbaar voor apparaten waarop Red Hat Enterprise Linux 4.x of 5.x en afgeleiden daarvan worden uitgevoerd.

4.3 Ondersteunde webbrowsers

De webinterface ondersteunt de volgende webbrowsers:

- Google Chrome 29 of later
- Mozilla Firefox 23 of later
- Opera 16 of later
- Windows Internet Explorer 11 of later
- Microsoft Edge 25 of later
- Safari 8 of later uitgevoerd op de besturingssystemen macOS en iOS

Het is mogelijk dat de gebruikersinterface in andere webbrowsers (inclusief Safari-browsers die worden uitgevoerd op andere besturingssystemen) niet goed wordt weergegeven of dat bepaalde functies niet beschikbaar zijn.

5 De beheerportal gebruiken

De volgende stappen helpen u de basisfuncties van de beheerportal te gebruiken.

5.1 Het beheerdersaccount activeren

Nadat u de partnerschapsovereenkomst hebt ondertekend, ontvangt u een e-mailbericht met de volgende informatie:

- **Een activeringslink voor het account**. Klik op de link en stel het wachtwoord voor het beheerdersaccount in. Het wachtwoord moet minimaal acht tekens lang zijn. Onthoud de gebruikersnaam die wordt weergegeven op de activeringspagina voor het account.
- **Een link naar de aanmeldingspagina**. De gebruikersnaam en het wachtwoord zijn hetzelfde als in de vorige stap.

5.2 Toegang tot de beheerportal

1. Ga naar de aanmeldingspagina voor de service.
   Het adres van de aanmeldingspagina is opgenomen in de activerings-e-mail die u hebt ontvangen.
2. Typ de gebruikersnaam en klik op **Volgende**.
3. Typ het wachtwoord en klik op **Volgende**.

   Opmerking
   Na 10 mislukte aanmeldingspogingen wordt de toegang tot de portal vergrendeld om beveiligingsaanvallen tegen Cyber Cloud te voorkomen. De vergrendelingsperiode is 5 minuten. Het aantal mislukte aanmeldingspogingen wordt na 15 minuten opnieuw ingesteld.

4. Gebruik het menu aan de rechterkant om te navigeren in de beheerportal.

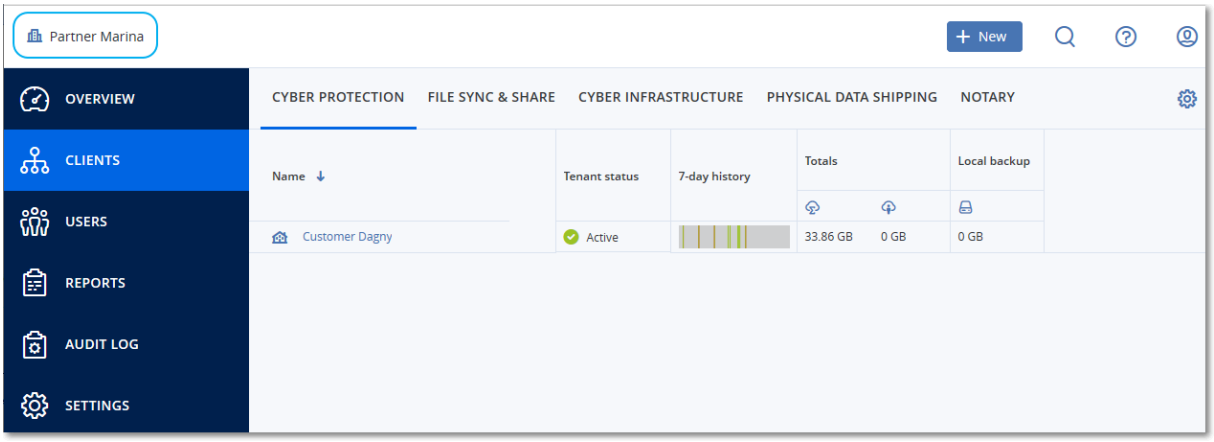
De time-outperiode voor de beheerportal is 24 uur voor actieve sessies en 1 uur voor niet-actieve sessies.

Sommige services bieden een functie om naar de beheerportal over te schakelen vanuit de serviceconsole.

5.3 Navigatie in de beheerportal

Wanneer u de beheerportal gebruikt, werkt u steeds binnen een tenant. Dit wordt aangegeven in de linkerbovenhoek.

Standaard wordt het bovenste hiërarchische niveau geselecteerd dat beschikbaar is voor u. Klik op de naam van de tenant om in te zoomen op de hiërarchie. Klik op een naam in de linkerbovenhoek om terug te navigeren naar een hoger niveau.



Alleen de tenant waarin u op dat moment werkt, wordt weergegeven en beïnvloed door de diverse delen van de gebruikersinterface. Bijvoorbeeld:

- Op het tabblad **Clients** worden alleen de tenants weergegeven die de directe onderliggende tenants zijn van de tenant waarin u op dat moment werkt.
- Op het tabblad **Gebruikers** worden alleen de gebruikersaccounts weergegeven die bestaan in de tenant waarin u op dat moment werkt.
- Met de knop **Nieuw** kunt u alleen een tenant of nieuw gebruikersaccount maken in de tenant waarin u op dat moment werkt.

5.4 Toegang tot de services

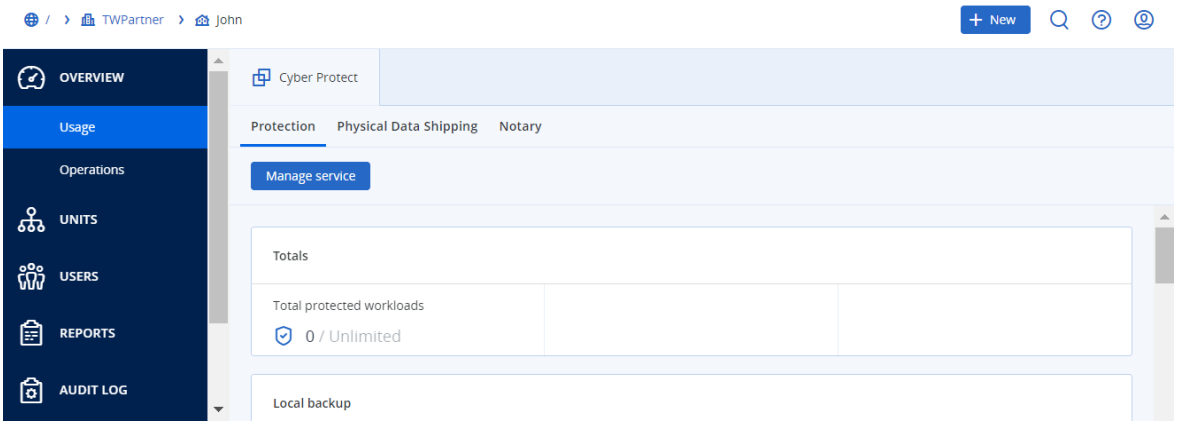
5.4.1 Tabblad Overzicht

Het gedeelte **Overzicht** > **Gebruik** bevat een overzicht van het servicegebruik. In dit gedeelte hebt u toegang tot de services binnen de tenant waarin u werkt.

Een service beheren voor een tenant via het tabblad Overzicht

1. Navigeer naar de tenant waarvoor u een service wilt beheren en klik op **Overzicht** > **Gebruik**.
   Let op: sommige services kunnen worden beheerd op het niveau van de partnertenant en klanttenant, maar andere services kunnen alleen worden beheerd op het niveau van de klanttenant.
2. Klik op de naam van de service die u wilt beheren en klik vervolgens op **Service beheren** of **Service configureren**.
   Raadpleeg de gebruikershandleidingen in de serviceconsoles voor meer informatie over het

gebruik van de services.

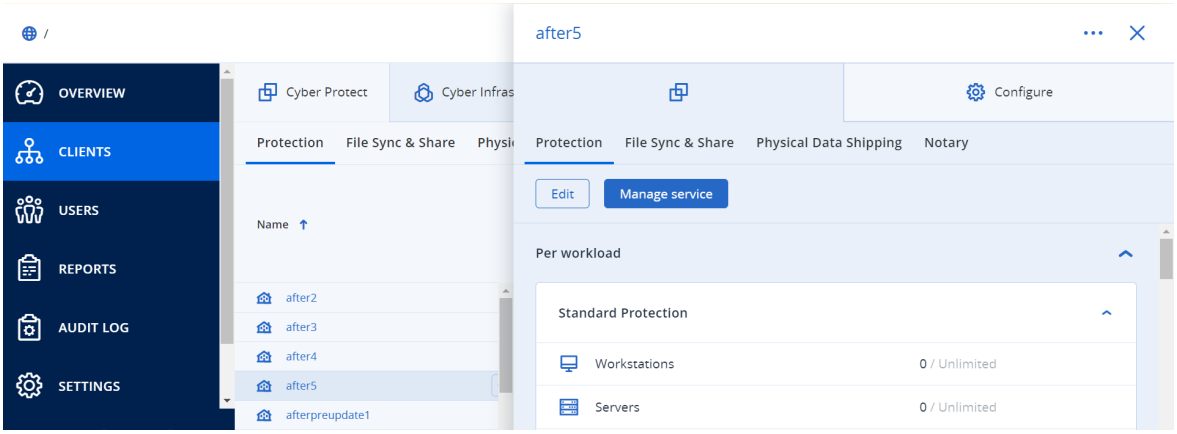


5.4.2 Tabblad Clients

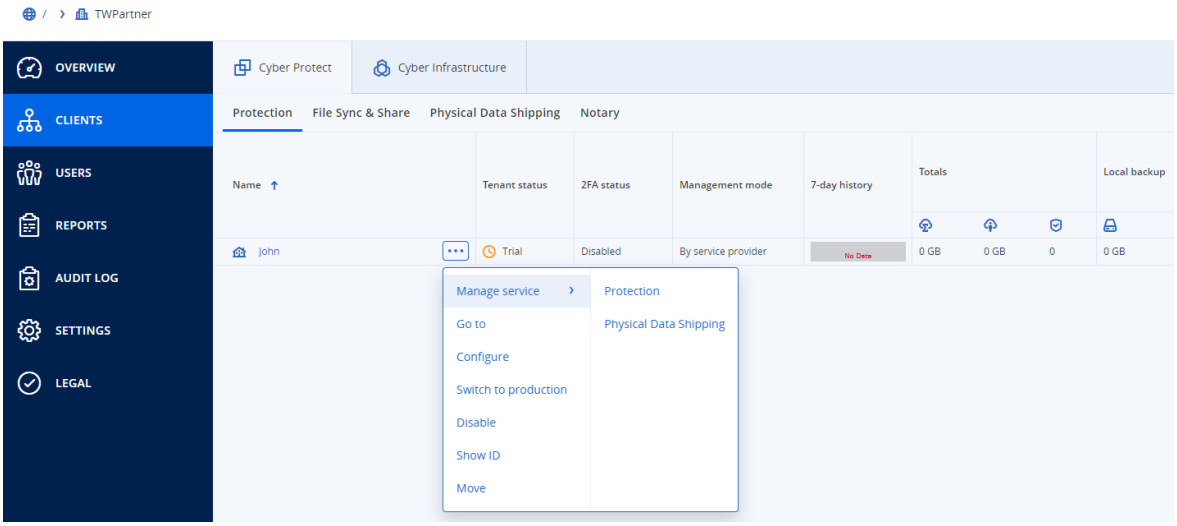
Het tabblad **Clients** geeft de onderliggende tenants weer waarin u werkt. Op dit tabblad hebt u toegang tot de services binnen de onderliggende tenants.

Een service beheren voor een tenant via het tabblad Clients

1. Voer een van de volgende handelingen uit:
   - Klik op **Clients**, selecteer de tenant waarvoor u een service wilt beheren, klik op de naam of het pictogram van de service die u wilt beheren en klik vervolgens op **Service beheren** of **Service configureren**.



   - Klik op **Clients**, klik op het ellipspictogram naast de naam van de tenant waarvoor u een service wilt beheren, klik op **Service beheren** en selecteer de service die u wilt beheren.



Let op: sommige services kunnen worden beheerd op het niveau van de partnertenant en klanttenant, maar andere services kunnen alleen worden beheerd op het niveau van de klanttenant.

Raadpleeg de gebruikershandleidingen in de serviceconsoles voor meer informatie over het gebruik van de services.

5.5 De balk 7 dagen geschiedenis

Op het scherm **Clients** wordt de balk **7 dagen geschiedenis** weergegeven met de status van de workloadback-ups voor elke klanttenant gedurende de afgelopen zeven dagen. De balk is verdeeld in 168 gekleurde lijnen. Elke lijn vertegenwoordigt een interval van één uur, en geeft de slechtste status van een back-up binnen het overeenkomstige interval van één uur weer.

De volgende tabel bevat informatie over de betekenis van elke kleur van de lijnen.

Kleur	Beschrijving
rood	ten minste één van de back-ups tijdens de periode van één uur is mislukt
oranje	ten minste één van de back-ups tijdens de periode van één uur is voltooid met een waarschuwing, maar zonder back-upfouten
groen	er is ten minste één geslaagde back-up tijdens de periode van één uur, zonder back-upfouten en -waarschuwingen
grijs	er waren geen voltooide back-ups tijdens de periode van één uur

Op de balk **7 dagen geschiedenis** wordt 'Geen back-ups' weergegeven totdat de betreffende statistieken zijn verzameld.

De balk **7 dagen geschiedenis** is leeg in het geval van partnertenants, omdat de geaggregeerde statistieken niet worden ondersteund.

5.6 Tenants maken en configureren

De volgende tenants zijn beschikbaar in Cyber Protect:

- Doorgaans wordt er een **Partner**tenant gemaakt voor elke partner die de partnerschapsovereenkomst ondertekent.
- Doorgaans wordt er voor elke groep partners en klanten een **Map**tenant gemaakt om afzonderlijke opties en/of verschillende branding te configureren.
- Doorgaans wordt er een **Klant**tenant gemaakt voor elke organisatie die zich aanmeldt voor een service.
- Een **eenheid**tenant wordt gemaakt binnen een klanttenant om de service uit te breiden naar een nieuwe organisatie-eenheid.

De stappen voor het maken en configureren van een tenant variëren naargelang de tenant die u maakt, maar over het algemeen bestaat het proces uit de volgende stappen:

1. Maak de tenant.
2. Selecteer services voor de tenant.
3. Configureer de opties voor de tenant.

5.6.1 Een tenant maken

1. Meld u aan bij de beheerportal.
2. Navigeer naar de tenant waarvoor u een tenant wilt maken.
3. Klik in de rechterbovenhoek op **Nieuw** en vervolgens op een van de volgende opties, afhankelijk van het type tenant dat u wilt maken:
   - Doorgaans wordt er een **Partner**tenant gemaakt voor elke partner die de partnerschapsovereenkomst ondertekent.
   - Doorgaans wordt er voor elke groep partners en klanten een **Map**tenant gemaakt om afzonderlijke opties en/of verschillende branding te configureren.
   - Doorgaans wordt er een **Klant**tenant gemaakt voor elke organisatie die zich aanmeldt voor een service.
   - Een **eenheid**tenant wordt gemaakt binnen een klanttenant om de service uit te breiden naar een nieuwe organisatie-eenheid.

   Welke typen beschikbaar zijn, hangt af van het bovenliggende type tenant.
4. Geef bij **Naam** een naam op voor de nieuwe tenant.
5. [Alleen wanneer u een klanttenant maakt] Selecteer bij **Modus** of de tenant de services in de proef- of productiemodus gebruikt. De maandelijkse rapporten met het servicegebruik bevatten geen gebruiksgegevens voor tenants in de proefmodus.

Belangrijk
Als u halverwege de maand overschakelt van de proefmodus naar de productiemodus, wordt de volledige maand opgenomen in het maandelijkse rapport over het servicegebruik. Daarom adviseren we u over te schakelen op de eerste dag van de maand. Wanneer een tenant een volledige maand in de proefmodus blijft, wordt automatisch overgeschakeld naar de productiemodus.

6. Selecteer in de **Beheermodus** een van de volgende modi voor het beheren van toegang tot de tenant:
   - **Selfservice**: Met deze modus hebben beheerders van de bovenliggende tenant beperkte toegang tot deze tenant: ze kunnen alleen de eigenschappen van de tenant wijzigen, maar hebben geen toegang tot items binnen de tenant (bijvoorbeeld tenants, gebruikers, services, back-ups en andere resources) en kunnen deze niet beheren.
   - **Beheerd door serviceprovider**: Met deze modus krijgen beheerders van de bovenliggende tenant volledige toegang tot de tenant: ze kunnen eigenschappen wijzigen; tenants, gebruikers en services beheren en hebben toegang tot back-ups en andere resources.

   Alleen de beheerder van de door u gemaakte tenant kan de beheermodus wijzigen als deze **Selfservice** is. De beheerder van de gemaakte tenant kan dit doen via **Instellingen** > **Beveiliging** en de schakelaar **Toegang tot ondersteuning**.

   Ga naar **Clients** om de geselecteerde beheermodus voor uw onderliggende tenants te bekijken.
7. In **Beveiliging** kunt u tweeledige verificatie voor de tenant in- of uitschakelen.
   Indien deze optie is ingeschakeld, moeten alle gebruikers van deze tenant tweeledige verificatie instellen voor hun accounts om veiligere toegang te waarborgen. Gebruikers moeten de verificatietoepassing installeren op hun tweede-factor-apparaten en de eenmalig gegenereerde TOTP-code samen met hun gebruikelijke gebruikersnaam en wachtwoord gebruiken om zich aan te melden bij de console. Zie 'Tweeledige verificatie instellen' voor meer informatie. Ga naar **Clients** om de status van tweeledige verificatie te bekijken voor uw klanten.
8. [Alleen wanneer u een klanttenant maakt in de modus Verbeterde beveiliging] Schakel in **Beveiliging** het selectievakje voor de **modus Verbeterde beveiliging** in.
   In deze modus zijn alleen versleutelde back-ups toegestaan. Het versleutelingswachtwoord moet zijn ingesteld op het beschermde apparaat. Anders kunnen er geen back-ups worden gemaakt. Alle bewerkingen waarbij het versleutelingswachtwoord moet worden opgegeven voor een cloudservice, zijn niet beschikbaar. Zie "Modus Verbeterde beveiliging" (p. 36) voor meer informatie.

   Belangrijk
   U kunt de modus Verbeterde beveiliging niet uitschakelen wanneer de tenant al is gemaakt.

9. In **Beheerder maken** voert u een gebruikersnaam en e-mailadres in voor het beheerdersaccount.
   Indien gewenst kunt u een taal kiezen. Engels is de standaardtaal.

Opmerking
Als de **Beheermodus** is ingesteld op **Selfservice**, moet er een beheerder worden gemaakt voor een klanttenant en partnertenant.

10. Selecteer bij **Taal** de standaardtaal voor meldingen, rapporten en de software die binnen deze tenant worden gebruikt.
11. Voer een van de volgende handelingen uit:
    - Klik op **Opslaan en sluiten** om het maken van de tenant te voltooien. In dit geval worden alle services ingeschakeld voor de tenant. De factureringsmodus voor de Bescherming-service wordt ingesteld op Per workload.
    - Klik op **Volgende** om services te selecteren voor de tenant. Zie "De services selecteren voor een tenant" (p. 44).

5.6.2 De services selecteren voor een tenant

Standaard worden alle services ingeschakeld wanneer u een nieuwe tenant maakt. U kunt selecteren welke services beschikbaar zijn voor de gebruikers binnen de tenant en de onderliggende tenants.

Deze procedure is niet van toepassing op een eenheidtenant.

De services selecteren voor een tenant

1. In het gedeelte **Services selecteren** van het dialoogvenster Tenant maken/bewerken selecteert u een factureringsmodus of een editie.
    - Selecteer de factureringsmodus **Per workload** of **Per gigabyte** en schakel vervolgens de selectievakjes uit voor de services die u wilt uitschakelen voor de tenant.
      De set services is identiek voor beide factureringsmodi.

      Als u voor Advanced Disaster Recovery uw eigen locatie voor noodherstel hebt geregistreerd onder uw account, kunt u de locatie voor noodherstel selecteren in de vervolgkeuzelijst.
    - Als u een verouderde editie wilt gebruiken, selecteert u het keuzerondje **Verouderde edities** en selecteert u een editie in de vervolgkeuzelijst.

    Uitgeschakelde services worden verborgen voor de gebruikers binnen de tenant en de onderliggende tenants.
2. Voer een van de volgende handelingen uit:
    - Klik op **Opslaan en sluiten** om het maken van de tenant te voltooien. In dit geval worden alle opties voor de geselecteerde services ingeschakeld voor de tenant, met onbeperkte quota.
    - Klik op **Volgende** om de opties voor de tenant te configureren. Zie "De opties voor een tenant configureren" (p. 44).

5.6.3 De opties voor een tenant configureren

Wanneer u een nieuwe tenant maakt, worden alle opties voor de geselecteerde services ingeschakeld. U kunt selecteren welke opties beschikbaar zijn voor de gebruikers binnen de tenant en de onderliggende tenants, en hiervoor quota's instellen.

Deze procedure is niet van toepassing op een eenheidtenant.

De opties voor een tenant configureren

1. Ga naar het gedeelte **Services configureren** van het dialoogvenster Tenant maken/bewerken en schakel op elk servicetabblad de selectievakjes uit voor de opties die u wilt uitschakelen.
   De functionaliteit die overeenkomt met de uitgeschakelde opties, is niet beschikbaar voor de gebruikers binnen de tenant en de onderliggende tenants.

   Opmerking
   U kunt de opties uitschakelen die verband houden met geavanceerde beschermingsfunctionaliteit, maar ze zullen automatisch weer worden ingeschakeld wanneer een gebruiker een geavanceerde functie inschakelt in een beschermingsschema.

2. Voor sommige services kunt u de opslagruimten selecteren die beschikbaar zijn voor de nieuwe tenant. Opslagruimten worden gegroepeerd op locatie. U kunt kiezen uit de lijst met locaties en opslagruimten die beschikbaar zijn voor uw tenant.
   - Wanneer u een partner-/maptenant maakt, kunt u meerdere locaties en opslagruimten selecteren voor elke service.
   - Wanneer u een klanttenant maakt, moet u één locatie selecteren en vervolgens één opslagruimte per service binnen die locatie selecteren. De opslagruimten die aan de klant zijn toegewezen, kunnen later worden gewijzigd, maar alleen als hun gebruik 0 GB is, dat wil zeggen, ofwel voordat de klant de opslag begint te gebruiken ofwel nadat de klant alle back-ups uit deze opslag heeft verwijderd. De informatie over het gebruik van opslagruimte wordt niet in real time bijgewerkt. Het kan tot 24 uur duren voordat de informatie wordt bijgewerkt.

   Zie 'Locaties en opslag beheren' voor meer informatie over opslag.
3. Als u de quota voor een optie wilt opgeven, klikt u op de link **Onbeperkt** naast de optie.
   Deze quota's zijn 'soft', dat wil zeggen dat ze niet strikt worden gehandhaafd. Als een van deze waarden wordt overschreden, ontvangen de tenantbeheerders en de beheerders van de bovenliggende tenant een e-mailmelding. Beperkingen met betrekking tot het gebruik van de services worden niet toegepast. Het gebruik van de optie voor een partnertenant kan naar verwachting de quota overschrijden, omdat de uitbreiding niet kan worden ingesteld bij het maken van een partnertenant.
4. [Alleen bij het maken van een klanttenant] Geef de quota-uitbreidingen op.
   Met een uitbreiding kan een klanttenant de quota overschrijden met de opgegeven waarde. Wanneer de uitbreiding wordt overschreden, worden er beperkingen toegepast voor het gebruik van de betreffende service.
5. Klik op **Opslaan en sluiten**.

De zojuist gemaakte tenant wordt weergegeven op het tabblad **Clients** van de beheerconsole.

Als u de tenantinstellingen wilt bewerken of de beheerder wilt wijzigen, selecteert u de tenant op het tabblad **Clients** en klikt u op het potloodpictogram in het gedeelte dat u wilt bewerken.

5.6.4 Contacten configureren ...

U kunt de informatie over de contacten van de tenants configureren. Een tenant kan meerdere contacten hebben.

Een contact configureren voor een tenant

1. Ga in de beheerconsole naar **Klanten**.
2. Klik op de tenant en klik op **Configureren**.
3. Klik in het gedeelte **Contacten** op **+**.
4. Geef de contactgegevens op.

Veld	Beschrijving
Voornaam	Voornaam van de contactpersoon. Dit is een verplicht veld.
Achternaam	Achternaam van de contactpersoon. Dit is een verplicht veld.
E-mail	E-mailadres van de contactpersoon. Dit is een verplicht veld.
Telefoon	Telefoonnummer van de contactpersoon. Dit is een verplicht veld.
Land	Land van verblijf van de contactpersoon. Dit veld is optioneel.
Plaats	Woonplaats van de contactpersoon. Dit veld is optioneel.
Adres	Adres van de contactpersoon. Dit veld is optioneel.
Postcode	Postcode op het adres van de contactpersoon. Dit veld is optioneel.

5. Selecteer het **contacttype**.
   - Facturering
   - Technisch
   - Juridisch
   - Management

   Opmerking
   U kunt meer dan één contacttype aan een contactpersoon toewijzen.

6. Klik op **Opslaan**.

5.7 Een tenant in- en uitschakelen

Mogelijk moet u een tenant tijdelijk uitschakelen. Bijvoorbeeld als uw tenant niet heeft betaald voor het gebruik van de services.

Een tenant uitschakelen

1. Ga in de beheerportal naar **Klanten**.
2. Selecteer de tenant die u wilt uitschakelen en klik vervolgens op de ellips > **Uitschakelen**.
3. Bevestig uw actie door te klikken op **Uitschakelen**.

Het resultaat:

- De tenant en alle bijbehorende sub-tenants worden dan uitgeschakeld en de betreffende services gestopt.
- De facturering van de tenant en bijbehorende sub-tenants wordt voortgezet, aangezien hun gegevens bewaard blijven en worden opgeslagen in Cyber Cloud.
- Alle API-clients binnen de tenant en de bijbehorende sub-tenants worden uitgeschakeld en alle integraties die gebruikmaken van deze clients, werken dan niet meer.

Als u een tenant wilt inschakelen, selecteert u deze in de lijst met klanten en klikt u vervolgens op de ellips > **Inschakelen**.

5.8 Een tenant verwijderen

Mogelijk wilt u een tenant definitief verwijderen om de gebruikte resources vrij te maken. De gebruiksstatistieken worden binnen een dag na verwijdering bijgewerkt. Voor grote tenants kan dit langer duren.

Voordat u een tenant verwijdert, moet u deze uitschakelen. Zie Een tenant uitschakelen en inschakelen voor meer informatie hierover.

Belangrijk
Een verwijderde tenant kan niet meer worden hersteld!

Een tenant verwijderen

1. Ga in de beheerportal naar **Klanten**.
2. Selecteer de uitgeschakelde tenant die u wilt verwijderen en klik vervolgens op het ellipspictogram > **Uitschakelen**.
3. Bevestig de actie door uw gebruikersnaam in te voeren en klik vervolgens op **Verwijderen**.

Het resultaat:

- De tenants en sub-tenants worden verwijderd.
- Alle services die zijn ingeschakeld binnen de tenant en bijbehorende sub-tenants, worden stopgezet.
- Alle gebruikers binnen de tenant en bijbehorende sub-tenants worden verwijderd.
- De registratie wordt ongedaan gemaakt voor alle machines in deze tenant en de bijbehorende sub-tenants.

- Alle servicegerelateerde gegevens, zoals back-ups en gesynchroniseerde bestanden, in de tenant en de bijbehorende sub-tenants worden verwijderd.
- Alle API-clients binnen de tenant en de bijbehorende sub-tenants worden verwijderd en alle integraties die gebruikmaken van deze clients, werken dan niet meer.

5.9 Een gebruikersaccount maken

In de volgende gevallen kan het handig zijn om aanvullende accounts te maken:

- Accounts voor partner/mapbeheerders: hiermee kunt u de taken voor het servicebeheer delen met andere mensen.
- Accounts voor klant/eenheidbeheerders: hiermee kunt u de service delegeren aan andere mensen van wie de toegangsrechten strikt zijn beperkt tot de betreffende klant/eenheid.
- Gebruikersaccounts binnen de klant- of eenheidtenant: hiermee kunt u instellen dat gebruikers alleen toegang hebben tot een subset van de services.

Let op: bestaande accounts kunnen niet worden verplaatst tussen tenants. U moet eerst een tenant maken en hierin vervolgens de accounts laden.

Een gebruikersaccount maken

1. Meld u aan bij de beheerportal.
2. Navigeer naar de tenant waarvoor u een gebruikersaccount wilt maken.
3. Klik in de rechterbovenhoek op **Nieuw** > **Gebruiker**.
4. Geef de volgende contactgegevens op voor het account:
   - **Gebruikersnaam**

     Belangrijk
     Elk account moet een unieke gebruikersnaam hebben.

   - **E-mail**
   - [Optioneel]**Voornaam**
   - [Optioneel] **Achternaam**
   - Selecteer bij **Taal** de standaardtaal voor meldingen, rapporten en de software die wordt gebruikt voor dit account.
5. [Niet beschikbaar wanneer u een account maakt in een partner/maptenant] Selecteer de services waartoe de gebruiker toegang heeft en de rollen in iedere service.

   Welke services beschikbaar zijn, hangt af van de services die zijn ingeschakeld voor de tenant waarin het gebruikersaccount is gemaakt.
   - Als u het selectievakje **Bedrijfbeheerder** inschakelt, heeft de gebruiker toegang tot de beheerportal en de beheerdersrol in alle services die op dat moment zijn ingeschakeld voor de tenant. De gebruiker heeft ook toegang tot de beheerdersrol in alle services die later worden ingeschakeld voor de tenant.

- Als u het selectievakje **Eenheidbeheerder** inschakelt, heeft de gebruiker toegang tot de beheerportal, maar mogelijk niet tot de beheerdersrol voor de service. Dit hangt af van de service.
- Anders heeft de gebruiker de rollen die u selecteert in de geselecteerde services.

6. Klik op **Maken**.

Het zojuist gemaakte gebruikersaccount wordt weergegeven op het tabblad **Gebruikers**.

Als u de gebruikersinstellingen wilt bewerken of de instellingen voor meldingen en quota's (niet beschikbaar voor partner-/mapbeheerders) voor de gebruiker wilt opgeven, selecteert u de gebruiker op het tabblad **Gebruikers** en klikt u op het potloodpictogram in het gedeelte dat u wilt bewerken.

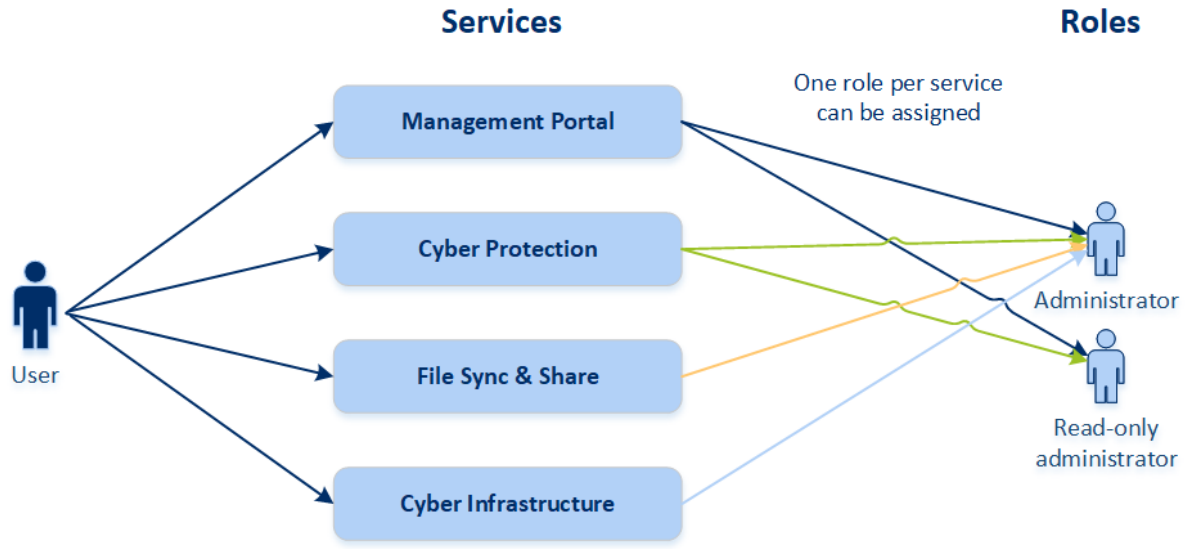
Het wachtwoord van een gebruiker opnieuw instellen

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer de gebruiker van wie u het wachtwoord opnieuw wilt instellen en klik vervolgens op het ellipspictogram > **Wachtwoord opnieuw instellen**.
3. Bevestig uw actie door te klikken op **Opnieuw instellen**.

De gebruiker kan het proces voor opnieuw instellen nu voltooien door de instructies in de ontvangen e-mail te volgen.

5.10 Gebruikersrollen beschikbaar voor elke service

Een gebruiker kan meerdere rollen hebben, maar slechts één rol per service.



Voor elke service kunt u definiëren welke rol aan een gebruiker wordt toegewezen.

Service	Rol	Beschrijving

N.v.t.	Bedrijfbeheerder	Met deze rol worden ook beheerdersrechten voor alle services verleend. Deze rol geeft toegang tot de witte lijst van het bedrijf. Als de Disaster Recovery-add-on van de Cyber Protection-service is ingeschakeld voor het bedrijf, biedt deze rol ook toegang tot de functionaliteit voor noodherstel.
Beheerportal	Beheerder	Met deze rol wordt toegang verkregen tot de beheerportal waar de beheerder gebruikers binnen de hele organisatie kan beheren.
	Alleen-lezen beheerder	De rol biedt alleen-lezen toegang tot alle objecten in de beheerportal. Dergelijke gebruikers hebben alleen-lezen toegang tot gegevens van andere gebruikers binnen de organisatie.
Cyber Protection	Beheerder	Met deze rol kunt u Cyber Protection configureren en beheren voor uw klanten. Deze rol is vereist voor het configureren en beheren van de functionaliteit voor noodherstel en de witte lijst van het bedrijf.
	Alleen-lezen beheerder	De rol biedt alleen-lezen toegang tot alle objecten van de Cyber Protection-service. Dergelijke gebruikers hebben alleen-lezen toegang tot gegevens van andere gebruikers binnen de organisatie. De alleen-lezen beheerder kan de functionaliteit voor noodherstel of de witte lijst van het bedrijf niet configureren en beheren.
	Operator herstellen	De rol biedt toegang tot back-ups van Microsoft 365- en Google Workspace-organisaties en maakt herstel mogelijk, terwijl de toegang tot gevoelige inhoud wordt beperkt.
File Sync & Share	Beheerder	Met deze rol kunt u File Sync & Share configureren en beheren voor uw gebruikers.
Cyber Infrastructure	Beheerder	Met deze rol kunt u Cyber Infrastructure configureren en beheren voor uw gebruikers.

5.10.1 Rol van alleen-lezen beheerder

Een account met deze rol biedt alleen-lezen toegang tot de Cyberbescherming-webconsole en kan:

- Diagnostische gegevens verzamelen, zoals systeemrapporten.
- De herstelpunten van een back-up zien, maar niet de gedetailleerde inhoud van back-ups en geen bestanden, mappen of e-mails zien.

Een alleen-lezen beheerder kan niet:

- Taken starten of stoppen.

  Een alleen-lezen-beheerder kan bijvoorbeeld geen herstelbewerking starten en geen actieve back-up stoppen.

- Het bestandssysteem openen op bron- of doelmachines.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen bestanden, mappen of e-mails zien op een machine waarvan een back-up is gemaakt.
- De instellingen wijzigen.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen beschermingsschema maken of de instellingen ervan wijzigen.
- Gegevens maken, bijwerken of verwijderen.
  Een alleen-lezen-beheerder kan bijvoorbeeld geen back-ups verwijderen.

Alle UI-objecten die niet toegankelijk zijn voor een alleen-lezen beheerder, worden verborgen, met uitzondering van de standaardinstellingen van het beschermingsschema. Deze instellingen worden weergegeven, maar de knop **Opslaan** is niet actief.

Eventuele wijzigingen van de accounts en rollen worden weergegeven op het tabblad **Activiteiten**, inclusief de volgende details:

- Nieuwe wijzigingen
- Wie de wijzigingen heeft gemaakt
- Datum en tijd van de wijzigingen

5.10.2 Operator-rol herstellen

Deze rol is alleen beschikbaar in de Cyber Protection-service en is beperkt tot Microsoft 365- en Google Workspace-back-ups.

Een hersteloperator kan het volgende doen:

- Waarschuwingen en activiteiten bekijken.
- Door de lijst met back-ups bladeren en deze vernieuwen.
- Door back-ups bladeren zonder toegang tot de inhoud. De hersteloperator kan de namen van de back-upbestanden en de onderwerpen en afzenders van e-mails in de back-up zien.
- Zoeken in back-ups (zoeken in volledige tekst wordt niet ondersteund).
- Cloud-to-cloud back-ups herstellen binnen de oorspronkelijke Microsoft 365- of Google Workspace-organisatie.

Een hersteloperator kan niet het volgende doen:

- Waarschuwingen verwijderen.
- Microsoft 365- of Google Workspace-organisaties toevoegen of verwijderen.
- Back-uplocaties toevoegen of verwijderen of de naam ervan wijzigen.
- Back-ups verwijderen of de naam ervan wijzigen.
- Mappen maken, verwijderen of de naam ervan wijzigen tijdens het herstellen van een back-up naar een aangepaste locatie.
- Een back-upschema toepassen of een back-up uitvoeren.

- Back-upbestanden of de inhoud van e-mails in de back-up openen.
- Back-upbestanden of e-mailbijlagen downloaden.
- Cloudresources waarvan een back-up is gemaakt, zoals e-mails of agenda-items, verzenden als e-mail.
- Microsoft 365 Teams-gesprekken bekijken of herstellen.

5.11 De instellingen voor de meldingen voor een gebruiker wijzigen ...

Als u de instellingen voor de meldingen voor een gebruiker wilt wijzigen, selecteert u de gebruiker op het tabblad **Gebruikers** en klikt u op het potloodpictogram in het gedeelte **Instellingen**. De volgende meldingsinstellingen zijn beschikbaar als de Cyber Protection-service is ingeschakeld voor de tenant waar de gebruiker is gemaakt:

- **Meldingen over quotumoverschrijdingen** (standaard ingeschakeld)
  Meldingen over quotaoverschrijdingen.
- **Geplande gebruiksrapporten** (standaard ingeschakeld)
  Gebruiksrapporten die op de eerste dag van elke maand worden verzonden.
- **Foutmeldingen**, **waarschuwingsmeldingen** en **gereedmeldingen** (standaard uitgeschakeld)
  Meldingen over de uitvoeringsresultaten van beschermingsschema's en de resultaten van noodherstelbewerkingen voor elk apparaat.
- **Dagelijkse samenvatting over actieve waarschuwingen** (standaard ingeschakeld)
  De dagelijkse samenvatting wordt gegenereerd op basis van de lijst met actieve waarschuwingen die aanwezig zijn in de serviceconsole op het moment dat de samenvatting wordt gegenereerd. De samenvatting wordt één keer per dag gegenereerd en verzonden tussen 10:00 en 23:59 uur UTC. Het tijdstip waarop het rapport wordt gegenereerd en verzonden, is afhankelijk van de workload in het datacentrum. Als er op dat moment geen actieve waarschuwingen zijn, wordt de samenvatting niet verzonden. De samenvatting bevat geen informatie over eerdere waarschuwingen die niet meer actief zijn. Als een gebruiker bijvoorbeeld een mislukte back-up vindt en de waarschuwing wist, of als de back-up opnieuw met succes wordt geprobeerd voordat de samenvatting wordt gegenereerd, dan is de waarschuwing niet meer aanwezig en wordt deze niet opgenomen in de samenvatting.
- **Meldingen van apparaatbeheer** (standaard uitgeschakeld)
  Meldingen over pogingen om randapparatuur en poorten te gebruiken die zijn beperkt door beschermingsschema's (alleen wanneer de apparaatbeheermodule is ingeschakeld).
- **Herstelmeldingen** (standaard uitgeschakeld)
  Meldingen over herstelacties voor de volgende resources: e-mailberichten van gebruikers en volledige mailbox, openbare mappen, OneDrive/GoogleDrive: volledige OneDrive en bestanden of mappen, SharePoint-bestanden, Teams: kanalen, hele team, e-mailberichten, en teamsite.
  In het kader van deze meldingen worden de volgende acties als herstelacties beschouwd: verzenden als e-mail, downloaden, of een herstelbewerking starten.

Alle meldingen worden verzonden naar het e-mailadres van de gebruiker.

5.11.1 Meldingen ontvangen door gebruikersrol

Welke meldingen worden verzonden door Cyber Protection hangt af van de gebruikersrol.

Type melding\Gebruikersrol	Gebruiker	Klant- en eenheidbeheerders	Partner- en mapbeheerder
Meldingen voor eigen apparaten	Ja	Ja	n.v.t.*
Meldingen voor alle apparaten van de onderliggende tenants	N.v.t.	Ja	Ja
Meldingen voor Microsoft 365, Google Workspace en andere back-ups in de cloud	N.v.t.	Ja	Ja

* Partnerbeheerders kunnen geen eigen apparaten registreren, maar ze kunnen hun eigen klantbeheerderaccounts maken en die accounts gebruiken om eigen apparaten toe te voegen. Zie Gebruikersaccounts en tenants.

5.12 Een gebruikersaccount uitschakelen en inschakelen

Mogelijk moet u een gebruikersaccount uitschakelen om de toegang tot het cloudplatform tijdelijk te beperken.

Een gebruikersaccount uitschakelen

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer het gebruikersaccount dat u wilt uitschakelen en klik vervolgens op het ellipspictogram > **Uitschakelen**.
3. Bevestig uw actie door te klikken op **Uitschakelen**.

Deze gebruiker kan het cloudplatform dan niet gebruiken en geen meldingen ontvangen.

Als u een uitgeschakeld gebruikersaccount wilt inschakelen, selecteert u het account in de gebruikerslijst en klikt u vervolgens op het ellipspictogram > **Inschakelen**.

5.13 Een gebruikersaccount verwijderen

Mogelijk moet u een gebruikersaccount definitief verwijderen om de gebruikte resources vrij te maken, bijvoorbeeld opslagruimte of een licentie. De gebruiksstatistieken worden binnen een dag na verwijdering bijgewerkt. Voor accounts met veel gegevens kan dit langer duren.

Voordat u een gebruikersaccount verwijdert, moet u dit uitschakelen. Zie Een gebruikersaccount uitschakelen en inschakelen voor meer informatie hierover.

Belangrijk
Een verwijderd gebruikersaccount kan niet meer worden hersteld!

Een gebruikersaccount verwijderen

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer het uitgeschakelde gebruikersaccount en klik vervolgens op het ellipspictogram > **Verwijderen**.
3. Bevestig de actie door uw gebruikersnaam in te voeren en klik vervolgens op **Verwijderen**.

Het resultaat:

- Dit gebruikersaccount wordt verwijderd.
- Alle gegevens die bij dit gebruikersaccount horen, worden verwijderd.
- De registratie wordt ongedaan gemaakt voor alle machines die aan dit gebruikersaccount zijn gekoppeld.

5.14 Eigendom van een gebruikersaccount overdragen

Mogelijk moet u het eigendom van een gebruikersaccount overdragen als u toegang wilt behouden tot de gegevens van een beperkte gebruiker.

Belangrijk
U kunt de inhoud van een verwijderd account niet opnieuw toewijzen.

Het eigendom van een gebruikersaccount overdragen:

1. Ga in de beheerportal naar **Gebruikers**.
2. Selecteer het gebruikersaccount waarvan u het eigendom wilt overdragen en klik vervolgens op het potloodpictogram in het gedeelte **Algemene informatie**.
3. Vervang het bestaande e-mailadres door het e-mailadres van de toekomstige accounteigenaar en klik vervolgens op **Gereed**.
4. Bevestig uw actie door te klikken op **Ja**.
5. Laat de toekomstige accounteigenaar het e-mailadres verifiëren door de instructies te volgen die naar dat adres zijn gestuurd.
6. Selecteer het gebruikersaccount waarvan u het eigendom overdraagt en klik vervolgens op het ellipspictogram > **Wachtwoord opnieuw instellen**.
7. Bevestig uw actie door te klikken op **Opnieuw instellen**.

8. Laat de toekomstige accounteigenaar het wachtwoord opnieuw instellen door de instructies te volgen die naar het betreffende e-mailadres zijn gestuurd.

De nieuwe eigenaar heeft nu toegang tot dit account.

5.15 Tweeledige verificatie instellen

Tweeledige verificatie (2FA) is een vorm van meervoudige verificatie waarmee een gebruikersidentiteit wordt gecontroleerd door een combinatie van twee verschillende factoren:

- Iets wat een gebruiker weet (pincode of wachtwoord)
- Iets wat een gebruiker heeft (token)
- Iets wat een gebruiker is (biometrie)

Tweeledige verificatie biedt extra beveiliging tegen ongeautoriseerde toegang tot uw account.

Het platform ondersteunt **Time-Based One-Time Password (TOTP)**-verificatie. Als de TOTP-verificatie in het systeem is ingeschakeld, moeten gebruikers hun traditionele wachtwoord en de eenmalige TOTP-code invoeren om toegang te krijgen tot het systeem. Met andere woorden: een gebruiker geeft het wachtwoord én de TOTP-code op (deze twee samen vormen de twee factoren van tweeledige verificatie). De TOTP-code wordt gegenereerd in de verificatietoepassing op een apparaat ('tweede-factor-apparaat') van de gebruiker op basis van de huidige tijd en het geheim (QR-code of alfanumerieke code) van het platform.

5.15.1 Zo werkt het

1. U kunt tweeledige verificatie inschakelen op het niveau van de organisatie.
2. Alle gebruikers van uw organisatie moeten een verificatietoepassing installeren op hun 'tweede-factor-apparaat' (mobiele telefoon, laptop, desktop of tablet). Deze toepassing wordt gebruikt voor het genereren van eenmalige TOTP-codes. De aanbevolen verificatietoepassingen:
   - Google Authenticator
     iOS-appversie (https://apps.apple.com/app/google-authenticator/id388497605)
     Android-versie (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     iOS-appversie (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Android-versie (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Belangrijk
   De tijd op het gebruikersapparaat waarop de verificatietoepassing is geïnstalleerd, moet correct zijn ingesteld en de huidige tijd weergeven.
3. De gebruikers van uw organisatie moeten zich opnieuw aanmelden bij het systeem.

4. Wanneer ze hun gebruikersnaam en wachtwoord hebben ingevoerd, wordt ze gevraagd om tweeledige verificatie in te stellen voor hun gebruikersaccount.
5. Ze moeten de QR-code scannen met hun verificatietoepassing. Als de QR-code niet kan worden gescand, kunnen ze het TOTP-geheim onder de QR-code gebruiken en dit handmatig toevoegen in de verificatietoepassing.

   Belangrijk
   We raden u met klem aan om de code en het geheim op te slaan (print de QR-code, schrijf het TOTP-geheim op of gebruik de toepassing waarmee een back-up van codes kan worden gemaakt in de cloud). U hebt het TOTP-geheim nodig om tweeledige verificatie opnieuw in te stellen voor het geval u uw 'tweede-factor-apparaat' kwijtraakt.

6. De eenmalige TOTP-code wordt gegenereerd in de verificatietoepassing. De code wordt om de 30 seconden automatisch opnieuw gegenereerd.
7. Wanneer gebruikers hun wachtwoord hebben ingevoerd, moeten ze vervolgens de TOTP-code invoeren op het scherm 'Tweeledige verificatie instellen'.
8. Hierdoor wordt tweeledige verificatie voor de gebruikers ingesteld.

Wanneer gebruikers zich dan aanmelden bij het systeem, wordt ze gevraagd om de gebruikersnaam en het wachtwoord in te voeren, plus de eenmalige TOTP-code die wordt gegenereerd in de verificatietoepassing. Als gebruikers de browser als vertrouwd markeren wanneer ze zich aanmelden bij het systeem, wordt niet meer om de TOTP-code gevraagd bij de volgende aanmelding via deze browser.

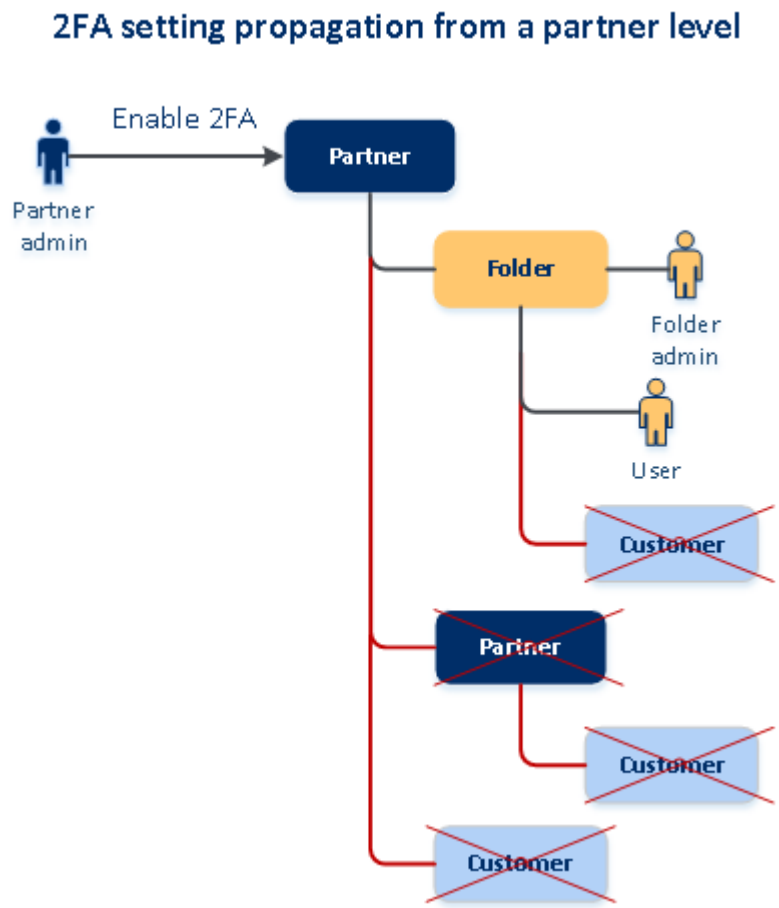
5.15.2 Tweeledige verificatie doorvoeren bij de tenants

Tweeledige verificatie wordt ingesteld op **organisatieniveau**. U kunt tweeledige verificatie in- of uitschakelen:

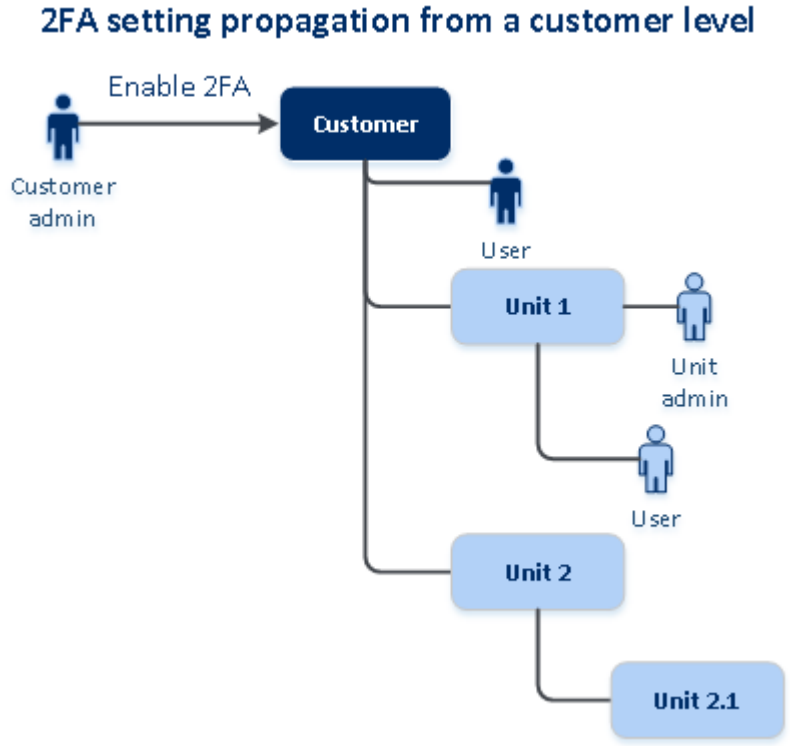
- Voor uw eigen organisatie.
- Voor uw onderliggende tenant (alleen als de optie **Toegang tot ondersteuning** is ingeschakeld in die onderliggende tenant).

De instellingen voor tweeledige verificatie worden als volgt doorgevoerd op tenantniveau:

- Voor mappen worden automatisch de instellingen voor tweeledige verificatie van de betreffende partnerorganisatie overgenomen. De rode lijnen in het onderstaande schema geven aan dat het niet mogelijk is om de instellingen voor tweeledige verificatie door te voeren.



- Voor eenheden worden automatisch de instellingen voor tweeledige verificatie van de betreffende klantorganisatie overgenomen.



Opmerking

1. U kunt tweeledige verificatie voor uw onderliggende organisaties alleen in- of uitschakelen als de optie **Toegang tot ondersteuning** is ingeschakeld in die onderliggende organisatie.
2. U kunt de instellingen voor tweeledige verificatie voor gebruikers van de onderliggende organisaties alleen beheren als de optie **Toegang tot ondersteuning** is ingeschakeld in die onderliggende organisatie.
3. Het is niet mogelijk om tweeledige verificatie in te stellen op het niveau van mappen of eenheden.
4. U kunt de instelling voor tweeledige verificatie configureren, zelfs als deze instelling niet is ingeschakeld voor uw bovenliggende organisatie.

5.15.3 Tweeledige verificatie instellen voor uw tenant

Tweeledige verificatie inschakelen voor uw tenant

1. Ga in de beheerportal naar **Instellingen** > **Beveiliging**.
2. Schakel de schuifregelaar in om tweeledige verificatie in te schakelen. Klik op **Inschakelen** om te bevestigen.

Op de voortgangsbalk ziet u hoeveel gebruikers tweeledige verificatie hebben ingesteld voor hun accounts. Tweeledige verificatie is dan ingeschakeld voor uw organisatie. Alle gebruikers van de organisatie moeten dan tweeledige verificatie instellen voor hun accounts. Daarna wordt aan de gebruikers gevraagd om hun gebruikersnaam en wachtwoord én de TOTP-code in te voeren om zich aan te melden bij het systeem.

Op het tabblad **Gebruikers** wordt de kolom **Status van tweeledige verificatie** weergegeven. U kunt volgen welke gebruikers tweeledige verificatie hebben ingesteld voor hun accounts.

Tweeledige verificatie uitschakelen voor uw tenant

1. Ga in de beheerportal naar **Instellingen** > **Beveiliging**.
2. Schakel de schuifregelaar uit om tweeledige verificatie uit te schakelen. Klik op **Uitschakelen** om te bevestigen.
3. [Als ten minste één gebruiker in de organisatie tweeledige verificatie heeft geconfigureerd] Voer de TOTP-code in die is gegenereerd in uw verificatietoepassing op het mobiele apparaat.

Tweeledige verificatie wordt dan uitgeschakeld voor uw organisatie, alle geheimen worden verwijderd en alle vertrouwde browsers worden uit het geheugen gewist. Alle gebruikers kunnen zich dan bij het systeem aanmelden met alleen hun gebruikersnaam en wachtwoord. Op het tabblad **Gebruikers** wordt de kolom **Status van tweeledige verificatie** verborgen.

5.15.4 Configuratie voor tweeledige verificatie beheren voor gebruikers

U kunt de instellingen voor tweeledige verificatie voor al uw gebruikers controleren en opnieuw configureren op het tabblad **Gebruikers** in de beheerportal.

Controle

In de beheerportal, op het tabblad **Gebruikers**, ziet u een lijst met alle gebruikers binnen uw organisatie. Bij **Status van tweeledige verificatie** ziet u of tweeledige verificatie is ingesteld voor een gebruiker.

Tweeledige verificatie opnieuw instellen voor een gebruiker

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Tweeledige verificatie opnieuw instellen**.
3. Voer de TOTP-code in die is gegenereerd in uw verificatietoepassing op uw 'tweede-factor-apparaat' en klik op **Opnieuw instellen**.

De gebruiker kan tweeledige verificatie dan opnieuw instellen.

De vertrouwde browser opnieuw instellen voor een gebruiker

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Alle vertrouwde browsers opnieuw instellen**.
3. Voer de TOTP-code in die is gegenereerd in de verificatietoepassing op uw 'tweede-factor-apparaat' en klik op **Opnieuw instellen**.

Gebruikers voor wie u alle vertrouwde browsers opnieuw hebt ingesteld, moeten de TOTP-code opgeven wanneer ze zich opnieuw aanmelden.

Gebruikers kunnen zelf alle vertrouwde browsers en de instellingen voor tweeledige verificatie opnieuw configureren. Wanneer ze zich aanmelden bij het systeem, kunnen ze op de betreffende link klikken en de TOTP-code invoeren om de bewerking te bevestigen.

Tweeledige verificatie uitschakelen voor een gebruiker

Het kan nodig zijn om tweeledige verificatie uit te schakelen voor een gebruiker, terwijl de andere gebruikers van het account tweeledige verificatie blijven gebruiken. Dit is het geval als deze gebruiker wordt gebruikt om toegang te krijgen tot de API.

Belangrijk
Zet normale gebruikers niet om naar servicegebruikers om tweeledige verificatie uit te schakelen, want anders kunnen de gebruikers zich mogelijk niet aanmelden.

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Markeren als serviceaccount**. De gebruiker krijgt dan een speciale status voor tweeledige verificatie, genaamd **Serviceaccount.**
3. [Als ten minste één gebruiker binnen een tenant tweeledige verificatie heeft geconfigureerd] Bevestig het uitschakelen door de TOTP-code in te voeren die is gegenereerd in de verificatietoepassing op uw 'tweede-factor-apparaat'.

Tweeledige verificatie inschakelen voor een gebruiker

Mogelijk moet u tweeledige verificatie inschakelen voor een bepaalde gebruiker voor wie u tweeledige verificatie eerder hebt uitgeschakeld.

1. Als u de instellingen voor een gebruiker wilt wijzigen, gaat u in de beheerportal naar het tabblad **Gebruikers** en vervolgens selecteert u de gebruiker en klikt u op de ellips.
2. Klik op **Markeren als gewoon account**. De gebruiker moet tweeledige verificatie dan opnieuw instellen of de TOTP-code invoeren voor toegang tot het systeem.

5.15.5 Tweeledige verificatie opnieuw instellen voor het geval u uw 'tweede-factor-apparaat' kwijtraakt

Als u uw 'tweede-factor-apparaat' bent kwijtgeraakt en u de toegang tot uw account opnieuw wilt instellen, volgt u een van de aangegeven methoden:

- Herstel uw TOTP-geheim (QR-code of alfanumerieke code) vanuit een back-up.
  Gebruik een ander 'tweede-factor-apparaat' en voeg het opgeslagen TOTP-geheim toe aan de verificatietoepassing die op dit apparaat is geïnstalleerd.
- Vraag uw beheerder om de instellingen voor tweeledige verificatie opnieuw te configureren voor u.

5.15.6 Bescherming tegen beveiligingsaanvallen

Een beveiligingsaanval is een aanval waarbij een indringer probeert toegang te krijgen tot het systeem door veel wachtwoorden in te voeren, in de hoop bij toeval het juiste wachtwoord te vinden.

Voor de bescherming van het platform tegen beveiligingsaanvallen wordt gebruikgemaakt van apparaatcookies.

De instellingen voor de bescherming tegen beveiligingsaanvallen die op het platform worden gebruikt, zijn vooraf gedefinieerd:

Parameter	Wachtwoord invoeren	TOTP-code invoeren
Maximaal aantal pogingen	10	5
Maximale periode voor de pogingen (deze limiet wordt opnieuw ingesteld na een time-out)	15 min (900 sec)	15 min (900 sec)
Vergrendeling vindt plaats na	Maximaal aantal pogingen +1 (11e poging)	Maximaal aantal pogingen
Vergrendelingsperiode	5 min (300 sec)	5 min (300 sec)

Als u tweeledige verificatie hebt ingeschakeld, krijgt een client(browser) alleen een apparaatcookie nadat verificatie met beide factoren (wachtwoord en TOTP-code) is uitgevoerd.

Voor vertrouwde browsers volstaat een verificatie met slechts één factor (wachtwoord) om de appraatcookie te krijgen.

Het aantal pogingen om de TOTP-code in te voeren wordt geregistreerd per gebruiker, niet per apparaat. Dus gebruikers worden geblokkeerd, zelfs als ze proberen de TOTP-code in te voeren via verschillende apparaten.

5.16 Upsell-scenario's voor uw klanten configureren

Upselling is een techniek om uw klanten ertoe aan te zetten extra functies te kopen.

Cyber Protection heeft meerdere verouderde edities, die allemaal verschillen in functionaliteit en prijs. Mogelijk wilt u duurdere edities met meer geavanceerde mogelijkheden promoten bij uw bestaande klanten die standaardedities gebruiken.

U kunt de upsell-mogelijkheid per klant in- of uitschakelen. De upsell-optie is standaard uitgeschakeld. Als u upsell inschakelt voor een klant, ziet deze aanvullende functionaliteit die pas beschikbaar is als de klant de gepromote editie koopt. Deze extra functionaliteit is gemarkeerd met labels die de naam of pictogrammen van de gepromote editie weergeven, alles gemarkeerd in het oranje. Deze upsell-punten worden weergegeven voor een klant om deze te motiveren een duurdere versie te kopen. Wanneer een klant op deze upsell-punten klikt, ziet deze een dialoogvenster waarin wordt voorgesteld een duurdere editie te kopen om de gewenste functionaliteit in te schakelen.

Het actie-item hangt af van het type klantgebruiker. Het type gebruikers (koper of geen koper) kan worden geconfigureerd via de platform-API. Zie de API-documentatie voor meer informatie. Raadpleeg de onderstaande tabel voor meer informatie over actie-items die worden weergegeven voor uw klanten:

Type gebruikers in klanttenant	Actie-item
Beheerder; koper	De knop **Nu kopen** wordt weergegeven in de gebruikersinterface.*

Beheerder; geen koper	Het bericht 'Neem contact op met uw partner om de editie te upgraden' wordt weergegeven in de gebruikersinterface.
Gebruiker; koper	Het bericht 'Neem contact op met uw partner om de editie te upgraden' wordt weergegeven in de gebruikersinterface.
Gebruiker; geen koper	Het bericht 'Neem contact op met uw partner om de editie te upgraden' wordt weergegeven in de gebruikersinterface.

* Met de knop **Nu kopen** wordt een klant omgeleid naar een website waar een meer geavanceerde versie kan worden gekocht. De link naar de knop kan worden geconfigureerd in **Instellingen** > **Branding**. In het gedeelte **Upsell** kunt u **URL voor kopen** opgeven. De brandingopties worden toegepast op de tenant waarvoor branding is geconfigureerd, en alle directe en indirecte onderliggende partners/mappen en klanten.

De upsell-mogelijkheid voor een klant in- of uitschakelen

1. Ga in de beheerportal naar **Klanten**.
2. Selecteer de klant, ga naar het linkerdeelvenster en ga vervolgens naar het tabblad **Configureren**.
3. In de sectie **Upsell** doet u het volgende:
   - Schakel **Meer geavanceerde edities promoten** in om het upsell-scenario voor klanten in te schakelen.
   - Schakel **Meer geavanceerde edities promoten** uit om het upsell-scenario voor klanten uit te schakelen.

5.16.1 Upsell-punten weergegeven voor een klant

Lijst met beveiligingsprobleem

De lijst met beveiligingsproblemen vindt u in de serviceconsole onder **Softwarebeheer** > **Beveiligingsproblemen**. Wanneer een gebruiker op het verticale ellipspictogram klikt, wordt het dialoogvenster voor promotie van de editie geopend en wordt de gebruiker gevraagd om de duurdere editie te kopen.

Een beschermingsschema maken of bewerken

Ga in de serviceconsole naar **Schema's** > **Bescherming**. Klik op **Schema maken**. In de Cyber Backup-edities zijn alleen de modules **Back-up** en **Beveiligingsproblemen** ingeschakeld. Alle andere modules zijn alleen beschikbaar in de Cyber Protect-edities. Uw klant kan alle modules inschakelen na aanschaf van een van de Cyber Protect-edities.

Wizard Automatische detectie

Deze wizard is te vinden in de serviceconsole onder **Apparaten** > **Alle apparaten**. Uw klant kan de wizard Automatische detectie starten met de volgende procedure: klik op **Toevoegen**, ga naar het

gedeelte **Meerdere apparaten** en klik vervolgens op **Alleen Windows**. De methoden voor automatische detectie van machines zijn alleen beschikbaar in de Advanced-edities.

Acties in de lijst met apparaten

Deze lijst is te vinden in de serviceconsole onder **Apparaten** > **Alle apparaten**. Uw klant moet de machine selecteren en vervolgens worden twee extra opties weergegeven in het linkerdeelvenster:

- **Verbinding maken via HTML5-client**
- **Patch**

Deze opties zijn alleen beschikbaar als een klant een duurdere editie koopt dan de bestaande.

5.17 Locaties en opslag beheren

In het gedeelte **Instellingen** > **Locaties** worden de cloudopslagruimten en infrastructuren voor noodherstel weergegeven die u kunt gebruiken om de service **Cyber Protection** en de service **File Sync & Share** te leveren aan uw partners en klanten.

In toekomstige releases worden in het gedeelte **Locaties** ook opslagruimten weergegeven die zijn geconfigureerd voor andere services.

5.17.1 Locaties

Een locatie is een container waarmee u gemakkelijk de cloudopslagruimten en infrastructuren voor noodherstel kunt groeperen. U kunt zelf bepalen wat u gebruikt als container, bijvoorbeeld een specifiek datacentrum of een geografische locatie van uw infrastructuurcomponenten.

U kunt een willekeurig aantal locaties maken en deze vullen met opslagruimten voor back-ups, opslagruimten voor **File Sync & Share** en infrastructuren voor noodherstel. Een locatie kan meerdere cloudopslagruimten bevatten, maar slechts één infrastructuur voor noodherstel.

Ga voor meer informatie over bewerkingen met opslag naar 'Opslag beheren'.

Locaties en opslagruimten voor partners en klanten kiezen

Wanneer u een partner-/maptenant maakt, kunt u meerdere locaties en hierin meerdere opslagruimten per service selecteren die in de nieuwe tenant beschikbaar zijn.

Wanneer u een klanttenant maakt, moet u één locatie selecteren en vervolgens één opslagruimte per service binnen die locatie selecteren. De opslagruimten die aan de klant zijn toegewezen, kunnen later worden gewijzigd, maar alleen als hun gebruik 0 GB is, dat wil zeggen, ofwel voordat de klant de opslag begint te gebruiken ofwel nadat de klant alle back-ups uit deze opslag heeft verwijderd.

De informatie over de opslagruimten die zijn toegewezen aan een klanttenant, wordt weergegeven in het deelvenster voor tenantgegevens wanneer u de tenant selecteert op het tabblad **Clients**. De

informatie over het gebruik van opslagruimte wordt niet in real time bijgewerkt. Het kan tot 24 uur duren voordat de informatie wordt bijgewerkt.

Bewerkingen met locaties

Als u een nieuwe locatie wilt maken, klikt u op **Locatie toevoegen** en geeft u vervolgens een nieuwe naam op voor de locatie.

Als u een opslagruimte of infrastructuur voor noodherstel naar een andere locatie wilt verplaatsen, selecteert u de opslagruimte of de infrastructuur, klikt u op het potloodpictogram in het veld **Locatie** en selecteert u de doellocatie.

Als u de naam van een locatie wilt wijzigen, klikt u op het ellipspictogram naast de naam van de locatie, klikt u op **Naam wijzigen** en geeft u vervolgens de nieuwe naam van de locatie op.

Als u een locatie wilt verwijderen, klikt u op het ellipspictogram naast de naam van de locatie, klikt u op **Verwijderen** en bevestigt u dat u deze wilt verwijderen. Alleen lege locaties kunnen worden verwijderd.

5.17.2 Opslag beheren

Nieuwe opslagruimten toevoegen

- **Cyber Protection** service:
  - De opslaglocaties voor back-ups bevinden zich standaard in datacentrums van .
  - Als de optie **Back-upopslag in eigendom van partner** door een hogere beheerder is ingeschakeld voor een partnertenant, kunnen de partnerbeheerders de Cyber Infrastructure-software gebruiken om de opslag te organiseren in het eigen datacentrum van de partner. Klik in het gedeelte **Locaties** op **Back-upopslag toevoegen** voor meer informatie over het organiseren van een back-upopslag in uw eigen datacentrum.
  - Als de optie **Infrastructuur voor noodherstel in eigendom van partner** door een hogere beheerder is ingeschakeld voor een partnertenant, kunnen de partnerbeheerders een infrastructuur voor noodherstel organiseren in het eigen datacentrum van de partner. Neem contact op met de technische ondersteuning voor informatie over het toevoegen van een infrastructuur voor noodherstel.

Opmerking
Back-upvalidatie is niet mogelijk met objectopslagplaatsen in de publieke cloud, zoals Amazon S3, Microsoft Azure, Google Cloud Storage en Wasabi, die worden gebruikt door de -datacentrums.
Back-upvalidatie is mogelijk met objectopslagplaatsen in de publieke cloud die worden gebruikt door -partners. Het is echter niet aan te bevelen om deze optie in te schakelen, want de validatiebewerkingen kunnen leiden tot meer uitgaand verkeer vanaf deze publieke objectopslagplaatsen en tot aanzienlijk hogere kosten.

- Neem contact op met de technische ondersteuning voor informatie over het toevoegen van opslagruimten die door andere services moeten worden gebruikt.

Opslagruimten verwijderen

U kunt opslagruimten verwijderen die door u of uw onderliggende tenants zijn toegevoegd.

Als de opslag wordt toegewezen aan klanttenants, moet u eerst de service uitschakelen die de opslag gebruikt voor alle klanttenants, en vervolgens de opslag verwijderen.

Een opslagruimte verwijderen

1. Meld u aan bij de beheerportal.
2. Navigeer naar de tenant waaraan de opslag is toegevoegd.
3. Klik op **Instellingen** > **Locaties**.
4. Selecteer de opslag die u wilt verwijderen.
5. Klik in het deelvenster voor opslageigenschappen op het ellipsvormige pictogram en klik vervolgens op **Opslag verwijderen**.
6. Bevestig uw beslissing.

5.18 Branding configureren

In het gedeelte **Instellingen** > **Branding** kunnen partnerbeheerders de gebruikersinterface van de beheerportal en de **Cyber Protection**-service aanpassen om koppelingen naar partners op hoger niveau te verwijderen.

Branding kan worden geconfigureerd op het niveau van de partner en de map. Branding wordt toegepast op de tenant waarvoor branding is geconfigureerd, en alle directe en indirecte onderliggende partners/mappen en klanten.

De mogelijkheid om branding te configureren voor alle services zal worden geïntegreerd in toekomstige releases. Sommige services bieden afzonderlijke functionaliteit voor branding. Raadpleeg de gebruikershandleidingen in de serviceconsoles voor meer informatie.

5.18.1 Branding-items

Uiterlijk

- **Servicenaam**. Deze naam wordt gebruikt in alle e-mailberichten die worden verzonden vanuit de beheerportal en cloudservices (berichten over accountactivering, e-mailberichten met servicemeldingen), op het **Welkomstscherm** na de eerste aanmelding, en als de naam van het browsertabblad van de beheerportal.
- **Logo**. Het logo wordt weergegeven in de beheerportal en de services. Klik op het logo om een afbeeldingsbestand te uploaden.

- **Kleurenschema**. Het kleurenschema definieert de combinatie van kleuren die wordt gebruikt voor alle elementen van de gebruikersinterface. Klik op het schema en kies een van de vooraf gedefinieerde schema's die het beste past bij uw behoeften.

  Opmerking
  Klik op **Schemavoorbeeld bekijken op nieuw tabblad** om een voorbeeld te zien van de interfaceweergave voor uw onderliggende tenants. Branding wordt alleen toegepast als u op **Gereed** klikt in het deelvenster **Kleurenschema kiezen**.

- **White-label Cyber Protection-agent**. Met deze optie kunt u voor al uw onderliggende partners en klanten bepalen of de Cyber Protection-agent (voor Windows, macOS en Linux) en Cyber Protection Monitor (voor Windows, macOS en Linux) de merknaam of een white-label krijgen. Als u de optie inschakelt, krijgen de agent en tray monitor een white-label. Deze optie is van invloed op de namen en logo's die worden gebruikt in het installatieprogramma en Cyber Protection Monitor.

Documentatie en ondersteuning

- **URL van startpagina**. Deze pagina wordt geopend wanneer een gebruiker klikt op de bedrijfsnaam in het deelvenster **Over**.
- **URL voor ondersteuning**. Deze pagina wordt geopend wanneer een gebruiker klikt op de link **Contact opnemen met Support** in het deelvenster **Over** of in een e-mailbericht dat is verzonden vanuit de beheerportal.
- **Telefoonnummer voor ondersteuning**. Dit telefoonnummer wordt weergegeven in het deelvenster **Over**.
- **URL van Knowledge Base**. Deze pagina wordt geopend wanneer een gebruiker klikt op de link **Knowledge base** in een foutbericht.
- **Beheerdershandleiding voor beheerportal**. Deze pagina wordt geopend wanneer een gebruiker klikt op het vraagtekenpictogram in de rechterbovenhoek in de gebruikersinterface van de beheerportal en vervolgens op **Over** > **Beheerdershandleiding**.
- **Help voor beheerders van beheerportal**. Deze pagina wordt geopend wanneer een gebruiker klikt op het vraagtekenpictogram in de rechterbovenhoek in de gebruikersinterface van de beheerportal en vervolgens op **Help**.

Instellingen voor juridische documenten

- **URL van de Licentieovereenkomst voor eindgebruikers**. Deze pagina wordt geopend wanneer een gebruiker klikt op de link **Licentieovereenkomst voor eindgebruikers** in het deelvenster **Over** of op het **Welkomstscherm** na de eerste aanmelding.
- **URL van platformvoorwaarden**. Deze pagina wordt geopend wanneer een partnerbeheerder klikt op de link **Platformvoorwaarden** in het deelvenster **Over** of op het **Welkomstscherm** na de eerste aanmelding.
- **URL van de Privacyverklaring**. Deze pagina wordt geopend wanneer een gebruiker klikt op de link **Privacyverklaring** op het **Welkomstscherm** na de eerste aanmelding.

Belangrijk
Als u niet wilt dat een document op het welkomstscherm wordt weergegeven, voer dan geen URL in voor dat document.

Upsellen

- **URL voor kopen**. Deze pagina wordt geopend wanneer een gebruiker op **Nu kopen** klikt om te upgraden naar een meer geavanceerde editie van de Cyber Protection-service. Zie 'Upsell-scenario's voor uw klanten configureren' voor meer informatie over upsell-scenario's.

Mobiele apps

- **App Store**. Deze pagina wordt geopend wanneer de gebruiker op **Toevoegen** > **iOS** klikt in de **Cyber Protection**-service.
- **Google Play**. Deze pagina wordt geopend wanneer de gebruiker op **Toevoegen** > **Android** klikt in de **Cyber Protection**-service.

Instellingen e-mailserver

U kunt een aangepaste e-mailserver opgeven die wordt gebruikt om e-mailmeldingen te verzenden vanuit de beheerportal en de services. Als u een aangepaste e-mailserver wilt opgeven, klikt u op **Aanpassen** en geeft u de volgende instellingen op:

- Voer bij **Van** de naam in die wordt weergegeven in het veld **Van** van de e-mailmeldingen.
- Voer bij **SMTP** de naam in van de server voor uitgaande e-mail (SMTP).
- Voer bij **Poort** de poort in van de server voor uitgaande e-mail. De poort is standaard ingesteld op 25.
- Selecteer bij **Versleuteling** of u SSL- of TLS-versleuteling wilt gebruiken. Selecteer **Geen** als u versleuteling wilt uitschakelen.
- Geef bij **Gebruikersnaam** en **Wachtwoord** de referenties op van een account dat u wilt gebruiken om berichten te verzenden.

5.18.2 Branding configureren

1. Meld u aan bij de beheerportal.
2. Navigeer naar de tenant waarvoor u branding wilt configureren.
3. Klik op **Instellingen** > **Branding**.
4. Klik op **Branding inschakelen**.
5. Voer een van de volgende handelingen uit:
   - Configureer de branding-items die eerder zijn beschreven.

- Klik op **Wit label** om alle branding-items te wissen, behalve **Servicenaam**, **URL van de Licentieovereenkomst voor eindgebruikers**, **Beheerdershandleiding voor beheerportal**, **Help voor beheerders van beheerportal** en **Instellingen e-mailserver**.
- Klik op **Standaardinstellingen herstellen** om de standaardwaarden te herstellen voor alle branding-items.

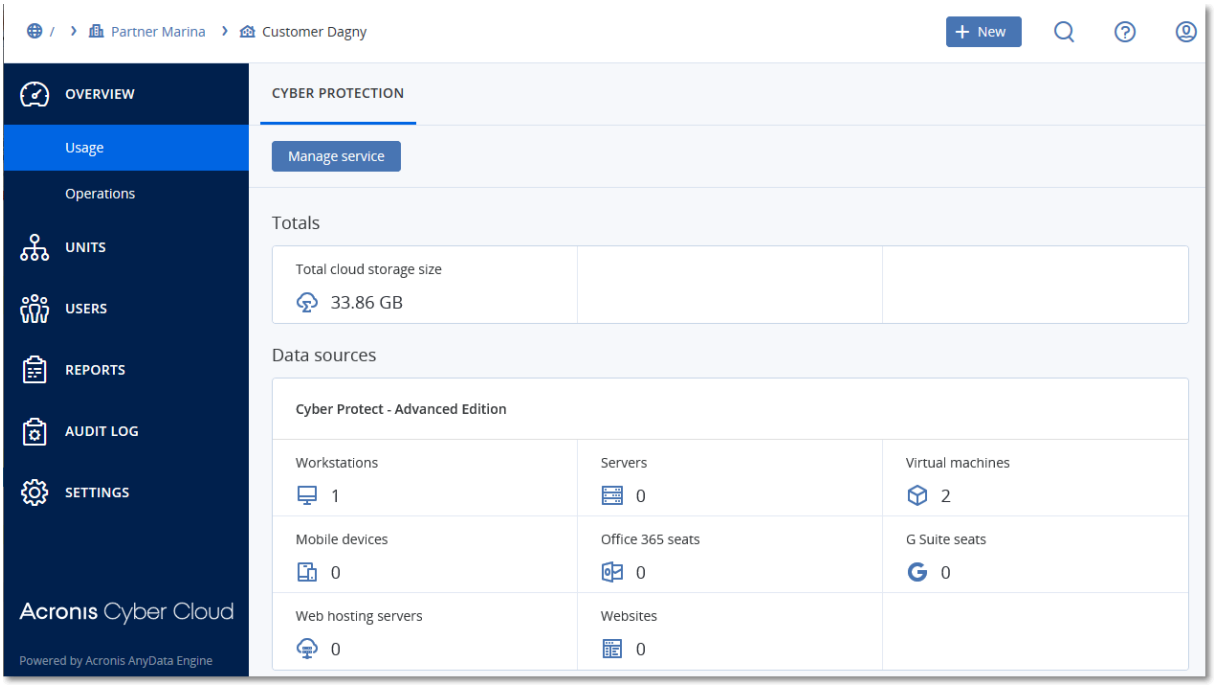
5.19 Controle

Klik op **Overzicht** voor toegang tot informatie over het gebruik en de bewerkingen van services.

5.19.1 Gebruik

Het tabblad **Gebruik** bevat een overzicht van het servicegebruik. Op dit tabblad hebt u toegang tot de services binnen de tenant waarin u werkt.

De gebruiksrapporten bevatten gegevens voor de inbegrepen functies, zowel standaard als geavanceerd.



5.19.2 Bewerkingen

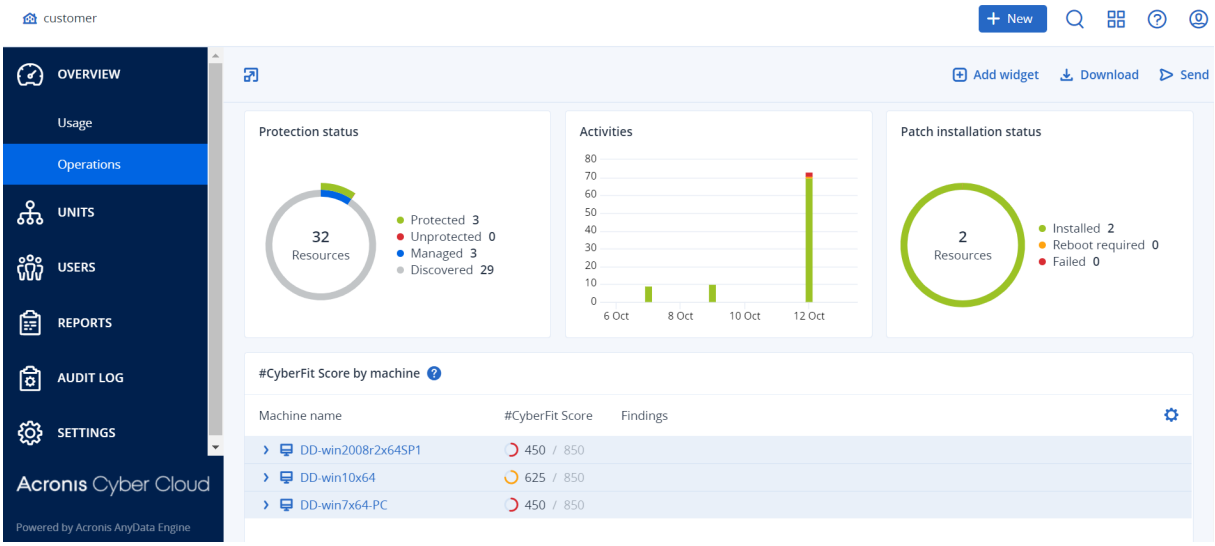
Het dashboard **Bewerkingen** bevat enkele aanpasbare widgets die een overzicht bieden van de bewerkingen voor de Cyber Protection-service. Widgets voor andere services worden in toekomstige releases beschikbaar gesteld.

Standaard worden de gegevens weergegeven voor de tenant waarin u werkt. U kunt de weergegeven tenant voor elke widget afzonderlijk wijzigen door deze te bewerken. Samengevoegde informatie over de directe onderliggende klanttenants van de geselecteerde tenant wordt ook weergegeven, inclusief de informatie die zich in mappen bevindt. Het dashboard geeft *geen*

informatie over onderliggende partners en hun onderliggende tenants weer; u moet inzoomen naar de specifieke partner om het betreffende dashboard te bekijken. Als u echter een onderliggende partnertenant converteert naar een maptenant, wordt de informatie over de onderliggende klanten van deze tenant weergegeven op het dashboard van de bovenliggende tenant.

De widgets worden elke twee minuten bijgewerkt. De widgets hebben klikbare elementen waarmee u problemen kunt onderzoeken en oplossen. U kunt de huidige status van het dashboard downloaden in PDF en/of XLSX-indeling, of deze via e-mail verzenden naar elk gewenst adres, inclusief externe ontvangers.

U kunt kiezen uit verschillende widgets in de vorm van tabellen, cirkeldiagrammen, staafdiagrammen, lijsten en structuurkaarten. U kunt meerdere widgets van hetzelfde type toevoegen voor verschillende tenants of met verschillende filters.



De widgets op het dashboard opnieuw indelen

Versleep de widgets door op de betreffende namen te klikken.

Een widget bewerken

Klik op het potloodpictogram naast de naam van de widget. Wanneer u een widget bewerkt, kunt u de naam ervan wijzigen, de periode wijzigen, de tenant selecteren waarvoor de gegevens worden weergegeven en filters instellen.

Een widget toevoegen

Klik op **Widget toevoegen** en voer vervolgens een van de volgende acties uit:

- Klik op de widget die u wilt toevoegen. De widget wordt toegevoegd met de standaardinstellingen.
- Als u de widget wilt bewerken voordat u deze toevoegt, klikt u op het tandwielpictogram wanneer de widget is geselecteerd. Wanneer u de widget hebt bewerkt, klikt u op **Gereed**.

Een widget verwijderen

Klik op de X naast de naam van de widget.

Beveiligingsstatus

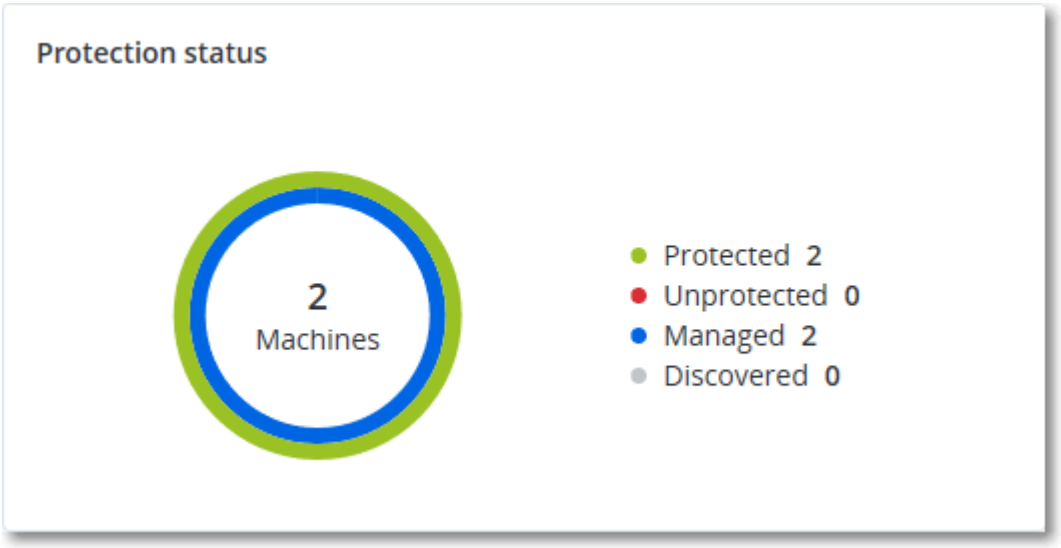
Beveiligingsstatus

Deze widget geeft de huidige beveiligingsstatus voor alle machines weer.

Een machine kan een van de volgende statussen hebben:

- **Beschermd**: machines met toegepast beschermingsschema.
- **Onbeschermd**: machines zonder toegepast beschermingsschema. Dit kunnen zowel gedetecteerde als beheerde machines zonder beschermingsschema zijn.
- **Beheerd**: machines met geïnstalleerde beveiligingsagent.
- **Gedetecteerd**: machines waarop geen beveiligingsagent is geïnstalleerd.

Als u op de machinestatus klikt, wordt u voor meer informatie omgeleid naar de lijst met machines die deze status hebben.



Gedetecteerde machines

Deze widget geeft de lijst met gedetecteerde machines tijdens het opgegeven tijdbereik weer.

Discovered machines

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

#CyberFit-score per machine

In deze widget ziet u voor elke machine de totale #CyberFit-score, de samengestelde scores en de bevindingen voor elk van de beoordeelde metrieken:

- Antimalware
- Back-up
- Firewall
- VPN
- Versleuteling
- NTLM-verkeer

Als u de score voor de verschillende metrieken wilt verbeteren, kunt u de aanbevelingen in het rapport bekijken.

Raadpleeg '#CyberFit-score voor machines' voor meer informatie over de #CyberFit-score.

#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 ...

Schijfintegriteitscontrole

Schijfintegriteitscontrole geeft informatie over de huidige status van de schijfintegriteit en een prognose daarover, zodat u gegevensverlies door een eventuele schijffout kunt voorkomen. Zowel HDD- als SSD-schijven worden ondersteund.

Beperkingen

- Prognose van schijfintegriteit wordt alleen ondersteund voor machines met Windows.
- Alleen schijven van fysieke machines worden gecontroleerd. De schijven van virtuele machines kunnen niet worden gecontroleerd en weergegeven in de widgets voor schijfintegriteit.
- RAID-configuraties worden niet ondersteund.
- Op NVMe-stations wordt schijfintegriteitscontrole alleen ondersteund voor stations die de SMART-gegevens via de Windows-API communiceren. Schijfintegriteitscontrole wordt niet ondersteund voor NVMe-stations waarop de SMART-gegevens rechtstreeks van het station moeten worden gelezen.

Schijfintegriteit kan een van de volgende statussen hebben:

- **OK**
  : de schijfintegriteit is tussen de 70 en 100%.
- **Waarschuwing**
  : de schijfintegriteit is tussen de 30 en 70%.
- **Kritiek**
  : de schijfintegriteit is tussen de 0 en 30%.
- **Schijfgegevens berekenen**
  : de huidige schijfstatus en -prognose worden berekend.

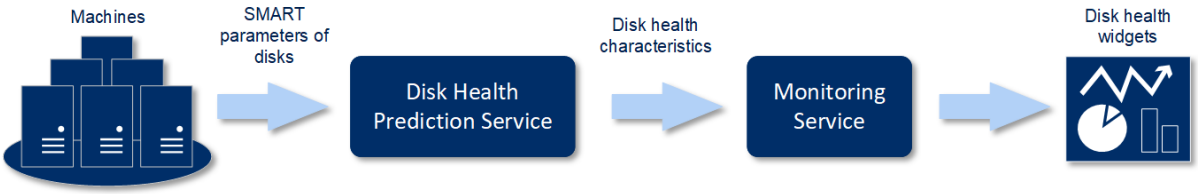
Zo werkt het

De service Voorspelling van schijfintegriteit maakt gebruik van een op kunstmatige intelligentie gebaseerd voorspellingsmodel.

1. De agent verzamelt de SMART-parameters van de schijven en geeft deze gegevens door aan de service Voorspelling van schijfintegriteit:
   - SMART 5: aantal opnieuw toegewezen sectoren.
   - SMART 9: uren ingeschakeld.
   - SMART 187: gerapporteerde niet-corrigeerbare fouten.
   - SMART 188: time-out van opdrachten.
   - SMART 197: huidig aantal sectoren in behandeling.
   - SMART 198: aantal offline niet-corrigeerbare sectoren.
   - SMART 200: percentage schrijffouten.

2. De service Voorspelling van schijfintegriteit verwerkt de ontvangen SMART-parameters, maakt prognoses en genereert de volgende kenmerken van de schijfintegriteit:
   - Huidige status van schijfintegriteit: OK, Waarschuwing, Kritiek.
   - Prognose van schijfintegriteit: negatief, stabiel, positief.
   - Prognose van schijfintegriteit, waarschijnlijkheid uitgedrukt als percentage.

   De periode van de voorspelling is één maand.
3. De controleservice ontvangt deze kenmerken en toont vervolgens de relevante informatie in de widgets voor schijfintegriteit in de serviceconsole.



Widgets voor schijfintegriteit

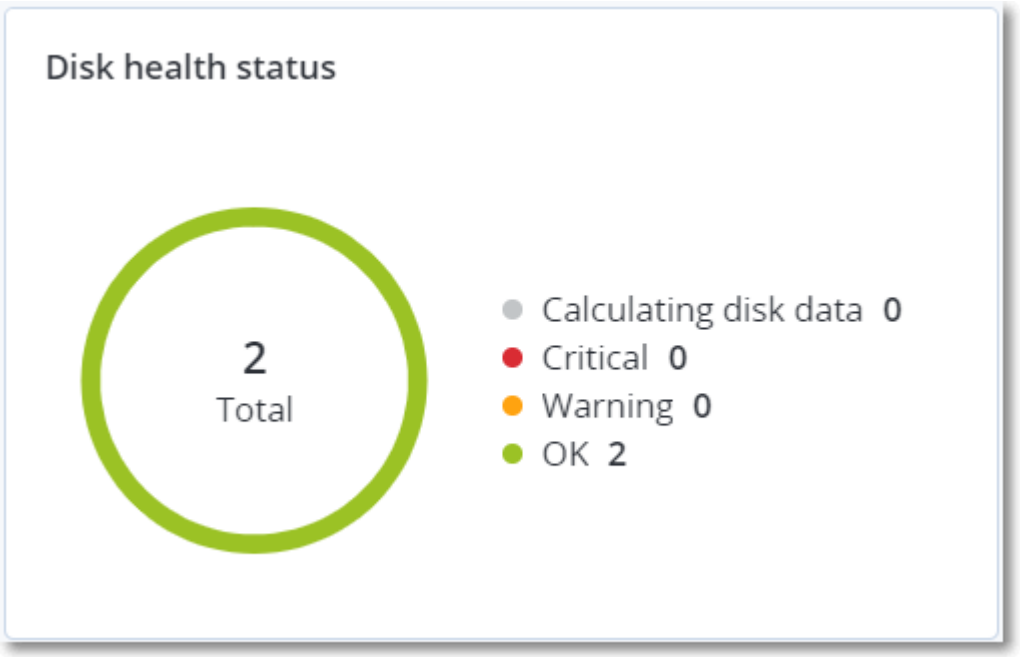
De resultaten van de schijfintegriteitscontrole worden weergegeven in de volgende widgets die beschikbaar zijn in de serviceconsole.

- **Overzicht van schijfintegriteit**: een widget met een structuurkaart op twee detailniveaus waartussen kan worden geschakeld.
  - Machineniveau
    : Geeft samengevatte informatie weer over de status van de schijfintegriteit van de geselecteerde klantmachines. Alleen de meest kritieke schijfstatus wordt weergegeven. De andere statussen worden in een knopinfo weergegeven wanneer u het betreffende blok aanwijst met de muis. Hoe groot het blok van de machine is, hangt af van de totale grootte van alle schijven van de machine. Welke kleur het blok van de machine heeft, hangt af van de meest kritieke schijfstatus die is gevonden.

- Schijfniveau
  : Geeft de huidige status van de schijfintegriteit weer van alle schijven voor de geselecteerde machine. Elk schijfblok toont een van de volgende prognoses van schijfintegriteit en de waarschijnlijkheid ervan in procenten:
  - Zal minder worden
  - Zal stabiel blijven

- Zal beter worden

- **Status van schijfintegriteit**: Een widget met een cirkeldiagram met het aantal schijven voor elke status.



Waarschuwingen over de status van de schijfintegriteit

De controle van de schijfintegriteit wordt elke 30 minuten uitgevoerd en de bijbehorende waarschuwing wordt een keer per dag gegenereerd. Wanneer de status van de schijfintegriteit verandert van **Waarschuwing** in **Kritiek**, wordt er altijd een waarschuwing gegenereerd.

Naam van de waarschuwing	Ernstgraad	Status van schijfintegriteit	Beschrijving
Schijffout is mogelijk	Waarschuwing	(30 – 70)	De schijf <schijfnaam> op deze machine zal waarschijnlijk defect raken in de toekomst. Voer zo snel mogelijk een volledige systeemkopieback-up van deze schijf uit, vervang deze en herstel de systeemkopie vervolgens op de nieuwe schijf.
Schijf zal binnenkort defect raken	Kritiek	(0 – 30)	De status van de schijf <schijfnaam> op deze machine is kritiek en de schijf zal waarschijnlijk binnenkort defect raken. Een imageback-up van deze schijf wordt op dit moment niet aanbevolen, omdat de schijf defect kan raken door de extra belasting. Maak nu meteen een back-up van de belangrijkste bestanden op deze schijf en vervang de schijf.

Overzicht van gegevensbescherming

Met de functie Overzicht van gegevensbescherming kunt u alle gegevens onderzoeken die belangrijk voor u zijn en gedetailleerde informatie krijgen over het aantal, de grootte, de locatie en de beveiligingsstatus van alle belangrijke bestanden in een schaalbare weergave met structuurkaart.

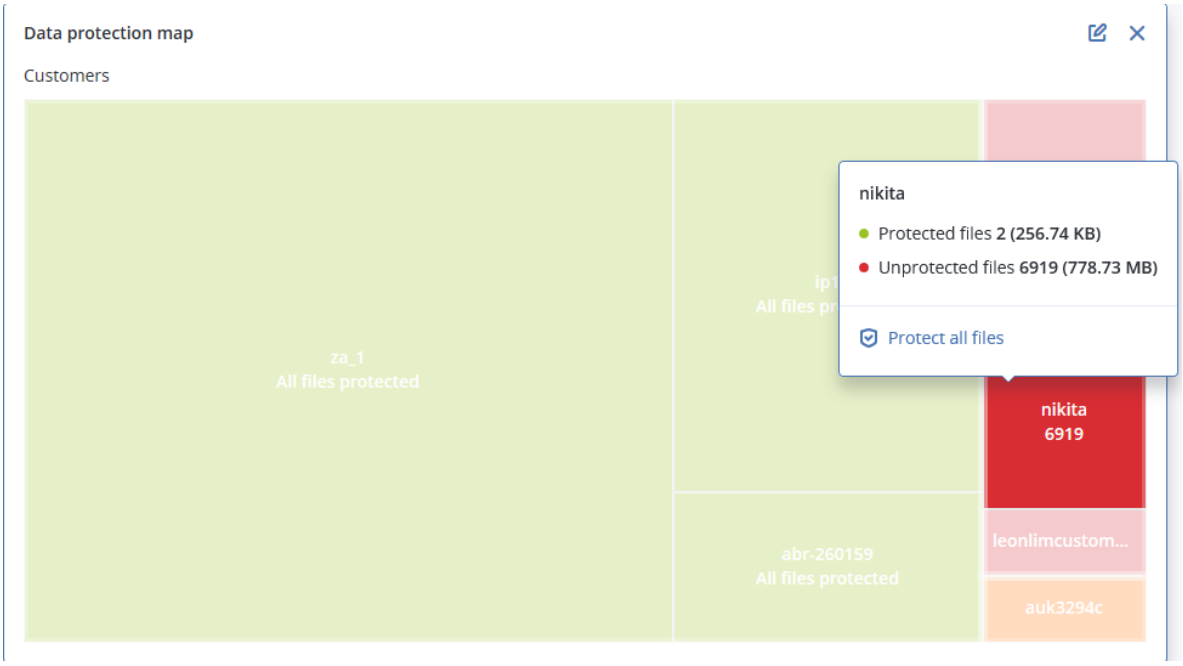
De grootte van elke blok hangt af van het totale aantal/de grootte van alle belangrijke bestanden die bij een klant/machine horen.

Bestanden kunnen een van de volgende beveiligingsstatussen hebben:

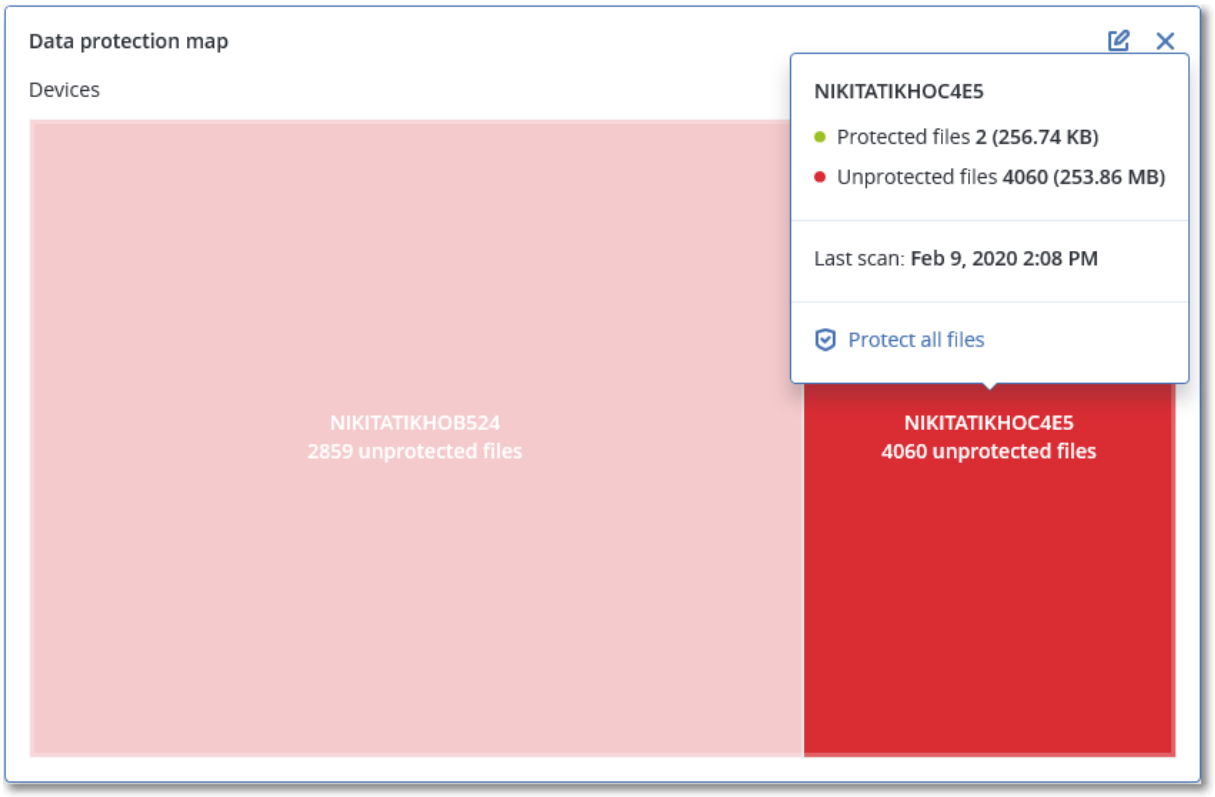
- **Kritiek**: er zijn 51-100% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt voor de geselecteerde klanttenant/machine/locatie.
- **Laag**: er zijn 21-50% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt voor de geselecteerde klanttenant/machine/locatie.
- **Medium:** er zijn 1-20% onbeschermde bestanden met de door u opgegeven extensies waarvan geen back-up wordt gemaakt voor de geselecteerde klanttenant/machine/locatie.
- **Hoog**: alle bestanden met de door u opgegeven extensies worden beschermd (er wordt een back-up van gemaakt) voor de geselecteerde klanttenant/machine/locatie.

De resultaten van het gegevensbeschermingsonderzoek zijn te vinden op het dashboard in de widget Overzicht van gegevensbescherming, een widget met een structuurkaart op twee detailniveaus waartussen kan worden geschakeld:

- Klanttenantniveau: geeft samengevatte informatie weer over de beveiligingsstatus van belangrijke bestanden per geselecteerde klant.



- Machineniveau: geeft samengevatte informatie weer over de beveiligingsstatus van belangrijke bestanden per geselecteerde klant.



Als u onbeschermde bestanden wilt beschermen, wijst u het blok aan en klikt u op **Alle bestanden beschermen**. In het dialoogvenster vindt u informatie over het aantal onbeschermde bestanden en de locatie hiervan. Klik op **Alle bestanden beschermen** om ze te beschermen.

U kunt ook een gedetailleerd rapport in CSV-indeling downloaden.

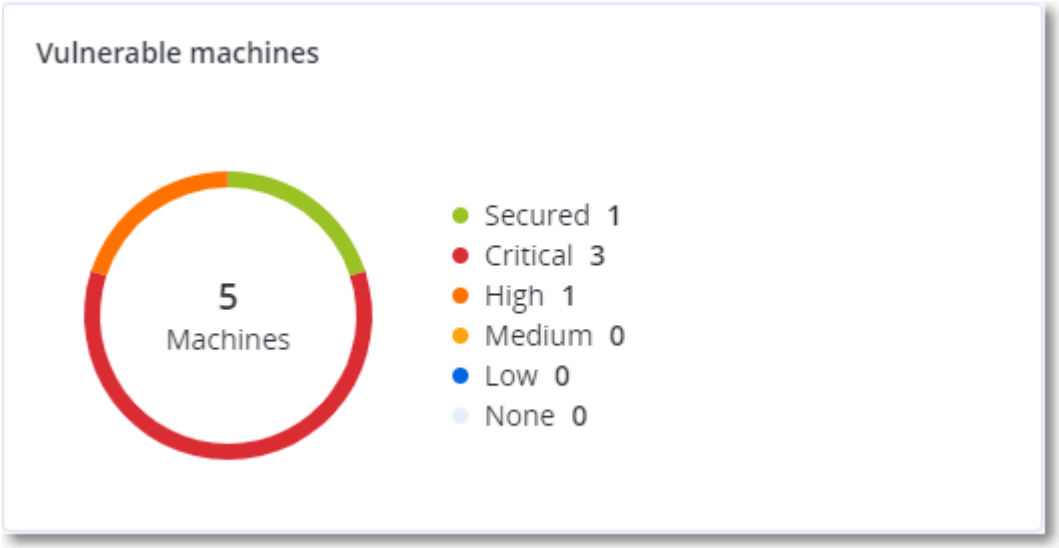
Widgets voor evaluatie van beveiligingsproblemen

Machines met beveiligingsproblemen

Deze widget geeft de machines met beveiligingsproblemen weer per ernstgraad.

Het gevonden beveiligingsprobleem kan een van de volgende ernstgraden hebben volgens het Common Vulnerability Scoring System (CVSS) v3.0:

- Beveiligd: geen beveiligingsproblemen gevonden
- Kritiek: 9,0 – 10,0 CVSS
- Hoog: 7,0 – 8,9 CVSS
- Medium: 4,0 – 6,9 CVSS
- Laag: 0,1 – 3,9 CVSS
- Geen: 0,0 CVSS



Bestaande kwetsbaarheden

Deze widget geeft de momenteel bestaande beveiligingsproblemen op machines weer. De widget **Bestaande beveiligingsproblemen** bevat twee kolommen met tijdstempels:

- **Eerst gedetecteerd**: datum en tijd waarop een beveiligingsprobleem voor het eerst is gedetecteerd op de machine.
- **Laatst gedetecteerd**: datum en tijd waarop een beveiligingsprobleem voor het laatst is gedetecteerd op de machine.

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

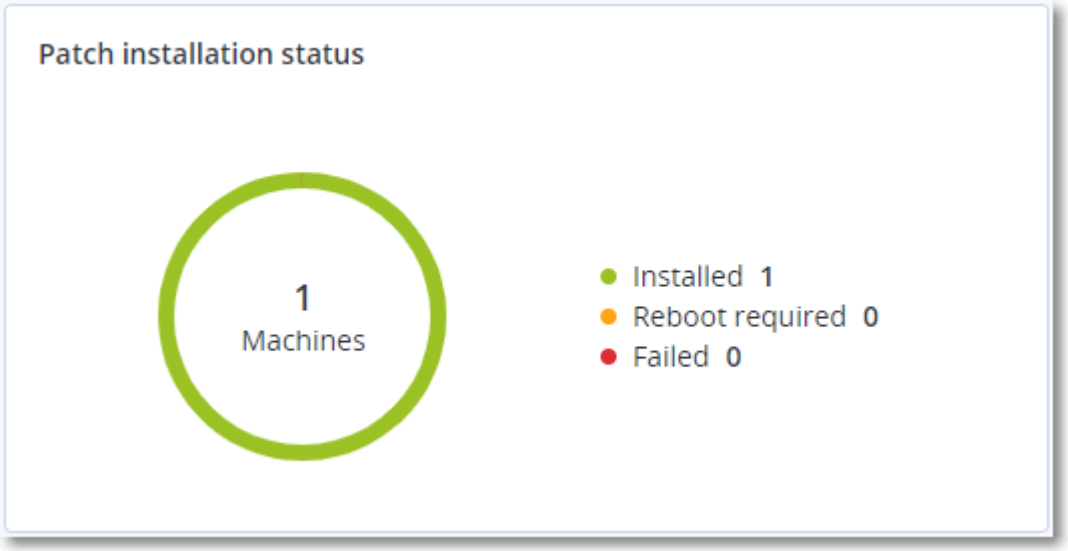
Widgets voor patchinstallatie

Er zijn vier widgets gerelateerd aan de functionaliteit voor patchbeheer.

Status van patchinstallatie

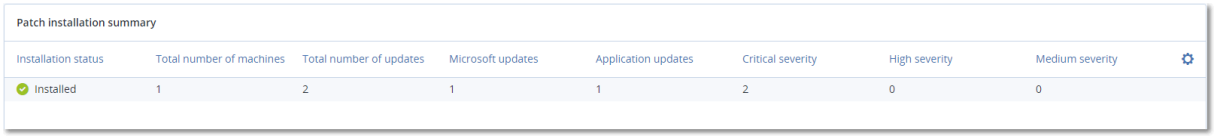
Deze widget geeft het aantal machines weer, gegroepeerd op status van de patchinstallatie.

- **Geïnstalleerd**: alle beschikbare patches zijn geïnstalleerd op een machine
- **Opnieuw opstarten vereist**: opnieuw opstarten is vereist voor een machine na de patchinstallatie
- **Mislukt**: patchinstallatie is mislukt op een machine



Overzicht van patchinstallatie

Deze widget geeft een overzicht van de patches op machines weer, gesorteerd op de status van de patchinstallatie.



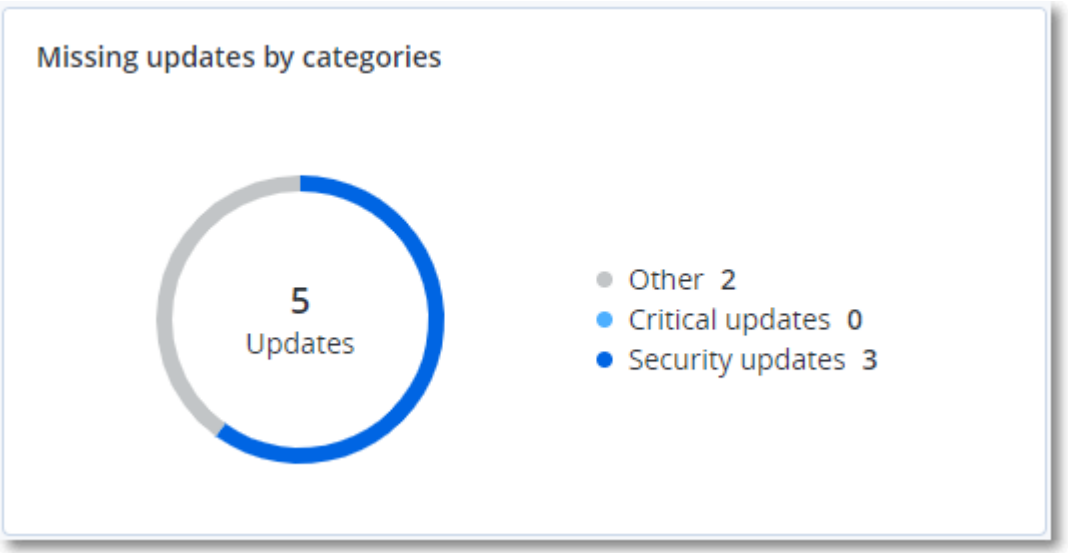
Geschiedenis van patchinstallatie

Deze widget geeft gedetailleerde informatie over patches op machines weer.

Ontbrekende updates per categorie

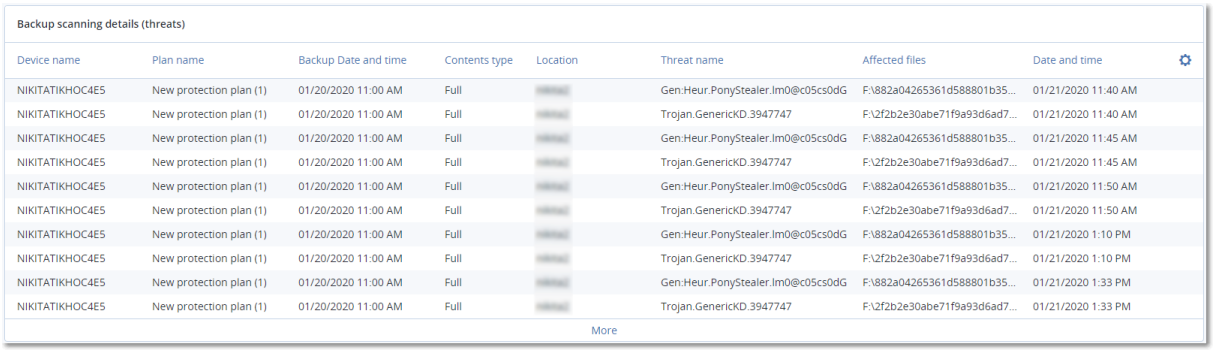
Deze widget geeft het aantal ontbrekende updates per categorie weer. De volgende categorieën worden weergegeven:

- Beveiligingsupdates
- Kritieke updates
- Anders



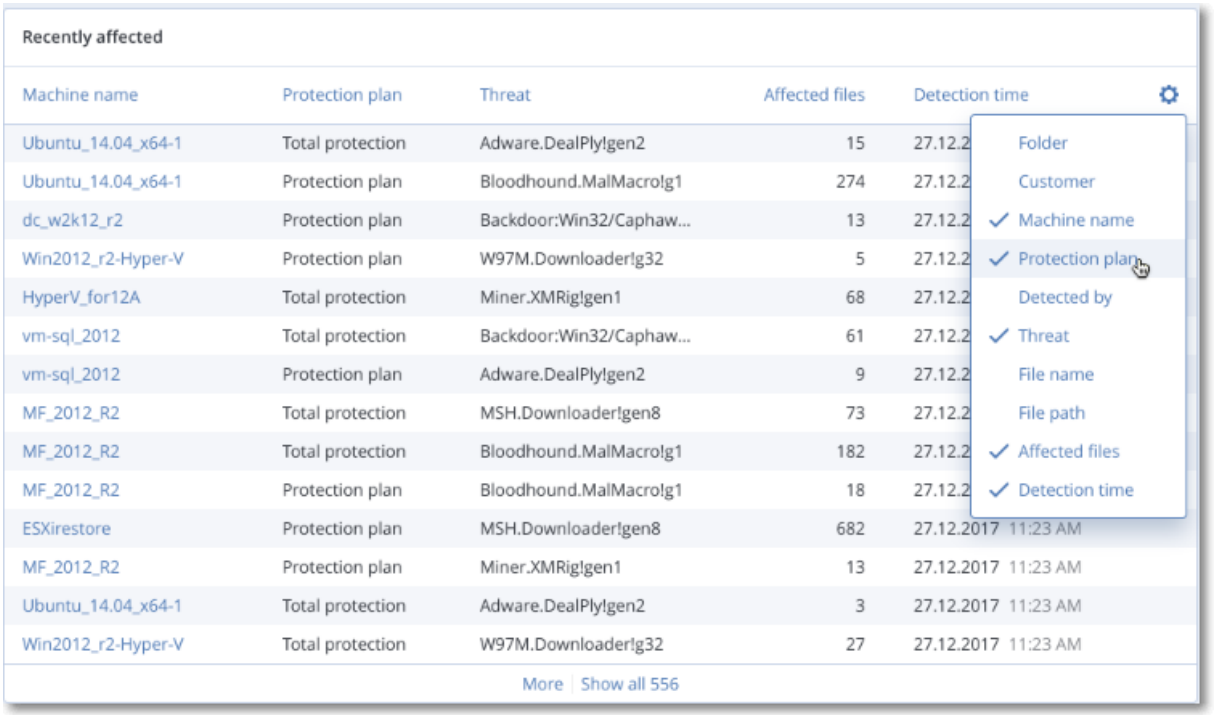
Gegevens van back-upscan

Deze widget geeft gedetailleerde informatie over de gedetecteerde bedreigingen in back-ups weer.



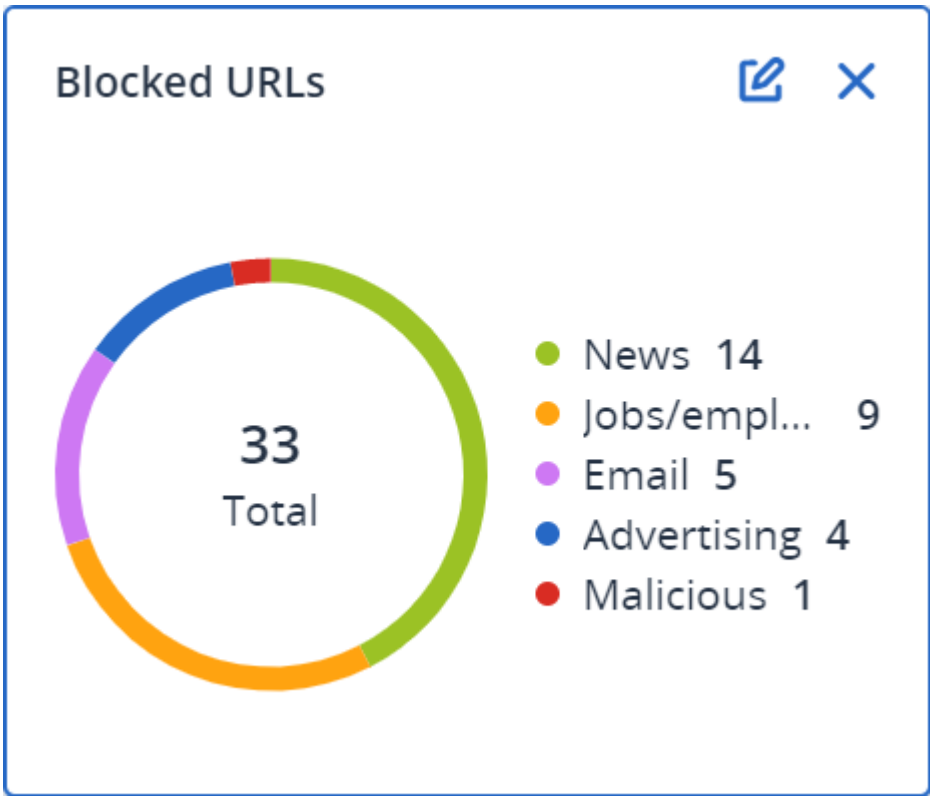
Onlangs beïnvloed

Deze widget geeft gedetailleerde informatie over recent geïnfecteerde machines weer. U kunt informatie vinden over welke bedreiging is gedetecteerd en hoeveel bestanden zijn geïnfecteerd.



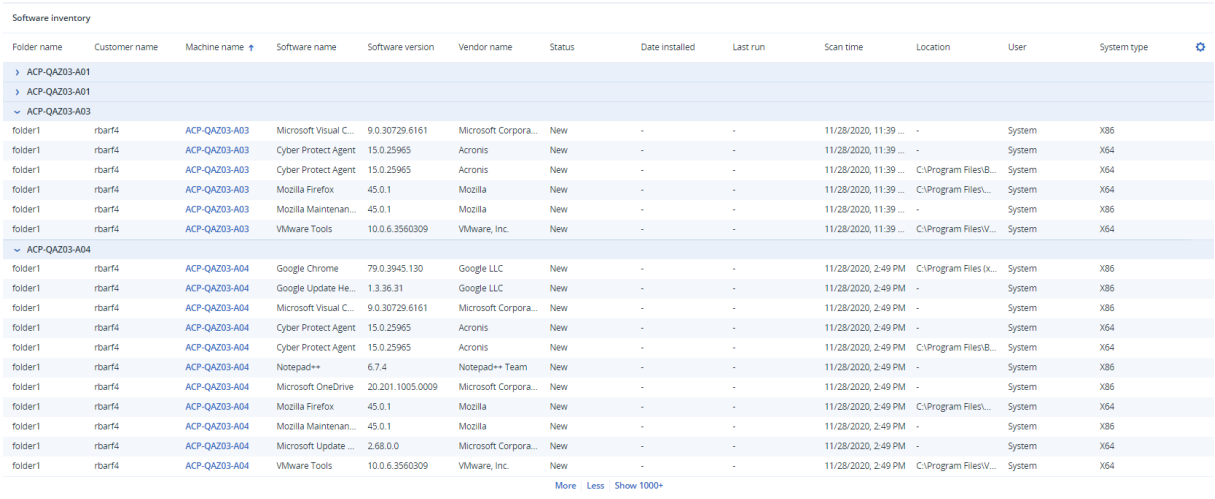
Geblokkeerde URL's

De widget geeft de statistieken van geblokkeerde URL's per categorie weer. Zie de Cyber Protection-gebruikershandleiding voor meer informatie over URL-filtering en -categorisering.



Widgets voor software-inventaris

De widget voor de tabel **Software-inventaris** geeft gedetailleerde informatie weer over alle software die is geïnstalleerd op Windows- en macOS-apparaten in de organisaties van uw klanten.

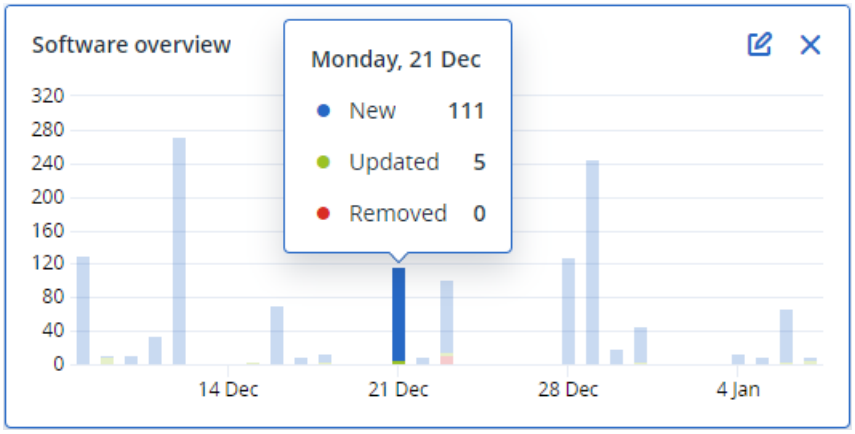


Software inventory

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+

De widget **Softwareoverzicht** geeft het aantal nieuwe, bijgewerkte en verwijderde toepassingen weer gedurende een bepaalde periode (7 dagen, 30 dagen of de huidige maand) op Windows- en macOS-apparaten in de organisaties van uw klanten.



Wanneer u met de muis een bepaalde balk in het diagram aanwijst, wordt er knopinfo weergegeven met de volgende informatie:

Nieuw: het aantal nieuw geïnstalleerde toepassingen.

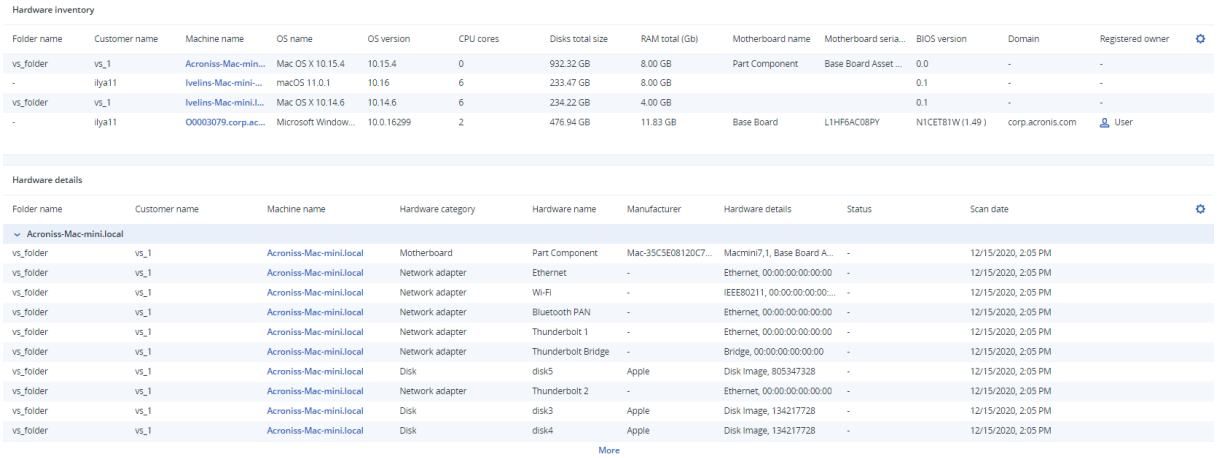
Bijgewerkt: het aantal bijgewerkte toepassingen.

Verwijderd: het aantal verwijderde toepassingen.

Wanneer u op het gedeelte van de balk klikt dat overeenkomt met een bepaalde status, wordt een pop-upvenster geladen. Het bevat een lijst met alle klanten die apparaten met toepassingen met de geselecteerde status hebben op de geselecteerde datum. U kunt een klant selecteren in de lijst en klikken op **Ga naar klant**. U wordt vervolgens omgeleid naar de pagina **Softwarebeheer** -> **Software-inventaris** in de serviceconsole van de klant. De informatie op de pagina wordt gefilterd op de betreffende datum en status.

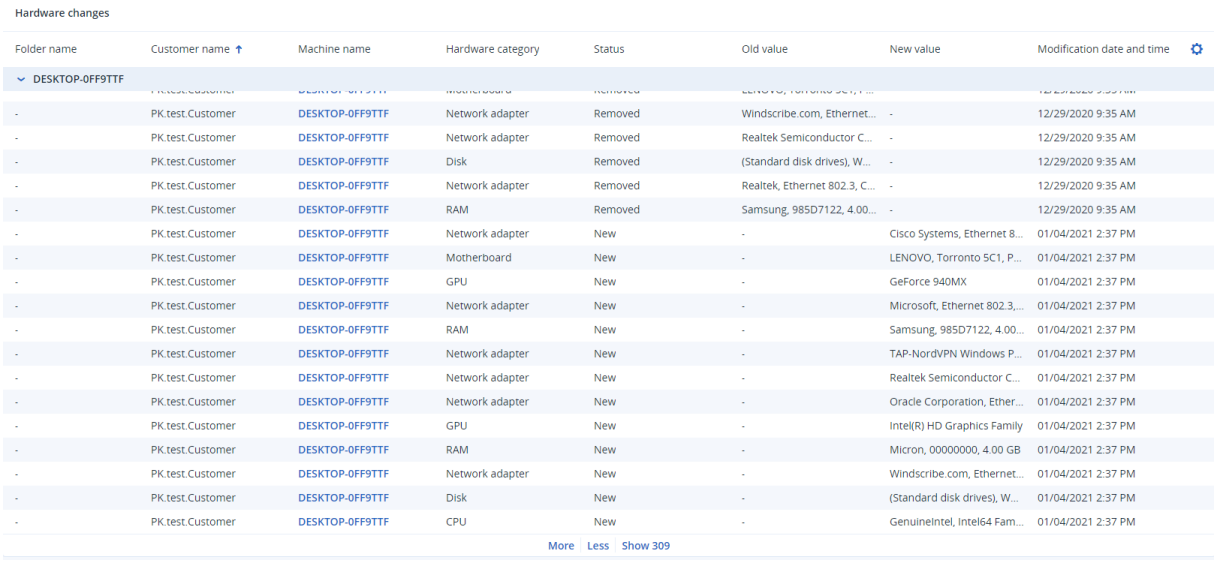
Widgets voor hardware-inventaris

De widgets voor de tabel **Hardware-inventaris** en **Hardwaregegevens** geven informatie weer over alle hardware die is geïnstalleerd op fysieke en virtuele Windows- en macOS-apparaten in de organisaties van uw klanten.



De widget voor de tabel **Hardwarewijzigingen** geeft informatie weer over de hardware die gedurende een bepaalde periode (7 dagen, 30 dagen of de huidige maand) is toegevoegd,

verwijderd of gewijzigd op fysieke en virtuele Windows- en macOS-apparaten in de organisaties van uw klanten.



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

5.20 Rapportage

Klik op **Rapporten** om rapporten over het gebruik en de bewerkingen van services te maken.

5.20.1 Gebruik

Gebruiksrapporten bevatten historische gegevens over het gebruik van de services. Gebruiksrapporten zijn beschikbaar in zowel CSV- als HTML-indeling.

Type rapport

U kunt een van de volgende rapporttypen selecteren:

- **Huidig gebruik**

  Het rapport bevat de huidige gebruiksmetrieken van de service.

  De gebruiksmetrieken worden berekend binnen elk van de factureringsperioden van de onderliggende tenants. Als de tenants in het rapport verschillende factureringsperioden hebben, kan het gebruik van de bovenliggende tenant verschillen van de som van het gebruik van de onderliggende tenants.
- **Huidige gebruiksdistributie**

  Dit rapport is alleen beschikbaar voor bovenliggende tenants die worden beheerd door een extern inrichtingssysteem. Dit rapport is nuttig wanneer de factureringsperioden van onderliggende tenants niet overeenkomen met de factureringsperiode van de bovenliggende tenant. Het rapport bevat de gebruiksmetrieken van de service voor onderliggende tenants, berekend binnen de huidige factureringsperiode van de bovenliggende tenant. Het gebruik van de bovenliggende tenant is gegarandeerd gelijk aan de som van het gebruik van de onderliggende tenants.

- **Samenvatting voor de hele periode**
  Het rapport bevat de gebruiksmetrieken van de service voor het einde van de opgegeven periode, en het verschil tussen de metrieken aan het begin en aan het einde van de opgegeven periode.
- **Elke dag gedurende de periode**
  Het rapport bevat de gebruiksmetrieken van de service en de wijzigingen voor elke dag van de opgegeven periode.

Bereik van het rapport

Voor het bereik van het rapport kunt u een van de volgende waarden selecteren:

- **Directe klanten en partners**
  Dit rapport bevat alleen de servicegebruiksmetrieken voor de directe onderliggende tenants van de tenant waarin u werkt.
- **Alle klanten en partners**
  Dit rapport bevat de servicegebruiksmetrieken voor alle onderliggende tenants van de tenant waarin u werkt.
- **Alle klanten, partners en gebruikers**
  Dit rapport bevat de servicegebruiksmetrieken voor alle onderliggende tenants van de tenant waarin u werkt en voor alle gebruikers binnen de tenants.

Geplande rapporten

Een gepland rapport bevat de servicegebruiksmetrieken voor de laatste volledige kalendermaand. De rapporten worden gegenereerd om 23:59:59 UTC op de eerste dag van een maand en verzonden op de tweede dag van die maand. De rapporten worden verzonden naar alle beheerders van uw tenant die het selectievakje **Geplande gebruiksrapporten** hebben ingeschakeld in de gebruikersinstellingen.

Een gepland rapport inschakelen of uitschakelen

1. Meld u aan bij de beheerportal.
2. Controleer of u werkt in de tenant op het hoogste niveau dat beschikbaar is voor u.
3. Klik op **Rapporten** > **Gebruik**.
4. Klik op **Gepland**.
5. Schakel het selectievakje **Een maandelijks overzichtsrapport verzenden** in of uit.
6. Ga naar **Detailniveau** en selecteer een van de eerder vermelde opties voor het bereik van het rapport.

Aangepaste rapporten

Dit type rapport wordt on-demand gegenereerd en kan niet worden gepland. Het rapport wordt verzonden naar uw e-mailadres.

Een aangepast rapport genereren

1. Meld u aan bij de beheerportal.
2. Navigeer naar de tenant waarvoor u een rapport wilt maken.
3. Klik op **Rapporten** > **Gebruik**.
4. Selecteer het tabblad **Aangepast**.
5. Ga naar **Type** en selecteer het rapporttype zoals eerder beschreven.
6. [Niet beschikbaar voor het rapporttype **Huidig gebruik**] Ga naar **Periode** en selecteer de rapportageperiode:
   - **Huidige kalendermaand**
   - **Vorige kalendermaand**
   - **Aangepast**
7. [Niet beschikbaar voor het rapporttype **Huidig gebruik**] Als u een aangepaste rapportageperiode wilt opgeven, selecteert u de begin- en einddatum. Anders kunt u deze stap overslaan.
8. Ga naar **Detailniveau** en selecteer een van de eerder vermelde opties voor het bereik van het rapport.
9. Klik op **Genereren en verzenden** om het rapport te genereren.

5.20.2 Rapporten over bewerkingen

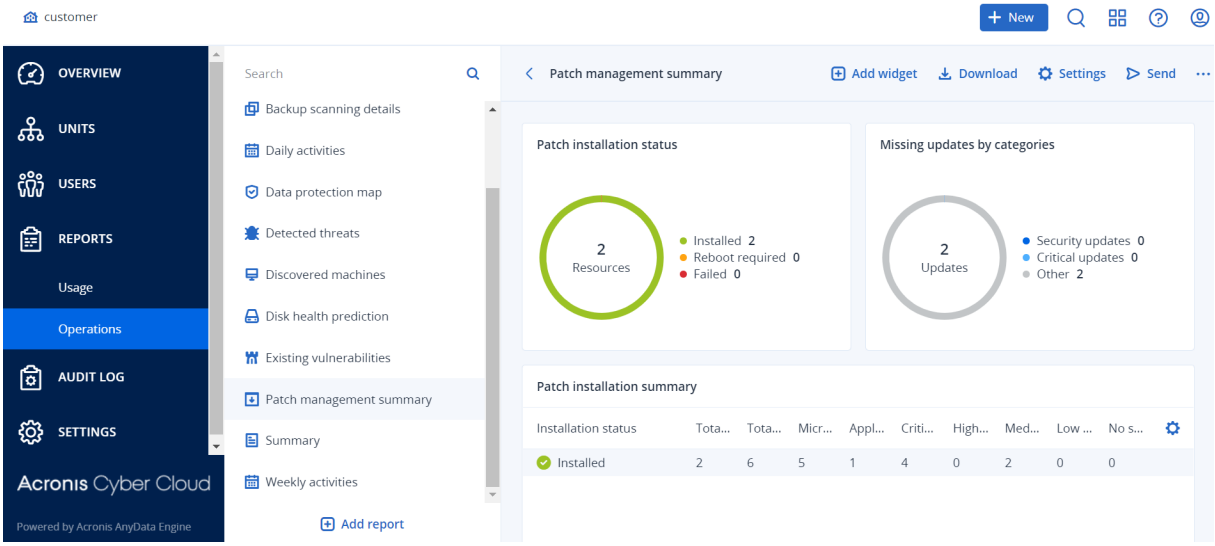
Een rapport over bewerkingen kan elke serie van de dashboardwidgets voor **Bewerkingen** bevatten. Standaard tonen alle widgets de overzichtsinformatie voor de tenant waarin u werkt. U kunt dit voor elke widget afzonderlijk wijzigen door deze te bewerken of voor alle widgets in de rapportinstellingen.

Afhankelijk van het widgettype bevat het rapport gegevens voor een tijdbereik of voor het moment van browsen of het genereren van rapporten. Zie "Gerapporteerde gegevens per type widget" (p. 103).

Alle historische widgets tonen gegevens voor hetzelfde tijdbereik. U kunt dit bereik wijzigen in de rapportinstellingen.

U kunt standaardrapporten gebruiken of een aangepast rapport maken.

U kunt een rapport over de activiteiten in Excel- (XLSX) of PDF-indeling downloaden of per e-mail verzenden.



De standaardrapporten worden hieronder weergegeven:

Naam van rapport	Beschrijving
#CyberFit-score per machine	Geeft de #CyberFit-score weer, gebaseerd op de evaluatie van de beveiligingsmetrieken en -configuraties voor elke machine, en geeft aanbevelingen voor verbeteringen.
Waarschuwingen	Geeft de waarschuwingen weer die zijn gegenereerd tijdens een bepaalde periode.
Gegevens van back-upscan	Geeft gedetailleerde informatie weer over gedetecteerde bedreigingen in de back-ups.
Dagelijkse activiteiten	Geeft de overzichtsinformatie weer over activiteiten die zijn uitgevoerd tijdens een bepaalde periode.
Overzicht van gegevensbescherming	Geeft gedetailleerde informatie weer over het aantal, de grootte, de locatie en de beveiligingsstatus van alle belangrijke bestanden op machines.
Gedetecteerde bedreigingen	Geeft details weer over de betroffen machines en het aantal geblokkeerde bedreigingen, en over de machines die in orde zijn en de machines met beveiligingsproblemen.
Gedetecteerde machines	Geeft alle gevonden machines in het organisatienetwerk weer.
Voorspelling van schijfintegriteit	Geeft voorspellingen weer over wanneer uw HDD/SSD zal uitvallen en de huidige schijfstatus.
Bestaande kwetsbaarheden	Geeft de bestaande beveiligingsproblemen voor het besturingssysteem en de toepassingen in uw organisatie weer. Het rapport geeft ook de details van de betroffen machines in uw

	netwerk weer voor elk product dat wordt vermeld.
Overzicht van patchbeheer	Geeft het aantal ontbrekende patches, geïnstalleerde patches en toepasselijke patches weer. U kunt de rapporten analyseren om de gegevens over ontbrekende/geïnstalleerde patches en de details van alle systemen te krijgen.
Overzicht	Geeft de overzichtsinformatie over de beschermde apparaten tijdens een bepaalde periode weer.
Wekelijkse activiteiten	Geeft de overzichtsinformatie weer over activiteiten die zijn uitgevoerd tijdens een bepaalde periode.
Software-inventaris	Geeft gedetailleerde informatie weer over alle software die is geïnstalleerd op Windows- en macOS-machines in de organisaties van uw klanten.
Hardware-inventaris	Geeft gedetailleerde informatie weer over alle hardware die beschikbaar is op fysieke en virtuele Windows- en macOS-machines in de organisaties van uw klanten.

Als u een rapport wilt bekijken, klikt u op de naam ervan.

Als u bewerkingen met een rapport wilt openen, klikt u op het verticale ellipspictogram op de rapportregel. Dezelfde bewerkingen zijn beschikbaar vanuit het rapport.

Rapport toevoegen

1. Klik op **Rapport toevoegen**.
2. Voer een van de volgende handelingen uit:
   - Als u een vooraf gedefinieerd rapport wilt toevoegen, klikt u op de naam ervan.
   - Als u een aangepast rapport wilt toevoegen, klikt u op **Aanpassen**, klikt u op de naam van het rapport (de standaard toegewezen namen zien eruit als **Aangepast (1)**) en vervolgens voegt u widgets toe aan het rapport.
3. [Optioneel] Versleep de widgets om ze opnieuw te rangschikken.
4. [Optioneel] Bewerk het rapport zoals hieronder beschreven.

De rapportinstellingen bewerken

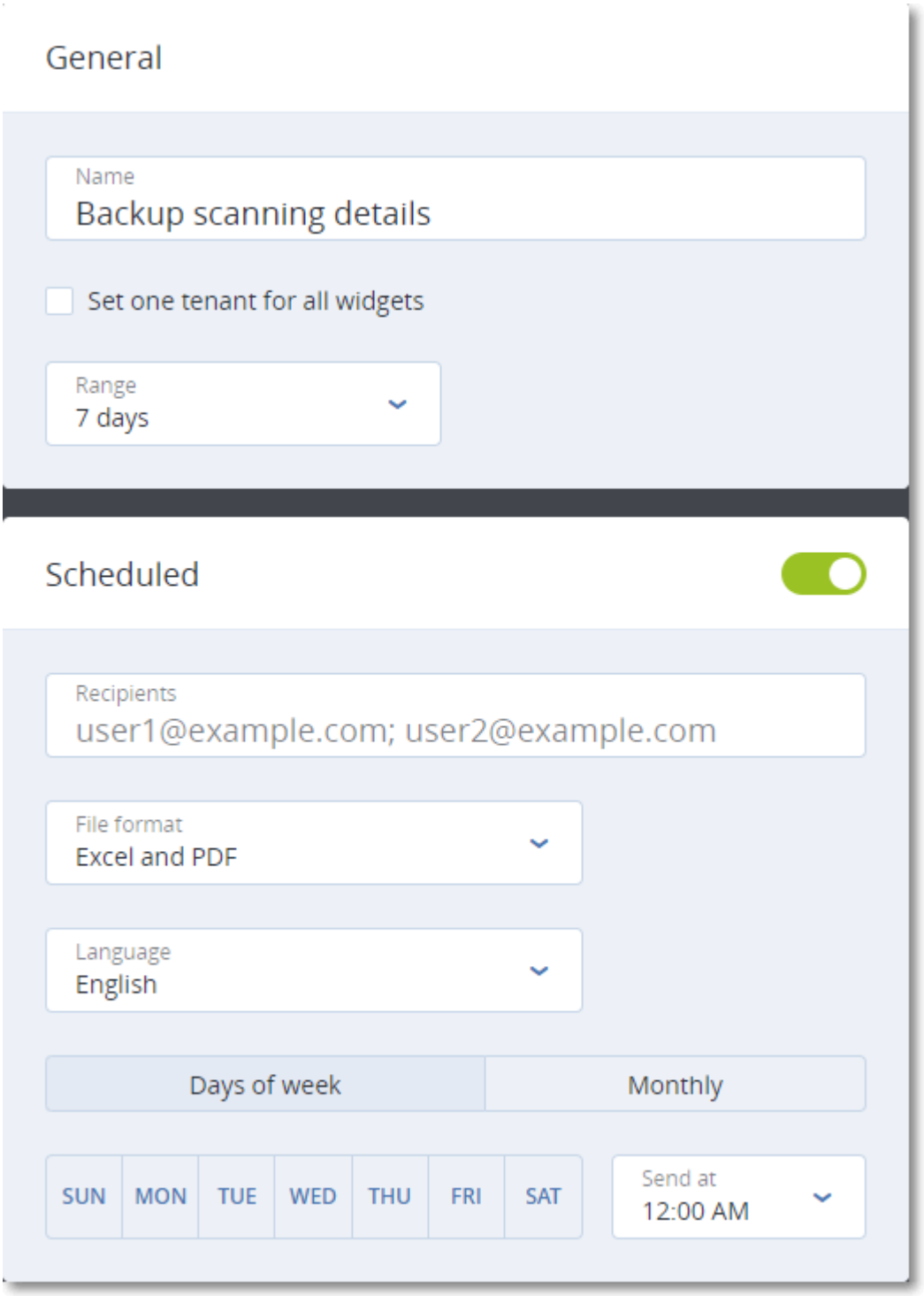
Als u een rapport wilt bewerken, klikt u op de naam ervan en vervolgens klikt u op **Instellingen**. Wanneer u een rapport bewerkt, kunt u het volgende doen:

- De naam van het rapport wijzigen
- De weergegeven tenant voor alle widgets in het rapport wijzigen

  Als u onderliggende tenants hebt, dan is de optie **Eén tenant instellen voor alle widgets** beschikbaar. Met deze optie kunt u gegevens in alle widgets van het rapport filteren op de

geselecteerde tenant. Als deze optie niet is geselecteerd, dan worden de gegevens voor alle onderliggende tenants van uw huidige tenant weergegeven.

- Het tijdbereik voor alle widgets in het rapport wijzigen
- Plan om het rapport in PDF- en/of Excel-indeling te verzenden via e-mail.



Een rapport plannen

1. Klik op de naam van het rapport en klik vervolgens op **Instellingen**.
2. Schakel de switch **Gepland** in.
3. Geef de e-mailadressen van de ontvangers op.
4. Selecteer de rapportindeling: PDF, Excel of beide.
5. Selecteer de dagen en het tijdstip waarop het rapport wordt verzonden.
6. Klik op **Opslaan** in de rechterbovenhoek.

De rapportstructuur exporteren en importeren

U kunt de rapportstructuur (de set widgets en de rapportinstellingen) exporteren en importeren naar een JSON-bestand. Dit kan handig zijn voor het kopiëren van de rapportstructuur tussen verschillende tenants.

Als u de rapportstructuur wilt exporteren, klikt u op de naam van het rapport, klikt u op het verticale ellipspictogram in de rechterbovenhoek en klikt u vervolgens op **Exporteren**.

Als u de rapportstructuur wilt importeren, klikt u op **Rapport toevoegen** en vervolgens op **Importeren**.

Een rapport downloaden

U kunt een rapport downloaden. Klik op **Downloaden** en selecteer de gewenste indelingen:

- Excel en PDF
- Excel
- PDF

Een dump maken van de rapportgegevens

U kunt een dump van de rapportgegevens in een CSV-bestand verzenden via e-mail. De dump bevat alle rapportgegevens (zonder dat deze gefilterd zijn) voor een aangepast tijdbereik. De tijdstempels in CSV-rapporten hebben de UTC-indeling, terwijl de tijdstempels in Excel- en PDF-rapporten de huidige tijdzone van het systeem weergeven.

De software genereert de gegevensdump binnen een mum van tijd. Als u een lange tijdsduur opgeeft, kan deze actie lang duren.

Een dump maken van de rapportgegevens

1. Klik op de naam van het rapport.
2. Klik op het verticale ellipsvormige pictogram in de rechterbovenhoek en klik vervolgens op **Dumpgegevens**.
3. Geef de e-mailadressen van de ontvangers op.

4. Geef in **Tijdbereik** het tijdbereik op.
5. Klik op **Verzenden**.

5.20.3 Overzicht

Het overzichtsrapport bevat een overzicht van de beschermingsstatus van de omgevingen van uw klanten en hun beschermde apparaten voor een bepaald tijdbereik.

Het overzichtsrapport bevat secties met dynamische widgets die de belangrijkste prestatiegegevens tonen over het gebruik van de volgende cloudservices door de klant: Back-up, antimalwarebeveiliging, evaluatie van beveiligingsproblemen, patchbeheer, preventie van gegevensverlies, Notary, noodherstel en Files Sync & Share.

Er zijn verschillende manieren waarop u het rapport kunt aanpassen.

- Secties toevoegen of verwijderen.
- De volgorde van secties wijzigen.
- De naam van secties wijzigen.
- Widgets verplaatsen naar een andere sectie.
- Wijzig de volgorde van de widgets in elke sectie.
- Voeg widgets toe of verwijder ze.
- Pas widgets aan.

U kunt overzichtsrapporten genereren in PDF- en Excel-indeling, en deze naar de belanghebbenden of eigenaren van de organisaties van uw klanten sturen, zodat zij gemakkelijk de technische en zakelijke waarde van de geleverde services kunnen zien.

Partnerbeheerders kunnen het samenvattingsrapport alleen genereren en naar directe klanten verzenden. In het geval van een complexere tenanthiërarchie met subpartners moeten de subpartners het rapport genereren.

Widgets voor het overzichtsrapport

U kunt secties en widgets toevoegen aan of verwijderen uit het overzichtsrapport en zo bepalen welke informatie wordt opgenomen in het rapport.

Widgets voor overzicht van workloads

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Overzicht van workloads**.

Widget	Beschrijving
Overzicht van cyberbescherming	De widget toont de belangrijkste prestatiegegevens van cyberbescherming voor het opgegeven tijdbereik.

Widget	Beschrijving
	Gegevens met back-up: de totale grootte van de archieven die zijn gemaakt in de cloudopslag en lokale opslag. **Verholpen bedreigingen**: het totale aantal keren dat malware is geblokkeerd op alle apparaten. **Schadelijke URL's geblokkeerd**: het totale aantal URL's dat is geblokkeerd op alle apparaten. **Gepatchte beveiligingsproblemen**: het totale aantal beveiligingsproblemen dat is verholpen door de installatie van softwarepatches op alle apparaten. **Geïnstalleerde patches**: het totale aantal geïnstalleerde patches op alle apparaten. **Servers beschermd door DR**: het totale aantal servers dat wordt beschermd door Disaster Recovery. **File Sync & Share-gebruikers**: het totale aantal eind- en gastgebruikers dat gebruikmaakt van Cyber Files. **Genotariseerde bestanden**: het totale aantal genotariseerde bestanden. **Elektronisch ondertekende documenten**: het totale aantal elektronisch ondertekende documenten. **Geblokkeerde randapparaten**: het totale aantal geblokkeerde randapparaten.
Beveiligingsstatus van workloads	De widget toont de beschermde en niet-beschermde workloads per type op het moment dat het rapport werd gegenereerd. Beschermde workloads zijn workloads waarop ten minste één beschermings- of back-upschema wordt toegepast. Niet-beschermde workloads zijn workloads waarop geen beschermings- of back-upschema wordt toegepast. De volgende workloads worden meegeteld: **Servers**: fysieke servers en domeincontrollerservers. **Werkstations**: fysieke werkstations. **Virtuele machines**: zowel virtuele machines met agent als zonder agent. **Webhostingservers**: virtuele of fysieke server met geïnstalleerde cPanel of Plesk. **Mobiele apparaten**: fysieke mobiele apparaten. Een workload kan tot meer dan één categorie behoren. Een webhostingserver wordt bijvoorbeeld in twee categorieën ondergebracht: **Servers** en **Webhostingservers**.

Widget	Beschrijving
Beveiligingsstatus van workloads in de cloud	**Beveiligingsstatus van workloads in de cloud** De widget toont het aantal beschermde en niet-beschermde workloads in de cloud per type op het moment dat het rapport werd gegenereerd. Beschermde cloudworkloads zijn cloudworkloads waarop ten minste één back-upschema wordt toegepast. Niet-beschermde cloudworkloads zijn cloudworkloads waarop geen back-upschema wordt toegepast. De volgende typen cloudworkloads worden weergegeven in het diagram (in alfabetische volgorde van A tot Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace - Gedeelde Drive • Gehoste Exchange-postvakken • Microsoft 365-postvakken • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites Voor sommige workloadtypen worden de volgende workloadgroepen gebruikt: • Microsoft 365: Gebruikers, groepen, openbare mappen, teams en siteverzamelingen • Google Workspace: Gebruikers en Shared Drives • Gehoste Exchange: Gebruikers Als er in een workloadgroep meer dan 10.000 workloads zijn, toont de widget geen gegevens voor de betreffende workloads. Als de klant bijvoorbeeld een Microsoft 365-account heeft met 10.000 postvakken en OneDrive-service voor 500 gebruikers, behoren deze allemaal tot de workloadgroep. De som van deze workloads is 10.500, waardoor de limiet van 10.000 per workloadgroep wordt overschreden. Daarom worden de betreffende workloads verborgen in de widget: Microsoft 365-postvakken en Microsoft 365 OneDrive.

Widgets voor antimalwarebeveiliging

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Antimalwarebeveiliging**.

Widget	Beschrijving
Antimalwarescan van bestanden	De widget toont de resultaten van de antimalwarescan op aanvraag van de apparaten binnen het opgegeven datumbereik.

Widget	Beschrijving
	Bestanden: het totale aantal gescande bestanden **Opschonen**: het totale aantal schone bestanden **Gedetecteerd, in quarantaine geplaatst**: het totale aantal geïnfecteerde bestanden die in quarantaine zijn geplaatst **Gedetecteerd, niet in quarantaine geplaatst**: het totale aantal geïnfecteerde bestanden die niet in quarantaine zijn geplaatst **Beschermde apparaten**: het totale aantal apparaten waarop een beleid voor antimalwarebeveiliging wordt toegepast **Totaal aantal geregistreerde apparaten**: het totale aantal geregistreerde apparaten op het moment dat het rapport wordt gegenereerd
Geblokkeerde URL's	De widget toont het aantal geblokkeerde URL's gegroepeerd per websitecategorie voor het opgegeven datumbereik. De widget geeft de zeven websitecategorieën weer met het grootste aantal geblokkeerde URL's en combineert de rest van de websitecategorieën in **Overige**. Zie het onderwerp URL-filtering in Cyber Protection voor meer informatie over de websitecategorieën.
Bedreigingen gedetecteerd door beschermingstechnologie	De widget toont het aantal gedetecteerde bedreigingen voor het opgegeven datumbereik, gegroepeerd per beschermingstechnologie: • Antimalwarescan • Gedragengine • Bescherming tegen cryptomining • Preventie tegen aanvallen • Actieve bescherming tegen ransomware • Realtime bescherming • URL-filtering
Antimalwarescan van back-ups	De widget toont de resultaten van de antimalwarescans van de back-ups voor het opgegeven datumbereik, op basis van de volgende metrieken: • Totale aantal gescande herstelpunten • Aantal schone herstelpunten • Aantal schone herstelpunten met niet-ondersteunde partities • Aantal geïnfecteerde herstelpunten. Deze metriek omvat het aantal geïnfecteerde herstelpunten met niet-ondersteunde partities.

Back-upwidgets

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Back-up**.

Widget	Beschrijving
Workloads waarvan een back-up is gemaakt	De widget toont het totaal aantal geregistreerde workloads per back-upstatus. **Back-up gemaakt**: het aantal workloads waarvan een back-up is gemaakt (ten minste één back-up is uitgevoerd) gedurende het datumbereik van het rapport. **Geen back-up gemaakt**: het aantal workloads waarvan geen back-up is gemaakt (er is geen enkele back-up uitgevoerd) gedurende het datumbereik van het rapport.
Status van schijfintegriteit per fysiek apparaat	De widget toont de geaggregeerde integriteitsstatus van fysieke apparaten, gebaseerd op de integriteitsstatus van hun schijven. **OK**: deze status van de schijfintegriteit wordt gebruikt voor de waarden [70-100]. De status van het apparaat is **OK** wanneer alle schijven de status **OK** hebben. **Waarschuwing**: deze status van de schijfintegriteit wordt gebruikt voor de waarden [30-70]. De status van een apparaat is **Waarschuwing** wanneer de status van ten minste een van de schijven **Waarschuwing** is en wanneer er geen schijven de status **Fout** hebben. **Fout**: deze status van de schijfintegriteit wordt gebruikt voor de waarden [0-30]. De status van het apparaat is **Fout** wanneer de status van ten minste een van de schijven de status **Fout** heeft. **Schijfgegevens berekenen**: de status van het apparaat is **Schijfgegevens berekenen** wanneer de statussen van de schijven van het apparaat nog niet zijn berekend.
Opslaggebruik voor back-ups	De widget toont het totale aantal en de totale grootte van de back-ups in de cloud en de lokale opslag voor het opgegeven tijdbereik.

Widgets voor evaluatie van beveiligingsproblemen en patchbeheer

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Evaluatie van beveiligingsproblemen en patchbeheer**.

Widget	Beschrijving
Gepatchte beveiligingsproblemen	De widget toont de prestatieresultaten van de evaluatie van beveiligingsproblemen voor het opgegeven datumbereik. **Totaal**: het totale aantal gepatchte beveiligingsproblemen.

Widget	Beschrijving
	Microsoft-softwarebeveiligingsproblemen: het totale aantal verholpen problemen met de Microsoft-beveiliging op alle Windows-apparaten. **Beveiligingsproblemen van Windows-software van derden**: het totale aantal verholpen beveiligingsproblemen met Windows-software van derden op alle Windows-apparaten. **Gescande workloads**: het totale aantal apparaten dat minstens eenmaal is gescand op beveiligingsproblemen binnen het opgegeven datumbereik.
Geïnstalleerde patches	De widget toont de prestatieresultaten van het patchbeheer voor het opgegeven datumbereik. **Geïnstalleerd**: het totaal getal patches dat is geïnstalleerd op alle apparaten. **Microsoft-softwarepatches**: het totale aantal Microsoft-softwarepatches dat is geïnstalleerd op alle Windows-apparaten. **Patches voor Windows-software van derden**: het totale aantal patches voor Windows-software van derden dat is geïnstalleerd op alle Windows-apparaten. **Gepatchte workloads**: het totale aantal apparaten dat is gepatcht (ten minste één patch is geïnstalleerd binnen het opgegeven datumbereik).

Widgets voor noodherstel

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Noodherstel**.

Widget	Beschrijving
Disaster Recovery-statistieken	De widget toont de belangrijkste prestatiegegevens van noodherstel voor het opgegeven datumbereik. **Productiefailovers**: het aantal productiefailoverbewerkingen voor het opgegeven tijdbereik. **Testfailovers**: het totale aantal testfailoverbewerkingen in het opgegeven tijdbereik. **Primaire servers**: het totale aantal primaire servers op het moment dat het rapport werd gegenereerd. **Herstelservers**: het totale aantal herstelservers op het moment dat het rapport werd gegenereerd. **Openbare IP's**: het totale aantal openbare IP-adressen (op het moment dat het rapport werd gegenereerd).

Widget	Beschrijving
	Totaal verbruikte compute-punten: het totale aantal compute-punten dat is verbruikt in het opgegeven tijdbereik.
Disaster Recovery - Servers getest	De widget toont informatie over de servers die zijn beschermd door Disaster Recovery en zijn getest met testfailover. De widget toont de volgende metrieken: **Server beschermd**: het aantal servers dat wordt beschermd door Disaster Recovery (servers die ten minste één herstelserver hebben) op het moment dat het rapport werd gegenereerd. **Getest**: het aantal door Disaster Recovery beschermde servers dat is getest met testfailover gedurende het geselecteerde tijdbereik, ten opzichte van alle door Disaster Recovery beschermde servers. **Niet getest**: het aantal door Disaster Recovery beschermde servers dat niet is getest met testfailover gedurende het geselecteerde tijdbereik, ten opzichte van alle door Disaster Recovery beschermde servers. De widget toont ook de grootte van de Disaster Recovery-opslag (in GB) op het moment dat het rapport werd gegenereerd. Het is de som van de back-upgrootten van de cloudservers.
Servers beschermd door Disaster Recovery	De widget toont informatie over de servers die zijn beschermd door Disaster Recovery en de niet-beschermde servers. De widget toont de volgende metrieken: Het totale aantal servers geregistreerd in de klanttenant op het moment dat het rapport werd gegenereerd. **Beschermd**: het aantal servers dat wordt beschermd door Disaster Recovery (servers die ten minste één herstelserver en een volledige serverback-up hebben), ten opzichte van alle geregistreerde servers op het moment dat het rapport werd gegenereerd. **Niet beschermd**: het totale aantal niet-beschermde servers ten opzichte van alle geregistreerde servers op het moment dat het rapport werd gegenereerd.

Widget voor de preventie van gegevensverlies

Het volgende onderwerp bevat meer informatie over de geblokkeerde randapparaten in het gedeelte **Preventie van gegevensverlies**.

De widget toont het totale aantal geblokkeerde apparaten en het totale aantal geblokkeerde apparaten per apparaattype voor het opgegeven datumbereik.

- Verwisselbare opslag
- Versleuteld verwisselbaar

- Printers
- Klembord: omvat de apparaattypen Klembord en Schermopname.
- Mobiele apparaten
- Bluetooth
- Optische stations
- Diskettestations
- USB: omvat de apparaattypen USB-poort en Omgeleide USB-poort.
- FireWire
- Toegewezen stations
- Omgeleid klembord: omvat de apparaattypen Omgeleid klembord inkomend en Omgeleid klembord uitgaand.

De widget toont de eerste zeven apparaattypen met het hoogste aantal geblokkeerde apparaten, en combineert de rest van de apparaattypen in het apparaattype **Overige**.

Widgets voor File Sync & Share

De volgende tabel bevat informatie over de widgets in het gedeelte **File Sync & Share**.

Widget	Beschrijving
File Sync & Share-statistieken	De widget toont de volgende metrieken: **Totaal gebruikte cloudopslag**: het totale opslaggebruik van alle gebruikers. **Eindgebruikers**: het totale aantal eindgebruikers. **Gemiddeld gebruikte opslag per eindgebruiker**: het gemiddelde opslaggebruik per eindgebruiker. **Gastgebruikers**: het totale aantal gastgebruikers.
File Sync & Share-opslaggebruik door eindgebruikers	De widget toont het totale aantal File Sync & Share-eindgebruikers die een opslaggebruik hebben in de volgende bereiken: • 0 – 1 GB • 1 – 5 GB • 5 – 10 GB • 10 – 50 GB • 50 – 100 GB • 100 – 500 GB • 500 GB – 1 TB • 1+ TB

Widgets voor Notary

De volgende tabel bevat meer informatie over de widgets in het gedeelte **Notary**.

Widget	Beschrijving
Cyber Notary-statistieken	De widget toont de volgende Notary-metrieken: **Gebruikte cloudopslag voor Notary**: de totale grootte van de gebruikte opslag voor Notary-services. **Genotariseerde bestanden**: het totale aantal genotariseerde bestanden. **Elektronisch ondertekende documenten**: het totale aantal elektronisch ondertekende documenten en elektronisch ondertekende bestanden.
Genotariseerde bestanden van eindgebruikers	Geeft het totale aantal genotariseerde bestanden van alle eindgebruikers weer. De gebruikers worden gegroepeerd op basis van het aantal genotariseerde dat ze hebben. • Maximaal 10 bestanden • 11 – 100 bestanden • 101 – 500 bestanden • 501 – 1000 bestanden • 1000+ bestanden
Elektronisch ondertekende documenten van eindgebruikers	De widget toont het totale aantal elektronisch ondertekende documenten en elektronisch ondertekende bestanden van alle eindgebruikers. De gebruikers worden gegroepeerd op basis van het aantal elektronisch ondertekende documenten en bestanden dat ze hebben. • Maximaal 10 bestanden • 11 – 100 bestanden • 101 – 500 bestanden • 501 – 1000 bestanden • 1000+ bestanden

De instellingen van het overzichtsrapport configureren

U kunt de rapportinstellingen bijwerken die zijn geconfigureerd toen het overzichtsrapport werd gemaakt.

De instellingen van het overzichtsrapport bijwerken

1. Ga in de beheerconsole naar **Rapporten**>**Overzichtsrapport**.
2. Klik op de naam van het overzichtsrapport dat u wilt bijwerken.

3. Klik op **Instellingen**.
4. Wijzig de waarden van de velden zoals gewenst.
5. Klik op **Opslaan**.

Een overzichtsrapport maken

U kunt een overzichtsrapport maken, de inhoud ervan bekijken, de ontvangers van het rapport configureren en plannen wanneer het automatisch wordt verzonden.

Een overzichtsrapport maken

1. Ga in de beheerconsole naar **Rapporten**>**Overzichtsrapport**.
2. Klik op **Overzichtsrapport maken**.
3. Typ bij **Naam van rapport** de naam van het rapport.
4. Selecteer de ontvangers van het rapport.
   - Als u het rapport naar alle directe klanten wilt sturen, selecteert u **Verzenden naar alle directe klanten**.
   - Als u het rapport naar specifieke klanten wilt sturen
     a. Schakel het selectievakje **Verzenden naar alle directe klanten** uit.
     b. Klik op **Contacten selecteren**.
     c. Selecteer de specifieke klanten. U kunt de zoekfunctie gebruiken om gemakkelijk een specifiek contact te vinden.
     d. Klik op **Selecteren**.
5. Selecteer een bereik: **30 dagen** of **Deze maanden**
6. Selecteer een bestandsindeling: **PDF**, **Excel** of **Excel en PDF**.
7. Configureer de planningsinstellingen.
   - Als u het rapport op een bepaalde datum en tijd naar de ontvangers wilt sturen:
     a. Schakel de optie **Gepland** in.
     b. Klik op het veld **Dag van de maand**, wis het veld Laatste dag en klik op de datum die u wilt instellen.
     c. Geef in het veld **Tijd** de tijd op die u wilt instellen.
     d. Klik op **Toepassen**.
   - Als u het rapport wilt maken zonder het naar de ontvangers te sturen, schakelt u de optie **Gepland** uit.
8. Klik op **Opslaan**.

Het overzichtsrapport aanpassen

U kunt bepalen welke informatie in het overzichtsrapport moet worden opgenomen. U kunt secties toevoegen of verwijderen, widgets toevoegen of verwijderen, de naam van secties wijzigen, widgets aanpassen, en widgets en secties slepen en neerzetten om de volgorde te wijzigen waarin de informatie in het rapport wordt weergegeven.

Een sectie toevoegen

1. Klik op **Item toevoegen** > **Sectie toevoegen**.
2. Typ in het venster **Sectie toevoegen** een sectienaam of gebruik de standaard sectienaam.
3. Klik op **Toevoegen aan rapport**.

De naam van een sectie wijzigen

1. Klik in de sectie waar u de naam wilt wijzigen, op **Bewerken**.
2. Typ de nieuwe naam in het venster **Sectie bewerken**.
3. Klik op **Opslaan**.

Een sectie verwijderen

1. Klik in de sectie waar u wilt verwijderen, op **Sectie verwijderen**.
2. Klik in het bevestigingsvenster voor **Sectie verwijderen** op **Verwijderen**.

Een widget met standaardinstellingen toevoegen aan een sectie

1. Klik in de sectie waar u de widget wilt toevoegen, op **Widget toevoegen**.
2. Klik in het venster **Widget toevoegen** op de widget die u wilt toevoegen.

Een aangepaste widget toevoegen aan een sectie

1. Klik in de sectie waar u de widget wilt toevoegen, op **Widget toevoegen**.
2. Zoek in het venster **Widget toevoegen** naar de widget die u wilt toevoegen en klik op **Aanpassen**.
3. Configureer de velden indien nodig.
4. Klik op **Widget toevoegen**.

Een widget met standaardinstellingen toevoegen aan het rapport

1. Klik op **Item toevoegen** > **Widget toevoegen**.
2. Klik in het venster **Widget toevoegen** op de widget die u wilt toevoegen.

Een aangepaste widget toevoegen aan het rapport

1. Klik op **Widget toevoegen**.
2. Zoek in het venster **Widget toevoegen** naar de widget die u wilt toevoegen en klik op **Aanpassen**.
3. Configureer de velden indien nodig.
4. Klik op **Widget toevoegen**.

De standaardinstellingen van een widget herstellen

1. Klik in de widget die u wilt aanpassen, op **Bewerken**.
2. Klik op **Terugzetten naar standaardwaarden**.
3. Klik op **Gereed**.

Een widget aanpassen

1. Klik in de widget die u wilt aanpassen, op **Bewerken**.
2. Bewerk de velden zoals gewenst.
3. Klik op **Gereed**.

Overzichtsrapporten verzenden

U kunt een overzichtsrapport op aanvraag verzenden. In dit geval wordt de instelling **Planning** genegeerd en wordt het rapport onmiddellijk verzonden. Bij het verzenden van het rapport gebruikt het systeem de waarden voor Ontvangers, Bereik en Bestandsindeling die zijn geconfigureerd in **Instellingen**. U kunt deze instellingen handmatig wijzigen voordat u het rapport verzendt. Zie "De instellingen van het overzichtsrapport configureren" (p. 99) voor meer informatie.

Een overzichtsrapport verzenden

1. Ga in de beheerportal naar **Rapporten**>**Overzichtsrapport**.
2. Klik op de naam van het overzichtsrapport dat u wilt verzenden.
3. Klik op **Nu verzenden**.
   Het overzichtsrapport wordt automatisch verzonden naar de geselecteerde ontvangers.

5.20.4 Tijdzones in rapporten

De tijdzones die in rapporten worden gebruikt, zijn afhankelijk van het rapporttype. De volgende tabel bevat informatie ter referentie.

Locatie en type van het rapport	Tijdzone gebruikt in het rapport
Beheerportal> Overzicht> Bewerkingen (widgets)	De tijd waarop rapporten worden gemaakt, komt overeen met de tijdzone van de machine met de gebruikte browser.

Beheerportal> Overzicht> Bewerkingen (geëxporteerd naar PDF of xslx)	• De tijdstempel van het geëxporteerde rapport komt overeen met de tijdzone van de machine die is gebruikt om het rapport te exporteren. • De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC.
Beheerportal> Rapporten> Gebruik> Geplande rapporten	• Het rapport is gegenereerd op de eerste dag van de maand om 23:59:59 UTC. • Het rapport wordt verzonden op de tweede dag van de maand.
Beheerportal> Rapporten> Gebruik> Aangepaste rapporten	De tijdzone en datum van het rapport is UTC.
Beheerportal> Rapporten> Bewerkingen (widgets)	• De tijd waarop rapporten worden gemaakt, komt overeen met de tijdzone van de machine met de gebruikte browser. • De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC.
Beheerportal> Rapporten> Bewerkingen (geëxporteerd naar PDF of xslx)	• De tijdstempel van het geëxporteerde rapport komt overeen met de tijdzone van de machine die is gebruikt om het rapport te exporteren. • De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC.
Beheerportal> Rapporten> Bewerkingen (geplande levering)	• De tijdzone van de rapportlevering is UTC. • De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC.
Beheerportal> Gebruikers> Dagelijks overzicht van actieve waarschuwingen	• Dit rapport wordt één keer per dag verzonden tussen 10:00 en 23:59 UTC. Het tijdstip waarop het rapport wordt verzonden, is afhankelijk van de workload in het datacentrum. • De tijdzone van de activiteiten die in het rapport worden weergegeven, is UTC.
Beheerportal> Gebruikers> Statusmeldingen over cyberbeveiliging	• Dit rapport wordt verzonden wanneer een activiteit is voltooid. **Opmerking** Afhankelijk van de workload in het datacentrum kunnen sommige rapporten vertraagd worden verzonden. • De tijdzone van de activiteit in het rapport is UTC.

5.20.5 Gerapporteerde gegevens per type widget

Er zijn twee typen widgets op het dashboard, afhankelijk van het gegevensbereik dat ze weergeven:

- Widgets die actuele gegevens weergeven op het moment van browsen of het genereren van rapporten.
- Widgets die historische gegevens weergeven.

Wanneer u een datumbereik in de rapportinstellingen configureert om gegevens voor een bepaalde periode te dumpen, is het geselecteerde tijdbereik alleen van toepassing op widgets die historische gegevens weergeven. Voor widgets die actuele gegevens weergeven op het moment van browsen, is de parameter tijdbereik niet van toepassing.

In de volgende tabel worden de beschikbare widgets weergegeven, met de respectievelijke gegevensbereiken.

Naam van widget	Gegevens weergegeven in widget en rapporten
#CyberFit-score per machine	Actueel
5 meest recente waarschuwingen	Actueel
Gegevens van actieve waarschuwingen	Actueel
Overzicht van waarschuwingen activeren	Actueel
Activiteiten	Historisch
Activiteitenlijst	Historisch
Geschiedenis van waarschuwingen	Historisch
Antimalwarescan van back-ups	Historisch
Antimalwarescan van bestanden	Historisch
Back-upscangegevens (bedreigingen)	Historisch
Back-upstatus	Historisch: in de kolommen **Totaal aantal uitgevoerde bewerkingen** en **Aantal voltooide bewerkingen** Actueel: in alle andere kolommen
Opslaggebruik voor back-ups	Historisch
Geblokkeerde randapparaten	Historisch
Geblokkeerde URL's	Actueel
Cloudtoepassingen	Actueel
Beveiligingsstatus van workloads in de cloud	Actueel
Cyberbescherming	Actueel
Overzicht van cyberbescherming	Historisch
Overzicht van gegevensbescherming	Historisch
Apparaten	Actueel

Disaster Recovery - Servers getest	Historisch
Disaster Recovery-statistieken	Historisch
Gedetecteerde machines	Actueel
Overzicht van schijfintegriteit	Actueel
Status van schijfintegriteit	Actueel
Status van schijfintegriteit per fysiek apparaat	Actueel
Elektronisch ondertekende documenten van eindgebruikers	Actueel
Bestaande kwetsbaarheden	Historisch
File Sync & Share-statistieken	Actueel
File Sync & Share-opslaggebruik door eindgebruikers	Actueel
Hardwarewijzigingen	Historisch
Hardwaredetails	Actueel
Hardware-inventaris	Actueel
Overzicht van historische waarschuwingen	Historisch
Locatieoverzicht	Actueel
Ontbrekende updates per categorie	Actueel
Niet beschermd	Actueel
Genotariseerde bestanden van eindgebruikers	Actueel
Notary-statistieken	Actueel
Geschiedenis van patchinstallatie	Historisch
Status van patchinstallatie	Historisch
Overzicht van patchinstallatie	Historisch
Gepatchte beveiligingsproblemen	Historisch
Geïnstalleerde patches	Historisch
Beveiligingsstatus	Actueel
Onlangs beïnvloed	Historisch

Servers beschermd door Disaster Recovery	Actueel
Software-inventaris	Actueel
Softwareoverzicht	Historisch
Bedreigingen gedetecteerd door beschermingstechnologie	Historisch
Machines met beveiligingsproblemen	Actueel
Workloads waarvan een back-up is gemaakt	Historisch
Beveiligingsstatus van workloads	Actueel

5.21 Auditlogboek

Als u het auditlogboek wilt bekijken, klikt u op **Auditlogboek**.

Het auditlogboek geeft een chronologisch overzicht van de volgende gebeurtenissen:

- Bewerkingen uitgevoerd door gebruikers in de beheerportal
- Bewerkingen met cloud-to-cloud resources die door gebruikers worden uitgevoerd in de Cyber Protection-serviceconsole
- Systeemberichten over bereikte quota en quotagebruik

Het logboek bevat gebeurtenissen voor de tenant waarin u momenteel werkt, met de onderliggende tenants. U kunt op een gebeurtenis klikken als u meer informatie wilt zien.

Auditlogboeken worden opgeslagen in het datacenter en hun beschikbaarheid kan niet worden beïnvloed door problemen op machines van eindgebruikers.

Het logboek wordt dagelijks opgeschoond. De gebeurtenissen worden na 180 dagen verwijderd.

5.21.1 Velden van het auditlogboek

Het logboek bevat de volgende informatie voor elke gebeurtenis:

- **Gebeurtenis**
  Korte beschrijving van de gebeurtenis. Bijvoorbeeld: **Tenant is gemaakt**, **Tenant is verwijderd**, **Gebruiker is gemaakt**, **Gebruiker is verwijderd**, **Quotum is bereikt**, **Back-upinhoud is doorzocht**.
- **Ernstgraad**
  Kan een van de volgende waarden zijn:
  - **Fout**
    Geeft een fout aan.

- **Waarschuwing**
  Geeft een mogelijk negatieve actie aan. Bijvoorbeeld: **Tenant is verwijderd**, **Gebruiker is verwijderd**, **Quotum is bereikt**.
- **Kennisgeving**
  Geeft een gebeurtenis aan die mogelijk uw aandacht vereist. Bijvoorbeeld: **Tenant is bijgewerkt**, **Gebruiker is bijgewerkt**.
- **Informatie**
  Geeft neutrale informatie aan over een verandering of actie. Bijvoorbeeld: **Tenant is gemaakt**, **Gebruiker is gemaakt**, **Quotum is bijgewerkt**.

- **Datum**
  De datum en tijd waarop de gebeurtenis zich heeft voorgedaan.
- **Naam van object**
  Het object waarvoor de bewerking is uitgevoerd. Bijvoorbeeld: het object van de gebeurtenis **Gebruiker is bijgewerkt** is de gebruiker van wie de eigenschappen zijn gewijzigd. Voor gebeurtenissen die zijn gerelateerd aan een quotum, is het quotum het object.
- **Tenant**
  De naam van de tenant waarvan het object deel uitmaakt.
- **Initiator**
  De gebruikersnaam van de gebruiker die de gebeurtenis heeft geïnitieerd. Voor systeemberichten en gebeurtenissen die worden geïnitieerd door beheerders op het hoogste niveau, wordt **Systeem** gebruikt als waarde voor de initiator.
- **Tenant van initiator**
  De naam van de tenant waarvan de initiator deel uitmaakt. Voor systeemberichten en gebeurtenissen die worden geïnitieerd door beheerders op het hoogste niveau, wordt dit veld leeg gelaten.
- **Methode**
  Geeft aan of de gebeurtenis is geïnitieerd via de webinterface of via de API.
- **IP**
  Het IP-adres van de machine van waaraf de gebeurtenis is geïnitieerd.

5.21.2 Filteren en zoeken

U kunt de gebeurtenissen filteren op beschrijving, ernstgraad of datum. U kunt ook naar de gebeurtenissen zoeken per object, eenheid, initiator en eenheid van de initiator.

6 Geavanceerde scenario's

6.1 Een tenant verplaatsen naar een andere tenant

In de beheerportal kunt u een tenant verplaatsen van een bovenliggende tenant naar een andere bovenliggende tenant. Dit kan nuttig zijn als u een klant wilt overzetten naar een andere partner, of als u een maptenant hebt gemaakt om uw clients te organiseren en u enkele clients wilt verplaatsen naar de nieuwe maptenant.

6.1.1 Beperkingen

- Een partner/maptenant kan alleen worden verplaatst naar een partner/maptenant.
- Een klanttenant kan alleen worden verplaatst naar een partner/maptenant.
- Een eenheidtenant kan niet worden verplaatst.
- Een tenant kan alleen worden verplaatst als de bovenliggende doeltenant minstens net zoveel services en opties biedt als de oorspronkelijke bovenliggende tenant.
- Tenants kunnen slechts binnen één partneraccounthiërarchie worden verplaatst. Het verplaatsen van klanten tussen verschillende partneraccounthiërarchieën wordt niet ondersteund.
- Wanneer u een klanttenant verplaatst, moeten alle opslagruimten die aan de klanttenant zijn toegewezen in de oorspronkelijke bovenliggende tenant, ook bestaan in de bovenliggende doeltenant. Dit is vereist omdat aan de klantenservice gerelateerde gegevens niet naar een andere opslag kunnen worden verplaatst.

6.1.2 Een tenant verplaatsen

1. Meld u aan bij de beheerportal.
2. Ga naar het tabblad **Clients** en selecteer de doeltenant waarnaar u een tenant wilt verplaatsen.
3. Klik in het deelvenster voor tenanteigenschappen op de verticale ellips en klik vervolgens op **Id weergeven**.
4. Kopieer de tekenreeks die wordt weergegeven in het veld **Interne id** en klik op **Annuleren**.
5. Ga naar het tabblad **Clients** en selecteer de tenant die u wilt verplaatsen.
6. Klik in het deelvenster voor tenanteigenschappen op het verticale ellipsvormige pictogram en klik vervolgens op **Verplaatsen**.
7. Plak de interne id van de doeltenant en klik op **Verplaatsen**.

6.2 Een partnertenant converteren naar een maptenant en vice versa

In de beheerportal kunt u een partnertenant converteren naar een maptenant.

Dit kan handig zijn als u een partnertenant hebt gebruikt om items te groeperen en u nu uw tenant-infrastructuur op de juiste manier wilt organiseren. Dit is ook handig als u wilt dat het operationele dashboard samengevoegde informatie over de tenant bevat.

U kunt ook een maptenant converteren naar een partnertenant.

Opmerking
De conversie is een veilige bewerking en heeft geen gevolgen voor de gebruikers binnen de tenant en eventuele servicegerelateerde gegevens.

Een tenant converteren

1. Meld u aan bij de beheerportal.
2. Ga naar het tabblad **Clients** en selecteer de tenant die u wilt converteren.
3. Voer een van de volgende handelingen uit:
   - Klik op het ellipsvormige pictogram naast de naam van de tenant.
   - Selecteer de tenant en klik in het deelvenster voor tenanteigenschappen op het ellipsvormige pictogram.
4. Klik op **Converteren naar map** of **Converteren naar partner**.
5. Bevestig uw beslissing.

6.3 Toegang tot de webinterface beperken

Beheerders kunnen toegang tot de webinterface beperken door een lijst met IP-adressen op te geven die de leden van een tenant kunnen gebruiken om zich aan te melden.

Deze beperking is ook van toepassing op toegang tot de beheerportal via de API.

Deze beperking is alleen van toepassing op het niveau waar het is ingesteld. De beperking wordt *niet* toegepast op de leden van de onderliggende tenants.

Toegang tot de webinterface beperken

1. Meld u aan bij de beheerportal.
2. Navigeer naar de tenant waarvoor u de toegang wilt beperken.
3. Klik op **Instellingen** > **Beveiliging**.
4. Schakel de optie **Aanmeldingsbeheer** in.
5. Ga naar **Toegestane IP-adressen** en geef de toegestane IP-adressen op.
   U kunt de volgende parameters opgeven, gescheiden door puntkomma's:
   - IP-adres, bijvoorbeeld: 192.0.2.0
   - IP-bereik, bijvoorbeeld: 192.0.2.0-192.0.2.255
   - Subnetten, bijvoorbeeld: 192.0.2.0/24
6. Klik op **Opslaan**.

6.4 Toegang tot uw tenant beperken

Beheerders op klantniveau en hoger kunnen de toegang tot hun tenants beperken voor beheerders op een hoger niveau.

Als toegang tot de tenant is beperkt, kunnen beheerders van de bovenliggende tenant alleen de eigenschappen van de tenant wijzigen. Ze krijgen de accounts en onderliggende tenants niet te zien.

Voorkomen dat beheerders op hoger niveau toegang hebben tot uw tenant

1. Meld u aan bij de beheerportal.
2. Ga naar **Instellingen** > **Beveiliging**.
3. Schakel de optie **Toegang tot ondersteuning** uit.

Hierdoor hebben de beheerders van de bovenliggende tenants beperkte toegang tot uw tenant. Ze kunnen alleen de eigenschappen van de tenant wijzigen, maar hebben geen toegang tot items binnen de tenant (bijvoorbeeld tenants, gebruikers, services, back-ups en andere resources) en kunnen deze niet beheren.

Als de schakelaar **Toegang tot ondersteuning** is ingeschakeld, hebben de beheerders van de bovenliggende tenants volledige toegang tot uw tenant. Ze kunnen eigenschappen wijzigen; tenants, gebruikers en services beheren; en toegang krijgen tot back-ups en andere resources.

6.5 Integratie met externe systemen

Een serviceprovider kan Cyber Cloud integreren met een systeem van derden, als volgt:

- Door een platformuitbreiding te installeren in dit systeem.

  Op de **Integratiepagina** van de beheerportal vindt u een lijst met uitbreidingen die beschikbaar zijn voor de populairste Professional Services Automations (PSA)- en Remote Monitoring and Management (RMM)-systemen.

  Dit is de aanbevolen manier om het platform te integreren.
- Door een API-client voor het systeem te maken en zo het systeem toegang te geven tot de applicatieprogrammeerinterfaces (API's) van het platform en bijbehorende services. API-clients maken deel uit van het OAuth 2.0-autorisatieframework van het platform. Zie https://tools.ietf.org/html/rfc6749 voor meer informatie over OAuth 2.0.

  Dit is een manier op laag niveau om het platform te integreren en hiervoor zijn programmeervaardigheden vereist. We raden aan hiervoor te kiezen wanneer er geen platformuitbreiding voor het systeem is of wanneer het systeem moet worden aangepast voor gevallen van platform- en servicebeheer waarin de beschikbare uitbreiding niet voorziet.

6.5.1 Een uitbreiding instellen voor Cyber Cloud

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **Integratie**.

3. Klik op de naam van het externe systeem waarvoor u de integratie wilt inschakelen.
4. Volg de instructies op het scherm.

Meer informatie over integratie met systemen van derden is beschikbaar in het gedeelte 'Integratiereferenties' op https://www.acronis.com/en-us/support/documentation/.

6.5.2 API-clients beheren

Systemen van derden kunnen worden geïntegreerd met Cyber Cloud door gebruik te maken van de Application Programming Interfaces (API's). Toegang tot deze API's wordt ingeschakeld via API-clients, een integraal onderdeel van het OAuth 2.0-autorisatieframework van het platform.

Wat is een API-client?

Een API-client is een speciaal platformaccount dat is bedoeld om een systeem van derden te vertegenwoordigen dat moet worden geverifieerd en geautoriseerd om toegang te krijgen tot gegevens in de API's van het platform en de bijbehorende services.

De toegang van de client is beperkt tot een tenant, waarbij een beheerder de client en bijbehorende sub-tenants maakt.

Wanneer de client wordt gemaakt, worden hiervoor de servicerollen van het beheerdersaccount overgenomen en deze rollen kunnen later niet worden gewijzigd. Als de rollen van het beheerdersaccount worden gewijzigd of uitgeschakeld, heeft dit geen invloed op de client.

De clientreferenties bestaan uit de unieke identificatie (id) en de geheime waarde. De referenties verlopen niet en kunnen niet worden gebruikt om u aan te melden op de beheerportal of bij een serviceconsole. De geheime waarde kan opnieuw worden ingesteld.

Het is niet mogelijk tweeledige verificatie voor de client in te schakelen.

Typische integratieprocedure

1. Een beheerder maakt een API-client in een tenant die wordt beheerd door een systeem van derden.
2. De beheerder activeert de stroom van de OAuth 2.0-clientreferenties in het systeem van derden.
   Volgens deze stroom moet het systeem eerst de referenties van de gemaakte client naar het platform sturen met behulp van de autorisatie-API voordat toegang kan worden verkregen tot de tenant en bijbehorende services via de API. Het platform genereert en retourneert een beveiligingstoken (de unieke cryptische tekenreeks die aan deze specifieke client is toegewezen). Vervolgens moet het systeem dit token toevoegen aan alle API-aanvragen.
   Met een beveiligingstoken hoeft u geen clientreferenties meer door te geven bij de API-aanvragen. Voor extra veiligheid verloopt het token binnen twee uur. Daarna mislukken alle API-aanvragen met het verlopen token en moet het systeem een nieuw token aanvragen vanaf het platform.

Raadpleeg de handleiding voor ontwikkelaars op https://developer.acronis.com/doc/account-management/v2/guide/index voor meer informatie over het gebruik van de autorisatie- en platform-API's.

Een API-client maken

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients** > **API-client maken**.
3. Voer een naam in voor de API-client.
4. Klik op **Volgende**.
   De API-client wordt standaard gemaakt met de status **Actief**.
5. Kopieer en bewaar de id en de geheime waarde van de client en de datacenter-URL. U hebt ze nodig wanneer u de stroom van de OAuth 2.0-clientreferenties inschakelt in het systeem van derden.

   Belangrijk
   Om veiligheidsredenen wordt de geheime waarde slechts één keer weergegeven. Er is geen manier om deze waarde op te halen als u deze kwijtraakt. U kunt deze alleen opnieuw instellen.

6. Klik op **Gereed**.

De geheime waarde van een API-client opnieuw instellen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op en klik vervolgens op **Geheim opnieuw instellen**.
5. Bevestig uw beslissing door op **Volgende** te klikken.
   Er wordt een nieuwe geheime waarde gegenereerd. De client-id en datacenter-URL veranderen niet.
   Alle beveiligingstokens die aan deze client zijn toegewezen, verlopen onmiddellijk en API-aanvragen met deze tokens mislukken.
6. Kopieer en bewaar de nieuwe geheime waarde van de client.

   Belangrijk
   Om veiligheidsredenen wordt de geheime waarde slechts één keer weergegeven. Er is geen manier om deze waarde op te halen als u deze kwijtraakt. U kunt deze alleen opnieuw instellen.

7. Klik op **Gereed**.

Een API-client uitschakelen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op en vervolgens op **Uitschakelen**.
5. Bevestig uw beslissing.
   De status van de client verandert in **Uitgeschakeld**.
   API-aanvragen met beveiligingstokens die aan deze client zijn toegewezen, mislukken, maar de tokens zullen niet onmiddellijk verlopen. Het uitschakelen van de client heeft geen invloed op de vervaltijd van tokens.
   U kunt de client op elk gewenst moment opnieuw inschakelen.

Een uitgeschakelde API-client inschakelen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op en vervolgens op **Inschakelen**.
   De status van de client verandert in **Actief**.
   API-aanvragen met beveiligingstokens die aan deze client zijn toegewezen, lukken nog zolang deze tokens nog niet zijn verlopen.

Een API-client verwijderen

1. Meld u aan bij de beheerportal.
2. Klik op **Instellingen** > **API-clients**.
3. Zoek de gewenste client in de lijst.
4. Klik op en vervolgens op **Verwijderen**.
5. Bevestig uw beslissing.
   Alle beveiligingstokens die aan deze client zijn toegewezen, verlopen onmiddellijk en API-aanvragen met deze tokens mislukken.

Belangrijk
Er is geen manier om een verwijderde client te herstellen.

6.6 Integratie met VMware Cloud Director

Een serviceprovider kan VMware Cloud Director (voorheen VMware vCloud Director) integreren met Cyber Cloud om klanten een kant-en-klare back-upoplossing te bieden voor hun virtuele machines.

De integratie omvat de volgende stappen:

1. De RabbitMQ-berichtenbroker configureren voor de VMware Cloud Director-omgeving.
   Met RabbitMQ kunt u de wijzigingen in de VMware Cloud Director-omgeving synchroniseren met Cyber Cloud.
2. De plug-in voor VMware Cloud Director installeren.
   Met deze plug-in voegt u Cyber Protection toe aan de VMware Cloud Director-gebruikersinterface.
3. Een beheeragent implementeren.
   De beheeragent koppelt VMware Cloud Director-organisaties automatisch aan klanttenants in Cyber Cloud en organisatiebeheerders aan klanttenantbeheerders. Ga voor meer informatie over organisaties naar Een organisatie maken in VMware Cloud Director in de VMware Knowledge Base.
   De klanttenants worden gemaakt binnen de partnertenant waarvoor de VMware Cloud Director-integratie is geconfigureerd. Deze nieuwe klanttenants zijn in de modus **Vergrendeld** en kunnen niet worden beheerd door partnerbeheerders binnen Cyber Cloud.

   Opmerking
   Alleen organisatiebeheerders met unieke e-mailadressen in VMware Cloud Director worden gekoppeld aan Cyber Cloud.

4. Een of meer back-upagenten implementeren.
   De back-upagent biedt back-up- en herstelfunctionaliteit voor de virtuele machines in de VMware Cloud Director-omgeving.

Neem contact op met de technische ondersteuning om de integratie tussen VMware Cloud Director en Cyber Cloud uit te schakelen.

6.7 Beperkingen

- Integratie met VMware Cloud Director is alleen mogelijk voor partnertenants in de modus **Beheerd door serviceprovider** als de eventuele partnertenant ook de modus **Beheerd door serviceprovider** gebruikt. Zie "Een tenant maken" (p. 42) voor meer informatie over de typen tenants en de respectievelijke beheermodi.
  Alle bestaande directe partners kunnen de integratie met VMware Cloud Director configureren. Partnerbeheerders kunnen deze optie ook inschakelen voor subtenants door het selectievakje **VMware Cloud Director-infrastructuur in eigendom van partner** in te schakelen bij het maken van een onderliggende partnertenant.

- Tweeledige verificatie moet worden uitgeschakeld voor de partnertenant waarin de integratie met VMware Cloud Director wordt geconfigureerd.
- Een beheerder die de rol van organisatiebeheerder heeft in meerdere VMware Cloud Director-organisaties, kan back-up en herstel slechts voor één klanttenant beheren in Cyber Protection.
- De Cyber Protection-webconsole wordt geopend op een nieuw tabblad.

6.7.1 Softwarevereisten

Ondersteunde VMware Cloud Director-versies

- VMware Cloud Director 10.x

Ondersteunde webbrowsers

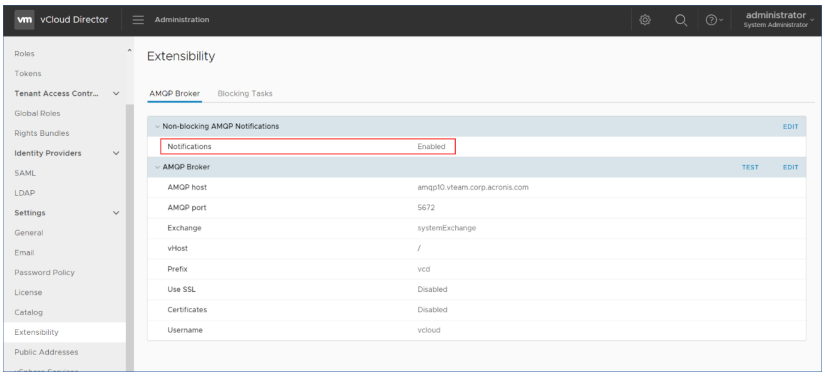
De Cyber Protection-webconsole ondersteunt de volgende webbrowsers:

- Google Chrome 29 of later
- Mozilla Firefox 23 of later
- Opera 16 of later
- Windows Internet Explorer 11 of later
- Microsoft Edge 25 of later
- Safari 8 of later uitgevoerd op de besturingssystemen macOS en iOS

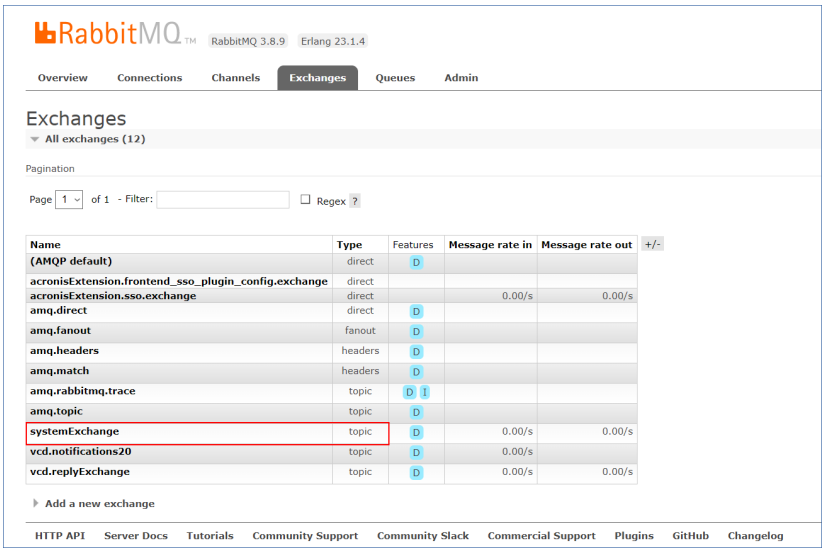
Het is mogelijk dat de gebruikersinterface in andere webbrowsers (inclusief Safari-browsers die worden uitgevoerd op andere besturingssystemen) niet goed wordt weergegeven of dat bepaalde functies niet beschikbaar zijn.

6.7.2 RabbitMQ-berichtenbroker configureren

1. Installeer een RabbitMQ AMQP-broker voor uw VMware Cloud Director-omgeving.
   Voor meer informatie over het installeren van RabbitMQ raadpleegt u de VMware-documentatie: Een RabbitMQ AMQP-broker installeren en configureren.
2. Meld u als systeembeheerder aan bij de portal van de VMware Cloud Director-provider.
3. Ga naar **Beheer** > **Uitbreidbaarheid**, ga naar **Niet-blokkerende AMQP-meldingen** en controleer of **Meldingen** zijn ingeschakeld.



4. Meld u als beheerder aan bij de RabbitMQ-beheerconsole.
5. Controleer op het tabblad **Uitwisselingen** of de uitwisseling (standaard met de naam **SystemExchange**) is gemaakt en het type **topic** heeft.



6.7.3 De plug-in voor VMware Cloud Director installeren

1. Klik op de volgende link om het bestand **vCDPlugin.zip** te downloaden: https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Meld u als systeembeheerder aan bij de portal van de VMware Cloud Director-provider.
3. Selecteer **Portal aanpassen in het navigatiemenu**.
4. Klik op het tabblad **Plug-ins beheren** op **Uploaden**.

   De wizard **Plug-in uploaden** wordt geopend.
5. Klik op **Plug-inbestand selecteren** en selecteer vervolgens het bestand **vCDPlugin.zip**.
6. Klik op **Volgende**.
7. Configureer het bereik en de publicatie:
   a. Schakel in het gedeelte **Aanpassen aan** alleen het selectievakje **Tenants** in.
   b. Selecteer in het gedeelte **Publiceren naar** de optie **Alle tenants** om de plug-in voor alle bestaande en toekomstige tenants in te schakelen, of selecteer afzonderlijke tenants waarvoor u de plug-in wilt inschakelen.

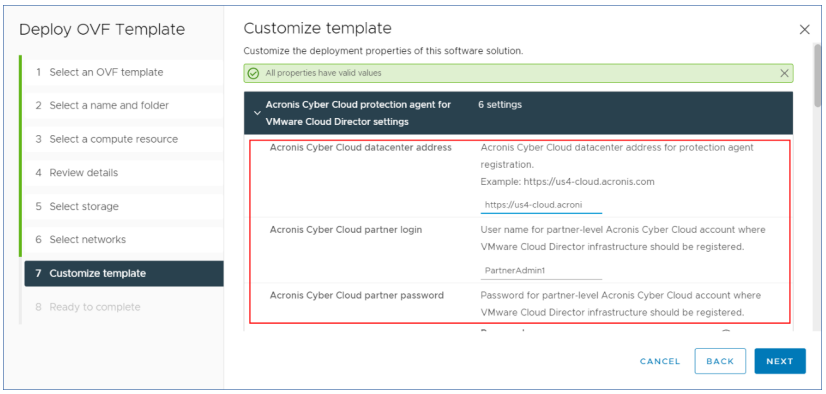
8. Klik op **Volgende**.
9. Controleer uw instellingen en klik vervolgens op **Voltooien**.

6.7.4 Een beheeragent installeren

1. Meld u als partnerbeheerder aan bij de Cyber Cloud-beheerportal.
2. Ga naar **Instellingen** > **Locatie** en klik vervolgens op **VMware Cloud Director toevoegen**.
3. Klik op de link **Beheeragent** en download het ZIP-bestand.
4. Pak het sjabloonbestand voor de beheeragent `vCDManagementAgent.ovf` en het bestand met de virtuele harde schijf `vCDManagementAgent-disk1.vmdk` uit.
5. Ga naar vSphere Client en implementeer de OVF-sjabloon voor de beheeragent op een ESXi-host voor een vCenter-exemplaar dat wordt beheerd door VMware Cloud Director.

   Belangrijk
   Installeer slechts één beheeragent per VMware Cloud Director-omgeving.

6. In de wizard **OVF-sjabloon implementeren** configureert u de beheeragent door het volgende in te stellen:



   a. URL van het Cyber Cloud-datacenter. Bijvoorbeeld: `https://us5-cloud.example.com`.
   b. Gebruikersnaam en wachtwoord van de partnerbeheerder.
   c. Id van de back-upopslag voor virtuele machines in de VMware Cloud Director-omgeving. Deze back-upopslag kan alleen eigendom zijn van een partner. Zie "Locaties en opslag beheren" (p. 63) voor meer informatie over opslagruimten.

      Als u de id wilt controleren, gaat u in de beheerportal naar **Instellingen** > **Locaties** en selecteert u de gewenste opslag. U kunt de id zien na het gedeelte **uuid=** in de URL.
   d. Cyber Cloud-factureringsmodus: **Per gigabyte** of **Per workload**.

      Opmerking
      De geselecteerde factureringsmodus is van toepassing op alle nieuwe klanttenants die worden gemaakt.

e. VMware Cloud Director-parameters: infrastructuuradres, gebruikersnaam van systeembeheerder en wachtwoord.

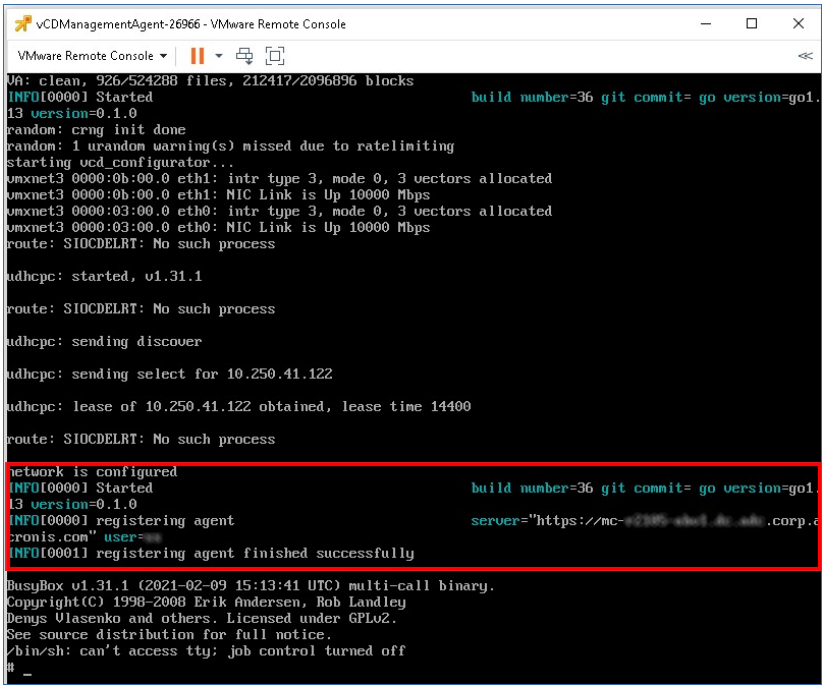
f. RabbitMQ-parameters: serveradres, poort, naam van virtuele host, gebruikersnaam van beheerder en wachtwoord.

g. Netwerkparameters: IP-adres, subnetmasker, standaardgateway, DNS, DNS-achtervoegsel. Standaard is slechts één netwerkinterface ingeschakeld. Als u een tweede netwerkinterface wilt inschakelen, schakelt u het selectievakje naast **Eth1 inschakelen** in.

> **Opmerking**
> Controleer in uw netwerkinstellingen of de beheeragent toegang heeft tot zowel de VMware Cloud Director-omgeving als uw Cyber Cloud-datacenter.

U kunt de instellingen van de beheeragent ook configureren na de eerste implementatie. In vSphere Client schakelt u de virtuele machine met de beheeragent uit en klikt u vervolgens op **Configureren** > **Instellingen** > **vApp-opties**. Pas de gewenste instellingen toe en schakel dan de virtuele machine met de beheeragent in.

7. [Optioneel] Open in vSphere Client de console van de virtuele machine met de beheeragent en controleer uw installatie.

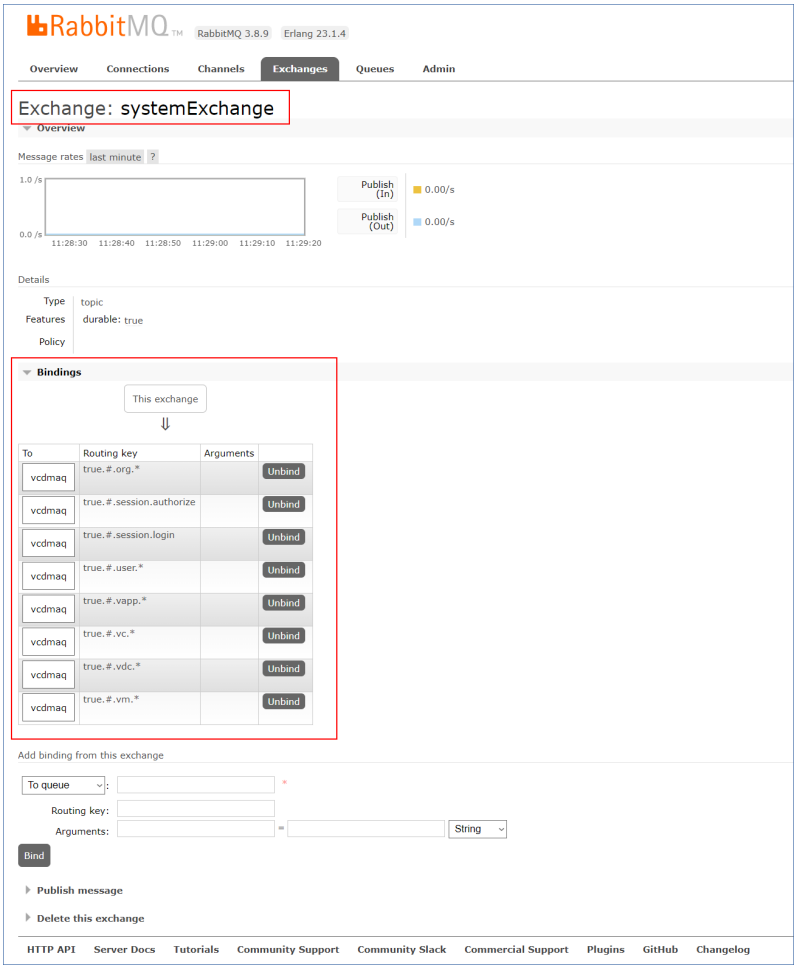


8. Controleer de RabbitMQ-verbinding.

a. Meld u als beheerder aan bij de RabbitMQ-beheerconsole.

b. Ga naar het tabblad **Uitwisselingen** en selecteer de uitwisseling die u hebt ingesteld tijdens de installatie van RabbitMQ. Standaard wordt de naam **systemExchange** gebruikt.

c. Controleer de bindingen met de **vcdmaq**-wachtrij.



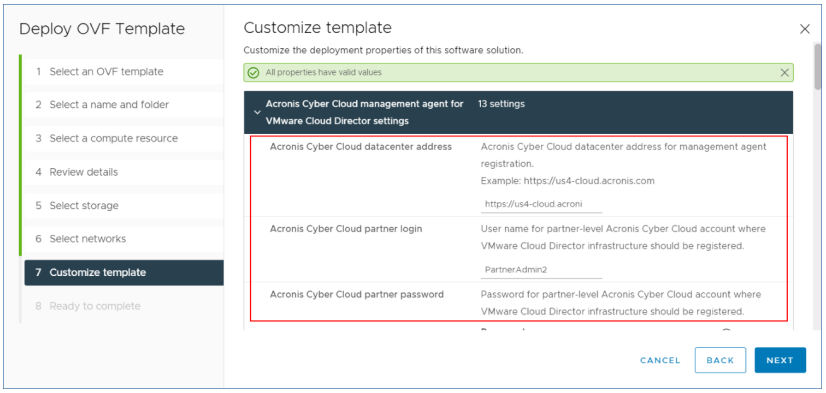
6.7.5 Back-upagenten installeren

1. Meld u als partnerbeheerder aan bij de beheerportal.
2. Ga naar **Instellingen** > **Locatie** en klik vervolgens op **VMware Cloud Director toevoegen**.
3. Klik op de link **Back-upagent** en download het ZIP-bestand.
4. Pak het sjabloonbestand voor de back-upagent `vCDCyberProtectAgent.ovf` en het bestand met de virtuele harde schijf `vCDCyberProtectAgent-disk1.vmdk` uit.
5. Ga naar vSphere Client en implementeer de sjabloon voor de back-upagent op de gewenste ESXi-host.

   U hebt minimaal één back-upagent per host nodig. Aan de back-upagent worden standaard 8 GB RAM en 2 CPU's toegewezen. De back-upagent kan tot 10 back-up- of hersteltaken tegelijk verwerken. Als u meer taken wilt verwerken of het back-up- en herstelverkeer wilt distribueren, implementeert u extra agenten op dezelfde host.

Opmerking
Back-ups van virtuele machines op ESXi-hosts waarop geen back-upagent is geïnstalleerd, mislukken met de fout 'Taaktime-out verlopen'.

6. In de wizard **OVF-sjabloon implementeren** configureert u de back-upagent door het volgende in te stellen:



   a. URL van het Cyber Cloud-datacenter. Bijvoorbeeld: `https://us5-cloud.example.com`.

   b. Gebruikersnaam en wachtwoord van de partnerbeheerder.

   c. VMware vCenter-parameters: serveradres, gebruikersnaam en wachtwoord.

      De agent zal deze referenties gebruiken om verbinding te maken met vCenter Server. We raden aan een account te gebruiken waaraan de rol **Beheerder** is toegewezen. Anders moet u een account met de nodige rechten beschikbaar maken op vCenter Server.

   d. Netwerkparameters: IP-adres, subnetmasker, standaardgateway, DNS, DNS-achtervoegsel.

      Standaard is slechts één netwerkinterface ingeschakeld. Als u een tweede netwerkinterface wilt inschakelen, schakelt u het selectievakje naast **Eth1 inschakelen** in.

      Opmerking
      Controleer in uw netwerkinstellingen of de back-upagent toegang heeft tot zowel vCenter Server als uw Cyber Cloud-datacenter.

   e. Downloadlimiet: de maximale downloadsnelheid (in kbps), waarmee de leessnelheid van het back-uparchief wordt bepaald tijdens de herstelbewerking. De standaardwaarde is 0 - onbeperkt.

   f. Downloadlimiet: de maximale downloadsnelheid (in kbps), waarmee de schrijfsnelheid van het back-uparchief wordt bepaald tijdens de back-upbewerking. De standaardwaarde is 0 - onbeperkt.

   U kunt de parameters voor het instellen van de back-upagent ook configureren na de eerste implementatie. In vSphere Client schakelt u de virtuele machine met de back-upagent uit en klikt u vervolgens op **Configureren** > **Instellingen** > **vApp-opties**. Pas de gewenste instellingen toe en schakel vervolgens de virtuele machine met de back-upagent in.

7. Controleer in vSphere Client of **Host** en **Storage vMotion** zijn uitgeschakeld voor de virtuele machine met de back-upagent.

6.7.6 De agenten bijwerken

Een beheeragent bijwerken

1. Meld u als partnerbeheerder aan bij de Cyber Cloud-beheerportal.
2. Ga naar **Instellingen** > **Locatie** en klik vervolgens op **VMware Cloud Director toevoegen**.
3. Klik op de link **Beheeragent** en download het ZIP-bestand met de nieuwste agent.
4. Pak het sjabloonbestand voor de beheeragent `vCDManagementAgent.ovf` en het bestand met de virtuele harde schijf `vCDManagementAgent-disk1.vmdk` uit.
5. Schakel in vSphere Client de virtuele machine met de huidige beheeragent uit.
6. Implementeer een virtuele machine met de nieuwe beheeragent door de nieuwste versies van de bestanden `vCDManagementAgent.ovf` en `vCDManagementAgent-disk1.vmdk` te gebruiken.
7. Configureer de beheeragent met dezelfde instellingen als in de oude.
8. [Optioneel] Verwijder de virtuele machine met de oude beheeragent.

Belangrijk
U kunt slechts één actieve beheeragent per VMware Cloud Director-omgeving hebben.

Een back-upagent bijwerken

1. Meld u als partnerbeheerder aan bij de Cyber Cloud-beheerportal.
2. Ga naar **Instellingen** > **Locatie** en klik vervolgens op **VMware Cloud Director toevoegen**.
3. Klik op de link **Back-upagent** en download het ZIP-bestand met de nieuwste agent.
4. Pak het sjabloonbestand voor de beheeragent `vCDCyberProtectAgent.ovf` en het bestand voor de virtuele harde schijf `vCDCyberProtectAgent-disk1.vmdk` uit.
5. Schakel in vSphere Client de virtuele machine met de huidige back-upagent uit.
   Alle back-up- en hersteltaken die op dat moment worden uitgevoerd, zullen mislukken. Als u wilt controleren of er taken worden uitgevoerd, opent u in vSphere Client de console van de virtuele machine met de back-upagent en voert u de volgende opdracht uit: `ps | grep esx_worker`. Controleer of er geen actieve `esx_worker`-processen zijn.
6. Implementeer een virtuele machine met de nieuwe back-upagent door de nieuwste versies van de bestanden `vCDCyberProtectAgent.ovf` en `vCDCyberProtectAgent-disk1.vmdk` te gebruiken.
7. Configureer de back-upagent met dezelfde instellingen als in de oude.
8. [Optioneel] Verwijder de virtuele machine met de oude back-upagent.

6.7.7 Toegang tot de Cyber Protection-webconsole

De volgende beheerders kunnen de back-up van virtuele machines beheren in VMware Cloud Director-organisaties:

- Organisatiebeheerders
- Specifiek toegewezen back-upbeheerders

  Zie "Een back-upbeheerder maken" (p. 122) voor meer informatie over het maken van een dergelijke beheerder.

Beheerders hebben toegang tot de aangepaste Cyber Protection-webconsole door te klikken op **Cyber Protection** in het navigatiemenu van de VMware Cloud Director-tenantportal.

Opmerking
De eenmalige aanmelding is alleen beschikbaar voor organisatiebeheerders en wordt niet ondersteund voor systeembeheerders die de VMware Cloud Director-tenantportal gebruiken.

In de Cyber Protection-webconsole hebben beheerders alleen toegang tot de elementen van de VMware Cloud Director-organisatie: virtuele datacenters, vApps en afzonderlijke virtuele machines. Ze kunnen de back-up en het herstel van de resources van de VMware Cloud Director-organisatie beheren.

Partnerbeheerders hebben toegang tot de Cyber Protection-webconsoles van hun klanttenants en kunnen back-up en herstel namens hen beheren.

Beperkingen

De lijst met beperkingen kan worden gewijzigd bij de komende releases van Cyber Cloud.

Back-up

- Alleen back-up van de hele machine wordt ondersteund. Bestandsfilters of opties voor het selecteren van schijven of volumes zijn niet beschikbaar.
- Alleen cloudopslag wordt ondersteund als back-uplocatie. De opslag wordt geconfigureerd in de instellingen van de beheeragent en gebruikers kunnen deze niet wijzigen in het beschermingsschema.
- Dynamische groepen worden niet ondersteund.
- De volgende back-upschema's worden ondersteund: **Altijd incrementeel (één bestand)**, **Altijd volledig** en **Wekelijks volledig, Dagelijks incrementeel**.
- Opschonen alleen na back-up wordt ondersteund.

Herstel

- Alleen herstel naar de oorspronkelijke virtuele machine wordt ondersteund. De oorspronkelijke virtuele machine moet bestaan in de VMware Cloud Director-omgeving.
- Herstel op bestandsniveau wordt niet ondersteund.

6.7.8 Een back-upbeheerder maken

Organisatiebeheerders kunnen het back-upbeheer delegeren aan specifiek toegewezen back-upbeheerders.

Een back-upbeheerder maken

1. Klik in de VMware Cloud Director-tenantportal op **Beheer** > **Rollen** > **Nieuw**.
2. Geef in het venster **Rol toevoegen** een naam en beschrijving op voor de nieuwe rol.
3. Blader door de lijst met machtigingen en selecteer vervolgens onder **Overige** de optie **Selfservice VM-back-upoperator**.

   Opmerking
   De machtiging **Selfservice VM-back-upoperator** is beschikbaar nadat u de plug-in voor VMware Cloud Director hebt geïnstalleerd. Zie "De plug-in voor VMware Cloud Director installeren" (p. 116) voor meer informatie over hoe u dit kunt doen.

4. Klik in de VMware Cloud Director-tenantportal op **Gebruikers**.
5. Selecteer een gebruiker en klik vervolgens op **Bewerken**.
6. Wijs deze gebruiker de nieuwe rol toe die u hebt gemaakt.

De geselecteerde gebruiker kan dan de back-ups voor de virtuele machines in deze organisatie beheren.

Opmerking
Systeembeheerders van de VMware Cloud Director-omgeving kunnen een globale rol definiëren waarvoor de machtiging **Selfservice VM back-upoperator** is ingeschakeld, en deze rol vervolgens publiceren naar de tenants. De organisatiebeheerders hoeven de rol dan alleen nog maar aan een gebruiker toe te wijzen.

6.7.9 Systeemrapport, logbestanden en configuratiebestanden

Voor het oplossen van problemen moet u mogelijk een systeemrapport maken met de tool `sysinfo`, of de logboek- en configuratiebestanden controleren op een virtuele machine met een agent.

U hebt rechtstreeks toegang tot de virtuele machine door de console in vSphere Client te openen, of op afstand via een SSH-client. Als u toegang wilt krijgen tot de virtuele machine via een SSH-client, moet u eerst de SSH-verbinding met deze machine inschakelen.

De SSH-verbinding met een virtuele machine inschakelen

1. Open in vSphere Client de console van de virtuele machine met de agent.
2. Voer op de opdrachtprompt de opdracht `/bin/sshd` uit om de SSH-daemon te starten.

U kunt dan verbinding maken met deze virtuele machine via een SSH-client zoals WinSCP.

De tool `sysinfo` uitvoeren

1. Krijg toegang tot de virtuele machine met de agent.
   - Voor rechtstreekse toegang opent u in vSphere Client de console van de virtuele machine.
   - Voor toegang op afstand maakt u verbinding met de virtuele machine via een SSH-client.

Gebruik de volgende standaardcombinatie voor gebruikersnaam:wachtwoord: `root`:`root`.

2. Ga naar de map `/bin` en voer vervolgens de tool `sysinfo` uit.

```
# cd /bin/
# ./sysinfo
```

Hierdoor wordt er een systeemrapportbestand opgeslagen in de standaardmap `/var/lib/Acronis/sysinfo`.

U kunt een andere map opgeven door de tool `sysinfo` uit te voeren met de optie `--target_dir`.

```
./sysinfo --target_dir path/to/report/dir
```

3. Download het gegenereerde systeemrapport via een SSH-client.

Toegang tot een logboek- of configuratiebestand

1. Maak verbinding met de virtuele machine via een SSH-client.
   Gebruik de volgende standaardcombinatie voor gebruikersnaam:wachtwoord: `root`:`root`.
2. Download het gewenste bestand.
   De logbestanden vindt u op de volgende locaties:
   - Back-upagent: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Beheeragent: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   De configuratiebestanden vindt u op de volgende locaties:
   - Back-upagent: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Beheeragent: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Index

S

T

U

V

W

Z