Cloud Cyber Protect

23.02

Guide de l'administrateur partenaire

RÉVISION : 28/02/2023

Table des matières

À propos de ce document

Ce document s'adresse aux administrateurs partenaires désireux d'utiliser Cloud Cyber Protect pour fournir des services à leur clientèle.

Ce document décrit comment configurer et gérer les services disponibles dans Cloud Cyber Protect à l'aide du portail de gestion.

À propos de Cyber Protect

Cyber Protect est une plate-forme cloud qui permet aux fournisseurs de services, revendeurs et distributeurs de délivrer des services de protection de données à leurs partenaires et clients.

Les services sont fournis à l'échelle des partenaires, des sociétés clientes et des utilisateurs finaux.

La gestion des services est disponible via des applications Web appelées **Consoles de services**. La gestion du locataire et du compte utilisateur est disponible via une application Web appelée **Portail de gestion**.

Le portail de gestion permet aux administrateurs de :

- Surveiller l'utilisation des services et accéder aux consoles de service
- Gérer les locataires
- Gérer les comptes utilisateur
- Configurer les services et quotas pour les locataires
- Gérer le stockage
- Gérer la marque
- Générer des rapports concernant l'utilisation des services

Services Cyber Protect

Cette section décrit les ensembles de fonctionnalités introduites en mars 2021 avec le nouveau modèle de facturation. Pour en savoir plus sur les avantages du nouveau modèle de facturation, consultez la fiche produit Cyber Protect.

Les ensembles de services et de fonctionnalités suivants sont disponibles dans Cloud Cyber Protect :

- **Cyber Protect**
  - **Protection** - cyberprotection complète avec fonctionnalités de sécurité et de gestion incluses dans la solution de base ; reprise d'activité après sinistre, sauvegarde et reprise, automatisation et sécurité des e-mails disponibles sous forme de fonctionnalités facturées en fonction de l'utilisation. Cette fonctionnalité peut être étendue grâce aux packs de protection avancée, qui sont soumis à des frais supplémentaires.
    Les packs de protection avancés sont des ensembles de fonctionnalités uniques qui répondent à des scénarios plus sophistiqués dans un domaine fonctionnel spécifique, par exemple Advanced Backup, Advanced Security et autres. Les packs avancés étendent la fonctionnalité disponible dans le service Cyber Protect standard.
    Pour en savoir plus sur les scénarios Advanced Protection, consultez "Packs de protection avancés" (p. 128).
  - **File Sync & Share** : une solution de partage sécurisé de contenu appartenant à l'entreprise, où que vous soyez, à n'importe quel moment, et sur n'importe quel appareil.

- **Envoi de données physiques** : une solution qui vous aide à gagner du temps et à réduire le trafic réseau grâce à l'envoi de données au centre de données du Cloud sur un disque dur.
- **Notary** : une solution basée sur la blockchain, qui garantir l'authenticité du contenu partagé.

- **SPLA Cyber Infrastructure**

Dans le portail de gestion, vous pouvez sélectionner le service et les ensembles de fonctionnalités qui seront disponibles à vos locataires. Cette configuration s'effectue par locataire, lorsque vous en provisionnez ou en modifiez un, comme décrit dans Création d'un locataire.

Méthodes de facturation pour Cyber Protect

Une méthode de facturation est un modèle de comptabilité et de facturation destiné à l'utilisation des services et de leurs fonctionnalités. La méthode de facturation détermine quelles unités seront utilisées comme base pour les calculs de prix. Les méthodes de facturation peuvent être configurées par le partenaire au niveau du client.

Le moteur de licences acquiert automatiquement les éléments selon les fonctionnalités demandées dans les plans de protection. Les utilisateurs peuvent optimiser le niveau de protection ainsi que le coût en personnalisant leurs plans de protection.

Remarque
Vous ne pouvez utiliser qu'un seul mode de facturation par tenant client.

Méthodes de facturation pour le composant Protection

Le Protection possède deux méthodes de facturation :

- Par charge de travail
- Par gigaoctet

L'ensemble des fonctionnalités des deux méthodes de facturation est identique.

Le service de protection des deux méthodes de facturation inclut des fonctionnalités de protection standard qui couvrent la majorité des risques de cybersécurité. Il est disponible aux utilisateurs sans frais supplémentaires. L'utilisation des fonctionnalités incluses sera comptabilisée, mais pas facturée. Pour obtenir une liste exhaustive des éléments inclus facturables, consultez "Services Cyber Protect" (p. 7).

Même si un pack avancé est activé pour un client, la facturation commence uniquement après qu'il a commencé à utiliser les fonctionnalités du pack dans le cadre d'un plan de protection. Lorsqu'une fonctionnalité avancée est appliquée dans un plan de protection, le moteur de licences attribue automatiquement la licence demandée à la charge de travail protégée.

Lorsque cette fonctionnalité avancée n'est plus utilisée, la licence est révoquée et la facturation s'arrête. Le moteur de licences attribue automatiquement la licence qui reflète la réelle utilisation des fonctionnalités.

Vous ne pouvez affecter des licences que pour les fonctionnalités du service Cyber Protect standard. Les fonctionnalités avancées sont facturées sur la base de l'utilisation et leurs licences ne peuvent pas être modifiées manuellement. Le moteur de licences attribue et annule l'attribution de ces licences automatiquement. Vous pouvez modifier manuellement le type de licence d'une charge de travail, mais elle sera réattribuée lorsque le plan de protection de cette charge de travail sera modifié par un utilisateur.

Remarque
La facturation des fonctionnalités de protection avancée ne commence pas au moment où vous les activez. Elle commence uniquement une fois que le client a commencé à utiliser les fonctionnalités avancées d'un plan de protection. Les ensembles de fonctionnalités activés seront comptabilisés et inclus dans des rapports d'utilisation, mais ne seront pas facturés, sauf si leurs fonctionnalités sont utilisées.

Méthodes de facturation pour File Sync & Share

File Sync & Share possède les méthodes de facturation suivantes :

- Par utilisateur
- Par gigaoctet

Vous pouvez également appliquer les règles de facturation de l'ancienne édition de File Sync & Share.

Remarque
La facturation des fonctionnalités Advanced File Sync & Share ne commence pas au moment où vous les activez. Elle commence uniquement une fois que le client a commencé à utiliser ses fonctionnalités avancées. L'ensemble de fonctionnalités avancées actives sera comptabilisé et inclus dans des rapports d'utilisation, mais ne sera pas facturé, sauf si ses fonctionnalités sont utilisées.

Facturation pour l'envoi de données physiques

La facturation pour l'envoi de données physiques suit le modèle de tarification en fonction de vos besoins.

Facturation pour Notary

La facturation pour Notary suit le modèle de tarification en fonction de vos besoins.

Utilisation des méthodes de facturation avec les anciennes éditions

Si vous n'avez pas encore migré vers le modèle de facturation en cours, utilisez les offres qui se trouvent dans l'une des méthodes de facturation pour remplacer les anciennes éditions. Le moteur de licences optimisera automatiquement les licences attribuées au client afin de minimiser le montant facturable.

Remarque
Les méthodes de facturation ne vous permettent pas de combiner les éditions.

Passer des anciennes éditions au modèle de licences actuel

Vous pouvez changer manuellement les offres pour vos tenants en modifiant leur profil et en sélectionnant les offres à leur place. Pour en savoir plus sur le processus de changement, consultez "Changer les éditions et les méthodes de facturation" (p. 10).

Pour passer des éditions aux méthodes de facturation pour plusieurs clients, consultez l'article Mass edition switch for multiple customers (67942).

Changer les éditions et les méthodes de facturation

Dans le portail de gestion, vous pouvez modifier le compte d'un tenant afin de changer les éléments entre les méthodes de facturation (pour passer du mode « par charge de travail » au mode « par gigaoctet » et vice-versa), et de passer d'une édition existante à une autre, et d'un mode de facturation à un autre.

Pour en savoir plus sur le changement en masse de tenants, consultez l'article Mass edition switch for multiple customers (67942).

Le processus de changement comporte les étapes suivantes.

1. Provisionner les nouveaux éléments vers un locataire client (activation des éléments et configuration des quotas) pour obtenir une correspondance avec la fonctionnalité disponible dans l'élément d'origine.
2. Annuler l'attribution des éléments non utilisés et attribuer les éléments à des charges de travail selon les fonctionnalités utilisées dans les plans de protection (réconciliation de l'utilisation).

Le tableau suivant illustre le processus dans les deux sens.

	Changement de direction	
	Édition > Méthodes de facturation	**Méthode de facturation > Méthode de facturation**
Changement des éléments	Activez les éléments pour remplir la fonctionnalité disponible dans l'édition source.	L'ensemble identique d'éléments sera activé.
Changement de quotas	Le quota sera répliqué depuis l'élément source vers les éléments de destination. Standard source → produit Standard de destination. Standard source → packs de destination.	Les quotas seront répliqués depuis l'élément source vers l'élément de destination.

	Changement de direction	
	Édition > Méthodes de facturation	**Méthode de facturation > Méthode de facturation**
	Remarque Si vous changez depuis une édition contenant des éditions secondaires (par exemple, « Cyber Protect (par charge de travail) »), les quotas seront résumés.	
Changement d'utilisation	Les éléments seront réattribués aux charges de travail sur la base des fonctionnalités demandées dans les plans de protection attribués sur ces charges de travail.	

Exemple : Passage de Cyber Protect Advanced Edition à la facturation par charge de travail

Dans ce scénario, un tenant client utilise l'édition Cyber Protect Advanced Edition, utilisée sur huit postes de travail, et le quota est défini sur dix charges de travail. Trois des postes de travail utilisent l'inventaire logiciel et la gestion des correctifs dans leurs plans de protection, deux y ont activé le filtrage d'URL, et l'une des machines utilise la protection continue des données. Le tableau suivant illustre la conversion de l'édition en nouveaux éléments.

Éléments source – utilisation/quota	Éléments de destination – utilisation/quota
Poste de travail Cyber Protect Advanced – 8/10	• Poste de travail – 8/10 • Advanced Security – 2/10 • Poste de travail Advanced Backup – 1/10 • Advanced Management – 3/10

Les étapes suivantes ont été exécutées lors du changement :

1. Les éléments qui couvrent la fonctionnalité disponible dans l'édition source ont été automatiquement activés.
2. Le quota a été répliqué sur les nouveaux éléments.
3. L'utilisation a été réconciliée en fonction de l'utilisation réelle dans les plans de protection : trois charges de travail utilisent les fonctionnalités du pack Advanced Management, deux utilisent des fonctionnalités du pack Advanced Security et une utilise les fonctionnalités du pack Advanced Backup.

Exemple : Cyber Protect par charge de travail vers facturation par charge de travail

Dans cet exemple, les charges de travail du client possèdent plusieurs éditions. Chaque charge de travail ne peut avoir qu'une seule édition ou une seule méthode de facturation attribuée.

Éléments source – utilisation/quota	Éléments de destination – utilisation/quota
Poste de travail Cyber Protect Essentials – 6/12	• Poste de travail – 14/42 • Poste de travail Advanced Backup – 2/42 • Advanced Security – 13/42 • Advanced Management – 5/42
Poste de travail Cyber Protect Standard – 5/10	
Poste de travail Cyber Protect Advanced – 2/10	
Poste de travail Cyber Backup Standard – 1/10	

Les étapes suivantes ont été exécutées lors du changement :

1. Les éléments qui couvrent la fonctionnalité disponible dans toutes les éditions sources ont été activés automatiquement. Grâce aux méthodes de facturation, plusieurs éléments peuvent être attribués à une charge de travail si besoin est.
2. Les quotas ont été résumés et répliqués.
3. L'utilisation a été réconciliée en fonction des plans de protection.

Changement de mode de facturation d'un tenant partenaire

Pour changer le mode de facturation d'un tenant partenaire

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le tenant partenaire pour lequel vous souhaitez changer de mode de facturation, cliquez sur l'icône en forme de points de suspension , puis cliquez sur **Configurer**.
3. Dans l'onglet **Cyber Protect**, sélectionnez le service pour lequel vous souhaitez changer de mode de facturation, puis cliquez sur **Modifier**.
4. Sélectionnez le mode de facturation souhaité, puis activez ou désactiver les éléments disponibles en fonction de vos besoins.
5. Cliquez sur **Enregistrer**.

Changement de mode de facturation d'un tenant client

Vous pouvez changer la facturation d'un tenant client :

- En modifiant le mode de facturation d'origine, en activant ou en désactivant des éléments.
- En passant à un nouveau mode de facturation complètement différent.

Pour plus d'informations sur la modification des éléments disponibles, consultez la section Activation ou désactivation d'éléments.

Pour changer le mode de facturation d'un tenant client

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le locataire client pour lequel vous souhaitez changer d'édition, cliquez sur l'icône en forme de points de suspension , puis cliquez sur **Configurer**.

3. Dans l'onglet **Configurer**, sous **Service**, sélectionnez le nouveau mode de facturation.
   Une boîte de dialogue s'affiche pour vous informer des conséquences du choix du nouveau mode de facturation.
4. Saisissez votre nom d'utilisateur pour confirmer votre choix.

Remarque
La prise en compte de cette modification peut prendre jusqu'à 10 minutes.

Gestion des éléments et des quotas

Cette section décrit les éléments suivants :

- Que sont les services et les éléments ?
- Comment les éléments sont-ils activés ou désactivés ?
- Que sont les méthodes de facturation ?
- Que sont les packs de protection avancés ?
- Que sont les anciennes éditions et les éditions secondaires ?
- Quels sont les quotas souples et durs ?
- Quand un quota dur peut-il être dépassé ?
- Qu'est-ce qu'une transformation du quota de sauvegarde ?
- Comment la disponibilité de l'élément affecte-t-elle la disponibilité de l'installateur dans la console de service ?

Services et éléments

Services

Un service Cloud est un ensemble de fonctionnalités hébergé par un partenaire ou sur le Cloud privé d'un client final. Les services sont généralement vendus en tant qu'abonnement ou sur une base de tarification en fonction de vos besoins.

Le service Cyber Protect intègre la cybersécurité, la protection des données et la gestion en vue de protéger vos terminaux, systèmes et données des menaces relatives à la cybersécurité. Le service Cyber Protect comprend plusieurs composants : Protection, File Sync & Share, Notary et l'envoi de données physiques. Certains peuvent être étendus avec des fonctionnalités avancées en utilisant les packs de protection avancés. Pour des informations détaillées concernant les fonctionnalités incluses et avancées, consultez "Services Cyber Protect" (p. 7).

Éléments

 Un élément est un ensemble de fonctionnalités de service regroupées par type de charge de travail ou de fonctionnalité spécifique, par exemple, stockage, infrastructure de reprise d'activité après sinistre et autres. En activant certains éléments spécifiques, vous déterminez les charges de travail

pouvant être protégées, la façon dont elles peuvent l'être (en définissant des quotas) et le niveau de protection disponible pour vos partenaires, vos clients et leurs utilisateurs finaux (en activant ou en désactivant les packs de protection avancés).

La fonctionnalité non activée sera masquée pour les clients et les utilisateurs, sauf si vous configurez un scénario de vente additionnelle. Pour en savoir plus sur les scénarios de vente additionnelle, consultez "Configuration de scénarios de vente additionnelle pour vos clients" (p. 68).

L'utilisation des fonctionnalités est recueillie dans les services et reflétée dans les éléments, puis utilisée dans les rapports et les facturations suivantes.

Méthodes de facturation et éditions

Les anciennes éditions vous permettent d'activer un élément par charge de travail. Les méthodes de facturation permettent de diviser les fonctionnalités, afin de pouvoir activer plusieurs éléments (fonctionnalités de service et packs avancés) par charge de travail, et ainsi mieux répondre aux besoins de vos clients et appliquer une facturation plus précise, uniquement pour les fonctionnalités que vos clients utilisent réellement.

Pour en savoir plus sur les méthodes de facturation pour Cyber Protect, consultez "Méthodes de facturation pour Cyber Protect" (p. 8).

Vous pouvez utiliser les méthodes de facturation ou les éditions pour configurer les services disponibles pour vos locataires. Vous pouvez sélectionner une méthode de facturation ou une édition par locataire client. Par conséquent, afin d'appliquer différentes méthodes de facturation à différentes fonctionnalités de service, vous devez créer plusieurs locataires par client. Par exemple, si le client souhaite que la méthode de facturation de ses boîtes aux lettres Microsoft 365 soit « par gigaoctet », et que celui de Teams soit « par charge de travail », vous devez créer deux clients locataires différents pour ce client.

Pour limiter l'utilisation des services dans un élément, vous pouvez définir des quotas pour cet élément. Consultez "Quotas souples et durs" (p. 15).

Activer ou désactiver des éléments

Vous pouvez activer tous les éléments disponibles pour une édition donnée ou une méthode de facturation, comme décrit dans la section Création d'un locataire.

Remarque
Désactiver tous les éléments d'un service ne désactive pas automatiquement le service.

Certaines limites à la désactivation des éléments sont énumérées dans le tableau ci-dessous.

Élément	Désactivation	Résultat
Stockage de sauvegarde	Peut être désactivé lorsque l'utilisation est égale à zéro.	Le stockage dans le Cloud n'est alors plus disponible en tant que destination au sein d'un locataire client.

Sauvegarde locale	Peut être désactivé lorsque l'utilisation est égale à zéro.	Le stockage local n'est alors plus disponible en tant que destination au sein d'un locataire client.
Sources de données (y compris Microsoft 365 et Google Workspace)	Peut être désactivé lorsque l'utilisation est égale à zéro.	La sauvegarde et la récupération des sources de données (y compris Microsoft 365 et Google Workspace) ne sont alors plus disponibles au sein d'un locataire client.
Tous les éléments de reprise d'activité après sinistre	Peut être désactivé lorsque l'utilisation est supérieure à zéro.	Pour plus de détails, voir la section « Quotas souples et durs ».
Tous les éléments Notary	Peut être désactivé lorsque l'utilisation est égale à zéro.	Le service Notary ne sera pas disponible au sein d'un locataire client.
Tous les éléments de File Sync & Share	Les éléments ne peuvent pas être activés ou désactivés séparément.	Le service de File Sync & Share ne sera pas disponible au sein d'un locataire client.
Tous les éléments d'envoi de données physiques	Peut être désactivé lorsque l'utilisation est égale à zéro.	Le service d'envoi de données physiques ne sera pas disponible au sein d'un locataire client.

Pour un élément qui ne peut pas être désactivé lorsque son utilisation est supérieure à zéro, vous pouvez supprimer l'utilisation manuellement, puis désactiver l'élément correspondant.

Quotas souples et durs

Les **quotas** vous permettent de limiter la capacité d'un locataire à utiliser le service. Pour définir les quotas, sélectionnez le client dans l'onglet **Clients**, sélectionnez l'onglet du service, puis cliquez sur **Modifier**.

Lorsqu'un quota est dépassé, une notification est envoyée à l'adresse e-mail de l'utilisateur. Si vous ne définissez pas de dépassement de quota, le quota est considéré comme « **souple** ». Cela signifie que les restrictions d'utilisation du service Cyber Protection ne sont pas activées.

Lorsque vous précisez un dépassement de quota, le quota est alors considéré comme « **dur** ». Un **dépassement** permet à un utilisateur de dépasser le quota, selon la valeur indiquée. Lorsque le dépassement est atteint, des restrictions sont appliquées à l'utilisation du service.

Exemple

Quota souple : Vous avez défini le quota des postes de travail sur 20. Lorsque le nombre de postes de travail protégés du client atteint 20, le client reçoit une notification par e-mail, mais le service Cyber Protection reste disponible.

Quota dur : Si vous avez défini le quota de postes de travail sur 20 et que le dépassement est de 5, votre client reçoit alors une notification par e-mail lorsque le nombre de postes de travail protégés atteint 20, et le service Cyber Protection est désactivé lorsque ce nombre atteint 25.

Lorsqu'un quota inconditionnel est atteint, le service est limité (il n'est pas possible de protéger une autre charge de travail ou d'utiliser davantage de stockage). Lorsque le quota inconditionnel est dépassé, une notification est envoyée à l'adresse e-mail de l'utilisateur.

Niveaux sur lesquels les quotas peuvent être définis

Les quotas peuvent être définis sur les niveaux répertoriés dans le tableau ci-dessous.

Locataire/Utilisateur	Quota souple (quota uniquement)	Quota dur (quota et dépassement)
Partenaire	oui	non
Dossier	oui	non
Client	oui	oui
Unité	non	non
Utilisateur	oui	oui

Les quotas souples peuvent être définis aux niveaux du partenaire et du dossier. Aucun quota ne peut être défini au niveau de l'unité. Les quotas durs peuvent être définis aux niveaux du client et de l'utilisateur.

Le montant total de quotas durs définis au niveau de l'utilisateur ne peut pas dépasser le quota client dur associé.

Configuration de quotas conditionnels et inconditionnels

Pour configurer des quotas pour vos clients

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le client pour lequel vous souhaitez configurer des quotas.
3. Sélectionnez l'onglet **Protection**, puis cliquez sur **Modifier**.
4. Sélectionnez le type de quota que vous souhaitez configurer. Par exemple, sélectionnez **Postes de travail** ou **Serveurs**.
5. Cliquez sur le lien **Illimité** à droite pour ouvrir la fenêtre **Modification du quota**.
   - Si vous souhaitez informer le client de l'existence du quota, mais ne souhaitez pas limiter sa capacité à utiliser le service, définissez la valeur de quota dans le champ **Quota conditionnel**. Le client recevra un e-mail de notification lorsqu'il atteindra le quota, mais le service Cyber Protection restera disponible.
   - Si vous souhaitez limiter la capacité du client à utiliser le service, sélectionnez **Quota inconditionnel** et définissez la valeur de quota dans le champ **Quota inconditionnel**.

Le client recevra un e-mail de notification lorsqu'il atteindra le quota et le service Cyber Protection restera disponible.

6. Dans la fenêtre **Modification du quota**, cliquez sur **Terminé**, puis cliquez sur **Enregistrer**.

Quotas de sauvegarde

Indiquez le quota de stockage dans le Cloud, le quota de sauvegarde au niveau local et le nombre maximum de machines/terminaux/sites Web qu'un utilisateur est autorisé à protéger. Les quotas suivants sont disponibles.

Quotas pour les périphériques

- **Postes de travail**
- **Serveurs**
- **Machines virtuelles**
- **Terminaux mobiles**
- **Serveurs d'hébergement Web** (Serveurs physiques et virtuels Linux qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager)
- **Sites Web**

Une machine, un périphérique ou un site Web sont considérés comme protégés tant qu'au moins un plan de protection leur est appliqué. Un terminal mobile devient protégé après la première sauvegarde.

Lorsque le dépassement du quota de périphériques est atteint, l'utilisateur ne peut plus activer de plans de protection sur d'autres périphériques.

Quotas pour les sources de données Cloud

- **Postes Microsoft 365**
  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion.
  Les licences des postes Microsoft 365 dépendent du mode de facturation sélectionné pour Cyber Protection.
  En mode de facturation **Par charge de travail**, le quota de **Postes Microsoft 365** est comptabilisé par utilisateurs uniques. Un utilisateur unique est un utilisateur qui dispose d'au moins l'un des éléments suivants :
  - Boîte aux lettres protégée
  - OneDrive protégé
  - Accès à au moins une ressource protégée de l'entreprise : Site Microsoft 365 SharePoint Online ou Microsoft 365 Teams.
    Pour apprendre à contrôler le nombre de membres d'un site Microsoft 365 SharePoint ou Teams, reportez-vous à cet article de la base de connaissances.

Remarque

Les utilisateurs Microsoft 365 bloqués qui ne disposent pas d'une boîte aux lettres personnelle protégée ou de OneDrive, et n'ont accès qu'à des ressources partagées (boîtes aux lettres partagées, sites SharePoint et Microsoft Teams) ne sont pas chargés.

Les utilisateurs bloqués sont ceux qui n'ont pas d'informations de connexion valides et ne peuvent pas accéder aux services Microsoft 365. Pour savoir comment bloquer tous les utilisateurs sans licence d'une organisation Microsoft 365, voir "Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter" (p. 20).)

Les postes Microsoft 365 suivants ne font pas l'objet d'une facturation et ne nécessitent pas de licence par poste :

- Boîtes aux lettres partagées
- Salles et équipement
- Utilisateurs externes avec accès aux sites SharePoint et/ou équipes Microsoft Teams sauvegardés

Pour plus d'informations sur les options de licence avec le mode de facturation par gigaoctet, reportez-vous à Cyber Protect Cloud: Microsoft 365 per GB licensing.

Pour plus d'informations sur les options de licence avec le mode de facturation par charge de travail, reportez-vous à Cyber Protect Cloud: Microsoft 365 licensing and pricing changes.

- **Microsoft 365 Teams**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des équipes Microsoft 365 Teams et définit le nombre maximum d'équipes pouvant être protégées. Pour la protection d'une équipe, quel que soit le nombre de membres ou de canaux, un quota est nécessaire. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion.

- **Microsoft 365 SharePoint Online**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des sites SharePoint Online et définit le nombre maximum de collections de sites et de sites de groupe pouvant être protégés.

  Les administrateurs de l'entreprise peuvent afficher le quota dans le portail de gestion. Ils peuvent également consulter le quota, ainsi que la quantité de stockage occupée par les sauvegardes SharePoint Online, dans les rapports d'utilisation.

- **Postes Google Workspace**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. L'entreprise peut être autorisée à protéger des boîtes aux lettres **Gmail** (y compris des agendas et des contacts), des fichiers **Google Drive** ou les deux. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion.

- **Drive partagé Google Workspace**

  Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des Drive partagés Google Workspace. Si le quota est activé, un nombre illimité de Drive partagés peut être protégé. Les administrateurs de l'entreprise ne

peuvent pas consulter le quota dans le portail de gestion, mais peuvent consulter la quantité de stockage occupée par les sauvegardes de Drive partagé dans les rapports d'utilisation.

La sauvegarde de Drive partagés Google Workspace n'est disponible que pour les clients qui disposent d'au moins un quota de postes Google Workspace en plus. Ce quota est uniquement vérifié et ne sera pas utilisé.

Un poste Microsoft 365 est considéré comme protégé si au moins un plan de protection est appliqué à la boîte aux lettres ou au OneDrive de l'utilisateur. Un poste Google Workspace est considéré comme protégé si au moins un plan de protection est appliqué à la boîte aux lettres ou au Google Drive de l'utilisateur.

Lorsque le dépassement du quota de postes est atteint, un administrateur d'entreprise ne peut plus activer de plans de protection sur d'autres postes.

Quotas pour le stockage

- **Sauvegarde locale**

  Le quota **Sauvegarde locale** limite la taille totale des sauvegardes locales créées à l'aide de l'infrastructure Cloud. Aucun dépassement ne peut être défini pour ce quota.
- **Ressources Cloud**

  Le quota de **ressources Cloud** combine le quota de stockage de sauvegarde et le quota de reprise d'activité après sinistre. Le quota de stockage des sauvegardes limite la taille totale des sauvegardes situées dans le stockage dans le Cloud. Lorsque le dépassement de quota de stockage de sauvegarde est dépassé, la sauvegarde échoue.

Dépassement du quota pour le stockage de sauvegarde

Le quota pour le stockage de sauvegarde ne peut pas être dépassé. Le certificat de l'agent de protection a un quota technique qui correspond au quota de sauvegarde du tenant + la surconsommation. Il n'est pas possible de lancer une sauvegarde si le quota est dépassé. Si le quota dans le certificat est atteint pendant la création de la sauvegarde, mais que la surconsommation n'est pas atteinte, alors la sauvegarde sera effectuée avec succès. Si la surconsommation est atteinte pendant la création de la sauvegarde, alors la sauvegarde échouera.

Exemple :

Un tenant d'utilisateur 1 To d'espace libre par rapport à son quota, et la surconsommation configurée pour cet utilisateur est de 5 To. L'utilisateur lance une sauvegarde. Si la taille de la sauvegarde créée est, par ex. de 3 To, la sauvegarde sera effectuée avec succès, car la surconsommation n'est pas dépassée. Si la taille de la sauvegarde créée est supérieure à 6 To, la sauvegarde échouera lorsque la surconsommation sera dépassée.

Transformation du quota de sauvegarde

En général, voici la façon dont fonctionne l'acquisition d'un quota de sauvegarde et le mappage d'un élément sur un type de ressource : le système compare les éléments disponibles avec le type de ressources, puis acquiert le quota pour l'élément correspondant.

Il existe également une capacité pour attribuer un autre quota d'élément, même s'il ne correspond pas exactement au type de ressource. Cela s'appelle une **transformation du quota de sauvegarde**. S'il n'existe pas d'élément correspondant, le système essaie de trouver un quota approprié plus cher pour le type de ressource (transformation de quota de sauvegarde automatique). Si rien d'approprié n'est trouvé, vous pouvez alors attribuer manuellement le quota de service au type de ressource dans la console de service.

Exemple

Vous souhaitez sauvegarder une machine virtuelle (poste de travail, basée sur un agent).

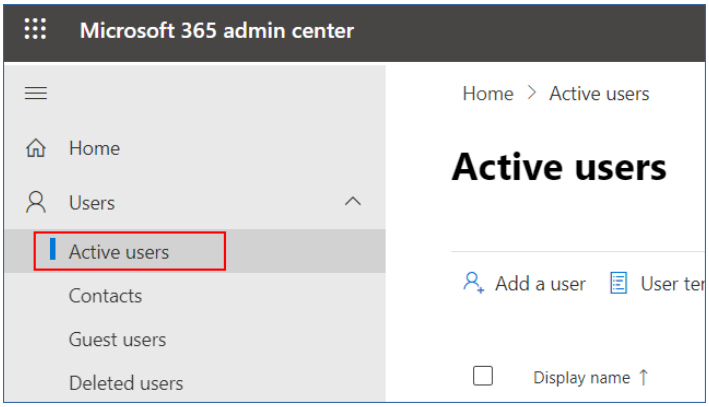
Premièrement, le système vérifiera s'il existe un quota de **machines virtuelles** attribué. Si aucun n'est trouvé, le système essaiera alors automatiquement d'acquérir le quota de **Postes de travail**. Si, encore une fois, aucun n'est trouvé, l'autre quota ne sera pas automatiquement acquis. Si vous disposez de suffisamment de quota plus cher que le quota de **machines virtuelles** et qu'il est applicable à une machine virtuelle, vous pouvez alors vous connecter à la console de service et attribuer le quota de **serveurs** manuellement.

Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter

Vous pouvez empêcher tous les utilisateurs sans licence de votre organisation Microsoft 365 de se connecter en modifiant leur statut de connexion.

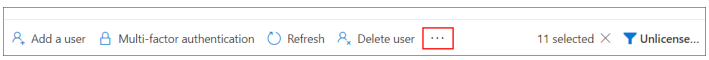
Pour empêcher les utilisateurs sans licence de se connecter

1. Connectez-vous au centre d'administration de Microsoft 365 (https://admin.microsoft.com) en tant qu'administrateur général.
2. Dans le menu de navigation, accédez à **Utilisateurs** > **Utilisateurs actifs**.



3. Cliquez sur **Filtre**, puis sélectionnez **Utilisateurs sans licence**.

4. Cochez les cases situées à côté des noms d'utilisateurs, puis cliquez sur l'icône en forme de points de suspension (...).



5. Dans le menu, sélectionnez **Modifier l'état de connexion**.
6. Cochez la case **Empêcher la connexion d'utilisateurs**, puis cliquez sur **Enregistrer**.

Quotas de reprise d'activité après sinistre

Remarque
Les éléments de reprise d'activité après sinistre ne sont disponibles qu'avec le module complémentaire de reprise d'activité après sinistre.

Ces quotas sont appliqués par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher les quotas et l'utilisation dans le portail de gestion, mais ne peuvent pas définir de quotas pour un utilisateur.

- **Stockage pour la reprise d'activité après sinistre**
  Le stockage de reprise d'activité après sinistre affiche la taille du stockage froid des serveurs protégés avec Disaster Recovery. Ce stockage est calculé à partir du moment où un serveur de restauration est créé, qu'il soit en cours d'exécution ou non. Si le quota est dépassé, il ne sera pas possible de créer des serveurs primaires et de restauration, ni d'ajouter/étendre des disques des serveurs primaires existants. Si le quota est dépassé, il ne sera pas possible d'initier un basculement ni de simplement démarrer un serveur arrêté. Les serveurs en cours d'exécution continuent à fonctionner.
- **Points de calcul**
  Ce quota limite les ressources processeur et les ressources RAM utilisées par les serveurs primaires et de restauration pendant une période de facturation. Si le quota est atteint, tous les serveurs primaires et de restauration sont coupés. Ces serveurs ne pourront plus être utilisés avant le début de la prochaine période de facturation. La période de facturation par défaut est un mois complet.
  Lorsque le quota est désactivé, les serveurs ne peuvent pas être utilisés, quelle que soit la période de facturation.
- **Adresses IP publiques**
  Ce quota limite le nombre d'adresses IP publiques qui peuvent être attribuées à des serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible d'activer des adresses IP publiques pour d'autres serveurs. Vous pouvez interdire à un serveur d'utiliser une adresse IP publique en désactivant la case à cocher **Adresse IP publique** dans les paramètres du serveur. Après cela, vous pouvez autoriser un autre serveur à utiliser une adresse IP publique, qui ne sera généralement pas la même.
  Lorsque le quota est désactivé, tous les serveurs cessent d'utiliser des adresses IP publiques et ne sont donc plus accessibles depuis Internet.
- **Serveurs Cloud**
  Ce quota limite le nombre total de serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible de créer des serveurs primaires ou de restauration.
  Lorsque le quota est désactivé, les serveurs sont visibles dans la console de service, mais seule l'option **Supprimer** est disponible.
- **Accès Internet**
  Ce quota active ou désactive l'accès à Internet à partir de serveurs primaires ou de restauration.

Lorsque ce quota est désactivé, les serveurs primaires ou de restauration ne peuvent pas établir de connexion à Internet.

Quotas pour la File Sync & Share

Vous pouvez définir les quotas suivants pour la File Sync & Share pour un locataire :

- **Utilisateurs**
  Le quota définit le nombre d'utilisateurs pouvant accéder à ce service.
  Les comptes administrateur ne sont pas comptabilisés dans ce quota.
- **Stockage dans le Cloud**
  Il s'agit d'un stockage dans le Cloud, destiné à stocker les fichiers des utilisateurs. Le quota définit l'espace alloué à un locataire dans le stockage dans le Cloud.

Quotas d'envoi de données physiques

Les quotas du service d'envoi de données physiques sont consommés sur une base par lecteur. Vous pouvez enregistrer les sauvegardes initiales de plusieurs machines sur un seul disque dur.

Vous pouvez définir les quotas suivants pour l'envoi de données physiques pour un locataire :

- **Vers le Cloud**
  Permet d'envoyer une sauvegarde initiale vers le centre de données du Cloud en utilisant un lecteur de disque dur. Ce quota définit le nombre maximum de lecteurs à transférer vers le centre de données du Cloud.

Quotas pour Notary

Vous pouvez définir les quotas suivants pour Notary pour un locataire :

- **Stockage Notary**
  Le stockage de notarisation est le stockage Cloud dans lequel sont stockés les fichiers notariés, les fichiers signés et ceux dont la notarisation ou la signature est en progrès. Ce quota définit l’espace maximum pouvant être occupé par ces fichiers.
  Pour réduire cette utilisation de quota, vous pouvez supprimer les fichiers déjà notariés ou signés du stockage de notarisation.
- **Notarisations**
  Ce quota définit le nombre maximal de fichiers pouvant être notariés à l’aide du service Notary. Un fichier est considéré comme notarié dès qu’il est transféré vers le stockage de notarisation et que son état de notarisation passe à En progrès.
  Si le même fichier est notarié plusieurs fois, chaque notarisation compte comme une nouvelle.
- **Signatures électroniques**
  Ce quota définit le nombre maximal de fichiers pouvant être signés à l’aide du service Notary. Un fichier est considéré comme signé dès qu’il est envoyé pour signature.

Modification du quota de service des ordinateurs

Le niveau de protection d'une machine est défini par le quota de service qui lui est appliqué.Les quotas de service concernent les éléments disponibles pour le locataire sur lequel la machine est enregistrée.

Un quota de service est affecté automatiquement lorsqu'un plan de protection est appliqué à une machine pour la première fois.

Le quota le plus approprié est attribué, en fonction du type de la machine protégée, de son système d'exploitation, du niveau de protection requis et de la disponibilité du quota. Si le quota le plus approprié n'est pas disponible dans votre organisation, le quota suivant dans la classification est attribué. Par exemple, si le quota le plus approprié est **Serveur d'hébergement Web**, mais n'est pas disponible, le quota **Serveur** est attribué.

Exemples d'affectation de quota :

- Une machine physique exécutant un système d'exploitation Windows Server ou Linux reçoit le quota **Serveur**.
- Une machine physique exécutant un système d'exploitation Windows pour ordinateur reçoit le quota **Poste de travail**.
- Une machine physique exécutant Windows 10 avec rôle Hyper-V activé reçoit le quota **Poste de travail**.
- Un ordinateur s'exécutant sur une infrastructure de poste de travail virtuel et dont l'agent de protection est installé à l'intérieur du système d'exploitation invité (par exemple, agent pour Windows), reçoit le quota **Machine virtuelle**. Ce type d'ordinateur peut également utiliser le quota **Poste de travail** si le quota **Machine virtuelle** n'est pas disponible.
- Un ordinateur s'exécutant sur une infrastructure de poste de travail virtuel et qui est sauvegardé en mode sans agent (par exemple, par l'agent pour VMware ou pour Hyper-V) reçoit le quota **Machine virtuelle**.
- Un serveur Hyper-V ou vSphere reçoit le quota **Serveur**.
- Un serveur avec cPanel ou Plesk reçoit le quota **Serveur d'hébergement Web**. Si le quota Serveur d'hébergement Web n'est pas disponible, il peut également utiliser le quota **Machine virtuelle** ou **Serveur** selon le type d'ordinateur sur lequel s'exécute le serveur Web.
- La sauvegarde reconnaissant les applications nécessite le quota **Serveur**, même pour un poste de travail.

Vous pourrez modifier manuellement l'attribution originale ultérieurement. Par exemple, pour appliquer un plan de protection plus avancé au même ordinateur, vous devez mettre à niveau le quota de service de l'ordinateur. Si les fonctionnalités requises par ce plan de protection ne sont pas prises en charge par le quota de service actuellement affecté, le plan de protection échouera.

Vous pouvez également modifier le quota de service si vous faites l'acquisition d'un quota plus approprié après l'affectation de celui d'origine. Par exemple, le quota **Poste de travail** est attribué

à une machine virtuelle. Après l'achat d'un quota **Machines virtuelles**, vous pouvez l'attribuer manuellement à cet ordinateur à la place du quota **Poste de travail** d'origine.

Vous pouvez également libérer le quota de service attribué, puis l'attribuer à un autre ordinateur.

Vous pouvez modifier le quota de service d'un ordinateur ou d'un groupe d'ordinateurs.

Pour changer le quota de service d'un ordinateur

1. Dans la console de services Cyber Protection, accédez à **Périphériques**.
2. Sélectionnez la machine souhaitée, puis cliquez sur **Détails**.
3. Dans la section **Quota de service**, cliquez sur **Modifier**.
4. Dans la fenêtre **Changer de licence**, sélectionnez le quota de service souhaité ou **Aucun quota**, puis cliquez sur **Modifier**.

Pour modifier le quota de service d'un groupe d'ordinateurs

1. Dans la console de services Cyber Protection, accédez à **Périphériques**.
2. Sélectionnez plusieurs ordinateurs, puis cliquez sur **Attribuer un quota**.
3. Dans la fenêtre **Changer de licence**, sélectionnez le quota de service souhaité ou **Aucun quota**, puis cliquez sur **Modifier**.

Dépendance aux éléments du programme d'installation de l'agent

En fonction des éléments autorisés, le programme d'installation de l'agent correspondant sera disponible dans la section **Ajouter des périphériques** de la console de service. Dans le tableau ci-dessous, vous pouvez voir les programmes d'installation de l'agent et leur disponibilité dans votre console de service, selon les éléments activés.

Élément désactivé **Programme d'installation de l'agent**	**Serveurs**	**Postes de travail**	**Machines virtuelles**	**Postes Microsoft 365**	**Postes Google Workspace**	**Terminaux mobiles**	**Serveurs d'hébergement Web**	**Sites Web**
Postes de travail – Agent pour Windows		+	+					+
Postes de travail – Agent pour Mac OS X		+	+					+
Serveurs –	+		+				+	+

Agent pour Windows								
Serveurs – Agent pour Linux	+		+				+	+
Agent pour Hyper-V			+					
Agent pour VMware			+					
Agent pour Virtuozzo			+					
Agent pour SQL	+		+					
Agent pour Exchange	+		+					
Agent pour Active Directory	+		+					
Agent pour Microsoft 365				+				
Agent pour Google Workspace					+			
Programme d'installation complet pour Windows	+	+	+				+	+
Mobile (iOS et Android)						+		

Utilisation du portail de gestion

Les étapes suivantes vous guideront à travers l'installation et l'utilisation de base du portail de gestion.

Navigateurs Web pris en charge

L'interface Web prend en charge les navigateurs suivants :

- Google Chrome 29 ou version ultérieure
- Mozilla Firefox 23 ou version ultérieure
- Opera 16 ou version ultérieure
- Microsoft Edge 25 ou version ultérieure
- Safari 8 ou version ultérieure s'exécutant sur les systèmes d'exploitation macOS et iOS

Il est possible que les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) n'affichent pas correctement l'interface utilisateur ou ne proposent pas certaines fonctions.

Activation du compte administrateur

Après avoir signé l'accord de partenariat, vous recevrez un e-mail contenant les informations suivantes :

- **Votre identifiant.** Nom d'utilisateur que vous utilisez pour vous connecter. Votre identifiant figure également sur la page d'activation du compte.
- Bouton **Activer le compte**. Cliquez sur le bouton et configurez le mot de passe de votre compte. Assurez-vous que le mot de passe contient au moins neuf caractères. Pour plus d'informations sur le mot de passe, reportez-vous à "Exigences relatives au mot de passe" (p. 26).

Exigences relatives au mot de passe

Le mot de passe d'un compte utilisateur doit comporter au moins 9 caractèresLa complexité des mots de passe est également vérifiée et les mots de passe sont classés dans les catégories suivantes :

- Faible
- Moyenne
- Fort

Vous ne pouvez pas enregistrer un mot de passe faible, même s'il contient 9 caractères ou plus. Les mots de passe qui contiennent le nom de l'utilisateur, l'identifiant, l'adresse e-mail de l'utilisateur ou le nom du tenant auquel le compte utilisateur appartient sont toujours considérés comme faibles. La plupart des mots de passe courants sont également considérés comme faibles.

Pour renforcer un mot de passe, ajoutez-lui des caractères. L'utilisation de différents types de caractères (chiffres, majuscules, minuscules et caractères spéciaux) n'est pas obligatoire, mais permet d'obtenir des mots de passe plus forts, mais aussi plus courts.

Accès au portail de gestion

1. Allez sur la page de connexion au service.
   L'adresse de la page de connexion apparaît dans l'e-mail d'activation que vous avez reçu.
2. Saisissez l'identifiant, puis cliquez sur **Suivant**.
3. Saisissez le mot de passe, puis cliquez sur **Suivant**.

   Remarque
   Afin d'éviter des attaques de force Cloud Cyber Protect, le portail verrouillera votre accès après 10 tentatives de connexion infructueuses. Le verrouillage dure 5 minutes. Le nombre de tentatives de connexion infructueuses est réinitialisé après 15 minutes.
4. Utilisez le menu à droite pour naviguer dans le portail de gestion.

Le délai d'expiration pour le portail de gestion est de 24 heures pour les sessions actives et d'une heure pour les sessions inactives.

Certains services comprennent la possibilité de passer au portail de gestion à partir de la console de service.

Configuration des contacts dans l'assistant Profil de l'entreprise

Vous pouvez configurer des informations de contact pour votre entreprise. Nous enverrons des mises à jour au sujet des nouvelles fonctionnalités et d'autres modifications importantes de la plate-forme aux contacts que vous fournirez.

Lorsque vous vous connectez au portail de gestion pour la première fois, l'assistant Profil de l'entreprise vous indique les informations de base à fournir concernant l'entreprise et les contacts.

Vous pouvez créer des contacts à partir d'utilisateurs qui existent dans la plate-forme Cyber Protect ou ajouter des informations de contact de personnes qui n'ont pas accès au service.

Pour configurer des contacts de l'entreprise à l'aide de l'assistant Profil de l'entreprise

1. Dans **Informations sur l'entreprise**, indiquez les détails suivants concernant votre entreprise :
   - **Nom officiel (juridique) de l'entreprise**
   - **Adresse juridique de l'entreprise (adresse du siège)**
     - **Pays**
     - **Code postal**
2. Cliquez sur **Suivant**.

3. Dans **Contacts de l'entreprise**, configurez les contacts pour les objectifs suivants :
   - **Contact de facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
   - **Contact professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.
   - **Contact technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.

   Vous pouvez utiliser un contact pour plusieurs objectifs.

   Sélectionnez une option pour créer le contact.
   - **Créer à partir d'un utilisateur existant**. Sélectionnez un utilisateur dans la liste déroulante.
   - **Créer un nouveau contact**. Fournissez les informations suivantes concernant le contact :
     - **Prénom** : prénom de la personne de contact. Ce champ est obligatoire.
     - **Nom** : nom de la personne de contact. Ce champ est obligatoire.
     - **Adresse e-mail professionnelle** : adresse e-mail de la personne de contact. Ce champ est obligatoire.
     - **Téléphone professionnel** : ce champ est facultatif.
     - **Titre** : ce champ est facultatif.
4. Si vous prévoyez d'utiliser également le Contact de facturation en tant que contact professionnel ou contact technique, sélectionnez les indicateurs correspondants dans la section **Contact de facturation** :
   - **Utiliser le même contact pour le contact professionnel**
   - **Utiliser le même contact pour le contact technique**
5. Cliquez sur **Valider**.

   En conséquence, les contacts sont créés. Vous pouvez modifier les informations et configurer d'autres contacts dans la section **Dirigeant(e)s de l'entreprise > Profil de l'entreprise** de la console de gestion, comme décrit dans Configuration des contacts de l'entreprise.

Accès à la console Cyber Protection à partir du portail de gestion

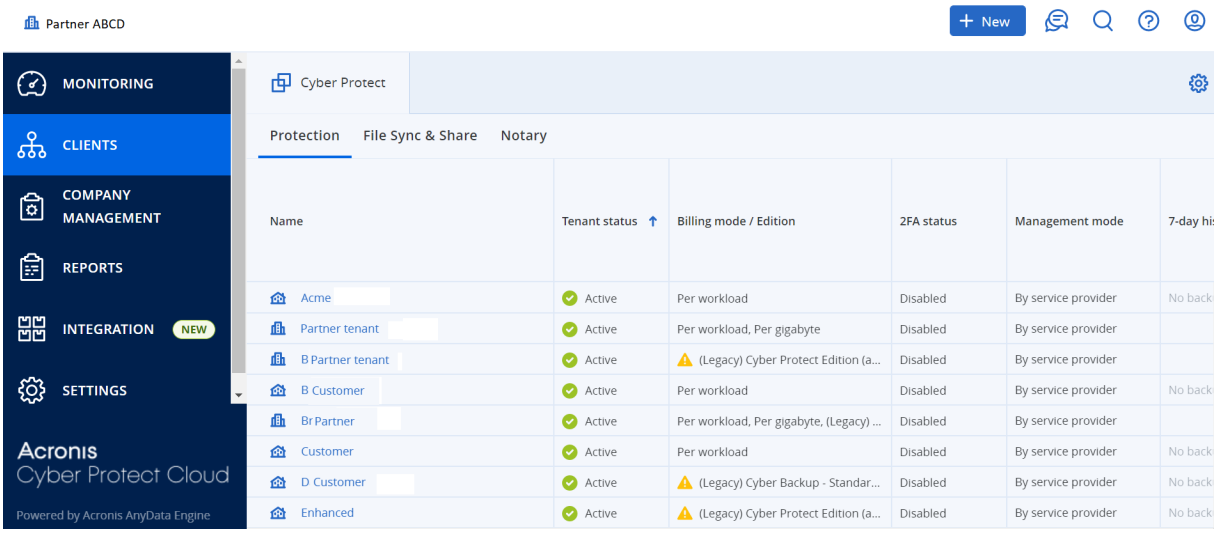
1. Dans le portail de gestion, accédez à **Surveillance** > **Utilisation**.
2. Sous **Cyber Protect**, sélectionnez **Protection**, puis cliquez sur **Gérer le service**.
   Vous pouvez aussi sélectionner un client sous **Clients**, puis cliquer sur **Gérer le service**.

Vous serez alors redirigé vers la console Cyber Protection.

Navigation dans le portail de gestion

Lorsque vous utilisez le portail de gestion, vous travaillez au sein d'un locataire à tout moment. Le nom de ce tenant est indiqué dans le coin supérieur gauche.

Le plus haut niveau de hiérarchie à votre disposition est sélectionné par défaut. Cliquez sur le nom d'un tenant pour explorer la hiérarchie. Pour revenir à un niveau supérieur, cliquez sur son nom dans le coin supérieur gauche.



Toutes les parties de l'interface utilisateur s'affichent et affectent uniquement le locataire dans lequel vous travaillez actuellement. Par exemple :

- L'onglet **Clients** affiche uniquement les locataires qui sont enfants directs du locataire dans lequel vous travaillez actuellement.
- L'onglet **Gestion d'entreprise** affiche le profil d'entreprise et les comptes utilisateur existant dans le tenant dans lequel vous travaillez actuellement.
- En utilisant le bouton **Nouveau**, vous pouvez créer un locataire ou un nouveau compte utilisateur uniquement dans le locataire dans lequel vous travaillez actuellement.

Limitation de l'accès à l'interface Web

Les administrateurs peuvent limiter l'accès à l'interface Web en indiquant une liste d'adresses IP à partir desquelles les membres d'un locataire sont autorisés à se connecter.

Cette restriction s'applique également à l'accès au portail de gestion via une API.

Cette restriction s'applique uniquement au niveau où elle est paramétrée. Elle ne s'applique *pas* aux membres des locataires enfants.

Pour limiter l'accès à l'interface Web

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire auquel vous souhaitez limiter l'accès.
3. Cliquez sur **Paramètres** > **Sécurité**.
4. Activez le commutateur **Contrôle de connexion**.
5. Dans **Adresses IP autorisées**, spécifiez les adresses IP autorisées.

Vous pouvez saisir n'importe quels paramètres suivants, séparés par des points virgules :

- Des adresses IP, par exemple : 192.0.2.0
- Des plages IP, par exemple : 192.0.2.0-192.0.2.255
- Des sous-réseaux, par exemple : 192.0.2.0/24

6. Cliquez sur **Enregistrer**.

Remarque
Pour les fournisseurs de services qui utilisent Cyber Infrastructure (modèle hybride) :

Si le commutateur **Contrôle de connexion** est activé sous **Paramètres** > **Sécurité** dans le portail de gestion, ajoutez l'adresse (ou les adresses) IP publique externe des nœuds Cyber Infrastructure à la liste **Adresses IP autorisées**.

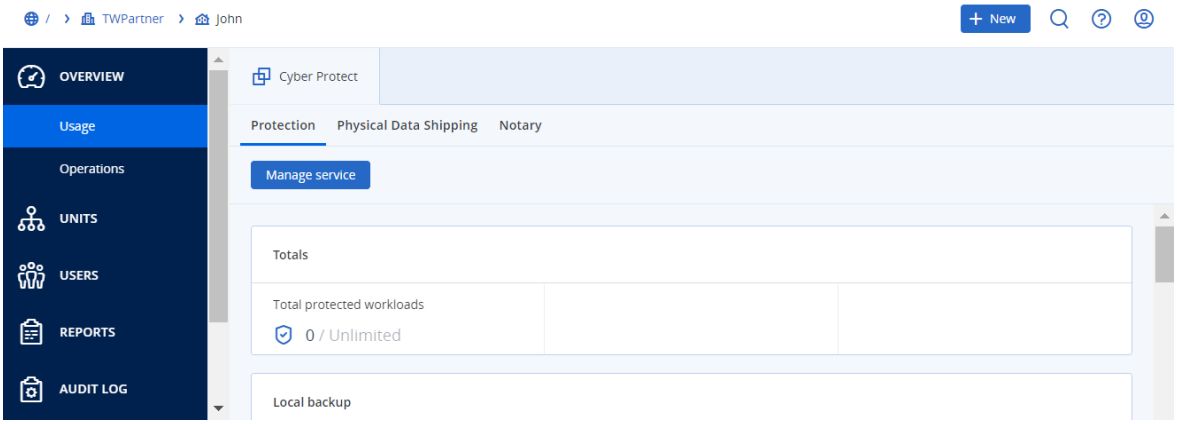
Accès aux services

Onglet Vue d'ensemble

La section **Vue d'ensemble** > **Utilisation** fournit une présentation de l'utilisation du service et vous permet d'accéder aux services au sein du locataire dans lequel vous travaillez.

Gérer un service pour un locataire à l'aide de l'onglet Vue d'ensemble

1. Naviguez vers le locataire pour lequel vous souhaitez gérer un service, puis cliquez sur **Vue d'ensemble** > **Utilisation**.
   Remarque : certains services peuvent être gérés au niveau du locataire parent et du locataire client, alors que d'autres services ne peuvent être gérés qu'au niveau du locataire client.
2. Cliquez sur le nom du service que vous souhaitez gérer, puis cliquez sur **Gérer le service** ou sur **Configurer le service**.
   Pour obtenir des informations concernant l'utilisation des services, consultez les guides de l'utilisateur disponibles dans les consoles de service.

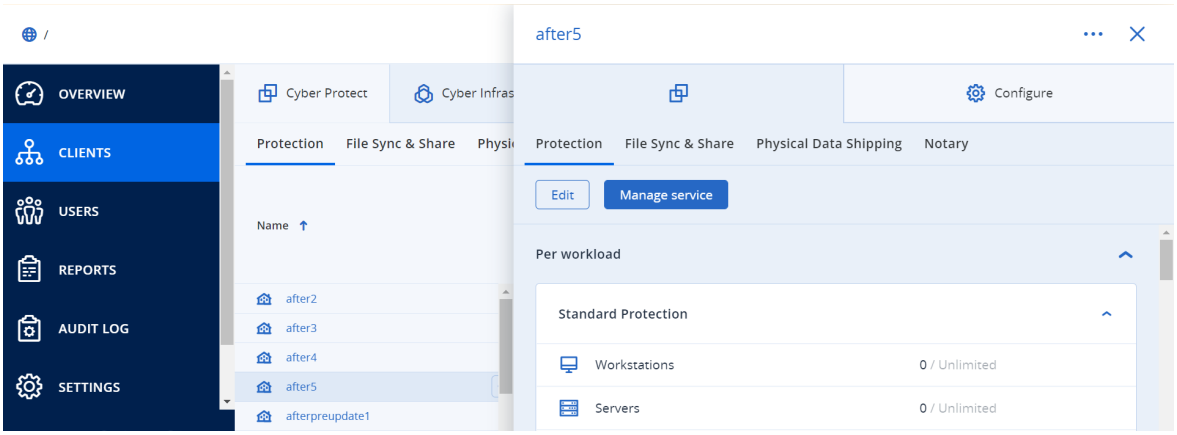


Onglet Clients

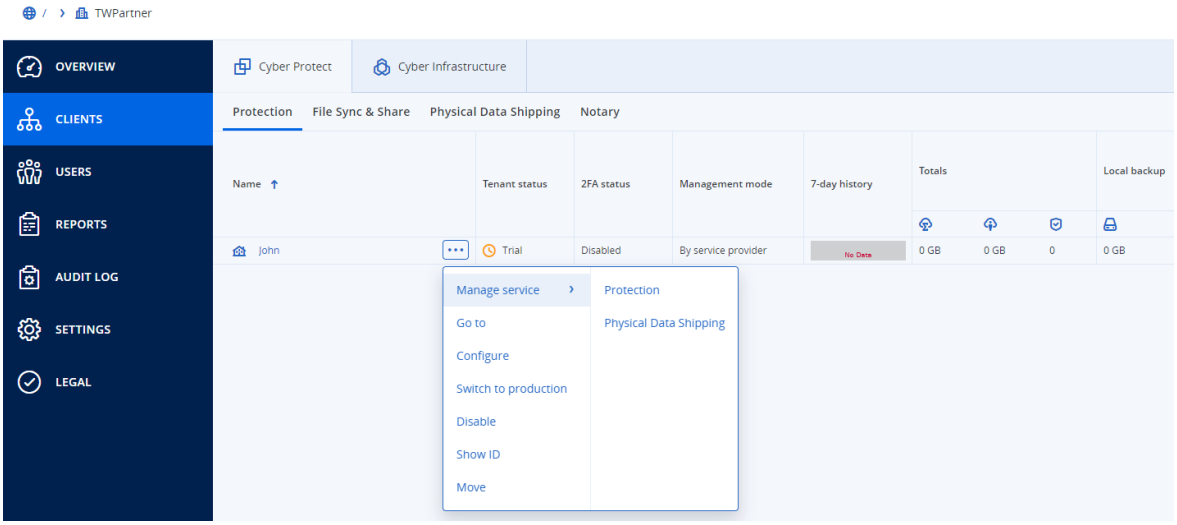
L'onglet **Clients** affiche les locataires enfants du locataire dans lequel vous travaillez et vous permet d'accéder aux services de ce locataire.

Gérer un service pour un locataire à l'aide de l'onglet Clients

1. Effectuez l'une des actions suivantes :
   - Cliquez sur **Clients**, sélectionnez le locataire pour lequel vous souhaitez gérer un service, cliquez sur le nom ou sur l'icône du service que vous souhaitez gérer, puis cliquez sur **Gérer le service** ou sur **Configurer le service**.



   - Cliquez sur **Clients**, cliquez sur l'icône en forme de points de suspension à côté du nom du locataire pour lequel vous souhaitez gérer un service, cliquez sur **Gérer le service**, puis sélectionnez le service que vous souhaitez gérer.



Remarque : certains services peuvent être gérés au niveau du locataire parent et du locataire client, alors que d'autres services ne peuvent être gérés qu'au niveau du locataire client.

Pour obtenir des informations concernant l'utilisation des services, consultez les guides de l'utilisateur disponibles dans les consoles de service.

Barre Historique de 7 jours

À l'écran **Clients**, la barre **Historique de 7 jours** montre l'état des sauvegardes de charge de travail pour chaque tenant client au cours des sept derniers jours. La barre est divisée en 168 lignes colorées. Chaque barre représente un intervalle d'une heure et affiche le pire état d'une sauvegarde dans l'intervalle d'une heure correspondant.

Le tableau suivant fournit des informations sur la signification de chaque couleur de ligne.

Couleur	Description
Rouge	Échec d'au moins une sauvegarde lors de la période d'une heure
Orange	Réussite d'au moins une sauvegarde avec un avertissement lors de la période d'une heure, mais sans erreur de sauvegarde
vert	Réussite d'au moins une sauvegarde lors de la période d'une heure, sans avertissement ni erreur de sauvegarde
Gris	Aucune sauvegarde effectuée lors de la période d'une heure

La barre **Historique de 7 jours** affiche le message « Aucune sauvegarde » jusqu'à ce que les statistiques correspondantes soient recueillies.

Pour les tenants partenaires, la barre **Historique de 7 jours** est vide, car l'agrégation des statistiques n'est pas prise en charge.

Comptes utilisateur et locataires

Il existe deux types de comptes utilisateur : les comptes administrateur et les comptes utilisateur.

- Les **administrateurs** ont accès au portail de gestion. Ils possèdent le rôle d'administrateur dans tous les services.
- Les **utilisateurs** n'ont pas accès au portail de gestion. Leur accès aux services et leurs rôles dans ces services sont définis par un administrateur.

Chaque compte fait partie d'un locataire. Un locataire est une partie des ressources (tel que des comptes utilisateur et des locataires enfants) et des offres de service (les services et éléments activés en son sein) d'un portail de gestion, dédiée à un partenaire ou à un client. La hiérarchie établie dans le locataire est supposée correspondre aux relations entre client et distributeur parmi les utilisateurs du service et leurs fournisseurs.

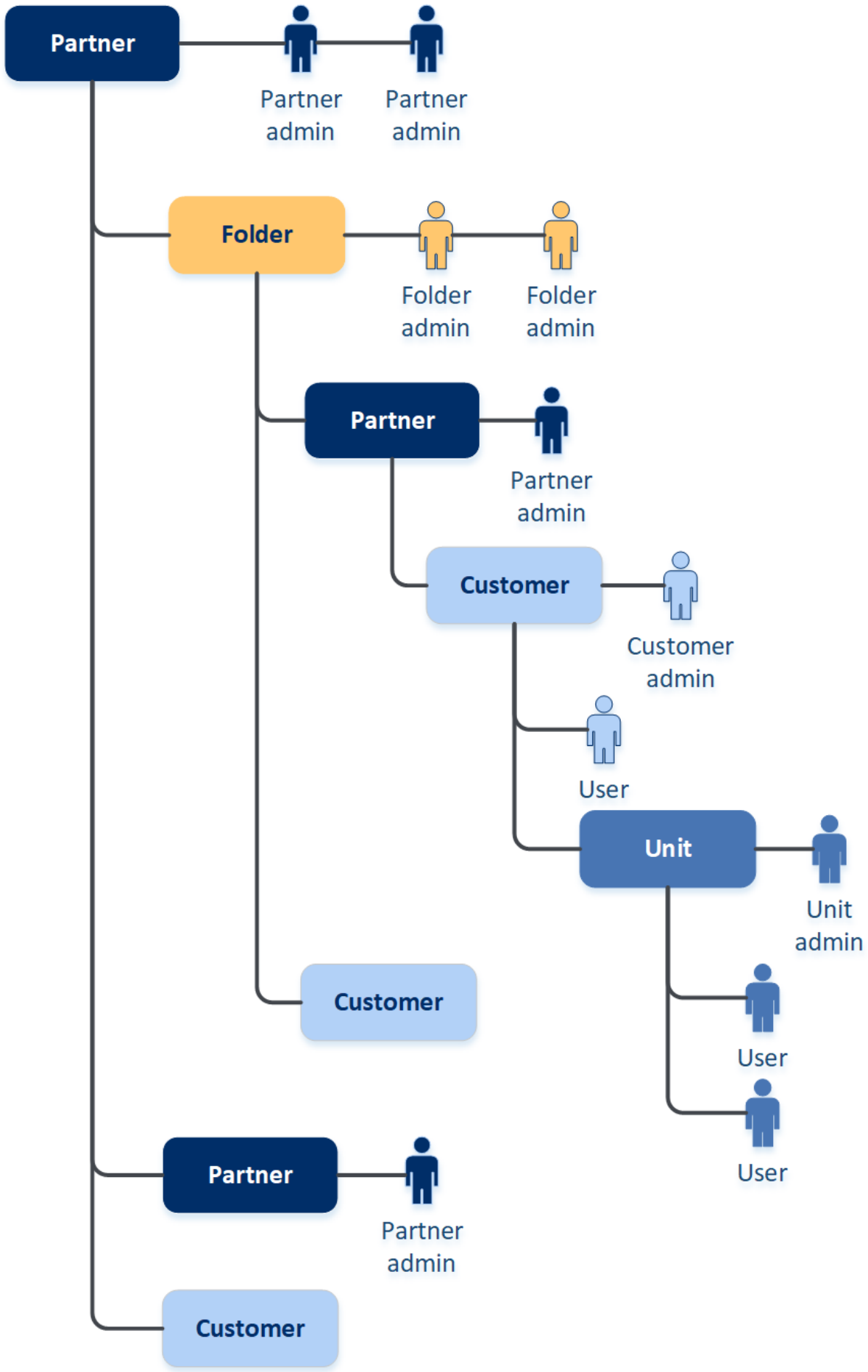
- Un type de locataire **partenaire** correspond généralement aux fournisseurs de service revendant les services.
- Un type de locataire **dossier** est un locataire complémentaire généralement utilisé par des administrateurs partenaires pour regrouper des partenaires et des clients afin de configurer des offres séparées et/ou des marques différentes.
- Un type de locataire **client** correspond généralement aux organisations qui utilisent les services.

- Un type de locataire **unité** correspond généralement aux unités ou départements au sein de l'organisation.

Un administrateur peut créer et gérer des locataires, des comptes administrateur et des comptes utilisateur de même niveau ou hiérarchiquement inférieurs.

Un administrateur du locataire parent de type **Partenaire** peut servir d'administrateur de niveau inférieur dans les locataires de type **Client** ou **Partenaire**, dont le mode de gestion est **Géré par le fournisseur de services**. Par conséquent, l'administrateur de niveau partenaire peut, par exemple, gérer des comptes utilisateur et des services, ou accéder à des sauvegardes et autres ressources dans le locataire enfant. Toutefois, les administrateurs de niveau inférieur peuvent limiter l'accès des administrateurs de niveau supérieur à leur locataire.

Le diagramme ci-dessous présente un exemple de hiérarchie des locataires partenaire, dossier, client et unité.


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

Le tableau ci-dessous résume les opérations pouvant être effectuées par les administrateurs et les utilisateurs.

Opération	Utilisateurs	Administrateurs de clients et d'unités	Administrateurs partenaire et dossier
Créez des locataires	Non	Oui	Oui
Créer des comptes	Non	Oui	Oui
Téléchargez et installez le logiciel	Oui	Oui	Non*
Gérer les services	Oui	Oui	Oui
Créer des rapports concernant l'utilisation du service	Non	Oui	Oui
Configurez la marque	Non	Non	Oui

*Un administrateur partenaire devant effectuer ces opérations peut se créer un compte d'administrateur de client ou d'utilisateur.

Gestion des tenants

Les locataires suivants sont disponibles dans Cyber Protect :

- Un locataire **Partenaire** est normalement créé pour chaque partenaire ayant signé l'accord de partenariat.
- Un locataire **Dossier** est normalement créé pour regrouper des partenaires et des clients afin de configurer des offres séparées et/ou des marques différentes.
- Un locataire **Client** est normalement créé pour chaque organisation ayant contracté un service.
- Un locataire **Unité** est créé dans un locataire client existant lorsque vous étendez le service à une nouvelle unité d'organisation.

Les étapes de création et de configuration d'un locataire varient en fonction du locataire créé. Cependant, le processus consiste en général à suivre les étapes ci-dessous :

1. Créer le locataire.
2. Sélectionner des services pour le locataire.
3. Configurer les éléments pour le locataire.

Création d'un locataire

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire dans lequel vous souhaitez créer un locataire.
3. Dans l'angle supérieur droit, cliquez sur **Nouveau**, puis cliquez sur l'un des éléments suivants, selon le type de tenant que vous souhaitez créer :

- Un locataire **Partenaire** est normalement créé pour chaque partenaire ayant signé l'accord de partenariat.
- Un locataire **Dossier** est normalement créé pour regrouper des partenaires et des clients afin de configurer des offres séparées et/ou des marques différentes.
- Un locataire **Client** est normalement créé pour chaque organisation ayant contracté un service.
- Un locataire **Unité** est créé dans un locataire client existant lorsque vous étendez le service à une nouvelle unité d'organisation.

4. Dans la section **Nom**, indiquez le nom du nouveau locataire.
5. [Uniquement lors de la création d'un tenant partenaire] Saisissez **le nom officiel (juridique) de la société** (requis) et **le numéro de TVA/l'identifiant de taxe/numéro d'inscription de l'entreprise** (facultatif).
6. [Uniquement lors de la création d'un locataire client] Dans **Mode**, indiquez si le locataire utilise les services en mode d'évaluation ou de production. Les rapports mensuels d'utilisation du service n'incluent pas les données d'utilisation pour les locataires en mode d'évaluation.

   Important
   Si vous passez du mode d'évaluation au mode de production en cours de mois, le mois complet sera intégré au rapport mensuel d'utilisation du service. C'est pourquoi nous vous recommandons de passer d'un mode à l'autre le premier jour du mois. Lorsqu'un tenant reste en mode d'évaluation pendant un mois complet, le mode passe automatiquement en mode production.
   Il existe deux scénarios dans lesquels le mode d'évaluation des tenants passe automatiquement au mode de production :
   - En cours de mois, auquel cas le mois ***suivant*** complet sera également intégré au rapport mensuel d'utilisation du service.
   - [Option recommandée] Le premier jour du mois, auquel cas, seul le mois en cours est compté.

7. Dans **Mode de gestion**, sélectionnez l'un des modes suivants pour gérer l'accès au locataire :
   - **Libre-service** – ce mode limite l'accès à ce locataire pour les administrateurs du locataire parent : ils peuvent uniquement modifier les propriétés du locataire, mais ne peuvent pas accéder à quoi que ce soit au sein de celui-ci ni y gérer quoi que ce soit (ex. locataires, utilisateurs, services, sauvegardes et autres ressources).
   - **Géré par le fournisseur de services** – ce mode accorde un accès total au locataire pour l'administrateur du locataire parent : modification des propriétés, gestion des locataires, utilisateurs et services ; accès aux sauvegardes et autres ressources.

   Seul l'administrateur du locataire créé par vous pourra modifier le mode Gestion s'il s'agit du **Libre-service**. Pour cela, l'administrateur du tenant créé peut accéder à **Paramètres** > **Sécurité** et configurer le commutateur **Accès à l'assistance**.
   Vous pouvez vérifier le mode de gestion sélectionné pour vos tenants enfants dans l'onglet **Clients**.

8. Dans **Sécurité**, activez ou désactivez l'authentification à deux facteurs pour le locataire.
   Si elle est activée, tous les utilisateurs de ce locataire devront configurer l'authentification à deux facteurs pour leur compte, afin de bénéficier d'un accès plus sécurisé. Les utilisateurs doivent installer l'application d'authentification sur l'appareil qui applique le second facteur et utiliser le code TOTP unique généré en plus de saisir les identifiants traditionnels pour se connecter à la console. Pour en savoir plus, reportez-vous à l'article « Configurer l'authentification à deux facteurs ». Pour afficher l'état de l'authentification à deux facteurs pour vos clients, accédez à **Clients**.
9. [Uniquement lors de la création d'un tenant dans le mode sécurité renforcée] Dans **Sécurité**, cochez la case **Mode sécurité renforcée**.
   Grâce à ce mode, seules les sauvegardes chiffrées sont autorisées. Le mot de passe de chiffrement doit être défini sur le terminal protégé, car sans ce mot de passe, les sauvegardes échoueront. Toutes les opérations nécessitant de fournir le mot de passe de chiffrement à un service Cloud ne sont pas disponibles. Pour en savoir plus, consultez "Mode sécurité renforcée" (p. 38).

   Important
   Vous ne pouvez pas désactiver le mode sécurité renforcée une fois le tenant créé.

10. Dans **Créer un administrateur**, configurez un compte administrateur.

    Remarque
    La création d'un administrateur est obligatoire pour un locataire client et un locataire partenaire dont le **mode Gestion** est défini sur **Libre-service**.

    a. Saisissez un nom et une adresse e-mail de connexion pour le compte administrateur. Les autres champs sont facultatifs, mais veuillez indiquer d'autres canaux de communication si nous devons contacter l'administrateur.
    b. Sélectionnez une langue.
       Si vous ne sélectionnez aucune langue, l'anglais est utilisé par défaut.
    c. Indiquez les contacts d'entreprise.
       - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
       - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.
       - **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

         Vous pouvez affecter plusieurs contacts d'entreprise à un utilisateur.
11. Dans **Langue**, modifiez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée au sein de ce tenant.
12. Effectuez l'une des actions suivantes :
    - Pour terminer la création du locataire, cliquez sur **Enregistrer et fermer** Dans ce cas, tous les services seront activés pour ce locataire. La méthode de facturation du service Protection sera

définie sur « par charge de travail ».

- Pour sélectionner des services pour le locataire, cliquez sur **Suivant**. Consultez "Sélectionner les services pour un locataire" (p. 39).

Mode sécurité renforcée

Le mode sécurité renforcée offre des paramètres spéciaux pour les clients ayant des exigences de sécurité accrues. Ce mode nécessite un chiffrement obligatoire pour toutes les sauvegardes et autorise uniquement les mots de passe de chiffrement définis localement.

Un administrateur partenaire peut activer le mode sécurité renforcée uniquement lors de la création d'un tenant client, et ne peut pas désactiver ce mode ultérieurement. L'activation du mode sécurité renforcée pour des tenants existants n'est pas possible.

Avec le mode sécurité renforcée, toutes les sauvegardes créées dans un tenant client et dans ses unités sont automatiquement chiffrées avec l'algorithme AES et une clé de chiffrement 256 bits. Les utilisateurs peuvent définir leurs mots de passe de chiffrement uniquement sur les terminaux protégés et ne peuvent pas définir les mots de passe de chiffrement dans les plans de protection.

Les services Cloud n'ont pas accès aux mots de passe de chiffrement. En raison de cette limitation, les fonctionnalités suivantes ne sont pas disponibles pour les tenants en mode sécurité renforcée :

- Restauration depuis la console de service
- Parcours des sauvegardes de niveau fichier depuis la console de service
- Sauvegarde de Cloud à Cloud
- Sauvegarde des sites Web
- Sauvegarde d'applications
- Sauvegarde des terminaux mobiles
- Analyse anti-malware des sauvegardes
- Restauration sûre
- Création automatique de listes blanches d'entreprise
- Carte de la protection des données
- Reprise d'activité après sinistre
- Rapports et tableaux de bord liés aux fonctionnalités non disponibles

Limites

- Le mode sécurité renforcée est compatible uniquement avec les agents dont la version est égale ou supérieure à 15.0.26390.
- Le mode sécurité renforcée n'est pas disponible pour les terminaux exécutant Red Hat Enterprise Linux 4.x ou 5.x ou leurs dérivés.

Sélectionner les services pour un locataire

Par défaut, tous les services sont activés lorsque vous créez un locataire. Vous pouvez sélectionner les services qui seront disponibles pour les utilisateurs au sein du locataire et de ses locataires enfants.

Vous pouvez également sélectionner et activer des services pour plusieurs tenants existants simultanément. Pour plus d'informations, voir "Activation de services pour plusieurs tenants existants" (p. 40).

Cette procédure n'est pas applicable à un locataire unité.

Pour sélectionner les services pour un locataire

1. Dans la section **Sélectionner des services** de la boîte de dialogue « créer/modifier le locataire », sélectionnez une méthode de facturation ou une édition.
   - Sélectionnez la méthode de facturation **Par charge de travail** ou **Par gigaoctet**, puis désélectionnez les cases correspondant aux services que vous souhaitez désactiver pour le tenant.
     L'ensemble des services est identique pour les deux méthodes de facturation.
     Pour Advanced Disaster Recovery, si vous avez enregistré votre propre emplacement de reprise d'activité après sinistre sous votre compte, vous pouvez sélectionner l'emplacement de la reprise d'activité après sinistre dans la liste déroulante.
   - Pour utiliser une ancienne version, sélectionnez le bouton radio **Anciennes éditions**, puis sélectionnez une édition dans la liste déroulante.

   Les services désactivés seront cachés aux utilisateurs au sein du locataire et de ses locataires enfants.
2. Effectuez l'une des actions suivantes :
   - Pour terminer la création du locataire, cliquez sur **Enregistrer et fermer** Dans ce cas, tous les éléments des services sélectionnés seront activés pour ce locataire, avec un quota illimité.
   - Pour configurer les éléments pour le locataire, cliquez sur **Suivant**. Consultez "Configurer les éléments pour un locataire" (p. 39).

Configurer les éléments pour un locataire

Lorsque vous créez un locataire, tous les éléments des services sélectionnés sont activés. Vous pouvez sélectionner les éléments qui seront disponibles pour les utilisateurs au sein du locataire et de ses locataires enfants, et en définir les quotas.

Cette procédure n'est pas applicable à un locataire unité.

Pour configurer les éléments pour un locataire

1. Dans la section **Configurer les services** de la boîte de dialogue « créer/modifier le locataire », sous chaque onglet de service, décochez les cases correspondant aux éléments que vous souhaitez désactiver.

Les fonctionnalités correspondant aux services désactivés seront indisponibles pour les utilisateurs au sein du locataire et de ses locataires enfants.

Remarque
Vous pouvez désactiver les éléments associés à la fonctionnalité de protection avancée, mais ils seront automatiquement réactivés lorsqu'un utilisateur activera une fonctionnalité avancée dans un plan de protection.

2. Certains services vous permettent de sélectionner des stockages qui seront disponibles au nouveau locataire. Les stockages sont regroupés par emplacement. Vous pouvez choisir dans la liste contenant tous les emplacements et stockages disponibles pour votre locataire.
   - Lors de la création d'un locataire partenaire/dossier, vous pouvez sélectionner plusieurs emplacements et stockages pour chaque service.
   - Lors de la création d'un locataire client, vous devez sélectionner un emplacement, puis un stockage par service au sein de cet emplacement. Les stockages affectés au client peuvent être modifiés ultérieurement, mais uniquement si leur utilisation est de 0 Go, c'est-à-dire, soit avant que le client n'ait commencé à utiliser le stockage, soit après qu'il a supprimé toutes les sauvegardes de ce stockage. Les informations concernant l'utilisation de l'espace de stockage ne sont pas mises à jour en temps réel. Veuillez prévoir jusqu'à 24 heures pour que les informations soient mises à jour.

   Pour en savoir plus sur les stockages, consultez « Gérer les emplacements et le stockage ».
3. Pour indiquer un quota pour un élément, cliquez sur le lien **Illimité** à côté de l'élément.
   Ces quotas sont « souples ». Si une de ces valeurs est dépassée, une notification par messagerie électronique est envoyée aux administrateurs du locataire et aux administrateurs du locataire parent. Les restrictions d'utilisation des services ne sont pas activées. Pour un locataire partenaire, il est possible que l'utilisation de l'élément dépasse le quota, car le dépassement de quota ne peut pas être défini lors de la création du locataire partenaire.
4. [Facultatif, uniquement lors de la création d'un locataire client] Indiquez les dépassements de quota.
   Un dépassement permet à un locataire client de dépasser le quota, selon la valeur indiquée. Lorsque le dépassement est dépassé, des restrictions sont appliquées à l'utilisation du service correspondant.
5. Cliquez sur **Enregistrer et fermer**.

Le locataire nouvellement créé s'affiche dans l'onglet **Clients** de la console de gestion.

Si vous souhaitez modifier les paramètres du locataire ou changer l'administrateur, sélectionnez le locataire dans l'onglet **Clients**, puis cliquez sur l'icône en forme de crayon dans la section que vous souhaitez modifier.

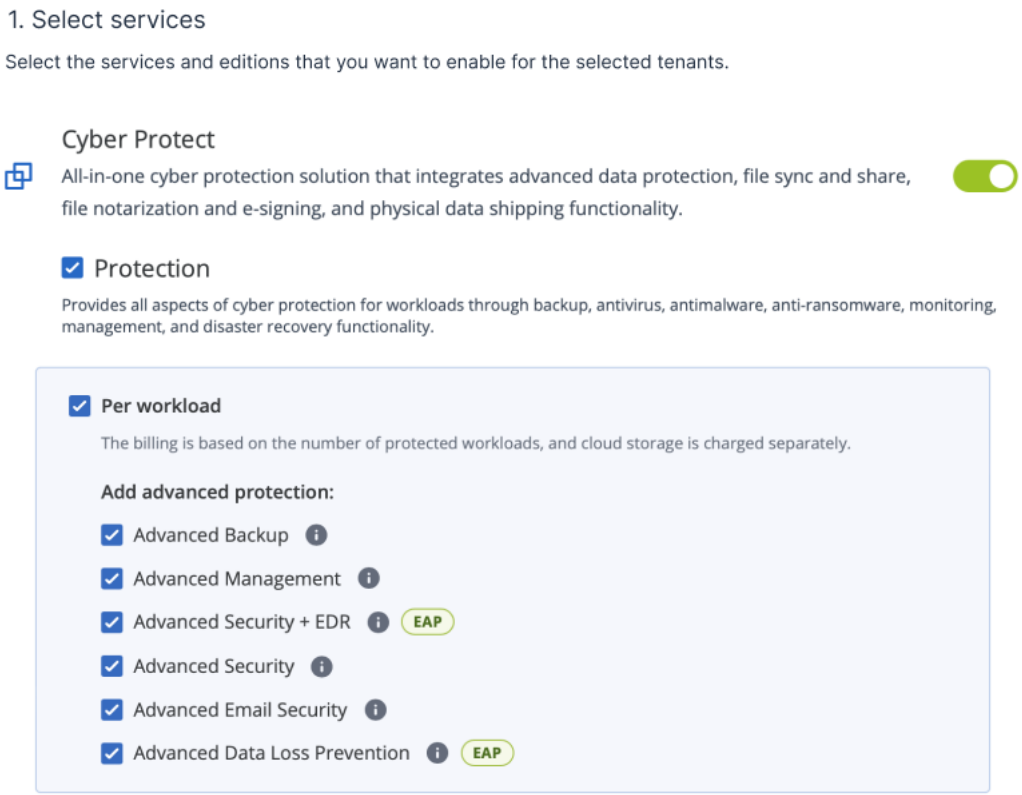
Activation de services pour plusieurs tenants existants

Vous pouvez activer les services, les éditions, les packs et les éléments de nombreux tenants simultanément (jusqu'à 100 tenants par session).

Cette procédure s'applique aux tenants de sous-root (superutilisateur), de partenaire, de dossier et de client. Les tenants de l'un de ces types peuvent être sélectionnés simultanément.

Pour activer les services pour plusieurs tenants

1. Dans le portail de gestion, accédez à **Clients**.
2. En haut à droite, cliquez sur **Configurer les services**.
3. Sélectionnez les tenants pour lesquels vous souhaitez activer des services en cochant la case située à côté de leur nom, puis cliquez sur **Suivant**.
4. Dans la section **Sélectionner des services**, sélectionnez les services que vous souhaitez appliquer à tous les tenants sélectionnés, puis cliquez sur **Suivant**.

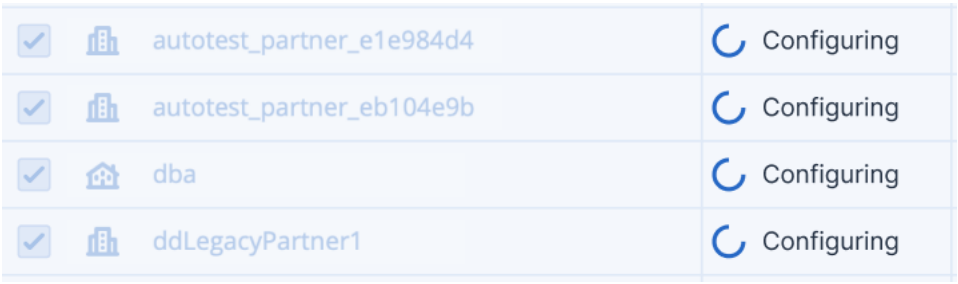


Remarque
Vous ne pouvez pas désactiver dans cet écran un service activé. Tous les services, éditions et éléments sélectionnés avant cette procédure restent activés.

5. Dans la section **Configurer les services**, sélectionnez les fonctionnalités de services et les éléments que vous souhaitez activer pour les tenants sélectionnés, puis cliquez sur **Suivant**.
6. Dans la section **Résumé**, examinez les modifications qui seront appliquées aux tenants sélectionnés.

   Vous pouvez cliquer sur **Tout développer** pour voir tous les services et éléments sélectionnés qui seront appliqués aux tenants. Vous pouvez également développer la vue de chaque tenant pour voir les services et éléments sélectionnés pour ce tenant.

7. Cliquez sur **Appliquer les changements**. Les services étant configurés pour chaque tenant, le tenant est désactivé et la colonne **État du tenant** indique les services et éléments en cours de configuration, comme indiqué ci-dessous.



8. Lorsque la configuration des services et des éléments est appliquée aux tenants sélectionnés, un message de confirmation est affiché.
   Si le service et les éléments n'ont pas pu être appliqués à un tenant, la colonne **État du tenant** indique **Non appliqué**. Cliquez sur **Réessayer** pour examiner la configuration des tenants sélectionnés.

Activation des notifications de maintenance

En tant qu'utilisateur Partenaire, vous pouvez autoriser vos tenants enfant (partenaires et clients) à recevoir des e-mails de notification de maintenance provenant directement du centre de données Cyber Protect et à recevoir des notifications de maintenance intégrées au produit sur le portail de gestion. Cela vous aidera à réduire le nombre d'appels au support concernant la maintenance.

Remarque
Les e-mails de notification de maintenance sont labellisés en fonction du centre de données. La labellisation personnalisée n'est pas prise en charge pour ces notifications.

Activer les notifications de maintenance pour les partenaires ou clients enfant

1. Connectez-vous au portail de gestion en tant qu'utilisateur Partenaire, cliquez sur **Clients**, puis cliquez sure nom d'un tenant partenaire ou client pour lequel vous souhaitez activer les notifications de maintenance.
2. Cliquez sur **Configurer**.
3. Dans l'onglet **Paramètres généraux**, trouvez l'option **Notifications de maintenance** et activez-la.
   Si vous ne voyez pas l'option **Notifications de maintenance**, contactez votre fournisseur de services.

Remarque
Les notifications de maintenance sont activées, mais ne seront pas envoyées tant que le tenant sélectionné ne les aura pas activées pour ses utilisateurs ou ne les aura pas propagées à ses partenaires ou clients enfant afin d'activer les notifications pour leurs utilisateurs.

Activer les notifications de maintenance pour un utilisateur

1. Connectez-vous au portail de gestion en tant qu'utilisateur Partenaire ou en tant qu'administrateur d'entreprise.
   En tant que partenaire, vous pouvez accéder aux utilisateurs de tous les tenants que vous gérez.
2. Accédez à **Dirigeant(e)s de l'entreprise** > **Utilisateurs**, puis cliquez sur le nom d'un utilisateur pour lequel vous souhaitez activer les notifications de maintenance.
3. Dans l'onglet **Services**, dans la section **Paramètres**, cliquez sur le crayon pour modifier les options.
4. Cochez la case **Notifications de maintenance**, puis cliquez sur **Terminé**.

L'utilisateur sélectionné recevra des notifications par e-mail concernant les activités de maintenance à venir sur le centre de données.

Configuration du profil client autogéré

En tant que partenaire, vous pouvez configurer des profils client autogérés pour les tenants que vous gérez. Cette option vous permet de contrôler la visibilité du profil et des coordonnées des tenants pour chacun de vos clients.

Configurer un profil client autogéré

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le client pour lequel vous souhaitez configurer le profil client auto-géré.
3. Sélectionnez l'onglet **Configurer**, puis sélectionnez l'onglet **Paramètres généraux**.
4. Activez ou désactivez le commutateur **Activer le profil client autogéré**.

Lorsque le profil client autogéré est activé, ce client voit la section **Profil de l'entreprise** dans le menu de navigation, ainsi que les champs associés au contact dans l'assistant de création d'utilisateurs (**Téléphone professionnel**, **Contact d'entreprise** et **Titre**).

Lorsque le profil client autogéré est désactivé, la section **Profil de l'entreprise** dans le menu de navigation, ainsi que les champs associés au contact dans l'assistant de création d'utilisateurs sont masqués.

Configuration des contacts de l'entreprise

En tant que partenaire, vous pouvez configurer des informations de contact pour votre entreprise et pour le tenant que vous gérez. Nous enverrons des mises à jour au sujet des nouvelles fonctionnalités et d'autres modifications importantes de la plate-forme aux contacts de cette liste.

Vous pouvez ajouter de nombreux contacts et affecter des contacts d'entreprise en fonction du rôle de l'utilisateur. Vous pouvez créer des contacts à partir d'utilisateurs qui existent dans la plate-forme Cyber Protect ou ajouter des informations de contact de personnes qui n'ont pas accès au service.

Pour configurer des contacts pour votre entreprise

1. Dans la console de gestion, accédez à **Dirigeant(e)s de l'entreprise** > **Profil de l'entreprise**.
2. Dans la section **Contacts**, cliquez sur **+**.
3. Sélectionnez une option pour créer le contact.
   - **Créer à partir d'un utilisateur existant**
     - Sélectionnez un utilisateur dans la liste déroulante.
     - Sélectionnez un contact d'entreprise.
       - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
       - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.
       - **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

       Vous pouvez affecter plusieurs contacts d'entreprise à un utilisateur.

     Si vous supprimez un contact associé à un utilisateur de la liste des contacts du profil d'entreprise, l'utilisateur n'est pas supprimé. Le système annule l'affectation de tous les contacts d'entreprise pour l'utilisateur afin qu'ils n'apparaissent plus dans la colonne **Contacts de l'entreprise** de la liste **Utilisateurs**.

     Si vous souhaitez changer l'adresse e-mail du contact associé à l'utilisateur, le système exige la vérification de la nouvelle adresse. Un e-mail est envoyé à cette adresse et l'utilisateur doit confirmer la modification.
   - **Créer un nouveau contact**
     - Spécifiez les informations de contact.
       - **Prénom** : prénom de la personne de contact. Ce champ est obligatoire.
       - **Nom** : nom de la personne de contact. Ce champ est obligatoire.
       - **Adresse e-mail professionnelle** : adresse e-mail de la personne de contact. Ce champ est obligatoire.
       - **Téléphone professionnel** : ce champ est facultatif.
       - **Titre** : ce champ est facultatif.
     - Sélectionnez les **Contacts de l'entreprise**.
       - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
       - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.
       - **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

       Vous pouvez affecter plusieurs contacts d'entreprise à un utilisateur.
4. Cliquez sur **Ajouter**.

Pour configurer des contacts pour un tenant

Remarque
Si vous modifiez les informations de contact d'un tenant enfant, vos modifications seront visibles par le tenant.

1. Dans le portail de gestion, accédez à **Clients**.
2. Cliquez sur le tenant, puis sur **Configurer**.
3. Dans la section **Contacts**, cliquez sur **+**.
4. Sélectionnez une option pour créer le contact.
   - **Créer à partir d'un utilisateur existant**
     - Sélectionnez un utilisateur dans la liste déroulante.
     - Sélectionnez un contact d'entreprise.
       - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
       - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.
       - **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

       Vous pouvez affecter plusieurs contacts d'entreprise à un utilisateur.

     Si vous supprimez un contact associé à un utilisateur de la liste des contacts du profil d'entreprise, l'utilisateur n'est pas supprimé. Le système annule l'affectation de tous les contacts d'entreprise pour l'utilisateur afin qu'ils n'apparaissent plus dans la colonne **Contacts de l'entreprise** de la liste **Utilisateurs**.

     Si vous souhaitez changer l'adresse e-mail du contact associé à l'utilisateur, le système exige la vérification de la nouvelle adresse. Un e-mail est envoyé à cette adresse et l'utilisateur doit confirmer la modification.
   - **Créer un nouveau contact**
     - Spécifiez les informations de contact.
       - **Prénom** : prénom de la personne de contact. Ce champ est obligatoire.
       - **Nom** : nom de la personne de contact. Ce champ est obligatoire.
       - **Adresse e-mail professionnelle** : adresse e-mail de la personne de contact. Ce champ est obligatoire.
       - **Téléphone professionnel** : ce champ est facultatif.
       - **Titre** : ce champ est facultatif.
     - Sélectionnez les **Contacts de l'entreprise**.
       - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
       - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.

- **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

  Vous pouvez affecter plusieurs contacts d'entreprise à un utilisateur.

5. Cliquez sur **Ajouter**.

Actualisation des données d'utilisation d'un tenant

Par défaut, les données d'utilisation sont actualisées à intervalles fixes. Vous pouvez actualiser les données d'utilisation d'un tenant manuellement.

1. Dans la console de gestion, accédez à **Clients**.
2. Cliquez sur le tenant, puis sur les points de suspension présents sur sa ligne.
3. Sélectionnez **Actualiser l'utilisation**.

   Remarque
   La récupération des données peut prendre jusqu'à 10 minutes.

4. Rechargez la page pour afficher les données mises à jour.

Désactivation et activation d'un locataire

Vous devez temporairement désactiver un locataire. Par exemple, dans le cas où votre locataire a des dettes pour l'utilisation de services.

Pour désactiver un locataire

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le locataire que vous souhaitez désactiver, puis cliquez sur l'icône en forme de points de suspension > **Désactiver**.
3. Confirmez votre action en cliquant sur **Désactiver**.

En conséquence :

- Le locataire et ses sous-locataires seront désactivés, et leurs services seront arrêtés.
- Le locataire et ses sous-locataires continueront d'être facturés, car leurs données sont conservées et stockées dans Cloud Cyber Protect.
- Tous les clients d'API au sein du locataire et de ses sous-locataires seront désactivés, et toutes les intégrations utilisant ces clients cesseront de fonctionner.

Pour activer un locataire, sélectionnez-le dans la liste des clients, puis cliquez sur l'icône en forme de points de suspension > **Activer**.

Déplacer un locataire vers un autre locataire

Le portail de gestion vous permet de déplacer un locataire d'un locataire parent à un autre locataire parent. Cela peut être utile si vous souhaitez transférer un client d'un partenaire à un autre, ou si

vous avez créé un locataire dossier pour organiser vos clients et souhaitez en déplacer certains vers le nouveau locataire dossier.

Type de tenants pouvant être déplacés

Type de tenant	Déplaçable	Tenant cible
Partenaire	Oui	Partenaire ou dossier
Dossier	Oui	Partenaire ou dossier
Client	Oui	Partenaire ou dossier
Unité	Non	Aucun

Exigences et restrictions

- Vous pouvez déplacer un tenant uniquement si le tenant parent cible possède le même ensemble de services et éléments, ou un plus grand, que le tenant parent d'origine.
- Lors du déplacement d'un locataire client, tous les stockages affectés à ce locataire client dans le locataire parent d'origine doivent exister dans le locataire parent de destination. Cette étape est nécessaire, car les données relatives au service client ne peuvent pas être déplacées d'un stockage à un autre.
- Dans les tenants clients gérés par des fournisseurs de services, des plans peuvent être appliqués aux ressources des clients au niveau du fournisseur de services (par exemple, des plans de création de scripts).

  Lors du déplacement d'un tenant client de ce type, les plans du fournisseur de services sont révoqués des ressources clients et tous les services associés à ces plans cessent de fonctionner pour ce client.
- Vous pouvez déplacer les tenants dans votre hiérarchie des comptes partenaires. Vous pouvez également déplacer des tenants clients vers un tenant cible extérieur à votre hiérarchie de comptes partenaires. Pour savoir si cette opération est possible, contactez le gestionnaire de compte dans .
- Seuls les administrateurs (par exemple, l'administrateur du portail de gestion ou l'administrateur de l'entreprise) peuvent déplacer des tenants vers d'autres tenants parents.

Comment déplacer un locataire

1. Connectez-vous au portail de gestion.
2. Recherchez l'**identifiant interne** du partenaire cible ou du tenant du dossier vers lequel vous souhaitez déplacer un tenant, puis copiez-le. Faites ce qui suit :
   a. Dans l'onglet **Clients**, sélectionnez le locataire de destination vers lequel vous souhaitez déplacer un locataire.
   b. Dans le volet Propriétés du locataire, cliquez sur l'icône en forme de points de suspension verticaux, puis sur **Afficher l'identifiant**.

c. Copiez la chaîne de texte affichée dans le champ **Identifiant interne**, puis cliquez sur **Annuler**.

3. Sélectionnez le tenant à déplacer, puis déplacez-le vers le partenaire/dossier cible. Faites ce qui suit :
   a. Dans l'onglet **Clients**, sélectionnez le tenant que vous souhaitez déplacer.
   b. Dans le volet Propriétés du locataire, cliquez sur l'icône elliptique verticale, puis sur **Déplacer**.
   c. Coller l'identificateur interne du locataire de destination, puis cliquez sur **Déplacer**.

L'opération commence immédiatement et prend jusqu'à 10 minutes.

Si le tenant que vous déplacez comporte des tenants enfants (par exemple, s'il s'agit d'un tenant partenaire ou d'un tenant de dossier avec un tenant client à l'intérieur), l'intégralité de la sous-arborescence de tenants est déplacée vers le tenant cible.

Conversion d'un locataire partenaire en locataire dossier et vice-versa

Le portail de gestion vous permet de convertir un locataire partenaire en locataire dossier.

Cela peut être utile si vous avez utilisé un locataire partenaire à des fins de regroupement et que vous souhaitez à présent organiser correctement votre infrastructure de locataires. Cela est également utile si vous souhaitez que votre tableau de bord opérationnel inclue le rassemblement d'informations à propos du locataire.

Vous pouvez également convertir un locataire dossier en locataire partenaire.

Remarque
La conversion est une opération sécurisée qui n'affecte pas les utilisateurs au sein du locataire ni les autres données associées au service.

Pour convertir un locataire

1. Connectez-vous au portail de gestion.
2. Dans l'onglet **Clients**, sélectionnez le locataire que vous souhaitez convertir.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur l'icône de points de suspension à côté du nom du locataire.
   - Sélectionnez le locataire, puis cliquez sur l'icône de points de suspension dans le volet Propriétés du locataire.
4. Cliquez sur **Convertir en un dossier** ou **Convertir en un partenaire**.
5. Confirmez votre choix.

Limitation de l'accès à votre tenant

Les administrateurs de niveau client ou supérieur peuvent limiter l'accès des administrateurs de niveau supérieur à leur tenant.

Si l'accès au locataire est limité, les administrateurs du locataire parent peuvent modifier uniquement les propriétés du locataire. Ils n'ont plus du tout accès aux comptes ni aux locataires enfants.

Afin d'éviter que les administrateurs de niveau supérieur accèdent à votre locataire

1. Connectez-vous au portail de gestion.
2. Accédez à **Paramètres** > **Sécurité**.
3. Désactivez le commutateur **Accès à l'assistance**.

Par conséquent, les administrateurs des locataires parents auront un accès limité à votre locataire. Ils peuvent uniquement modifier les propriétés du locataire, mais ne pourront pas accéder à quoi que ce soit au sein de celui-ci ni y gérer quoi que ce soit (ex. locataires, utilisateurs, services, sauvegardes et autres ressources).

Si le commutateur **Accès à l'assistance** est activé, les administrateurs des locataires parents bénéficieront donc d'un accès complet à votre locataire. Ils pourront effectuer les actions suivantes : modification des propriétés ; gestion des locataires, utilisateurs et services ; accès aux sauvegardes et autres ressources.

Suppression d'un locataire

Il se peut que vous souhaitiez supprimer un locataire afin de libérer les ressources qu'il utilise. Les statistiques d'utilisation seront mises à jour sous un jour après suppression. Pour les locataires plus importants, il se peut que l'opération prenne plus de temps.

Avant de supprimer un locataire, vous devez le désactiver. Pour en savoir plus sur la façon de procéder, reportez-vous à « Désactivation et activation d'un locataire ».

Important
La suppression d'un locataire est irréversible !

Pour supprimer un client

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le locataire désactivé que vous souhaitez supprimer, puis cliquez sur l'icône en forme de points de suspension > **Supprimer**.
3. Pour confirmer votre action, saisissez votre identifiant, puis cliquez sur **Supprimer**.

En conséquence :

- Le locataire et ses sous-locataires seront supprimés.
- Tous les services activés au sein d'un locataire et de ses sous-locataires seront stoppés.
- Tous les utilisateurs au sein du locataire et de ses sous-locataires seront supprimés.
- Toutes les machines du locataire et de ses sous-locataires seront désenregistrées.
- Toutes les données associées au service, par exemple les sauvegardes et les fichiers synchronisés, contenues dans le locataire et ses sous-locataires seront supprimées.
- Tous les clients d'API au sein du locataire et de ses sous-locataires seront supprimés, et toutes les intégrations utilisant ces clients cesseront de fonctionner.

Gestion des utilisateurs

Les administrateurs partenaires, les administrateurs clients et les administrateurs d'unités peuvent configurer et gérer les comptes utilisateur dans les tenants auxquels ils ont accès.

Création d'un compte utilisateur

Vous pouvez créer des comptes supplémentaires dans les cas suivants :

- Comptes administrateur partenaire/dossier — pour partager les fonctions de gestion des services avec d'autres personnes.
- Comptes administrateur client/prospect/unité — pour déléguer la gestion du service à d'autres personnes dont les droits d'accès seront strictement limités au client/au prospect/à l'unité correspondants.
- Les comptes utilisateur au sein du client ou du locataire unité — pour autoriser les utilisateurs à accéder uniquement à un sous-ensemble des services.

Notez que les comptes existants ne peuvent pas être déplacés entre les tenants. Vous devez d'abord créer un locataire, puis le remplir de comptes.

Pour créer un compte utilisateur

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire dans lequel vous souhaitez créer un compte utilisateur. Consultez "Navigation dans le portail de gestion" (p. 28).
3. Dans l'angle supérieur droit, cliquez sur **Nouveau** > **Utilisateur**.

   Vous pouvez également accéder à **Dirigeant(e)s de l'entreprise > Utilisateurs** et cliquer sur **+ Nouveau**.
4. Indiquez les informations de contact suivantes relatives au compte :
   - **Connexion**

     Important
     Chaque compte doit disposer d'un identifiant unique.

- **E-mail**

  Important
  Si l'utilisateur est enregistré dans le service File Sync & Share, indiquez l'adresse e-mail qui a été utilisée pour l'inscription File Sync & Share.
  Veuillez noter que chaque compte utilisateur du client doit disposer d'une adresse e-mail unique.

- **Prénom**
- **Nom**
- [Facultatif] **Téléphone professionnel**

  Remarque
  Les champs **Téléphone professionnel**, **Titre** et **Contact d'entreprise** s'affichent dans l'assistant de création d'utilisateurs uniquement si le partenaire parent a activé l'option **Activer le profil client autogéré** pour le tenant du client. Dans les autres cas, ces champs ne sont pas affichés.

- [Facultatif] **Titre**
- Dans **Langue**, changez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée pour ce compte.

5. [Facultatif] Indiquez les contacts d'entreprise.
   - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
   - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.
   - **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

     Vous pouvez affecter plusieurs contacts d'entreprise à un utilisateur.

   Vous pouvez afficher les contacts d'entreprise affectés pour un utilisateur de la liste **Utilisateurs**, dans la colonne **Contacts de l'entreprise**, puis modifiez le compte utilisateur afin de changer les contacts d'entreprise si nécessaire.
6. [Non disponible lors de la création d'un compte dans un locataire partenaire/dossier] Sélectionnez les services auxquels l'utilisateur aura accès ainsi que les rôles dans chaque service.

   Les services disponibles dépendent des services activés pour le locataire dans lequel le compte utilisateur a été créé.
   - Si vous sélectionnez la case **Administrateur d'entreprise**, l'utilisateur aura accès au portail de gestion et au rôle d'administrateur dans tous les services actuellement activés pour le locataire. L'utilisateur aura le rôle d'administrateur dans tous les services qui seront activés pour le locataire à l'avenir.
   - Si vous sélectionnez la case **Administrateur d'unité**, l'utilisateur aura accès au portail de gestion, mais n'aura pas forcément le rôle d'administrateur de service, selon le service.

- Autrement, l'utilisateur se verra attribuer les rôles que vous choisirez dans les services que vous choisirez.

7. Cliquez sur **Créer**.

Le compte utilisateur nouvellement créé s'affiche dans l'onglet **Utilisateurs**, sous **Gestion d'entreprise**.

Si vous souhaitez modifier les paramètres utilisateur ou spécifier des paramètres de notification et des quotas (non disponible pour les administrateurs partenaires et dossiers) pour l'utilisateur, sélectionnez l'utilisateur dans l'onglet **Utilisateurs**, puis cliquez sur l'icône en forme de crayon dans la section que vous souhaitez modifier.

Réinitialiser le mot de passe d'un utilisateur

1. Dans le portail de gestion, accédez à **Gestion de l'entreprise** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez réinitialiser le mot de passe, puis cliquez sur l'icône en forme de points de suspension > **Réinitialiser le mot de passe**.
3. Confirmez votre action en cliquant sur **Réinitialiser**.

L'utilisateur peut désormais suivre le processus de réinitialisation à l'aide des instructions contenues dans l'e-mail qui lui a été envoyé.

Pour les services qui ne prennent pas en charge l'authentification à deux facteurs (par exemple, l'inscription dans Cyber Infrastructure), vous devrez peut-être convertir un compte utilisateur en *compte de service*, c'est-à-dire en un compte qui ne nécessite pas d'authentification à deux facteurs.

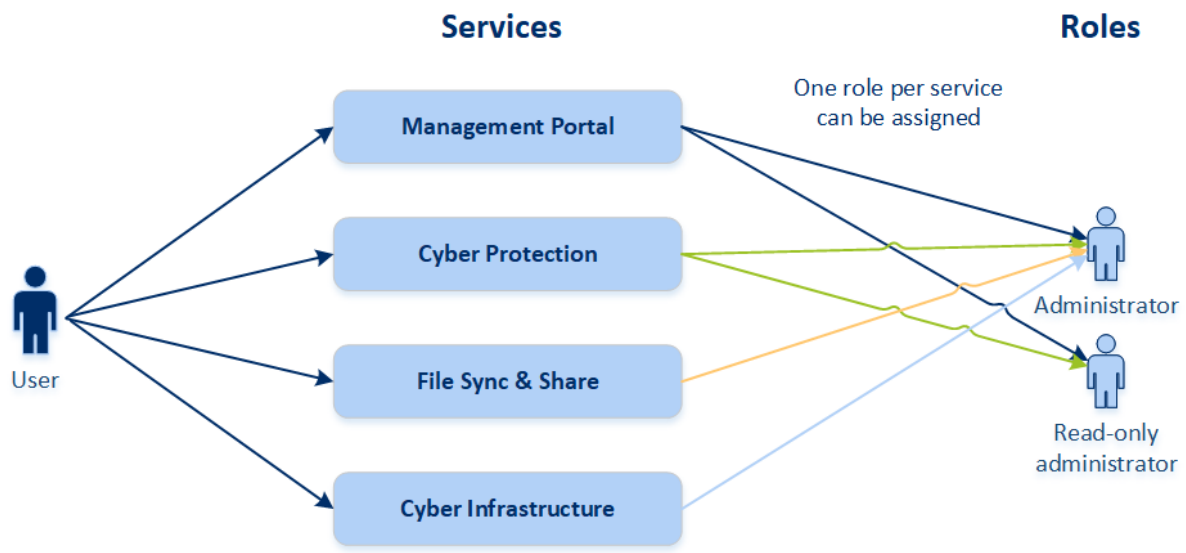
Pour convertir un compte utilisateur dans le type du compte de service

1. Dans le portail de gestion, accédez à **Gestion de l'entreprise** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez convertir le compte dans le type du compte de service, puis cliquez sur l'icône en forme de points de suspension > **Marquer comme compte de service**.
3. Dans la fenêtre de confirmation, saisissez le code de l'authentification à deux facteurs et confirmez votre action.

Le compte peut désormais être utilisé pour les services qui ne prennent pas en charge l'authentification à deux facteurs.

Rôles utilisateur disponibles pour chaque service

Un utilisateur peut détenir plusieurs rôles, mais un seul par service.



Pour chaque service, vous pouvez définir quel rôle sera attribué à un utilisateur.

Service	Rôle	Description
N/D	Administrateur d'entreprise	Ce rôle accorde des droits d'administrateur complets pour tous les services. Ce rôle donne accès à la liste d'autorisation de l'entreprise. Si le module complémentaire de reprise d'activité après sinistre du service Cyber Protection est activé pour l'entreprise, ce rôle donne également accès à la fonctionnalité de reprise d'activité après sinistre.
Portail de gestion	Administrateur	Ce rôle donne accès au portail de gestion, où l'administrateur peut gérer les utilisateurs dans l'ensemble de l'organisation.
	Administrateur en lecture seule Niveau partenaire	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion du partenaire, ainsi que du portail de gestion de tous les clients de ce partenaire. Ces utilisateurs peuvent accéder aux données des autres utilisateurs des organisations en lecture seule.
	Administrateur en lecture seule Niveau client	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion de toute l'entreprise. Ces utilisateurs peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule.
	Administrateur en lecture seule Niveau unité	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion de l'unité et des sous-unités de l'entreprise. Ces utilisateurs peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule.
Cyber Protection	Cyberadministrateur	En plus d'accorder des droits d'administrateur, ce rôle permet la configuration et la gestion du service Cyber Protection, ainsi

		que l'approbation d'actions dans la création de cyber-scripts. Le rôle Cyberadministrateur n'est disponible que pour les tenants pour lesquels le pack Advanced Management est activé.
	Administrateur	Ce rôle active la configuration et la gestion de Cyber Protection pour vos clients. Ce rôle est nécessaire pour la configuration et la gestion de la fonctionnalité de reprise d'activité après sinistre, ainsi que de la liste d'autorisation de l'entreprise.
	Administrateur en lecture seule	Ce rôle fournit un accès en lecture seule à tous les objets du service Cyber Protection. Ces utilisateurs peuvent accéder aux données des autres utilisateurs de l'organisation en mode lecture seule. L'administrateur en lecture seule ne peut pas configurer ni gérer la fonctionnalité de reprise d'activité après sinistre ou la liste d'autorisation de l'entreprise.
	Opérateur de restauration	Le rôle donne accès aux sauvegardes des organisations Microsoft 365 et Google Workspace et permet leur restauration, tout en limitant l'accès au contenu sensible.
File Sync & Share	Administrateur	Ce rôle permet de configurer et de gérer le service File Sync & Share pour vos utilisateurs.
Cyber Infrastructure	Administrateur	Ce rôle permet de configurer et de gérer Cyber Infrastructure pour vos utilisateurs.

Rôle d'administrateur en lecture seule

Un compte avec ce rôle bénéficie d'un accès en lecture seule à la console Web Cyber Protection et peut effectuer les opérations suivantes :

- Collecter des données de diagnostic, comme les rapports système.
- Voir les points de récupération d'une sauvegarde, mais pas explorer le contenu de la sauvegarde ni voir les fichiers, dossiers ou e-mails.

Un administrateur en lecture seule ne peut pas effectuer les opérations suivantes :

- Démarrer ou arrêter une tâche.

  Par exemple, un administrateur en lecture seule ne peut pas démarrer une restauration ou arrêter une sauvegarde en cours d'exécution.
- Accéder au système de fichiers sur les ordinateurs source ou cible.

  Par exemple, un administrateur en lecture seule ne peut pas voir de fichiers, dossiers ou e-mails sur un ordinateur sauvegardé.
- Changer des paramètres.

Par exemple, un administrateur en lecture seule ne peut pas créer de plan de protection ni modifier l'un de ses paramètres.

- Créer, mettre à jour ni supprimer de données.

  Par exemple, un administrateur en lecture seule ne peut pas supprimer de sauvegardes.

Tous les objets d'interface qui ne sont pas accessibles pour un administrateur en lecture seule sont masqués, excepté les paramètres par défaut du plan de protection. Ces paramètres sont affichés, mais le bouton **Enregistrer** n'est pas actif.

Toute modification apportée aux comptes et aux rôles s'affiche dans l'onglet **Activités**, avec les détails suivants :

- Ce qui a été modifié
- L'utilisateur ayant effectué la modification
- La date et l'heure des modifications

Rôle d'opérateur de restauration

Ce rôle n'est disponible que dans le service Cyber Protection et est limité aux sauvegardes Microsoft 365 et Google Workspace.

Un opérateur de restauration peut effectuer les actions suivantes :

- Afficher les alertes et les activités
- Parcourir et actualiser la liste des sauvegardes.
- Parcourir les sauvegardes sans accéder à leur contenu. L'opérateur de restauration peut voir les noms des fichiers sauvegardés et les objets et expéditeurs des e-mails sauvegardés.
- Rechercher des sauvegardes (recherche dans le texte intégral non prise en charge).
- Restaurer des sauvegardes cloud à cloud dans leur l'emplacement d'origine au sein de l'organisation d'origine Microsoft 365 ou Google Workspace.

Un opérateur de restauration ne peut pas effectuer les actions suivantes :

- Supprimer les alertes.
- Ajouter ou supprimer des organisations Microsoft 365 ou Google Workspace.
- Ajouter, supprimer ou renommer des emplacements de sauvegarde.
- Supprimer ou renommer des sauvegardes.
- Créer, supprimer ou renommer des dossiers lors de la restauration d'une sauvegarde vers un emplacement personnalisé.
- Appliquer un plan de sauvegarde ou exécuter une sauvegarde.
- Accéder aux fichiers sauvegardés ou au contenu des e-mails sauvegardés.
- Télécharger les fichiers sauvegardés ou les pièces jointes des e-mails sauvegardés.

- Envoyer des ressources cloud sauvegardées, comme des e-mails ou des éléments de calendrier, en tant qu'e-mail.
- Afficher ou restaurer des conversations Microsoft 365 Teams.
- Restaurer des sauvegardes cloud à cloud ailleurs que dans leur emplacement d'origine, par exemple une autre boîte aux lettres, OneDrive, Google Drive ou Microsoft 365 Team.

Rôles d'utilisateur et droits de création de cyber-scripts

Les actions disponibles avec les scripts et les plans de création de scripts dépendent de l'état du script et de votre rôle d'utilisateur.

Les administrateurs peuvent gérer les objets dans leur propre tenant et dans ses tenants enfants. Ils ne peuvent pas voir les objets disponibles dans un niveau d'administration plus élevé (le cas échéant), ni y accéder.

Les administrateurs de niveau inférieur n'ont qu'un accès en lecture seule aux plans de création de scripts appliqués à leurs charges de travail par un administrateur de niveau supérieur.

Les rôles suivants octroient des droits en matière de création de cyber-scripts :

- Administrateur d'entreprise
  Ce rôle octroie des droits d'administrateur complets dans tous les services. Concernant la création de cyber-scripts, il octroie les mêmes droits que le rôle Cyberadministrateur.
- Cyberadministrateur
  Ce rôle octroie des autorisations complètes, y compris l'approbation des scripts qui peuvent être utilisés dans le tenant, et la capacité à exécuter des scripts avec l'état **Test**.
- Administrateur
  Ce rôle octroie des autorisations partielles, avec la capacité d'exécuter des scripts approuvés, ainsi que de créer et d'exécuter des plans de création de scripts qui utilisent des scripts approuvés.
- Administrateur en lecture seule
  Ce rôle octroie des autorisations limitées, avec la capacité de visualiser les scripts et les plans de protection utilisés dans le tenant.
- Utilisateur
  Ce rôle octroie des autorisations partielles, avec la capacité d'exécuter des scripts approuvés, ainsi que de créer et d'exécuter des plans de création de scripts qui utilisent des scripts approuvés, mais uniquement sur le propre ordinateur de l'utilisateur.

Le tableau suivant résume toutes les actions disponibles, en fonction de l'état du script et du rôle de l'utilisateur.

Rôle	Objet	État du script		
		Brouillon	Test...	Approuvé

Cyberadministrateur Administrateur d'entreprise	Plan de création de script	Modifier (supprimer un brouillon de script d'un plan) Supprimer Retirer Désactiver Arrêter	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter
	Script	Créer Modifier Modifier l'état Cloner Supprimer Annuler l'exécution	Créer Modifier Modifier l'état Exécuter Cloner Supprimer Annuler l'exécution	Créer Modifier Modifier l'état Exécuter Cloner Supprimer Annuler l'exécution
Administrateur Utilisateur (pour ses propres charges de travail)	Plan de création de script	Affichage Retirer Désactiver Arrêter	Affichage Annuler l'exécution	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter
	Script	Créer Modifier Cloner Supprimer Annuler l'exécution	Affichage Cloner Annuler l'exécution	Exécuter Cloner Annuler l'exécution

Administrateur en lecture seule	Plan de création de script	Affichage	Affichage	Affichage
	Script	Affichage	Affichage	Affichage

La modification des paramètres de notification pour un utilisateur

Pour modifier les paramètres de notification d'un utilisateur, accédez à **Gestion d'entreprise** > **Utilisateurs**. Sélectionnez l'utilisateur dont vous souhaitez configurer les notifications, puis cliquez sur l'icône en forme de crayon dans la section **Paramètres**. Les paramètres de notifications suivants sont disponibles si le service Cyber Protection est activé pour le tenant dans lequel l'utilisateur est créé :

- **Notifications relatives aux dépassements de quotas** (activé par défaut)
  Les notifications relatives aux dépassements de quotas.
- **Rapports d'utilisation planifiés** (activés par défaut)
  Rapports d'utilisation envoyés le premier jour de chaque mois.
- **Notifications de labellisation d'URL** (désactivées par défaut)
  Notifications concernant l'expiration prochaine du certificat utilisé pour l'URL personnalisée des services cloud Cyber Protect. Les notifications sont envoyées à tous les administrateurs du tenant sélectionné : 30 jours, 15 jours, 7 jours, 3 jours et 1 jour avant l'expiration du certificat.
- **Notifications d'échec**, **Notifications d'avertissement** et **Notifications de réussite** (désactivées par défaut)
  Les notifications relatives aux résultats d'exécution des plans de protection et aux résultats des opérations de reprise d'activité après sinistre pour chaque terminal.
- **Résumé quotidien concernant les alertes actives** (activé par défaut)
  Le résumé quotidien est généré sur la base de la liste des alertes actives présentes dans la console de service au moment de la génération du résumé. Le résumé est généré et envoyé une fois par jour entre 10:00 et 23:59 UTC. L'heure à laquelle le rapport est généré et envoyé dépend de la charge de travail du centre de données. S'il n'y a aucune alerte active, aucun résumé n'est envoyé. Le résumé n'inclut pas d'informations concernant les alertes passées qui ne sont plus actives. Par exemple, si un utilisateur trouve une sauvegarde échouée et supprime l'alerte, ou qu'il relance une sauvegarde et que celle-ci réussit avant que le résumé ne soit généré, l'alerte ne sera plus présente et le résumé ne l'affichera pas.
- **Notifications de contrôle des terminaux** (désactivées par défaut)
  Les notifications concernant les tentatives d'utilisation de terminaux et de ports restreints par des plans de protection avec le module de contrôle des terminaux activé.
- **Notifications de restauration** (désactivées par défaut)
  Les notifications concernant les actions de récupération sur les ressources suivantes : messages e-mail et boîte aux lettres complètes d'utilisateurs, dossiers publics, OneDrive / GoogleDrive :

OneDrive complet et fichiers ou dossiers, Fichiers SharePoint, Teams : canaux, équipes complètes, messages e-mail et sites d'équipe.

Dans le cadre de ces notifications, les actions suivantes sont considérées comme des actions de restauration : envoi en tant qu'e-mail, téléchargement ou lancement d'une opération de récupération.

- **Notifications de prévention de perte de données** (désactivées par défaut)
  Notifications concernant les alertes de prévention de la perte de données relatives à l'activité de cet utilisateur sur le réseau.
- **Notifications d'incident de sécurité** (désactivées par défaut)
  Les notifications concernant la détection de malwares durant les analyses lors de l'accès, lors de l'exécution ou à la demande, et concernant les éléments détectés par le moteur de comportement et par le moteur de filtrage d'URL.

  Il existe deux options disponibles : **Atténué** et **Non atténué**. Ces options sont pertinentes pour les alertes d'incident de protection évolutive des points de terminaison, les alertes de protection évolutive des points de terminaison issues des flux d'informations sur les menaces et des alertes individuelles (pour les charges de travail dans lesquelles la protection évolutive des points de terminaison n'est pas activée).

  Lors de la création d'une alerte EDR, un e-mail est envoyé à l'utilisateur pertinent. Si le statut de la menace identifiée dans l'incident change, un nouvel e-mail est envoyé. Les e-mails comportent des boutons d'action qui permettent à l'utilisateur de voir les détails de l'incident (s'il a été atténué), ou de mener une enquête et de traiter l'incident (s'il n'a pas été atténué).
- **Notifications d'infrastructure** (désactivées par défaut)
  Notifications concernant des problèmes avec l'infrastructure de reprise d'activité après sinistre : lorsque l'infrastructure de reprise d'activité après sinistre ou les tunnels VPN ne sont pas disponibles.

Toutes les notifications sont envoyées à l'adresse e-mail de l'utilisateur.

Notifications reçues par rôle utilisateur

Les notifications envoyées par Cyber Protection dépendent du rôle utilisateur.

Types de notification\Rôle utilisateur	Utilisateur	Administrateur client
Notifications pour tous les périphériques	Oui	Oui
Notifications pour tous les périphériques de votre organisation	N/D	Oui (à l'exception des **notifications d'incident de sécurité**)
Notifications pour Microsoft 365, Google Workspace et les autres sauvegardes basées sur le Cloud	N/D	Oui

Types de notification\Rôle utilisateur	Utilisateur	Administrateurs de clients et d'unités	Administrateur partenaire et dossier

Notifications pour tous les périphériques	Oui	Oui	n/d*
Notifications pour tous les périphériques des locataires enfants	N/D	Oui	Oui
Notifications pour Microsoft 365, Google Workspace et les autres sauvegardes basées sur le Cloud	N/D	Oui	Oui

* Les administrateurs partenaires ne peuvent pas enregistrer leurs propres périphériques, mais ils peuvent créer leurs propres comptes administrateur client et s'en servir pour ajouter leurs propres périphériques. Voir Comptes utilisateur et locataires.

Désactivation et activation d'un compte utilisateur

Il se peut que vous deviez désactiver un compte utilisateur afin de restreindre temporairement son accès à la plate-forme Cloud.

Pour désactiver un compte utilisateur

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez le compte utilisateur que vous souhaitez désactiver, puis cliquez sur l'icône en forme de points de suspension > **Désactiver**.
3. Confirmez votre action en cliquant sur **Désactiver**.

Par conséquent, cet utilisateur ne pourra plus utiliser la plate-forme Cloud ni recevoir de notifications.

Pour activer un compte utilisateur désactivé, sélectionnez-le dans la liste des utilisateurs, puis cliquez sur l'icône en forme de points de suspension > **Activer**.

Suppression d'un compte utilisateur

Il se peut que vous deviez supprimer un compte utilisateur de façon permanente afin de libérer les ressources qu'il utilise, comme de l'espace de stockage ou une licence. Les statistiques d'utilisation seront mises à jour sous un jour après suppression. En ce qui concerne les comptes contenant beaucoup de données, il se peut que ce délai soit plus long.

Avant de supprimer un compte utilisateur, vous devez le désactiver. Pour en savoir plus sur la façon de procéder, reportez-vous à « Désactivation et activation d'un compte utilisateur ».

Important
La suppression d'un compte utilisateur est irréversible !

Pour supprimer un compte utilisateur

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez le compte utilisateur désactivé, puis cliquez sur l'icône en forme de points de suspension > **Supprimer**.
3. Pour confirmer votre action, saisissez votre identifiant, puis cliquez sur **Supprimer**.

En conséquence :

- Ce compte utilisateur sera supprimé.
- Toutes les données appartenant à ce compte utilisateur seront supprimées.
- Toutes les machines associées à ce compte utilisateur seront désenregistrées.

Transférer la propriété d'un compte utilisateur

Il se peut que vous deviez transférer la propriété d'un compte utilisateur si vous souhaitez conserver l'accès aux données d'un utilisateur restreint.

Important
Vous ne pouvez pas réaffecter le contenu d'un compte supprimé.

Pour transférer la propriété d'un compte utilisateur :

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez le compte utilisateur dont vous souhaitez transférer la propriété, puis cliquez sur l'icône en forme de crayon dans la section **Informations générales**.
3. Remplacez l'adresse e-mail existante par l'adresse e-mail du futur propriétaire du compte, puis cliquez sur **Terminé**.
4. Confirmez votre action en cliquant sur **Oui**.
5. Laissez le futur propriétaire du compte valider son adresse e-mail en suivant les instructions qui lui seront envoyées.
6. Sélectionnez le compte utilisateur dont vous transférez la propriété, puis cliquez sur l'icône en forme de points de suspension > **Réinitialiser le mot de passe**.
7. Confirmez votre action en cliquant sur **Réinitialiser**.
8. Laissez le futur propriétaire du compte réinitialiser le mot de passe en suivant les instructions qui lui seront envoyées par e-mail.

Le nouveau propriétaire peut désormais accéder à ce compte.

Configurer l'authentification à deux facteurs

L'authentification à deux facteurs (2FA) est un type d'authentification à plusieurs facteurs, qui vérifie l'identité d'un utilisateur en utilisant une association de deux facteurs différents :

- Un élément qu'un utilisateur connaît (un code PIN ou un mot de passe)
- Un élément qu'un utilisateur possède (un jeton)
- Un élément qui fait partie d'un utilisateur (biométrie)

L'authentification à deux facteurs vous protège davantage contre l'accès non autorisé à votre compte.

La plate-forme est compatible avec l'authentification par **mot de passe unique basée sur le temps (TOTP)** . Si l'authentification TOTP est activée dans le système, les utilisateurs doivent saisir leur mot de passe habituel ainsi que le code TOTP unique pour accéder au système. En d'autres termes, un utilisateur fournit le mot de passe (premier facteur) et le code TOTP (second facteur). Le code TOTP est généré dans l'application d'authentification de l'appareil qui applique le second facteur, sur la base de l'heure actuelle et du code secret (QR code ou code alphanumérique) fourni par la plateforme.

Fonctionnement

1. Vous activez l'authentification à deux facteurs au niveau de votre organisation.
2. Tous les utilisateurs de l'organisation doivent installer une application d'authentification sur l'appareil qui applique le second facteur (téléphone mobile, ordinateur portable ou de bureau, ou tablette). Cette application sera utilisée pour générer des codes TOTP uniques. Les authentificateurs recommandés sont les suivants :
   - Google Authenticator
     Version de l'application iOS (https://apps.apple.com/app/google-authenticator/id388497605)
     Version Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     Version de l'application iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Version Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Important
   Les utilisateurs doivent s'assurer que l'heure indiquée sur le périphérique sur lequel l'application d'authentification est installée est correctement définie, et reflète bien l'heure actuelle.
3. Les utilisateurs de votre organisation doivent se reconnecter au système.
4. Après avoir saisi leur identifiant et leur mot de passe, ils seront invités à configurer l'authentification à deux facteurs pour leur compte utilisateur.
5. Ils doivent scanner le QR code en utilisant leur application d'authentification. S'il est impossible de scanner le QR code, ils peuvent utiliser le code secret TOTP affiché en dessous et l'ajouter manuellement dans l'application d'authentification.

Important
Il est fortement recommandé de l'enregistrer (imprimez le QR code, notez le code secret TOTP, utilisez l'application compatible avec la sauvegarde de codes dans un Cloud). Vous aurez besoin du code secret TOTP pour réinitialiser l'authentification à deux facteurs si vous perdez l'appareil qui applique le second facteur.

6. Le code TOTP unique sera généré dans l'application d'authentification. Il est automatiquement régénéré toutes les 30 secondes.
7. Sur l'écran « Configurer l'authentification à deux facteurs », les utilisateurs doivent saisir le code TOTP après avoir saisi leur mot de passe.
8. En conséquence, l'authentification à deux facteurs sera configurée pour les utilisateurs.

Désormais, lorsque les utilisateurs se connecteront au système, ils seront invités à fournir l'identifiant et le mot de passe, puis le code TOTP unique généré dans l'application d'authentification. Les utilisateurs peuvent indiquer que le navigateur est un navigateur fiable lorsqu'ils se connectent au système. Le code TOTP ne sera pas demandé lors des connexions suivantes effectuées avec ce navigateur.

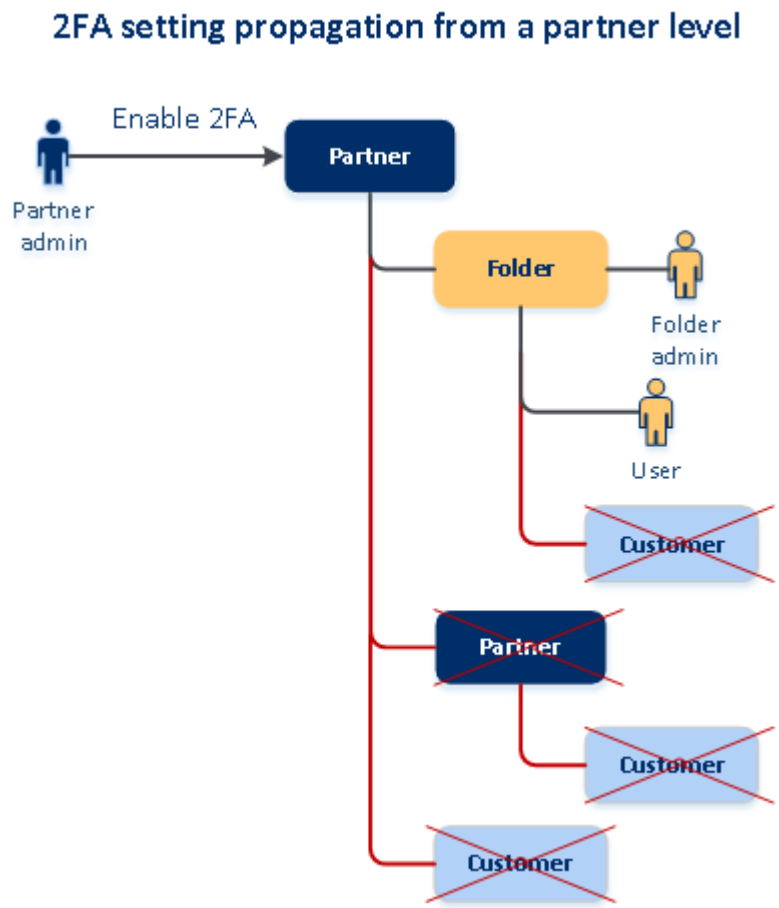
Propagation de la configuration de l'authentification à deux facteurs à tous les niveaux de locataires

L'authentification à deux facteurs est définie au niveau de l'**organisation**. Vous pouvez activer ou désactiver l'authentification à deux facteurs :

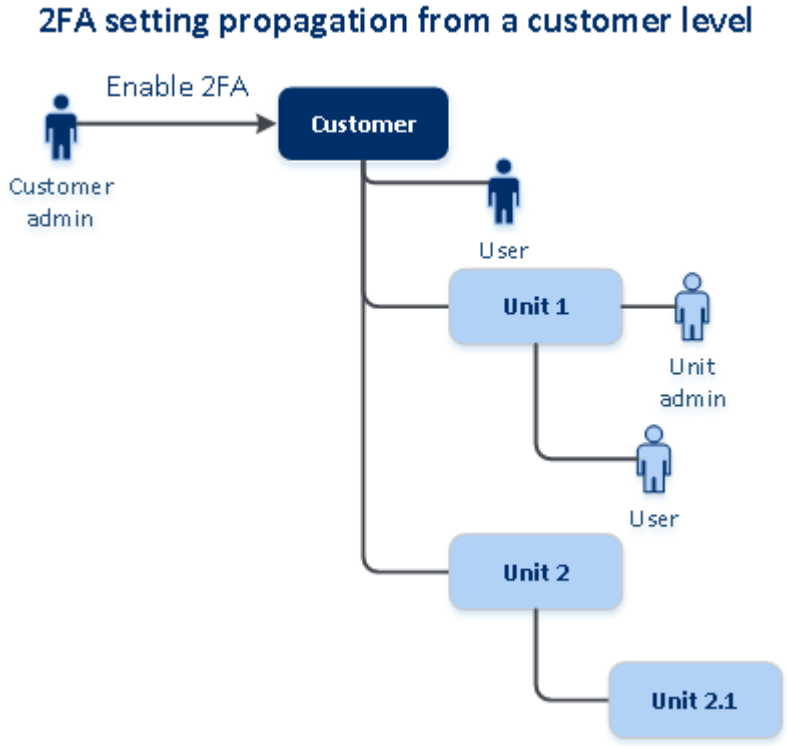
- Pour votre propre organisation.
- Pour votre locataire enfant (uniquement si l'option **Accès à l'assistance** est activée au sein de ce locataire enfant).

Les paramètres de l'authentification à deux facteurs se propagent à tous les niveaux de locataires de la façon suivante :

- Les dossiers héritent automatiquement des paramètres d'authentification à deux facteurs de l'organisation partenaire. Dans le modèle ci-dessous, les lignes rouges signifient que la propagation des paramètres de l'authentification à deux facteurs n'est pas possible.



- Les unités héritent automatiquement des paramètres d'authentification à deux facteurs de l'organisation cliente.



Remarque

1. Vous pouvez activer ou désactiver l'authentification à deux facteurs pour vos organisations enfants uniquement si l'option **Accès à l'assistance** est activée au sein des organisations enfants en question.
2. Vous pouvez gérer les paramètres d'authentification à deux facteurs pour les utilisateurs des organisations enfants uniquement si l'option **Accès à l'assistance** est activée au sein des organisations enfants en question.
3. Il est impossible de configurer l'authentification à deux facteurs au niveau du dossier ou de l'unité.
4. Vous pouvez configurer l'authentification à deux facteurs même si votre organisation parente n'a pas activé ce paramètre.

Configurer l'authentification à deux facteurs pour votre locataire

En tant qu'administrateur, vous pouvez activer l'authentification à deux facteurs pour votre organisation.

Pour activer l'authentification à deux facteurs pour votre locataire

1. Dans le portail de gestion, accédez à **Paramètres** > **Sécurité**.
2. Faites glisser le commutateur **Authentification à deux facteurs**, puis cliquez sur **Activer**.

À présent, tous les utilisateurs dans l'organisation doivent configurer l'authentification à deux facteurs pour leur compte. Ils seront invités à le faire la prochaine fois qu'ils essaieront de se connecter ou lors de l'expiration de leur session actuelle.

La barre de progression sous le commutateur affiche le nombre d'utilisateurs ayant configuré l'authentification à deux facteurs pour leur compte. Pour vérifier quels utilisateurs ont configuré leur compte, accédez à **Gestion d'entreprise** > onglet **Utilisateurs**, puis consultez la colonne **Statut 2FA**. Le statut 2FA (authentification à deux facteurs) des utilisateurs qui n'ont pas encore configuré ce type d'authentification pour leur compte est **Configuration requise**.

Une fois la configuration de l'authentification à deux facteurs réussie, les utilisateurs devront saisir leur identifiant, leur mot de passe et un code TOTP à chaque connexion à la console de service.

Pour désactiver l'authentification à deux facteurs pour votre locataire

1. Dans le portail de gestion, accédez à **Paramètres** > **Sécurité**.
2. Pour désactiver l'authentification à deux facteurs, désactivez le commutateur, puis cliquez sur **Désactiver**.
3. [Si au moins un utilisateur au sein de l'organisation a configuré l'authentification à deux facteurs] Saisissez le code TOTP généré dans l'application d'authentification de votre terminal mobile.

En conséquence, l'authentification à deux facteurs est désactivée pour votre organisation, tous les secrets sont supprimés et tous les navigateurs fiables sont oubliés. Tous les utilisateurs se

connecteront au système en utilisant uniquement leur identifiant et leur mot de passe. Dans **Gestion d'entreprise** > onglet **Utilisateurs**, la colonne **Statut 2FA** est masquée.

Gestion de l'authentification à 2 facteurs pour les utilisateurs

Vous pouvez surveiller les paramètres d'authentification à deux facteurs de tous vos utilisateurs et réinitialiser les paramètres dans le portail de gestion, dans **Gestion de l'entreprise** > **Utilisateurs**.

Surveillance

Dans le portail de gestion, sous **Gestion d'entreprise** > **Utilisateurs**, vous pouvez voir la liste de tous les utilisateurs de votre organisation. Le **statut 2FA** indique si l'authentification à deux facteurs est configurée pour un utilisateur.

Pour réinitialiser l'authentification à deux facteurs pour un utilisateur

1. Dans le portail de gestion, accédez à **Gestion de l'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Réinitialiser l'authentification à deux facteurs**.
4. Saisissez le code TOTP généré dans l'application d'authentification de l'appareil qui applique le second facteur, puis cliquez sur **Réinitialiser**.

En conséquence, l'utilisateur pourra de nouveau configurer l'authentification à deux facteurs.

Pour réinitialiser les navigateurs fiables pour un utilisateur

1. Dans le portail de gestion, accédez à **Gestion de l'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Réinitialiser tous les navigateurs fiables**.
4. Saisissez le code TOTP généré dans l'application d'authentification de l'appareil qui applique le second facteur, puis cliquez sur **Réinitialiser**.

L'utilisateur pour qui vous avez réinitialisé tous les navigateurs fiables devra fournir le code TOTP lors de sa prochaine connexion.

Les utilisateurs peuvent eux-mêmes réinitialiser tous les navigateurs fiables, ainsi que les paramètres d'authentification à deux facteurs. Cette opération peut être effectuée lorsqu'ils se connectent au système, en cliquant sur le lien respectif et en saisissant le code TOTP pour confirmer l'opération.

Pour désactiver l'authentification à deux facteurs pour un utilisateur

Nous ne recommandons pas de désactiver l'authentification à deux facteurs parce que cela peut créer des brèches dans la sécurité des tenants.

À titre d'exception, vous pouvez désactiver l'authentification à deux facteurs pour un utilisateur et la conserver pour tous les autres utilisateurs du tenant. C'est une solution de contournement pour les cas où l'authentification à deux facteurs est activée au sein d'un tenant où une configuration cloud est configurée, et où cette intégration s'authentifie sur la plate-forme via le compte utilisateur (identifiant et mot de passe). Pour poursuivre l'utilisation de l'intégration en tant que solution temporaire, il est possible de transformer l'utilisateur en un compte de service auquel l'authentification à deux facteurs n'est pas applicable.

Important
La transformation d'utilisateurs standard en utilisateurs de service afin de désactiver l'authentification à deux facteurs n'est pas recommandée parce qu'elle est risquée pour la sécurité des tenants.

La solution sûre et recommandée pour l'utilisation d'intégrations cloud sans désactivation de l'authentification à deux facteurs pour les tenants consiste à créer des clients API et à configurer vos intégrations cloud de manière à ce qu'elles fonctionnent de concert.

1. Dans le portail de gestion, accédez à **Gestion de l'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Marquer comme compte de service**. En conséquence, un utilisateur reçoit un statut spécial d'authentification à deux facteurs, appelé **Compte de service.**
4. [Si au moins un utilisateur au sein d'un locataire a configuré l'authentification à deux facteurs] Pour confirmer la désactivation, saisissez le code TOTP généré dans l'application d'authentification de l'appareil qui applique le second facteur.

Pour activer l'authentification à deux facteurs pour un utilisateur

Vous devrez peut-être activer l'authentification à deux facteurs pour un utilisateur en particulier, pour qui vous l'aviez auparavant désactivée.

1. Dans le portail de gestion, accédez à **Gestion de l'entreprise** > **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, recherchez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
3. Cliquez sur **Marquer comme compte normal**. En conséquence, un utilisateur devra configurer l'authentification à deux facteurs ou fournir le code TOTP lorsqu'il accèdera au système.

Réinitialisation de l'authentification à deux facteurs en cas de perte de l'appareil qui applique le second facteur

Pour réinitialiser l'accès à votre compte en cas de perte de l'appareil qui applique le second facteur, suivez l'une des approches suggérées :

- Restaurez votre code secret TOTP (QR code ou code alphanumérique) depuis une sauvegarde. Utilisez un autre appareil appliquant le second facteur et ajoutez le code secret TOTP dans l'application d'authentification installé sur ce périphérique.
- Demandez à votre administrateur de réinitialiser les paramètres de l'authentification à deux facteurs pour vous.

Protection contre les attaques en force brute

Une attaque en force brute est une attaque au cours de laquelle un intrus tente d'accéder au système en soumettant plusieurs mots de passe, dans l'espoir que l'un de ces mots de passe soit correct.

Le mécanisme de protection contre les attaques en force brute de la plateforme est basé sur les cookies de périphérique.

Les paramètres de protection contre les attaques en force brute qui sont utilisés sur la plateforme sont prédéfinis :

Paramètre	Saisie du mot de passe	Saisie du code TOTP
Limite de tentatives	10	5
Période de la limite de tentatives (la limite est réinitialisée une fois le délai expiré)	15 min (900 s)	15 min (900 s)
Le verrouillage a lieu au	Limite de tentatives + 1 (11e tentative)	Limite de tentatives
Période de verrouillage	5 min (300 s)	5 min (300 s)

Si vous avez activé l'authentification à deux facteurs, un cookie de périphérique est envoyé au client (navigateur) uniquement après que l'authentification ait réussi à l'aide des deux facteurs (mot de passe et code TOTP).

Pour les navigateurs fiables, le cookie de périphérique est envoyé après que l'authentification ait réussi uniquement à l'aide d'un facteur (mot de passe).

Les tentatives de saisie de code TOTP sont enregistrées pour chaque utilisateur, et non pour chaque périphérique. Cela signifie que si un utilisateur tente de saisir le code TOTP à l'aide de différents périphériques, il sera bloqué.

Configuration de scénarios de vente additionnelle pour vos clients

La vente additionnelle est une technique consistant à inviter vos clients à acheter des fonctionnalités supplémentaires.

Cyber Protection possède plusieurs éditions différentes, dont les fonctionnalités et le prix varient. Nous vous invitons à promouvoir des éditions plus onéreuses et proposant des capacités plus avancées auprès des clients qui utilisent déjà une édition de base.

Vous pouvez activer ou désactiver la capacité de vente additionnelle par client. Par défaut, l'option de vente additionnelle est désactivée. Si vous activez la vente additionnelle pour un client, celui-ci verra des fonctionnalités supplémentaires qui ne seront pas disponibles tant qu'il n'aura pas acheté l'édition promue. Ces fonctionnalités supplémentaires sont identifiées par des étiquettes qui montrent le nom ou les icônes de l'édition promue, le tout surligné en orange. Ces arguments de vente additionnelle seront présentés au client, pour l'encourager à acheter une édition plus onéreuse. Lorsque le client clique sur ces arguments de vente additionnelle, une boîte de dialogue s'affiche et l'encourage à acheter une édition plus onéreuse afin d'activer les fonctionnalités désirées.

L'appel à l'action dépend du type d'utilisateur client. Le type d'utilisateur (acheteur ou non-acheteur) peut être configuré à l'aide de l'API de plate-forme. Pour en savoir plus, consultez la documentation de l'API. Pour en savoir plus sur les appels à l'action qui s'affichent chez vos clients, consultez le tableau ci-dessous :

Type d'utilisateurs dans le locataire client	Appel à l'action
Administrateur ; acheteur	Le bouton **Acheter maintenant** s'affiche dans l'interface utilisateur.*
Administrateur ; pas acheteur	Le message « Contactez votre partenaire pour mettre l'édition à niveau » s'affiche dans l'interface utilisateur.
Utilisateur ; acheteur	Le message « Contactez votre partenaire pour mettre l'édition à niveau » s'affiche dans l'interface utilisateur.
Utilisateur ; pas acheteur	Le message « Contactez votre partenaire pour mettre l'édition à niveau » s'affiche dans l'interface utilisateur.

* Le lien du bouton **Acheter maintenant**, qui redirigera un client vers un site Web lui permettant d'acheter une édition plus avancée, peut être configuré dans **Paramètres** > **Marque**. Dans la section **Vente additionnelle**, vous pouvez spécifier l'**URL d'achat**. Les paramètres de marque seront appliqués à tous les partenaires/dossiers enfants et clients directs et indirects du locataire où la marque est configurée.

Pour activer ou désactiver la capacité de vente additionnelle pour un client.

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le client, accédez au volet de droite, puis cliquez sur l'onglet **Configurer**.
3. Dans la section **Vente additionnelle**, procédez comme suit :
   - Activez l'option **Promouvoir des éditions plus avancées**, pour activer le scénario de vente additionnelle pour les clients.
   - Désactivez l'option **Promouvoir des éditions plus avancées**, pour désactiver le scénario de vente additionnelle pour les clients.

Arguments de vente additionnelle présentés au client

Liste des vulnérabilités

Dans la console de service, la liste des vulnérabilités est disponible dans **Gestion de logiciel** > **Vulnérabilités**. Lorsque le client clique sur l'icône en forme de pansement, la boîte de dialogue de promotion de l'édition s'ouvre et invite l'utilisateur à acheter l'édition plus onéreuse.

Créer ou modifier un plan de protection

Dans la console de service, accédez à **Plans** > **Protection**. Cliquez sur **Création d'un plan**. Pour les éditions Cyber Backup, seuls les modules **Sauvegarde** et **Vulnérabilité** sont activés. Les autres modules ne sont disponibles que dans les éditions Cyber Protect. Votre client pourra activer tous les modules une fois qu'il aura acheté l'une des éditions Cyber Protect.

Assistant de découverte automatique

Dans la console de service, cet assistant se trouve dans **Périphériques** > **Tous les périphériques**. Votre client doit lancer l'assistant de découverte automatique en cliquant sur **Ajouter**, puis en accédant à la section **Périphériques multiples** et en cliquant sur **Windows uniquement**. Les méthodes de découverte automatique de machines seront disponibles uniquement dans les éditions avancées.

Actions dans la liste des périphériques.

Dans la console de service, cette liste se trouve dans **Périphériques** > **Tous les périphériques**. Votre client doit sélectionner la machine, puis deux autres options s'afficheront dans le volet de gauche :

- **Se connecter via un client HTML5**
- **Correctif**

Ces options ne seront disponibles que si le client achète une version plus onéreuse que la version existante.

Gérer les emplacements et le stockage

La section **Paramètres** > **Emplacements** affiche les stockages dans le Cloud et les infrastructures de reprise d'activité après sinistre que vous pouvez utiliser pour fournir les services **Cyber Protection** et **File Sync & Share** à vos partenaires et clients.

Les stockages configurés pour d'autres services s'afficheront dans la section **Emplacements** dans les prochaines versions.

Emplacements

Un emplacement est un conteneur qui vous permet de regrouper les stockages Cloud et les infrastructures de reprise d'activité après sinistre de façon pratique. Ce conteneur peut être ce que vous voulez, par exemple un centre de données spécifique ou l'emplacement géographique des composants de votre infrastructure.

Vous pouvez créer un nombre illimité d'emplacements et les peupler à l'aide de stockages de sauvegarde, d'infrastructures de reprise d'activité après sinistre, et de stockages **de File Sync & Share**. Un emplacement peut contenir plusieurs stockages Cloud, mais une seule infrastructure de reprise d'activité après sinistre.

Pour en savoir plus sur les opérations que vous pouvez réaliser avec les stockages, consultez la section « Gérer le stockage ».

Choisir les emplacements et les stockages pour les partenaires et les clients

Lors de la création d'un locataire partenaire/dossier, vous pouvez sélectionner plusieurs emplacements et plusieurs stockages par service au sein de ces emplacements, qui seront disponibles dans le nouveau locataire.

Lors de la création d'un locataire client, vous devez sélectionner un emplacement, puis un stockage par service au sein de cet emplacement. Les stockages affectés au client peuvent être modifiés ultérieurement, mais uniquement si leur utilisation est de 0 Go, c'est-à-dire, soit avant que le client n'ait commencé à utiliser le stockage, soit après qu'il a supprimé toutes les sauvegardes de ce stockage.

Les informations concernant les stockages affectés à un locataire client sont affichées dans le volet d'informations locataire lorsque le locataire est sélectionné dans l'onglet **Clients**. Les informations concernant l'utilisation de l'espace de stockage ne sont pas mises à jour en temps réel. Veuillez prévoir jusqu'à 24 heures pour que les informations soient mises à jour.

Opérations avec les emplacements

Pour créer un emplacement, cliquez sur **Ajouter un emplacement**, puis saisissez le nom de l'emplacement.

Pour déplacer un stockage ou une infrastructure de reprise d'activité après sinistre vers un autre emplacement, sélectionnez le stockage ou l'infrastructure en question, cliquez sur l'icône en forme de crayon dans le champ **Emplacement**, puis sélectionnez l'emplacement cible.

Pour renommer un emplacement, cliquez sur l'icône en forme de points de suspension à côté du nom de l'emplacement en question, cliquez sur **Renommer**, puis saisissez le nouveau nom de l'emplacement.

Pour supprimer un emplacement, cliquez sur l'icône en forme de points de suspension à côté du nom de l'emplacement en question, cliquez sur **Supprimer**, puis confirmez votre choix. Seuls les emplacements vides peuvent être supprimés.

Gestion du stockage

Ajouter de nouveaux stockages

- Service **Cyber Protection** :
  - Par défaut, les stockages de sauvegarde sont situés dans les centres de données .
  - Si l'élément **Stockage de sauvegarde appartenant à un partenaire** est activé pour un locataire partenaire par un administrateur de haut niveau, les administrateurs partenaires peuvent organiser le stockage dans le propre centre de données du partenaire, en utilisant le logiciel de Cyber Infrastructure de . Cliquez sur **Ajouter un stockage de sauvegarde** dans la section **Emplacements** pour obtenir des informations sur la manière d'organiser un stockage de sauvegarde dans votre propre centre de données.
  - Si l'élément **Infrastructure de reprise d'activité après sinistre appartenant à un partenaire** est activé pour un locataire partenaire par un administrateur de haut niveau, les administrateurs partenaires peuvent organiser une infrastructure de reprise d'activité après sinistre dans le propre centre de données du partenaire. Pour des informations concernant l'ajout d'une infrastructure de reprise d'activité après sinistre, contactez l'assistance technique.

Remarque
La validation de la sauvegarde n'est pas possible avec les stockages d'objets du Cloud public, tels qu'Amazon S3, Microsoft Azure, Google Cloud Storage et Wasabi, utilisés par les centres de données .
La validation de la sauvegarde est possible avec les stockages d'objets du Cloud public utilisés par les partenaires . Il n'est toutefois pas recommandé de l'activer, car les opérations de validation augmentent le transfert de données vers des emplacements externes depuis ces stockages d'objets publics et peuvent conduire à des dépenses considérables.

- Pour des informations concernant l'ajout de stockages qui seront utilisés par d'autres services, contactez l'assistance technique.

Suppresion de stockages

Vous pouvez supprimez des stockages qui ont été ajoutés par vous ou par vos locataires enfants.

Si le stockage est attribué à un locataire client, vous devez désactiver le service qui utilise le stockage pour tous les locataires clients avant de supprimer le stockage.

Pour supprimer un stockage

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire pour lequel le stockage a été ajouté.
3. Cliquez sur **Paramètres** > **Emplacements**.
4. Sélectionnez le stockage que vous souhaitez supprimer.

5. Dans le volet Propriétés de stockage, cliquez sur l'icône en forme de points de suspension, puis sur **Supprimer stockage**.
6. Confirmez votre choix.

Configuration d'un stockage immuable

Vous pouvez configurer le stockage immuable au niveau du partenaire et du client.

Pour les tenants partenaires, aucun mode de stockage immuable ne doit être sélectionné. Un administrateur peut désactiver et réactiver le stockage immuable, et modifier son mode et sa période de rétention.

Pour les tenants de clients, le stockage immuable est disponible dans les modes suivants :

- **Mode de gouvernance**
  Dans ce mode, un administrateur peut désactiver et réactiver le stockage immuable, et modifier son mode et sa période de rétention.
- **Mode de conformité**
  Une fois que ce mode est sélectionné, le stockage immuable ne peut pas être désactivé, et son mode ou sa période de rétention ne peuvent plus être modifiés.

Si aucun paramètre personnalisé n'est appliqué à un tenant enfant, celui-ci hérite des paramètres du tenant parent.

Vous pouvez configurer les paramètres de stockage immuable uniquement si l'authentification à deux facteurs est activée pour le tenant à qui le compte administrateur appartient.

Les sauvegardes supprimées dans le stockage immuable continuent à utiliser de l'espace de stockage et sont facturées en conséquence.

Remarque
À partir de la version 21.12, le stockage immuable avec une période de rétention de 14 jours est activé par défaut pour les nouveaux tenants partenaires. Pour les tenants existants, vous devez activer le stockage immuable manuellement.

Pour activer le stockage immuable d'un tenant partenaire

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Paramètres** > **Sécurité**.
2. Activez le commutateur **Stockage immuable**.
3. Spécifiez une période de rétention comprise entre 14 et 999 jours.
   Par défaut, la période de rétention est de 14 jours. Une période de rétention plus longue pourrait augmenter l'utilisation du stockage.
4. Cliquez sur **Enregistrer**.

Pour désactiver le stockage immuable d'un tenant partenaire

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Paramètres** > **Sécurité**.
2. Désactivez le commutateur **Stockage immuable**.

   Avertissement !
   Cette modification sera héritée par tous les tenants enfants qui n'utilisent pas de paramètres personnalisés pour le stockage immuable. Toutes les sauvegardes supprimées seront définitivement effacées. La suppression des nouvelles sauvegardes sera elle aussi permanente.

3. Confirmez votre choix en cliquant sur **Désactiver**.

Pour activer le stockage immuable d'un tenant client

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Clients**.
2. Pour modifier les paramètres d'un tenant client, cliquez sur son nom.
3. Dans le menu de navigation, accédez à **Paramètres** > **Sécurité**.
4. Activez le commutateur **Stockage immuable**.
5. Spécifiez une période de rétention comprise entre 14 et 999 jours.
   Par défaut, la période de rétention est de 14 jours. Une période de rétention plus longue pourrait augmenter l'utilisation du stockage.
6. Sélectionnez le mode de stockage immuable.

   Avertissement !
   La sélection du **mode de conformité** est irréversible. Vous ne pouvez plus désactiver le stockage immuable ni modifier son mode ou sa période de rétention.

7. Cliquez sur **Enregistrer**.

Pour désactiver le stockage immuable d'un tenant client

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Clients**.
2. Pour modifier les paramètres d'un tenant client, cliquez sur son nom.
3. Dans le menu de navigation, accédez à **Paramètres** > **Sécurité**.
4. Désactivez le commutateur **Stockage immuable**.

   Remarque
   Vous pouvez désactiver le stockage immuable uniquement en mode de gouvernance.

   Avertissement !
   Si vous désactivez le stockage immuable, toutes les sauvegardes seront définitivement supprimées. La suppression des nouvelles sauvegardes sera elle aussi permanente.

5. Confirmez votre choix en cliquant sur **Désactiver**.

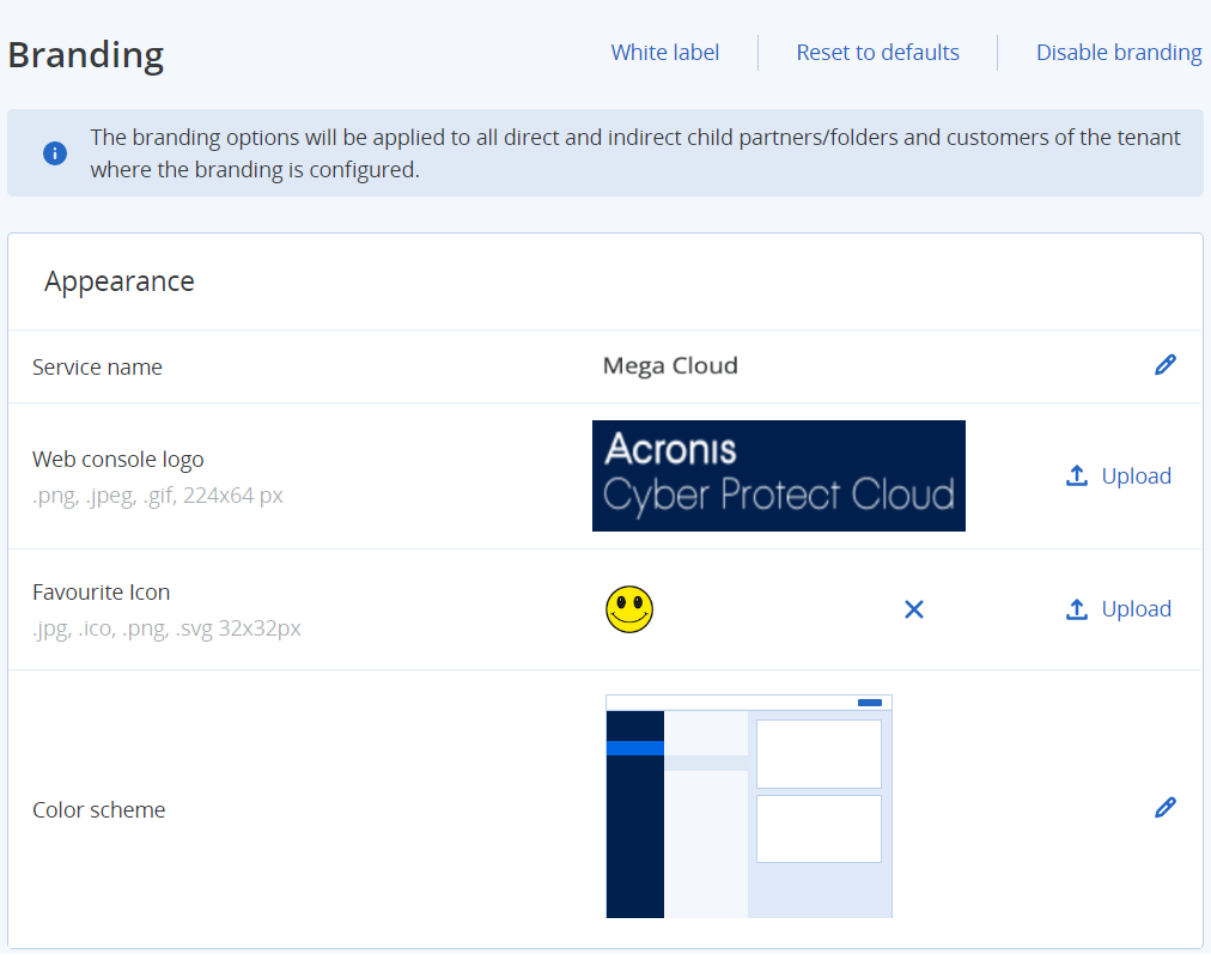
Limites

- Le stockage immuable est disponible pour les stockages hébergés par Acronis et pour ceux hébergés par des partenaires. Ces stockages doivent, par ailleurs, utiliser Acronis Cyber Infrastructure 4.7.1 ou une version ultérieure.

  Le stockage immuable requiert que le port TCP 40440 soit ouvert pour le service Backup Gateway dans Acronis Cyber Infrastructure. Dans la version 4.7.1 et les versions ultérieures, le port TCP 40440 est automatiquement ouvert avec le type de trafic **Sauvegarde (ABGW) publique**. Pour plus d'informations sur les types de trafic, reportez-vous à la documentation concernant Acronis Cyber Infrastructure.
- Le stockage immuable nécessite un agent de protection version 21.12 (15.0.28532) ou ultérieure.
- Seules les sauvegardes TIBX (version 12) sont prises en charge.

Configuration de la marque et de la marque blanche

La section **Paramètres** > **Marque** permet aux administrateurs partenaires de personnaliser l'interface utilisateur du portail de gestion et le service **Cyber Protection** pour supprimer toute association avec les partenaires de niveau supérieur.



La marque peut être configurée aux niveaux partenaire et dossier. La marque est appliquée à tous les partenaires/dossiers enfants et clients directs et indirects du locataire où la marque est configurée.

D'autres services fournissent des fonctionnalités de marque séparées dans leur console de service. Pour obtenir davantage d'informations, consultez les guides de l'utilisateur des services correspondants.

Éléments de marquage

Apparence

- **Nom du service**. Ce nom est utilisé dans tous les e-mails envoyés par le portail de gestion et les services Cloud (messages d'activation de compte, e-mail de notification de service), sur l'écran d'**accueil** après la première connexion au portail de gestion, et dans le nom de l'onglet du navigateur du portail de gestion.
- **Logo de la console Web**. Le logo est également affiché dans le portail de gestion et les services. Cliquez sur **Transférer** pour transférer un fichier image.
- **Icône favorite** [disponible uniquement si une URL personnalisée est configurée]. L'icône favorite s'affiche à côté du titre de la page dans l'onglet du navigateur. Cliquez sur **Transférer** pour transférer un fichier image.
- **Modèle de couleurs**. Le modèle de couleurs définit la combinaison de couleurs utilisée pour tous les éléments de l'interface utilisateur.

Remarque
Cliquez sur **Prévisualiser le schéma dans un nouvel onglet** pour voir à quoi ressemblera l'interface pour vos locataires enfants. La marque ne s'appliquera pas tant que vous n'aurez pas cliqué sur **Terminé** dans le volet **Choisir le schéma de couleurs**.

Marque d'agent et d'installateur

Vous pouvez personnaliser la marque des fichiers d'installation de l'agent et de la zone de notification pour Windows et macOS.

Remarque
Pour activer cette fonctionnalité de marque, vous devez mettre à jour les agents Cyber Protection vers la version 15.0.28816 (22.01) ou une version ultérieure.

- **Nom de fichier de l'installateur de l'agent**. Le nom du fichier d'installation téléchargé sur les charges de travail protégées.
- **Logo de l'installateur de l'agent**. Le logo affiché dans l'assistant de configuration lors de l'installation de l'agent. Cliquez sur **Transférer** pour transférer un fichier image.
- **Nom de l'agent**. Le nom affiché dans l'assistant de configuration lors de l'installation de l'agent.

- **Nom du contrôle de la zone de notification**. Le nom affiché en haut de la fenêtre de contrôle de la zone de notification.

Documentation et assistance

- **URL de la page d'accueil**. Cette page s'ouvre lorsqu'un utilisateur clique sur le nom de société dans le volet **À propos de**.
- **URL du support technique**. Cette page s'ouvre lorsqu'un utilisateur clique sur le lien **Contacter le support** dans le volet **À propos de** ou dans un e-mail envoyé par le portail de gestion.
- **Téléphone du support**. Ce numéro de téléphone s'affiche dans le volet **À propos de**.
- **URL de la Base de connaissances**. Cette page s'ouvre lorsqu'un utilisateur clique sur le lien **Base de connaissances** dans un message d'erreur.
- **Guide de l'administrateur du portail de gestion**. Cette page s'ouvre lorsqu'un utilisateur clique sur l'icône en forme de point d'interrogation dans l'angle supérieur droit de l'interface utilisateur du portail de gestion, puis sur **À propos de** > **Guide administrateur**.
- **Aide de l'administrateur du portail de gestion**. Cette page s'ouvre lorsqu'un utilisateur clique sur l'icône en forme de point d'interrogation dans l'angle supérieur droit de l'interface utilisateur du portail de gestion, puis sur **Aide**.

URL des services Cyber Protect Cloud

Vous pouvez rendre les services Cyber Protect Cloud disponibles depuis votre domaine personnalisé. Cliquez sur **Configurer** pour définir une URL personnalisée pour la première fois, ou cliquez sur **Reconfigurer** pour en modifier une existante. Pour utiliser l'URL par défaut (https://cloud.acronis.com), cliquez sur **Réinitialiser les paramètres par défaut**. Pour en savoir plus sur les URL personnalisées, reportez-vous à « Configuration d'URL d'interface Web personnalisées ».

Paramètres de documents juridiques

- **URL du Contrat de licence d'utilisateur final (CLUF)**. Cette page s'ouvre lorsqu'un utilisateur clique sur le lien **Contrat de licence d'utilisateur final** dans le volet **À propos de** ou sur la page d'**Accueil** après la première connexion, et sur les pages de destination Requête de transfert File Sync & Share.
- **URL des conditions d'utilisation de la plate-forme**. Cette page s'ouvre lorsqu'un administrateur partenaire clique sur le lien **Conditions d'utilisation de la plate-forme** dans le volet **À propos de** ou sur la page d'**Accueil** après la première connexion.
- **URL de Déclaration de confidentialité**. Cette page s'ouvre lorsqu'un utilisateur clique sur le lien **Déclaration de confidentialité** sur la page d'**Accueil** après la première connexion, et sur les pages de destination Requête de transfert File Sync & Share.

Important
Si vous ne souhaitez pas qu'un document apparaisse sur l'écran d'accueil, ne saisissez pas d'URL pour ce document.

Remarque
Pour plus d'informations sur les Requêtes de transfert File Sync & Share, consultez la section Guide de l'utilisateur Cloud Cyber Files.

Vente incitative

- **URL d'achat**. Cette page s'ouvre lorsqu'un utilisateur clique sur **Acheter maintenant** pour mettre à niveau vers une version plus avancée du service Cyber Protection. Pour en savoir plus sur les scénarios de vente additionnelle, consultez la section « Configuration de scénarios de vente additionnelle pour vos clients ».

Applications mobiles :

- **App Store**. Cette page s'ouvre lorsqu'un utilisateur clique sur **Ajouter** > **iOS** dans le service **Cyber Protection**.
- **Google Play**. Cette page s'ouvre lorsqu'un utilisateur clique sur **Ajouter** > **Android** dans le service **Cyber Protection**.

Paramètres du serveur de courrier

Vous pouvez indiquer un serveur de messagerie personnalisé qui servira à envoyer des notifications par courrier électronique depuis le portail de gestion et les services. Pour indiquer un serveur de messagerie personnalisé, cliquez sur **Personnaliser**, puis indiquez les paramètres suivants :

- Dans le champ **De**, saisissez le nom qui apparaîtra dans le champ **De** des notifications par e-mail.
- Dans le champ **SMTP**, saisissez le nom du serveur de messagerie sortant (SMTP).
- Dans le champ **Port**, saisissez le port du serveur de messagerie sortant. Par défaut, le port est défini sur 25.
- Dans **Chiffrement**, choisissez le chiffrement que vous souhaitez utiliser, SSL ou TLS. Sélectionnez **Aucun** pour désactiver le chiffrement.
- Dans **Nom d'utilisateur** et **Mot de passe**, indiquez les informations d'identification d'un compte qui sera utilisé pour envoyer les messages.

Configuration de la marque

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire dans lequel vous souhaitez configurer le marquage.
3. Cliquez sur **Paramètres** > **Marque**.
4. [Si le marquage n'a pas encore été activé] Cliquez sur **Permettre le marquage**.
5. Configurez les éléments de marquage décrits ci-dessus.

Restauration des paramètres de marquage par défaut

Vous pouvez réinitialiser tous les éléments de marquage à leurs valeurs par défaut.

1. Connectez-vous au portail de gestion.
2. Accédez au tenant dans lequel vous souhaitez réinitialiser la marque.
3. Cliquez sur **Paramètres** > **Marque**.
4. En haut à droite, cliquez sur **Restaurer les paramètres par défaut**.

Désactivation de la marque

Vous pouvez désactiver la marque pour votre compte et tous les tenants enfants.

1. Connectez-vous au portail de gestion.
2. Accédez au tenant dans lequel vous souhaitez désactiver la marque.
3. Cliquez sur **Paramètres** > **Marque**.
4. En haut à droite, cliquez sur **Désactiver la marque**.

Commercialisation en marque blanche

Vous pouvez contrôler si l'agent Cyber Protection (pour Windows, macOS et Linux) et le moniteur Cyber Protection (pour Windows, macOS et Linux) seront de marque ou à marque blanche pour tous vos partenaires enfants et vos clients. Si vous activez la commercialisation en marque blanche, l'agent et le contrôle de la zone de notification seront à marque blanche. Ce paramètre affecte aussi les noms et les logos utilisés dans l'installateur et le moniteur Cyber Protection.

Application de la commercialisation en marque blanche

1. Connectez-vous au portail de gestion.
2. Accédez au tenant dans lequel vous souhaitez appliquer la commercialisation en marque blanche.
3. Cliquez sur **Paramètres** > **Marque**.
4. Dans la partie supérieure de la fenêtre, cliquez sur **Marque blanche** pour effacer tous les éléments de marquage, excepté le **Nom du service**, l'**URL du Contrat de licence d'utilisateur final (CLUF) URL**, le **Guide de l'administrateur du portail de gestion**, l'**Aide de l'administrateur du portail de gestion** et les **Paramètres du serveur de messagerie**.

Configuration d'URL d'interface Web personnalisées

Remarque
Une URL personnalisée pointera vers une autre adresse IP par rapport à l'URL par défaut. Gardez cette information à l'esprit lorsque vous configurez des règles de pare-feu.

Configurer l'URL d'interface Web pour les services Cyber Protect Cloud

1. Dans le portail de gestion, cliquez sur **Paramètres** > **Labellisation**.
2. Dans la section **URL des services Cyber Protect Cloud** :
   - Cliquez sur **Configurer** pour définir une URL personnalisée pour la première fois.
   - Cliquez sur **Reconfigurer** pour modifier l'URL personnalisée existante.
3. À l'étape **Paramètres de domaine**, préparez votre domaine et l'enregistrement CNAME.
   Pour utiliser une URL personnalisée, vous devez disposer d'un nom de domaine actif et d'un enregistrement CNAME configuré pour pointer vers le centre de données où se trouve votre compte. La configuration de l'enregistrement CNAME est effectuée par votre bureau d'enregistrement DNS et sa propagation peut prendre jusqu'à 48 heures.
   Pour trouver le nom de domaine de votre centre de données et demander la configuration de votre enregistrement CNAME, reportez-vous à l'article Labellisation de l'URL de la console Web (58275).
4. À l'étape **Vérifier votre URL**, vérifiez que votre URL personnalisée est accessible et que votre enregistrement CNAME est configuré correctement. Pour cela, saisissez le nom de l'URL principale, puis cliquez sur **Vérifier**. Si vous utilisez un certificat SSL avec caractères génériques, vous pouvez ajouter jusqu'à dix autres noms de domaine. Si vous utilisez un certificat « Let's Encrypt », les autres noms de domaine seront ignorés.
5. À l'étape **Certificat SSL**, vous pouvez effectuer l'une des opérations suivantes :
   - Créez un certificat « Let's Encrypt ». Pour cela, cliquez sur **Certificat SSL gratuit avec Let's Encrypt**. Cette option utilise les certificats Let's Encrypt émis par une entité tierce. Le fournisseur de services n'est pas responsable des problèmes qui pourraient survenir à la suite de l'utilisation de ces certificats gratuits. Pour plus d'informations sur les conditions de « Let's Encrypt », reportez-vous à https://letsencrypt.org/repository/.
   - Transférez votre certificat avec caractères génériques. Pour cela, cliquez sur **Transférer un certificat avec caractères génériques**, puis fournissez un certificat avec caractères génériques, ainsi qu'une clé privée.
6. Cliquez sur **Envoyer** pour appliquer les modifications.

Rétablir la valeur par défaut de l'URL personnalisée

1. Dans le portail de gestion, cliquez sur **Paramètres** > **Labellisation**.
2. Dans la section **URL des services Acronis Cyber Protect Cloud**, cliquez sur **Réinitialiser les paramètres par défaut** pour utiliser l'URL par défaut (https://cloud.acronis.com).

Mise à jour automatique des agents

Cyber Protect possède trois types d'agents qui peuvent être installés sur des machines protégées : Agent pour Windows, agent pour Linux et agent pour Mac.

Cloud Cyber Files possède une version de l'agent de bureau File Sync & Share pour Windows et une autre pour macOS, qui permet la synchronisation de fichiers et de dossiers entre un ordinateur et la zone de stockage dans le cloud File Sync & Share d'un utilisateur afin de promouvoir le travail hors

ligne, ainsi que le télétravail et les pratiques BYOD (Bring Your Own Device - Apporter votre propre terminal).

Pour faciliter la gestion de plusieurs ressources, vous pouvez configurer (et désactiver) les mises à jour automatiques et sans assistance pour tous les agents sur tous les ordinateurs.

Important
Actuellement, les partenaires et les clients n'ont accès à la fonctionnalité de gestion de mise à jour des agents que s'ils ont activé Protection.

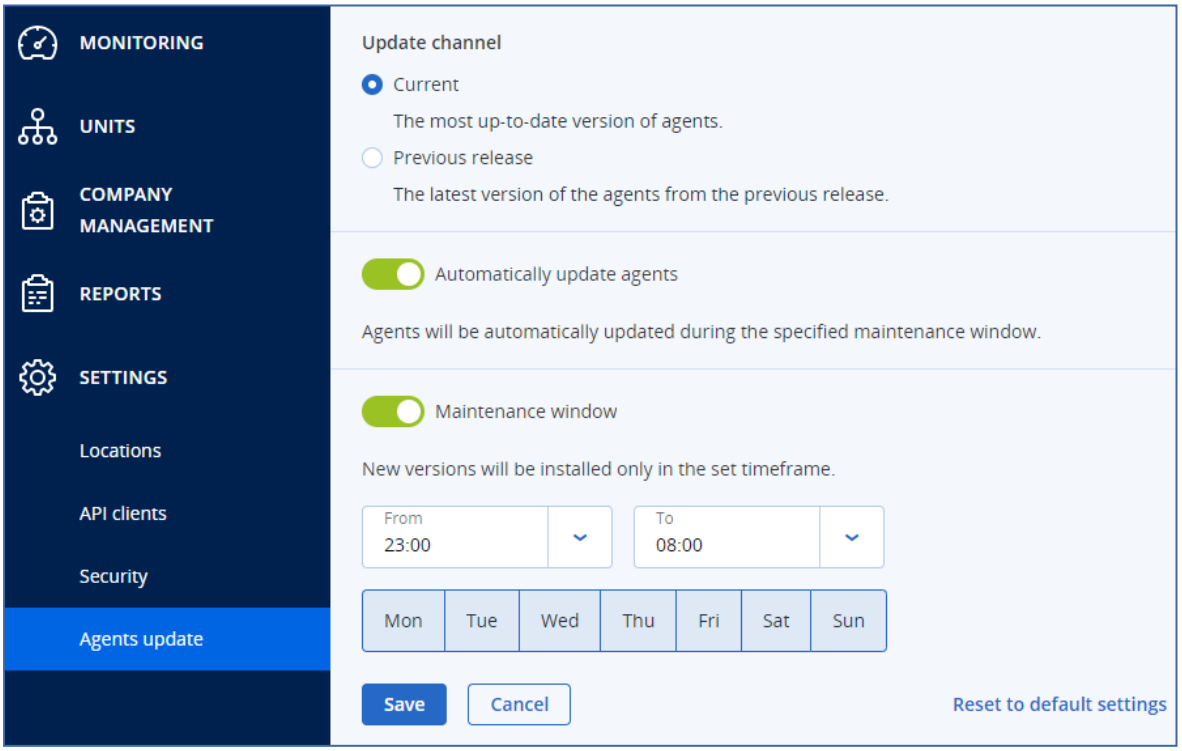
Remarque
Pour gérer les agents sur des machines individuelles, et personnaliser les paramètres de mise à jour automatique, veuillez consulter la section du Guide de l'utilisateur Cyber Protect consacrée à la Mise à jour des agents.

Mettre à jour automatiquement des agents

Remarque
Les paramètres de mise à jour automatique de l'agent pour File Sync & Share sont hérités par les partenaires et les clients qui n'ont pas activé le module Protection.

Configurer une mise à jour automatique des agents depuis la page initiale du portail de gestion

1. Cliquez sur **Paramètres > Mise à jour des agents**.



2. Sélectionnez la version à détecter pour les mises à jour automatiques : **Actuelle** ou **Version précédente**.
(la valeur par défaut est **Actuelle**.)

3. Activez l'option **Mettre à jour automatiquement les agents**.
   (L'option est **activée** par défaut.)
4. Définissez la fenêtre de maintenance.
   (La fenêtre de maintenance par défaut est 23 h à 08 h.)

   Remarque
   Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

5. [Facultatif] Sélectionnez les jours lors desquels effectuer les mises à jour.
6. Sélectionnez **Enregistrer.**

Remarque
Les mises à jour automatiques sont uniquement disponibles pour :

- Les agents Cyber Protect version 15.0.26986 (publiée en mai 2021) et versions ultérieures.
- L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

Pour les agents plus anciens, vous devez d'abord effectuer une mise à jour à la dernière version avant que les mises à jour automatiques puissent prendre effet.

Surveiller les mises à jour des agents

Important
Les mises à jour des agents ne peuvent être surveillées que par les administrateurs des partenaires et des clients qui ont activé le module Protection.

Pour surveiller les mises à jour des agents, veuillez consulter les sections Alertes et Activités du Guide de l'utilisateur Cyber Protect.

Surveillance

Pour accéder aux informations relatives à l'utilisation des services et aux opérations, cliquez sur **Surveillance**.

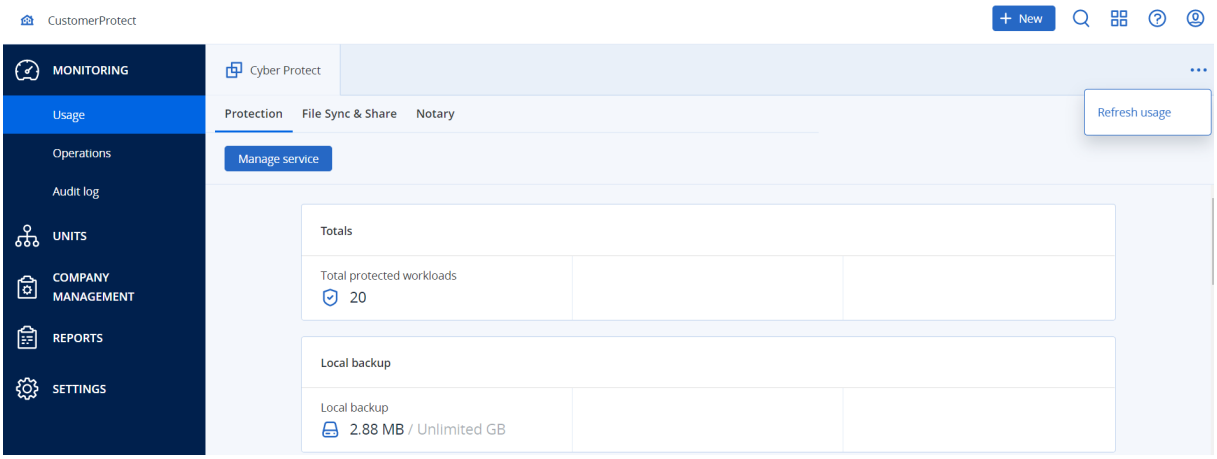
Utilisation

L'onglet **Utilisation** fournit une vue d'ensemble de l'utilisation du service et vous permet d'accéder aux services au sein du locataire dans lequel vous travaillez.

Les données d'utilisation incluent aussi bien les fonctionnalités standard que les fonctionnalités avancées.

Pour actualiser les données d'utilisation qui s'affichent dans l'onglet, cliquez sur les points de suspension en haut à droite de l'écran, puis sélectionnez **Actualiser l'utilisation**.

Remarque
La récupération des données peut prendre jusqu'à 10 minutes. Rechargez la page pour afficher les données mises à jour.



Opérations

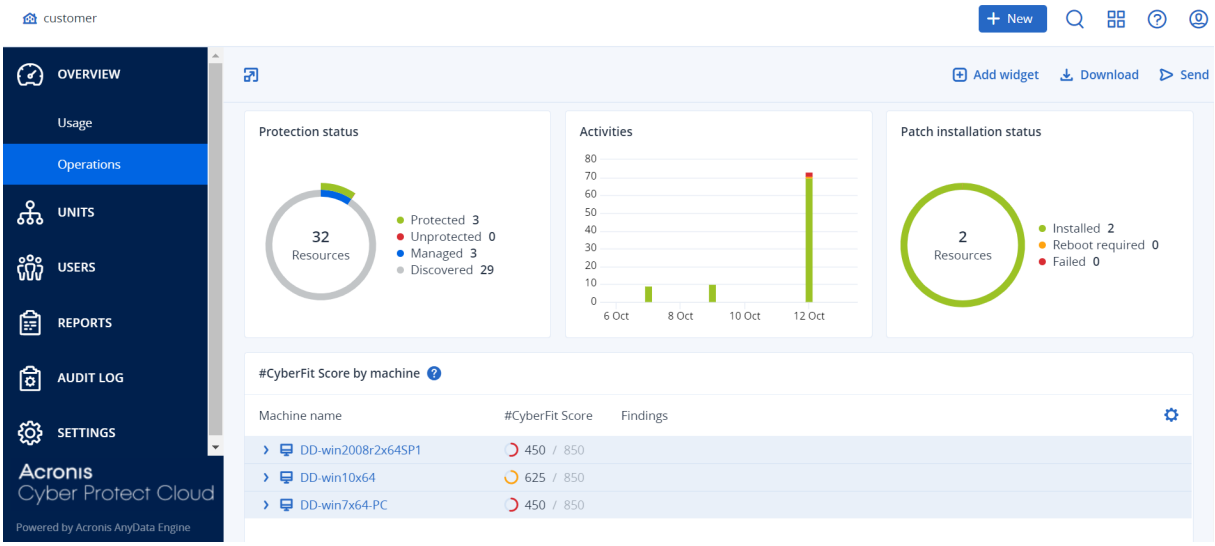
Le tableau de bord **Opérations** fournit un certain nombre de widgets personnalisables qui apporteront une vue d'ensemble des opérations liées au service Cyber Protection. Des widgets pour d'autres services seront disponibles dans les versions à venir.

Par défaut, les données sont affichées pour le locataire dans lequel vous travaillez. Vous pouvez changer le locataire affiché pour chaque widget en le modifiant. Les informations rassemblées à propos des locataires clients enfants directs du locataire sélectionné s'affichent également, notamment ceux situés dans les dossiers. Le tableau de bord n'affiche *pas* les informations concernant les partenaires enfants et leurs locataires enfants ; vous devez développer le partenaire en question pour afficher son tableau de bord. Toutefois, si vous convertissez un locataire partenaire enfant en locataire dossier, les informations concernant les clients enfants de ce locataire apparaîtront sur le tableau de bord du locataire parent.

Les widgets sont mis à jour toutes les deux minutes. Les widgets disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Vous pouvez télécharger l'état actuel du tableau de bord au format .pdf et/ou .xlsx, ou bien l'envoyer par courrier électronique à n'importe quelle adresse, notamment des destinataires externes.

Vous pouvez faire un choix parmi de nombreux widgets se présentant sous la forme de tableaux, de diagrammes circulaires, de graphiques à barres, de listes et de cartes proportionnelles. Vous pouvez

ajouter plusieurs widgets du même type en choisissant différents tenants ou différents filtres.



Pour réorganiser les widgets sur le tableau de bord

Glissez-déplacez les widgets en cliquant sur leur nom.

Pour modifier un widget

Cliquez sur l'icône en forme de crayon à côté du nom du widget. Modifier un widget vous permet de le renommer, de modifier l'intervalle de temps, de sélectionner le locataire pour lequel les données sont affichées, et de définir des filtres.

Pour ajouter un widget

Cliquez sur **Ajouter widget**, puis effectuez l'une des actions suivantes :

- Cliquez sur le widget que vous désirez ajouter. Le widget sera ajouté avec les paramètres par défaut.
- Pour modifier le widget avant de l'ajouter, cliquez sur l'icône en forme de roue dentée lorsque le widget est sélectionné. Lorsque vous avez terminé de modifier le widget, cliquez sur **Terminé**.

Pour supprimer un widget

Cliquez sur le signe X à côté du nom du widget.

État de protection

État de protection

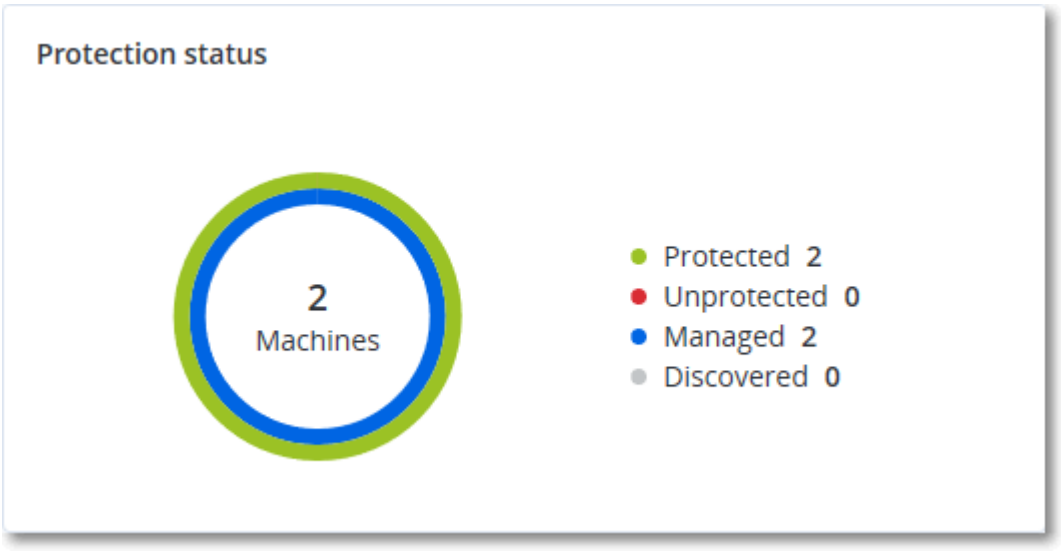
Ce widget affiche l'état de protection actuel de toutes les machines.

Une machine peut présenter l'un des états suivants :

- **Protégé :** machines sur lesquelles le plan de protection est appliqué.

- **Non protégé :** machines sur lesquelles le plan de protection n'est pas appliqué. Elles comprennent à la fois les machines découvertes et les machines gérées auxquelles aucun plan de protection n'est appliqué.
- **Géré :** machines sur lesquelles l'agent de protection est installé.
- **Découvert :** les machines sur lesquelles l'agent de protection n'est pas installé.

Si vous cliquez sur l'état de la machine, vous serez redirigé vers la liste des machines qui présentent le même état pour en savoir plus.



Machines découvertes

Ce widget affiche la liste des machines découvertes pendant la période spécifiée.

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

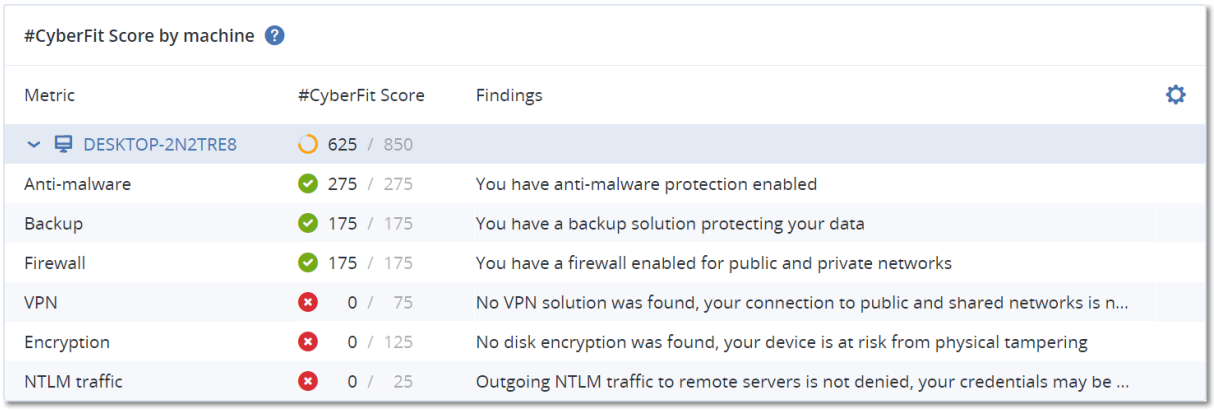
Score #CyberFit par machine

Ce widget affiche, pour chaque machine, le Score #CyberFit total, une combinaison de ses scores ainsi que les résultats pour chaque indicateur évalué :

- Anti-malware
- Sauvegarde
- Pare-feu
- VPN
- Chiffrement
- Trafic NTLM

Afin d'améliorer le score de chaque indicateur, vous pouvez afficher les recommandations disponibles dans le rapport.

Pour en savoir plus sur le Score #CyberFit, reportez-vous à « Score #CyberFit pour les machines ».



Widgets de protection évolutive des points de terminaison

Important
Il s'agit d'une version d'accès anticipé de la documentation sur la protection évolutive des points de terminaison. Certaines des fonctionnalités est descriptions sont peut-être incomplètes.

La protection évolutive des points de terminaison comprend un certain nombre de widgets qui sont accessibles depuis le tableau de bord **Opérations**.

Les widgets disponibles sont :

- Distribution des principaux incidents par charge de travail
- MTTR de l'incident
- Résolution des incidents de sécurité
- Statut réseau des charges de travail

Distribution des principaux incidents par charge de travail

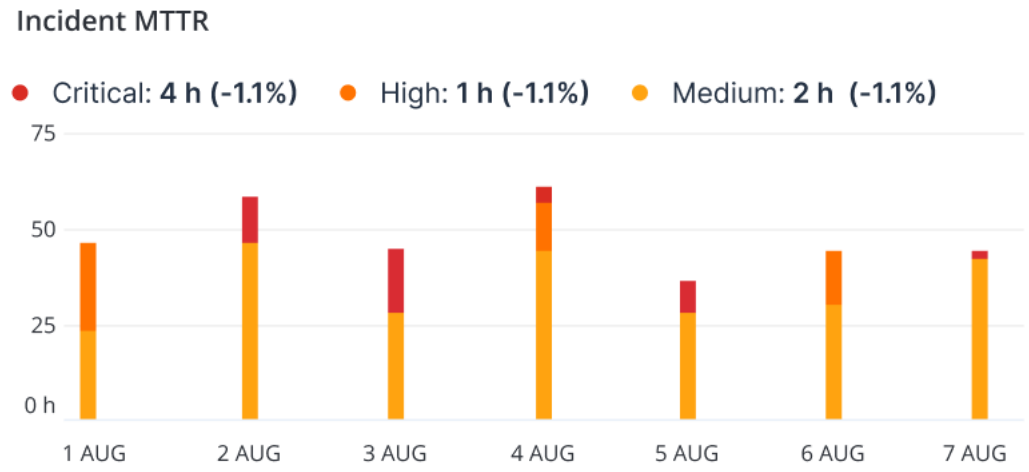
Ce widget affiche les cinq premières charges de travail qui comportent le plus d'incidents (cliquez sur **Afficher tout** pour rediriger l'utilisateur vers la liste des incidents ; elle est filtrée en fonction des paramètres du widget).

Survolez une ligne de charge de travail pour afficher le détail de l'état des enquêtes en cours menées sur les incidents ; les états d'enquête sont les suivants : **Non démarrée**, **Enquête en cours**, **Clôturée** et **Faux positif**. Cliquez ensuite sur la charge de travail que vous souhaitez analyser plus en détail, puis sélectionnez le client pertinent dans la fenêtre contextuelle qui s'affiche ; la liste des incidents est mise à jour en fonction des paramètres du widget.

MTTR de l'incident

Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus.

Cliquez sur une colonne pour afficher le détail des incidents en fonction de la gravité (**Critique**, **Élevé** et **Moyen**), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.

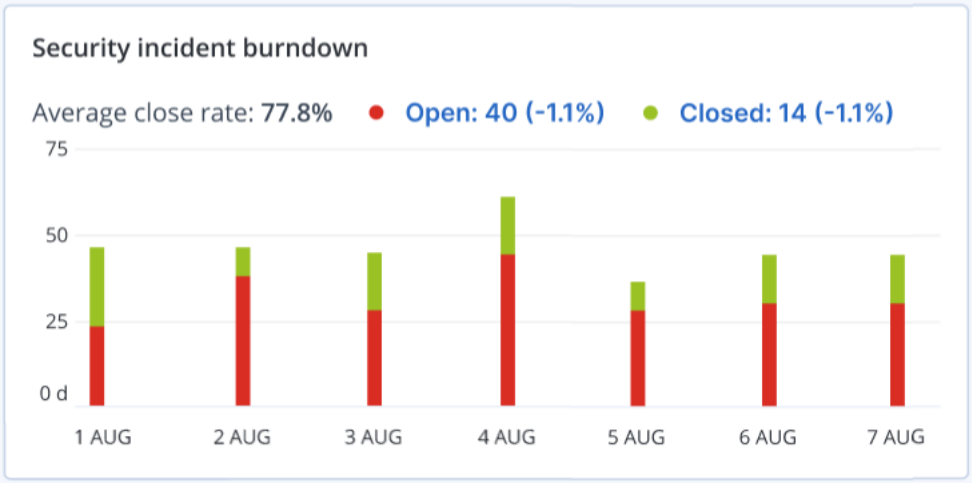


Résolution des incidents de sécurité

Ce widget indique l'efficacité de la clôture des incidents ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie.

Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. Si vous cliquez sur Ouvrir, une fenêtre contextuelle s'affiche dans laquelle vous pouvez y sélectionner le tenant approprié. La liste filtrée des incidents concernant le tenant sélectionné s'affiche et répertorie les incidents ouverts (état **Enquête en cours** ou **Non démarré**) Si vous cliquez sur Clôturé, la liste des incidents concernant le tenant sélectionné s'affiche et exclut les incidents qui ne sont plus ouverts (état **Clôturé** ou **Faux positif**).

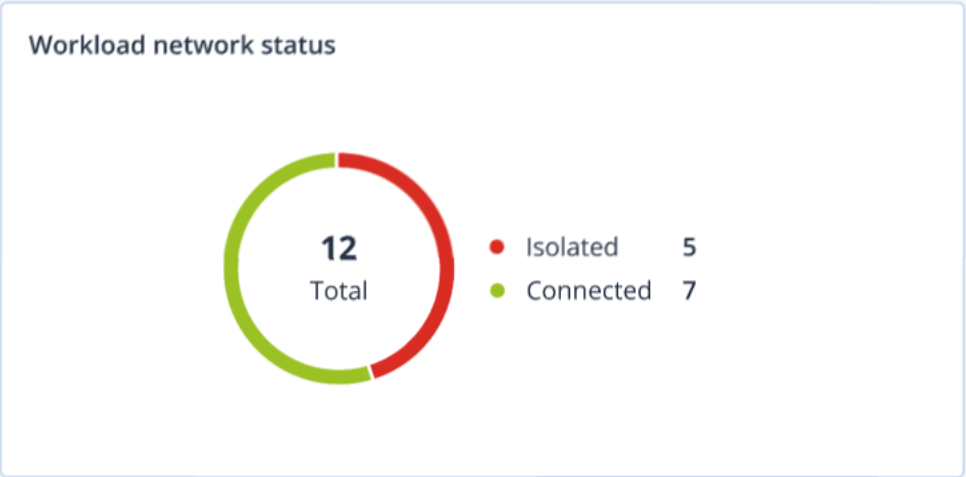
La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.



Statut réseau des charges de travail

Ce widget affiche le statut réseau actuel de vos charges de travail ; il indique le nombre de charges de travail isolées et le nombre de charges de travail connectées.

Si vous cliquez sur Isolé, une fenêtre contextuelle s'affiche dans laquelle vous pouvez sélectionner le tenant approprié. La vue des charges de travail est filtrée et n'affiche que les charges de travail isolées. Cliquez sur la valeur Connecté pour afficher la liste des charges de travail avec agent qui ne répertorie que les charges de travail connectées (du tenant sélectionné).



Surveillance de l'intégrité du disque

La surveillance de l'intégrité du disque fournit des informations sur l'intégrité actuelle du disque, ainsi que des prévisions concernant cette dernière. Vous pouvez ainsi prévenir les pertes de données liées à une panne du disque. Les disques durs, tout comme les SSD, sont pris en charge.

Limites

- La prévision de l'intégrité du disque est prise en charge uniquement pour les ordinateurs Windows.
- Seuls les disques des machines physiques sont surveillés. Les disques des machines virtuelles ne peuvent pas être surveillés et ne s'affichent pas dans les widgets d'intégrité du disque.
- Les configurations RAID ne sont pas prises en charge.
- Sur les lecteurs NVMe, la surveillance de l'intégrité du disque n'est prise en charge que pour les lecteurs qui communiquent des données SMART via l'API Windows. La surveillance de l'intégrité du disque n'est pas prise en charge pour les lecteurs NVMe qui nécessitent la lecture des données SMART directement depuis le lecteur.

L'intégrité du disque est représentée par l'un des états suivants :

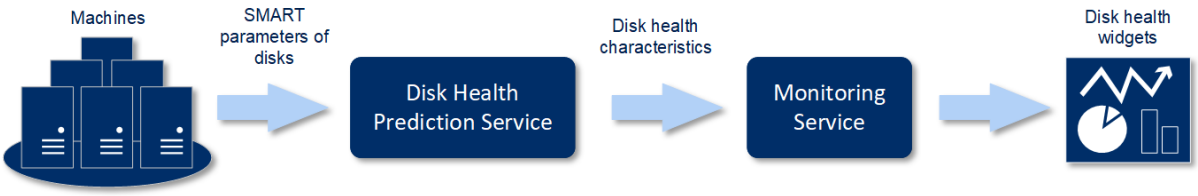
- **OK :**
  l'intégrité du disque est comprise entre 70 et 100 %.
- **Avertissement :**
  l'intégrité du disque est comprise entre 30 et 70 %.
- **Critique :**
  l'intégrité du disque est comprise entre 0 et 30 %.
- **Calcul des données du disque :**
  l'intégrité actuelle et la prévision de l'intégrité du disque sont en cours de calcul.

Fonctionnement

Le service Prévision de l'intégrité du disque se sert d'un modèle de prévision basé sur l'intelligence artificielle.

1. L'agent de protection collecte les paramètres SMART des disques et transmet ces données au service Prévision de l'intégrité du disque :
   - SMART 5 : nombre de secteurs réalloués.
   - SMART 9 : nombre d'heures de fonctionnement.
   - SMART 187 : nombre d'erreurs signalées qui n'ont pas été corrigées.
   - SMART 188 : expiration de commandes.
   - SMART 197 : nombre actuel de secteurs en attente.
   - SMART 198 : nombre de secteurs hors ligne impossible à corriger.
   - SMART 200 : taux d'erreurs d'écriture.
2. Le service Prévision de l'intégrité du disque traite les paramètres SMART reçus, effectue des prévisions, puis fournit les caractéristiques d'intégrité du disque suivantes :
   - État de santé actuel du disque : OK, Avertissement, Critique.
   - Prévision de l'état de santé du disque : négatif, stable, positif.
   - Probabilité de prévision de l'état de santé du disque en pourcentage.

   La période de prévision est d'un mois.
3. Le service de surveillance reçoit ces caractéristiques, puis affiche les informations pertinentes dans les widgets d'intégrité du disque dans la console de service.



Widgets de l'état de santé du disque

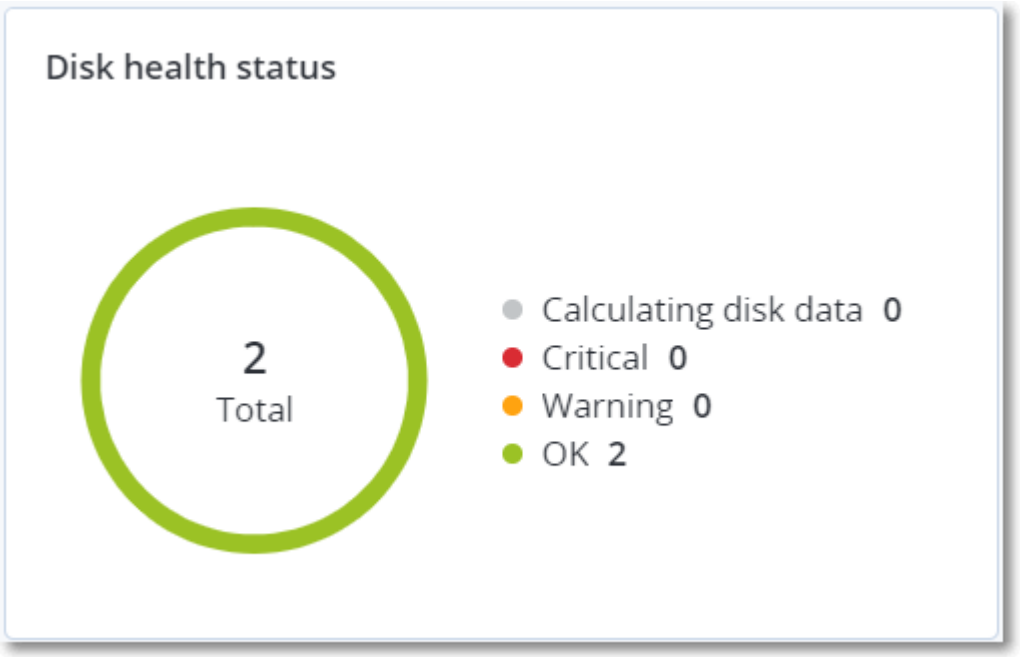
Les résultats de la surveillance de l'intégrité du disque sont présentés dans les widgets suivants, disponibles dans la console de service.

- **Vue d'ensemble de l'intégrité du disque** est un widget en forme de carte proportionnelle, qui possède deux niveaux de détails que vous pouvez explorer :
  - Niveau ordinateur
    Affiche des informations résumées concernant l'intégrité du disque en fonction des ordinateurs client que vous avez sélectionnés. Seul l'état de disque le plus critique est affiché. Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur sur un bloc en particulier. La taille du bloc d'un ordinateur dépend de la taille totale de l'ensemble de ses disques. La couleur du bloc d'une machine dépend de l'état de disque le plus critique identifié.

- Niveau disque
  Affiche l'intégrité actuelle de tous les disques pour l'ordinateur sélectionné. Chaque bloc de disque affiche les prévisions d'intégrité du disque suivantes, ainsi que leur probabilité en pourcentage :
  - Sera altéré
  - Restera stable

- Sera amélioré

- **Intégrité du disque** est un widget de graphique circulaire qui affiche le nombre de disques pour chaque état.



Alertes relatives à l'état de santé du disque

La vérification de l'intégrité du disque est exécutée toutes les 30 minutes, alors que l'alerte correspondante n'est générée qu'une fois par jour. Lorsque l'intégrité du disque passe de **Avertissement** à **Critique**, une alerte est toujours générée.

Nom de l'alerte	La gravité	Intégrité du disque	Description
Une défaillance du disque dur est possible	Avertissement	(30 – 70)	Il est possible que le disque <nom du disque> sur cet ordinateur échoue à l'avenir. Exécutez une sauvegarde d'image complète du disque dès que possible, remplacez ce dernier, puis restaurez l'image sur le nouveau disque.
La défaillance du disque dur est imminente	Critique	(0 – 30)	Le disque <nom du disque> sur cet ordinateur est dans un état critique, et risque fortement d'échouer très bientôt. Une sauvegarde d'image de ce disque n'est pas recommandée à ce stade, car la contrainte supplémentaire risque de causer la défaillance du disque. Sauvegardez les fichiers les plus importants sur le disque dès maintenant et remplacez-le.

Carte de la protection des données

La fonctionnalité Carte de la protection des données vous permet d'examiner toutes les données qui ont une importance à vos yeux, et d'obtenir des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants, le tout sous la forme d'une carte proportionnelle dont vous pouvez faire varier l'échelle.

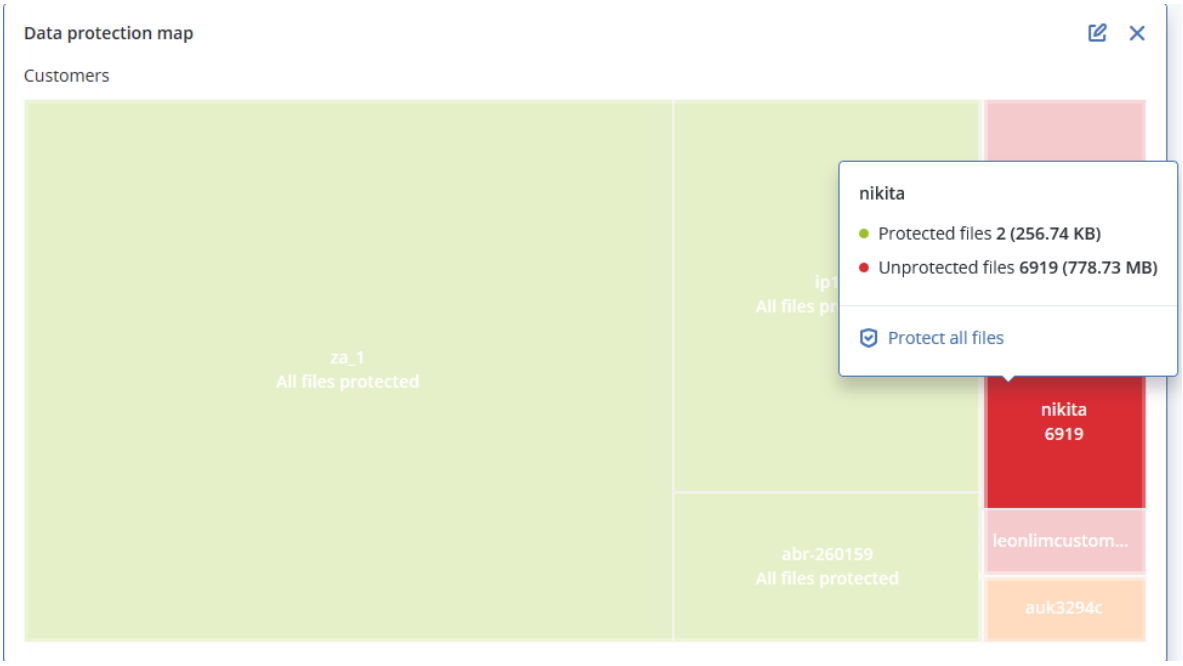
La taille de chaque bloc dépend du nombre total ou de la taille totale des fichiers importants qui appartiennent à un client ou à une machine.

Les fichiers peuvent présenter l'un des états de protection suivants :

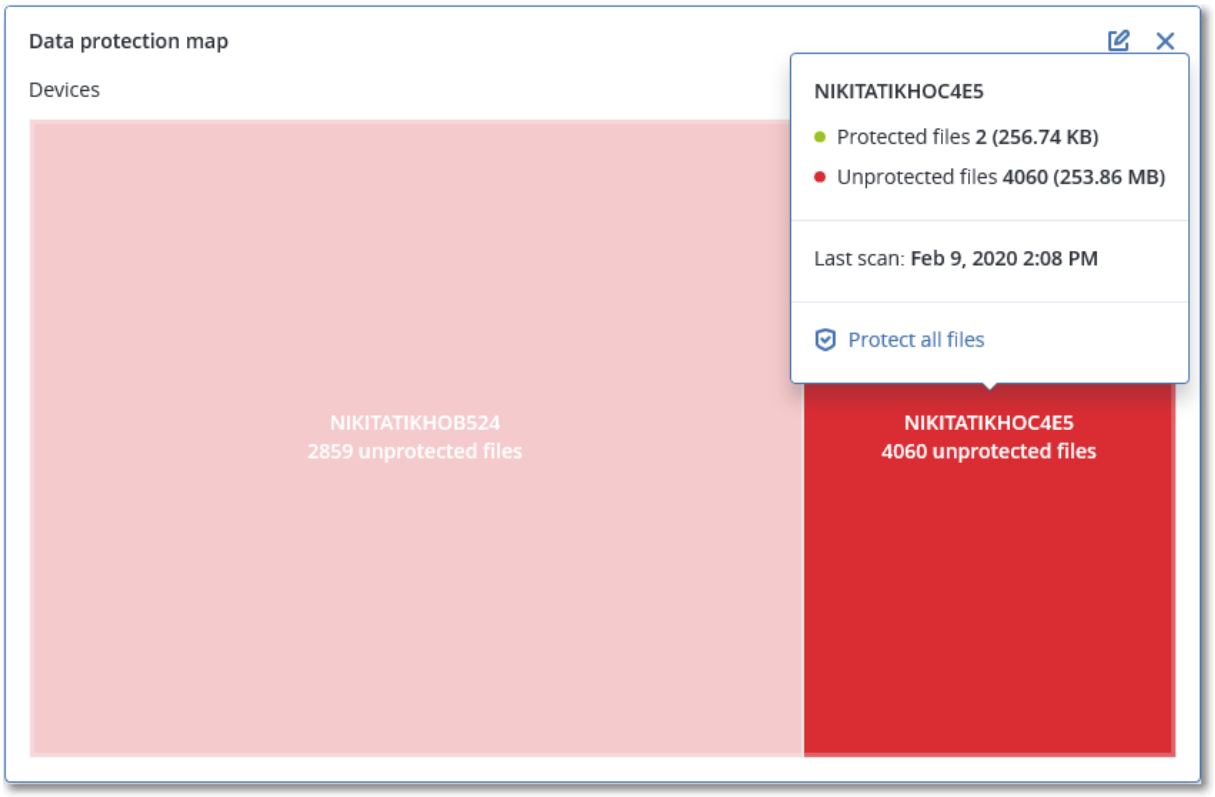
- **Critique :** de 51 à 100 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés pour le locataire, la machine ou l'emplacement client sélectionné.
- **Faible :** de 21 à 50 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés pour le locataire, la machine ou l'emplacement client sélectionné.
- **Moyen :** de 1 à 20 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés pour le locataire, la machine ou l'emplacement client sélectionné.
- **Élevé :** tous les fichiers présentant l'extension que vous avez spécifiée sont protégés (sauvegardés) pour le locataire, la machine ou l'emplacement client sélectionné.

Les résultats de l'examen de la protection des données sont disponibles sur le tableau de bord dans le widget Carte de la protection des données, un widget sous forme de carte proportionnelle, qui possède deux niveaux de détail que vous pouvez explorer tour à tour :

- Niveau locataire client : affiche des informations résumées concernant l'état de protection de fichiers importants en fonction des clients que vous avez sélectionnés.



- Niveau machine : affiche des informations concernant l'état de protection de fichiers importants en fonction des machines du client sélectionné.



Pour protéger des fichiers qui ne sont pas protégés, passez le pointeur de la souris sur le bloc, puis cliquez sur **Protéger tous les fichiers**. Dans la boîte de dialogue, vous trouverez des informations concernant le nombre de fichiers non protégés, ainsi que leur emplacement. Pour les protéger, cliquez sur **Protéger tous les fichiers**.

Vous pouvez aussi télécharger un rapport détaillé au format CSV.

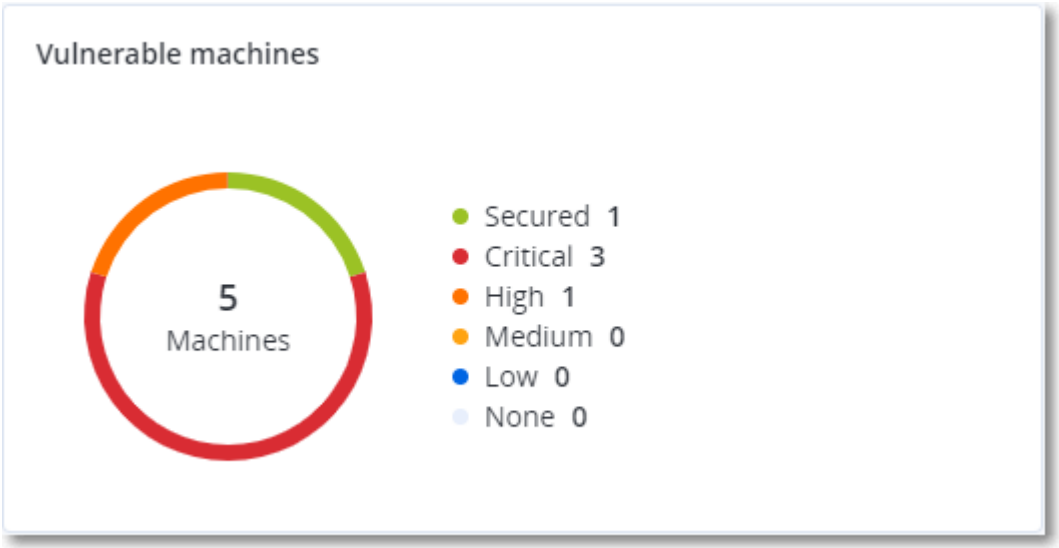
Widgets d'évaluation des vulnérabilités

Machines vulnérables

Ce widget affiche les ordinateurs vulnérables en les classant en fonction de la gravité de leur vulnérabilité.

La vulnérabilité découverte peut présenter l'un des niveaux de gravité suivants, d'après le système d'évaluation des vulnérabilités (CVSS) v3.0 :

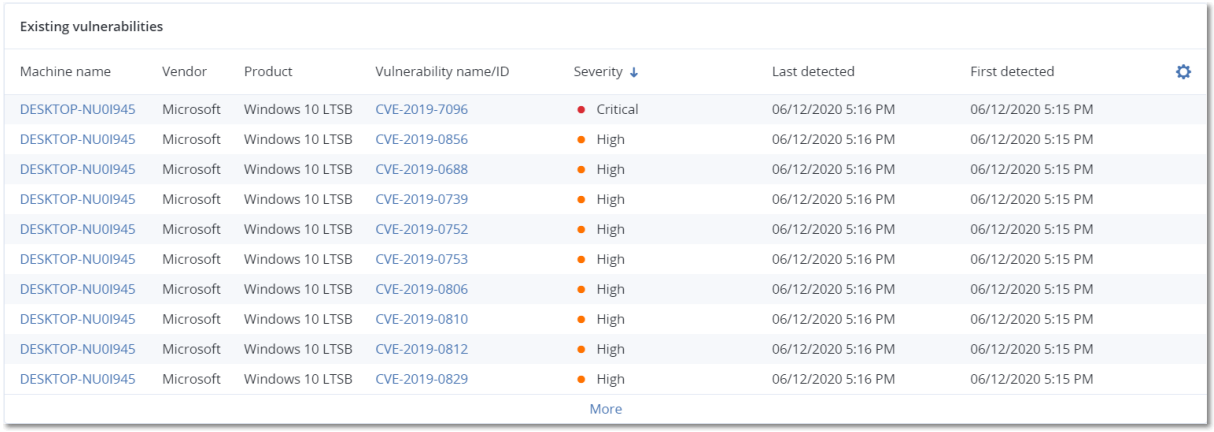
- Sécurisé : aucune vulnérabilité n'a été trouvée
- Critique : 9,0 – 10,0 CVSS
- Élevé : 7,0 – 8,9 CVSS
- Moyen : 4,0 – 6,9 CVSS
- Faible : 0,1 – 3,9 CVSS
- Aucun : 0,0 CVSS



Vulnérabilités existantes

Ce widget affiche les vulnérabilités existant actuellement sur les machines. Dans le widget **Vulnérabilités existantes**, il existe deux colonnes affichant la date et l'heure de la dernière modification :

- **Première détection** : date et heure à laquelle une vulnérabilité a initialement été détectée sur une machine.
- **Dernière détection** : date et heure à laquelle une vulnérabilité a été détectée sur une machine pour la dernière fois.



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

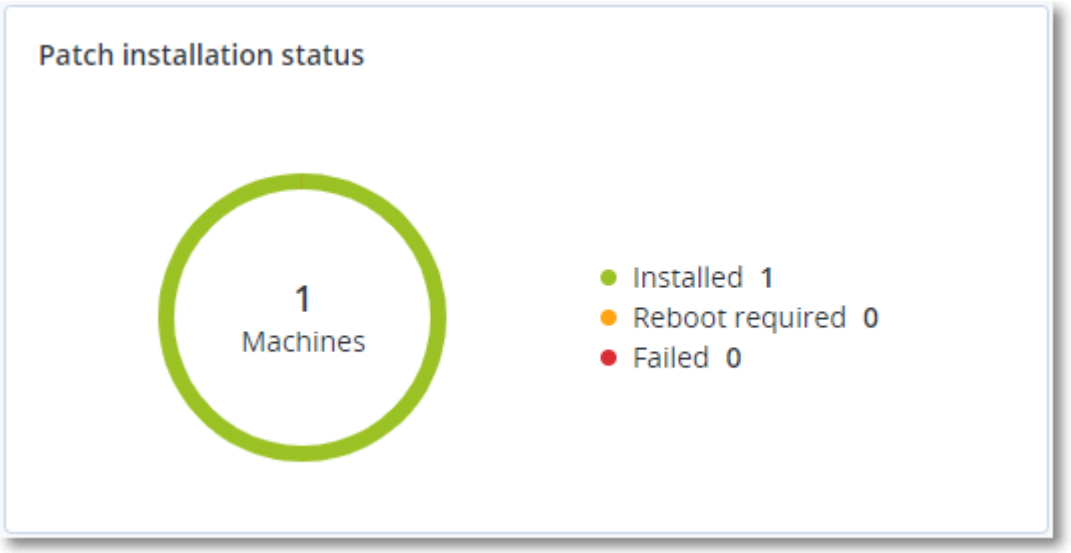
Widgets d'installation des correctifs

Il existe quatre widgets en lien avec la fonctionnalité de gestion des correctifs.

Statut d'installation des correctifs

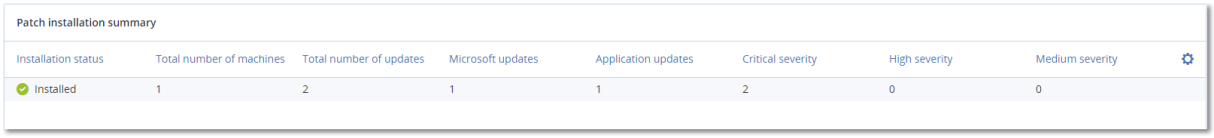
Ce widget affiche le nombre de machines, en les regroupant par statut d'installation des correctifs.

- **Installé :** tous les correctifs disponibles sont installés sur une machine.
- **Redémarrage nécessaire :** après l'installation des correctifs, un redémarrage est requis pour une machine.
- **Échec :** l'installation des correctifs sur une machine a échoué.



Résumé d'installation des correctifs

Ce widget affiche le résumé des correctifs sur les machines, en les regroupant par statut d'installation des correctifs.



Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

Historique d'installation des correctifs

Ce widget affiche des informations détaillées au sujet des correctifs sur les machines.

Patch installation history

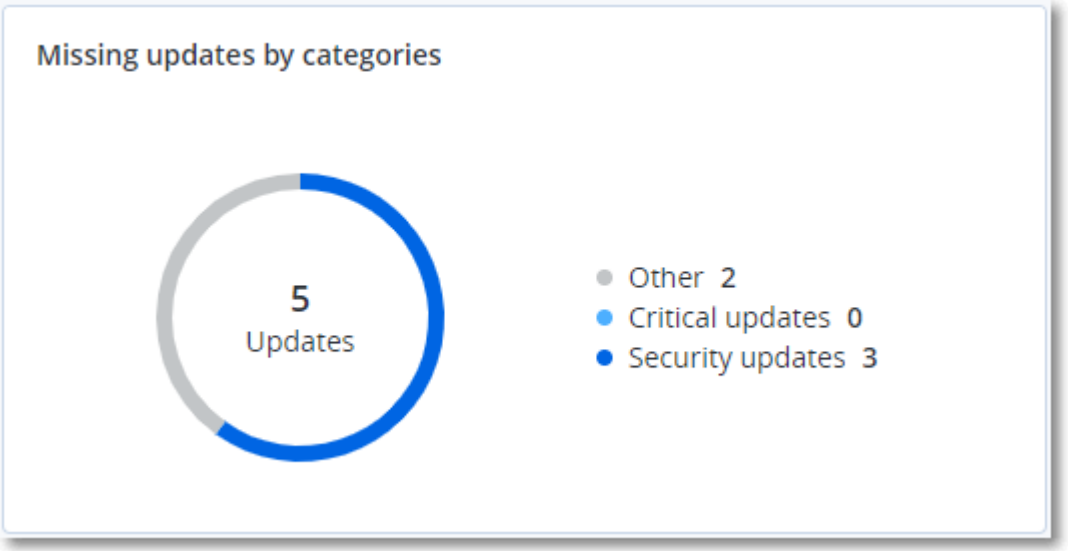
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical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

More

Mises à jour manquantes, par catégorie

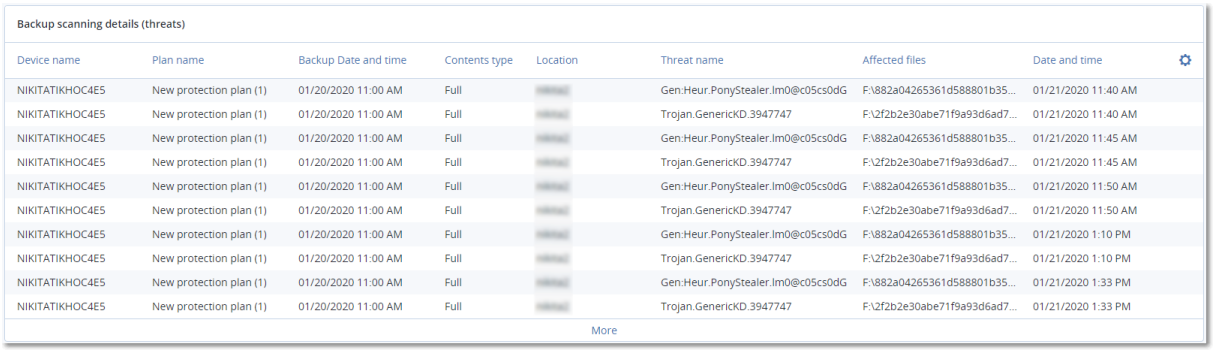
Ce widget affiche le nombre de mises à jour manquantes, en les classant par catégorie Les catégories suivantes sont répertoriées :

- Mises à jour de sécurité
- Mises à jour critiques
- Autre



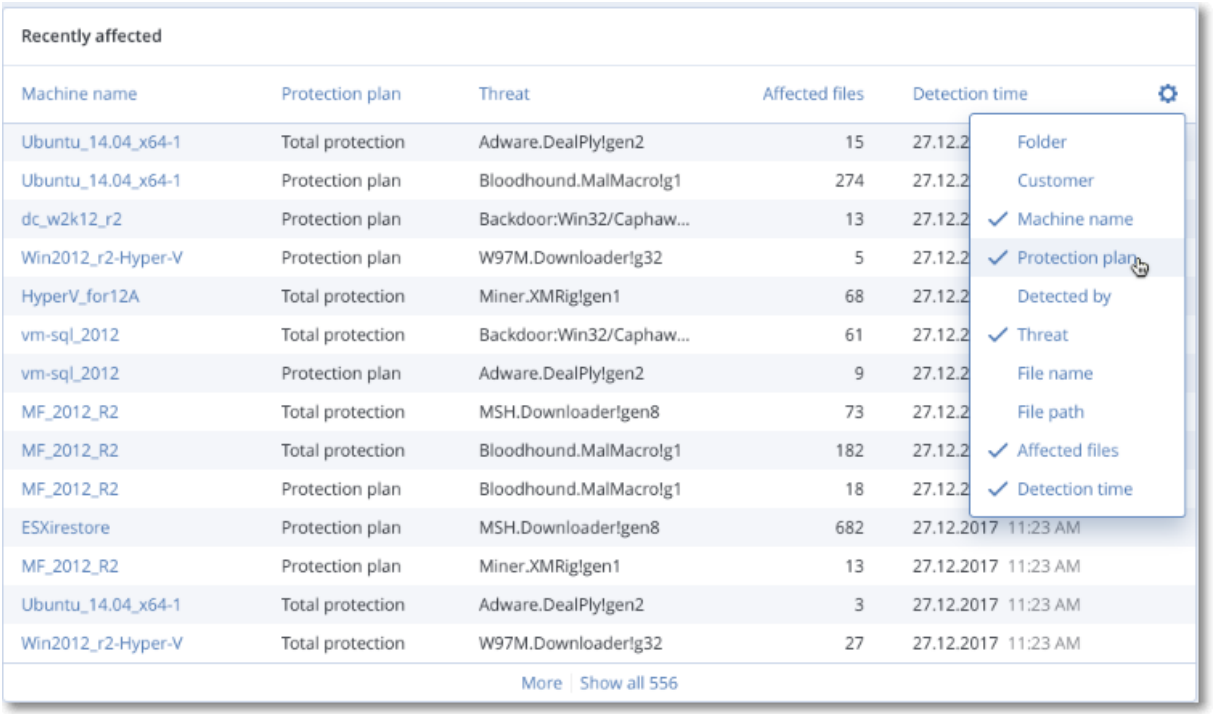
Détails de l'analyse de la sauvegarde

Ce widget affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.



Affectés récemment

Ce widget montre des informations détaillées au sujet des charges de travail touchées par des menaces telles que des virus, des malwares et des ransomwares. Vous y trouverez des informations concernant les menaces détectées, l'heure de détection et le nombre de fichiers touchés.



Téléchargement de données pour les charges de travail récemment affectées

Vous pouvez télécharger les données pour les charges de travail récemment affectées, générer un fichier CSV et l'envoyer aux destinataires que vous spécifiez.

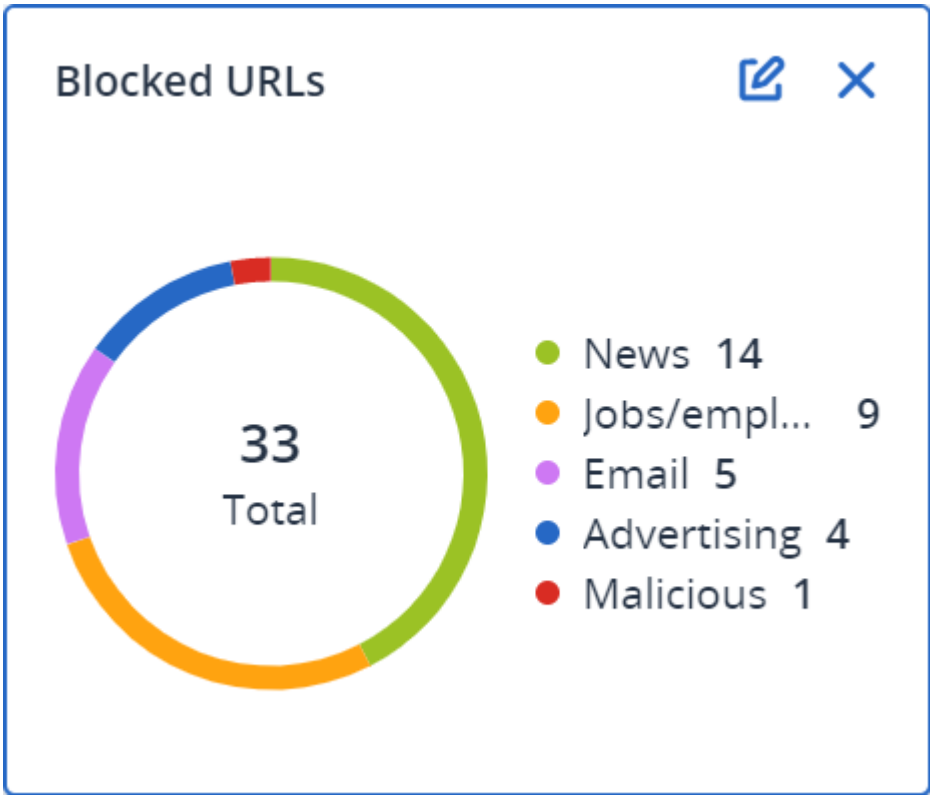
Pour télécharger les données pour les charges de travail récemment affectées

1. Dans le widget **Affectés récemment**, cliquez sur **Télécharger les données**.
2. Dans le champ **Période**, saisissez le nombre de jours pendant lequel vous souhaitez télécharger des données. Le nombre maximum de jours que vous pouvez entrer est 200.
3. Dans le champ **Destinataires**, saisissez l'adresse e-mail de toutes les personnes qui recevront un e-mail avec un lien pour télécharger le fichier CSV.
4. Cliquez sur **Télécharger**.

   Le système commence à générer le fichier CSV avec les données pour les charges de travail qui ont été affectées au cours de la période que vous avez spécifiée. Quand le fichier CSV est prêt, le système envoie un e-mail aux destinataires. Chaque destinataire peut ensuite télécharger le fichier CSV.

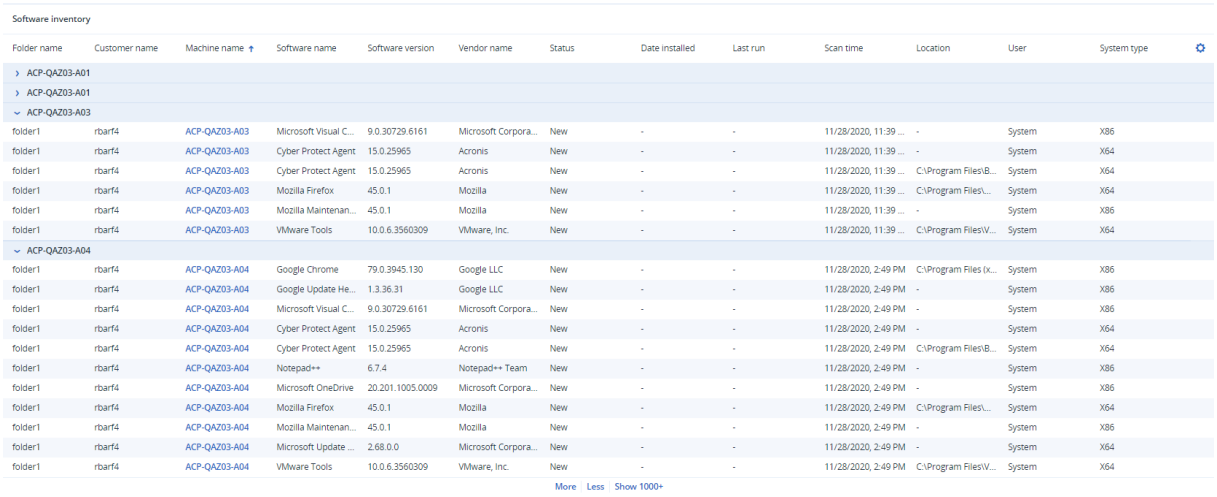
URL bloquées

Le widget affiche les statistiques des URL bloquées par catégorie. Pour en savoir plus sur le filtrage et la catégorisation des URL, consultez le Guide de l'utilisateur de Cyber Protect.

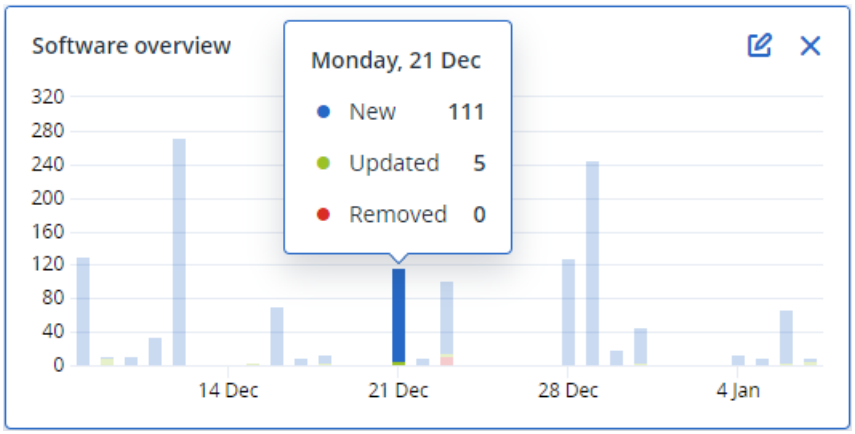


Widget d'inventaire du logiciel

Le widget de tableau **Inventaire du logiciel** contient des informations détaillées concernant tout le logiciel installé sur les terminaux Windows et macOS des organisations de vos clients.



Le widget **Aperçu du logiciel** contient le nombre de nouvelles applications ou d'applications mises à jour et supprimées sur les terminaux physiques Windows et macOS des organisations de vos clients sur une période donnée (7 jours, 30 jours ou le mois en cours).



Lorsque vous passez le pointeur sur une barre en particulier, une infobulle contenant les informations suivantes s'affiche :

Nouvelles – le nombre d'applications nouvellement installées.

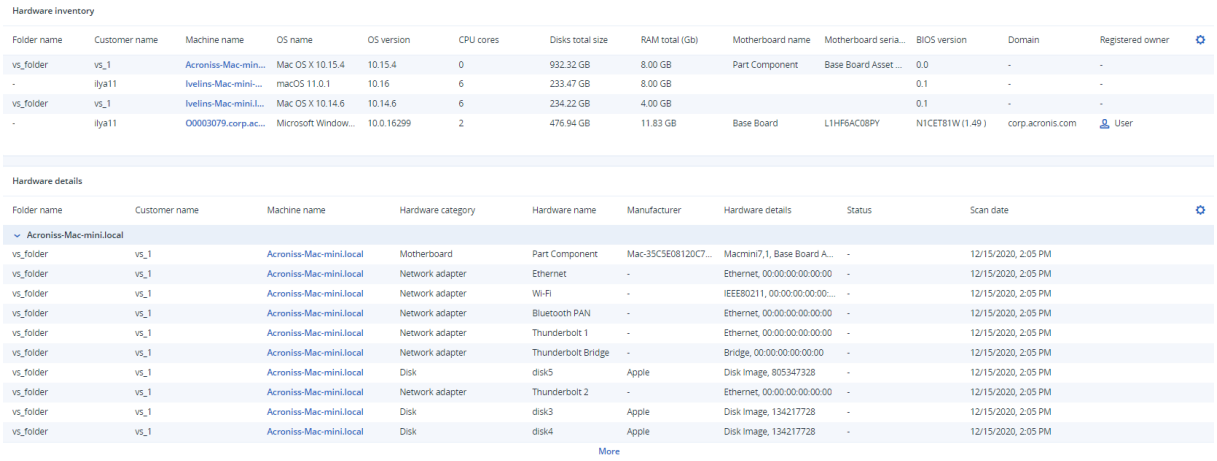
Mises à jour – le nombre d'applications mises à jour.

Supprimées – le nombre d'applications supprimées.

Lorsque vous cliquez sur la partie de la barre qui correspond à un certain statut, une fenêtre contextuelle se charge. Elle répertorie tous les clients possédant des terminaux dotés d'applications avec le statut sélectionné à la date sélectionnée. Vous pouvez sélectionner un client de la liste, cliquer sur **Aller au client**, et vous serez redirigés vers la page **Gestion de logiciel** -> **Inventaire du logiciel** de la console de service du client. Les informations de cette page sont filtrées en fonction de la date et du statut correspondants.

Widgets d'inventaire du matériel

Les widgets de tableau **Inventaire du matériel** et **Détails du matériel** contiennent des informations concernant tout le matériel installé sur les terminaux physiques et virtuels Windows et macOS de l'organisation de votre client.



Hardware inventory

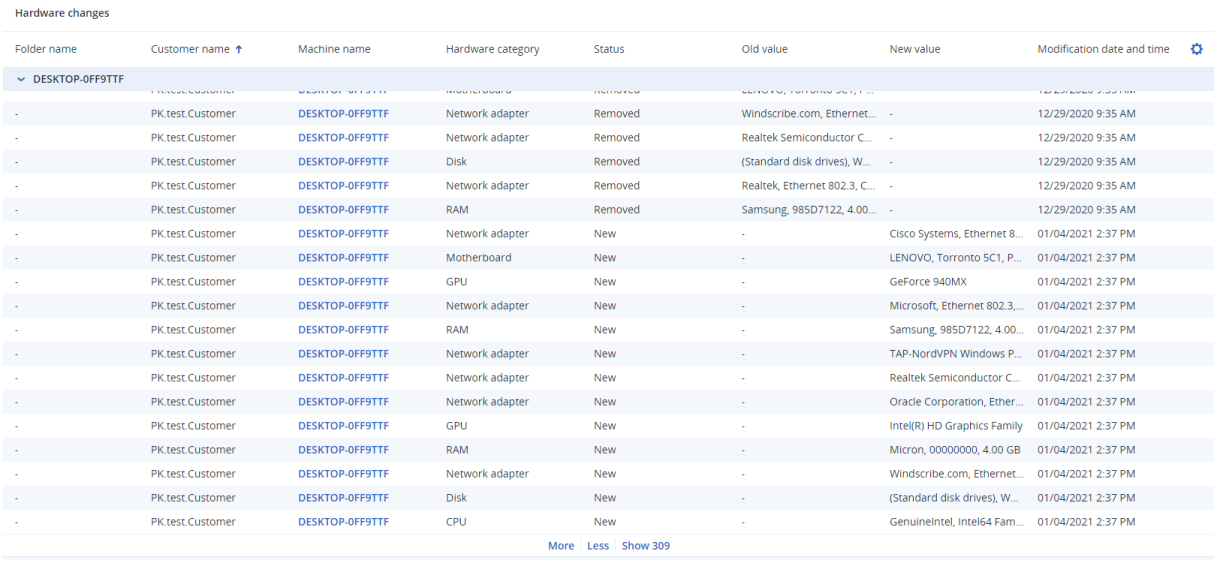
Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-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

Hardware details

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

More

Le widget de tableau **Inventaire du matériel** contient des informations concernant le matériel ajouté, supprimé et modifié sur les terminaux physiques et virtuels Windows et macOS de l'organisation de votre client sur une période donnée (7 jours, 30 jours ou le mois en cours).



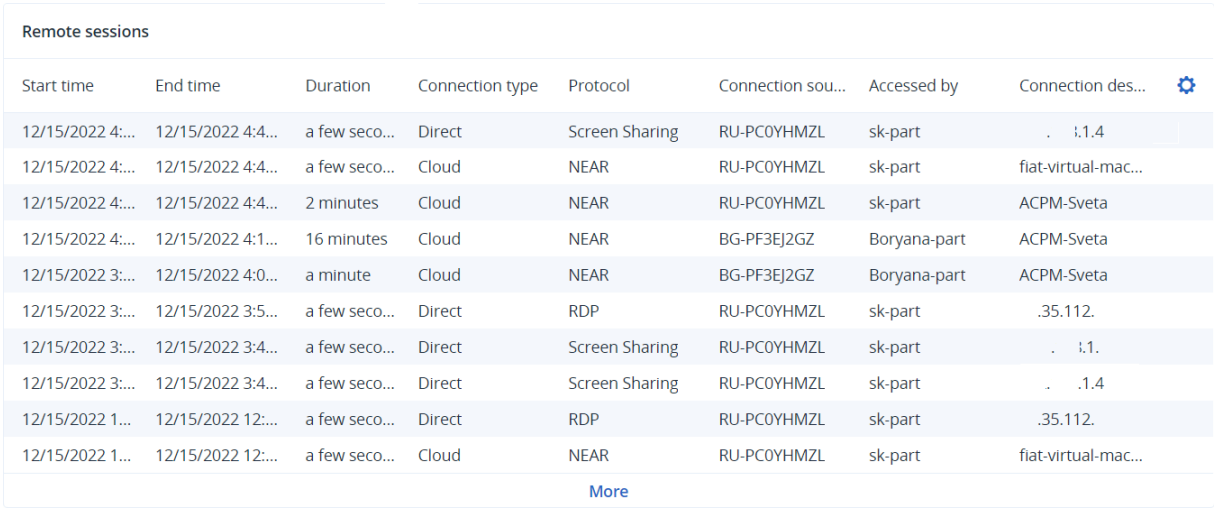
Hardware changes

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

Historique des sessions

Le widget affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers effectuées dans l'organisation de vos clients pendant une période spécifiée.



Remote sessions

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

More

Rapports

Pour créer des rapports relatifs à l'utilisation du service et aux opérations, cliquez sur **Rapports**.

Utilisation

Les rapports d'utilisation fournissent des données historiques sur l'utilisation des services. Les rapports d'utilisation sont disponibles aussi bien au format CSV qu'au format HTML.

Type de rapport

Vous pouvez sélectionner l'un des types de rapports suivants :

- **Utilisation actuelle**

  Ce rapport contient les mesures de l'utilisation actuelle du service.

  Les mesures d'utilisation sont calculées dans chacune des périodes de facturation des locataires enfants. Si les locataires inclus dans le rapport ont des périodes de facturation différentes, l'utilisation du locataire parent peut différer de la somme des utilisations des locataires enfants.
- **Distribution de l'utilisation actuelle**

  Ce rapport est disponible uniquement pour les locataires partenaires gérés par un système d'approvisionnement externe. Ce rapport est utile lorsque les périodes de facturation des locataires enfants ne correspondent pas à la période de facturation du locataire parent. Le rapport contient les mesures de l'utilisation du service pour les locataires enfant, calculées au sein de la période de facturation actuelle du locataire parent. L'utilisation du locataire parent sera forcément égale à la somme des utilisations des locataires enfants.
- **Résumé pour cette période**

  Ce rapport contient les indicateurs de l'utilisation du service pour la fin de la période spécifiée, et la différence entre les mesures au début et à la fin de la période spécifiée.
- **Jour par jour pour cette période**

  Ce rapport contient les indicateurs de l'utilisation du service et leurs changements pour chaque jour de la période spécifiée.

Champ d'application du rapport

Vous pouvez choisir le champ d'application du rapport parmi les valeurs suivantes :

- **Clients directs et partenaires**
  Le rapport comprendra uniquement les mesures d'utilisation de service pour les locataires enfants immédiats du locataire dans lequel vous travaillez.
- **Tous les clients et partenaires**
  Le rapport comprendra les valeurs des paramètres de rapport pour tous les locataires enfants du locataire dans lequel vous travaillez.
- **Tous les clients et partenaires (y compris les informations d'utilisateur)**
  Le rapport comprendra les valeurs des paramètres de rapport pour tous les locataires enfants du locataire dans lequel vous travaillez et pour tous les utilisateurs au sein des locataires.

Indicateurs avec zéro utilisation

Vous pouvez réduire le nombre de lignes présentées dans le rapport en masquant les informations relatives aux indicateurs avec zéro utilisation.

Configuration de rapports d'utilisation planifiés

Un rapport planifié regroupe les mesures d'utilisation du service pour le mois précédent complet. Les rapports sont générés à 23:59:59 (UTC) le premier jour du mois et sont envoyés le second jour de ce même mois. Ils sont envoyés à tous les administrateurs de votre locataire qui ont sélectionné la case à cocher **Rapports d'utilisation planifiés** dans leurs paramètres utilisateur.

Pour activer ou désactiver un rapport planifié

1. Connectez-vous au portail de gestion.
2. Assurez-vous de travailler dans le locataire le plus haut disponible.
3. Cliquez sur **Rapports** > **Utilisation**.
4. Cliquez sur **Planifié**.
5. Cochez ou décochez la case **Envoyer un rapport de synthèse mensuel**.
6. Dans **Niveau de détail**, sélectionnez le champ d'application du rapport.
7. [Facultatif] Sélectionnez **Masquer les indicateurs avec zéro utilisation** si vous souhaitez exclure du rapport les indicateurs avec zéro utilisation.

Configuration de rapports d'utilisation personnalisés

Ce type de rapport peut être généré à la demande et ne peut être planifié. Le rapport sera envoyé à votre adresse e-mail.

Pour générer un rapport personnalisé

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire pour lequel vous souhaitez créer un rapport.
3. Cliquez sur **Rapports** > **Utilisation**.
4. Sélectionnez l'onglet **Personnalisé**.
5. Dans **Type**, sélectionnez le type de rapport comme décrit ci-dessus.
6. [Non disponible pour le type de rapport **d'utilisation actuelle**] Dans **Période**, sélectionnez la période couverte par le rapport :
   - **Mois actuel**
   - **Mois précédent**
   - **Personnalisée**
7. [Non disponible pour le type de rapport **d'utilisation actuelle**] Si vous souhaitez indiquer une période de rapport personnalisée, sélectionnez les dates de début et de fin. Sinon, ignorez cette étape.
8. Dans **Niveau de détail**, sélectionnez le champ d'application du rapport comme décrit ci-dessus.
9. [Facultatif] Sélectionnez **Masquer les indicateurs avec zéro utilisation** si vous souhaitez exclure du rapport les indicateurs avec zéro utilisation.
10. Pour générer le rapport, cliquez sur **Générer et envoyer**.

Rapports d'opération

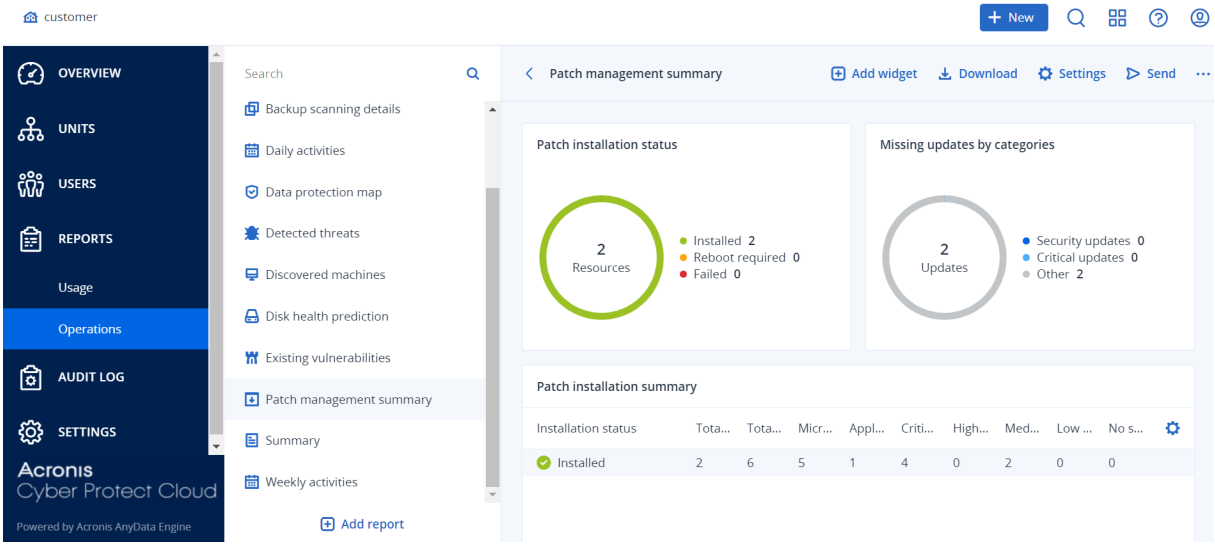
Un rapport au sujet des opérations peut inclure n'importe quel ensemble de widgets du tableau de bord **Opérations**. Par défaut, tous les widgets présentent un résumé concernant le tenant dans lequel vous travaillez. Pour modifier cela, vous pouvez accéder aux paramètres du rapport et appliquer une modification à tous les widgets, ou vous pouvez modifier chaque widget de manière individuelle.

En fonction du type de widget, le rapport inclut les données pour une période ou pour le moment de la navigation ou de la génération de rapport. Consultez "Données rapportées en fonction du type de widget" (p. 123).

Tous les widgets historiques présentent les données pour le même intervalle de temps. Vous pouvez modifier cela dans les paramètres de rapport.

Vous pouvez utiliser des rapports par défaut ou créer un rapport personnalisé.

Vous pouvez télécharger un rapport au sujet des opérations ou l'envoyer par e-mail au format Excel (XLSX) ou au format PDF.



Les rapports par défaut sont répertoriés ci-dessous :

Nom du rapport	Description
Score #CyberFit par machine	Affiche le score #CyberFit basé sur l'évaluation des indicateurs et des configurations de sécurité pour chaque machine, ainsi que des recommandations d'amélioration.
Alertes	Affiche les alertes survenues pendant une période donnée.
Détails de l'analyse de la sauvegarde	Affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.
Activités quotidiennes	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Carte de la protection des données	Affiche des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants présents sur des machines.
Menaces détectées	Affiche les détails des machines affectées en les classant par nombre de menaces bloquées, ainsi que le nombre de machines saines et vulnérables.
Machines découvertes	Affiche toutes les machines trouvées dans le réseau de l'organisation.
Prévision de l'état de santé du disque	Affiche des prévisions concernant le moment où votre disque dur/SSD tombera en panne, ainsi que l'état actuel des disques.
Vulnérabilités existantes	Affiche les vulnérabilités existantes pour le système d'exploitation et les applications dans votre organisation. Le rapport affiche également les détails des machines affectées dans votre réseau

	pour chaque produit répertorié.
Résumé de la gestion des correctifs	Affiche le nombre de correctifs manquants, installés et applicables. Vous pouvez explorer les rapports pour obtenir des informations sur les correctifs manquants/installés, ainsi que sur tous les systèmes
Résumé	Affiche des informations résumées au sujet des périphériques protégés pendant une période donnée.
Activités hebdomadaires	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Inventaire du logiciel	Affiche des informations détaillées concernant tout le logiciel installé sur les ordinateurs Windows et macOS des organisations de vos clients.
Inventaire du matériel	Affiche des informations détaillées concernant tout le matériel disponible sur les ordinateurs physiques et virtuels Windows et macOS de l'organisation de votre client.
Sessions distantes	Affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers effectuées dans l'organisation de vos clients pendant une période spécifiée.

Pour afficher un rapport, cliquez sur son nom.

Pour accéder aux opérations avec un rapport, cliquez sur l'icône de points de suspension verticaux à la ligne du rapport. Vous pouvez accéder aux mêmes informations au sein du rapport.

Ajout d'un rapport

1. Cliquez sur **Ajouter un rapport**.
2. Effectuez l'une des actions suivantes :
   - Pour ajouter un rapport prédéfini, cliquez sur son nom.
   - Pour ajouter un rapport personnalisé, cliquez sur **Personnalisé**, cliquez sur le nom du rapport (les noms attribués par défaut sont similaires à **Personnalisé(1)**), puis ajoutez des widgets au rapport.
3. [Facultatif] Glissez-déplacez les widgets pour les réorganiser.
4. [Facultatif] Modifiez le rapport comme décrit ci-dessous.

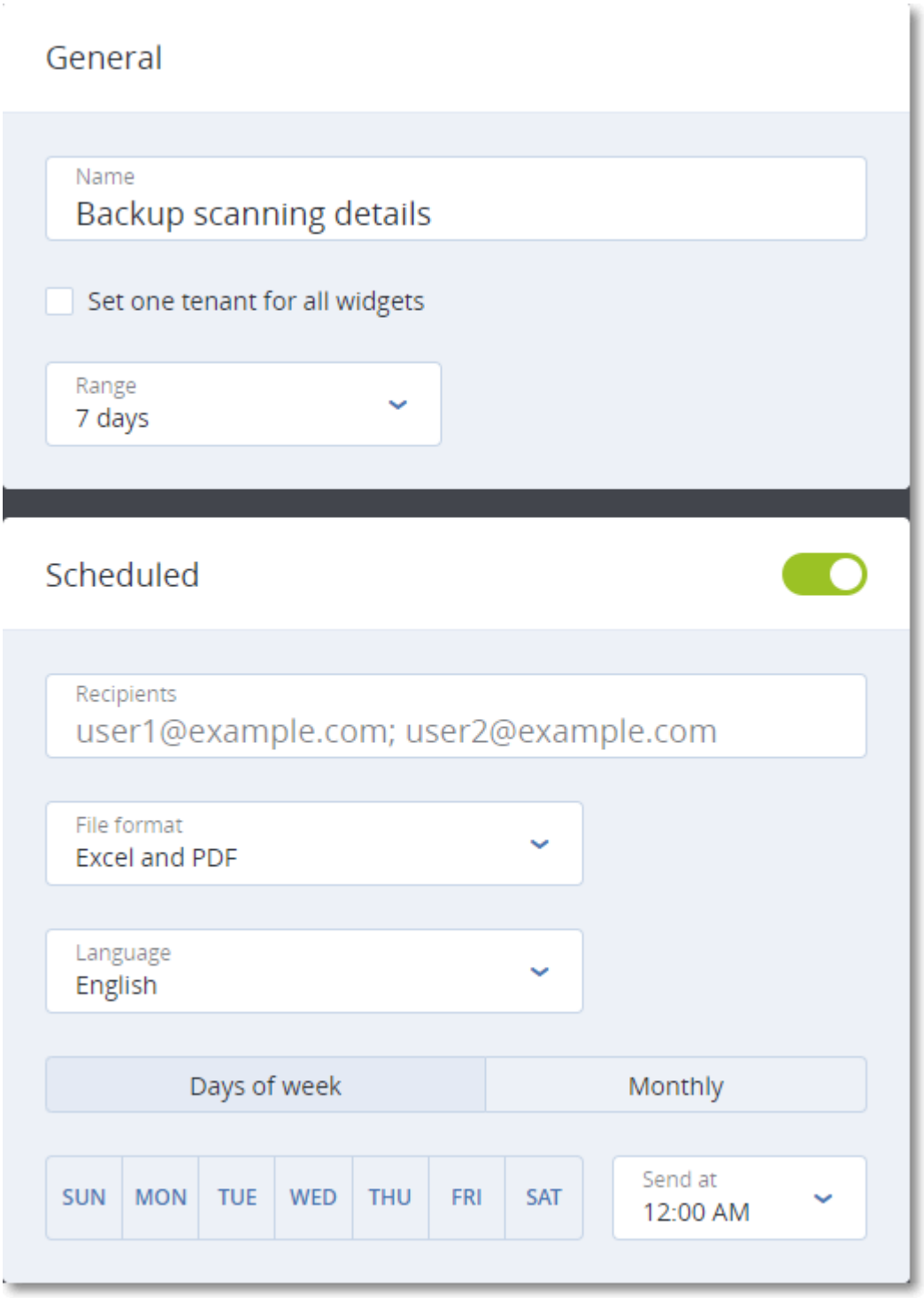
Modifier les paramètres de création de rapport

Pour modifier un rapport, cliquez sur son nom, puis sur **Paramètres**. Lorsque vous modifiez un rapport, les actions suivantes sont possibles :

- Renommer le rapport
- Modifier le locataire affiché pour tous les widgets présents dans le rapport

Si vous possédez des locataires enfants, vous aurez alors accès à l'option **Définir un locataire pour tous les widgets**. Cette option vous permet de filtrer les données de tous les widgets du rapport en fonction du locataire sélectionné. Si cette option n'est pas sélectionnée, les widgets afficheront alors les données de tous les locataires enfants de votre locataire actuel.

- Modifier l'intervalle de temps pour tous les widgets présents dans le rapport
- Planifier l'envoi du rapport par e-mail au format PDF et/ou Excel.



Planification d'un rapport

1. Cliquez sur le nom du rapport, puis sur **Paramètres**.
2. Activez le commutateur **Planifié**.
3. Indiquez l'adresse électronique des destinataires.
4. Sélectionnez le format du rapport : PDF, Excel, ou les deux.
5. Sélectionnez les jours et l'heure auxquels le rapport sera envoyé.
6. Cliquez sur **Enregistrer** dans l'angle supérieur droit.

Exportation et importation de la structure des rapports

Vous pouvez exporter et importer la structure du rapport (l'ensemble de widgets et les paramètres du rapport) via un fichier JSON. Cela peut être utile pour copier la structure du rapport d'un locataire à un autre.

Pour exporter la structure d'un rapport, cliquez sur le nom du rapport, sur l'icône en forme de points de suspension verticaux dans l'angle supérieur droit, puis sur **Exporter**.

Pour importer la structure d'un rapport, cliquez sur **Ajouter un rapport**, puis sur **Importer**.

Télécharger un rapport

Pour télécharger un rapport, cliquez sur **Télécharger** et sélectionnez les formats dont vous avez besoin :

- Excel et PDF
- Excel
- PDF

Vidage mémoire des données du rapport

Vous pouvez envoyer un vidage mémoire des données du rapport dans un fichier CSV par e-mail. Le vidage mémoire inclut toutes les données du rapport (sans filtrage) pour une plage de temps personnalisée. Dans les rapports CSV, la date et l'heure de la dernière modification sont indiqués au format UTC. Dans les rapports Excel et PDF, ils sont indiqués dans le fuseau horaire du système en cours.

Le logiciel génère le vidage mémoire des données à la volée. Si vous indiquez une plage de temps longue, cette action peut prendre plus de temps.

Pour vider les données du rapport

1. Cliquez sur le nom du rapport.
2. Cliquez sur l'icône en forme de points de suspension verticaux dans l'angle supérieur droit, puis sur **Vider les données**.

3. Indiquez l’adresse électronique des destinataires.
4. Dans **Plage de temps**, indiquez la plage de temps.
5. Cliquez sur **Envoyer**.

Synthèse

Le rapport de synthèse fournit une vue d'ensemble du statut de protection de l'environnement de vos clients et de leurs terminaux protégés pour une période spécifiée.

Le rapport de synthèse inclut des sections avec des widgets dynamiques qui affichent les indicateurs de performances clés liés à l'utilisation par les clients des services Cloud suivants : Sauvegarde, Protection antimalware, Évaluation de la vulnérabilité, Gestion des correctifs, Prévention contre la perte de données, Notary, Reprise d'activité après sinistre et File Sync & Share.

Vous pouvez personnaliser le rapport de différentes manières.

- Ajouter ou supprimer des sections.
- Changer l'ordre des sections.
- Renommer des sections.
- Déplacer des widgets d'une section à une autre.
- En changeant l'ordre des widgets de chaque section.
- En ajoutant ou en supprimant des widgets.
- En personnalisant les widgets.

Vous pouvez générer des rapports de synthèse aux formats PDF et Excel et les envoyer aux parties prenantes ou propriétaires des organisations de vos clients afin qu'ils puissent facilement consulter les indicateurs techniques et commerciaux relatifs aux services fournis.

Les administrateurs de partenaire peuvent générer et envoyer les rapports de synthèse aux clients directs uniquement. Dans le cas d'une hiérarchie de tenant plus complexe avec des sous-partenaires, les sous-partenaires doivent générer le rapport par eux-mêmes.

Widgets de synthèse

Vous pouvez supprimer ou ajouter des sections et widgets du rapport de synthèse. Cela permet de définir les informations qui y sont incluses.

Widgets d'aperçu des charges de travail

Le tableau suivant fournit plus de détails sur les widgets de la section **Aperçu des charges de travail**.

Widget	Description
Statut de	Ce widget indique le nombre de charges de travail cloud protégées et

Widget	Description
protection des charges de travail Cloud	non protégées par type au moment de la génération du rapport. Une charge de travail Cloud est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une charge de travail Cloud est considérée comme non protégée si aucun plan de protection ou de sauvegarde ne lui est appliqué. Les types de charges de travail Cloud suivants sont référencés dans le graphique (dans l'ordre alphabétique, de A à Z) : • Drive Google Workspace • Gmail Google Workspace • Drive partagé Google Workspace • Boîtes aux lettres Exchange hébergées • Boîtes aux lettres Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Sites Web Pour certains types de charges de travail, les groupes de charges de travail suivants sont utilisés : • Microsoft 365 : Utilisateurs, Groupes, Dossiers publics, Équipes et Collections de sites • Google Workspace : Utilisateurs et Disques partagés • Exchange hébergé : Utilisateurs Si l'un des groupes de charge de travail contient plus de 10 000 charges de travail, le widget n'affiche pas de données correspondant à ces charges de travail. Par exemple, si le client possède un compte Microsoft 365 avec 10 000 boîtes aux lettres et le service OneDrive pour 500 utilisateurs, étant donné que le tout est comptabilisé dans le même groupe de charge de travail utilisateurs, la somme de ces charges de travail est 10 500, ce qui dépasse la limite de 10 000 pour un groupe de charges de travail. Le widget n'affichera donc pas les types de charges de travail correspondants : Boîtes aux lettres Microsoft 365 et OneDrive Microsoft 365.
Résumé Cyber Protection	Ce widget affiche les indicateurs de performance clés de la cyberprotection pour une période spécifiée. **Données sauvegardées** : taille totale des archives créées dans les stockages local et Cloud. **Menaces atténuées** : nombre total de malware bloqués sur l'ensemble des terminaux. **URL malveillantes bloquées** : nombre total d'URL bloquées sur

Widget	Description
	l'ensemble des terminaux. **Vulnérabilités corrigées** : nombre total de vulnérabilités qui ont été corrigées par l'installation de correctifs logiciels sur l'ensemble des terminaux. **Correctifs installés** : nombre total de correctifs installés sur l'ensemble des terminaux. **Serveurs protégés par la RAS** : nombre total de serveurs protégés par la reprise d'activité après sinistre. **Utilisateurs File Sync & Share** : nombre total des utilisateurs finaux et invités qui utilisent Cyber Files. **Fichiers notarisés** : nombre total de fichiers notarisés. **Documents signés de façon électronique** : nombre total de documents signés de façon électronique. **Terminaux périphériques bloqués** : nombre total de terminaux périphériques bloqués.
Statut réseau des charges de travail	Ce widget affiche le nombre de charges de travail isolées et le nombre de charges de travail connectées (état normal des charges de travail). Sélectionnez le client pertinent ; la vue des charges de travail est filtrée et n'affiche que les charges de travail isolées. Cliquez sur Connecté pour afficher la liste des charges de travail avec agent qui ne répertorie que les charges de travail connectées (du client sélectionné).
Statut de protection des charges de travail	Ce widget indique le nombre de charges de travail protégées et non protégées par type au moment de la génération du rapport. Une charge de travail est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une charge de travail est considérée comme non protégée si aucun plan de protection ou de sauvegarde ne lui est appliqué. Les charges de travail suivantes sont prises en compte : **Serveurs** : serveurs physiques et serveurs contrôleur de domaine. **Stations de travail** : stations de travail physiques. **Machines virtuelles** : machines virtuelles avec agent et sans agent. **Serveurs d'hébergement Web** : serveurs virtuels or physiques avec cPanel ou Plesk installé. **Terminaux mobiles** : terminaux mobiles physiques. Une charge de travail peut appartenir à plusieurs catégories. Par exemple, un serveur d'hébergement Web est compté dans deux catégories : **Serveurs** et **Serveurs d'hébergement Web**.

Widget	Description
Statut de protection des charges de travail Cloud	**Statut de protection des charges de travail Cloud** Ce widget indique le nombre de charges de travail Cloud protégées et non protégées par type au moment de la génération du rapport. Une charge de travail Cloud est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une charge de travail Cloud est considérée comme non protégée si aucun plan de protection ou de sauvegarde ne lui est appliqué. Les types de charges de travail Cloud suivants sont référencés dans le graphique (dans l'ordre alphabétique, de A à Z) : • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Boîtes aux lettres Exchange hébergées • Boîtes aux lettres Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Sites Web Pour certains types de charges de travail, les groupes de charges de travail suivants sont utilisés : • Microsoft 365 : Utilisateurs, Groupes, Dossiers publics, Équipes et Collections de sites • Google Workspace : Utilisateurs et Disques partagés • Exchange hébergé : Utilisateurs Si l'un des groupes de charge de travail contient plus de 10 000 charges de travail, le widget n'affiche pas de données correspondant à ces charges de travail. Par exemple, si le client possède un compte Microsoft 365 avec 10 000 boîtes aux lettres et le service OneDrive pour 500 utilisateurs, étant donné que le tout est comptabilisé dans le même groupe de charge de travail utilisateurs, la somme de ces charges de travail est 10 500, ce qui dépasse la limite de 10 000 pour un groupe de charges de travail. Le widget n'affichera donc pas les types de charges de travail correspondants : Boîtes aux lettres Microsoft 365 et OneDrive Microsoft 365.

Widgets de protection antimalware

Le tableau suivant fournit plus de détails sur les widgets de la section **Défense contre les menaces**.

Widget	Description
Analyse antimalware des fichiers	Ce widget affiche les résultats des analyses antimalware effectuées à la demande sur les terminaux pour une période spécifiée. **Fichiers** : nombre total de fichiers analysés **Propres** : nombre total de fichiers propres **Détectés, mis en quarantaine** : nombre total de fichiers infectés mis en quarantaine **Détectés, non mis en quarantaine** : nombre total de fichiers infectés, non mis en quarantaine **Terminaux protégés** : nombre total de terminaux auxquels une règle de protection antimalware est appliquée **Total de terminaux enregistrés** : nombre total de terminaux enregistrés au moment de la génération du rapport
Analyse anti-malware des sauvegardes	Ce widget affiche les résultats des analyses antimalware des sauvegardes pour une période spécifiée, en utilisant les indicateurs suivants : • Nombre total de points de restauration analysés • Nombre de points de récupération propres • Nombre de points de récupération propres avec partitions non prises en charge • Nombre de points de récupération infectés. Cet indicateur inclut le nombre de points de récupération infectés avec partitions non prises en charge.
URL bloquées	Ce widget affiche les URL bloquées classées par catégorie de site Web pour une période spécifiée. Le widget liste les sept catégories de site Web qui totalisent le plus grand nombre d'URL bloquées. Les autres catégories sont regroupées dans la section **Autres**. Pour plus d'informations sur les catégories de site Web, consultez la section dédiée au filtrage des URL dans Cyber Protection.
Résolution des incidents de sécurité	Ce widget indique l'efficacité de la clôture des incidents pour la société sélectionnée ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie. Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.
MTTR de l'incident	Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus. Cliquez sur une colonne pour afficher le détail des incidents en fonction de la

Widget	Description
	gravité (**Critique**, **Élevé** et **Moyen**), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.
Statut de la menace	Ce widget affiche le statut de menace actuel pour les charges de travail d'une entreprise (quel que soit le nombre de charges de travail) en mettant en évidence le nombre actuel d'incidents qui ne sont pas résolus et doivent faire l'objet d'enquêtes. Le widget indique également le nombre d'incidents résolus (manuellement et/ou automatiquement par le système).
Menaces détectées par la technologie de protection	Ce widget affiche le nombre de menaces détectées durant une période spécifique, classées selon les technologies de protection suivantes : • Analyse antimalware • Moteur de comportement • Protection contre le cryptomining • Prévention des exploits • Protection active contre les ransomwares • Protection en temps réel • Filtrage d'URL

Widgets de sauvegarde

Le tableau suivant fournit plus de détails sur les widgets de la section **Sauvegarde**.

Widget	Description
Charges de travail sauvegardées	Ce widget indique le nombre total de charges de travail enregistrées classées par statut de sauvegarde. **Sauvegardées** : nombre total de charges de travail sauvegardées (au moins une sauvegarde effectuée avec succès) durant la période couverte par le rapport. **Non sauvegardées** : nombre total de charges de travail non sauvegardées (aucune sauvegarde effectuée avec succès) durant la période couverte par le rapport.
Intégrité de disque par terminaux physiques	Ce widget affiche les statuts d'intégrité agrégés des terminaux physiques basés sur le statut d'intégrité de leurs disques. **OK** : le statut d'intégrité du disque correspond à une valeur comprise entre [70 à 100]. Le statut du terminal est **OK** quand tous les statuts de ces disques sont **OK**. **Avertissement** : le statut d'intégrité du disque correspond à une valeur comprise entre [30 et 70]. Le statut du terminal est **Avertissement** quand au moins un de ses disques a pour statut **Avertissement**, mais qu'aucun

Widget	Description
	disque n'a pour statut **Erreur**. **Erreur** : le statut d'intégrité du disque correspond à une valeur comprise entre [0 et 30]. Le statut du terminal est **Erreur** quand au moins un de ses disques a pour statut **Erreur**. **Calcul des données du disque** : le statut du terminal est **Calcul des données du disque** lorsque tous les statuts des disques ne sont pas encore déterminés.
Utilisation du stockage de sauvegarde	Ce widget affiche le nombre total et la taille totale des sauvegardes dans les stockages local et Cloud pour une période spécifiée.

Widgets Évaluation des vulnérabilités et gestion des correctifs

Le tableau suivant fournit plus de détails sur les widgets de la section **Évaluation des vulnérabilités et gestion des correctifs**.

Widget	Description
Vulnérabilités corrigées	Ce widget affiche les résultats de performance du plan d'évaluation de la vulnérabilité pour la période spécifiée. **Total** : le nombre total de vulnérabilités corrigées. **Vulnérabilités logicielles Microsoft** : le nombre total de vulnérabilités Microsoft corrigées sur l'ensemble des terminaux Windows. **Vulnérabilités logicielles tierces Windows** : le nombre total de vulnérabilités tierces corrigées sur l'ensemble des terminaux Windows. **Charges de travail analysées** : le nombre total de charges de travail analysées avec succès à la recherche de vulnérabilités au moins une fois durant la période spécifiée.
Correctifs installés	Ce widget affiche les résultats de performance de gestion des correctifs pour la période spécifiée. **Installés** : le nombre total de correctifs installés avec succès sur l'ensemble des terminaux. **Correctifs logiciels Microsoft** : le nombre total de correctifs logiciels Microsoft installés avec succès sur l'ensemble des terminaux Windows. **Correctifs logiciels tiers Windows** : le nombre total de correctifs logiciels tiers Windows installés avec succès sur l'ensemble des terminaux Windows. **Charges de travail corrigées** : le nombre total de terminaux corrigés avec succès (au moins un correctif a été installé avec succès durant la période spécifiée).

Widgets de reprise d'activité après sinistre

Le tableau suivant fournit plus de détails sur les widgets de la section **Reprise d'activité après sinistre**.

Widget	Description
Statistiques de reprise d'activité après sinistre	Ce widget affiche les indicateurs de performance clés du plan de reprise d'activité après sinistre pour la période spécifiée. **Basculements de production** : nombre d'opérations de basculement de production pour la période spécifiée. **Basculements de test** : nombre d'opérations de basculement de test effectuées durant la période spécifiée. **Serveurs primaires** : nombre total de serveurs primaires existant au moment de la génération du rapport. **Serveurs de restauration** : nombre total de serveurs de restauration existant au moment de la génération du rapport. **IP publiques** : nombre total d'adresses IP publiques (existant au moment de la génération du rapport). **Total des points de calcul consommés** : nombre total des points de calcul consommés durant la période spécifiée.
Serveurs de reprise d'activité après sinistre testés	Ce widget fournit des informations sur les serveurs protégés par la reprise d'activité après sinistre et vérifiés avec le basculement test. Le widget affiche les indicateurs suivants : **Serveurs protégés** : nombre de serveurs protégés par la reprise d'activité après sinistre (serveurs avec au moins un serveur de restauration) au moment de la génération du rapport. **Testés** : nombre de serveurs protégés par la reprise d'activité après sinistre qui ont été vérifiés avec le basculement test au cours de la période spécifiée, par rapport au nombre total de serveurs protégés par la reprise d'activité après sinistre. **Non testés** : nombre de serveurs protégés par la reprise d'activité après sinistre qui n'ont pas été vérifiés avec le basculement test au cours de la période spécifiée, par rapport au nombre total de serveurs protégés par la reprise d'activité après sinistre. Le widget indique également le volume en Go du stockage de reprise d'activité après sinistre au moment de la génération du rapport. Cela correspond à la somme des volumes de sauvegardes des serveurs Cloud.
Serveurs protégés par la	Ce widget fournit des informations sur les serveurs protégés par la reprise d'activité après sinistre et les serveurs non protégés.

Widget	Description
reprise d'activité après sinistre	Le widget affiche les indicateurs suivants : Le nombre total de serveurs enregistrés dans le tenant client au moment de la génération du rapport. **Protégés** : nombre de serveurs protégés par la reprise d'activité après sinistre (avec au moins un serveur de restauration et une sauvegarde de serveur complète), par rapport au nombre total de serveurs enregistrés au moment de la génération du rapport. **Non protégés** : nombre total de serveurs non protégés, par rapport au le nombre total de serveurs enregistrés au moment de la génération du rapport.

Widget de prévention des pertes de données

Vous trouverez de plus amples informations sur les terminaux périphériques bloqués dans la section **Prévention contre la perte de données** de la rubrique suivante.

Ce widget indique le nombre total de terminaux bloqués et le nombre total de terminaux bloqués par type de terminaux pour une période spécifique.

- Stockage amovible
- Amovible chiffré
- Imprimantes
- Presse-papiers : inclut les types de terminaux Presse-papiers et Capture d'écran.
- Terminaux mobiles
- Bluetooth
- Lecteurs optiques
- Disquettes
- USB : inclut les types de terminaux Port USB et Port USB redirigé.
- FireWire
- Lecteurs mappés :
- Presse-papiers redirigé : inclut les types de terminaux Presse-papiers redirigé entrant et Presse-papiers redirigé sortant.

Ce widget affiche les sept types de terminaux qui comptabilisent le plus de terminaux bloqués et rassemble les autres types de terminaux sous la classe **Autres**.

Widget File Sync & Share

Le tableau suivant fournit plus de détails sur les widgets de la section **File Sync & Share**.

Widget	Description
Statistiques File Sync & Share	Le widget affiche les indicateurs suivants : **Total de stockage dans le Cloud utilisé** : le total de stockage Cloud utilisé par tous les utilisateurs. **Utilisateurs finaux** : le nombre total d'utilisateurs finaux. **Moyenne du stockage utilisé par utilisateur final** : le stockage utilisé en moyenne par un utilisateur final. **Utilisateurs invités** : le nombre total d'utilisateurs invités.
Utilisation du stockage File Sync & Share par les utilisateurs finaux	Ce widget indique le nombre total d'utilisateurs File Sync & Share qui utilisent un stockage correspond aux plages suivantes : • 0 à 1 Go • 1 à 5 Go • 5 à 10 Go • 10 à 50 Go • 50 à 100 Go • 100 à 500 Go • 500 Go à 1 To • Plus d'1 To

Widgets de Notary

Le tableau suivant fournit plus de détails sur les widgets de la section **Notary**.

Widget	Description
Statistiques Cyber Notary	Le widget affiche les indicateurs Notary suivants : **Stockage Notary Cloud utilisé** : la taille totale du stockage utilisé pour le service Notary. **Fichiers notarisés** : nombre total de fichiers notarisés. **Documents signés de façon électronique** : le nombre total de documents et fichiers signés de façon électronique.
Fichiers notarisés pour l'ensemble des utilisateurs finaux	Indique le nombre total de fichiers notarisés pour l'ensemble des utilisateurs finaux. Les utilisateurs sont regroupés en fonction de leur nombre de fichiers notarisés. • Jusqu'à 10 fichiers • 11 à 100 fichiers • 101 à 500 fichiers • 501 à 1000 fichiers • Plus de 1 000 fichiers

Widget	Description
Documents signés de façon électronique pour l'ensemble des utilisateurs finaux	Ce widget indique le nombre total de documents et fichiers signés de façon électronique pour l'ensemble des utilisateurs finaux. Les utilisateurs sont regroupés en fonction de leur nombre de fichiers et documents signés de façon électronique. • Jusqu'à 10 fichiers • 11 à 100 fichiers • 101 à 500 fichiers • 501 à 1000 fichiers • Plus de 1 000 fichiers

Configuration des paramètres du rapport de synthèse

Vous pouvez modifier les paramètres du rapport de synthèse qui ont été définis lors de sa création.

Pour modifier les paramètres du rapport de synthèse

1. Dans la console de gestion, accédez à **Rapports**>**Synthèse**.
2. Cliquez sur le nom du rapport de synthèse dont vous souhaitez modifier les paramètres.
3. Cliquez sur **Paramètres**.
4. Modifiez les valeurs des champs selon vos besoins.
5. Cliquez sur **Enregistrer**.

Création d'un rapport de synthèse

Pour pouvez créer un rapport de synthèse, visualiser son contenu, configurer ses destinataires et planifier son envoi automatique.

Pour créer un rapport de synthèse

1. Dans la console de gestion, accédez à **Rapports**>**Synthèse**.
2. Cliquez sur **Créer un rapport de synthèse**.
3. Sous **Nom du rapport**, saisissez le nom du rapport.
4. Sélectionnez les destinataires du rapport.
   - Si vous souhaitez envoyer le rapport à tous les clients directs, sélectionnez **Envoyer à tous les clients directs**.
   - Si vous souhaitez envoyer le rapport à des clients spécifiques
     a. Désélectionnez **Envoyer à tous les clients directs**.
     b. Cliquez sur **Sélectionner des contacts**.
     c. Sélectionnez les clients spécifiques. Vous pouvez effectuer une Recherche pour trouver

facilement un contact spécifique.

d. Cliquez sur **Sélectionner**.

5. Sélectionnez une plage : **30 jours** ou **Ce mois-ci**
6. Sélectionnez un format de fichier : **PDF**, **Excel** ou **Excel et PDF**.
7. Configurer les paramètres de planification.
   - Si vous souhaitez envoyer le rapport aux destinataires à une heure et une date spécifiques :
     a. Activez l'option **Planifié**.
     b. Cliquez sur le champ **Jour du mois**, désélectionnez Dernier jour, et cliquez sur le jour souhaité.
     c. Dans le champ **Heure**, saisissez l'heure souhaitée.
     d. Cliquez sur **Appliquer**.
   - Si vous souhaitez créer le rapport sans l'envoyer à ses destinataires, désactivez l'option **Planifié**.
8. Cliquez sur **Enregistrer**.

Personnalisation du rapport de synthèse

Vous pouvez définir les informations à inclure dans le rapport de synthèse. Vous pouvez ajouter ou supprimer des sections, ajouter ou supprimer des widgets, renommer des sections, personnaliser des widgets et glisser-déposer les widgets et sections pour modifier leur ordre d'affichage dans le rapport.

Pour ajouter une section

1. Cliquez sur **Ajouter un élément** > **Ajouter une section**.
2. Dans la fenêtre **Ajouter une section**, saisissez un nom de section, ou utilisez le nom de section par défaut.
3. Cliquez sur **Ajouter au rapport**.

Pour renommer une section

1. Dans la section que vous désirez renommer, cliquez sur **Modifier**.
2. Dans la fenêtre **Modifier la section**, saisissez le nouveau nom.
3. Cliquez sur **Enregistrer**.

Pour supprimer une section

1. Dans la section que vous désirez supprimer, cliquez sur **Modifier la section**.
2. Dans la fenêtre de confirmation **Supprimer la section**, cliquez sur **Supprimer**.

Pour ajouter un widget avec ses paramètres par défaut à une section

1. Dans la section à laquelle vous souhaitez ajouter le widget, cliquez sur **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, cliquez sur le widget que vous désirez ajouter.

Pour ajouter un widget personnalisé à une section

1. Dans la section à laquelle vous souhaitez ajouter le widget, cliquez sur **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, recherchez le widget que vous désirez ajouter, puis cliquez sur **Personnaliser**.
3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Ajouter un widget**.

Pour ajouter un widget avec ses paramètres par défaut au rapport

1. Cliquez sur **Ajouter un élément** > **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, cliquez sur le widget que vous désirez ajouter.

Pour ajouter un widget personnalisé au rapport

1. Cliquez sur **Ajouter un widget**.
2. Dans la fenêtre **Ajouter un widget**, recherchez le widget que vous désirez ajouter, puis cliquez sur **Personnaliser**.
3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Ajouter un widget**.

Pour rétablir les paramètres par défaut d'un widget

1. Dans le widget que vous désirez personnaliser, cliquez sur **Modifier**.
2. Cliquez sur **Rétablir les paramètres par défaut**.
3. Cliquez sur **Valider**.

Pour personnaliser un widget

1. Dans le widget que vous désirez personnaliser, cliquez sur **Modifier**.
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Valider**.

Envoi des rapports de synthèse

Vous pouvez envoyer un rapport de synthèse à la demande. Dans ce cas, le paramètre **Planifié** est ignoré, et le rapport est envoyé immédiatement. Pour l'envoi, le système utilise les valeurs de Destinataires, Plage et Format de fichier paramétrées dans les **Paramètres**. Vous pouvez modifier manuellement ces paramètres avant l'envoi du rapport. Pour plus d'informations, voir "Configuration des paramètres du rapport de synthèse" (p. 119).

Pour envoyer un rapport de synthèse

1. Dans le portail de gestion, accédez à **Rapports**>**Synthèse**.
2. Cliquez sur le nom du rapport de synthèse que vous souhaitez envoyer.
3. Cliquez sur **Envoyer maintenant**.
   Le rapport envoie alors le rapport de synthèse aux destinataires sélectionnés.

Fuseaux horaires dans les rapports

Les fuseaux horaires utilisés dans les rapports varient selon le type de rapport. Le tableau suivant contient des informations pour votre information.

Emplacement et type du rapport	Fuseaux horaires utilisés dans le rapport
Portail de gestion > Aperçu > Opérations (widgets)	L'heure de génération du rapport est indiquée dans le fuseau horaire de la machine sous laquelle le navigateur s'exécute.
Portail de gestion > Aperçu > Opérations (exporté vers PDF ou xslx)	• L'horodatage du rapport exporté est indiqué dans le fuseau horaire de la machine utilisée pour exporter le rapport. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Utilisation > Rapports planifiés	• Le rapport est généré à 23:59:59 (UTC) le premier jour du mois. • Le rapport est envoyé le deuxième jour du mois.
Portail de gestion > Rapports > Utilisation > Rapports personnalisés	Le fuseau horaire et la date du rapport sont indiqués en UTC.
Portail de gestion > Rapports > Opérations (widgets)	• L'heure de génération du rapport est indiquée dans le fuseau horaire de la machine sous laquelle le navigateur s'exécute. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Opérations (exporté vers PDF ou xslx)	• L'horodatage du rapport exporté est indiqué dans le fuseau horaire de la machine utilisée pour exporter le rapport. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Opérations (livraison planifiée)	• Le fuseau horaire de la livraison du rapport est indiqué en UTC. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Utilisateurs > Résumé quotidien concernant les alertes actives	• Ce rapport est envoyé une fois entre 10:00 et 23:59 UTC. L'heure à laquelle le rapport est envoyé dépend de la charge de travail du centre de données. • Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Utilisateurs >	• Ce rapport est envoyé lorsqu'une activité est terminée.

Notifications du statut de cyberprotection	**Remarque** En fonction de la charge de travail du centre de données, il se peut que certains rapports soient envoyés en retard. • Le fuseau horaire de l'activité du rapport est indiqué en UTC.

Données rapportées en fonction du type de widget

Les widgets du tableau de bord peuvent être classés selon deux catégories, selon le type de données qu'ils présentent :

- Les widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.
- Les widgets qui affichent les données historiques.

Lorsque vous configurez une plage de dates dans les paramètres de rapport afin d'effectuer un vidage mémoire des données d'une certaine période, la plage de dates sélectionnée s'applique uniquement aux widgets qui affichent des données historiques. Elle n'est pas applicable aux widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.

Le tableau suivant énumère les widgets et leurs plages de données.

Nom du widget	Données affichées dans le widget et les rapports
Score #CyberFit par machine	Actuelles
5 dernières alertes	Actuelles
Détails des alertes actives	Actuelles
Résumé des alertes actives	Actuelles
Activités	Historiques
Liste des activités	Historiques
Historique des alertes	Historiques
Analyse anti-malware des sauvegardes	Historiques
Analyse antimalware des fichiers	Historiques
Détails de l'analyse de la sauvegarde (menaces)	Historiques
État de la sauvegarde	Historiques, dans les colonnes **Exécutions totales** et **Nombre d'exécutions réussies** Actuelles, dans toutes les autres colonnes
Utilisation du stockage de sauvegarde	Historiques

Terminaux périphériques bloqués	Historiques
URL bloquées	Actuelles
Applications dans le Cloud	Actuelles
Statut de protection des charges de travail Cloud	Actuelles
Cyber protection	Actuelles
Résumé Cyber Protection	Historiques
Carte de la protection des données	Historiques
Appareils	Actuelles
Serveurs de reprise d'activité après sinistre testés	Historiques
Statistiques de reprise d'activité après sinistre	Historiques
Machines découvertes	Actuelles
Vue d'ensemble de l'état de santé du disque	Actuelles
Intégrité du disque	Actuelles
Intégrité de disque par terminaux physiques	Actuelles
Documents signés de façon électronique pour l'ensemble des utilisateurs finaux	Actuelles
Vulnérabilités existantes	Historiques
Statistiques File Sync & Share	Actuelles
Utilisation du stockage File Sync & Share par les utilisateurs finals	Actuelles
Modifications apportées au matériel	Historiques
Détails du matériel	Actuelles
Inventaire matériel	Actuelles
Résumé des alertes d'historique	Historiques
Résumé des emplacements	Actuelles
Mises à jour manquantes, par catégorie	Actuelles
Non protégé	Actuelles
Fichiers notarisés pour l'ensemble des utilisateurs finaux	Actuelles
Statistiques Notary	Actuelles

Historique d'installation des correctifs	Historiques
Statut d'installation des correctifs	Historiques
Résumé d'installation des correctifs	Historiques
Vulnérabilités corrigées	Historiques
Correctifs installés	Historiques
État de protection	Actuelles
Affectés récemment	Historiques
Sessions distantes	Historiques
Résolution des incidents de sécurité	Historiques
Temps moyen de réparation des incidents de sécurité	Historiques
Serveurs protégés par la reprise d'activité après sinistre	Actuelles
Inventaire du logiciel	Actuelles
Aperçu du logiciel	Historiques
Statut de la menace	Actuelles
Menaces détectées par la technologie de protection	Historiques
Distribution des principaux incidents par charge de travail	Actuelles
Machines vulnérables	Actuelles
Statut réseau des charges de travail	Actuelles
Charges de travail sauvegardées	Historiques
Statut de protection des charges de travail	Actuelles

Journal d'audit

Pour afficher le journal d'audit, cliquez sur **Journal d'audit**.

Le journal d'audit fournit un enregistrement chronologique des événements suivants :

- Opérations effectuées par les utilisateurs dans le portail de gestion
- Opérations avec des ressources Cloud à Cloud effectuées par des utilisateurs dans la console de service Cyber Protection

- Opérations de création de scripts effectuées par des utilisateurs dans la console de service Cyber Protection
- Messages système concernant les quotas atteints et l'utilisation des quotas

Le journal affiche les événements du locataire dans lequel vous fonctionnez actuellement, et de ses unités enfants. Vous pouvez cliquer sur un événement pour afficher davantage d'informations le concernant.

Les journaux d'audit sont stockés dans le centre de données, et leur disponibilité ne peut pas être affectée par des problèmes survenant sur les ordinateurs de l'utilisateur final.

Le journal est nettoyé quotidiennement. Les événements sont supprimés au bout de 180 jours.

Champs de journal d'audit

Pour chaque événement, le journal affiche :

- **L'événement**
  Courte description de l'événement. Par exemple, **Tenant créé**, **Tenant supprimé**, **Utilisateur créé**, **Utilisateur supprimé**, **Quota atteint**, **Le contenu de la sauvegarde a été parcouru**, **Le script a été modifié**.
- **La gravité**
  Peut être l'une des options suivantes :
  - **Erreur**
    Indique une erreur.
  - **Avertissement**
    Indique une action négative potentielle. Par exemple, **Locataire supprimé**, **Utilisateur supprimé**, **Quota atteint**.
  - **Les mentions légales**
    Indique un événement qui peut nécessiter votre attention. Par exemple, **Locataire mis à jour**, **Utilisateur supprimé**.
  - **Les informations**
    Indique un changement ou une action informatifs neutres. Par exemple, **Tenant créé**, **Utilisateur créé**, **Utilisateur mis à jour**, **Le plan de création de script a été supprimé**.
- **La date**
  Date et heure auxquelles l'événement a eu lieu.
- **Le nom d'objet**
  Objet avec lequel l'opération a été effectuée. Par exemple, l'objet de l'événement **Utilisateur mis à jour** est l'utilisateur dont les propriétés ont été modifiées. Pour les événements associés à un quota, le quota est l'objet.
- **Le locataire**
  Nom du locataire auquel l'objet appartient.
- **L'initiateur**

Identifiant de l’utilisateur qui a initié l'événement. Pour les messages système et événements initiés par des administrateurs de haut niveau, l'initiateur est affiché comme **Système**.

- **L'initiateur du locataire**

  Nom du locataire auquel l'initiateur appartient. Pour les messages système et les événements initiés par des administrateurs de haut niveau, le champ est vide.
- **Méthode**

  Indique si l'événement a été initié via l'interface Web ou via l'API.
- **IP**

  L'adresse IP de la machine à partir de laquelle l'événement a été initié.

Filtrer et rechercher

Vous pouvez filtrer les événements par type, gravité ou date. Vous pouvez également rechercher les événements par nom, objet, tenant, initiateur et initiateur du tenant.

Packs de protection avancés

Vous pouvez activer les packs de protection avancés en plus du service Protection. Ils sont soumis à des frais supplémentaires. Les packs de protection avancés fournissent une fonctionnalité unique qui n'interfère pas avec l'ensemble de fonctionnalités standard, ni d'autres packs avancés. Les clients peuvent protéger leur charge de travail avec un, plusieurs ou tous les packs avancés. Les packs de protection avancés sont disponibles pour les deux méthodes de facturation du service Protection : par charge de travail et par gigaoctet.

Les fonctionnalités Advanced File Sync & Share peuvent être activées avec le service File Sync & Share. Il est disponible dans les deux modes de facturation : par utilisateur et par gigaoctet.

Vous pouvez activer les packs de protection avancés suivants :

- Advanced - Sauvegarde
- Advanced - Gestion
- Advanced - Sécurité
- Advanced Security + EDR
- Advanced Data Loss Prevention
- Advanced - Reprise d’activité après sinistre
- Advanced - Sécurité e-mail
- Advanced - File Sync & Share

Remarque
Les packs avancés ne peuvent être utilisés que lorsque la fonctionnalité qu'ils étendent est activée. Les utilisateurs ne peuvent pas utiliser de fonctionnalités avancées lorsque la fonctionnalité de service standard est désactivée. Par exemple, ils ne peuvent pas utiliser les fonctionnalités du pack Advanced Backup si la fonctionnalité Protection est désactivée.

Si un pack de protection avancée est activé, ses fonctionnalités apparaissent dans le plan de protection et sont identifiées par l'icône Fonctionnalité avancée  . Lorsque les utilisateurs essaient d'activer la fonctionnalité, ils sont avertis que des frais supplémentaires s'appliquent.

Si un pack de protection avancée n'est pas activé, mais que la vente additionnelle est activée, les fonctionnalités de protection avancées apparaissent dans le plan de protection, mais ne sont pas utilisables. L'icône suivant s'affiche à côté du nom de la fonctionnalité . Un message invite alors les utilisateurs à contacter leur administrateur afin qu'il puisse activer l'ensemble de fonctionnalités avancées requis.

Si un pack de protection avancée n'est pas activé et que la vente additionnelle est désactivée, les clients ne voient pas les fonctionnalités avancées dans leurs plans de protection.

Fonctionnalités incluses et packs avancés dans les services Cyber Protect

Lorsque vous activez un service ou un ensemble de fonctionnalités dans Cyber Protect, vous activez un certain nombre de fonctionnalités incluses et disponibles par défaut. Vous pouvez également activer les packs de protection avancés.

Les sections suivantes contiennent un aperçu de haut niveau des fonctionnalités et packs avancés du service Cyber Protect. Pour obtenir la liste de toutes les offres, consultez le Guide des licences Cyber Protect.

Fonctionnalités incluses et avancées du service Protection

Fonctionnalités incluses et avancées du service Protection

Groupe de fonctionnalités	Fonctionnalités standard incluses	Fonctionnalités avancées
Sécurité	• Score #CyberFit • Évaluation des vulnérabilités • Protection anti-ransomware : Active Protection • Protection contre les virus et les malwares : Détection de fichier basée sur la signature dans le Cloud (aucune protection en temps réel, uniquement une analyse programmée)* • Protection contre les virus et les malwares : Analyse de fichier basée sur l'IA avant exécution, cyber-moteur basé sur le comportement • Gestion de Microsoft Defender *Afin de détecter les attaques au jour zéro, Cyber Protect utilise des règles et algorithmes d'analyse heuristiques pour rechercher des commandes malveillantes.	Il existe deux packs de protection avancée disponibles : **Advanced Security** et **Advanced Security + EDR**. Le pack Advanced Security comprend : • Protection en temps réel contre les virus et les malwares avec détection basée sur la signature locale (avec protection en temps réel) • Prévention des exploits • Filtrage d'URL • Gestion du pare-feu des terminaux • Sauvegarde d'investigation, analyse des sauvegardes à la recherche de malwares, reprise sécurisée, liste d'autorisation de l'entreprise • Plans de protection intelligent (Intégration avec des alertes CPOC) • Analyse de sauvegarde centralisée à la recherche de malwares • Effacement à distance Le pack de protection Advanced Security + EDR comprend toutes les fonctionnalités ci-dessus, ainsi que les fonctionnalités EDR (Endpoint Detection and Response) suivantes pour

Groupe de fonctionnalités	Fonctionnalités standard incluses	Fonctionnalités avancées
		l'identification des menaces avancées ou des attaques en cours : • Gérer les incidents dans une page Incident centralisée • Visualiser la portée et l'impact des incidents • Recommandations et étapes de réparation • Consulter les attaques publiquement dévoilées sur vos ressources à l'aide de flux d'informations sur les menaces • Stocker les événements de sécurité pendant 180 jours Pour plus d'informations sur l'activation du pack Advanced Security + EDR, voir "Activation d'Advanced Security + EDR" (p. 134).
Prévention contre la perte de données	• Contrôle du périphérique	• Solution sensible au contenu pour la protection des charges de travail contre la perte de données via les terminaux et communications réseau • Détection automatique intégrée des informations personnelles identifiables (PII), des informations de santé protégées (PHI) et des données de l'industrie des cartes de paiement (PCI DSS), ainsi que des documents présents dans la catégorie « Marqué confidentiel » • Création automatique de règles de prévention de la perte de données avec assistance facultative pour l'utilisateur final • Application de la prévention de la perte de données avec ajustement des règles en fonction de l'apprentissage automatique • Centralisation des journaux d'audit, des alertes et des notifications à destination de l'utilisateur final dans le cloud

Groupe de fonctionnalités	Fonctionnalités standard incluses	Fonctionnalités avancées
Gestion	• Gestion de groupe des charges de travail • Gestion centralisée des plans de protection • Inventaire matériel • Contrôle distant • Actions à distance • Connexions simultanées par technicien • Protocole de connexion à distance : RDP	• Gestion des correctifs • État de santé du disque • Inventaire du logiciel • Application de correctifs sans échec • Création de cyber-scripts • Assistance à distance • Transfert et partage de fichiers • Sélection d'une session à laquelle se connecter • Observation de charges de travail en vue multiple • Modes de connexion : contrôle, observation et rideau • Connexion via l'application Quick Assist • Protocoles de connexion à distance : NEAR et Partage d'écran • Enregistrement de session pour les connexions NEAR • Transmission de captures d'écran • Rapport d'historique des sessions
Sécurité de la messagerie électronique	Aucun	Protection en temps réel pour vos boîtes aux lettres Microsoft 365 et Gmail : • Antimalware et antispam • Analyse d'URL dans les e-mails • Analyse DMARC • Anti-hameçonnage • Protection contre l'usurpation d'identité • Analyse des pièces jointes • Désarmement et reconstruction du contenu • Schéma de confiance Consultez le guide de configuration.
Cyber Disaster Recovery Cloud	Vous pouvez utiliser les fonctionnalités standard de Disaster Recovery pour tester les scénarios de reprise d'activité après sinistre pour vos charges de travail.	Vous pouvez activer le pack Advanced Disaster Recovery et protéger vos charges de travail à l'aide de la fonctionnalité Disaster Recovery complète.

Groupe de fonctionnalités	Fonctionnalités standard incluses	Fonctionnalités avancées
	Notez les fonctionnalités standard disponibles dans Disaster Recovery, ainsi que leurs limites : • Basculement test dans un environnement réseau isolé. Limité à 32 points de calcul par mois, et jusqu'à 5 opérations de basculement test en même temps. • Configurations de serveur de restauration : 1 processeur et 2 Go de RAM, 1 processeur et 4 Go de RAM, et 2 processeurs et 8 Go de RAM. • Nombre de points de récupération disponibles pour le basculement : uniquement le dernier point de récupération disponible juste après une sauvegarde. • Modes de connectivité disponibles : Cloud uniquement et de point à site. • Disponibilité de la passerelle VPN : La passerelle VPN sera temporairement suspendue si elle reste inactive pendant 4 heures une fois le dernier basculement test terminé, et sera de nouveau déployée lorsque vous démarrerez un basculement test. • Nombre de réseaux Cloud : 1. • Accès Internet • Opérations avec les runbooks : création et édition.	Notez les fonctionnalités avancées disponibles dans Disaster Recovery : • Basculement de la production • Basculement test dans un environnement réseau isolé. • Nombre de points de récupération disponibles pour le basculement : tous les points de récupération disponibles après la création d'un serveur de restauration. • Serveurs primaires • Configurations des serveurs de restauration/primaire : Aucune limite • Modes de connectivité disponibles : Cloud uniquement, De point à site, OpenVPN de site à site, et VPN IPsec multi-site. • Disponibilité de la passerelle VPN : toujours disponible. • Nombre de réseaux Cloud : 23. • Adresses IP publiques • Accès Internet • Opérations avec les runbooks : création, édition et exécution.

Fonctionnalités avancées facturées en fonction de l'utilisation, dans le cadre du service Protection

Fonctionnalités avancées facturées en fonction de l'utilisation, dans le cadre du service Protection

Groupe de fonctionnalités	Fonctionnalités de facturation à l'utilisation	Fonctionnalités avancées
Sauvegarde	• Sauvegarde de fichiers • Sauvegarde d'images • Sauvegarde d'applications • Sauvegarde de partages réseau	• Serveur Microsoft SQL et clusters Microsoft Exchange • Base de données Oracle • SAP HANA

Groupe de fonctionnalités	Fonctionnalités de facturation à l'utilisation	Fonctionnalités avancées
	• Sauvegarde dans le stockage dans le Cloud • Sauvegarde dans le stockage local **Remarque** Des frais sont applicables pour l'utilisation du stockage dans le Cloud.	• Carte de la protection des données • Protection continue des données • Plans de traitement des données hors hôte • Notarisation des sauvegardes • Postes Microsoft 365 • Postes Google Workspace
File Sync & Share	• Stocker du contenu chiffré, basé sur des fichiers • Synchroniser des fichiers entre tous vos terminaux désignés • Partager des dossiers et fichiers avec des personnes et systèmes désignés	• Notarisation et signature électronique • Modèles de document* * Sauvegarde de fichiers de synchronisation et de partage
Envoi de données physiques	Fonctionnalité d'envoi de données physiques	Sans Objet
Notary	• Notarisation de fichiers • Signature électronique de fichiers • Modèles de document	Sans Objet

Remarque
Vous ne pouvez pas activer les packs de protection avancés sans activer la fonctionnalité de protection standard qu'ils étendent. Si vous désactivez une fonctionnalité, ses packs avancés sont automatiquement désactivés, et les plans de protection qui les utilisent seront automatiquement révoqués. Par exemple, si vous désactivez la fonctionnalité de protection, ses packs avancés seront automatiquement désactivés, et tous les plans qui les utilisent seront révoqués.

Les utilisateurs ne peuvent pas utiliser de packs de protection avancés sans protection standard, mais peuvent utiliser uniquement les fonctionnalités incluses de la protection standard de concert avec les packs avancés sur des charges de travail spécifiques. Dans ce cas, ils ne seront facturés que pour les packs avancés qu'ils utilisent.

Pour en savoir plus sur la facturation, consultez "Méthodes de facturation pour Cyber Protect" (p. 8).

Advanced Data Loss Prevention

Le module Advanced Data Loss Prevention évite les fuites d'informations sensibles depuis des postes de travail, des serveurs et des machines virtuelles en inspectant le contenu des données transférées via des canaux locaux et réseaux et en appliquant les règles de flux de données propres à l'organisation.

Avant de commencer à utiliser le module Advanced Data Loss Prevention, veillez à lire et à comprendre les concepts de base et la logique de la gestion Advanced Data Loss Prevention qui sont décrits dans le guides des principes fondamentaux.

Vous souhaiterez peut-être consulter également le document Caractéristiques techniques.

Activation du module Advanced Data Loss Prevention

Par défaut, le module Advanced Data Loss Prevention est activé dans la configuration des nouveaux tenants. Si la fonctionnalité a été désactivée pendant la création des tenants, les administrateurs partenaires peuvent l'activer ultérieurement.

Pour activer le module Advanced Data Loss Prevention

1. Dans la console de gestion Cloud Cyber Protect, accédez à **Clients**.
2. Sélectionnez le tenant à modifier.
3. Dans la section **Sélectionner des services**, accédez à la zone **Protection**, puis sélectionnez **Advanced Data Loss Prevention** dans le mode de facturation que vous appliquez.
4. Dans Configurer les services, accédez à la section **Advanced Data Loss Prevention** et configurez les quotas.
   Par défaut, le quota est illimité.
5. Enregistrez vos paramètres.

Advanced Security + EDR

La fonctionnalité EDR (Endpoint Detection and Response) détecte toute activité suspecte sur les ressources, y compris les attaques qui n'ont pas été identifiées, et génère des incidents. Ces incidents présentent en détail chaque attaque, ce qui vous permet de comprendre comment l'attaque s'est produite et comment éviter qu'elle se reproduise. Grâce aux interprétations faciles à comprendre de chaque phase de l'attaque, le temps consacré aux enquêtes sur les attaques peut être réduit à quelques minutes.

Activation d'Advanced Security + EDR

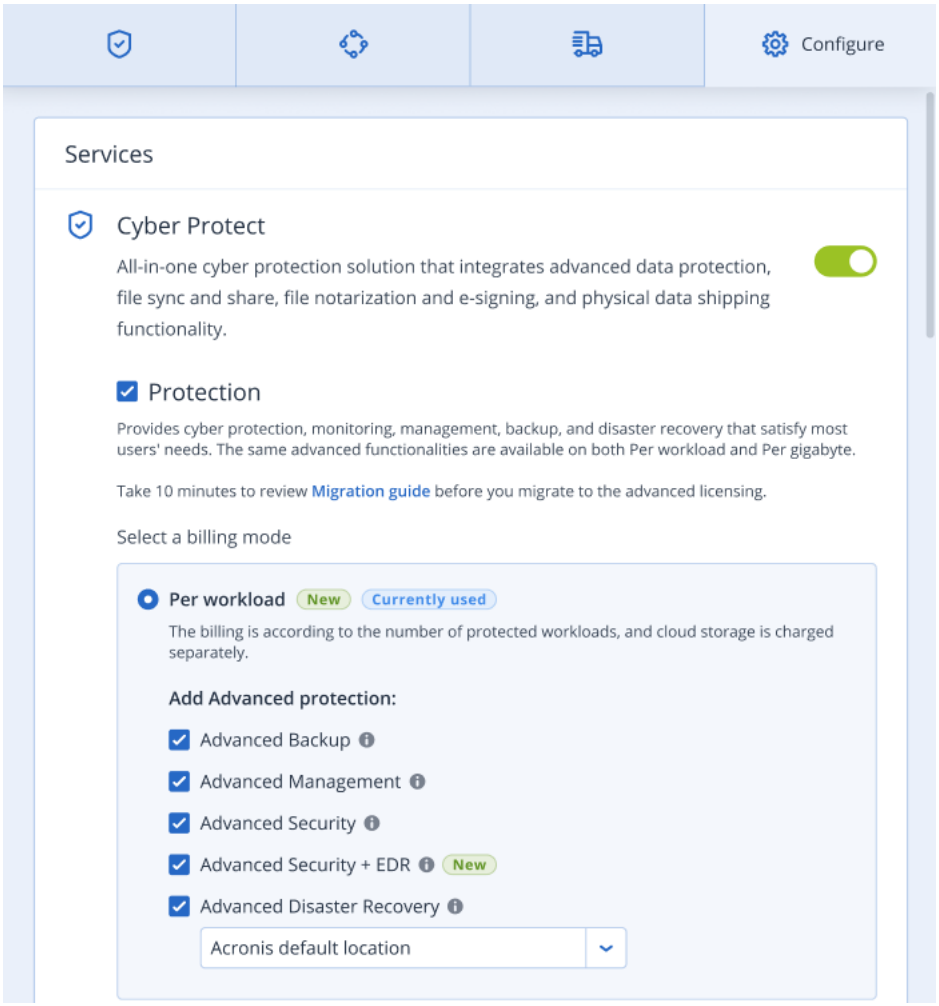
En tant qu'administrateur partenaire, vous pouvez activer le pack de protection Advanced Security + EDR afin de fournir la fonctionnalité EDR (Endpoint Detection and Response) dans les plans de protection du client.

Pour activer le pack Advanced Security + EDR

1. Connectez-vous au portail de gestion.

> **Remarque**
> Si le système vous y invite, sélectionnez les clients auxquels vous souhaitez appliquer le pack de protection Advanced Security + EDR, puis cliquez sur **Activer**.

2. Dans le volet de navigation de gauche, cliquez sur **CLIENTS**.
3. Dans Cyber Protect, cliquez sur l'onglet **Protection**.
   La liste des clients existants abonnés au service Protection s'affiche.
4. Cliquez sur le client pertinent auquel vous souhaitez appliquer le pack Advanced Security + EDR.
   Dans l'onglet **Configurer**, section Protection, vérifiez que la case **Advanced Security + EDR** est cochée.



Advanced - Reprise d'activité après sinistre

Vous pouvez activer le pack Advanced Disaster Recovery et protéger vos charges de travail à l'aide de la fonctionnalité Disaster Recovery complète.

Les fonctionnalités avancées de reprise d'activité après sinistre suivantes sont disponibles :

- Basculement de la production
- Basculement test dans un environnement réseau isolé.
- Nombre de points de récupération disponibles pour le basculement : tous les points de récupération disponibles après la création d'un serveur de restauration.
- Serveurs primaires

- Configurations des serveurs de restauration/primaire : Aucune limite
- Modes de connectivité disponibles : Cloud uniquement, De point à site, OpenVPN de site à site, et VPN IPsec multi-site.
- Disponibilité de la passerelle VPN : toujours disponible.
- Nombre de réseaux Cloud : 23.
- Adresses IP publiques
- Accès Internet
- Opérations avec les runbooks : création, édition et exécution.

Advanced - Sécurité e-mail

Le pack Advanced Email Security fournit une protection en temps réel pour vos boîtes aux lettres Microsoft 365, Google Workspace ou Open-Xchange :

- Anti-malware et antispam
- Analyse d'URL dans les e-mails
- Analyse DMARC
- Anti-hameçonnage
- Protection contre l'usurpation d'identité
- Analyse des pièces jointes
- Désarmement et reconstruction du contenu
- Schéma de confiance

Pour en savoir plus sur Advanced Email Security dans la fiche solution Advanced Email Security.

Pour obtenir des instructions de configuration, voir Advanced Email Security avec Perception Point.

Intégrations

Intégration à des systèmes tiers

Un fournisseur de services peut intégrer un système tiers à Cloud Cyber Protect de la façon suivante :

- En définissant une extension de plate-forme dans ce système.

  La page d'**Intégration** du portail de gestion répertorie les extensions de listes disponibles pour les Automatisations de services professionnels (Professional Services Automations - PSA) et systèmes de Surveillance et gestion à distance (Remote Monitoring and Management - RMM) les plus répandus.

  C'est ce qui est recommandé pour intégrer la plate-forme.
- En créant un client d'API pour le système et en permettant ainsi au système d'accéder aux interfaces de programmation d'application (API) de la plate-forme et à ses services. Les clients d'API font partie de l'infrastructure d'autorisation OAuth 2.0 de la plate-forme. Pour plus d'informations à propos d'OAuth 2.0, visitez https://tools.ietf.org/html/rfc6749.

  Cette façon d'intégrer la plate-forme nécessite des compétences de programmation basiques. Nous vous recommandons de la choisir lorsqu'il n'existe aucune extension de plate-forme pour le système, ou que le système doit être personnalisé pour répondre à des cas dans lesquels la gestion de la plate-forme et de ses services n'est pas couverte par l'extension disponible.

Configuration d'une intégration pour Cloud Cyber Protect

1. Connectez-vous au portail de gestion.
2. Dans le menu de navigation principal, accédez à **Intégrations**.
3. Cliquez sur le nom du système tiers avec lequel vous souhaitez activer l'intégration.
4. Suivez les instructions affichées à l'écran.

Pour plus d'informations sur les intégrations disponibles avec des systèmes tiers, y compris la documentation, à cette adresse : https://solutions.acronis.com.

Gestion des clients d'API

Des systèmes tiers peuvent être intégrés à Cloud Cyber Protect en utilisant ses interfaces de programmation d'application (API). L'accès à ces API est fourni par des clients d'API, qui font partie intégrante de l'infrastructure d'autorisation OAuth 2.0 de la plate-forme.

Qu'est-ce qu'un client d'API ?

Un client d'API est un compte de plate-forme spécial dont le but est de représenter un système tiers nécessitant de s'authentifier et d'être autorisé à accéder à des données dans les API des plates-formes et de ses services.

L'accès du client est limité à un locataire, dans lequel l'administrateur crée le client, et à ses sous-locataires.

Lors de sa création, le client hérite des rôles de service du compte administrateur, et ces rôles ne peuvent pas être modifiés ultérieurement. Modifier les rôles d'un compte administrateur ou le désactiver n'affecte pas le client.

Les identifiants du client consistent en un identificateur unique (ID) et une valeur de code secret. Les identifiants n'expirent pas et ne peuvent pas servir à se connecter au portail de gestion ou à une console de service. La valeur du code secret peut être réinitialisée.

Il est impossible d'activer l'authentification à deux facteurs pour le client.

Procédure d'installation typique

1. Un administrateur crée un client d'API dans le locataire, qu'un système tiers gèrera.
2. L'administrateur active le flux d'identifiants du client OAuth 2.0 dans le système tiers.
   En fonction de ce flux, avant d'accéder au locataire et à ses services via l'API, le système doit d'abord envoyer les identifiants du client créé à la plate-forme à l'aide de l'API d'autorisation. La plate-forme génère et envoie un jeton de sécurité, c'est-à-dire la chaîne chiffrée unique attribuée à ce client en particulier. Le système doit ensuite ajouter ce jeton à toutes les demandes d'API.
   Un jeton de sécurité élimine le besoin de passer par des demandes d'API pour obtenir les identifiants du client. Pour plus de sécurité, le jeton expire au bout de deux heures. Une fois ce délai écoulé, toutes les demandes d'API effectuées avec le jeton expiré échoueront, et le système devra demander un nouveau jeton à la plate-forme.

Pour plus d'informations à propos de l'utilisation des API d'autorisation et de plate-forme, reportez-vous au guide du développeur à l'adresse https://developer.acronis.com/doc/account-management/v2/guide/index.

Création d'un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients d'API** > **Créer un client d'API**.
3. Saisissez un nom pour le client d'API.
4. Cliquez sur **Suivant**.
   Le client d'API est créé avec l'état **Activé** par défaut.
5. Copiez et enregistrez l'ID et le code secret du client, ainsi que l'URL du centre de données. Vous en aurez besoin pour activer le flux d'identifiant du client OAuth 2.0 dans un système tiers.

   Important
   Pour des raisons de sécurité, la valeur du code secret ne s'affiche qu'une seule fois. Il n'existe aucun moyen de récupérer cette valeur si vous la perdez, vous serez obligé de la réinitialiser.

6. Cliquez sur **Valider**.

Réinitialiser la valeur du code secret d'un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis cliquez sur **Réinitialiser le code secret**.
5. Confirmez votre choix en cliquant sur **Suivant**.
   Un nouveau code secret sera généré. L'ID du client et l'URL du centre de données ne changeront pas.
   Tous les jetons de sécurité attribués à ce client expireront immédiatement et les demandes d'API pour ces jetons échoueront.
6. Copiez et enregistrez la valeur du nouveau code secret du client.

   Important
   Pour des raisons de sécurité, la valeur du code secret ne s'affiche qu'une seule fois. Il n'existe aucun moyen de récupérer cette valeur si vous la perdez, vous serez obligé de la réinitialiser.

7. Cliquez sur **Valider**.

Désactiver un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis sur **Désactiver**.
5. Confirmez votre choix.
   L'état du client changera pour **Désactivé**.
   Toutes les demandes effectuées avec des jetons de sécurité attribués à ce client échoueront, mais les jetons n'expireront pas immédiatement. Désactiver le client n'affecte pas le délai d'expiration des jetons.
   Il sera possible de réactiver le client à tout moment.

Activation d'un client d'API désactivé

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur  , puis sur **Activer**.

L'état du client changera pour **Activé**.

Les demandes effectuées avec des jetons de sécurité attribués à ce client réussiront si ces jetons n'ont pas encore expiré.

Suppression d'un client d'API

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Clients de l'API**.
3. Trouvez le client requis dans la liste.
4. Cliquez sur , puis sur **Supprimer**.
5. Confirmez votre choix.

   Tous les jetons de sécurité attribués à ce client expireront immédiatement et les demandes d'API pour ces jetons échoueront.

Important
Il est impossible de restaurer un client supprimé.

Références relatives à l'intégration

Le tableau suivant répertorie les intégrations implémentées avec des tiers et fournit des liens vers les documentations correspondantes.

NOM D'INTÉGRATION	Afficher en ligne	Ouvrir le PDF
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
Commerce CloudBlue	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf

NOM D'INTÉGRATION	Afficher en ligne	Ouvrir le PDF
ConnectWise Control	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf
ConnectWise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableNsightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
ServiceNow	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-

NOM D'INTÉGRATION	Afficher en ligne	Ouvrir le PDF
		US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

Intégration avec VMware Cloud Director

Un fournisseur de services peut intégrer VMware Cloud Director (anciennement VMware vCloud Director) avec Cloud Cyber Protect et fournir à ses clients une solution de sauvegarde clé en main pour leurs machines virtuelles.

L'intégration inclut les étapes suivantes :

1. Configuration du courtier de message RabbitMQ pour l'environnement VMware Cloud Director.
   RabbitMQ permet la synchronisation des changements apportés à l'environnement VMware Cloud Director vers Cloud Cyber Protect.
2. Installation du plug-in pour VMware Cloud Director.
   Ce plug-in ajoute Cyber Protection à l'interface utilisateur VMware Cloud Director.
3. Déploiement d'un agent de gestion.
   L'agent de gestion mappe automatiquement les organisations VMware Cloud Director aux tenants client dans Cloud Cyber Protect, et les administrateurs de l'organisation aux administrateurs de tenants client. Pour plus d'informations à propos des organisations, consultez Création d'une organisation dans VMware Cloud Director dans la base de connaissances VMware.
   Les tenants client sont créés au sein du tenant partenaire pour lequel l'intégration VMware Cloud Director est configurée. Ces nouveaux tenants client sont en mode **Verrouillé** et ne peuvent pas être gérés par l'administrateur partenaire au sein d' Cloud Cyber Protect.

   Remarque
   Seuls les administrateurs de l'organisation avec une adresse e-mail unique dans VMware Cloud Director sont mappés à Cloud Cyber Protect.

4. Déploiement d'un ou plusieurs agents de sauvegarde.

   L'agent de sauvegarde assure des fonctionnalités de sauvegarde et de restauration pour les machines virtuelles de l'environnement VMware Cloud Director.

Pour désactiver l'intégration entre VMware Cloud Director et Cloud Cyber Protect, contactez l'équipe d'assistance technique.

Limites

- L'intégration à VMware Cloud Director est uniquement possible pour les tenants partenaire avec le mode de gestion **Géré par le fournisseur de services**, dont le tenant parent (le cas échéant) utilise aussi le mode de gestion **Géré par le fournisseur de services**. Pour plus d'informations sur les types de tenants et leur mode de gestion, consultez "Création d'un locataire" (p. 35).

  Tous les partenaires directs existants peuvent configurer une intégration avec VMware Cloud Director. Les administrateurs partenaires peuvent activer cette option pour les sous-tenants également, en cochant la case **Infrastructure VMware Cloud Director appartenant à un partenaire** lors de la création d'un tenant partenaire enfant.
- L'authentification à deux facteurs doit être désactivée pour le tenant partenaire dans lequel l'intégration avec VMware Cloud Director est configurée.
- Un administrateur qui a le rôle d'administrateur de l'organisation dans plusieurs organisations VMware Cloud Director ne peut gérer la sauvegarde et la restauration que d'un seul tenant client dans Cyber Protection.
- La console Web Cyber Protection s'ouvre dans un nouvel onglet.

Exigences logicielles

Versions de VMware Cloud Director prises en charge

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

Navigateurs Web pris en charge

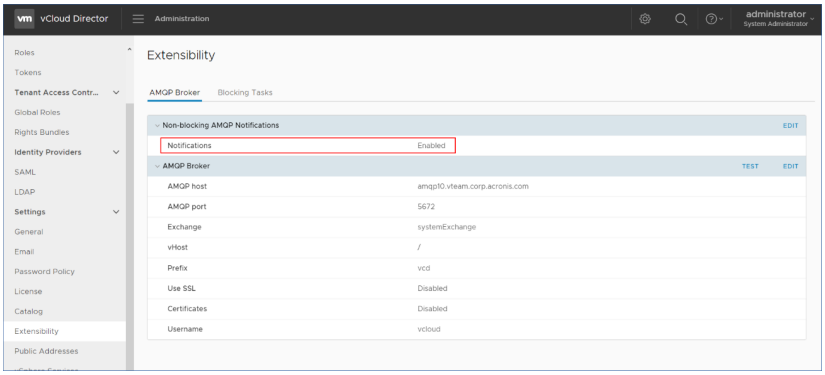
- Google Chrome 29 ou version ultérieure
- Mozilla Firefox 23 ou version ultérieure
- Opera 16 ou version ultérieure
- Microsoft Edge 25 ou version ultérieure
- Safari 8 ou version ultérieure s'exécutant sur les systèmes d'exploitation macOS et iOS

Il est possible que les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) n'affichent pas correctement l'interface utilisateur ou ne proposent pas certaines fonctions.

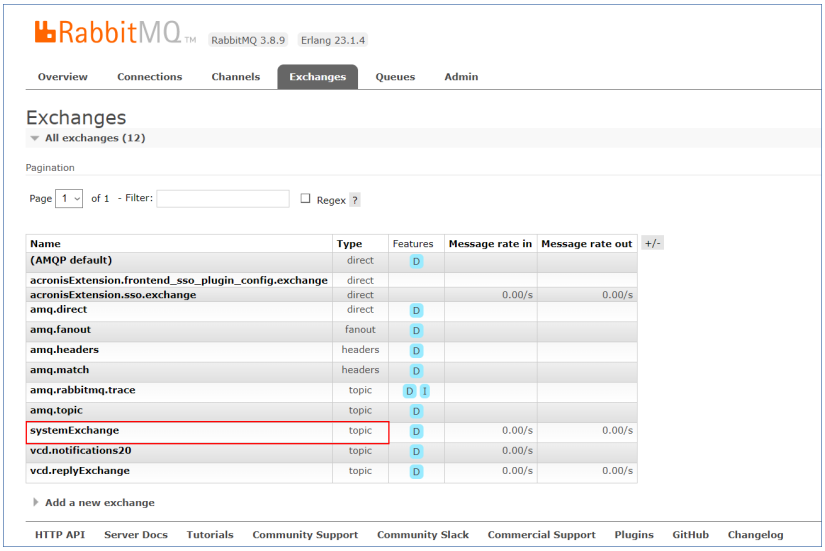
Configuration du courtier de message RabbitMQ

1. Installez un courtier AMPQ pour votre environnement VMware Cloud Director.

   Pour en savoir plus sur l'installation de RabbitMQ, reportez-vous à la documentation VMware : Installer et configurer un courtier AMPQ RabbitMQ.
2. Connectez-vous au portail de fournisseur VMware Cloud Director en tant qu'administrateur système.
3. Accédez à **Administration** > **Extensibilité**, puis vérifiez sous **Notifications AMQP non bloquantes**, que les **Notifications** sont activées.



4. Connectez-vous à la console de gestion RabbitMQ en tant qu'administrateur.
5. Sous l'onglet **Exchanges**, vérifiez que l'exchange (nommé **SystemExchange** par défaut) est créé et que son type est **topic**.



Installation du plug-in pour VMware Cloud Director

1. Cliquez sur le lien suivant pour télécharger le fichier **vCDPlugin.zip** : https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Connectez-vous au portail de fournisseur VMware Cloud Director en tant qu'administrateur système.

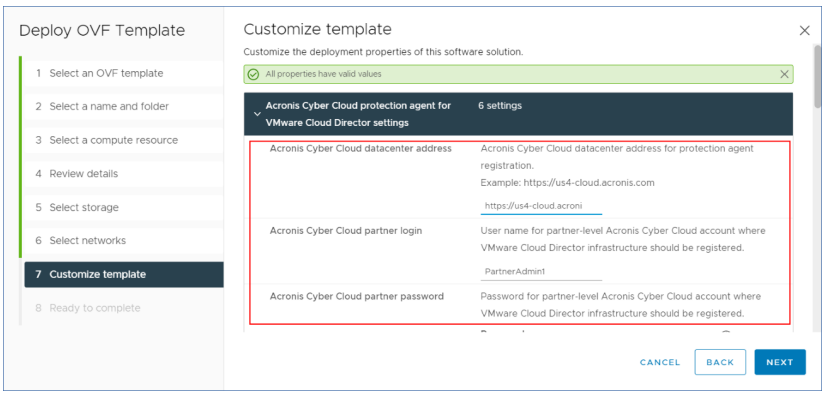
3. Depuis le menu de navigation, sélectionnez **Personnaliser le portail**.
4. Sous l'onglet **Gérer les plug-ins**, cliquez sur **Télécharger**.
   L'assistant de **Téléchargement de plug-in** s'affiche.
5. Cliquez sur **Sélectionner le fichier de plug-in**, puis sélectionnez le fichier **vCDPlugin.zip**.
6. Cliquez sur **Suivant**.
7. Configurer la portée et la publication :
   a. Dans la section **Portée vers**, ne cochez que la case **Tenants**.
   b. Dans la section **Publier vers**, sélectionnez **Tous les tenants** pour activer le plug-in pour tous les tenants existants et futurs, ou sélectionnez les tenants individuels pour lesquels vous souhaitez activer le plug-in.
8. Cliquez sur **Suivant**.
9. Vérifiez vos paramètres, puis cliquez sur **Terminer**.

Installation d'un agent de gestion

1. Connectez-vous au portail de gestion Cloud Cyber Protect en tant qu'administrateur partenaire.
2. Accédez à **Paramètres** > **Emplacement**, puis cliquez sur **Ajouter VMware Cloud Director**.
3. Cliquez sur le lien de l'**agent de gestion** et téléchargez le fichier ZIP.
4. Extrayez le fichier de modèle de l'agent de gestion `vCDManagementAgent.ovf` et le fichier de disque dur virtuel `vCDManagementAgent-disk1.vmdk`.
5. Dans vSphere Client, déployez le modèle OVF d'agent de gestion sur un hôte ESXi sous une instance vCenter gérée par VMware Cloud Director.

   Important
   Installez un seul agent de gestion par environnement VMware Cloud Director.

6. Dans l'assistant **Déployer le modèle OVF**, configurez l'agent de gestion comme suit :



   a. URL du centre de données Cloud Cyber Protect. Par exemple, `https://us5-cloud.example.com`.
   b. Identifiant et mot de passe de l'administrateur partenaire.

c. ID du stockage de sauvegarde des machines virtuelles dans l'environnement VMware Cloud Director. Ce stockage de sauvegarde peut uniquement appartenir à un partenaire. Pour plus de détails sur les stockages, consultez "Gérer les emplacements et le stockage" (p. 70).

   Pour vérifier l'ID, depuis le portail de gestion, accédez à **Paramètres** > **Emplacements**, puis sélectionnez le stockage concerné. Vous trouverez son ID après l'expression **uuid=** de l'URL.

d. Mode de facturation Cloud Cyber Protect : **Par gigaoctet** ou **Par charge de travail**.

   Remarque
   Le mode de facturation sélectionné s'applique à tous les nouveaux tenants client créés.

e. Paramètres VMware Cloud Director : adresse de l'infrastructure, identifiant et mot de passe de l'administrateur.

f. Paramètres RabbitMQ : adresse de serveur, port, nom d'hôte virtuel, identifiant et mot de passe administrateur.

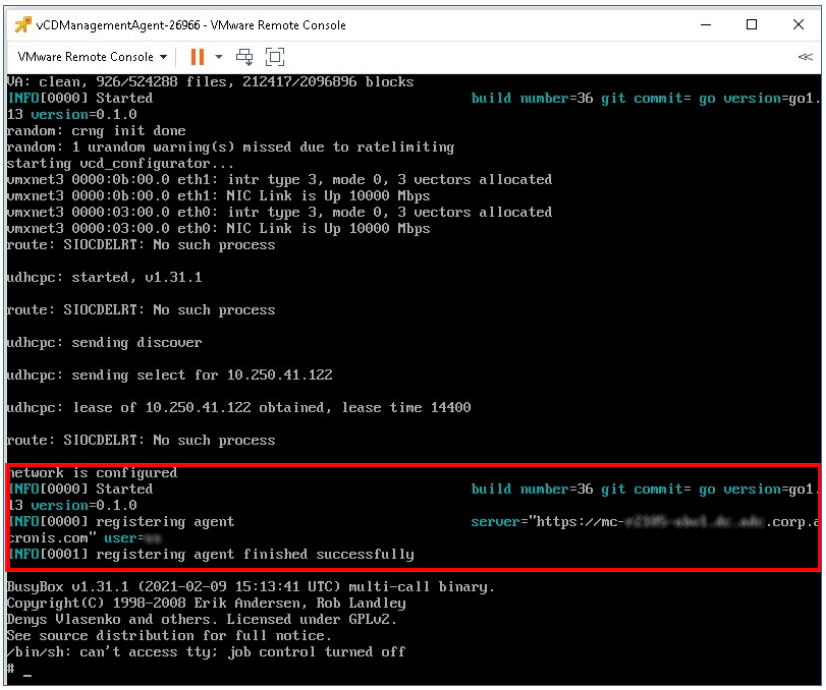
g. Paramètres réseau : adresse IP, masque de sous-réseau, passerelle par défaut, DNS, suffixe DNS.

   Par défaut, une seule l'interface réseau est activée. Pour activer une deuxième interface réseau, cochez la case en regard de **Activer eth1**.

   Remarque
   Assurez-vous que vos paramètres réseau autorisent l'agent de gestion à accéder à la fois à l'environnement VMware Cloud Director et à votre centre de données Cloud Cyber Protect.

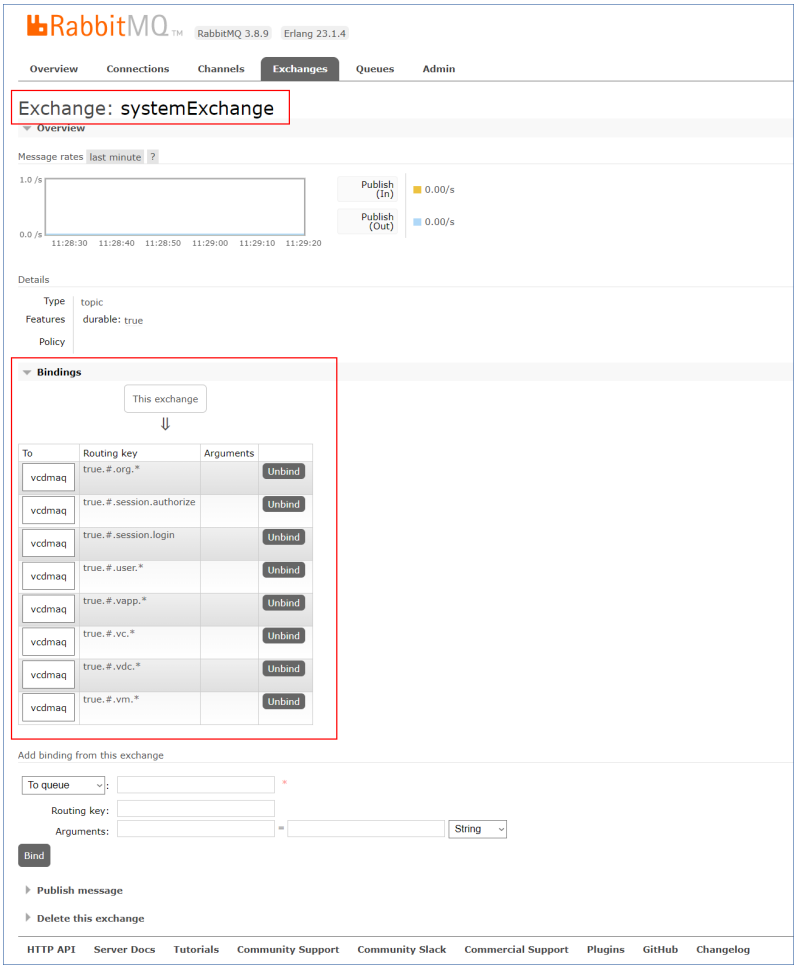
Vous pouvez également configurer les paramètres de l'agent de gestion après le déploiement initial. Dans vSphere Client, mettez hors tension la machine virtuelle avec l'agent de gestion, puis cliquez sur **Configurer** > **Paramètres** > **Options vApp**. Appliquez les paramètres souhaités, puis mettez sous tension la machine virtuelle avec l'agent de gestion.

7. [Facultatif] Dans vSphere Client, ouvrez la console de la machine virtuelle avec l'agent de gestion, puis vérifiez vos paramètres.



8. Vérifier la connexion RabbitMQ.
   a. Connectez-vous à la console de gestion RabbitMQ en tant qu'administrateur.
   b. Dans l'onglet **Exchanges**, sélectionnez l'exchange configuré lors de l'installation RabbitMQ. Par défaut, son nom est **systemExchange**.

c. Vérifiez les liens avec la file d'attente **vcdmaq**.



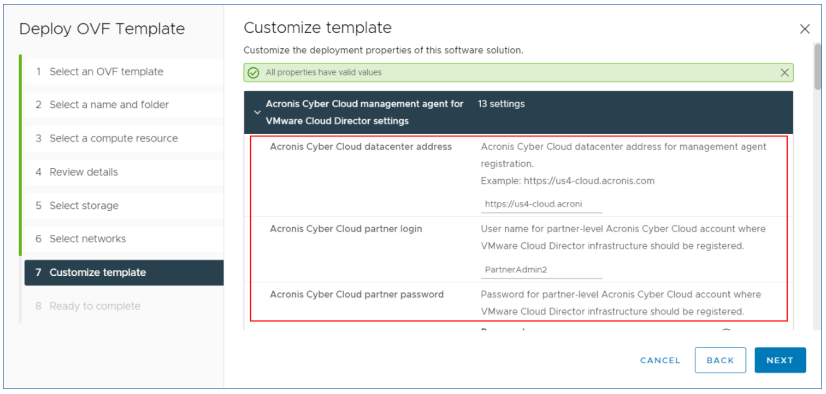
Installation des agents de sauvegarde

1. Connectez-vous au portail de gestion en tant qu'administrateur partenaire.
2. Accédez à **Paramètres** > **Emplacement**, puis cliquez sur **Ajouter VMware Cloud Director**.
3. Cliquez sur le lien de l'**agent de sauvegarde** et téléchargez le fichier ZIP.
4. Extrayez le fichier de modèle de l'agent de sauvegarde `vCDCyberProtectAgent.ovf` et le fichier de disque dur virtuel `vCDCyberProtectAgent-disk1.vmdk`.
5. Dans vSphere Client, déployez le modèle d'agent de sauvegarde sur l'hôte ESXi désiré.

   Il vous faut au moins un agent de sauvegarde par hôte. Par défaut, 8 Go de RAM et 2 CPU sont attribués à l'agent de sauvegarde, et il peut traiter jusqu'à 10 tâches de sauvegarde ou de récupération simultanément. Pour traiter plus de tâches ou pour redistribuer le trafic de sauvegarde et de récupération, déployez d'autres agents de sauvegarde sur le même hôte.

   Remarque
   Les sauvegardes de machines virtuelles sur les hôtes ESXi sur lesquels aucun agent de sauvegarde n'est installé échouent et retournent l'erreur « Délai d'attente de tâche expiré ».

6. Dans l'assistant **Déployer le modèle OVF**, configurez l'agent de sauvegarde comme suit :



   a. URL du centre de données Cloud Cyber Protect. Par exemple, `https://us5-cloud.example.com`.
   b. Identifiant et mot de passe de l'administrateur partenaire.
   c. Paramètres de vCenter VMware : adresse de serveur, identifiant et mot de passe.

      L'agent utilisera ces identifiants pour se connecter à vCenter Server. Nous vous conseillons d'utiliser un compte avec un rôle **Administrateur**. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server.
   d. Paramètres réseau : adresse IP, masque de sous-réseau, passerelle par défaut, DNS, suffixe DNS.

      Par défaut, une seule l'interface réseau est activée. Pour activer une deuxième interface réseau, cochez la case en regard de **Activer eth1**.

      Remarque
      Assurez-vous que vos paramètres réseau autorisent l'agent de sauvegarde à accéder à la fois au vCenter Server et à votre centre de données Cloud Cyber Protect.

   e. Limite de téléchargement : le débit maximum de téléchargement (en kbit/s), qui définit la vitesse de lecture de l'archive de sauvegarde lors de l'opération de récupération. La valeur par défaut est 0 - illimité.
   f. Limite de transfert : le débit maximum de transfert (en kbit/s), qui définit la vitesse d'écriture de l'archive de sauvegarde lors de l'opération de sauvegarde. La valeur par défaut est 0 - illimité.

   Vous pouvez également configurer les paramètres de l'agent de sauvegarde après le déploiement initial. Dans vSphere Client, mettez hors tension la machine virtuelle avec l'agent de sauvegarde, puis cliquez sur **Configurer** > **Paramètres** > **Options vApp**. Appliquez les paramètres souhaités, puis mettez sous tension la machine virtuelle avec l'agent de sauvegarde.
7. Dans vSphere Client, assurez-vous que l'**Hôte** et **Storage vMotion** sont désactivés pour la machine virtuelle avec l'agent de sauvegarde.

Mise à jour des agents

Pour mettre à jour un agent de gestion

1. Connectez-vous au portail de gestion Cloud Cyber Protect en tant qu'administrateur partenaire.
2. Accédez à **Paramètres** > **Emplacement**, puis cliquez sur **Ajouter VMware Cloud Director**.
3. Cliquez sur le lien de l'**agent de gestion** et téléchargez le fichier ZIP du dernier agent.
4. Extrayez le fichier de modèle de l'agent de gestion `vCDManagementAgent.ovf` et le fichier de disque dur virtuel `vCDManagementAgent-disk1.vmdk`.
5. Dans vSphere Client, mettez hors tension la machine virtuelle avec l'agent de gestion actuel.
6. Déployez une machine virtuelle avec le nouvel agent de gestion en utilisant les derniers fichiers `vCDManagementAgent.ovf` et `vCDManagementAgent-disk1.vmdk`.
7. Configurez l'agent de gestion selon les mêmes paramètres que l'ancien.
8. [Facultatif] Supprimez la machine virtuelle avec l'ancien agent de gestion.

Important
Vous ne devez avoir qu'un seul agent de gestion actif par environnement VMware Cloud Director.

Pour mettre à jour un agent de sauvegarde

1. Connectez-vous au portail de gestion Cloud Cyber Protect en tant qu'administrateur partenaire.
2. Accédez à **Paramètres** > **Emplacement**, puis cliquez sur **Ajouter VMware Cloud Director**.
3. Cliquez sur le lien de l'**agent de sauvegarde** et téléchargez le fichier ZIP du dernier agent.
4. Extrayez le fichier de modèle de l'agent de sauvegarde `vCDCyberProtectAgent.ovf` et le fichier de disque dur virtuel `vCDCyberProtectAgent-disk1.vmdk`.
5. Dans vSphere Client, mettez hors tension la machine virtuelle avec l'agent de sauvegarde actuel.
   Toutes les tâches de sauvegarde et de récupération en cours d'exécution échoueront. Pour vérifier si des tâches sont en cours d'exécution, dans vSphere Client, ouvrez la console de la machine virtuelle avec l'agent de sauvegarde, puis exécutez la commande `ps | grep esx_worker`. Assurez-vous qu'il n'y a pas de processus `esx_worker` actif.
6. Déployez une machine virtuelle avec le nouvel agent de sauvegarde en utilisant les fichiers `vCDCyberProtectAgent.ovf` et `vCDCyberProtectAgent-disk1.vmdk` les plus récents.
7. Configurez l'agent de sauvegarde selon les mêmes paramètres que l'ancien.
8. [Facultatif] Supprimez la machine virtuelle avec l'ancien agent de sauvegarde.

Accéder à la console Web Cyber Protection

Les administrateurs suivants peuvent gérer la sauvegarde des machines virtuelles dans les organisations VMware Cloud Director :

- Administrateurs de l'organisation
- Administrateurs de sauvegarde spécialement affectés
  Pour en savoir plus sur la création d'un tel administrateur, reportez-vous à "Création d'un administrateur de sauvegarde" (p. 151).

Les administrateurs peuvent accéder à la console Web Cyber Protection personnalisée en cliquant sur **Cyberprotection** dans le menu de navigation du portail de tenant VMware Cloud Director.

Remarque
L'authentification unique est uniquement disponible pour les administrateurs de l'organisation et n'est pas prise en charge pour les administrateurs système qui utilisent le portail de tenant VMware Cloud Director.

Dans la console Web Cyber Protection, les administrateurs peuvent seulement accéder à leurs propres éléments de l'organisation VMware Cloud Director : centres de données virtuels, vApps et machines virtuelles individuelles. Ils peuvent gérer la sauvegarde et la restauration des ressources d'organisation VMware Cloud Director.

Les administrateurs partenaires peuvent accéder aux consoles Web Cyber Protection de leurs tenants client et peuvent gérer la sauvegarde et la restauration en leur nom.

Limites

La liste des limitations est sujette aux modifications apportées aux prochaines versions de Cloud Cyber Protect.

Sauvegarde

- Seules les sauvegardes complètes de machine sont prises en charge. Les filtres de fichiers et la sélection de disques ou volumes ne sont pas disponibles.
- Seul le stockage dans le Cloud est pris en charge comme emplacement de sauvegarde. Le stockage est configuré dans les paramètres de l'agent de gestion et les utilisateurs ne peuvent pas le modifier depuis le plan de protection.
- Les groupes dynamiques ne sont pas pris en charge.
- Les modèles de sauvegarde suivants sont pris en charge : **Sauvegarde toujours incrémentielle (fichier unique)**, **Sauvegarde toujours complète** et **Sauvegarde complète hebdomadaire, incrémentielle quotidienne**.
- Seul le nettoyage après la sauvegarde est pris en charge.

Restauration

- Seule la restauration à la machine virtuelle d'origine est prise en charge. La machine virtuelle d'origine doit être présente dans l'environnement VMware Cloud Director.
- La restauration au niveau des fichiers n'est pas prise en charge.

Création d'un administrateur de sauvegarde

Les administrateurs de l'organisation peuvent déléguer la gestion de la sauvegarde à des administrateurs de sauvegarde spécialement affectés.

Pour créer un administrateur de sauvegarde

1. Dans le portail de tenant VMware Cloud Director, cliquez sur **Administration** > **Rôles** > **Nouveau**.
2. Dans la fenêtre **Ajouter un rôle**, spécifiez un nom et une description pour le nouveau rôle.
3. Faites défiler la liste de permissions, puis sous **Autres**, sélectionnez **Opérateur de sauvegarde de MV en libre-service**.

   Remarque
   La permission **Opérateur de sauvegarde de MV en libre-service** devient disponible après que vous avez installé le plug-in pour VMware Cloud Director. Pour en savoir plus sur la façon de procéder, reportez-vous à "Installation du plug-in pour VMware Cloud Director" (p. 144).

4. Dans le portail de tenant VMware Cloud Director, cliquez sur **Utilisateurs**.
5. Sélectionnez un utilisateur, puis cliquez sur **Modifier**.
6. Affectez cet utilisateur au nouveau rôle que vous avez créé.

En conséquence, l'utilisateur sélectionné pourra de nouveau gérer les sauvegardes des machines virtuelles de cette organisation.

Remarque
Les administrateurs système de l'environnement VMware Cloud Director peuvent définir un rôle global avec la permission **Opérateur de sauvegarde de MV en libre-service** activée, puis publier ce rôle pour les tenants. Ainsi, les administrateurs de l'organisation auront seulement besoin d'affecter le rôle à un utilisateur.

Rapport système, fichiers journaux et fichiers de configuration

À des fins de dépannage, il vous faudra peut-être créer un rapport système en utilisant l'outil `sysinfo`, ou vérifier les fichiers journaux et de configuration sur une machine virtuelle avec l'agent.

Vous pouvez accéder à la machine virtuelle, soit directement, en ouvrant sa console dans vSphere Client, ou à distance, via un client SSH. Pour accéder à la machine virtuelle via un client SSH, vous devez d'abord activer la connexion SSH vers cette machine.

Pour activer la connexion SSH vers une machine virtuelle

1. Dans vSphere Client, ouvrez la console de la machine virtuelle avec l'agent.
2. À l'invite de commandes, exécutez la commande suivante : `/bin/sshd` pour démarrer le démon SSH.

Ce faisant, vous pourrez vous connecter à cette machine virtuelle en utilisant un client SSH, comme WinSCP.

Pour exécuter l'outil `sysinfo`

1. Accédez à la machine virtuelle avec l'agent.
   - Pour y accéder directement, dans vSphere Client, ouvrez la console de la machine virtuelle avec l'agent.
   - Pour y accéder à distance, connectez-vous à la machine virtuelle via un client SSH.

     Utilisez la combinaison identifiant:mot de passe par défaut suivante : `root`:`root`.
2. Accédez au répertoire `/bin`, puis exécutez l'outil `sysinfo`.

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

   Ce faisant, un rapport système sera enregistré dans le répertoire par défaut : `/var/lib/Acronis/sysinfo`.

   Vous pouvez spécifier un autre répertoire en exécutant l'outil `sysinfo` avec l'option `--target_dir`.

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```
3. Téléchargez le rapport système généré en utilisant un client SSH.

Pour accéder à un fichier journal ou de configuration

1. Connectez-vous à la machine virtuelle via un client SSH.

   Utilisez la combinaison identifiant:mot de passe par défaut suivante : `root`:`root`.
2. Téléchargez le fichier souhaité.

   Vous pouvez trouver les fichiers journaux sous les emplacements suivants :
   - Agent de sauvegarde : `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Agent de gestion : `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   Vous pouvez trouver les fichiers de configuration sous les emplacements suivants :
   - Agent de sauvegarde : `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Agent de gestion : `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Suppression de l'intégration à VMware Cloud Director

Le rétablissement de la configuration et la désinscription de l'instance VMware Cloud Director de Cloud Cyber Protect est une procédure complexe. Veuillez contacter votre représentant du support pour obtenir de l'aide.

Paramètres de confidentialité

Les paramètres de confidentialité vous aident à indiquer si vous donnez ou non votre consentement pour la collecte, l'utilisation et la divulgation de vos informations personnelles.

En fonction du pays dans lequel vous utilisez Cyber Protect et du centre de données Cloud Cyber Protect qui vous fournit des services, lors du lancement initial de Cyber Protect vous serez peut-être invité à confirmer si vous acceptez ou non d'utiliser Google Analytics dans Cyber Protect.

Google Analytics nous aide à mieux comprendre le comportement des utilisateurs et à leur offrir une meilleure expérience dans Cyber Protect en collectant des données avec pseudonyme.

Si le consentement et les menus Google Analytics n'apparaissent pas dans l'interface Cyber Protect, cela signifie que Google Analytics n'est pas utilisé dans votre pays.

Si vous avez activé ou refusé d'activer Google Analytics lors du lancement initial de Cyber Protect, vous pouvez changer d'avis ultérieurement.

Activer ou désactiver Google Analytics

1. Dans la console Cyber Protect, cliquez sur l'icône de compte dans l'angle supérieur droit.
2. Sélectionnez **Mes paramètres de confidentialité**.
3. Dans la section **Collecte de données Google Analytics**, cliquez sur l'un des boutons suivants :
   - **Activé** pour activer Google Analytics
   - **Désactivé** pour désactiver Google Analytics

Index

F

G

H

I

J

L

M

N

O

P

Q

R